

PRTG Network Monitor User Manual



Bandwidth monitoring | Availability monitoring | Usage monitoring

PRTG Network Monitor User Manual

© 2014 Paessler AG

All rights reserved. No parts of this work may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems—without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: April 2014 in Nuremberg

Table of Contents

Part 1 Welcome to PRTG Network Monitor	14
1 About this Document	15
2 Key Features	16
3 New in This Version	18
4 Available Licenses	19
5 System Requirements	21
Detailed System Requirements	23
Part 2 Quick Start Guide	32
1 ONE—Download, Installation, and First Login	33
2 TWO—Using the Configuration Guru	36
Part 3 Installing the Software	44
1 Download PRTG	45
2 Update From Previous Versions	47
3 Install a PRTG Core Server	51
4 Install a PRTG Cluster	56
5 Enter a License Key	57
6 Activate the Product	60
7 Install a PRTG Remote Probe	62
8 Install the Enterprise Console	67
9 Uninstall PRTG Products	71
Part 4 Understanding Basic Concepts	76
1 Architecture and User Interfaces	77
2 Clustering	81
3 Object Hierarchy	83
4 Inheritance of Settings	87
5 Tags	89
6 Dependencies	90
7 Scheduling	91
8 Notifying	92
9 Data Reporting	93
10 User Access Rights	94
11 IPv6	97
Part 5 Ajax Web Interface—Basic Procedures	100
1 Login	102
2 SSL Certificate Warning	105
3 General Layout	108

4	Sensor States	121
5	Review Monitoring Data	124
6	Compare Sensors	129
7	Historic Data Reports	132
8	Similar Sensors	137
9	Object Settings	141
10	Alarms	143
11	Logs	146
12	Tickets	148
13	Working with Table Lists	155
14	Object Selector	158
15	Priority and Favorites	159
16	Pause	161
17	Context Menus	162
18	Hover Popup	173
19	Main Menu Structure	174
Part 6	Ajax Web Interface—Device and Sensor Setup	188
1	Auto-Discovery	190
2	Create Objects Manually	204
	Add a Group	205
	Add a Device	211
	Add a Sensor	220
3	Manage Device Tree	222
4	Root Group Settings	224
5	Probe Settings	238
6	Group Settings	253
7	Device Settings	272
8	Sensor Settings	290
	List of Available Sensor Types	291
	Active Directory Replication Errors Sensor	308
	ADO SQL Sensor	315
	Amazon CloudWatch Sensor	322
	AVM FRITZ!Box WAN Interface Sensor	330
	Cisco IP SLA Sensor	336
	Citrix XenServer Host Sensor	342
	Citrix XenServer Virtual Machine Sensor	348
	Cluster Probe Health Sensor	354
	Core Health Sensor	358
	Dell PowerVault MDi Sensor	362
	DHCP Sensor	368
	DNS Sensor	375
	Enterprise Virtual Array Sensor	381
	Event Log (Windows API) Sensor	388
	Exchange Backup (Powershell) Sensor	396
	Exchange Database (Powershell) Sensor	403
	Exchange Mailbox (Powershell) Sensor	410
	Exchange Mail Queue (Powershell) Sensor	417

Contents

Exchange Public Folder (Powershell) Sensor	423
EXE/Script Sensor	430
EXE/Script Advanced Sensor	439
File Sensor	447
File Content Sensor	453
Folder Sensor	459
FTP Sensor	465
FTP Server File Count Sensor	471
Google Analytics Sensor	477
HTTP Sensor	484
HTTP Advanced Sensor	491
HTTP Apache ModStatus PerfStats Sensor	503
HTTP Apache ModStatus Totals Sensor	510
HTTP Content Sensor	517
HTTP Full Web Page Sensor	526
HTTP Push Count Sensor	533
HTTP Push Data Sensor	539
HTTP SSL Certificate Expiry Sensor	545
HTTP Transaction Sensor	551
HTTP XML/REST Value Sensor	561
Hyper-V Cluster Shared Volume Disk Free Sensor	572
Hyper-V Host Server Sensor	579
Hyper-V Virtual Machine Sensor	585
Hyper-V Virtual Network Adapter Sensor	593
Hyper-V Virtual Storage Device Sensor	600
IMAP Sensor	607
INI File Content Check Sensor	618
IP on DNS Blacklist Sensor	624
IPFIX Sensor	630
IPFIX (Custom) Sensor	638
jFlow V5 Sensor	646
jFlow V5 (Custom) Sensor	654
LDAP Sensor	662
Microsoft SQL Sensor	667
MySQL Sensor	675
NetFlow V5 Sensor	682
NetFlow V5 (Custom) Sensor	690
NetFlow V9 Sensor	698
NetFlow V9 (Custom) Sensor	706
Oracle SQL Sensor	714
Packet Sniffer Sensor	722
Packet Sniffer (Custom) Sensor	729
Passive Application Performance Sensor	736
PerfCounter Custom Sensor	742
PerfCounter IIS Application Pool Sensor	749
Ping Sensor	756
Ping Jitter Sensor	762
Pingdom Sensor	767
POP3 Sensor	773
POP3 Email Count Sensor	779
Port Sensor	785

Port Range Sensor	792
Probe Health Sensor	797
QoS (Quality of Service) One Way Sensor	801
QoS (Quality of Service) Round Trip Sensor	807
RADIUS Sensor	813
RDP (Remote Desktop) Sensor	818
SCVMM Host Sensor	823
SCVMM Virtual Machine Sensor	830
Sensor Factory Sensor	837
sFlow Sensor	852
sFlow (Custom) Sensor	860
SFTP Secure File Transfer Protocol Sensor	868
Share Disk Free Sensor	874
SIP Options Ping Sensor	880
SMTP Sensor	886
SMTP&IMAP Round Trip Sensor	892
SMTP&POP3 Round Trip Sensor	900
SNMP APC Hardware Sensor	908
SNMP Cisco ADSL Sensor	914
SNMP Cisco ASA VPN Connections Sensor	919
SNMP Cisco ASA VPN Traffic Sensor	924
SNMP Cisco ASA VPN Users Sensor	929
SNMP Cisco CBQoS Sensor	934
SNMP Cisco System Health Sensor	939
SNMP Cisco UCS Chassis Sensor	945
SNMP Cisco UCS Physical Disk Sensor	951
SNMP Cisco UCS System Health Sensor	957
SNMP CPU Load Sensor	963
SNMP Custom Sensor	968
SNMP Custom String Sensor	975
SNMP Dell Hardware Sensor	983
SNMP Dell PowerEdge Physical Disk Sensor	989
SNMP Dell PowerEdge System Health Sensor	995
SNMP Disk Free Sensor	1001
SNMP GSA System Health Sensor	1007
SNMP Hardware Status Sensor	1012
SNMP HP LaserJet Hardware Sensor	1017
SNMP HP ProLiant Logical Disk Sensor	1023
SNMP HP ProLiant Memory Controller Sensor	1029
SNMP HP ProLiant Network Interface Sensor	1035
SNMP HP ProLiant Physical Disk Sensor	1041
SNMP HP ProLiant System Health Sensor	1047
SNMP IBM System X Logical Disk Sensor	1053
SNMP IBM System X Physical Disk Sensor	1059
SNMP IBM System X Physical Memory Sensor	1065
SNMP IBM System X System Health Sensor	1071
SNMP interSeptor Pro Environment Sensor	1077
SNMP LenovoEMC Physical Disk Sensor	1083
SNMP LenovoEMC System Health Sensor	1089
SNMP Library Sensor	1094
SNMP Linux Disk Free Sensor	1102

Contents

SNMP Linux Load Average Sensor	1110
SNMP Linux Meminfo Sensor	1115
SNMP Linux Physical Disk Sensor	1120
SNMP Memory Sensor	1128
SNMP NetApp Disk Free Sensor	1134
SNMP NetApp Enclosure Sensor	1140
SNMP NetApp I/O Sensor	1146
SNMP NetApp License Sensor	1152
SNMP NetApp Logical Unit Sensor	1158
SNMP NetApp Network Interface Sensor	1164
SNMP NetApp System Health Sensor	1170
SNMP Poseidon Environment Sensor	1176
SNMP QNAP Logical Disk Sensor	1181
SNMP QNAP Physical Disk Sensor	1186
SNMP QNAP System Health Sensor	1192
SNMP RMON Sensor	1197
SNMP SonicWALL System Health Sensor	1203
SNMP SonicWALL VPN Traffic Sensor	1208
SNMP Synology Logical Disk Sensor	1214
SNMP Synology Physical Disk Sensor	1219
SNMP Synology System Health Sensor	1224
SNMP System Uptime Sensor	1229
SNMP Traffic Sensor	1234
SNMP Trap Receiver Sensor	1241
SNMP Windows Service Sensor	1250
SNTP Sensor	1255
SSH Disk Free Sensor	1260
SSH INodes Free Sensor	1269
SSH Load Average Sensor	1275
SSH Meminfo Sensor	1281
SSH Remote Ping Sensor	1287
SSH SAN Logical Disk Sensor	1294
SSH SAN Physical Disk Sensor	1301
SSH SAN System Health Sensor	1308
SSH Script Sensor	1315
SSH Script Advanced Sensor	1324
SSH VMWare ESX(i) Disk Sensor	1332
Syslog Receiver Sensor	1338
System Health Sensor	1347
TFTP Sensor	1351
Traceroute Hop Count Sensor	1357
Virtuozzo Container Disk Sensor	1363
Virtuozzo Container Network Sensor	1369
VMware Host Hardware (WBEM) Sensor	1375
VMware Host Hardware Status (SOAP) Sensor	1381
VMware Host Performance (SOAP) Sensor	1387
VMware Virtual Machine (SOAP) Sensor	1393
WBEM Custom Sensor	1400
Windows CPU Load Sensor	1406
Windows IIS 6.0 SMTP Received Sensor	1412
Windows IIS 6.0 SMTP Sent Sensor	1418

Windows IIS Application Sensor	1424
Windows Last Update Sensor	1431
Windows Logged In Users Sensor	1437
Windows MSMQ Queue Length Sensor	1443
Windows Network Card Sensor	1450
Windows Pagefile Sensor	1457
Windows Physical Disk Sensor	1463
Windows Print Queue Sensor	1470
Windows Registry Sensor	1476
Windows Scheduled Task Sensor	1484
Windows System Uptime Sensor	1491
Windows Updates Status (Powershell) Sensor	1497
WMI Custom Sensor	1503
WMI Custom String Sensor	1510
WMI Event Log Sensor	1519
WMI Exchange Server Sensor	1527
WMI Exchange Transport Queue Sensor	1534
WMI File Sensor	1541
WMI Free Disk Space (Multi Drive) Sensor	1547
WMI HDD Health Sensor	1555
WMI Logical Disk Sensor	1561
WMI Memory Sensor	1567
WMI Microsoft SQL Server 2005 Sensor (Deprecated)	1572
WMI Microsoft SQL Server 2008 Sensor	1581
WMI Microsoft SQL Server 2012 Sensor	1589
WMI Process Sensor	1597
WMI Remote Ping Sensor	1603
WMI Security Center Sensor	1608
WMI Service Sensor	1614
WMI Share Sensor	1620
WMI SharePoint Process Sensor	1627
WMI Terminal Services (Windows 2008) Sensor	1633
WMI Terminal Services (Windows XP/Vista/2003) Sensor	1638
WMI UTC Time Sensor	1643
WMI Vital System Data (V2) Sensor	1648
WMI Volume Sensor	1654
WMI Volume Fragmentation Sensor	1660
WMI Windows Version Sensor	1667
WSUS Statistics Sensor	1673
9 Additional Sensor Types (Custom Sensors)	1680
10 Sensor Channels Settings	1683
11 Sensor Notifications Settings	1690

Part 7 Ajax Web Interface—Advanced Procedures 1700

1 Toplists	1702
2 Arrange Objects	1707
3 Clone Object	1708
4 Multi-Edit	1710
5 Create Device Template	1715
6 Geo Maps	1718

Contents

7	Notifications	1723
	Setting Up Notifications Based on Sensor Limits: Example	1725
8	Libraries	1733
	Libraries Step By Step	1736
	Management	1740
	Libraries and Node Settings	1742
	Context Menus	1748
9	Reports	1749
	Reports Step By Step	1752
	View and Run Reports	1755
	Reports Settings	1758
10	Maps	1768
	Maps Step By Step	1771
	Maps Designer	1774
	Maps Settings	1780
11	Setup	1784
	Account Settings—My Account	1786
	Account Settings—Notifications	1791
	Account Settings—Schedules	1801
	System Administration—System and Website	1805
	System Administration—Notification Delivery	1815
	System Administration—Probes	1821
	System Administration—Cluster	1823
	System Administration—User Accounts	1824
	System Administration—User Groups	1829
	System Administration—Administrative Tools	1833
	PRTG Status—System Status	1837
	PRTG Status—Auto-Update	1846
	PRTG Status—Cluster Status	1850
	PRTG Status—Activation Status	1851
	Optional Downloads and Add-Ons	1852
	Chrome Desktop Notifications	1854
	Support—Contact Support	1856

Part 8 Enterprise Console 1860

1	First Start	1863
2	General Layout	1864
3	Menu Tabs and Page Content	1868
	Devices	1869
	Libraries	1876
	Sensors	1878
	Alarms	1880
	Maps	1882
	Reports	1884
	Logs	1886
	Tickets	1888
	Setup	1890
	Search Results	1892
4	PRTG Servers	1893
5	Options	1896

6	Windows Menu Structure	1902
7	Context Menus	1907
8	Shortcuts Overview	1908
Part 9	Other User Interfaces	1912
1	Mobile Web GUI	1913
2	Smartphone Apps	1916
Part 10	Sensor Technologies	1922
1	Monitoring via SNMP	1923
2	Monitoring via WMI	1927
3	Monitoring via SSH	1930
4	Monitoring Bandwidth via Packet Sniffing	1932
5	Monitoring Bandwidth via Flows	1934
6	Bandwidth Monitoring Comparison	1937
7	Monitoring Quality of Service and VoIP	1939
8	Monitoring Email Round Trip	1943
9	Monitoring Backups	1945
10	Monitoring Virtual Environments	1946
11	Monitoring Databases	1955
Part 11	System Administration Tools	1958
1	PRTG Server Administrator	1959
2	PRTG Probe Administrator	1979
Part 12	Advanced Topics	1990
1	Active Directory Integration	1991
2	Application Programming Interface (API) Definition	1993
3	Filter Rules for xFlow, IPFIX and Packet Sniffer Sensors	1994
4	Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors	1998
5	Define IP Ranges	2000
6	Define Lookups	2001
7	Regular Expressions	2010
8	Add Remote Probe	2011
	Remote Probes and Multiple Probes	2012
	Remote Probe Quick Setup	2015
	Remote Probe Setup Using Installer	2020
9	Failover Cluster Configuration	2026
	Failover Cluster Step by Step	2029
10	Data Storage	2036
11	Using Your Own SSL Certificate with PRTG's Web Server	2038
12	Calculating Percentiles	2040
Part 13	Appendix	2042
1	Glossary	2043
2	List of Abbreviations	2047

Contents

3	Support and Troubleshooting	2050
4	Legal Notices	2051
Index		2053

Part 1

Welcome to PRTG Network Monitor

1 Welcome to PRTG Network Monitor

Welcome to PRTG Network Monitor! You have chosen an easy-to-use software product that comes with a powerful set of features to monitor your entire network.

Why Network Monitoring is Important

Today, most businesses rely on a computer and network infrastructure for internet, internal management, telephone, and email. A complex set of servers and network equipment is required to ensure that business data flows seamlessly between employees, offices, and customers. The economical success of an organization is tightly connected with the flow of data.

The computer network's reliability, speed, and efficiency are crucial for businesses to be successful. But, like all other technical objects, network devices may fail from time to time—potentially causing trouble and loss of sales, no matter what migration efforts have been made up-front.

Network administrators need to take three key steps to maintain network uptime, reliability, and speed:

1. Set up a well-planned network with reliable components.
2. Create recovery plans for the event of device failure.
3. Monitor their network to know about failures as they build up or actually happen.

PRTG Network Monitor, the software described in this document, is a complete solution for monitoring small, medium, and large networks.

Monitoring Networks with PRTG Network Monitor

PRTG Network Monitor is a powerful network monitoring application for Windows-based systems. It is suitable for small, medium, and large networks and capable of LAN, WAN, WLAN, and VPN monitoring. You can also monitor physical or virtual web, mail, and file servers, Linux systems, Windows clients, routers, and many more. PRTG monitors network availability and bandwidth usage, as well as various other network parameters such as quality of service, memory load, and CPU usages. It provides system administrators with live readings and periodical usage trends to optimize the efficiency, layout, and setup of leased lines, routers, firewalls, servers, and other network components.

The software is easy to set up and use and monitors a network using Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), packet sniffer, Cisco NetFlow (as well as IPFIX, sFlow, and jFlow), and many other industry standard protocols. It runs on a Windows-based machine in your network for 24-hours every day. PRTG Network Monitor constantly records the network usage parameters and the availability of network systems. The recorded data is stored in an internal database for later analysis.

1.1 About this Document

This document introduces you to the system concepts of **PRTG Network Monitor** and explains how to set up the software to achieve the best monitoring results. You will learn how to plan your monitoring setup, how to set up your devices and sensors, dependencies, reports, notifications, maps, user accounts, and clustering for fail-safe monitoring.

This document is also meant as a reference for all available settings. Short contextual help is already provided within the Ajax web interface; in this manual you often get some more help regarding the different options available.

This document does **not** explain monitoring protocols and file formats in-depth. Also, the use of the Application Programming Interface (API) built into PRTG is only briefly addressed. Whenever possible, hyperlinks to more detailed resources are provided, such as articles in the [Paessler Knowledge Base](#).

To start using PRTG right away, please see the [Quick Start Guide](#)³²⁾ section. For more detailed instructions, see the other sections.

1.2 Key Features

PRTG Network Monitor monitors your network and requires no third party software. Conducting a quick ad-hoc download, you do not need to fill web forms and will not have any registration hassles. The installation process requires only a few minutes, as well as the first configuration which is mainly done automatically. The initial setup is achieved by an interactive guidance by the software.

What PRTG Can Be Used For

- Monitor and alert due to uptimes/downtimes or slow servers.
- Monitor system health of various hardware devices.
- Monitor and account bandwidth and network device usage.
- Monitor applications.
- Monitor virtual servers.
- Monitor Service Level Agreement (SLA).
- Monitor system usage (CPU loads, free memory, free disk space, etc.).
- Monitor performance of databases as well as monitor databases directly.
- Monitor email servers and use this feature to monitor various backup solutions.
- Monitor the environment.
- Classify network traffic by source/destination and content.
- Discover unusual, suspicious, or malicious activity with devices or users.
- Measure QoS and VoIP parameters and control service level agreements (SLA).
- Discover and assess network devices.
- Find unexpected relationships between your network components to detect potential security issues and to explore the real usage of your network and hardware.
- Monitor fail-safe using a failover cluster setup.

What PRTG Includes

The PRTG installer contains all modules and software necessary to run the monitoring system without the need for third party modules, including:

- High performance: PRTG's own fast and efficient database system to store the raw monitoring results as well as logs, Toplists, and tickets (outperforms SQL servers for monitoring data), accessible through Application Programming Interface (API). You can distribute high loads over multiple probes.
- Low system requirements: an average PC from the year 2007 is sufficient and even a netbook can monitor over thousand sensors.

- High security standards: SSL encryption for connections and web server, and multiple user accounts with shared and private sensors, as well as rights management, and many more.
- Built-in SSL secured web server with HTTP and HTTPS support for the user interface.
- Fast web interface, works as Single Page Application (SPA) to avoid time-extensive reloading of the page.
- Mail server for automatic email delivery.
- Flexible alerting
 - including nine notification technologies, for example, email, SMS, syslog and SNMP trap, HTTP request, event log, Amazon SNS, executing scripts, etc.
 - including various triggers, for example, status alerts, limit alerts, threshold alerts, multiple condition alerts, escalation alerts.
 - including dependencies to avoid alarms floods, acknowledging alarms to avoid further notifications for this alarm, and alert scheduling.
- In-depth report generator to create reports on-the-fly as well as scheduled reports in HTML or Portable Document Format (PDF). Many report templates are available by default.
- Graphics engine for user-friendly live and historic data charts.
- Network analysis module to automatically discover network devices and sensors.
- Distributed monitoring to monitor several networks in different locations.
- Special features for Managed Service Provider (MSP) to monitor customer networks and increase the quality of service.
- Data publishing with real time dashboards—private and public—including live performance and status information. You can design these maps as you like with many different objects, as well as you can integrate external custom objects.
- Different languages like English, German, Spanish, French, Portuguese, Dutch, Czech, Japanese, and Simplified Chinese.
- Customizations: The PRTG Application Programming Interface (API) allows you to program your own features and to customize and re-brand PRTG's web interface to your needs. In addition, you can create custom sensors, notifications, and device templates.

PRTG Network Monitor supports monitoring up to 20,000 thousand sensors per installation. It can optionally work with multiple remote probes to monitor multiple sites or network segments from one central core installation, and to distribute high loads. You can also configure fail-safe monitoring using a cluster installation to perform automatic failovers. Single failover installations are allowed with every PRTG license.

The software is based on Paessler's reliable monitoring technology, which has been constantly improved since 1997 and is already used by more than 150,000 users around the world every day. An outstanding support ensures that your inquiries are answered within one business day in order to ensure best possible network monitoring. Attractive licensing packages from freeware (up to 10 sensors) to enterprise level (with thousands of sensors) make sure that every user finds the proper solution.

1.3 New in This Version

With ongoing **continuous development and rollout**, we constantly extend and improve on the functionalities provided by PRTG. Instead of delivering just a few versions distributed over the year with massive changes in every version, PRTG is automatically and seamlessly enhanced with new features and fixes—fast and with high quality. There are three release channels for PRTG:

- **Stable**: best tested version of PRTG for live systems; updated about once or twice a month; for usage on live systems
- **Preview**: offering the latest features and fixes; updated about once a week; consider this version as "beta", thus, **do not use** this version on live systems you have to depend on!
- **Canary**: providing "nightly builds"; updated very often; not tested extensively; **never use** on live systems you have to depend on!

Because of these three channels, you can choose either maximum stability, earlier access to new features, or a mixture of both.

For an overview of all most recent changes in the current version, please visit the version history on our website. Please see the [More](#)¹⁸ section below for more information.

More

Paessler Website: PRTG Network Monitor Version History

- <http://www.paessler.com/prtg/history>

Paessler Blog: Version 12 of PRTG introduces "Continuous Rollout"

- <http://www.paessler.com/blog/2012/04/25/>

1.4 Available Licenses

There are four different PRTG flavors available.

Freeware Edition

The Freeware Edition is a good solution to get started with PRTG, or for private use:

- May be used for free for personal and commercial use.
- Can monitor up to 10 sensors.
- Supports all available sensor types.
- Shortest available monitoring interval is one minute.

Note: If you want to use the Freeware Edition, please first install the [Trial Edition](#)^[19] and get a free trial key. After the trial period has ended, your Trial Edition will automatically revert into a Freeware Edition.

Special Edition

The Special Edition has all the features of the Freeware Edition, plus it supports up to 30 sensors. By entering a Special Edition key, you can extend your Freeware Edition. This key is not for download, we only hand it out on special request. For detailed information, see [More](#)^[20] section below.

Trial Edition

The Trial Edition is intended for evaluation purposes for customers who are interested in purchasing commercial licenses:

- Can monitor an unlimited number of sensors.
- Supports all available sensor types.
- Shortest available monitoring interval is one second (not officially supported; a minimum interval of 10 seconds is recommended).
- Temporary license key must be requested from Paessler's website.
- Trial period limited to 30 days (automatically reverts to [Freeware Edition](#)^[19] afterwards).
- With each license one single failover [cluster setup](#)^[81], consisting of two nodes, is included. Cluster installations with two and three failover nodes will require one additional trial license key; a cluster installation with four failover nodes will require two additional trial license keys.

After the trial period has ended, a Trial Edition will revert into a Freeware Edition, allowing you to monitor up to 10 sensors for free.

Commercial Editions

There are several licenses of PRTG Network Monitor available to suit the demands of smaller, as well as larger customers and organizations:

- Can monitor maximum number of sensors (from 100 to unlimited).
- Supports all available sensor types.
- Shortest available monitoring interval is one second (not officially supported; a minimum interval of 10 seconds is recommended).
- With each license one single failover [cluster setup](#)^[81], consisting of two nodes, is included. Cluster installations with two and three failover nodes will require one additional license of the same size; a cluster installation with four failover nodes will require two additional licenses of the same size.

For more information about available commercial licenses, please see [More](#)^[20] section below.

More

Knowledge Base: What is the PRTG Special Edition license?

- <http://www.paessler.com/knowledgebase/en/topic/8063>

Paessler Website: Request a Free PRTG Trial Key for Evaluation

- <http://www.paessler.com/prtg/trial>

Paessler FAQs: What is the difference between the PRTG Network Monitor licenses?

- <http://www.paessler.com/support/faqs#e1912>

1.5 System Requirements

In order to install and work with PRTG Network Monitor, you need to meet the following requirements:

- A PC server or virtual machine with roughly the CPU performance of an average PC built in the year 2007 or later and minimum 1024 RAM memory. For [cluster](#)^[81] installations, use systems with similar performance.
- Operating system Microsoft Windows XP, Windows 2003 SP1 or later, Windows 2008 R2, Windows 7, 8, Server 2012, or Server 2012 R2 (all 32-bit or 64-bit). You can also use Windows Vista or 2008 R1, but we recommend not using these systems, because there are known performance issues related to them.
- Web browser to access the web interface. The following browsers are supported:
 - Google Chrome 31 or later (recommended)
 - Mozilla Firefox 25 or later
 - Microsoft Internet Explorer 10 or 11

Planning an Installation With Hundreds of Sensors or More?

As a rule of thumb, an average PC/server built in the year 2007 or later should be able to monitor 1,000 sensors with ease. Some exceptions apply for version 3 of Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI) and packet sniffer. The maximum number of sensors you can monitor with one installation of PRTG mainly depends on the monitoring technology and the monitoring intervals you use. In general, consider the following rules:

- **SNMP V1 and V2, Ping, Port, and HTTP**
These sensor types are recommended for scenarios with thousands of sensors. With these technologies up to 20,000 sensors are possible.
- **SNMP V3**
You will be able to monitor about 5,000 SNMP V3 sensors with an interval of 60 seconds on a common two core computer, and about 10,000 sensors on a four core system (the main limiting factor is your CPU power).
- **WMI**
Try to keep the number of WMI sensors per probe below 120 sensors (with 60s interval), or 600 sensors (with 300s interval).
- **xFlow (IPFIX, NetFlow, sFlow, jFlow)**
Monitoring the maximum number of sensors depends on the traffic pattern, the number of xFlow packets per second received by the PRTG probe, as well as the performance of the probe system (see site planner tool linked in the [More](#)^[22] section below).
- **Packet Sniffer**
These sensors create the highest CPU load on the probe system. This technology is only recommended for monitoring of low traffic connections (<50 Mbit/s steady stream). When traffic is often over 10 Mbit/s a dedicated [remote probe](#)^[201] should be used.

- **VMware Monitoring**

Monitoring of VMware is limited to about 20 sensors at a 60 seconds monitoring interval, or 100 sensors at a 5 minutes interval. These limitations issue from the VMware platform. A registry hack is available to boost this to 150 sensors at a 5 minutes interval (this will require a change in the ESX/vCenter configuration). For details please see [More](#)^[22] section below.

- **Other sensor types**

The impact of a specific sensor type on performance is indicated by a color range when adding a sensor to a device. It ranges from dark green (very low impact; 5,000 sensors per probe) to bold red (very high impact; 50 sensors per probe).

To overcome any limitations mentioned above you should distribute the sensors over two [remote probes](#)^[20] or more. For detailed information please use the site planner tool to plan large installations. See [More](#)^[22] section below.

We recommend using a dedicated physical machine to run both the PRTG core server and PRTG remote probes. For more information please see the [Detailed System Requirements](#)^[23] section.

More

- [Update From Previous Versions](#)^[47]

Knowledge Base: Planning Large Installations of PRTG Network Monitor

- <http://www.paessler.com/knowledgebase/en/topic/26383>

Knowledge Base: Paessler PRTG Site Planner Tool

- <http://www.paessler.com/knowledgebase/en/topic/41373>

Knowledge Base: How can I speed up PRTG—especially for large installations?

- <http://www.paessler.com/knowledgebase/en/topic/2733>

Knowledge Base: Increasing Maximum Connections for VMware Sensors

- <http://www.paessler.com/knowledgebase/en/topic/30643>

Knowledge Base: Checklist for Running PRTG on VMware

- <http://www.paessler.com/knowledgebase/en/topic/49193>

1.5.1 Detailed System Requirements

This section lists different aspects of system requirements for PRTG. Please consider these requirements in order to avoid issues while network monitoring.

- [Supported Operating Systems](#)^[23]
- [Hardware Requirements](#)^[24]
- [Sample Configurations](#)^[25]
- [Running PRTG on Virtual Machines](#)^[27]
- [Web Browser Requirements](#)^[27]
- [Screen Resolution](#)^[28]
- [Requirements for Monitored Devices](#)^[28]
- [Requirements for the Enterprise Console](#)^[28]
- [Requirements for Mobile Web GUI](#)^[29]
- [Requirements for Smart phones](#)^[29]
- [More](#)^[29]

Supported Operating Systems

The 32-bit and 64-bit versions of the following operating systems are officially supported for PRTG **Core Service** and **Probe Service** (Intel x86/x64 architectures only):

- Microsoft Windows XP SP2 or later
- Microsoft Windows Server 2003 SP1 or later
- Microsoft Windows Vista*
- Microsoft Windows Server 2008*
- Microsoft Windows Server 2008 R2
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows Server 2012**
- Microsoft Windows Server 2012 R2**

* For performance reasons, we do not recommend using Windows Vista or Windows Server 2008 R1, especially when monitoring via Windows Management Instrumentation (WMI). Using these operating systems, you will only be able to add a limited number of WMI sensors! For detailed information, please see [More](#)^[29] section below. If you need to use Windows Server 2008 R1, we strongly recommend installing Service Pack 2 (SP2).

** Windows Server 2012 in **Core** mode and the **Minimal Server Interface** are not officially supported.

The version (32-bit or 64-bit) of the PRTG Core Server depends on the version of your operating system. The 64-bit version of the PRTG Core Server will be installed if

- the operating system is a 64-bit Windows system, **and**
- the system provides 6GB RAM or more.

Otherwise the 32-bit version of the PRTG Core Server will be installed.

We recommend you to provide Microsoft .NET Framework versions 3.5 and 4.0 (with latest updates) on all systems running a PRTG probe. **Note:** Version 4.0 is imperatively needed for monitoring VMware and XenServer virtual environments.

More details: Some sensor types need the Microsoft .NET Framework to be installed on the computer running the PRTG probe. This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)²⁰¹². Depending on the sensor type, the required versions are 2.0, 3.0, or 4.0. **Note:** According to the Microsoft website, .NET version 3.5 contains versions 2.0 SP1 and 3.0 SP1. Version 4.0 is not downward compatible, but must be installed side-by-side to older version(s), if required.

For best performance of hybrid sensors using Windows Performance Counters and Windows Management Instrumentation (WMI), we recommend Windows 2008 R2 or higher on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)²⁰¹².

Hardware Requirements

Hardware requirements for PRTG **Core Service** and **Probe Service** mainly depend on the sensor types and intervals used. The following values are provided as reference for common usage scenarios of PRTG (based on a default sensor interval of 60 seconds).

- **CPU**
An average PC built in 2007 can easily monitor 1,000 sensors (see sensor type specific notes below). PRTG supports native x86 architectures.
- **RAM memory**
Minimum requirement: 1024 MB RAM. You will need about 150 KB of RAM per sensor.
- **Hard Disk Drive**
You will need about 200 KB of disk space per sensor per day (for sensors with 60 second interval).
- **Internet connection**
An internet connection is required for license activation (via HTTP or email).
- **Stable network connection for remote probes**
Remote probes require a stable network connection between the PRTG core server and the remote probe. Unstable connections, for example via 3G, might work but it could be possible that you lose monitoring data if the connection is non-reliable.

There are also non-hardware dependent limitations for some sensor types, for example, WMI and SNMP V3 sensors. These limitations can be overcome by distributing the sensors across multiple [remote probes](#)^[2011]. If you plan installations with more than 500 to 1,000 sensors, or more than 10 Packet Sniffer or xFlow (NetFlow, sFlow) sensors, please consult the site planner tool linked in the [More](#)^[29] section below.

Sample Configurations

The sample configurations in the table below will give you an overview of the hardware requirements for PRTG, based on your configuration.

Part 1: Welcome to PRTG Network Monitor | 5 System Requirements

1 Detailed System Requirements

	Large Installation A	Large Installation B	Netbook Installation
System	DELL Alienware	DELL PowerEdge 2900 III	DELL Inspiron Mini 10
CPU	Intel Core2 Quad-Core 2.6 GHz	Intel Xeon Quad-Core 1.87 GHz	Intel Atom Z520 1.33 GHz
RAM	8 GB	16 GB	1 GB
Operating System	Windows 7 64-Bit	Windows 2003 64-Bit	Windows XP 32-Bit
Sensors	20,000 SNMP 100 Other	20,000 SNMP	600 SNMP 750 WMI
Installation Corresponds To	400 switches à 48 ports	400 switches à 48 ports	24 switches à 25 ports + 30 Windows server
Scanning Interval	1 minute	1 minute	5 minutes
Number of Probes	4	1	1
Average CPU Load While Monitoring*	3 %	20 %	35 %
Average CPU Load While Generating Reports*	20 %	30 %	85 %
Average Memory Used	3 GB	3.5 GB	260 MB
Average Data Written to Disk Per Year	800 GB	800 GB	55 GB
Average Network Load	80 kbit/s	550 kbit/s	150 kbit/s

* CPU load is higher while users are accessing the web interface.

Running PRTG on Virtual Machines

PRTG core server as well as PRTG probe can be run on virtualized platforms. The following platforms were tested successfully:

Virtual Host Technology	Client OS
VMware ESX/ESXi versions 3.5, 4.0, or 5.0	Windows XP, Windows 2003 SP1 or later (32/64 bit), Windows Vista, Windows 7 (32/64 bit), Windows 2008 (32/64 bit)
VMware Server 2.0	Windows XP, Windows 2003 SP1 or later (32/64 bit), Windows 2008
XEN Server 5.0	Windows XP, Windows 2003 SP1 or later (32/64 bit), Windows 2008
Parallels Virtuozzo Containers	Windows 2003 Server SP1 or later (32/64 bit), Windows 2008 Server
Cloud Hosting Platforms (Amazon EC2, TheRackspaceCloud, and others)	Windows Server 2003 SP1 or later, Windows Server 2008

Important notice: We recommend using a dedicated physical machine to run both the PRTG core server and PRTG remote probes. If you run PRTG on a virtual machine, we strongly recommend to stay below 2,000 sensors for performance reasons. Unfortunately, we cannot offer technical support regarding performance and stability problems for PRTG installations on virtual machines that run with more than 5,000 sensors. In this case, please migrate PRTG to one or more, preferably physical, machines.

Note: When running PRTG on a virtual machine, do **not** use dynamic resource allocation, but please make sure that full resources are available to the virtual machine at any time. In our experience, dynamic resource allocation is not working efficiently for a monitoring software and can therefore lead to massive performance issues.

Please see also section [More](#)^[29] regarding running PRTG on VMware.

Web Browser Requirements

The following browsers are officially supported by the PRTG web interface (in order of performance and reliability):

- Google Chrome 31 or later (recommended)
- Mozilla Firefox 25 or later

- Microsoft Internet Explorer 10 or 11

Note: Deprecated Internet Explorer versions as well as mobile browsers might not be able to display the full featured [Ajax web interface](#)^[100]. Using these browsers, you can access the feature-limited [Mobile Web GUI](#)^[1913], which does not require CSS or Javascript capability.

PRTG's web interface makes heavy use of Javascript and AJAX. We found that for some functions Chrome is up to 10 times faster than Internet Explorer, and 3 to 5 times faster than Firefox.

Screen Resolution

A screen resolution of at least 1024x768 pixels is sufficient for most functions of PRTG. However, we recommend a screen resolution of 1200x800 or higher.

Requirements for Monitored Devices

- **SNMP monitoring**

The monitored device(s) must be equipped with SNMP Version 1, 2c, or 3 (i.e., an SNMP-compatible software must be installed on the device). SNMP must be enabled on the device and the machine running PRTG must be granted access to the SNMP interface.

- **WMI monitoring**

In order to use WMI (Windows Management Instrumentation) monitoring, you will need a Windows network. For client PCs monitored with WMI, only Windows XP and later are officially supported (XP, 2003, Vista, 2008, etc.). Windows 2000 is not officially supported. Please do not use Windows Vista or Windows 2008 R1 for WMI monitoring (they both have WMI performance issues).

- **xFlow (IPFIX, NetFlow, sFlow) monitoring**

The device must be configured to send NetFlow data packets (NetFlow version 5 or 9; IPFIX is the successor protocol of NetFlow 9) or sFlow packets (version 5) to the machine running the PRTG probe.

- **Packet Sniffer monitoring**

Only data packets passing the local machine's network card can be analyzed. Switches with so-called 'monitoring ports' are necessary for network-wide monitoring in switched networks.

- **Other sensor types**

Depending on the specific sensor type, you can find requirements (for example, modules, components, device configurations) which may have to be fulfilled in the corresponding manual section, as well as partly when adding the sensor to a device.

Requirements for the Enterprise Console

The optional PRTG [Enterprise Console](#)^[1860] runs under all Windows versions XP or later. It has a built-in webkit browser engine and requires no specific browser installed on the system. See also section [Enterprise Console—Requirements for Connections to PRTG Web Server\(s\)](#)^[1860].

Requirements for Mobile Web GUI

The feature-limited mobile web interface is optimized for low bandwidth and mobile access. It has been designed for and tested with iOS (iPhone, iPad), Android, Blackberry, Windows Mobile, and also deprecated Internet Explorer versions.

Requirements for Smartphones

The optional smartphone apps for iOS devices require iOS version 6 or later and PRTG v12 or later. For Android devices, the app "PRTG for Android" requires Android OS 4.0 or later (version 4.1 or later recommended), as well as PRTG Network Monitor 13.1 or later. For more information, please see [Smartphone Apps](#)^[1916]. The [Mobile Web GUI](#)^[1913] interface can be used on most phones with a browser. We successfully tested it on Symbian, BlackBerry, Windows, Android, and iOS devices.

More

- [Update From Previous Versions](#)^[47]

Paessler Blog: Don't Use Windows Vista And Windows 2008 R1 for Network Monitoring via WMI!

- <http://www.paessler.com/blog/2010/09/22/>

Paessler Website: Paessler PRTG Site Planner Tool

- <http://www.paessler.com/knowledgebase/en/topic/41373>

Knowledge Base: How can I speed up PRTG—especially for large installations?

- <http://www.paessler.com/knowledgebase/en/topic/2733>

Knowledge Base: My WMI sensors don't work. What can I do?

- <http://www.paessler.com/knowledgebase/en/topic/1043>

Knowledge Base: Frequent Questions about xFlow, Packet Sniffing, Traffic Monitoring and Cisco

- <http://www.paessler.com/knowledgebase/en/topic/3733>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <http://www.paessler.com/knowledgebase/en/topic/46863>

Knowledge Base: Checklist for Running PRTG on VMware

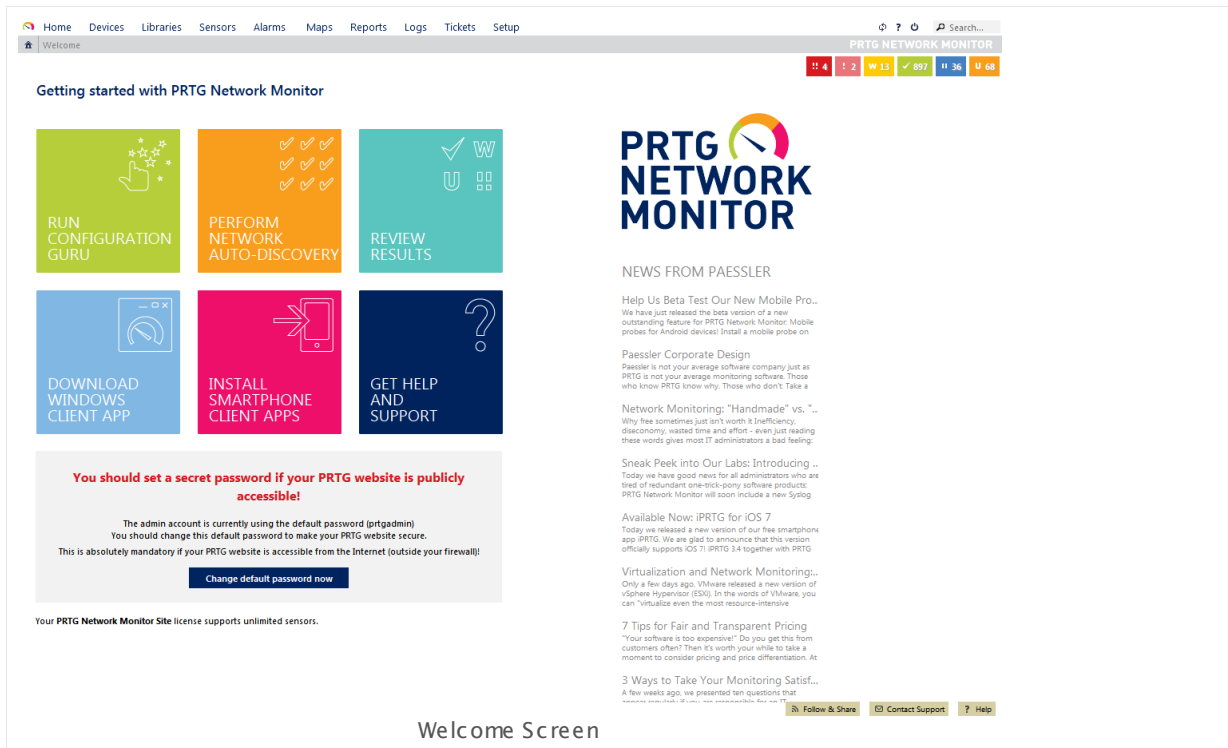
- <http://www.paessler.com/knowledgebase/en/topic/49193>

Part 2

Quick Start Guide

2 Quick Start Guide

Welcome to PRTG Network Monitor! This section will support you with a quick start into PRTG, so you can start monitoring your network right away!



Setting up monitoring for your network is easy! You only need to download the installer from Paessler's website, run through the installation wizard, and provide some information in the configuration guru. PRTG will start monitoring your network immediately without any further complicated stumbling blocks! Of course, later on, you still can adjust everything to your needs.

Please see the following quick steps.

Quick Start Guide—Topics

- [ONE—Download, Installation, and First Login](#) ^[33]
- [TWO—Using the Configuration Guru](#) ^[36]

2.1 ONE—Download, Installation, and First Login

Simply download and install the version of PRTG Network Monitor which meets your needs. For video tutorials with PRTG basics, please see section [More](#) ³⁵ below.

Download

On the Paessler website, you find two different installers for PRTG, a public download for the Freeware, Special, and Trial editions, and a login link to download the commercial editions (which is only available for paying customers).

“Installation of PRTG Takes Less Than 2 Minutes!”

Monitor your network now! No additional software is required. All you need is a Windows PC or VM.

Running PRTG in your network is quick&easy. After installation it will scan your network and the Auto-Discovery will create all the sensors that are required to monitor your network.

Free Trial Download
No limitations for 30 days

Freeware Download
Limited to 10 Sensors, Free Forever

Version Number, File Size	Version 13.4.7.3531 (November 19th, 2013), 120 MB
Available Translations	English, German, Spanish, French, Portuguese, Dutch, Czech, Japanese, and Simplified Chinese
Operating Systems	All Windows versions (XP or later, see System Requirements)
What's new?	See Version History/Release Notes
Do you need the full version download?	Please log into our website

PRTG Download on Paessler Website with Marked Full Version Download Link

Downloading the Freeware, Special, or Trial Edition

Please download the latest publicly available file from the Paessler website. You can also request a trial key there, which must be entered during installation:

- <http://www.paessler.com/prtg/download>

Note: Every Freeware installation will start as a Trial version, giving you an unlimited number of sensors for 30 days. After the trial period has expired, your installation will automatically revert to a Freeware edition with 10 sensors.

Note: A Special Edition is an extended Freeware version. If you meet certain requirements, you can receive a Special Edition key from us which gives you an extended number of sensors for free. For details, please see:

- <http://www.paessler.com/prtg/download#30sensors>

Downloading the Commercial Edition

Downloads and updates are free to customers with an active maintenance contract. Please log into the Paessler website to get the latest download. You can also find your license key there, which must be entered during installation:

- <http://www.paessler.com/login>

If you do not have an active maintenance contract, please contact sales@paessler.com.

Note: Once installed, you will usually use the [Software Auto-Update](#)  function of PRTG to download and install new versions. This will further ease the process of installing updates.

Installation

Please double click the setup file on the computer that will be your PRTG server. Follow the installation wizard and install the software.

At the end of the installation, a browser window will be opened automatically, and it will connect to the PRTG web interface, showing the **Configuration Guru**. Please make sure you load the web interface with one of the supported browsers:

- Google Chrome 31 or later (recommended),
- Mozilla Firefox 25 or later, or
- Microsoft Internet Explorer 10 or 11.

Note: Due to scripting incompatibilities, you might not be able to use all functionalities of the PRTG Ajax web interface with Internet Explorer 9 or earlier and other older browsers. If you cannot access the **Configuration Guru**, please open the URL of the PRTG web interface in another browser.

Login

If everything works fine, you will not see the login screen on first startup. Only when switching browsers you will have to log in.

PRTG NETWORK MONITOR

PAESSLER

PRTG NETWORK MONITOR

Login Name

Password

☒ Use AJAX Web GUI (All features, optimized for desktop access)
☐ Use Mobile Web GUI (Limited functionality, optimized for mobile access)
☐ Download Client Software (for Windows, iOS, Android)

Login Default Login

Forgot password? Need Help?

NEWS FROM PAESSLER

Help Us Beta Test Our New Mobile Pro...
We have just released the beta version of a new...
outstanding feature for PRTG Network Monitor: Mobile...
probes for Android devices! Install a mobile probe on...

Paessler Corporate Design
Paessler is not your average software company just as...
PRTG is not your average monitoring software. Those...
who know PRTG know why. Those who don't: Take a...

PRTG Network Monitor 3.4.9.3596

© 2013 Paessler AG

PRTG Login Screen

- Leave the **Login Name** and **Password** fields empty.
- Choose the **AJAX Web GUI (All features, optimized for desktop access)** option.
- Click on the **Default Login** button to login.

Please make sure you use a supported web browser when logging in to PRTG. Please use Google Chrome 31 or later (recommended), Mozilla Firefox 25 or later, or Microsoft Internet Explorer 10 or 11. Only with a supported browser you can use the **AJAX Web GUI (All features, optimized for desktop access)** option. If you see this option grayed out, please change your browser and open the URL again.

Please see the next step for more information about [Using the Configuration Guru](#) ³⁶.

More

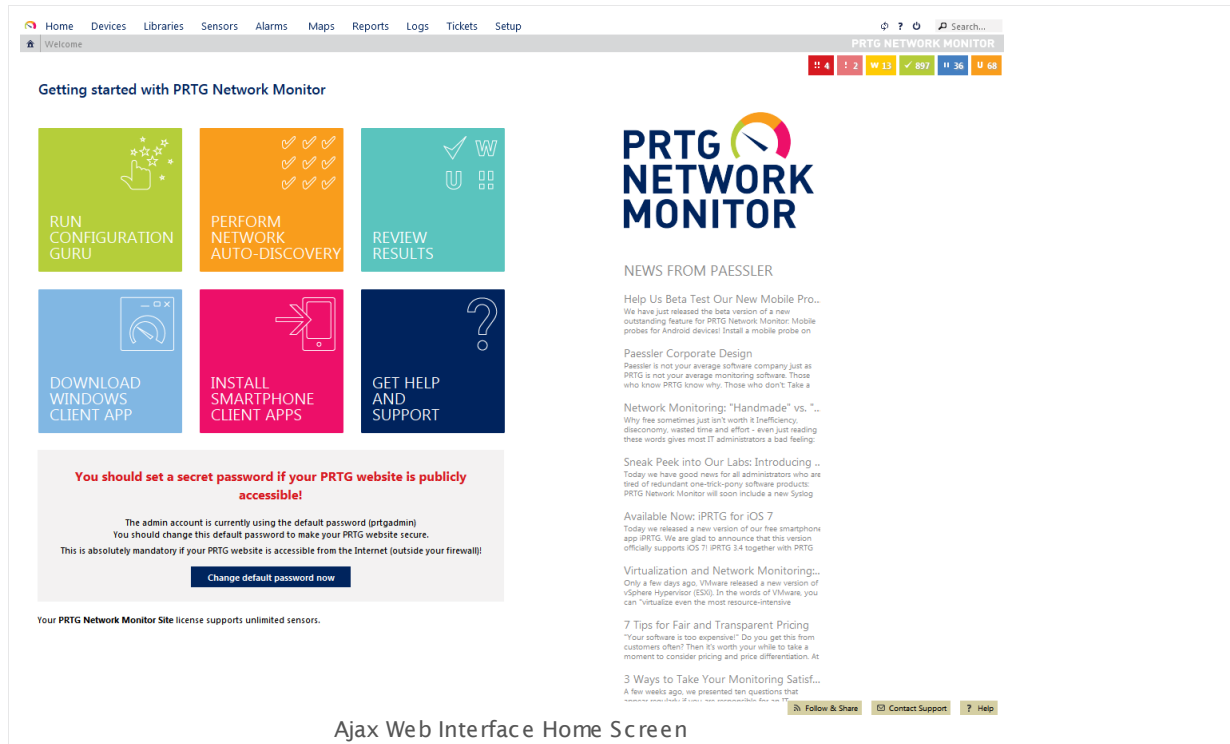
Video Tutorials for PRTG Network Monitor:

- http://www.paessler.com/support/video_tutorials

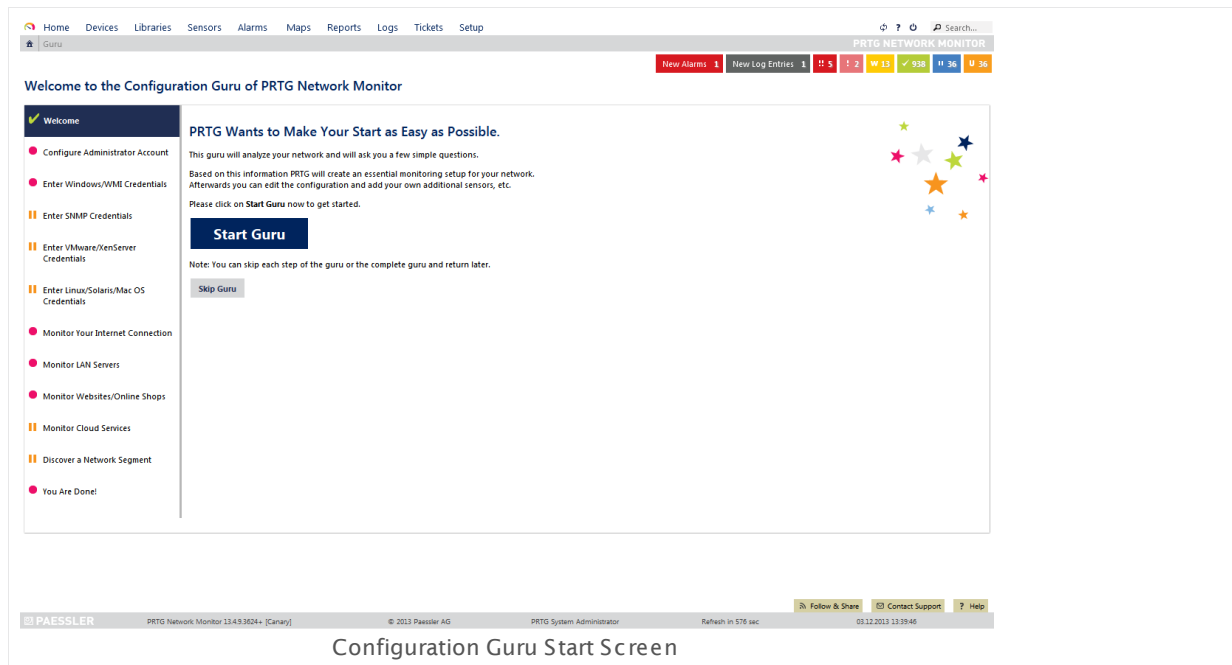
2.2 TWO—Using the Configuration Guru

For a new installation, PRTG will open the Configuration Guru automatically after each login. It will reappear until you either ran through it completely or skipped it. In order to open it at any time, please click the Run Configuration Guru button on PRTG's Home screen.

Note: When using the [Enterprise Console](#)¹⁸⁶⁰, please start the Guru by selecting **Help | Run Configuration Guru** from the main menu.



By answering about ten simple questions, this assistant will guide you through an initial setup and pre-configure an essential monitoring of your network including important devices, servers, and websites. You can later adjust these automatically generated monitoring settings later by hand.



Configuration Guru Start Screen

The steps to go are:

- [Enable SSL Encryption](#) ^[38]
- [Configure Administrator Account](#) ^[38]
- [Enter Windows/WMI Credentials](#) ^[38]
- [Enter SNMP Credentials](#) ^[39]
- [Enter VMware/XenServer Credentials](#) ^[39]
- [Enter Linux/Solaris/Mac OS Credentials](#) ^[40]
- [Monitor Your Internet Connection](#) ^[40]
- [Monitor LAN Servers](#) ^[40]
- [Monitor Websites/Online Shops](#) ^[41]
- [Monitor Cloud Services](#) ^[41]
- [Discover a Network Segment](#) ^[41]
- [You Are Done!](#) ^[42]

Click on the **Start Guru** button to start. You can skip a step at any time by clicking on the **Skip** button.

Enable SSL Encryption

This step is shown only if your web server runs on http. We recommend running the PRTG web interface using SSL encryption (https), especially if you make your web interface available from the internet. Without encryption your passwords are sent over your network unencrypted. Choose between:

- **Yes:** Switch the PRTG web server to use SSL. A popup will appear, showing you the screen shot of a certificate security warning that will be shown the next time you load the PRTG web interface. Confirm by clicking the button **Yes, switch to SSL now**. After you confirm, the PRTG core server Windows service will be restarted and the web interface will be reloaded, most likely showing a certificate warning. Confirm it to proceed to the login screen. For more information, please see [SSL Certificate Warning](#)^[105].
- **No:** Skip this step and keep using an unencrypted http connection. Once you skipped this step, it will not be shown again. You can switch to SSL later by using the PRTG Server Administrator tool from the Windows start menu. For more information, please see [PRTG Server Administrator](#)^[106].

Click the **Save & Next** button to apply your settings, or click the **Skip** button to skip this step. Both buttons will take you to the next step.

Configure Administrator Account

By default, PRTG uses the administrator account with login name **prtadmin** and password **prtadmin**. For security reasons you should at least change the password.

Please enter credentials and email address for the administrator account.

The password must meet the following requirements:

- at least eight characters long
- at least one number
- at least one capital letter

Click the **Save & Next** button to apply your settings, or click the **Skip** button to skip this step. Both buttons will take you to the next step.

Enter Windows/WMI Credentials

In order to monitor your Windows clients and servers via Windows Management Instrumentation (WMI), please enter Windows administrator credentials for your network. We recommend using Domain Administrator credentials (if you're using an Active Directory).

PRTG will store these credentials in the [Root](#)^[224] group of your device tree. All Windows-based devices will automatically inherit and use them for monitoring. You can discontinue [Inheritance of Settings](#)^[87] at any level, entering other credentials instead.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Click the **Save & Next** button to apply your settings, or click the **Skip** button to skip this step. Both buttons will take you to the next step.

Enter SNMP Credentials

In order to monitor your hardware (router, switches, etc.), Simple Network Management Protocol (SNMP) is the most common protocol used. Usually, all SNMP-enabled devices use the same settings by default: SNMP **version 1**, community string **public**, SNMP **port 161**).

You only need to change values here if the SNMP-enabled devices in your network use other settings. Choose between:

- **No:** You SNMP-enabled devices use the default configuration. If you're not sure, choose this option.
- **Yes:** Choose this option to enter your own SNMP credentials and settings. More settings will appear. Choose the SNMP version, enter the community string and SNMP port number, and define a time out for SNMP connections.

PRTG will store these credentials in the [Root](#)^[224] group of your device tree. All SNMP-based devices will automatically inherit and use them for monitoring. You can discontinue [Inheritance of Settings](#)^[87] at any level, entering other credentials instead.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)^[1928] section.

Click the **Save & Next** button to apply your settings, or click the **Skip** button to skip this step. Both buttons will take you to the next step.

Enter VMware/XenServer Credentials

If you use the virtual environments VMware or Citrix XenServer, PRTG can monitor them as well. To do so, please enter root access credentials for those systems. Choose between:

- **No:** PRTG will not monitor virtual environments. You can later add those credentials.
- **Yes:** Please enter user name and password for VMware or XenServer systems. For VMware, please also specify the protocol that will be used to connect.

PRTG will store these credentials in the [Root](#)^[224] group of your device tree. All VMware/XenServer-based devices will automatically inherit and use them for monitoring. You can discontinue [Inheritance of Settings](#)^[87] at any level, entering other credentials instead.

For an overview of all available VMware and XenServer sensors, please see [List of Available Sensor Types](#)^[296], section "Virtual Servers Sensors".

Click the **Save & Next** button to apply your settings, or click the **Skip** button to skip this step. Both buttons will take you to the next step.

Enter Linux/Solaris/Mac OS Credentials

If you have systems running on Linux, Solaris, or Mac OS X, PRTG can monitor them as well. To do so, please enter root access credentials for those systems. Choose between:

- **No:** PRTG will not monitor devices via SSH/WBEM. You can later add those credentials.
- **Yes:** Please enter SSH/WBEM credentials. You can either provide username and password, or paste a private key. For WBEM access, please also define protocol and port. Additionally, specify the rights an SSH command will be executed with.

PRTG will store these credentials in the [Root](#)^[224] group of your device tree. All SSH/WBEM-based devices will automatically inherit and use them for monitoring. You can discontinue [Inheritance of Settings](#)^[87] at any level, entering other credentials instead.

For a general introduction to SSH monitoring, please see [Monitoring via SSH](#)^[1930] section.

Click the **Save & Next** button to apply your settings, or click the **Skip** button to skip this step. Both buttons will take you to the next step.

Monitor Your Internet Connection

PRTG can monitor the availability of your default gateway and DNS servers. It will try to automatically detect and pre-populate the respective fields with the correct IP addresses. Please review and/or enter the IP addresses of your default (internet) gateway and your DNS server(s). Enter each IP address/DNS name in one line.

Note: For most networks, the gateway is the IP address or DNS name of your firewall or router. If you do not have a second DNS server, simply leave the respective field blank.

PRTG will create a new device for each entry and run an auto-discovery to set up sensors. In the background, auto-discovery will start immediately after you confirm this step.

Click the **Save & Next** button to apply your settings, or click the **Skip** button to skip this step. Both buttons will take you to the next step.

Monitor LAN Servers

PRTG can monitor your AD domain controllers, Exchange or other mail servers, as well as additional servers in your network. PRTG will try to automatically detect and pre-populate the respective fields with the correct IP addresses. Please review and/or enter the entries for your Active Directory domain controllers and mail servers. Enter each IP address/DNS name in one line.

PRTG will create a new device for each entry and run an auto-discovery to set up sensors. In the background, auto-discovery will start immediately after you confirm this step. **Note:** Your entries will not be shown in the Configuration Guru after confirming this step but will be added as devices to your device tree nevertheless. The Configuration Guru option **Monitor LAN Servers** will be marked with a green check mark as well if one or more servers were defined in this section.

Click the **Save & Next** button to apply your settings, or click the **Skip** button to skip this step. Both buttons will take you to the next step.

Monitor Websites/Online Shops

PRTG can monitor your website and online shop using http. Simply enter the URLs you want to monitor, each in one line.

PRTG will create a new device for all of your websites, with one sensor for each URL.

Click the **Save & Next** button to apply your settings, or click the **Skip** button to skip this step. Both buttons will take you to the next step.

Monitor Cloud Services

To see if the cloud services that you usually use are up and running, PRTG can set up http sensors for those as well. In the list of services, simply switch the radio button to **Yes** for each service you want to monitor. Choose from:

- **Google Search, Google Mail, Google Drive**
- **Microsoft Office 365**
- **Salesforce**
- **Dropbox**
- **iCloud**
- **Facebook**
- **Twitter**
- **Skype**

PRTG will create a new device for all of cloud services, with one sensor for each URL.

Click the **Save & Next** button to apply your settings, or click the **Skip** button to skip this step. Both buttons will take you to the next step.

Discover a Network Segment

PRTG can scan an entire network segment, automatically detect devices, and create sensors using its auto-discovery.

PRTG will try to automatically detect and pre-populate the respective fields with the correct IP range. Please review and/or enter the entries. In the **IPv4 Base** field, enter the first three octets of your network's IP range, for example **192.168.0** or **10.0.0**, or whatever IP address range you use. If you don't change the default values for **IPv4 Range Start** and **End**, PRTG will automatically complete the IP base and scan all IP addresses ending in **.1** to **.254**.

If you need more options regarding the definition of IP ranges, you can run additional auto-discoveries later. Please see [Auto-Discovery](#)^[190] for more details.

Click the **Save & Next** button to apply your settings, or click the **Skip** button to skip this step. Both buttons will take you to the next step.

You Are Done!

While you were busy using the guru, PRTG has already created devices and sensors for you. There are first monitoring values available, too. In the meantime, you can follow PRTG on your favorite social network by clicking on of the buttons for Facebook, Twitter, or Google +.

Click on the **OK! Let me view my new sensors!** button to view the device tree.

In order to get familiar with the PRTG web interface, we recommend you proceed with section [General Layout](#)^[108] of the web interface, or with [General Layout](#)^[1864] of the Enterprise Console.

Part 3

Installing the Software

3 Installing the Software

This section describes how to download and install your PRTG product.



PRTG Setup

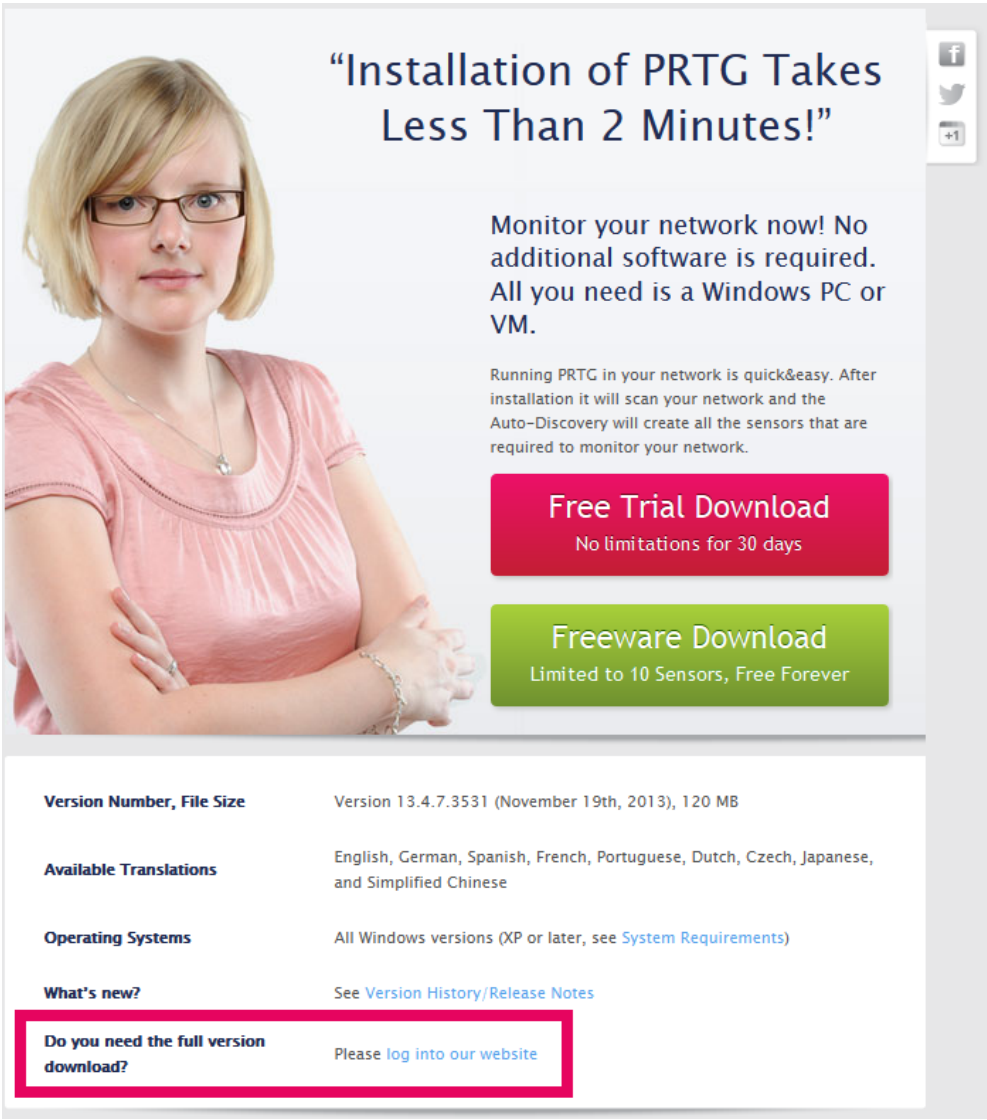
Please see the following sections for more information.

Installing the Software—Topics

- [Download PRTG](#) ⁴⁵
- [Update From Previous Versions](#) ⁴⁷
- [Install a PRTG Core Server](#) ⁵¹
- [Install a PRTG Cluster](#) ⁵⁶
- [Enter a License Key](#) ⁵⁷
- [Activate the Product](#) ⁶⁰
- [Install a PRTG Remote Probe](#) ⁶²
- [Install the Enterprise Console](#) ⁶⁷
- [Uninstall PRTG Products](#) ⁷¹

3.1 Download PRTG

On the Paessler website, you find two different installers for PRTG, a public download for the Freeware, Special, and Trial editions, and a login link to download the commercial editions (which is only available for paying customers).



“Installation of PRTG Takes Less Than 2 Minutes!”

Monitor your network now! No additional software is required. All you need is a Windows PC or VM.

Running PRTG in your network is quick&easy. After installation it will scan your network and the Auto-Discovery will create all the sensors that are required to monitor your network.

Free Trial Download
No limitations for 30 days

Freeware Download
Limited to 10 Sensors, Free Forever

Version Number, File Size	Version 13.4.7.3531 (November 19th, 2013), 120 MB
Available Translations	English, German, Spanish, French, Portuguese, Dutch, Czech, Japanese, and Simplified Chinese
Operating Systems	All Windows versions (XP or later, see System Requirements)
What's new?	See Version History/Release Notes
Do you need the full version download?	Please log into our website

PRTG Download on Paessler Website with Marked Full Version Download Link

Downloading the Freeware, Special, or Trial Edition

Please download the latest publicly available file from the Paessler website. You can also request a trial key there, which must be entered during installation:

- <http://www.paessler.com/prtg/download>

Note: Every Freeware installation will start as a Trial version, giving you an unlimited number of sensors for 30 days. After the trial period has expired, your installation will automatically revert to a Freeware edition with 10 sensors.

Note: A Special Edition is an extended Freeware version. If you meet certain requirements, you can receive a Special Edition key from us which gives you an extended number of sensors for free. For details, please see:

- <http://www.paessler.com/prtg/download#30sensors>

Downloading the Commercial Edition

Downloads and updates are free to customers with an active maintenance contract. Please log into the Paessler website to get the latest download. You can also find your license key there, which must be entered during installation:

- <http://www.paessler.com/login>

If you do not have an active maintenance contract, please contact sales@paessler.com.

Note: Once installed, you will usually use the **Software Auto-Update**  function of PRTG to download and install new versions. This will further ease the process of installing updates.

3.2 Update From Previous Versions

If you already have installed a previous software version, there are several things you should consider before updating to the current PRTG version.

Note: We recommend you always have a proper backup of your monitoring data and configuration. In most cases both will be maintained when upgrading. Anyway, we recommend a backup before upgrading. Please see [More](#)^[49] section below.

Update From PRTG Network Monitor 12 or later

If you have been running PRTG Network Monitor with version 12, 13 or 14, simply [install](#)^[51] the latest version on top of the previous version. Your configuration will be kept. If you have configured PRTG as a cluster, you only have to install an update on any node server (master or failover). The new version will then be deployed to the cluster automatically. **Note:** We recommend you always have a proper backup of your monitoring data.

Note: As of PRTG 14, **Internet Explorer 9 is no longer officially supported** for access to the PRTG web interface.

Web Interface Customizations as of PRTG Network Monitor 13.2.3

As of PRTG version 13.2.3, the **website** folder of the PRTG program directory is not used any more. This means that if you update from an older PRTG version than 13.2.3 to the current version, all existing customizations of the web interface will be disabled and have to be revised. You may find a way for a similar customization that can be applied to the files in the current **webroot** folder which contains the web interface files now. For details, please see section [More](#)^[49].

Update From PRTG Network Monitor 9

If you are using PRTG 9 now, your configuration will be kept when installing the current PRTG version in **Standalone Mode** or when installing a **Master Node**. There are only a few things you should consider.

- **Discontinued Sensors:** Existing instances of the following sensor types will stop working as of PRTG V12 and must be replaced with their successor sensor types!

- VMware Host Server (SOAP)
- VMware Virtual Machine (SOAP)
- Xen Virtual Machine

If your configuration contains these sensor types, they will stop monitoring after upgrading to the current version. We recommend you to pause them to keep their data. In order to continue monitoring, please add the sensors anew (for example, using the auto-discovery).

- **Please install .NET 4.0:** We strongly recommend installing .NET 4.0 on systems that run the core server (and the remote probes, if you use those). Otherwise the following features will not work: [VMware](#)^[296] auto-discovery and monitoring, [Citrix XenServer](#)^[342] auto-discovery and monitoring, [SIP Options Ping Sensor](#)^[880], [Windows Last Update Sensor](#)^[1431].

- **Changed Geo Maps Provider:** When you update to the current PRTG version, the provider for geographical maps will automatically be switched from Google Maps to MapQuest (using Open Street Map data).
- **Windows 2000 Not Supported:** Since PRTG 7 we do not officially support Windows 2000 systems any more. This means, PRTG cannot be installed on systems running Windows 2000, and you cannot officially monitor Windows 2000 systems (for example, via WMI). However, if you could successfully monitor your Windows 2000 systems with PRTG 9, this might actually not be possible any more with the current PRTG version. Especially the [WMI Service Sensor](#) [1614] will show an error message when monitoring Windows 2000 systems under the current PRTG version. For a work around, please see [More](#) [49] section below.

Update From PRTG Network Monitor 7 or 8

If you are using PRTG 7 or 8 now, your configuration will be kept when installing the current PRTG version in **Standalone Mode** or when installing a **Master Node**. There are only a few things you should consider.

Note: If you're running PRTG 7 or 8 we recommend you first update to the latest PRTG 8 version as an intermediate step, in order to make sure all data is carried over correctly. Please [contact technical support](#) [2050] to obtain a download link for PRTG 8. In any case we recommend you always keep a proper backup of your configuration and monitoring data.

Updating from PRTG 7 or 8 to Current PRTG Version

- Packet Sniffer (Content) sensors are not supported any more. Existing sensors of this type will automatically be switched to Packet Sniffer (Header) sensors after the update. As a benefit, you can now also sniff IPv6 traffic.
- Internet Explorer 8 is no longer supported for access to the PRTG Ajax web interface or to the mobile web GUI.
- You may experience a slow [Enterprise Console](#) [1890] (former 'Windows GUI') due to different reasons. For detailed information, please see the knowledge base article linked in the [More](#) [49] section below.
- When installing a failover node on top of an existing stand-alone PRTG 7, 8, 9, 12, or 13+ installation, the configuration cannot be kept and is written to a backup folder. Then, the new cluster configuration is received from the master node of the cluster. As all nodes work with the same configuration, a failover node's old configuration and monitoring data can no longer be used. If you want to keep a configuration of PRTG 7, please install the master node on top of the old installation and use other servers for the failover node installations.
- Since PRTG 9 the SNMP sensors use the **IPv4 Outgoing IP** set for the probe service (this setting was formerly ignored by those sensors, using the **auto** setting instead). If you experience failing sensors, please check the setting in the [PRTG Probe Administrator](#) [1981]. For detailed information please see [More](#) [49] section below.
- If you have (manually) configured the PRTG probe or PRTG core service to run under a different Windows user account (for example, for successful internet access through an ISA server firewall), please apply the respective Windows user account for the "PRTGProbeService" and/or "PRTGCoreService" anew after installing the current PRTG version. For detailed information please see [More](#) [49] section below.

- Probe core and probe now require: SP1 (or later) on Windows 2003, and SP2 (or later) on Windows XP.
- If you use the default data path in your PRTG setup, it will be changed automatically. Up to version 8 all data was stored in a sub folder reflecting a PRTG version number (v7 or v8). As of version 9 this sub folder is omitted, and data is stored directly at %ALLUSERSPROFILE%\Application data\Paessler\PRTG Network Monitor. During setup, all data will be moved to the new directory. If you use a custom data path it will not be changed.
- Up to version 8 all data in the registry was stored in a sub key reflecting a PRTG version number (v7 or v8). As of version 9 this sub key is omitted, and registry data is stored directly under the key HKEY_LOCAL_MACHINE\SOFTWARE\Paessler\PRTG Network Monitor (on 32-bit systems) respectively HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Paessler\PRTG Network Monitor (on 64-bit systems). During setup, all existing registry values will be moved to the new key.

Updating from PRTG 7 to Current PRTG Version

- Regarding custom sensors, the interpretation of returned values is handled more strict as of PRTG 8. If you're using custom sensors with PRTG 7, these may not work with the current PRTG version if they do not fully apply to the [API definition](#)^[199].

Update From Older PRTG Products

For all other predecessor products, a direct data import into the current version is not possible.

If you have been using IPCheck 5 or PRTG Traffic Grapher 6, please perform a clean installation of PRTG Network Monitor and set up your configuration anew. Using PRTG's [Auto-Discovery](#)^[190] is the easiest way to quickly configure a monitoring of your entire network. Please see [Quick Start Guide](#)^[32] section for more information.

More

Knowledge Base: How do I backup all data and configuration of my PRTG installation?

- <http://www.paessler.com/knowledgebase/en/topic/523>

Knowledge Base: What about my web interface customizations as of PRTG 13.2.3?

- <http://www.paessler.com/knowledgebase/en/topic/44703>

Knowledge Base: How can I monitor a Windows service on Windows 2000?

- <http://www.paessler.com/knowledgebase/en/topic/36483>

Knowledge Base: Why is the Enterprise Console so slow?

- <http://www.paessler.com/knowledgebase/en/topic/25413>

Knowledge Base: Some of my SNMP sensors do not work after updating from PRTG 8 to PRTG 9 or later

- <http://www.paessler.com/knowledgebase/en/topic/25663>

Knowledge Base: Probe Service or Core Service stop working after updating from PRTG 8 to PRTG 9 or later

- <http://www.paessler.com/knowledgebase/en/topic/25463>

Knowledge Base: How and where does PRTG store its data?

- <http://www.paessler.com/knowledgebase/en/topic/463>

Knowledge Base: Can I update from PRTG Traffic Grapher or IP Check 5 to the current PRTG version?

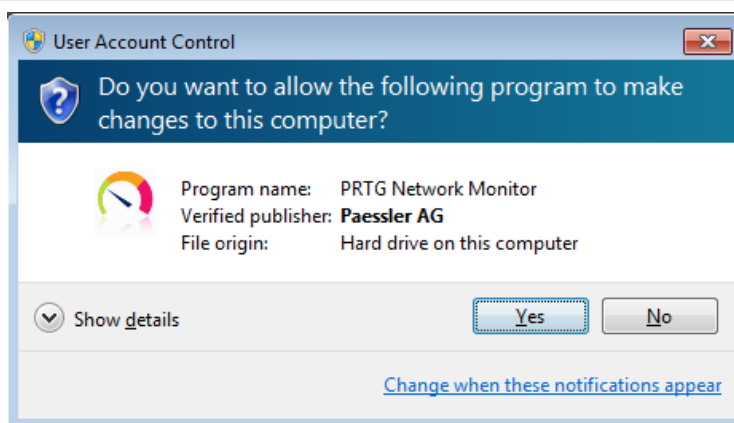
- <http://www.paessler.com/knowledgebase/en/topic/26553>

Knowledge Base: How do I Import Data from PRTG Traffic Grapher 6 or IPCheck Server Monitor 5 in PRTG Network Monitor?

- <http://www.paessler.com/knowledgebase/en/topic/253>

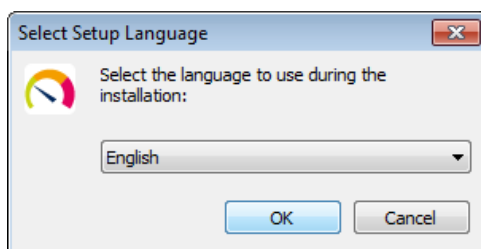
3.3 Install a PRTG Core Server

Installing PRTG is easy. It is similar to other Windows-based applications. To install the application please run the installation setup program from the ZIP file that you have downloaded.



Windows User Account Control Confirmation Request

Confirm the question of the Windows User Account Control with **Yes** to allow the program to install. The usual software installation wizard will guide you through the installation process.



Setup Language Selection

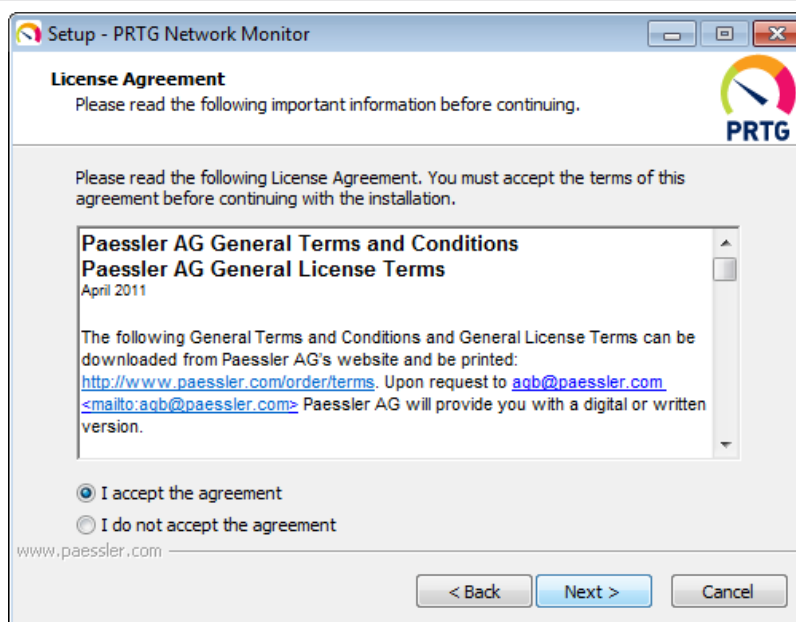
Please select a language for your product and click the **OK** button. The available language options depend on both your Windows version and the setup file.

Part 3: Installing the Software | 3 Install a PRTG Core Server



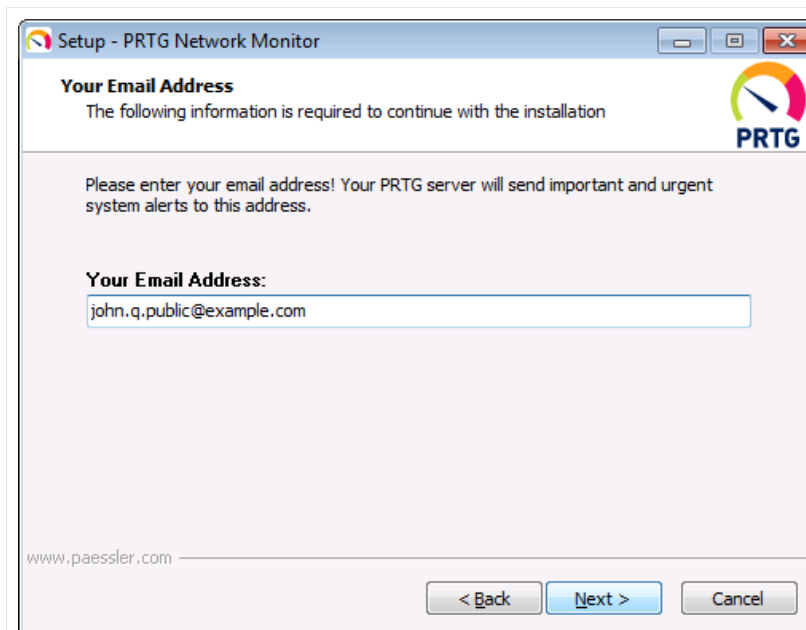
Setup Wizard Start Screen

Please click **Next** to walk through the wizard.



Setup Wizard License Agreement

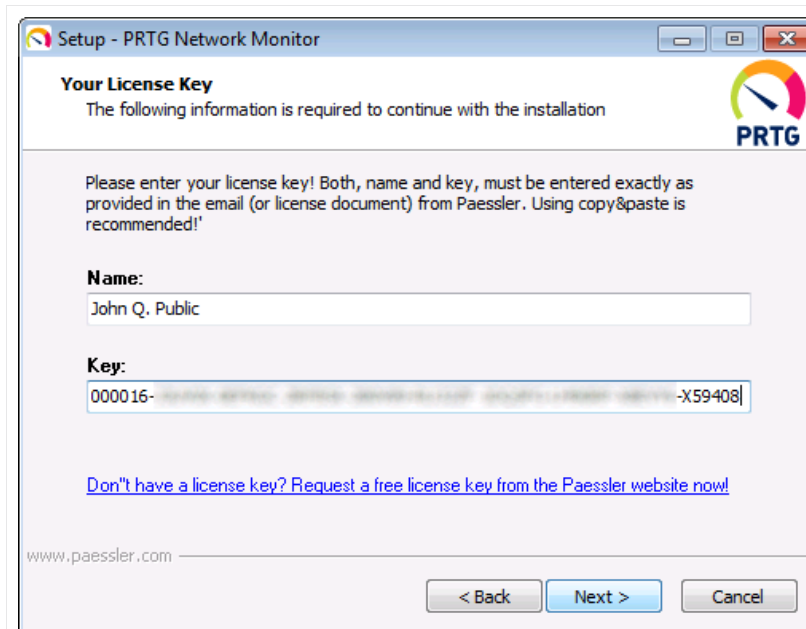
Please accept the license agreement and click **Next**.



The screenshot shows the 'Setup - PRTG Network Monitor' window. The title bar includes the PRTG logo and standard window controls. The main heading is 'Your Email Address'. Below it, a message states: 'The following information is required to continue with the installation'. A sub-message reads: 'Please enter your email address! Your PRTG server will send important and urgent system alerts to this address.' There is a text input field labeled 'Your Email Address:' containing the email 'john.q.public@example.com'. At the bottom left is the URL 'www.paessler.com'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

Administrator Email Address

Please enter a valid email address. Your PRTG server will send important and urgent system alerts to this address. Click the **Next** button to continue.

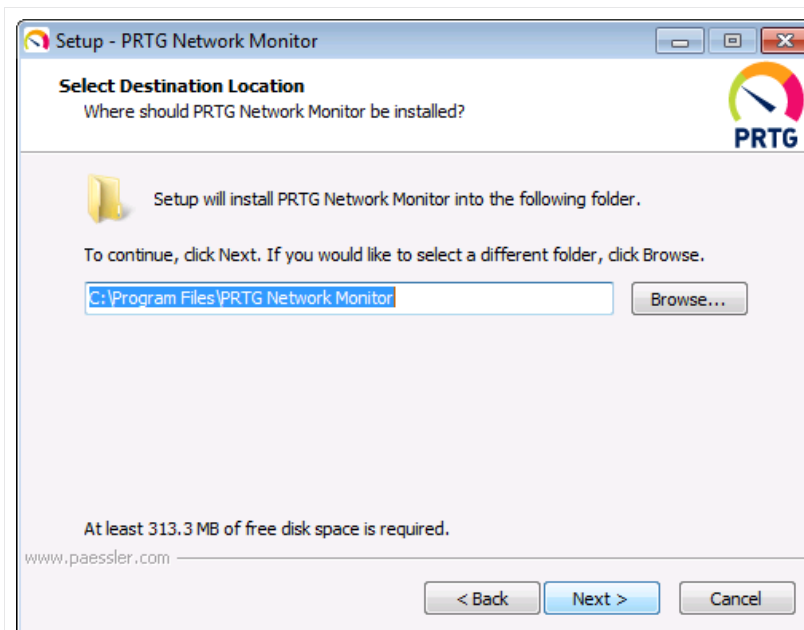


The screenshot shows the 'Setup - PRTG Network Monitor' window. The title bar includes the PRTG logo and standard window controls. The main heading is 'Your License Key'. Below it, a message states: 'The following information is required to continue with the installation'. A sub-message reads: 'Please enter your license key! Both, name and key, must be entered exactly as provided in the email (or license document) from Paessler. Using copy&paste is recommended!'. There are two text input fields: 'Name:' containing 'John Q. Public' and 'Key:' containing '000016-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-X59408'. Below the key field is a blue hyperlink: 'Don't have a license key? Request a free license key from the Paessler website now!'. At the bottom left is the URL 'www.paessler.com'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

License Key Information

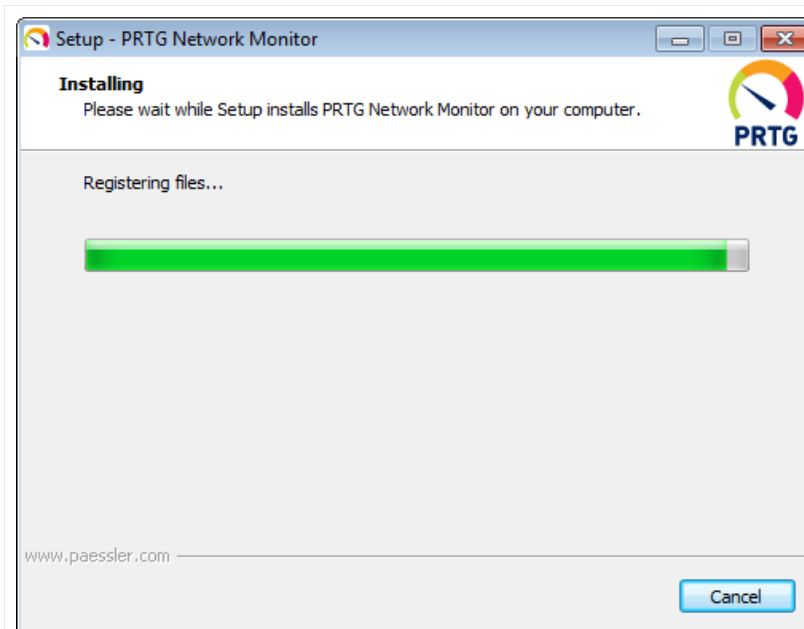
Please choose the folder you wish to install the software in. We recommend using the default value.

Part 3: Installing the Software | 3 Install a PRTG Core Server



Setup Wizard Destination Location

As soon as you click **Next**, the necessary files will be copied to your disk.



Setup Wizard Installing

After installation, the [Ajax Web Interface](#)^[100] is opened in your system's default browser. Please make sure there is Google Chrome 31 or later (recommended), Mozilla Firefox 25 or later, or Microsoft Internet Explorer 10 or 11 available on the system, and set as default browser (see [System Requirements](#)^[21]).

Enter License Information

Only if you entered incorrect license information before you will be asked to enter a correct license name and key.

PAESSLER PRTG Network Monitor

Enter License Key

Name: John Q. Public

Key: 0000- - - - - 9408

Instructions:

Please request a free trial key from the [Paessler Website](#). It consists of two parts: The **license name** (usually the company name) and the **license key** (10 groups of 6 letters and numbers each, separated by a dash). It is recommended to use copy&paste via the clipboard to make sure that both strings are entered exactly as given in your license document.

Product:	PRTG Network Monitor 100 with 12 months maintenance
License name:	My Company Name Inc.
License key:	0e#5V8-1JQdED-SB10KC-H85ZQ9-548C61-8QTH91-QWCH99-5MY
Download:	Download link

< Back Next >

Welcome Wizard Enter License Information

Please enter both **Name** and **Key** exactly as stated in the email received from Paessler. We recommend using copy&paste to avoid typing mistakes. For details, please see [Enter a License Key](#)^[57].

More

Knowledge Base: What is the PRTG Special Edition license?

- <http://www.paessler.com/knowledgebase/en/topic/8063>

Knowledge Base: How can I establish a secure web interface connection to PRTG?

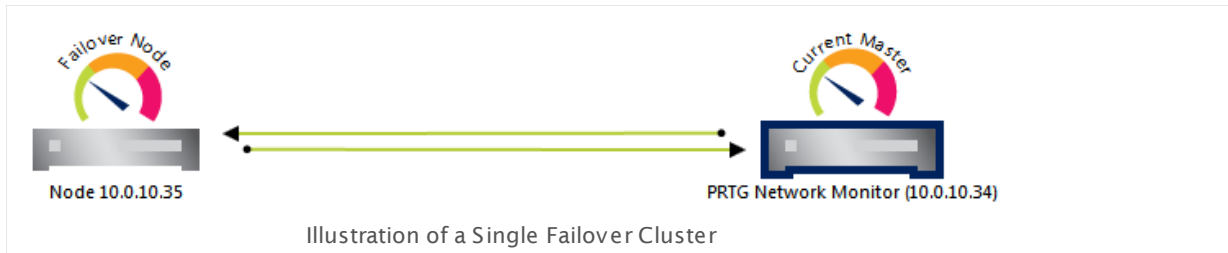
- <http://www.paessler.com/knowledgebase/en/topic/273>

Knowledge Base: PRTG blocks port 80 although I'm using SSL on port 443. How to free port 80?

- <http://www.paessler.com/knowledgebase/en/topic/5373>

3.4 Install a PRTG Cluster

PRTG offers single failover clustering in all licenses—even using the freeware edition. A single failover cluster consists of two servers ("Current Master" Node and "Failover Node"), each of them running one installation of PRTG. They are connected to each other and exchange configuration and monitoring data. You can run a cluster with up to 5 nodes.



For detailed information, please see [Failover Cluster Configuration](#) .

More

Knowledge Base: What's the Clustering Feature in PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/6403>

3.5 Enter a License Key

A license key for PRTG Network Monitor consists of the license name and a license key. The key is a string consisting of approx. 70 characters.

Your Personal License Information

You should have received license name and key via email. This is either the information for a Trial or a Commercial Edition.

Example of License Information

License Name: **John Q. Public**
License Key: **0223515-FFSEJC-ZHGRDFM-UR1CS8-U73FGK-G645F2-YVF1DD-H8323N-D11HG9-M2DRG**

During the setup process, PRTG will ask you to enter your license information. Please use copy and paste to fill out the form in the dialog shown by the installer.

- **Trial/Freeware license key:** When entering a Trial license key you can experience unlimited functionality of PRTG during the trial period. Your installation will automatically switch to a Freeware Edition afterwards. In details how to get your free Trial installer, please see [Download PRTG](#)^[45] section.
- **Commercial license key:** This key can only be entered if you install the Commercial Edition of PRTG, available for download in the customer service center. See [Download PRTG](#)^[46] section for details. Your installation will allow the number of sensors according to your license.

Change License Key

Usually you do not need to enter a key manually, as it is prompted during installation. However, there are still scenarios where you want to change your key, for example, when switching from a Trial Edition to a [Special Edition](#)^[19].

If you need to enter new license information, please follow these steps.

Step 1: Make Sure You Have Installed the Correct Edition

Please check first if you have installed the proper edition and then enter the license key.

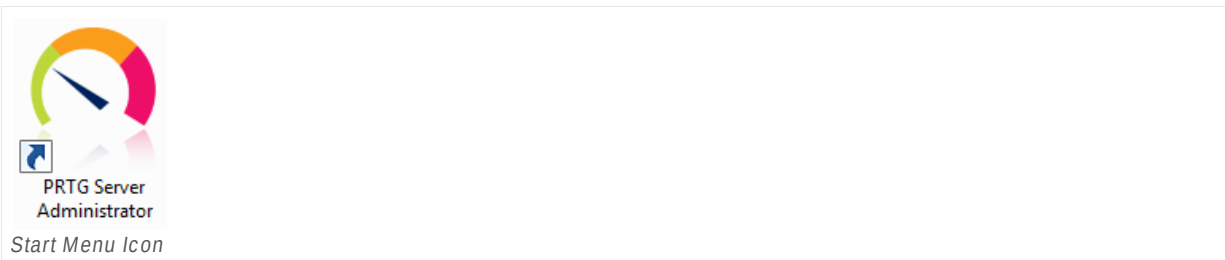
There are two different installers available for PRTG (see [Download](#)^[45] section):

- The publicly available installer only contains the Freeware, Special, and Trial Editions. It does not accept any commercial license keys.
- The Commercial installer is only available for download to paying customers.

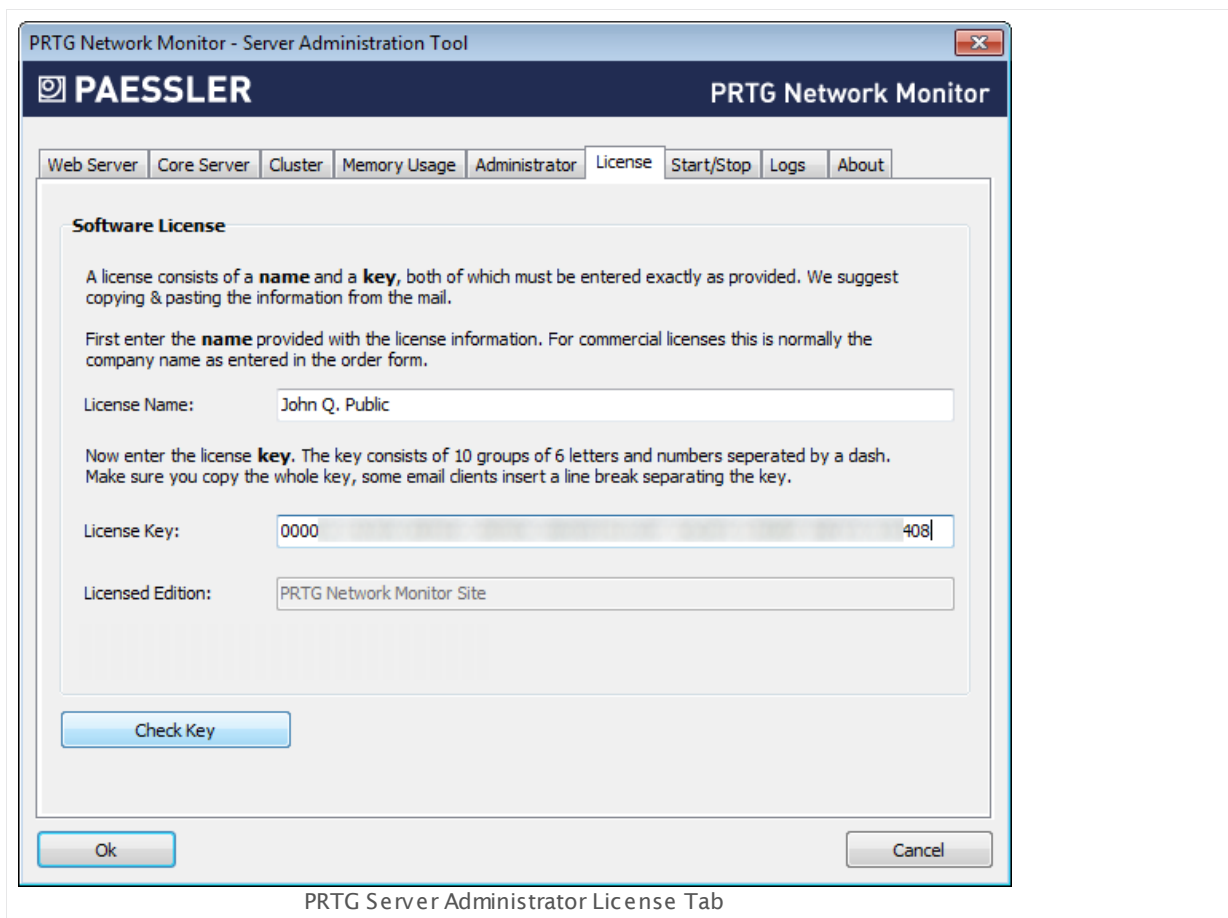
The Commercial Installer must be installed to run the commercial editions of PRTG Network Monitor. **If you have purchased a license key for PRTG, please download and install the latest Commercial Installer from the Paessler website in order to apply your license key.** **Note:** You can install a commercial version "on top" of an existing Trial Edition in order to maintain your configuration and monitoring data.

Step 2: Enter the License Key in the PRTG Server Administrator

Please start the **PRTG Server Administrator** program from the Windows Start Menu. In the program, select the **License** tab.



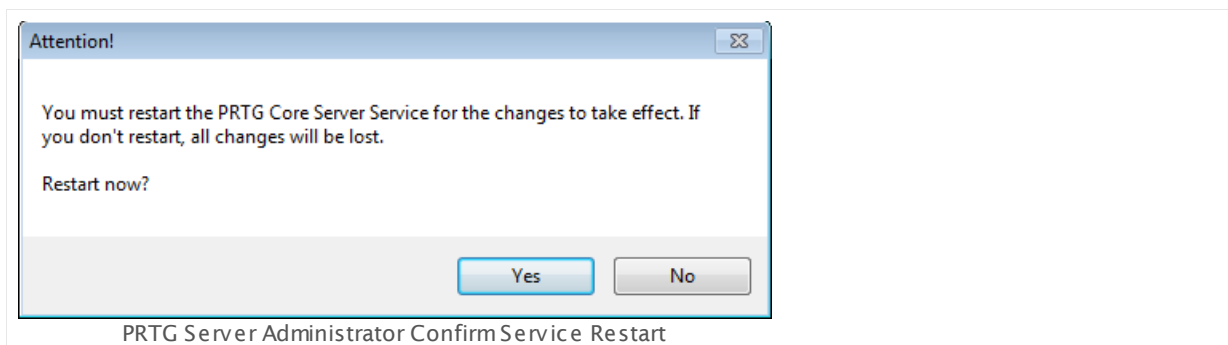
To use a PRTG license with this installation of PRTG, please enter the license information you have received from Paessler via email. To avoid typing errors, please copy and paste both the **License Name** and the **License Key** from the email. Both must be transferred exactly as shown in the email.



To make sure your key has been entered correctly please click on the **Check Key** button. A popup box will either show success or denial of your license information. License information is also checked if you change tabs.

In the **Licensed Edition** field you will see an accepted license key.

Click on the **Ok** button to save and confirm to restart the core server service by clicking on the **Yes** button.



3.6 Activate the Product

PRTG tries to activate your license automatically via the internet on first start up. Only if PRTG cannot connect to the internet directly, the web interface will display a **Software Activation Required** notice.

You have to run through the product activation process once in order to use PRTG continuously (only Freeware and Trial Edition are always activated automatically and do not require a special procedure). The activation has to be done within ten days after installation and only takes a few minutes. If you do not activate PRTG for ten days, it will temporarily revert to the Freeware Edition (with a maximum of 10 sensors) until you activate. [Login to the PRTG web interface](#)^[102] to activate.

Activate via Internet

In the PRTG web interface, choose **Setup | PRTG Status | Activation Status** from the main menu.

Click on the button **Start Activation Now** to start product activation. PRTG will now connect with the Paessler license server to check your license (via SSL on port 443). A few seconds later you should see **Activation OK** in the License Activation Status.

Note: The PRTG core server needs an internet connection on port 443 to activate. If a proxy connection is needed, please configure it in the [System Administration—System and Website](#)^[181] settings. Please see [More](#)^[61] section for details about activation servers. In case activation fails, you can activate via email.

Activate via Email

In the PRTG Web Interface, choose **Setup | PRTG Status | Activation Status** from the main menu.

If there is no internet connection available, you can activate PRTG via email. To do so, first click on the **Start Activation Now** button. You will then see **Last message about activation: Activation failed** in the License Activation Status.

- Once the activation via internet fails, the activation via email is available.
- Click on the **Start Activation per Email** tab. You will see an **Activation Request Code**.
- Copy it and send it to the email address shown.
- Within two business days you will receive an email reply from Paessler, containing an activation code.
- Once you've received this email, go the **Finalize Activation per Email** tab and copy the activation code into the according field. **Note:** Please make sure you only copy the code itself and nothing else from the email. Also, please omit the "Activation Code Start/End" markers.
- Click on **Confirm Activation**.

A few seconds later you should see **Activation OK** in the License Activation Status.

More

Knowledge Base: Which servers does PRTG connect to for Software Auto-Update and for Activation?

- <http://www.paessler.com/knowledgebase/en/topic/32513>

3.7 Install a PRTG Remote Probe

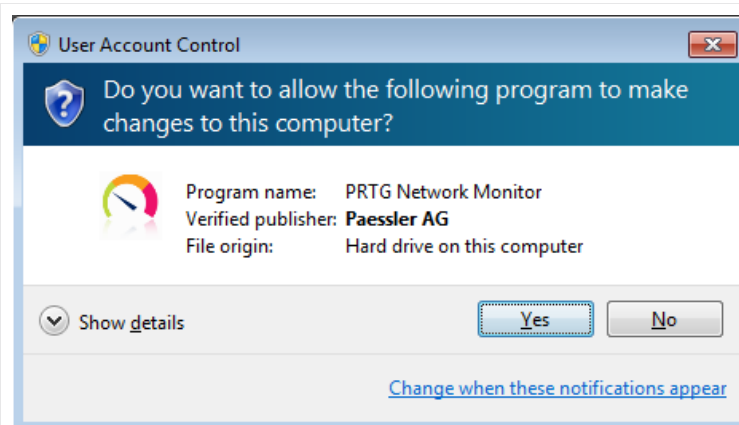
The local probe is already included in a [PRTG core server installation](#)^[51]. You can install additional remote probes on other computers in order to take load from the system running the core installation or to extend monitoring to distributed networks. **Note:** You cannot install a remote probe on a system already running a PRTG core installation.

Download Remote Probe Installer from the Web Interface

The remote probe version has to fit the PRTG core server version you will connect to. In order to download your setup program to the computer you want to install it on, please [connect to the Ajax web interface](#)^[102]. On the [login screen](#)^[102], enter login name and password and from the main menu, select **Setup | Downloads / Add-Ons | Remote Probe Installer**. Click on the **Download: Remote Probe Installer** button. Your browser will show a download dialog. Save the setup program to your local hard disk drive.

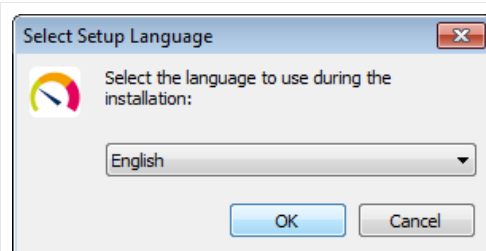
Install Remote Probe

Please execute the setup program you've just downloaded.



Windows User Account Control Confirmation Request

Confirm the question of the Windows User Account Control with **Yes** to allow the program to install. The usual software installation wizard will guide you through the installation process.



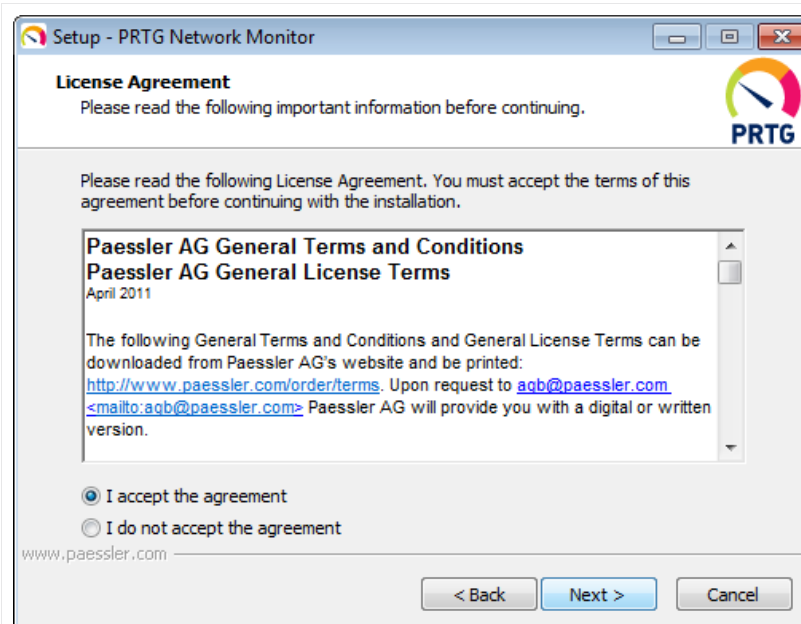
Setup Language Selection

Please select a language for your product and click the **OK** button. The available language options depend on both your Windows version and the setup file.



Remote Probe Setup Wizard Welcome Screen

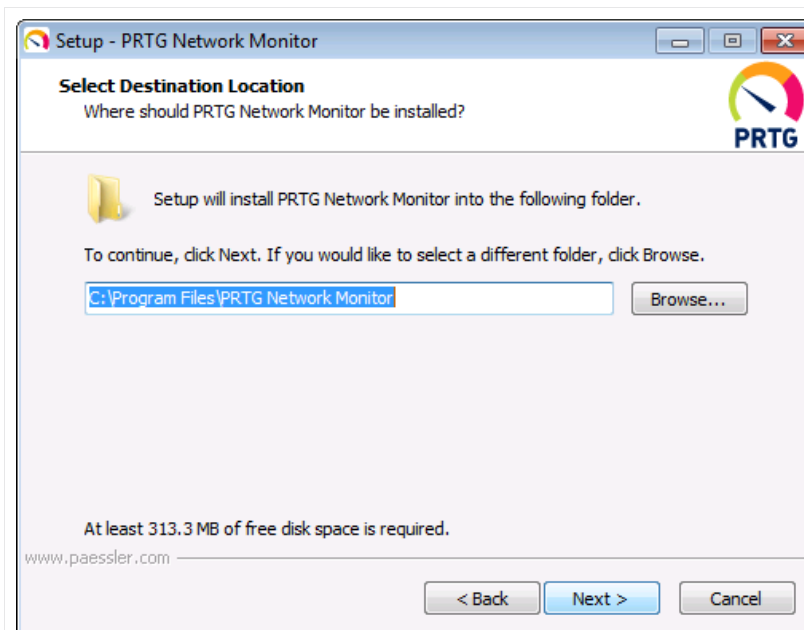
Please click **Next** to walk through the wizard.



Setup Wizard License Agreement

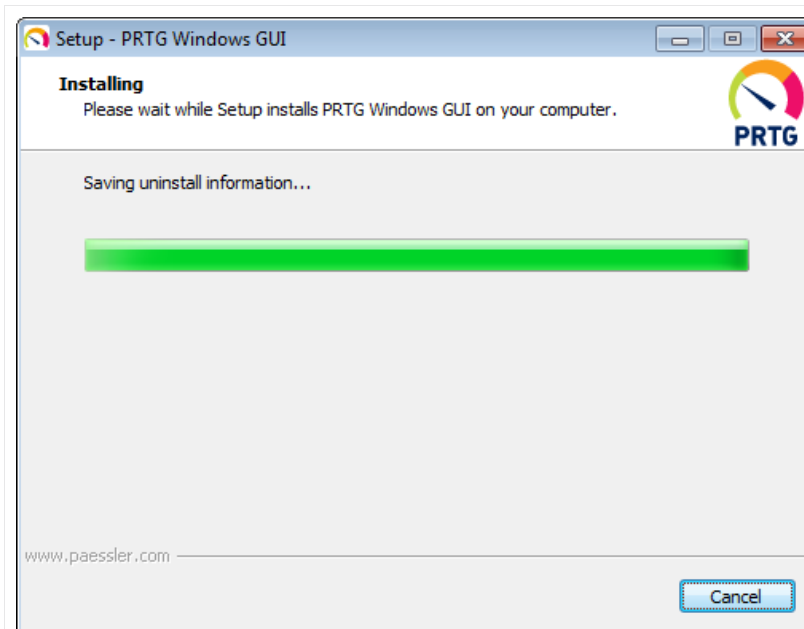
After accepting the license agreement, you can choose the folder you wish to install the software in. We recommend using the default value.

Part 3: Installing the Software | 7 Install a PRTG Remote Probe



Setup Wizard Destination Location

As soon as you click **Next**, the necessary files will be copied to your disk.



Windows GUI Setup Wizard Install

The PRTG Probe Administrator is shown. Please enter the correct settings in order to connect with your PRTG core installation. See [Remote Probe Setup](#) ²⁰²⁰ section for more information. Click **Ok** to continue.

PRTG Network Monitor - Probe Administration Tool

PAESSLER PRTG Network Monitor

Probe Settings | Outgoing IP Settings | Start/Stop | Logs / Directory | About

Probe Settings

Name of Probe: Probe on 10.0.9.45 Reconnect Time: 300 sec

Connection to PRTG Core Server

Configured as Remote Probe: Connect to a core server using the following settings

Server (IPv4 address or DNS name): 10.0.10.34 Port: 23560 (Standard: 23560)

Probe GID: {4FBA6B3E-AAE5-4CF3-9975-08B88C09679F} Edit GID...

Probe Access key: Confirm Access Key:

Language

English

Ok Cancel

Probe Settings in PRTG Probe Administrator

When asked if you want to start the probe service, confirm with **Yes**. The installation is completed.

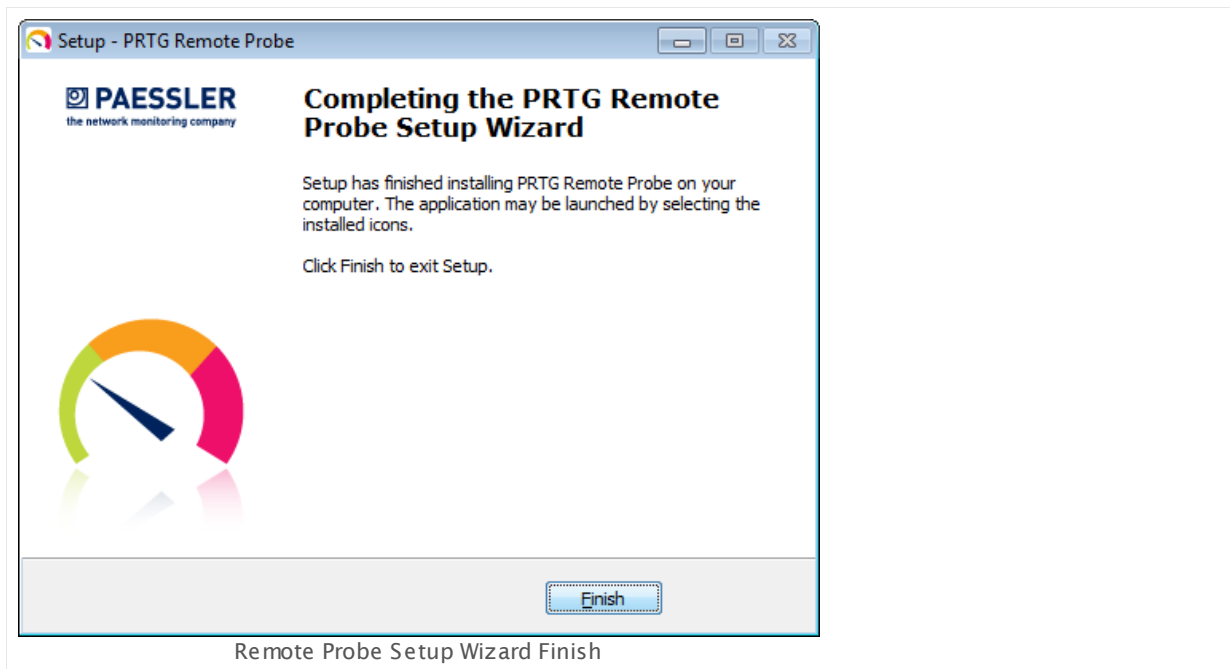
Attention!

The PRTG 8 Probe Service is not running. Do you wish to start it?

Yes No

PRTG Probe Administrator Start Service Request

After installation, click **Finish**.



Your remote probe is now installed on this computer as Windows service.

More

After you click the **Finish** button, the PRTG Probe Administrator is shown, allowing you to configure connections. Please see section [Remote Probe Setup](#)^[2020] for more information on how to connect the remote probe with your PRTG core server installation.

Note: You can also install a Remote Probe directly from PRTG's web interface. For details, refer to [Remote Probe Quick Install](#)^[2015].

3.8 Install the Enterprise Console

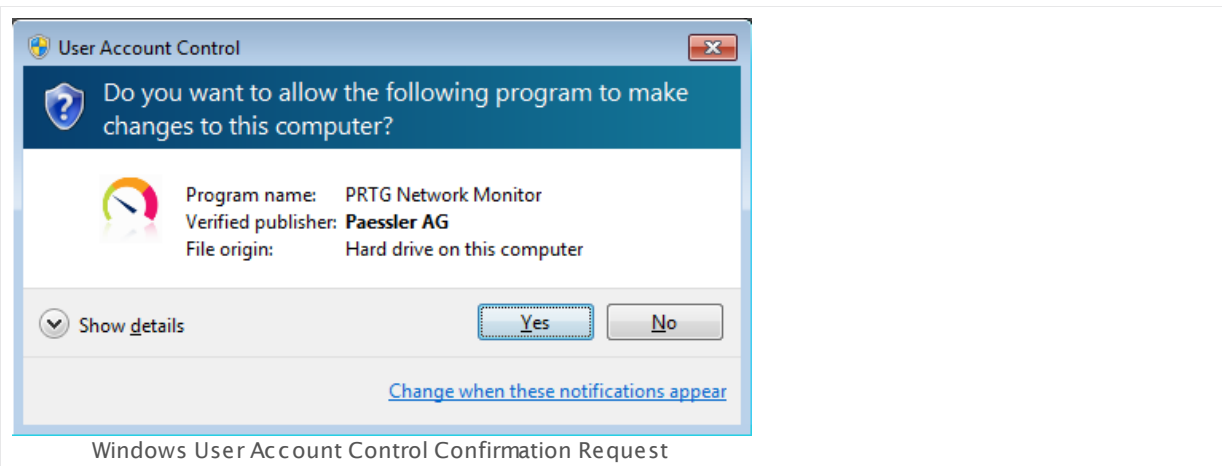
The Enterprise Console is already included in a [PRTG core server installation](#)^[51]. You can install additional Enterprise Consoles on other computers.

Download Enterprise Console from the Web Interface

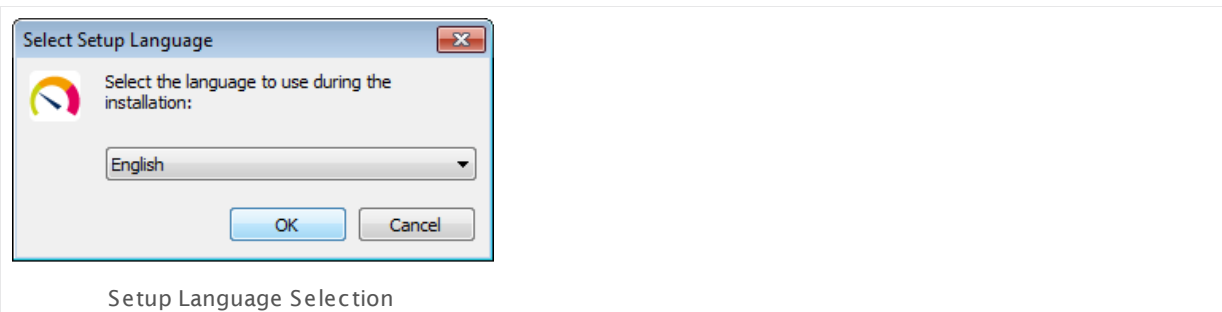
The version of the Enterprise Console has to fit exactly the PRTG core server version you will connect to. From the computer you want to install the Enterprise Console on, please connect to the [Ajax](#)^[100] web interface. On the [login screen](#)^[102] of the web interface, enter login name and password and select the **Enterprise Console (Download for Windows)** option. Your browser will show a download dialog. Save the setup program to the local hard disk drive.

Install Enterprise Console

Please execute the setup program you just have downloaded.

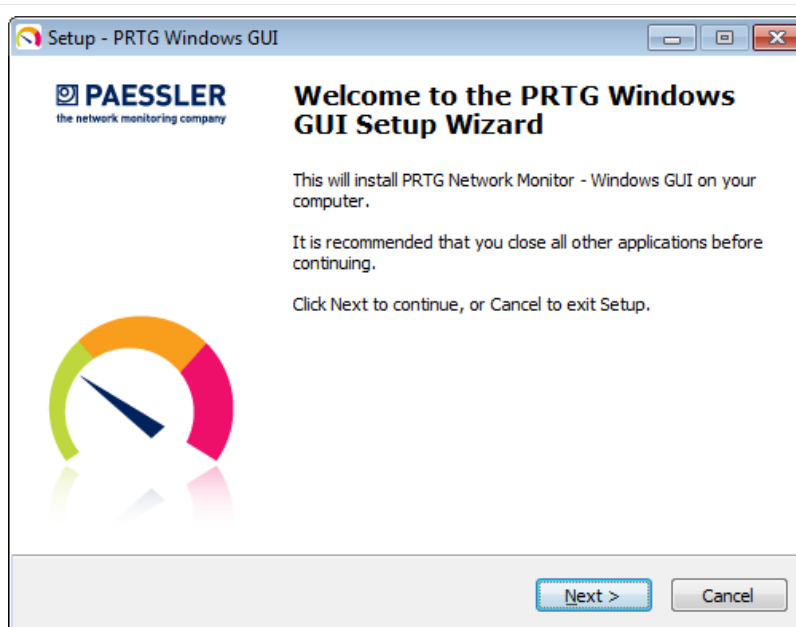


Confirm the question of the Windows User Account Control with **Yes** to allow the program to install. The usual software installation wizard will guide you through the installation process.



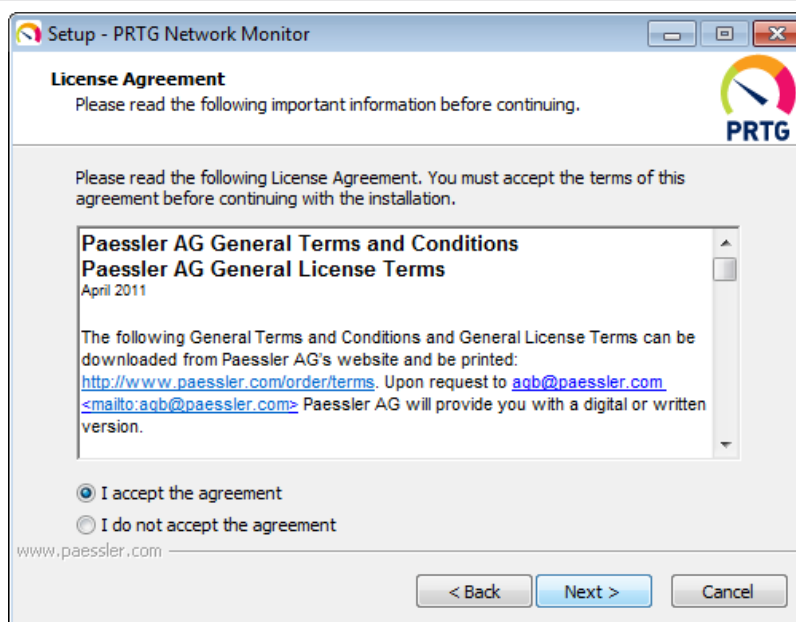
Please select a language for your product and click the **OK** button. The available language options depend on both your Windows version and the setup file.

Part 3: Installing the Software | 8 Install the Enterprise Console



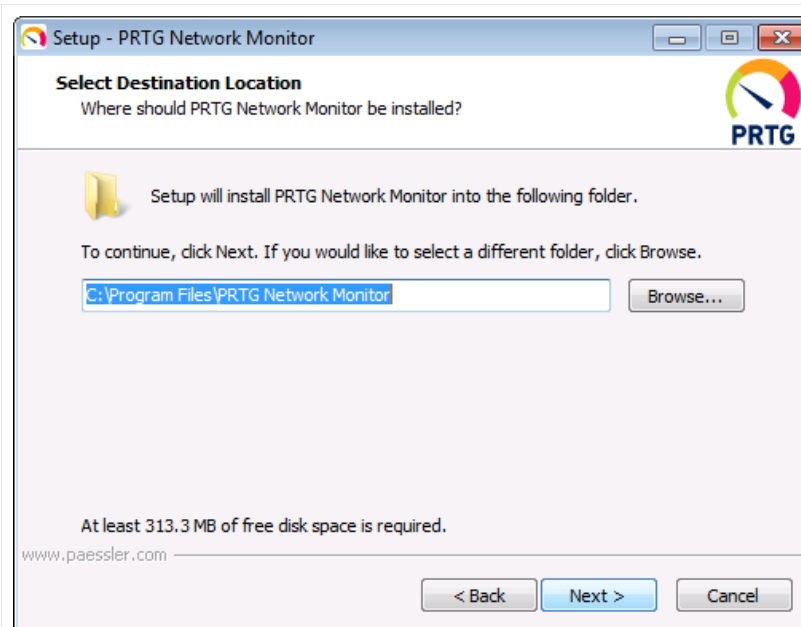
Windows GUI Setup Wizard Welcome Screen

Please click **Next** to walk through the wizard.



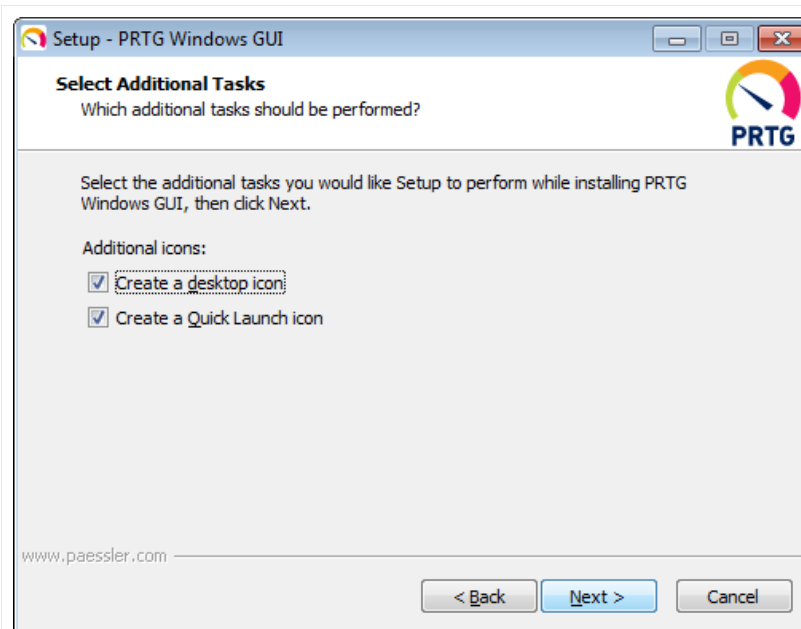
Setup Wizard License Agreement

After accepting the license agreement, you can choose the folder you wish to install the software in. We recommend using the default value.



Setup Wizard Destination Location

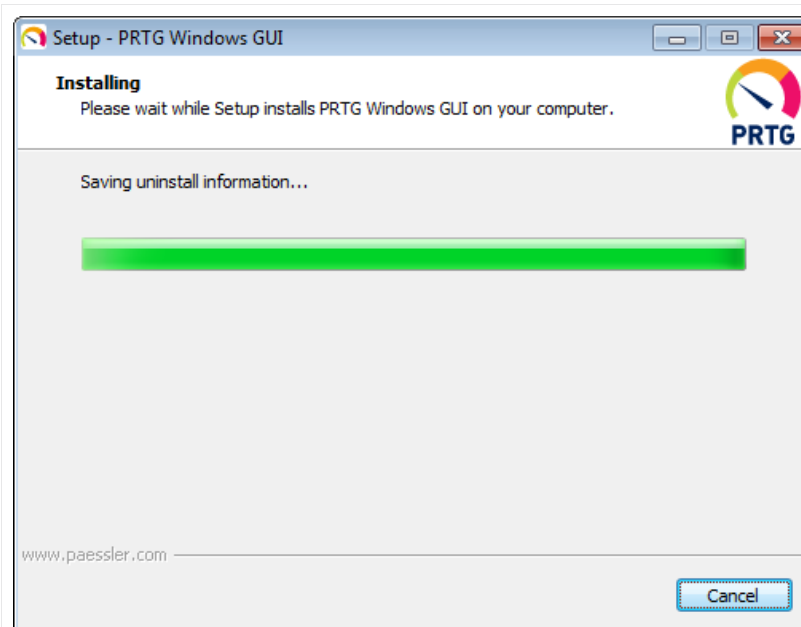
Select which icons will be created. We recommend using the default value.



Windows GUI Setup Wizard Additional Tasks

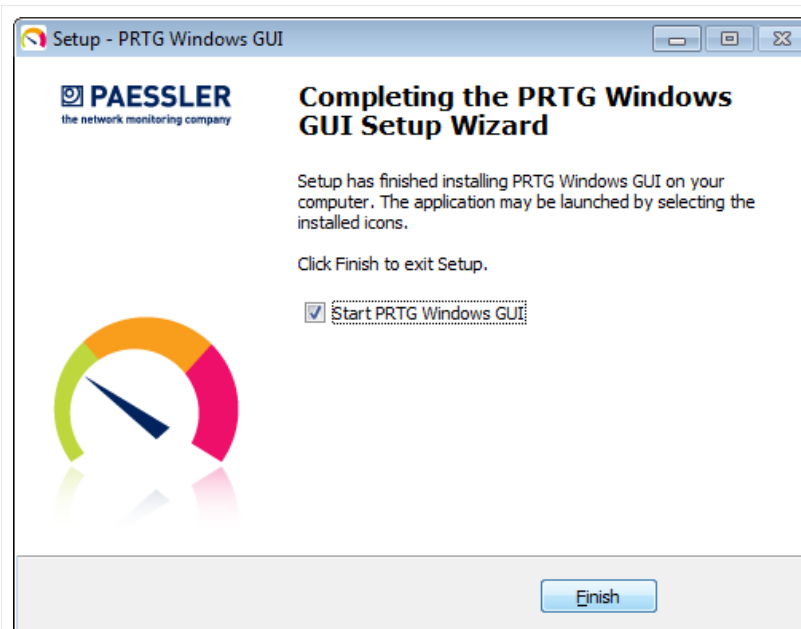
As soon as you click **Next**, the necessary files will be copied to your disk.

Part 3: Installing the Software | 8 Install the Enterprise Console



Windows GUI Setup Wizard Install

After installation, click **Finish** to start the Enterprise Console.



Windows GUI Setup Wizard Finish

More

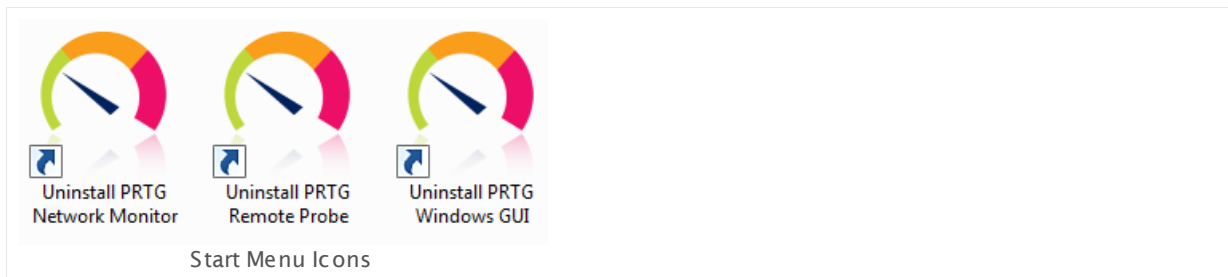
Please see section [Enterprise Console](#) ¹⁸⁶⁰ for more information on how to use this Graphical User Interface (GUI).

3.9 Uninstall PRTG Products

The uninstall process has six steps—regardless of if you are uninstalling an entire PRTG Network Monitor installation, a single Enterprise Console installation, or a PRTG Remote Probe installation. Use the Windows uninstall routines to remove the PRTG software from your system.

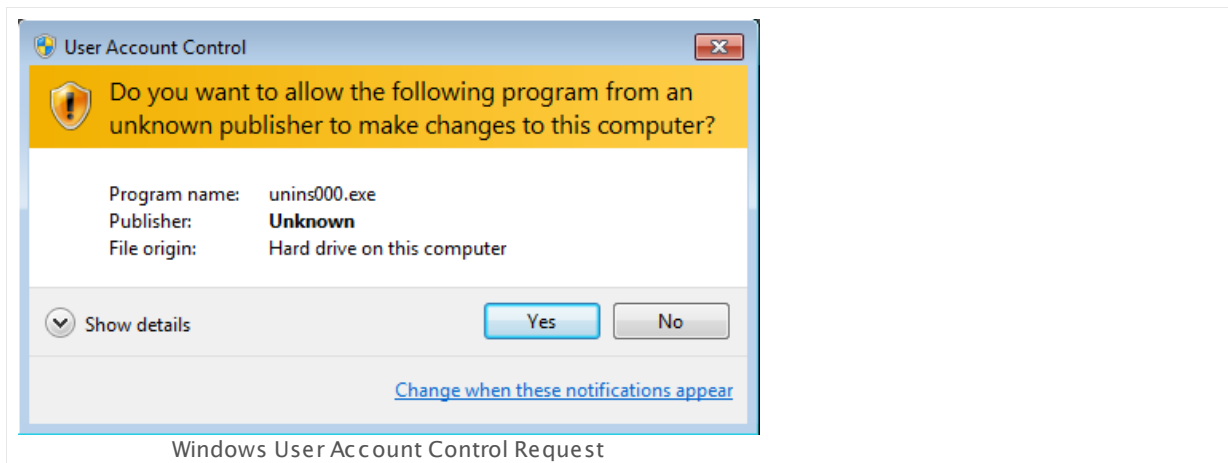
Step 1

From the Windows Start Menu, select the **Uninstall PRTG Network Monitor** icon, the **Uninstall PRTG Enterprise Console** icon, or the **Uninstall PRTG Remote Probe** icon, or open your Windows Control Panel and choose the respective entry in the **Programs** section. Depending on the installed products, not all uninstall programs are available.



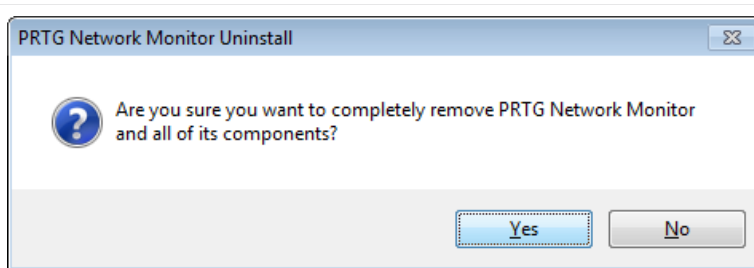
Step 2

If asked, confirm the question of the Windows User Account Control with **Yes** to allow the program to uninstall. The usual software uninstall wizard will guide you through the uninstall process.



Step 3

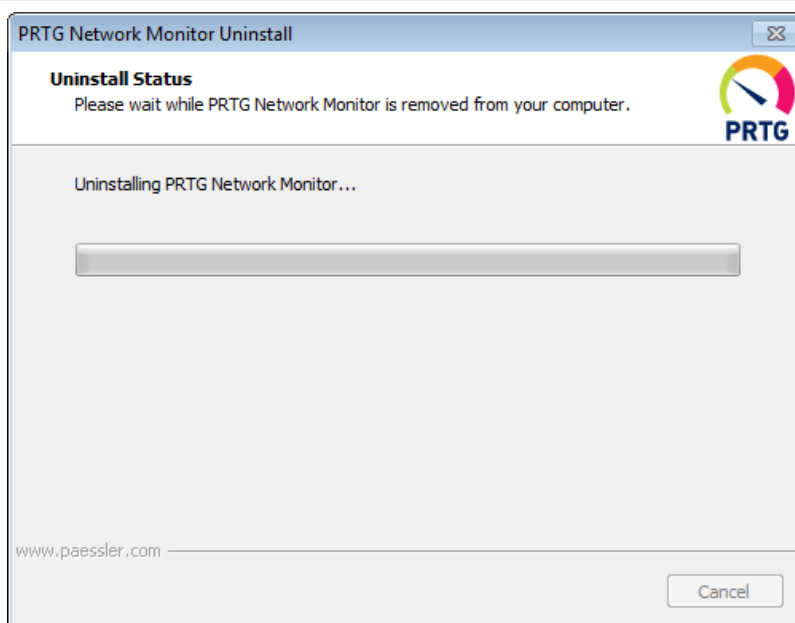
Confirm the removal of the software by clicking the **Yes** button.



Uninstall PRTG Network Monitor Step 1

Step 4

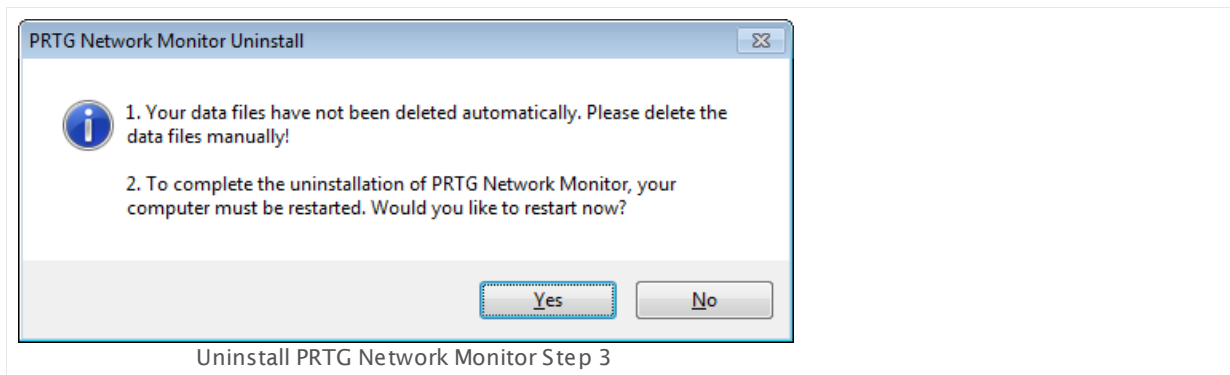
Wait while the software is being removed.



Uninstall PRTG Network Monitor Step 2

Step 5

Confirm a system restart by clicking the **Yes** button.



Step 6

After system restart, the software is removed. However, there are still custom data in the PRTG program folder left. If you have uninstalled an entire PRTG Network Monitor installation or a remote probe installation, your monitoring data is still stored on the system. To completely remove all PRTG data, please delete the **PRTG Network Monitor** program folder as well as the **Paessler\PRTG Network Monitor** folder in your data path. For more information where data is stored see [Data Storage](#) 2036 section.

More

Knowledge Base: Can we remotely and silently uninstall a Remote Probe?

- <http://www.paessler.com/knowledgebase/en/topic/27383>

Part 4

Understanding Basic Concepts

4 Understanding Basic Concepts

There are a number of basic concepts that are essential for understanding the functionality and ease of use of PRTG Network Monitor. We have made using our software as easy as possible; setting it up for the first start and getting first monitoring results happens almost automatically. Nevertheless, there are some basic principles we would like to explain to you. Please read this section carefully to understand the underlying workflow like architecture of the monitoring system, hierarchy of objects, settings inheritance, notifying, etc. Afterwards, you will be able to enhance your monitoring experience permanently.

Understanding Basic Concepts—Topics

- [Architecture and User Interfaces](#) ⁷⁷
- [Clustering](#) ⁸¹
- [Object Hierarchy](#) ⁸³
- [Inheritance of Settings](#) ⁸⁷
- [Tags](#) ⁸⁹
- [Dependencies](#) ⁹⁰
- [Scheduling](#) ⁹¹
- [Notifying](#) ⁹²
- [Data Reporting](#) ⁹³
- [User Access Rights](#) ⁹⁴
- [IPv6](#) ⁹⁷

4.1 Architecture and User Interfaces

PRTG Network Monitor consists of different parts which can be divided into three main categories: System parts, control interfaces, and basic administration interfaces.

Type	Part of PRTG
System Parts	Core Server  ⁷⁸ This is the central part of a PRTG installation and includes data storage, web server, report engine, a notification system, and more. The core server is configured as Windows service which runs permanently.
	Probe(s)  ⁷⁸ The part of PRTG on which the actual monitoring is performed. There are local probes, remote probes, and cluster probes available. All monitoring data is forwarded to the central core server. Probes are configured as Windows services which run permanently.
User Interfaces	Ajax Web Interface  ¹⁰⁰ The Ajax-based web interface is used for configuration of devices and sensors, as well as the review of monitoring results. Also system administration and user management are configured here.
	Enterprise Console  ¹⁸⁹⁰ A native Windows application (former Windows GUI) as alternative to the web interface to manage your monitoring. With the Enterprise Console, you can connect to different independent PRTG core server installations and review their data at a glance!
	Mobile Web GUI  ¹⁹¹³ A read-only interface optimized for mobile access to your PRTG installation. View latest states, tables, and graphs. Using jQuery Mobile, this interface is compatible with almost all mobile devices available on the market, as well as with older and unsupported browser versions.
	Smart Phone Apps  ¹⁹¹⁶ Monitor your network on the go with PRTG and apps for iOS and Android devices.
System Administration Programs	PRTG Server Administrator  ¹⁹⁵⁰ Used to configure basic core server settings, such as administrator login, web server IPs and port, probe connection settings, cluster mode, system language, and more.

Type	Part of PRTG
	PRTG Probe Administrator ¹⁹⁷⁹ Used to configure basic probe settings such as name of the probe, IP and server connection settings, and more.

Core Server

The core server is the heart of your PRTG system and performs the following processes:

- Configuration management for object monitoring
- Management and configuration of the connected probes
- Cluster management
- Database for monitoring results
- Notification management including a mail server for email delivery
- Report generator and scheduler
- User account management
- Data purging (culling data that is older than 365 days, for example)
- Web server and API server

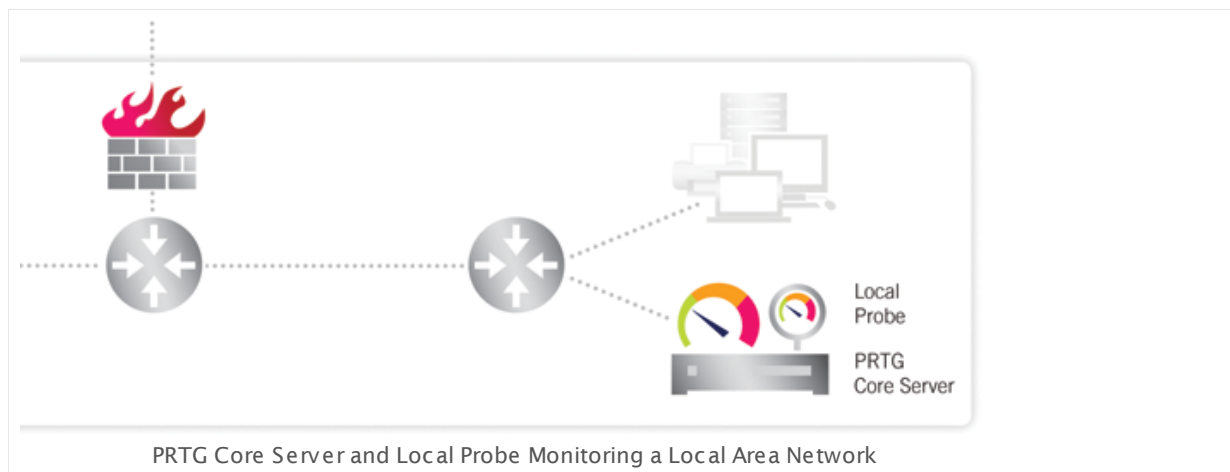
In a [cluster](#)⁸¹, the current master node is responsible for all of these tasks.

The built-in, fast, and secure web server (no additional IIS or Apache is required) supports HTTP as well as secure HTTPS (via SSL). It serves the web interface when accessed with a browser and also answers PRTG Application Programming Interface (API) calls (for example, for user scripts or the Enterprise Console).

Note: Core server and probe(s) are configured as Windows services which are permanently run by the Windows system without the requirement for a logged-in user.

Probe(s)

On a probe, PRTG performs the actual monitoring with the sensors created on a device (for example, computer, router, server, firewall, etc.). The probe receives its configuration from the core server, runs the monitoring processes, and delivers monitoring results back to the core server. On every system running a PRTG core server, there is always a local probe running with it on the same machine.



The actual monitoring is performed by PRTG probe processes which run on one or more computers. During installation, the system automatically creates the so-called **Local Probe**. In a single-probe installation—which is the default setup—the local probe performs all monitoring.

The PRTG core server inside the corporate LAN (bottom right in the figure above) is able to monitor services and servers in the entire Local Area Network (LAN). **Note:** Core server and probe(s) are configured as Windows services which are permanently run by the Windows system without the requirement for a logged-in user.

In a [cluster setup](#)^[81], a cluster probe runs on all nodes. There is an additional so-called **Cluster Probe**. All devices created on it are monitored by all nodes in the cluster, so data from different perspectives is available and monitoring for these devices always continues, also if one of the nodes fails.

PRTG automatically monitors system health of its own core server and of each probe in order to discover overloading situations that may distort monitoring results. To monitor the system status of the probe computer, PRTG automatically creates a few sensors. These include **Core** and **Probe Health**, **System Health**, **Cluster Probe Health**, **Disk Free**, and a bandwidth sensor for all installed network cards. We recommend keeping these sensors, but you can optionally remove all except the **Health** sensors. They measure various internal system parameters of the probe system hardware and the probe's internal processes and then computes a resulting value. Frequent or repeated values below 100% should be investigated. Please check the [channels](#)^[124] of a particular sensor for details.

Additional so-called **Remote Probes** can be created by the user in order to achieve monitoring of multiple locations, or for several other scenarios. They are using SSL-secured connections to the core and allow to securely monitor services and systems inside remote networks which are not openly accessible or secured by firewalls. For more information, please see [Remote Probes and Multiple Probes](#)^[201] section. For a video on this please see [More](#)^[203] section below.

More

Video Tutorial: There is a video available on the Paessler video tutorials page.

- http://www.paessler.com/support/video_tutorials

4.2 Clustering

A PRTG Cluster consists of two or more [installations of PRTG](#)^[51] that work together to form a high availability monitoring system. The objective is to reach true 100% uptime for the monitoring tool. Using [clustering](#)^[2026], the uptime will no longer be degraded by failing connections because of an internet outage at a PRTG server's location, failing hardware, or because of downtime due to a software update for the operating system or PRTG itself.

How a PRTG Cluster Works

A PRTG cluster consists of one **Primary Master Node** and one or more **Failover Nodes**. Each node is simply a full installation of PRTG which could perform the whole monitoring and alerting on its own. Nodes are connected to each other using two TCP/IP connections. They communicate in both directions and a single node only needs to connect to one other node to integrate into the cluster.

During normal operation the **Primary Master** is used to configure devices and sensors (using the [web interface](#)^[100] or [Enterprise Console](#)^[1960]). The master automatically distributes the configuration to all other nodes in real time. All nodes are permanently monitoring the network according to this common configuration and each node stores its results into its own database. This way, the storage of monitoring results also is distributed among the cluster (the downside of this concept is that monitoring traffic and load on the network is multiplied by the number of cluster nodes, but this will not be a problem for most usage scenarios). The user can review the monitoring results by logging into the web interface of any of the cluster nodes in read only mode. Because the monitoring configuration is centrally managed, it can only be changed on the master node, though.

By default, all devices created on the **Cluster Probe** are monitored by all nodes in the cluster, so data from different perspective is available and monitoring for these devices always continues, even if one of the nodes fails. In case the **Primary Master** fails, one of the **Failover Nodes** takes over the master role and controls the cluster until the master node is back. This ensures a fail-safe monitoring with gapless data. **Note:** During the outage of a node, it will not be able to collect monitoring data. The data of this single node will show gaps. However, monitoring data for this time span is still available on the other node(s). There is no functionality to actually fill in other nodes' data into those gaps.

If downtimes or threshold breaches are discovered by one or more nodes, only one installation, either the Primary Master or the Failover Master, will send out notifications (via email, SMS text message, etc.). Thus, the administrator will not be flooded with notifications from all cluster nodes in case of failures.

Set Up a PRTG Cluster

For detailed information, please see [Failover Cluster Configuration](#)^[2026].

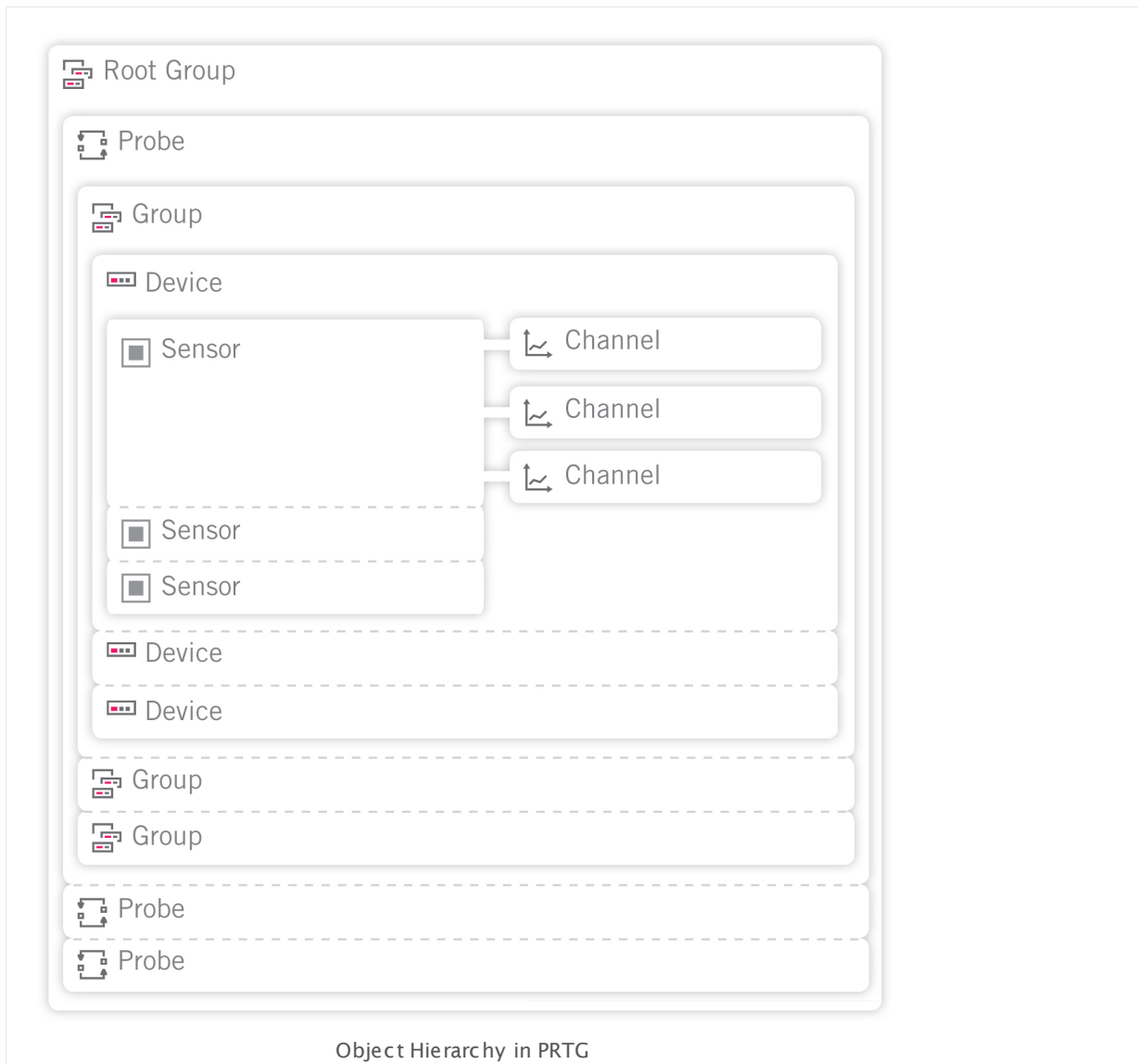
More

Knowledge Base: What's the Clustering Feature in PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/6403>

4.3 Object Hierarchy

All objects in a PRTG monitoring configuration are arranged in a tree-like hierarchy to create an easy to navigate list and to give the user the possibility to arrange them in groups that monitor similar devices, services, or same locations. The hierarchical order described is also used to define common settings for larger groups of objects, for example, settings of the **Root** group apply by default to all other objects underneath (see section [Inheritance of Settings](#)^[87]).



The figure shows the object hierarchy in PRTG:

- **Root** group contains all objects in your setup; all probes are directly under the root node.
- A **Probe** contains one or more groups.
- A **Group** contains one or more devices.

- A **Device** represents one component in your network which is reachable via an IP address. On a device are several sensors.
- A **Sensor** monitors one single aspect of a device and has at least one channel.
- A **Channel** receives the monitoring results and is part of a sensor.

Root Group

The **Root** group is the topmost instance in PRTG. It contains all other objects in your setup. Using the [inheritance](#)^[87] mechanism, we recommend [adjusting the default settings for the Root group](#)^[224]. This makes configuration easier later on, because all other objects inherit these standard settings by default and, thus, you will not have to set up the same configuration for each object anew.

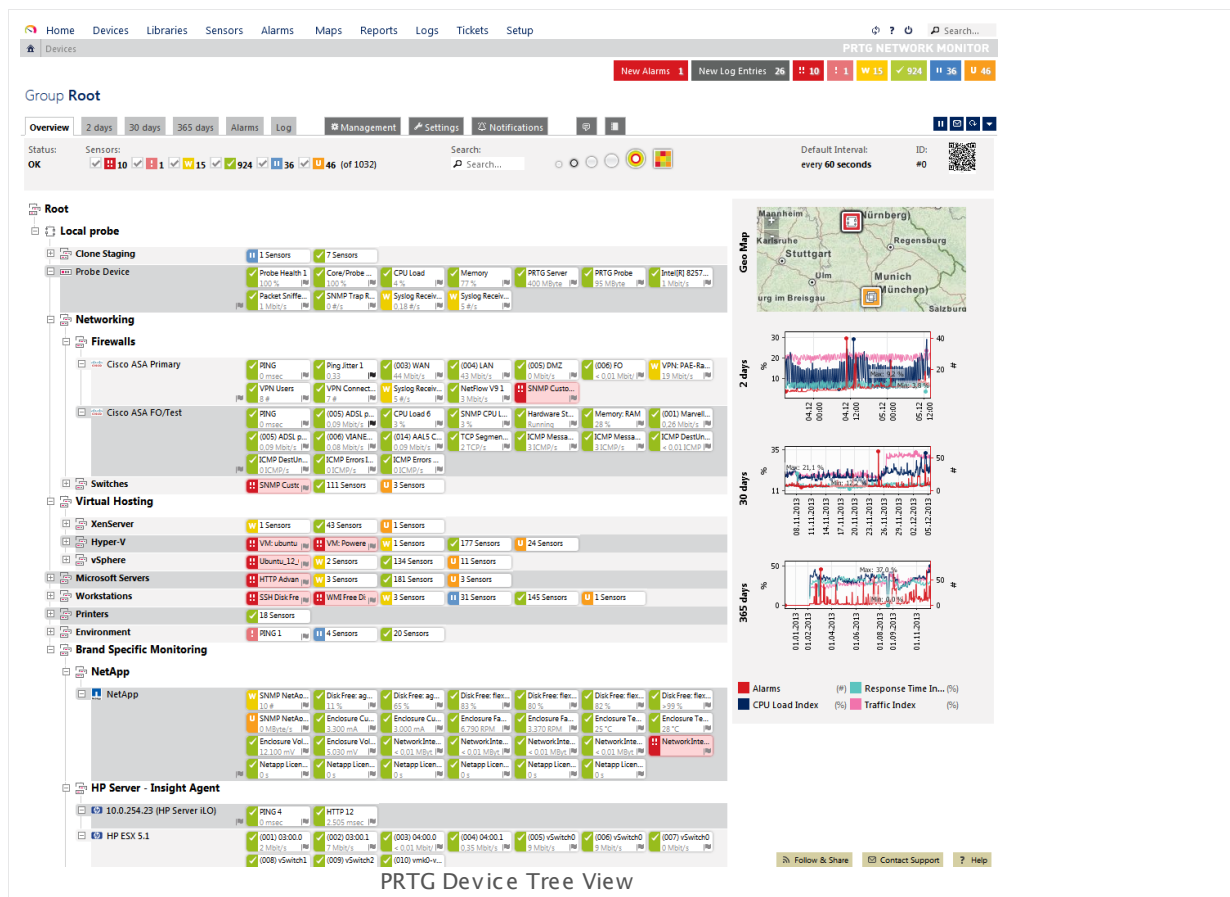
Probe

Each group (except the **Root** group) is part of a **Probe**. This is the platform on which the monitoring takes place. All objects configured below a probe will be monitored via that probe. Every PRTG core installation automatically installs a **Local Probe** service. You can add additional probes and remote probes to your configuration to include remote devices from outside your network into the monitoring (see section [Multiple Probes and Remote Probes](#)^[201]). In a cluster, there is an additional **Cluster Probe** running on all nodes. Devices on the cluster probe are monitored by all nodes of the cluster, so data from a different perspective is available and monitoring for these devices will always continue, even if one of the nodes fails.

Group

On each probe, there are one or more **Groups**, which serve merely structural purposes. Use groups to arrange similar objects in order to inherit same settings to them. To a group, you add the devices. You can arrange your devices in different nested groups to reflect the structure of your network.

Find below a sample configuration: A device tree with local probe, several groups, devices and their sensors.



Device

To each probe or group, you can add **Devices** that you want to monitor. Each device in your PRTG configuration represents a real hardware or virtual device in your network. These can be, for example:

- Web or file server
- Client computer (Windows, Linux, or Mac OS)
- Router or network switch
- Almost every device in your network that has its own IP address

Note: Sometimes you may want to add the same device in PRTG several times, in order to get a better overview when using many sensors for a very detailed monitoring, or to use different device settings for different groups of sensors. In PRTG you can simply add multiple devices with the same IP address or DNS name. The sensors on all of these PRTG devices will then query the same real hardware device in your network.

PRTG additionally adds a so called **Probe Device** to the local probe. This is an internal system device. It has access to the computer on which the probe is running on and monitors its health parameters with several sensors running on it.

Sensor

On each device you can create a number of **Sensors**. Every sensor monitors one single aspect of a device. This can be, for example:

- One network service like SMTP, FTP, HTTP, etc.
- One network switch port's traffic
- CPU load of a device
- Memory load of a device
- Traffic on one network card
- One NetFlow device
- System health of a device
- Other content (for example, of databases, mails, HTTP, XML, files, etc.)
- etc.

Channel

Every sensor has a number of **Channels** through which it receives the different data streams. The available channels depend on the type of sensor. One sensor channel can contain, for example:

- **Downtime** and **uptime** of a device
- **Traffic in** of a bandwidth device (for example, a router)
- **Traffic out** of a bandwidth device (for example, a router)
- **Traffic sum** of a bandwidth device (for example, a router)
- **WWW traffic** of a NetFlow device
- **Mail traffic** of a NetFlow device
- **Other traffic** of a NetFlow device
- **CPU load** of a device
- **Loading time** of a web page
- **Download bandwidth** of a web page
- **Time to first byte** of a web page
- **Response time** of a Ping request to a device
- **Response time** of a Remote Desktop service
- etc.

4.4 Inheritance of Settings

The [hierarchical tree](#)^[83] is not only used to group sensors for organizational reasons, there is also an important aspect involved that we call **inheritance**. To ensure administration is quick and easy—especially for large monitoring setups—certain settings are inherited from the overlying level. For example, you can change the monitoring interval for all sensors by editing the interval setting of the topmost **Root** group (unless no other setting is defined below).

Settings are Inherited to Child Objects

You can override this inheritance on any level of the hierarchy by setting a different value for a specific probe, group, device, or sensor. All objects below will inherit these new settings; object settings from levels above will stay unchanged.

Settings that are inherited among all objects include:

- Monitoring interval
- Notification triggers
- Authentication settings for several systems
- Compatibility settings (for certain types of sensors)
- Channel and unit configuration
- [User access rights](#)^[94]
- [Tags](#)^[89]
- Paused status: If an object is paused by the user, or a schedule, all sensors on it are paused as well
- etc.

There is one exception for devices and sensors: The **IP address** or **DNS name** of a device and compatibility settings are always inherited by sensors and can not be changed on sensor level.

The actual overriding of the parent's settings takes place in an object's settings: Remove the check mark symbol at the beginning of the respective line **inherit from [parent object]**. For example, the screenshot below shows Windows systems credentials settings after removing the check mark symbol.

CREDENTIALS FOR WINDOWS SYSTEMS

☐ inherit from User Group home (Domain or Computer Name: paessler, Username: ...)

Domain or Computer Name:

Username:

Password:

Credentials for Windows Systems

Default Values Set in Root Group

For all settings (except passwords), PRTG already includes a set of default values so you can get started with the software immediately. For example, the following settings will be inherited by all sensors from the **Root** group:

- Default monitoring interval of one minute
- SNMP version 1 with community string set to **public** (default values for most devices)
- Dependency type **Use parent**
- etc.

You may need to change some of the default entries as you become used to the interface. However, these settings will initially suffice for most situations.

Before sensor setup, please review the **Root** group's settings and set the default values to suit your setup, including necessary credentials for all kinds of systems in your network you want to monitor (Windows, Linux, virtual servers, etc.).

See section [Root Group Settings](#)²²⁴ for more details.

Inheritance of Notification Triggers

If you add notification triggers on probe, group, or devices level, these will also be inherited to all sensors underneath, unless you cancel inheritance with specific settings.

See section [Sensor Notifications Settings](#)¹⁶⁹⁰ for details.

4.5 Tags

For every object in your PRTG setup, you cannot only name objects, but also define tags in an [object's settings](#)^[141] to additionally mark an object as a member of certain categories. Although there are tags predefined when [adding objects](#)^[204], you are completely free in the way you add tags. For example, you can mark all of the bandwidth sensors which are especially important for you with the tag **bandwidth_important**. Later, you can view lists of objects with certain tags (helpful for [multi-edit](#)^[1710] of settings), or choose sensors by tag when creating [reports](#)^[1749]. A clever arrangement of tags can save you a lot of time at some point. **Note:** You can also change tags for several objects at a time using the [multi-edit](#)^[1710] function.

The screenshot displays the 'BASIC SENSOR SETTINGS' section of the PRTG interface. The 'Sensor Name' is '(001) Ethernet Interface'. Under the 'Tags' section, 'bandwidthsensor' and 'snmptrafficsensor' are listed with close buttons, and a 'disk' tag is being selected from a dropdown menu. The 'Priority' is set to five stars. Below this is the 'TRAFFIC SPECIFIC' section with 'Interface number' set to '1:Uplink .38 Port 15'. A small '6' icon is visible in the bottom right corner of the settings area.

View and Edit Tags in Basic Sensor Settings

Tags Are Inherited

The tags in an object's settings are automatically [inherited](#)^[87] to all other objects further down in the hierarchy. So, for example, a device with the tag **myExampleTag** will automatically and invisibly inherit this tag to all sensors created on it. This will not be visible in the sensor's tag settings, but the sensors will appear in the list whenever you search for **myExampleTag**. This is useful, for example, when adding sensors by tag in [reports](#)^[1749] settings. This way, in order to configure your setup for fetching all sensors on a device by tag, you do not have to tag every single sensor, but it is enough to tag the device. Inheritance for tags cannot be disabled.

4.6 Dependencies

Using dependencies, you can pause sensor monitoring based on the status of another sensor in order to avoid false alarms and incorrect downtime recording. A dependency stops the monitoring of one sensor or a set of sensors as soon as a specific sensor is not in an **Up** status. This means, for example, you can stop monitoring remote network services when the corresponding firewall is down due to connection problems.

When using the [auto-discovery](#)^[190] function, the **Ping** sensor on a device is by default set as the master object for this device. This means that monitoring for the entire device is paused if the Ping sensor is in a **Down** status. Usually, it does not make sense to monitor other aspects of a device with other sensors, while the **Ping** sensor indicates that the device is not even reachable.

In order to view a list of all dependencies or only selected dependencies, choose **Devices | Dependencies** from the [main menu](#)^[175].

For more information about the dependency settings, please see the [settings of the respective object](#)^[141] you want to set a dependency for.

4.7 Scheduling

Using schedules, monitoring of an object can be [paused](#)^[161] for a certain time, for example, Sundays between 4 and 8 a.m. A paused sensor will not collect monitoring data, will not change its status, and will not trigger any [notifications](#)^[92]. With schedules you can limit the monitoring time automatically. You can also pause monitoring for planned system maintenance time spans to avoid false alarms. You can apply different schedules to every object. They are also used for reports and notifications.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

☐ inherit from  Switches

Dependencies, schedules and maintenance windows always pause all sensors inside a group/device. This pausing is always inherited to all sub-objects and the inheritance can not be disabled. Below you can set additional schedules, maintenance windows or dependencies that will be used on top of any inherited setting.

Schedule	None
Maintenance Window	None
Dependency Type	Weekdays Eight-To-Eight (8:00 - 20:00) [GMT+0200]
Delay (Seconds)	Weekdays Nine-To-Five (9:00 - 17:00) [GMT+0200]

Available Default Schedules in Device Settings

Schedules are user account specific. To change the default pre-defined schedules or to add your own schedule, please see [Account Settings—Schedules](#)^[1801] section.

Note: If you use failover clustering with nodes in different timezones, scheduling applies at the local time of each node. For more information, please see section [Failover Cluster Configuration—Before Getting Started](#)^[2026].

4.8 Notifying

PRTG Network Monitor keeps the administrator or other responsible persons informed about the current status of the network. There are several methods how the administrator can stay up to date.

Notifications

This is the most powerful information tool. Whenever PRTG discovers downtime, an overloaded system, threshold breach (for example, a disk runs full), or similar situations, it can send a notification. Notifications use various methods by which you can be notified (for example, email, SMS, pager message, and others). After creating notifications in the system settings, you can select them on the notifications tab of probes, groups, devices, and sensors, as well as on the root group. See [Notifications](#)^[1725] section for more details.

Limits

In a [sensor channel's settings](#)^[1693], you can set limits to change the status of the sensor when certain limits are breached. This way, you can set, for example, a traffic sensor (typically never in a error status) to **Down** status whenever bandwidth values are measured that you consider critical. This sensor will then show up in the alarms list.

Alarms

The alarms list shows all sensors that are currently in a **Down**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. This is useful to keep track of all irregularities in your network. In the table list, you can re-sort the items by clicking on the column's header items. See [Alarms](#)^[143] section for more details.

Logs

In the logs list, the log file with all monitoring events is shown. In a typical setup, a huge amount of data is produced here. As the activity of every single object is minuted, you can use this data to check exactly if your setup works as expected. See [Logs](#)^[146] section for more information.

Tickets

The tickets list shows items with important system information or action steps to take for the administrator. You should view every ticket and take appropriate actions. Per default, an email is sent to the administrator for every new ticket that is created by the system or another user. If a ticket is assigned to a specific user, this user will get an email by default. See [Tickets](#)^[148] section for more information.

4.9 Data Reporting

With [Reports](#)^[1749] you can analyze and review monitoring data for specific time spans. There are several ways to create data reports in PRTG for your individual needs.

View Historic Data

To get a report for a single sensor, there is a function included to review historic data in PRTG. It allows you to generate reports and charts for a single sensor's data. See [Historic Data Reports](#)^[132] section for more information.

Generate Reports

You can use the sophisticated reports machine included in PRTG to create exhaustive reports for all monitoring data. See [Reports](#)^[1749] section for more information.

Export Data Using the API

You can also export all monitoring raw data to XML or CSV files and generate your own reports using any third party software. See [Using the PRTG API \(Application Programming Interface\)](#)^[1993] section for more information.

Make Data Available

You can make monitoring data available to other persons using a special user with read-only rights (see [User Access Rights](#)^[94] section), or you can create public or semi-public HTML pages with monitoring data using the Maps feature. See [Maps](#)^[1768] section for more information.

Bill Customers

You can also create custom billing reports based on PRTG's monitoring data, using the open source **Billing Tool** for PRTG. For details and download, please see [More](#)^[93] section below.

More

- [Data Storage](#)^[2036]

Paessler Website: Billing Tool

- <http://www.paessler.com/tools/billingtool>

4.10 User Access Rights

The default administrator can use the PRTG installation as the only user or can create an unlimited number of users. Users are organized in an unlimited number of user groups. Access rights for each [individual object in your PRTG device tree](#)^[83] can be given separately for each user group (except for sensor channels). Access rights to objects can also be [inherited](#)^[87].

In addition, every single user has specific rights: There are administrator users, read/write users, and read only users. You can define these settings in [System Administration—User Accounts](#)^[1824]. With these tools, you can create a rights management that allows you to specify exactly what users will be able to see and edit.

ACCOUNT CONTROL

Account Type	☐ Read/Write User ☒ Read Only User
Allow Acknowledge Alarms	☐ Allow ☒ Deny
Primary Group	User Group Read Only
Status	☒ Active ☐ Inactive
Last Login	02.12.2013 18:53:54

User Rights in User Account Settings

Individual user rights in combination with access rights of the group(s) they belong to conduct the access rights to certain objects in the device tree. This means that group membership particularly controls what a user is allowed to do and which objects the user will see when logged in.

The actual access rights for each object in the device tree can be defined in an object's settings. You can define different access rights for all sensors, devices, groups, or probes via the corresponding [Context Menus](#)^[162] or in the [Object Settings](#)^[141].

Access Rights Overview

The following classes of access rights for objects are available in hierarchical order as they can be given to user groups (lowest rights to highest rights):

- **None:** The object will not be displayed to the users of the group; no logs, no tickets, no alarms regarding this object will appear.
- **Read:** Only monitoring results can be seen.
- **Write:** Reviewing monitoring results and editing settings is allowed. In addition, objects can be added to and deleted from the device tree.
- **Full:** Reviewing monitoring results, editing settings, and editing access rights is allowed. In addition, objects can be added to and deleted from the device tree.
- **Admin rights:** If a user group has administrator rights, all options are available, including creating users, creating user groups, and deleting objects from the device tree. Access restrictions to objects cannot be set for this type of user group.

Note: Access rights that are defined locally on an object, for example, on a device, override inherited rights. On a certain object, the highest directly set access right applies for a user group. If there is no access right set directly on an object, the next higher object level will be checked for access rights. This process is repeated until defined access rights are found to be inherited or there is no higher object level.

The screenshot shows the PRTG Network Monitor interface with a modal dialog titled "Edit Rights for Cisco ASA Primary". The dialog contains a table of access rights for different user groups. The table has columns for Object, Access, and Comments. The user groups listed are PRTG Administrators (Full), PRTG Users Group (Read), and Tech Staff (Write). The dialog also includes a "CHANGE ACCESS RIGHTS" section with a checkbox for "Inherit from Firewalls".

Object	Access	Comments
Intens	None	Inherited from Root
PRTG Administrators	Full	Admin User
PRTG Users Group	Read	Inherited from Root
Tech Staff	Write	Inherited from Root

CHANGE ACCESS RIGHTS

ACCESS RIGHTS

☒ Inherit from Firewalls

Continue Cancel

Different Access Rights for a Firewall in the Device Tree Depending on User Groups

Please see the table below for which user rights apply when. Column headings show access rights of user groups for objects in the device tree; line headings show the type of user.

Note: Users are either in PRTG user groups or in Active Directory Domain user groups. They cannot be in both. We recommend to use only one type of user group (either PRTG or Active Directory) to minimize your administration effort.

	- PRTG User Group - Domain User Group	- PRTG User Group - Domain User Group	- PRTG User Group - Domain User Group	- PRTG System Administrator - Domain Administrator
	Read Access	Read/Write Access	Full Access	
- PRTG User Read Only - Domain User Read Only	Read-only rights	Read-only rights	Read-only rights	Admin rights

▪ PRTG User Read/Write	Read-only rights	Read/write rights	Full access	Admin rights
▪ Domain User Read/Write				

- **Users in an administrator group** have always administrator access rights, no matter of the access rights of an object.
- **Read-only users** have just read rights, no matter of the access rights of their group, except for users which are members of an administrator group.
- **Read/write users** in a group with full access to an object have full access rights to this object only.
- If a user is in more than one group, access rights of the user group with the **highest rights** apply.
- Administrator rights can only be given via the administrator group.

For more information about defining access rights, please see the following sections:

- [System Administration—User Accounts](#)  1824
- [System Administration—User Groups](#)  1829

For information about connecting PRTG to an existing Active Directory, please see [Active Directory Integration](#)  1991.

4.11 IPv6

PRTG supports the IPv6 protocol for most sensor types. You can define whether data from your network is queried via IPv4 or IPv6: For each device in PRTG you can select whether PRTG will connect to it using either IPv4 or IPv6. This is a simple selection in the [Device Settings](#)²⁷² of each device. Depending on the setting, the sensors created on this device will use the respective protocol.

In the **Outgoing IP Settings** of the [PRTG Probe Administrator](#)¹⁹⁸¹ you can additionally choose which IPv6 address will be used for outgoing monitoring requests. **Note:** There is the same option for IPv4, too.

Part 5

Ajax Web Interface—Basic Procedures

5 Ajax Web Interface—Basic Procedures

The Ajax-based web interface is your access to PRTG. It is used to configure devices and sensors, and to set up notifications, as well as to review monitoring results and to create reports. This web interface is highly interactive, uses Asynchronous Java Script and XML (AJAX) to deliver a powerful and easy-to-use user experience. While the user is [logged in](#)¹⁰², the data on the screen is permanently refreshed (via Ajax calls) so it always shows the current monitoring results (refresh interval and method can be [set](#)¹⁸²⁴ by the user).

Because the web interface works as a **Single Page Application (SPA)**, you will rarely see a full page refresh to avoid this performance impact due to redundant processing. Only single page elements will be refreshed when necessary. All object setting dialogs are shown as pop-up layers, so you will never lose the current context. This speeds up the user experience appreciably and makes the configuration of objects in PRTG comprehensible.

The following sections introduce the features and concepts of the Ajax Graphical User Interface (GUI).

Ajax Web Interface—Basic Procedures—Topics

- [Login](#)  102
- [SSL Certificate Warning](#)  105
- [General Layout](#)  108
- [Sensor States](#)  121
- [Review Monitoring Data](#)  124
- [Compare Sensors](#)  129
- [Historic Data Reports](#)  132
- [Similar Sensors](#)  137
- [Object Settings](#)  141
- [Alarms](#)  143
- [Logs](#)  146
- [Tickets](#)  148
- [Working with Table Lists](#)  155
- [Object Selector](#)  158
- [Priority and Favorites](#)  159
- [Pause](#)  161
- [Context Menus](#)  162
- [Hover Popup](#)  173
- [Main Menu Structure](#)  174

Other Ajax Web Interface Sections

- [Ajax Web Interface—Device and Sensor Setup](#)  188
- [Ajax Web Interface—Advanced Procedures](#)  1700

Related Topics

- [Enterprise Console](#)  1860
- [Other User Interfaces](#)  1912

5.1 Login

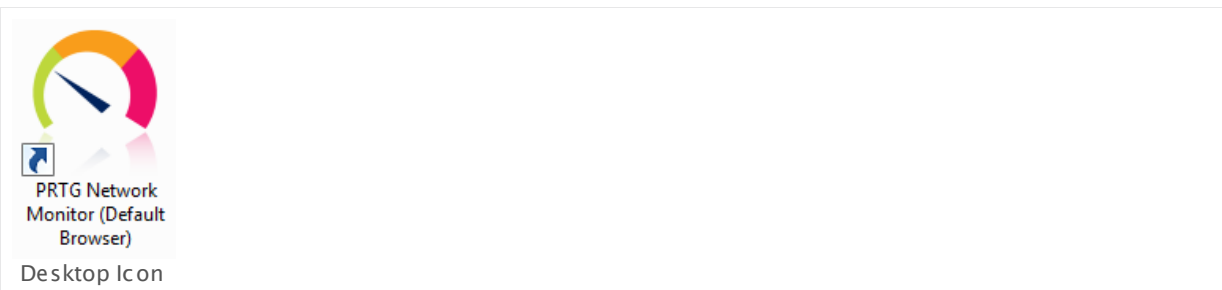
Once the PRTG core server is [installed](#)^[51], you can log in to the web interface. In your browser, load the IP address or DNS name of the computer PRTG is installed on and log in using the **Default Login** button.

You can look up and change PRTG's web server settings at any time using the [PRTG Server Administrator](#)^[1959] Windows application on the system where the PRTG core server is installed on. Especially when accessing PRTG from the internet you should use an SSL encrypted connection. You can easily switch to SSL using the **Yes, switch to SSL** button shown on the welcome screen.

Loading the Web Interface

In a web browser window, please enter the IP address or URL of the system PRTG is installed on. When using a cluster, please connect to the primary master node. You can also double click on the **PRTG Network Monitor** icon on the desktop of the system PRTG is installed on.

Note: If you run PRTG on localhost, please do not use the DNS name <http://localhost> to log in to the web server, as this may considerably slow down PRTG's web interface. Please use your local IP address or <http://127.0.0.1> instead.



If you see a certificate warning in your browser, you can usually just confirm it. For more information please see [SSL Certificate Warning](#)^[105].

Login Screen

After loading the web interface, the login screen is shown. You can either login as default administrator or as an other PRTG user. As **Administrator** user you can use all functionalities of the web interface. Administrators can [create additional users](#)^[1824] with administrator rights or with more restricted privileges (for example, read only users).

Additionally, there are different GUI versions available.

PRTG NETWORK MONITOR

Login Name

Password

☒ Use AJAX Web GUI (All features, optimized for desktop access)
☐ Use Mobile Web GUI (Limited functionality, optimized for mobile access)
☐ Download Client Software (for Windows, iOS, Android)

Login **Default Login**

[Forgot password? Need Help?](#)

PRTG NETWORK MONITOR

NEWS FROM PAESSLER

PRTG Network Monitor: Quality and Pe...
Here at Paessler, our QA team puts PRTG and all of its new features to the test on a daily basis. We do this to make sure that our customers can work with a powerful,

Help Us Beta Test Our New Mobile Pro...
We have just released the beta version of a new outstanding feature for PRTG Network Monitor: Mobile probes for Android devices! Install a mobile probe on

PRTG Login Screen

Login as Default Administrator (First Time Login)

When logging in for the first time, login name and password for the default administrator login are both **prtgadmin**. You can leave the **login name** and **password** fields empty and click on the **Default Login** button to log in using these default credentials.

Note: After login you should change the default password. To do so, go to **Setup | Account Settings | My Account** and specify a new password in section **User Account**.

Note: If you are not logged in into the web interface, you can change the credentials for this default user account any time in the [PRTG Server Administrator](#)¹⁹⁷² Windows application.

Login as PRTG User

If you have received user credentials from your administrator, please enter them here to login. Also, when using other administrator credentials, please enter them here.

Choose GUI version

Depending on the used browser, different Graphical User Interface (GUI) options are shown:

- **Use AJAX Web GUI (All features, optimized for desktop access):** The standard interface. We recommend to use this option for PRTG whenever possible. It offers the full functionality of PRTG. Use Google Chrome 31 or later (recommended) or Mozilla Firefox 25 or later for best performance. In some browsers, the Ajax option is not shown, for example, in old browser versions.
- **Note:** Although you can login using Microsoft Internet Explorer 10 or 11, the Ajax web interface might **not** be fully compatible with Internet Explorer! When using Microsoft Internet Explorer 10 or 11, please set the security level at least to **Default level Medium-high** and make sure you do not use the **Compatibility View**! For detailed information, please see [More](#)¹⁰⁴ section below.

- **Use Mobile Web GUI (Limited functionality, optimized for mobile access):** The [Mobile Web GUI](#)^[1913] interface is optimized for slow network connections and old browsers. It only offers read-only functionality and comes with less scripting. It is also a fallback solution when using a browser that is not supported by the Ajax interface.
- **Download Client Software (for Windows, iOS, Android):** This option calls PRTG's download page in the **Mobile Web GUI**. You can optionally download the native Windows application **Enterprise Console** to the desktop (called **Windows GUI** in previous deprecated PRTG versions). It has to be [installed](#)^[1890] on the client computer before use. The [Enterprise Console](#)^[1890] provides full functionality; however, for some functions the Ajax Web GUI is opened. As an additional feature, the Enterprise Console can view data of several independent PRTG core installations in a single application. You can also access pages on Paessler's website from here for information about the [PRTG apps](#)^[1916] **PRTG for Android** and **iPRTG for iOS**. These pages contain also the download links for the apps for your mobile device. **Note:** Also when using this download option, login name and password (or a **Default Login**) are required!

Note: Only Google Chrome 31 or later (recommended) and Mozilla Firefox 25 or later are fully compatible with the Ajax web interface. For more information about Internet Explorer support, please see [More](#)^[104] section below.

Click on the **Login** button to proceed to the PRTG web interface.

More

Knowledge Base: Why are Internet Explorer IE6 and IE7 not supported by PRTG's Ajax Interface?

- <http://www.paessler.com/knowledgebase/en/topic/7633>

Knowledge Base: How can I access the AJAX web interface of PRTG with Internet Explorer 9 or IE10?

- <http://www.paessler.com/knowledgebase/en/topic/46893>

5.2 SSL Certificate Warning

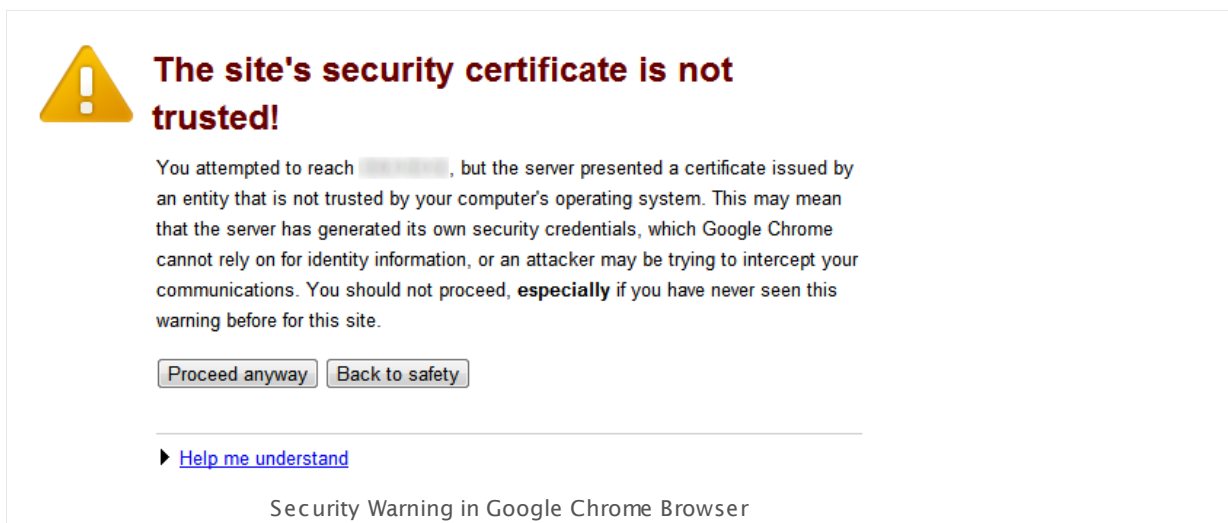
If you use PRTG outside your internal LAN, especially when using it on the internet, you should switch the internal web server to use SSL. After doing so, your browser will show a certificate warning, as the certificate that comes with PRTG cannot be signed by a valid authority. Anyway, the connection to your PRTG web server will be secured via SSL, and you can confirm the claimed security risk. For more information on secure browser connections, please see the [More](#)^[104] section below.

Every browser shows the certificate warning in a different layout. The steps to take are similar for every browser, yet different in detail:

- [Google Chrome](#)^[105]
- [Mozilla Firefox](#)^[105]
- [Internet Explorer](#)^[106]
- [Other](#)^[107]

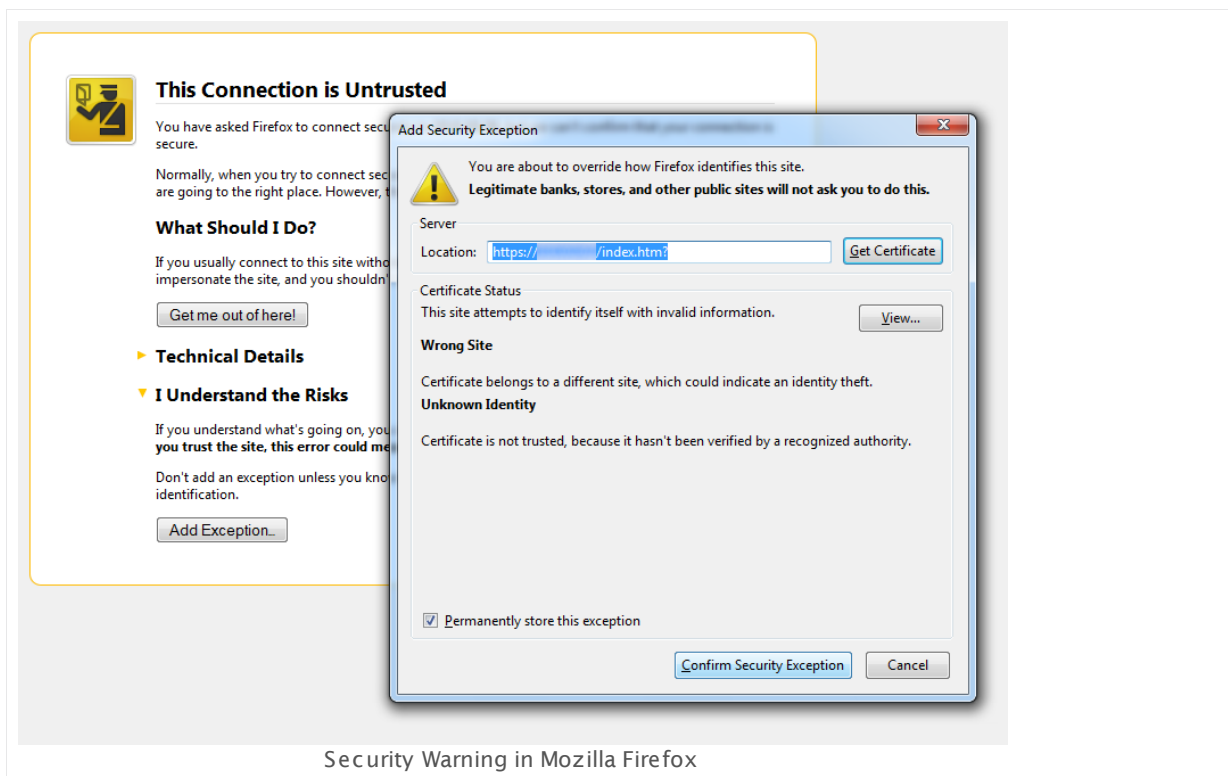
Google Chrome

In **Google Chrome**, click on **Proceed anyway** every time you call the web interface.



Mozilla Firefox

In **Mozilla Firefox**, click on **I Understand the Risks** and then on the **Add Exception...** button. In the appearing window, leave the check mark for **Permanently store this exception** and finally click on the **Confirm Security Exception** button.

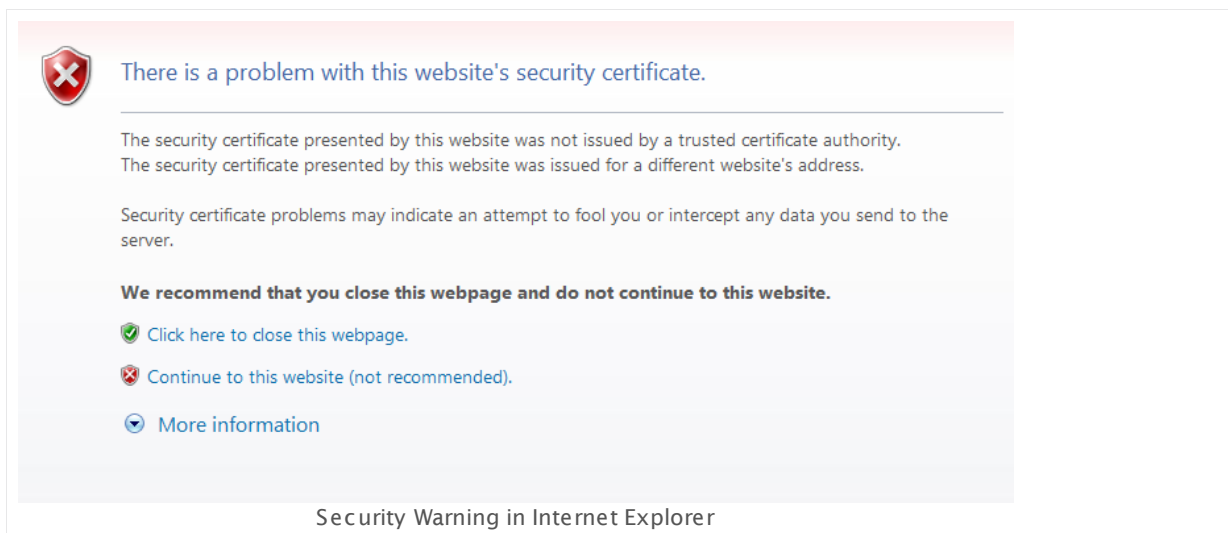


Security Warning in Mozilla Firefox

You only have to go through this procedure once for every Firefox browser and PRTG core server.

Internet Explorer

In **Internet Explorer**, click on **Continue to this website (not recommended)** every time you call the web interface.



Security Warning in Internet Explorer

Other

For other browsers, the procedures to confirm the certificate will be similar to the ones described above.

More

- [Using Your Own SSL Certificate](#) 

Knowledge Base: Why don't I get an SSL connection to the PRTG web interface?

- <http://www.paessler.com/knowledgebase/en/topic/11813>

5.3 General Layout

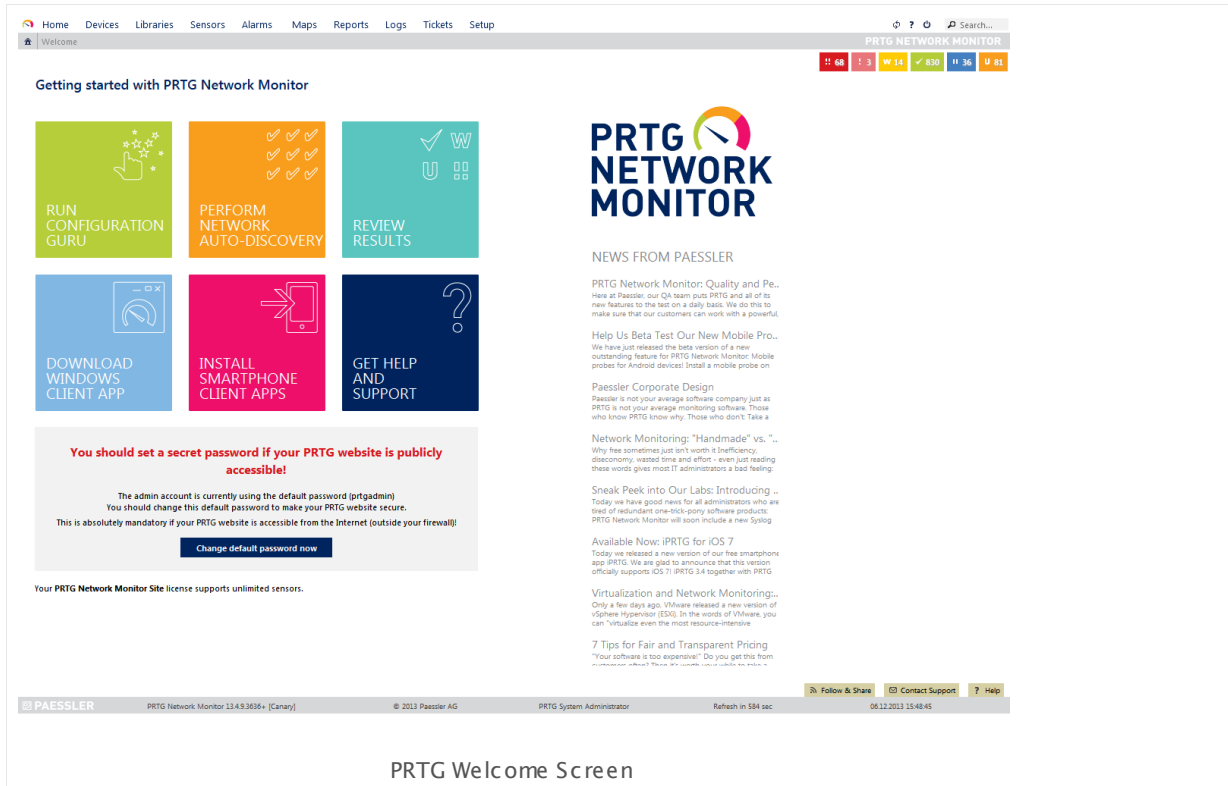
This manual section provides an overview about the structure of PRTG's web interface. The main focus is on the **Devices** view which you can select via the main menu bar, because there you see your monitoring results at a glance and, thus, you will widely use it.

Welcome Page

Once you have run through the [Configuration Guru](#)³⁶, you will see PRTG's welcome page as default after you log in to the web interface. You can set another homepage in your [account settings](#)¹⁷⁸⁶, section **Web Interface**.

You have the following options on the welcome page:

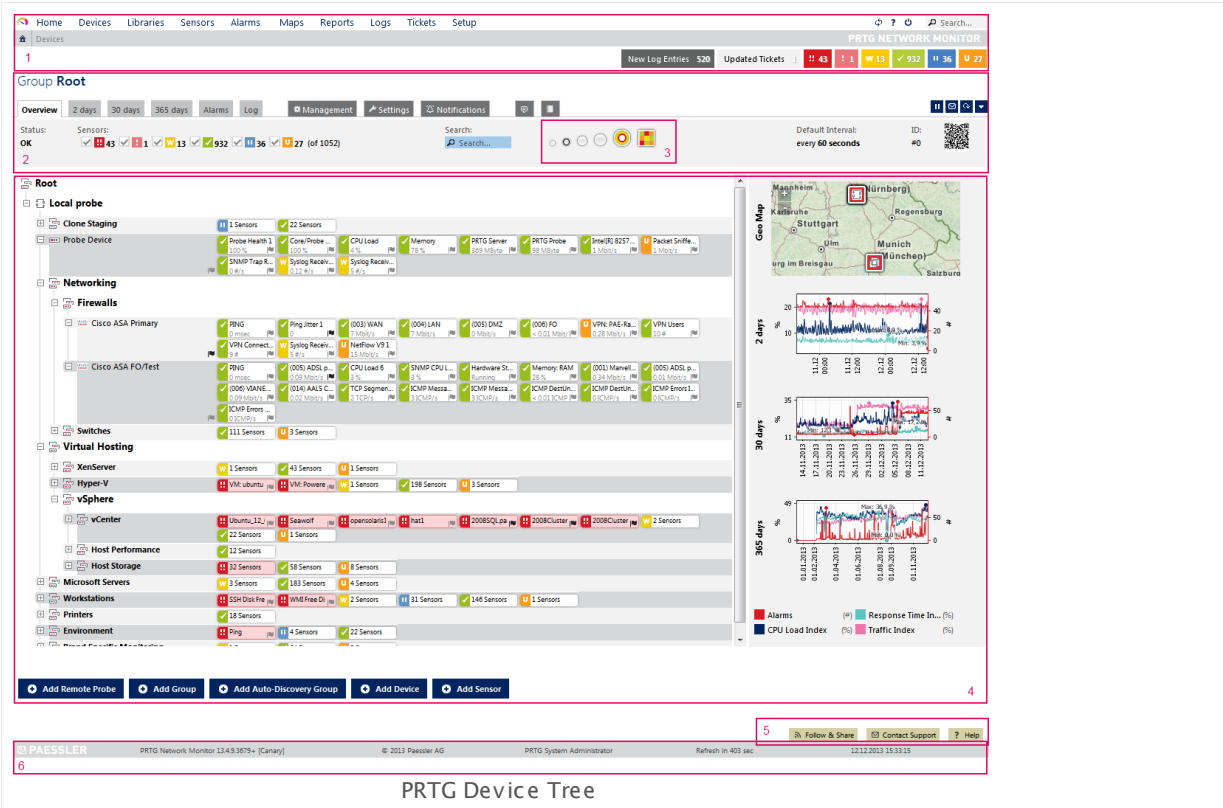
- [Run Configuration Guru](#)³⁶
- [Download Windows Client App](#)¹⁸⁵²
- [Perform Network Auto-Discovery](#)¹⁹⁰
- [Install Smart phone Client Apps](#)¹⁹¹⁶
- [Review Results](#)¹³²
- **Get Help and Support**: Opens the help center where you find links to this manual, to the Knowledge Base, and the [contact Paessler support form](#)¹⁸⁵⁶.



PRTG Welcome Screen

Tree View Layout

Click on the **Review Results** option on the welcome screen to display the tree-like device view which will be a starting point for everyday use or on **Devices** in the main menu bar.



PRTG Device Tree

From top to bottom, the main layout consists of:

Screen Number	Part	Description
1	Global Header Area ¹¹¹	This element contains the main menu at the top, the global status bar, the path to the currently selected object, and a quick search box.
2	Page Header Bar ¹¹³	This element contains the page heading with the name of the current object, several tabs with settings, monitoring data, etc. of the current object, the object's status bar, quick action buttons, and the QR code linking to the current URL.
3	Device Tree View ¹¹⁵	This selection is part of the page header bar. Using the provided options you can define how your device tree is displayed.
4	Page Content ¹¹⁹	This element contains information about the current object and all other objects underneath in the tree hierarchy.
5	Page Footer Icons	With these icons you have quick access to the PRTG Auto-Update page, to PRTG's social network accounts, and to the contact support form¹⁸⁵⁶. There is also a link to context sensitive help. When running PRTG in a cluster, you will also see a cluster related element. It shows the name of the node you are logged in and displays whether this is a master or a failover node. Click the bar to show the Cluster Status¹⁸⁵⁰. In a failover node, you can review all data, but changes in the settings will not be saved. In order to change settings, please log into the master node of your cluster.
6	Page Footer	Shows information about the current version of PRTG, the logged in user, the time remaining to the next automatic page refresh, and the current time.

Simply click on an object to see more details about it. In the page heading of the [page header bar](#)¹¹³ you always see which object you're looking at.

When you navigate through PRTG's web interface you will always use one of the following navigational paths:

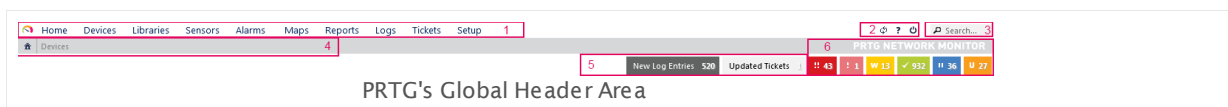
- The main menu provides access to all important aspects of the software.
- The quick search is often the fastest way to navigate to an object.
- Using the page's tabs, you can switch between various sub-pages for an object.
- Many objects offer a context menu that will pop up when you right-click them.
- Many objects offer a quick-info menu that will pop up when hovering an object

- And, finally, you are able to drill down into the object hierarchy of probes, groups, devices, and sensors in the object tree by merely clicking an sub-object of the currently displayed object (for example, a sensor on the device page).

These six navigation paths put PRTG's complete functionality at your fingertips. Quite likely you are already familiar with these techniques from many other websites and web-based user interfaces.

In the following, the different areas of the web interface are described.

Global Header Area



The header area of the web interface is both base for the most important information of your installation and starting point for all actions. You can view the global status and navigate through the web interface using the main menu.

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

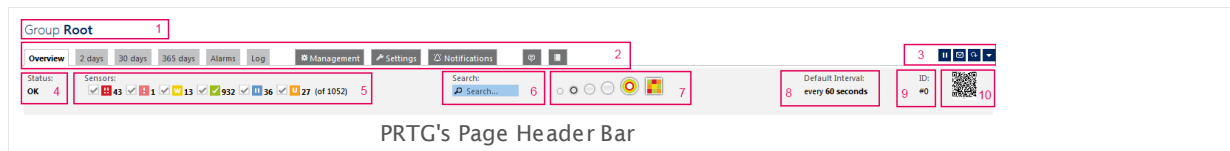
The global header area consists of the following parts:

Screen Number	Part	Description
1	Main Menu Bar	Navigating through the web interface is performed using the main menu. Please take a few minutes to familiarize yourself with all menu items and sub-items. A detailed description can be found in the Main Menu Structure ^[174] section.
2	Icons Refresh, Help Center, Logout	With the icons on the right you can reload the current page, open the help center or log the current user out.
3	White Search Box	To search for any monitoring object, enter the name, part of the name, an IP address, a DNS name or a tag in the search box on the right and hit the enter key. A web page with all items that fit the search term will be returned—even displaying online help articles.
4	'Breadcrumbs'	Below the main menu, there is always a path shown, leading to the homepage. Use it to go back to where you came from. It can also help you to orient yourself in case you get lost. If you click on a 'breadcrumb' item to open a drop-down menu showing all available object on the same level. Enter a view letters to search for a name, or select an object directly. For example, you can use this to directly access all other sensors or a device, the other devices within a group, another group on the same probe, or other probes in your root group.
5	Buttons New Alarms, New Log Entries, New Tickets	These buttons show the number of new alarms and new log entries, as well as the number of new tickets. Click on the respective button to view the Alarms ^[143] , Logs ^[146] , or Tickets ^[148] .
6	Global Sensor Status Symbols	This area shows the aggregated status of all sensors you have configured for monitoring, divided into different sensor states. Depending on the sensors' status you will see colored boxes with numbers which symbolize the sensors. For example, you can see how many sensors are in Up , Down , or Warning state. Click on a box to view a list of all sensors in the respective status. For a detailed description, please see Sensor States ^[121] section.

Page Header Bar

In the page header under the global header area, you see the name of the current object and the page content underneath. When displaying a group, aggregated sensor states are shown in a sensor bar and there is an option to change the tree view. Furthermore, various information about the current object is reported here.

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

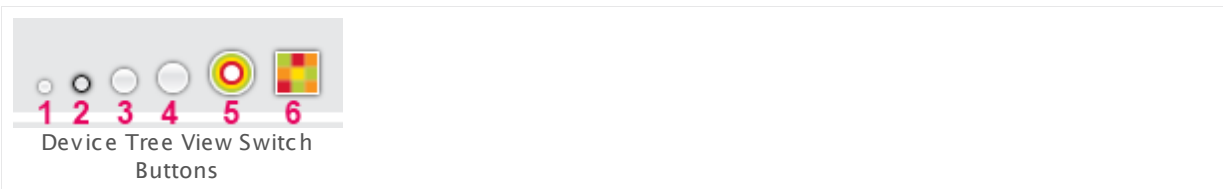


The page header and tabs area consists of the following parts:

Screen Number	Part	Description
1	Page Heading	This line displays the kind of the current object and the name as page heading. In the screenshot above, it is a group which is called Root . Here you also can add the current object to favorites by clicking on the flag, as well as you can define the object's priority by clicking on one of the five stars (not available for the Root group). For details, please see section Priority and Favorites ^[159] .
2	Tabs	Using the tabs you can navigate to various sub-pages of an object, showing monitoring data or changing settings. For more information, please see sections Review Sensor Data ^[124] and Change Device and Sensor Settings ^[141] .
3	Context Buttons	On the right side there are icons to pause or delete this object, to add another object, to send a link to the current page per email, or to perform an immediate scan. By clicking on the down arrow, you can open the context menu for the currently displayed object with even more options. For more information, please see Context Menus ^[162] section.
4	Object Status	This element indicates the current status of the selected object.
5	Sensor Status Bar	This element is visible when viewing a probe, a group (including Root), or a device. It is not available when viewing a sensor's details. The sensor status bar shows the aggregated status of all sensors for the current object, divided into different sensor states. They show the number of sensors in the respective state. For example, you can see how many sensors are in Up , Down , or Warning state. For a detailed description of sensor states, please see Sensor States ^[121] section. You can hide sensors that are in a certain state by removing the check mark symbol in front of the respective sensor symbol. To show them again, re-add the check mark.
6	Tree Search	In the white search box next to the tree view selection, enter a key word to search the device tree for matching names. The tree will then highlight matching devices and sensors by graying out all others. This can help to gain a quick overview over sensors monitoring a specific part of your network. For example, you can enter the keyword "firewall" to highlight devices and sensors which match this name.
7	Device Tree View	This element is only visible when viewing a probe or a group. It is not available when viewing a device's or sensor's details. For a detailed description, see Switch Device Tree View ^[115] below.
8	Scanning Interval	This element shows in what time interval PRTG scans the current object.
9	Object ID	This element shows the ID of the current object.

Switch Device Tree View

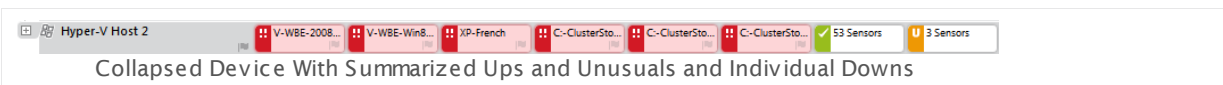
When viewing a probe or group, you can choose the way your device tree is shown.



Switch Device Tree View—Classic Device Tree

Using the different circle symbols in the page header bar, you can define how much space is used to show devices and sensors in a hierarchical tree structure. In four steps, you can switch from a very condensed view (small circle; marked with **1** in the screenshot) up to an extra large view (big circle; marked with **4** in the screenshot).

In the classic device tree view you can **collapse** devices, groups, and probes. Click on the minus box left to the object's name. The sensor states will be summarized then. Each status of the sensors on this object will be displayed with the number of sensors currently being in this status—with the exception of the states **Down**, **Down (Partial)**, and **Down (Acknowledged)**. These will be summarized respectively not before there are more than ten sensors in this status, otherwise they are displayed individually.



Switch Device Tree View—Extended Views

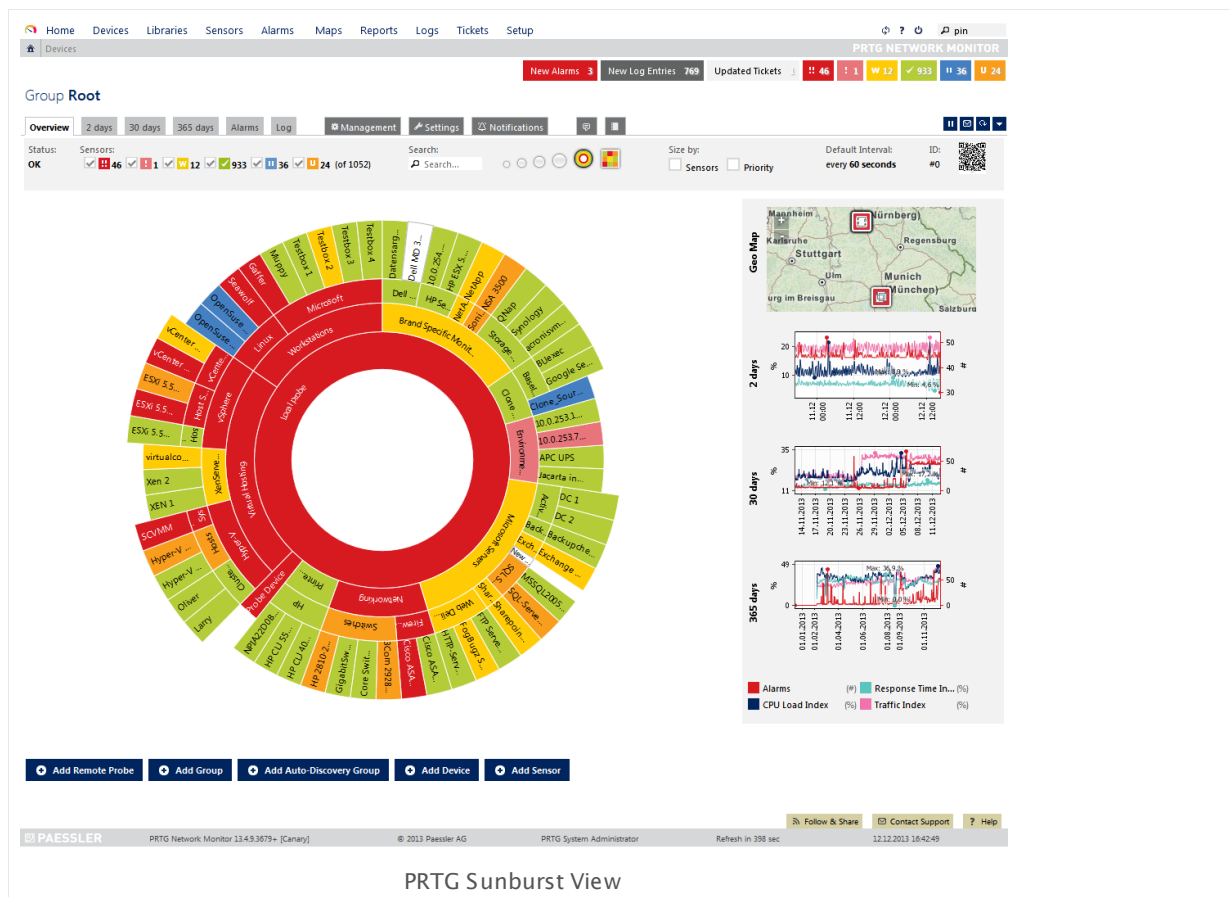
There are two additional options to the simple tree views which enable you to display the status of all sensors of your entire installation in a single overview. Click on one of the icons to change the view:

Tree Map View (6)

The tree map view tiles all devices of your entire installation into one square, arranged by the groups you put them into. Each device changes color dynamically to reflect the overall status of the sensors on the device. You can also adjust the size of the squares: either depending on a device's priority, or depending on the number of sensors on a device, or depending on both. For this concern, add a check mark under the point **Size by:** in front of **Sensors** and/or **Priority** in the page header bar (see the mark in the screenshot below).

The screenshot displays the PRTG Network Monitor interface in 'Tree Map View'. The top navigation bar includes tabs for Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. Below the navigation bar, a status bar shows 'New Alarms 3', 'New Log Entries 769', and 'Updated Tickets'. The main area is a tree map where different colors represent various device types and their status. A sidebar on the right shows a 'Geo Map' of Germany with markers for monitored locations, and three line graphs showing 'Alarms', 'CPU Load Index', 'Response Time In...', and 'Traffic Index' over 2 days, 30 days, and 365 days. At the bottom, there are buttons for 'Add Remote Probe', 'Add Group', 'Add Auto-Discovery Group', 'Add Device', and 'Add Sensor'.

The sunburst view shows your entire installation in one circle diagram. The groups are represented as inner circles, and all devices contained within a group are shown as 'cake slices' attached to the outside of a circle element.



PRTG Sunburst View

For both views:

Colors

A device (or group) element can have different colors, depending on the states of the sensors running on this device or group (see [Sensor States](#)). A more severe status is regarded more important and wins the color battle. For example, if a device currently has sensors in the states **Up** (green), **Paused** (blue), and **Warning** (yellow), the according device tile in this view would be yellow, indicating that at least one sensor on this device is in **Warning** status. If there are any red **Down** sensors, the according device tile will turn red. Following, all possible states in both views are listed ordered by their hierarchy:

Flag	Flag Color	Object Status	Meaning
	Red	Down	At least one sensor of this object shows a red Down status. Hover an object's name to view the total number of alarms concerning this object.
	Bright-Red	Down (Acknowledged)	At least one sensor of this object is Down and the status was acknowledged by a PRTG user, applying the Acknowledge Alarm function. The Down states of all sensors of this object have to be acknowledged—if at least one sensor is unacknowledged down, this object will be displayed as Down .
	Yellow	Warning	At least one sensor of this object shows a yellow Warning status. There is no sensor in a Down or Down (Acknowledged) status concerning this object.
	Orange	Unusual	At least one sensor of this object shows an orange Unusual status. There is no sensor in a Down , Down (Acknowledged) , or Warning status concerning this object.
	Green	Up	All sensors of this object are in a green Up status. There is no sensor in a Down , Down (Acknowledged) , Warning , Paused , or Unusual status concerning this object.
	Blue	Paused	All sensors of this object show a blue Paused status. There is no sensor in a Down , Down (Acknowledged) , Warning , Unusual , or Up status concerning this object.
	Black (Grey)	Unknown	All sensors of this object have an Unknown status. There is no sensor in a Down , Down (Acknowledged) , Warning , Unusual , Paused , or Up status concerning this object.

▪ **Size by Sensors / Size by Priority**

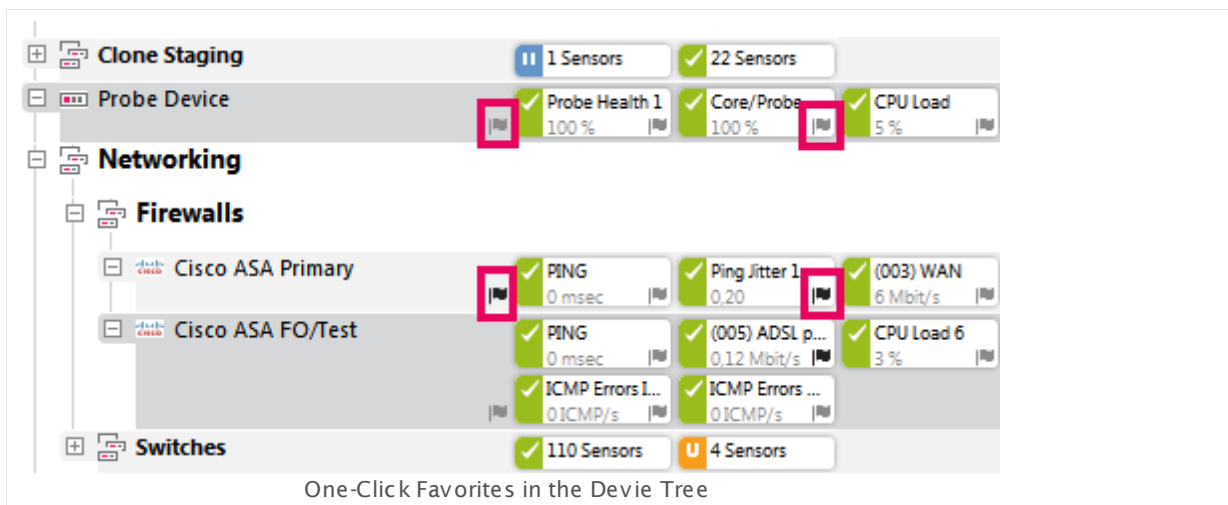
You can adjust the size of the different squares. They can be calculated by the number of sensors running on a device or within a group, or by the sensors' priority (see [Priority and Favorites](#) ¹⁵⁹), or both. Use the check boxes in the page header bar (see the mark in the tree map view screenshot) to change view immediately, then use the setting that suits best for your needs.

Page Content

The page content of the general layout varies dependent on the selected object. It shows information about the current object and all other objects underneath in the tree hierarchy. The deeper down in the hierarchy you select an object, the more detailed is the displayed information.

By default, a **Probe Device** is created in the device tree on the local probe. It represents the probe system running with your PRTG installation. PRTG automatically monitors the system health of the core server and each probe in order to discover overloading situations that may distort monitoring results. To monitor the system status of the probe computer, PRTG automatically creates a few sensors. These include a **Core/Probe Health Sensor**, a WMI sensor that measures disk usage, and a bandwidth sensor for all installed network cards. It is recommended to keep these sensors, but you can optionally remove all except the **Core/Probe Health** sensor. In a cluster installation, PRTG also creates a **Cluster Probe Device** with a [Cluster Probe Health Sensor](#)^[354] that monitors the cluster's system health.

You can add (or remove) a device or sensor to favorites by one click on the respective flag displayed with an object (please see the marks in the screenshot below).



Another one-click option for adding/removing favorites or setting the priority for a selected device or sensor is given in the [page header bar](#)^[113] right to the object name (please see screen number 1 in that subsection). Simply click on the flag for favorites or on a star for priority.

Device **Cisco ASA Primary** | ★★★★★
One-Click Favorite and Priority in the Page Header Bar

A black flag means that the respective object is a favorite already; clicking on the black flag will remove the object from favorites. A gray flag indicates that it is not a favorite yet. Please see also [Priority and Favorites](#)^[159] for this concern.

For more details about page contents, please see the following sections:

- [Review Monitoring Data](#)  124
- [Historic Data Reports](#)  132
- [Object Settings](#)  141
- [Compare Sensors](#)  129
- [Geo Maps](#)  1718

More

Knowledge Base: How can I change the width of the devices and group "boxes" shown in the PRTG 9 device tree?

- <http://www.paessler.com/knowledgebase/en/topic/24963>

5.4 Sensor States

In PRTG's device tree you usually create several sensors on each [device](#)^[272]. With sensors, you can monitor different aspects of your devices. Using a simple color code, they always show you what is going on in your network.

The color of a sensor always shows its current status. Following, you find a list of states a sensor can show. This list also reflects the hierarchy of states whenever summarized sensor states are shown (in the [device tree](#)^[109], or on [geo maps](#)^[1718]): the higher a status is in the hierarchy, the higher will be its priority in displaying sensor states. For example, if all the sensors of a specific device are **Up**, but one of its sensors reached a **Down** status, then the overall status of this device will be **Down** as well (for example, displayed red in the [Tree Map View](#)^[115]), as this state is hierarchically higher. **Note:** **Down** and **Down (Partial)** states are hierarchically equal.

Sensor	Color	Status Name	Meaning
	Red	Down	1. PRTG is not able to reach the device or the sensor has reached an error state. Please see Sensor Warning and Down Behavior^[122] below for more information. Note: By design, a sensor does not record any data in its channels while it shows this status. 2. Another reason for this status can be an error limit that is set in the Sensor Channels Settings^[1683], or an error status due to a sensor Lookup^[2001]. Note: In this case, the sensor continues to record data in all sensor channels although the sensor shows an error.
	Red/Green	Down (Partial)	In a cluster, at least one node reports this sensor as Down , while at least one other node reports the same sensor as Up .
	Bright-Red	Down (Acknowledged)	The sensor is Down and the status was acknowledged by a PRTG user, applying the Acknowledge Alarm function. This can be helpful to mark that an alarm has already been attended to. For acknowledged alarms no more notifications ^[1723] are sent. To set this sensor status, right-click on a sensor in a Down status and from the context menu ^[162] , select Acknowledge Alarm... . Then enter a comment and click OK .

Sensor	Color	Status Name	Meaning
	Yellow	Warning	There was an error reading the sensor, but PRTG will try again. The sensor may soon change to a down status. Please see Sensor Warning and Down Behavior ^[122] below for more information. Another reason for this state can be a warning limit set in a sensor's Sensor Channels Settings ^[188] .
	Orange	Unusual	The sensor reports unusual values for this weekday and time of day. The unusual detection is based on the historic average data and can be configured or disabled in the system administration ^[180] . You can also disable unusual detection for certain groups only (see Group Settings ^[270]).
	Green	Up	The last check was okay and the sensor receives data.
	Blue	Paused	The sensor is currently paused (for a certain time or unlimitedly, or by dependency).
	Black (Gray)	Unknown	The sensor has not been checked yet by PRTG or there is an error in (network) communication, likely on the probe system. If sensors show this status persistently, a PRTG restart may be necessary. For extended trouble shooting please see More ^[123] section below.

Sensor Warning and Down Behavior

The **Down** status symbolizes that something is wrong with a monitored device. There can be various reasons for a down status, for example, an interruption in the physical connection to the device, an internet connection outage, or a crashed server.

After a failed request, PRTG tries to reach the device again before setting a sensor to **Down** status (this is true for almost all types of sensors):

1. If a request to a device fails for the first time, the sensor is set to **Warning** status. PRTG repeats the request and tries to re-scan the device immediately.
2. If also the second request fails, the sensor is set to **Down** status until the device is reachable again. PRTG tries to reach the device with every scanning interval.

This procedure gives devices and services the chance to recover from a momentary overload and prevents false alarms. Still, you are informed promptly about any failures occurring.

Note: The behavior described above does **not** apply to a **Warning** or **Down** status that is activated due to a warning or error limit set in the [Sensor Channels Settings](#) .

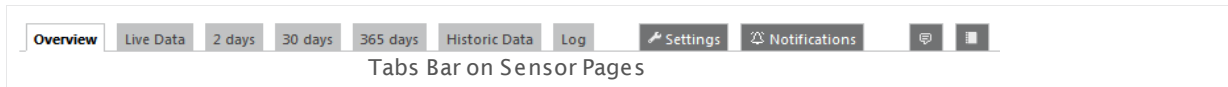
More

Knowledge Base: What to check if sensors are black (gray)?

- <http://www.paessler.com/knowledgebase/en/topic/25643>

5.5 Review Monitoring Data

Pages of probes, groups, device, and sensors have a tab-like interface. Using the tabs you can navigate through various sub-pages of an object in order to show your network's status, view monitoring results, or change settings.



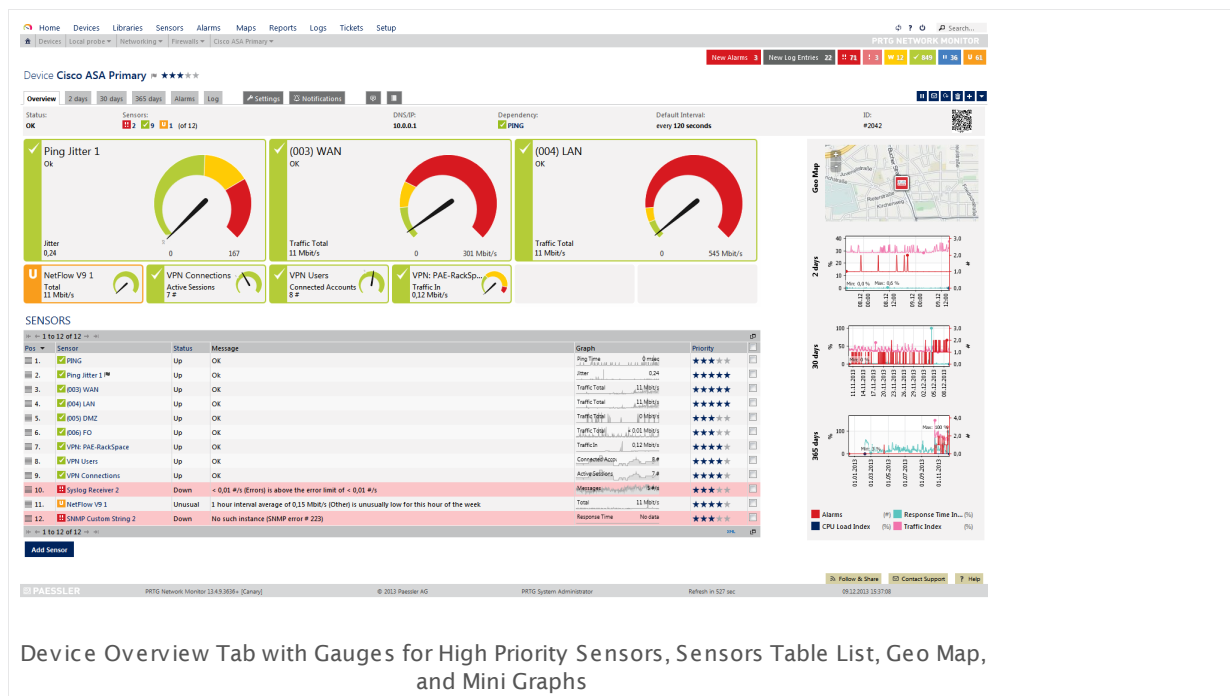
Overview

The **Overview** tab shows an overview of the currently selected object and of its sensors. The pages share a common layout, but include different elements, depending on the kind of object you look at:

- For **probes** and **groups**, the **Overview** tab shows a tree-like view with devices and sensors, a GeoMap, as well as summary graphs for different time spans of the current probe or group.
- For **devices**, the **Overview** tab shows device details, a GeoMap, and summary graphs for different time spans, colored gauges for high priority sensors, as well as a table list of all sensors on this device.
Note: In order to display gauges which represent sensor states, corresponding sensors need to be tagged with 4 stars (****) or 5 stars (*****). In the [priority settings](#)^[159], 5 stars sensors will be represented with bigger gauges than 4 stars sensors.
- For **sensors**, the **Overview** tab shows sensor details, current status, a GeoMap, colored gauges which represent the last value of particular sensor channels (the primary channel in biggest size; not available for the **Downtime** channel), sensor graphs for different time spans, a table with all sensor channels, as well as [similar sensors](#)^[137] which show correlations in your network.

Note: For sensors using [lookups](#)^[2001], we recommend staying below 120 lookup values in the primary channel to get expressive gauges. For sensors with a priority of 4 stars, the upper limit is around 40 lookup values.

Part 5: Ajax Web Interface—Basic Procedures | 5 Review Monitoring Data



Toplists

Toplists are available for [xFlow and Packet Sniffer sensors](#)^[291] only. Toplist graphs are displayed right on the sensor overview page. Please see section [Toplists](#)^[1702].

Live Data and Data By x Days

Select one of the tabs **Live Data** (available for sensors only), **2 days**, **30 days**, or **365 days** to display an object's monitoring data live (sensors only), or for different time spans and in more or less detail. **Note:** The days mentioned here are the default setting. You can change the detail of the different graphs any time in the [PRTG Server Administrator](#)^[1909] program, tab **Memory Usage**.

Part 5: Ajax Web Interface—Basic Procedures | 5 Review Monitoring Data



Live Data and Data By x Days—Probes, Groups, and Devices

For probes, groups, and devices, each of the tabs shows a summary graph for the current object and mini graphs for all sensors on this object, as well as a data table for the current object. There are never more than 50 mini graphs displayed for performance reasons. **Hover** a mini graph to see the graph legend.

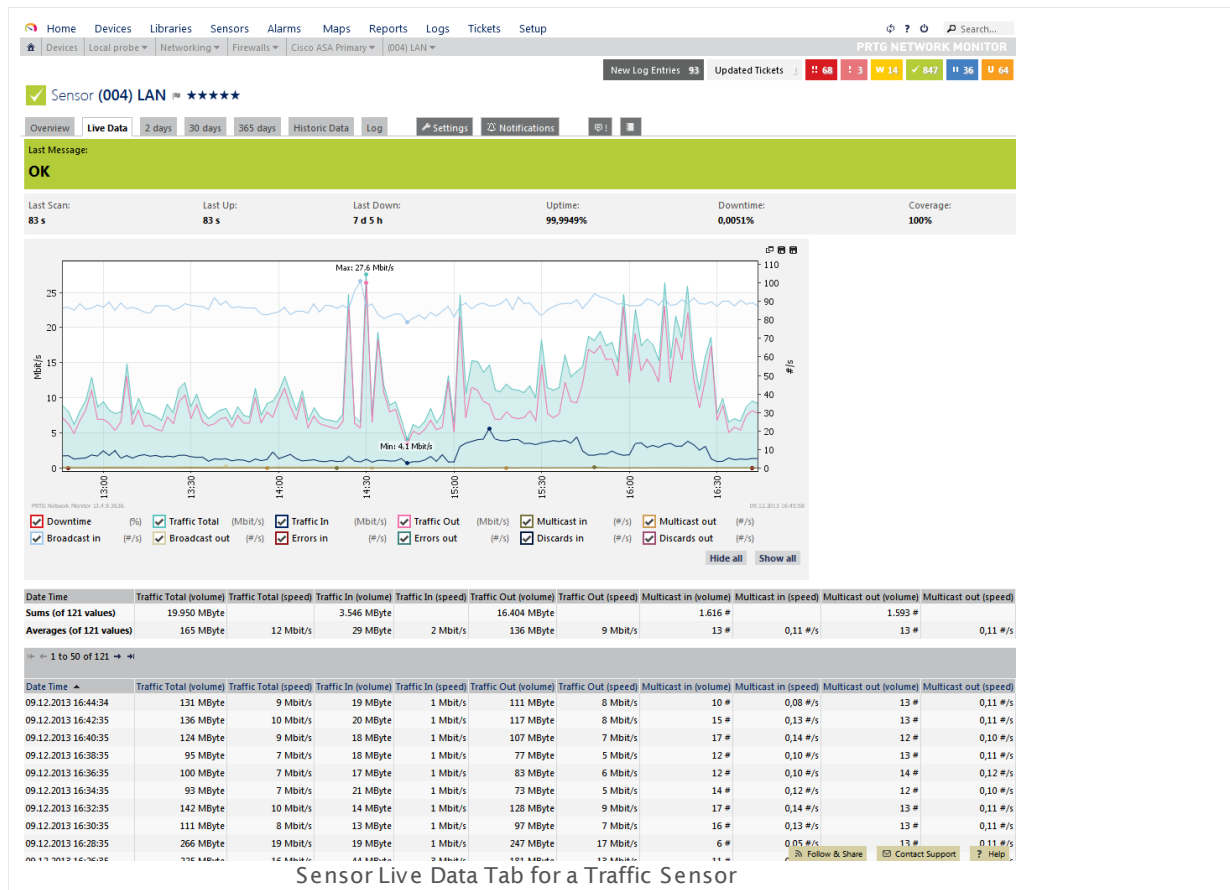
The summary graph shows the number of alarms as well as three **index graphs**. These graphs indicate response time, CPU usage, and bandwidth usage for all sensors. Index graphs are similar to a stock index. The shown values are based on the readings of all sensors of this object. PRTG computes these values using statistics and by comparing the values to the highest and lowest readings ever recorded.

The three index graphs shows overall (or global) trends in your network. If these values increase during a specific time frame, then CPU load, bandwidth load, or response time respectively have worsened during this time. For example, a **CPU Load Index** value of 90% means that the average CPU load for all CPU sensors of your current configuration is at 90% of the highest ever measured CPU usage value.

The following four channels are available in the summary graph:

- **Alarms:** Sums up the number of all down states of sensors on this object during the given time span. This graph provides you a bird's eye view of trouble in your network. It cannot be hidden.
- **Response Time Index:** Indicates request times in your network.
- **CPU Load Index:** Indicates the CPU usage in your network.
- **Traffic Index:** Indicates the bandwidth usage in your network.

You can hide single channels individually except the "Alarms" channel. Simply remove the check mark symbol in front of a channel name besides the graph, and the according channel's line will disappear. You can also **Show all** or **Hide all** channels by clicking on the buttons underneath the channel names. The graph view will be reset immediately.



Sensor Live Data Tab for a Traffic Sensor

Live Data and Data By x Days—Sensors

For sensors, the tabs show a graph and data table of the selected sensor. When viewing data of a sensor running on a cluster probe, you can additionally select if you want to show the data of all nodes, or of one specific node only. Please use the **Select Cluster Member** bar below the tabs. **Note:** Multi-node graphs are never displayed filled here, but with single lines only. However, historic data reports can have filled multi-node graphs.

While viewing a sensor graph you can hide single sensor channels individually. Simply remove the check mark symbol in front of a channel name underneath the graph, and the according channel's line will disappear. You can also **Show all** or **Hide all** channels by clicking on the buttons besides the channel names. The graph view will be reset immediately.

In the upper right corner of every graph, you will find three small icons. Using them, you can do the following:

- **Zoom graph in new window:** This will open a larger version of the graph in a new browser window.
- **Download the graph (PNG or SVG):** This will show a PNG or SVG file of the graph in a new browser window. You can then save or copy it for later use.

Historic Data

The **Historic Data** tab is available for sensors only. Please see section [Historic Data Reports](#) ¹³².

Sensors Lists

Viewing lists of sensors is a great way to keep an eye on your network's status, as you can select which kind of sensors you would like to see. There are many different sensor list views available, such as a list of favorite sensors and top 10 lists; lists filtered by current sensor status, value, availability, tag, or type; there is a sensor cross reference, and many more.

Sensor lists are available from the main menu bar. **Click** the **Sensors** entry to show a table list of all sensors. In the [table list](#) ¹⁵⁵ appearing, you can re-sort the items by clicking on the column's header items. **Hover** to show other menu options. For detailed information about the available options, please see [Main Menu Structure](#) ¹⁷⁷ (**Sensors**) section.

Alarms

The **Alarms** tab is not available for sensors, but for probes, groups, and devices only. Please see section [Alarms](#) ¹⁴³.

Log

The logs tab shows past activities and events regarding the currently selected object. Please see section [Logs](#) ¹⁴⁶.

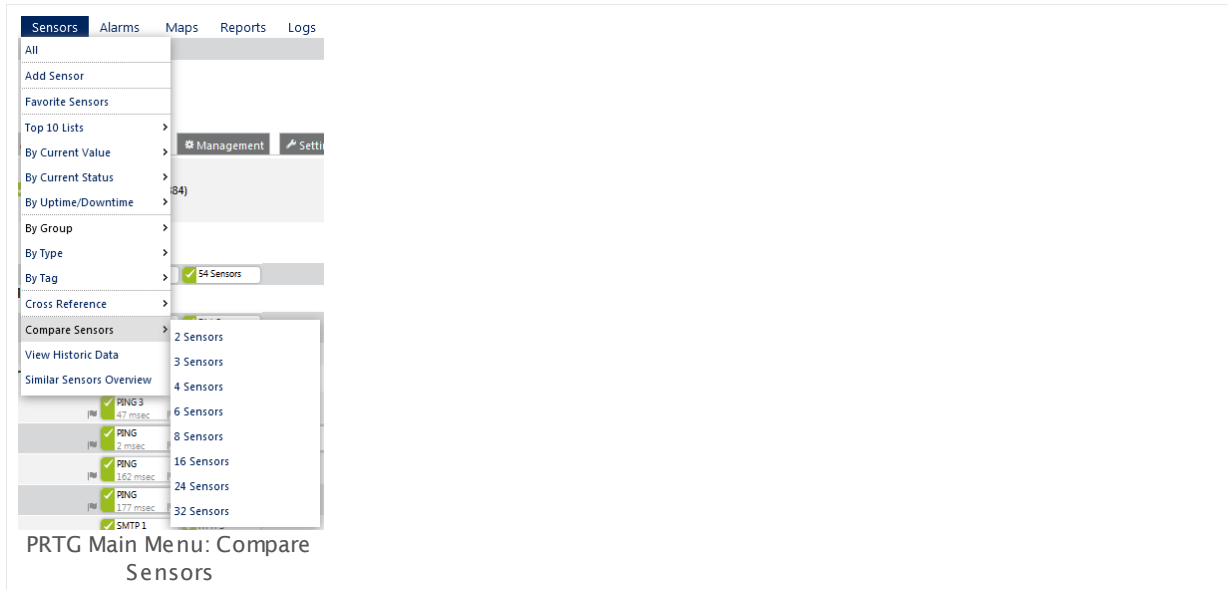
Related Topics

- [Object Settings](#) ¹⁴¹
- [Compare Sensors](#) ¹²⁹

5.6 Compare Sensors

This function allows you to visually compare the graphs of two or more specific objects. The selected graphs will be shown next to each other so you can have a look at all of them at the same time.

To open the page to compare graphs of several monitoring objects, from the main menu, choose **Sensors | Compare Sensors**. Select how many sensors you want to compare.



Once you have chosen the number of sensors that will be compared, an assistant will open where you can define your desired sensors and the time span shown in the graphs.

Part 5: Ajax Web Interface—Basic Procedures | 6 Compare Sensors



Compare Sensors Settings

Options

Time Span

Specify the time span for which you want to show the graphs for. Choose between:

- 2 days
- 30 days
- 365 days

Data Comparison

Select the objects you want to show a graph for. Click on **Please click here to edit!** to open the [Object Selector](#)¹⁵⁸. There will appear as many selection screens as you have defined before.



The graphs will be shown immediately after object selection.

Related Topics

If you want to create a sensor that combines the data of different other sensors, please see the following sensor type:

- [Sensor Factory Sensor](#) ⁸³⁷

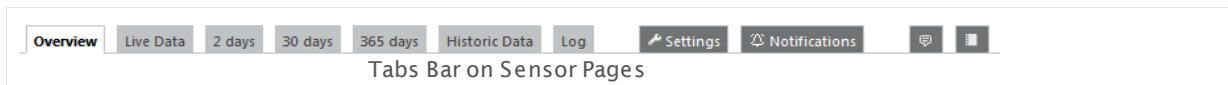
5.7 Historic Data Reports

For quick reporting on monitoring data, use historic data reports as an alternative to the exhaustive [reports](#)^[1749] function. You can view a report of the historic data for each single sensor, on demand. Additionally, you can also export this data and download it to your computer for further processing in external applications.

There are two possibilities to call the function for historic data reports: Either you click on the **Historic Data** tab on a sensor's detail page, or you choose **Sensors | View Historic Data** from the [main menu](#)^[177].

Historic Data (Sensor Tab)

Pages of probes, groups, device, and sensors have a tab-like interface. Using the tabs you can navigate through various sub-pages of an object in order to show your network's status, view monitoring results, or change settings.



The **Historic Data** tab is available for sensors only (not for probes, groups, or devices). When calling the historic data reports via this tab, there is no sensor selection available, because you have already determined which sensor you would like to create a report for.

The screenshot shows the 'Historic Data' tab for a sensor named 'PING 8'. The interface includes a top navigation bar with links like Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. Below this is a status bar showing 'New Alarms: 2', 'New Log Entries: 68', and various status icons. The main content area is titled 'REVIEW OR DOWNLOAD HISTORIC SENSOR DATA' and contains several configuration options:

- Start:** 2013-12-09 11:42
- End:** 2013-12-10 11:42
- Quick Range:** A grid of buttons for 1 Day, 2 Days, 7 Days, 14 Days, Today, Yesterday, Last Week (Mo-Su), Last Week (Su-Sa), Last Month, 2 Months, 6 Months, and 12 Months.
- Average Interval:** 60 Minutes/1 Hour
- File Format:** Radio buttons for HTML web page (selected), XML file, and CSV file.
- INCLUDE PERCENTILES:** Radio buttons for Off (selected) and On.

At the bottom of the configuration section are 'Start' and 'Cancel' buttons. The footer of the interface includes the Paessler logo, version information (PRTG Network Monitor 13.4.9.3636+ [Canary]), copyright (© 2013 Paessler AG), user information (PRTG System Administrator), a refresh timer (Refresh in 591 sec), and a timestamp (10.12.2013 11:42:09).

Historic Data Tab of a Ping Sensor

Historic Monitoring Data (Sensors Menu)

When calling the historic data reports via the **View Historic Data** entry from the **Sensors** entry in the main menu, an additional option is available, enabling you to choose the sensor you want to create a report for.

Part 5: Ajax Web Interface—Basic Procedures | 7 Historic Data Reports

Historic Monitoring Data

SETTINGS

Sensor: Local probe (Local Probe on 127.0.0.1)

Probe Device: ☒ Core/Probe Health

Start: 2013-12-03 11:43

End: 2013-12-10 11:43

Quick Range:

1 Day	2 Days	7 Days	14 Days
Today	Yesterday	Last Week (Mo-Su)	Last Week (Su-Sa)
Last Month	2 Months	6 Months	12 Months

Average Interval: 60 Minutes/1 Hour

File Format:

- ☒ HTML web page
- ☐ XML file
- ☐ CSV file

INCLUDE PERCENTILES

Percentile Results: ☒ Off ☐ On

Start **Cancel**

PAESSLER PRTG Network Monitor 13.4.9.3636+ [Canary] © 2013 Paessler AG PRTG System Administrator Refresh in 569 sec 10.12.2013 11:43:57

[Follow & Share](#) [Contact Support](#) [? Help](#)

View Historic Data Function Called from Main Menu

Historic Monitoring Data Settings

Settings	
Sensor	This field is only visible if you called this function via the main menu. Select the sensor you would like to create the report for: Click on the reading-glass symbol to open the object selector. For more information, please see section Object Selector ¹⁵⁸ .
Start	Specify the start date and time of the data you want to review. Use the date time picker to enter the date and time.
End	Specify the end date and time of the data you want to review. Use the date time picker to enter the date and time.
Quick Range	In this section several links are provided for a faster selection of start and end date. Click on any of these links to change the Start and End values above. Choose between: ▪ 1 Day, 2 Days, 7 Days, or 14 Days: Set the date range to the respective day(s). The current time of today will be the end date.

Settings	
	▪ Today, Yesterday, Last Week (Mo-Su), Last Week (Su-Sa), Last Month, 2 Months, 6 Months, 12 Months: Set the date range to the last matching period, starting 00:00, ending 00:00 of the particularly following day.
Average Interval	With this option, you can activate and set up averaging. Select an interval for which the average value should be calculated. You can choose between No Interval (no averaging will be performed and only raw data displayed), a few seconds, minutes, hours, or a whole day (24 Hours). A smaller interval will result in a more detailed report for this sensor. The best settings for you vary, depending on the scanning interval of the sensor, the selected date period and, of course, the intended use for the report. It might be useful to try different settings to see what the results look like. Please also see the section Automatic Averaging¹³⁶ below.
Cluster Node	This field is only visible if the sensor is running on a cluster probe. Select the cluster node's data that will be used for the report. Choose between: ▪ All nodes: Include the data of all cluster nodes in the report. ▪ [Several specific nodes]: Use a specific node's data for the report. The nodes shown are specific to your setup.
File Format	Select the output format for the report. Choose between: ▪ HTML web page: Display the result directly as HTML web page. This is also a good option to check results before exporting to another file format. ▪ XML file: Export the data as Extensible Markup Language (XML) file. Usually, your browser will show a download dialog. ▪ CSV file: Export the data as Comma Separated Values (CSV) file, for example, for import into Microsoft Excel. Usually, your browser will show a download dialog.
Include Percentiles	
Percentile Results	Select if percentiles will be shown in the report. Choose between: ▪ Off: No percentiles will be calculated. ▪ On: Percentiles will be enabled in the report. In the overview table, additional values will be displayed with averages/sums for each sensor channel. Please define additional settings below. For more information about percentiles, please see section Calculating Percentiles²⁰⁴⁰.

Include Percentiles	
Percentile	This field is only visible if percentile results are enabled above. Enter which percentile you would like to calculate. Please enter an integer value.
Percentile Average	This field is only visible if percentile results are enabled above. Enter the averaging interval in seconds that will be used for percentile calculation. Please enter an integer value.
Percentile Mode	This field is only visible if percentile results are enabled above. Choose between: ▪ Discrete: Chooses the next smaller discrete value. ▪ Continuous: Interpolates between discrete values.

Click on **Start** to start the generation of a historic data report. **Note:** Data reporting is limited to 5 requests per minute.

Automatic Averaging

For performance reasons, PRTG automatically averages monitoring data when calculating data for large time spans. Data is then averaged regardless of the selected average interval.

Time Span in Report	Minimum Level of Detail (Average Interval)
Up to 40 days	Any
40 to 500 days	60 minutes/1 hour or larger

A report for a time span of more than 500 days is not possible. If you try to set a larger time span, it will be reduced to 365 days automatically.

Related Topics

- [Review Monitoring Data](#)  124
- [Reports](#)  1749

5.8 Similar Sensors

With PRTG you can detect relationships between different components in your network. This function is called **similar sensors analysis**, a heuristic calculation showing similar behavior of your sensors. The analysis is completely automated and sensor type agnostic. It is based on mathematics and fuzzy logic. This feature will help you to find interconnections in your network you were not aware of and optimizes your sensor usage by tracking redundant monitoring of some aspects of your system.

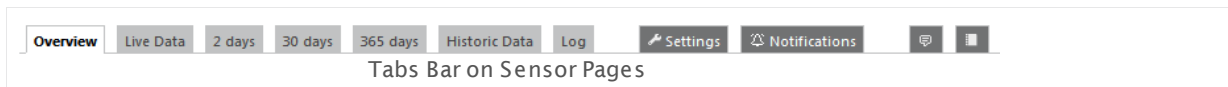
You can adjust the depth of similar sensors analysis in [System Administration—System and Website](#)¹⁸⁰⁹. You can toggle on/off similarity analysis on group basis in the settings of an object (probes, groups, devices) in the device tree.

There are two possibilities to view similar sensors:

- Each sensor's overview page contains a similar sensors section. PRTG lists channels there which show similarities to channels of the current sensor.
- In addition, you can call a similar sensors overview page via **Sensors | Similar Sensors Overview** from the [main menu](#)¹⁷⁷.

Similar Sensors (Sensor Overview Tab)

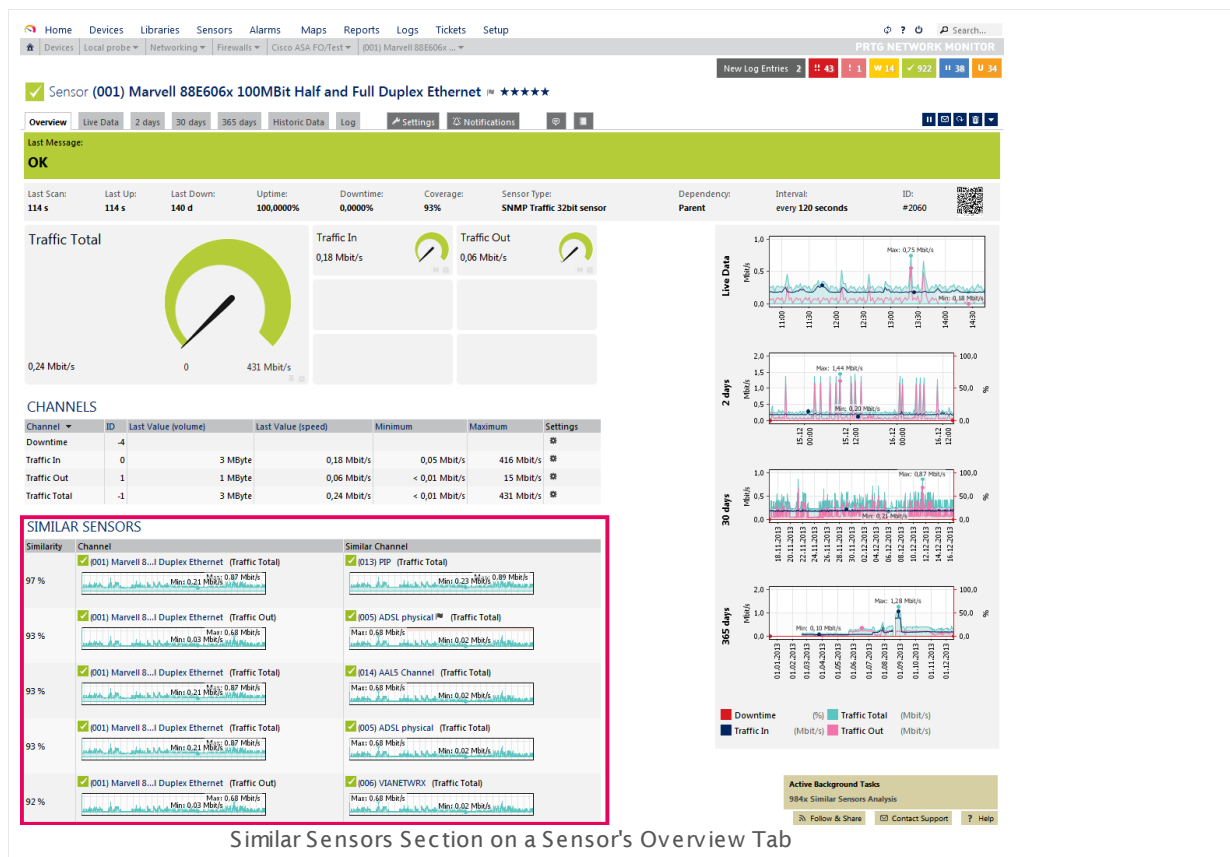
Pages of probes, groups, device, and sensors have a tab-like interface. Using the tabs you can navigate through various sub-pages of an object in order to show your network's status, view monitoring results, or change settings.



On the overview tab of a sensor, PRTG lists channels which show similarities to channels of the currently selected sensor. The table will be empty if PRTG detects no similarities regarding the selected sensor.

Note: PRTG will only show similar sensors here when channels have at least 85% similarity. Furthermore, the analysis saves up to 15 entries per sensor at most.

Part 5: Ajax Web Interface—Basic Procedures | 8 Similar Sensors



The similar sensors section provides the following information:

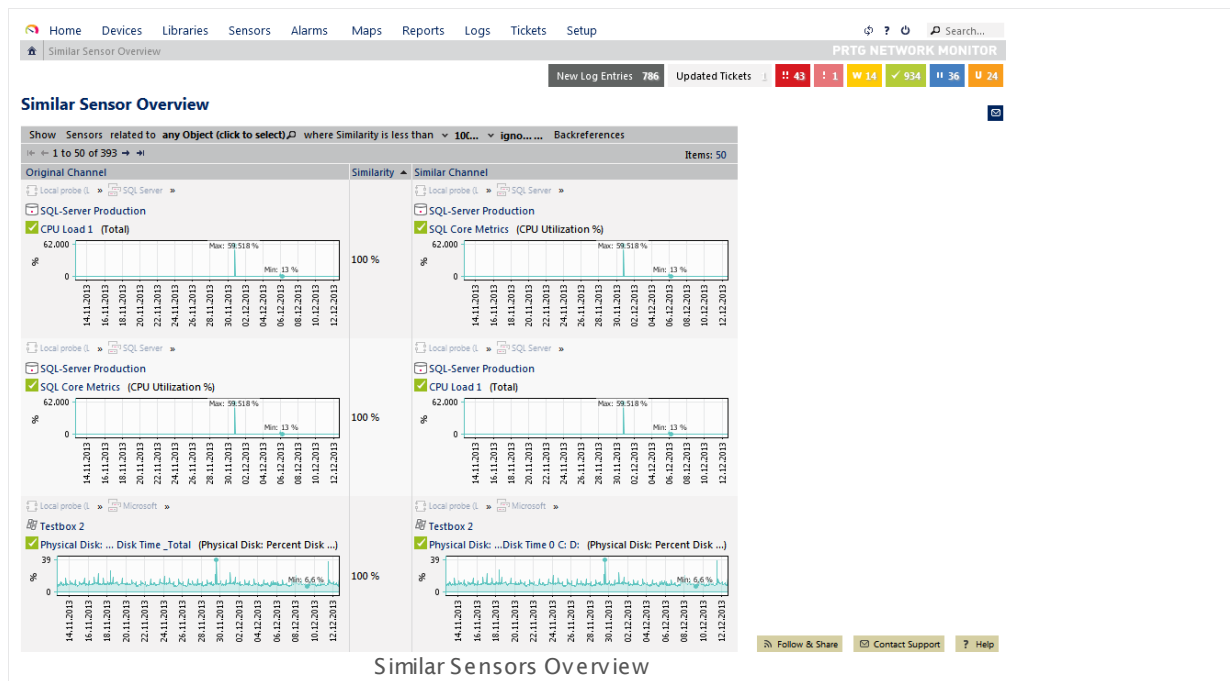
Similar Sensors	
Similarity	Shows a measurement of similarity between two channels in percent.
Channel	Shows a channel of the currently selected sensor.
Similar Channel	Shows a channel of another sensor similar to a channel of the currently selected sensor (the one in the "Channel" column in the same row).

Note: The similar sensors section will not be shown when the analysis is turned off or you have exceeded 1,000 sensor and selected the automatic analysis depth option.

Similar Sensors Overview (Sensors Menu)

This page shows the results of the similar sensors analysis from the entire monitoring database. PRTG will list all channels with similarities to another one here. On the table top, you have several filter options to display similar sensors as you need it. Choose the object of interest, the degree of similarity, and if you want to display back references. For more details, see also section [Working with Table Lists](#) ¹⁵⁵.

Note: PRTG will only show similar sensors here when channels have at least 85% similarity. Furthermore, the analysis saves up to 15 entries per sensor at most.



You can sort the list by clicking on the column headers. The similar sensors overview page provides the following information:

Similar Sensors Overview

Original Channel

Shows channels to which other channels are compared. Clicking on the column header sorts the list according to the order on the device tree in ascending or descending order.

Similarity

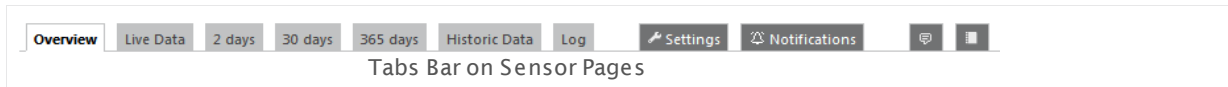
Shows a measurement of similarity between two channels in percent. Clicking on the column header sorts the list according to the similarities in ascending or descending order.

Similar Sensors Overview	
Similar Channel	Shows a channel compared to the original channel. Clicking on the column header sorts the list according to the order on the device tree in ascending or descending order.
Item Count	Define how many channel similarities are shown on this page. Choose between 50 , 100 , or 500 .

Note: The similar sensors overview option will not be shown in the main menu when the analysis is turned off or you have exceeded 1,000 sensor and selected the automatic analysis depth option.

5.9 Object Settings

Pages of probes, groups, device, and sensors have a tab-like interface. Using the tabs you can navigate through various sub-pages of an object in order to show your network's status, view monitoring results, or change settings.



Device Tree Management

The **Management** tab is available when viewing probes or groups. After clicking this tab you can move devices and sensors right within the tree view. If moving is not possible, the web interface will start a clone process automatically.

For more information, please see [Manage Device Tree](#)²²² section.

General Settings

In the **Settings** tab you can define all settings of the current object. The available options vary, depending on the kind of object you're changing. Please see the following sections for information about the respective object types:

- [Root Group Settings](#)²²⁴
- [Probe Settings](#)²³⁸
- [Group Settings](#)²⁵³
- [Device Settings](#)²⁷²
- [Sensor Settings](#)²⁹⁰

Note: The available setting options are different for **each** sensor, but always the same for probes, groups, and devices. [Sensor Channels Settings](#)¹⁶⁸³ are not reachable via tab but directly on a sensor's overview page via channel gauges and the channels table.

Notifications Settings

In the **Notifications** tab, notification triggers can be set for every object. When using these settings for a probe, group, or device, they will be inherited to all sensors on these objects. Available notification trigger options are the same for all objects.

For more information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Comments

In the **Comments** tab you can enter free text for each object. This can be used for documentation purposes or to leave information for other users.

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the PRTG user which conducted the change, and a message. The history log keeps the last 100 entries.

Related Topics

- [General Layout](#)  108
- [Review Monitoring Data](#)  124
- [Toplists](#)  1702

5.10 Alarms

The Alarm list shows all sensors that are currently in a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. Sensors in other states (for example, **Up**, **Paused**, or **Unknown**) do not appear here. This is useful to keep track of all irregularities in your network.

In the table list, you can re-sort the items by clicking on the column's header items.

The screenshot displays the 'Alarms List' in the PRTG Network Monitor interface. At the top, there's a navigation bar with tabs like Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. Below this, a summary bar shows 'New Log Entries: 45' and a color-coded status bar with counts for different alarm levels. The main section is titled 'Sensors With Alarms' and contains a table with the following columns: 'Down for', 'Probe Group Device', 'Sensor', 'Last Value', 'Status', 'Message', 'Priority', 'Graph', and 'Items'. The table lists several sensors with their respective alarm details, such as 'PING 1' being 'Down (Acknowledged)' and 'SSH Disk Free 4' being 'Down' with 49% free space. At the bottom of the table, there are links for 'Follow & Share', 'Contact Support', and 'Help'.

There are two possibilities to call the alarms list: Either you click on the **Alarms** tab on the detail page of a probe, group, or device (not available for sensors), or you choose the **Alarms** entry in the main menu.

Alarms (Object Tab)

Pages of probes, groups, device, and sensors have a tab-like interface. Using the tabs you can navigate through various sub-pages of an object in order to show your network's status, view monitoring results, or change settings.

The screenshot shows a 'Tabs Bar on Group and Probe Level'. It features a series of tabs: 'Overview', '2 days', '30 days', '365 days', 'Alarms', 'Log', 'Management', 'Settings', and 'Notifications'. The 'Alarms' tab is highlighted, indicating it is the active view. The bar is located at the top of the object's detail page.

On an object's detail view, click on the **Alarms** tab to show a table list of all sensors **on this object** that currently show a **Down**, **Down (Partial)**, **Warning**, or **Unusual** status. You will see a subset of sensors in an alarm state for the current object only. This is a subset of the entries available via the **Alarms | All** option in [main menu](#)^[180]. The tab is not available on a sensor's detail page.

Alarms (Main Menu)

Click the **Alarms** entry from the [main menu](#)^[180] to show a table list of **all** sensors in your configuration that currently show a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. You can also show these sensors as gauges. **Hover** the **Alarms** entry and select another option to only show a subset of sensors in certain states. Choose between:

- **All**
Shows a list of all sensors which currently show a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status.
- **Show as Gauges**
Shows the gauges of all sensors which currently show a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. The size of the sensor gauges corresponds to their respective priority.
- **Errors Only**
Shows a list of all sensors which currently show a **Down**, **Down (Partial)**, or **Down (Acknowledged)** status.
- **Warnings Only**
Shows a list of all sensors which currently show a **Warning** status.
- **Unusals Only**
Shows a list of all sensors which currently show an **Unusual** status.

Acknowledge Alarm

An acknowledged alarm will show up in the alarms list as "acknowledged" (see [Sensor States](#)^[121]) and will not [trigger](#)^[1690] any more [notifications](#)^[1723]. **Note:** If the alarm condition clears, the sensor will usually return into an **Up** status immediately with the next sensor scan.

In order to acknowledge an alarm, right-click on a sensor and choose **Acknowledge Alarm...** from the context menu, enter a message and click the **OK** button. The message will appear in the sensor's last message value. You can choose between: **Acknowledge Indefinitely...**, **acknowledge For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Until...**

If you choose **Until...** a popup window will appear:

Acknowledge Alarm until	
Selected Objects	Shows the sensor(s) for which you want to acknowledge the alarm. You can acknowledge alarms for more than one sensor using multi-edit ^[1710] .
Message	Enter a text, for example, the reason why you acknowledge the alarm.

Acknowledge Alarm until**Until**

Enter the date when the acknowledge status will end. Use the date time picker to enter the date and time. **Note:** If the alarm condition still persists after the specified date, the sensor will show a **Down** status again.

Only [users](#) with write access rights may acknowledge alarms. Read-only users can be given the right to acknowledge alarms, too. See section [User Accounts Settings](#), section **Account Control**.

More

Knowledge Base: Which audible notifications are available in PRTG? Can I change the default sound?

- <http://www.paessler.com/knowledgebase/en/topic/26303>

5.11 Logs

The Logs list shows all past activities and events of your PRTG monitoring setup. This is useful to keep track of all important activities and, for example, to check whether messages were sent, etc. In a typical setup, a huge amount of data is produced here. As the activity of every single object is minuted, you can use this data to check exactly if your setup works as expected.

To support you when viewing the log files, there are several filters available. Please see [Working with Table Lists](#)¹⁵⁵ section for more information.

Date Time	Parent	Type	Object	Status	Message
10.12.2013 16:00:04	Firewall 1	Ping	PING	Warning	10 % (Packet Loss) is above the warning limit of 1 %
10.12.2013 15:57:22	www3.paessler.com (192...)	SNMP Traffic 32bit	(002) eth0	Down	4,228 kbit/s (Traffic Total) is above the error limit of 3,000 kbit/s. Possible log-sync procedure or website hack-attack
10.12.2013 15:57:17	www4.paessler.com (192...)	SNMP Traffic 32bit	(002) eth0	Up	2,477 kbit/s
10.12.2013 15:56:22	www3.paessler.com (192...)	SNMP Traffic 32bit	(002) eth0	Warning	2,569 kbit/s (Traffic Total) is above the warning limit of 2,500 kbit/s. Possible log-sync procedure or website hack-attack
10.12.2013 15:55:22	www3.paessler.com (192...)	SNMP Traffic 32bit	(002) eth0	Down	3,813 kbit/s (Traffic Total) is above the error limit of 3,000 kbit/s. Possible log-sync procedure or website hack-attack
10.12.2013 15:55:17	www4.paessler.com (192...)	SNMP Traffic 32bit	(002) eth0	Warning	2,669 kbit/s (Traffic Total) is above the warning limit of 2,500 kbit/s. Possible log-sync procedure or website hack-attack
10.12.2013 15:53:54	Firewall 2	Ping	PING	Up	174 msec

List with Log Entries

There are two possibilities to call the logs list: Either you click on the **Log** tab on the detail page of a probe, group, device, or sensor, or you choose the **Logs** entry in the main menu.

Log (Object Tab)

Pages of probes, groups, device, and sensors have a tab-like interface. Using the tabs you can navigate through various sub-pages of an object in order to show your network's status, view monitoring results, or change settings.

Overview	2 days	30 days	365 days	Alarms	Log	Management	Settings	Notifications	Help

Tabs Bar on Group and Probe Level

On an object's detail view, click on the **Log** tab to show a table list with all log information **on this object**. This is a more detailed log than the system log available via the **Logs | All** option in [main menu](#)¹⁸².

Logs (Main Menu)

Click the **Logs** entry from the [main menu](#)¹⁸² to show a table list of all system log entries in your configuration. **Hover** the Logs entry and select another option to only show a subset of entries for certain objects for certain kind of entries. Choose between:

- **All**
Show log information for all objects in your configuration, newest first.

- **By Group ›**
Show log information for objects in a certain group only, newest first. **Hover** to show other menu items. Select **All**, or follow the menu path (it is specific to your setup) to select a group you would like to show log information for.
- **Status Changes ›**
Show log information for certain status changes only. **Hover** to show other menu items. Follow the menu path to view log entries with a special value in the **Status** field only. Select between **Up & Down** (shows entries with either **Up** or **Down** in the **Status** field), **Down**, **Warning**, **Unusual**, **Up**, **Paused/Resumed** (shows entries with either **Paused** or **Resumed** in the **Status** field), or **Acknowledged Alarms**.
- **System Events ›**
Show log information regarding certain system event types only. **Hover** to show other menu items. Select between the following event types: **Probe Related**, **Cluster Related**, **Auto-Discovery**, **Notifications**, or **Status Messages**.

5.12 Tickets

PRTG Network Monitor includes its own ticket system. With tickets you can manage and maintain various issues which may appear while monitoring a network. A ticket in PRTG contains information about recent events in your PRTG installation which need a closer look by the administrator or another responsible person. You can see each ticket as a task for a particular PRTG user.

Each monitoring related task has a lifecycle in the ticket system. PRTG itself can create tickets, for example, when [Auto-Discovery](#)^[190] has finished, as well as PRTG users can create tickets for every kind of issue. In addition, you can set up notifications which open a ticket when something uncommon occurs in your network. The task gets alive when a ticket is created. Responsible PRTG users then take care of this issue. Once the issue has been resolved, the ticket can be closed and the lifecycle of the task ends.

Every ticket has a unique ID, a priority, and a status, and you can take several actions on each ticket. You should view every ticket and conduct a corresponding action. This way, you always keep an overview about each task and its history in your PRTG installation.

PRTG can also send an email to you whenever there is a ticket assigned to you or one of your tickets has been changed. See section [Tickets as Emails](#)^[152] for details and how to turn off emails about tickets.

The screenshot displays the 'Tickets' section of the PRTG Network Monitor web interface. The top navigation bar includes links for Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. A search bar is located on the right. Below the navigation bar, a summary bar shows statistics: 44 tickets, 10 critical, 14 warning, 909 resolved, 36 pending, and 32 unknown. The main area is titled 'Tickets' and shows a list of 50 items. The list has columns for 'Last modified', 'Priority', 'Ticket ID', 'Subject', 'Assigned to', 'Status', 'Object', and 'Actions'. The tickets are sorted by 'Last modified' in descending order. The subjects include software updates, auto-discovery, and various reports. The 'Assigned to' column shows 'PRTG Administrators' for most tickets. The 'Status' column shows various icons representing different states. The 'Object' column shows the specific system or device associated with the ticket. The 'Actions' column provides links for 'Edit', 'Assign', 'Resolve', and 'Close' for each ticket. At the bottom of the list, there is a 'List of Tickets' label.

Last modified	Priority	Ticket ID	Subject	Assigned to	Status	Object	Actions
3 h 17 m ago	★★★★★	#1285	Software update available for PRTG Network Monitor	PRTG Administrators	Open	System	Edit Assign Resolve Close
13 h 56 m ago	★★★★★	#1284	Auto-Discovery finished for "acronismprotect.pae...de (Acronis Appliance)"	PRTG Administrators	Open	acronismprotect.pae...de (Acronis Appliance)	Edit Assign Resolve Close
23 h 48 m ago	★★★★★	#1283	Software update is not available	PRTG Administrators	Open	System	Edit Assign Resolve Close
09.12.2013 00:00:17	★★★★★	#1282	Report finished	PRTG Administrators	Open	Report	Edit Assign Resolve Close
05.12.2013 12:48:19	★★★★★	#1281	Software update available for PRTG Network Monitor	PRTG Administrators	Open	System	Edit Assign Resolve Close
04.12.2013 12:47:12	★★★★★	#1280	Software update available for PRTG Network Monitor	PRTG Administrators	Open	System	Edit Assign Resolve Close
04.12.2013 06:37:36	★★★★★	#1279	Flow processor buffer full (code: PE110)	PRTG Administrators	Open	NetFlow V9 1	Edit Assign Resolve Close
03.12.2013 12:46:24	★★★★★	#1278	Software update available for PRTG Network Monitor	PRTG Administrators	Open	System	Edit Assign Resolve Close
03.12.2013 11:20:11	★★★★★	#1277	Auto-Discovery finished for "NPIA22D0B (Support Printer) [HP Printer]"	PRTG Administrators	Open	NPIA22D0B (Support Printer) [HP Printer]	Edit Assign Resolve Close
02.12.2013 15:07:22	★★★★★	#1274	Software update is not available	PRTG Administrators	Open	System	Edit Assign Resolve Close
02.12.2013 00:00:35	★★★★★	#1273	Report finished	PRTG Administrators	Open	Report	Edit Assign Resolve Close
29.11.2013 12:43:04	★★★★★	#1272	Software update available for PRTG Network Monitor	PRTG Administrators	Open	System	Edit Assign Resolve Close
27.11.2013 12:40:33	★★★★★	#1271	Software update available for PRTG Network Monitor	PRTG Administrators	Open	System	Edit Assign Resolve Close
25.11.2013 16:18:57	★★★★★	#1270	Flow processor buffer full (code: PE110)	PRTG Administrators	Open	NetFlow V9 1	Edit Assign Resolve Close
25.11.2013 15:16:26	★★★★★	#1269	Report finished	PRTG Administrators	Open	Top 100 Uptime/Downtime Report	Edit Assign Resolve Close
25.11.2013 15:08:09	★★★★★	#1268	Software update is not available	PRTG Administrators	Open	System	Edit Assign Resolve Close
25.11.2013 15:00:35	★★★★★	#1267	Report finished	PRTG Administrators	Open	Firewall Report	Edit Assign Resolve Close
25.11.2013 14:00:58	★★★★★	#1266	Report finished	PRTG Administrators	Open	Firewall Report	Edit Assign Resolve Close

List of Tickets

Note: You can turn off the tickets system for particular user groups in [System Administration—User Groups](#)^[1829]. You cannot disable tickets for the PRTG Administrators group because of important system information which PRTG communicates via tickets. A PRTG System Administrator user will always receive tickets because this user has to be in the administrators group. You cannot change this behavior. However, you can [turn off ticket emails](#)^[152] for every user account.

Types of Tickets

New tickets are created in the following cases:

- New devices or sensors have been created by the auto-discovery process. **Note:** In the corresponding ticket, only device templates will be listed through which PRTG created sensors.
- A new probe connects to the core and must be acknowledged.
- A new cluster node connects to the cluster and must be acknowledged.
- A new version of the software is available.
- A new report is ready for review.
- In a few other situations, such as when the system runs out of disk space, for licensing issues, when an error occurred, etc.
- A [notification](#)^[1723] opened a ticket if set in the notification settings.
- A user opened a ticket.

Overall, there are three types of tickets:

- **User Tickets:** Tickets created by PRTG users, for example, to assign monitoring related tasks to a particular PRTG user (or user group)
- **ToDo Tickets:** Tickets created by PRTG to show important system information and in case of specific system events. They are assigned to **all** PRTG system administrators and cannot be switched off.
Note: The **Related Object** of ToDo tickets is **System**.
- **Notification Tickets:** Tickets created via [Notifications](#)^[1723] in case of monitoring alerts

States of Tickets

Tickets can have three different states depending on the working process regarding the corresponding issue:

- **Open:** New tickets will be open as long as the corresponding issue exists as described in the ticket.
- **Resolved:** The issue as described in the ticket does not persist any longer. Someone took care of it.
- **Closed:** Usually, the ticket has been resolved before, the solution to the issue has been checked for correctness, and the ticket does not require any other action.

Tickets (Main Menu)

Note: This option is only shown in the main menu bar if the user group of the current user is allowed to use the ticket system. You can turn off tickets for particular user groups in [System Administration—User Groups](#)^[1829]. Users with **read-only** rights are always excluded from the ticket system and cannot see the tickets entry in the main menu bar.

You have several options to display a list of tickets which is filtered to your needs. In the [main menu bar](#)^[174], **hover** on **Tickets**^[1829] to show all available filter options or **click** directly to show all tickets assigned to the current user. You can also create a new ticket via the main menu. Available options are:

- **My Tickets**
Click to show all open tickets which are assigned to the current user. **Hover** to show other menu items for filtering these tickets depending on their status:
 - **Open**
 - **Resolved**
 - **Closed**
 - **All**
- **All Tickets**
Click to show all open tickets of all PRTG users. **Hover** to show other menu items for filtering these tickets depending on their status:
 - **Open**
 - **Resolved**
 - **Closed**
 - **All**
- **ToDo Tickets**
Click to show all open tickets from the [type](#)^[149] **ToDo**. **Hover** to show other menu items for filtering these tickets depending on their status:
 - **Open**
Click to show all open ToDo tickets. **Hover** to show other menu items for filtering these tickets depending on their event type:
 - **Report Related**
 - **Auto-Discovery Related**
 - **Probe Related**
 - **System Errors**
 - **New Software Version**
 - **Resolved**
 - **Closed**

- **All**
- **Open Ticket**
This will open the **New Ticket** dialog. In the first step, select the object on which you want to focus in the ticket via the [Object Selector](#)^[158]. Click on **Continue**. **Note:** You can leave this step out when using the [context menu](#)^[162] of this object in the device tree to open the ticket.

In step 2, provide the following information and confirm by clicking on **Save** to create a **User Ticket**:
 - **Subject:** Enter a meaningful title for the ticket which indicates the topic of the issue.
 - **Assigned to:** Select a user (or user group) who will be responsible for this issue from the drop down list.
 - **Priority:** Define a [priority](#)^[159] from one to five stars.
 - **Comments:** Enter a text message. This message should describe the issue in detail.

After selecting the desired filter or opening a new user ticket, a corresponding list of tickets will appear. In this table list, you can re-sort the items by using the [respective options](#)^[155]. Additionally, you have several search options using the inline filter directly above the table. The following filters are available:

- **Ticket status:** all, open, resolved, closed
- **Ticket type:** User, ToDo, Notification
- **Concerned user(s):** Show only tickets which are assigned to a specific user or user group. There are the following types:
 - **anyone:** no user filter is applied so all tickets on this PRTG server are shown
 - **me:** show tickets which are assigned to you (the user who is currently logged in)
 - **Groups:** show tickets which are assigned to a specific user group only
 - **Users:** show tickets which are assigned to a specific user only
 - **Disallowed:** users or user groups which do not have access rights to the selected object are displayed under **Disallowed**. This for your information only; you cannot select them!
- **Relationship to a monitoring object:** Choose groups, probes, devices, sensors with the [Object Selector](#)^[158].
Note: ToDo tickets are related to **System**.
- **Time span** to view tickets by last edit of a ticket: Use the date time picker to enter the date and time.

Click on the subject of a ticket to open the ticket's detail page. There you can find all related information, as well as you can conduct several actions.

The screenshot shows the PRTG Network Monitor web interface. The top navigation bar includes links for Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. A search bar is on the right. Below the navigation bar, there's a status bar with various icons and counts. The main content area displays a ticket for 'Flow processor buffer full (code: PE110)' with a status of 'Open'. It is assigned to 'PRTG Administrators' and has a related object of 'NetFlow V9 1'. The ticket type is 'ToDo Ticket Info' and the ID is '#1279'. Below the ticket details, there are buttons for 'Edit', 'Assign', 'Resolve', and 'Close'. A 'LAST UPDATE' section shows a message: 'The flow processor has dropped flows. Try optimizing your include, exclude and filter rules (Most likely matches first, use brackets to structure the rule, use ip ranges and masks instead of separate IPs) (code: PE111)'. At the bottom, it says 'An Open ToDo Ticket with Instructions'.

Actions

For best experience with PRTG, check every ticket and select appropriate actions. **Note:** Only members of user groups which have the corresponding [access rights](#)^[94] can view and edit to tickets which are related to a certain monitoring object.

The following actions are available when viewing the tickets list or a specific ticket:

- **Edit:** Opens a dialog where you can change the subject and the priority of the ticket, as well as you can assign the ticket to another user. Furthermore, you can add a text message to this ticket. Confirm your changes by clicking on **Save**.
- **Assign:** Opens a dialog in which you can give the ticket to another user. Select a user (or user group) via the drop down menu. Furthermore, you can add a text message to this ticket. Confirm your assignment by clicking on **Save**.
- **Resolve:** Opens a dialog where you can resolve the ticket by clicking on **Save**. The status **resolved** indicates that the issue as described in this ticket does not persist. Furthermore, you can add a text message to this ticket which indicates, for example, what has been done concerning the issue.
- **Close:** Opens a dialog where you can close the ticket by clicking on **Save**. Usually, this ticket has been resolved before and the correct solution of the issue has been checked. Furthermore, you can add a text message to this ticket.
- **Reopen:** Opens a dialog where you can reopen a ticket after it has been resolved or closed. Do so, for example, if the solution of the issue turned out to be incorrect. Furthermore, you can add a text message to this ticket which indicates, for example, why you have opened the ticket again. Confirm reopening and assignment by clicking on **Save**.

Tickets as Emails

You can receive all tickets which are assigned to you or to your user group as emails. You will be also notified each time this ticket is edited via email. This way, you will keep always informed about new notifications (if set), important system information, or within the communication with other PRTG users. You can turn off the setting **Tickets as Emails** in [System Administration—User Accounts](#)^[1024]. If you disable emails for tickets for a user account, this particular user will not receive any ticket emails anymore.

Note: If you have defined to get tickets as emails and you are PRTG System Administrator, you will receive emails for ToDo tickets as well, although ToDo tickets are considered to be opened by the PRTG System Administrator.

More

Paessler Blog: A New Feature Was Assigned to You in PRTG: Ticket System Keeps Track of Network Monitoring Issues

- <http://www.paessler.com/blog/2014/02/03/news/ticket-system-keeps-track-of-network-monitoring-issues>

Ajax Web Interface—Basic Procedures—Topics

- [Login](#)  102
- [SSL Certificate Warning](#)  105
- [General Layout](#)  108
- [Sensor States](#)  121
- [Review Monitoring Data](#)  124
- [Compare Sensors](#)  129
- [Historic Data Reports](#)  132
- [Similar Sensors](#)  137
- [Object Settings](#)  141
- [Alarms](#)  143
- [Logs](#)  146
- [Tickets](#)  148
- [Working with Table Lists](#)  155
- [Object Selector](#)  158
- [Priority and Favorites](#)  159
- [Pause](#)  161
- [Context Menus](#)  162
- [Hover Popup](#)  173
- [Main Menu Structure](#)  174

Other Ajax Web Interface Sections

- [Ajax Web Interface—Device and Sensor Setup](#)  188
- [Ajax Web Interface—Advanced Procedures](#)  1700

Related Topics

- [Enterprise Console](#)  1860
- [Other User Interfaces](#)  1912

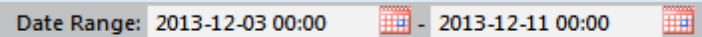
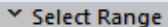
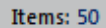
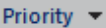
5.13 Working with Table Lists

Throughout the web interface often you will see table lists of items, for example, sensor or device lists. Table lists are also available in the **Overview** tab of [Libraries](#)^[173], [Maps](#)^[176], [Reports](#)^[174], [Notifications](#)^[173], and [Schedules](#)^[180], as well as in [Logs](#)^[146] and [Tickets](#)^[148]. All these provide common functionality.

On certain overview pages, such as for [sensors](#)^[177], [tickets](#)^[150], and [similar sensors](#)^[139], there is also an inline filter available directly above the table. The filter options depend on the current page.

Example of a Table List

Probe Group Device	Sensor	Status	Message	Last Value	Graph	Priority	Fav.
Local probe (0) > Firewalls > Cisco ASA Primary	✓ (003) WAN	Up	OK	23 Mbit/s	Traffic Total 23 Mbit/s	★★★★★	⌵
Local probe (0) > Firewalls > Cisco ASA Primary	✓ (004) LAN	Up	OK	24 Mbit/s	Traffic Total 24 Mbit/s	★★★★★	⌵
Local probe (0) > Firewalls > Cisco ASA FO/Test	✓ (001) Marvell 88E606x 100MBIT Half and Full Duplex Ethernet	Up	OK	0,19 Mbit/s	Traffic Total 0,19 Mbit/s	★★★★★	⌵
Local probe (0) > Switches > Core Switch	✓ (012) Service NAS1	Up	OK	0,18 Mbit/s	Traffic Total 0,18 Mbit/s	★★★★★	⌵
Local probe (0) > Switches > GigabitSwitch Server	✓ (001) Ethernet Interface	Up	OK	0,20 Mbit/s	Traffic Total 0,20 Mbit/s	★★★★★	⌵
Local probe (0) > Baseline > Google Search Appliance	✓ (001) io	Up	OK	0,38 Mbit/s	Traffic Total 0,38 Mbit/s	★★★★★	⌵

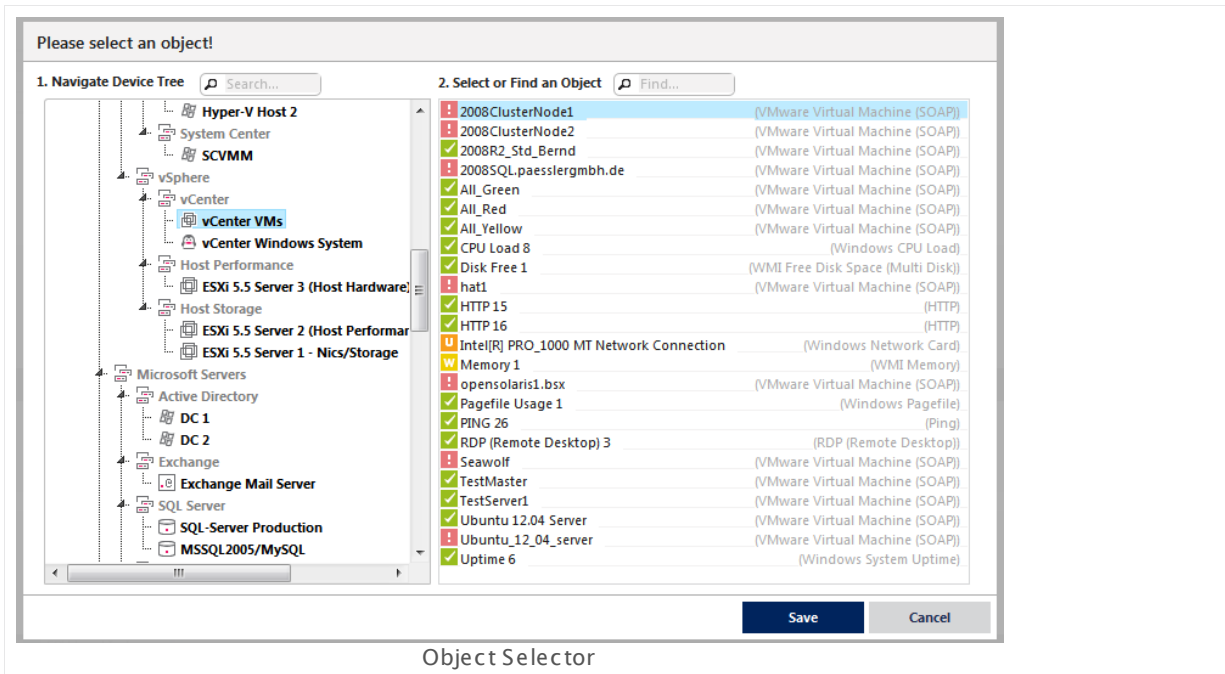
Feature	Display	What it does
Paging		The content of a table is displayed on several pages. Click on the arrow symbols at the beginning or the end of a list to view other pages, or to jump to the beginning or the end of the list.
New Window		Click on the window symbol at the beginning or the end of a list to open the table in a new window.
Date Range		Use the date time picker to show table list entries within a specific time span only. Click on the first date field for the start date and on the second field for the end date. A calendar will open where you can particularly select date and time. Click on the Done button to apply the selected date and time.
Select Range		When viewing log lists (not available in other lists), hover the Select Range option at the upper right corner of the list to select the time span you want to show log entries for. Choose between Today , Yesterday , and several other time spans. Choose Unlimited to disable this filter again.
Items		Hover the Items option at the beginning or end of the list to select how many rows are shown on each page. Choose between 50, 100, 500, and 1000.
Sorting		Click on the column headers to sort lists by the respective column.

Related Topics

- [Multi-Edit Lists](#) 

5.14 Object Selector

For some functions, the object selector is shown. It enables you to browse all objects in your configuration and select an object in two steps.



Step 1: Navigate Device Tree

On the left hand side, you see a device tree specific to your setup that you can browse by clicking on the corresponding nodes. Click on a device to view its sensors on the right hand side.

You can directly browse for objects in the device tree by entering a probe name, group name, or device name into the **Search...** field above the device tree navigation. You can also use a substring only. The resulting objects will be displayed immediately without any manual confirmation.

Step 2: Select an Object

If you have selected a device on the left hand side, you will see the sensors on this device here, on the right hand side. Also, the sensor type is shown. **Hover** a sensor on the right side to view its parent device and group.

You can also directly search and find sensors by entering its sensor name, group name, device name, or tag into the **Find...** box above the sensor list.

Select an object and click on the **Save** button.

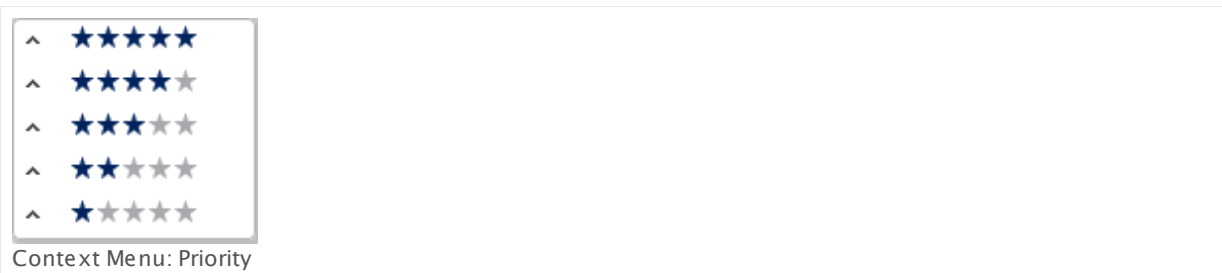
5.15 Priority and Favorites

You can set priorities for all objects in your setup as well as categorize devices or sensors as favorites. Both settings affect how your objects will be displayed. **Note:** Settings for priority and favorites are stored for the entire installation; they are not user specific.

Priority for All Objects

The priority setting will affect in which order your objects will be displayed when viewing table lists. Objects with a higher priority are listed first, others underneath, depending on their own priority.

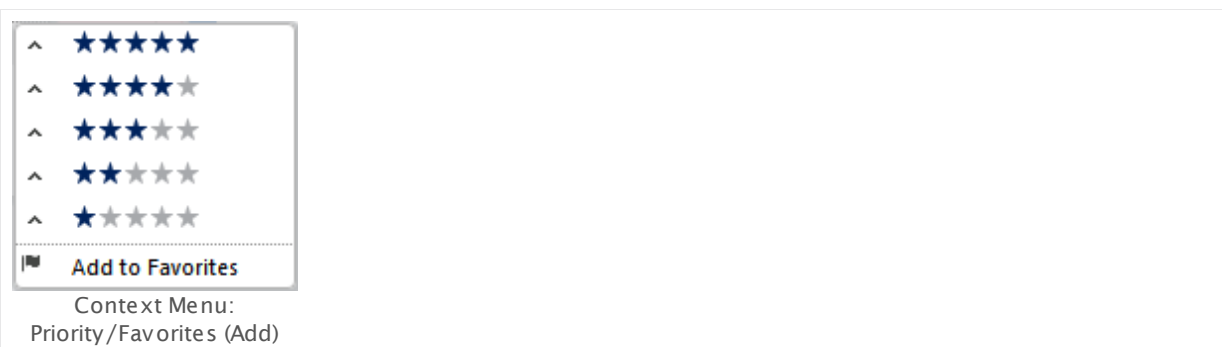
To change priority settings, **right-click** an object to open the [context menu](#)¹⁶² and select **Priority**. You can choose between 5 stars ********* (top priority) and one star ***** (lowest priority). By default, all objects are set to medium priority (3 stars *****)**. In the page header bar and in lists, you can set a priority directly by one click on a star, for example, for sensors on a device overview page.



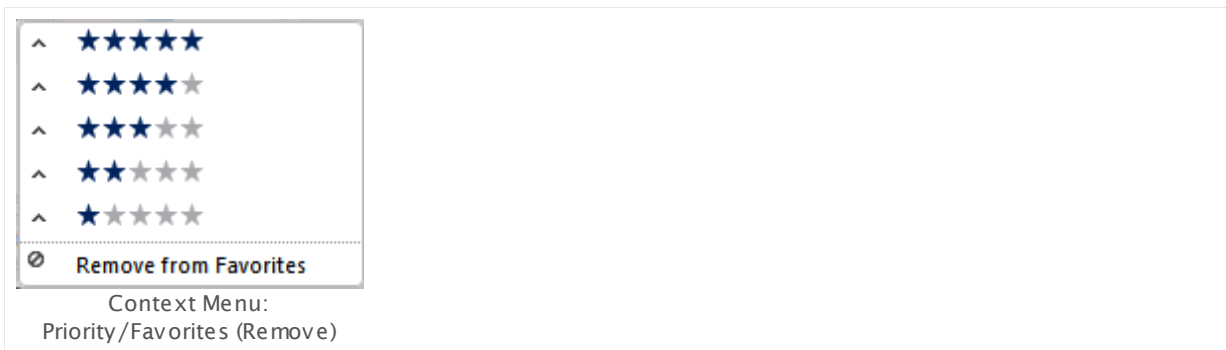
Favorites for Devices and Sensors

To call a list of all your favorite devices or sensors, select **Devices | Favorite Devices** or **Sensors | Favorite Sensors** from the main menu. These lists are sorted by priority as well.

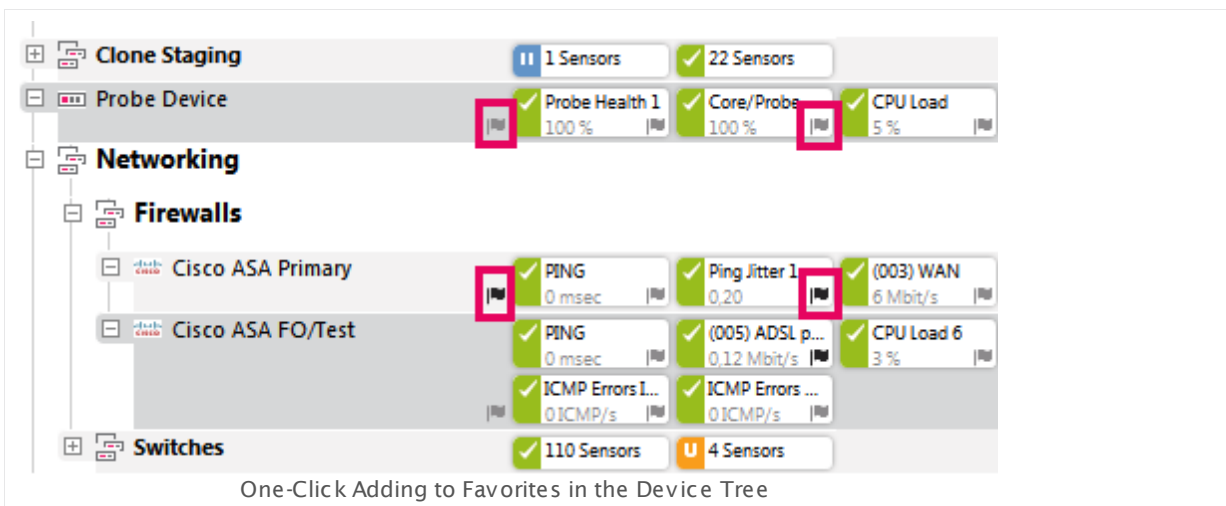
You can mark any device or sensor as favorite to add it to the favorite list. Right click on it to open the [context menu](#)¹⁶². Select **Priority/Favorite | Add to Favorites**. A small black flag symbol will be added next to the object's name.



To remove an object from the favorites list, select **Priority/Favorite | Remove from Favorites** from the [context menu](#)¹⁶².



There is also the option to add a device or sensor to favorites by one click in the device tree. Just click on the small flag symbol right to the respective object name for this concern. If the flag is black, the specific object is already a favorite; clicking anew on the flag will remove it from favorites and the flag will turn gray again.



Priority and Favorites in the Page Header Bar

You can add any device or sensor to favorites on its respective details page by clicking on the small flag symbol in the [page header bar](#)¹¹³. If the flag is black, the selected object is already a favorite; clicking anew on the flag will remove it from favorites and the flag will turn gray again. It is also possible to set the priority of the object by a click on one of the five stars in the page header; five stars ***** means top priority, one star * is the lowest priority.

Device **Cisco ASA Primary** | ★★★★★

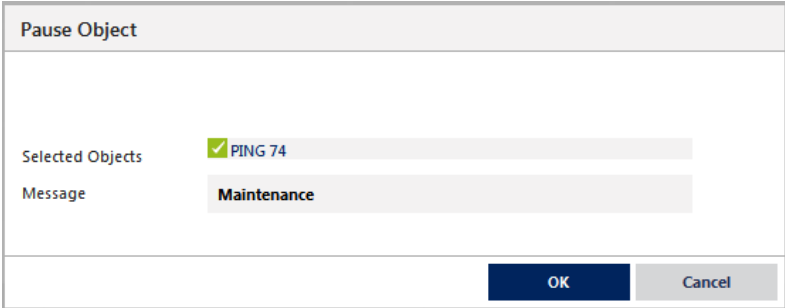
One-Click Favorite and Priority in the Page Header Bar

5.16 Pause

While a sensor is paused, it will not collect any monitoring data, will not change its [status](#)^[121], and will not trigger any [notifications](#)^[92]. You can pause monitoring for every object by selecting **Pause** from the [context menu](#)^[162] of a probe, a group, a device, or a sensor. All sensors on this object will then be paused. You can choose **Pause Indefinitely**, or select a time after which monitoring will be resumed automatically, such as **5 or 15 minutes**, **1 or 3 hours**, **1 day**, or **Until** a certain date. You can also set up a one-time maintenance window to pause sensors automatically at a specified time.

Note: When selecting the **Pause** symbol from an object's [hover popup](#)^[173] or while using [multi-edit](#)^[1710], the object(s) will be paused indefinitely until resumed.

When selecting a pause option, you are prompted to enter a message. This will be shown in the status message of the object as long as it is paused. Confirm with **OK** to pause the object; click **Cancel** to not pause it.



PRTG Pause Message Prompt

Note: Monitoring for objects can also be paused by applying a schedule (see [Account Settings—Schedules](#)^[1801]) in the [Object Settings](#)^[141].

Inheritance and Resume

If you pause monitoring for an object in the [device tree](#)^[108], all child objects underneath will be paused as well. For example, when pausing a group, all sensors on all devices in it will also be paused. Once an object is paused, you can resume monitoring any time by selecting **Resume** from the [context menu](#)^[162]. However, you cannot resume monitoring for single child objects that are paused by a parent object, but only for the object you originally set to pause. **Note:** Also after a restart of PRTG, a pause status will be kept.

5.17 Context Menus

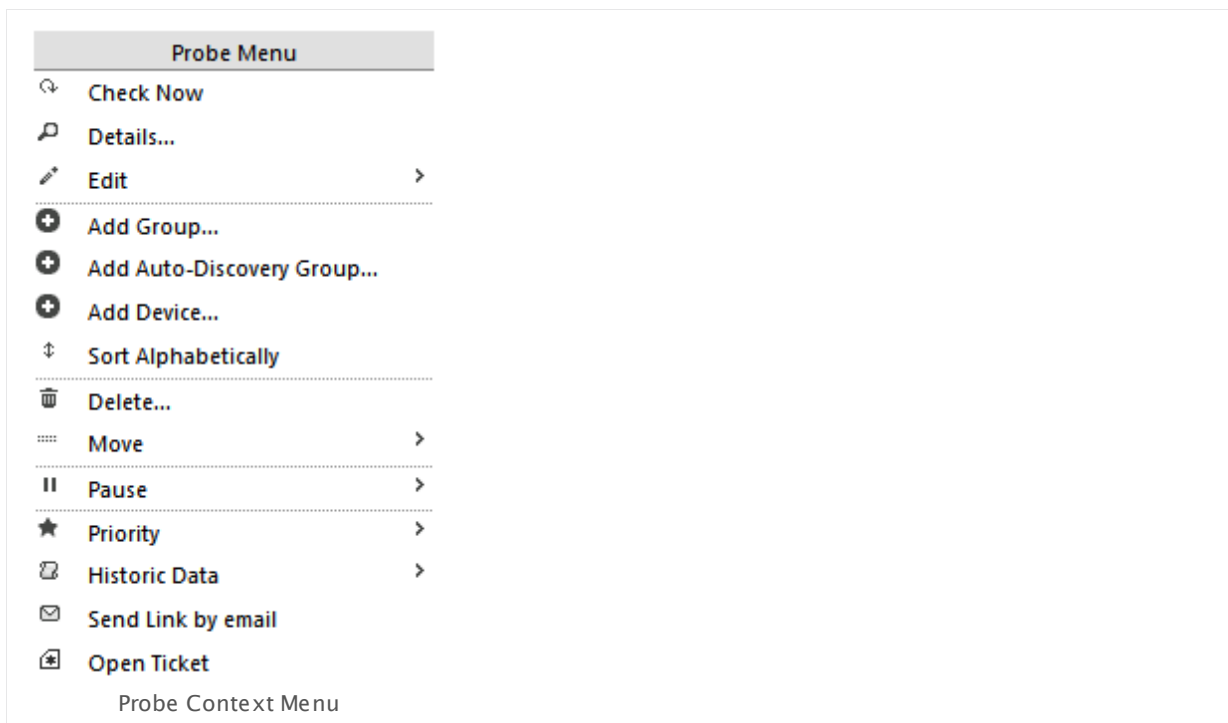
Right-click on an object to view a context menu with many options for direct access to monitoring data and functions. You can also access many of the functionalities via the [main menu](#)^[174] or the [hover popup](#)^[173] window. However, using the context menus is the easier way in most cases.

Note: In order to view your browser's context menu, hold down the **Ctrl** key (Chrome) or the **Shift** key (Firefox) while right-clicking. You will then see your browser's instead of the PRTG menu. This is not possible with Internet Explorer.

The content of the PRTG context menu varies, depending on the type of object you have selected. Please see the following sub sections for an overview of the available options.

- [Probe Context Menu](#)^[162]
- [Group Context Menu](#)^[165]
- [Device Context Menu](#)^[167]
- [Sensor Context Menu](#)^[170]

Probe Context Menu



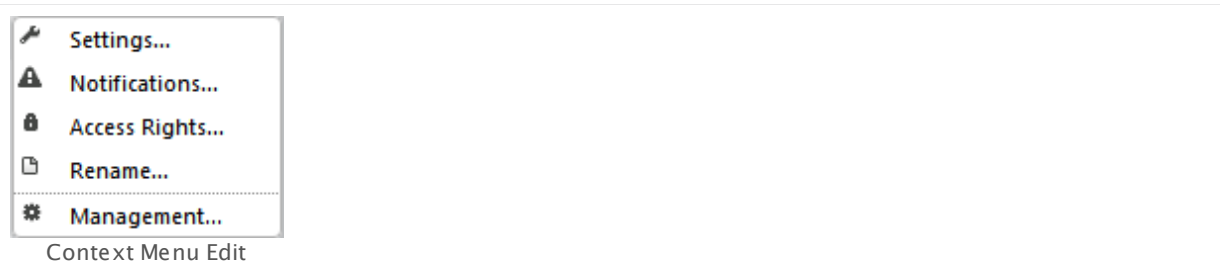
- **Check Now**
This will perform an immediate scan for the selected probe. The data for all devices and sensors in the [object hierarchy](#)^[83] underneath will be queried.

- **Details...**

This will show the details of the selected probe, such as its status, the groups on the selected probe, and an overview about the sensor states on the selected probe.

- **Edit >**

The edit menu will appear.



- **Edit > Settings...**

This will open the [Probe Settings](#)^[238] tab.

- **Edit > Notifications...**

This will open the [Notifications](#)^[1728] tab.

- **Edit > Access Rights...**

This will open a popup to edit [access rights](#)^[94].

- **Edit > Rename...**

This will open a popup to edit the name of the selected probe.

- **Edit > Management...**

This will open the [management](#)^[222] tab.

- **Add Group...**

This will open an assistant which guides you through the process of adding a new group to the selected probe. For detailed instructions, please see [Add a Group](#)^[205].

- **Add Auto-Discovery Group...**

This will open an assistant which guides you through the process of adding a new auto-discovery group to your setup. PRTG will create a new group and run an auto-discovery in your network in order to add devices and sensors for these devices automatically. For more information, please see section [Using the Auto-Discovery](#)^[190].

- **Add Device...**

This will open an assistant which guides you through adding a new device to the selected probe. For detailed instructions, please see [Add a Device](#)^[211].

- **Sort Alphabetically**

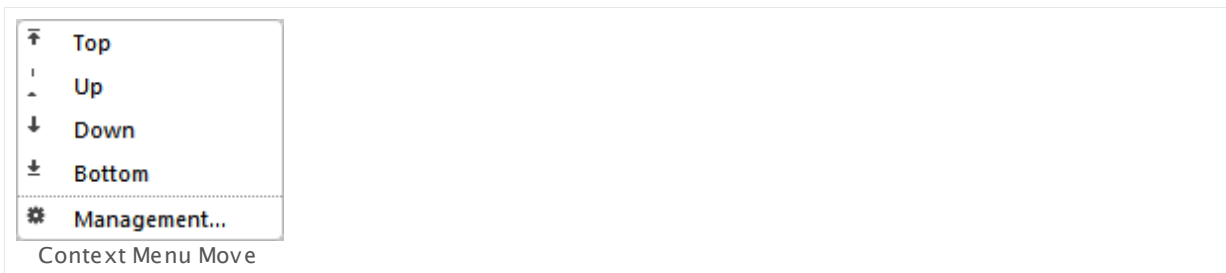
This will sort direct children (groups and devices) of the selected probe in alphabetical order. The ordering will be stored in the monitoring configuration and cannot be revoked.

- **Delete...**

This will delete the selected probe. You will be asked for confirmation before anything is actually deleted.

- **Move >**

The move menu will appear.



- This will move the selected probe. Choose between
 - **Move > Top**: This will move the probe to the top of the mother node (here the root group).
 - **Move > Up**: This will move the probe one entry up under the root group.
 - **Move > Down**: This will move the probe one entry down under the root group.
 - **Move > Bottom**: This will move the probe to the bottom of the root group.
 - **Move > Management...**: This will open the [management](#)^[222] tab.
- **Pause >**
The pause menu will appear.



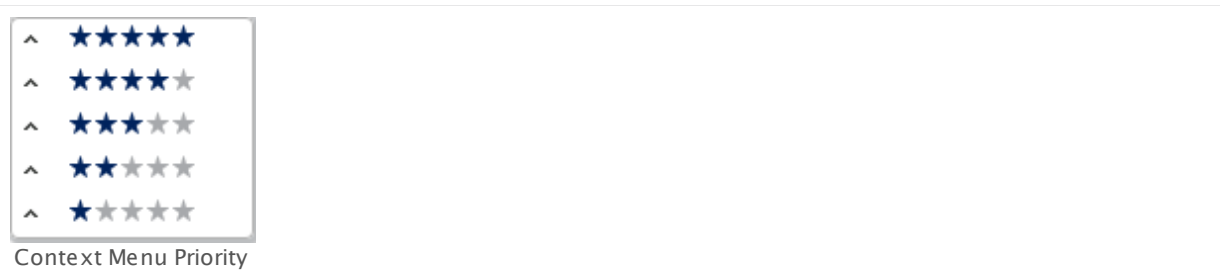
- If the probe is already in a paused state, **Resume** will appear in the context menu instead of **Pause >**.



- You can pause and resume monitoring on the selected probe. The monitoring for all sensors in the [object hierarchy](#)^[83] underneath will be paused resp. resumed. You can choose between: **Pause Indefinitely...**, **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Pause Until...**. If you choose **Pause Until...** a popup window will appear where you can define a date. Monitoring will be resumed after this date.
- You can directly add a **One-time maintenance window** to pause monitoring during a planned downtime. In the appearing window, use the date time picker to enter the start date and time of the maintenance window, as well as the end time, for the selected object.

- **Priority >**

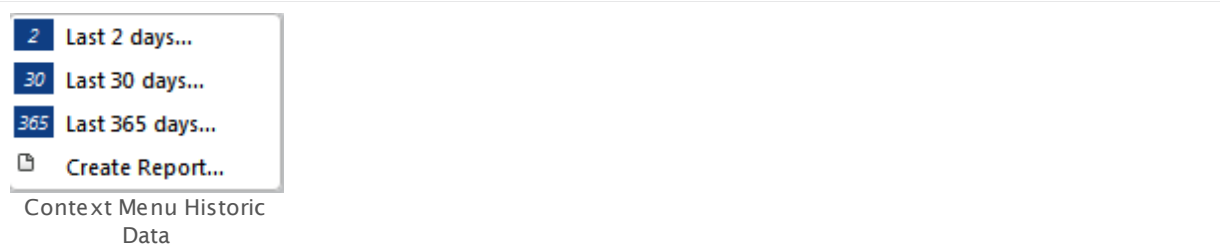
The priority menu will appear.



- Define the priority of the selected probe. For details, please see [Priority and Favorites](#) ¹⁵⁹.

- **Historic Data >**

The historic data menu will appear.



- Depending on what time interval you choose, **Last 2 days...**, **Last 30 days...**, or **Last 365 days...**, the [Historic Data Reports](#) ¹³² tab for the specified interval will be opened.
- **Historic Data > Create Report...** will open an assistant to add a report. For details, please see [Reports Step by Step](#) ¹⁷⁵².
- **Send Link by email**
You can send the link to the selected probe by email. This will open a new email using your system's standard email client. It will contain a direct link to the selected probe's details page.
- **Open Ticket**
This will open the **New Ticket** dialog. For details, see section [Tickets](#) ¹⁵¹.

Group Context Menu

Note: The context menu of the **Root** group is special and differs from the other groups' menu.

- **Check Now**
This will perform an immediate scan for the selected group. The data for all devices and sensors in the [object hierarchy](#) ⁸³ underneath will be queried.
- **Details...**
This will show the details of the selected group, such as its status, the devices on the selected group, and an overview about the sensor states on the selected group.
- **Edit >**
The edit menu will appear.

- **Settings...**
This will open the [Group Settings](#)^[253] tab.
- **Notifications...**
This will open the [Notifications](#)^[1723] tab.
- **Access Rights...**
This will open a popup to edit [access rights](#)^[94].
- **Rename...**
This will open a popup to edit the name of the selected group.
- **Management...**
This will open the [management](#)^[222] tab.
- **Add Group...**
This will open an assistant which guides you through the process of adding a new group to the selected group. For detailed instructions, please see [Add a Group](#)^[205].
- **Add Auto-Discovery Group...**
This will open an assistant which guides you through the process of adding a new auto-discovery group to your setup. PRTG will create a new group and run an auto-discovery in your network in order to add devices and sensors for these devices automatically. For more information, please see section [Using the Auto-Discovery](#)^[190].
- **Add Device...**
This will open an assistant which guides you through adding a new device to the selected group. For detailed instructions, please see [Add a Device](#)^[211].
- **Run Auto-Discovery**
If you select this option, an automatic search is started, adding new sensors to the selected group. The search is running in the background. If found, you will see new sensors after a few minutes automatically. For more information, please see [Auto-Discovery](#)^[191] (**Run Auto-Discovery Now**).
- **Sort Alphabetically**
This will sort direct children (devices and other groups) of the selected group in alphabetical order. The ordering will be stored in the monitoring configuration and cannot be revoked.
- **Delete...**
This will delete the selected group. You will be asked for confirmation before anything is actually deleted.
- **Clone**
This will open an assistant which guides you through cloning the selected group. For detailed instructions, please see [Clone Object](#)^[1708].
- **Move >**
The move menu will appear.
 - This will move the selected group. Choose between:
 - **Move > Top**: This will move the group to the top of the mother node (here usually a probe or another group).
 - **Move > Up**: This will move the group one entry up under the mother node.
 - **Move > Down**: This will move the group one entry down under the mother node.
 - **Move > Bottom**: This will move the group to the bottom of the mother node.

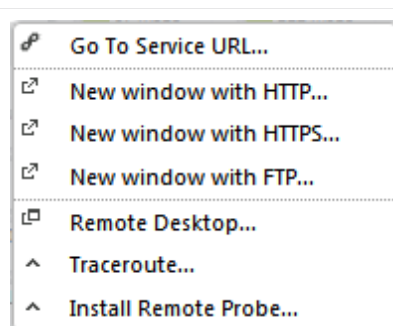
- **Move > To Other Group:** This will move the group to another group. An assistant will appear in this case with information about the selected group and the sub-objects which also will be moved. Please choose a target group from the list.
- **Move > Management...** This will open the [management](#)^[222] tab.
- **Pause >**
The pause menu will appear.
 - If the group is already in a paused state, **Resume** will appear in the context menu instead of **Pause >**.
 - You can pause and resume monitoring on the selected group. The monitoring for all sensors in the [object hierarchy](#)^[83] underneath will be paused resp. resumed. You can choose between: **Pause Indefinitely...**, pause **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Pause Until...** If you choose **Pause Until...** a popup window will appear where you can define a date. Monitoring will be resumed after this date.
 - You can directly add a **One-time maintenance window** to pause monitoring during a planned downtime. In the appearing window, use the date time picker to enter the start date and time of the maintenance window, as well as the end time, for the selected object.
- **Priority >**
The priority menu will appear. Define the priority of the selected group. For details, please see [Priority and Favorites](#)^[159].
- **Historic Data >**
The historic data menu will appear.
 - Depending on what time interval you choose, **Last 2 days...**, **Last 30 days...**, or **Last 365 days...**, the [Historic Data Reports](#)^[132] tab for the specified interval will be opened.
 - **Historic Data > Create Report...** will open an assistant to add a report. For details, please see [Reports Step by Step](#)^[1752].
- **Send Link by email**
You can send the link to the selected group by email. This will open a new email using your system's standard email client. It will contain a direct link to the selected probe's details page.
- **Open Ticket**
This will open the **New Ticket** dialog. For details, see section [Tickets](#)^[151].

Device Context Menu

- **Check Now**
This will perform an immediate scan for the selected device. The data for all sensors in the [object hierarchy](#)^[83] underneath will be queried.
- **Details...**
This will show the details of the selected device, such as its status and the sensor states on the selected device.
- **Edit >**
The edit menu will appear.

- **Settings...**
This will open the [Device Settings](#)^[272] tab.
- **Notifications...**
This will open the [Notifications](#)^[1723] tab.
- **Access Rights...**
This will open a popup to edit [access rights](#)^[94].
- **Rename...**
This will open a popup to edit the name of the selected device.
- **Add Sensor...**
This will open an assistant which guides you through adding a new sensor to the selected device. For detailed instructions, please see [Add a Sensor](#)^[220].
- **Run Auto-Discovery**
If you select this option, an automatic search is started, adding new sensors to the selected device. The search is running in the background. If found, you will see new sensors after a few minutes automatically. For more information, please see [Auto-Discovery](#)^[191] (**Run Auto-Discovery Now**).
- **Create Device Template...**
This will open an assistant which guides you through creating a new device template; this will then be available in [auto-discovery](#)^[190]. For detailed instructions, please see [Create Device Template](#)^[1715].
- **Sort Alphabetically**
This will sort direct children (sensors) of the selected device in alphabetical order. The ordering will be stored in the monitoring configuration and cannot be revoked.
- **Delete...**
This will delete the selected device. You will be asked for confirmation before anything is actually deleted.
- **Clone**
This will open an assistant which guides you through cloning the selected device. For detailed instructions, please see [Clone Object](#)^[1708].
- **Move >**
The move menu will appear. This will move the selected device. Choose between:
 - **Move > Top**: This will move the device to the top of the mother node (here usually a group or a probe).
 - **Move > Up**: This will move the device one entry up under the mother node.
 - **Move > Down**: This will move the device one entry down under the mother node.
 - **Move > Bottom**: This will move the device to the bottom of the mother node.
 - **Move > To Other Group**: This will move the device to another group. An assistant will appear in this case with information about the selected device and the sub-objects which also will be moved. Please choose a target group from the list.
- **Pause >**
The pause menu will appear. If the device is already in a paused state, **Resume** will appear in the context menu instead of **Pause >**.

- You can pause and resume monitoring on the selected device. The monitoring for all sensors in the [object hierarchy](#)^[83] underneath will be paused resp. resumed. You can choose between: **Pause Indefinitely...**, pause **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Pause Until...**. If you choose **Pause Until...** a popup window will appear where you can define a date. Monitoring will be resumed after this date.
- You can directly add a **One-time maintenance window** to pause monitoring during a planned downtime. In the appearing window, use the date time picker to enter the start date and time of the maintenance window, as well as the end time, for the selected object.
- **Priority/Favorite >**
The priority/favorite menu will appear. Define the priority of the selected device, or add resp. remove the device to resp. from the favorites. For details, please see [Priority and Favorites](#)^[159].
- **Historic Data >**
The historic data menu will appear.
 - Depending on what time interval you choose, **Last 2 days...**, **Last 30 days...**, or **Last 365 days...**, the [Historic Data Reports](#)^[132] tab for the specified interval will be opened.
 - **Historic Data > Create Report...** will open an assistant to add a report. For details, please see [Reports Step by Step](#)^[1752].
- **Device Tools >**
The device tools menu will appear.



Context Menu Device Tools

- **Go To Service URL..**
This will open the service page you have defined in the [Device Settings](#)^[272].
- **New window with HTTP...**
This will open a new browser window with Hypertext Transfer Protocol (HTTP) and the IP address / DNS name of the device.
- **New window with HTTPS...**
This will open a new browser window with Hypertext Transfer Protocol Secure (HTTPS) and the IP address / DNS name of the device.
- **New window with FTP...**
This will open a new browser window with File Transfer Protocol (FTP) and the IP address / DNS name of the device.

- **Remote Desktop...**

This will download a .rdp file. When you execute the file remote desktop will start with the IP address / DNS name of the device. **Note:** In Firefox you have to use mstsc.exe (Microsoft Terminal Service) to open the file.

- **Traceroute...**

This will start a traceroute on the selected device. PRTG will display the route and measure transit delays of packets across the IP network.

- **Install Remote Probe...**

This will open an assistant to install a **Remote Probe** of PRTG on this device. For more details, please see [Remote Probe Quick Install](#)  ²⁰¹⁵.

- **Find Duplicates...**

Search in your PRTG configuration for devices with the same IP address or DNS name as the selected device. A window with the results will appear, either showing existing duplicates or a message indicating that there are no duplicates.

- **Send Link by email**

You can send the link to the selected device by email. This will open a new email using your system's standard email client. It will contain a direct link to the selected probe's details page.

- **Open Ticket**

This will open the **New Ticket** dialog. For details, see section [Tickets](#)  ¹⁵¹.

Sensor Context Menu

- **Check Now**

This will perform an immediate scan for the selected sensor.

- **Details...**

This will show the details of the selected sensor, such as its status and channels.

- **Edit ›**

The edit menu will appear.

- **Settings...**

This will open the [Sensor Settings](#)  ²⁹⁰ tab.

- **Notifications...**

This will open the [Notifications](#)  ¹⁷²³ tab.

- **Channels...**

This will open the **Channels** tab.

- **Access Rights...**

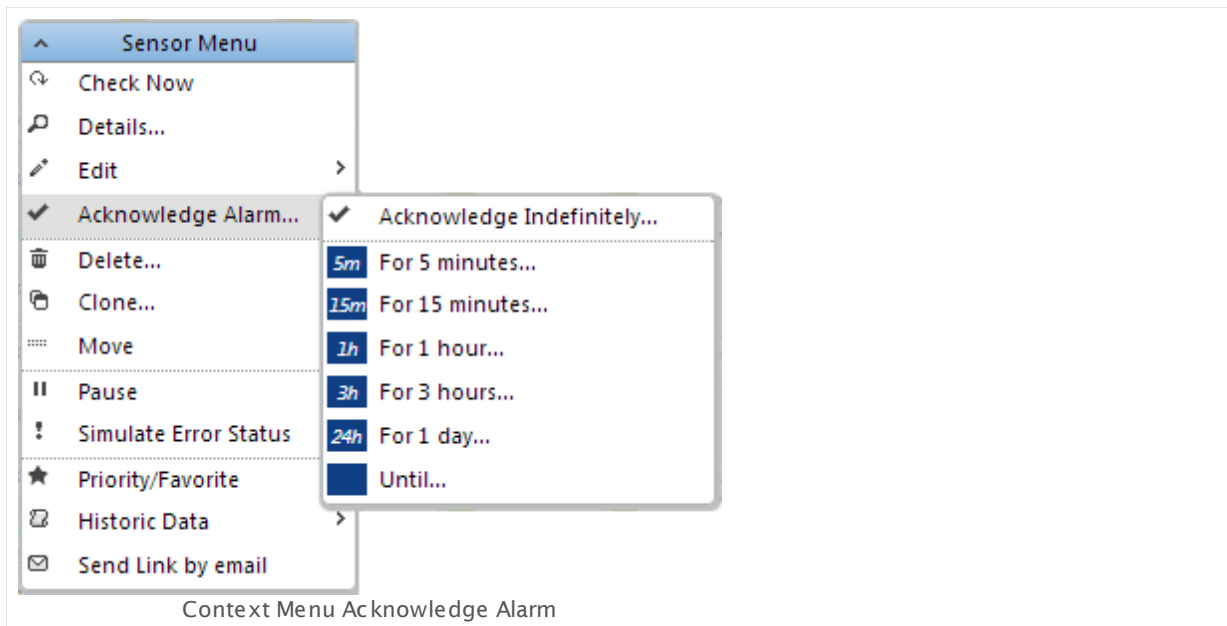
This will open a popup to edit [access rights](#)  ⁹⁴.

- **Rename...**

This will open a popup to edit the name of the selected device.

- **Acknowledge Alarm ›**

This option is available only in the sensor context menu when a sensor in a **Down** or **Down (Partial)** status is selected.



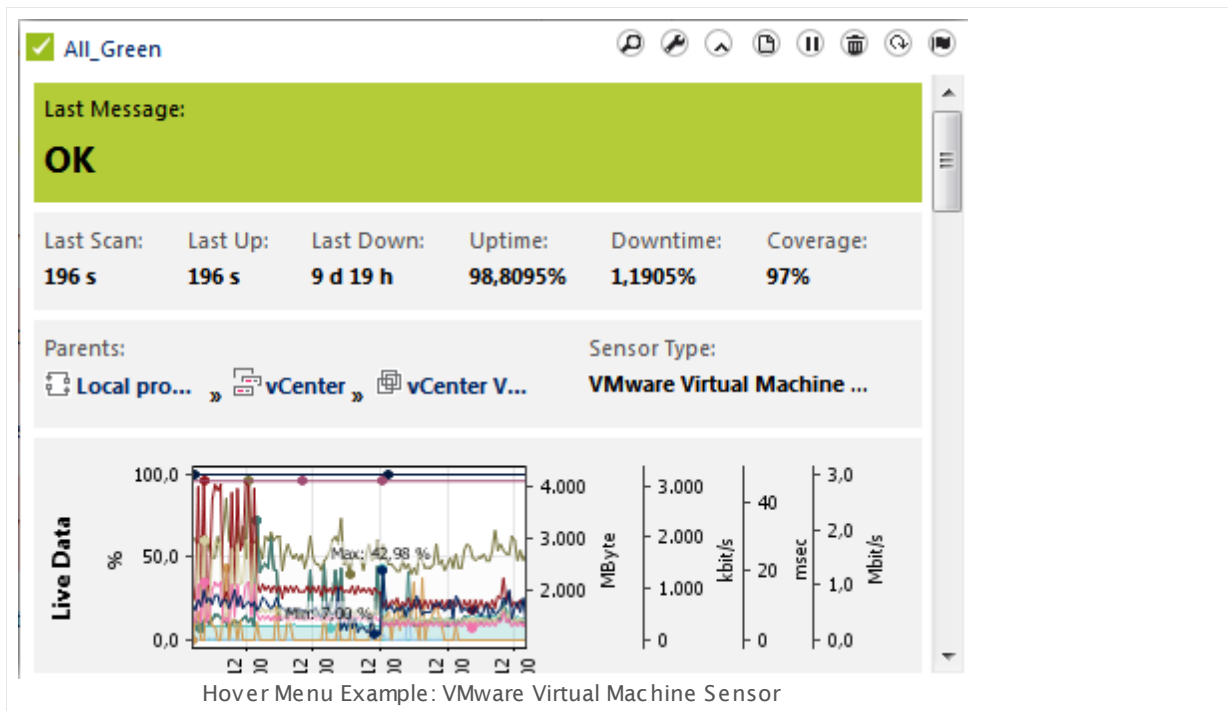
Context Menu Acknowledge Alarm

- You can acknowledge an alarm for the selected sensor. An acknowledged alarm will show up in the alarms list as "acknowledged" (see [Sensor States](#)^[121]) and will not [trigger](#)^[1090] any more [notifications](#)^[1723]. You can choose between: **Acknowledge Indefinitely...**, **acknowledge For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Until...**. If you choose **Until...** a popup window will appear where you can define a date. If the alarm condition still exists after this date, the sensor will show a **Down** status again. **Note:** If the alarm condition clears, the sensor will usually return into an **Up** status immediately with the next sensor scan. For details about acknowledging an alarm, please see [Alarms](#)^[144] section.
- **Delete...**
This will delete the selected sensor. You will be asked for confirmation before anything is actually deleted.
- **Clone**
This will open an assistant which guides you through cloning the selected sensor. For detailed instructions, please see [Clone Object](#)^[1708].
- **Move >**
The move menu will appear. This will move the selected sensor. Choose between:
 - **Move > Top:** This will move the sensor to the top of the mother node (here a device).
 - **Move > Up:** This will move the sensor one entry up under the device.
 - **Move > Down:** This will move the sensor one entry down under the device.
 - **Move > Bottom:** This will move the sensor to the bottom of the device.
- **Pause >**
The pause menu will appear. If the sensor is already in a paused state, **Resume** will appear in the context menu instead of **Pause >**.

- You can pause and resume monitoring on the selected sensor. You can choose between: **Pause Indefinitely...**, pause **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Pause Until...**. If you choose **Pause Until...** a popup window will appear where you can define a date. Monitoring will be resumed after this date.
- You can directly add a **One-time maintenance window** to pause monitoring during a planned downtime. In the appearing window, use the date time picker to enter the start date and time of the maintenance window, as well as the end time, for the selected object.
- **Simulate Error Status**
This will set the selected sensor to a simulated error state. As for the paused state, **Resume** will appear in the context menu if a the selected sensor is already in a simulated error state.
- **Priority/Favorite >**
The priority/feature menu will appear.
 - Define the priority of the selected sensor. For details, please see [Priority and Favorites](#) ¹⁵⁹.
- **Historic Data >**
The historic data menu will appear.
 - Depending on what time interval you choose, **Last 2 days...**, **Last 30 days...**, or **Last 365 days...**, the [Historic Data Reports](#) ¹³² tab for the specified interval will be opened.
 - **Historic Data > Create Report...** will open an assistant to add a report. For details, please see [Reports Step by Step](#) ¹⁷⁵².
- **Send Link by email**
You can send the link to the selected sensor by email. This will open a new email using your system's standard email client. It will contain a direct link to the selected probe's details page.
- **Open Ticket**
This will open the **New Ticket** dialog. For details, see section [Tickets](#) ¹⁵¹.

5.18 Hover Popup

Whenever you rest the mouse pointer for a second over an object's icon in the [device tree](#)^[108], a hover popup window will appear, showing details about this object. It contains information from the object's [overview tab](#)^[124], as well as several graphs. The exact information provided depends on the kind of object you are hovering.



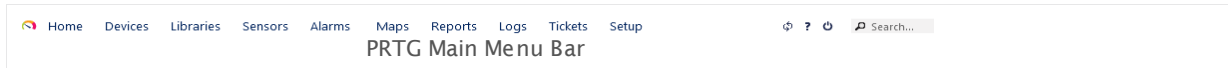
Note: The hover popup does only appear if your browser is the currently focused window on your desktop. It disappears with every (automatic) page refresh.

Menu Icons

At the top of the hover popup window, several icons are shown which enable you to view or edit the current object. These are the most important options from this object's [context menu](#)^[162] which is shown when right-clicking it.

5.19 Main Menu Structure

Using the main menu, you can access all functions of PRTG. Following, the most important menu items are described. Often, you can either **click** on an item directly, or **hover** it to show more items.



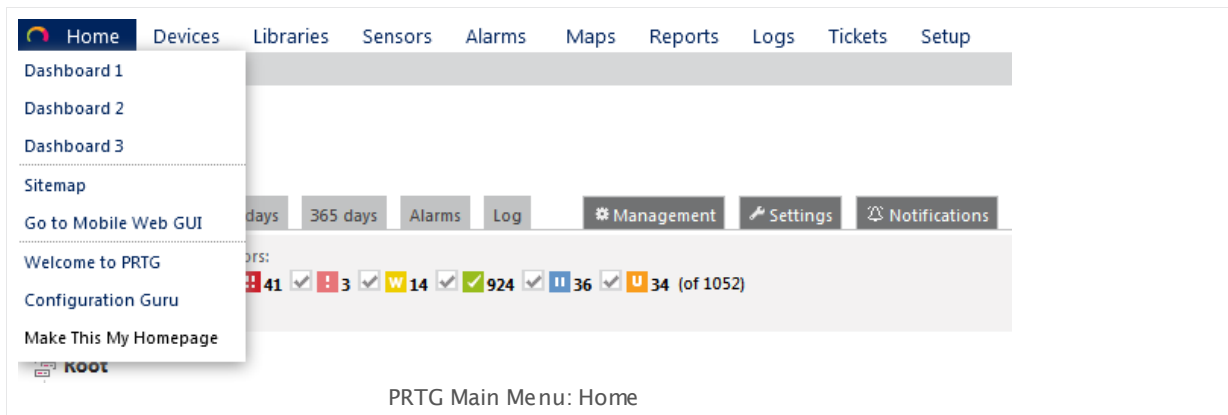
Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

The following menu items are available:

- [Home](#)  174
- [Devices](#)  175
- [Libraries](#)  177
- [Sensors](#)  177
- [Alarms](#)  180
- [Maps](#)  181
- [Reports](#)  181
- [Logs](#)  182
- [Tickets](#)  182
- [Setup](#)  183
- [Refresh \(Arrows Symbol\)](#)  184
- [Help Center \(? Symbol\)](#)  185
- [Logout \(Off Symbol\)](#)  185
- [Search Box](#)  185

Home

Click to open the user's homepage. The default setting is PRTG's welcome page. The homepage can be changed in the user's [account settings](#)  1786. **Hover** to show other menu items.



▪ Dashboard 1 – Dashboard 3

The dashboards provide different preset overviews with the status of your sensors. Choose the one that fits your needs. **Note:** Dashboards are not customizable. You can create your own overview pages using the [Maps](#) ¹⁷⁶⁸ feature.

▪ Switch Cluster Node >

This option is only available if PRTG runs in [Clustering](#) ⁸¹ mode. Show available cluster nodes. **Hover** to show other menu items. Follow the menu path (it is specific to your setup) to select another cluster node. The current Master node is shown in bold letters. Click on a node's name and you will leave the current node and connect to the other, showing the same page there.

▪ Sitemap

The sitemap contains a flat text view of all menu items. You can easily search for key words using the search function in your browser (usually shortcut **CTRL-F**).

▪ Go to Mobile Web GUI

This switches to the [Mobile Web GUI](#) ¹⁹¹³ optimized for low bandwidth and mobile devices. Less scripting is used for more compatibility. However, this is a read-only interface.

▪ Welcome to PRTG

Shows the welcome screen which leads you to the major sections of the web interface.

▪ Configuration Guru

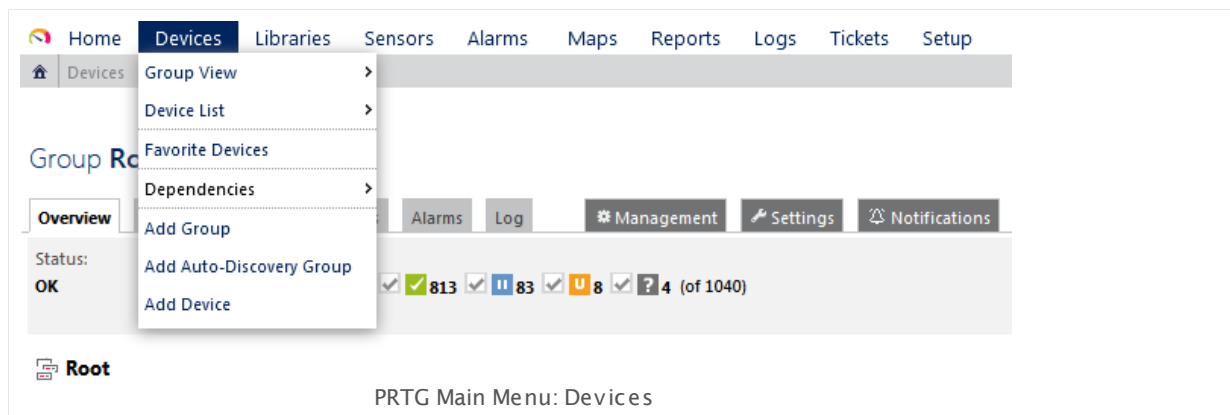
This will open the **Configuration Guru** welcome page. For details about the guru, please see section [Using the Configuration Guru](#) ³⁶.

▪ Make This My Homepage

Change the page that is loaded when you click on the **Home** button in the main menu. Select this menu item on any page and its URL will be set as the current user's homepage immediately. This setting is user sensitive. The default homepage is [/welcome.htm](#). You can change this setting any time by clicking on this menu item again, or by changing the **Homepage URL** in the [My Account](#) ¹⁷⁸⁶ settings.

Devices

Click to show a group view of all your devices, starting with the **Root** group which contains all other groups of your setup. **Hover** to show other menu items.



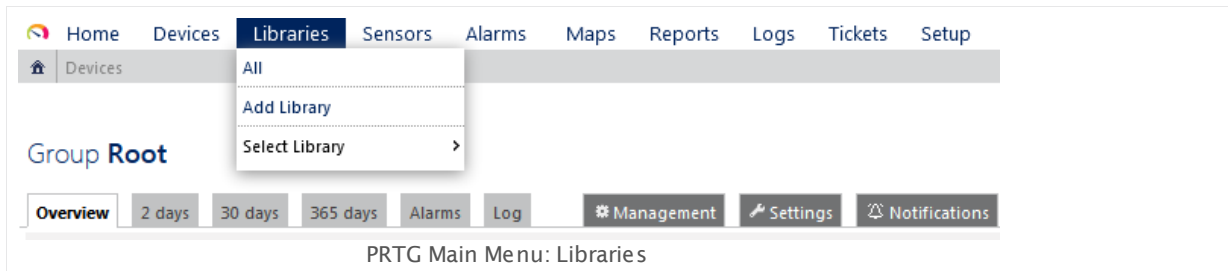
- **Group View** ›
Shows a tree view of all probes and groups in your setup. **Click** to show a group view of all your devices, starting with the **Root** group which contains all other groups of your setup. **Hover** to show other menu items. Follow the menu path (it is specific to your setup) to view the devices in a specific probe or group only.
- **Device List** ›
Shows a list view of all devices in your setup. **Click** to show a table list of all devices in your setup. **Hover** to show other menu items. Choose **Favorite Devices** to show a list of all devices marked as **Favorite**^[159]. **Note:** Follow the menu path (it is specific to your setup) to view a table list of the devices in a specific probe or group only. In the **table list**^[155] appearing, you can re-sort the items by clicking on the column's header items.
- **Favorite Devices**
Shows a table list of all devices marked as **Favorite**^[159]. **Note:** To mark any device as a favorite device, select **Priority/Favorite | Add to Favorites** from its context menu or click on the small flag on a device's details page.
- **Dependencies** ›
Shows an overview list of the dependencies configured for the objects in your setup. **Hover** the menu item to show other menu items. Choose between **Selected Dependencies** and **Master Dependencies** to view a list of all dependencies or explicit ones. Follow the menu path (it is specific to your setup) to view dependencies of the objects in a specific probe or group only.
- **Add Group**
Start an assistant which guides you through the process of adding a new group to your setup. For more information, please see section **Create Objects Manually**^[204]. **Tip:** You can create new groups much faster by choosing **Add Group...** from a probe's or group's context menu!
- **Add Auto-Discovery Group**
Start an assistant which guides you through the process of adding a new auto-discovery group to your setup. PRTG will create a new group and run an auto-discovery in your network in order to add devices and sensors for these devices automatically. For more information, please see section **Using the Auto-Discovery**^[190]. **Tip:** You can create new groups much faster by choosing **Add Auto-Discovery Group...** from a probe's or group's context menu!

▪ Add Device

Start an assistant which guides you through the process of adding a new device to an existing group. During the process, you can choose if PRTG should run an auto-discover for the new device in order to add sensors automatically. For more information, please see section [Create Objects Manually](#)^[204]. **Tip:** You can create new devices much faster by choosing **Add Device...** from a group's context menu!

Libraries

Click to call the Libraries feature where you can view or add custom views of your network's status and monitoring data. For more information, please see [Libraries](#)^[1733] section. **Hover** to show other menu items.



▪ All

Calls the Libraries feature where you can view or add custom device tree views of your network's status and monitoring data.

▪ Add Library

Lets you directly [add](#)^[1736] a new library.

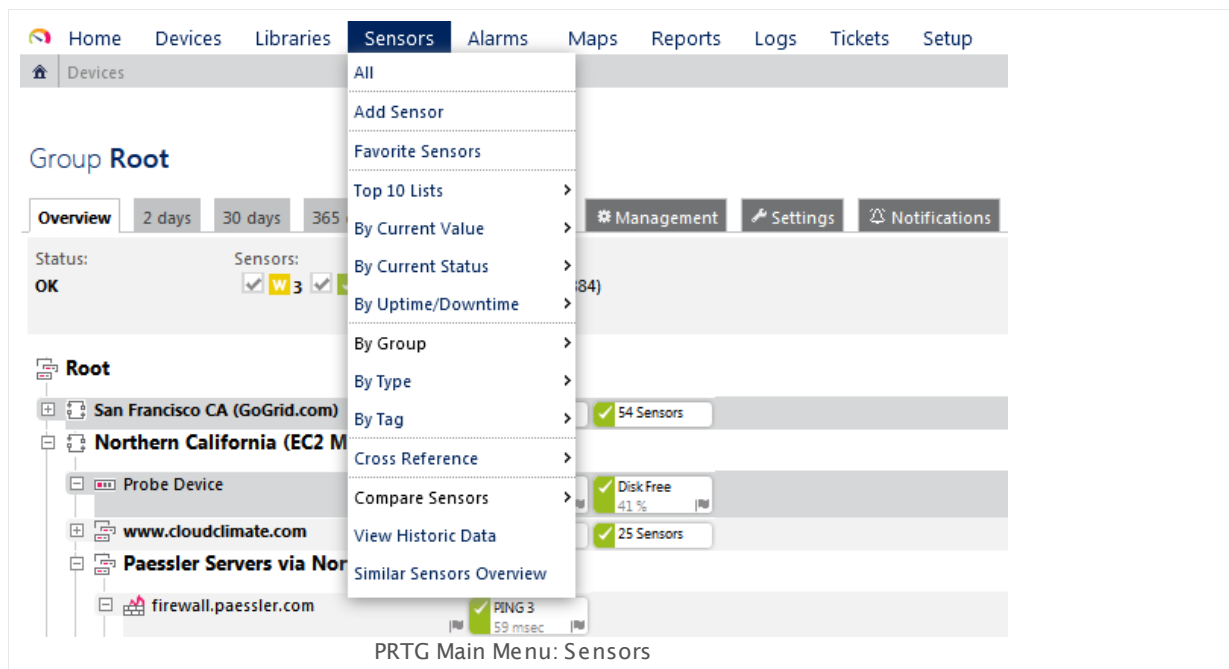
▪ Select Library ›

Show existing libraries. **Hover** to show other menu items. Follow the menu path (it is specific to your setup) to select a library.

Sensors

Click to show a table list of all sensors. In the [table list](#)^[155] appearing, you can re-sort the items by clicking on the column's header items, as well as you can filter the list by related object and tag with the inline filter directly above the table.

Hover Sensors in the main menu bar to show other menu items. **Note:** In the column **Last Value** only the last value of the sensor's **primary channel** will be shown.



- **All**
Shows a table list of all sensors. In the table list appearing, you can re-sort the items by clicking on the column's header items. **Note:** In the column **Last Value** only the last value of the sensor's **primary channel** will be shown.
- **Add Sensor**
Start an assistant which guides you through the process of adding a new sensor to an existing device. For more information, please see section [Add a Sensor](#)^[220]. During the process, you can also choose to create a new device. This will bring you to the "Add Device" assistant you can call from the "Devices" menu directly.
- **Favorite Sensors**
Shows a table list of all sensors marked as [Favorite](#)^[159]. **Note:** To mark any sensor as a favorite sensor, select **Priority/Favorite | Add to Favorites** from its context menu or click on the small flag on a device's details page.
- **Top 10 Lists >**
This is an option to show a dashboard view with different Top 10 lists regarding best/worst uptime, Ping, bandwidth usage, website response times, memory usage, and system uptime. **Click** to show Top 10 lists out of all sensors. **Hover** to show other menu items. Follow the menu path (it is specific to your setup) to view Top 10 lists out of a specific probe or group only. **Note:** The sensors will be selected by default tags.
- **By Current Value >**
This is an option to show a filtered sensor list. **Hover** to show other menu items. Follow the menu path to view [table lists](#)^[155] of **Fastest** or **Slowest** sensors regarding
 - **Ping**
 - **Port**
 - **Webpages**
 - **IMAP/POP3/SMTP**
 - **FTP**

as well as **Most Used** or **Least Used** sensors regarding

- **Bandwidth**
- **CPU**
- **Disk**
- **Memory**

Note: The sensors will be selected by default tags.

- **By Current Status ›**

This is an option to show a filtered sensor list. **Hover** to show other menu items. Follow the menu path to view [table lists](#)^[1667] of all sensors in a certain state. Select between status

- **Up**
- **Warning**
- **Down**
- **Down (Partial)**
- **Down (Acknowledged)**
- **Unusual**
- **Paused**
- **Unknown**

For more information about sensor states, please see [Sensor States](#)^[1221] section.

- **By Uptime/Downtime ›**

This is an option to show a filtered sensor list. **Hover** to show other menu items. Follow the menu path to view [table lists](#)^[155] of all sensors sorted by their up- or downtime. Select between

- **Best Uptime (%)**
- **Highest Uptime (Time)**
- **Worst Downtime (%)**
- **Highest Downtime (Time)**

- **By Group ›**

This is an option to show a filtered sensor list. **Hover** to show other menu items. Follow the menu path (it is specific to your setup) to view a sensor [table list](#)^[155] of a specific probe or group only.

- **By Type ›**

This is an option to show a filtered sensor list. **Hover** to show other menu items. Follow the alphabetical menu path (it is specific to your setup) to view a sensor [table list](#)^[155] containing only sensors of one specific sensor type.

- **By Tag ›**

This is an option to show a filtered sensor list. **Hover** to show other menu items. Follow the alphabetical menu path (it is specific to your setup) to see available tags. Select a tag view a [table list](#)^[155] containing only sensors marked with this tag.

- **Cross Reference** ›

The cross reference shows information about all sensors including the set interval, access rights, notification trigger settings, schedule, and dependency. **Click** to show a sensor cross reference for all sensors. **Hover** to show other menu items. Follow the menu path (it is specific to your setup) to view cross reference information for sensors in a specific probe or group only, or to view them by type or tag.

- **Compare Sensors** ›

Calls a function to compare graphs of two or more monitoring objects. **Hover** to show other menu items. Follow the menu path to open an assistant for comparing several monitoring objects. For more information, please see [Compare Sensors](#)^[129] section.

- **View Historic Data**

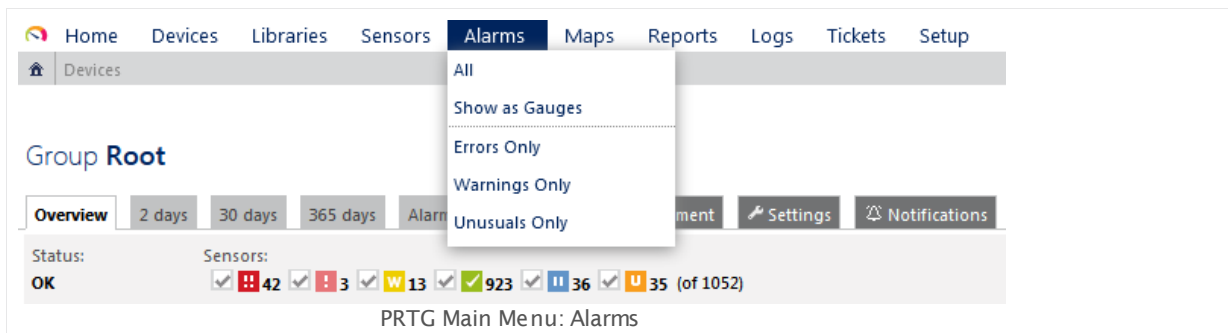
Calls a function for quick generation of sensor data reports. For more information, please see [Historic Data Reports](#)^[132] section.

- **Similar Sensors Overview**

Calls an overview page listing similar sensors. For more information, please see [Similar Sensors](#)^[137] section.

Alarms

Click to show a all sensors that currently show a **Down**, **Down (Partial)**, **Warning**, or **Unusual** status. In the [table list](#)^[155] appearing, you can re-sort the items by clicking on the column's header items. If you select **Show as Gauges**, the sensor gauges will be displayed in a size corresponding to their priority. **Hover** to show other menu items.



- **All**

Shows a list of all sensors which currently show a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status.

- **Show as Gauges**

Shows the gauges of all sensors which currently show a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. The size of the sensor gauges corresponds to their respective priority.

- **Errors Only**

Shows a list of all sensors which currently show a **Down**, **Down (Partial)**, or **Down (Acknowledged)** status.

- **Warnings Only**

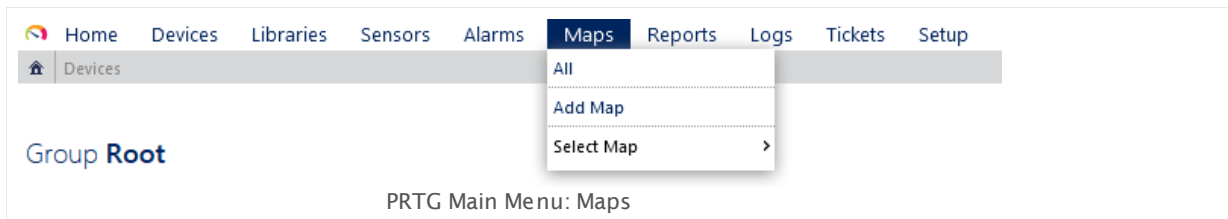
Shows a list of all sensors which currently show a **Warning** status.

- **Unusuals Only**

Shows a list of all sensors which currently show an **Unusual** status.

Maps

Click to call the Maps feature where you can view or add custom views of your network's status and monitoring data. For more information, please see [Maps](#)¹⁷⁶⁸ section. **Hover** to show other menu items.



- **All**

Calls the Maps feature where you can view or add custom views of your network's status and monitoring data.

- **Add Map**

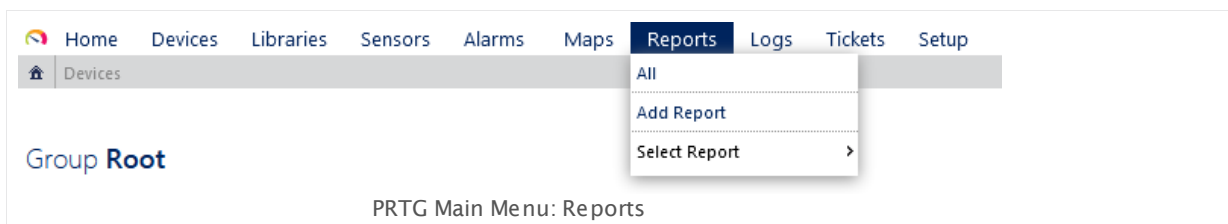
Lets you directly [add](#)¹⁷⁷¹ a new map.

- **Select Map ›**

Show existing maps. **Hover** to show other menu items. Follow the menu path (it is specific to your setup) to select a map.

Reports

Click to call the Reports feature where you can view or add reports of your monitoring data. For more information, please see [Reports](#)¹⁷⁴⁹ section. **Hover** to show other menu items.



- **All**

Calls the Reports feature where you can view or add reports of your monitoring data.

- **Add Report**

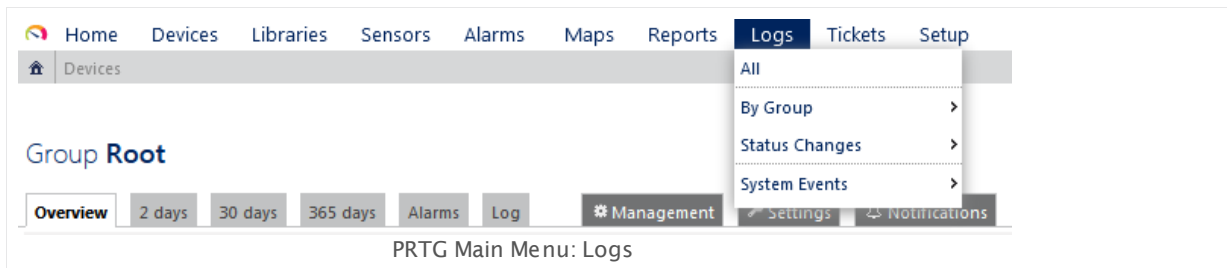
Lets you directly add a new report.

- **Select Report ›**

Show existing reports. **Hover** to show other menu items. Follow the menu path (it is specific to your setup) to select a report.

Logs

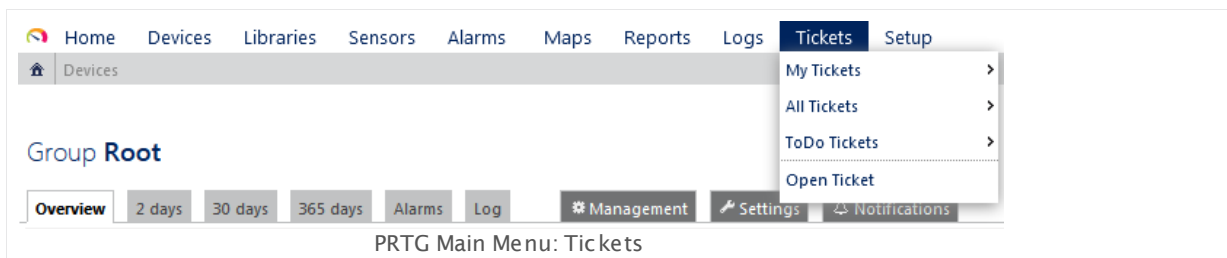
Click to show log information for all objects in your configuration, newest first. In the [table list](#) ^[155] appearing, you can filter the items by using the [respective options](#) ^[155]. **Hover** to show other menu items. For more information, please see [Logs](#) ^[146] section.



- **All**
Show log information for all objects in your configuration, newest first.
- **By Group >**
Show log information for objects in a certain group only, newest first. **Hover** to show other menu items. Select **All**, or follow the menu path (it is specific to your setup) to select a group you would like to show log information for.
- **Status Changes >**
Show log information for certain status changes only. **Hover** to show other menu items. Follow the menu path to view log entries with a special value in the **Status** field only. Select between **Up & Down** (shows entries with either **Up** or **Down** in the **Status** field), **Down**, **Warning**, **Unusual**, **Up**, **Paused/Resumed** (shows entries with either **Paused** or **Resumed** in the **Status** field), or **Acknowledged Alarms**.
- **System Events >**
Show log information regarding certain system event types only. **Hover** to show other menu items. Select between the following event types: **Probe Related**, **Cluster Related**, **Auto-Discovery**, **Notifications**, or **Status Messages**.

Tickets

Tickets show important system information or action steps to take for the administrator. For best experience with PRTG, check every ticket and conduct appropriate actions. **Click** to show all tickets which are assigned to the current user. In the [table list](#) ^[155] appearing, you can re-sort the items by clicking on the column's header items, as well as you can filter the list with the inline filter directly above the table. **Hover** to show other menu items. For more information, please see section [Tickets](#) ^[148].



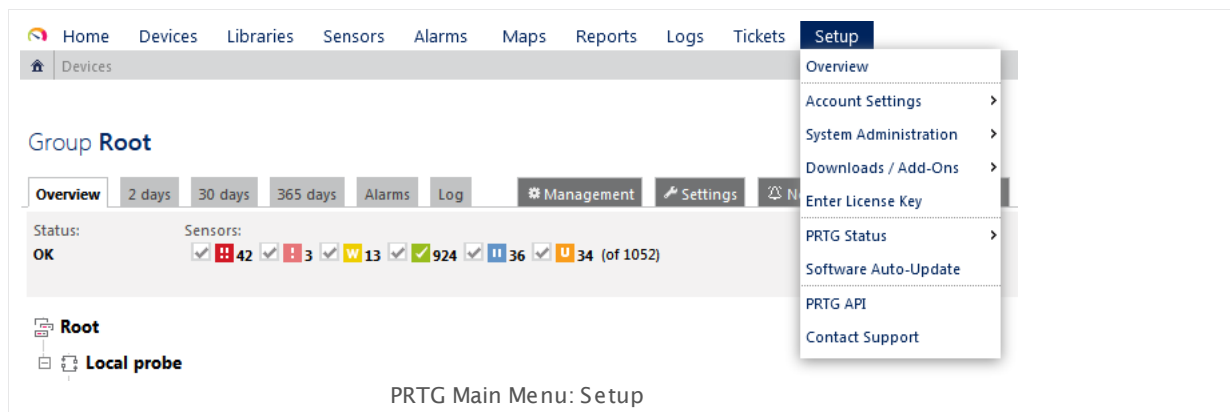
You have several options to display a list of tickets which is filtered to your needs. You can also create a new ticket via the main menu. Available options are:

- **My Tickets**
Click to show all open tickets which are assigned to the current user. Hover to show other menu items for filtering these tickets depending on their status.
- **All Tickets**
Click to show all open tickets of all PRTG users. Hover to show other menu items for filtering these tickets depending on their status.
- **ToDo Tickets**
Click to show all open tickets from the type **ToDo**. Hover to show other menu items for filtering these tickets depending on their status.
- **Open Ticket**
This will open the **New Ticket** dialog. Provide the needed information and confirm by clicking on **Save** to create a **User Ticket**.

For more information about available options, please refer to section [Tickets](#)¹⁴⁸.

Setup

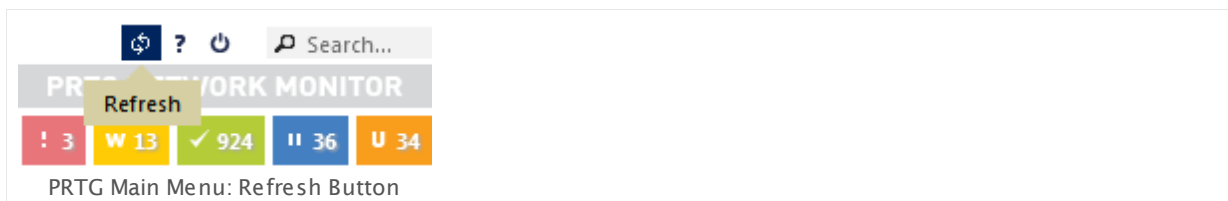
Click to show the setup page. Hover to show other menu items. For more information, please see [Setup](#)¹⁷⁸⁴ section.



- **Overview**
Shows the [setup page](#)¹⁷⁸⁴.
- **Account Settings** ›
Hover to show menu items of the account settings. Choose from:
 - [My Account](#)¹⁷⁸⁶
 - [Notifications](#)¹⁷⁹¹
 - [Schedules](#)¹⁸⁰¹
- **System Administration** ›
Hover to show menu items of the system administration settings. Choose from:
 - [System & Website](#)¹⁸⁰⁶

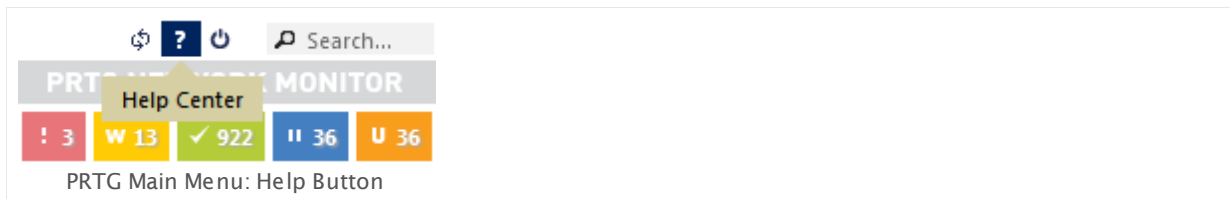
- [Notification Delivery](#)  1815
- [Probes](#)  1821
- [Cluster](#)  1823
- [User Accounts](#)  1824
- [User Groups](#)  1829
- [Administrative Tools](#)  1833
- **Downloads / Add-Ons >**
Shows additional downloads for PRTG. Choose from:
 - [PRTG Enterprise Console](#)  1852
 - [Apps for iOS & Android](#)  1852
 - [Remote Probe Installer](#)  1852
 - [PRTG Add-Ons](#)  1852
 - [PRTG Billing Tool](#)  1853
 - [Chrome Desktop Notifications](#)  1854
- **Enter License Key**
Shows help on how to [Enter a License Key](#)  1857.
- **PRTG Status >**
Hover to show menu items of the PRTG status. Choose from:
 - [System Status](#)  1837
 - [Cluster Status](#)  1850
 - [Activation Status](#)  1851
- **Software Auto-Update**
Shows the [Software Auto-Update](#)  1846 status of your PRTG installation. On this page, you can also download and install available updates.
- **PRTG API**
Shows documentation about the [Application Programming Interface \(API\) Definition](#)  1993 for your installation.
- **Contact Support**
Calls the [Contact Paessler Support / Send Your Feedback to Paessler](#)  1856 page.

Refresh (Arrows Symbol)



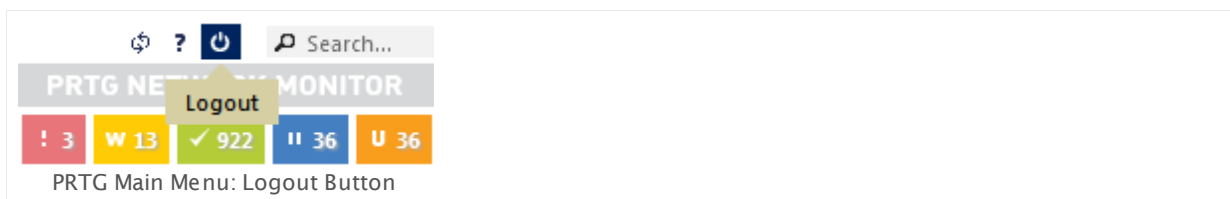
Click this symbol to refresh all elements on the current page to display current data. Unlike the reload function of your browser, this merely refreshes the single page elements, not the whole page. During the refresh process, this symbol flashes.

Help Center (? Symbol)



Shows the help center which supports you if you have any questions regarding your PRTG setup.

Logout (Off Symbol)



Logs out the current user and shows the [login screen](#)^[102].

Search Box

Use the search box to find objects and reports, and other items by name or tag, or to search for help.

Context Menu

Additionally, there are [Context Menus](#)^[162] available for all objects. Right-click on an object to open it.

Part 6

Ajax Web Interface—Device and Sensor Setup

6 Ajax Web Interface—Device and Sensor Setup

The Ajax-based web interface is your access to PRTG. It is used to configure devices and sensors, and to set up notifications, as well as to review monitoring results and to create reports. This web interface is highly interactive, uses Asynchronous Java Script and XML (AJAX) to deliver a powerful and easy-to-use user experience. While the user is [logged in](#)^[102], the data on the screen is permanently refreshed (via Ajax calls) so it always shows the current monitoring results (refresh interval and method can be [set](#)^[102] by the user).

Because the web interface works as a **Single Page Application (SPA)**, you will rarely see a full page refresh to avoid this performance impact due to redundant processing. Only single page elements will be refreshed when necessary. All object setting dialogs are shown as pop-up layers, so you will never lose the current context. This speeds up the user experience appreciably and makes the configuration of objects in PRTG comprehensible.

The following sections introduce device and sensor setup in the Ajax Graphical User Interface (GUI).

Ajax Web Interface—Device and Sensor Setup—Topics

- [Auto-Discovery](#)  190
- [Create Objects Manually](#)  204
- [Manage Device Tree](#)  222
- [Root Group Settings](#)  224
- [Probe Settings](#)  238
- [Group Settings](#)  253
- [Device Settings](#)  272
- [Sensor Settings](#)  290 — [List of Available Sensor Types](#)  291
- [Sensor Channels Settings](#)  1683
- [Sensor Notifications Settings](#)  1690

Other Ajax Web Interface Sections

- [Ajax Web Interface—Basic Procedures](#)  100
- [Ajax Web Interface—Advanced Procedures](#)  1700

Related Topics

- [Enterprise Console](#)  1860
- [Other User Interfaces](#)  1912

6.1 Auto-Discovery

PRTG's auto-discovery function is a great way to automatically create a sophisticated and concise set of sensors for your complete network. It is mainly suitable for LAN discovery since it involves a lot of SNMP and WMI. For video instructions, please see the [More](#)^[203] section below.

For a quick start auto-discovery, please see [TWO—Using the Configuration Guru](#)^[36] section.

How Auto-Discovery Works

PRTG's auto-discovery process has three stages:

- **Step 1**
Scanning a network segment for devices using Ping (for groups only).
- **Step 2**
Assessing the device type for all devices discovered in Step 1 (using SNMP, WMI, and other protocols).
- **Step 3a**
Creating sensor sets that match the discovered device types of step 2. This is done based on built-in device templates with recommended sensors for many device types.

Step 3b (optional)

Creating sensor sets using user created device templates (see [Create Device Template](#)^[1715] section).

The auto-discovery can be used on a group level for a range of IP addresses, or for individual devices which you might have created manually. It can be run just once, on demand via the context menu, or scheduled every hour, day or week. Running the auto-discovery every day or week will automatically create new sensors when new devices are connected to the network. As soon as new devices or sensors are discovered, new [Tickets](#)^[148] are created (which are mailed to the system administrator by default).

Please be aware of the following restrictions of the auto-discovery:

- PRTG can not discover devices that can not be pinged, since Step 1 uses pings. If, for example, a firewall blocks echo requests, a device behind it cannot be discovered.
- You should supply authentication settings for **Windows Systems**, **Linux (SSH/WBEM) Systems**, **VMware/XEN Servers**, and **SNMP Devices** in order to fully exploit the power of this feature. We recommend defining these in the [Root group settings](#)^[224].
- If a device has more than one IP address, it may show up more than once in the discovery results, even though PRTG tries to identify these situations.
- If a device already exists on the same **probe**, the auto-discovery will skip this device and **not** create a duplicate.
- Using frequent auto-discoveries of large network segments can lead to performance issues. We therefore recommend to only schedule regular auto-discoveries where necessary. For detailed information see the [More](#)^[203] section below.

Run Auto-Discovery Now

You can run an auto-discovery at any time for a group or a device. To do so, **right-click** on the respective object and from the context menu, select **Run Auto-Discovery**. PRTG will immediately start searching for new objects which can be added to the device tree. If used for a group, PRTG will add devices and sensors, if found. If used for a device, it will add new sensors, if found.

Note: The auto-discovery will also re-add devices or sensors you have manually deleted. If you do not want this, please create objects [manually](#)^[204] only.

Creating an Auto-Discovery Group

There are several ways to start auto-discovery:

- On the [welcome screen](#)^[108], click on the **Perform Network Auto-Discovery** option,
- or select **Devices | Add Auto-Discovery Group** from the main menu.

To start an automatic detection of devices and sensors in your network an assistant will appear, leading you through two steps. For faster setup, you can select **Add Auto-Discovery Group...** in the [context menu](#)^[162] of a probe or group to which you want to add the new group. This will skip step 1 and lead you directly to step 2.

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Part 6: Ajax Web Interface—Device and Sensor Setup | 1 Auto-Discovery

Add Auto-Discovery Group to Group User Group X home

Define a group name, the IP range for discovery, and credential settings for Windows, Linux, VMware/XEN, and SNMP, if necessary.

[Help: Auto-Discovery](#)

GROUP NAME AND TAGS

Group Name:

Tags:

GROUP TYPE

Sensor Management

- ☒ Automatic device identification (standard, recommended)
- ☐ Automatic device identification (detailed, may create many sensors)
- ☐ Automatic sensor creation using specific device template(s)

Discovery Schedule:

IP Selection Method

- ☒ Class C base IP with start/end (IPv4)
- ☐ List of individual IPs and DNS Names (IPv4)
- ☐ IP and Subnet (IPv4)
- ☐ IP with octet range (IPv4)
- ☐ List of individual IPs and DNS Names (IPv6)
- ☐ Use computers from the active directory (maximum 1000 computers)

IPv4 Base:

IPv4 Range Start:

IPv4 Range End:

Name Resolution

- ☒ Use DNS / WMI / SNMP names (recommended)
- ☐ Use IP addresses

Device Rescan

- ☒ Skip auto-discovery for known devices/IPs (recommended)
- ☐ Perform auto-discovery for known devices/IPs

CREDENTIALS FOR WINDOWS SYSTEMS

☒ inherit from [User Group X home](#) (Domain or Computer Name: paesslergmbh, Userna...)

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

☒ inherit from [User Group X home](#) (Username: <empty>, Login: 0, For WBEM Use Por...)

CREDENTIALS FOR VMWARE/XENSERVER

Add Auto-Discovery Group Dialog

- **Step 1**
Please choose a probe or group you want to add the new group to. Click on **Continue**.
- **Step 2**
Add auto-discovery settings as described below.

Add Auto-Discovery Group Settings

Group Name and Tags	
Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Tags	Enter one or more tags; confirm each tag by hitting the space, comma, or enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive. Tags are automatically inherited ⁸⁹ .

Group Type	
Sensor Management	Select the method for automatic network discovery. Choose between: ▪ Automatic device identification (standard, recommended): Detect mainly based on Ping, SNMP, and WMI. This option should work fine for most installations. ▪ Automatic device identification (detailed, may create many sensors): Detect in a more detailed way and create more sensors. This option uses all standard device templates for auto-discovery. It is suitable for small network segments and whenever you want to monitor the maximum number of sensors available. ▪ Automatic sensor creation using specific device template(s): Manually define the device templates used for auto-discovery. From the list below, select one or more templates.
Device Template(s)	This option is only visible if using specific device templates (last option) is enabled above. Please choose one or more templates by adding a check mark in front of the respective template name. You can also select and deselect all items by using the check box in the table head. These will be used for auto-discovery on the current device. Choose from: ▪ ADSL ▪ Cisco ASA VPN ▪ Cisco Device (Generic) ▪ Dell MDI ▪ DNS Server ▪ Environment Jakarta ▪ Environment Poseidon ▪ Fritzbox ▪ FTP Server ▪ Generic Device (PING only) ▪ Generic Device (SNMP-enabled) ▪ Generic Device (SNMP-enabled, Detailed) ▪ HTTP Web Server ▪ Hyper V Host Server ▪ Linux/UNIX Device (SNMP or SSH enabled) ▪ Mail Server (Generic)

	▪ Mail Server (MS Exchange) ▪ Microsoft Sharepoint 2010 ▪ NAS LenovoEMC ▪ NAS QNAP ▪ NAS Synology ▪ NetApp ▪ NTP Server ▪ Printer (HP) ▪ RDP Server ▪ RMON compatible device ▪ Server (Compaq/HP agents) ▪ Server (Dell) ▪ Sever Cisco UCS ▪ Server IBM ▪ SonicWALL ▪ Switch (Cisco Catalyst) ▪ Switch (Cisco IOS Based) ▪ Switch (HP Procurve) ▪ UNIX/Linux Device ▪ UPS (APC) ▪ Virtuozzo Server ▪ VMware ESX / vCenter Server ▪ Windows (Detailed via WMI) ▪ Windows (via Remote Powershell) ▪ Windows (via WMI) ▪ Windows IIS (via SNMP) ▪ XEN Hosts ▪ XEN Virtual Machines Once the auto-discovery is finished, PRTG will create a new ticket ¹⁴⁸ and list the device templates which were actually used to create new sensors. Templates which were not applied will not be shown in the ticket.
Discovery Schedule	Define when the auto-discovery will be run. Choose between:

	▪ Once: Perform auto-discovery only once. New devices and sensors will be added once. You can run auto-discovery manually any time using an object's context menu^[162]. ▪ Hourly: Perform auto-discovery for new devices and sensors every 60 minutes. Note: Please use this option with caution! Frequently executed auto-discoveries might cause performance issues, especially when large network segments are scanned every hour. ▪ Daily: Perform auto-discovery for new devices and sensors every 24 hours. The first auto-discovery will run immediately, all other discoveries will start on the time defined in the Auto-Discovery Settings section of the System Administration—System and Website^[1805] settings. ▪ Weekly: Perform auto-discovery for new devices and sensors every 7 days. The first auto-discovery will run immediately, all other discoveries will start on the time defined in the Auto-Discovery Settings section of the System Administration—System and Website^[1805] settings.
IP Selection Method	Define how you want to define the IP range for auto-discovery. Choose between: ▪ Class C base IP with start/end (IPv4): Define an IPv4 class C address range. ▪ List of individual IPs and DNS names (IPv4): Enter a list of individual IPv4 addresses or DNS names. ▪ IP and Subnet (IPv4): Enter an IPv4 address and subnet mask. ▪ IP with octet range (IPv4): Enter an IPv4 address range for every IP octet individually. With this, you can define very customizable IP ranges. ▪ List of individual IPs and DNS names (IPv6): Enter a list of individual IPv6 addresses or DNS names. ▪ Use computers from the active directory (maximum 1000 computers): Search in the active directory for computers to perform auto-discovery. Note: Only subnets with up to 65,536 IP addresses can be discovered! If you define a range with a higher number of addresses, discovery will stop before it is completed.
IPv4 Base	This field is only visible if Class C network detection is selected above. Enter a class C network as IP base for the auto-discovery. Enter the first three octets of an IPv4 IP address, for example, 192.168.0

IPv4 Range Start	This field is only visible if Class C network detection is selected above. Enter the IP octet of the class C network specified above from which PRTG will start the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter 1 to discover from 192.168.0.1 .
IPv4 Range End	This field is only visible if Class C network detection is selected above. Enter the IP octet of the class C network specified above at which PRTG will stop the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter 254 to discover up to 192.168.0.254 .
IPv4/DNS Name List IPv6/DNS Name List	This field is only visible if the IP list option is selected above. Enter a list of IP addresses or DNS names which the auto-discovery will scan. Enter each address in a separate line.
IPv4 and Subnet (IPv4)	This field is only visible if the IP and subnet option is selected above. Enter an expression in the format address/subnet , e.g. 192.168.3.0/255.255.255.0 . You can also use the short form like 192.168.3.0/24 in this example. PRTG will scan the complete host range (without network and broadcast address) defined by the IP address and the subnet mask.
IP with Octet Range	This field is only visible if the octet range option is selected above. Enter an expression in the format a1.a2.a3.a4 , where a1 , a2 , a3 , and a4 are each a number between 0-255, or a range with two numbers and a hyphen like 1-127 . All permutations of all ranges are calculated, e.g. 10.0.1-10.1-100 results in 1,000 addresses that PRTG will scan during auto-discovery.
Organizational Unit	This field is only visible if active directory is selected above. Enter an organizational unit (OU) to restrict the active directory search to computers which are part of this OU. Just enter the name of the OU without any other term (i.e., without "OU" in front). If you leave this field empty, there will not be any restriction. If you have sub-OU's, too, please consider the correct syntax in the format Y,OU=X: OUs that are part of another OU have to be listed together with their parent(s). Enter the sub-OU followed by ,OU= and the name of the parent OU. For example, assuming that the organizational unit 'Y' is part of the OU named 'X'. Then the syntax would be Y,OU=X. For three OUs 'X', 'Y' part of 'X', and 'Z' part of 'Y', the syntax would be Z,OU=Y,OU=X. Note that the order is important, sub-OU's have to be listed left of its according parents!
Name Resolution	Define how newly discovered devices will be monitored. This only affects new devices. The setting for existing devices will be kept. Choose between: ▪ Use DNS / WMI / SNMP names (recommended): Monitor newly discovered devices via their DNS, WMI, or SNMP names (if available).

	▪ Use IP addresses: Monitor newly discovered devices via their IP address. We recommend using the default value.
Device Rescan	Define if you want to rescan known devices. Choose between: ▪ Skip auto-discovery for known devices/IPs (recommended): Do not re-scan known devices or IP addresses, but only scan for new devices/IPs when auto-discovering. This can avoid re-creation of manually deleted sensors. PRTG will also avoid adding devices that are already included elsewhere in your configuration, e.g. in other groups. ▪ Perform auto-discovery for known devices/IPs: Re-scan known devices and IP addresses with every auto-discovery. This will re-create manually deleted sensors on existing devices. We recommend using the default value.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

If you have not set credentials yet, set them now before starting the auto-discovery in order to fully exploit the power of this feature!

Credentials for Windows Systems

Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, please enter the computer name here. If you want to use a Windows domain user account (recommended), please enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Please do not leave this field empty.
Username	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
Username	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	Define which authentication method will be used for login. Choose between: ▪ Login via Password: Provide a password for login. Enter below. ▪ Login via Private Key: Provide a private key for authentication. Note: PRTG can only handle keys in OpenSSH format which are not encrypted. You cannot use password protected keys here. In the text field, please paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, please see Monitoring via SSH¹⁹³⁰.
Password	This field is only visible if password login is selected above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	This field is only visible if private key login is selected above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges. Note: If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service in order for the private key change to take effect! For details, please see Monitoring via SSH ¹⁹³⁰ .
For WBEM Use Protocol	Define the protocol that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: ▪ HTTP: Use an unencrypted connection for WBEM. ▪ HTTPS: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: ▪ Set automatically (port 5988 or 5989): Use one of the standard ports, depending on whether unencrypted or encrypted connection is chosen above. ▪ Set manually: Use a custom port. Define below.
WBEM Port	This setting is only visible if manual port selection is enabled above. Enter the WBEM port number.
SSH Port	Define the port number which will be used for SSH connections. Note: By default, this setting is automatically used for all SSH sensors²⁹⁶, unless you define a different port number in the sensor settings.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
SSH Rights Elevation	Define with which rights the command will be executed on the target system. Choose between: ▪ Run the command as the user connecting (default): Use the rights of the user who establishes the SSH connection. ▪ Run the command as another user using 'sudo': Use the rights of another user, for example, the administrator. ▪ Run the command as another user using 'su': Use the rights of another target user.
Target Username	This field is only visible if sudo or su is enabled above. Enter a username to run the specified command as another user than root. If you leave this field empty, the command will be run as root. Ensure that you set the Linux password even you use a public/private key for authentication. This is not necessary if the user is allowed to execute the command without a password.
Password Target User	This field is only visible if su is enabled above. Enter the password for the specified target user.

Credentials for VMware/XenServer	
User	Enter a login name for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: ▪ HTTPS (recommended): Use an SSL-encrypted connection to VMware and XenServers. ▪ HTTP: Use an unencrypted connection to VMware and XenServers.

Credentials for SNMP Devices	
SNMP Version	Select the SNMP version that will be used for device connection. Choose between: ▪ v1: Use the simple standard v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices.

Credentials for SNMP Devices	
	▪ v2c: Use the more advanced v2c protocol for SNMP connections. Data is still transferred as clear-text, but it supports 64-bit counters. ▪ v3: Use the latest v3 protocol for SNMP connections. It provides secure authentication and data encryption. Note for SNMP v3: Due to internal limitations you can only monitor a limited number of sensors per second using SNMP v3. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds you are limited to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased "Interval Delay" or "Open Requests" reading of the probe health sensor, you need to distribute the load over multiple probes. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if SNMP version v1 or v2c are enabled above. Enter the community string of your devices. This is a kind of "clear-text password" used for simple authentication. We recommend using the default value.
Authentication Type	This setting is only visible if SNMP version v3 is enabled above. Choose between: ▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. The chosen type has to match the authentication type of your device. Note: If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field password empty. In this case, SNMP_SEC_LEVEL_NOAUTH will be used and authentication will be deactivated entirely.
User	This setting is only visible if SNMP version v3 is enabled above. Enter a username for secure authentication. This value has to match the username of your device.
Password	This setting is only visible if SNMP version v3 is enabled above. Enter a password for secure authentication. This value has to match the password of your device.
Encryption Type	This setting is only visible if SNMP version v3 is enabled above. Select an encryption type. Choose between: ▪ DES: Use Data Encryption Standard (DES) as encryption algorithm.

Credentials for SNMP Devices	
	▪ AES: Use Advanced Encryption Standard (AES) as encryption algorithm. The chosen type has to match the encryption type of your device.
Data Encryption Key	This setting is only visible if SNMP version v3 is enabled above. Enter an encryption key here. If you provide a key in this field, SNMP data packets will be encrypted using the encryption algorithm selected above, providing increased security. The provided key here has to match the encryption key of your device. Note: If the key entered in this field does not match the key configured in the target SNMP device, you will not get an error message! Please enter a string or leave the field empty.
Context Name	This setting is only visible if SNMP version v3 is enabled above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port used for SNMP communication. We recommend using the default value.
SNMP Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Proxy Settings for HTTP Sensors	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS. Note: This setting is valid for the monitoring only and determines the behavior of sensors. In order to change proxy settings for the core server, please see System Administration—System and Website ¹⁸¹¹ .
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists. ▪ Read: Users in this group can see the object and review its settings. ▪ Write: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. ▪ Full: Users in this group can see the object, as well as review and edit its settings and edit access rights settings. You can create new user groups in the System Administration—User Groups ¹⁸²⁹ settings.

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Auto-Discovery in Progress

While auto-discovery is running you may experience a lower system performance as usual, because PRTG works in the background in order to discover your network. Depending on the IP ranges defined (up to 65,536 addresses) , the discovery may run up to several days before complete. You can review the status of the discovery process as follows:

- In the device tree, behind the group or device name, you will see a percentage value showing the progress of auto-discovery.
- During auto-discovery, the web interface will display a box in the lower right corner, showing the number of active auto-discovery tasks.
- In order to stop a running auto-discovery, right-click the group or device, and select **Pause | For 5 minutes...** from the [context menu](#)¹⁶². Monitoring will be paused for 5 minutes, and auto-discovery tasks will be shut down.

Related Topics

- [Create Device Template](#)¹⁷¹⁵

More

Video Tutorial: There is a video available on the Paessler video tutorials page.

- http://www.paessler.com/support/video_tutorials

Knowledge Base: Why can automatic auto-discoveries evoke performance issues?

- <http://www.paessler.com/knowledgebase/en/topic/14423>

6.2 Create Objects Manually

We recommend using the [auto-discovery](#)^[190] function to create a basic monitoring setup for your network. Afterwards, you can manually create devices that could not be discovered, or [arrange](#)^[1707] detected devices in groups.

The procedure depends on the kind of object you want to add. Choose between:

- [Add a Group](#)^[205]
- [Add a Device](#)^[211]
- [Add a Sensor](#)^[220]

Add a Remote Probe

Please see [Multiple Probes and Remote Probes](#)^[2011] section for more information.

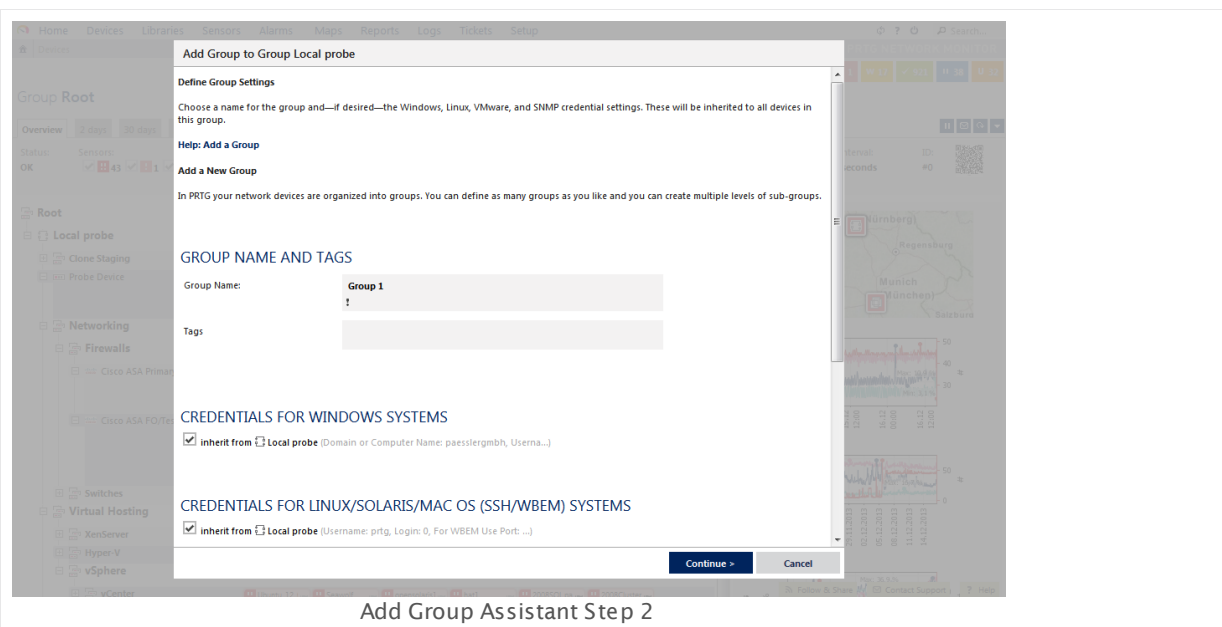
6.2.1 Add a Group

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

In order to add a group manually, select **Devices | Add Group** from the main menu. An assistant will appear, leading you through two steps. For faster setup, you can select **Add Group...** in the [context menu](#)¹⁶² of a probe or group to which you want to add the new group. This will skip step 1 and lead you directly to step 2.

■ Step 1

Please choose a probe or group you want to add the new group to. Click on **Continue**.



■ Step 2

Add group settings as described below.

Add Group Settings

Group Name and Tags

Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Tags	Enter one or more tags; confirm each tag by hitting the space, comma, or enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive. Tags are automatically inherited ¹⁶³ .

Credentials for Windows Systems	
Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, please enter the computer name here. If you want to use a Windows domain user account (recommended), please enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Please do not leave this field empty.
Username	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
Username	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	Define which authentication method will be used for login. Choose between: ▪ Login via Password: Provide a password for login. Enter below. ▪ Login via Private Key: Provide a private key for authentication. Note: PRTG can only handle keys in OpenSSH format which are not encrypted. You cannot use password protected keys here. In the text field, please paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, please see Monitoring via SSH.
Password	This field is only visible if password login is selected above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	This field is only visible if private key login is selected above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges. Note: If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service in order for the private key change to take effect! For details, please see Monitoring via SSH .
For WBEM Use Protocol	Define the protocol that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: ▪ HTTP: Use an unencrypted connection for WBEM.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
	▪ HTTPS: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: ▪ Set automatically (port 5988 or 5989): Use one of the standard ports, depending on whether unencrypted or encrypted connection is chosen above. ▪ Set manually: Use a custom port. Define below.
WBEM Port	This setting is only visible if manual port selection is enabled above. Enter the WBEM port number.
SSH Port	Define the port number which will be used for SSH connections. Note: By default, this setting is automatically used for all SSH sensors, unless you define a different port number in the sensor settings.
SSH Rights Elevation	Define with which rights the command will be executed on the target system. Choose between: ▪ Run the command as the user connecting (default): Use the rights of the user who establishes the SSH connection. ▪ Run the command as another user using 'sudo': Use the rights of another user, for example, the administrator. ▪ Run the command as another user using 'su': Use the rights of another target user.
Target Username	This field is only visible if sudo or su is enabled above. Enter a username to run the specified command as another user than root. If you leave this field empty, the command will be run as root. Ensure that you set the Linux password even you use a public/private key for authentication. This is not necessary if the user is allowed to execute the command without a password.
Password Target User	This field is only visible if su is enabled above. Enter the password for the specified target user.
Credentials for VMware/XenServer	
User	Enter a login name for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.

Credentials for VMware/XenServer	
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: ▪ HTTPS (recommended): Use an SSL-encrypted connection to VMware and XenServers. ▪ HTTP: Use an unencrypted connection to VMware and XenServers.
Credentials for SNMP Devices	
SNMP Version	Select the SNMP version that will be used for device connection. Choose between: ▪ v1: Use the simple standard v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. ▪ v2c: Use the more advanced v2c protocol for SNMP connections. Data is still transferred as clear-text, but it supports 64-bit counters. ▪ v3: Use the latest v3 protocol for SNMP connections. It provides secure authentication and data encryption. Note for SNMP v3: Due to internal limitations you can only monitor a limited number of sensors per second using SNMP v3. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds you are limited to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased "Interval Delay" or "Open Requests" reading of the probe health sensor, you need to distribute the load over multiple probes. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if SNMP version v1 or v2c are enabled above. Enter the community string of your devices. This is a kind of "clear-text password" used for simple authentication. We recommend using the default value.
Authentication Type	This setting is only visible if SNMP version v3 is enabled above. Choose between: ▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. The chosen type has to match the authentication type of your device.

Credentials for SNMP Devices	
	Note: If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field password empty. In this case, SNMP_SEC_LEVEL_NOAUTH will be used and authentication will be deactivated entirely.
User	This setting is only visible if SNMP version v3 is enabled above. Enter a username for secure authentication. This value has to match the username of your device.
Password	This setting is only visible if SNMP version v3 is enabled above. Enter a password for secure authentication. This value has to match the password of your device.
Encryption Type	This setting is only visible if SNMP version v3 is enabled above. Select an encryption type. Choose between: ▪ DES: Use Data Encryption Standard (DES) as encryption algorithm. ▪ AES: Use Advanced Encryption Standard (AES) as encryption algorithm. The chosen type has to match the encryption type of your device.
Data Encryption Key	This setting is only visible if SNMP version v3 is enabled above. Enter an encryption key here. If you provide a key in this field, SNMP data packets will be encrypted using the encryption algorithm selected above, providing increased security. The provided key here has to match the encryption key of your device. Note: If the key entered in this field does not match the key configured in the target SNMP device, you will not get an error message! Please enter a string or leave the field empty.
Context Name	This setting is only visible if SNMP version v3 is enabled above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port used for SNMP communication. We recommend using the default value.
SNMP Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists. ▪ Read: Users in this group can see the object and review its settings. ▪ Write: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. ▪ Full: Users in this group can see the object, as well as review and edit its settings and edit access rights settings. You can create new user groups in the System Administration—User Groups settings.

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

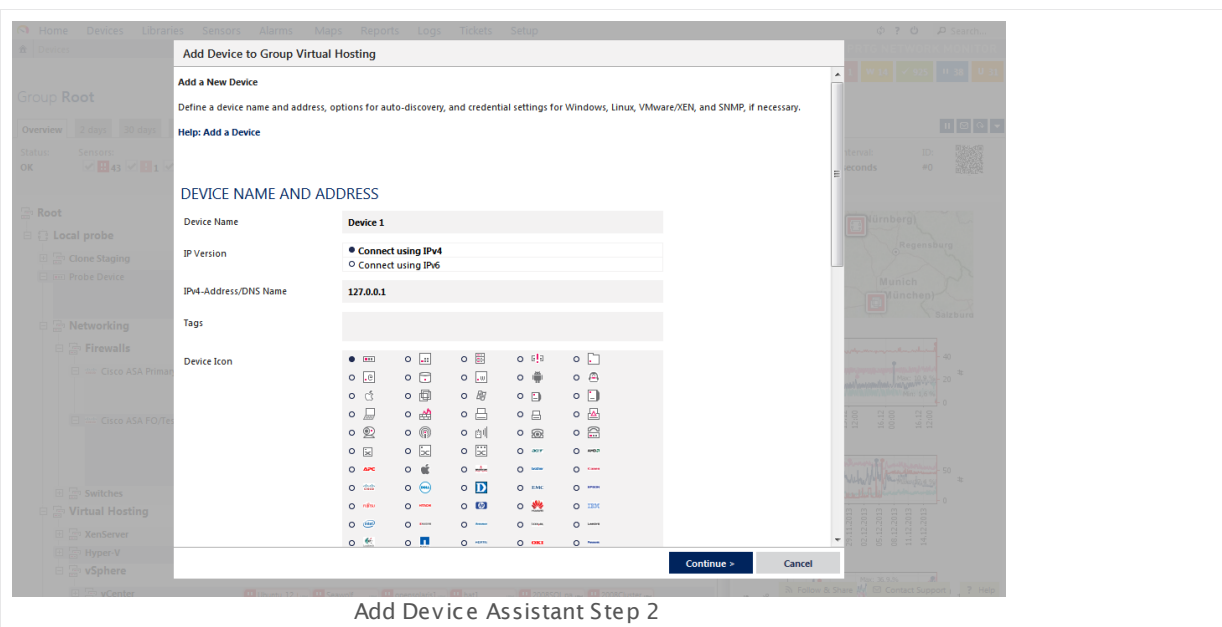
6.2.2 Add a Device

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

To manually add a device, select **Devices | Add Device** from the main menu. An assistant will appear, leading you through two steps. For faster setup, you can select **Add Device...** in the [context menu](#)¹⁶² of a group to which you want to add the new device. This will skip step 1 and lead you directly to step 2.

■ Step 1

Please choose a group you want to add the new device to. Click on **Continue**.



■ Step 2

Add device settings as described below.

Add Device Settings

Device Name and Address

Device Name	Enter a meaningful name to identify the device. The name will be shown by default in the device tree and in all alarms.
IP Version	Define which IP protocol PRTG will use to connect to this device. The setting is valid for all sensors created on this device. Choose between: ■ Connect using IPv4: Use IP version 4 for all requests to this device.

Part 6: Ajax Web Interface—Device and Sensor Setup | 2 Create Objects Manually
2 Add a Device

Device Name and Address	
	▪ Connect using IPv6: Use IP version 6 for all requests to this device.
IP Address/DNS Name	Enter the IP address (either v4 or v6, depending on your selection above) or DNS name for the device. Most sensors created on this device will inherit this setting and they will try to connect to this address for monitoring. Note: There are some sensor types that still have their own setting for IP address/DNS name. Those sensors will use their own settings.
Tags	Enter one or more tags; confirm each tag by hitting space, comma, or enter key. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. Tags are automatically inherited .
Device Icon	Choose a device icon from the list. It will be shown in the device tree.

Device Type	
Sensor Management	Select which type of auto-discovery you would like to perform for this device. Choose between: ▪ Manual (no auto-discovery): Do not auto-discover any sensors, but only add sensors manually. ▪ Automatic device identification (standard, recommended): Use a small set of auto-discovery templates. This will scan your LAN and usually create a view standard sensors on your device. ▪ Automatic device identification (detailed, may create many sensors): Use an extended set of auto-discovery templates. This will scan your LAN and usually create many sensors on your device. ▪ Automatic sensor creation using specific device templates: Use specific auto-discovery templates only. Please select templates below. This will scan your LAN and add sensors defined in the template.
Discovery Schedule	This option is only visible if one of the auto-discovery options is selected above. Define when the auto-discovery will be run. Choose between: ▪ Once: Perform auto-discovery only once. For existing devices, this will initiate a one-time sensor update for the current device. ▪ Hourly: Perform auto-discovery for new sensors every hour. ▪ Daily: Perform auto-discovery for new sensors every day.

Device Type	
	▪ Weekly: Perform auto-discovery for new sensors every week.
Device Template(s)	This option is only visible if using specific device templates (last option) is enabled above. Please choose one or more templates by adding a check mark in front of the respective template name. You can also select and deselect all items by using the check box in the table head. These will be used for auto-discovery on the current device. Choose from: ▪ ADSL ▪ Cisco ASA VPN ▪ Cisco Device (Generic) ▪ Dell MDI ▪ DNS Server ▪ Environment Jakarta ▪ Environment Poseidon ▪ Fritzbox ▪ FTP Server ▪ Generic Device (PING only) ▪ Generic Device (SNMP-enabled) ▪ Generic Device (SNMP-enabled, Detailed) ▪ HTTP Web Server ▪ Hyper V Host Server ▪ Linux/UNIX Device (SNMP or SSH enabled) ▪ Mail Server (Generic) ▪ Mail Server (MS Exchange) ▪ Microsoft Sharepoint 2010 ▪ NAS LenovoEMC ▪ NAS QNAP ▪ NAS Synology ▪ NetApp ▪ NTP Server ▪ Printer (HP) ▪ RDP Server ▪ RMON compatible device

Device Type	
	▪ Server (Compaq/HP agent s) ▪ Server (Dell) ▪ Sever Cisco UCS ▪ Server IBM ▪ SonicWALL ▪ Switch (Cisco Catalyst) ▪ Switch (Cisco IOS Based) ▪ Switch (HP Procurve) ▪ UNIX/Linux Device ▪ UPS (APC) ▪ Virtuozzo Server ▪ VMware ESX / vCenter Server ▪ Windows (Detailed via WMI) ▪ Windows (via Remote Powershell) ▪ Windows (via WMI) ▪ Windows IIS (via SNMP) ▪ XEN Host s ▪ XEN Virtual Machines Once the auto-discovery is finished, PRTG will create a new ticket [146] and list the device templates which were actually used to create new sensors. Templates which were not applied will not be shown in the ticket.

Credentials for Windows Systems	
Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, please enter the computer name here. If you want to use a Windows domain user account (recommended), please enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Please do not leave this field empty.

Credentials for Windows Systems	
Username	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
Username	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	Define which authentication method will be used for login. Choose between: ▪ Login via Password: Provide a password for login. Enter below. ▪ Login via Private Key: Provide a private key for authentication. Note: PRTG can only handle keys in OpenSSH format which are not encrypted. You cannot use password protected keys here. In the text field, please paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, please see Monitoring via SSH.
Password	This field is only visible if password login is selected above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	This field is only visible if private key login is selected above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges. Note: If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service in order for the private key change to take effect! For details, please see Monitoring via SSH .
For WBEM Use Protocol	Define the protocol that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: ▪ HTTP: Use an unencrypted connection for WBEM. ▪ HTTPS: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: ▪ Set automatically (port 5988 or 5989): Use one of the standard ports, depending on whether unencrypted or encrypted connection is chosen above.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
	▪ Set manually: Use a custom port. Define below.
WBEM Port	This setting is only visible if manual port selection is enabled above. Enter the WBEM port number.
SSH Port	Define the port number which will be used for SSH connections. Note: By default, this setting is automatically used for all SSH sensors^[296], unless you define a different port number in the sensor settings.
SSH Rights Elevation	Define with which rights the command will be executed on the target system. Choose between: ▪ Run the command as the user connecting (default): Use the rights of the user who establishes the SSH connection. ▪ Run the command as another user using 'sudo': Use the rights of another user, for example, the administrator. ▪ Run the command as another user using 'su': Use the rights of another target user.
Target Username	This field is only visible if sudo or su is enabled above. Enter a username to run the specified command as another user than root. If you leave this field empty, the command will be run as root. Ensure that you set the Linux password even you use a public/private key for authentication. This is not necessary if the user is allowed to execute the command without a password.
Password Target User	This field is only visible if su is enabled above. Enter the password for the specified target user.
Credentials for VMware/XenServer	
User	Enter a login name for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: ▪ HTTPS (recommended): Use an SSL-encrypted connection to VMware and XenServers. ▪ HTTP: Use an unencrypted connection to VMware and XenServers.

Credentials for SNMP Devices	
SNMP Version	Select the SNMP version that will be used for device connection. Choose between: ▪ v1: Use the simple standard v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. ▪ v2c: Use the more advanced v2c protocol for SNMP connections. Data is still transferred as clear-text, but it supports 64-bit counters. ▪ v3: Use the latest v3 protocol for SNMP connections. It provides secure authentication and data encryption. Note for SNMP v3: Due to internal limitations you can only monitor a limited number of sensors per second using SNMP v3. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds you are limited to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased "Interval Delay" or "Open Requests" reading of the probe health sensor, you need to distribute the load over multiple probes. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if SNMP version v1 or v2c are enabled above. Enter the community string of your devices. This is a kind of "clear-text password" used for simple authentication. We recommend using the default value.
Authentication Type	This setting is only visible if SNMP version v3 is enabled above. Choose between: ▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. The chosen type has to match the authentication type of your device. Note: If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field password empty. In this case, SNMP_SEC_LEVEL_NOAUTH will be used and authentication will be deactivated entirely.
User	This setting is only visible if SNMP version v3 is enabled above. Enter a username for secure authentication. This value has to match the username of your device.
Password	This setting is only visible if SNMP version v3 is enabled above. Enter a password for secure authentication. This value has to match the password of your device.

Credentials for SNMP Devices	
Encryption Type	This setting is only visible if SNMP version v3 is enabled above. Select an encryption type. Choose between: ▪ DES: Use Data Encryption Standard (DES) as encryption algorithm. ▪ AES: Use Advanced Encryption Standard (AES) as encryption algorithm. The chosen type has to match the encryption type of your device.
Data Encryption Key	This setting is only visible if SNMP version v3 is enabled above. Enter an encryption key here. If you provide a key in this field, SNMP data packets will be encrypted using the encryption algorithm selected above, providing increased security. The provided key here has to match the encryption key of your device. Note: If the key entered in this field does not match the key configured in the target SNMP device, you will not get an error message! Please enter a string or leave the field empty.
Context Name	This setting is only visible if SNMP version v3 is enabled above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port used for SNMP communication. We recommend using the default value.
SNMP Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Part 6: Ajax Web Interface—Device and Sensor Setup | 2 Create Objects Manually

3 Add a Sensor

6.2.3 Add a Sensor

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

In order to add a sensor manually, select **Sensors | Add Sensor** from the main menu. An assistant will appear, leading you through two steps. For faster setup, you can select **Add Sensor...** in the [context menu](#)¹⁶² of a device to which you want to add the new sensor. This will skip step 1 and lead you directly to step 2.

▪ Step 1

Please select **Add sensor to an existing device** and choose a device you want to add the new sensor to. Click on **Continue**.

Add Sensor to Device Cisco ASA Primary [10.0.0.1] (Step 1 of 2)

SEARCH

209 Matching Sensor Types

MONITOR WHAT?	TARGET SYSTEM TYPE?	TECHNOLOGY USED?
- Availability/Uptime - Bandwidth/Traffic - Speed/Performance - CPU Usage - Disk Usage - Memory Usage - Hardware Parameters - Network Infrastructure - Custom Sensors	- Windows - Linux/MacOS - Virtualization OS - File Server - Email Server - SQL Server	- Ping - SNMP - WMI - Performance Counters - HTTP - SSH - Packet Sniffing - NetFlow, sFlow, jFlow - Powershell - Push Message Receiver

MOST USED SENSOR TYPES

HTTP Monitors a web server using HTTP (Hypertext Transfer Protocol) Add This	Ping Monitors connectivity using Ping Add This	SNMP Custom Monitors a numerical value returned by a specific OID using SNMP Add This	SNMP Traffic Monitors bandwidth and traffic on servers, PCs, switches, etc. using SNMP Add This
VMware Virtual Machine (SOAP) Monitors virtual machines on a VMware host server version 4.0 or later using SOAP Add This	Windows CPU Load Monitors CPU load using performance counters or WMI Add This	Windows Network Card Monitors bandwidth usage and traffic of a network interface using performance counters or WMI Add This	WMI Exchange Server Monitors a Microsoft Exchange Server using WMI Add This
WMI Service Monitors a service using WMI Add This	WMI Vital System Data (V2) Monitors vital system parameters using WMI (CPU, memory, disk, network) Add This		

MATCHING SENSOR TYPES

Active Directory Replication Errors Checks Windows domain controllers for replication errors. Add This	ADO SQL Monitors a database using an ADO connection Add This	Amazon CloudWatch Monitors performance of an Amazon Web Services instance Add This	AVM FRITZ!Box WAN Interface Monitors the internet connection traffic of an AVM Fritz!Box Add This
Cisco IP SLA Monitors VoIP network parameters using IP SLA from Cisco (uses SNMP) Add This	Citrix XenServer Host Monitors a Citrix XenServer host version 5.0 or later Add This	Citrix XenServer Virtual Machine Monitors a virtual machine on a Citrix XenServer version 5.0 or later Add This	Dell PowerVault MDI This sensor shows stats for one drive on your Dell PowerVault MD3000 Add This
DNS Monitors a DNS server (Domain Name Service) Add This	Enterprise Virtual Array BETA Monitors the status of the different modules. Add This	Event Log (Windows API) Monitors Event Log entries using Windows API Add This	Exchange Backup (Powershell) Monitors backups of Add This

Follow & Share | Contact Support | Help

Add Sensor Assistant Step 1

- **Step 2**

The **Add Sensor** assistant is shown (see screenshot above). Select a sensor you want to add and enter the needed settings. You can filter the listed sensors by type, by target system, and by the used technology. You can choose one aspect per filter. Alternatively or additionally, you can use the live search by typing in a key term (or a substring) in the **Search** box. PRTG also suggests sensor types to create on the selected device; this recommendation is automatically calculated based on the current user's sensor usage and shows the ten commonest sensor types by default (if enough sensor types are already in use). The chosen filter also applies to the recommendation. See section **More** if you want to adjust the number of most used sensor types which are shown here or to hide this option completely.

For more information about a sensor type, please see the manual section of the respective sensor. See [List of Available Sensor Types](#)^[291] section to find detailed information about every sensor type.

More

Knowledge Base: How can I change the number of entries in most used sensor types?

- <http://www.paessler.com/knowledgebase/en/topic/59788>

6.3 Manage Device Tree

While viewing the device tree (or parts of it), click on the **Management** tab to enter a different tree view which shows your devices and sensors in a less colorful way. While in this view, you can move monitoring objects using **drag&drop** in your browser window. You can also view and edit object settings by selecting it. Changes take effect immediately. When done, leave the **Management** tab.

In order to arrange objects in the tree, you have the following options:

Drag&Drop a Sensor

You can either move a sensor within the same device, or clone a sensor to another device.

- Within the same device, drag any sensor and drop it to the place where you want to have it. A shade will show the future position. When dropping, the sensor will be **moved** to this position and existing sensors will be lined up after it. This is a very easy way to reposition your sensors.
- Drag any sensor from one device and drop it on another to **clone** a sensor. This will create the same sensor type, with the same settings, on the new device, while maintaining the original sensor. A shade will show the future position. **Note:** Cloned sensors are put to **Pause** status initially to give you the chance to change any settings before monitoring begins. Please check the [settings](#)^[141] and [resume](#)^[161] monitoring.

Note: You cannot clone 'fixed' objects, such as the root group or a probe device. You cannot clone the sensor types [QoS \(Quality of Service\) One Way Sensor](#)^[801] and [QoS \(Quality of Service\) Round Trip Sensor](#)^[807].

Note: In order to **clone** entire groups or devices, please use the [Clone Object](#)^[1708] functionality accessible via the objects' [Context Menu](#)^[162].

Drag&Drop a Group or Device

You can change a group's or device's position by using drag&drop.

- Within the same probe or group, drag any group or device and move it up or down in the device tree. A small red arrow will appear, showing the future position. When dropping, the group or device will be moved to this position and existing probes, groups, and devices will be lined up underneath. This is a very easy way to reposition your groups or devices.
- Drag any group or device from one probe or group and drop it on another probe or group. A small red arrow will appear, showing the future position. When dropping, the group or device will be moved to the new probe or group. Existing groups and devices will be lined up underneath. This is a very easy way to change the probe a group or device is part of, or to add groups or devices to other groups.

Note: The **Local Probe** and Remote Probes cannot be moved.

Multi-Edit Object Properties

You can use Multi-Edit for object settings:

- Hold down the **Ctrl** key and select multiple groups, devices, or sensors (one of a kind).
- In the appearing dialog, select the settings you would like to edit, change the according values and click on **Save**. The changes will be applied to all selected objects.

The dialog is the same as described in the [Multi-Edit](#)¹⁷¹² (Edit Settings) section.

Related Topics

For other ways to arrange objects, please see

- [Arrange Objects](#)¹⁷⁰⁷
- [Create Device Template](#)¹⁷¹⁵
- [Clone Object](#)¹⁷⁰⁸

6.4 Root Group Settings

On the **Root** group's overview page, click on the **Settings** tab to change settings.

The Root Group is Special

The **Root** group is the highest instance in the object hierarchy of your PRTG setup and parent to all other objects. Therefore, all objects inherit settings from the **Root** group. If you define important settings on this high level, work will be easier later on. So, before you create your own sensors, it is a good idea to review the **Root** group's settings to ensure they suit your network. There are already reasonable presets made with installation.

Note: If necessary, you can override every setting for every single child object later. To do so, simply disable the respective **Inherit** option of an object.

Root Group Settings

The following settings are available in the **Settings** tab. As you may not need all of these, just regard those settings you really need, ignoring the others. All settings you define here can easily be inherited to all other objects in your setup.

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Basic Group Settings

Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Status	Define if monitoring for this group is started or paused. Choose between: ▪ Started: Monitor this group. ▪ Paused: Pause monitoring for this group. All sensors on all devices in this group will be paused until this setting is changed again.

Location	
Location (for geo maps)	When using geo maps using Google's API^[1710] please enter a location in the first line. Objects will then be displayed on a geographical map with a flag, showing the current status using a color code similar to the sensor status icons^[121] (green - yellow - orange - red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, PRTG will parse latitude and longitude automatically; for example: 49.452778 11.077778 or enter 49.452778 any 11.077778 text A minus sign (-) in the first line will hide an object from geo maps. In this case you can enter location information in line two and following. You can define a specific label for each location: enter a string denoting the label in the first line and provide geo coordinates in the second line. This object will be displayed then with the label in PRTG's geo map.

Credentials for Windows Systems	
Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, please enter the computer name here. If you want to use a Windows domain user account (recommended), please enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Please do not leave this field empty.
Username	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
Username	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	Define which authentication method will be used for login. Choose between: ▪ Login via Password: Provide a password for login. Enter below.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
	▪ Login via Private Key: Provide a private key for authentication. Note: PRTG can only handle keys in OpenSSH format which are not encrypted. You cannot use password protected keys here. In the text field, please paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, please see Monitoring via SSH.
Password	This field is only visible if password login is selected above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	This field is only visible if private key login is selected above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges. Note: If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service in order for the private key change to take effect! For details, please see Monitoring via SSH .
For WBEM Use Protocol	Define the protocol that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: ▪ HTTP: Use an unencrypted connection for WBEM. ▪ HTTPS: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: ▪ Set automatically (port 5988 or 5989): Use one of the standard ports, depending on whether unencrypted or encrypted connection is chosen above. ▪ Set manually: Use a custom port. Define below.
WBEM Port	This setting is only visible if manual port selection is enabled above. Enter the WBEM port number.
SSH Port	Define the port number which will be used for SSH connections. Note: By default, this setting is automatically used for all SSH sensors , unless you define a different port number in the sensor settings.
SSH Rights Elevation	Define with which rights the command will be executed on the target system. Choose between: ▪ Run the command as the user connecting (default): Use the rights of the user who establishes the SSH connection.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
	▪ Run the command as another user using 'sudo': Use the rights of another user, for example, the administrator. ▪ Run the command as another user using 'su': Use the rights of another target user.
Target Username	This field is only visible if sudo or su is enabled above. Enter a username to run the specified command as another user than root. If you leave this field empty, the command will be run as root. Ensure that you set the Linux password even you use a public/private key for authentication. This is not necessary if the user is allowed to execute the command without a password.
Password Target User	This field is only visible if su is enabled above. Enter the password for the specified target user.

Credentials for VMware/XenServer	
User	Enter a login name for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: ▪ HTTPS (recommended): Use an SSL-encrypted connection to VMware and XenServers. ▪ HTTP: Use an unencrypted connection to VMware and XenServers.

Credentials for SNMP Devices	
SNMP Version	Select the SNMP version that will be used for device connection. Choose between: ▪ v1: Use the simple standard v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. ▪ v2c: Use the more advanced v2c protocol for SNMP connections. Data is still transferred as clear-text, but it supports 64-bit counters. ▪ v3: Use the latest v3 protocol for SNMP connections. It provides secure authentication and data encryption.

Credentials for SNMP Devices	
	Note for SNMP v3: Due to internal limitations you can only monitor a limited number of sensors per second using SNMP v3. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds you are limited to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased "Interval Delay" or "Open Requests" reading of the probe health sensor, you need to distribute the load over multiple probes. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if SNMP version v1 or v2c are enabled above. Enter the community string of your devices. This is a kind of "clear-text password" used for simple authentication. We recommend using the default value.
Authentication Type	This setting is only visible if SNMP version v3 is enabled above. Choose between: ▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. The chosen type has to match the authentication type of your device. Note: If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field password empty. In this case, SNMP_SEC_LEVEL_NOAUTH will be used and authentication will be deactivated entirely.
User	This setting is only visible if SNMP version v3 is enabled above. Enter a username for secure authentication. This value has to match the username of your device.
Password	This setting is only visible if SNMP version v3 is enabled above. Enter a password for secure authentication. This value has to match the password of your device.
Encryption Type	This setting is only visible if SNMP version v3 is enabled above. Select an encryption type. Choose between: ▪ DES: Use Data Encryption Standard (DES) as encryption algorithm. ▪ AES: Use Advanced Encryption Standard (AES) as encryption algorithm. The chosen type has to match the encryption type of your device.

Credentials for SNMP Devices	
Data Encryption Key	This setting is only visible if SNMP version v3 is enabled above. Enter an encryption key here. If you provide a key in this field, SNMP data packets will be encrypted using the encryption algorithm selected above, providing increased security. The provided key here has to match the encryption key of your device. Note: If the key entered in this field does not match the key configured in the target SNMP device, you will not get an error message! Please enter a string or leave the field empty.
Context Name	This setting is only visible if SNMP version v3 is enabled above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port used for SNMP communication. We recommend using the default value.
SNMP Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Windows Compatibility Options	
When experiencing problems while monitoring via Windows sensors, you can set some compatibility options for trouble shooting.	
Preferred Data Source	Define the method Windows sensors will use to query data. This setting is valid only for hybrid sensors offering performance counter and Windows Management Instrumentation (WMI) technology. The setting will be ignored for all other sensors! Choose between: ▪ Performance Counters and fallback to WMI (recommended): Try to query data via performance counters. If this is not possible, establish a connection via WMI. This is the recommended setting to best balance resource usage and functionality. ▪ Performance Counters only: Query data via performance counters only. If this is not possible, a sensor will return no data. ▪ WMI only: Query data via WMI only. If this is not possible, a sensor will return no data.
Timeout Method	Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between:

Windows Compatibility Options	
	▪ Use 1.5x scanning interval (recommended): Use a default of one and a half times the scanning interval set for the sensor (see below in this settings). ▪ Set manually: Enter a timeout value manually. We recommend using the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.
Timeout Value (Sec.)	This field is only visible if the manual timeout method is selected above. Specify the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value.

SNMP Compatibility Options	
When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for trouble shooting.	
SNMP Delay (ms)	Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend using the default value. If you experience SNMP connection failures, please increase it. You can define a delay between 0 and 100 , higher delays are not supported and will be discarded.
Failed Requests	Define if an SNMP sensor will try again after a request fails. ▪ Retry (recommended): Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures. ▪ Do not retry: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be set to error status earlier.
Overflow Values	Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks. ▪ Ignore overflow values (recommended): Ignore overflow values and do not include them in the monitoring data. ▪ Handle overflow values as valid results: Regard all overflow values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.
Zero Values	Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks.

SNMP Compatibility Options	
	▪ Ignore zero values for delta sensors (recommended): Ignore zero values and do not include them in the monitoring data. ▪ Handle zero values as valid results for delta sensors: Regard all zero values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.
32-bit/64-bit Counters	Define which kind of traffic counters PRTG will search for on a device. ▪ Use 64-bit counters if available (recommended): The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices. ▪ Use 32-bit counters only: The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices. We recommend using the default value. If you experience problems, change this option.
Request Mode	Define which kind of request method PRTG uses for SNMP sensors. ▪ Use multi get (recommended): Bundle multiple SNMP requests into one request. ▪ Use single get: Use one request for each SNMP value. This can increase compatibility with older devices. We recommend using the default value. If you experience problems, change this option.
Port Name Template	Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device/OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, [port] [ifalias] is set as port name template, which will create a name such as (001) Ethernet1, for example. You can use any field names available at a certain OID of your device, among which are: ▪ [port]: The port number of the monitored interface. ▪ [ifalias]: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling. ▪ [ifname]: The textual name of the monitored interface as assigned by the local device.

SNMP Compatibility Options	
	▪ [ifindex]: A unique value, greater than zero, for the monitored interface. ▪ [ifdescr]: A textual string containing information about the monitored device or interface, for example, manufacturer, product name, version. ▪ [ifspeed]: An estimate of the monitored interface's current bandwidth (KBit/s). Combine them as you like to obtain suitable sensor names. See the More section below for more information about SNMP sensor names.
Port Name Update	Define how PRTG will react if you change port names in your physical device (e.g. a switch or router). Choose between: ▪ Keep port names (use this if you edit the names in PRTG): Do not automatically adjust sensor names. This is the best option if you want to change names in PRTG manually. ▪ Automatic sensor name update if name changes in device: If PRTG detects changes of port names in your physical device, it will try to automatically adjust sensor names accordingly. For detailed information please see More section below.
Port Identification	Define which field will be used for SNMP interface identification. Choose between: ▪ Automatic (recommended): Tries the ifAlias field first to identify an SNMP interface and then ifDescr. Note: ifName will not be tried automatically. ▪ Use ifAlias: For most devices ifAlias is the best field to get unique interface names. ▪ Use ifDescr: Use this option if the port order of your device changes after a reboot, and there is no ifAlias field available. For example, this is the best option for Cisco ASA devices. Note: When using this option it is important that your device returns unique interface names in the ifDescr field. ▪ Use ifName: You can also use this option if there is no unique ifAlias available. Note: When using this option it is important that your device returns unique interface names in the ifName field. ▪ No Port Update: Use this option to disable automatic port identification.
Start Port	For SNMP Traffic sensors, define at which port number PRTG will start to create sensors. Use 0 for automatic. We recommend using the default value.

SNMP Compatibility Options	
End Port	For SNMP Traffic sensors, define at which port number PRTG will stop to create sensors. Use 0 for automatic. We recommend using the default value.
SNMP Debug Log	Define if you want to create an SNMP log file for debugging purposes. This is only recommended for debugging low level SNMP issues. Choose between: ▪ No log (recommended): No SNMP debug log file will be created. ▪ Enable debug log: An SNMP log file is written to the Logs (Debug) directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage¹⁸⁰⁶ section.

Proxy Settings for HTTP Sensors	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS. Note: This setting is valid for the monitoring only and determines the behavior of sensors. In order to change proxy settings for the core server, please see System Administration—System and Website ¹⁸¹¹ .
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings ^[1791] . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency settings are available only in [Probe Settings](#)^[238], [Group Settings](#)^[253], [Device Settings](#)^[272], and [Sensor Settings](#)^[290].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Automatic Monitoring Data Analysis	
Unusual Detection	Define if unusual detection is enabled for sensors. You can configure the behavior of unusual detection (or disable it completely) in the system settings ¹⁸⁰⁸. ▪ Enabled: Enable unusual detection for this group. Sensors in this group will turn to orange color if unusual activity is detected. ▪ Disabled: Disable unusual detection for this group. Unusual values will be ignored for sensors in this group; they will not show an unusual sensor status.
Similar Sensors Detection	Define if similar sensors detection is enabled for sensors. You can configure the depth of analysis of similar sensors detection (or disable it completely) in the system settings ¹⁸⁰⁹. ▪ Enabled: Enable similar sensors detection for this group. Sensors in this group will be considered during similarity analysis. ▪ Disabled: Disable similar detection for this group. Sensors in this group will not be taken into account during similarity analysis.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to you needs. In an object's detail page, click on the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, please see [Sensor Notifications Settings](#) ¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#) ¹⁴¹ section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- <http://www.paessler.com/knowledgebase/en/topic/313>

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?

- <http://www.paessler.com/knowledgebase/en/topic/7313>

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?

- <http://www.paessler.com/knowledgebase/en/topic/7363>

Knowledge Base: Automatically update port name and number for SNMP Traffic sensors when the device changes them

- <http://www.paessler.com/knowledgebase/en/topic/25893>

6.5 Probe Settings

On a probe's overview page, click on the **Settings** tab to change settings.

Add Remote Probe

You can add additional remote probes to your setup to extend your monitoring to networks that are not directly reachable by your PRTG core installation or cluster.

See [Add Remote Probe](#)^[2011] section for more details.

Probe Settings

The following settings are available in the **Settings** tab of every probe. As you may not need all of these for every probe, just regard those settings you really need, ignoring the others.

We recommend defining as many settings as possible in the [Root](#)^[224] group, so you can inherit them to all other objects further down in the tree hierarchy.

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Basic Probe Settings	
Probe Name	Enter a meaningful name to identify the probe. The name will be shown by default in the devices tree and in all alarms.
Tags	Enter one or more tags; confirm each tag by hitting space, comma, or enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive.
Status	Choose if monitoring for this probe is started or paused. ▪ Started: Monitor this probe. ▪ Paused: Pause monitoring for this probe. All sensors on all devices on this probe will be paused until this setting is changed again.
Priority	Select a priority for the probe. This setting determines where the probe will be placed in list views. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[224] group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Location	
Location (for geo maps)	When using geo maps using Google's API^[1718] please enter a location in the first line. Objects will then be displayed on a geographical map with a flag, showing the current status using a color code similar to the sensor status icons^[121] (green - yellow - orange - red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, PRTG will parse latitude and longitude automatically; for example: 49.452778 11.077778 or enter 49.452778 any 11.077778 text A minus sign (-) in the first line will hide an object from geo maps. In this case you can enter location information in line two and following. You can define a specific label for each location: enter a string denoting the label in the first line and provide geo coordinates in the second line. This object will be displayed then with the label in PRTG's geo map.
Credentials for Windows Systems	
Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, please enter the computer name here. If you want to use a Windows domain user account (recommended), please enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Please do not leave this field empty.
Username	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
Username	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	Define which authentication method will be used for login. Choose between: ▪ Login via Password: Provide a password for login. Enter below. ▪ Login via Private Key: Provide a private key for authentication. Note: PRTG can only handle keys in OpenSSH format which are not encrypted. You cannot use password protected keys here. In the text field, please paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, please see Monitoring via SSH¹⁹³⁰.
Password	This field is only visible if password login is selected above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	This field is only visible if private key login is selected above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges. Note: If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service in order for the private key change to take effect! For details, please see Monitoring via SSH ¹⁹³⁰ .
For WBEM Use Protocol	Define the protocol that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: ▪ HTTP: Use an unencrypted connection for WBEM. ▪ HTTPS: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: ▪ Set automatically (port 5988 or 5989): Use one of the standard ports, depending on whether unencrypted or encrypted connection is chosen above. ▪ Set manually: Use a custom port. Define below.
WBEM Port	This setting is only visible if manual port selection is enabled above. Enter the WBEM port number.
SSH Port	Define the port number which will be used for SSH connections. Note: By default, this setting is automatically used for all SSH sensors²⁹⁶, unless you define a different port number in the sensor settings.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
SSH Rights Elevation	Define with which rights the command will be executed on the target system. Choose between: ▪ Run the command as the user connecting (default): Use the rights of the user who establishes the SSH connection. ▪ Run the command as another user using 'sudo': Use the rights of another user, for example, the administrator. ▪ Run the command as another user using 'su': Use the rights of another target user.
Target Username	This field is only visible if sudo or su is enabled above. Enter a username to run the specified command as another user than root. If you leave this field empty, the command will be run as root. Ensure that you set the Linux password even you use a public/private key for authentication. This is not necessary if the user is allowed to execute the command without a password.
Password Target User	This field is only visible if su is enabled above. Enter the password for the specified target user.

Credentials for VMware/XenServer	
User	Enter a login name for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: ▪ HTTPS (recommended): Use an SSL-encrypted connection to VMware and XenServers. ▪ HTTP: Use an unencrypted connection to VMware and XenServers.

Credentials for SNMP Devices	
SNMP Version	Select the SNMP version that will be used for device connection. Choose between: ▪ v1: Use the simple standard v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices.

Credentials for SNMP Devices	
	▪ v2c: Use the more advanced v2c protocol for SNMP connections. Data is still transferred as clear-text, but it supports 64-bit counters. ▪ v3: Use the latest v3 protocol for SNMP connections. It provides secure authentication and data encryption. Note for SNMP v3: Due to internal limitations you can only monitor a limited number of sensors per second using SNMP v3. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds you are limited to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased "Interval Delay" or "Open Requests" reading of the probe health sensor, you need to distribute the load over multiple probes. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if SNMP version v1 or v2c are enabled above. Enter the community string of your devices. This is a kind of "clear-text password" used for simple authentication. We recommend using the default value.
Authentication Type	This setting is only visible if SNMP version v3 is enabled above. Choose between: ▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. The chosen type has to match the authentication type of your device. Note: If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field password empty. In this case, SNMP_SEC_LEVEL_NOAUTH will be used and authentication will be deactivated entirely.
User	This setting is only visible if SNMP version v3 is enabled above. Enter a username for secure authentication. This value has to match the username of your device.
Password	This setting is only visible if SNMP version v3 is enabled above. Enter a password for secure authentication. This value has to match the password of your device.
Encryption Type	This setting is only visible if SNMP version v3 is enabled above. Select an encryption type. Choose between: ▪ DES: Use Data Encryption Standard (DES) as encryption algorithm.

Credentials for SNMP Devices	
	▪ AES: Use Advanced Encryption Standard (AES) as encryption algorithm. The chosen type has to match the encryption type of your device.
Data Encryption Key	This setting is only visible if SNMP version v3 is enabled above. Enter an encryption key here. If you provide a key in this field, SNMP data packets will be encrypted using the encryption algorithm selected above, providing increased security. The provided key here has to match the encryption key of your device. Note: If the key entered in this field does not match the key configured in the target SNMP device, you will not get an error message! Please enter a string or leave the field empty.
Context Name	This setting is only visible if SNMP version v3 is enabled above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port used for SNMP communication. We recommend using the default value.
SNMP Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Windows Compatibility Options	
When experiencing problems while monitoring via Windows sensors, you can set some compatibility options for trouble shooting.	
Preferred Data Source	Define the method Windows sensors will use to query data. This setting is valid only for hybrid sensors offering performance counter and Windows Management Instrumentation (WMI) technology. The setting will be ignored for all other sensors! Choose between: ▪ Performance Counters and fallback to WMI (recommended): Try to query data via performance counters. If this is not possible, establish a connection via WMI. This is the recommended setting to best balance resource usage and functionality. ▪ Performance Counters only: Query data via performance counters only. If this is not possible, a sensor will return no data. ▪ WMI only: Query data via WMI only. If this is not possible, a sensor will return no data.

Windows Compatibility Options

Timeout Method	Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between: ▪ Use 1.5x scanning interval (recommended): Use a default of one and a half times the scanning interval set for the sensor (see below in this settings). ▪ Set manually: Enter a timeout value manually. We recommend using the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.
Timeout Value (Sec.)	This field is only visible if the manual timeout method is selected above. Specify the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value.

SNMP Compatibility Options

When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for trouble shooting.

SNMP Delay (ms)	Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend using the default value. If you experience SNMP connection failures, please increase it. You can define a delay between 0 and 100, higher delays are not supported and will be discarded.
Failed Requests	Define if an SNMP sensor will try again after a request fails. ▪ Retry (recommended): Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures. ▪ Do not retry: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be set to error status earlier.
Overflow Values	Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks. ▪ Ignore overflow values (recommended): Ignore overflow values and do not include them in the monitoring data. ▪ Handle overflow values as valid results: Regard all overflow values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.

SNMP Compatibility Options	
Zero Values	Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks. ▪ Ignore zero values for delta sensors (recommended): Ignore zero values and do not include them in the monitoring data. ▪ Handle zero values as valid results for delta sensors: Regard all zero values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.
32-bit/64-bit Counters	Define which kind of traffic counters PRTG will search for on a device. ▪ Use 64-bit counters if available (recommended): The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices. ▪ Use 32-bit counters only: The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices. We recommend using the default value. If you experience problems, change this option.
Request Mode	Define which kind of request method PRTG uses for SNMP sensors. ▪ Use multi get (recommended): Bundle multiple SNMP requests into one request. ▪ Use single get: Use one request for each SNMP value. This can increase compatibility with older devices. We recommend using the default value. If you experience problems, change this option.
Port Name Template	Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device/OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, [port] [ifalias] is set as port name template, which will create a name such as (001) Ethernet1, for example. You can use any field names available at a certain OID of your device, among which are: ▪ [port]: The port number of the monitored interface. ▪ [ifalias]: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.

SNMP Compatibility Options	
	▪ [ifname]: The textual name of the monitored interface as assigned by the local device. ▪ [ifindex]: A unique value, greater than zero, for the monitored interface. ▪ [ifdescr]: A textual string containing information about the monitored device or interface, for example, manufacturer, product name, version. ▪ [ifspeed]: An estimate of the monitored interface's current bandwidth (KBit/s). Combine them as you like to obtain suitable sensor names. See the More section below for more information about SNMP sensor names.
Port Name Update	Define how PRTG will react if you change port names in your physical device (e.g. a switch or router). Choose between: ▪ Keep port names (use this if you edit the names in PRTG): Do not automatically adjust sensor names. This is the best option if you want to change names in PRTG manually. ▪ Automatic sensor name update if name changes in device: If PRTG detects changes of port names in your physical device, it will try to automatically adjust sensor names accordingly. For detailed information please see More section below.
Port Identification	Define which field will be used for SNMP interface identification. Choose between: ▪ Automatic (recommended): Tries the ifAlias field first to identify an SNMP interface and then ifDescr. Note: ifName will not be tried automatically. ▪ Use ifAlias: For most devices ifAlias is the best field to get unique interface names. ▪ Use ifDescr: Use this option if the port order of your device changes after a reboot, and there is no ifAlias field available. For example, this is the best option for Cisco ASA devices. Note: When using this option it is important that your device returns unique interface names in the ifDescr field. ▪ Use ifName: You can also use this option if there is no unique ifAlias available. Note: When using this option it is important that your device returns unique interface names in the ifName field. ▪ No Port Update: Use this option to disable automatic port identification.

SNMP Compatibility Options	
Start Port	For SNMP Traffic sensors, define at which port number PRTG will start to create sensors. Use 0 for automatic. We recommend using the default value.
End Port	For SNMP Traffic sensors, define at which port number PRTG will stop to create sensors. Use 0 for automatic. We recommend using the default value.
SNMP Debug Log	Define if you want to create an SNMP log file for debugging purposes. This is only recommended for debugging low level SNMP issues. Choose between: ▪ No log (recommended): No SNMP debug log file will be created. ▪ Enable debug log: An SNMP log file is written to the Logs (Debug) directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.

Proxy Settings for HTTP Sensors	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS. Note: This setting is valid for the monitoring only and determines the behavior of sensors. In order to change proxy settings for the core server, please see System Administration—System and Website ¹⁰¹¹ .
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Cluster Usage	
Scanning Distribution	This box is only visible if you're running a PRTG cluster. Sometimes you want to exclude a certain node from monitoring the sensors running on this probe, group, or device, for example, if a device is not reachable from every node configured in your cluster. In the list of cluster nodes, please select the nodes that will not be included in sensor scans. By default, this setting is inherited ⁸⁷ to all objects underneath.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window	
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current object if its parent object is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current object if its parent object is in a Down status, or if it is paused by another dependency. Additionally, pause the current object if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector¹⁵⁸ to choose an object on which the current object will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds.

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Automatic Monitoring Data Analysis	
Unusual Detection	Define if unusual detection is enabled for sensors. You can configure the behavior of unusual detection (or disable it completely) in the system settings^[1808]. ▪ Enabled: Enable unusual detection for this group. Sensors in this group will turn to orange color if unusual activity is detected. ▪ Disabled: Disable unusual detection for this group. Unusual values will be ignored for sensors in this group; they will not show an unusual sensor status.
Similar Sensors Detection	Define if similar sensors detection is enabled for sensors. You can configure the depth of analysis of similar sensors detection (or disable it completely) in the system settings^[1809]. ▪ Enabled: Enable similar sensors detection for this group. Sensors in this group will be considered during similarity analysis. ▪ Disabled: Disable similar detection for this group. Sensors in this group will not be taken into account during similarity analysis.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to you needs. In an object's detail page, click on the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- <http://www.paessler.com/knowledgebase/en/topic/313>

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?

- <http://www.paessler.com/knowledgebase/en/topic/7313>

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?

- <http://www.paessler.com/knowledgebase/en/topic/7363>

Knowledge Base: Automatically update port name and number for SNMP Traffic sensors when the device changes them

- <http://www.paessler.com/knowledgebase/en/topic/25893>

6.6 Group Settings

On a group's overview page, click on the **Settings** tab to change settings.

Add Group

The **Add Group** dialog appears when adding a new group to a parent group. It only shows the setting fields that are imperative for creating the group. Therefore, you will not see all setting fields in this dialog. For example, the **Group Status** option is not available in this step.

You can change all settings in the group's **Settings** tab later.

Group Settings

The following settings are available in the **Settings** tab of every group. As you may not need all of these for every group, just regard those settings you really need, ignoring the others.

Note: This documentation does not refer to the setting of the special **Root** group. The settings available there differ from those described here.

We recommend defining as many settings as possible in the **Root**  group, so you can inherit them to all other objects further down in the tree hierarchy.

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Basic Group Settings	
Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Status	Choose if monitoring for this group is started or paused. .We recommend using the default value. You can add additional tags to it, if you like. ▪ Started: Monitor this group. ▪ Paused: Pause monitoring for this group. All sensors on all devices in this group will be paused until this setting is changed again.
Tags	Enter one or more tags; confirm each tag by hitting space, comma, or enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive.

Basic Group Settings	
Priority	Select a priority for the group. This setting determines where the group will be placed in list views. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Group Type	
Sensor Management	Select which type of auto-discovery you would like to perform for this group. Choose between: ▪ Manual (no auto-discovery): Do not auto-discover any sensors, but only add sensors manually. ▪ Automatic device identification (standard, recommended): Use a small set of auto-discovery templates. This will scan your LAN and usually create a view standard sensors on your device. ▪ Automatic device identification (detailed, may create many sensors): Use an extended set of auto-discovery templates. This will scan your LAN and usually create many sensors on your device. ▪ Automatic sensor creation using specific device templates: Use specific auto-discovery templates only. Please select templates below. This will scan your LAN and add sensors defined in the template.
Device Template(s)	This option is only visible if using specific device templates (last option) is enabled above. Please choose one or more templates by adding a check mark in front of the respective template name. You can also select and deselect all items by using the check box in the table head. These will be used for auto-discovery on the current device. Choose from: ▪ ADSL ▪ Cisco ASA VPN ▪ Cisco Device (Generic) ▪ Dell MDI ▪ DNS Server ▪ Environment Jakarta ▪ Environment Poseidon ▪ Fritzbox ▪ FTP Server ▪ Generic Device (PING only)

- **Generic Device (SNMP-enabled)**
- **Generic Device (SNMP-enabled, Detailed)**
- **HTTP Web Server**
- **Hyper V Host Server**
- **Linux/UNIX Device (SNMP or SSH enabled)**
- **Mail Server (Generic)**
- **Mail Server (MS Exchange)**
- **Microsoft Sharepoint 2010**
- **NAS LenovoEMC**
- **NAS QNAP**
- **NAS Synology**
- **NetApp**
- **NTP Server**
- **Printer (HP)**
- **RDP Server**
- **RMON compatible device**
- **Server (Compaq/HP agents)**
- **Server (Dell)**
- **Server Cisco UCS**
- **Server IBM**
- **SonicWALL**
- **Switch (Cisco Catalyst)**
- **Switch (Cisco IOS Based)**
- **Switch (HP Procurve)**
- **UNIX/Linux Device**
- **UPS (APC)**
- **Virtualization Server**
- **VMware ESX / vCenter Server**
- **Windows (Detailed via WMI)**
- **Windows (via Remote Powershell)**
- **Windows (via WMI)**
- **Windows IIS (via SNMP)**
- **XEN Hosts**

	▪ XEN Virtual Machines Once the auto-discovery is finished, PRTG will create a new ticket ¹⁴⁸ and list the device templates which were actually used to create new sensors. Templates which were not applied will not be shown in the ticket.
Discovery Schedule	Define when the auto-discovery will be run. Choose between: ▪ Once: Perform auto-discovery only once. New devices and sensors will be added once. You can run auto-discovery manually any time using an object's context menu ¹⁶². ▪ Hourly: Perform auto-discovery for new devices and sensors every 60 minutes. Note: Please use this option with caution! Frequently executed auto-discoveries might cause performance issues, especially when large network segments are scanned every hour. ▪ Daily: Perform auto-discovery for new devices and sensors every 24 hours. The first auto-discovery will run immediately, all other discoveries will start on the time defined in the Auto-Discovery Settings section of the System Administration—System and Website ¹⁸⁰⁵ settings. ▪ Weekly: Perform auto-discovery for new devices and sensors every 7 days. The first auto-discovery will run immediately, all other discoveries will start on the time defined in the Auto-Discovery Settings section of the System Administration—System and Website ¹⁸⁰⁵ settings.
IP Selection Method	Define how you want to define the IP range for auto-discovery. Choose between: ▪ Class C base IP with start/end (IPv4): Define an IPv4 class C address range. ▪ List of individual IPs and DNS names (IPv4): Enter a list of individual IPv4 addresses or DNS names. ▪ IP and Subnet (IPv4): Enter an IPv4 address and subnet mask. ▪ IP with octet range (IPv4): Enter an IPv4 address range for every IP octet individually. With this, you can define very customizable IP ranges. ▪ List of individual IPs and DNS names (IPv6): Enter a list of individual IPv6 addresses or DNS names. ▪ Use computers from the active directory (maximum 1000 computers): Search in the active directory for computers to perform auto-discovery. Note: Only subnets with up to 65,536 IP addresses can be discovered! If you define a range with a higher number of addresses, discovery will stop before it is completed.

IPv4 Base	This field is only visible if Class C network detection is selected above. Enter a class C network as IP base for the auto-discovery. Enter the first three octets of an IPv4 IP address, for example, 192.168.0
IPv4 Range Start	This field is only visible if Class C network detection is selected above. Enter the IP octet of the class C network specified above from which PRTG will start the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter 1 to discover from 192.168.0.1 .
IPv4 Range End	This field is only visible if Class C network detection is selected above. Enter the IP octet of the class C network specified above at which PRTG will stop the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter 254 to discover up to 192.168.0.254 .
IPv4/DNS Name List IPv6/DNS Name List	This field is only visible if the IP list option is selected above. Enter a list of IP addresses or DNS names which the auto-discovery will scan. Enter each address in a separate line.
IPv4 and Subnet (IPv4)	This field is only visible if the IP and subnet option is selected above. Enter an expression in the format address/subnet , e.g. 192.168.3.0/255.255.255.0 . You can also use the short form like 192.168.3.0/24 in this example. PRTG will scan the complete host range (without network and broadcast address) defined by the IP address and the subnet mask.
IP with Octet Range	This field is only visible if the octet range option is selected above. Enter an expression in the format a1.a2.a3.a4 , where a1 , a2 , a3 , and a4 are each a number between 0-255, or a range with two numbers and a hyphen like 1-127 . All permutations of all ranges are calculated, e.g. 10.0.1-10.1-100 results in 1,000 addresses that PRTG will scan during auto-discovery.
Organizational Unit	This field is only visible if active directory is selected above. Enter an organizational unit (OU) to restrict the active directory search to computers which are part of this OU. Just enter the name of the OU without any other term (i.e., without "OU" in front). If you leave this field empty, there will not be any restriction. If you have sub-OUs, too, please consider the correct syntax in the format Y,OU=X: OUs that are part of another OU have to be listed together with their parent(s). Enter the sub-OU followed by ,OU= and the name of the parent OU. For example, assuming that the organizational unit 'Y' is part of the OU named 'X'. Then the syntax would be Y,OU=X. For three OUs 'X', 'Y' part of 'X', and 'Z' part of 'Y', the syntax would be Z,OU=Y,OU=X. Note that the order is important, sub-OUs have to be listed left of its according parents!

Name Resolution	Define how newly discovered devices will be monitored. This only affects new devices. The setting for existing devices will be kept. Choose between: ▪ Use DNS / WMI / SNMP names (recommended): Monitor newly discovered devices via their DNS, WMI, or SNMP names (if available). ▪ Use IP addresses: Monitor newly discovered devices via their IP address. We recommend using the default value.
Device Rescan	Define if you want to rescan known devices. Choose between: ▪ Skip auto-discovery for known devices/IPs (recommended): Do not re-scan known devices or IP addresses, but only scan for new devices/IPs when auto-discovering. This can avoid re-creation of manually deleted sensors. PRTG will also avoid adding devices that are already included elsewhere in your configuration, e.g. in other groups. ▪ Perform auto-discovery for known devices/IPs: Re-scan known devices and IP addresses with every auto-discovery. This will re-create manually deleted sensors on existing devices. We recommend using the default value.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Location	
Location (for geo maps)	When using geo maps using Google's API¹⁷¹⁸ please enter a location in the first line. Objects will then be displayed on a geographical map with a flag, showing the current status using a color code similar to the sensor status icons¹²¹ (green - yellow - orange - red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, PRTG will parse latitude and longitude automatically; for example: 49.452778 11.077778 or enter 49.452778 any 11.077778 text A minus sign (-) in the first line will hide an object from geo maps. In this case you can enter location information in line two and following.

Location	
	You can define a specific label for each location: enter a string denoting the label in the first line and provide geo coordinates in the second line. This object will be displayed then with the label in PRTG's geo map.

Credentials for Windows Systems	
Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, please enter the computer name here. If you want to use a Windows domain user account (recommended), please enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Please do not leave this field empty.
Username	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
Username	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	Define which authentication method will be used for login. Choose between: ▪ Login via Password: Provide a password for login. Enter below. ▪ Login via Private Key: Provide a private key for authentication. Note: PRTG can only handle keys in OpenSSH format which are not encrypted. You cannot use password protected keys here. In the text field, please paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, please see Monitoring via SSH ¹⁹³⁰.
Password	This field is only visible if password login is selected above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
Private Key	This field is only visible if private key login is selected above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges. Note: If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service in order for the private key change to take effect! For details, please see Monitoring via SSH .
For WBEM Use Protocol	Define the protocol that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: ▪ HTTP: Use an unencrypted connection for WBEM. ▪ HTTPS: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: ▪ Set automatically (port 5988 or 5989): Use one of the standard ports, depending on whether unencrypted or encrypted connection is chosen above. ▪ Set manually: Use a custom port. Define below.
WBEM Port	This setting is only visible if manual port selection is enabled above. Enter the WBEM port number.
SSH Port	Define the port number which will be used for SSH connections. Note: By default, this setting is automatically used for all SSH sensors , unless you define a different port number in the sensor settings.
SSH Rights Elevation	Define with which rights the command will be executed on the target system. Choose between: ▪ Run the command as the user connecting (default): Use the rights of the user who establishes the SSH connection. ▪ Run the command as another user using 'sudo': Use the rights of another user, for example, the administrator. ▪ Run the command as another user using 'su': Use the rights of another target user.
Target Username	This field is only visible if sudo or su is enabled above. Enter a username to run the specified command as another user than root. If you leave this field empty, the command will be run as root. Ensure that you set the Linux password even you use a public/private key for authentication. This is not necessary if the user is allowed to execute the command without a password.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems

Password Target User	This field is only visible if su is enabled above. Enter the password for the specified target user.

Credentials for VMware/XenServer

User	Enter a login name for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: ▪ HTTPS (recommended): Use an SSL-encrypted connection to VMware and XenServers. ▪ HTTP: Use an unencrypted connection to VMware and XenServers.

Credentials for SNMP Devices

SNMP Version	Select the SNMP version that will be used for device connection. Choose between: ▪ v1: Use the simple standard v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. ▪ v2c: Use the more advanced v2c protocol for SNMP connections. Data is still transferred as clear-text, but it supports 64-bit counters. ▪ v3: Use the latest v3 protocol for SNMP connections. It provides secure authentication and data encryption. Note for SNMP v3: Due to internal limitations you can only monitor a limited number of sensors per second using SNMP v3. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds you are limited to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased "Interval Delay" or "Open Requests" reading of the probe health sensor, you need to distribute the load over multiple probes. SNMP v1 and v2 do not have this limitation.

Credentials for SNMP Devices	
Community String	This setting is only visible if SNMP version v1 or v2c are enabled above. Enter the community string of your devices. This is a kind of "clear-text password" used for simple authentication. We recommend using the default value.
Authentication Type	This setting is only visible if SNMP version v3 is enabled above. Choose between: ▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. The chosen type has to match the authentication type of your device. Note: If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field password empty. In this case, SNMP_SEC_LEVEL_NOAUTH will be used and authentication will be deactivated entirely.
User	This setting is only visible if SNMP version v3 is enabled above. Enter a username for secure authentication. This value has to match the username of your device.
Password	This setting is only visible if SNMP version v3 is enabled above. Enter a password for secure authentication. This value has to match the password of your device.
Encryption Type	This setting is only visible if SNMP version v3 is enabled above. Select an encryption type. Choose between: ▪ DES: Use Data Encryption Standard (DES) as encryption algorithm. ▪ AES: Use Advanced Encryption Standard (AES) as encryption algorithm. The chosen type has to match the encryption type of your device.
Data Encryption Key	This setting is only visible if SNMP version v3 is enabled above. Enter an encryption key here. If you provide a key in this field, SNMP data packets will be encrypted using the encryption algorithm selected above, providing increased security. The provided key here has to match the encryption key of your device. Note: If the key entered in this field does not match the key configured in the target SNMP device, you will not get an error message! Please enter a string or leave the field empty.

Credentials for SNMP Devices	
Context Name	This setting is only visible if SNMP version v3 is enabled above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port used for SNMP communication. We recommend using the default value.
SNMP Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Windows Compatibility Options	
When experiencing problems while monitoring via Windows sensors, you can set some compatibility options for trouble shooting.	
Preferred Data Source	Define the method Windows sensors will use to query data. This setting is valid only for hybrid sensors offering performance counter and Windows Management Instrumentation (WMI) technology. The setting will be ignored for all other sensors! Choose between: ▪ Performance Counters and fallback to WMI (recommended): Try to query data via performance counters. If this is not possible, establish a connection via WMI. This is the recommended setting to best balance resource usage and functionality. ▪ Performance Counters only: Query data via performance counters only. If this is not possible, a sensor will return no data. ▪ WMI only: Query data via WMI only. If this is not possible, a sensor will return no data.
Timeout Method	Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between: ▪ Use 1.5x scanning interval (recommended): Use a default of one and a half times the scanning interval set for the sensor (see below in this settings). ▪ Set manually: Enter a timeout value manually. We recommend using the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.

Windows Compatibility Options

Timeout Value (Sec.)	This field is only visible if the manual timeout method is selected above. Specify the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value.

SNMP Compatibility Options

When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for trouble shooting.

SNMP Delay (ms)	Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend using the default value. If you experience SNMP connection failures, please increase it. You can define a delay between 0 and 100 , higher delays are not supported and will be discarded.
Failed Requests	Define if an SNMP sensor will try again after a request fails. ▪ Retry (recommended): Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures. ▪ Do not retry: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be set to error status earlier.
Overflow Values	Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks. ▪ Ignore overflow values (recommended): Ignore overflow values and do not include them in the monitoring data. ▪ Handle overflow values as valid results: Regard all overflow values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.
Zero Values	Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks. ▪ Ignore zero values for delta sensors (recommended): Ignore zero values and do not include them in the monitoring data. ▪ Handle zero values as valid results for delta sensors: Regard all zero values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.

SNMP Compatibility Options	
32-bit/64-bit Counters	Define which kind of traffic counters PRTG will search for on a device. ▪ Use 64-bit counters if available (recommended): The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices. ▪ Use 32-bit counters only: The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices. We recommend using the default value. If you experience problems, change this option.
Request Mode	Define which kind of request method PRTG uses for SNMP sensors. ▪ Use multi get (recommended): Bundle multiple SNMP requests into one request. ▪ Use single get: Use one request for each SNMP value. This can increase compatibility with older devices. We recommend using the default value. If you experience problems, change this option.
Port Name Template	Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device/OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, ([port]) [ifalias] is set as port name template, which will create a name such as (001) Ethernet1, for example. You can use any field names available at a certain OID of your device, among which are: ▪ [port]: The port number of the monitored interface. ▪ [ifalias]: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling. ▪ [ifname]: The textual name of the monitored interface as assigned by the local device. ▪ [ifindex]: A unique value, greater than zero, for the monitored interface. ▪ [ifdescr]: A textual string containing information about the monitored device or interface, for example, manufacturer, product name, version. ▪ [ifspeed]: An estimate of the monitored interface's current bandwidth (KBit/s).

SNMP Compatibility Options	
	Combine them as you like to obtain suitable sensor names. See the More section below for more information about SNMP sensor names.
Port Name Update	Define how PRTG will react if you change port names in your physical device (e.g. a switch or router). Choose between: ▪ Keep port names (use this if you edit the names in PRTG): Do not automatically adjust sensor names. This is the best option if you want to change names in PRTG manually. ▪ Automatic sensor name update if name changes in device: If PRTG detects changes of port names in your physical device, it will try to automatically adjust sensor names accordingly. For detailed information please see More section below.
Port Identification	Define which field will be used for SNMP interface identification. Choose between: ▪ Automatic (recommended): Tries the ifAlias field first to identify an SNMP interface and then ifDescr. Note: ifName will not be tried automatically. ▪ Use ifAlias: For most devices ifAlias is the best field to get unique interface names. ▪ Use ifDescr: Use this option if the port order of your device changes after a reboot, and there is no ifAlias field available. For example, this is the best option for Cisco ASA devices. Note: When using this option it is important that your device returns unique interface names in the ifDescr field. ▪ Use ifName: You can also use this option if there is no unique ifAlias available. Note: When using this option it is important that your device returns unique interface names in the ifName field. ▪ No Port Update: Use this option to disable automatic port identification.
Start Port	For SNMP Traffic sensors, define at which port number PRTG will start to create sensors. Use 0 for automatic. We recommend using the default value.
End Port	For SNMP Traffic sensors, define at which port number PRTG will stop to create sensors. Use 0 for automatic. We recommend using the default value.
SNMP Debug Log	Define if you want to create an SNMP log file for debugging purposes. This is only recommended for debugging low level SNMP issues. Choose between: ▪ No log (recommended): No SNMP debug log file will be created.

SNMP Compatibility Options

- **Enable debug log:** An SNMP log file is written to the **Logs (Debug)** directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see [Data Storage](#)^[2036] section.

Proxy Settings for HTTP Sensors

HTTP Proxy Settings

The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS. **Note:** This setting is valid for the monitoring only and determines the behavior of sensors. In order to change proxy settings for the core server, please see [System Administration—System and Website](#)^[1811].

Name

Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port

Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

User

If the proxy requires authentication, enter the username for the proxy login. **Note:** Only basic authentication is available! Please enter a string or leave the field empty.

Password

If the proxy requires authentication, enter the password for the proxy login. **Note:** Only basic authentication is available! Please enter a string or leave the field empty.

Scanning Interval

Scanning Interval

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)^[1905].

Cluster Usage

Scanning Distribution

This box is only visible if you're running a PRTG cluster. Sometimes you want to exclude a certain node from monitoring the sensors running on this probe, group, or device, for example, if a device is not reachable from every node configured in your cluster. In the list of cluster nodes, please select the nodes that will **not** be included in sensor scans. By default, this setting is [inherited](#)^[87] to all objects underneath.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current object if its parent object is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current object if its parent object is in a Down status, or if it is paused by another dependency. Additionally, pause the current object if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.

Schedules, Dependencies, and Maintenance Window	
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current object will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds.

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.
Automatic Monitoring Data Analysis	
Unusual Detection	Define if unusual detection is enabled for sensors. You can configure the behavior of unusual detection (or disable it completely) in the system settings ¹⁸⁰⁸. ▪ Enabled: Enable unusual detection for this group. Sensors in this group will turn to orange color if unusual activity is detected. ▪ Disabled: Disable unusual detection for this group. Unusual values will be ignored for sensors in this group; they will not show an unusual sensor status.
Similar Sensors Detection	Define if similar sensors detection is enabled for sensors. You can configure the depth of analysis of similar sensors detection (or disable it completely) in the system settings ¹⁸⁰⁹. ▪ Enabled: Enable similar sensors detection for this group. Sensors in this group will be considered during similarity analysis. ▪ Disabled: Disable similar detection for this group. Sensors in this group will not be taken into account during similarity analysis.
Number of Sensors Limitation	
Sensor Limit	This setting allows the administrator to set a limit for the maximum number of sensors in this group. Subgroups are also included. If sensors exceed this limitation, they will be paused. This is of special interest for a Managed Service Provider (MSP). Choose between: ▪ Allow unlimited number of sensors: Disable a limitation of the number of sensors for this group. Any number of sensors can be added to this group.

Number of Sensors Limitation	
	▪ Limit number of sensors in this group: Enables a limitation of the number of sensors for this group. Only a limited number of sensors can be added to this group.
Maximum Number of Sensors	This field is only visible if limitation is enabled above. Define how many sensors can be added to this group. Please enter an integer value.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to your needs. In an object's detail page, click on the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- <http://www.paessler.com/knowledgebase/en/topic/313>

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?

- <http://www.paessler.com/knowledgebase/en/topic/7313>

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?

- <http://www.paessler.com/knowledgebase/en/topic/7363>

Knowledge Base: Automatically update port name and number for SNMP Traffic sensors when the device changes them

- <http://www.paessler.com/knowledgebase/en/topic/25893>

6.7 Device Settings

On a device's details page, click on the **Settings** tab to change settings.

Add Device

The **Add Device** dialog appears when adding a new device to a group. It only shows the setting fields that are imperative for creating the device. Therefore, you will not see all setting fields in this dialog. For example, the **Device Status** option is not available in this step.

You can change all settings in the device's **Settings** tab later.

Device Settings

The following settings are available in the **Settings** tab of every device. As you may not need all of these for every device, just regard those settings you really need, ignoring the others.

We recommend defining as many settings as possible in the [Root](#)²²⁴ group, so you can inherit them to all other objects further down in the tree hierarchy.

For device settings, there is also multi-edit available. This enables you to change properties of many devices at a time. For more details, please see [Multi-Edit Lists](#)¹⁷¹⁰ section.

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Basic Device Settings	
Device Name	Enter a meaningful name to identify the device. The name will be shown by default in the device tree and in all alarms.
Status	Choose if monitoring for this device is started or paused. ▪ Started: Monitor this device. ▪ Paused: Pause monitoring for this device. All sensors on it will be paused until this setting is changed again.
IP Version	Define which IP protocol PRTG will use to connect to this device. The setting is valid for all sensors created on this device. Choose between: ▪ Connect using IPv4: Use IP version 4 for all requests to this device. ▪ Connect using IPv6: Use IP version 6 for all requests to this device.

Basic Device Settings	
IP Address/DNS Name	Enter the IP address (either v4 or v6, depending on your selection above) or DNS name for the device. Most sensors created on this device will inherit this setting and they will try to connect to this address for monitoring. (However, some sensor types still have their own setting for IP address/DNS name.)
Tags	Enter one or more tags; confirm each tag by hitting space, comma, or enter key. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Additional Device Information	
Device Icon	Choose a device icon from the list. It will be shown in the device tree. For information on how to add your custom icons, please see the link in the More ^[288] section below.
Service URL	Specify a URL you would like to open directly when choosing Device Tools Go To Service URL from the device's context menu ^[167] . For example, you can configure this option to call the address http://www.example.com/service.html . Enter a valid URL or leave the field empty.
Device Type	
Sensor Management	Select which type of auto-discovery you would like to perform for this device. Choose between: ▪ Manual (no auto-discovery): Do not auto-discover any sensors, but only add sensors manually. ▪ Automatic device identification (standard, recommended): Use a small set of auto-discovery templates. This will scan your LAN and usually create a view standard sensors on your device. ▪ Automatic device identification (detailed, may create many sensors): Use an extended set of auto-discovery templates. This will scan your LAN and usually create many sensors on your device.

Device Type	
	▪ Automatic sensor creation using specific device templates: Use specific auto-discovery templates only. Please select templates below. This will scan your LAN and add sensors defined in the template.
Discovery Schedule	This option is only visible if one of the auto-discovery options is selected above. Define when the auto-discovery will be run. Choose between: ▪ Once: Perform auto-discovery only once. For existing devices, this will initiate a one-time sensor update for the current device. ▪ Hourly: Perform auto-discovery for new sensors every hour. ▪ Daily: Perform auto-discovery for new sensors every day. ▪ Weekly: Perform auto-discovery for new sensors every week.
Device Template(s)	This option is only visible if using specific device templates (last option) is enabled above. Please choose one or more templates by adding a check mark in front of the respective template name. You can also select and deselect all items by using the check box in the table head. These will be used for auto-discovery on the current device. Choose from: ▪ ADSL ▪ Cisco ASA VPN ▪ Cisco Device (Generic) ▪ Dell MDI ▪ DNS Server ▪ Environment Jakarta ▪ Environment Poseidon ▪ Fritzbox ▪ FTP Server ▪ Generic Device (PING only) ▪ Generic Device (SNMP-enabled) ▪ Generic Device (SNMP-enabled, Detailed) ▪ HTTP Web Server ▪ Hyper V Host Server ▪ Linux/UNIX Device (SNMP or SSH enabled) ▪ Mail Server (Generic) ▪ Mail Server (MS Exchange)

Device Type	
	▪ Microsoft Sharepoint 2010 ▪ NAS LenovoEMC ▪ NAS QNAP ▪ NAS Synology ▪ NetApp ▪ NTP Server ▪ Printer (HP) ▪ RDP Server ▪ RMON compatible device ▪ Server (Compaq/HP agents) ▪ Server (Dell) ▪ Sever Cisco UCS ▪ Server IBM ▪ SonicWALL ▪ Switch (Cisco Catalyst) ▪ Switch (Cisco IOS Based) ▪ Switch (HP Procurve) ▪ UNIX/Linux Device ▪ UPS (APC) ▪ Virtuozzo Server ▪ VMware ESX / vCenter Server ▪ Windows (Detailed via WMI) ▪ Windows (via Remote Powershell) ▪ Windows (via WMI) ▪ Windows IIS (via SNMP) ▪ XEN Hosts ▪ XEN Virtual Machines Once the auto-discovery is finished, PRTG will create a new ticket ^[146] and list the device templates which were actually used to create new sensors. Templates which were not applied will not be shown in the ticket.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[224] group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Location	
Location (for geo maps)	When using geo maps using Google's API^[1718] please enter a location in the first line. Objects will then be displayed on a geographical map with a flag, showing the current status using a color code similar to the sensor status icons^[121] (green - yellow - orange - red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, PRTG will parse latitude and longitude automatically; for example: 49.452778 11.077778 or enter 49.452778 any 11.077778 text A minus sign (-) in the first line will hide an object from geo maps. In this case you can enter location information in line two and following. You can define a specific label for each location: enter a string denoting the label in the first line and provide geo coordinates in the second line. This object will be displayed then with the label in PRTG's geo map.
Credentials for Windows Systems	
Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, please enter the computer name here. If you want to use a Windows domain user account (recommended), please enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Please do not leave this field empty.
Username	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
Username	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	Define which authentication method will be used for login. Choose between: ▪ Login via Password: Provide a password for login. Enter below. ▪ Login via Private Key: Provide a private key for authentication. Note: PRTG can only handle keys in OpenSSH format which are not encrypted. You cannot use password protected keys here. In the text field, please paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, please see Monitoring via SSH¹⁹³⁰.
Password	This field is only visible if password login is selected above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	This field is only visible if private key login is selected above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges. Note: If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service in order for the private key change to take effect! For details, please see Monitoring via SSH ¹⁹³⁰ .
For WBEM Use Protocol	Define the protocol that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: ▪ HTTP: Use an unencrypted connection for WBEM. ▪ HTTPS: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port that will be used for WBEM. This setting is only relevant when using WBEM sensors. Choose between: ▪ Set automatically (port 5988 or 5989): Use one of the standard ports, depending on whether unencrypted or encrypted connection is chosen above. ▪ Set manually: Use a custom port. Define below.
WBEM Port	This setting is only visible if manual port selection is enabled above. Enter the WBEM port number.
SSH Port	Define the port number which will be used for SSH connections. Note: By default, this setting is automatically used for all SSH sensors²⁹⁶, unless you define a different port number in the sensor settings.

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems	
SSH Rights Elevation	Define with which rights the command will be executed on the target system. Choose between: ▪ Run the command as the user connecting (default): Use the rights of the user who establishes the SSH connection. ▪ Run the command as another user using 'sudo': Use the rights of another user, for example, the administrator. ▪ Run the command as another user using 'su': Use the rights of another target user.
Target Username	This field is only visible if sudo or su is enabled above. Enter a username to run the specified command as another user than root. If you leave this field empty, the command will be run as root. Ensure that you set the Linux password even you use a public/private key for authentication. This is not necessary if the user is allowed to execute the command without a password.
Password Target User	This field is only visible if su is enabled above. Enter the password for the specified target user.

Credentials for VMware/XenServer	
User	Enter a login name for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and XEN servers. Usually, you will use credentials with administrator privileges.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: ▪ HTTPS (recommended): Use an SSL-encrypted connection to VMware and XenServers. ▪ HTTP: Use an unencrypted connection to VMware and XenServers.

Credentials for SNMP Devices	
SNMP Version	Select the SNMP version that will be used for device connection. Choose between: ▪ v1: Use the simple standard v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices.

Credentials for SNMP Devices	
	▪ v2c: Use the more advanced v2c protocol for SNMP connections. Data is still transferred as clear-text, but it supports 64-bit counters. ▪ v3: Use the latest v3 protocol for SNMP connections. It provides secure authentication and data encryption. Note for SNMP v3: Due to internal limitations you can only monitor a limited number of sensors per second using SNMP v3. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds you are limited to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased "Interval Delay" or "Open Requests" reading of the probe health sensor, you need to distribute the load over multiple probes. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if SNMP version v1 or v2c are enabled above. Enter the community string of your devices. This is a kind of "clear-text password" used for simple authentication. We recommend using the default value.
Authentication Type	This setting is only visible if SNMP version v3 is enabled above. Choose between: ▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. The chosen type has to match the authentication type of your device. Note: If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field password empty. In this case, SNMP_SEC_LEVEL_NOAUTH will be used and authentication will be deactivated entirely.
User	This setting is only visible if SNMP version v3 is enabled above. Enter a username for secure authentication. This value has to match the username of your device.
Password	This setting is only visible if SNMP version v3 is enabled above. Enter a password for secure authentication. This value has to match the password of your device.
Encryption Type	This setting is only visible if SNMP version v3 is enabled above. Select an encryption type. Choose between: ▪ DES: Use Data Encryption Standard (DES) as encryption algorithm.

Credentials for SNMP Devices	
	▪ AES: Use Advanced Encryption Standard (AES) as encryption algorithm. The chosen type has to match the encryption type of your device.
Data Encryption Key	This setting is only visible if SNMP version v3 is enabled above. Enter an encryption key here. If you provide a key in this field, SNMP data packets will be encrypted using the encryption algorithm selected above, providing increased security. The provided key here has to match the encryption key of your device. Note: If the key entered in this field does not match the key configured in the target SNMP device, you will not get an error message! Please enter a string or leave the field empty.
Context Name	This setting is only visible if SNMP version v3 is enabled above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port used for SNMP communication. We recommend using the default value.
SNMP Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Windows Compatibility Options	
When experiencing problems while monitoring via Windows sensors, you can set some compatibility options for trouble shooting.	
Preferred Data Source	Define the method Windows sensors will use to query data. This setting is valid only for hybrid sensors offering performance counter and Windows Management Instrumentation (WMI) technology. The setting will be ignored for all other sensors! Choose between: ▪ Performance Counters and fallback to WMI (recommended): Try to query data via performance counters. If this is not possible, establish a connection via WMI. This is the recommended setting to best balance resource usage and functionality. ▪ Performance Counters only: Query data via performance counters only. If this is not possible, a sensor will return no data. ▪ WMI only: Query data via WMI only. If this is not possible, a sensor will return no data.

Windows Compatibility Options	
Timeout Method	Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between: ▪ Use 1.5x scanning interval (recommended): Use a default of one and a half times the scanning interval set for the sensor (see below in this settings). ▪ Set manually: Enter a timeout value manually. We recommend using the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.
Timeout Value (Sec.)	This field is only visible if the manual timeout method is selected above. Specify the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value.
SNMP Compatibility Options	
When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for trouble shooting.	
SNMP Delay (ms)	Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend using the default value. If you experience SNMP connection failures, please increase it. You can define a delay between 0 and 100, higher delays are not supported and will be discarded.
Failed Requests	Define if an SNMP sensor will try again after a request fails. ▪ Retry (recommended): Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures. ▪ Do not retry: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be set to error status earlier.
Overflow Values	Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks. ▪ Ignore overflow values (recommended): Ignore overflow values and do not include them in the monitoring data. ▪ Handle overflow values as valid results: Regard all overflow values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.

SNMP Compatibility Options	
Zero Values	Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks. ▪ Ignore zero values for delta sensors (recommended): Ignore zero values and do not include them in the monitoring data. ▪ Handle zero values as valid results for delta sensors: Regard all zero values as regular data and include them in the monitoring data. We recommend using the default value. If you experience problems, change this option.
32-bit/64-bit Counters	Define which kind of traffic counters PRTG will search for on a device. ▪ Use 64-bit counters if available (recommended): The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices. ▪ Use 32-bit counters only: The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices. We recommend using the default value. If you experience problems, change this option.
Request Mode	Define which kind of request method PRTG uses for SNMP sensors. ▪ Use multi get (recommended): Bundle multiple SNMP requests into one request. ▪ Use single get: Use one request for each SNMP value. This can increase compatibility with older devices. We recommend using the default value. If you experience problems, change this option.
Port Name Template	Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device/OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, [port] [ifalias] is set as port name template, which will create a name such as (001) Ethernet1, for example. You can use any field names available at a certain OID of your device, among which are: ▪ [port]: The port number of the monitored interface. ▪ [ifalias]: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.

SNMP Compatibility Options	
	▪ [ifname]: The textual name of the monitored interface as assigned by the local device. ▪ [ifindex]: A unique value, greater than zero, for the monitored interface. ▪ [ifdescr]: A textual string containing information about the monitored device or interface, for example, manufacturer, product name, version. ▪ [ifspeed]: An estimate of the monitored interface's current bandwidth (KBit/s). Combine them as you like to obtain suitable sensor names. See the More section below for more information about SNMP sensor names.
Port Name Update	Define how PRTG will react if you change port names in your physical device (e.g. a switch or router). Choose between: ▪ Keep port names (use this if you edit the names in PRTG): Do not automatically adjust sensor names. This is the best option if you want to change names in PRTG manually. ▪ Automatic sensor name update if name changes in device: If PRTG detects changes of port names in your physical device, it will try to automatically adjust sensor names accordingly. For detailed information please see More section below.
Port Identification	Define which field will be used for SNMP interface identification. Choose between: ▪ Automatic (recommended): Tries the ifAlias field first to identify an SNMP interface and then ifDescr. Note: ifName will not be tried automatically. ▪ Use ifAlias: For most devices ifAlias is the best field to get unique interface names. ▪ Use ifDescr: Use this option if the port order of your device changes after a reboot, and there is no ifAlias field available. For example, this is the best option for Cisco ASA devices. Note: When using this option it is important that your device returns unique interface names in the ifDescr field. ▪ Use ifName: You can also use this option if there is no unique ifAlias available. Note: When using this option it is important that your device returns unique interface names in the ifName field. ▪ No Port Update: Use this option to disable automatic port identification.

SNMP Compatibility Options	
Start Port	For SNMP Traffic sensors, define at which port number PRTG will start to create sensors. Use 0 for automatic. We recommend using the default value.
End Port	For SNMP Traffic sensors, define at which port number PRTG will stop to create sensors. Use 0 for automatic. We recommend using the default value.
SNMP Debug Log	Define if you want to create an SNMP log file for debugging purposes. This is only recommended for debugging low level SNMP issues. Choose between: ▪ No log (recommended): No SNMP debug log file will be created. ▪ Enable debug log: An SNMP log file is written to the Logs (Debug) directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.

Proxy Settings for HTTP Sensors	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS. Note: This setting is valid for the monitoring only and determines the behavior of sensors. In order to change proxy settings for the core server, please see System Administration—System and Website ¹⁰¹¹ .
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Cluster Usage	
Scanning Distribution	This box is only visible if you're running a PRTG cluster. Sometimes you want to exclude a certain node from monitoring the sensors running on this probe, group, or device, for example, if a device is not reachable from every node configured in your cluster. In the list of cluster nodes, please select the nodes that will not be included in sensor scans. By default, this setting is inherited ⁸⁷ to all objects underneath.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window	
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current object if its parent object is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current object if its parent object is in a Down status, or if it is paused by another dependency. Additionally, pause the current object if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector¹⁵⁸ to choose an object on which the current object will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds.

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Automatic Monitoring Data Analysis	
Unusual Detection	Define if unusual detection is enabled for sensors. You can configure the behavior of unusual detection (or disable it completely) in the system settings^[1808]. ▪ Enabled: Enable unusual detection for this group. Sensors in this group will turn to orange color if unusual activity is detected. ▪ Disabled: Disable unusual detection for this group. Unusual values will be ignored for sensors in this group; they will not show an unusual sensor status.
Similar Sensors Detection	Define if similar sensors detection is enabled for sensors. You can configure the depth of analysis of similar sensors detection (or disable it completely) in the system settings^[1809]. ▪ Enabled: Enable similar sensors detection for this group. Sensors in this group will be considered during similarity analysis. ▪ Disabled: Disable similar detection for this group. Sensors in this group will not be taken into account during similarity analysis.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to you needs. In an object's detail page, click on the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- <http://www.paessler.com/knowledgebase/en/topic/313>

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?

- <http://www.paessler.com/knowledgebase/en/topic/7313>

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?

- <http://www.paessler.com/knowledgebase/en/topic/7363>

Knowledge Base: Automatically update port name and number for SNMP Traffic sensors when the device changes them

- <http://www.paessler.com/knowledgebase/en/topic/25893>

6.8 Sensor Settings

There are more than 210 different sensor types available. In the **Add Sensor** dialog, all sensors are categorized into groups to help you quickly find what you need. Once you are familiar with the interface, you will probably enter the first letters of a sensor type's name into the **Search** field in the upper left corner and get to a sensor even faster.

Available Sensor Types

There is a dedicated manual section for every sensor type with details about the available settings. For more information, please see [List of Available Sensors](#)²⁹¹ section.

For sensor settings, there is also multi-edit available. This enables you to change properties of many sensors at a time. For more details, please see [Multi-Edit Lists](#)¹⁷¹⁰ section.

In order to detect unexpected correlations between your network components, PRTG provides a [Similar Sensors](#)¹³⁷ analysis.

Sensor Settings Overview

For information about sensor settings, please see the following sections:

- [Sensor Settings](#)²⁹⁰
- [List of Available Sensor Types](#)²⁹¹
- [Additional Sensor Types \(Custom Sensors\)](#)¹⁶⁸⁰
- [Sensor Channels Settings](#)¹⁶⁸³
- [Sensor Notifications Settings](#)¹⁶⁹⁰

6.8.1 List of Available Sensor Types

This chapter lists all available sensors, arranged both by different categories and in alphabetical order. **Note:** In the [Add a Sensor](#) ²²⁰ assistant, PRTG offers you various options to filter for fitting sensor types easily.

- [Common Sensors](#) ²⁹¹
 - [Bandwidth Monitoring Sensors](#) ²⁹¹
 - [Web Servers \(HTTP\) Sensors](#) ²⁹²
 - [SNMP Sensors](#) ²⁹³
 - [Windows WMI/Performance Counters Sensors](#) ²⁹⁴
 - [Linux/Unix/OS X Sensors](#) ²⁹⁶
 - [Virtual Servers Sensors](#) ²⁹⁶
 - [Mail Servers Sensors](#) ²⁹⁷
 - [SQL Database Servers Sensors](#) ²⁹⁷
 - [File Servers Sensors](#) ²⁹⁸
 - [Various Servers Sensors](#) ²⁹⁸
 - [VoIP and QoS Sensors](#) ²⁹⁹
 - [Hardware Parameters Sensors](#) ²⁹⁹
 - [Custom Sensors](#) ³⁰⁰
 - [PRTG Internal Sensors](#) ³⁰¹
 - [All Sensors in Alphabetical Order](#) ³⁰¹
 - [More](#) ³⁰⁷
-

Common Sensors

- [HTTP Sensor](#) ⁴⁸⁴
- [Ping Sensor](#) ⁷⁵⁶
- [Port Sensor](#) ⁷⁸⁵
- [Port Range Sensor](#) ⁷⁹²
- [SNMP Traffic Sensor](#) ¹²³⁴
- [Windows Network Card Sensor](#) ¹⁴⁵⁰

Bandwidth Monitoring Sensors

- [AVM FRITZ!Box WAN Interface Sensor](#) ³³⁰

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [IPFIX Sensor](#)  630
- [IPFIX \(Custom\) Sensor](#)  638
- [jFlow V5 Sensor](#)  646
- [jFlow V5 \(Custom\) Sensor](#)  654
- [NetFlow V5 Sensor](#)  682
- [NetFlow V5 \(Custom\) Sensor](#)  690
- [NetFlow V9 Sensor](#)  698
- [NetFlow V9 \(Custom\) Sensor](#)  706
- [Packet Sniffer Sensor](#)  722
- [Packet Sniffer \(Custom\) Sensor](#)  729
- [sFlow Sensor](#)  852
- [sFlow \(Custom\) Sensor](#)  860
- [SNMP Cisco ADSL Sensor](#)  914
- [SNMP Cisco ASA VPN Traffic Sensor](#)  924
- [SNMP Library Sensor](#)  1094
- [SNMP NetApp Network Interface Sensor](#)  1164
- [SNMP RMON Sensor](#)  1197
- [SNMP Traffic Sensor](#)  1294
- [Windows Network Card Sensor](#)  1450

Web Servers (HTTP) Sensors

- [Google Analytics Sensor](#)  477
- [HTTP Sensor](#)  484
- [HTTP Advanced Sensor](#)  491
- [HTTP Apache ModStatus PerfStats Sensor](#)  503
- [HTTP Apache ModStatus Totals Sensor](#)  510
- [HTTP Content Sensor](#)  517
- [HTTP Full Web Page Sensor](#)  526
- [HTTP Push Count Sensor](#)  533
- [HTTP Push Data Sensor](#)  539
- [HTTP SSL Certificate Expiry Sensor](#)  545
- [HTTP Transaction Sensor](#)  551
- [HTTP XML/REST Value Sensor](#)  561

- [Windows IIS Application Sensor](#) 

SNMP Sensors

- [SNMP APC Hardware Sensor](#) 
- [SNMP Cisco ADSL Sensor](#) 
- [SNMP Cisco ASA VPN Connections Sensor](#) 
- [SNMP Cisco ASA VPN Traffic Sensor](#) 
- [SNMP Cisco ASA VPN Users Sensor](#) 
- [SNMP Cisco CBooS Sensor](#) 
- [SNMP Cisco System Health Sensor](#) 
- [SNMP Cisco UCS Chassis Sensor](#) 
- [SNMP Cisco UCS Physical Disk Sensor](#) 
- [SNMP Cisco UCS System Health Sensor](#) 
- [SNMP CPU Load Sensor](#) 
- [SNMP Custom Sensor](#) 
- [SNMP Custom String Sensor](#) 
- [SNMP Dell Hardware Sensor](#) 
- [SNMP Dell PowerEdge Physical Disk Sensor](#) 
- [SNMP Dell PowerEdge System Health Sensor](#) 
- [SNMP Disk Free Sensor](#) 
- [SNMP GSA System Health Sensor](#) 
- [SNMP Hardware Status Sensor](#) 
- [SNMP HP LaserJet Hardware Sensor](#) 
- [SNMP HP ProLiant Logical Disk Sensor](#) 
- [SNMP HP ProLiant Memory Controller Sensor](#) 
- [SNMP HP ProLiant Network Interface Sensor](#) 
- [SNMP HP ProLiant Physical Disk Sensor](#) 
- [SNMP HP ProLiant System Health Sensor](#) 
- [SNMP IBM System X Logical Disk Sensor](#) 
- [SNMP IBM System X Physical Disk Sensor](#) 
- [SNMP IBM System X Physical Memory Sensor](#) 
- [SNMP IBM System X System Health Sensor](#) 
- [SNMP interSeptor Pro Environment Sensor](#) 

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [SNMP LenovoEMC Physical Disk Sensor](#)  1083
- [SNMP LenovoEMC System Health Sensor](#)  1089
- [SNMP Library Sensor](#)  1094
- [SNMP Linux Disk Free Sensor](#)  1102
- [SNMP Linux Load Average Sensor](#)  1110
- [SNMP Linux Meminfo Sensor](#)  1115
- [SNMP Linux Physical Disk Sensor](#)  1120
- [SNMP Memory Sensor](#)  1128
- [SNMP NetApp Disk Free Sensor](#)  1134
- [SNMP NetApp Enclosure Sensor](#)  1140
- [SNMP NetApp I/O Sensor](#)  1146
- [SNMP NetApp License Sensor](#)  1152
- [SNMP NetApp Logical Unit Sensor](#)  1158
- [SNMP NetApp Network Interface Sensor](#)  1164
- [SNMP NetApp System Health Sensor](#)  1170
- [SNMP Poseidon Environment Sensor](#)  1176
- [SNMP QNAP Logical Disk Sensor](#)  1181
- [SNMP QNAP Physical Disk Sensor](#)  1186
- [SNMP QNAP System Health Sensor](#)  1192
- [SNMP RMON Sensor](#)  1197
- [SNMP SonicWALL System Health Sensor](#)  1203
- [SNMP SonicWALL VPN Traffic Sensor](#)  1208
- [SNMP Synology Logical Disk Sensor](#)  1214
- [SNMP Synology Physical Disk Sensor](#)  1219
- [SNMP Synology System Health Sensor](#)  1224
- [SNMP System Uptime Sensor](#)  1229
- [SNMP Traffic Sensor](#)  1234
- [SNMP Trap Receiver Sensor](#)  1241
- [SNMP Windows Service Sensor](#)  1250

Windows WMI/Performance Counters Sensors

- [Active Directory Replication Errors Sensor](#)  308
- [Event Log \(Windows API\) Sensor](#)  388
- [PerfCounter Custom Sensor](#)  742

- [PerfCounter IIS Application Pool Sensor](#)  749
- [Windows CPU Load Sensor](#)  1406
- [Windows Last Update Sensor](#)  1431
- [Windows Logged In Users Sensor](#)  1437
- [Windows MSMQ Queue Length Sensor](#)  1443
- [Windows Print Queue Sensor](#)  1470
- [Windows Registry Sensor](#)  1476
- [Windows Scheduled Task Sensor](#)  1484
- [Windows Updates Status \(Powershell\) Sensor](#)  1497
- [WMI Custom Sensor](#)  1503
- [WMI Custom String Sensor](#)  1510
- [WMI Event Log Sensor](#)  1519
- [WMI Exchange Server Sensor](#)  1527
- [WMI Exchange Transport Queue Sensor](#)  1534
- [WMI File Sensor](#)  1541
- [WMI Free Disk Space \(Multi Drive\) Sensor](#)  1547
- [WMI HDD Health Sensor](#)  1555
- [Windows IIS 6.0 SMTP Received Sensor](#)  1412
- [Windows IIS 6.0 SMTP Sent Sensor](#)  1418
- [WMI Logical Disk Sensor](#)  1561
- [WMI Memory Sensor](#)  1567
- [WMI Microsoft SQL Server 2005 Sensor](#)  1572
- [WMI Microsoft SQL Server 2008 Sensor](#)  1581
- [WMI Microsoft SQL Server 2012 Sensor](#)  1589
- [Windows Network Card Sensor](#)  1450
- [Windows Pagefile Sensor](#)  1457
- [Windows Physical Disk Sensor](#)  1463
- [WMI Process Sensor](#)  1597
- [WMI Remote Ping Sensor](#)  1603
- [WMI Security Center Sensor](#)  1608
- [WMI Service Sensor](#)  1614
- [WMI Share Sensor](#)  1620
- [WMI SharePoint Process Sensor](#)  1627
- [Windows System Uptime Sensor](#)  1491

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [WMI Terminal Services \(Windows 2008\) Sensor](#)  1633
- [WMI Terminal Services \(Windows XP/Vista/2003\) Sensor](#)  1630
- [WMI UTC Time Sensor](#)  1643
- [WMI Vital System Data \(V2\) Sensor](#)  1648
- [WMI Volume Sensor](#)  1654
- [WMI Windows Version Sensor](#)  1667
- [WSUS Statistics Sensor](#)  1673

Linux/Unix/OS X Sensors

- [SNMP Linux Disk Free Sensor](#)  1102
- [SNMP Linux Load Average Sensor](#)  1110
- [SNMP Linux Meminfo Sensor](#)  1115
- [SNMP Linux Physical Disk Sensor](#)  1120
- [SSH Disk Free Sensor](#)  1200
- [SSH INodes Free Sensor](#)  1209
- [SSH Load Average Sensor](#)  1275
- [SSH Meminfo Sensor](#)  1281
- [SSH Remote Ping Sensor](#)  1287
- [SSH Script Sensor](#)  1315
- [SSH Script Advanced Sensor](#)  1324
- [SSH SAN Logical Disk Sensor](#)  1294
- [SSH SAN Physical Disk Sensor](#)  1301
- [SSH SAN System Health Sensor](#)  1308
- [WBEM Custom Sensor](#)  1400

Virtual Servers Sensors

- [Amazon CloudWatch Sensor](#)  322
- [Citrix XenServer Host Sensor](#)  342
- [Citrix XenServer Virtual Machine Sensor](#)  348
- [Enterprise Virtual Array Sensor](#)  381
- [Hyper-V Cluster Shared Volume Disk Free Sensor](#)  572
- [Hyper-V Host Server Sensor](#)  579
- [Hyper-V Virtual Machine Sensor](#)  585

- [Hyper-V Virtual Network Adapter Sensor](#)  593
- [Hyper-V Virtual Storage Device Sensor](#)  600
- [SCVMM Host Sensor](#)  823
- [SCVMM Virtual Machine Sensor](#)  830
- [SSH VMWare ESX\(i\) Disk Sensor](#)  1332
- [Virtuozzo Container Disk Sensor](#)  1363
- [Virtuozzo Container Network Sensor](#)  1369
- [VMware Host Hardware \(WBEM\) Sensor](#)  1375
- [VMware Host Hardware Status \(SOAP\) Sensor](#)  1381
- [VMware Host Performance \(SOAP\) Sensor](#)  1387
- [VMware Virtual Machine \(SOAP\) Sensor](#)  1393

Mail Servers Sensors

- [Exchange Backup \(Powershell\) Sensor](#)  396
- [Exchange Database \(Powershell\) Sensor](#)  403
- [Exchange Mailbox \(Powershell\) Sensor](#)  410
- [Exchange Mail Queue \(Powershell\) Sensor](#)  417
- [Exchange Public Folder \(Powershell\) Sensor](#)  423
- [IMAP Sensor](#)  607
- [IP on DNS Blacklist Sensor](#)  624
- [POP3 Sensor](#)  773
- [POP3 Email Count Sensor](#)  779
- [SMTP Sensor](#)  886
- [SMTP&IMAP Round Trip Sensor](#)  892
- [SMTP&POP3 Round Trip Sensor](#)  900
- [WMI Exchange Server Sensor](#)  1527
- [WMI Exchange Transport Queue Sensor](#)  1534
- [Windows IIS 6.0 SMTP Received Sensor](#)  1412
- [Windows IIS 6.0 SMTP Sent Sensor](#)  1418

SQL Database Servers Sensors

- [ADO SQL Sensor](#)  315
- [Microsoft SQL Sensor](#)  667

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [MySQL Sensor](#)  675
- [Oracle SQL Sensor](#)  714
- [WMI Microsoft SQL Server 2005 Sensor](#)  1572
- [WMI Microsoft SQL Server 2008 Sensor](#)  1581
- [WMI Microsoft SQL Server 2012 Sensor](#)  1580

File Servers Sensors

- [Dell PowerVault MDi Sensor](#)  362
- [File Sensor](#)  447
- [File Content Sensor](#)  453
- [Folder Sensor](#)  459
- [FTP Sensor](#)  465
- [FTP Server File Count Sensor](#)  471
- [INI File Content Check Sensor](#)  618
- [SFTP Secure File Transfer Protocol Sensor](#)  868
- [Share Disk Free Sensor](#)  874
- [SNMP NetApp Disk Free Sensor](#)  1134
- [SNMP NetApp Enclosure Sensor](#)  1140
- [SNMP NetApp I/O Sensor](#)  1146
- [SNMP NetApp License Sensor](#)  1152
- [SNMP NetApp Network Interface Sensor](#)  1164
- [SNMP NetApp System Health Sensor](#)  1170
- [TFTP Sensor](#)  1361
- [WMI File Sensor](#)  1541
- [WMI Free Disk Space \(Multi Drive\) Sensor](#)  1547
- [WMI Volume Sensor](#)  1654

Various Servers Sensors

- [DHCP Sensor](#)  368
- [DNS Sensor](#)  375
- [LDAP Sensor](#)  662
- [Ping Sensor](#)  756
- [Ping litter Sensor](#)  762

- [Pingdom Sensor](#)  767
- [Port Sensor](#)  785
- [Port Range Sensor](#)  792
- [RADIUS Sensor](#)  813
- [RDP \(Remote Desktop\) Sensor](#)  818
- [SNMP Trap Receiver Sensor](#)  1241
- [SNTP Sensor](#)  1255
- [Syslog Receiver Sensor](#)  1338
- [Traceroute Hop Count Sensor](#)  1357

VoIP and QoS Sensors

- [Cisco IP SLA Sensor](#)  336
- [SIP Options Ping Sensor](#)  880
- [QoS \(Quality of Service\) One Way Sensor](#)  801
- [QoS \(Quality of Service\) Round Trip Sensor](#)  807
- [SNMP Cisco CBQoS Sensor](#)  934

Hardware Parameter Sensors

- [Dell PowerVault MDi Sensor](#)  362
- [Enterprise Virtual Array Sensor](#)  381
- [SNMP APC Hardware Sensor](#)  908
- [SNMP Cisco System Health Sensor](#)  939
- [SNMP Cisco UCS Chassis Sensor](#)  945
- [SNMP Cisco UCS Physical Disk Sensor](#)  951
- [SNMP Cisco UCS System Health Sensor](#)  957
- [SNMP CPU Load Sensor](#)  963
- [SNMP Dell Hardware Sensor](#)  983
- [SNMP Dell PowerEdge Physical Disk Sensor](#)  989
- [SNMP Dell PowerEdge System Health Sensor](#)  995
- [SNMP Disk Free Sensor](#)  1001
- [SNMP GSA System Health Sensor](#)  1007
- [SNMP Hardware Status Sensor](#)  1012
- [SNMP HP LaserJet Hardware Sensor](#)  1017

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [SNMP HP ProLiant Memory Controller Sensor](#) 
- [SNMP HP ProLiant Network Interface Sensor](#) 
- [SNMP HP ProLiant Physical Disk Sensor](#) 
- [SNMP HP ProLiant System Health Sensor](#) 
- [SNMP IBM System X Physical Disk Sensor](#) 
- [SNMP IBM System X Physical Memory Sensor](#) 
- [SNMP IBM System X System Health Sensor](#) 
- [SNMP LenovoEMC Physical Disk Sensor](#) 
- [SNMP LenovoEMC System Health Sensor](#) 
- [SNMP Library Sensor](#) 
- [SNMP Memory Sensor](#) 
- [SNMP NetApp I/O Sensor](#) 
- [SNMP NetApp Enclosure Sensor](#) 
- [SNMP NetApp Logical Unit Sensor](#) 
- [SNMP NetApp Network Interface Sensor](#) 
- [SNMP NetApp System Health Sensor](#) 
- [SNMP QNAP Physical Disk Sensor](#) 
- [SNMP QNAP System Health Sensor](#) 
- [SNMP SonicWALL System Health Sensor](#) 
- [SNMP SonicWALL VPN Traffic Sensor](#) 
- [SNMP Synology Physical Disk Sensor](#) 
- [SNMP Synology System Health Sensor](#) 
- [SSH SAN Logical Disk Sensor](#) 
- [SSH SAN Physical Disk Sensor](#) 
- [SSH SAN System Health Sensor](#) 
- [WMI HDD Health Sensor](#) 

Custom Sensors

- [EXE/Script Sensor](#) 
- [EXE/Script Advanced Sensor](#) 
- [IPFIX \(Custom\) Sensor](#) 
- [iFlow V5 \(Custom\) Sensor](#) 
- [NetFlow V5 \(Custom\) Sensor](#) 

- [NetFlow V9 \(Custom\) Sensor](#)^[706]
- [Packet Sniffer \(Custom\) Sensor](#)^[729]
- [Pingdom Sensor](#)^[767]
- [Sensor Factory Sensor](#)^[837]
- [sFlow \(Custom\) Sensor](#)^[860]
- [SNMP Custom Sensor](#)^[968]
- [SNMP Custom String Sensor](#)^[975]
- [SSH Script Sensor](#)^[1315]
- [WBEM Custom Sensor](#)^[1400]
- [WMI Custom Sensor](#)^[1503]
- [WMI Custom String Sensor](#)^[1510]

PRTG Internal Sensors

- [Core Health Sensor](#)^[358]
- [Probe Health Sensor](#)^[797]
- [System Health Sensor](#)^[1347]

All Sensors in Alphabetical Order

The version numbers show when the respective sensor type was originally introduced to PRTG.

- [Active Directory Replication Errors Sensor](#)^[308] (v8.3.0)
- [ADO SQL Sensor](#)^[315] (v8.1.0)
- [Amazon CloudWatch Sensor](#)^[322] (v7)
- [AVM FRITZ!Box WAN Interface Sensor](#)^[330] (v12.x.1)
- [Cisco IP SLA Sensor](#)^[336] (v7)
- [Citrix XenServer Host Sensor](#)^[342] (v12.x.1)
- [Citrix XenServer Virtual Machine Sensor](#)^[348] (v8.1.0)
- [Cluster Probe Health Sensor](#)^[354] (v9.1.0)
- [Core Health Sensor](#)^[358] (v9.1.0)
- [Dell PowerVault MDi Sensor](#)^[362] (v12.x.1)
- [DHCP Sensor](#)^[368] (v8.2.0)
- [DNS Sensor](#)^[375] (v7)
- [Enterprise Virtual Array Sensor](#)^[381] (v13.x.6)

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [Event Log \(Windows API\) Sensor](#)^[388] (v7)
- [Exchange Backup \(Powershell\) Sensor](#)^[396] (v13.x.5)
- [Exchange Database \(Powershell\) Sensor](#)^[403] (v13.x.5)
- [Exchange Mailbox \(Powershell\) Sensor](#)^[410] (v13.x.5)
- [Exchange Mail Queue \(Powershell\) Sensor](#)^[417] (v13.x.5)
- [Exchange Public Folder \(Powershell\) Sensor](#)^[423] (v13.x.5)
- [EXE/Script Sensor](#)^[430] (v7)
- [EXE/Script Advanced Sensor](#)^[439] (v7)
- [File Sensor](#)^[447] (v7)
- [File Content Sensor](#)^[453] (v7)
- [Folder Sensor](#)^[459] (v7)
- [FTP Sensor](#)^[465] (v7)
- [FTP Server File Count Sensor](#)^[471] (v8.3.0)
- [Google Analytics Sensor](#)^[477] (v12.x.1)
- [HTTP Sensor](#)^[484] (v7)
- [HTTP Advanced Sensor](#)^[491] (v7)
- [HTTP Apache ModStatus PerfStats Sensor](#)^[503] (v12.x.3)
- [HTTP Apache ModStatus Totals Sensor](#)^[510] (v12.x.3)
- [HTTP Content Sensor](#)^[517] (v7)
- [HTTP Full Web Page Sensor](#)^[526] (v7)
- [HTTP Push Count Sensor](#)^[533] (v13.x.8)
- [HTTP Push Data Sensor](#)^[539] (v13.x.8)
- [HTTP SSL Certificate Expiry Sensor](#)^[545] (v8.3.0)
- [HTTP Transaction Sensor](#)^[551] (v7)
- [HTTP XML/REST Value Sensor](#)^[561] (v8.3.0)
- [Hyper-V Cluster Shared Volume Disk Free Sensor](#)^[572] (v12.3.4)
- [Hyper-V Host Server Sensor](#)^[579] (v7)
- [Hyper-V Virtual Machine Sensor](#)^[585] (v7)
- [Hyper-V Virtual Network Adapter Sensor](#)^[593] (v9.1.0)
- [Hyper-V Virtual Storage Device Sensor](#)^[600] (v12.4.4)
- [IMAP Sensor](#)^[607] (v7)
- [INI File Content Check Sensor](#)^[618] (v8.3.0)
- [IP on DNS Blacklist Sensor](#)^[624] (v8.3.0)
- [IPFIX Sensor](#)^[630] (v13.x.7)

- [IPFIX \(Custom\) Sensor](#)^[638] (v13.x.7)
- [iFlow V5 Sensor](#)^[646] (v8.2.0)
- [iFlow V5 \(Custom\) Sensor](#)^[654] (v8.2.0)
- [LDAP Sensor](#)^[662] (v8.1.0)
- [Microsoft SQL Sensor](#)^[667] (v7)
- [MySQL Sensor](#)^[675] (v7)
- [NetFlow V5 Sensor](#)^[682] (v7)
- [NetFlow V5 \(Custom\) Sensor](#)^[690] (v7)
- [NetFlow V9 Sensor](#)^[698] (v7)
- [NetFlow V9 \(Custom\) Sensor](#)^[706] (v7)
- [Oracle SQL Sensor](#)^[714] (v7)
- [Packet Sniffer Sensor](#)^[722] (v7)
- [Packet Sniffer \(Custom\) Sensor](#)^[729] (v7)
- [Passive Application Performance Sensor](#)^[736] (v13.x.4)
- [PerfCounter Custom Sensor](#)^[742] (v12.x.3)
- [PerfCounter IIS Application Pool Sensor](#)^[749] (v12.x.6)
- [Ping Sensor](#)^[756] (v7)
- [Ping Jitter Sensor](#)^[762] (v8.3.0)
- [Pingdom Sensor](#)^[767] (v8.4.0)
- [POP3 Sensor](#)^[773] (v7)
- [POP3 Email Count Sensor](#)^[779] (v8.3.0)
- [Port Sensor](#)^[785] (v7)
- [Port Range Sensor](#)^[792] (v12.x.4)
- [Probe Health Sensor](#)^[797] (v9.1.0)
- [QoS \(Quality of Service\) One Way Sensor](#)^[801] (v7)
- [QoS \(Quality of Service\) Round Trip Sensor](#)^[807] (v9.1.0)
- [RADIUS Sensor](#)^[813] (v7)
- [RDP \(Remote Desktop\) Sensor](#)^[818] (v7)
- [SCVMM Host Sensor](#)^[823] (v12.x.6)
- [SCVMM Virtual Machine Sensor](#)^[830] (v12.x.6)
- [Sensor Factory Sensor](#)^[837] (v7)
- [sFlow Sensor](#)^[852] (v7)
- [sFlow \(Custom\) Sensor](#)^[860] (v7)
- [SFTP Secure File Transfer Protocol Sensor](#)^[868] (v12.x.6)

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [Share Disk Free Sensor](#)^[874] (v7)
- [SIP Options Ping Sensor](#)^[880] (v12.x.1)
- [SMTP Sensor](#)^[886] (v7)
- [SMTP&IMAP Round Trip Sensor](#)^[892] (v7)
- [SMTP&POP3 Round Trip Sensor](#)^[900] (v7)
- [SNMP APC Hardware Sensor](#)^[908] (v9.1.0)
- [SNMP Cisco ADSL Sensor](#)^[914] (v12.x.1)
- [SNMP Cisco ASA VPN Connections Sensor](#)^[919] (v12.x.1)
- [SNMP Cisco ASA VPN Traffic Sensor](#)^[924] (v12.x.1)
- [SNMP Cisco ASA VPN Users Sensor](#)^[929] (v12.x.5)
- [SNMP Cisco CBOoS Sensor](#)^[934] (v13.x.5)
- [SNMP Cisco System Health Sensor](#)^[939] (v12.x.4)
- [SNMP Cisco UCS Chassis Sensor](#)^[945] (v13.x.8)
- [SNMP Cisco UCS Physical Disk Sensor](#)^[951] (v14.1.10)
- [SNMP Cisco UCS System Health Sensor](#)^[957] (v13.x.8)
- [SNMP CPU Load Sensor](#)^[963] (v12.x.4)
- [SNMP Custom Sensor](#)^[968] (v7)
- [SNMP Custom String Sensor](#)^[975] (v9.1.0)
- [SNMP Dell Hardware Sensor](#)^[983] (v7)
- [SNMP Dell PowerEdge Physical Disk Sensor](#)^[989] (v12.x.4)
- [SNMP Dell PowerEdge System Health Sensor](#)^[995] (v12.x.4)
- [SNMP Disk Free Sensor](#)^[1001] (v12.x.4)
- [SNMP GSA System Health Sensor](#)^[1007] (v13.x.5)
- [SNMP Hardware Status Sensor](#)^[1012] (v13.x.5)
- [SNMP HP LaserJet Hardware Sensor](#)^[1017] (v9.1.0)
- [SNMP HP ProLiant Logical Disk Sensor](#)^[1023] (v12.x.6)
- [SNMP HP ProLiant Memory Controller Sensor](#)^[1029] (v12.x.6)
- [SNMP HP ProLiant Network Interface Sensor](#)^[1035] (v12.x.4)
- [SNMP HP ProLiant Physical Disk Sensor](#)^[1041] (v12.x.6)
- [SNMP HP ProLiant System Health Sensor](#)^[1047] (v12.x.4)
- [SNMP IBM System X Logical Disk Sensor](#)^[1053] (v13.x.4)
- [SNMP IBM System X Physical Disk Sensor](#)^[1059] (v13.x.4)
- [SNMP IBM System X Physical Memory Sensor](#)^[1065] (v13.x.4)
- [SNMP IBM System X System Health Sensor](#)^[1071] (v13.x.4)

- [SNMP interSeptor Pro Environment Sensor](#)^[1077] (v14.1.10)
- [SNMP LenovoEMC Physical Disk Sensor](#)^[1083] (v13.x.8)
- [SNMP LenovoEMC System Health Sensor](#)^[1089] (v13.x.8)
- [SNMP Library Sensor](#)^[1094] (v7)
- [SNMP Linux Disk Free Sensor](#)^[1102] (v8.1.0)
- [SNMP Linux Load Average Sensor](#)^[1110] (v8.1.0)
- [SNMP Linux Meminfo Sensor](#)^[1115] (v8.1.0)
- [SNMP Linux Physical Disk Sensor](#)^[1120] (v13.x.5)
- [SNMP Memory Sensor](#)^[1128] (v12.x.4)
- [SNMP NetApp Disk Free Sensor](#)^[1134] (v12.x.3)
- [SNMP NetApp Enclosure Sensor](#)^[1140] (v12.x.4)
- [SNMP NetApp I/O Sensor](#)^[1146] (v12.x.3)
- [SNMP NetApp License Sensor](#)^[1152] (v12.x.4)
- [SNMP NetApp Logical Unit Sensor](#)^[1158] (v13.x.7)
- [SNMP NetApp Network Interface Sensor](#)^[1164] (v12.x.3)
- [SNMP NetApp System Health Sensor](#)^[1170] (v12.x.3)
- [SNMP Poseidon Environment Sensor](#)^[1176] (v13.x.5)
- [SNMP QNAP Logical Disk Sensor](#)^[1181] (v13.x.4)
- [SNMP QNAP Physical Disk Sensor](#)^[1186] (v13.x.4)
- [SNMP QNAP System Health Sensor](#)^[1192] (v13.x.4)
- [SNMP RMON Sensor](#)^[1197] (v12.x.1)
- [SNMP SonicWALL System Health Sensor](#)^[1203] (v13.x.5)
- [SNMP SonicWALL VPN Traffic Sensor](#)^[1208] (v13.x.6)
- [SNMP Synology Logical Disk Sensor](#)^[1214] (v13.x.4)
- [SNMP Synology Physical Disk Sensor](#)^[1219] (v13.x.4)
- [SNMP Synology System Health Sensor](#)^[1224] (v13.x.4)
- [SNMP System Uptime Sensor](#)^[1229] (v7)
- [SNMP Traffic Sensor](#)^[1234] (v7)
- [SNMP Trap Receiver Sensor](#)^[1241] (v7)
- [SNMP Windows Service Sensor](#)^[1250] (v13.x.8)
- [SNTP Sensor](#)^[1255] (v8.1.0)
- [SSH Disk Free Sensor](#)^[1260] (v8.1.0)
- [SSH INodes Free Sensor](#)^[1269] (v8.1.1)
- [SSH Load Average Sensor](#)^[1275] (v8.1.0)

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [SSH Meminfo Sensor](#)¹²⁸¹ (v8.1.0)
- [SSH Remote Ping Sensor](#)¹²⁸⁷ (v12.x.1)
- [SSH SAN Logical Disk Sensor](#)¹²⁹⁴ (v14.1.9)
- [SSH SAN Physical Disk Sensor](#)¹³⁰¹ (v14.1.9)
- [SSH SAN System Health Sensor](#)¹³⁰⁸ (v14.1.9)
- [SSH Script Sensor](#)¹³¹⁵ (v12.x.1)
- [SSH Script Advanced Sensor](#)¹³²⁴ (v12.x.6)
- [SSH VMWare ESX\(i\) Disk Sensor](#)¹³³² (v8.2.0)
- [Syslog Receiver Sensor](#)¹³³⁸ (v7)
- [System Health Sensor](#)¹³⁴⁷ (v9.1.0)
- [TFTP Sensor](#)¹³⁵¹ (v8.1.0)
- [Traceroute Hop Count Sensor](#)¹³⁵⁷ (v8.3.0)
- [Virtuozzo Container Disk Sensor](#)¹³⁶³ (v8.2.1)
- [Virtuozzo Container Network Sensor](#)¹³⁶⁹ (v8.2.1)
- [VMware Host Hardware \(WBEM\) Sensor](#)¹³⁷⁵ (v8.1.0)
- [VMware Host Hardware Status \(SOAP\) Sensor](#)¹³⁸¹ (v12.x.1)
- [VMware Host Performance \(SOAP\) Sensor](#)¹³⁸⁷ (v12.x.1)
- [VMware Virtual Machine \(SOAP\) Sensor](#)¹³⁹³ (v7)
- [WBEM Custom Sensor](#)¹⁴⁰⁰ (v8.1.0)
- [Windows CPU Load Sensor](#)¹⁴⁰⁶ (v7)
- [Windows IIS 6.0 SMTP Received Sensor](#)¹⁴¹² (v8.1.0)
- [Windows IIS 6.0 SMTP Sent Sensor](#)¹⁴¹⁸ (v8.1.0)
- [Windows IIS Application Sensor](#)¹⁴²⁴ (v12.x.1)
- [Windows Last Update Sensor](#)¹⁴³¹ (v8.3.0)
- [Windows Logged In Users Sensor](#)¹⁴³⁷ (v8.3.0)
- [Windows MSMQ Queue Length Sensor](#)¹⁴⁴³ (v8.3.0)
- [Windows Network Card Sensor](#)¹⁴⁵⁰ (v7)
- [Windows Pagefile Sensor](#)¹⁴⁵⁷ (v12.x.4)
- [Windows Physical Disk Sensor](#)¹⁴⁶³ (v9.1.0)
- [Windows Print Queue Sensor](#)¹⁴⁷⁰ (v8.3.0)
- [Windows Registry Sensor](#)¹⁴⁷⁶ (v9.1.0)
- [Windows Scheduled Task Sensor](#)¹⁴⁸⁴ (v9.1.1)
- [Windows System Uptime Sensor](#)¹⁴⁹¹ (v8.1.0)
- [Windows Updates Status \(Powershell\) Sensor](#)¹⁴⁹⁷ (v13.x.6)

- [WMI Custom Sensor](#)  (v7)
- [WMI Custom String Sensor](#)  (v12.x.4)
- [WMI Event Log Sensor](#)  (v7)
- [WMI Exchange Server Sensor](#)  (v7.1.1)
- [WMI Exchange Transport Queue Sensor](#)  (v12.x.1)
- [WMI File Sensor](#)  (v7)
- [WMI Free Disk Space \(Multi Drive\) Sensor](#)  (v7)
- [WMI HDD Health Sensor](#)  (v12.x.1)
- [WMI Logical Disk Sensor](#)  (v7)
- [WMI Memory Sensor](#)  (v7)
- [WMI Microsoft SQL Server 2005 Sensor](#)  (v8.1.0)
- [WMI Microsoft SQL Server 2008 Sensor](#)  (v8.1.0)
- [WMI Microsoft SQL Server 2012 Sensor](#)  (v12.x.6)
- [WMI Process Sensor](#)  (v7)
- [WMI Remote Ping Sensor](#)  (v12.x.1)
- [WMI Security Center Sensor](#)  (v9)
- [WMI Service Sensor](#)  (v7)
- [WMI Share Sensor](#)  (v8.1.0)
- [WMI SharePoint Process Sensor](#)  (v12.x.1)
- [WMI Terminal Services \(Windows 2008\) Sensor](#)  (v8.1.0)
- [WMI Terminal Services \(Windows XP/Vista/2003\) Sensor](#)  (v8.1.0)
- [WMI UTC Time Sensor](#)  (v9.2.0)
- [WMI Vital System Data \(V2\) Sensor](#)  (v7)
- [WMI Volume Sensor](#)  (v7)
- [WMI Volume Fragmentation Sensor](#)  (v13.x.8)
- [WMI Windows Version Sensor](#)  (v8.3.0)
- [WSUS Statistics Sensor](#)  (v9.1.0)

More

Did not find what you are looking for? Have a look into the [Additional Sensor Types \(Custom Sensors\)](#)  section.

6.8.2 Active Directory Replication Errors Sensor

The Active Directory Replication Errors sensor uses its parent device's Windows credentials to check domain controllers for replication errors. It can show the number of consecutive sync failures, if the source is deleted, if the scheduled sync is disabled, when the last sync attempt took place, the result of the last sync, when there was the last sync success, the number of modified consecutive sync failures, and the number of pending replication operations.

Please make sure you enter valid domain credentials in the parent device's settings.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)^[2001].

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Requirement: Member of Windows Domain

This sensor only works if the computer running the PRTG probe is part of the domain whose AD should be monitored. The probe runs either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If this requirement is not met, the sensor will fail.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Note: Your Windows credentials may not contain any double quotation marks ("). If they do, this sensor will not work!

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor replications, PRTG will create one sensor for each replication neighbor you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Replication Neighbor	Select the replication neighbor whose replication you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
2 Active Directory Replication Errors Sensor

Sensor Settings	
Replication Neighbor	Shows the replication neighbor whose replication this sensor monitors. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration settings.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.3 ADO SQL Sensor

The ADO SQL sensor monitors a database using an ActiveX Data Objects (ADO) connection. It connects to the server and shows the response time. Additionally, it can read the number of records and a value.

Note: For security reasons, you can only create a sensor on a device for which Windows Credentials have been defined. With these credentials, the PRTG probe must be able to connect to the Windows domain. If you don't enter valid credentials, you will get an **Access denied** error message when scanning. For detailed information, please see [More](#)^[321] section below.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
3 ADO SQL Sensor

ADO Specific Data	
Connection String	Enter the string that will be used to connect to the database. For example, such a string could be: Provider=SQLOLEDB.1;Data Source=10.0.0.200\SQLEXPRESS;UserID=user;Password=userpass;Initial Catalog=Northwind . For more information on how to build connection strings, please see More 321 section below.
Data	
SQL Expression	Enter a valid SQL statement to execute on the server. In your SELECT statement, please specify the field name explicitly. Do not use SELECT * ! For example, a correct expression could be: SELECT AVG(UnitPrice) FROM Products . When a cursor is returned (i.e. with a SELECT statement), only the first row of data will be processed.
Record Count	If you want to know how many records in your database were affected by your SQL expression as defined above, you can count the number of concerned records. Choose between: ▪ Do not count number of records: Affected records will not be counted. ▪ Count number of records: The number of affected records will be counted. Note: Enabling this option might increase the execution time of this sensor.
Post-Processing	If the SQL expression returns a result set, please define if you want to further process it. Choose between: ▪ Ignore result set: Do not do anything with the data returned. ▪ Process numerical result: Regard the result set returned as integer or float. You can set the sensor to Warning or Down status for specific thresholds. Define below. ▪ Process string result: Regard the result set returned as a string. You can set the sensor to error for certain sub-strings contained or missing. Define below. ▪ Monitor for changes: Monitor if the result set has changed since last check. The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification 1690 whenever a sensor value changes.
Condition "Warning"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a Warning status. Choose between:

	▪ none: Do not set the sensor to Warning status for any condition. ▪ equals: Result set must be the same as the value provided below. ▪ is above: Result set must be above the value provided below. ▪ lower than: Result set must be below the value provided below. ▪ does not equal: Result set must be unequal to the value provided below. Note: This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings .
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor into a Warning status. Please enter an integer or float value.
Condition "Down"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a Down status. Choose between: ▪ none: Do not set the sensor to Down status for any condition. ▪ equals: Result set must be the same as the value provided below. ▪ is above: Result set must be above the value provided below. ▪ lower than: Result set must be below the value provided below. ▪ does not equal: Result set must be unequal to the value provided below. Note: This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings .
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor to a Down status. Please enter an integer value.
Response Must Include	This field is only visible if string results is enabled above. Enter a string that must be part of the returned SQL string. If it is not, the sensor will be set to an error state. Please enter a string or leave the field empty.
Response Must Not include	This field is only visible if string results is enabled above. Enter a string that must not be part of the returned SQL string. If it is, the sensor will be set to an error state. Please enter a string or leave the field empty.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

More

Knowledge Base: Monitoring (Almost) Any SQL Server Through ADO with PRTG Network Monitor

- <http://www.paessler.com/knowledgebase/en/topic/2053>

Knowledge Base: How do I correctly configure credentials for ADO SQL sensors?

- <http://www.paessler.com/knowledgebase/en/topic/13103>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.4 Amazon CloudWatch Sensor

The Amazon CloudWatch sensor monitors performance of Amazon Cloud services, such as Elastic Compute Cloud (EC2), Simple Queue Service (SQS), Elastic Load Balancing (ELB), Elastic Block Store (EBS), Simple Notification Service (SNS), Relational Database Service (RDS), and ElastiCache.

Depending on the selected service, the sensor can show CPU utilization, network load in and out, and disk read and write speed.

Note: The CloudWatch option must be enabled for the instance you want to monitor (you can do this, for example, using Amazon's AWS console). Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US\$ 0.014 per 1,000 requests (depending on your region). Please see [More](#)^[328] section for detailed information.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[202]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page:

Amazon Credentials	
Region	Select the region in which the instance to be monitored is running. The settings you make in this dialog are valid for all of the sensors that are created. Choose between: ▪ US East (Northern Virginia) ▪ US West (Oregon) ▪ US West (Northern California) ▪ EU (Ireland) ▪ Asia Pacific (Singapore) ▪ Asia Pacific (Tokyo) ▪ Asia Pacific (Sydney) ▪ South America (Sao Paulo) Note: The CloudWatch option must be enabled for the instance you want to monitor (you can do this e.g. using Amazon's AWS console).

Select which service instances you want to monitor. PRTG will create one sensor for each instance you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Amazon CloudWatch Specific	
Service Instance	Select the instances you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
4 Amazon CloudWatch Sensor

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Amazon Credentials	
AWS Access Key ID	Enter your access key. You can obtain it from aws.amazon.com .
AWS Secret Access Key	Enter your secret access key. You can obtain it from aws.amazon.com .
Region	Shows the region your instance is located at. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Amazon CloudWatch Specific	
Period (Interval)	Define in what granularity you want to receive datapoints from CloudWatch. Choose between: ▪ 1 Minute ▪ 2 Minutes ▪ 5 Minutes ▪ 10 Minutes ▪ 30 Minutes ▪ 1 Hour

Amazon CloudWatch Specific	
Service	Shows the service this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Instance	Shows the Instance ID of the Amazon Web Services instance this sensor is monitoring. When using the "Simple Notification Service (SNS)" service, this field is not visible. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Topic Name	This field is only visible if you selected a "Simple Notification Service (SNS)" instance before. It shows the topic name that is monitored by this sensor. The sensor will show the number and size of messages published, and the number of notifications delivered and failed. Each sensor can monitor one topic name only. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Availability Zone	This field is only visible if you selected a "Elastic Load Balancing (ELB)" instance before. Enter the name of the Availability Zone of your Load Balancer you want to monitor. If you leave this field empty, the average value of all zones will be taken.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 1683 settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Note: For Amazon CloudWatch sensors, the scanning interval cannot be inherited. Please use the individual settings of the sensor to define the interval in which data is received.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#). **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Maintenance Begins At

This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- <http://www.paessler.com/knowledgebase/en/topic/38083>

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- <http://www.paessler.com/knowledgebase/en/topic/37543>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.5 AVM FRITZ!Box WAN Interface Sensor

The AVM FRITZ!Box WAN Interface Sensor monitors the internet traffic of a FRITZ!Box internet access router from European manufacturer AVM. It returns the incoming and outgoing internet traffic.

Note: There are no credentials necessary, but transmission of status information via Universal Plug and Play (UPnP) must be enabled in the network settings of your FRITZ!Box. See [More](#)^[334] section below for detailed information.

Note: This sensor type might not support FRITZ!Boxes with firmware of **Kabel Deutschland**. Also, it might only support FRITZ!Boxes until operating system version 6.03. See section [More](#)^[334] below for details.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[202]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[168] settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[224] group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: How do I activate UPnP for my Fritz!Box?

- <http://www.paessler.com/knowledgebase/en/topic/38603>

Knowledge Base: FRITZ!Box Sensor shows 401

- <http://www.paessler.com/knowledgebase/en/topic/59909>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.6 Cisco IP SLA Sensor

The Cisco IP SLA sensor monitors Voice over IP (VoIP) network parameters using IP Service Level Agreement (SLA) from Cisco via Simple Network Management Protocol (SNMP). It shows different aspects provided by the queried device.

For a general introduction to the technology behind Quality of Service monitoring, please see [Monitoring Quality of Service](#)^[1939] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

IP SLA Specific	
IP SLAs	Select the IP SLAs you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head. The list options depend on the configuration of the queried device. If you're missing a type here, please check your device's configuration. PRTG can support the following operations: ▪ echo ▪ pathEcho ▪ fileIO ▪ script ▪ udpEcho ▪ tcpConnect ▪ http ▪ dns ▪ jitter ▪ dls ▪ dhcp ▪ ftp ▪ path-jitter

IP SLA Specific

Note: Packet Loss values are summarized, but have no explicit channel for Source—Destination or Destination—Source values

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

IP SLA Specific

ID	These fields show SLA specific settings provided by the queried SLA device. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Type	
Name (Tag)	
Owner	
Frequency	

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1791. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.7 Citrix XenServer Host Sensor

The Citrix XenServer Host Sensor monitors a Xen host server via Hypertext Transfer Protocol (HTTP). It shows CPU, memory, and network usage, as well as the number of running virtual machines and load average.

Note: The parent device must be a Citrix XenServer (version 5.0 or later).

For this sensor type credentials for Xen servers must be defined for the device you want to use the sensor on.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Monitoring a XenServer Pool

In a XenServer pool there is one "pool master" that manages the pool. Incoming queries on any host are automatically forwarded to the pool master. If you want to monitor your virtual machines, or host servers, simply create respective sensors on a device that represents **one** host server of your pool. Internal processes will make sure that monitoring will take place and continue independently from the physical host. **Note:** In PRTG's device tree, the sensors for virtual machines will always remain on the host you originally created it on, also if it is currently running on a different host.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

If you select more than one host, multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Host Settings

Host	Select the hosts you want to add a sensor for, including the ones that are not running. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Host Settings

UUID	Shows the Universally Unique Identifier (UUID) of the host monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the host monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.8 Citrix XenServer Virtual Machine Sensor

The Citrix XenServer Virtual Machine Sensor monitors a virtual machine on a Xen server via Hypertext Transfer Protocol (HTTP). It shows CPU usage and free memory in percent.

Note: The parent device must be a Citrix XenServer (version 5.0 or later).

For this sensor type credentials for Xen servers must be defined for the device you want to use the sensor on.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[220]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Monitoring a XenServer Pool

In a XenServer pool there is one "pool master" that manages the pool. Incoming queries on any host are automatically forwarded to the pool master. If you want to monitor your virtual machines, or host servers, simply create respective sensors on a device that represents **one** host server of your pool. Internal processes will make sure that monitoring will take place and continue independently from the physical host. **Note:** In PRTG's device tree, the sensors for virtual machines will always remain on the host you originally created it on, also if it is currently running on a different host.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Note: PRTG requests a full list of all virtual machines configured on the device. Therefore, it may take a few seconds before the dialog is loaded.

If you select more than one virtual machine, multiple sensors are created at once in the **Add Sensor** dialog. The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Virtual Machine Settings

Virtual Machine	Select the Virtual Machine (VM) you want to add a sensor for, including the ones that are not running. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Virtual Machine Settings

UUID	Shows the Universally Unique Identifier (UUID) of the virtual machine. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the virtual machine. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.9 Cluster Probe Health Sensor

The Cluster Probe Health sensor is a system device indicating PRTG's own system health status. It is created automatically with a PRTG cluster installation and cannot be deleted. It measures various internal system parameters of the cluster system and the probe's internal processes and then computes a resulting value. Frequent or repeated health values below 100 % should be investigated, please check the sensor's channels for details.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.10 Core Health Sensor

The Core Health sensor monitors internal PRTG parameters. It shows the state of the PRTG core server. It is created automatically by PRTG and cannot be deleted. This sensor type checks various parameters of your PRTG core which have an impact on the stability of the system:

- **Health:** This index value sums up the core state into a value between 100% (healthy) and 0% (failing). Frequent or repeated health values below 100% should be investigated.
- **CPU Load:** This channel shows the current percentage CPU load. Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value usually should stay below 50%.
- **Handles:** This is a counter for the data structures of the operating system. It is responsible for internal resource management. Repeated obviously increasing values should be investigated.
- **Committed Memory:** This channel shows the amount of memory committed to the PRTG core server as reported by the memory manager.
- **Free Page File Memory:** This channel shows the amount of free page file memory currently available on the system. Page file memory is aggregated RAM and the size of page file. It is the maximum amount of memory that is available on the system to be used for all currently running processes. If it gets too low the system can crash, at least some applications will throw "Out of memory" errors.
- **Free Physical Memory:** This channel shows the amount of free physical memory currently available on the system. This is the RAM that is physically built-in in the computer. If it gets too low the system will become very slow and PRTG is not usable in a reasonable way anymore. It can happen that some sensors will not be displayed correctly in that case, they will appear disabled (grayed out).
- **Free Virtual Memory:** This channel shows the accessible address space on the system for PRTG. PRTG cannot use more memory than reported here, independently from free page file and physical memory. On a 32bit OS (operating system) the maximum is 2 GB (3 GB with special settings under Windows); on a 64bit OS it is 4 GB if PRTG is running as 32bit version, and unlimited as 64bit version (only Core). If free virtual memory gets too low, PRTG will throw "Out of memory" errors or the message "not enough storage to process this command" (visible in the Core log).
- **Threads:** This channel shows the number of program parts which are currently running simultaneously. This number can increase with heavy load. The number should not exceed 100 in normal operation.

This sensor can be set up on a Probe Device only!

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[100] settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)⁹⁴.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.11 Dell PowerVault MDi Sensor

The Dell PowerVault MDi sensor monitors a virtual disk on a Dell PowerVault MD3000i, MD3620i, MD3000f, or MD3620f. It may work with additional models, too. This sensor can show current, maximum, and total IOs, current and maximum speed, as well as read and cache hit percentages.

Requirement: Dell Modular Disk Storage Manager

This sensor requires an installation of Dell's "Modular Disk Storage Manager" program. This has to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. For details about setup, please see [More](#)^[366] section below.

Note: Please create this sensor on a device which has the SAN's IP address configured in the "IP address/DNS name" field.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

If you select more than one disk, multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Virtual Disks	Select the disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ¹⁶⁸⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings

Virtual Disk	Shows the name of the virtual disk monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).

Sensor Display

Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

More

Where do I find the Dell PowerVault Modular Disk Storage Manager for use with my MDi SAN?

- <http://www.paessler.com/knowledgebase/en/topic/38743>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁹ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.12 DHCP Sensor

The DHCP sensor monitors a Dynamic Host Configuration Protocol (DHCP) server. It sends a broadcast message to the network and waits for a DHCP server to respond. If a server responds, the sensor shows both the address of the server and the offered IP in the sensor's **Message** field. You can check the server's response using [Regular Expressions](#)^[220]. The sensor's channels include response time (msec) and the lease time given by the server (in days).

This sensor can be set up on a Probe Device only! On sensor creation, choose the network card on the probe system which will be used to send the broadcast message.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor DHCP servers, PRTG will create one sensor for each network interface you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

DHCP Specific

Specify Network Interface

Select the network adapters you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name

Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
DHCP Specific	
MAC	Shows the MAC address of the network adapter that is used to send the broadcast message to the network. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Client IP	Specify if you want to check the returned client IP with a regular expression. Choose between: ▪ Don't check: The IP will only appear in the sensor message without further processes. ▪ Check: Enter the regular expression you want to use below.
Client IP Must Include	This field will only appear if you chose to check the client IP above. In the response of the DHCP server, search using a regular expression. If the answer for the client IP does not contain the defined string, the sensor will change to a Down status. For example, enter 10\0\5\.* to make sure any answering DHCP server returns an client IP address starting with "10.0.5.". If it doesn't, the sensor will show an error. For more details, see Regular Expressions ^[2010] section. Leave empty to not use this field.
Client IP Must Not Include	This field will only appear if you chose to check the client IP above. In the response of the DHCP server, search using a regular expression. If the answer for the client IP contains the defined string, the sensor will change to a Down status. See example above. For more details, see Regular Expressions ^[2010] section. Leave empty to not use this field.
Server IP	Specify if you want to check the returned server IP with a regular expression. Choose between:

DHCP Specific	
	▪ Don't check: The IP will only appear in the sensor message without further processes. ▪ Check: Enter the regular expression you want to use below.
Server IP Must Include	This field will only appear if you chose to check the server IP above. In the response of the DHCP server, search using a regular expression. If the answer for the server IP does not contain the defined string, the sensor will change to a Down status. See example above. For more details, see Regular Expressions^[2010] section. Leave empty to not use this field.
Server IP Must Not Include	This field will only appear if you chose to check the server IP above. In the response of the DHCP server, search using a regular expression. If the answer for the server IP contains the defined string, the sensor will change to a Down status. See example above. For more details, see Regular Expressions^[2010] section. Leave empty to not use this field.
Timeout (sec)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
DHCP Server Change	If there is more than one DHCP server in the network that may answer to the broadcast message, the sensor can receive an answer from a different DHCP server, compared to the last scan of the sensor. In this case, PRTG can write an entry to the system Logs^[146]. Choose between: ▪ Ignore: Do not write a log entry if the DHCP server changes. ▪ Write log entry: Write an entry to the system Logs whenever the DHCP server changes between two sensor scans. Note: Regardless of this setting, those entries will always be added to the sensor Log.
Offered IP Change	If the IP address offered by the DHCP server changes between two sensor scans, PRTG can write an entry to the system Logs^[146]. Choose between: ▪ Ignore: Do not write a log entry if the offered IP address changes. ▪ Write log entry: Write an entry to the system Logs whenever the DHCP server offers a different IP address compared to the last sensor scan. Note: Regardless of this setting, those entries will always be added to the sensor Log.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.13 DNS Sensor

The DNS sensor monitors a Domain Name Service (DNS) server. It resolves a domain name and compares it to a given IP address. The sensor shows the response time and goes to an error state if the DNS server does not resolve a given domain name correctly.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
DNS Specific	
Timeout (sec)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
13 DNS Sensor

DNS Specific	
Port	Enter the number of the port the sensor will try to connect to. This must be the port the sensor's parent device is running the DNS service on. Usually you will use port 53. We recommend using the default value. Note: The sensor will connect to the IP Address or DNS Name value of the device it is created on.
Domain	Enter the domain name that will be resolved by the sensor using the Domain Name Service (DNS) server specified in the sensor's parent device's settings. You can enter an internet domain name here (for example, example.com), or a DNS name in your internal network (such as computer-xyz); depending on the type of DNS server you will monitor. You can also enter an IP address here.
Query Type	Select the type of query that should be sent to the DNS server. Choose between: ▪ Host address IPv4 (A) ▪ Host address IPv6 (AAAA) ▪ Authoritative name server (NS) ▪ Start of a zone of authority marker (SOA) ▪ Domain name pointer (PTR) ▪ Mail exchange (MX) ▪ Canonical name for an alias (CNAME)
Check Result	Define if the result received from the DNS server will be checked. Choose between: ▪ Ignore result: Any valid answer of the DNS server will be accepted by the sensor. ▪ Check result: Check if the response contains certain strings. Define below.
Value	This field is only visible if result checking is enabled above. Enter elements that must be contained in the response of the DNS server. Enter each entry in one line. At least one of the elements must be contained in the received result. If none of the element matches the response, the sensor will show a red Down status. For example, you can enter an IP address here if your Domain field contains a host name. Only if the host name is resolved to the correct IP address your sensor will show a green Up status.
Write Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results.

DNS Specific

- **Write sensor result to disk (Filename: "Result of Sensor (ID).txt"):** Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see [Data Storage](#)^[2036] section.

Sensor Display**Primary Channel**

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. **Note:** You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.

Chart Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. **Note:** This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)^[1683] settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[224] group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁸ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.14 Enterprise Virtual Array Sensor

The Enterprise Virtual Array sensor monitors an HP StorageWorks Enterprise Virtual Array (EVA) using the `ssu.exe` from **HP Command View EVA Software**. It can show the status of several EVA modules, for example, status of system, controllers, enclosures, disks, disk groups, folders, hosts, snapshots, data replication, cabinets, and many more, depending on the available measurement components. If devices have measuring tools for fans and temperature, the corresponding data will be displayed as well.

For these EVA components, this sensor type can show the operational status, predicted failures, accessible media, allocation in percent, availability for VRaids in bytes, exaggerated bytes, group host access, the number of grouped and ungrouped disks, the age of snapshots, and the license status.

Note: You have to explicitly specify the credentials of the EVA in the sensor settings.

Important notice: This sensor is an experimental sensor. Currently, it is in **beta** status. The methods of operating can change at any time, as well as the available settings. **Do not expect** that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)^[200].

Requirement: Command View

The EVA sensor needs the HP Command View EVA Software to be installed on the probe system. If you do not want to install the whole command view tool, you can alternatively use another approach. For details, please see section [More](#)^[386].

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page:

EVA Credentials	
Scanning Mode	Specify the depth of the meta scan. Choose between: ▪ Basic: We recommend using this scanning mode. Various modules of your EVA will be available for monitoring.

EVA Credentials

- **Full Detail:** PRTG will scan for each disk of your EVA. Every disk will be listed in the module selection.

Select which modules you want to monitor. PRTG will create one sensor for each module you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

EVA Settings**Modules**

Select the modules you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings**Sensor Name**

Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Tags

Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. Those are not visible here.

Priority

Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

EVA Credentials	
Username	Enter the username for the EVA.
Password	Enter the password for the EVA.

EVA Settings	
Module	Shows the monitored module. You can adjust this setting if the module was renamed or moved to another folder. This way, PRTG can find the module again and the monitoring history will not be lost.
System	Shows further information about the monitored module. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Module Type	
Description	
Sensor Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage 2036 section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.
Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹². Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

HP Command View EVA Software

- <http://www8.hp.com/us/en/products/storage-software/product-detail.html?oid=471497>

Knowledge Base: Do I really have to install the whole Command View on the probe to use the EVA sensor?

- <http://www.paessler.com/knowledgebase/en/topic/55983>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.15 Event Log (Windows API) Sensor

The Event Log (Windows API) sensor monitors Event Log entries using Windows Application Programming Interface (API). It shows the number of new records per second (speed).

You can set the sensor to a desired status individually according to a new event log entry. For details and how to find out the correct filter, see section [More](#)^[394].

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Windows API Event Log Specific

Log File	Specify the log file the sensor will monitor. The Windows event log provides several different log files which are shown below. Choose between: ▪ Application ▪ System ▪ Security ▪ Directory Service ▪ DNS Server ▪ File Replication Service

Filter Event Log Entries

Event Type	Specify the type of event that will be considered by this sensor. Other event type will not be processed. Choose between the following event types: ▪ Any ▪ Error ▪ Warning ▪ Information ▪ Security Audit Success ▪ Security Audit Failure
Filter by Source	Filter all received events for a certain event source. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • Off: Do not filter by event source. • On: Enable filtering by event source.
Match String (Event Source)	This field is only visible if filtering is enabled above. Enter a source from which the events are to come from. Only events from a source matching this string will be regarded, others ignored. Please enter a string.
Filter by ID	Filter all received events for a certain event ID. If enabled, only messages matching the defined value(s) will be considered by the sensor. Choose between: • Off: Do not filter by event ID.

Filter Event Log Entries	
	• On: Enable filtering by event ID.
Match Value (Event ID)	This field is only visible if filtering is enabled above. Enter one or more event IDs (comma separated) from which the events are to come from. Only events with an ID matching one of the values will be regarded. Please enter one integer value or more comma separated integer values.
Filter by Category	Filter all received events for a certain event category. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • Off: Do not filter by event category. • On: Enable filtering by event category.
Match String (Event Category)	This field is only visible if filtering is enabled above. Enter a category which the events are to have. Only events with a category matching this string will be regarded. Please enter a string.
Filter by Event User	Filter all received events for a certain event user. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • Off: Do not filter by event user. • On: Enable filtering by event user.
Match String (Event User)	This field is only visible if filtering is enabled above. Enter a user name which the event are to be assigned to. Only events with a user name matching this string will be regarded. Please enter a string.
Filter by Event Computer	Filter all received events for a certain event computer. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • Off: Do not filter by event computer. • On: Enable filtering by event computer.
Match String (Event Computer)	This field is only visible if filtering is enabled above. Enter a computer name which the events are to be assigned to. Only events with a computer name matching this string will be regarded. Please enter a string.
Filter by Event Message	Filter all received events for a certain event message. If enabled, only messages matching the defined value will be considered by the sensor. Choose between:

Filter Event Log Entries	
	• Off: Do not filter by event message. • On: Enable filtering by event message.
Match String (Event Message)	This field is only visible if filtering is enabled above. Enter a message which the event must contain. Only events with a message matching this string will be regarded. Please enter a string.

Note: The **Event Log (Windows API) Sensor** always performs a substring match. Please do not use any placeholder character. For example, enter **RAS** for any event source containing this string in partial or whole form.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

More

Knowledge Base: Event Log Sensors: Setting Correct Status and Source Filter

- <http://www.paessler.com/knowledgebase/en/topic/59803>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#) section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#) section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.16 Exchange Backup (Powershell) Sensor

The Exchange Backup (Powershell) sensor monitors backups of an Exchange server using Remote PowerShell. It shows several states of an Exchange database backup, for example, the last full backup, the last differential backup, and if currently a backup is running.

Note: The parent device for this sensor must be an Exchange server version 2010 or higher.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Requirement: Remote PowerShell and Remote Exchange Management Shell

This sensor type uses PowerShell commands. In order to monitor devices with this sensor, **Remote PowerShell** and **Remote Exchange Management Shell** have to be enabled on the server. Ensure that you have installed **PowerShell 2.0** or later on your probe machine. For more information, please see section **More** below.

Requirement: Fully Qualified Domain Name (FQDN)

In order to connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address. For more information, please see section **More** below.

Requirement: Elevated Rights

The user of this sensor needs elevated rights on the Exchange system. It is not sufficient to have administrator rights. Please see section **More** below for detailed information on rights management.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor backups of Exchange server databases, PRTG will create one sensor for each database you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings

Exchange Databases to be monitored on this server

Select the databases you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name

Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Tags

Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically [inherited](#)^[89] from objects further up in the device tree. Those are not visible here.

Priority

Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings

Database

Shows the name of the monitored database. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Result

Define what will be done with the results the sensor receives. Choose between:

- **Discard sensor result:** Do not store the results.

Sensor Settings

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see [Data Storage](#)^[2036] section.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[1683] settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[224] group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- <http://www.paessler.com/knowledgebase/en/topic/54353>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <http://www.paessler.com/knowledgebase/en/topic/44453>

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- <http://www.paessler.com/knowledgebase/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <http://www.paessler.com/knowledgebase/en/topic/59745>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.17 Exchange Database (Powershell) Sensor

The Exchange Database (Powershell) sensor monitors database information of an Exchange server using Remote PowerShell. It shows several states of an Exchange database, for example, its size, if the database is mounted, and if the database is recognized as valid.

Note: The parent device for this sensor must be an Exchange server version 2010 or higher.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Requirement: Remote PowerShell and Remote Exchange Management Shell

This sensor type uses PowerShell commands. In order to monitor devices with this sensor, **Remote PowerShell** and **Remote Exchange Management Shell** have to be enabled on the server. Ensure that you have installed **PowerShell 2.0** or later on your probe machine. For more information, please see section **More** below.

Requirement: Fully Qualified Domain Name (FQDN)

In order to connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address. For more information, please see section **More** below.

Requirement: Elevated Rights

The user of this sensor needs elevated rights on the Exchange system. It is not sufficient to have administrator rights. Please see section **More** below for detailed information on rights management.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor databases of an Exchange server, PRTG will create one sensor for each database you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Exchange Databases to be monitored on this server	Select the databases you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Database	Shows the name of the monitored database. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
AutoRemount Database	Define if you want the sensor to try to remount the database automatically if it is unmounted. Choose between: ▪ Try to remount ▪ Just report the current reading, keep unmounted if so

Sensor Settings	
Sensor Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage^[2036] section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[1685] settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[224] group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- <http://www.paessler.com/knowledgebase/en/topic/54353>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <http://www.paessler.com/knowledgebase/en/topic/44453>

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- <http://www.paessler.com/knowledgebase/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <http://www.paessler.com/knowledgebase/en/topic/59745>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.18 Exchange Mailbox (Powershell) Sensor

The Exchange Mailbox (Powershell) sensor monitors mailboxes of an Exchange server using Remote PowerShell. It shows several states of a mailbox, for example, total size of items, the number of items, and the time of the last login.

Note: The parent device for this sensor must be an Exchange server version 2010 or higher.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Requirement: Remote PowerShell and Remote Exchange Management Shell

This sensor type uses PowerShell commands. In order to monitor devices with this sensor, **Remote PowerShell** and **Remote Exchange Management Shell** have to be enabled on the server. Ensure that you have installed **PowerShell 2.0** or later on your probe machine. For more information, please see section **More** below.

Requirement: Fully Qualified Domain Name (FQDN)

In order to connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address. For more information, please see section **More** below.

Requirement: Elevated Rights

The user of this sensor needs elevated rights on the Exchange system. It is not sufficient to have administrator rights. Please see section **More** below for detailed information on rights management.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor mailboxes of Exchange servers, PRTG will create one sensor for each mailbox you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Mailboxes to be monitored	Select the mailboxes you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Mailbox Name	Shows the name of the monitored mailbox. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results.

Sensor Settings	
	▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage^[2036] section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[1683] settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[224] group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- <http://www.paessler.com/knowledgebase/en/topic/54353>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <http://www.paessler.com/knowledgebase/en/topic/44453>

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- <http://www.paessler.com/knowledgebase/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <http://www.paessler.com/knowledgebase/en/topic/59745>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.19 Exchange Mail Queue (Powershell) Sensor

The Exchange Mail Queue (Powershell) sensor monitors the number of items in the outgoing mail queue of an Exchange server using Remote PowerShell. It shows, for example, queued mails, retrying mails, unreachable mails, and poisonous mails. See section [More](#)^[422] below for an explanation of the transport queue types.

Note: The parent device for this sensor must be an Exchange server version 2010 or higher.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Requirement: Remote PowerShell and Remote Exchange Management Shell

This sensor type uses PowerShell commands. In order to monitor devices with this sensor, **Remote PowerShell** and **Remote Exchange Management Shell** have to be enabled on the server. Ensure that you have installed **PowerShell 2.0** or later on your probe machine. For more information, please see section **More** below.

Requirement: Fully Qualified Domain Name (FQDN)

In order to connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address. For more information, please see section **More** below.

Requirement: Elevated Rights

The user of this sensor needs elevated rights on the Exchange system. It is not sufficient to have administrator rights. Please see section **More** below for detailed information on rights management.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor message queues of Exchange servers, PRTG will create one sensor for each role you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Hub-Transport or Edge-Server	Select the roles you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Sensor Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage^[2036] section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁹⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1793. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- <http://www.paessler.com/knowledgebase/en/topic/54353>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <http://www.paessler.com/knowledgebase/en/topic/44453>

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- <http://www.paessler.com/knowledgebase/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <http://www.paessler.com/knowledgebase/en/topic/59745>

Knowledge Base: Types of Transport Queues in Microsoft Exchange

- <http://www.paessler.com/knowledgebase/en/topic/55413>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁰ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹¹ section.

6.8.20 Exchange Public Folder (Powershell) Sensor

The Exchange Public Folder (Powershell) sensor monitors public folders of an Exchange server using Remote PowerShell. It shows several states of a public folder, for example, its total size, the number of items, and the time of the last access.

Note: The parent device for this sensor must be an Exchange server version 2010 or higher.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Requirement: Remote PowerShell and Remote Exchange Management Shell

This sensor type uses PowerShell commands. In order to monitor devices with this sensor, **Remote PowerShell** and **Remote Exchange Management Shell** have to be enabled on the server. Ensure that you have installed **PowerShell 2.0** or later on your probe machine. For more information, please see section **More** below.

Requirement: Fully Qualified Domain Name (FQDN)

In order to connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address. For more information, please see section **More** below.

Requirement: Elevated Rights

The user of this sensor needs elevated rights on the Exchange system. It is not sufficient to have administrator rights. Please see section **More** below for detailed information on rights management.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor public folders of Exchange servers, PRTG will create one sensor for each folder you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Public Folder	Select the folders you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Public Folder	Shows the name of the monitored folder. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results.

Sensor Settings	
	▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage^[2036] section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[1683] settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[224] group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- <http://www.paessler.com/knowledgebase/en/topic/54353>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <http://www.paessler.com/knowledgebase/en/topic/44453>

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- <http://www.paessler.com/knowledgebase/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <http://www.paessler.com/knowledgebase/en/topic/59745>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.21 EXE/Script Sensor

The EXE/Script sensor runs an executable file (EXE, DLL) or a script (batch file, VBScript, Powershell) on the computer running the local or remote probe. This option is provided as part of PRTG's Application Programming Interface (API). The sensor shows the execution time, and can show one value returned by the executable file or script (in one channel only). For details about the return value format please see the [Application Programming Interface \(API\) Definition](#)¹⁹⁹³.

Note: The executable or script file must be stored on the system of the probe the sensor is created on: If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.

Note: If you want to execute a custom Windows Management Instrumentation Query Language (WQL) script, please use the [WMI Custom Sensor](#)¹⁵⁰⁸.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Script	Select an executable file from the list. It will be executed with every scanning interval. In this list, files in the corresponding /Custom Sensors/EXE sub-directory of the probe system's PRTG program directory are shown (see Data Storage²⁰³⁶). In order for the files to appear in this list, please store them into this folder. Store files ending in BAT, CMD, DLL, EXE, PS1, and VBS. In order for the sensor to show the expected values and sensor status, your files must use the right format for the returned values (in this case, value:message to standard output). The file's exitcode will determine the sensor status. For detailed information on how to build custom sensors and for the expected return format, please see the API documentation (Application Programming Interface (API) Definition¹⁹⁹³). There, find detailed information the the "Custom Sensors" tab. Note: Please do not use the folder \Custom Sensors\Powershell Scripts to store your files. This remnant from previous software versions is not used any more and may usually be deleted. Note: When using custom sensors on the Cluster Probe, please copy your files to every cluster node installation.
Value Type	Define what kind of values your executable or script file gives back. Choose between: ▪ Integer: An integer is expected as return value. If the script gives back a float, PRTG will display the value 0. ▪ Float: A float is expected as return value, with a dot (.) between pre-decimal position and decimal places. In this setting, the sensor will also display integer values unless they don't produce a buffer overflow. ▪ Counter: Your script returns an integer which increases. PRTG will show the difference between the values of two sensor scans. Note: A counter must return an integer; float is not supported here!
Channel Name	Enter a name for the channel in which the returned values will be shown. This is for display purposes only. Please enter a string.
Unit String	Enter a string describing the unit of the returned values. This is for display purposes only. Please enter a string.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
EXE/Script	Shows the executable or script file that is executed with each sensor scan, as defined on sensor creation. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Parameters	If your executable or script file catches command line parameters, you can define them here. Placeholders can be used as well. For a full list of all placeholders please see the API documentation (Application Programming Interface (API) Definition). Note: Please make sure you write the placeholders in quotes to ensure that they are working properly if their values contain blanks. Use single quotation marks ' ' with PowerShell scripts, and double quotes " " with all others. Please enter a string or leave the field empty.
Environment	Choose if PRTG's command line parameters will also be available as environment parameters. ▪ Default Environment: Do not provide PRTG placeholders' values in the environment. Choose this secure option if you're not sure.

Sensor Settings	
	▪ Set placeholders as environment values: From within your executable or script, the values of PRTG's command line parameters will be available via environment variables. For example, you can then read and use the current host value of the PRTG device this EXE/script sensor is created on from within your script. This option can mean a security risk, because also credentials are provided in several variables. For a full list of all available variables please see the API documentation (Application Programming Interface (API) Definition¹⁹⁹³).
Security Context	Define the Windows user account that will be used to run the executable or script file. Choose between: ▪ Use security context of probe service: Run the selected file under the same Windows user account the probe is running on. By default, this is the Windows system user account (if not manually changed). ▪ Use Windows credentials of parent device: Use the Windows user account defined in the settings of the parent device this sensor is created on. Please go to sensor's parent device's settings to change these Windows credentials.
Mutex Name	Define any desired mutex name for the process. All EXE/Script sensors having the same mutex name will be executed serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running simultaneously. For links to more information, please see the More⁴³⁷ section below. Please enter a string or leave the field empty.
Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the external process is killed and an error message is triggered.
Value Type	Shows the expected value type, chosen on sensor creation. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Note: The sensor cannot handle string values.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: ▪ Ignore changes (default): No action will be taken on change. ▪ Trigger 'On Change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification¹⁶⁹⁰ whenever the sensor value changes.

Sensor Settings	
EXE Result	Define what will be done with the result the executable file gives back. Choose between: ▪ Discard EXE result: Do not store the requested web page. ▪ Write EXE result to disk: Store the last result received from the script with the file name "Result of Sensor [ID].txt" to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section. ▪ Write EXE result to disk in case of error: Store the last result received from the script only if the sensor is in a down status. The file name is "Result of Sensor [ID].txt" in the "Logs (Sensors)" directory. Enable this option if you do not want failures to be overwritten by a following success of the script.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window**Dependency Type**

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency.
- **Select object:** Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency.

Note: Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.

Dependency

This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the [object selector](#)^[158] to choose an object on which the current sensor will be dependent on.

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Information about custom scripts and executables

- [Application Programming Interface \(API\) Definition](#) 
- [Additional Sensor Types \(Custom Sensors\)](#) 

Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?

- <http://www.paessler.com/knowledgebase/en/topic/6673>

Knowledge Base: How and Where Does PRTG Store its Data?

- <http://www.paessler.com/knowledgebase/en/topic/463>

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- <http://www.paessler.com/knowledgebase/en/topic/11283>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)  section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)  section.

Others

For more general information about settings, please see [Object Settings](#)  section.

6.8.22 EXE/Script Advanced Sensor

The EXE/Script Advanced sensor runs an executable file (EXE, DLL) or a script (batch file, VBScript, Powershell) on the computer running the local or remote probe. This option is provided as part of PRTG's Application Programming Interface (API). The sensor shows the execution time, and can show values returned by the executable file or script in multiple channels. The return value of this sensor must be valid XML. For details about the return value format please see the [Application Programming Interface \(API\) Definition](#)^[1993].

Note: The executable or script file must be stored on the system of the probe the sensor is created on: If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.

Note: If you want to execute a custom Windows Management Instrumentation Query Language (WQL) script, please use the [WMI Custom Sensor](#)^[1509].

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
EXE/Script	Select an executable file from the list. It will be executed with every scanning interval. In this list, files in the corresponding /Custom Sensors/EXEXML sub-directory of the probe system's PRTG program directory are shown (see Data Storage ^[2036]). In order for the files to appear in this list, please store them into this folder. Store files ending in BAT, CMD, DLL, EXE, PS1, and VBS. In order for the sensor to show the expected values and sensor status, your files must return the expected XML format to standard output. Values and message must be embedded in the XML. For detailed information on how to build custom sensors and for the expected return format, please see the API documentation (Application Programming Interface (API) Definition ^[1993]). There, find detailed information the the "Custom Sensors" tab.

Sensor Settings

Note: Please do not use the folder `\Custom Sensors\Powershell Scripts` to store your files. This remnant from previous software versions is not used any more and may usually be deleted.

Note: When using custom sensors on the **Cluster Probe**, please copy your files to every cluster node installation.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings

EXE/Script	Shows the executable or script file that is executed with each sensor scan, as defined on sensor creation. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Settings	
Parameters	If your executable or script file catches command line parameters, you can define them here. Placeholders can be used as well. For a full list of all placeholders please see the API documentation (Application Programming Interface (API) Definition^[1993]). Note: Please make sure you write the placeholders in quotes to ensure that they are working properly if their values contain blanks. Use single quotation marks <code>'</code> with PowerShell scripts, and double quotes <code>"</code> with all others. Please enter a string or leave the field empty.
Environment	Choose if PRTG's command line parameters will also be available as environment parameters. ▪ Default Environment: Do not provide PRTG placeholders' values in the environment. Choose this secure option if you're not sure. ▪ Set placeholders as environment values: From within your executable or script, the values of PRTG's command line parameters will be available via environment variables. For example, you can then read and use the current host value of the PRTG device this EXE/script sensor is created on from within your script. This option can mean a security risk, because also credentials are provided in several variables. For a full list of all available variables please see the API documentation (Application Programming Interface (API) Definition^[1993]).
Security Context	Define the Windows user account that will be used to run the executable or script file. Choose between: ▪ Use security context of probe service: Run the selected file under the same Windows user account the probe is running on. By default, this is the Windows system user account (if not manually changed). ▪ Use Windows credentials of parent device: Use the Windows user account defined in the settings of the parent device this sensor is created on. Please go to sensor's parent device's settings to change these Windows credentials.
Mutex Name	Define any desired mutex name for the process. All EXE/Script sensors having the same mutex name will be executed serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running simultaneously. For links to more information, please see the More^[445] section below. Please enter a string or leave the field empty.
Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the external process is killed and an error message is triggered.

Sensor Settings	
EXE Result	Define what will be done with the results the executable file gives back. Choose between: ▪ Discard EXE result: Do not store the requested web page. ▪ Write EXE result to disk: Store the last result received from the script with the file name "Result of Sensor [ID].txt" to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section. ▪ Write EXE result to disk in case of error: Store the last result received from the script only if the sensor is in a down status. The file name is "Result of Sensor [ID].txt" in the "Logs (Sensors)" directory. Enable this option if you do not want failures to be overwritten by a following success of the script.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Note: The **Stack Unit** option for stacking graphs will only work if you explicitly define the same **<unit>** for at least two channels. For detailed information about sensor settings please see the API documentation ([Application Programming Interface \(API\) Definition](#) ¹⁹⁹³).

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window**Dependency Type**

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency.
- **Select object:** Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency.

Note: Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.

Dependency

This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the [object selector](#)^[158] to choose an object on which the current sensor will be dependent on.

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Information about custom scripts and executables

- [Application Programming Interface \(API\) Definition](#)¹⁹⁹³
- [Additional Sensor Types \(Custom Sensors\)](#)¹⁶⁸⁰

Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?

- <http://www.paessler.com/knowledgebase/en/topic/6673>

Knowledge Base: How and Where Does PRTG Store its Data?

- <http://www.paessler.com/knowledgebase/en/topic/463>

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- <http://www.paessler.com/knowledgebase/en/topic/11283>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³¹ section.

6.8.23 File Sensor

The File sensor monitors a file located on the probe's local disk, or a file accessible via Server Message Block (SMB). You can monitor file content and file time stamp changes. The sensor shows the file size, and a last modified value in days and hours.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Specific	
File Name	Enter the full path to the file this sensor will monitor. For example, enter C:\Windows\file.txt . If the file is located on a network device use the Uniform Naming Convention (UNC) path without the server part (you would only enter share\folder\file.txt). The server part (\server\) is taken from this sensor's parent device's settings. Please enter a valid path and file name. Note: In order to provide any shares, the LanmanServer "Server" Windows service must be running on the target computer.
Check If	Specify when the sensor will send an alert. Choose between: ▪ File exists: The sensor will send an alert if the file does not exist. ▪ File does not exist: The sensor will send an alert if the file exists.
Monitor File Content	Specify if the sensor will send a change notification when the content of the file changes (based on a checksum). Choose between: ▪ Ignore changes: No action will be taken on change. ▪ Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.
Monitor File Time Stamp	Specify if the sensor will send a change notification when the content of the file's time stamp changes. Choose between: ▪ Ignore changes: No action will be taken on change. ▪ Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

- <http://www.paessler.com/knowledgebase/en/topic/513>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.24 File Content Sensor

The File Content sensor checks a text file for certain strings and returns the line number of the last match and the number of total matches. Additionally, matching lines are quoted in the sensor message field.

Note: This sensor does **not** support UTF-16 encoded files! In this case, please try use a custom sensor like the [EXE/Script Sensor](#)^[430] or the [EXE/Script Advanced Sensor](#)^[439].

Note: This sensor supports Unix line feeds.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
File Name	Enter the full path to the file this sensor will monitor. For example, enter C:\Windows\file.txt. If the file is located on a network device use the Uniform Naming Convention (UNC) path without the server part (you would only enter share\folder\file.txt). The server part (\server\) is taken from this sensor's parent device's settings. Please enter a valid path and file name. Note: In order to provide any shares, the LanmanServer "Server" Windows service must be running on the target computer. Note: If you define a file on your network here, please be aware that this might produce high network traffic, because PRTG will query the entire file with every scanning interval.
Search String	Define the string inside the log file you would like to check for. The input is not case-sensitive. Please enter a string.
Search Method	Define the method you want to provide the search string with. The pattern must be contained in one line and only the last matching line will be given back. Choose between: ▪ Simple string search: Search for a simple string. ▪ Regular Expression: Search using a regular expression. For more details, see Regular Expressions 2010 section.
Warning Behaviour	Define under which condition the sensor will show a Warning status. Choose between: ▪ Go into warning status when string is not found: The sensor will show a Warning status if there is no match. Otherwise it will remain in Up status. ▪ Go into warning status when string is found: The sensor will show a Warning status if there is a match. Otherwise it will remain in Up status.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: ▪ Ignore changes: No action will be taken on change. ▪ Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification 1690 whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.25 Folder Sensor

The Folder sensor monitors a folder using Server Message Block (SMB). You can monitor file changes and file ages. It shows the folder size and file count, as well as the oldest and newest file value in days and hours.

Note: The Folder sensor counts all files in a folder, including **hidden files**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Folder Monitor	
Folder Name	Enter the full path to the folder this sensor will monitor. For example, enter C:\Windows . If the file is located on a network device, use the Uniform Naming Convention (UNC) path without the server part (you would only enter share\folder). The server part (\server\) is taken from this sensor's parent device's settings. Please enter a valid path name. Note: In order to provide any shares, the LanmanServer "Server" Windows service must be running on the target computer.
Sub-Folder Recursion	Specify if subfolders will be included in the monitoring. Choose between: • Do not recurse sub-folders: Only monitor the folder specified above; do not monitor its subfolders. • Monitor the folder and its sub-folders (use with caution!): Monitor the folder specified above and all of its subfolders. Note: Recursing sub-folders in large directories with a high number of branches may evoke timeout errors or performance issues.
Monitor Folder Changes	Specify if the sensor will send a change notification when the content of the folder changes. Choose between: • Ignore changes: Changes to the folder will not trigger a change notification. • Trigger 'On Change' notification: The sensor will trigger a change notification if a file changes its timestamp or filename, or if there are new or deleted files.
Check of File Ages	Specify if the sensor will monitor the folder for certain file ages. Choose between: • Don't check: Do not check for the age of the files in the specified folder(s). • Show Warning if older: Set the sensor to warning status if one of the files in the specified folder is older than a specific time unit. • Show Error if older: Set the sensor to error status if one of the files in the specified folder is older than a specific time unit. • Show Warning if younger: Set the sensor to warning status if one of the files in the specified folder is younger than a specific time unit. • Show Error if younger: Set the sensor to error status if one of the files in the specified folder is younger than a specific time unit.
File Age Limit	This field is only visible if a file age check is enabled above. Enter the age of a file in the folder that will trigger the sensor's status change if undershot respectively overrun. Please enter an integer value. The value will be interpreted as days, hours, or minutes; according to your setting below.
File Age Limit Unit	This field is only visible if a file age check is enabled above. Specify the unit for the file age value you entered above. Choose between:

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1791 . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

- <http://www.paessler.com/knowledgebase/en/topic/513>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.26 FTP Sensor

The FTP sensor monitors file servers using File Transfer Protocol (FTP) and FTP over SSL (FTPS). It shows the response time.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Sensor Specific	
Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered. The highest timeout supported is 900 seconds (15 minutes). Please enter an integer value.

Sensor Specific	
Port	Enter the number of the port the sensor will try to connect to. For non-secure connections usually port 21 is used, for implicit secure connections usually port 990 . Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
FTP Mode	Specify which FTP mode will be used for the connection. Choose between: ▪ Use active mode ▪ Use passive mode We recommend using the default value. If you do not get a connection, please try the passive mode.

Authentication	
Username	Enter a username for the FTP login. Please enter a string or leave the field empty.
Password	Enter a password for the FTP login. Please enter a string or leave the field empty.
TLS (Transport-Level-Security)	Specify if an encryption will be used for the connection. Choose between: ▪ Don't use SSL (Basic FTP, recommended): In most cases, you will use basic FTP without encryption. ▪ Use Explicit SSL/TLS if available: The sensor will try to connect via Explicit SSL. If SSL/TLS is not supported by the server, the sensor will try to connect without SSL/TLS and is set to Up if this works. If the server supports SSL/TLS but the connection fails (for example, due to a TLS handshake failure), the sensor will turn into Down status. ▪ Enforce Explicit SSL/TLS: The connection must be established using Explicit SSL/TLS. Otherwise, the sensor will go into Down status. ▪ Use Implicit SSL/TLS: The sensor will try to connect using Implicit SSL/TLS. Negotiating authentication and security is not allowed in implicit mode. The client is expected to challenge the FTP server with a TLS/SSL ClientHello message. If the server does not receive such a message, it will drop the connection. The sensor will go into Down status.

Authentication	
	Note: Ensure that you choose the method your FTP server uses! If your server uses Implicit SSL/TLS, the Explicit SSL/TLS connection will not work.
Sensor Result	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸⁵ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1688] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.27 FTP Server File Count Sensor

The FTP Server File Count sensor logs in to an FTP server and returns the number of files available in the directory listing.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Channel Name	Enter a name for the channel in which the returned values will be shown. This is for display purposes only. Please enter a string.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
FTP URL	Enter the URL to check (this sensor does not use the IP Address/DNS value of the parent device).
Username	Define the username for the login. Please enter a string.
Password	Define the password for the login. Please enter a string.
Count Only New Files	Define if only new files will be counted. Choose between: ▪ No: Always show the total number of files. ▪ Yes: Show the number of new files since the last scanning interval. Note: With the next sensor scan, any new files from the previous scan will be regarded as old.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: ▪ Ignore changes: No action will be taken on change. ▪ Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification^[1090] whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.28 Google Analytics Sensor

The Google Analytics sensor queries data from a Google Analytics account via Hypertext Transfer Protocol (HTTP). It shows the values for different metrics in different sensor channels.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
28 Google Analytics Sensor

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Google Analytics Settings

Period (Interval)	Enter how often the sensor will query data. Choose between: ▪ 1 Day ▪ 2 Days ▪ 3 Days ▪ 1 Week
Username	Please enter the username of the Google Analytics account you want to query. Please enter a string.
Password	Please enter the password of the Google Analytics account you want to query. Please enter a string.
Profile ID	Enter the 8-digits profile ID of the Google Analytics account. For help, please see More ⁴⁸² section below.
Metrics	Enter a comma separated list with all metrics you want to query. A default set of metrics is already predefined. For help, please see More ⁴⁸² section below.
Days	Define for how many days the sensor will query data. Enter 1 to query yesterday's data only, or define any number of days. Please enter an integer value.
Average	Define if the sensor will query averaged data. Select between: ▪ Use: Query averaged data. This setting only takes effect if your entered more than "1" in the Days setting above. Data will be averaged over the number of days. ▪ Don't use: Do not query averaged data, but receive raw data.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Note: For Google Analytics sensors, the scanning interval cannot be inherited. Please use the individual settings of the sensor to define the interval in which data is received.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration**Channel Unit Types**

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Proxy Settings for HTTP Sensors**HTTP Proxy Settings**

The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS. **Note:** This setting is valid for the monitoring only and determines the behavior of sensors. In order to change proxy settings for the core server, please see [System Administration—System and Website](#) ¹⁸¹¹.

Name

Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port

Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

User

If the proxy requires authentication, enter the username for the proxy login. **Note:** Only basic authentication is available! Please enter a string or leave the field empty.

Password

If the proxy requires authentication, enter the password for the proxy login. **Note:** Only basic authentication is available! Please enter a string or leave the field empty.

More

Knowledge Base: Where do I find my Google Analytics profile ID?

- <http://www.paessler.com/knowledgebase/en/topic/35363>

Knowledge Base: Where do I find available Google Analytics metrics?

- <http://www.paessler.com/knowledgebase/en/topic/35373>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[1441] section.

6.8.29 HTTP Sensor

The HTTP sensor monitors a web server using Hypertext Transfer Protocol (HTTP). It shows the loading time. This is the easiest way to monitor if a website (or a specific website element) is reachable.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
HTTP Specific	
Timeout (Sec.)	Enter a timeout in seconds for the HTTP request. If the reply takes longer than this value the request is aborted and an error message is triggered. The maximum value is 900 seconds (15 minutes).

HTTP Specific	
URL	Please enter the URL the sensor will connect to. If you enter an absolute URL, this address will be independent from the IP address/DNS name setting of the device this sensor is created on. You can enter an URL leading to a webpage (to measure the page source code's loading time), or enter the URL of an image or of another page asset to measure this element's availability and loading time. PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section Smart URL Replacement below.
Request Method	The request method determines how the given URL is requested. ▪ GET: Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page. ▪ POST: Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the Postdata field below. ▪ HEAD: Only request the HTTP header from the server; without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.
Postdata	This field is only visible when POST is selected in the Request Method setting above. Please enter the data part for the POST request here. Note: No XML is allowed here!
Content Type	This setting is only visible when POST is selected in the Request Method setting above. Define the content type of a POST request. Choose between: ▪ Default (application/x-www-form-urlencoded): This is the default content type used to encode the form data set for submission to the server. ▪ Custom: If you need another content type than default, enter this content type below.
Custom Content Type	This field is only visible when Custom is selected above. Define the content type which is needed, e.g., XML, JSON, HTTP.
SSL Specific	
SSL Method	This setting is relevant only when using https in the URL field. We recommend using the default value. If you experience connection problems, please select another SSL method from the list. Choose between:

SSL Specific	
	▪ SSL V2 ▪ SSL V2 or V3: This is the default setting. ▪ SSL V3 ▪ TLS V1 Note: Other TLS versions are not supported.

Note: This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Proxy Settings for HTTP Sensors

HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS. Note: This setting is valid for the monitoring only and determines the behavior of sensors. In order to change proxy settings for the core server, please see System Administration—System and Website ¹⁸¹¹ .
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either **http:///** or **https:///** or even a simple slash **/** as equivalent for **http:///**). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** **www.example.com** and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value **https:///** in the URL field, PRTG will automatically create the URL **https://www.example.com/** from that.
- Using the value **/help** in the URL field, PRTG will automatically create and monitor the URL **http://www.example.com/help**
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, **http://:8080/**

Note: Smart URL replacement does not work for sensors running on the "Probe Device".

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁹³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.30 HTTP Advanced Sensor

The HTTP Advanced sensor monitors the source code of a web page using Hypertext Transfer Protocol (HTTP). It supports authentication, content checks, and other advanced parameters. It shows the loading time, bytes received, download bandwidth (speed), and time to first byte.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
HTTP Specific	
Timeout (Sec.)	Enter a timeout in seconds for the HTTP request. If the reply takes longer than this value the request is aborted and an error message is triggered. The maximum value is 900 seconds (15 minutes).

HTTP Specific	
URL	Please enter the URL the sensor will connect to. If you enter an absolute URL, this address will be independent from the IP address/DNS name setting of the device this sensor is created on. You can enter an URL leading to a webpage (to measure the page source code's loading time), or enter the URL of an image or of another page asset to measure this element's availability and loading time. PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section Smart URL Replacement below.
Request Method	The request method determines how the given URL is requested. ▪ GET: Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page. ▪ POST: Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the Postdata field below. ▪ HEAD: Only request the HTTP header from the server; without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.
Postdata	This field is only visible when POST is selected in the Request Method setting above. Please enter the data part for the POST request here. Note: No XML is allowed here!
Content Type	This setting is only visible when POST is selected in the Request Method setting above. Define the content type of a POST request. Choose between: ▪ Default (application/x-www-form-urlencoded): This is the default content type used to encode the form data set for submission to the server. ▪ Custom: If you need another content type than default, enter this content type below.
Custom Content Type	This field is only visible when Custom is selected above. Define the content type which is needed, e.g., XML, JSON, HTTP.

HTTP Engine	
Monitoring Engine	If you encounter unexpected errors with the standard method that is used to monitor an URL, try to use the compatibility mode which is based on .Net (introduced in PRTG v13.x.7). Choose between:

HTTP Engine

- **Default/High Performance (recommended):** This is the default monitoring method for this sensor type.
- **Alternate/Compatibility Mode:** Try this method as an alternative for websites that do not work with the default approach. Using the compatibility mode, this sensor will execute an external **exe**. Thus, this method will need more resources, but it can be helpful in particular cases. **Note:** If you select the compatibility mode, the options for the SSL method will be slightly different. You can also check for trusted certificates. Please see below.
Note: When using the Compatibility Mode, **Smart URL Replacement** will not work, i.e., this sensor does **not** use the **IP Address/DNS value** of the parent device automatically then.

SSL Specific

SSL Method

This setting is relevant only when using https in the **URL** field. We recommend using the default value. If you experience connection problems, please select another SSL method from the list. Choose between:

- **SSL V2**
- **SSL V2 or V3:** This is the default setting.
- **SSL V3**
- **TLS V1**

Note: Other TLS versions are not supported.

SSL Specific (when using Compatibility Mode)

SSL Method

When using the compatibility mode, the SSL specific settings are a bit different to the default SSL settings. SSL V2 is not available. You can choose between:

- **SSL V3**
- **TLS V1**
- **SSL V3 or TLS V1:** This is the default setting.

Check SSL Certificates

Specify if the certificate of the monitored URL will be checked. Choose between:

- **Do not check used certificates:** This the default setting.

SSL Specific (when using Compatibility Mode)

- **Check if the used certificates are trusted:** If the certificate of the server is not trusted, the sensor will go into a **Down** status and display a corresponding message.

Note: This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

Advanced Sensor Data

Protocol Version	Define the HTTP protocol version that will be used when connecting to the URL. Choose between: ▪ HTTP 1.0 ▪ HTTP 1.1: This is the default setting.
User Agent	Choose which user agent string will be sent by this sensor when connecting to the URL defined above. Choose between: ▪ Use PRTG's Default String: Do not enter a specific user agent, use default setting. Usually, this is: Mozilla/5.0 (compatible; PRTG Network Monitor (www.paessler.com); Windows) ▪ Use a Custom String: Use a custom user agent. Define below.
Custom User Agent	This field is only visible if custom user agent is enabled above. Enter a string which will be used as user agent when connecting to the URL specified above.
Content Changes	Define what will be done in case the content of the monitored web page (element) changes. You can choose between: • Ignore changes: No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that the web page content has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the web page content changes.
Check For Existing Key Words (Positive)	Define whether the the result at the configured URL will be checked for keywords. Choose between: ▪ Disable: Do not search for keywords. ▪ Enable key word check (positive): In the result returned at the URL, check if a key word exists. Note: The content check is only intended for html websites and might not work with other target URLs.

Advanced Sensor Data	
Response Must Include	This field is only visible if keyword checking is enabled above. Define which string must be part of the source code at the given URL. You can either enter plain text or a Regular Expression ²⁰¹⁰ . If the data does not include the search pattern, the sensor will be set to an error state. Please enter a string.
For Key Word Search Use	Define in which format you have entered the search expression in the field above. ▪ Plain Text: Search for the string as plain text. The characters * and ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible with plain text search. ▪ Regular Expression: Treat the search pattern as a Regular Expression²⁰¹⁰.
Check For Existing Key Words (Negative)	Define whether the the result at the configured URL will be checked for keywords. Choose between: ▪ Disable: Do not search for keywords. ▪ Enable key word check (negative): In the result returned at the URL, check if a key word does not exist. Note: The content check is only intended for html websites and might not work with other target URLs.
Response must not include	This field is only visible if keyword checking is enabled above. Define which string must not be part of the source code at the given URL. You can either enter plain text or a Regular Expression ²⁰¹⁰ . If the data does include this string, the sensor will be set to an error state. Please enter a string.
For Key Word Search Use	Define in which format you have entered the search expression in the field above. ▪ Plain Text: Search for the string as plain text. The characters * and ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible with plain text search. ▪ Regular Expression: Treat the search pattern as a Regular Expression²⁰¹⁰.

Advanced Sensor Data	
Limit Download (kb)	Enter a maximum amount of data that will be transferred per every single request. If you set content checks, please be aware that only the content downloaded up to this limit can be checked for search expressions.
Result Handling	Define what will be done with the web page loaded at the given URL. Choose between: • Discard HTML result: Do not store the requested web page. • Store latest HTML result: Store the last result of the requested web page to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes, especially in combination with content checks. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage 2036 section.

Note: This sensor loads the source code at the given URL. If you set up a content check, only this source code is checked for the keywords. The code is not necessarily identical to the one used to display the page when opening the same URL in a web browser, as there may be a reload configured or certain information may be inserted after loading, e.g. via Javascript. PRTG does not follow links to embedded objects nor does it execute scripts. Only the first page at the given URL is loaded and checked against the expressions configured. For debugging, please use the **Result** option to write the source code file to disk and look up what exactly PRTG gets when calling the URL. If the URL configured does not point to a web page, but to a binary file, for example, to an image, you usually won't check for content.

Authentication	
Authentication	Define if the web page at the configured URL need authentication. Choose between: ▪ No authentication needed ▪ Web page needs authentication
User	This field is only visible if authentication is enabled above. Enter a username. Please enter a string.
Password	This field is only visible if authentication is enabled above. Enter a password. Please enter a string.
Authentication Method	This field is only visible if authentication is enabled above. Please select the authentication method the given URL is protected with. Choose between:

Authentication	
	• Basic access authentication (HTTP): Use simple HTTP authentication. This is the default setting and suitable for most cases. Note: This authentication method will transmit credentials as plain text! • Windows NT LAN Manager (NTLM): Use the Microsoft NTLM protocol for authentication. This is sometimes used in Intranets for single sign-on. We recommend using the default value.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Proxy Settings for HTTP Sensors	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS. Note: This setting is valid for the monitoring only and determines the behavior of sensors. In order to change proxy settings for the core server, please see System Administration—System and Website ¹⁸¹¹ .
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.
Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either **http:///** or **https:///** or even a simple slash **/** as equivalent for **http:///**). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** **www.example.com** and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value **https:///** in the URL field, PRTG will automatically create the URL **https://www.example.com/** from that.
- Using the value **/help** in the URL field, PRTG will automatically create and monitor the URL **http://www.example.com/help**
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, **http://:8080/**

Note: Smart URL replacement does not work for sensors running on the "Probe Device".

More

Knowledge Base: Which user agent should I use in the HTTP Advanced sensor's settings?

- <http://www.paessler.com/knowledgebase/en/topic/30593>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.31 HTTP Apache ModStatus PerfStats Sensor

The HTTP Apache ModStatus PerfStats sensor monitors performance statistics of an Apache web server using `mod_status` over HTTP. It can show the CPU load, the uptime (in seconds), the requests per second, the bytes per request, and the number of current busy and idle worker threads of the Apache at scan time.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
HTTP Specific	
Timeout (Sec.)	Enter a timeout in seconds for the HTTP request. If the reply takes longer than this value the request is aborted and an error message is triggered. The maximum value is 900 seconds (15 minutes).

HTTP Specific	
URL	Please enter the URL to the mod_status module on your Apache server; PRTG will append a <code>/server_status?auto</code> part automatically. If you enter an absolute URL, this address will be independent from the IP address/DNS name setting of the device this sensor is created on. PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section Smart URL Replacement below.

SSL Specific	
SSL Method	This setting is relevant only when using https in the URL field. We recommend using the default value. If you experience connection problems, please select another SSL method from the list. Choose between: ▪ SSL V2 ▪ SSL V2 or V3: This is the default setting. ▪ SSL V3 ▪ TLS V1 Note: Other TLS versions are not supported.

Note: This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

Authentication	
Authentication	Define if the web page at the configured URL need authentication. Choose between: ▪ No authentication needed ▪ Web page needs authentication
User	This field is only visible if authentication is enabled above. Enter a username. Please enter a string.
Password	This field is only visible if authentication is enabled above. Enter a password. Please enter a string.
Authentication Method	This field is only visible if authentication is enabled above. Please select the authentication method the given URL is protected with. Choose between:

Authentication	
	• Basic access authentication (HTTP): Use simple HTTP authentication. This is the default setting and suitable for most cases. Note: This authentication method will transmit credentials as plain text! • Windows NT LAN Manager (NTLM): Use the Microsoft NTLM protocol for authentication. This is sometimes used in Intranets for single sign-on. We recommend using the default value.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸⁵ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Proxy Settings for HTTP Sensors

HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS. Note: This setting is valid for the monitoring only and determines the behavior of sensors. In order to change proxy settings for the core server, please see System Administration—System and Website ¹⁸¹¹ .
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either **http:///** or **https:///** or even a simple slash **/** as equivalent for **http:///**). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** **www.example.com** and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value **https:///** in the URL field, PRTG will automatically create the URL **https://www.example.com/** from that.
- Using the value **/help** in the URL field, PRTG will automatically create and monitor the URL **http://www.example.com/help**
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, **http://:8080/**

Note: Smart URL replacement does not work for sensors running on the "Probe Device".

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.32 HTTP Apache ModStatus Totals Sensor

The HTTP Apache ModStatus Totals sensor monitors accesses and transferred data (in kBytes) of an Apache web server using mod_status over HTTP.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
HTTP Specific	
Timeout (Sec.)	Enter a timeout in seconds for the HTTP request. If the reply takes longer than this value the request is aborted and an error message is triggered. The maximum value is 900 seconds (15 minutes).

HTTP Specific	
URL	Please enter the URL to the mod_status module on your Apache server; PRTG will append a "/server_status?auto" part automatically. If you enter an absolute URL, this address will be independent from the IP address/DNS name setting of the device this sensor is created on. PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section Smart URL Replacement below.

SSL Specific	
SSL Method	This setting is relevant only when using https in the URL field. We recommend using the default value. If you experience connection problems, please select another SSL method from the list. Choose between: ▪ SSL V2 ▪ SSL V2 or V3: This is the default setting. ▪ SSL V3 ▪ TLS V1 Note: Other TLS versions are not supported.

Note: This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

Authentication	
Authentication	Define if the web page at the configured URL need authentication. Choose between: ▪ No authentication needed ▪ Web page needs authentication
User	This field is only visible if authentication is enabled above. Enter a username. Please enter a string.
Password	This field is only visible if authentication is enabled above. Enter a password. Please enter a string.
Authentication Method	This field is only visible if authentication is enabled above. Please select the authentication method the given URL is protected with. Choose between:

Authentication	
	• Basic access authentication (HTTP): Use simple HTTP authentication. This is the default setting and suitable for most cases. Note: This authentication method will transmit credentials as plain text! • Windows NT LAN Manager (NTLM): Use the Microsoft NTLM protocol for authentication. This is sometimes used in Intranets for single sign-on. We recommend using the default value.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Proxy Settings for HTTP Sensors	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS. Note: This setting is valid for the monitoring only and determines the behavior of sensors. In order to change proxy settings for the core server, please see System Administration—System and Website ¹⁸¹¹ .
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.
Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either **http:///** or **https:///** or even a simple slash **/** as equivalent for **http:///**). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** **www.example.com** and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value **https:///** in the URL field, PRTG will automatically create the URL **https://www.example.com/** from that.
- Using the value **/help** in the URL field, PRTG will automatically create and monitor the URL **http://www.example.com/help**
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, **http://:8080/**

Note: Smart URL replacement does not work for sensors running on the "Probe Device".

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.33 HTTP Content Sensor

The HTTP Content sensor monitors a numerical value returned by a Hypertext Transfer Protocol (HTTP) request. In the returned HTML page, each value must be placed between square brackets `[ ]`.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[226]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

HTTP Specific	
Value Type	Define what kind of values your HTML file gives back. Choose between: ▪ Integer: An integer is expected as return value. ▪ Float: A float is expected as return value, with a dot (.) between pre-decimal position and decimal places. In this setting, the sensor will also display integer values unless they don't produce a buffer overflow. Note: The sensor cannot handle string values.
Number of Channels	Define how many values your HTML file gives back. Each value will be handled in its own sensor channel. Each value must be placed between square brackets <code>[]</code>. Enter the number of bracket-value pairs that will be returned at the defined URL. Note: Do not enter a number less than the number of values returned. Otherwise you will get an error message.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
HTTP Specific	
Timeout (Sec.)	Enter a timeout in seconds for the HTTP request. If the reply takes longer than this value the request is aborted and an error message is triggered. The maximum value is 900 seconds (15 minutes).
Script URL	Please enter the URL the sensor will connect to. If you enter an absolute URL, this address will be independent from the IP address/DNS name setting of the device this sensor is created on. PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section Smart URL Replacement below.
Value Type	The kind of values the HTML file gives back. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
SSL Specific	
SSL Method	This setting is relevant only when using https in the URL field. We recommend using the default value. If you experience connection problems, please select another SSL method from the list. Choose between: ▪ SSL V2 ▪ SSL V2 or V3: This is the default setting. ▪ SSL V3

SSL Specific	
	▪ TLS V1 Note: Other TLS versions are not supported.

Note: This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

Advanced Sensor Data	
Content Changes	Define what will be done in case the content of the monitored web page changes. You can choose between: • Ignore changes: No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that the web page content has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the web page content changes.
Sensor Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results. ▪ Write sensor result to disk (Filename: "Result of Sensor (ID).txt"): Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage section.

Authentication	
Authentication	Define if the web page at the configured URL need authentication. Choose between: ▪ No authentication needed ▪ Web page needs authentication
User	This field is only visible if authentication is enabled above. Enter a username. Please enter a string.
Password	This field is only visible if authentication is enabled above. Enter a password. Please enter a string.

Authentication	
Authentication Method	This field is only visible if authentication is enabled above. Please select the authentication method the given URL is protected with. Choose between: • Basic access authentication (HTTP): Use simple HTTP authentication. This is the default setting and suitable for most cases. Note: This authentication method will transmit credentials as plain text! • Windows NT LAN Manager (NTLM): Use the Microsoft NTLM protocol for authentication. This is sometimes used in Intranets for single sign-on. We recommend using the default value.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Example

At the URL <http://www.example.com/status.html> a PHP script is giving back the current system status in a simple HTML page, as follows:

```
<html>
<body>
  Description: Script gives back current status of disk free (%) and CPU usage (%).
  [85.5][12.0]
</body>
</html>
```

You would configure the HTTP Content sensor using the mentioned script **URL**, value type **Float**, and number of channels **2**. The sensor will call the URL with every scanning interval and only regard the two values in square brackets **[]**, handling each of them in one sensor channel. The additional description text and HTML tags are not necessary; in this example they are added in case a human calls the URL.

Note: If you define the number of channels as **1**, only the first value will be read by the sensor; the second value will be ignored. Using **3** as number of channels will result in a sensor error message.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Proxy Settings for HTTP Sensors	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS. Note: This setting is valid for the monitoring only and determines the behavior of sensors. In order to change proxy settings for the core server, please see System Administration—System and Website ¹⁸¹¹ .
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.
Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either [http:///](#) or [https:///](#) or even a simple slash [/](#) as equivalent for [http:///](#)). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** [www.example.com](#) and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value [https:///](#) in the URL field, PRTG will automatically create the URL [https://www.example.com/](#) from that.
- Using the value [/help](#) in the URL field, PRTG will automatically create and monitor the URL [http://www.example.com/help](#)
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, [http://:8080/](#)

Note: Smart URL replacement does not work for sensors running on the "Probe Device".

More

Knowledge Base article: How can I monitor internal values of a web application with PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/4>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³¹ section.

6.8.34 HTTP Full Web Page Sensor

The HTTP Full Web Page sensor monitors the full download time of a web page including assets such as images etc. In the background, it opens the web page in a browser instance to perform the measurement. Links are not followed. The sensor shows the loading time of the full page. **Note:** Be careful with this sensor, as it can generate considerable internet traffic if used with a low scanning interval!

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[226]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Full Page Download Settings	
Timeout (Sec.)	Enter a timeout in seconds for the HTTP request. If the reply takes longer than this value the request is aborted and an error message is triggered. The maximum value is 900 seconds (15 minutes).
URL	Please enter the URL the sensor will load. If you enter an absolute URL, this address will be independent from the IP address/DNS name setting of the device this sensor is created on. PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section Smart URL Replacement below.
Browser Engine	Define which browser will be used to load the web page. Choose between: ▪ Chromium (recommended): Use the "WebKit" engine that is delivered with PRTG to perform the loading test. With each scanning interval, PRTG will load the URL defined above in an instance of "Chromium" and measure the time until the page is fully loaded. This is the recommended setting. ▪ PhantomJS (Headless Webkit): Use the "PhantomJS" engine. This engine can have a high impact on your probe system's CPU and memory load, but there are additional options for result handling available (see below). ▪ Internet Explorer: With each scanning interval, the URL defined above is loaded in the background in an instance of Internet Explorer. PRTG uses the Internet Explorer of the system running the PRTG probe. Note: For full functionality we strongly recommend installing Internet Explorer 8 or higher on the system running the PRTG probe. The probe machine is either the local system (on every node, if on a cluster probe), or the system running the remote probe 2012 on which the sensor is created on. Note: For all browser engines, the same proxy settings are used that are configured for the Windows user account the PRTG probe is running on (this is usually the Windows local "system" user account, if not changed). Those settings are accessible via the Internet Explorer of this system. If you want to e.g. use a proxy for this full web page sensor test, please adjust the Internet Explorer's settings accordingly (on the computer running the probe; on all nodes, if in a cluster).
Security Context	Define the Windows user account that will be used to run the browser engine. Choose between: ▪ Use security context of probe service (default): Run the browser engine under the same Windows user account the probe is running on. By default, this is the local Windows "system" user account (if not manually changed).

Full Page Download Settings

	▪ Use Windows credentials of parent device: Use the Windows user account defined in the settings of the parent device this sensor is created on. Please go to the sensor's parent device's settings to change the Windows credentials. Note: When using the Chromium browser engine above, this is the recommended setting here.
Result Handling	This setting is only visible if the PhantomJS engine is selected above. This browser engine can render and store screenshots of the loaded web page. Choose between: ▪ Discard loaded web page (recommended): Do not store the requested web page. ▪ Store latest screenshot of the web page: Render and store the last result of the web page to the "Logs (Sensors)" directory (on the remote system, when used on a remote probe; on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. It will be named after the pattern "Fullpage of Sensor (ID).jpg". For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section. ▪ Store ongoing screenshots of the web page (use with caution!): Render and store one new screenshot of the web page with each sensor scan, and store the pictures in the "Screenshots (Fullpage Sensor)" directory (on the remote system, when used on a remote probe). For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section. This option can be used to create a visual history of the web page. Note: Depending on the monitored website and the scanning interval of the sensor, a very high amount of data can be created! Use with care, and make sure you set appropriate data purging limits in the System Administration—System and Website ¹⁸⁰⁷ settings.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either **http:///** or **https:///** or even a simple slash **/** as equivalent for **http:///**). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** **www.example.com** and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value **https:///** in the URL field, PRTG will automatically create the URL **https://www.example.com/** from that.
- Using the value **/help** in the URL field, PRTG will automatically create and monitor the URL **http://www.example.com/help**
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, **http://:8080/**

Note: Smart URL replacement does not work for sensors running on the "Probe Device".

More

Knowledge Base: What to do when I see a CreateUniqueTempDir() error message for my HTTP Full Webpage Sensor?

- <http://www.paessler.com/knowledgebase/en/topic/40783>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.35 HTTP Push Count Sensor

The HTTP Push Count sensor counts received messages which are pushed via an Hypertext Transfer Protocol (HTTP) request to the PRTG server. It provides a URL that can be used to push messages to the PRTG server using HTTP.

This function is known as **webhook**. Basically, a webhook works like a **push notification**: Webhooks are usually triggered by some event (for example, a new comment to a blog post) and send according information to a specified URL. The HTTP Push Count sensor then displays the number of pushed and received messages.

Use the following URL to receive the HTTP requests of the webhook:

http://<probe_ip>:<port_number>/<token>

Replace the parameters **<probe_ip>**, **<port_number>**, and **<token>** with the corresponding values. You can define port number and identification token in the sensor settings; the "probe IP" is the IP address of the system your PRTG probe with the sensor is running on.

Example: `http://127.0.0.1:5050/XYZ123`

Note: You can use several sensors with the same port and identification token. In this case, the number of push messages will be shown in each of these sensors.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
HTTP Push	
Request Method	Select the request method of your webhook: ▪ ANY: Do not use any filter for the request method. ▪ GET: Choose this method if your webhook uses GET. ▪ POST: Choose this method if your webhook sends post form data.
Port	Enter the port number on which this sensor listens for incoming HTTP requests. Default is 5050.
Identification Token	This is the token that is used to find the matching sensor for the incoming message. While you create the sensor, this token is <code>{__guid__}</code> . It will be replaced with an automatically generated token after you have completed the sensor creation. If you want to use another identification token, you can edit it while or after sensor creation. Note: The token will not be replaced automatically if you change it already during sensor creation.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.36 HTTP Push Data Sensor

The HTTP Push Data sensor displays data from received messages which are pushed via an Hypertext Transfer Protocol (HTTP) request to the PRTG server. It provides a URL that can be used to push messages to the PRTG server using HTTP.

This function is known as **webhook**. Basically, a webhook works like a **push notification**: Webhooks are usually triggered by some event (for example, a new comment to a blog post) and send according information to a specified URL. The HTTP Push Data sensor then displays the data of pushed and received messages.

Use the following URL to receive the HTTP requests of the webhook:

http://<probe_ip>:<port_number>/<token>?value=<integer_or_float>&text=<text message>

Replace the parameters **<probe_ip>**, **<port_number>**, **<token>**, and **<integer_or_float>** with the corresponding values. The **&text** parameter is optional: You can omit it.

- You can define **port number** and **identification token** in the sensor settings.
- The **probe IP** is the IP address of the system on which your PRTG probe with this sensor is running on.
- The **value** can be an integer or a float value, depending on the data of your application; you have to set the value type accordingly in the sensor settings. This parameter will be the sensor value.
- You can **optionally** add a custom text message by replacing the parameter **<text message>** with it. The text will be shown as sensor message. If there is no value but only a text, the text will be shown as error message.
Note: This text message has to be URL encoded (for example, the whitespace in the sample URL below); most browsers achieve this automatically.

Example: `http://127.0.0.1:5050/XYZ123?value=0&text=this is a message`

Note: You can use several sensors with the same port and identification token. In this case, the data of push messages will be shown in each of these sensors.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

HTTP Push	
Request Method	Select the request method of your webhook: ▪ ANY: Do not use any filter for the request method. ▪ GET: Choose this method if your webhook uses GET. ▪ POST: Choose this method if your webhook sends post form data.
Port	Enter the port number on which this sensor listens for incoming HTTP requests. Default is 5050.
Identification Token	This is the token that is used to find the matching sensor for the incoming message. While you create the sensor, this token is <code>{__guid__}</code> . It will be replaced with an automatically generated token after you have completed the sensor creation. If you want to use another identification token, you can edit it while or after sensor creation. Note: The token will not be replaced automatically if you change it already during sensor creation.

HTTP Push Data	
No Incoming Data	Define which status the sensor will attain if no push message has been received for at least two sensor scans. Choose between: ▪ Ignore and keep last status (default): The sensor will remain in the status as defined by the last message received. ▪ Switch to "Unknown" status: The sensor will turn into the Unknown status if there has not been received any message for at least two sensor scans.
Value Type	Define which type the value of the received data has. If this setting does not match, the sensor will go into an Error status. Choose between: ▪ Integer ▪ Float (with dot "." as delimiter)
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1688] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.37 HTTP SSL Certificate Expiry Sensor

The HTTP SSL Certificate Expiry Sensor checks a specific https-URL and returns the number of days remaining until the site's SSL certificate expires. It shows a **Warning** when only 60 days are left, and an **Error** status when only 30 days are remaining until the certificate expires.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings

URL	Enter the absolute URL to check (this sensor does not use the IP Address/DNS value of the parent device).
Force SSL V3	Define if you want to allow SSL V3 only for connections to the URL configured above. Choose between: ▪ No ▪ Yes
Certificate Name Validation	Define if you want to check if the defined URL matches the certificate. Choose between: ▪ Yes ▪ No

Proxy Settings for HTTP Sensors	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS. Note: This setting is valid for the monitoring only and determines the behavior of sensors. In order to change proxy settings for the core server, please see System Administration—System and Website ¹⁸¹¹ .
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1688] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.38 HTTP Transaction Sensor

The HTTP Transaction sensor monitors an interactive website, such as a web shop, by performing a transaction using a set of Hypertext Transfer Protocol (HTTP) URLs. The sensor monitors whether logins or shopping carts work properly. It returns the loading time.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
HTTP Specific	
Timeout (Sec.)	Enter a timeout in seconds for all HTTP requests. If the complete transaction takes longer than this value the request is aborted and an error message is triggered. The maximum value is 900 seconds (15 minutes).

HTTP Specific	
Single URL Timeout (Sec.)	Enter a timeout in seconds for one single HTTP request. If the reply of any single request takes longer than this value the transaction is aborted and an error message is triggered. The maximum value is 900 seconds (15 minutes).
HTTP Engine	
Monitoring Engine	If you encounter unexpected errors with the standard method that is used to monitor an URL, try to use the compatibility mode which is based on .Net (introduced in PRTG v13.x.7). Choose between: ▪ Default/High Performance (recommended): This is the default monitoring method for this sensor type. ▪ Alternate/Compatibility Mode: Try this method as an alternative for websites that do not work with the default approach. Using the compatibility mode, this sensor will execute an external exe. Thus, this method will need more resources, but it can be helpful in particular cases. Note: If you select the compatibility mode, the options for the SSL method will be slightly different. You can also check for trusted certificates. Please see below. Note: When using the Compatibility Mode, Smart URL Replacement will not work, i.e., this sensor does not use the IP Address/DNS value of the parent device automatically then.
SSL Specific	
SSL Method	This setting is relevant only when using https in the URL field. We recommend using the default value. If you experience connection problems, please select another SSL method from the list. Choose between: ▪ SSL V2 ▪ SSL V2 or V3: This is the default setting. ▪ SSL V3 ▪ TLS V1 Note: Other TLS versions are not supported.

SSL Specific (when using Compatibility Mode)	
SSL Method	When using the compatibility mode, the SSL specific settings are a bit different to the default SSL settings. SSL V2 is not available. You can choose between: ▪ SSL V3 ▪ TLS V1 ▪ SSL V3 or TLS V1: This is the default setting.
Check SSL Certificates	Specify if the certificate of the monitored URL will be checked. Choose between: ▪ Do not check used certificates: This the default setting. ▪ Check if the used certificates are trusted: If the certificate of the server is not trusted, the sensor will go into a Down status and display a corresponding message.

Note: This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

Advanced Sensor Data	
Limit Download (kb)	Enter a maximum amount of data that will be transferred per every single request. If you set content checks below, please be aware that only the content downloaded within this limit can be checked for certain search expressions.
Cookie Management	Select if cookies will be used for the transaction. Choose between: • Use cookies (recommended): Allow cookies to be set and read during the transaction cycle. • Ignore cookies: Do not allow cookies. Use this option if you want to test the transaction without the use of cookies. We recommend using the default value.
Result Handling	Define what will be done with the web page loaded at the given URL. Choose between: • Discard HTML result: Do not store the requested web page. • Store latest HTML result: Store the last result of the requested web page to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes, especially in combination with content checks. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage 2036 section.

Authentication	
Authentication	Define if the web page at the configured URL need authentication. Choose between: ▪ No authentication needed ▪ Web page needs authentication
User	This field is only visible if authentication is enabled above. Enter a username. Please enter a string.
Password	This field is only visible if authentication is enabled above. Enter a password. Please enter a string.
Authentication Method	This field is only visible if authentication is enabled above. Please select the authentication method the given URL is protected with. Choose between: • Basic access authentication (HTTP): Use simple HTTP authentication. This is the default setting and suitable for most cases. Note: This authentication method will transmit credentials as plain text! • Windows NT LAN Manager (NTLM): Use the Microsoft NTLM protocol for authentication. This is sometimes used in Intranets for single sign-on. We recommend using the default value.

Transaction URL	
You can define up to 10 different transaction URLs which will all be called in a row. Only if the complete transaction can be completed, the sensor will be in an Up status¹²¹. Using this mechanism you can set up an extended monitoring with multiple URLs. Please enter settings for at least one transaction URL. You can use as many steps as needed and disable the other steps.	
Transaction Step #x	This setting is available for URL #2 through #10. Define if you want to use this step for your transaction check. Choose between: ▪ Disable step #x: Do not use this step. Choose this option if you do not need all 10 steps for your transaction check. ▪ Enable step #x: Enable this step. Further options will be viewed, as described below.

Transaction URL	
URL	Please enter the URL the sensor will connect to. If you enter an absolute URL, this address will be independent from the IP address/DNS name setting of the device this sensor is created on. PRTG uses a smart URL replacement which allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section Smart URL Replacement below.
Request Method	The request method determines how the given URL is requested. • GET: Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page. • POST: Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the Postdata field below. • HEAD: Only request the HTTP header from the server; without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.
Postdata	This field is only active when POST is selected in the Request Method setting above. Please enter the data part for the post request here. Note: No XML is allowed here!
Check For Existing Key Words (Positive)	Define whether the result at the configured URL will be checked for keywords. Choose between: ▪ Disable: Do not search for keywords. ▪ Enable key word check (positive): In the result returned at the URL, check if a key word exists. Note: The content check is only intended for html websites and might not work with other target URLs.
Response Must Include	Define which string must be part of the web at the given URL. If the data does not include this string, the sensor will be set to an error state. Please enter a string. Note: Only simple text search is available here. The characters * and ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible.
Check For Existing Key Words (Negative)	Define whether the the result at the configured URL will be checked for keywords. Choose between: ▪ Disable: Do not search for keywords.

Transaction URL	
	▪ Enable key word check (negative): In the result returned at the URL, check if a key word does not exist. Note: The content check is only intended for html websites and might not work with other target URLs.
Response Must Not Include	Define which string must not be part of the web at the given URL. If the data does include this string, the sensor will be set to an error state. Please enter a string. Note: Only simple text search is available here. The characters * and ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Proxy Settings for HTTP Sensors	
HTTP Proxy Settings	The proxy settings determine how a sensor connects to a given URL. You can enter data for a proxy server that will be used when connecting via HTTP or HTTPS. Note: This setting is valid for the monitoring only and determines the behavior of sensors. In order to change proxy settings for the core server, please see System Administration—System and Website¹⁸¹¹.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login. Note: Only basic authentication is available! Please enter a string or leave the field empty.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either **http:///** or **https:///** or even a simple slash **/** as equivalent for **http:///**). PRTG will then fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** **www.example.com** and you put an HTTP sensor on it, you can provide values the following ways:

- Providing the value **https:///** in the URL field, PRTG will automatically create the URL **https://www.example.com/** from that.
- Using the value **/help** in the URL field, PRTG will automatically create and monitor the URL **http://www.example.com/help**
- It is also possible to provide a port number in the URL field which will be taken over by the device's DNS name and internally added, for example, **http://:8080/**

Note: Smart URL replacement does not work for sensors running on the "Probe Device".

More

Knowledge Base: Configuration Tips for HTTP Transaction Sensors needed

- <http://www.paessler.com/knowledgebase/en/topic/443>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.39 HTTP XML/REST Value Sensor

The HTTP XML/REST Value sensor retrieves an XML file from a given URL and parses it. It can return the values of specific nodes.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Channel Name	Enter a name for the channel which will display the value at the given URL. The name can be changed later in the Sensor Channels Settings ^[1683] .

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ⁵⁶⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
URL	Enter the absolute URL that returns the XML file (this sensor does not use the IP Address/DNS value of the parent device).
XML Node (and optional property)	Enter the name of the node this sensor will check, or enter a node name and a property name to check a property value. To obtain a value from nested tags, please enter the tag names separated by a slash symbol, for example, use myTag/myTagInside as XML node value. Note: You can also check values in JavaScript Object Notation (JSON) notation. Please see Checking JSON⁵⁶⁸ section below. Note: You can try using XPath syntax here but it will not work in all cases and we do not provide any technical support for XPath issues. For further documentation about XPath please see More⁵⁶¹ section below.
HTTP Username	If the URL requires authentication, enter the username. Please enter a string or leave the field empty.
HTTP Password	If the URL requires authentication, enter the password. Please enter a string or leave the field empty.
Sensor Value	Choose between:

Sensor Settings	
	▪ Use the value of the selected XML node: Return the value found at the specified XML node. If this is non-numeric, this will return 0. ▪ Use the number of occurrences of the selected XML node or its children/siblings: Return the number of occurrences found. Define further below.
Count XML Nodes	This setting is only visible if the return number option is enabled above. Define which count will be returned. Choose between: ▪ Occurrences of the selected XML node: Return how often the defined XML node occurs at the defined URL. ▪ Child nodes of the selected XML node: Return the number of child nodes that exist below the node at the defined URL. ▪ Sibling nodes of the selected XML node: Return the number of sibling nodes that exist next to the node at the defined URL.
Namespaces	Define whether namespaces in the XML document will be used or not. Choose between: ▪ Use Namespaces: Process the value entered in the "XML Node (and optional property)" field including possibly existing namespace information. ▪ Remove Namespaces: Ignore namespace information in the XML document and process the value entered in the "XML Node (and optional property)" field as node names only. For more information see About Namespaces⁵⁶⁹ section below.
Content Type in Header	Choose if PRTG will include <code>content-type="text/xml"</code> in the header of the request sent to the URL defined above. Choose between: ▪ Enable (recommended): This works for most web servers and is the recommended setting. ▪ Disable: Only very few web servers cannot handle this content-type and need this setting. Try this if you get an error message with the enabled option. ▪ Custom: You can use a custom content type.
Custom Content Type	Only visible when "Custom" is enabled above. Enter a custom content type like <code>text/xml</code> or <code>text/html</code>.

Sensor Settings	
Characters to Remove	Only visible when using value of XML node is enabled above. Optionally enter a string which will be removed from the returned XML value. Use this to remove any unwanted characters from the result, for example, a thousands separator from numeric values. Please enter a string or leave the field empty.
Decimal Delimiter	This setting is only visible if "use value" is enabled above. If the sensor value of the selected XML node is of the type float , you can define any character here which is the decimal delimiter. Enter one character or leave the field empty.
Custom Message	Optionally enter a custom sensor message. Use %1 as a placeholder to automatically fill in the returned XML value. Please enter a string or leave the field empty.
Force SSL V3	Define if you only want to allow SSL V3 connections to the URL defined above. Choose between: ▪ No ▪ Yes
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • Ignore changes (default): No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification¹⁶⁹⁰ whenever the sensor value changes.
Results	Define what will be done with the results given back. Choose between: • Discard result: Do not store the requested web page. • Write result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see More⁴³⁷ section below.
Unit String	Enter a string that will be added to the values as a unit description. This is for display purposes only.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁹⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Checking JSON

With the **XML Node (and optional property)** field you can also check values that are returned in JavaScript Object Notation (JSON) notation under the defined URL.

Example

A JSON notated section may look like the following:

```
{
  "test": "Hello World",
  "object": {
    "value": "content",
    "AnotherValue": "AnotherContent"
  },
  "arraytest": [
    "one",
    "two"
  ]
}
```

Depending on your entries in the **XML Node** field, the sensor will process the respective values:

Entry in Sensor's "XML Node" Field (from Example Above)	Processed Value (from Example Above)
test	Hello World
object/value	content
object/AnotherValue	AnotherContent
object	contentAnotherContent
arraytest[1]	one
arraytest[2]	two

About Namespaces

In an XML document, tags may use namespaces.

Example

A namespace notated section may look like the following:

```
<myNamespace:myNode>
  some information
</myNamespace:myNode>
```

If you set this sensor to **Use Namespaces** (this is the default setting), it will expect the full node name, including the namespace information, in the **XML Node (and optional property)** field. In the example above, this would be **myNamespace:myNode**.

If your node names are unique even without the namespace information, you can simplify the settings by setting this sensor to **Remove Namespaces**. The sensor will then expect the node name only in the **XML Node (and optional property)** field. In the example above, this would be **myNode**.

More

Knowledge Base: Is there a tool available that can help me building queries for the XML/Rest Sensor?

- <http://www.paessler.com/knowledgebase/en/topic/48783>

Knowledge Base: How do I extract values from XML nodes (with nested tags) using PRTG's XML/Rest Value Sensor?

- <http://www.paessler.com/knowledgebase/en/topic/43223>

Knowledge Base: How can I use XPath with PRTG's XML/Rest Value Sensor?

- <http://www.paessler.com/knowledgebase/en/topic/26393>

Knowledge Base: HTTP XML/REST Value Sensor shows protocol violation. What can I do?

- <http://www.paessler.com/knowledgebase/en/topic/26793>

Knowledge Base: Why does my HTTP XML/REST Value Sensor return a 404 error?

- <http://www.paessler.com/knowledgebase/en/topic/46503>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)  section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[1441] section.

6.8.40 Hyper-V Cluster Shared Volume Disk Free Sensor

The Hyper-V Cluster Shared Volume Disk Free sensor monitors a Microsoft Hyper-V cluster shared volume via PowerShell and shows the available disk space. **Note:** The parent device for this sensor must be a Windows Server running Hyper-V.

Note: We recommend using System Center Virtual Machine Manager (SCVMM) as parent device, because this way PRTG will continue to monitor your virtual machines also when they change the physical host using Live Migration.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: Remote PowerShell

The Hyper-V Cluster Shared Volume Disk Free sensor uses PowerShell commands. In order to monitor devices with this sensor **Remote PowerShell** has to be enabled. For detailed information, please see [More](#)⁵⁷⁷ section below.

Requirement: WSFC PowerShell Interface

This sensor type needs the WSFC (Windows Server Failover Clustering) PowerShell Interface to be installed on the target machine. You can list all modules in the PowerShell console with the command **Get-Module -ListAvailable**. Here **FailoverClusters** has to appear. Under Windows 2008 and 2012 the interface is part of the VMM Administrator Console, or the VMM 2012 Management Console, respectively.

The interface is everywhere available where the WSFC feature is installed: Windows Server 2008 R2 (SP1) Full and Core (not installed by default); Microsoft Hyper-V Server 2008 R2 (SP1); Remote Server Administration Tools (RSAT) for Windows 7 (SP1).

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor cluster disks, PRTG will create one sensor for each disk. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Disk Free Settings**Disk**

Select the disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head. **Note:** Please make sure the resource name of your disks do not contain unsupported characters, especially avoid the hash ('#') sign. We recommend to not rename resource disk name once you've set up monitoring. For detailed information, please see [More](#)^[591] section below.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings**Sensor Name**

Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Tags

Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically [inherited](#)^[89] from objects further up in the device tree. Those are not visible here.

Priority

Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Disk Free Settings**Disk**

Shows further information about the disk. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

If Value Changes

Define what will be done in case the value of a sensor channel changes. Choose between:

Disk Free Settings	
	▪ Ignore changes: No action will be taken on change. ▪ Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification¹⁶⁹⁰ whenever the sensor value changes.
Sensor Result	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage²⁰³⁶ section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸⁸ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: Why don't my Hyper-V sensors work after changing names?

- <http://www.paessler.com/knowledgebase/en/topic/15533>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <http://www.paessler.com/knowledgebase/en/topic/44453>

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- <http://www.paessler.com/knowledgebase/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <http://www.paessler.com/knowledgebase/en/topic/59745>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.41 Hyper-V Host Server Sensor

The Hyper-V Host Server sensor monitors a Microsoft Hyper-V host server via Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device. It shows CPU usage in percent of guests, hypervisor, and total, as well as host health critical values, the number of deposited pages, and network traffic. Network traffic sums up the total bytes per second (received and sent) on all ports of your virtual switch.

Note: The parent device for this sensor must be a Windows Server running Hyper-V.

Note: We recommend using System Center Virtual Machine Manager (SCVMM) as parent device, because this way PRTG will continue to monitor your virtual machines also when they change the physical host using Live Migration.

Note: By default, this sensor type uses a hybrid approach, first trying to query data via Windows Performance Counters (which needs less system resources), and using Windows Management Instrumentation (WMI) as a fallback in case Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours. The default behavior can be changed in the **Windows Compatibility Options** of the parent [device's settings](#)^[280] this sensor is created on.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the [local system](#) (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[2012]. **Note:** The target system may well run on Windows 2003 or later.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (e.g. via **services.msc**). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Sensor Result	Define what will be done with the result of the sensor. Choose between:

	▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁹ section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1688] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.42 Hyper-V Virtual Machine Sensor

The Hyper-V Virtual Machine sensor monitors a virtual machine running on a Microsoft Hyper-V host server, via Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device. It shows CPU usage in percent of guests, hypervisor, and total, as well as disk read and write values, per second. **Note:** The parent device for this sensor must be a Hyper-V server.

Note: In order to monitor a virtual machine with this sensor, **disable** User Account Control (UAC) in the control panel of the Windows operating system which is running on this virtual machine. Otherwise, the sensor might switch into a down status with the error message "The virtual is not running or is powered off".

Note: We recommend using System Center Virtual Machine Manager (SCVMM) as parent device, because this way PRTG will continue to monitor your virtual machines also when they change the physical host using Live Migration.

Note: By default, this sensor type uses a hybrid approach, first trying to query data via Windows Performance Counters (which needs less system resources), and using Windows Management Instrumentation (WMI) as a fallback in case Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours. The default behavior can be changed in the **Windows Compatibility Options** of the parent [device's settings](#)^[280] this sensor is created on.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[2012]. **Note:** The target system may well run on Windows 2003 or later.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (e.g. via **services.msc**). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor virtual machines, PRTG will create one sensor for each machine. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Virtual Machine Settings	
Virtual Machine	Select the virtual machines (VMs) you want to add a sensor for, including the ones that are not running. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head. Note: Please make sure the name of your VMs do not contain unsupported characters, especially avoid the hash ('#') sign. We recommend to not rename virtual machines once you've set up monitoring. For detailed information, please see More ⁵⁹¹ section below.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Virtual Machine Settings	
GUID	Shows the Globally Unique Identifier (GUID) of the virtual machine monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the virtual machine monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the host server. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Powered Off VMs	Choose how the sensor will react to a virtual machine that is powered off. Please choose between: • Alarm when powered off (default): The sensor will change to a Down^[121] status if the virtual machine is powered off. Note: While in Down status, a sensor does not record any data in all of its channels. • Ignore powered off state: The sensor will not change to a Down status if the virtual machine is powered off; it will report zero values instead.
Sensor Result	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result.

Virtual Machine Settings

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: **Result of Sensor [ID].txt**. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see [Data Storage](#) ²⁰³⁶ section.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

More

Knowledge Base: Why don't my Hyper-V Virtual Machine / Network Adapter Sensor work after changing names?

- <http://www.paessler.com/knowledgebase/en/topic/15533>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁸⁸⁰ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁸⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.43 Hyper-V Virtual Network Adapter Sensor

The Hyper-V Network Adapter sensor monitors virtual network adapters running on a Microsoft Hyper-V host server, via Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device. It shows sent and received bytes, packets, broadcast packets, directed packets, and multicast packets, per second. **Note:** The parent device for this sensor must be a Hyper-V server.

Note: We recommend using System Center Virtual Machine Manager (SCVMM) as parent device, because this way PRTG will continue to monitor your virtual machines also when they change the physical host using Live Migration.

Note: By default, this sensor type uses a hybrid approach, first trying to query data via Windows Performance Counters (which needs less system resources), and using Windows Management Instrumentation (WMI) as a fallback in case Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours. The default behavior can be changed in the **Windows Compatibility Options** of the parent [device's settings](#)^[280] this sensor is created on.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[2012]. **Note:** The target system may well run on Windows 2003 or later.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (e.g. via **services.msc**). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor network adapters, PRTG will create one sensor for each adapter. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Virtual Machine Settings	
Hyper-V Virtual Network Adapter	Select the virtual network adapters you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head. Note: We recommend to not rename virtual machines once you have set up monitoring. Renaming them will also change the internal virtual network adapter names, causing the monitoring to be interrupted. For detailed information about virtual machine naming, please see More ^[591] section below.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Hyper-V Virtual Network Adapter Settings	
Virtual Network Adapter	Shows the name of the virtual network adapter monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage^[208] section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor.

Sensor Display	
	▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹². Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

More

Knowledge Base: Why don't my Hyper-V Virtual Machine / Network Adapter Sensor work after changing names?

- <http://www.paessler.com/knowledgebase/en/topic/15533>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.44 Hyper-V Virtual Storage Device Sensor

The Hyper-V Virtual Storage sensor monitors a virtual storage device running on a Microsoft Hyper-V host server, via Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device. It shows read and write values in second, and the number of errors. **Note:** The parent device for this sensor must be a Hyper-V server.

Note: We recommend using System Center Virtual Machine Manager (SCVMM) as parent device, because this way PRTG will continue to monitor your virtual machines also when they change the physical host using Live Migration.

Note: By default, this sensor type uses a hybrid approach, first trying to query data via Windows Performance Counters (which needs less system resources), and using Windows Management Instrumentation (WMI) as a fallback in case Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours. The default behavior can be changed in the **Windows Compatibility Options** of the parent [device's settings](#)^[280] this sensor is created on.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[2012]. **Note:** The target system may well run on Windows 2003 or later.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (e.g. via **services.msc**). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor storage devices, PRTG will create one sensor for each device. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Hyper-V Virtual Storage Device Settings

Hyper-V Virtual Storage Device	Select the virtual storage devices you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Hyper-V Virtual Storage Device Settings	
Virtual Storage Device	Shows the unique name of the device monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.45 IMAP Sensor

The IMAP sensor monitors a mail server using Internet Message Access Protocol (IMAP) and shows the server's response time as well as the number of emails in the defined mailbox. It can also check the content of emails for certain key words. This way, you can use this sensor to monitor backup solutions via emails that are sent out by these solutions. For more information, see section [More](#)^[616].

Note: If you use content checks, we recommend using a dedicated IMAP account that is only checked by PRTG. Editing existing mails in the mailbox of the monitored IMAP account can lead to false alarms or malfunctions of this sensor type.

Note: This sensor type might not work properly when monitoring sub-folders of mailboxes. If it has to check subsequent emails with identical subjects, later on incoming emails might not be recognized.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

IMAP Specific	
Timeout (sec.)	Enter a timeout in seconds for the SMTP connect. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port	Enter the number of the port that will be used to connect via IMAP. For non-secure connections usually port 143 is used; usually port 993 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
Authentication	
Authentication Type	Select the kind of authentication for the IMAP connection. Choose between: • Username/Password: Authenticate at the IMAP server via username and password. • Simple Authentication and Security Layer (SASL): Use a secure connection for the authentication at the IMAP server.
Username	Enter a username for IMAP authentication. Please enter a string or leave the field empty. Note: If you leave this field empty, PRTG will not attempt to log in to the mail server. The sensor will show a green Up status if the IMAP server is available.
Password	Enter a password for IMAP authentication. Please enter a string or leave the field empty. Note: If you leave this field empty, PRTG will not attempt to log in to the mail server. The sensor will show a green Up status if the IMAP server is available.
TLS (Transport-Level Security)	This setting is only relevant if authentication is used. Choose if a secure connection via TLS/SSL will be used. Choose between: • Don't use • Use

SSL-Method	This field is only visible if security is enabled above. Select the SSL method that will be used when connecting to the server. We recommend using the default value. Only if you experience connection problems, try another setting. Choose between: ▪ SSL V2 ▪ SSL V2 or V3 ▪ SSL V3 ▪ TLS V1
Identify Email	
Process Email Content	This sensor can additionally check the content of all incoming emails. Choose between: ▪ Do not check email content: Only check availability of the IMAP server and check if a login is successful (if defined). Do not process any mails in the IMAP mail account. ▪ Process emails in this mailbox: Login in to the IMAP mail account and check the mails contained there. Define further options below.
Mailbox Name	This field is only visible if email content processing is enabled above. Enter the name of the mailbox (e.g. the name of the IMAP folder) that will be checked. Default value is Inbox. Unless you set a last message date check below, the sensor will always look at all emails contained in the mailbox. Note: Please make sure that you do not manually edit mails in this mailbox with another mail client, as this can lead to malfunctions of this sensor's email identification.
Identify by "From" Field	This option is only visible if email content processing is enabled above. Define if you want to check the "From" field of the emails. Choose between: ▪ Don't check: Do not check this field in emails. ▪ Check using string search: Check this field in emails using simple string search. ▪ Check using regular expression: Check this field in emails using a regular expression. For more information about syntax, please see Regular Expressions ²⁰¹⁰ section. When using a search, the sensor will scan all emails from the newest to the oldest. Note: The scan will be finished with the first match! That means: After a match is found in one email, there will be no further checks performed in older emails.
Search For	This field is only visible if a check is enabled above. Enter a search string using the method defined above.

Identify Email	
Identify by "Subject" Field	This option is only visible if email content processing is enabled above. Define if you want to check the "Subject" field of the emails. Choose between: ▪ Don't check: Do not check this field in emails. ▪ Check using string search: Check this field in emails using simple string search. ▪ Check using regular expression: Check this field in emails using a regular expression. For more information about syntax, please see Regular Expressions 2010 section. When using a search, the sensor will scan all emails from the newest to the oldest. Note: The scan will be finished with the first match! That means: After a match is found in one email, there will be no further checks performed in older emails.
Search For	This field is only visible if a check is enabled above. Enter a search string using the method defined above.
Identify by Mail Body	This option is only visible if email content processing is enabled above. Define if you want to check the mail body of the emails. Choose between: ▪ Don't check: Do not check the mail body. ▪ Check using string search: Check the mail body using simple string search. ▪ Check using regular expression: Check the mail body using a regular expression. For more information about syntax, please see Regular Expressions 2010 section. When using a search, the sensor will scan all emails from the newest to the oldest. Note: The scan will be finished with the first match! That means: After a match is found in one email, there will be no further checks performed in older emails.
Search For	This field is only visible if a check is enabled above. Enter a search string using the method defined above.
Check Last Message Date	This option is only visible if email content processing is enabled above. Define if you want to check all emails in the mailbox, or only mails that were received within the last x hours. Choose between: ▪ Don't check message age: Always check all emails contained in the mailbox. ▪ Check for new messages received within the last x hours: Only regard emails that were received in the last hours. Define below.

Identify Email	
Error Threshold (Hours)	Enter the maximum age in hours. Only emails that are younger will be processed. If there is no matching email in the defined time span, the sensor will show a Down status.
Warning Threshold (Hours)	Enter the maximum age in hours. Only emails that are younger will be processed. If there is no matching email in the defined time span, the sensor will show a Warning status.
Sensor Behavior	
Set to Alarm	This setting is only visible if email content check is enabled above. Define in which cases the sensor will show a Down status. Choose between: ▪ If subject contains ▪ If subject does not contain ▪ If mail body contains ▪ If mail body does not contain ▪ Always: Always set this sensor to a Down status in case any emails could be identified. ▪ Never: Never set this sensor to a Down status based on email content.
Check Method	This setting is only visible if an if-condition is selected above. Define how you want to check for the above condition. Choose between: ▪ String search: Check the mail body using simple string search. ▪ Regular expression: Check the mail body using a regular expression. For more information about syntax, please see Regular Expressions 2010 section. When using a search, the sensor will scan all emails from the newest to the oldest. Note: The scan will be finished with the first match! That means: After a match is found in one email, there will be no further checks performed in older emails.
Search Text	This setting is only visible if an if-condition is selected above. Enter a search string using the method defined above.
Error Message	This setting is only visible if an alarm condition is selected above. Define the message that will be shown in case the sensor shows a Down status.

Sensor Behavior	
Set to Warning	This setting is only visible if email content check is enabled above. Define in which cases the sensor will show a Warning status. Choose between: ▪ If subject contains ▪ If subject does not contain ▪ If mail body contains ▪ If mail body does not contain ▪ Always: Always set this sensor to a Warning status in case any emails could be identified. ▪ Never: Never set this sensor to a Warning status based on email content.
Check Method	This setting is only visible if an if-condition is selected above. Define how you want to check for the above condition. Choose between: ▪ String search: Check the mail body using simple string search. ▪ Regular expression: Check the mail body using a regular expression. For more information about syntax, please see Regular Expressions [2010] section. When using a search, the sensor will scan all emails from the newest to the oldest. Note: The scan will be finished with the first match! That means: After a match is found in one email, there will be no further checks performed in older emails.
Search Text	This setting is only visible if an if-condition is selected above. Enter a search string using the method defined above.
Warning Message	This setting is only visible if a warning condition is selected above. Define the message that will be shown in case the sensor shows a Warning status.
No Matching Mail Behavior	This setting is only visible if email content check is enabled above. Define how the sensor will react if no matching emails are found in the mailbox that is being scanned. Choose between: ▪ Set sensor to "Down" status ▪ Set sensor to "Warning" status ▪ None: Don't do anything in this case.

Sensor Behavior	
Message	This field is only effective if a sensor change in case of no matching mail is defined above. Define the message that will be shown in case the sensor could not find any matching emails. It will be shown together with a Warning or Down status, just as defined above.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

More

Knowledge Base: How can I monitor my backup software to be sure backup succeeded last night?

- <http://www.paessler.com/knowledgebase/en/topic/47023>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#) section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#) section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.46 INI File Content Check Sensor

The INI File Content Check sensor reads an *.ini file. It indicates if the file exists and if a specified section and field are found. The sensor returns the field's integer value (or -1 if the field does not contain an integer). It will show a **Warning** status if a section or field is not found, and a **Down** status if the file could not be opened.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
INI Filename	Enter the full path to the file this sensor will monitor. For example, enter C:\Windows\win.ini . If the file is located on a network device use the Uniform Naming Convention (UNC) path without the server part (you would only enter share\folder\file.ini). The server part (\server\) is taken from this sensor's parent device's settings. Please enter a valid path and file name. Note: In order to provide any shares, the LanmanServer "Server" Windows service must be running on the target computer.
INI Section	Define the section inside the INI file you would like to check. A section within the INI file is denoted in square brackets [] . Enter the section name without the brackets here, for example, enter Mail . This value is not case sensitive. If the section is not found, the sensor will show a Warning status.
INI Field	Define the field inside the section you would like to check. In the INI file, a field name is written before an equal sign = , followed by its value. Enter the field name here, for example, enter MAPI . This value is not case sensitive. The sensor will return the value of this field, i.e. the value on the right side of the equal sign. If the field is not found, the sensor will show a Warning status.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • Ignore changes: No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.47 IP on DNS Blacklist Sensor

The IP on DNS Blacklist sensor checks if the IP address of its parent device is listed on specific blacklist servers and returns the number of hits found. If a DNS name is used as the parent device's hostname, PRTG will resolve it to an IP address first.

During normal operation, there should be **0** hits and the sensor should show a green **Up** status. If the IP address is found on at least one of the blacklist servers, the sensor changes to a yellow **Warning** status by default. **Note:** You can set additional thresholds in the sensor's [Sensor Channels Settings](#)^[1683], if you like.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Blacklist Servers	Define the blacklist servers that will be used for the check. You can enter a comma separated list. Default is bl.spamcop.net . For a list of servers, please see More ^[628] section below. Note: With each scanning interval, PRTG will query all servers in the list! We recommend you do not enter more than 10 servers to make sure the check can be completed within the scanning interval of this sensor. If you use too many blacklist servers, the sensor will show a "Timeout (code: PE018)" error message.
Timeout (sec.)	Define a timeout in seconds for the check. If the reply takes longer than this value the request is aborted and an error message is triggered.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

More

Knowledge Base: Is there a list of anti spam black list servers?

- <http://www.paessler.com/knowledgebase/en/topic/37633>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.48 IPFIX Sensor

The IPFIX sensor receives traffic data from an IPFIX (Internet Protocol Flow Information Export) compatible device and shows traffic by type. There are several filter options available to divide traffic into different channels. Please make sure your device supports IPFIX when using this sensor.

Note: In order for this sensor to work, you have to enable IPFIX export on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe). This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

For a general introduction to the technology behind flow monitoring, please see [Monitoring Bandwidth via Flows](#)^[1904] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

IPFIX Specific Settings	
Receive IPFIX Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the IPFIX export options of your hardware router device. Please enter an integer value.
Sender IP	Enter the IP address of the sending device you want to receive the IPFIX data from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive IPFIX Packets on IP	Select the IP address(es) on which PRTG listens to IPFIX packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line or in the top level box to select all. The IP address selected here must match the one configured in the IPFIX export options of your hardware router device.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an Unknown status. Please enter an integer value. We recommend setting this one minute longer than the respective timeout configured in your hardware router device. Note: If you set this value too low, flow information might get lost!
Sampling Mode	Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between: ▪ Off: The standard flow will be used. ▪ On: Switch into sampling mode and specify the sampling rate below.
Sampling Rate	This field is only visible when sampling mode is enabled above. Enter a number that matches the sampling rate in your exporter device. If the number is different, monitoring results will be incorrect. Please enter an integer value.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to the data folder (see Data Storage ²⁰³⁶). Choose between: ▪ None (recommended): Do not write additional log files. Recommended for normal use cases. ▪ Only for the 'Other' channel: Only write log files of data that is not filtered otherwise and therefore accounted to the default Other channel. ▪ All stream data: Write log files for all data received.

IPFIX Specific Settings	
	Note: Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.
Channel Configuration	
Channel Selection	Define the categories the traffic will be accounted to. There are different groups of traffic available. Choose between: ▪ Web: Internet web traffic. ▪ File Transfer: Traffic caused by FTP. ▪ Mail: Internet mail traffic. ▪ Chat: Traffic caused by chat and instant messaging. ▪ Remote Control: Traffic caused by remote control applications, such as RDP, SSH, Telnet, VNC. ▪ Infrastructure: Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, SNMP. ▪ NetBIOS: Traffic caused by NetBIOS communication. ▪ Other Protocols: Traffic caused by various other protocols via UDP and TCP. For each traffic group, you can select how many channels will be used for each group, i.e. how detailed traffic will be divided. For each group, choose between: ▪ No: Do not account traffic of this group in an own channel. All traffic of this group will be accounted to the default channel named Other. ▪ Yes: Count all traffic of this group and summarize it into one channel. ▪ Detail: Count all traffic of this group and further divide it into different channels. The traffic will appear in several channels as shown in the Content column. Note: Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyse.
Filtering	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors ¹⁹⁹⁴

Filtering	
	section.
Exclude Filter	First, the filters defined in the Include Filter field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors ¹⁹⁹⁴ section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ Top Talkers ▪ Top Connections ▪ Top Protocols ▪ [Any custom toplist you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail. For more information, please see [Toplists](#)¹⁷⁰² section.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹¹ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁴
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁸

6.8.49 IPFIX (Custom) Sensor

The IPFIX (Custom) sensor receives traffic data from an IPFIX (Internet Protocol Flow Information Export) compatible device and shows the traffic by type. In this custom sensor, you can define your own channel definitions to divide traffic into different channels. Please make sure your device supports IPFIX when using this sensor.

Note: In order for this sensor to work, you have to enable IPFIX export on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe). This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

For a general introduction to the technology behind flow monitoring, please see [Monitoring Bandwidth via Flows](#)^[1904] section.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

IPFIX Specific Settings

Receive IPFIX Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one configured in the IPFIX export options of your hardware router device. Please enter an integer value.
Sender IP	Enter the IP address of the sending device you want to receive the IPFIX data from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive IPFIX Packets on IP	Select the IP address(es) on which PRTG listens to IPFIX packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the IPFIX export options of your hardware router device.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an Unknown status. Please enter an integer value. We recommend setting this one minute longer than the respective timeout configured in your hardware router device. Note: If you set this value too low, flow information might get lost!
Sampling Mode	Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between: ▪ Off: The standard flow will be used. ▪ On: Switch into sampling mode and specify the sampling rate below.
Sampling Rate	This field is only visible when sampling mode is enabled above. Enter a number that matches the sampling rate in your device. If the number is different, monitoring results will be incorrect. Please enter an integer value.

IPFIX Specific Settings

Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see Channel Definitions for xFlow and Packet Sniffer Sensors^[1998] section. All traffic for which no channel is defined will be accounted to the default channel named Other. Note: Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to the data folder (see Data Storage^[2036]). Choose between: ▪ None (recommended): Do not write additional log files. Recommended for normal use cases. ▪ Only for the 'Other' channel: Only write log files of data that is not filtered otherwise and therefore accounted to the default Other channel. ▪ All stream data: Write log files for all data received. Note: Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[1683] settings).

Sensor Display	
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.
Filtering	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors ¹⁹⁹⁴ section.
Exclude Filter	First, the filters defined in the Include Filter field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors ¹⁹⁹⁴ section.
Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ Top Talkers ▪ Top Connections ▪ Top Protocols ▪ [Any custom toplist you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail. For more information, please see [Toplists](#)¹⁷⁰² section.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁴
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁸

6.8.50 jFlow V5 Sensor

The jFlow V5 sensor receives traffic data from a jFlow V5 compatible device and shows the traffic by type. On your hardware device, please make sure it matches jFlow V5 and disable any sampling option! There are several filter options available to divide traffic into different channels.

Note: In order for the sensor to work, jFlow export of the respective version must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe). The sensor does not support sampling, so please disable sampling in your jFlow device! This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

For a general introduction to the technology behind flow monitoring, please see [Monitoring Bandwidth via Flows](#)¹⁹³⁴ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ⁸⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

jFlow V5 Specific Settings	
Receive jFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the jFlow export options of your hardware router device. Please enter an integer value. Note: When configuring export, please make sure you select the appropriate jFlow version for this sensor.
Sender IP	Enter the IP address of the sending device you want to receive the jFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive jFlow Packets on IP	Select the IP address(es) on which PRTG listens to jFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the jFlow export options of your hardware router device. Note: When configuring export, please make sure you select the appropriate jFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an Unknown status. Please enter an integer value. We recommend setting this one minute longer than the respective timeout configured in your hardware router device. Note: If you set this value too low, flow information might get lost!
Sampling Mode	Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between: ▪ Off: The standard flow will be used. ▪ On: Switch into sampling mode and specify the sampling rate below.
Sampling Rate	This field is only visible when sampling mode is enabled above. Enter a number that matches the sampling rate in your exporter device. If the number is different, monitoring results will be incorrect. Please enter an integer value.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to the data folder (see Data Storage ²⁰³⁶). Choose between: ▪ None (recommended): Do not write additional log files. Recommended for normal use cases. ▪ Only for the 'Other' channel: Only write log files of data that is not filtered otherwise and therefore accounted to the default Other channel. ▪ All stream data: Write log files for all data received.

jFlow V5 Specific Settings

Note: Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Channel Configuration**Channel Selection**

Define the categories the traffic will be accounted to. There are different groups of traffic available. Choose between:

- **Web:** Internet web traffic.
- **File Transfer:** Traffic caused by FTP.
- **Mail:** Internet mail traffic.
- **Chat:** Traffic caused by chat and instant messaging.
- **Remote Control:** Traffic caused by remote control applications, such as RDP, SSH, Telnet, VNC.
- **Infrastructure:** Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, SNMP.
- **NetBIOS:** Traffic caused by NetBIOS communication.
- **Other Protocols:** Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, i.e. how detailed traffic will be divided. For each group, choose between:

- **No:** Do not account traffic of this group in an own channel. All traffic of this group will be accounted to the default channel named **Other**.
- **Yes:** Count all traffic of this group and summarize it into one channel.
- **Detail:** Count all traffic of this group and further divide it into different channels. The traffic will appear in several channels as shown in the **Content** column. **Note:** Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyse.

Filtering**Include Filter**

Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#) ¹⁹⁹⁴

Filtering	
	section.
Exclude Filter	First, the filters defined in the Include Filter field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors ¹⁹⁹⁴ section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ Top Talkers ▪ Top Connections ▪ Top Protocols ▪ [Any custom toplists you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail. For more information, please see [Toplists](#)¹⁷⁰² section.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁴
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁸

6.8.51 jFlow V5 (Custom) Sensor

The jFlow V5 (Custom) sensor receives traffic data from a jFlow V5 compatible device and shows the traffic by type. On your hardware device, please make sure it matches jFlow V5 and disable any sampling option! In this custom sensor, you can define your own channel definitions to divide traffic into different channels.

Note: In order for the sensor to work, jFlow export of the respective version must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe). The sensor does not support sampling, so please disable sampling in your jFlow device! This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

For a general introduction to the technology behind flow monitoring, please see [Monitoring Bandwidth via Flows](#)¹⁹³⁴ section.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name

Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
jFlow Specific Settings	
Receive jFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one configured in the jFlow export options of your hardware router device. Please enter an integer value. Note: When configuring export, please make sure you select the appropriate jFlow version for this sensor.
Sender IP	Enter the IP address of the sending device you want to receive the jFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive jFlow Packets on IP	Select the IP address(es) on which PRTG listens to jFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the jFlow export options of your hardware router device. Note: When configuring export, please make sure you select the appropriate jFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an Unknown status. Please enter an integer value. We recommend setting this one minute longer than the respective timeout configured in your hardware router device. Note: If you set this value too low, flow information might get lost!
Sampling Mode	Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between: ▪ Off: The standard flow will be used. ▪ On: Switch into sampling mode and specify the sampling rate below.

jFlow Specific Settings	
Sampling Rate	This field is only visible when sampling mode is enabled above. Enter a number that matches the sampling rate in your exporter device. If the number is different, monitoring results will be incorrect. Please enter an integer value.
Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see Channel Definitions for xFlow and Packet Sniffer Sensors ¹⁹⁹⁸ section. All traffic for which no channel is defined will be accounted to the default channel named Other . Note: Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyse.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to the data folder (see Data Storage²⁰³⁶). Choose between: ▪ None (recommended): Do not write additional log files. Recommended for normal use cases. ▪ Only for the 'Other' channel: Only write log files of data that is not filtered otherwise and therefore accounted to the default Other channel. ▪ All stream data: Write log files for all data received. Note: Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.
Filtering	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors ¹⁹⁹⁴ section.
Exclude Filter	First, the filters defined in the Include Filter field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors ¹⁹⁹⁴ section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ Top Talkers ▪ Top Connections ▪ Top Protocols ▪ [Any custom toplist you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail. For more information, please see [Toplists](#)^[1702] section.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)^[1994]
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)^[1998]

6.8.52 LDAP Sensor

The LDAP sensor monitors directory services using Lightweight Directory Access Protocol (LDAP), connecting to the server trying a "bind". It shows the response time. If the server does not respond or authentication fails, an error message will be triggered.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
LDAP Specific	
Port	Enter the LDAP port number, usually port 389 for unencrypted connections. Please enter an integer value.
Distinguished Name	Enter the Distinguished Name (DN) you want to authenticate to the LDAP server. Usually, this is the information for the user you want to authenticate with. For example, use the format cn=Manager,dc=my-domain,dc=com for a DN on an OpenLDAP server.

LDAP Specific	
Passwort	Enter the password for the entered Distinguished Name.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1688] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.53 Microsoft SQL Sensor

The Microsoft SQL sensor monitors a Microsoft Structured Query Language (SQL) server. It shows the response time, the number of records, and the value. The sensor can monitor if the database server accepts connections, processes requests, and returns an expected result when executing a custom SQL command.

The following SQL servers are supported: SQL Server 2008, SQL Server 2005 (including SQL Server Express / Server Compact Editions), SQL Server 2000, SQL Server 7 and MSDE (requires OLE DB installed on the machine running the PRTG probe that accesses the server)

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
SQL-Server Specific Data	
Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

SQL-Server Specific Data	
Instance	Enter the SQL server instance's name if you want to connect to a "named instance". For example, such an instance's name could be SQLEXPRESS . Note: Sometimes you will see connection strings like SQLSERVER\SQLINSTANCE in database clients. The first part is the server name configured under the general server settings. The second part refers to the instance name mentioned above. Never enter this complete string in this PRTG form, merely provide the second part (without the backslash). Please enter a string or leave the field empty.
Port	Define the port for the SQL connection. Choose between: ▪ Automatic: Automatically choose the right port. ▪ Manual: Use a specific port. Define below. Standard value is 1433.
Port	This field is only visible if manual port selection is enabled above. Define the port number for the SQL connection. Please enter an integer value.

Database	
Database	Enter the name of the SQL database the sensor will connect to. For example, such a database's name could be Northwind
Authentication	Define the kind of authentication used for the connection to the database. Choose between: ▪ SQL Server: Use credentials specific to the SQL server. Please enter them below. ▪ Windows Authentication: Use the Windows credentials defined for the parent device this sensor is created on. Note: For successful authentication, the defined Windows credentials must be known to the SQL server, and SQL server and the computer the PRTG probe is running on must be in the same domain.
User	This field is only visible if SQL server authentication is enabled above. Enter the user name that will be used for the database connection.
Password	This field is only visible if SQL server authentication is enabled above. Enter the password that will be used for the database connection.

Data	
SQL Expression	Enter a valid SQL statement to execute on the server. In your SELECT statement, please specify the field name explicitly. Do not use SELECT *! For example, a correct expression could be: SELECT ProductName FROM Northwind.dbo.Products. When a cursor is returned (i.e. with a SELECT statement), only the first row of data will be processed. Note: Executing stored procedures is currently not supported.
Record Count	If you want to know how many records in your database were affected by your SQL expression as defined above, you can count the number of concerned records. Choose between: ▪ Do not count number of records: Affected records will not be counted. ▪ Count number of records: The number of affected records will be counted. Note: Enabling this option might increase the execution time of this sensor.
Post-Processing	If the SQL expression returns a result set, please define if you want to further process it. Choose between: ▪ Ignore result set: Do not do anything with the data returned. ▪ Process numerical result: Regard the result set returned as integer or float. You can set the sensor to Warning or Down status for specific thresholds. Define below. ▪ Process string result: Regard the result set returned as a string. You can set the sensor to error for certain sub-strings contained or missing. Define below. ▪ Monitor for changes: Monitor if the result set has changed since last check. The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever a sensor value changes.
Condition "Warning"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a Warning status. Choose between: ▪ none: Do not set the sensor to Warning status for any condition. ▪ equals: Result set must be the same as the value provided below. ▪ is above: Result set must be above the value provided below. ▪ lower than: Result set must be below the value provided below.

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
53 Microsoft SQL Sensor

	▪ does not equal: Result set must be unequal to the value provided below. Note: This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings .
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor into a Warning status. Please enter an integer or float value.
Condition "Down"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a Down status. Choose between: ▪ none: Do not set the sensor to Down status for any condition. ▪ equals: Result set must be the same as the value provided below. ▪ is above: Result set must be above the value provided below. ▪ lower than: Result set must be below the value provided below. ▪ does not equal: Result set must be unequal to the value provided below. Note: This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings .
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor to a Down status. Please enter an integer value.
Response Must Include	This field is only visible if string results is enabled above. Enter a string that must be part of the returned SQL string. If it is not, the sensor will be set to an error state. Please enter a string or leave the field empty.
Response Must Not include	This field is only visible if string results is enabled above. Enter a string that must not be part of the returned SQL string. If it is, the sensor will be set to an error state. Please enter a string or leave the field empty.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.

Sensor Display	
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹². Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.54 MySQL Sensor

The MySQL sensor monitors a MySQL server. It connects to the server and shows the response time. Additionally, it can read the number of records and a value.

The following SQL servers are supported: MySQL server 5.1, 5.0, 4.1, 4.0, and 3.23

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
MySQL Server Specific Data	
Port	Define the port for the SQL connection. Choose between: ▪ Automatic: Automatically choose the right port. ▪ Manual: Use a specific port. Define below. Standard value is 3306.

MySQL Server Specific Data	
Timeout (sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

DB/SQL Data	
Database	Enter the name of the SQL database the sensor will connect to. For example, such a database's name could be MyDatabase . This is a logical entity on the database server where database objects like tables or stored procedures exist. In case of the MySQL server it also reflects a physical directory structure where your database objects are stored. Enter the appropriate string which is the same as you would supply when invoking the mysql.exe admin tool (with the command line switch -p) or after the login with mysql.exe with the command use .
User	Enter the user name that will be used for the database connection.
Password	Enter the password that will be used for the database connection.

Data	
SQL Expression	Enter a valid SQL statement to execute on the server. In your SELECT statement, please specify the field name explicitly. Do not use SELECT * ! For example, a correct expression could be: SELECT AVG(UnitPrice) FROM Products . When a cursor is returned (i.e. with a SELECT statement), only the first row of data will be processed.
Record Count	If you want to know how many records in your database were affected by your SQL expression as defined above, you can count the number of concerned records. Choose between: ▪ Do not count number of records: Affected records will not be counted. ▪ Count number of records: The number of affected records will be counted. Note: Enabling this option might increase the execution time of this sensor.
Post-Processing	If the SQL expression returns a result set, please define if you want to further process it. Choose between: ▪ Ignore result set: Do not do anything with the data returned.

	▪ Process numerical result: Regard the result set returned as integer or float. You can set the sensor to Warning or Down status for specific thresholds. Define below. ▪ Process string result: Regard the result set returned as a string. You can set the sensor to error for certain sub-strings contained or missing. Define below. ▪ Monitor for changes: Monitor if the result set has changed since last check. The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever a sensor value changes.
Condition "Warning"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a Warning status. Choose between: ▪ none: Do not set the sensor to Warning status for any condition. ▪ equals: Result set must be the same as the value provided below. ▪ is above: Result set must be above the value provided below. ▪ lower than: Result set must be below the value provided below. ▪ does not equal: Result set must be unequal to the value provided below. Note: This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings.
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor into a Warning status. Please enter an integer or float value.
Condition "Down"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a Down status. Choose between: ▪ none: Do not set the sensor to Down status for any condition. ▪ equals: Result set must be the same as the value provided below. ▪ is above: Result set must be above the value provided below. ▪ lower than: Result set must be below the value provided below. ▪ does not equal: Result set must be unequal to the value provided below. Note: This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings.

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

54 MySQL Sensor

Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor to a Down status. Please enter an integer value.
Response Must Include	This field is only visible if string results is enabled above. Enter a string that must be part of the returned SQL string. If it is not, the sensor will be set to an error state. Please enter a string or leave the field empty.
Response Must Not include	This field is only visible if string results is enabled above. Enter a string that must not be part of the returned SQL string. If it is, the sensor will be set to an error state. Please enter a string or leave the field empty.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Note: For this sensor type, no port number can be set.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁹⁰ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.55 NetFlow V5 Sensor

The NetFlow V5 sensor receives traffic data from a NetFlow V5 compatible device and shows the traffic by type. Please make sure the sensor matches the NetFlow version your device is exporting! There are several filter options available to divide traffic into different channels.

Note: In order for the sensor to work, NetFlow export of the respective version must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe). This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

For a general introduction to the technology behind flow monitoring, please see [Monitoring Bandwidth via Flows](#)^[1904] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

NetFlow Specific Settings	
Receive NetFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the NetFlow export options of your hardware router device. Please enter an integer value. Note: When configuring export, please make sure you select the appropriate NetFlow version for this sensor.
Sender IP	Enter the IP address of the sending device you want to receive the NetFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive NetFlow Packets on IP	Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the NetFlow export options of your hardware router device. Note: When configuring export, please make sure you select the appropriate NetFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an Unknown status. Please enter an integer value. We recommend setting this one minute longer than the respective timeout configured in your hardware router device. Note: If you set this value too low, flow information might get lost!
Sampling Mode	Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between: ▪ Off: The standard flow will be used. ▪ On: Switch into sampling mode and specify the sampling rate below.
Sampling Rate	This field is only visible when sampling mode is enabled above. Enter a number that matches the sampling rate in your exporter device. If the number is different, monitoring results will be incorrect. Please enter an integer value.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to the data folder (see Data Storage). Choose between: ▪ None (recommended): Do not write additional log files. Recommended for normal use cases. ▪ Only for the 'Other' channel: Only write log files of data that is not filtered otherwise and therefore accounted to the default Other channel. ▪ All stream data: Write log files for all data received.

NetFlow Specific Settings

Note: Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Channel Configuration**Channel Selection**

Define the categories the traffic will be accounted to. There are different groups of traffic available. Choose between:

- **Web:** Internet web traffic.
- **File Transfer:** Traffic caused by FTP.
- **Mail:** Internet mail traffic.
- **Chat:** Traffic caused by chat and instant messaging.
- **Remote Control:** Traffic caused by remote control applications, such as RDP, SSH, Telnet, VNC.
- **Infrastructure:** Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, SNMP.
- **NetBIOS:** Traffic caused by NetBIOS communication.
- **Other Protocols:** Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, i.e. how detailed traffic will be divided. For each group, choose between:

- **No:** Do not account traffic of this group in an own channel. All traffic of this group will be accounted to the default channel named **Other**.
- **Yes:** Count all traffic of this group and summarize it into one channel.
- **Detail:** Count all traffic of this group and further divide it into different channels. The traffic will appear in several channels as shown in the **Content** column. **Note:** Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyse.

Filtering**Include Filter**

Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#) ¹⁹⁹⁴

Filtering	
	section.
Exclude Filter	First, the filters defined in the Include Filter field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors ¹⁹⁹⁴ section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ Top Talkers ▪ Top Connections ▪ Top Protocols ▪ [Any custom toplist you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail. For more information, please see [Toplists](#)¹⁷⁰² section.

More

Paessler Website: Paessler NetFlow Testers

- <http://www.paessler.com/tools/netflowtester>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹¹ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁴
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁸

6.8.56 NetFlow V5 (Custom) Sensor

The NetFlow V5 (Custom) sensor receives traffic data from a NetFlow V5 compatible device and shows the traffic by type. Please make sure the sensor matches the NetFlow version your device is exporting! In this custom sensor, you can define your own channel definitions to divide traffic into different channels.

Note: In order for the sensor to work, NetFlow export of the respective version must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe). This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

For a general introduction to the technology behind flow monitoring, please see [Monitoring Bandwidth via Flows](#)^[1994] section.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[226]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

NetFlow Specific Settings

Receive NetFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one configured in the NetFlow export options of your hardware router device. Please enter an integer value. Note: When configuring export, please make sure you select the appropriate NetFlow version for this sensor.
Sender IP	Enter the IP address of the sending device you want to receive the NetFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive NetFlow Packets on IP	Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the NetFlow export options of your hardware router device. Note: When configuring export, please make sure you select the appropriate NetFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an Unknown status. Please enter an integer value. We recommend setting this one minute longer than the respective timeout configured in your hardware router device. Note: If you set this value too low, flow information might get lost!
Sampling Mode	Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between: ▪ Off: The standard flow will be used. ▪ On: Switch into sampling mode and specify the sampling rate below.
Sampling Rate	This field is only visible when sampling mode is enabled above. Enter a number that matches the sampling rate in your device. If the number is different, monitoring results will be incorrect. Please enter an integer value.

NetFlow Specific Settings

Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors¹⁹⁹⁸ section. All traffic for which no channel is defined will be accounted to the default channel named Other. Note: Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to the data folder (see Data Storage²⁰³⁶). Choose between: ▪ None (recommended): Do not write additional log files. Recommended for normal use cases. ▪ Only for the 'Other' channel: Only write log files of data that is not filtered otherwise and therefore accounted to the default Other channel. ▪ All stream data: Write log files for all data received. Note: Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Filtering

Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors¹⁹⁹⁴ section.
Exclude Filter	First, the filters defined in the Include Filter field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors¹⁹⁹⁴ section.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor.

Sensor Display	
	▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ Top Talkers ▪ Top Connections ▪ Top Protocols ▪ [Any custom toplist you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail. For more information, please see [Toplists](#)¹⁷⁰² section.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁴
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁸

6.8.57 NetFlow V9 Sensor

The NetFlow V9 sensor receives traffic data from a NetFlow V9 compatible device and shows the traffic by type. Please make sure the sensor matches the NetFlow version your device is exporting! There are several filter options available to divide traffic into different channels.

Note: In order for the sensor to work, NetFlow export of the respective version must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe). This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

For a general introduction to the technology behind flow monitoring, please see [Monitoring Bandwidth via Flows](#)^[1904] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

NetFlow Specific Settings	
Receive NetFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the NetFlow export options of your hardware router device. Please enter an integer value. Note: When configuring export, please make sure you select the appropriate NetFlow version for this sensor.
Sender IP	Enter the IP address of the sending device you want to receive the NetFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive NetFlow Packets on IP	Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the NetFlow export options of your hardware router device. Note: When configuring export, please make sure you select the appropriate NetFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an Unknown status. Please enter an integer value. We recommend setting this one minute longer than the respective timeout configured in your hardware router device. Note: If you set this value too low, flow information might get lost!
Sampling Mode	Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between: ▪ Off: The standard flow will be used. ▪ On: Switch into sampling mode and specify the sampling rate below.
Sampling Rate	This field is only visible when sampling mode is enabled above. Enter a number that matches the sampling rate in your exporter device. If the number is different, monitoring results will be incorrect. Please enter an integer value.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to the data folder (see Data Storage ²⁰³⁶). Choose between: ▪ None (recommended): Do not write additional log files. Recommended for normal use cases. ▪ Only for the 'Other' channel: Only write log files of data that is not filtered otherwise and therefore accounted to the default Other channel. ▪ All stream data: Write log files for all data received.

NetFlow Specific Settings

Note: Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Channel Configuration**Channel Selection**

Define the categories the traffic will be accounted to. There are different groups of traffic available. Choose between:

- **Web:** Internet web traffic.
- **File Transfer:** Traffic caused by FTP.
- **Mail:** Internet mail traffic.
- **Chat:** Traffic caused by chat and instant messaging.
- **Remote Control:** Traffic caused by remote control applications, such as RDP, SSH, Telnet, VNC.
- **Infrastructure:** Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, SNMP.
- **NetBIOS:** Traffic caused by NetBIOS communication.
- **Other Protocols:** Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, i.e. how detailed traffic will be divided. For each group, choose between:

- **No:** Do not account traffic of this group in an own channel. All traffic of this group will be accounted to the default channel named **Other**.
- **Yes:** Count all traffic of this group and summarize it into one channel.
- **Detail:** Count all traffic of this group and further divide it into different channels. The traffic will appear in several channels as shown in the **Content** column. **Note:** Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyse.

Filtering**Include Filter**

Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#) ¹⁹⁹⁴

Filtering	
	section.
Exclude Filter	First, the filters defined in the Include Filter field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors ¹⁹⁹⁴ section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ Top Talkers ▪ Top Connections ▪ Top Protocols ▪ [Any custom toplists you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail. For more information, please see [Toplists](#)¹⁷⁰² section.

More

Paessler Website: Paessler NetFlow Testers

- <http://www.paessler.com/tools/netflowtester>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁴
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁸

6.8.58 NetFlow V9 (Custom) Sensor

The NetFlow V9 (Custom) sensor receives traffic data from a NetFlow V9 compatible device and shows the traffic by type. Please make sure the sensor matches the NetFlow version your device is exporting! In this custom sensor, you can define your own channel definitions to divide traffic into different channels.

Note: In order for the sensor to work, NetFlow export of the respective version must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe). This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

For a general introduction to the technology behind flow monitoring, please see [Monitoring Bandwidth via Flows](#)^[1994] section.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[226]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

NetFlow Specific Settings

Receive NetFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one configured in the NetFlow export options of your hardware router device. Please enter an integer value. Note: When configuring export, please make sure you select the appropriate NetFlow version for this sensor.
Sender IP	Enter the IP address of the sending device you want to receive the NetFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive NetFlow Packets on IP	Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the NetFlow export options of your hardware router device. Note: When configuring export, please make sure you select the appropriate NetFlow version for this sensor.
Active Flow Timeout (Minutes)	Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an Unknown status. Please enter an integer value. We recommend setting this one minute longer than the respective timeout configured in your hardware router device. Note: If you set this value too low, flow information might get lost!
Sampling Mode	Define if you want to use the sampling mode. This setting must accord to the setting in the flow exporter. Choose between: ▪ Off: The standard flow will be used. ▪ On: Switch into sampling mode and specify the sampling rate below.
Sampling Rate	This field is only visible when sampling mode is enabled above. Enter a number that matches the sampling rate in your device. If the number is different, monitoring results will be incorrect. Please enter an integer value.

NetFlow Specific Settings

Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors¹⁹⁹⁸ section. All traffic for which no channel is defined will be accounted to the default channel named Other. Note: Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to the data folder (see Data Storage²⁰³⁶). Choose between: ▪ None (recommended): Do not write additional log files. Recommended for normal use cases. ▪ Only for the 'Other' channel: Only write log files of data that is not filtered otherwise and therefore accounted to the default Other channel. ▪ All stream data: Write log files for all data received. Note: Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Filtering

Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors¹⁹⁹⁴ section.
Exclude Filter	First, the filters defined in the Include Filter field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors¹⁹⁹⁴ section.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor.

Sensor Display	
	▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ Top Talkers ▪ Top Connections ▪ Top Protocols ▪ [Any custom toplist you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail. For more information, please see [Toplists](#)¹⁷⁰² section.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁴
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁸

6.8.59 Oracle SQL Sensor

The Oracle SQL sensor monitors an Oracle SQL server. It connects to the server and shows the response time (measured from the time when the connection is opened to the time when the return values of the SQL query—if configured—have been received). Additionally, it can read the number of records and a value.

The following SQL servers are supported: Supports Oracle servers 11g, 10g, 9i, 8i, 8.0, and 7.3, including Oracle 10g Express, and Oracle 8i Personal and Lite editions (requires default TCP port setting 1521).

Note: On the client computer running the PRTG probe where this sensor is created on, **Oracle Net** is used for direct TCP/IP communication; OCI is not supported any more. You do not need to install an Oracle client or define a **TNSNAMES.ORA** on the client computer.

Note: With **Oracle version 11.2.0.4**, Oracle's TCP/IP authentication method has changed. You will encounter connection problems with credential errors when using the direct connection mode as of this Oracle version. In this case, please install the 32-bit Oracle client on the machine which is running the PRTG probe and choose **Use Oracle client** as connection mode in the sensor settings.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Oracle Specific Data

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port	Enter the port number that will be used for the connection. Default value is 1521 . Please enter an integer value.
Connection Mode	Select which mode you want to use to connect to the Oracle server. Choose between: ▪ Use direct mode (TCP/IP): Use Oracle Net for direct TCP/IP communication. Note: As of Oracle version 11.2.0.4, please use the Oracle client (see sensor description above). ▪ Use Oracle client: Use the Oracle client for communication. It needs to be installed the machine which is running the PRTG probe.

DB/SQL Data

Service Name / Alias	Enter the name of the SQL database the sensor will connect to. For example, such a database's name could be orcl
User	Enter the user name that will be used for the database connection.
Password	Enter the password that will be used for the database connection.

Data

SQL Expression	Enter a valid SQL statement to execute on the server. In your SELECT statement, please specify the field name explicitly. Do not use SELECT * ! For example, a correct expression could be: SELECT sum(salary) FROM hr.employees . When a cursor is returned (i.e. with a SELECT statement), only the first row of data will be processed.

Record Count	If you want to know how many records in your database were affected by your SQL expression as defined above, you can count the number of concerned records. Choose between: ▪ Do not count number of records: Affected records will not be counted. ▪ Count number of records: The number of affected records will be counted. Note: Enabling this option might increase the execution time of this sensor.
Post-Processing	If the SQL expression returns a result set, please define if you want to further process it. Choose between: ▪ Ignore result set: Do not do anything with the data returned. ▪ Process numerical result: Regard the result set returned as integer or float. You can set the sensor to Warning or Down status for specific thresholds. Define below. ▪ Process string result: Regard the result set returned as a string. You can set the sensor to error for certain sub-strings contained or missing. Define below. ▪ Monitor for changes: Monitor if the result set has changed since last check. The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever a sensor value changes.
Condition "Warning"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a Warning status. Choose between: ▪ none: Do not set the sensor to Warning status for any condition. ▪ equals: Result set must be the same as the value provided below. ▪ is above: Result set must be above the value provided below. ▪ lower than: Result set must be below the value provided below. ▪ does not equal: Result set must be unequal to the value provided below. Note: This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings.
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor into a Warning status. Please enter an integer or float value.

Condition "Down"	This field is only visible if numeric results is enabled above. Define a condition of the returned numeric SQL result set that will set the sensor to a Down status. Choose between: ▪ none: Do not set the sensor to Down status for any condition. ▪ equals: Result set must be the same as the value provided below. ▪ is above: Result set must be above the value provided below. ▪ lower than: Result set must be below the value provided below. ▪ does not equal: Result set must be unequal to the value provided below. Note: This threshold check the SQL result set only. You can set additional thresholds in the sensor's channel settings 1683.
Value	This field is only visible if numeric results is enabled above. Enter a value of the returned numeric SQL result set that will set the sensor to a Down status. Please enter an integer value.
Response Must Include	This field is only visible if string results is enabled above. Enter a string that must be part of the returned SQL string. If it is not, the sensor will be set to an error state. Please enter a string or leave the field empty.
Response Must Not include	This field is only visible if string results is enabled above. Enter a string that must not be part of the returned SQL string. If it is, the sensor will be set to an error state. Please enter a string or leave the field empty.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 1685 settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

More

Knowledge Base: How do PRTG sensors connect to Oracle databases?

- <http://www.paessler.com/knowledgebase/en/topic/52803>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#) section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#) section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.60 Packet Sniffer Sensor

Monitors the headers of data packets passing a local network card using built-in packet sniffer. You can choose from predefined channels. Only header traffic will be analyzed.

Note: This sensor can be set up on a Probe Device only! By default, you can only monitor traffic passing the PRTG probe system on which's **Probe Device** the sensor is set up (either a local or remote probe). To monitor other traffic in your network, you can configure a monitoring port (if available) to which the switch sends a copy of all traffic. You can then physically connect this port to a network card of the computer the PRTG probe (either local or remote probe) is running on. This way, PRTG will be able to analyze the complete traffic that passes through the switch. This feature of your hardware may be called Switched Port Analyzer (SPAN), port mirroring, or port monitoring.

For a general introduction to the technology behind packet sniffing, please see [Monitoring Bandwidth via Packet Sniffing](#)^[1932] section.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sniffer Specific

Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors ¹⁹⁹⁴ section.
Exclude Filter	First, the filters defined in the Include Filter field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors ¹⁹⁹⁴ section.
Network Adapters	Define the network adapters that will be monitored by the sensor. You see a list of names with all adapters available on the probe system. To select an adapter, set a check mark symbol in front of the respective name.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to the data folder (see Data Storage²⁰³⁶). Choose between: ▪ None (recommended): Do not write additional log files. Recommended for normal use cases. ▪ Only for the 'Other' channel: Only write log files of data that is not filtered otherwise and therefore accounted to the default Other channel. ▪ All stream data: Write log files for all data received. Note: Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Channel Configuration

Channel Selection	Define the categories the traffic will be accounted to. There are different groups of traffic available. Choose between: ▪ Web: Internet web traffic. ▪ File Transfer: Traffic caused by FTP.

Channel Configuration	
	▪ Mail: Internet mail traffic. ▪ Chat: Traffic caused by chat and instant messaging. ▪ Remote Control: Traffic caused by remote control applications, such as RDP, SSH, Telnet, VNC. ▪ Infrastructure: Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, SNMP. ▪ NetBIOS: Traffic caused by NetBIOS communication. ▪ Other Protocols: Traffic caused by various other protocols via UDP and TCP. For each traffic group, you can select how many channels will be used for each group, i.e. how detailed traffic will be divided. For each group, choose between: ▪ No: Do not account traffic of this group in an own channel. All traffic of this group will be accounted to the default channel named Other. ▪ Yes: Count all traffic of this group and summarize it into one channel. ▪ Detail: Count all traffic of this group and further divide it into different channels. The traffic will appear in several channels as shown in the Content column. Note: Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyse.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings  settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist**Primary Toplist**

Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from:

- **Top Talkers**
- **Top Connections**
- **Top Protocols**
- **[Any custom toplist you have added]**

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#) ¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail. For more information, please see [Toplists](#)  section.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)  section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)  section.

Others

For more general information about settings, please see [Object Settings](#)  section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#) 
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#) 

6.8.61 Packet Sniffer (Custom) Sensor

Monitors the headers of data packets passing a local network card using built-in packet sniffer. You can define your own channels. There are no predefined channels for this sensor type. Only header traffic will be analyzed.

Note: This sensor can be set up on a Probe Device only! By default, you can only monitor traffic passing the PRTG probe system on which's **Probe Device** the sensor is set up (either a local or remote probe). To monitor other traffic in your network, you can configure a monitoring port (if available) to which the switch sends a copy of all traffic. You can then physically connect this port to a network card of the computer the PRTG probe (either local or remote probe) is running on. This way, PRTG will be able to analyze the complete traffic that passes through the switch. This feature of your hardware may be called Switched Port Analyzer (SPAN), port mirroring, or port monitoring.

For a general introduction to the technology behind packet sniffing, please see [Monitoring Bandwidth via Packet Sniffing](#)¹⁹³² section.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name

Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Sniffer specific	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors ^[1994] section.
Exclude Filter	First, the filters defined in the Include Filter field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow and Packet Sniffer Sensors ^[1994] section.
Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see Channel Definitions for xFlow and Packet Sniffer Sensors ^[1990] section. All traffic for which no channel is defined will be accounted to the default channel named Other . Note: Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyse. We recommend to not use more than 20 channels in graphs and tables, and not more than 100 channels in total. For performance reasons, it is better to add several sensors with less channels each.
Network Adapters	Define the network adapters that will be monitored by the sensor. You see a list of names with all adapters available on the probe system. To select an adapter, set a check mark symbol in front of the respective name.
Log Stream Data to Disk (for Debugging)	Define if the probe will write a log file of the stream and packet data to the data folder (see Data Storage ^[2036]). Choose between: ▪ None (recommended): Do not write additional log files. Recommended for normal use cases.

Sniffer specific	
	▪ Only for the 'Other' channel: Only write log files of data that is not filtered otherwise and therefore accounted to the default Other channel. ▪ All stream data: Write log files for all data received. Note: Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.
Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ Top Talkers ▪ Top Connections ▪ Top Protocols ▪ [Any custom toplist you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail. For more information, please see [Toplists](#)¹⁷⁰² section.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁴
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁸

6.8.62 Passive Application Performance Sensor

The Passive Application Performance sensor monitors Transport Control Protocol (TCP) connection timings using packet sniffer. It can measure the performance of many different web applications without actually having direct access to neither the client nor the server. In order to obtain valuable data, these applications must work TCP-based and initiate a new session with each request.

The sensor shows the total number of packets per second on the selected network card, the number of dropped packets per second by PRTG because of system overload (more processor power is required if this value is above zero to cope with the traffic), as well as the number of currently active connections on all monitored applications.

For defined applications, the sensor can show (together with the corresponding application name):

- Request time in msec: average time between the initial (SYN) packet from the client and the first request package from the client
- Response time in msec: average time between the initial (SYN) packet from the client and first packet of the result from the server
- ACK (acknowledge) time in msec: average time between the initial (SYN) packet of a connection from the client until the server sends an ACK (acknowledge) packet. This means that a TCP connection was successfully established (in LANs this value is zero in most cases and only increases for extreme loads).
- Count: total number of observed connections to the service in the last monitoring interval. This is the number of measurements the average is based on. The higher the value the more reliable/averaged the data is. If this value is zero, PRTG did not see any packets for this service.

Important notice: This sensor is an experimental sensor. Currently, it is in **beta** status. The methods of operating can change at any time, as well as the available settings. **Do not expect** that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

For a general introduction to the technology behind packet sniffing, please see [Monitoring Bandwidth via Packet Sniffing](#)^[1932] section.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Applications	
Network Adapter	Select the network adapter you want to monitor.
Applications	Define the applications you want to monitor. For each application, use one dedicated line. Use the following syntax to define an application to be monitored: ip:port=application . Provide the IP address and port number of the application. Behind the equals sign, enter a name for the application which will be displayed in the channels. Please enter a string. This sensor will create four sensor channels with the application name, e.g., "Application (ACK)".

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.

Sensor Display	
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹¹. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.63 PerfCounter Custom Sensor

The PerfCounter Custom sensor monitors a configured set of Windows Performance Counters. You can define your own channels. There are no predefined channels available for this sensor type. To find out which performance counters are available on the target system and what their names are, please see section [More](#)^[747].

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible.

Note: The user account has to be a member of the **Performance Monitor Users** user group on the target system.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the **RemoteRegistry** "Remote Registry" Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible.

To enable the service, please log in to the respective computer and open the services manager (e.g. via **services.msc**). In the list, find the respective service and set its **Start Type** to **Automatic**.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[2012]. **Note:** The target system may well run on Windows 2003 or later.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Performance Counter Settings	
List of Counters	Enter a list of performance counters which will be queried. Define one counter per row. PRTG will create one channel for each counter. Use the following syntax: the name of the counter, followed by two colons (::) and the unit. Example: <code>\Processor(_Total)\% Processor Time::%</code>
Mode	This setting determines if the returning value will be displayed as absolute value or if the difference between the last and the current value will be used. Choose between: ▪ Absolute (recommended): The returning value will be displayed as absolute value. ▪ Difference: The difference between last and current value will be displayed. Note: Please make sure that all counters which are monitored are capable of this mode if you select it.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Performance Counter Settings	
List of Counters	The list of counters monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Mode	The mode in which the returning values are displayed. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: How can I find out the names of available Performance Counters?

- <http://www.paessler.com/knowledgebase/en/topic/50673>

Knowledge Base: Remote Monitoring of Specific Performance Counters

- <http://www.paessler.com/knowledgebase/en/topic/59804>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.64 PerfCounter IIS Application Pool Sensor

The PerfCounter IIS Application Pool sensor monitors a Microsoft Internet Information Services (IIS) application pool using Windows Performance Counters. This sensor can show the overall state of an application pool, the number of worker processes, the number of failures in worker processes, as well as the number of ping failures, shutdown failures, and startup failures in worker processes.

Requirement: Microsoft IIS Version 7.5

In order to monitor Microsoft Internet Information Services (IIS) application pools, this sensor needs IIS version 7.5 or later to be installed on the target system.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible.

Note: The user account has to be a member of the **Performance Monitor Users** user group on the target system.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the **RemoteRegistry** "Remote Registry" Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible.

To enable the service, please log in to the respective computer and open the services manager (e.g. via **services.msc**). In the list, find the respective service and set its **Start Type** to **Automatic**.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[2012]. **Note:** The target system may well run on Windows 2003 or later.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor Microsoft Internet Information Services (IIS) application pools, PRTG will create one sensor for each pool. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

IIS Application Pool Specific

Application Pool	A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

IIS Application Pool Specific

Application Pool	The name of the application pool that is monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration settings.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.65 Ping Sensor

The Ping sensor sends an Internet Control Message Protocol (ICMP) echo request ("Ping") from the computer running the probe to the device it is created on, in order to monitor the availability of a device. When using more than one Ping per interval, it also measures minimum and maximum Ping time as well as packet loss in percent.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[226]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Ping Settings	
Timeout (seconds)	Enter a timeout in seconds for the Ping. If the reply takes longer than this value the request is aborted and an error message is triggered.
Packet Size (Bytes)	Enter the packet size in bytes for the Ping. You can choose any value between 1 and 10000 . We recommend using the default value.

Ping Settings	
Ping Method	Define the kind of Ping check that will be performed. Choose between: ▪ Send one single Ping: With each scanning interval, send a single Ping only. A sensor in this setting will show the Ping time only. This setting is good for simply availability monitoring. ▪ Send multiple Ping request: With each scanning interval, send multiple Pings in a row. A sensor in this setting will also show minimum and maximum Ping time as well as packet loss (in percent). This setting is good if you want to create reports about average Ping times out of a series of ping requests. Note: When using multiple request, all of them have to get lost in order for the sensor to switch to a Down status. For example, if there is only one Ping request answered in a series of five, the sensor will still show a green Up status.
Ping Count	This field is only visible if sending multiple Pings is enabled above. Enter the number of Pings that are sent in a row for one interval. Please enter an integer value.
Ping Delay (in ms)	This field is only visible if sending multiple Pings is enabled above. Enter the time in milliseconds PRTG has to wait between two Ping requests. Please enter an integer value. Note: Increase the value if the target device drops Ping packets due to denial-of-service (DOS) suspicion.
Auto Acknowledge	You can define that a Down status of this sensor will be acknowledged^[144] automatically. ▪ Show "Down" status on error (default): Do not automatically acknowledge an alarm if this sensor changes to a Down status. ▪ Show "Down (Acknowledged)" status on error: Automatically acknowledge an alarm. If this sensor changes to a Down status, it will automatically change to Down (Acknowledged). Note: The sensor will also go through a Down status, so any sensor state triggers^[1690] using this will still provoke notifications, as configured.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.

Sensor Display	
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹¹. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

More

Knowledge Base: How to create/customize statistical PING sensor?

- <http://www.paessler.com/knowledgebase/en/topic/1873>

Knowledge Base: Can I create an inverse Ping sensor?

- <http://www.paessler.com/knowledgebase/en/topic/10203>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[1441] section.

6.8.66 Ping Jitter Sensor

The Ping Jitter sensor sends a series of Internet Control Message Protocol (ICMP) echo requests ("Pings") to the given URI to determine the statistical jitter. The Real Time Jitter value is updated every time a packet is received using the formula described in RFC 1889:

$$\text{Jitter} = \text{Jitter} + (\text{abs}(\text{ElapsedTime} - \text{OldElapsedTime}) - \text{Jitter}) / 16$$

The Statistical Jitter value is calculated on the first x packets received using the statistical variance formula:

$$\text{Jitter Statistical} = \text{SquareRootOf}(\text{SumOf}((\text{ElapsedTime}[i] - \text{Average}) ^ 2) / (\text{ReceivedPacketCount} - 1))$$

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be

Basic Sensor Settings	
	shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Ping Count	Define the number of pings that will be sent. Please enter an integer value.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[168] settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1680] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.67 Pingdom Sensor

The Pingdom sensor queries an account at Pingdom.com and retrieves values for one "check" configured in the respective Pingdom account. With every scanning interval, the sensor will always catch the last value available in the "detailed check log" of your Pingdom account.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[202]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings

Pingdom Check Name	Enter the name of the "check" you want to retrieve data for. Enter it exactly the way configured in your Pingdom account. This setting is case sensitive! Please enter a string.
Username	Please enter the username of the Pingdom account you want to query. Please enter a string.
Password	Please enter the password of the Pingdom account you want to query. Please enter a string.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • Ignore changes (default): No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ . Note: Please make sure you select the same scanning interval you configured for the "check" in your Pingdom account. Only if the intervals match PRTG can catch every measurement from your "check".
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.68 POP3 Sensor

The POP3 sensor monitors a mail server using Post Office Protocol version 3 (POP3). It shows the response time of the server.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Pop3 Specific	
Timeout	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port	Specify the port that will be used for the POP3 connection. For non-secure connections usually port 110 is used; usually port 995 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
Security	Specify if an encryption will be used for the connection. Choose between: ▪ Encrypt data using Transport-Level Security (TLS) ▪ No encryption (use plain text)
SSL-Method	This field is only visible if security is enabled above. Select the SSL method that will be used when connecting to the server. We recommend using the default value. Only if you experience connection problems, try another setting. Choose between: ▪ SSL V2 ▪ SSL V2 or V3 ▪ SSL V3 ▪ TLS V1

Pop3 Authorisation	
POP3 Authentication Type	Select the kind of authentication for the POP3 connection. Choose between: • Without Login: Monitor the connection to the POP3 server only. • Username and Password: Log into the POP3 server with user name and password (simple login, non-secure). • 128-bit MD5 hash value (APOP): Send the password in an encrypted form using APOP. This option must be supported by the POP3 server you're connecting to.
Username	This field is only visible if an option with login is selected above. Enter a username for POP3 authentication. Please enter a string.
Password	This field is only visible if an option with login is selected above. Enter a password for POP3 authentication. Please enter a string.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1688] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.69 POP3 Email Count Sensor

The POP3 Email Count sensor connects to a POP3 email account and returns the number of emails stored in it. Additionally, you can filter by **to** or **from** address, or by **subject**, to only count mails matching the search pattern.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[202]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings

Username	Define the username of the POP3 account you want to log into. Note: As POP3 server, this sensor will use the parent device's IP Address/DNS Name value.
Password	Define the password for the POP3 account. Note: As POP3 server, this sensor will use the parent device's IP Address/DNS Name value.
Mailserver POP3 Port	Define the port number the POP3 server is running at. Please enter an integer value. Note: As POP3 server, this sensor will use the parent device's IP Address/DNS Name value.
Use SSL	Define whether to use SSL for the connection to the POP3 server. Choose between: ▪ No ▪ Yes Note: As POP3 server, this sensor will use the parent device's hostname.
Filter To Address	Optionally define a To address. Only mails containing this will be counted by the sensor. Please enter a string or leave the field empty.
Filter From Address	Optionally define a From address. Only mails containing this will be counted by the sensor. Please enter a string or leave the field empty.
Filter Subject Content	Optionally define an email Subject . Only mails containing this will be counted by the sensor. Please enter a string or leave the field empty.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁹⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.70 Port Sensor

The Port sensor monitors a network service by connecting to its port. It tries to connect to the specified TCP/IP port number of a device and waits for the request to be accepted. Depending on your settings, it can alert you either when the monitored port is open, or when it is closed.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[226]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Port Specific	
Timeout (sec.)	Enter a timeout in seconds for the port connect. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port	Enter the number of the port the sensor will try to connect to. Please enter an integer value.

Port Specific	
SSL (Secure Sockets Layer)	Specify if an encryption will be used for the connection. Choose between: ▪ Don't use SSL (recommended) ▪ Use SSL
SSL-Method	This field is only visible if security is enabled above. Select the SSL method that will be used when connecting to the server. We recommend using the default value. Only if you experience connection problems, try another setting. Choose between: ▪ SSL V2 ▪ SSL V2 or V3 ▪ SSL V3 ▪ TLS V1
Advanced Sensor Settings	
Goal	Define how the sensor will report on the port defined above. Choose between: ▪ Open: The sensor will return a green OK status if the port is open, and show a red Down status if the port is closed. ▪ Closed: The sensor will return a green OK status if the port is closed, and show a red Down status if the port is open.
Command	Define whether a command will be sent after the port is opened. Choose between: ▪ Don't send command: Only check if a connection to the port is possible. ▪ Send command: Open a Telnet session to the respective port and send the command. Note: You cannot use this option if the target machine is a webserver.
Command	This field is only visible if sending a command is enabled above. Enter a command that will be sent in Telnet session to the respective port. You cannot use line breaks, but a simple Telnet command in a single line only. Please enter a string.
Response	Define if the response received will be further processed. Choose between: ▪ Ignore response: Do not check the response.

Advanced Sensor Settings	
	▪ Check response code (integer): Check if the response matches a defined response code. Define below. ▪ Check response text: Check if the response matches a defined response text. Define below.
Allowed Code	This field is only visible if response code check is enabled above. Enter a code that must be returned. If it does not match the sensor will be set to a Down status. Please enter an integer value.
Check For Existing Keywords (Positive)	This setting is only visible if text processing is activated above. Check if a certain keyword is part of the received value. If there is no match, the sensor will show a "Down" status. ▪ Disable: Do not check for positive keywords. ▪ Enable keyword check (positive): Check if a certain keyword exists in the received value. Define below.
Text Must Include	This setting is only visible if keyword check is activated above. Enter a search string that must be contained in the returned value.
For Keyword Search Use	Define the method you want to provide the search string with. Choose between: ▪ Plain Text: Search for a simple string. ▪ Regular Expression: Search using a regular expression. For more details, see Regular Expressions ²⁰¹⁰ section.
Check For Existing Keywords (Negative)	This setting is only visible if text processing is activated above. Check if a certain keyword is not part of the received value. If there is a match, the sensor will show a "Down" status. ▪ Disable: Do not check for negative keywords. ▪ Enable keyword check (negative): Check if a certain keyword does not exist in the received value. Define below.
Text Must Not Include	This setting is only visible if keyword check is activated above. Enter a search string that must not be contained in the returned value.
For Keyword Search Use	Define the method you want to provide the search string with. Choose between: ▪ Plain Text: Search for a simple string. ▪ Regular Expression: Search using a regular expression. For more details, see Regular Expressions ²⁰¹⁰ section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1791. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.71 Port Range Sensor

The Port Range sensor monitors a network service by connecting to various TCP/IP ports. It tries to connect to the specified TCP/IP port numbers of a device in succession and waits for each request to be accepted. It returns the number of closed ports and open ports in two different channels. Optionally, you can set limits in the sensor's channel settings. This way you can get alerted about open/closed ports.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Port Range Specific	
Timeout (sec.)	Enter a timeout in seconds for the port connect. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port-by-Port-Delay (ms)	Specify in milliseconds how long the sensor will wait to go to the next port while running through all given ports.

Port Range Specific	
Port Range Selection Method	Define whether you want to monitor all ports within a range or if you want to monitor several individual ports. Choose between: ▪ Port Range with start/end: Monitor ports within a range. ▪ List of Ports: Provide a list of several individual ports to monitor.
Range Start	This field is only visible if the port range method is enabled above. Enter the port number where the scan will start. Please enter an integer value.
Range End	This field is only visible if the port range method is enabled above. Enter the port number where the scan will end. Please enter an integer value.
Port List	This field is only visible if the list of ports method is enabled above. Enter the numbers of the ports the sensor will try to connect to. Please enter one or more individual integer values.
If Value Changes	Define what will be done in case the value of a sensor channel changes. Choose between: ▪ Ignore changes: No action will be taken on change. ▪ Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification 1690 whenever the sensor value changes.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 1683 settings).

Sensor Display

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1688] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.72 Probe Health Sensor

The Probe Health sensor monitors internal PRTG parameters. It shows the state of the PRTG probe (either for the local probe, a [remote probe](#)^[2012], or a [cluster](#)^[81] probe). This sensor type is created automatically by PRTG and cannot be deleted. It checks various parameters of your PRTG system which can affect the quality of the monitoring results:

- **Health:** This index value sums up the probe state into a value between 100% (healthy) and 0% (failing). Frequent or repeated health values below 100% should be investigated.
- **CPU Load:** This channel shows the current percentage CPU load. Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value usually should stay below 50%.
- **Handles:** This is a counter for the data structures of the operating system. It is responsible for internal resource management. Repeated obviously increasing values should be investigated.
- **Interval Delay non-WMI&SNMP:** This channel shows the percentage interval delay for all sensor types which are not from the type SNMP or WMI.
- **Interval Delay SNMP:** This channel shows the percentage interval delay for SNMP sensors. If this value is above 0% there are probably very slow SNMP V3 sensors. In this case, try to increase the monitoring intervals or distribute the sensors over several probes.
- **Interval Delay WMI:** This channel shows the percentage interval delay for WMI sensors. If this value is above 0% WMI sensors could not be checked according to their interval. 100% means that WMI sensors on the average are checked with twice their interval. For values above 0% try to increase the monitoring intervals or distribute the sensors over several probes to keep the number of WMI sensors per probe below 120 (with 60 seconds interval) or 600 (with 300 seconds interval).
- **Lost Flow Packets:** This channel shows the percentage of lost flow packets.
- **Memory Usage:** This channel shows the amount of memory being used by the PRTG probe service as reported by the memory manager. Repeated obviously increasing values should be investigated. If the value is constantly above 2 GB this indicates that PRTG runs at its limits. In this case you should distribute some sensors to [Remote Probe](#)^[2012].
- **Message Queue:** This channel shows the number of monitoring results from the probe which have not been processed yet by the core. This value usually should stay below 1/10 of the sensor count.
- **Open Requests:** This channel shows the number of currently active monitoring requests. This value should stay below the maximum of 500 open requests.
- **Threads:** This channel shows the number of program parts which are running simultaneously currently. This value can increase with heavy load. The number should not exceed 100 in normal operation.

This sensor can be set up on a Probe Device only!

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ⁸⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)⁹⁴.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.73 QoS (Quality of Service) One Way Sensor

The QoS (Quality of Service) One Way sensor monitors parameters regarding the quality of a network connection between two probes, which is important, for example, when using Voice over IP (VoIP) over this connection. The sensor sends a series of UDP packets from the parent probe to another probe and measures packet loss, jitter, Packet Delay Variation (PDV), etc.

Note: In order for this sensor to work, there has to be at least one [remote probe](#)^[2011] configured in your setup. The sensor can be created on the **Probe Device** of either a local or remote probe.

Note: This sensor type cannot be cloned using the [Clone Object](#)^[1708] function.

For a general introduction to the technology behind Quality of Service monitoring, please see [Monitoring Quality of Service](#)^[1939] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Quality of Service Measurement	
Timeout (sec)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
Target Probe	Define the target probe that will receive the UDP packets. In the drop down menu, all local and remote probes of your setup are shown. When running the sensor on the local probe, select a remote probe as Target Probe ; if no remote probe is available, please install and connect a remote probe ²⁰¹¹ first. When running the sensor on a remote probe, select either another remote probe or the local probe as target. The sensor will measure values for the network track between the probe the sensor is created on and the target probe. Note: You must ensure that firewalls, NAT rules, etc. will allow the UDP packets to reach the target probe. The Windows firewall on the target system will be automatically opened by the probe.
Target IP	Define the IP address of the target probe to which the probe the sensor is created on will connect. When you're not using NAT rules, this is usually the address shown above next to the target probe's name.
Port	Define the source and target port for the UDP packets. This port will be used on both the source and target probe. Please use a different port for each QoS sensor to make sure packets can be assigned correctly. Enter an integer value between 1024 and 65536 . Note: This port must be available on both the source and target system.
Number of Packets	Define how many packets are sent for each scanning interval. We recommend using 1000 . Please enter an integer value.
Size of Packets (Bytes)	Define the size in bytes of the packets sent. We recommend using 172 . Please enter an integer value.
Time between packets (ms)	Define the size in milliseconds that will be waited between two packets. We recommend using 20 . Please enter an integer value.
DSCP	Enter a Differentiated Services Code Point (DSCP) to mark the traffic sent by this sensor. This is useful for Class of Service (CoS) measurements. Enter a value between 0 and 64 . Note: This setting may be ignored on Windows systems prior to Vista. You can check the PRTG Probe Log file in your PRTG data directory to see if the traffic control API has been initialized.
802.1p	Enter an IEEE 802.1p priority class to mark the traffic sent by this sensor. This is useful for Class of Service (CoS) measurements. Enter a value between 0 and 7 . Note: This setting may be ignored on Windows systems prior to Vista. You can check the PRTG Probe Log file in your PRTG data directory to see if the traffic control API has been initialized.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁹⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1793. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.74 QoS (Quality of Service) Round Trip Sensor

The QoS (Quality of Service) Round Trip sensor monitors parameters regarding the quality of a network connection between two probes. This is important, for example, when using Voice over IP (VoIP) over this connection. The sensor sends a series of UDP packets from the parent probe to another probe. Then, the traffic is sent back to the original probe. The sensor measures packet loss, jitter, Packet Delay Variation (PDV), the round trip time (RTT), etc.

Note: In order for this sensor to work, there has to be at least one [remote probe](#)^[2011] configured in your setup. The sensor can be created on the **Probe Device** of either a local or remote probe.

Note: This sensor type cannot be cloned using the [Clone Object](#)^[1708] function.

For a general introduction to the technology behind Quality of Service monitoring, please see [Monitoring Quality of Service](#)^[1999] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Quality of Service Measurement	
Timeout (sec)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
Target Probe	Define the target probe that will receive the UDP packets. In the drop down menu, all local and remote probes of your setup are shown. When running the sensor on the local probe, select a remote probe as Target Probe ; if no remote probe is available, please install and connect a remote probe ²⁰¹¹ first. When running the sensor on a remote probe, select either another remote probe or the local probe as target. The sensor will measure values for the network track between the probe the sensor is created on and the target probe. Note: You must ensure that firewalls, NAT rules, etc. will allow the UDP packets to reach the target probe. The Windows firewall on the target system will be automatically opened by the probe.
Target IP	Define the IP address of the target probe to which the probe the sensor is created on will connect. When you're not using NAT rules, this is usually the address shown above next to the target probe's name.
Port	Define the source and target port for the UDP packets. This port will be used on both the source and target probe. Please use a different port for each QoS sensor to make sure packets can be assigned correctly. Enter an integer value between 1024 and 65536 . Note: This port must be available on both the source and target system.
Number of Packets	Define how many packets are sent for each scanning interval. We recommend using 1000 . Please enter an integer value.
Size of Packets (Bytes)	Define the size in bytes of the packets sent. We recommend using 172 . Please enter an integer value.
Time between packets (ms)	Define the size in milliseconds that will be waited between two packets. We recommend using 20 . Please enter an integer value.
DSCP	Enter a Differentiated Services Code Point (DSCP) to mark the traffic sent by this sensor. This is useful for Class of Service (CoS) measurements. Enter a value between 0 and 64 . Note: This setting may be ignored on Windows systems prior to Vista. You can check the PRTG Probe Log file in your PRTG data directory to see if the traffic control API has been initialized.
802.1p	Enter an IEEE 802.1p priority class to mark the traffic sent by this sensor. This is useful for Class of Service (CoS) measurements. Enter a value between 0 and 7 . Note: This setting may be ignored on Windows systems prior to Vista. You can check the PRTG Probe Log file in your PRTG data directory to see if the traffic control API has been initialized.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁹⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1793. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.75 RADIUS Sensor

The RADIUS sensor monitors a Remote Authentication Dial-In User Service (RADIUS) server. The sensor tries to authenticate at the server and shows the response time. If authentication fails, it will show an error.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Radius specific	
Timeout (sec)	Enter a timeout in seconds for the request. If the reply takes longer than this value, the request is aborted and an error message is triggered.
User	Define the user name used for authentication at the server. Please enter a string.
Password	Define the password used for authentication between the client and the RADIUS server. Please enter a string. Note: The password must not be longer than 6 characters.
Secret	Define the shared secret used for authentication between the authenticator (here the PRTG Probe) and the server. Please enter a string.
Port	Enter the port number used for connection to the server. Default value is 1812 . Please enter an integer value.
NAS IP Address	Define a valid NAS IP address or leave the field empty.
NAS-Identifier	Enter a NAS identifier. Please enter a string or leave the field empty.
Use Chap	Add a check mark if you want to use the Challenge Handshake Authentication Protocol .

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings  settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1888] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1890] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.76 RDP (Remote Desktop) Sensor

The RDP (Remote Desktop) Sensor monitors remote desktop services (RDP, Terminal Services Client).

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Specific	
Timeout (sec)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.
Port	Enter the number of the port the sensor will try to connect to. Please enter an integer value. Default value is 3389 . We recommend using the default value.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1793. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.77 SCVMM Host Sensor

The SCVMM Host sensor monitors a host that is managed by a Microsoft System Center Virtual Machine Manager (SCVMM). This can be, for example, a Hyper-V host, a VMware host, or a XenServer host. It can show the CPU usage, free memory (in bytes and percentage), the overall status, the communication status, the status of the cluster node, the status of the virtual server, the computer status, and the VM count.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Note: Your Windows credentials may not contain any double quotation marks ("). If they do, this sensor will not work!

Requirement: Remote PowerShell 2.0

This sensor type uses PowerShell commands. In order to monitor devices with this sensor, **Remote PowerShell 2.0** has to be enabled. For detailed information, please see [More](#)^[828] section below. **Note:** PowerShell 1.0 is not supported.

Requirement: VMM PowerShell Plugin

This sensor type needs the VMM PowerShell Plugin to be installed on the target machine. Under Windows 2008 and 2012 it is part of the VMM 2008 Administrator Console, or the VMM 2012 Management Console, respectively.

Note: To provide good performance, the System Center Virtual Manager (SCVMM) only reads the performance data from time to time and caches them. Because of this, updates can take up to several minutes. If your monitoring returns the same values again and again, please increase the scanning interval.

Requirement for Windows Server 2012 Compatibility

In order to make this sensor type compatible for Windows Server 2012 systems, the following requirements have to be met:

- The SCVMM PowerShell module has to be in the directory `C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager\bin\psModules\virtualmachinemanager\virtualmachinemanager`.
- You have to set the execution policy in PowerShell to allow the execution of `Import-Module C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager\bin\psModules\virtualmachinemanager\virtualmachinemanager`. Use the command `Set-ExecutionPolicy`. We recommend the execution policy `RemoteSigned`; `AllSigned` and `Unrestricted` are also possible.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor hosts, PRTG will create one sensor for each host. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Host Settings

Host

Select the hosts you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head. **Note:** Please make sure the name of your hosts do not contain unsupported characters, especially avoid the hash ('#') sign. We recommend to not rename hosts once you've set up monitoring. For detailed information, please see [More](#)^[591] section below.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Host Settings

Sensor Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage section.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

More

Knowledge Base: Why don't my Hyper-V sensors work after changing names?

- <http://www.paessler.com/knowledgebase/en/topic/15533>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <http://www.paessler.com/knowledgebase/en/topic/44453>

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- <http://www.paessler.com/knowledgebase/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <http://www.paessler.com/knowledgebase/en/topic/59745>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.78 SCVMM Virtual Machine Sensor

The SCVMM Virtual Machine sensor monitors a virtual machine (VM) that is managed by a Microsoft System Center Virtual Machine Manager (SCVMM). This can be, for example, a Hyper-V virtual machine, a VMware virtual machine, or a XenServer virtual machine. It can show the CPU usage, the status of a VM, and disk read and write speed.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Note: Your Windows credentials may not contain any double quotation marks ("). If they do, this sensor will not work!

Requirement: Remote PowerShell 2.0

This sensor type uses PowerShell commands. In order to monitor devices with this sensor, **Remote PowerShell 2.0** has to be enabled. For detailed information, please see [More](#)^[835] section below. **Note:** PowerShell 1.0 is not supported.

Requirement: VMM PowerShell Plugin

This sensor type needs the VMM PowerShell Plugin to be installed on the target machine. Under Windows 2008 and 2012 it is part of the VMM 2008 Administrator Console, or the VMM 2012 Management Console, respectively.

Note: To provide good performance, the System Center Virtual Manager (SCVMM) only reads the performance data from time to time and caches them. Because of this, updates can take up to several minutes. If your monitoring returns the same values again and again, please increase the scanning interval.

Requirement for Windows Server 2012 Compatibility

In order to make this sensor type compatible for Windows Server 2012 systems, the following requirements have to be met:

- The SCVMM PowerShell module has to be in the directory `C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager\bin\psModules\virtualmachinemanager\virtualmachinemanager`.
- You have to set the execution policy in PowerShell to allow the execution of `Import-Module C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager\bin\psModules\virtualmachinemanager\virtualmachinemanager`. Use the command `Set-ExecutionPolicy`. We recommend the execution policy `RemoteSigned`; `AllSigned` and `Unrestricted` are also possible.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor VMs, PRTG will create one sensor for each VM. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Virtual Machine Settings

Virtual Machine	Select the Virtual Machines (VMs) you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head. Note: Please make sure the name of your VMs do not contain unsupported characters, especially avoid the hash ('#') sign. We recommend to not rename VMs once you've set up monitoring. For detailed information, please see More ^[591] section below.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Virtual Machine Settings	
Sensor Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

More

Knowledge Base: Why don't my Hyper-V sensors work after changing names?

- <http://www.paessler.com/knowledgebase/en/topic/15533>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <http://www.paessler.com/knowledgebase/en/topic/44453>

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- <http://www.paessler.com/knowledgebase/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <http://www.paessler.com/knowledgebase/en/topic/59745>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.79 Sensor Factory Sensor

The Sensor Factory sensor is a powerful tool that allows you to create your own sensor with channels based on data from other sensors. You can define one or more channels using formulas that combine monitoring results from other sensors.

Samples for usage are:

- Show single channels of one or more sensors in one graph.
- Use the data from single channels of one or more sensors to calculate new values (for example, you can subtract, multiply, and divide).
- Create graphs with data from other sensor channels and add horizontal lines at specific vertical positions.

Note: A sensor factory sensor does not show a "Downtime" channel. Downtime cannot be calculated for this sensor type.

Note: The Sensor Factory sensor might not work with [flow sensors](#)^[1994]. Sensor types using **active flow timeout**, this is, [NetFlow and jFlow sensors](#)^[291], are not supported by the Sensor Factory sensor.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Factory Specific Settings	
Channel Definition	Enter a channel definition for the sensor. Using a specific syntax, you can refer to data from channels of other sensors here. You can also calculate values. Enter one channel definition for each new channel you want to add to this sensor. Please see section Define Sensor Channels ^[842] below.
Error Handling	Define the sensor's behavior if one of the sensors defined above is in an error status. In this case, you can set the sensor factory sensor either to error or to warning status. Choose between: • Factory sensor shows error status when one or more source sensors are in error status: If at least one sensor used in a channel definition is in a Down status, the factory sensor will show a Down status as well until all referred sensors leave this status. While the factory sensor is Down it will still show data of all available sensor channels. • Factory sensor shows warning status when one or more source sensors are in error status: If at least one sensor used in a channel definition is in a Down status, the factory sensor will show a Warning status until all referred sensors leave the Down status. • Use custom formula: Define the status of the factory sensor by adding a status definition in the field below.
Status Definition	This field is only visible if custom formula is enabled above. Define when the sensor will switch to a Down status. You can use the status() function in combination with Boolean operations. For advanced users it is also possible to calculate a status value. Please see section Define Sensor Status ^[849] below.
If a Sensor Has No Data	Choose how this Sensor Factory sensor will react in case a sensor referred to in the channel definition does not provide any data (for example, because it is paused or does not exist). Choose between: ▪ Do not calculate factory channels that use the sensor: For channels that are defined using one or more sensor(s) that deliver no data, no data will be shown. Additionally, the sensor will show a Warning state. ▪ Calculate the factory channels and use zero as source value: If a sensor used in a channel definition does not deliver any data, zero values will be filled in instead. The channel will be calculated and shown using these values.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

Define Sensor Channels

The channels of a Sensor Factory sensor are controlled by the **Channel Definition** text field. Using a special syntax you can refer to other sensor channels, calculate values, and add horizontal lines. You can define factory sensor channels using data from any other sensor's channels on your PRTG core server.

Example

You see a definition of two factory sensor channels, both using the `channel()` function which simply collects data from the channels of other sensors in your monitoring and displays them:

```
#1:Local Probe Health
channel(1001,0)
#2:Local Traffic Out[kbit]
channel(1004,1)
```

The first channel of the factory sensor (**#1**) collects data from the **Health** channel (**ID 0**) of the **Core/Probe Health** sensor (**ID 1001**) running on the Local Probe device. The second channel (**#2**) collects data from the **Traffic out** channel (**ID 1**) of a traffic sensor (**ID 1004**) measuring the system's local network card. Both channels will be shown together in the factory sensor's data tables and graphs.

The basic syntax for a sensor factory channel definition looks like this:

```
#<id>:<name>[<unit>]
<formula>
```

For each channel one section is used. A section begins with the **#** sign. Function names in formulas are not case sensitive.

The parameters are:

- **<id>** is the ID of the factory sensor's channel and must be a unique number > 0.
- **<name>** is the name of the factory sensor's channel (displayed in graphs and tables).
- **[<unit>]** is an optional unit description for the factory sensor's channel (e.g. bytes). If it is not provided a fitting unit string is selected automatically (recommended).
- **<formula>** contains the formula to calculate the factory sensor's channel. For the formula, you can use the following functions: [channel\(\)](#)⁸⁴⁴, [min\(\)](#)⁸⁴⁵, [max\(\)](#)⁸⁴⁵, [avg\(\)](#)⁸⁴⁵, or [percent\(\)](#)⁸⁴⁶.

Define Sensor Channels—Formula Calculations

Within a formula the following elements are allowed to perform calculations with the values that are returned by one or more functions:

- Basic operations: + (add), - (subtract), * (multiply), / (divide)
Example: `3 + 5 * 2`
- Brackets: `()`
Example: `3 * (2 + 6)`

- Compare: = (equal), <> (not equal), > (greater), < (less), >= (greater or equal), <= (less or equal)
If the compare is true the value is **10,000**; if false the value is **0**. For delta sensors the speed is compared.

Example

You see a Sensor Factory channel definition with calculation.

```
#1:Traffic Total x Minus Traffic Out y
( channel(2001,-1) - channel(1004,1) ) * 2
```

This full channel definition will result in a factory sensor showing a calculation with values from two channels (channel IDs **-1** and **1**) of two traffic sensors (sensor IDs **2001** and **1004**). The returned values will be subtracted and then multiplied by two.

Channels can be gauge values (e.g. Ping ms) or delta values (e.g. traffic kbit/s). Not all combinations are allowed in a formula. **Note:** When performing percentage calculation, please use the [percent\(\) Function](#) ⁸⁴⁶ to make sure you obtain the expected values!

There are calculations you **cannot** do:

- You cannot add/subtract a delta from a gauge channel (and vice versa).
- You cannot multiply two delta channels.
- You cannot compare a delta with a gauge channel.
- You cannot use a channel of (another) Sensor Factory sensor channel in the formula.

Define Sensor Channels—channel() Function

The **channel()** function allows to read the data from a channel of a different sensor. The syntax is:

```
channel(<sensorId>,<channelId>)
```

The parameters are:

- **<sensorId>** is the ID of the sensor. It is displayed on the sensor details page, in the **Overview** tab behind the sensor name.
- **<channelId>** is the ID of the sensor channel. It is displayed on the sensor details page, in the **Channels** tab for each channel behind the channel name.

Example

```
channel(2001,2)
```

This function reads the data from channel ID **2** of the sensor with the ID **2001**.

```
#1:Sample  
channel(2001,2)
```

This full channel definition reads the data from channel ID **2** of the sensor with the ID **2001** and displays it in the first factory sensor channel (**#1**), without any additional calculations.

Define Sensor Channels—min() and max() Functions

The **min()** and **max()** functions return the minimum or maximum of the two values. The syntax is:

```
min(<a>,<b>)  
max(<a>,<b>)
```

Values for **<a>** and **** are either numbers or [channel\(\)](#)⁸⁴⁴ functions.

Examples

```
min(10,5)
```

This function in the first line returns **5**, as this is the smaller value out of 10 and 5.

```
min( channel(2001,1),channel(2002,1) )
```

This function returns the minimum of channel **1** of the sensor with ID **2001** and channel **1** of the sensor with ID **2002**.

Define Sensor Channels—avg() Function

The **avg()** function returns the average of the two values. This equals: $(a+b) / 2$. The syntax is:

```
avg(<a>,<b>)
```

Values for **<a>** and **** are either numbers or [channel\(\)](#)⁸⁴⁴ functions.

Examples

```
avg(20,10)
```

This function returns **15**: $(20+10) / 2 = 15$.

```
avg( channel(2001,1),channel(2002,1) )
```

This function returns the average of channel **1** of the sensor with ID **2001** and channel **1** of the sensor with ID **2002**.

Define Sensor Channels—percent() Function

The **percent()** function calculates the percent value of two given values, for example, a channel and a fixed value. The syntax is:

```
percent(<source>,<maximum>[,<unit>])
```

The parameters are:

- **<source>** is the value the percent is calculated for. This is usually a [channel\(\)](#)⁸⁴⁴ function.
- **<maximum>** is the limit value used for the percent calculation.
- **[<unit>]** is an optional unit the maximum is provided in. You can use constants with this function (see [Constants](#)⁸⁴⁸ section below for a list). This can be used for gauge (e.g. Ping sensors) or delta (e.g. traffic sensors). If no unit is provided **1** will be used. Note: As unit string **%** will be added automatically.

PRTG will calculate: $\text{<source>} / \text{<maximum>} * \text{<unit>} * 100$

Examples

```
#1:Usage Traffic In
percent(channel(2001,0),100,kilobit)
#2:Usage Traffic Out
percent(channel(2001,1),100,kilobit)
```

This full channel definition will result in a factory sensor showing two channels of a traffic sensor (sensor ID **2001**): Traffic in (channel ID **0**) and traffic out (channel ID **1**). The values will be displayed as % of maximum bandwidth (100 kilobit/second).

```
#1:Ping %
percent(channel(2002,0),200)
```

This full channel definition will result in a factory sensor showing the **Ping Time** channel (channel ID **0**) of a Ping sensor (sensor ID **2002**). The values will be displayed as a percentage of 200 ms.

Define Sensor Channels—Horizontal Lines

You can add lines to the graph using a formula without **channel()** function. Use a fixed value instead. The syntax is:

```
#<id>:<name>[<unit>]
<value>
```

The parameters are:

- **<id>** is the ID of the factory sensor's channel and must be a unique number > 1. Although a horizontal line will not be shown as a channel, the ID has to be unique.
- **<name>** is the name of the factory sensor's channel. When used here it will not be displayed in graphs and tables, but can be used as a comment to describe the nature of the line.
- **[<unit>]** is an optional unit description (e.g. kbit/s). If it is not provided the line is applied automatically to the scale of the first factory sensor channel. If your factory sensor uses different units you should provide a unit to make sure the line is added for the right scale. Please enter the unit exactly as shown in your graphs' legend. If you enter a unit that does not yet exist in your graph, a new scale will be added automatically.
- **<value>** contains a number defining where the line will be shown in the graph.

Examples

```
#5:Line at 100ms [ms]
100
```

This channel definition will result in graph showing a horizontal line at the value of **100** on the **ms** scale.

```
#6:Line at 2 Mbit/s [kbit/s]
2000
```

This channel definition will result in graph showing a horizontal line at the value of **2000** on the **kbit/s** scale.

```
#1:Ping Time
channel(2002,0)
#2:Line at 120ms [ms]
120
```

This full channel definition will result in a factory sensor showing the **Ping Time** channel (channel ID **0**) of a Ping sensor (sensor ID **2002**). Additionally, the sensor's graphs will show a horizontal line at **120 ms**.

Define Sensor Channels—Constants

The following constants are defined and can be used in calculations:

- **one** = 1
- **kilo** = 1000
- **mega** = 1000 * kilo
- **giga** = 1000 * mega
- **tera** = 1000 * giga
- **byte** = 1
- **kilobyte** = 1024
- **megabyte** = 1024 * kilobyte
- **gigabyte** = 1024 * megabyte
- **terabyte** = 1024 * gigabyte
- **bit** = 1/8
- **kilobit** = kilo / 8

- **megabit** = mega / 8
- **gigabit** = giga / 8
- **terabit** = tera / 8

Define Sensor Status—status() Function

The status of a Sensor Factory sensor can be controlled by the **Status Definition** text field, if the custom formula option is enabled in the [Sensor Settings](#)⁸³⁷. Using a special syntax you can define when the factory sensor will change to a **Down** status. In all other cases the sensor will be in an **Up** status. The syntax is:

```
status(sensorID) <boolean> status(sensorID)
```

The parameters are:

- **<sensorid>** is the ID of the sensor you want to check the status of. The ID is displayed on the sensor details page, in the **Overview** tab behind the sensor name.
- **<boolean>** is one of the Boolean operators **AND**, **OR**, or **NOT**. If the resulting expression is **true**, the factory sensor will change to a **Down** status.

Examples

```
status(2031) AND status(2044)
```

This will change the factory sensor to a **Down** status if both sensors, with IDs **2031** and **2044**, are **Down**. Otherwise the factory sensor will show an **Up** status.

```
status(2031) OR status(2044)
```

This will change the factory sensor to a **Down** status if at least one of the sensors with ID **2031** or ID **2044** is **Down**. Otherwise the factory sensor will show an **Up** status.

```
status(2031) NOT status(2044)
```

This will change the factory sensor to a **Down** status if the sensor with ID **2031** is **Down**, but the sensor with ID 2044 is **not** in a **Down** status. Otherwise the factory sensor will show an **Up** status.

```
( status(2031) AND status(2044) ) OR status(2051)
```

This will change the factory sensor to a **Down** status if both the sensor with ID **2031** and the sensor with ID **2044** is **Down**, or if the sensor with ID **2051** is **Down**. Otherwise the factory sensor will show an **Up** status.

Additionally, the following elements are allowed to perform calculations and comparisons with the values that are returned by the status functions:

- Basic operations: + (add), - (subtract), * (multiply), / (divide)
Example: $3 + 5 * 2$
- Brackets: ()
Example: $3 * (2 + 6)$
- Compare: = (equal), <> (not equal), > (greater), < (less), >= (greater or equal), <= (less or equal)
If the compare is true the value is 10,000; if false the value is 0. For delta sensors the speed is compared.

Internally, the status() function returns the downtime channel of the sensor in hundreds of percent (10,000 = 100%).

- **true** corresponds to a value of 10,000 which is a **Down** status.
- **false** corresponds to a value of 0 which is an **Up** status.

Understanding this, more complex formulas are possible.

Example

```
( status(1031) + status(1032) + status(1033) + status(1034) ) >= 20000
```

This will change the factory sensor to a **Down** status if at least any two of the sensors with IDs 1031, 1032, 1033, or 1034 are **Down**. Otherwise the factory sensor will show an **Up** status.

Note: The status() function may also be used in [channel definitions](#)^[842]. Using this functionality, it is for example possible to display the numeric status value of sensors in a factory sensor channel.

Using Factory Sensors in a Cluster Setup

If you're running PRTG in [Clustering](#)^[81] mode, please note these additional facts:

- If you add a Sensor Factory sensor underneath the **Cluster Probe**, and in the Sensor Factory formula, you refer to a channel of a sensor running on the **Cluster Probe** as well, the Sensor Factory sensor will show the data of all cluster nodes for this sensor channel.
- If you add a Sensor Factory sensor underneath the **Local Probe**, and in the Sensor Factory formula, you refer to a channel of a sensor running on the **Cluster Probe**, the Sensor Factory sensor will only show data of the primary master node for this sensor channel.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁸ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.80 sFlow Sensor

The sFlow sensor receives traffic data from a sFlow V5 compatible device and shows the traffic by type. Only header traffic will be analyzed. Please make sure the device matches the sFlow version V5! There are several filter options available to divide traffic into different channels.

Note: In order for the sensor to work, sFlow V5 export must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).

The sensor accepts RAW data only. The stream must be sent via IPv4. This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

For a general introduction to the technology behind flow monitoring, please see [Monitoring Bandwidth via Flows](#)¹⁹³⁴ section.

Limitations of This Sensor Type

There are some limitations that you want to consider before using this sensor type:

- Only sFlow version 5 datagrams are supported
- Only IPv4 flows are supported
- Only the "raw packet header" format is supported
- Only the "Flow sample" format is supported. "Extended flow" and "Counter" formats cannot be processed
- PRTG processes only samples where the source ID matches the ifIndex of the input interface (avoiding double counted traffic) and ascending sequence numbers. Due to internal limitations, only interface numbers up to 65535 are supported.
- Sample packets have to be of ethernet type "IP" (with optional VLAN tag)
- Sampled packets of type TCP and UDP are supported

We recommend using sFlow tester for debugging (see **More** section below).

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

sFlow Specific Settings

Receive sFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the sFlow export options of your hardware router device. Default value is 6343 . Please enter an integer value. Note: When configuring export, please make sure you select the appropriate sFlow version 5.
Sender IP	Enter the IP address of the sending device you want to receive the sFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive sFlow Packets on IP	Select the IP address(es) on which PRTG listens to sFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the sFlow export options of your hardware router device. Note: When configuring export, please make sure you select the appropriate sFlow version 5.

Channel Configuration

Channel Selection	Define the categories the traffic will be accounted to. There are different groups of traffic available. Choose between: ▪ Web: Internet web traffic.

Channel Configuration

- **File Transfer:** Traffic caused by FTP.
- **Mail:** Internet mail traffic.
- **Chat:** Traffic caused by chat and instant messaging.
- **Remote Control:** Traffic caused by remote control applications, such as RDP, SSH, Telnet, VNC.
- **Infrastructure:** Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, SNMP.
- **NetBIOS:** Traffic caused by NetBIOS communication.
- **Other Protocols:** Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, i.e. how detailed traffic will be divided. For each group, choose between:

- **No:** Do not account traffic of this group in an own channel. All traffic of this group will be accounted to the default channel named **Other**.
- **Yes:** Count all traffic of this group and summarize it into one channel.
- **Detail:** Count all traffic of this group and further divide it into different channels. The traffic will appear in several channels as shown in the **Content** column. **Note:** Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyse.

Filtering

Include Filter

Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁴ section.

Exclude Filter

First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁴ section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist	
Primary Toplist	Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from: ▪ Top Talkers ▪ Top Connections ▪ Top Protocols ▪ [Any custom toplist you have added]

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail. For more information, please see [Toplists](#)¹⁷⁰² section.

More

Paessler Website: Paessler sFlow Tester

- <http://www.paessler.com/tools/sflowtester>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁴
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁸

6.8.81 sFlow (Custom) Sensor

The sFlow (Custom) sensor receives traffic data from a sFlow V5 compatible device and shows the traffic by type. Please make sure the device matches the sFlow version V5! There are several filter options available to divide traffic into different channels.

Note: In order for the sensor to work, sFlow V5 export must be enabled on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe). The sensor accepts RAW data. This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

For a general introduction to the technology behind flow monitoring, please see [Monitoring Bandwidth via Flows](#)¹⁹⁰⁴ section.

Limitations of This Sensor Type

There are some limitations that you want to consider before using this sensor type:

- Only sFlow version 5 datagrams are supported
- Only IPv4 flows are supported
- Only the "raw packet header" format is supported
- Only the "Flow sample" format is supported. "Extended flow" and "Counter" formats cannot be processed
- PRTG processes only samples where the source ID matches the ifIndex of the input interface (avoiding double counted traffic) and ascending sequence numbers. Due to internal limitations, only interface numbers up to 65535 are supported.
- Sample packets have to be of ethernet type "IP" (with optional VLAN tag)
- Sampled packets of type TCP and UDP are supported

We recommend using sFlow tester for debugging (see **More** section below).

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

sFlow Specific Settings	
Receive sFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the sFlow export options of your hardware router device. Default value is 6343 . Please enter an integer value. Note: When configuring export, please make sure you select the appropriate sFlow version 5.
Sender IP	Enter the IP address of the sending device you want to receive the sFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive sFlow Packets on IP	Select the IP address(es) on which PRTG listens to sFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the sFlow export options of your hardware router device. Note: When configuring export, please make sure you select the appropriate sFlow version 5.

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
81 sFlow (Custom) Sensor

Channel Definition	Please enter a channel definition to divide the traffic into different channels. Write each definition in one line. For detailed information, please see Channel Definitions for xFlow and Packet Sniffer Sensors ^[1990] section. All traffic for which no channel is defined will be accounted to the default channel named Other . Note: Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyse.
Filtering	
Include Filter	Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors ^[1994] section.
Exclude Filter	First, the filters defined in the Include Filter field are considered. From this subset, you can explicitly exclude traffic, using the same syntax. For detailed information, please see Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors ^[1994] section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[1683] settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Primary Toplist**Primary Toplist**

Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from:

- **Top Talkers**
- **Top Connections**
- **Top Protocols**
- **[Any custom toplist you have added]**

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹². **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

Schedules, Dependencies, and Maintenance Window	
	▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail. For more information, please see [Toplists](#) ¹⁷⁰² section.

More

Paessler Website: Paessler sFlow Tester

- <http://www.paessler.com/tools/sflowtester>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#) ¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#) ¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#) ¹⁴¹ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#) 
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#) 

6.8.82 SFTP Secure File Transfer Protocol Sensor

The sFTP Secure File Transfer Protocol sensor monitors FTP servers of a Linux/Unix system using SSH File Transfer Protocol (FTP over SSH). It tries to connect to a server and shows the response time.

For this sensor type credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems must be defined for the device you want to use the sensor on.

Note: Not all Linux/Unix and Mac OS distributions can be supported by this sensor type.

For a general introduction to SSH monitoring, please see [Monitoring via SSH](#)^[1930] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SSH Specific	
Connection Timeout (sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. <code>cat /proc/loadavg</code>).
SSH Port	Define which port this sensor will use for the SSH connection. Choose between: ▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems section of the device this sensor is created on. ▪ Enter custom port number: Do not use the port number from the parent device's settings, but define a different port number below.
Use Port Number	This field is only visible if the custom port number setting is enabled above. Enter the port number this sensor will use for the SSH connection. Please enter an integer value.
Result Handling	Define what will be done with the result data received by the sensor. Choose between: • Discard result: Do not store the result data. • Write result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the query to the "Logs (Sensors)" directory (on the Master node, if in a cluster). File name: <code>Result of Sensor [ID].txt</code>. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage 2036 section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings). ▪ Show in and out traffic as positive and negative area chart: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.83 Share Disk Free Sensor

The Share Disk Free sensor monitors free disk space of a share (Windows/Samba) using Server Message Block (SMB). It shows the free space in percent and total.

Note: This sensor only works if no quotas are enabled on the target share. If there are quotas enabled for the user account this sensor uses to connect to the share, the absolute value will be okay, but the percentage variable will show wrong values.

Requirement: Server Service

In order to monitor shares on Windows machines, please make sure the **LanmanServer** "Server" Windows service is running on the target computer.

To enable the service, please log in to the respective computer and open the services manager (e.g. via **services.msc**). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Share Configuration

Share	Enter the name of the share this sensor will monitor. Only a share name is allowed here (for example, enter C\$). Please do not enter a complete UNC name here. The server name (\\server\) is taken from the parent device of this sensor. Note: In order to provide any shares under Windows, the LanmanServer "Server" Windows service must be running on the target computer.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

More

Knowledge Base: What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

- <http://www.paessler.com/knowledgebase/en/topic/513>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#) section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#) section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.84 SIP Options Ping Sensor

The SIP Options Ping sensor monitors the connectivity for a Session Initiation Protocol (SIP) server using SIP options "Ping". It can be used to monitor voice-over-IP (VoIP) services. The sensor sends "auth" and "options" requests to the SIP server and shows the response time. It can alert in case of an error.

Note: A SIP server might return a **480 Service temporarily unavailable** error until at least one reachable SIP client is connected to the server.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SIP Specific	
Port	Define the UDP port this sensor will connect to. Please enter an integer value.
Username	Enter the username of the SIP account this sensor will log into after a connection to the SIP server has been established. Please enter a string.
Password	Enter the password of the SIP account this sensor will log into after a connection to the SIP server has been established. Please enter a string.
Timeout (Seconds)	Enter the timeout for the connection to the SIP server. Please enter an integer value.
Retry Count	In case the connection to the SIP server fails, the sensor can re-try to connect. Enter the maximum number of retries. After reaching the maximum count the sensor will show a red Down status. Please enter an integer value.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor.

Sensor Display	
	▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.85 SMTP Sensor

The SMTP sensor monitors a mail server using Simple Mail Transfer Protocol (SMTP) and shows the server's response time. It can optionally send a test email with every check.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
SMTP specific	
Timeout (sec)	Enter a timeout in seconds for the SMTP connect. If the reply takes longer than this value the request is aborted and an error message is triggered.

SMTP specific	
Port	Enter the number of the port that will be used to send an email via SMTP. For non-secure connections usually port 25 is used; usually port 465 or 587 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
TLS (Transport-Level Security)	Select if the SMTP connection will be secured via SSL. Choose between: • Don't use: Do not use encryption for the SMTP connection. • Use: Connect to the SMTP server using the SSL method selected below.
SSL-Method	This field is only visible if security is enabled above. Select the SSL method that will be used when connecting to the server. We recommend using the default value. Only if you experience connection problems, try another setting. Choose between: ▪ SSL V2 ▪ SSL V2 or V3 ▪ SSL V3 ▪ TLS V1
Authentication	
Type	Select whether to use an authentication method for the SMTP connection. Choose between: • None: Do not use any authentication method. • Username/Password: Authenticate at the SMTP server via username and password.
Username	This field is only visible if SMTP authentication is enabled above. Enter a username for SMTP authentication. Please enter a string.
Password	This field is only visible if SMTP authentication is enabled above. Enter a password for SMTP authentication. Please enter a string.

Monitoring	
Send Mail	Define if an email will be sent when connecting to the SMTP server. Choose between: • None: Do not send an email, just connect to the SMTP server. • Send Mail: Send an email through the SMTP server. If there is an error when sending mail, an error message will be triggered and the sensor will change to a Down status.
Helo Ident	Enter a server name for the helo part of the mail protocol. For some mail servers the helo ident must be the valid principal host domain name for the client host.
From	Specify which address the sent emails will contain in the from field. Please enter a valid email address.
To	Specify to which address the emails will be sent to. Please enter a valid email address.
Topic	Specify which subject will be used in the sent emails. Please enter a string or leave the field empty.
Content	Specify which body will be used in the sent emails. Please enter a string or leave the field empty.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁰ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.86 SMTP&IMAP Round Trip Sensor

The SMTP&IMAP Round Trip sensor monitors the time it takes for an email to reach an Internet Message Access Protocol (IMAP) mailbox after being sent using Simple Mail Transfer Protocol (SMTP). It sends an email to the parent device via SMTP and then scans a dedicated IMAP mailbox until this email comes in. The sensor shows the response time of SMTP and IMAP server, and the sum of both.

The SMTP&IMAP Round Trip sensor will delete these emails automatically from the mailbox as soon as PRTG retrieves them. Emails will only remain in the mailbox particularly if a timeout or a restart of the PRTG server occurred during sensor run-time.

Note: Please use dedicated email accounts with this sensor type. If you use more sensors of this type, please make sure that each sensor uses its own email accounts.

For a general introduction to the technology behind round trip monitoring, please see [Monitoring Email Round Trip](#)^[1943] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

We recommend adding this sensor on an SMTP server device only, because this sensor type's settings are optimized for this scenario.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings**Priority**

Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Result

Define what will be done with the result of the sensor. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: **Result of Sensor [ID].txt**. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see [Data Storage](#)  section.

Email Settings**From**

Specify which address the sent emails will contain in the from field. Please enter a valid email address.

To

Specify to which address the emails will be sent to. Please enter a valid email address.

Helo Ident

Enter a server name for the helo part of the mail protocol. For some mail servers the helo ident must be the valid principal host domain name for the client host.

Step 1: Send Email to Parent Device Using SMTP

In this step, you configure how emails will be sent. As SMTP server, the sensor uses the **IP-Address/DNS Name** property's value of the device it is added on.

Port	Enter the number of the port that will be used to send an email via SMTP. Please enter an integer value. For non-secure connections usually port 25 is used; usually port 465 or 587 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
Timeout for SMTP Connection (Sec.)	Enter a timeout in seconds for the SMTP connect. If the reply takes longer than this value the request is aborted and an error message is triggered.
TLS (Transport-Level Security)	Select if the SMTP connection will be secured via SSL. Choose between: • Don't use: Do not use encryption for the SMTP connection. • Use: Connect to the SMTP server using the SSL method selected below.
SSL-Method	This field is only visible if security is enabled above. Select the SSL method that will be used when connecting to the server. We recommend using the default value. Only if you experience connection problems, try another setting. Choose between: ▪ SSL V2 ▪ SSL V2 or V3 ▪ SSL V3 ▪ TLS V1
SMTP Authentication Type	Define if you want to use an authentication for the SMTP connection. Choose between: • None: Do not use any authentication method. • Username/Password: Authenticate at the SMTP server via username and password.
Username	This field is only visible if SMTP authentication is enabled above. Enter a username for SMTP authentication. Please enter a string.
Password	This field is only visible if SMTP authentication is enabled above. Enter a password for SMTP authentication. Please enter a string.
Additional Text for Email Subject	The subject part of the round trip email is created automatically by PRTG. It consists of the string "PRTG Roundtrip Mail:" followed by a unique GUID to correctly identify the email in the IMAP mailbox (e.g. PRTG Roundtrip Mail: {5E858D9C-AC70-466A-9B2A-55630165D276}). Use this field to place your custom text before the automatically created text.

Step 2: Check an IMAP Mailbox Until Email Arrives

In this step, you configure how the sent emails will be received.

IP-Address/DNS Name	Specify the IMAP server. Enter a valid IP address or DNS name.
Mailbox	Specify the IMAP Mailbox (resp. "IMAP folder") you want to check. Please enter the IMAP mailbox/folder name.
Port	Specify the port that will be used for the IMAP connection. For non-secure connections usually port 143 is used; usually port 993 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
TLS (Transport-Level Security)	Select if the IMAP connection will be secured via SSL. Choose between: • Don't use: Do not use encryption for the SMTP connection. • Use: Connect to the SMTP server using the SSL method selected below.
SSL-Method	This field is only visible when TLS is enabled above. Select the SSL method that will be used when connecting to the IMAP server. We recommend using the default value. If you experience connection problems, try another setting.
Connection Interval (Sec.)	Enter the number of seconds the sensor will wait between two connections to the IMAP server. PRTG will repeatedly check the mailbox in this interval until the email arrives. Please enter an integer value.
Maximum Trip Time (Sec.)	Enter the number of seconds an email may take to arrive in the IMAP mailbox. PRTG will repeatedly check the mailbox in the interval specified above until the email arrives. If it does not arrive within the maximum trip time, an error message will be triggered for the sensor. Please enter an integer value.
IMAP Authentication Type	Select the kind of authentication for the IMAP connection. Choose between: • Username and Password (simple) • Simple Authentication and Security Layer (SASL)
Username	Enter a username for IMAP authentication. Please enter a string.
Password	Enter a password for IMAP authentication. Please enter a string.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.87 SMTP&POP3 Round Trip Sensor

The SMTP&POP3 Round Trip sensor monitors the time it takes for an email to reach an Post Office Protocol version 3 (POP3) mailbox after being sent using Simple Mail Transfer Protocol (SMTP). It sends an email to the parent device via SMTP and then scans a dedicated POP3 mailbox until the email comes in. The sensor shows the response time of SMTP and POP3 server, and the sum of both.

The SMTP&POP3 Round Trip sensor will delete these emails automatically from the mailbox as soon as PRTG retrieves them. Emails will only remain in the mailbox particularly if a timeout or a restart of the PRTG server occurred during sensor run-time.

Note: Please use dedicated email accounts with this sensor type. If you use more sensors of this type, please make sure that each sensor uses its own email accounts.

For a general introduction to the technology behind round trip monitoring, please see [Monitoring Email Round Trip](#)^[1943] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

We recommend adding this sensor on an SMTP server device only, as the sensor's settings are optimized for this scenario.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings**Priority**

Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Result

Define what will be done with the result of the sensor. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: **Result of Sensor [ID].txt**. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see [Data Storage](#)  section.

Email Settings**From**

Specify which address the sent emails will contain in the from field. Please enter a valid email address.

To

Specify to which address the emails will be sent to. Please enter a valid email address.

Helo Ident

Enter a server name for the helo part of the mail protocol. For some mail servers the helo ident must be the valid principal host domain name for the client host.

Step 1: Send Email to the Parent Device Using SMTP

In this step, you configure how emails will be sent. As SMTP server, the sensor uses the **IP-Address/DNS Name** property's value of the device it is added on.

Port	Enter the number of the port that will be used to send an email via SMTP. Please enter an integer value. For non-secure connections usually port 25 is used; usually port 465 or 587 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
Timeout for SMTP Connection (Sec.)	Enter a timeout in seconds for the SMTP connect. If the reply takes longer than this value the request is aborted and an error message is triggered.
TLS (Transport-Level Security)	Select if the SMTP connection will be secured via SSL. Choose between: • Don't use: Do not use encryption for the SMTP connection. • Use: Connect to the SMTP server using the SSL method selected below.
SSL-Method	This field is only visible if security is enabled above. Select the SSL method that will be used when connecting to the server. We recommend using the default value. Only if you experience connection problems, try another setting. Choose between: ▪ SSL V2 ▪ SSL V2 or V3 ▪ SSL V3 ▪ TLS V1
SMTP Authentication Type	Define if you want to use an authentication for the SMTP connection. Choose between: • None: Do not use any authentication method. • Username/Password: Authenticate at the SMTP server via username and password.

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
87 SMTP&POP3 Round Trip Sensor

Username	This field is only visible if SMTP authentication is enabled above. Enter a username for SMTP authentication. Please enter a string.
Password	This field is only visible if SMTP authentication is enabled above. Enter a password for SMTP authentication. Please enter a string.
Additional Text for Email Subject	The subject part of the round trip email is created automatically by PRTG. It consists of the string "PRTG Roundtrip Mail:" followed by a unique GUID to correctly identify the email in the POP3 mailbox (e.g. PRTG Roundtrip Mail: {5E858D9C-AC70-466A-9B2A-55630165D276}). Use this field to place your custom text before the automatically created text.

Step 2: Check a POP3 Mailbox Until Email Arrives

In this step, you configure how the sent emails will be received.

IP-Address/DNS Name	Specify the POP3 server. Enter a valid IP address or DNS name.
Port	Specify the port that will be used for the POP3 connection. For non-secure connections usually port 110 is used; usually port 995 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend using the default value. If you do not get a connection, please try another port number.
TLS (Transport-Level Security)	Select if the POP3 connection will be secured via SSL. Choose between: • Don't use: Do not use encryption for the SMTP connection. • Use: Connect to the SMTP server using the SSL method selected below.
SSL-Method	This field is only visible when TLS is enabled above. Select the SSL method that will be used when connecting to the IMAP server. We recommend using the default value. If you experience connection problems, try another setting.
Connection Interval (Sec.)	Enter the number of seconds the sensor will wait between two connections to the IMAP server. PRTG will repeatedly check the mailbox in this interval until the email arrives. Please enter an integer value.
Maximum Trip Time (Sec.)	Enter the number of seconds an email may take to arrive in the IMAP mailbox. PRTG will repeatedly check the mailbox in the interval specified above until the email arrives. If it does not arrive within the maximum trip time, an error message will be triggered for the sensor. Please enter an integer value.
POP3 Authentication Type	Select the kind of authentication for the POP3 connection. Choose between: • Without Login: Monitor the connection to the POP3 server only. • Username and Password: Log into the POP3 server with user name and password (simple login, non-secure). • 128-bit MD5 hash value (APOP): Send the password in an encrypted form using APOP. This option must be supported by the POP3 server you're connecting to.
Username	This field is only visible if an option with login is selected above. Enter a username for POP3 authentication. Please enter a string.
Password	This field is only visible if an option with login is selected above. Enter a password for POP3 authentication. Please enter a string.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁰ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.88 SNMP APC Hardware Sensor

The SNMP APC Hardware sensor monitors performance counters on an APC UPS device using Simple Network Management Protocol (SNMP).

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)  section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) . It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

For devices with multiple performance counters multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

APC UPS Specific	
Library OIDs	Select the performance counters you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

APC UPS Specific	
Selected Interface	Shows the name of the interface (performance counter) monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Unit String	Define the unit of the numerical data that will be received at the given OID. Please enter a string.
Multiplication	If you want to multiply the received data with a certain value, enter the quotient here. Please enter an integer or float value.
Division	If you want to divide the received data by a certain value, enter the divisor here. Please enter an integer or float value.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • Ignore changes: No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.89 SNMP Cisco ADSL Sensor

The SNMP Cisco ADSL sensor monitors Asymmetric Digital Subscriber Line (ADSL) statistics of a Cisco router using Simple Network Management Protocol (SNMP). It shows the speed of downlink and uplink, remote and local attenuation, remote and local SNR (signal-to-noise ratio), and remote and local power output.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁹ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

For devices with multiple performance counters, multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Cisco ADSL Settings	
Line Index	Select the performance counters you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[168] settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[224] group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1688] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.90 SNMP Cisco ASA VPN Connections Sensor

The SNMP Cisco ASA VPN Connections sensor monitors the Virtual Private Network (VPN) connections on a Cisco Adaptive Security Appliance using Simple Network Management Protocol (SNMP). It shows the active sessions of the connection types email, IPsec, L2L, LB, SVC, WebVPN, as well as the total number of sessions, active users, and groups with active users.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁹ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ⁸⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹¹. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.91 SNMP Cisco ASA VPN Traffic Sensor

The SNMP Cisco ASA VPN Traffic sensor monitors the traffic of an Internet Protocol Security (IPsec) Virtual Private Network (VPN) connection on a Cisco Adaptive Security Appliance using Simple Network Management Protocol (SNMP). It shows incoming and outgoing traffic, as well as total traffic.

This sensor type is indented to monitor permanent connections. It will show an error if a connection is interrupted. It can monitor IPsec connections only!

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)  section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) . It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

If you select more than one connections, multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

ASA VPN Specific

Connections

Select the IPsec VPN connections you want to add a sensor for. You see a list of all active IPsec VPN connections available on the target ASA, listed with remote IP, user name, and the kind of connection. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head. **Note:** This sensor type can only monitor VPN connections based on **IPsec**. This means, for example, that connections using "Cisco AnyConnect" will not be listed here.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ¹⁶⁸⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

ASA VPN Specific

Remote IP	The IP address of the connection this sensor monitors. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Note: This sensor type can only monitor VPN connections based on IPsec .

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).

Sensor Display

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1688] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.92 SNMP Cisco ASA VPN Users Sensor

The SNMP Cisco ASA VPN Users sensor monitors account connections to a Virtual Private Network (VPN) on a Cisco Adaptive Security Appliance via Simple Network Management Protocol (SNMP). It can show the number of currently connected accounts and if a user account is currently offline or online.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁹ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ⁸⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹¹. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.93 SNMP Cisco CBQoS Sensor

The SNMP Cisco CBQoS sensor monitors network parameters using Cisco's Class Based Quality of Service (CBQoS) via Simple Network Management Protocol (SNMP). It supports the classes Class Map, Match Statement, and Queueing. The sensor shows current and maximum queue depth, pre policy packets, pre and post policy size, drop packets and size, drop packets without buffer, as well as fragment packets and size, depending on the particular class type.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁹ section.

For a general introduction to the technology behind Quality of Service monitoring, please see [Monitoring Quality of Service](#) ¹⁹³⁹ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor quality-of-service via compatible devices, PRTG will create one sensor for each CBQoS entry you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Class Based QoS Specific

CBQoS Entries	Select the measurements you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Class Based QoS Specific

Interface	Shows further information about the parameter this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	
Bitmask	
ObjectID	
ConfigID	

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ^[1805] .

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[224] group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1688] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.94 SNMP Cisco System Health Sensor

The SNMP Cisco System Health sensor monitors the system health of a Cisco device via Simple Network Management Protocol (SNMP). It can show the percentage CPU load, available memory in absolute and percentage values, the status of power supplies, temperatures (in Celsius), the current temperature states, and many more, depending on the available components of your device.

This sensor type has predefined limits for several metrics. These limits can be changed individually in the channel settings. For detailed information about channel limits please refer to the section [Sensor Channels Settings](#)¹⁶⁸³.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)²⁰⁰¹.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)¹⁹²³ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the system health of a Cisco device, PRTG will create one sensor for each measurement you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Cisco System Health Specific	
Measurement	Select the measurements you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ¹⁶⁸⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Cisco System Health Specific	
Measurement	Shows the ID of the measurement that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).

Sensor Display	
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.
Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.95 SNMP Cisco UCS Chassis Sensor

The SNMP Cisco UCS Chassis sensor monitors the health status of the chassis of a Cisco Unified Computing and Server (UCS) device via Simple Network Management Protocol (SNMP). It can show the states of configuration, license, oper, the operability, power status, thermal status, as well as the serial electronic erasable programmable read-only memory (SEEPROM) status. The creation of these channels depends on the available measurement components on the UCS chassis.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#) ²⁰⁰¹.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁹ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the health status of a Cisco UCS chassis, PRTG will create one sensor for each chassis you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Chassis	Select the chassis you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings

Chassis	Shows the chassis monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[1683] settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.96 SNMP Cisco UCS Physical Disk Sensor

The SNMP Cisco UCS Physical Disk sensor monitors a physical disk of a Cisco Unified Computing and Server (UCS) device via Simple Network Management Protocol (SNMP). It can show the operability status of the disk, as well as if the monitored disk is still connected.

Important notice: Currently, this sensor type is in **beta** status. The methods of operating can change at any time, as well as the available settings. **Do not expect** that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)²⁰⁰¹.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)¹⁹²³ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor physical disks in a UCS device, PRTG will create one sensor for each disk you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

UCS Physical Disk	
Disks	Select the disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head. Note: Only working disks (with the current status Up or Warning) will be shown here.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

UCS Physical Disk	
Disk	Shows the disk which this sensor monitors. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Display Name	Shows the display name of the physical disk which this sensor monitors. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.97 SNMP Cisco UCS System Health Sensor

The SNMP Cisco UCS System Health sensor monitors the system health of a Cisco Unified Computing and Server (UCS) device via Simple Network Management Protocol (SNMP). It can show the following: the number of operable resp. inoperable fans, the status of fan performance, fan thermal and fan voltage, and if a fan failure is predicted; the number of operable resp. inoperable fan modules, the status of fan module performance, fan module thermal and fan module voltage, and if a fan module failure is predicted; the number of operable resp. inoperable power supplies, the status of power supply performance, power supply thermal and power supply voltage, and if a power supply failure is predicted.

The creation of these channels depends on the available measurement components in the UCS device.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#) ^[2001].

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ^[1929] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration settings.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree.
Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.98 SNMP CPU Load Sensor

The SNMP CPU Load sensor monitors the system load using Simple Network Management Protocol (SNMP). It can show the load of several CPUs in percent.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ^[1923] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.

Sensor Display	
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹¹. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.99 SNMP Custom Sensor

The SNMP Custom sensor monitors a numerical value returned by a specific OID using Simple Network Management Protocol (SNMP).

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)  section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) . It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

OID values	
Channel Name	Enter a name for the channel the results at the given OID will be will shown in. You can change this value later in the sensor's channel settings  .
Value Type	Select how the results at the given OID will be handled. Choose between: ▪ Gauge (unsigned Integer): For integer values, such as 10 or 120. ▪ Gauge (signed integer): For integer values, such as -12 or 120. ▪ Gauge (float): For float values, such as -5.80 or 8.23. ▪ Delta (Counter): For counter values. PRTG will calculate the difference between the last and the current value. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

OID values	
OID value	Enter the OID of the SNMP object you want to receive numerical data from. Note: Most OIDs begin with 1.3.6.1 . However, entering OIDs starting with 1.0 , or 1.1 , or 1.2 is also allowed. If you want to disable the validation of your entry entirely, add the string norfccheck: at the beginning of your OID, for example, norfccheck:2.0.0.0.1 .
Unit String	Define the unit of the numerical data that will be received at the given OID. Please enter a string.
Value Type	Shows the value type of the numerical data that will be received at the given OID. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Multiplication	If you want to multiply the received data with a certain value, enter the quotient here. Please enter an integer or float value.
Division	If you want to divide the received data by a certain value, enter the divisor here. Please enter an integer or float value.
If value changes	Define what shall be done in case the value of this sensor changes. You can choose between: • Ignore changes (default): No action will be taken on change. • Trigger 'On Change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: How do I find out what OID I need to use for a custom sensor?

- <http://www.paessler.com/knowledgebase/en/topic/903>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.100 SNMP Custom String Sensor

The SNMP Custom String sensor monitors a string returned by a specific OID using Simple Network Management Protocol (SNMP). It can check for keywords. If you want to use limits for the sensor channel value, you can also extract a numeric value contained in the string.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ^[192] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
100 SNMP Custom String Sensor

OID Values	
OID Value	Enter the OID of the SNMP object you want to receive a string from. Note: Most OIDs begin with 1.3.6.1 . However, entering OIDs starting with 1.0 , or 1.1 , or 1.2 is also allowed. If you want to disable the validation of your entry entirely, add the string norfccheck : at the beginning of your OID, for example, norfccheck:2.0.0.0.1 .
Maximum Length of String	Define the maximum length of the string that will be received from the SNMP object at the given OID. If the string is longer than this value, the sensor will be set to an error status. Please enter an integer value or leave the field empty.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • Ignore changes (default): No action will be taken on change. • Trigger 'On Change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.

Keyword Search	
Response Must Include (Error State)	Define which string must be part of the data that is received from the SNMP object at the given OID. You can either enter plain text or a Regular Expression ²⁰¹⁰ . If the data does not include the search pattern, the sensor will be set to an error state. Please enter a string or leave the field empty.
For Keyword Search Use	Define in which format you have entered the search expression in the field above. ▪ Plain Text: Search for the string as plain text. The characters * and ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible with plain text search. ▪ Regular Expression: Treat the search pattern as a Regular Expression²⁰¹⁰.
Response Must Not Include (Error State)	Define which string must not be part of the data that is received from the SNMP object at the given OID. You can either enter plain text or a Regular Expression ²⁰¹⁰ . If the data does include the search pattern, the sensor will be set to an error state. Please enter a string or leave the field empty.
For Keyword Search Use	Define in which format you have entered the search expression in the field above. ▪ Plain Text: Search for the string as plain text. The characters * and ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible with plain text search. ▪ Regular Expression: Treat the search pattern as a Regular Expression²⁰¹⁰.
Response Must Include (Warning State)	Define which string must be part of the data that is received from the SNMP object at the given OID. You can either enter plain text or a Regular Expression ²⁰¹⁰ . If the data does not include the search pattern, the sensor will be set to a warning state. Please enter a string or leave the field empty.
For Keyword Search Use	Define in which format you have entered the search expression in the field above. ▪ Plain Text: Search for the string as plain text. The characters * and ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible with plain text search. ▪ Regular Expression: Treat the search pattern as a Regular Expression²⁰¹⁰.
Response Must Not	Define which string must not be part of the data that is received

Extended Processing	
Extract Number Using Regular Expression	Define if you want to filter out a numeric value from the string received from the SNMP object at the given OID. You can convert this into a float value in order to use it with channel limits (see Sensor Channels Settings¹⁶⁸³). ▪ No extraction: Do not extract a float value. Use the result as a string value. ▪ Extract a numeric value using a regular expression: Use a regular expression to identify a numeric value in the string and convert it to a float value. Define below. See also the example⁹⁸¹ below.
Regular Expression	This setting is only visible if number extraction is enabled above. Enter a Regular Expression²⁰¹⁰ to identify the numeric value you want to extract from the string returned by the SNMP object at the given OID. You can use capturing groups here. Make sure the expression returns numbers only (including decimal and thousands separators). The result will be further refined by the settings below.
Index of Capturing Group	This setting is only visible if number extraction is enabled above. If your regular expression uses capturing groups, please specify which one will be used to capture the number. Please enter an integer value or leave the field empty.
Decimal Separator	This setting is only visible if number extraction is enabled above. Define which character is used as decimal separator for the number extracted above. Please enter a string or leave the field empty.
Thousands Separator	This setting is only visible if number extraction is enabled above. Define which character is used as thousands separator for the number extracted above. Please enter a string or leave the field empty.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Example: Number Extraction with Regular Expression

If you want to extract a number in the response string using a regular expression, please note that the index for captures in this sensor is based on **1 (not on 0)**. Furthermore, capturing groups are not created automatically. The example below will illustrate this issue.

Consider the following string as returned by a request for CPU usage:

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

100 SNMP Custom String Sensor

```
5 Sec (3.49%), 1 Min (3.555%), 5 Min (3.90%)
```

Assuming you would like to filter for the number **3.555**, i.e., the percentage in the second parentheses. Then enter the following regex in the **Regular Expression** field:

```
(\d+\.\d+).* (\d+\.\d+).* (\d+\.\d+)
```

As **Index of Capturing Group** enter **3**. This will extract the desired number 3.555.

The index has to be 3 in this case because the capturing groups here are the following:

- Group 1 contains "3.49%, 1 Min (3.555), 5 Min (3.90"
- Group 2 contains "3.49"
- Group 3 contains "3.555"
- Group 4 contains "3.90"

Please keep in mind this note about index and capturing groups when using number extraction.

More

Knowledge Base: How do I find out what OID I need to use for a custom sensor?

- <http://www.paessler.com/knowledgebase/en/topic/903>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁸ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.101 SNMP Dell Hardware Sensor

The SNMP Dell Hardware sensor monitors performance counters on a Dell hardware device using Simple Network Management Protocol (SNMP).

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)  section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) . It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

For devices with multiple performance counters multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Dell Hardware Specific	
Library OIDs	Select the performance counters you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Dell Hardware Specific	
Selected Interface	Shows the name of the interface (performance counter) monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Unit String	Define the unit of the numerical data that will be received at the given OID. Please enter a string.
Multiplication	If you want to multiply the received data with a certain value, enter the quotient here. Please enter an integer or float value.
Division	If you want to divide the received data by a certain value, enter the divisor here. Please enter an integer or float value.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • Ignore changes: No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1793. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.102 SNMP Dell PowerEdge Physical Disk Sensor

The SNMP Dell PowerEdge Physical Disk sensor monitors a physical disk in a Dell PowerEdge server using Simple Network Management Protocol (SNMP). It can show the disk status, the roll up status, the component status, as well as if there is currently a warning regarding the Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) status.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#) ²⁰⁰¹.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²³ section.

Requirement: Dell OpenManage Server Administrator or iDRAC 7

This sensor needs the Dell OpenManage Server Administrator tool to be installed on the device in order to monitor PowerEdge servers. Please make sure that you enable SNMP in the OpenManage Server Administrator. For details, please see section **More** below. **Note:** You can also monitor Dell PowerEdge servers with this sensor type via Integrated Dell Remote Access Controller (iDRAC) 7.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰¹. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor physical disks in a Dell PowerEdge server, PRTG will create one sensor for each disk. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Dell PowerEdge Physical Disk Settings

Disk

Select the disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Dell PowerEdge Physical Disk Settings

Disk	Shows the name of the disk that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Data Source	Shows the interface which is used to get monitoring data. This is either Dell OpenManage Server Administrator (OMSA) or Integrated Dell Remote Access Controller (iDRAC).

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[100] settings).

Sensor Display	
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.
Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: What do I need to monitor Dell servers?

- <http://www.paessler.com/knowledgebase/en/topic/45333>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.103 SNMP Dell PowerEdge System Health Sensor

The SNMP Dell PowerEdge System Health sensor monitors the system health of a Dell PowerEdge server using Simple Network Management Protocol (SNMP). It can show the global system status, the power supply status, the temperature status, the cooling device status, the memory device status, the voltage status, and many more, depending on the available components of your device.

This sensor type has predefined limits for several metrics. These limits can be changed individually in the channel settings. For detailed information about channel limits please refer to the section [Sensor Channels Settings](#)¹⁶⁸³.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)²⁰⁰¹.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)¹⁹²³ section.

Requirement: Dell OpenManage Server Administrator or iDRAC 7

This sensor needs the Dell OpenManage Server Administrator tool to be installed on the device in order to monitor PowerEdge servers. Please make sure that you enable SNMP in the OpenManage Server Administrator. For details, please see section **More** below. **Note:** You can also monitor Dell PowerEdge servers with this sensor type via Integrated Dell Remote Access Controller (iDRAC) 7.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the health status of a Dell PowerEdge server, PRTG will create one sensor for each chassis you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Dell PowerEdge System Health Specific

Chassis

Select the chassis you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Dell PowerEdge System Health Specific	
Chassis	Shows the chassis this sensor monitors. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Channel Mask	Shows the channel mask that describes which sensors are available. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Data Source	Shows the interface which is used to get monitoring data. This is either Dell OpenManage Server Administrator (OMSA) or Integrated Dell Remote Access Controller (iDRAC).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.
Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: What do I need to monitor Dell servers?

- <http://www.paessler.com/knowledgebase/en/topic/45333>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[143] section.

6.8.104 SNMP Disk Free Sensor

The SNMP Disk Free sensor monitors the free disk space on a logical disk via Simple Network Management Protocol (SNMP). It can show free space in percent and in total, as well as the total space. **Note:** This sensor uses more generic Object Identifier (OID) values compared to the [SNMP Linux Disk Free Sensor](#)^[1102].

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)^[1929] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor memory usage, PRTG will create one sensor for each memory type you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Disk Free Settings	
Disk	Select one or more disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Disk Free Settings

Disk	Shows the name of the disk that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁰⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁰⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.105 SNMP GSA System Health Sensor

The SNMP GSA System Health sensor monitors the system health of a Google Search Appliance (GSA) via Simple Network Management Protocol (SNMP). It can show the number of queries per minute, the number of processed documents, the number of indexed documents, the number of processed bytes, the activity status of crawling, the crawling rate per second, as well as the health status of disk, temperature, and machine.

Note: The location you provide in the GSA's SNMP configuration section will be shown in PRTG's [GeoMaps](#)^[1718]. In order to use SNMP v3 for monitoring, you need to add an SNMP v3 user in the GSA's SNMP configuration.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)^[2001].

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)^[1923] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹¹. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.106 SNMP Hardware Status Sensor

The SNMP Hardware Status sensor monitors the status of a hardware component of a server via Simple Network Management Protocol (SNMP). It shows the current status of the component, as well as the number of errors per time period.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²³ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor hardware components of a server, PRTG will create one sensor for each component you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Hardware Specific	
Hardware Component	Select the hardware components you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Hardware Specific	
Hardware Component	Shows further information about the hardware component. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Product ID	
Description	
Type	
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[1683] settings).

Sensor Display

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1688] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.107 SNMP HP LaserJet Hardware Sensor

The SNMP HP LaserJet Hardware sensor monitors performance counters on a HP LaserJet hardware device using Simple Network Management Protocol (SNMP).

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)  section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) . It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

For devices with multiple performance counters multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Dell Hardware Specific	
Library OIDs	Select the performance counters you want to add a sensor for. A list of available counters for your device is shown with category and name: ▪ Toner/Status ▪ Paper/Status ▪ Jam/Status A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ¹⁶⁹⁰ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
HP LaserJet Specific	
Selected Interface	Shows the name of the interface (performance counter) monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • Ignore changes: No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification¹⁶⁹⁰ whenever the sensor value changes.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.108 SNMP HP ProLiant Logical Disk Sensor

The SNMP HP ProLiant Logical Disk sensor monitors a logical disk in an HP server via Simple Network Management Protocol (SNMP). It can show disk status and completion. Completion is only important when the disk status is "Reconstructing" or "Expanding" and illustrates the progress of this task.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)^[2001].

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)^[1923] section.

Requirement: HP System Management Tools

This sensor needs a specific HP system management tool to be installed on the target device, so it reports data via SNMP: [HP Insight Management Agents for Windows Server 2003/2008](#). In order to receive SNMP data from RAID controllers you will additionally need [HP Insight Management WBEM Providers](#). For more details and download links please refer to the subsection **More** below.

Note: Some of the HP [Object Identifiers \(OIDs\)](#) which this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG which points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend using the [Agentless Management](#) feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor logical disks in a HP server, PRTG will create one sensor for each disk you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

HP ProLiant Logical Disk Settings

Disk

Select the disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

HP ProLiant Logical Disk Settings

Disk	Shows the name of the disk that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- <http://www.paessler.com/knowledgebase/en/topic/33133>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.109 SNMP HP ProLiant Memory Controller Sensor

The SNMP HP ProLiant Memory Controller sensor monitors a memory controller in an HP server via Simple Network Management Protocol (SNMP). It shows the error status of the controller, the condition of the controller, and states and conditions of available modules. **Note:** If modules are inserted at a later point, the sensor has to be added again.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)²⁰⁰¹.

For supported lookup values of this specific sensor, please see subsection [More](#)¹⁰³⁴ below.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)¹⁹²³ section.

Requirement: HP System Management Tools

This sensor needs a specific HP system management tool to be installed on the target device, so it reports data via SNMP: **HP Insight Management Agents for Windows Server 2003/2008**. In order to receive SNMP data from RAID controllers you will additionally need **HP Insight Management WBEM Providers**. For more details and download links please refer to the subsection **More** below.

Note: Some of the HP **Object Identifiers (OIDs)** which this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG which points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend using the **Agentless Management** feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰¹. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor memory controllers in a HP server, PRTG will create one sensor for each controller you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

HP ProLiant Memory Controller Settings

Controller	Select the controllers you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

HP ProLiant Memory Controller Settings

Controller	Shows the name of the controller that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1793. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- <http://www.paessler.com/knowledgebase/en/topic/33133>

Knowledge Base: Which lookup values are supported by the SNMP HP ProLiant Memory Controller Sensor?

- <http://www.paessler.com/knowledgebase/en/topic/44803>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.110 SNMP HP ProLiant Network Interface Sensor

The SNMP HP ProLiant Network Interface sensor monitors a network interface in an HP server via Simple Network Management Protocol (SNMP). It can show traffic in and out, the number of transmitted and received good frames, the number of transmitted and received bad frames, alignment and FCS (Frame Check Sequence) errors, late and excessive collisions, carrier sense errors, and when the frames are too long.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁹ section.

Requirement: HP System Management Tools

This sensor needs a specific HP system management tool to be installed on the target device, so it reports data via SNMP: [HP Insight Management Agents for Windows Server 2003/2008](#). In order to receive SNMP data from RAID controllers you will additionally need [HP Insight Management WBEM Providers](#). For more details and download links please refer to the subsection **More** below.

Note: Some of the HP [Object Identifiers \(OIDs\)](#) which this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG which points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend using the [Agentless Management](#) feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor network interfaces in a HP server, PRTG will create one sensor for each interface. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

HP ProLiant Network Interface Settings

Network Interface

Select the interfaces you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Note: In the **HP ProLiant Network Interface Settings** section, the **Status** of each available network interface is shown. If this status is **Link Failure**, it is still possible to add a sensor for the respective interface. Though, most likely the sensor for this interface will not work correctly. The error message in this case will be **No Such Name (SNMP error # 2)**.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
HP ProLiant Network Interface Settings	
Network Interface	Shows the name of the interface that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.

Sensor Display	
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings). ▪ Show in and out traffic as positive and negative area chart: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹³. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- <http://www.paessler.com/knowledgebase/en/topic/33133>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.111 SNMP HP ProLiant Physical Disk Sensor

The SNMP HP ProLiant Physical Disk sensor monitors a physical disk in an HP server via Simple Network Management Protocol (SNMP). It can show read and written sectors, hard and corrected read errors, hard and corrected write errors, the disk status, the drive condition, the Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) status, and if the threshold is passed.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)²⁰⁰¹.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)¹⁹²³ section.

Requirement: HP System Management Tools

This sensor needs a specific HP system management tool to be installed on the target device, so it reports data via SNMP: [HP Insight Management Agents for Windows Server 2003/2008](#). In order to receive SNMP data from RAID controllers you will additionally need [HP Insight Management WBEM Providers](#). For more details and download links please refer to the subsection **More** below.

Note: Some of the HP [Object Identifiers \(OIDs\)](#) which this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG which points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend using the [Agentless Management](#) feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor physical disks in a HP server, PRTG will create one sensor for each disk. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

HP ProLiant Physical Disk Settings

Disk

Select the disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
HP ProLiant Physical Disk Settings	
Disk	Shows the name of the disk that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 1683 settings). ▪ Show in and out traffic as positive and negative area chart: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 1683 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) 224 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 1805 .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- <http://www.paessler.com/knowledgebase/en/topic/33133>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.112 SNMP HP ProLiant System Health Sensor

The SNMP HP ProLiant System Health sensor monitors the system health of an HP ProLiant server via Simple Network Management Protocol (SNMP). It can show the overall status, the thermal status, the system fan status, the CPU fan status, the number of broken and running fans, as well as the number of broken and running fans that are fault tolerant, and status and condition of the power supply.

Furthermore, it can show several temperatures for various components of an HP ProLiant server—for example: memory, power supply, CPU, system, and storage. It is also possible to display the power consumption and disk controller status. These channels are created at run-time, depending on the available measurement components.

The SNMP HP ProLiant System Health sensor has predefined limits for temperatures and broken frames. These limits can be changed individually in the channel settings. For detailed information about channel limits please refer to the subsection [Channels](#)¹⁰⁵² below.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)²⁰⁰¹.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)¹⁹²³ section.

Requirement: HP System Management Tools

This sensor needs a specific HP system management tool to be installed on the target device, so it reports data via SNMP: **HP Insight Management Agents for Windows Server 2003/2008**. In order to receive SNMP data from RAID controllers you will additionally need **HP Insight Management WBEM Providers**. For more details and download links please refer to the subsection **More** below.

Note: Some of the HP **Object Identifiers (OIDs)** which this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG which points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend using the **Agentless Management** feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings). ▪ Show in and out traffic as positive and negative area chart: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- <http://www.paessler.com/knowledgebase/en/topic/33133>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.113 SNMP IBM System X Logical Disk Sensor

The SNMP IBM System X Logical Disk sensor monitors a logical disk in an IBM server via Simple Network Management Protocol (SNMP). It shows the status of a logical disk.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)²⁰⁰¹.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)¹⁹²³ section.

Requirement: IBM Systems Director Platform Agent

This sensor type needs the IBM Systems Director Platform Agent to be installed on the target IBM device in order to monitor it through SNMP. For more information, please see section [More](#) below.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the logical disks of an IBM device, PRTG will create one sensor for each disk you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

IBM System X Logical Disk Settings

Disk	Select the logical disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

IBM System X Logical Disk Settings

Disk	Shows the ID of the logical disk. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: What are the requirements to monitor IBM System x?

- <http://www.paessler.com/knowledgebase/en/topic/59393>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.114 SNMP IBM System X Physical Disk Sensor

The SNMP IBM System X Physical Disk sensor monitors a physical disk in an IBM server via Simple Network Management Protocol (SNMP). It shows the status of a physical disk.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)²⁰⁰¹.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)¹⁹²³ section.

Requirement: IBM Systems Director Platform Agent

This sensor type needs the IBM Systems Director Platform Agent to be installed on the target IBM device in order to monitor it through SNMP. For more information, please see section [More](#) below.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the physical disks of an IBM device, PRTG will create one sensor for each disk you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

IBM System X Physical Disk Settings

Disk	Select the physical disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

IBM System X Physical Disk Settings

Disk	Shows the ID of the physical disk. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: What are the requirements to monitor IBM System x?

- <http://www.paessler.com/knowledgebase/en/topic/59393>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.115 SNMP IBM System X Physical Memory Sensor

The SNMP IBM System X Physical Memory sensor monitors the memory modules in an IBM server via Simple Network Management Protocol (SNMP). It shows the condition of a memory module, as well as its power status.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)²⁰⁰¹.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)¹⁹²³ section.

Requirement: IBM Systems Director Platform Agent

This sensor type needs the IBM Systems Director Platform Agent to be installed on the target IBM device in order to monitor it through SNMP. For more information, please see section **More** below.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the memory modules of an IBM device, PRTG will create one sensor for each module you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

IBM System X Physical Memory Settings	
Module	Select the memory modules you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

IBM System X Physical Memory Settings

Name	Shows further information about the module. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Caption	
Serial Number	
Size	

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[168] settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: What are the requirements to monitor IBM System x?

- <http://www.paessler.com/knowledgebase/en/topic/59393>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.116 SNMP IBM System X System Health Sensor

The SNMP IBM System X System Health sensor monitors the system health of an IBM device via Simple Network Management Protocol (SNMP). It can show revolutions per minute of fans (or the current percentage of the possible maximum), temperatures of ambient and CPUs, voltage, status of power supplies, and many more, depending on the available measurement components.

Note: If the IBM device returns a string in an unexpected format for the percentage of fan revolutions (for example, "offline"), this sensor will show **-1%** in the corresponding channel. You can define a **Down** status for this via [channel limits](#)^[1684].

This sensor type has predefined limits for several metrics. These limits can be changed individually in the channel settings. For detailed information about channel limits please refer to the section [Sensor Channels Settings](#)^[1685].

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)^[2001].

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)^[1923] section.

Requirement: IBM Systems Director Platform Agent

This sensor type needs the IBM Systems Director Platform Agent to be installed on the target IBM device in order to monitor it through SNMP. For more information, please see section **More** below.

Note: The SNMP IBM System X System Health sensor can also run directly on an Integrated Management Module (IMM) network port and can show the overall health on IMMs.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the system health of an IBM device, PRTG will create one sensor for each measurement you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

IBM System X System Health Specific

Measurement	Select the measurements you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

IBM System X System Health Specific

Source	Shows the source of the measurement. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Measurement	Shows the ID of the measurement that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁹⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1791. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: What are the requirements to monitor IBM System x?

- <http://www.paessler.com/knowledgebase/en/topic/59393>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.117 SNMP interSeptor Pro Environment Sensor

The SNMP interSeptor Pro Environment sensor queries data from a Jakarta interSeptor Pro environmental monitoring system via Simple Network Management Protocol (SNMP). It can monitor temperature and humidity as measured by the Jakarta interSeptor Pro device.

Note: In order to monitor an interSeptor Pro device's data with this sensor, you have to add the IP address of your PRTG installation to **Access Control** in the interSeptor Pro control panel. Open the interSeptor Pro web interface, select **InterSeptor Pro Menu | System Configuration | Access Control** for this purpose, and allow access for PRTG's IP address.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)  section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) . It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the environment via an interSeptor Pro device, PRTG will create one sensor for each measuring point you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

InterSeptor Environment Specific	
Measuring Point	Select the measuring points you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

InterSeptor Environment Specific

Name	Shows information about the measurement which this sensor monitors. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Measuring Point	Shows the measuring point which this sensor monitors. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[168] settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁰⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁰⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.118 SNMP LenovoEMC Physical Disk Sensor

The SNMP Lenovo Physical Disk sensor monitors a physical disk in a LenovoEMC Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP). It shows the overall disk status. States of the disk can be **Normal** (sensor status **Up**), **Unknown** and **Foreign** (both with sensor status **Warning**), as well as **Faulted** and **Missing** (both with sensor status **Down**).

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#) ²⁰⁰¹.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²³ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor physical disks in a LenovoEMC NAS, PRTG will create one sensor for each disk you select. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

LenovoEMC Physical Disk Settings

Disk	Select the disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

LenovoEMC Physical Disk Settings

Disk	Shows the disk monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the disk monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Size	Shows the size of the disk monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹³. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.119 SNMP LenovoEMC System Health Sensor

The SNMP LenovoEMC System Health sensor monitors the system health of a LenovoEMC Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP). It shows the overall status of the RAID. States can be **Normal** (sensor status **Up**), **Unknown**, **Rebuilding**, **Degraded**, and **RebuildFS** (all with sensor status **Warning**), as well as **Faulted** (sensor status **Down**).

Furthermore, this sensor can show, for example, states of several fans, voltages, and temperatures. These channels are created at run-time depending on the available measurement components in the LenovoEMC NAS.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)^[200].

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)^[192] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1093] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1090] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.120 SNMP Library Sensor

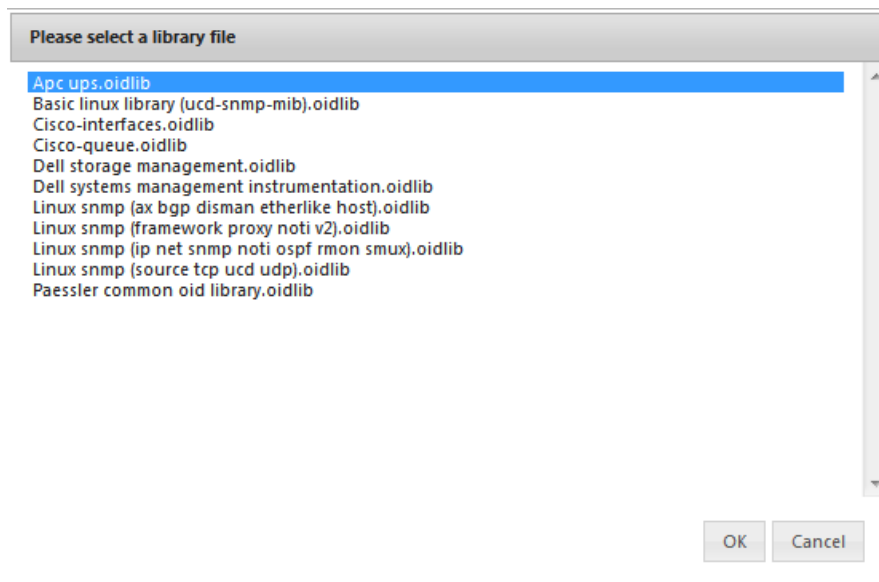
The SNMP Library sensor monitors a device using Simple Network Management Protocol (SNMP) in combination with a compiled Management Information Base (MIB) library file. This provides extended monitoring beyond the standard SNMP sensors of PRTG.

In order to monitor any SNMP capable device, you can download the manufacturer's MIB files for these devices, convert them to the Paessler **oidlib** format, and import them into PRTG. To make your monitoring setup as convenient as possible, PRTG is delivered with pre-compiled **oidlib** library files that already contain the Object Identifier (OID) of SNMP counters for the most common devices in a network.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁹ section.

Add Sensor

[Manually add](#) ²²⁰ a new sensor to an SNMP device and from the **Add Sensor** dialog, select **SNMP Library** sensor. PRTG will show a list of **oidlib** files available on the system. This contains all library files stored at the **\snmplibs** sub-directory of your PRTG installation directory—both the ones delivered with PRTG and your own files. For details about directory paths, please see section [Data Storage](#) ²⁰³⁶.



List of SNMP Default Library Files

The file names in the list indicate the potential purpose. Select a name that appears appropriate for your device and confirm with the **OK** button. Often, **Paessler common oid library.oidlib** is a good start. If the file does not fit to your device, this will result in an error message saying that no available interfaces were found on this device. If you see this message, please hit the **Go back and retry** button and try with another file. If counters were found for your device, you will see the sensor's settings.

Default OIDLIB Files Overview

The following files are delivered with PRTG and allow to extend your SNMP monitoring for many devices. Please be aware that not all devices and/or parameters may be supported by the libraries.

- **APC UPS.oidlib**
Can be used to monitor uninterruptible power supplies (UPS) from APC American Power Conversion Corp.
- **Basic Linux Library (UCD-SNMP-MIB).oidlib**
Can be used to monitor basic system parameters on Linux systems, such as memory, disk and swap, CPU, etc.
- **cisco-interfaces.oidlib**
Can be used to monitor Cisco specific parameters.
- **cisco-queue.oidlib**
Can be used to monitor Cisco specific parameters.
- **Dell Storage Management.oidlib**
Can be used to monitor Dell storage devices. Possible parameters include disk arrays, battery and power supply, fan and temperature, virtual disk, etc.
- **Dell Systems Management Instrumentation.oidlib**
Can be used to monitor the hardware of Dell systems. Possible parameters include ACPower and battery, alerts, base board, Bios, BMC, chassis, COO, cooling, event log, firmware, IDE, keyboard, memory, port, network, processor, SCSI, system, temperature, USB, UUID, etc.
- **Linux SNMP (AX BGP DisMan EtherLike Host).oidlib**
Can be used to monitor different aspects of Linux systems. **Note:** This file can find a very large number of possible interfaces. It may take a few seconds until the selection table is shown.
- **Linux SNMP (Framework Proxy Noti v2).oidlib**
Can be used to monitor different aspects of Linux systems. **Note:** This file can find a very large number of possible interfaces. It may take a few seconds until the selection table is shown.
- **Linux SNMP (IP Net SNMP Noti OSPF RMON SMUX).oidlib**
Can be used to monitor different aspects of Linux systems. **Note:** This file can find a very large number of possible interfaces. It may take a few seconds until the selection table is shown.
- **Linux SNMP (Source TCP UCD UDP).oidlib**
Can be used to monitor different aspects of Linux systems. **Note:** This file can find a very large number of possible interfaces. It may take a few seconds until the selection table is shown.

- **Paessler Common OID Library.oidlib**
Can be used to monitor many common hardware devices.

Import MIB Files

Additionally you can create your own **oidlib** files by importing your device manufacturers' MIB files, using a the free Paessler **MIB Importer**. Simply convert your **mib** files and save the resulting **oidlib** files to the **\snmplibs** sub-folder of your PRTG program directory. For details about directory paths, please see [Data Storage](#)^[2036]. For more information and download of **MIB Importer**, please see the link in the [More](#)^[1100] section below.

SNMP Library Sensor—Add Sensor Settings

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

SNMP Library Specific	
Library	This shows the path to the oidlib file selected before. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Library-OIDs	Select the aspects of the device you want to monitor. A list specific to your setup is shown. It contains all counters found in the chosen library that match your device. Select one or more items by adding a check mark in front of the respective line. For each selection one sensor will be created when you click the Continue button.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SNMP Library Specific

Selected Interface	Shows the interface monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Unit String	Enter a string describing the unit of the returned values. This is for display purposes only. Please enter a string.
Multiplication	If you want to multiply the received data with a certain value, enter the quotient here. Please enter an integer or float value, or leave the field empty.
Division	If you want to divide the received data by a certain value, enter the divisor here. Please enter an integer or float value, or leave the field empty.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

More

Knowledge Base: How can I import my MIB files into PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/733>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.121 SNMP Linux Disk Free Sensor

The SNMP Linux Disk Free sensor monitors free space on disks of a Linux/Unix system using Simple Network Management Protocol (SNMP). It shows the total free disk space (sum), and the free disk space in percent for every mounted partition (volume).

Note: The free space returned by this sensor type shows the disk space that is not yet used. Not all of this space may be available for use, as a part of this space can be reserved by the system, e.g. for redundancy purposes. For details, please see the article linked in the [More](#) ¹¹⁰⁹ section below.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²³ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ⁸⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Set limits checked against ALL disks

In this section you can set limits that are valid for all channels and all drives. By entering limits, you can define when the sensor will enter a **Warning** or **Down** status; depending on the data provided by all drives that this sensor monitors. If you want to define limits for separate channels individually please use the limit settings in the sensor's **Channels** settings. **Note:** All limits defined here are valid additionally to the limits defined in the particular **Channels** settings!

Percentage Limit Check	Enable or disable a limit check for the free space in percentage channels of all drives. By default percentage limits are enabled with lower warning and lower error limit. Choose between: • Disable Percentage Limits: Do not use the drives' data to control the sensor's status. • Enable Percentage Limits: Define limits. Additional fields appear below. The sensor will enter a warning or down state when free space limits are undercut or overrun.
Upper Error Limit	This field is only visible if percentage limit check is enabled above. Specify an upper limit in percent for a Down status. If the free disk space of one of your drives overruns this percent value, the sensor will be set to Down. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings¹⁶⁸³. The limits set here and in the channel settings are valid simultaneously!
Upper Warning Limit	This field is only visible if percentage limit check is enabled above. Specify an upper limit in percent for a Warning status. If the free disk space of one of your drives overruns this percent value, the sensor will be set to Warning. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings¹⁶⁸³. The limits set here and in the channel settings are valid simultaneously!
Lower Warning Limit	This field is only visible if percentage limit check is enabled above. Specify a lower limit in percent for a warning state. If the free disk space of one of your drives undercuts this percent value, the sensor will be set to warning. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings¹⁶⁸³. The limits set here and in the channel settings are valid simultaneously!

Set limits checked against ALL disks	
Lower Error Limit	This field is only visible if percentage limit check is enabled above. Specify a lower limit in percent for entering a Down status. If the free disk space of one of your drives undercuts this percent value, the sensor will be set to Down . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Byte Limit Check	Enable or disable a limit check for the free bytes channels of all drives. Choose between: • Disable Byte Limits: Do not use the drives' data to control the sensor's status. • Enable Byte Limits: Define limits. Additional fields appear below. The sensor will enter a warning or down state when free space limits are undercut or overrun.
Upper Error Limit	This field is only visible if byte limit check is enabled above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor will be set to Down . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Upper Warning Limit	This field is only visible if byte limit check is enabled above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor will be set to Warning . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Lower Warning Limit	This field is only visible if byte limit check is enabled above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor will be set to Warning . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!

Set limits checked against ALL disks

Lower Error Limit	This field is only visible if byte limit check is enabled above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor will be set to Down . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Alarm on Missing/ Removed Disk	If a monitored disk is removed or not found, values are set to zero. Select the alarming approach in this case. Choose between: ▪ Deactivate alarm (default): Select this option if you do not want an alarm for a removed disk. ▪ Activate Alarm: Select this option if you want to be alerted if a monitored disk is removed.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?

- <http://www.paessler.com/knowledgebase/en/topic/43183>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁰ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.122 SNMP Linux Load Average Sensor

The SNMP Load Average sensor monitors the system load average of a Linux/Unix system using Simple Network Management Protocol (SNMP). It shows the average system load within a one, five, and 15 minutes interval (each in one channel).

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ^[192] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol

Sensor Display	
	of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1791. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.123 SNMP Linux Meminfo Sensor

The SNMP Linux Meminfo sensor monitors the memory usage of a Linux/Unix system using Simple Network Management Protocol (SNMP). It shows the available memory in total and in percent.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ^[192] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol

Sensor Display	
	of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹¹. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.124 SNMP Linux Physical Disk Sensor

The SNMP Linux Physical Disk sensor monitors input/output (I/O) on disks of a Linux/Unix system using Simple Network Management Protocol (SNMP). It shows read and written bytes per second, read and write accesses per second, as well as load average within a specific time span (1, 5, and 15 minutes), depending on the counters available on the disk.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)  section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) . It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor I/O on disks of a Linux/Unix system, PRTG will create one sensor for each disk you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Physical Disk Settings	
Disk	Select one or more disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Physical Disk Settings

Disk	Shows further information about the disk that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Bitmask	

Set limits checked against ALL disks

In this section you can set limits that are valid for all channels and all drives. By entering limits, you can define when the sensor will enter a **Warning** or **Down** status; depending on the data provided by all drives that this sensor monitors. If you want to define limits for separate channels individually please use the limit settings in the sensor's **Channels** settings.

Note: All limits defined here are valid additionally to the limits defined in the particular **Channels** settings!

Percentage Limit Check	Enable or disable a limit check for load average in percentage channels of all drives. By default percentage limits are enabled with lower warning and lower error limit. Choose between: • Disable Percentage Limits: Do not use the drives' data to control the sensor's status. • Enable Percentage Limits: Define limits. Additional fields appear below. The sensor will enter a warning or down state when load average limits are undercut or overrun.

Set limits checked against ALL disks	
Upper Error Limit	This field is only visible if percentage limit check is enabled above. Specify an upper limit in percent for a Down status. If load average of one of your drives overruns this percent value, the sensor will be set to Down . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Upper Warning Limit	This field is only visible if percentage limit check is enabled above. Specify an upper limit in percent for a Warning status. If load average of one of your drives overruns this percent value, the sensor will be set to Warning . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Lower Warning Limit	This field is only visible if percentage limit check is enabled above. Specify a lower limit in percent for a warning state. If load average of one of your drives undercuts this percent value, the sensor will be set to warning. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Lower Error Limit	This field is only visible if percentage limit check is enabled above. Specify a lower limit in percent for entering a Down status. If load average of one of your drives undercuts this percent value, the sensor will be set to Down . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Byte Limit Check	Enable or disable a limit check for read and written bytes channels of all drives. Choose between: • Disable Byte Limits: Do not use the drives' data to control the sensor's status. • Enable Byte Limits: Define limits. Additional fields appear below. The sensor will enter a warning or down state when read and written bytes limits are undercut or overrun.

Set limits checked against ALL disks	
Upper Error Limit	This field is only visible if byte limit check is enabled above. Specify an upper limit. Use the same unit as shown by the bytes channels of this sensor (by default this is MByte). If the read and/or written bytes of one of your drives overruns this bytes value, the sensor will be set to Down . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Upper Warning Limit	This field is only visible if byte limit check is enabled above. Specify an upper limit. Use the same unit as shown by the bytes channels of this sensor (by default this is MByte). If the read and/or written bytes of one of your drives overruns this bytes value, the sensor will be set to Warning . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Lower Warning Limit	This field is only visible if byte limit check is enabled above. Specify a lower limit. Use the same unit as shown by the bytes channels of this sensor (by default this is MByte). If the read and/or written bytes of one of your drives undercuts this bytes value, the sensor will be set to Warning . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Lower Error Limit	This field is only visible if byte limit check is enabled above. Specify a lower limit. Use the same unit as shown by the bytes channels of this sensor (by default this is MByte). If the read and/or written bytes of one of your drives undercuts this bytes value, the sensor will be set to Down . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Alarm on Missing/ Removed Disk	If a monitored disk is removed or not found, values are set to zero. Select the alarming approach in this case. Choose between: ▪ Deactivate alarm (default): Select this option if you do not want an alarm for a removed disk. ▪ Activate Alarm: Select this option if you want to be alerted if a monitored disk is removed.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.125 SNMP Memory Sensor

The SNMP Memory sensor monitors the memory usage of a system via Simple Network Management Protocol (SNMP). It can show the available memory in total and in percent, as well as the total memory. **Note:** This sensor uses more generic Object Identifier (OID) values compared to the [SNMP Linux Meminfo Sensor](#)¹¹¹⁵.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)¹⁹²⁹ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor memory usage, PRTG will create one sensor for each memory type you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Memory Settings	
Memory	Select one or more memory types you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Memory Settings

Memory	Shows the type of the memory that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.126 SNMP NetApp Disk Free Sensor

The SNMP NetApp Disk Free sensor monitors free space on disks of a NetApp storage system via Simple Network Management Protocol (SNMP). It can show deduplication saved space and shared space, in total and in percent; disk free (total and percent), as well as percentage values for files free and inodes free.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁹ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor disk space on a NetApp, PRTG will create one sensor for each disk. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

NetApp Disk Free Settings	
File System	Select the disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

NetApp Disk Free Settings	
File System	Shows the name of the disk that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Virtual Disk	Shows the name of the virtual disk that this sensor is monitoring (if applicable). Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[168] settings).

Sensor Display	
	▪ Show in and out traffic as positive and negative area chart: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.127 SNMP NetApp Enclosure Sensor

The SNMP NetApp Enclosure sensor monitors the power supply and cooling of an enclosure that is part of a NetApp storage system via SNMP. It can measure temperatures, fans, voltages, and currents.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²³ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor power supply and cooling of an enclosure on a NetApp, PRTG will create one sensor for each enclosure/measurement combination. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

NetApp Enclosure Settings

Enclosure	Select the enclosures with the desired measurement you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

NetApp Enclosure Settings

Enclosure	Shows the identifier of the enclosure that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Measurement	Shows the monitored measurement. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[1683] settings).

Sensor Display	
	▪ Show in and out traffic as positive and negative area chart: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.128 SNMP NetApp I/O Sensor

The SNMP NetApp I/O sensor monitors input/output operations (IOPS) on a NetApp storage system via Simple Network Management Protocol (SNMP). It can show FCP Read, CIFS Ops, Disk Read, Disk Write, FCP Ops, FCP Write, HTTP Ops, iSCSI Ops, iSCSI Read, iSCSI Write, Network Received, Network Sent, NFS Ops, Tape Read, and Tape Write.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁹ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ⁸⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings). ▪ Show in and out traffic as positive and negative area chart: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.129 SNMP NetApp License Sensor

The SNMP NetApp License sensor monitors the licenses for the services of a NetApp storage system via Simple Network Management Protocol (SNMP). It indicates how much time is left until the license for a service expires. This can help you to detect when a timely limited NetApp license is going to expire.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁹ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor licenses on a NetApp, PRTG will create one sensor for each license. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

NetApp License Settings	
License for Service	Select the licenses you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

NetApp License Settings

License for Service	Shows the name of the license that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.130 SNMP NetApp Logical Unit Sensor

The SNMP NetApp Logical Unit sensor monitors the input/output operations (IOPS) on a logical unit of a NetApp storage system via Simple Network Management Protocol (SNMP). It can show the total number of operations, the amount of read and written data, the number of errors, the number of read, write, and other operations, as well as the overall status of the logical unit.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁹ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor logical units on a NetApp, PRTG will create one sensor for each unit. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

NetApp Disk Free Settings

Logical Unit	Select the logical units you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

NetApp Disk Free Settings

Logical Unit	Shows the name of the logical unit that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.131 SNMP NetApp Network Interface Sensor

The SNMP NetApp Network Interface sensor monitors a network card of a NetApp storage system via Simple Network Management Protocol (SNMP). It can show traffic in and out, as well as the number of errors per second (in and out).

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²³ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor network interfaces on a NetApp, PRTG will create one sensor for each interface. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

NetApp Network Interface Settings

Network Interface

Select the interfaces you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name

Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

NetApp Network Interface Settings

Network Interface	Shows the name of the interface that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings). ▪ Show in and out traffic as positive and negative area chart: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).

Sensor Display

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.132 SNMP NetApp System Health Sensor

The SNMP NetApp Disk Free sensor monitors free space on disks of a NetApp storage system via Simple Network Management Protocol (SNMP). It can show the CPU load in percent, active restore, current CIFS users; the number of disks active, being added, being scrubbed, failed, failing soon, being out of date, reconstructing (parity), spare, verifying parity, and total; the number of fans and power supplies failed; as well as the max used disk space and max used inodes, in percent.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²³ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ⁸⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings). ▪ Show in and out traffic as positive and negative area chart: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.133 SNMP Poseidon Environment Sensor

The SNMP Poseidon Environment sensor monitors performance counters for environmental measurements on Poseidon hardware via Simple Network Management Protocol (SNMP). It can show, for example, humidity and temperature in the environment, depending on available measurement components on the hardware device.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁰ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor performance counters for environmental measurements on Poseidon hardware, PRTG will create one sensor for each measuring point you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Poseidon Environment Specific	
Measuring Point	Select the measurements you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Poseidon Environment Specific

Name	Shows further information about the measurement. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Unit	
Measuring Point	

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).

Sensor Display

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1680] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.134 SNMP QNAP Logical Disk Sensor

The SNMP QNAP Logical Disk sensor monitors a logical disk in a QNAP Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP). It can show free space and free bytes, as well as the status of a volume.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)^[2001].

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)^[1923] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the logical disks in a QNAP NAS, PRTG will create one sensor for each disk you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

QNAP NAS Settings	
Disk	Select the logical disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
QNAP NAS Settings	
Disk	Shows further information about the disk. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	
File System	
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁹ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.135 SNMP QNAP Physical Disk Sensor

The SNMP QNAP Physical Disk sensor monitors a physical disk in a QNAP Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP). It can show the temperature, the HD status, and the Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) status of the disk.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)¹⁹²³.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)¹⁹²³ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the physical disks in a QNAP NAS, PRTG will create one sensor for each disk you choose. You can also define the unit of the temperature measurement. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

QNAP NAS Settings	
Disk	Select the physical disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.
Unit	Select the unit of the temperature measurement. Choose between Celsius and Fahrenheit .

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

QNAP NAS Settings	
Disk	Shows further information about the disk. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	
Model	
Capacity	
Unit	

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹³. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.136 SNMP QNAP System Health Sensor

The SNMP QNAP System Health sensor monitors the system health of a QNAP Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP). It can show the usage of the CPU, available memory in absolute numbers and percent, the temperature of CPU and system, as well as various other values, for example, revolutions of fans per minute, depending on the available measurement components.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁹ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the system health of a QNAP NAS, please specify the unit of the temperature measurement.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

QNAP NAS Settings	
Unit	Select the unit of the temperature measurement. Choose between Celsius and Fahrenheit .

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ⁸⁹ from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

QNAP NAS Settings

Unit	Shows the unit of temperatures as monitored with this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 1683 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window	
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1688] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.137 SNMP RMON Sensor

The SNMP RMON sensor monitors traffic on a device using the Remote Monitoring (RMON) standard via Simple Network Management Protocol (SNMP). It can be created on an SNMP compatible device which provides traffic data via RMON. Depending on the data returned by your device, traffic data for each port can be displayed in different channels, allowing detailed analysis.

For example, available channels for each traffic port may include Transmitted kbit/s, Packets (#/s), Broadcast Packets (#/s), Multicast Packets (#/s), CRC Errors (#/s), Undersize Packets (#/s), Oversize Packets (#/s), Fragments (#/s), Jabbers (#/s), Collisions (#/s), Packets <= 64 Byte (#/s), Packets 65 - 127 Bytes (#/s), Packets 128 - 255 Bytes (#/s), Packets 256 - 511 Bytes (#/s), Packets 512 - 1023 Bytes (#/s), Packets 1024 - 1518 Bytes (#/s), and Drop Events (#/s).

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²³ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

For SNMP devices with multiple interfaces multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

RMON Specific

Ports

Select the ports you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

In the **In Use** column you will see a **Yes** if there was already traffic detected on this interface in the past, and a **No** if there wasn't any traffic yet on this interface (since last device restart, usually). The **In Use** column does **not** show whether or not an interface is currently connected!

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ¹⁶⁸³ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
RMON Specific	
Port	Shows the number of the interface port in your physical device that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).

Sensor Display	
	▪ Show in and out traffic as positive and negative area chart: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.138 SNMP SonicWALL System Health Sensor

The SNMP SonicWALL System Health sensor monitors health values of a Dell SonicWALL Network Security Appliance (NSA) via Simple Network Management Protocol (SNMP). It shows usage of CPU and memory, as well as usage of the connection cache.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ^[192] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol

Sensor Display	
	of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.139 SNMP SonicWALL VPN Traffic Sensor

The SNMP SonicWALL VPN Traffic sensor monitors the traffic of an Internet Protocol Security (IPsec) Virtual Private Network (VPN) on a Dell SonicWALL Network Security Appliance (NSA) via Simple Network Management Protocol (SNMP). It can show the number of encrypted and decrypted packets, the number of bytes of encrypted and decrypted transmissions, as well as the number of in- and outgoing fragmented packets.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁹ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the traffic of a SonicWALL VPN, PRTG will create one sensor for each connection you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

SonicWALL VPN Specific	
Connections	Select the connections you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.
Identification Method	Select the criteria PRTG will use to identify the connection. PRTG will always use the first connection found that matches all criteria. Choose between: ▪ By Index: Every connection has a unique index. This is the safest method to identify your connection. Though, if the connection is lost and reconnected, a new index will be assigned. ▪ By Remote IP: If the target of the VPN has always the same IP, you can use this IP to identify the connection. ▪ By Security Policy Name: If you use a different Security Policy for every VPN, you can use its name to identify the connection. ▪ By Remote IP and Security Policy Name: You can also combine both identification methods.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SonicWALL VPN Specific

Security Policy	Shows further information about the monitored connection. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Remote IP	
Index	
Identification Method	

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.
Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹². Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.140 SNMP Synology Logical Disk Sensor

The SNMP Synology Logical Disk sensor monitors a logical disk in a Synology Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP). It can show the status of a volume.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)^[2001].

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)^[1923] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the logical disks in a Synology NAS, PRTG will create one sensor for each disk you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Synology NAS Settings

Disk	Select the logical disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Synology NAS Settings

Disk	Shows further information about the disk. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[168] settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#) section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#) section.

Others

For more general information about settings, please see [Object Settings](#) section.

6.8.141 SNMP Synology Physical Disk Sensor

The SNMP Physical Disk sensor monitors a physical disk in a Synology Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP). It can show temperature and disk status.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)^[2001].

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)^[1923] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the physical disks in a Synology NAS, PRTG will create one sensor for each disk you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Synology NAS Settings

Disk	Select the physical disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ¹⁶⁸³ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Synology NAS Settings

Disk	Shows further information about the disk. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	
Model	
Type	

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁹ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.142 SNMP Synology System Health Sensor

The SNMP Synology System Health sensor monitors the system health of a Synology Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP). It can show temperature, system status, power status, fan status, as well as several other values, depending on the available measurement components.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)²⁰⁰¹.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)¹⁹²³ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰¹. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the system health of a Synology NAS, please specify the unit of the temperature measurement.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Synology NAS Settings

Unit	Select the unit of the temperature measurement. Choose between Celsius and Fahrenheit .

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings

Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Synology NAS Settings

Unit	Shows the unit of temperatures as monitored with this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[168] settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1688] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.143 SNMP System Uptime Sensor

The SNMP System Uptime sensor monitors the time a device is running via Simple Network Management Protocol (SNMP). It reads the device's value for system uptime and shows it.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²³ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ⁸⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.

Sensor Display	
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹². Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[1441] section.

6.8.144 SNMP Traffic Sensor

The SNMP Traffic sensor monitors traffic on a device using Simple Network Management Protocol (SNMP). It can be created on a device which provides traffic data. For each individual port one traffic sensor is created. It can show traffic in, traffic out, and traffic total. Additional channels can be added.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)  section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) . It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

For SNMP devices with multiple interfaces multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Traffic Specific	
Interface Number	Select the interfaces you want to add a sensor for. A list of SNMP device interfaces is shown; containing all interfaces which your device provides. Connected interfaces are printed in bold face; not connected in non-bold face. One sensor will be created for each interface. You can group-select and -unselect interfaces by using the buttons Select all connected interfaces , Select all disconnected interfaces , and Deselect all interfaces . You can also select and deselect all items by using the check box in the table head.
Description IN	For the standard channel "Traffic In" enter the description here. It will be shown in graphs and tables. You can change this description and the description of all other channels in the sensor's channel settings  later.
Description OUT	For the standard channel "Traffic Out" enter the description here. It will be shown in graphs and tables. You can change this description and the description of all other channels in the sensor's channel settings  later.
Description SUM	For the standard channel traffic "Sum" enter the description here. It will be shown in graphs and tables. You can change this description and the description of all other channels in the sensor's channel settings  later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Traffic Specific	
Interface Number	Shows the number and name of the interface in your physical device that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Additional Channels	By default, the channels "Traffic In" and "Traffic out" are created for each sensor. Choose additional channels for all selected interfaces. Please click on the respective channel name(s); a check mark symbol will appear in front of them. You can choose from the following additional channels: • Errors In & Out • Discards In & Out • Unicast Packets In & Out • Non Unicast Packets In & Out (32-bit only) • Multicast Packets In & Out (64-bit only) • Broadcast Packets In & Out (64-bit only) • Unknown Protocols Channels that are once created cannot be deleted later. They can be disabled only.
Connection State Handling	Choose how PRTG will react when an interface is disconnected. A disconnected interface is, for example, an ethernet port on a switch with no cable plugged in. This setting is valid for all interfaces selected above. You can choose between: • Show alarm when disconnected (recommended): The sensor for the interface will turn into a red error state. • Ignore interface when disconnected: No alarm will be shown in PRTG; monitoring will be discontinued without notice.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor.

Sensor Display	
	▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 1683 settings). ▪ Show in and out traffic as positive and negative area chart: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 1683 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) 224 group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration 1805 .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1793. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights

User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: How do PRTG's automatic port name and number updates work for SNMP traffic sensors?

- <http://www.paessler.com/knowledgebase/en/topic/25893>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.145 SNMP Trap Receiver Sensor

The SNMP Trap Receiver sensor receives and analyzes Simple Network Management Protocol (SNMP) traps. It shows the overall number of received traps per second, warning and error traps per second, as well as the number of dropped packets per second.

With the available filter options, you can define individually which types of messages will be considered for monitoring, and which messages will be recognized as warning or error messages. Depending on the filters, received messages will be counted in the respective channels.

You can add the sensor to the probe device on the one hand; then the sensor will receive all messages of the system running the probe. Alternatively, you can add the sensor to a specific device to gain all messages from this device directly; this will make this sensor type faster than just using source filters.

Note: You can copy the Management Information Base (MIB) file for your traps into the **\MIB subfolder of your PRTG installation** ²⁰³⁶. PRTG will then be able to translate the OIDs for the traps into readable messages. For example, instead of the Object Identifier (OID) **1.3.6.1.4.1.32446.1.1.2** you would see **SNMPv2-SMI-v1::enterprises.32446.1.1.2 = 0** (example from the PRTG MIB).

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#) ¹⁹²⁵ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#) ²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ¹²⁴⁷ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
SNMP Trap Specific	
Listen on Port	Enter the port the sensor will listen on for SNMP traps. Usually port 162 is used. Please enter an integer value. We recommend using the default value.
Purge Messages After	Define how long received trap messages will be stored for analysis. Choose a period of time from the drop down list.
Filter	
Include Filter	Define if you want to filter traps. If you leave this field empty or use the keyword " any ", all data will be processed. To include specific types of traps only, define filters using a special syntax. For more information, see section Filter Rules ¹²⁴⁷ .
Exclude Filter	Define which types of traps will be discarded and not processed. To exclude specific types of traps, define filters using a special syntax. For more information, see section Filter Rules ¹²⁴⁷ .
Warning Filter	Define which types of traps will count for the Warnings channel. To categorize received traps as warning messages, define filters using a special syntax. For more information, see section Filter Rules¹²⁴⁷. Note: Messages are collected until a scanning interval ends; as long as the scanning interval is running, no status change will happen. By default, the sensor will turn into a Warning status after a scanning interval has finished and there was at least one warning message (and no error message) during this interval. The status will remain Warning at least until the succeeding scanning interval has finished. If in this scanning interval no warning or error message occurred, the status of the sensor will turn Up again after the interval.

Filter	
Error Filter	Define which types of traps will count for the Errors channel. To categorize received traps as error messages, define filters using a special syntax. For more information, see section Filter Rules ¹²⁴⁷. Note: Messages are collected until a scanning interval ends; as long as the scanning interval is running, no status change will happen. By default, the sensor will turn into a Down status after a scanning interval has finished and there was at least one error message during this interval. The status will remain Down at least until the succeeding scanning interval has finished. If in this scanning interval no warning or error message occurred, the status of the sensor will turn Up again after the interval.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Debugging**Log Data to Disk**

Define if the probe will write a log file of the received data to the data folder (see [Data Storage](#)²⁰³⁶) to the disk for debugging purposes. Choose between:

- **Off (recommended):** Do not write additional log files. Recommended for normal use cases.
- **On:** Write log files for all data received.

Note: Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Filter Rules for Traps

Filter rules are used for the include, exclude, warning, and error definition fields of the Trap Receiver sensor. They are based on the following format:

```
field[filter]
```

You can use various filters suitable to your needs. Include and exclude filters define which traps will be monitored; warning and error filters define how received traps will be categorized. Provide these filters in the sensor settings as formulas. Formulas are fields which can be combined with boolean operators (**AND**, **OR**, **NOT**) and brackets.

Field	Parameter	Examples
source [ip]	Enter an IP address where the UDPs come from; IP masks and ranges ²⁰⁰⁰ are also possible.	source[10.0.23.50], source[10.0.23.10-50], source[10.0.23.10/255]
agent [ip]	Enter an IP address which specifies the object that creates the SNMP trap. Only v1 is supported.	agent[10.0.0.1]
enterprise [oid]	Enter an OID which specifies the object that originates the trap. Only v1 is supported.	enterprise [1.3.6.1.4.1.2.6.182.1.2.3 1.1.0]
bindings [text]	Enter a substring to match all OIDs and values in the bindings.	bindings[ERROR], bindings [1.3.6.1.4.1.2.6.182.1.2.3 1.1.0]
bindings [oid,value]	Enter an OID and a substring to match a value in the given OID. Separate OID and value with a comma.	bindings [1.3.6.1.4.1.2.6.182.1.2.3 1.1.0,error]
gentrap [number]	Enter a number which specifies the generic trap type. Ranges are also possible.	gentrap[3], gentrap[2-6]

spectrap [number]	Enter a number which defines the specific trap code. Ranges are also possible.	spectrap[4], spectrap[0-3]
version [number]	Enter a number (1 or 2) which specifies the SNMP version.	version[1], version[2]
community [text]	Enter a community string for exact, case sensitive match.	community[public], community[private]

Review and Analyze Traps

Received traps are stored as common files in PRTG's data folder (see section [Data Storage](#)^[2036]). In order to review and analyze all received messages, you can access the data directly in PRTG's web interface via the respective sensors on the **Overview** tab in a [table list](#)^[155].

For more details and further filter options, click on the **Messages** tab of the SNMP Trap Receiver sensor. You will see all received messages in a [table list](#)^[155]. On the top, you have display filter options to drill down into the data for specific events of your interest. The filters are the same as available in the sensor settings, but you can define them without using formulas. Provide the desired parameters and PRTG will load the filtered list automatically.

Advanced Filter Settings

You can open advanced filter settings with a click on the gear icon in the **Filter** row. The **Advanced Filter** will appear in a popup window. In the text field, you can define a filter using the syntax as given in section [Filter Rules for Traps](#)^[1247]. If you have provided filter parameters on the **Messages** tab, these will be already included in the advanced filter as a corresponding formula with the correct syntax. You can adjust this filter to your needs. You can also copy the automatically created and manually adjusted formula for usage in the filter fields of the sensor settings.

More

Blog Article: Introducing the New High Performance Syslog and SNMP Trap Receiver Sensors

- <http://www.paessler.com/blog/2013/10/11/prtg/introducing-the-new-high-performance-syslog-and-snmp-trap-receiver-sensors>

Knowledge Base: How do I test an SNMP Trap Receiver Sensor?

- <http://www.paessler.com/knowledgebase/en/topic/10193>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1083] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[1441] section.

6.8.146 SNMP Windows Service Sensor

The SNMP Windows Service sensor monitors a Windows service via Simple Network Management Protocol (SNMP). It shows the operating status of the monitored service. Operating states can be **Active** (sensor status **Up**), or **Continue-Pending**, **Pause-Pending**, and **Paused** (all with sensor status **Down**).

Note: This sensor type cannot distinguish the status "not installed" from "not running".

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)²⁰⁰¹.

For a general introduction to the technology behind SNMP, please see [Monitoring via SNMP](#)¹⁹²³ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁶. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor services on Windows, PRTG will create one sensor for each service you select. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

SNMP Windows Service Monitor

Service	Select the services you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be

Basic Sensor Settings	
	shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SNMP Windows Service Monitor	
Service	Shows the service monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[168] settings).

Sensor Display

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁸ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.147 SNTP Sensor

The SNTP Sensor monitors a Simple Network Time Protocol (SNTP) server. It returns the response time and the time difference in comparison to the local system time.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Timeout (Sec.)	Enter a timeout in seconds. If the reply takes longer than this value the request is aborted and an error message is triggered. The maximum timeout value is 900 seconds (equals 15 minutes).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1791. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.148 SSH Disk Free Sensor

The SSH Disk Free sensor monitors free space on disks of a Linux/Unix system using Secure Shell (SSH). It shows the total free disk space (sum), and the free disk space in percent for every mounted partition (volume).

Note: The free space returned by this sensor type shows the available disk space of the volume, minus a reserve defined for this volume (e.g. for redundancy purposes). So, this sensor shows the disk space that is actually **available** for use. The size of the reserved disk space can be defined with `tune2fs`. For details, please see the article linked in the [More](#)^[1267] section below.

For this sensor type credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems must be defined for the device you want to use the sensor on.

Note: Not all Linux/Unix and Mac OS distributions can be supported by this sensor type.

For a general introduction to SSH monitoring, please see [Monitoring via SSH](#)^[1930] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings	
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
SSH Specific	
Connection Timeout (Sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (Sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. <code>cat /proc/loadavg</code>).
SSH Port	Define which port this sensor will use for the SSH connection. Choose between: ▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems section of the device this sensor is created on. ▪ Enter custom port number: Do not use the port number from the parent device's settings, but define a different port number below.
Use Port Number	This field is only visible if the custom port number setting is enabled above. Enter the port number this sensor will use for the SSH connection. Please enter an integer value.
Result Handling	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: <code>Result of Sensor [ID].txt</code>. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage  section.

Set limits checked against ALL disks

In this section you can set limits that are valid for all channels and all drives. By entering limits, you can define when the sensor will enter a **Warning** or **Down** status; depending on the data provided by all drives that this sensor monitors. If you want to define limits for separate channels individually please use the limit settings in the sensor's **Channels** settings. **Note:** All limits defined here are valid additionally to the limits defined in the particular **Channels** settings!

Percentage Limit Check	Enable or disable a limit check for the free space in percentage channels of all drives. By default percentage limits are enabled with lower warning and lower error limit. Choose between: • Disable Percentage Limits: Do not use the drives' data to control the sensor's status. • Enable Percentage Limits: Define limits. Additional fields appear below. The sensor will enter a warning or down state when free space limits are undercut or overrun.
Upper Error Limit	This field is only visible if percentage limit check is enabled above. Specify an upper limit in percent for a Down status. If the free disk space of one of your drives overruns this percent value, the sensor will be set to Down. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings¹⁶⁸³. The limits set here and in the channel settings are valid simultaneously!
Upper Warning Limit	This field is only visible if percentage limit check is enabled above. Specify an upper limit in percent for a Warning status. If the free disk space of one of your drives overruns this percent value, the sensor will be set to Warning. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings¹⁶⁸³. The limits set here and in the channel settings are valid simultaneously!
Lower Warning Limit	This field is only visible if percentage limit check is enabled above. Specify a lower limit in percent for a warning state. If the free disk space of one of your drives undercuts this percent value, the sensor will be set to warning. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings¹⁶⁸³. The limits set here and in the channel settings are valid simultaneously!

Set limits checked against ALL disks	
Lower Error Limit	This field is only visible if percentage limit check is enabled above. Specify a lower limit in percent for entering a Down status. If the free disk space of one of your drives undercuts this percent value, the sensor will be set to Down. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings¹⁶⁸³. The limits set here and in the channel settings are valid simultaneously!
Byte Limit Check	Enable or disable a limit check for the free bytes channels of all drives. Choose between: • Disable Byte Limits: Do not use the drives' data to control the sensor's status. • Enable Byte Limits: Define limits. Additional fields appear below. The sensor will enter a warning or down state when free space limits are undercut or overrun.
Upper Error Limit	This field is only visible if byte limit check is enabled above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor will be set to Down. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings¹⁶⁸³. The limits set here and in the channel settings are valid simultaneously!
Upper Warning Limit	This field is only visible if byte limit check is enabled above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor will be set to Warning. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings¹⁶⁸³. The limits set here and in the channel settings are valid simultaneously!
Lower Warning Limit	This field is only visible if byte limit check is enabled above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor will be set to Warning. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings¹⁶⁸³. The limits set here and in the channel settings are valid simultaneously!

Set limits checked against ALL disks

Lower Error Limit	This field is only visible if byte limit check is enabled above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor will be set to Down . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Alarm on Missing/ Removed Disk	If a monitored disk is removed or not found, values are set to zero. Select the alarming approach in this case. Choose between: ▪ Deactivate alarm (default): Select this option if you do not want an alarm for a removed disk. ▪ Activate Alarm: Select this option if you want to be alerted if a monitored disk is removed.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window	
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: How and Where Does PRTG Store its Data?

- <http://www.paessler.com/knowledgebase/en/topic/463>

Knowledge Base: Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?

- <http://www.paessler.com/knowledgebase/en/topic/43183>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[1441] section.

6.8.149 SSH INodes Free Sensor

The SSH INodes Free sensor monitors the free index nodes on disks of Linux/Unix and Mac OS systems via Secure Shell (SSH). It shows the free index nodes in percent, for each mount in an own sensor channel.

UNIX file systems only allow a limited number of index nodes. If the limit is exceeded, no more data can be stored, although there might be still free space available. This sensor can help you to notice early on if one of your drives is running out of INodes.

For this sensor type credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems must be defined for the device you want to use the sensor on.

Note: Not all Linux/Unix and Mac OS distributions can be supported by this sensor type.

For a general introduction to SSH monitoring, please see [Monitoring via SSH](#)^[1930] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SSH Specific	
Connection Timeout (Sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (Sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. <code>cat /proc/loadavg</code>).
SSH Port	Define which port this sensor will use for the SSH connection. Choose between: ▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems section of the device this sensor is created on. ▪ Enter custom port number: Do not use the port number from the parent device's settings, but define a different port number below.
Use Port Number	This field is only visible if the custom port number setting is enabled above. Enter the port number this sensor will use for the SSH connection. Please enter an integer value.
Result Handling	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: <code>Result of Sensor [ID].txt</code>. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: How and Where Does PRTG Store its Data?

- <http://www.paessler.com/knowledgebase/en/topic/463>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.150 SSH Load Average Sensor

The SSH Load Average sensor monitors the load average of a Linux/Unix system using Secure Shell (SSH). It shows the average system load within a one, five, and 15 minutes interval (each in one channel).

For this sensor type credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems must be defined for the device you want to use the sensor on.

Note: Not all Linux/Unix and Mac OS distributions can be supported by this sensor type.

For a general introduction to SSH monitoring, please see [Monitoring via SSH](#)^[1930] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Part 6: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
150 SSH Load Average Sensor

SSH Specific	
Connection Timeout (Sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (Sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. <code>cat /proc/loadavg</code>).
SSH Port	Define which port this sensor will use for the SSH connection. Choose between: ▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems section of the device this sensor is created on. ▪ Enter custom port number: Do not use the port number from the parent device's settings, but define a different port number below.
Use Port Number	This field is only visible if the custom port number setting is enabled above. Enter the port number this sensor will use for the SSH connection. Please enter an integer value.
Result Handling	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: <code>Result of Sensor [ID].txt</code>. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage 2036 section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: How and Where Does PRTG Store its Data?

- <http://www.paessler.com/knowledgebase/en/topic/463>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.151 SSH Meminfo Sensor

The SSH Meminfo sensor monitors the memory usage of a Linux/Unix system using Secure Shell (SSH). It shows the available memory in total and in percent. **Note:** This sensor type is not compatible with Mac OS systems.

For this sensor type credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems must be defined for the device you want to use the sensor on.

Note: Not all Linux/Unix and Mac OS distributions can be supported by this sensor type.

For a general introduction to SSH monitoring, please see [Monitoring via SSH](#)^[1930] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SSH Specific	
Connection Timeout (Sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (Sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. <code>cat /proc/loadavg</code>).
SSH Port	Define which port this sensor will use for the SSH connection. Choose between: ▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems section of the device this sensor is created on. ▪ Enter custom port number: Do not use the port number from the parent device's settings, but define a different port number below.
Use Port Number	This field is only visible if the custom port number setting is enabled above. Enter the port number this sensor will use for the SSH connection. Please enter an integer value.
Result Handling	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: <code>Result of Sensor [ID].txt</code>. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: How and Where Does PRTG Store its Data?

- <http://www.paessler.com/knowledgebase/en/topic/463>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.152 SSH Remote Ping Sensor

The SSH Remote Ping sensor remotely monitors the connectivity between a system running Linux/OS X and an other device, using Internet Control Message Protocol (ICMP) echo requests ("Ping") and Secure Shell (SSH). It can show packet loss, as well as minimum, maximum, and average response times; all measured from the remote device you connect to.

For this sensor type credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems must be defined for the device you want to use the sensor on.

Note: Not all Linux/Unix and Mac OS distributions can be supported by this sensor type.

For a general introduction to SSH monitoring, please see [Monitoring via SSH](#)^[1930] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SSH Remote Ping Configuration	
Target	Enter the DNS name or IP address of the target device the Ping is sent to. The sensor will remotely connect to the parent device it is created on via SSH, then perform a Ping request from this remote device to the target device/server. Please enter a string.
Packet Size (Bytes)	Enter the packet size in bytes for the Ping. You can choose any value between 1 and 10000 . Please enter an integer value. We recommend using the default value.
Packet Count	Enter the number of packets that is sent with each scanning interval.
Custom Parameter	Optionally enter additional parameters that will be added at the end of the ping command. Please do not use parameters that change the output format of the result to make sure it can still be parsed. You cannot enter another command here. Please enter a string or leave the field empty.
SSH Specific	
Connection Timeout (Sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (Sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. cat /proc/loadavg).
SSH Port	Define which port this sensor will use for the SSH connection. Choose between: ▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems section of the device this sensor is created on. ▪ Enter custom port number: Do not use the port number from the parent device's settings, but define a different port number below.
Use Port Number	This field is only visible if the custom port number setting is enabled above. Enter the port number this sensor will use for the SSH connection. Please enter an integer value.
Result Handling	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result.

SSH Specific	
	▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage²⁰³⁶ section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

More

Knowledge Base: How and Where Does PRTG Store its Data?

- <http://www.paessler.com/knowledgebase/en/topic/463>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁸⁸⁰ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁸⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.153 SSH SAN Logical Disk Sensor

The SSH SAN Logical Disk sensor monitors a logical disk on a Storage Area Network (SAN) via Secure Shell (SSH). The SAN has to provide a command-line interface (CLI) for this purpose. The sensor can show the health status of the disk.

Note: This sensor type does not support every SAN, even if it provides a CLI. The sensor only works with specific devices, for example, with the HP P2000.

Note: Sometimes the devices which you monitor with this sensor return status values which are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information regarding this issue, please see section **More** below.

For this sensor type, corresponding credentials must be defined in section **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) System** in the [settings of the device](#)^[272] you want to use the sensor on.

For a general introduction to SSH monitoring, please see [Monitoring via SSH](#)^[1930] section.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)^[2001].

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor volumes on an SAN device, PRTG will create one sensor for each volume you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

SSH SAN Logical Disk Settings	
Volume	Select the volumes you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SSH Specific	
Connection Timeout (Sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (Sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. <code>cat /proc/loadavg</code>).
SSH Port	Define which port this sensor will use for the SSH connection. Choose between: ▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems section of the device this sensor is created on. ▪ Enter custom port number: Do not use the port number from the parent device's settings, but define a different port number below.
Use Port Number	This field is only visible if the custom port number setting is enabled above. Enter the port number this sensor will use for the SSH connection. Please enter an integer value.
Result Handling	Define what will be done with the result of the sensor. Choose between:

SSH Specific	
	▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage 2036 section.
SSH SAN Logical Disk Settings	
Volume	Shows the volume that this sensor monitors. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Size	Shows the size of the volume that this sensor monitors. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 1683 settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: Why does my SSH SAN sensor show a wrong status?

- <http://www.paessler.com/knowledgebase/en/topic/60145>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1693] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[1441] section.

6.8.154 SSH SAN Physical Disk Sensor

The SSH SAN Physical Disk sensor monitors a physical disk on a Storage Area Network (SAN) via Secure Shell (SSH). The SAN has to provide a command-line interface (CLI) for this purpose. The sensor can show the health status of the disk, the total number of I/O operations, as well as the amount of transferred data.

Note: This sensor type does not support every SAN, even if it provides a CLI. The sensor only works with specific devices, for example, with the HP P2000.

Note: Sometimes the devices which you monitor with this sensor return status values which are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information regarding this issue, please see section **More** below.

For this sensor type, corresponding credentials must be defined in section **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) System** in the [settings of the device](#)^[272] you want to use the sensor on.

For a general introduction to SSH monitoring, please see [Monitoring via SSH](#)^[1930] section.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)^[2001].

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor disks on an SAN device, PRTG will create one sensor for each disk you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

SSH SAN Physical Disk Settings

Disk

Select the disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SSH Specific	
Connection Timeout (Sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (Sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. <code>cat /proc/loadavg</code>).
SSH Port	Define which port this sensor will use for the SSH connection. Choose between: ▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems section of the device this sensor is created on. ▪ Enter custom port number: Do not use the port number from the parent device's settings, but define a different port number below.
Use Port Number	This field is only visible if the custom port number setting is enabled above. Enter the port number this sensor will use for the SSH connection. Please enter an integer value.
Result Handling	Define what will be done with the result of the sensor. Choose between:

SSH Specific	
	▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage 2036 section.
SSH SAN Physical Disk Settings	
Disk	Shows the disk that this sensor monitors. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Disk Name	Shows the label of disk that this sensor monitors. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Size	Shows the size of the disk that this sensor monitors. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 1683 settings).

Sensor Display

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: Why does my SSH SAN sensor show a wrong status?

- <http://www.paessler.com/knowledgebase/en/topic/60145>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[1441] section.

6.8.155 SSH SAN System Health Sensor

The SSH SAN System Health sensor monitors the system health of a Storage Area Network (SAN) via Secure Shell (SSH). The SAN has to provide a command-line interface (CLI) for this purpose. The sensor can show several metrics of the SAN, such as temperatures, voltages, the overall unit status, as well as capacitor charge. Which monitoring data this sensor type shows exactly, depends on the available measurement components on the SAN.

Note: This sensor type does not support every SAN, even if it provides a CLI. The sensor only works with specific devices, for example, with the HP P2000.

Note: Sometimes the devices which you monitor with this sensor return status values which are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information regarding this issue, please see section **More** below.

For this sensor type, corresponding credentials must be defined in section **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) System** in the [settings of the device](#)^[272] you want to use the sensor on.

For a general introduction to SSH monitoring, please see [Monitoring via SSH](#)^[1930] section.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)^[2001].

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[226]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the system health of an SAN device, PRTG will create one sensor for each metric you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

SSH SAN Specific

Metric	
	Select the metrics you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SSH SAN Specific	
Metric	Shows the metric this sensor monitors. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SSH Specific	
Connection Timeout (Sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (Sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. <code>cat /proc/loadavg</code>).
SSH Port	Define which port this sensor will use for the SSH connection. Choose between:

SSH Specific	
	▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems section of the device this sensor is created on. ▪ Enter custom port number: Do not use the port number from the parent device's settings, but define a different port number below.
Use Port Number	This field is only visible if the custom port number setting is enabled above. Enter the port number this sensor will use for the SSH connection. Please enter an integer value.
Result Handling	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: Why does my SSH SAN sensor show a wrong status?

- <http://www.paessler.com/knowledgebase/en/topic/60145>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1693] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[1441] section.

6.8.156 SSH Script Sensor

The SSH Script sensor connects to a Linux/Unix system via Secure Shell (SSH) and executes a script file located on the target system. The sensor shows the execution time, and can show one value returned by the executable file or script (in one channel only). For details about the return value format please see the [Application Programming Interface \(API\) Definition](#)¹⁹⁹³.

Note: For security reasons, the script file must be stored on the target system. Please make sure the script has executable rights.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

For this sensor type credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems must be defined for the device you want to use the sensor on.

Note: Not all Linux/Unix and Mac OS distributions can be supported by this sensor type.

For a general introduction to SSH monitoring, please see [Monitoring via SSH](#)¹⁹³⁰ section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Script	Select a script file from the list. The drop down menu will list all script files available in the <code>/var/prtg/scripts</code> directory on the target Linux/Unix system. In order for the files to appear in this list, please store them into this directory. Please make sure the script has executable rights. In order for the sensor to show the expected values and sensor status, your files must use the right format for the returned values (in this case, <code>exitcode:value:message</code> to stdout). The exitcode will determine the sensor status. For detailed information on the expected return format and on how to build custom sensors, please see the API documentation (Application Programming Interface (API) Definition ¹⁹⁹³). There, find detailed information the the "Custom Sensors" tab. For an example script, please see More ¹³²² section below.
Value Type	Define what kind of values your script file gives back. Choose between: ▪ Integer: An integer is expected as return value. If the script gives back a float, PRTG will display the value 0. ▪ Float: A float is expected as return value, with a dot (.) between pre-decimal position and decimal places. In this setting, the sensor will also display integer values unless they don't produce a buffer overflow. ▪ Counter: Your script returns an integer which increases. PRTG will show the difference between the values of two sensor scans. Note: A counter must return an integer; float is not supported here!

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Script	Shows the script that is executed with each sensor scan, as defined on sensor creation. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Parameters	If your script file catches command line parameters, you can define them here. Placeholders can be used as well. For a full list of all placeholders please see the API documentation (Application Programming Interface (API) Definition ^[1993]). Note: Please make sure you write the placeholders in quotes to ensure that they are working properly if their values contain blanks. Use single quotation marks ' ' with PowerShell scripts, and double quotes " " with all others. Please enter a string or leave the field empty.
Mutex Name	Define any desired mutex name for the process. All EXE/Script sensors having the same mutex name will be executed serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running simultaneously. For links to more information, please see the More ^[437] section below. Please enter a string or leave the field empty.
Value Type	Shows the expected value type, chosen on sensor creation. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Note: The sensor cannot handle string values.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • Ignore changes (default): No action will be taken on change.

Sensor Settings	
	• Trigger 'On Change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.
SSH Specific	
Connection Timeout (Sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (Sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. <code>cat /proc/loadavg</code>).
SSH Port	Define which port this sensor will use for the SSH connection. Choose between: ▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems section of the device this sensor is created on. ▪ Enter custom port number: Do not use the port number from the parent device's settings, but define a different port number below.
Use Port Number	This field is only visible if the custom port number setting is enabled above. Enter the port number this sensor will use for the SSH connection. Please enter an integer value.
Result Handling	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: <code>Result of Sensor [ID].txt</code>. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: Is there a shell script example for PRTG's SSH Script Sensor?

- <http://www.paessler.com/knowledgebase/en/topic/39513>

Information about custom scripts and executables

- [Application Programming Interface \(API\) Definition](#) ¹⁹⁹³
- [Additional Sensor Types \(Custom Sensors\)](#) ¹⁶⁸⁰

Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?

- <http://www.paessler.com/knowledgebase/en/topic/6673>

Knowledge Base: How and Where Does PRTG Store its Data?

- <http://www.paessler.com/knowledgebase/en/topic/463>

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- <http://www.paessler.com/knowledgebase/en/topic/11283>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#) ¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.157 SSH Script Advanced Sensor

The SSH Script Advanced sensor connects to a Linux/Unix system via Secure Shell (SSH) and executes a script file located on the target system. The sensor shows the execution time, and can show values returned by the script in multiple channels. The return value of this sensor must be valid XML. For details about the return value format please see the [Application Programming Interface \(API\) Definition](#)^[1993].

Note: For security reasons, the script file must be stored on the target system. Please make sure the script has executable rights.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

For this sensor type credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems must be defined for the device you want to use the sensor on.

Note: Not all Linux/Unix and Mac OS distributions can be supported by this sensor type.

For a general introduction to SSH monitoring, please see [Monitoring via SSH](#)^[1930] section.

Limited to 50 Sensor Channels

PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Script	Select a script file from the list. The drop down menu will list all script files available in the <code>/var/prtg/scripts.xml</code> directory on the target Linux/Unix system. In order for the files to appear in this list, please store them into this directory. Please make sure the script has executable rights. In order for the sensor to show the expected values and sensor status, your files must return the expected XML format to standard output. Values and message must be embedded in the XML. For detailed information on the expected return format and on how to build custom sensors, please see the API documentation (Application Programming Interface (API) Definition ¹⁹⁹³). There, find detailed information the the "Custom Sensors" tab.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ⁸⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Script	Shows the script that is executed with each sensor scan, as defined on sensor creation. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Settings	
Parameters	If your script file catches command line parameters, you can define them here. Placeholders can be used as well. For a full list of all placeholders please see the API documentation (Application Programming Interface (API) Definition¹⁹⁹³). Note: Please make sure you write the placeholders in quotes to ensure that they are working properly if their values contain blanks. Use single quotation marks ' ' with PowerShell scripts, and double quotes " " with all others. Please enter a string or leave the field empty.
Mutex Name	Define any desired mutex name for the process. All EXE/Script sensors having the same mutex name will be executed serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running simultaneously. For links to more information, please see the More⁴³⁷ section below. Please enter a string or leave the field empty.
EXE Result	Define what will be done with the results the executable file gives back. Choose between: • Discard EXE result: Do not store the requested web page. • Write EXE result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the script to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage²⁰³⁶ section.
SSH Specific	
Connection Timeout (Sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (Sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. <code>cat /proc/loadavg</code>).
SSH Port	Define which port this sensor will use for the SSH connection. Choose between: ▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems section of the device this sensor is created on. ▪ Enter custom port number: Do not use the port number from the parent device's settings, but define a different port number below.

SSH Specific	
Use Port Number	This field is only visible if the custom port number setting is enabled above. Enter the port number this sensor will use for the SSH connection. Please enter an integer value.
Result Handling	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Information about custom scripts and executables

- [Application Programming Interface \(API\) Definition](#) 
- [Additional Sensor Types \(Custom Sensors\)](#) 

Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?

- <http://www.paessler.com/knowledgebase/en/topic/6673>

Knowledge Base: How and Where Does PRTG Store its Data?

- <http://www.paessler.com/knowledgebase/en/topic/463>

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- <http://www.paessler.com/knowledgebase/en/topic/11283>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)  section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)  section.

Others

For more general information about settings, please see [Object Settings](#)  section.

6.8.158 SSH VMWare ESX(i) Disk Sensor

The SSH VMWare ESX(i) Disk sensor monitors free space on disks of a VMware ESX(i) system using Secure Shell (SSH). It shows the free disk space for different mounts and total, in total and percent values.

For this sensor type credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems must be defined for the device you want to use the sensor on.

Note: Not all Linux/Unix and Mac OS distributions can be supported by this sensor type.

For a general introduction to SSH monitoring, please see [Monitoring via SSH](#)^[1930] section.

Requirement: Root Credentials

In the parent device's **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems** settings, please use the **root** user of your VMware host for authentication! See [More](#)^[1337] section below.

Please make sure you enable SSH on your VMware system!

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings	
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
SSH Specific	
Connection Timeout (Sec.)	Define a timeout for the connection. This is the the time the sensor waits to establish a connection to the host. You should keep this value as low as possible.
Shell Timeout (Sec.)	Define a timeout for the shell response. This is the time in seconds the sensor waits for the shell to return a response after it has sent its specific command (e.g. <code>cat /proc/loadavg</code>).
SSH Port	Define which port this sensor will use for the SSH connection. Choose between: ▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems section of the device this sensor is created on. ▪ Enter custom port number: Do not use the port number from the parent device's settings, but define a different port number below.
Use Port Number	This field is only visible if the custom port number setting is enabled above. Enter the port number this sensor will use for the SSH connection. Please enter an integer value.
Result Handling	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: <code>Result of Sensor [ID].txt</code>. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration**Channel Unit Types**

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: How and Where Does PRTG Store its Data?

- <http://www.paessler.com/knowledgebase/en/topic/463>

Knowledge Base: Settings on ESXi 5 host when monitoring via SSH VMware ESX(i) Disk Sensor

- <http://www.paessler.com/knowledgebase/en/topic/32603>

Knowledge Base: Why do I need root credentials when monitoring VMware hosts via SSH?

- <http://www.paessler.com/knowledgebase/en/topic/33763>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.159 Syslog Receiver Sensor

The Syslog Receiver sensor receives and analyzes syslog messages. It shows the overall number of received syslog messages per second, warning and error messages per second, as well as the number of dropped packets per second.

With the available filter options, you can define individually which types of messages will be considered for monitoring and thus stored, and which messages will be recognized as warning or error messages. Depending on the filters, received messages will be counted in the respective channels. The messages are stored in an internal database for later analysis. The received data will be available on your respective probe system as common files, as well as via the web interface.

You can add the sensor to the probe device on the one hand; then the sensor will receive all messages of the system running the probe. Alternatively, you can add the sensor to a specific device to gain all messages from this device directly; this will make this sensor type faster than just using source filters.

Note: This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings	
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Syslog Specific	
Listen on Port	Enter the port the sensor will listen on for Syslog messages. Usually port 514 is used. Please enter an integer value. We recommend using the default value.
Purge Messages After	Define how long received syslog messages will be stored for analysis. Choose a period of time from the drop down list.
Filter	
Include Filter	Define if you want to filter syslog messages. If you leave this field empty or use the keyword " any ", all data will be processed. To include specific types of messages only, define filters using a special syntax. For more information, see section Filter Rules ¹³⁴⁴ .
Exclude Filter	Define which types of syslog messages will be discarded and not processed. To exclude specific types of messages, define filters using a special syntax. For more information, see section Filter Rules ¹³⁴⁴ .
Warning Filter	Define which types of syslog messages will count for the Warnings channel. To categorize received messages as warning messages, define filters using a special syntax. For more information, see section Filter Rules ¹³⁴⁴. Note: Messages are collected until a scanning interval ends; as long as the scanning interval is running, no status change will happen. By default, the sensor will turn into a Warning status after a scanning interval has finished and there was at least one warning message (and no error message) during this interval. The status will remain Warning at least until the succeeding scanning interval has finished. If in this scanning interval no warning or error message occurred, the status of the sensor will turn Up again after the interval.
Error Filter	Define which types of syslog messages will count for the Errors channel. To categorize received messages as error messages, define filters using a special syntax. For more information, see section Filter Rules ¹³⁴⁴ .

Filter	
	Note: Messages are collected until a scanning interval ends; as long as the scanning interval is running, no status change will happen. By default, the sensor will turn into a Down status after a scanning interval has finished and there was at least one error message during this interval. The status will remain Down at least until the succeeding scanning interval has finished. If in this scanning interval no warning or error message occurred, the status of the sensor will turn Up again after the interval.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Debugging

Log Data to Disk

Define if the probe will write a log file of the received data to the data folder (see [Data Storage](#)²⁰³⁶) to the disk for debugging purposes. Choose between:

- **Off (recommended):** Do not write additional log files. Recommended for normal use cases.
- **On:** Write log files for all data received.

Note: Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Filter Rules for Syslog Messages

Filter rules are used for the include, exclude, warning, and error definition fields of the Syslog Receiver sensor. They are based on the following format:

```
field[filter]
```

You can use various filters suitable to your needs. Include and exclude filters define which messages will be monitored; warning and error filters define how received messages will be categorized. Provide these filters in the sensor settings as formulas. Formulas are fields which can be combined with boolean operators (**AND**, **OR**, **NOT**) and brackets.

Field	Parameter	Example
source [ip]	the IP address where the messages will be received from; masks and ranges are also possible	▪ source[10.0.23.50] ▪ source[10.0.23.10-50] ▪ source[10.0.23.10/255]
facility [number]	any number (or range) from 0 to 23 specifying the type of program sending the message	▪ facility[2] ▪ facility[5-7] ▪ facility[5] OR facility[6]
severity [number]	any number (or range) from 0 (emergency) to 7 (debug) specifying the type of message	▪ severity[4] ▪ severity[1-3] ▪ severity[1] AND severity [2]
host name [text]	any string specifying the hostname of a device in the message	▪ hostname [www.example.com]

tag [text]	any string specifying the tag of a program or process in the message	▪ tag[su]
appname [text]	any string specifying the appname part of the message	▪ appname[myproc] ▪ appname[demo] AND msgid[m42]
procid [text]	any string specifying the process identifier part of the message	▪ procid[1 860]
msgid [text]	any string specifying the message identifier part of the message	▪ msgid[ID47]
message [parttext]	any string specifying the message part of the message (substring will match; case insensitive !)	▪ message[Error]
data [id, param, value]	checks the SD-ID block of the message's structured data for a parameter matching the given value	▪ data [exampleSDID@1 2345,eventSource,Application]
data [parttext]	checks if the given substring matches on structured data as displayed in the corresponding table	▪ data [exampleSDID@1 234]
data [id, param]	checks if the parameter exists in the given ID element	▪ data [exampleSDID@1 234,eventSource]

Note: String parameters (except the substring in **message**) have to match **exactly** the particular parts of the message; they are case sensitive!

Messages Tab: Review and Analyze Syslog Messages

Received syslog messages are stored as common files in PRTG's data folder (see section [Data Storage](#)^[2036]). In order to review and analyze all received messages, you can access the data directly in PRTG's web interface via the **Overview** tab of the respective sensor in a [table list](#)^[155].

For more details and further filter options, click on the **Messages** tab of the Syslog Receiver sensor. You will see all received messages in a [table list](#)^[155]. On the top, you have display filter options to drill down into the data for specific events of your interest. The filters are the same as available in the sensor settings, but you can define them without using formulas. Provide the desired parameters and PRTG will load the filtered list automatically.

Advanced Filter Settings

You can open advanced filter settings with a click on the gear icon in the **Filter** row. The **Advanced Filter** will appear in a popup window. In the text field, you can define a filter using the syntax as given in section [Filter Rules for Syslog Messages](#)¹³⁴⁴. If you have provided filter parameters on the **Messages** tab, these will be already included in the advanced filter as a corresponding formula with the correct syntax. You can adjust this filter to your needs. You can also copy the automatically created and manually adjusted formula for usage in the filter fields of the sensor settings.

More

Blog Article: Introducing the New High Performance Syslog and SNMP Trap Receiver Sensors

- <http://www.paessler.com/blog/2013/10/11/prtg/introducing-the-new-high-performance-syslog-and-snmp-trap-receiver-sensors>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.160 System Health Sensor

The System Health sensor monitors internal PRTG parameters. It shows the status of the system. This sensor type is created automatically by PRTG and cannot be deleted. It checks various parameters of your PRTG system which can affect the quality of the monitoring results:

- **Health:** This index value sums up the probe state into a value between 100% (healthy) and 0% (failing). Frequent or repeated health values below 100% should be investigated.
- **Available Memory:** This channel shows the amount of free memory available on the system. This value should not fall below 500 MB. This way PRTG still can request resources during report generation, auto-discoveries, and other issues.
- **Available Memory Percent:** This channel shows the free memory available on the system in percent.
- **CPU Load:** This channel shows the current percentage CPU load. Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value usually should stay below 50%.

This sensor can be set up on a Probe Device only!

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.161 TFTP Sensor

The TFTP sensor monitors a Trivial File Transfer Protocol (TFTP) server and checks if a certain file is available for download. It shows the availability.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Sensor Specific	
Timeout (sec)	Enter a timeout in seconds for the TFTP connect. If the reply takes longer than this value the request is aborted and an error message is triggered. Please enter an integer value.
Port	Enter the number of the port the TFTP service is running on. The sensor will try to connect to it. Please enter an integer value.

Sensor Specific	
Filename	Enter the name of the file the sensor will check. If this filename is not available on the server, the sensor's state will be set to down. Please enter a string.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.162 Traceroute Hop Count Sensor

The Traceroute Hop Count sensor traces the number of hops needed from the probe system the sensor is running on to the **IP Address/DNS Name** defined in the sensor's parent device. It returns the number of hops. In case this number changes, you can additionally change the sensor's status.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 2.0.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings

If Route Changes	Define what will be done in case the route has changed since the last check. Choose between: ▪ Ignore: Do not perform any action. ▪ Set sensor to "Warning": Set the sensor to warning status. ▪ Set sensor to "Error": Set the sensor to error status.
Sensor Result	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹³. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.163 Virtuozzo Container Disk Sensor

The Virtuozzo Host Server sensor monitors a Parallels™ Virtuozzo host server. This sensor must be created on a Windows server parent device running Virtuozzo. For each container, it can show disk space used (kb-blocks), disk space soft and hard limit (kb-blocks), the number of inodes, and inodes soft and hard limit.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[226]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Container Settings	
Container	Select all containers for which you want to create a sensor for disk monitoring. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Container Settings

Env ID	Shows the unique ID of the container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the monitored container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
OS	Shows the operating system running on the container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	Shows a description for the container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Powered Off Containers	Define if the sensor will go into an error state if the container is powered off. • Alarm when powered off: Set the sensor for a container to error if the container is powered off. • Ignore powered off state: Only show zero values for a sensor when the monitored container is powered off. Do not set the sensor to error.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor.

Sensor Display	
	▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.164 Virtuozzo Container Network Sensor

The Virtuozzo Host Server sensor monitors a Parallels™ Virtuozzo host server. This sensor must be created on a Windows server parent device running Virtuozzo. For each container, it can show network usage as incoming and outgoing bytes, and the number of incoming and outgoing packets.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[226]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Container Settings	
Container	Select all containers for which you want to create a sensor. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Container Settings

Env ID	Shows the unique ID of the container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the monitored container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
OS	Shows the operating system running on the container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	Shows a description for the container. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Powered Off Containers	Define if the sensor will go into an error state if the container is powered off. • Alarm when powered off: Set the sensor for a container to error if the container is powered off. • Ignore powered off state: Only show zero values for a sensor when the monitored container is powered off. Do not set the sensor to error.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor.

Sensor Display	
	▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Scanning Interval	
Interval	The scanning interval of this sensor type cannot be inherited or changed. Due to internal restrictions of the Virtuozzo system, a fix value must be used.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.165 VMware Host Hardware (WBEM) Sensor

The VMware Host Hardware sensor monitors hardware information of a ESX/ESXi server using Web-Based Enterprise Management (WBEM). It shows the current reading and health state.

Note: The parent device must be a VMware ESX/ESXi server version 3.5, 4.0, 5.0, 5.1, or 5.5. For this sensor type credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems must be defined for the device you want to use the sensor on.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

If you select more than one elements multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

ESX Server Elements

ESX Element	Select the hardware elements you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
ESX Server Elements	
Element	Shows the ESX element monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Automatic Sensor State	Define if the sensor will change its status dependent on the health state reading. Choose between: ▪ Set sensor state automatically to 'Warning' or 'Down': Set the sensor to a Warning or Down status when the server returns respective values. The sensor will additionally change to a Down status if the connection to the server fails. ▪ Just report the current reading, ignore Server Health Value: Never change the sensor's status dependent on the values returned by the server. The sensor will only change to a Down status if the connection to the server fails.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.166 VMware Host Hardware Status (SOAP) Sensor

The VMware Host Hardware Status (SOAP) sensor monitors the hardware status of a VMware host server using Simple Object Access Protocol (SOAP). It shows the total number of items in "Normal", "Warning," and "Alert" states, just as shown in the vSphere client. This sensor is intended to give you a general status overview for your host. Any states other than "Normal" will be reported in the sensor message. **Note:** This sensor only shows items that report an actual state; therefore you might see more "sensors" in your vSphere client than the number of states available in the channels of this PRTG sensor.

Note: The parent device must be a VMware ESX/ESXi server version 3.5, 4.0, 5.0, 5.1, or 5.5. We recommend to **not** use this sensor type on your vCenter. Reliable hardware information can only be provided when this sensor is created on your physical host server as parent device.

For this sensor type credentials for VMware servers must be defined for the device you want to use the sensor on. Please make sure you enter a user with sufficient access rights to obtain statistics (read-only should work).

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Settings on VMware Host System

If you set up this sensor on different probes (for example, when using [remote probes](#)^[2012] or when running a [cluster](#)^[81] setup), you might need to change the settings of your VMware host, so it accepts more incoming connections. Otherwise you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

For details about this setting, please see **More** section below.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

VMware Host Settings	
Host Server	Select the host server you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

VMware Host Settings	
MoID	The Managed Object ID (MoID) of the host. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1793. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

More

Knowledge Base: How can I increase the connection limit on VMware systems?

- <http://www.paessler.com/knowledgebase/en/topic/30643>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.167 VMware Host Performance (SOAP) Sensor

The VMware Host Performance (SOAP) sensor monitors a VMware host server using Simple Object Access Protocol (SOAP). It shows CPU (percent) and memory (absolute) usage, disk read and write speed, and network received and transmitted speed of a VMware host server.

Note: The parent device must be a VMware ESX/ESXi server version 3.5, 4.0, 5.0, 5.1, or 5.5.

For this sensor type credentials for VMware servers must be defined for the device you want to use the sensor on. Please make sure you enter a user with sufficient access rights to obtain statics (read-only should work).

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Settings on VMware Host System

If you set up this sensor on different probes (for example, when using [remote probes](#)^[2012] or when running a [cluster](#)^[81] setup), you might need to change the settings of your VMware host, so it accepts more incoming connections. Otherwise you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

For details about this setting, please see **More** section below.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ⁸⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

More

Knowledge Base: How can I increase the connection limit on VMware systems?

- <http://www.paessler.com/knowledgebase/en/topic/30643>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁸⁸⁰ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁸⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.168 VMware Virtual Machine (SOAP) Sensor

The VMware Virtual Machine (SOAP) sensor monitors a virtual machine on a VMware host server using Simple Object Access Protocol (SOAP). It shows CPU (percent) and memory (absolute) usage, disk read and write speed, read and write latency, and network usage (total, received, and transmitted) of a single virtual machine.

Note: The parent device must be a VMware ESX/ESXi server version 3.5, 4.0, 5.0, 5.1, or 5.5; or a respective Virtual Center server. We recommend using Virtual Center as parent device, because this way PRTG will continue to monitor your virtual machines also when they change the physical host using vMotion.

For this sensor type credentials for VMware servers must be defined for the device you want to use the sensor on. Please make sure you enter a user with sufficient access rights to obtain statics (read-only should work).

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Settings on VMware Host System

If you set up this sensor on different probes (for example, when using [remote probes](#)^[2012] or when running a [cluster](#)^[81] setup), you might need to change the settings of your VMware host, so it accepts more incoming connections. Otherwise you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

For details about this setting, please see **More** section below.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Note: PRTG requests a full list of all virtual machines configured on the device. Therefore, it may take a few seconds before the dialog is loaded.

If you select more than one virtual machine, multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Virtual Machine Settings	
Virtual Machine	You see a list of all virtual machines (VMs) available on the host server on this device, including the ones that are not running. All VMs are listed with name and the OS it is running on. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Virtual Machine Settings

MoID	Shows the Managed Object ID (MoID) of the virtual machine. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Handling of "Powered off" VM	Choose how the sensor will react to a virtual machine that is powered off. Please choose between: • Ignore "powered off" state (default): The sensor will not change to a Down status if the virtual machine is powered off; it will report zero values instead. • Alarm when VM is "powered off": The sensor will change to a Down status if the virtual machine is powered off. Note: While in Down status, a sensor does not record any data in all of its channels.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

More

Knowledge Base: How can I increase the connection limit on VMware systems?

- <http://www.paessler.com/knowledgebase/en/topic/30643>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#) section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#) section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.169 WBEM Custom Sensor

The WBEM Custom Sensor performs a custom query via Web-Based Enterprise Management (WBEM). It can show the total and channels received.

For this sensor type credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems must be defined for the device you want to use the sensor on.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Custom Query Specific

Namespace	Enter the namespace for the query. Default value is root/cimv2 .
WBEM Query (WQL)	Enter the WBEM Query that will be performed with every scanning interval. It has to be written in CQL/WQL.

Custom Query Specific**Numeric Format**

Define the expected type of the returned values. Choose between:

- **Integer:** The query returns integer values.
- **Float:** The query returns float values.

Sensor Display**Primary Channel**

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. **Note:** You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.

Chart Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. **Note:** This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)¹⁶⁸³ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

For more tips and tricks regarding WQL scripts, please see the Paessler Knowledge Base and search for **WQL**.

- <http://www.paessler.com/knowledgebase>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.170 Windows CPU Load Sensor

The Windows CPU Load sensor monitors the CPU load on a computer via Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device. It shows the CPU usage in percent.

Note: By default, this sensor type uses a hybrid approach, first trying to query data via Windows Performance Counters (which needs less system resources), and using Windows Management Instrumentation (WMI) as a fallback in case Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours. The default behavior can be changed in the **Windows Compatibility Options** of the parent [device's settings](#)^[280] this sensor is created on.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[2012]. **Note:** The target system may well run on Windows 2003 or later.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (e.g. via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
WMI Alternative Query	
Errors and invalid data	This is an extended help field only. PRTG's WMI sensors are equipped with the most efficient and accurate WMI queries. However, Microsoft has changed (and will continue to do that in the future) some WMI classes over the various Windows/ServicePack/patchlevel versions, resulting in errors like "class not valid" or "invalid data". Wherever possible PRTG features an alternative query that might work in your specific circumstances. When you keep getting errors for this sensor please try enabling the alternative query method below.
Alternative query	Choose the method PRTG uses to query via WMI. For compatibility reasons, an alternative query method can be enabled. We recommend using the default value. You can choose between:

WMI Alternative Query

- **use default:** Use PRTG's standard method to query WMI. This is the best setting in most cases.
- **use alternative:** Use an alternative method to query WMI. If you keep getting errors, please try this setting.

Sensor Display**Primary Channel**

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. **Note:** You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.

Chart Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. **Note:** This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)¹⁶⁸³ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁰ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.171 Windows IIS 6.0 SMTP Received Sensor

The Windows IIS 6.0 SMTP Receiver Sensor monitors Microsoft's Internet Information Services regarding the number of received emails for an IIS 6.0 SMTP service (Exchange 2003) using Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device. It shows the number of messages, the bytes, and the number of retries, per second for received messages.

Note: This service is not used by Exchange Server 2007 and higher. Exchange Server 2007 uses its own SMTP stack implemented in the Microsoft Exchange Transport service.

Note: By default, this sensor type uses a hybrid approach, first trying to query data via Windows Performance Counters (which needs less system resources), and using Windows Management Instrumentation (WMI) as a fallback in case Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours. The default behavior can be changed in the **Windows Compatibility Options** of the parent [device's settings](#)^[280] this sensor is created on.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[2012]. **Note:** The target system may well run on Windows 2003 or later.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (e.g. via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹³. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.172 Windows IIS 6.0 SMTP Sent Sensor

The Windows IIS 6.0 SMTP Sent Sensor monitors Microsoft's Internet Information Services regarding the number of sent emails for an IIS 6.0 SMTP service (Exchange 2003) using Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device. It shows the number of messages, the bytes, and the number of retries, per second for sent messages.

Note: This service is not used by Exchange Server 2007 and higher. Exchange Server 2007 uses its own SMTP stack implemented in the Microsoft Exchange Transport service.

Note: By default, this sensor type uses a hybrid approach, first trying to query data via Windows Performance Counters (which needs less system resources), and using Windows Management Instrumentation (WMI) as a fallback in case Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours. The default behavior can be changed in the **Windows Compatibility Options** of the parent [device's settings](#)^[280] this sensor is created on.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[2012]. **Note:** The target system may well run on Windows 2003 or later.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (e.g. via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹³. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.173 Windows IIS Application Sensor

The Windows IIS Application sensor monitors a Microsoft Internet Information Services server using Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device. It can also monitor applications that use IIS, such as Microsoft SharePoint or Microsoft Reporting Services (SSRS). The sensor shows bytes sent and received as well as post, get, and CGI requests, not found errors, anonymous and known users, and received and sent files, in number/second.

Note: By default, this sensor type uses a hybrid approach, first trying to query data via Windows Performance Counters (which needs less system resources), and using Windows Management Instrumentation (WMI) as a fallback in case Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours. The default behavior can be changed in the **Windows Compatibility Options** of the parent [device's settings](#)^[280] this sensor is created on.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[2012]. **Note:** The target system may well run on Windows 2003 or later.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (e.g. via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

If you select more than one web service instance, multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Internet Information Services	
Specify Instance	You see a list of all web service instances running on this device. There is also a "_Total" instance available. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Internet Information Services

Instance	The name of the web services instance that is monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 1683 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window	
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[1441] section.

6.8.174 Windows Last Update Sensor

The Windows Last Update sensor reads the number of days since last Windows update from its parent device and returns the number of days. Use [threshold triggers](#)^[1690] to get notified in case this number breaches a certain value.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Note: Your Windows credentials may not contain any double quotation marks ("). If they do, this sensor will not work!

Requirement: Enable Remote Registry Service

In order for this sensor to work, you need to enable the **RemoteRegistry** "Remote Registry" Windows service on the target machine. To do so, please log in to this machine and open the services manager (e.g. start **services.msc**). In the list of services, find the **Remote Registry** service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Timeout (sec.)	Define the timeout for the internal process. It will be killed if it has not returned a result after this time. Please enter an integer value.
If Value Changes	Define what will be done in case the value of this sensor changes. You can choose between: • Ignore changes (default): No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1793. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

More

Knowledge Base: Fixing a Protocol Error Appearing With Windows Last Update Sensor

- <http://www.paessler.com/knowledgebase/en/topic/41113>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.175 Windows Logged In Users Sensor

The Windows Logged In Users sensor queries the number of users logged in to a Windows installation on the parent device. It returns the total number. You can optionally filter for certain user names.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[202]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 2.0.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Note: Your Windows credentials may not contain any double quotation marks ("). If they do, this sensor will not work!

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
User Filter (optional)	To filter the value returned by certain user names, define them here. Enter a comma separated list of user names, or leave the field empty.
Processing of Users in "User Filter"	Define how the user names entered above will be used. Choose between: ▪ Do not count users listed in "User Filter": Exclude the users entered above from counting and only count other uses. ▪ Only count users listed in "User Filter": Ignore all other users and only count user names from the list entered above.
If Value Changes	Define what will be done in case the value of this sensor changes. You can choose between: • Ignore changes (default): No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification^[1690] whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.176 Windows MSMQ Queue Length Sensor

The Windows MSMQ Queue Length sensor reads the number of messages in a Microsoft Message Queue of the parent device. It gives back the total number.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 2.0.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Note: Your Windows credentials may not contain any double quotation marks ("). If they do, this sensor will not work!

Requirement: Message Queuing Service

In order for this sensor to work, the **MSMQ** "Message Queuing" service must be started both on the target system and on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. Additionally, the MSMQ "Message Queuing" service must also be started on the target computer.

To enable the service, please log in to the respective computer and open the services manager (e.g. via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Depending on your Windows version you may first need to install the **Microsoft Message Queue (MSMQ) Server**.

Note: When installing Microsoft Message Queue (MSMQ) Server, make sure you install it including the **Directory Service**. Depending on your Windows installation this might have different names, such as

- MSMQ Active Directory Domain Service Integration
- Directory Service Integration
- Active Directory Integration

For details, please see [More](#)¹⁴⁴⁸ section below.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings

Message Queue	You see a list showing the names of all message queues found on the target device. If there are no message queues available, you will see a corresponding message. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head. Note: Sub-queues are not supported by this sensor.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ¹⁶⁹¹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Message Queue	Shows the name of the task monitored by this sensor. The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:
Min. Message Age	Optionally define an age in minutes the message has to be old. If set, messages younger than this will not be regarded. If you leave this field blank, the sensor will not check for the message age. Please enter an integer value or leave the field empty.
If Value Changes	Define what will be done in case the value of this sensor changes. You can choose between: • Ignore changes: No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification¹⁶⁹⁰ whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹³. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

More

Knowledge Base: How do I activate Message Queuing in my Windows installation?

- <http://www.paessler.com/knowledgebase/en/topic/25963>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[1441] section.

6.8.177 Windows Network Card Sensor

The Windows Network Card sensor monitors bandwidth usage and traffic of a network interface using Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device.

Note: By default, this sensor type uses a hybrid approach, first trying to query data via Windows Performance Counters (which needs less system resources), and using Windows Management Instrumentation (WMI) as a fallback in case Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours. The default behavior can be changed in the **Windows Compatibility Options** of the parent [device's settings](#)^[280] this sensor is created on.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[2012]. **Note:** The target system may well run on Windows 2003 or later.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (e.g. via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

For devices with multiple network cards multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Network Interface	Select the network card(s) you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Selected Interface	Shows the name of the network card that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings). ▪ Show in and out traffic as positive and negative area chart: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.178 Windows Pagefile Sensor

The Windows Pagefile sensor monitors the Windows pagefile usage via Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device. It shows the usage in percent. **Note:** This sensor does **not** work with Windows 2000, because the respective WMI class does not exist on this operating system!

Note: By default, this sensor type uses a hybrid approach, first trying to query data via Windows Performance Counters (which needs less system resources), and using Windows Management Instrumentation (WMI) as a fallback in case Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours. The default behavior can be changed in the **Windows Compatibility Options** of the parent [device's settings](#)^[280] this sensor is created on.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[2012]. **Note:** The target system may well run on Windows 2003 or later.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (e.g. via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.179 Windows Physical Disk Sensor

The Windows Physical Disk sensor monitors parameters of a physical disk of a Windows device using Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device. It shows accumulated disk read/write time and bytes, queue, split IO, etc. on physical disks.

Note: By default, this sensor type uses a hybrid approach, first trying to query data via Windows Performance Counters (which needs less system resources), and using Windows Management Instrumentation (WMI) as a fallback in case Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours. The default behavior can be changed in the **Windows Compatibility Options** of the parent [device's settings](#)^[280] this sensor is created on.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[2012]. **Note:** The target system may well run on Windows 2003 or later.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (e.g. via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Physical Disk Specific	
Physical Disks	You see a list showing the Name of the counters you can monitor as well as the Instance, i.e. the respective logical disk (or '_Total'). If there are no logical disks available, you will see a corresponding message. From the list, choose all Name/Instance combinations you want to monitor by adding a check mark in front of the respective line (for example, choose '% Disk Read Time for C:'). A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings

Counter	These fields show the parameters that are used to query data for this sensor from the target device. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Instance	
WMI Class	
Datafield	
Basefield	
Frequencyfield	
Countertype	
Sensor Result	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the results. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received to the "Logs (System)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor.

Sensor Display	
	▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹². Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.180 Windows Print Queue Sensor

The Windows Print Queue sensor reads the print queue on its parent device and gives back the number of jobs in the print queue. It can monitor queues for all printers that are installed locally. For example, you can use this sensor to monitor all print queues on your Windows print server. Additionally, this sensor can change to a **Warning** status if there is a printer problem, such as out of paper, etc.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Note: Your Windows credentials may not contain any double quotation marks ("). If they do, this sensor will not work!

Requirement: Print Spooler Service

In order for this sensor to work, the **Spooler** "Print Spooler" service must be started on the target computer.

To enable the service, please log in to the respective computer and open the services manager (e.g. via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Print Queue	You see a list showing the names of all print queues found on the target device. If there are no print queues available, you will see a corresponding message. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head. Note: If a printer name changes after you created a sensor for its queue, please add the sensor anew.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Print Queue Name	Shows the name of the task monitored by this sensor. The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:
Min. Print Job Age (sec.)	Optionally define the age in seconds. If set, jobs younger than this will not be regarded. If you leave this field blank, the sensor will not check for the print job age. Please enter an integer value or leave the field empty.
Set to Warning on Problem Reported	Define if the sensor will change to a Warning status in case a printer reports a problem. Choose between: ▪ No ▪ Yes
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window	
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁸⁸⁸ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁸⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.181 Windows Registry Sensor

The Windows Registry sensor reads a string value from the Windows registry and can process the result using a keyword search. The value is shown in the sensor's last message field. **Note:** Only **REG_SZ** values can be processed with this sensor.

Requirement: Remote Registry Service

In order for this sensor to work, please make sure the **RemoteRegistry** "Remote Registry" Windows service is running on both the computer running the PRTG probe and the target machine.

To enable the service, please log in to the respective computer and open the services manager (e.g. via **services.msc**). In the list, find the respective service and set its **Start Type** to **Automatic**.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Please make sure that the Windows user account running the **PRTGProbeService** "PRTG Probe Service" on the computer running the PRTG probe has access to the registry of the remote computer (by default, this is the probe computer's local Windows "system" account).

Additionally, the computer running the PRTG probe and the target computer must be member of the same Windows local domain.

Note: You cannot perform a remote registry call with a Windows user account for which no password is defined.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Registry Settings	
Root	Select the root key of the registry entry you want to monitor. Choose between: ▪ HKEY_CLASSES_ROOT ▪ HKEY_CURRENT_USER ▪ HKEY_LOCAL_MACHINE ▪ HKEY_USERS ▪ HKEY_PERFORMANCE_DATA ▪ HKEY_CURRENT_CONFIG ▪ HKEY_DYN_DATA
Key Name	Enter the path of the key you want to monitor. Enter the full path after the root, each subkey divided by a backslash. For example, enter Software\Microsoft\Windows\CurrentVersion
Value Name	Enter the name of the value you want to monitor. For example, enter ProductId to read the product ID of the target computer's Windows installation.
64-Bit Selection	Define how the provided key name will be looked up. This is relevant for some registry keys only, for example those containing the Wow6432Node subkey. Choose between: ▪ Use 32-bit registry view: The key provided above is copied from the 32-bit registry editor.

Registry Settings	
	▪ Use 64-bit registry view: The key provided above is copied from the 64-bit registry editor. For more information, see the More¹⁴⁸² section below.
Value	Select if the returned result will be further processed. Choose between: ▪ Ignore Value: Do not perform any more keyword checks. The registry value is shown in the sensor last message field only. ▪ Process Text: Use the returned value to perform keyword checks. Select below.
Check For Existing Keywords (Positive)	This setting is only visible if text processing is activated above. Check if a certain keyword is part of the received value. If there is no match, the sensor will show a "Down" status. ▪ Disable: Do not check for positive keywords. ▪ Enable keyword check (positive): Check if a certain keyword exists in the received value. Define below.
Text Must Include	This setting is only visible if keyword check is activated above. Enter a search string that must be contained in the returned value.
For Keyword Search Use	Define the method you want to provide the search string with. Choose between: ▪ Plain Text: Search for a simple string. ▪ Regular Expression: Search using a regular expression. For more details, see Regular Expressions²⁰¹⁰ section.
Check For Existing Keywords (Negative)	This setting is only visible if text processing is activated above. Check if a certain keyword is not part of the received value. If there is a match, the sensor will show a "Down" status. ▪ Disable: Do not check for negative keywords. ▪ Enable keyword check (negative): Check if a certain keyword does not exist in the received value. Define below.
Text Must Not Include	This setting is only visible if keyword check is activated above. Enter a search string that must not be contained in the returned value.
For Keyword Search Use	Define the method you want to provide the search string with. Choose between:

Check For Existing Keywords (Positive)	This setting is only visible if text processing is activated above. Check if a certain keyword is part of the received value. If there is no match, the sensor will show a "Down" status. ▪ Disable: Do not check for positive keywords. ▪ Enable keyword check (positive): Check if a certain keyword exists in the received value. Define below.
	▪ Plain Text: Search for a simple string. ▪ Regular Expression: Search using a regular expression. For more details, see Regular Expressions^[2010] section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[1685] settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[224] group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴¹.

More

How do I discern 32-bit registry values vs. 64-bit registry values?

- <http://www.paessler.com/knowledgebase/en/topic/25513>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁸⁸⁰ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁸⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.182 Windows Scheduled Task Sensor

The Windows Scheduled Task sensor returns the number of minutes since the last run of the specified task as well as the exit code. If a task was never run or if a defined Exit code does not match, the sensor shows an error.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Requirement: Remote Registry Service

In order for this sensor to work, please make sure the **RemoteRegistry** "Remote Registry" Windows service is running on both the computer running the PRTG probe and the target machine.

To enable the service, please log in to the respective computer and open the services manager (e.g. via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Note: Your Windows credentials may not contain any double quotation marks ("). If they do, this sensor will not work!

Requirement: Monitored Systems

Note: We recommend running the PRTG probe on Windows 2008 R2 or later.

Microsoft implemented two versions of scheduled task, V1 and V2. Windows 2000, Windows XP, and Windows Server 2003 create scheduled tasks V1 by default. Later Windows versions can create and read both versions.

- If the system running the PRTG probe (either on the core server or a remote probe) runs on one of these early Windows versions, you will not be able to monitor scheduled tasks of V2. In this case, please create the tasks on the monitored machines compatible with "Windows Server 2003, Windows XP, or Windows 2000" if there is a newer Windows version installed.
- If the system running the PRTG probe (either on the core server or a remote probe) runs on Windows Vista or later, you will be able to monitor scheduled tasks of both V1 and V2 (i.e. from all Windows versions).

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Sensor Settings	
Task Name	You see a list showing the names of all tasks found in the Windows Task Scheduler on the target device. If there are no scheduled tasks, you will see a corresponding message. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.. Note: If a task name changes after you created a sensor for it, please add the sensor anew.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Basic Sensor Settings	
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Name	Shows the name of the task monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • Ignore changes: No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹³. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.183 Windows System Uptime Sensor

The Windows System Uptime sensor monitors uptime of a Windows system using Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device. It returns the total uptime.

Note: By default, this sensor type uses a hybrid approach, first trying to query data via Windows Performance Counters (which needs less system resources), and using Windows Management Instrumentation (WMI) as a fallback in case Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours. The default behavior can be changed in the **Windows Compatibility Options** of the parent [device's settings](#)^[280] this sensor is created on.

Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Requirement: Windows Version

In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[2012]. **Note:** The target system may well run on Windows 2003 or later.

Requirement: Remote Registry Service

In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (e.g. via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.184 Windows Updates Status (Powershell) Sensor

The Windows Updates Status (Powershell) sensor monitors the status of Windows updates on a computer and counts the available and installed Windows updates—either from Microsoft or from the local Windows Server Update Services (WSUS) server. This sensor can show the time elapsed since the last update, as well as the following numbers:

- Installed Windows updates
- Missing Windows updates
- Installed security updates with low, moderate, important, and critical priority
- Missing security updates with low, moderate, important, and critical priority

You can find the considered updates in **Server Manager (WSUS)** under **Roles | Windows Server Update Services | Update Services | Computers | Reports**.

Note: If the sensor cannot determine the **Time since last update** (for example, because the list of updates is empty), it will show the value **-1s** and turn into a **Warning** status.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Note: We recommend setting the [scanning interval](#)¹⁴⁹⁹ of this sensor to at least 12 hours to limit the load on the server being monitored.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)²⁰¹². If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Requirement: Remote PowerShell

The Windows Updates Status (Powershell) sensor uses PowerShell commands. In order to monitor devices with this sensor, **Remote PowerShell** access has to be enabled on the target computer. For detailed information, please see [More](#)⁵⁷⁷ section below.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration¹⁸⁰⁵.
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings¹⁷⁹¹. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

More

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <http://www.paessler.com/knowledgebase/en/topic/44453>

Knowledge Base: My Powershell sensor returns an error message. What can I do?

- <http://www.paessler.com/knowledgebase/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <http://www.paessler.com/knowledgebase/en/topic/59745>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴³ section.

6.8.185 WMI Custom Sensor

The WMI Custom Sensor performs a custom query via Windows Management Instrumentation (WMI).

Note: Your Windows Management Instrumentation Query Language (WQL) query code must be stored in a file on the system of the probe the sensor is created on: If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Custom Query Specific	
Channel Name	Enter a name for the channel in which the received data will be presented. The name will be displayed in graphs and tables. Please enter a string. You can change the name later in the sensor's channel settings ^[1683] .
WQL File	Select a file that will be used for this sensor from the drop down menu. It will be executed with every scanning interval. The menu contains WQL scripts from the \Custom Sensors\WMI WQL scripts sub folder of your PRTG installation. Please store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node! For more information on how to find this path, please see Data Storage ^[2036] section. Note: Your query must return an integer or float value. Strings are not supported!

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Custom Query Specific	
Namespace	Enter the namespace for the query.
WQL File	Shows the WQL file that is executed by the sensor with every scanning interval. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Placeholder <#PH1>	In your WQL script, you can use up to three placeholders that you can assign a value to using this field. Please enter a string for variable <#PH1> or leave the field empty.
Placeholder <#PH2>	In your WQL script, you can use up to three placeholders that you can assign a value to using this field. Please enter a string for variable <#PH2> or leave the field empty.
Placeholder <#PH3>	In your WQL script, you can use up to three placeholders that you can assign a value to using this field. Please enter a string for variable <#PH3> or leave the field empty.

Custom Query Specific	
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • Ignore changes (default): No action will be taken on change. • Trigger 'On Change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification ¹⁶⁹⁰ whenever the sensor value changes.
Channel Name	Enter a name for the channel in which the received data will be presented. The name will be displayed in graphs and tables. Please enter a string.
Unit String	Enter a unit for the data that will be received by your script. This is for displaying purposes only. The unit will be displayed in graphs and tables. Please enter a string.
Multiplication	Define with which value the received values will be multiplied by. By default, this is set to 1 in order to not change the received values. Please enter an integer, a decimal value, or leave the field empty.
Division	Define with which value the received values will be divided by. By default, this is set to 1 in order to not change the received values. Please enter an integer, a decimal value, or leave the field empty.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

- [Additional Sensor Types \(Custom Sensors\)](#)¹⁶⁸⁰

Knowledge Base: How do I properly configure a WMI custom sensor?

- <http://www.paessler.com/knowledgebase/en/topic/163>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.186 WMI Custom String Sensor

The WMI Custom String sensor performs a custom string query via Windows Management Instrumentation (WMI).

Note: Your Windows Management Instrumentation Query Language (WQL) query code must be stored in a file on the system of the probe the sensor is created on: If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Custom Query Specific	
Channel Name	Enter a name for the channel in which the received data will be presented. The name will be displayed in graphs and tables. Please enter a string. You can change the name later in the sensor's channel settings ^[1683] .
WQL File	Select a file that will be used for this sensor from the drop down menu. It will be executed with every scanning interval. The menu contains WQL scripts from the \Custom Sensors\WMI WQL scripts sub folder of your PRTG installation. Please store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node! For more information on how to find this path, please see Data Storage ^[2036] section.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Custom Query Specific	
Namespace	Enter the namespace for the query.
WQL File	Shows the name of the file that this sensor is using. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Placeholder <#PH1>	In your WQL script, you can use up to three placeholders that you can assign a value to using this field. Please enter a string for variable <#PH1> or leave the field empty.
Placeholder <#PH2>	In your WQL script, you can use up to three placeholders that you can assign a value to using this field. Please enter a string for variable <#PH2> or leave the field empty.
Placeholder <#PH3>	In your WQL script, you can use up to three placeholders that you can assign a value to using this field. Please enter a string for variable <#PH3> or leave the field empty.

Custom Query Specific	
If Value Changes	Define what shall be done in case the value of this sensor changes. You can choose between: • Ignore changes (default): No action will be taken on change. • Trigger 'On Change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.
Channel Name	Enter a name for the channel in which the received data will be presented. The name will be displayed in graphs and tables. Please enter a string.
Unit String	Enter a unit for the data that will be received by your script. This is for displaying purposes only. The unit will be displayed in graphs and tables. Please enter a string.
Multiplication	Define with which value the received values will be multiplied by. By default, this is set to 1 in order to not change the received values. Please enter an integer, a decimal value, or leave the field empty.
Division	Define with which value the received values will be divided by. By default, this is set to 1 in order to not change the received values. Please enter an integer, a decimal value, or leave the field empty.
Response Must Include	Define which string must be part of the data that is received from the WMI object. You can either enter plain text or a Regular Expression . If the data does not include the search pattern, the sensor will be set to an error state. Please enter a string or leave the field empty.
Response Must Not Include	Define which string must not be part of the data that is received from the WMI object. You can either enter plain text or a Regular Expression . If the data does include the search pattern, the sensor will be set to an error state. Please enter a string or leave the field empty.
For Keyword Search Use	Define in which format you have entered the search expression in the field above. ▪ Plain Text: Search for the string as plain text. The characters * and ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible with plain text search.

Custom Query Specific	
	▪ Regular Expression: Treat the search pattern as a Regular Expression ²⁰¹⁰.
Maximum Length of String	Define the maximum allowed length of the string that will be received from the WMI object. If it is longer than this value, the sensor will be set to an error status. Please enter an integer value or leave the field empty.
Extract Number Using Regular Expression	Define if you want to filter out a numeric value from the string received from the WMI object. You can convert this into a float value, in order to use it with channel limits (see Sensor Channels Settings ¹⁶⁸³). ▪ No extraction: Do not extract a float value. Use the result as a string value. ▪ Extract a numeric value using a regular expression: Use a regular expression to identify a numeric value in the string and convert it to a float value. Define below. See also the example ¹⁵¹⁷ below.
Regular Expression	This setting is only visible if number extraction is enabled above. Enter a Regular Expression ²⁰¹⁰ to identify the numeric value you want to extract from the string returned by the WMI object. You can use capturing groups here. Make sure the expression returns numbers only (including decimal and thousands separators). The result will be further refined by the settings below.
Index of Capturing Group	This setting is only visible if number extraction is enabled above. If your regular expression uses capturing groups, please specify which one will be used to capture the number. Please enter an integer value or leave the field empty.
Decimal Separator	This setting is only visible if number extraction is enabled above. Define which character is used as decimal separator for the number extracted above. Please enter a string or leave the field empty.
Thousands Separator	This setting is only visible if number extraction is enabled above. Define which character is used as thousands separator for the number extracted above. Please enter a string or leave the field empty.
Sensor Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results.

Custom Query Specific

- **Write sensor result to disk (Filename: "Result of Sensor (ID).txt"):** Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see [Data Storage](#)^[2036] section.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[1683] settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[224] group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

Example: Number Extraction with Regular Expression

If you want to extract a number in the response string using a regular expression, please note that the index for captures in this sensor is based on **1 (not on 0)**. Furthermore, capturing groups are not created automatically. The example below will illustrate this issue.

Consider the following string as returned by a request for CPU usage:

```
5 Sec (3.49%), 1 Min (3.555%), 5 Min (3.90%)
```

Assuming you would like to filter for the number **3.555**, i.e., the percentage in the second parentheses. Then enter the following regex in the **Regular Expression** field:

```
(\d+\.\d+).* (\d+\.\d+).* (\d+\.\d+)
```

As **Index of Capturing Group** enter **3**. This will extract the desired number 3.555.

The index has to be 3 in this case because the capturing groups here are the following:

- Group 1 contains "3.49%), 1 Min (3.555), 5 Min (3.90"
- Group 2 contains "3.49"
- Group 3 contains "3.555"
- Group 4 contains "3.90"

Please keep in mind this note about index and capturing groups when using number extraction.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.187 WMI Event Log Sensor

The WMI Event Log sensor monitors a specific Windows log file using Windows Management Instrumentation (WMI). It shows the number of new records (volume), the number of new records per second (speed), and it returns the last message in the sensor status.

You can set the sensor to a desired status individually according to a new event log entry. For details and how to find out the correct filter, see section [More](#)^[1525].

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

If you select more than one log file, multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Event Log Monitor	
Log File	The Windows event log provides several different log files. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Event Log Monitor	
Log file	Shows the Windows log file that this sensor will monitor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Filter Event Log Entries	
Event Type	Specify the type of event that will be considered by this sensor. Other event type will not be processed. Choose between the following event types: ▪ Any ▪ Error ▪ Warning ▪ Information ▪ Security Audit Success ▪ Security Audit Failure
Filter by Source	Filter all received events for a certain event source. If enabled, only messages matching the defined value will be considered by the sensor. Choose between:

Filter Event Log Entries	
	• Off: Do not filter by event source. • On: Enable filtering by event source.
Match String (Event Source)	This field is only visible if filtering is enabled above. Enter a source from which the events are to come from. Only events from a source matching this string will be regarded, others ignored. Please enter a string.
Filter by ID	Filter all received events for a certain event ID. If enabled, only messages matching the defined value(s) will be considered by the sensor. Choose between: • Off: Do not filter by event ID. • On: Enable filtering by event ID.
Match Value (Event ID)	This field is only visible if filtering is enabled above. Enter one or more event IDs (comma separated) from which the events are to come from. Only events with an ID matching one of the values will be regarded. Please enter one integer value or more comma separated integer values.
Filter by Category	Filter all received events for a certain event category. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • Off: Do not filter by event category. • On: Enable filtering by event category.
Match String (Event Category)	This field is only visible if filtering is enabled above. Enter a category which the events are to have. Only events with a category matching this string will be regarded. Please enter a string.
Filter by Event User	Filter all received events for a certain event user. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • Off: Do not filter by event user. • On: Enable filtering by event user.
Match String (Event User)	This field is only visible if filtering is enabled above. Enter a user name which the event are to be assigned to. Only events with a user name matching this string will be regarded. Please enter a string.

Filter Event Log Entries	
Filter by Event Computer	Filter all received events for a certain event computer. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • Off: Do not filter by event computer. • On: Enable filtering by event computer.
Match String (Event Computer)	This field is only visible if filtering is enabled above. Enter a computer name which the events are to be assigned to. Only events with a computer name matching this string will be regarded. Please enter a string.
Filter by Event Message	Filter all received events for a certain event message. If enabled, only messages matching the defined value will be considered by the sensor. Choose between: • Off: Do not filter by event message. • On: Enable filtering by event message.
Match String (Event Message)	This field is only visible if filtering is enabled above. Enter a message which the event must contain. Only events with a message matching this string will be regarded. Please enter a string.

Note: For the **WMI Event Log Sensor**, you can use the percent sign (%) as placeholder for any or no character (as known from the asterisk sign (*)) in Windows search) in combination with a substring. For example, you can enter %RAS% for any event source containing the string RAS.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

More

Knowledge Base: Event Log Sensors: Setting Correct Status and Source Filter

- <http://www.paessler.com/knowledgebase/en/topic/59803>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁸⁸⁰ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁸⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.188 WMI Exchange Server Sensor

The WMI Exchange Server sensor monitors a Microsoft Exchange Server 2003, 2007, or 2010 using Windows Management Instrumentation (WMI). It can show information about the queue, delivery time, latency, users, etc.

Note: Existing former "WMI Exchange Server 2003/2007 Sensors" from previous PRTG versions will continue to monitor your Exchange server in PRTG 9, but newly added Exchange server sensors will be of the "WMI Exchange Server Sensor" type which is able to monitor Exchange servers regardless of their version.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[202] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor an Exchange Server, PRTG will create one sensor for each performance counter you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Exchange Server Data Readings Accessible Using WMI

Performance Counter

You see a list of data values the sensor can monitor on your Exchange server. The available options depend on your Exchange server configuration. PRTG shows all possible performance counters with name and instance description (if available). Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

You might be able to select aspects regarding:

- **SMTP Server:** Queue Lengths

Exchange Server Data Readings Accessible Using WMI

- **MSExchangeIS Mailbox:** Queue Sizes, Delivery Times, Operations, Messages
- **MSExchangeIS Public:** Queue Sizes, Delivery Times, Operations, Messages
- **MSExchangeIS:** Packets, Operations, Clients, Latency, Requests, Users
- **MS Exchange RPC Client Access:** Active User Count, User Count, Connection Count
- **MS Exchange OWA:** Current Unique Users, Average Response Time

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings

Counter	These fields show the parameters that are used to query data for this sensor from the target device. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Instance	

Sensor Settings	
WMI Class	
Datafield	
Basefield	
Frequencyfield	
Countertype	
Sensor Result	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the results. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received to the "Logs (System)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.189 WMI Exchange Transport Queue Sensor

The WMI Exchange Server sensor monitors the length of transport queues of a Microsoft Exchange Server 2003, 2007, or 2010 using Windows Management Instrumentation (WMI). It shows the same information as shown in Windows System Monitor ('perfmon'). See section [More](#)^[1539] below for an explanation of the transport queue types.

Possible values that can be monitored: Active Mailbox Delivery Queue Length, Active Non-Smtp Delivery Queue Length, Active Remote Delivery Queue Length, Aggregate Delivery Queue Length (All Queues), Aggregate Shadow Queue Length, Categorizer Job Availability, Items Completed Delivery Per Second, Items Completed Delivery Total, Items Deleted By Admin Total, Items Queued For Delivery Expired Total, Items Queued for Delivery Per Second, Items Queued For Delivery Total, Items Resubmitted Total, Largest Delivery Queue Length, Messages Completed Delivery Per Second, Messages Completed Delivery Total, Messages Completing Categorization, Messages Deferred Due To Local Loop, Messages Deferred during Categorization, Messages Queued For Delivery, Messages Queued for Delivery Per Second, Messages Queued For Delivery Total, Messages Submitted Per Second, Messages Submitted Total, Poison Queue Length, Retry Mailbox Delivery Queue Length, Retry Non-Smtp Delivery Queue Length, Retry Remote Delivery Queue Length, Shadow Queue Auto Discards Total, Submission Queue Items Expired Total, Submission Queue Length, Unreachable Queue Length.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

If you select more than one queue, multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Exchange Transport Queue Specific**MSExchangeTransport Queues**

You see a list of transport queues that can be monitored on your Exchange server. The available options depend on your Exchange server configuration. PRTG shows all possible queues with name and instance description (if available). Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head. **Note:** For performance reasons, we recommend to only select necessary items!

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings**Sensor Name**

Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Tags

Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. Those are not visible here.

Priority

Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Exchange Transport Queue Specific**Displayname****Instance****WMI Class**

These fields show different information about the transport queue monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

WMI Exchange Transport Queue Specific	
Counter	
TimeStamp	
TimeFreq	
Countertype	
Sensor Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results. ▪ Write sensor result to disk (Filename: "Result of Sensor (ID).txt"): Store the last result received to the "Logs (System)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window	
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

More

Knowledge Base: Types of Transport Queues in Microsoft Exchange

- <http://www.paessler.com/knowledgebase/en/topic/55413>

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.190 WMI File Sensor

The WMI File monitors a file using Windows Management Instrumentation (WMI). It shows the file size and the last modified date.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[226]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI File Monitor	
File name	Enter the name of the file that this sensor will check. Please enter a full local path. The file must exist on the computer your local or remote probe is running on; UNC paths are not allowed here. For example, when creating this sensor on a device under the local probe, the file be accessible on the local system.
If timestamp changes	Define what shall be done in case the timestamp of the file changes. You can choose between: • Ignore changes (default): No action will be taken on change. • Trigger 'On Change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window**Dependency Type**

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency.
- **Select object:** Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency.

Note: Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.

Dependency

This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the [object selector](#)^[158] to choose an object on which the current sensor will be dependent on.

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree.
Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#) settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#).

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[1441] section.

6.8.191 WMI Free Disk Space (Multi Drive) Sensor

The WMI Free Disk Space (Multi Drive) sensor monitors the free disk space of one or multiple drive(s) using Windows Management Instrumentation (WMI). It shows the space in percent and total. One single sensor is used for all drives; the data is presented in different channels.

This sensor monitors logical partitions of a hard or fixed disk drive. PRTG identifies logical disks by their drive letter, such as C.

Note: This sensor is also supported on Windows XP and earlier.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Volume Specific

Drive	From the drop down menu, select the drive(s) you want to monitor. We recommend using the default value. You can choose All to monitor all available drives or you can choose one specific drive letter to monitor this single drive only. The data in the drop down menu may also contain drive letters that do not exist on your device. The drive setting cannot be changed once the sensor is created.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Disk Free Configuration

Drive	Shows the drive(s) that this sensor is monitoring; either All or a specific drive letter. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Set limits checked against ALL disks

In this section you can set limits that are valid for all channels and all drives. By entering limits, you can define when the sensor will enter a **Warning** or **Down** status; depending on the data provided by all drives that this sensor monitors. If you want to define limits for separate channels individually please use the limit settings in the sensor's **Channels** settings.

Note: All limits defined here are valid additionally to the limits defined in the particular **Channels** settings!

Percentage Limit Check	Enable or disable a limit check for the free space in percentage channels of all drives. By default percentage limits are enabled with lower warning and lower error limit. Choose between: • Disable Percentage Limits: Do not use the drives' data to control the sensor's status. • Enable Percentage Limits: Define limits. Additional fields appear below. The sensor will enter a warning or down state when free space limits are undercut or overrun.

Set limits checked against ALL disks	
Upper Error Limit	This field is only visible if percentage limit check is enabled above. Specify an upper limit in percent for a Down status. If the free disk space of one of your drives overruns this percent value, the sensor will be set to Down . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Upper Warning Limit	This field is only visible if percentage limit check is enabled above. Specify an upper limit in percent for a Warning status. If the free disk space of one of your drives overruns this percent value, the sensor will be set to Warning . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Lower Warning Limit	This field is only visible if percentage limit check is enabled above. Specify a lower limit in percent for a warning state. If the free disk space of one of your drives undercuts this percent value, the sensor will be set to warning. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Lower Error Limit	This field is only visible if percentage limit check is enabled above. Specify a lower limit in percent for entering a Down status. If the free disk space of one of your drives undercuts this percent value, the sensor will be set to Down . Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings ¹⁶⁸³ . The limits set here and in the channel settings are valid simultaneously!
Byte Limit Check	Enable or disable a limit check for the free bytes channels of all drives. Choose between: • Disable Byte Limits: Do not use the drives' data to control the sensor's status. • Enable Byte Limits: Define limits. Additional fields appear below. The sensor will enter a warning or down state when free space limits are undercut or overrun.

Set limits checked against ALL disks	
Upper Error Limit	This field is only visible if byte limit check is enabled above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor will be set to Down. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings¹⁶⁸³. The limits set here and in the channel settings are valid simultaneously!
Upper Warning Limit	This field is only visible if byte limit check is enabled above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor will be set to Warning. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings¹⁶⁸³. The limits set here and in the channel settings are valid simultaneously!
Lower Warning Limit	This field is only visible if byte limit check is enabled above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor will be set to Warning. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings¹⁶⁸³. The limits set here and in the channel settings are valid simultaneously!
Lower Error Limit	This field is only visible if byte limit check is enabled above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor will be set to Down. Please enter an integer value or leave the field empty. Note: The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings¹⁶⁸³. The limits set here and in the channel settings are valid simultaneously!
Alarm on Missing/ Removed Disk	If a monitored disk is removed or not found, values are set to zero. Select the alarming approach in this case. Choose between: ▪ Deactivate alarm (default): Select this option if you do not want an alarm for a removed disk. ▪ Activate Alarm: Select this option if you want to be alerted if a monitored disk is removed.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁹⁰⁵ .

Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.192 WMI HDD Health Sensor

This sensor type connects to the parent device via Windows Management Instrumentation (WMI) and monitors the health of IDE disk drives on the target system, using Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.). This is built into most modern IDE hard disk drives.

Note: This sensor officially requires Windows Vista or later running on the target machine which holds the hard disk drives you want to monitor. The sensor may **not** work reliably when the target machine runs on Windows 2003 or Windows XP; due to a known bug in those systems, the sensor may not be able to detect available hard disk drives.

Available sensor channels may vary, depending on the hardware used on the target system. Available measurements may include: Read Error Rate, Spin-Up Time, Start/Stop Count, Reallocated Sectors Count, Seek Error Rate, Power-On Hours, Spin Retry Count, Calibration Retry Count, Power Cycle Count, Power-off Retract Count, Load Cycle Count, Temperature Celsius, Reallocation Event Count, Current Pending Sector Count, Uncorrectable Sector Count, UltraDMA CRC Error Count, Write Error Rate, Transfer Error Rate, Total LBAs Written, and Total LBAs Read.

The channel names indicate the ID of the channel, followed by a colon, and the typical meaning of the channel. **Note:** Some vendors define meanings other than the common one.

Every attribute of a disk assumes a value. PRTG shows these attributes as channels with their last, minimum, and maximum value. These channel values change over time and indicate the disk health—higher values correspond to a better health. The disk's attributes come with a threshold, defined by the manufacturer of the drive. If a channel value is lower than this threshold, the sensor is automatically set to a **Warning** status. This indicates that the Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) status of the HDD might break soon. **Note:** For some attributes are no thresholds defined and thus cannot be judged for a status other than **Up**.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[226]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor the health of a disk, PRTG will create one sensor for each IDE device you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

SMART Specific	
IDE Devices	Please select one or more hard disks you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head. . The items shown in the list are specific to the parent device you create the sensor on.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SMART Specific	
Serial No.	Shows the serial number of the monitored disk. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SMART Specific	
Size (GB)	Shows the size in Gigabyte of the monitored disk. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the monitored disk. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Timeout (sec)	Enter a timeout in seconds for the request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁸ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.193 WMI Logical Disk Sensor

The WMI Logical Disk sensor monitors parameters of a logical disk of a Windows device using Windows Management Instrumentation (WMI). It shows disk read/write time, queue, free space, etc. on logical partitions of a disk drive.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[202] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[192] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Logical Disk Specific

Logical Disks

You see a list showing the **Name** of the counters you can monitor as well as the **Instance**, i.e. the respective logical disk (or '_Total'). If there are no logical disks available, you will see a corresponding message. From the list, choose all **Name/Instance** combinations you want to monitor by adding a check mark in front of the respective line (for example, choose '% Disk Read Time for C:'). For each selection one sensor will be created using the defined settings.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Counter	These fields show the parameters that are used to query data for this sensor from the target device. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Instance	
WMI Class	
Datafield	
Basefield	
Frequencyfield	
Countertype	
Sensor Result	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the results. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received to the "Logs (System)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage^[2036] section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁹⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings 1793. Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.194 WMI Memory Sensor

The WMI Memory sensor monitors available (free) system memory on Windows systems using Windows Management Instrumentation (WMI).

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[226]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Alternative Query	
Errors and invalid data	This is an extended help field only. PRTG's WMI sensors are equipped with the most efficient and accurate WMI queries. However, Microsoft has changed (and will continue to do that in the future) some WMI classes over the various Windows/ServicePack/patchlevel versions, resulting in errors like "class not valid" or "invalid data". Wherever possible PRTG features an alternative query that might work in your specific circumstances. When you keep getting errors for this sensor please try enabling the alternative query method below.
Alternative query	Choose the method PRTG uses to query via WMI. For compatibility reasons, an alternative query method can be enabled. We recommend using the default value. You can choose between: • use default: Use PRTG's standard method to query WMI. This is the best setting in most cases. • use alternative: Use an alternative method to query WMI. If you keep getting errors, please try this setting.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note : You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 1683 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window**Dependency Type**

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device it is created on is in a **Down** status, or if it is paused by another dependency.
- **Select object:** Pause the current sensor if the device it is created on is in an **Down** status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a **Down** status, or if it is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a **Down** status, or if it is paused by another dependency.

Note: Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.

Dependency

This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the [object selector](#)^[158] to choose an object on which the current sensor will be dependent on.

Delay (Seconds)

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.195 WMI Microsoft SQL Server 2005 Sensor (Deprecated)

Important Notice

This sensor type is deprecated.

Monitoring of Microsoft SQL Server 2005 using PRTG is discontinued. It cannot be monitored with PRTG any more with the latest updates of SQL Server 2005. The reason for this is a software update delivered by Microsoft in August 2012. The following updates cause this issue:

- **Security Update for SQL Server 2005 Service Pack 4 (KB2716429)**
- **Security Update for SQL Server 2005 Service Pack 4 (KB2716427)**

We have made reasonable effort to fix this from our side but we were unable to. We do not have instructions to circumvent this issue at this time. Please ask the vendor to fix this.

More

Knowledge Base: Why does my WMI Microsoft SQL Server 2005 Sensor not work anymore?

- <http://www.paessler.com/knowledgebase/en/topic/44713>

The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL server via Windows Management Instrumentation (WMI). This sensor can monitor **SQL General Statistics**, **Access Methods**, the **Buffer Manager**, the **Memory Manager**, the **Locks Manager**, and **SQL Statistics**. The channels actually available for a sensor depend on which performance counters you choose during setup.

Channel Overview

User Connections	Number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.
Logins	Total number of logins started per second.
Logouts	Total number of logout operations started per second.
Full Scans	Number of unrestricted full scans per second. These can be either base-table or full-index scans.

Channel Overview	
Page Splits	Number of page splits per second that occur as the result of overflowing index pages.
Table Lock Escalations	Number of times locks on a table were escalated.
Buffer Cache Hit Ratio	Percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little. Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.
Database Pages	Number of pages in the buffer pool with database content.
Stolen Pages	Number of pages used for miscellaneous server purposes (including procedure cache).
Page Life Expectancy	Number of seconds a page will stay in the buffer pool without references.
Connection Memory (KB)	Total amount of dynamic memory the server is using for maintaining connections.
Optimizer Memory (KB)	Total amount of dynamic memory the server is using for query optimization.
Total Server Memory (KB)	Total amount of dynamic memory (in kilobytes) that the server is using currently.
Target Server Memory (KB)	Total amount of dynamic memory the server can consume.
SQL Cache Memory (KB)	Total amount of dynamic memory the server is using for the dynamic SQL cache.
Lock Requests	Number of new locks and lock conversions per second requested from the lock manager.
Deadlocks	Number of lock requests per second that resulted in a deadlock.
Average Wait Time	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait.

Channel Overview	
Batch Requests	Number of Transact-SQL command batches received per second. This statistic is affected by all constraints (such as I/O, number of users, cache size, complexity of requests, and so on). High batch requests mean good throughput.
SQL Compilations	Number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles due to recompiles. After SQL Server user activity is stable, this value reaches a steady state.
SQL Re-Compilations	Number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.

Note: This sensor can only be added to a device (computer) running a Microsoft SQL database.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

SQL Server Settings	
MS SQL Server Instance	You see a list of all server instances available on the device. Display name and service name are provided as returned by the SQL server. Please choose one or more instances by adding a check mark in front of the respective line. For each instance one sensor will be created.

SQL Server Settings	
SQL Server Version	Enter the version of the SQL server. Usually, you can keep the default value.
SQL Counter Specific	
SQL Performance Counters	You see a list of different performance counters which can be monitored for the instance(s) selected above. The sensors created for the server instances will all monitor the performance counter you select here. Choose from: ▪ General Statistics: Read general performance counters. This will show the number of user connections, and the number of logins and logouts per second. ▪ Access Methods: Read access method counters. This will show the number of full scans, page splits, and table lock escalations, per second. ▪ Buffer Manager: Read buffer manager counters. This will show the buffer cache hit ratio in percent, and the number of database pages and stolen pages. ▪ Memory Manager: Read memory manager counters. This will show the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory, in KB. ▪ Locks: Read locks counters. This will show the number of lock requests and deadlocks, per second, and the average wait time. ▪ SQL Statistics: Read SQL statistics. This will show the number of batch requests, SQL compilations, and SQL re-compilations, per second. Depending on your selection, a sensor with the specified channels will be created. Note: In order to monitor several performance counters for an instance, please add the sensor several times.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SQL Server Settings	
Service	Shows the service monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the server instance monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
WMI Class Name	Select whether PRTG will select the name of the WMI class used for monitoring automatically. Choose between: ▪ Automatic: Choose WMI class automatically. This is the recommended setting. ▪ Manual: Manually enter a WMI class name. Use this if your server instance returns an error code in automatic mode.
WMI Class	This field is only shown if manual WMI class selection is enabled above. This setting is intended for experienced users only. Enter the WMI class name that will be used for monitoring your server instance.
Sensor Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results.

SQL Server Settings

- **Write sensor result to disk (Filename: "Result of Sensor (ID).txt"):** Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see [Data Storage](#)^[2036] section.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[1683] settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[224] group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1689] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.196 WMI Microsoft SQL Server 2008 Sensor

The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL server via Windows Management Instrumentation (WMI). This sensor can monitor **SQL General Statistics**, **Access Methods**, the **Buffer Manager**, the **Memory Manager**, the **Locks Manager**, and **SQL Statistics**. The channels actually available for a sensor depend on which performance counters you choose during setup.

Channel Overview	
User Connections	Number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.
Logins	Total number of logins started per second.
Logouts	Total number of logout operations started per second.
Full Scans	Number of unrestricted full scans per second. These can be either base-table or full-index scans.
Page Splits	Number of page splits per second that occur as the result of overflowing index pages.
Table Lock Escalations	Number of times locks on a table were escalated.
Buffer Cache Hit Ratio	Percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little. Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.
Database Pages	Number of pages in the buffer pool with database content.
Stolen Pages	Number of pages used for miscellaneous server purposes (including procedure cache).
Page Life Expectancy	Number of seconds a page will stay in the buffer pool without references.
Connection Memory (KB)	Total amount of dynamic memory the server is using for maintaining connections.

Channel Overview	
Optimizer Memory (KB)	Total amount of dynamic memory the server is using for query optimization.
Total Server Memory (KB)	Total amount of dynamic memory (in kilobytes) that the server is using currently.
Target Server Memory (KB)	Total amount of dynamic memory the server can consume.
SQL Cache Memory (KB)	Total amount of dynamic memory the server is using for the dynamic SQL cache.
Lock Requests	Number of new locks and lock conversions per second requested from the lock manager.
Deadlocks	Number of lock requests per second that resulted in a deadlock.
Average Wait Time	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait.
Batch Requests	Number of Transact-SQL command batches received per second. This statistic is affected by all constraints (such as I/O, number of users, cache size, complexity of requests, and so on). High batch requests mean good throughput.
SQL Compilations	Number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles due to recompiles. After SQL Server user activity is stable, this value reaches a steady state.
SQL Re-Compilations	Number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.

Note: This sensor can only be added to a device (computer) running a Microsoft SQL database.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

SQL Server Settings	
MS SQL Server Instance	You see a list of all server instances available on the device. Display name and service name are provided as returned by the SQL server. Please choose one or more instances by adding a check mark in front of the respective line. For each instance one sensor will be created.
SQL Server Version	Enter the version of the SQL server. Usually, you can keep the default value.
SQL Counter Specific	
SQL Performance Counters	You see a list of different performance counters which can be monitored for the instance(s) selected above. The sensors created for the server instances will all monitor the performance counter you select here. Choose from: ▪ General Statistics: Read general performance counters. This will show the number of user connections, and the number of logins and logouts per second. ▪ Access Methods: Read access method counters. This will show the number of full scans, page splits, and table lock escalations, per second. ▪ Buffer Manager: Read buffer manager counters. This will show the buffer cache hit ratio in percent, and the number of database pages and stolen pages. ▪ Memory Manager: Read memory manager counters. This will show the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory, in KB. ▪ Locks: Read locks counters. This will show the number of lock requests and deadlocks, per second, and the average wait time. ▪ SQL Statistics: Read SQL statistics. This will show the number of batch requests, SQL compilations, and SQL re-compilations, per second.

SQL Counter Specific

Depending on your selection, a sensor with the specified channels will be created. **Note:** In order to monitor several performance counters for an instance, please add the sensor several times.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SQL Server Settings

Service	Shows the service monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the server instance monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
WMI Class Name	Select whether PRTG will select the name of the WMI class used for monitoring automatically. Choose between:

SQL Server Settings	
	▪ Automatic: Choose WMI class automatically. This is the recommended setting. ▪ Manual: Manually enter a WMI class name. Use this if your server instance returns an error code in automatic mode.
WMI Class	This field is only shown if manual WMI class selection is enabled above. This setting is intended for experienced users only. Enter the WMI class name that will be used for monitoring your server instance.
Sensor Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results. ▪ Write sensor result to disk (Filename: "Result of Sensor (ID).txt"): Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁸ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.197 WMI Microsoft SQL Server 2012 Sensor

The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL server via Windows Management Instrumentation (WMI). This sensor can monitor **SQL General Statistics**, **Access Methods**, the **Buffer Manager**, the **Memory Manager**, the **Locks Manager**, and **SQL Statistics**. The channels actually available for a sensor depend on which performance counters you choose during setup.

Channel Overview	
User Connections	Number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.
Logins	Total number of logins started per second.
Logouts	Total number of logout operations started per second.
Full Scans	Number of unrestricted full scans per second. These can be either base-table or full-index scans.
Page Splits	Number of page splits per second that occur as the result of overflowing index pages.
Table Lock Escalations	Number of times locks on a table were escalated.
Buffer Cache Hit Ratio	Percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little. Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.
Database Pages	Number of pages in the buffer pool with database content.
Stolen Pages	Number of pages used for miscellaneous server purposes (including procedure cache).
Page Life Expectancy	Number of seconds a page will stay in the buffer pool without references.
Connection Memory (KB)	Total amount of dynamic memory the server is using for maintaining connections.

Channel Overview	
Optimizer Memory (KB)	Total amount of dynamic memory the server is using for query optimization.
Total Server Memory (KB)	Total amount of dynamic memory (in kilobytes) that the server is using currently.
Target Server Memory (KB)	Total amount of dynamic memory the server can consume.
SQL Cache Memory (KB)	Total amount of dynamic memory the server is using for the dynamic SQL cache.
Lock Requests	Number of new locks and lock conversions per second requested from the lock manager.
Deadlocks	Number of lock requests per second that resulted in a deadlock.
Average Wait Time	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait.
Batch Requests	Number of Transact-SQL command batches received per second. This statistic is affected by all constraints (such as I/O, number of users, cache size, complexity of requests, and so on). High batch requests mean good throughput.
SQL Compilations	Number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles due to recompiles. After SQL Server user activity is stable, this value reaches a steady state.
SQL Re-Compilations	Number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.

Note: This sensor can only be added to a device (computer) running a Microsoft SQL database.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)²²⁰. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

SQL Server Settings	
MS SQL Server Instance	You see a list of all server instances available on the device. Display name and service name are provided as returned by the SQL server. Please choose one or more instances by adding a check mark in front of the respective line. For each instance one sensor will be created.
SQL Server Version	Enter the version of the SQL server. Usually, you can keep the default value.
SQL Counter Specific	
SQL Performance Counters	You see a list of different performance counters which can be monitored for the instance(s) selected above. The sensors created for the server instances will all monitor the performance counter you select here. Choose from: ▪ General Statistics: Read general performance counters. This will show the number of user connections, and the number of logins and logouts per second. ▪ Access Methods: Read access method counters. This will show the number of full scans, page splits, and table lock escalations, per second. ▪ Buffer Manager: Read buffer manager counters. This will show the buffer cache hit ratio in percent, and the number of database pages and stolen pages. ▪ Memory Manager: Read memory manager counters. This will show the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory, in KB. ▪ Locks: Read locks counters. This will show the number of lock requests and deadlocks, per second, and the average wait time. ▪ SQL Statistics: Read SQL statistics. This will show the number of batch requests, SQL compilations, and SQL re-compilations, per second.

SQL Counter Specific

Depending on your selection, a sensor with the specified channels will be created. **Note:** In order to monitor several performance counters for an instance, please add the sensor several times.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings

Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

SQL Server Settings

Service	Shows the service monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the server instance monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
WMI Class Name	Select whether PRTG will select the name of the WMI class used for monitoring automatically. Choose between:

SQL Server Settings	
	▪ Automatic: Choose WMI class automatically. This is the recommended setting. ▪ Manual: Manually enter a WMI class name. Use this if your server instance returns an error code in automatic mode.
WMI Class	This field is only shown if manual WMI class selection is enabled above. This setting is intended for experienced users only. Enter the WMI class name that will be used for monitoring your server instance.
Sensor Result	Define what will be done with the results the sensor receives. Choose between: ▪ Discard sensor result: Do not store the results. ▪ Write sensor result to disk (Filename: "Result of Sensor (ID).txt"): Store the last result received to the "Logs (Sensors)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁹ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.198 WMI Process Sensor

The WMI Process sensor monitors a Windows process using Windows Management Instrumentation (WMI). It shows the absolute working set and commit size, the number of threads and handles, as well as the average CPU usage (if there are multiple instances running) and the total CPU usage of the process.

For the "total CPU usage" value of a process, all CPU usage values are summed up. The total is divided by the number of all CPUs; the maximum value is 100%. This corresponds to the CPU usage of all instances of this specific process. Regarding the "per instance" value, the summed up CPU usage value is divided by the number of all instances. It shows the average CPU usage of a single instance of the process on one CPU.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Process Monitor

Executable	Enter the name of the process that will be monitored. Please enter the name of an executable file without the .exe extension. The sensor will be set to an error state if the process is not active on the device.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings 1683 settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.199 WMI Remote Ping Sensor

The WMI Remote Ping sensor connects remotely to a Windows system using Windows Management Instrumentation (WMI), then performs an Internet Control Message Protocol (ICMP) echo request ("Ping") from this device to a specified target. The sensor shows the Ping time from the remote device to the target device that is being pinged.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Remote Ping Configuration	
Target	Enter the DNS name or IP address of the target device the Ping is sent to. The sensor will remotely connect to the parent device it is created on via WMI, then perform a Ping request from this remote device to the target device/server. Please enter a string.
Timeout (Seconds)	Enter a timeout in seconds for the Ping. If the reply takes longer than this value the request is aborted and an error message is triggered. Please enter an integer value. The maximum is 300.
Packet Size (Bytes)	Enter the packet size in bytes for the Ping. You can choose any value between 1 and 10000. Please enter an integer value. We recommend using the default value.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1680] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.200 WMI Security Center Sensor

The WMI Security Center sensor monitors the security status of a Windows computer using Windows Management Instrumentation (WMI). It can monitor all security products that are controlled by Windows Security Center / Windows Action Center. It returns a status code of the monitored product and sets the sensor status to **Warning** if a product status is unknown, if it is reported as out of date, or if the access scan is disabled. A sensor status showing **Up** indicates that the product is up to date and the access scan is running.

Possible return values for status codes are:

Status Code	Meaning: Status of Monitored Security Product Is ...	Will Result in Sensor Status
0	Unknown	Warning
1	Not running, Out of date	Warning
2	Running, Out of date	Warning
3	Not running, Up to date	Warning
4	Running, Up to date	OK

Note: This sensor requires Windows XP SP2 or later on the target computer. The Windows Security Center / Windows Action Center is only available on client Windows versions.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Security Center Specific**Security Center Products**

You see a list showing the **Name** and **Type** of all security products found in the Windows Security Center on the target device. If there are no products, you will see a corresponding message. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings**Sensor Name**

Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.

Tags

Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically [inherited](#)^[89] from objects further up in the device tree. Those are not visible here.

Priority

Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Security Center Specific**Display Name**

Shows the name of the product monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Type

Shows the type of the product monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

WMI Security Center Specific

If Value Changes	Define what will be done in case the value of this sensor changes. You can choose between: • Ignore changes: No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification¹⁶⁹⁰ whenever the sensor value changes.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window

	▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁸ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.201 WMI Service Sensor

The WMI Service sensor monitors a Windows service using Windows Management Instrumentation (WMI). It shows the execution time of the monitoring request. Additionally, it can show CPU and pagefile usage, the number of handles and threads, and the working set of the monitored service. You can monitor these channels if you enable **Monitor extended values** in the sensor settings.

Note: The "Running (msec)" channel of this sensor shows the execution time of the monitoring request. It does **not** refer to the time the Windows service has been running! As of PRTG version 13, the name of this sensor channel is **Sensor Execution Time**.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

If you select more than one service multiple sensors are created at once in the **Add Sensor** dialog.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Service Monitor	
Service	A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head. Name and description are provided in the language of the device's Windows installation. Later on, a sensor's status will be set to Down if the service is not running.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).
WMI Service Monitor	
If Service is Not Running	Select whether the service will be (re-)started if it is stopped or paused. Choose between: ▪ Start/Restart service (default): PRTG will try to start the service if it is not running when scanning the device. ▪ Do nothing: PRTG will not start any service on the device automatically.
Monitoring	Select whether you want to monitor CPU usage and other useful performance counters. This may cause a "Class not found" error on some Windows systems. If you do not monitor these counters, the value '0' is returned for these channels. Choose between: ▪ Just check if services is running: PRTG will only monitor the channel "Sensor Execution Time". ▪ Monitor extended values: PRTG will monitor also other useful performance counters.
Service	Shows the Windows service this sensor will monitor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

WMI Service Monitor	
Description	Shows the description for the service. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the "Logs (Sensor)" directory (on the Master node, if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage ²⁰³⁶ section.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸⁵ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Schedules, Dependencies, and Maintenance Window

Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1688] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.202 WMI Share Sensor

The WMI Share sensor monitors a shared resource on a Windows system using Windows Management Instrumentation (WMI). It shows the availability; you can set a sensor to **Down** status for different share status messages.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[202] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

If you select more than one share multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Shared Resource	
Share	Select the shares you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head. Note: In order to provide any shares, the LanmanServer "Server" Windows service must be running on the target computer. If it is not, there are no shares and you will see a No Share available message here.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Shared Resource	
Shared Resource	Shows information about the shared resource monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	
Type	
TypeID	

Trigger Errorstate on following conditions	
Select under which conditions the sensor will change to a Down status from the list below. As long as the share returns OK, the sensor status will be Up . Choose a Down condition by adding a check mark symbol in front of the according line. Please choose none, one, or several from the following conditions. Note: While in Down status, a sensor does not record any data in all of its channels.	
Error	Set sensor to Down status if the share returns an error status. A share in this status is not operational.
Degraded	Set sensor to Down status if the share returns a degraded status. A share in this status is still operational.
Unknown	Set sensor to Down status if the share returns an unknown status.

Trigger Errorstate on following conditions	
Pred Fail	Set sensor to Down status if the share returns a "predicted fail" status. This indicates that an element is functioning properly but is predicting a failure (for example, a SMART-enabled hard drive). A share in this status is still operational.
Starting	Set sensor to Down status if the share returns a starting status. A share in this status is not operational.
Stopping	Set sensor to Down status if the share returns a stopping status. A share in this status is not operational.
Service	Set sensor to Down status if the share returns a service status. This can apply during disk mirror-resilvering, reloading a user permissions list, or other administrative work on the monitored device. Not all such work is online, but the managed element is neither OK nor in one of the other states. A share in this status is not operational.
Stressed	Set sensor to Down status if the share returns a stressed status.
Nonrecover	Set sensor to Down status if the share returns a "non recover" status.
NoContact	Set sensor to Down status if the share returns a "no contact" status.
LostComm	Set sensor to Down status if the share returns "lost communication" status.
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel.

Sensor Display	
	▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹³ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1629] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.203 WMI SharePoint Process Sensor

The WMI SharePoint Process sensor monitors a Microsoft SharePoint server using Windows Management Instrumentation (WMI). It shows the number of current page requests, active threads, and SQL queries currently executed, as well as global heap size, object cache always live size, template cache size, and CPU utilization.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

If you select more than one SharePoint process, multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Process Monitor	
SharePoint Processes	You see a list of all SharePoint processes running on this device. There is also a "_Total" process available. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ¹⁶⁸⁹ from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Process Monitor	
SharePoint Process	The name of the SharePoint process that is monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.204 WMI Terminal Services (Windows 2008) Sensor

The WMI Terminal Services sensor monitors the number of sessions on a Windows Terminal Services (Remote Desktop Services) server using Windows Management Instrumentation (WMI). It shows the number of active and total sessions. Active sessions are sessions with a currently logged in user; inactive sessions (included in total) can be sessions with a disconnected user that has not logged out, or system services using a session. **Note:** As "Total Sessions", this sensor type will return the number of the active sessions, plus two additional sessions: one for the console, and another for the services. So, the number of total sessions may actually be higher than expected.

Note: Depending on the OS that will be monitored, please select either the sensor for Windows XP/Vista/2003 or the one for Windows 2008.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration settings.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁹ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.205 WMI Terminal Services (Windows XP/Vista/2003) Sensor

The WMI Terminal Services sensor monitors the number of sessions on a Windows Terminal Services (Remote Desktop Services) server using Windows Management Instrumentation (WMI). It shows the number of active and total sessions. Active sessions are sessions with a currently logged in user; inactive sessions (included in total) can be sessions with a disconnected user that has not logged out, or system services using a session. **Note:** As "Total Sessions", this sensor type will return the number of the active sessions, plus two additional sessions: one for the console, and another for the services. So, the number of total sessions may actually be higher than expected.

Note: Depending on the OS that will be monitored, please select either the sensor for Windows XP/Vista/2003 or the one for Windows 2008.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.

Basic Sensor Settings

Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration settings.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸⁰ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.206 WMI UTC Time Sensor

The WMI UTC Time sensor monitors the UTC time of a target device using Windows Management Instrumentation (WMI). It shows the UTC time of the target device, and the time difference between the PRTG system time and the target device, in seconds.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.8.207 WMI Vital System Data (V2) Sensor

The WMI Vital System Data sensor monitors vital system parameters (CPU, system, memory, disk, network, pagefile, etc.) using Windows Management Instrumentation (WMI).

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

Vital System Data Readings Accessible Using WMI

Performance Counter

You see a list of available vital system data values the sensor can monitor on the target device. The available options depend on your configuration. PRTG shows all possible performance counters with name and instance description (if available). Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

You can choose between the following counters:

- CPU
- Thread
- Memory
- Network
- Pagefile

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
Counter	These fields show the parameters that are used to query data for this sensor from the target device. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Instance	
WMI Class	
Datafield	
Basefield	
Frequencyfield	
Countertype	
Sensor Result	Define what will be done with the result of the sensor. Choose between: ▪ Discard sensor result: Do not store the results. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received to the "Logs (System)" directory (on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. For information on how to find the folder used for storage, please see Data Storage^[2036] section.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	

Schedules, Dependencies, and Maintenance Window	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency.

Schedules, Dependencies, and Maintenance Window	
	Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups^[1829] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights^[94].

Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.208 WMI Volume Sensor

The WMI Volume sensor monitors the free disk space on one drive or one logical volume using Windows Management Instrumentation (WMI). It shows the space in percent and total. For each drive or logical volume, one sensor is used.

This sensor monitors an area of storage on a hard disk. It can monitor local volumes that are formatted, unformatted, mounted, or offline. A volume is formatted by using a file system, such as File Allocation Table (FAT) or New Technology File System (NTFS), and might have a drive letter assigned to it. One hard disk can have multiple volumes, and volumes can span multiple physical disks. The sensor does not support disk drive management.

Note: This sensor is not supported on Windows XP and earlier.

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[226]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

For devices with multiple volumes multiple sensors are created at once in the **Add Sensor** dialog. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Volume Specific	
Volumes	Select the volume(s) you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Volume Specific	
DeviceID	Shows the id of the volume that this sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Drive Type	Shows the type of the drive the sensor is monitoring. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Timeout (sec)	Enter a timeout in seconds for the WMI request. If the reply takes longer than this value the request is aborted and an error message is triggered.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor.

Sensor Display	
	▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings¹⁶⁸³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval	
Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .
Schedules, Dependencies, and Maintenance Window	
Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.	
Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹² . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Schedules, Dependencies, and Maintenance Window	
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ¹⁵⁸ to choose an object on which the current sensor will be dependent on.

Schedules, Dependencies, and Maintenance Window**Delay (Seconds)**

Define a time span. After the master object for this dependency comes back to an **Up** status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. **Note:** This setting is not available if you choose this sensor to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[272] or the superior [Group Settings](#)^[253].

Access Rights**User Group Access**

Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[1029] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

For more details about access rights, please see section [User Access Rights](#)^[94].

Channel Unit Configuration

Channel Unit Types

For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴¹ section.

6.8.209 WMI Volume Fragmentation Sensor

The WMI Volume Fragmentation sensor monitors the fragmentation of a logical volume via Windows Management Instrumentation (WMI). It can show if a defragmentation is recommended on the volume, the number of average fragments per file, the number of excess fragments in total, the number of fragmented files in total, and file fragmentation in percent.

Note: This sensor is not supported on Windows XP and earlier.

This sensor type uses lookups to determine the status values of some sensor channels. For details, please see section [Define Lookups](#)^[2001].

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[1927] section.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 4.0 (with latest update).

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

In order to monitor fragmentation on volumes, PRTG will create one sensor for each volume you choose. The settings you make in this dialog are valid for all of the sensors that are created.

The following settings for this sensor differ in the 'Add Sensor' dialog in comparison to the sensor's settings page:

WMI Volume Specific	
Volume	Select one or more volumes you want to add a sensor for. A list of all available items is shown with their name. Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

WMI Volume Specific	
DeviceID	Shows the unique identifier of the volume monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Drive Type	Shows the type of the disk drive monitored by this sensor. Once a sensor is created this value cannot be changed. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
ID Selection	Specify the way the volume is identified. Choose between: ▪ Use system device ID (recommended): This is usually the best option for this sensor type, because the device ID will not change when the volume is renamed. ▪ Use drive letter: In a Microsoft cluster environment, the device ID will change when the cluster is switched to another node. In this case, use the drive letter option to avoid issues regarding this.
Drive Letter	This field is only visible when the drive letter option is selected above. Enter the letter of the drive you want to monitor followed by a trailing colon, for example, C: .
Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.210 WMI Windows Version Sensor

The WMI Windows Version sensor reads the Windows version of the parent device via Windows Management Instrumentation (WMI). It returns the version number (in a channel) as well as the according version name (in the sensor message).

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[202]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 2.0.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Note: Your Windows credentials may not contain any double quotation marks ("). If they do, this sensor will not work!

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
If Value Changes	Define what will be done in case the value of this sensor changes. You can choose between: • Ignore changes (default): No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.

Sensor Display	
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).

Sensor Display**Stack Unit**

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval**Scanning Interval**

The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the [system administration](#)¹⁸⁰⁵.

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)¹⁷⁹¹. **Note:** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window

Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

Schedules, Dependencies, and Maintenance Window	
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent . In this case, please define delays in the parent Device Settings ^[272] or the superior Group Settings ^[253] .

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)¹⁶⁸³ section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)¹⁶⁹⁰ section.

Others

For more general information about settings, please see [Object Settings](#)¹⁴⁴¹ section.

6.8.211 WSUS Statistics Sensor

The WSUS Statistics sensor monitors various statistics on a Windows Server Update Services (WSUS) server using Windows Management Instrumentation (WMI).

It can show the number of: Approved updates, computers having update errors, computers needing updates, computers not synchronized for 7 days, computers registered, computers up to date, declined updates, expired updates, not approved critical or security updates, not approved updates, total updates, unapproved needed updates, updates needed by computers, updates needing files, updates up to date, updates with client errors, updates with server errors, updates with stale update approvals, and the number of WSUS infrastructure updates not approved for installation.

Note: This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend using not more than 50 sensors, on each probe, of this type of sensor.

Requirement: .NET Framework

This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[2012]. If the framework is missing, you cannot create this sensor. **Note:** You need to install the exact version required (a higher version will usually not work; an exception applies to .NET 3.5 which comprises .NET 2.0 and .NET 3.0). Generally, it is possible to run several .NET Framework versions on the same machine side-by-side. Please install the latest update available for the required version.

Required **.NET** version: 2.0.

Requirement: Windows Credentials

For this sensor type credentials for Windows systems must be defined for the device you want to use the sensor on. In the [parent device's](#)^[276] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

Note: If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Note: Your Windows credentials may not contain any double quotation marks ("). If they do, this sensor will not work!

Requirement: WSUS 3.0 Administration Console

In order for this sensor to work, Microsoft's **WSUS 3.0 Administration Console** must be installed on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the remote probe.

Add Sensor

The **Add Sensor** dialog appears when adding a new sensor on a device [manually](#)^[220]. It only shows the setting fields that are imperative for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change all settings in the sensor's **Settings** tab later.

Sensor Settings

On the sensor's details page, click on the **Settings** tab to change settings.

Note: If not set explicitly in a sensor's settings, it will connect to the **IP Address** or **DNS Name** defined in the settings of the parent device the sensor is created on.

Basic Sensor Settings	
Sensor Name	Enter a meaningful name to identify the sensor. The name will be shown by default in the device tree and in all alarms.
Tags	Enter one or more tags, separated by space or comma. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend using the default value. You can add additional tags to it, if you like. Other tags are automatically inherited ^[89] from objects further up in the device tree. Those are not visible here.
Priority	Select a priority for the sensor. This setting determines where the sensor will be placed in sensor lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Sensor Settings	
WSUS Server Port	Define the port where the WSUS server service is running on. Default value is 80 . Please enter an integer value.
Use SSL	Define if SSL-encryption will be used for the connection to the WSUS server. Choose between: ▪ Yes ▪ No
If Value Changes	Define what will be done in case the value of this sensor changes. You can choose between: • Ignore changes: No action will be taken on change.

Sensor Settings

- **Trigger 'change' notification:** The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#) ¹⁶⁹⁰ whenever the sensor value changes.

Sensor Display

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor. Note: You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.
Chart Type	Define how different channels will be shown for this sensor. ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph which visualizes the different components of your total traffic. Note: This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings ¹⁶⁹³ settings).
Stack Unit	This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) ²²⁴ group's settings. To change a setting for this object, disable inheritance by clicking on the check mark symbol in front of the respective setting name. You will then see the options described below.

Scanning Interval

Scanning Interval	The scanning interval determines the time the sensor waits between two scans. Select a scanning interval (seconds, minutes, or hours) from the list. You can change the available intervals in the system administration ¹⁸⁰⁵ .

Schedules, Dependencies, and Maintenance Window

Note: Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) throughout the week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ¹⁷⁹¹ . Note: Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.
Maintenance Window	Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between: ▪ Not set (monitor continuously): No maintenance window will be set. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window.
Maintenance Begins At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance End At	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between: ▪ Use parent: Pause the current sensor if the device it is created on is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current sensor if the device it is created on is in an Down status, or if it is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below.

Schedules, Dependencies, and Maintenance Window

	▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device it is created on: If the sensor is in a Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in a Down status, or if it is paused by another dependency. Note: Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused.
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector^[158] to choose an object on which the current sensor will be dependent on.
Delay (Seconds)	Define a time span. After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value in seconds. Note: This setting is not available if you choose this sensor to be the Master object for parent. In this case, please define delays in the parent Device Settings^[272] or the superior Group Settings^[253].

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights.
Channel Unit Configuration	
Channel Unit Types	For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available): ▪ Bandwidth ▪ Memory ▪ Disk ▪ File ▪ Custom Note: Custom channel types can be set on sensor level only.

Edit Sensor Channels

In order to change display settings, spike filter, and limits, please switch to the sensor's **Overview** tab and click on the gear icon of a specific channel. For detailed information, please see [Sensor Channels Settings](#)^[1683] section.

Notifications

Click on the **Notifications** tab to change notification triggers. For detailed information, please see [Sensor Notifications Settings](#)^[1690] section.

Others

For more general information about settings, please see [Object Settings](#)^[141] section.

6.9 Additional Sensor Types (Custom Sensors)

Users can create and use their own, self-written custom sensors in PRTG Network Monitor to go far beyond PRTG's standard sensor set. You can create your own sensors using Windows Management Instrumentation Query Language (WQL), visual basic scripting, PowerShell, batch scripting, and by compiling an EXE or DLL file (using any Windows software development tool).

Basics

For a general introduction, please see the sections about EXE/Script sensors and the API documentation which contains details about the necessary return format for those sensors. WMI Custom sensors allow executing WQL requests.

- [EXE/Script Sensor](#) 430
- [EXE/Script Advanced Sensor](#) 439
- [SSH Script Sensor](#) 1315
- [Application Programming Interface \(API\) Definition](#) 1993
- [WMI Custom Sensor](#) 1503

Custom Sensors Included in PRTG

After installing PRTG Network Monitor you will already find a selection of custom EXE/Script and WMI WQL script sensors in the [PRTG program directory](#) 2036. Many of these are sample projects that you can edit and improve for your needs.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\EXE

- Demo Batchfile - Returns 200.bat
- Demo Batchfile - Set sensorstate to error.bat
- Demo Batchfile - Set sensorstate to warning.bat
- Demo Cmd - Returns 200.cmd
- Demo Dll - Returns a random integer.dll
- Demo EXE - Returns a random integer.exe
- Demo EXE - Returns number of files in folder (parameter).exe
- Demo EXE - Returns user of process.exe
- Demo Powershell Script - Available MB via WMI.ps1
- Demo Powershell Script - InterruptsPerSec via WMI.ps1
- Demo Powershell Script - Returns a fixed integer value.ps1
- Demo Powershell Script - Returns a random integer value.ps1
- Demo Powershell Script - Returns Random Integer and Warnings.ps1

- Demo VBScript - InterruptsPerSec via WMI.vbs
- Demo VBScript - Multiplies two integers(2 parameters).vbs
- Demo VBScript - Returns a fixed float value.vbs
- Demo VBScript - Returns a fixed integer value.vbs
- Demo VBScript - Returns a random value.vbs
- Demo VBScript - Returns number of svchost processes.vbs
- Demo VBScript - Returns user of process.vbs
- Demo VBScript - Returns warning depending on number of svchost processes.vbs
- Demo VBScript - Timezone via WMI.vbs
- Demo VBScript - UTCTime via WMI.vbs
- Load_Test_CPU_1_Mio_Primes.exe
- Load_Test_CPU_10_Mio_Primes.exe
- Load_Test_Disk_Write_Read_1000_files.exe
- Load_Test_Disk_Write_Read_10000_files.exe
- Load_Test_Memory_Allocate_And_Free_400MB.exe

To create a new sensor based on one of these files, create a new [EXE/Script Sensor](#)⁴³⁰ and choose the respective file from the drop down list.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\EXEXML

- Demo Batchfile - Returns static values in four channels.bat

To create a new sensor based on one of these files, create a new [EXE/Script Advanced Sensor](#)⁴³⁹ and choose the respective file from the drop down list.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\WMI WQL scripts

- Demo WQL Script - Get Win32LogicalDiscFreeMB.wql
- Demo WQL Script - Get Win32OsBuildnumber.wql
- Demo WQL Script - Get Win32PercentProcessorIdleTime.wql
- Demo WQL Script - Get Win32PercentProcessorTime.wql

To create a new sensor based on one of these files, create a new [WMI Custom Sensor](#)¹⁵⁰³ and choose the respective file from the drop down list.

Downloading Pre-Build Custom Sensors

A good resource is the PRTG Add-Ons website on the open source platform [Google Code](#). There are also additional tools available.

Open Source Add-Ons for PRTG Network Monitor

- <http://code.google.com/p/prtg-addons/>

More

For the other sensor types that work out-of-the-box, please see

- [List of Available Sensor Types](#) 

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- <http://www.paessler.com/knowledgebase/en/topic/11283>

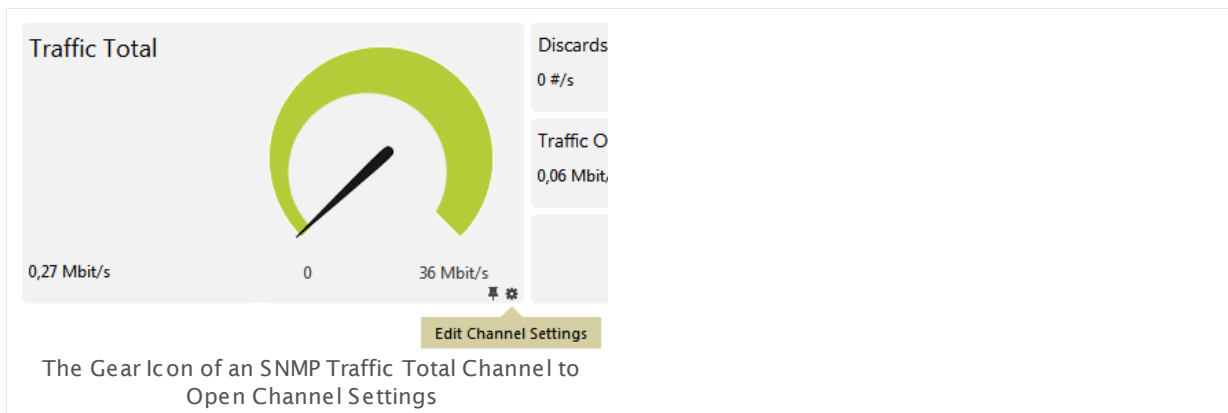
6.10 Sensor Channels Settings

A sensor has one or more channels in which it handles the actual monitoring data. In the channel settings you can define how the data from the sensor's different channels will be displayed in graphs, gauges, and tables. Additionally, the channel data can determine the sensor's status. Use the limit settings to achieve this.

On the sensor's **Overview** page, click on the gear icon of a specific channel gauge to change its settings. A click on the pin symbol on the left of the gear icon in a gauge will make this channel the primary channel of the selected sensor.

You can alternatively call the settings of a channel by clicking on the respective gear icon in the channels data table underneath the gauges.

Note: For [lookup](#) channels, we recommend staying below 120 lookup values to get expressive gauges. For non-primary lookup channels, the upper limit is around 40 lookup values.



The available options are nearly the same for all sensor types. An exception applies to the "Downtime" channel which is automatically calculated and does not offer all settings. Channels with "absolute" values additionally have an option for defining the **Value Mode**. You can quickly choose another channel of the selected sensor via the dropdown list on the top of the settings dialog.

Part 6: Ajax Web Interface—Device and Sensor Setup | 10 Sensor Channels Settings

Edit Channel

Traffic Total (ID -1)

Name

Traffic Total

ID

-1

Chart Rendering

☒ Show in Charts
☐ Hide from Charts

Table Rendering

☒ Show in Tables
☐ Hide from Tables

Line Color

☒ Automatic
☐ Manual

Line Width

1

Data

☒ Display actual values in Mbit/s
☐ Display in percent of maximum

Decimal Places

☒ Automatic
☐ All
☐ Custom

Vertical Axis Scaling

☒ Automatic Scaling
☐ Manual Scaling

Limits

☐ Disable Limits
☒ Enable Limits

Upper Error Limit (Mbit/s)

20

Upper Warning Limit (Mbit/s)

15

Lower Warning Limit (Mbit/s)

Lower Error Limit (Mbit/s)

Error Limit Message

Warning Limit Message

Save

Cancel

Channel Settings for an SNMP Traffic Sensor

Available Channel Settings

Edit Channel "[Name]"	
Name	Enter a meaningful name to identify the channel (not editable for script sensors after sensor creation). The name will be shown in graphs and tables. You can automatically add the sensor's ID to the name by using the placeholder [#id] .
Unit	This field is only visible for script sensors, the SNMP Custom sensor, and the SNMP Library sensor. Enter a string describing the unit of the returned values. This is for display purposes only. Please enter a string.

Edit Channel "[Name]"	
Value Lookup	This field is only visible for script sensors, the SNMP Custom sensor, and the SNMP Library sensor. Select the lookup list to be applied to this channel's settings.
ID	The ID of the channel cannot be changed; it is used for unique definition. For example, you need the ID when using Sensor Factory ⁸³⁷ sensors.
Display	Define where the channel will be displayed. Choose from: ▪ Show in Charts: The data of this channel will be shown in sensor graphs. Note: If you hide a channel here, it will also be hidden if this graph is used in a Report ¹⁷⁴⁹. ▪ Show in Tables: The data of this channel will be shown in sensor data tables. Note: If you hide a channel here, it will not be considered for the calculation of the "sum" (total) channel of this sensor! To change this setting, remove or add the check mark symbol in front of it.
Line Color	Define in what color the channel will be displayed in graphs. You can choose between ▪ Automatic ▪ Manual When you set this option to manual color definition please enter a color below.
Color (#rrggbb)	This option is only available if Manual is selected in the Line Color setting above. Please either enter a color in hexadecimal RGB notation (as in HTML/CSS), or choose a color from the visual color selector. The field containing the hexadecimal color value will change to the resulting color immediately in both cases.
Data	This setting is available for most channels. Define how data will be displayed. Choose between: ▪ Display actual values in [unit]: Display the values in the unit shown. ▪ Display in percent of maximum: Calculate and show percent values based on a maximum value. Provide a maximum below.
Maximum ([unit])	This field is only visible if the percent of maximum setting is selected above. Enter a value that will be regarded as maximum. Please pay attention to the given unit. All percent values will be calculated based on this value. Please enter an integer value.

Edit Channel "[Name]"	
Line Width	Define in what color the channel will be displayed in graphs. Enter an integer value in pixels. Although the line width is not limited, we recommend using values between 1 and 7 only in order to achieve optimal results.
Value Mode	This setting is only available for sensor channels which return absolute values. It is not available for sensors showing difference values, such as traffic sensors. Depending on this setting, the channel can not only show averages, but also minimum or maximum values in the graphs for the respective time spans. For example, in a 5 minutes graph, you can display maximum/minimum values within this time interval instead of the average. Choose between: ▪ Average: The channel shows average values. ▪ Minimum: The channel shows minimum values. ▪ Maximum: The channel shows maximum values.
Decimal Places	Define how many decimal places of the channel's data will be displayed in graphs and tables. Choose between: ▪ Automatic: Let PRTG choose how many decimal places will be used for optimal viewing results. ▪ All: Force display of all available decimal places. ▪ Custom: Manually define the number of decimal places. If you choose this option, an additional field will appear. Please enter an integer value there.
Spike Filter	A spike filter can be used to correct obviously faulty monitoring data. Sometimes, sensors report enormously high or far too low values; due to an error in data transmission, or due to incompatibilities of the physical device you are monitoring. This can make graphs unreadable. A spike filter can compensate for these flaws. When enabled values above and below a certain limit are disregarded in the monitoring data for graphs and tables. Note: The monitoring data itself will not be changed (but only the presentation of the data) and this setting is valid for all data of this channel (also the historic data). Choose between: ▪ Disable Filtering: Display all data as it is; do not filter out spikes. ▪ Enable Filtering: Enable a filter to remove spike values. Additional fields appear below. Note: The spike filter option is not available for the channel Downtime.

Edit Channel "[Name]"	
Spike Filter Max. Value [unit]	This field is only visible if spike filter is enabled above. Specify the maximum value allowed in the channel's data. All values above this value will be disregarded in graphs and tables. Please enter an integer value or leave the field empty.
Spike Filter Min. Value [unit]	This field is only visible if spike filter is enabled above. Specify the minimum value allowed in the channel's data. All values below this value will be disregarded in graphs and tables. Please enter an integer value or leave the field empty.
Vertical Axis Scaling	Define how the vertical axis for the channel is displayed in graphs. Choose between: ▪ Automatic Scaling: Let PRTG decide on the optimum scaling; usually ranging from the minimum to the maximum value. PRTG will use one single scale for each unit label only. ▪ Manual Scaling: Define the scaling manually. Additional fields appear below. Defining manual axis scaling can make low values better visible in your graph; but it may result in a chart with multiple vertical axis for the same unit label. Note: Settings for this option are ignored if Chart Type Stack channels on top of each other or Show in and out traffic as positive and negative area chart (available for traffic sensors) is enabled in the sensor's Settings tab.
Vertical Axis Maximum [unit]	This field is only visible if vertical axis scaling is enabled above. Specify the maximum value that will be used on the vertical axis for the channel. Enter an integer value.
Vertical Axis Minimum [unit]	This field is only visible if vertical axis scaling is enabled above. Specify the minimum value that will be used on the vertical axis for the channel. Enter an integer value.
Limits	The channel can affect the status of the sensor it is part of. By entering limits, you can define when the sensor will enter a Warning or Down status; depending on the channel's data. Using this function, you can e.g. set a traffic sensor (which is usually never in a down state) to error when certain limits that you consider critical are reached. Choose between: ▪ Disable Limits: Do not use the channel's data to control the sensor's status. ▪ Enable Limits: Define limits. Additional fields appear below. The sensor belonging to the channel will enter a Warning or Down status when limits are undercut or overrun.

Edit Channel "[Name]"	
	Note: The limits option is not available for the channel "Downtime". Note: If a channel uses lookups^[200], we strongly recommend you to control the sensor status only via the lookup definition. If you define limits in addition here, the sensor will use both the channel limits and the status as defined in the lookup file. In this case, channel limits will determine the overall status of the sensor and overwrite the sensor message while the channel gauge still shows the status as defined in the lookups.
Upper Error Limit [unit]	This field is only visible if limits are enabled above. Specify an upper limit for an error state. If the channel's values overrun this value, the sensor will be set to Down . Note: While a sensor shows a Down ^[121] status triggered by a limit, it will still receive data in its channels. Please enter a decimal value or leave the field empty.
Upper Warning Limit [unit]	This field is only visible if limits are enabled above. Specify an upper limit for a warning state. If the channel's values overrun this value, the sensor will be set to Warning . Please enter a decimal value or leave the field empty.
Lower Warning Limit [unit]	This field is only visible if limits are enabled above. Specify a lower limit for a warning state. If the channel's values undercut this value, the sensor will be set to Warning . Please enter a decimal value or leave the field empty.
Lower Error Limit [unit]	This field is only visible if limits are enabled above. Specify a lower limit for an error state. If the channel's values undercut this value, the sensor will be set to Down . Note: While a sensor shows a Down ^[121] status triggered by a limit, it will still receive data in its channels. Please enter a decimal value or leave the field empty.
Error Limit Message	This field is only visible if limits are enabled above. Enter an additional message. It will be added to the sensor's message when entering a Down status. Please enter a string or leave the field empty.
Warning Limit Message	This field is only visible if limits are enabled above. Enter an additional message. It will be added to the sensor's message when entering a Warning status. Please enter a string or leave the field empty.

Click on **Save** to store your settings or **Cancel** your changes.

Sensor Settings Overview

For information about sensor settings, please see the following sections:

- [Sensor Settings](#)  290
- [List of Available Sensor Types](#)  291
- [Additional Sensor Types \(Custom Sensors\)](#)  1680
- [Sensor Channels Settings](#)  1683
- [Sensor Notifications Settings](#)  1690

6.11 Sensor Notifications Settings

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to your needs.

The screenshot shows the PRTG Network Monitor interface for configuring a sensor's notifications. The sensor is 'WMI Free Disk Space (Multi Disk) 4'. The 'Notifications' tab is selected, showing a table of triggers that can be inherited from parent objects. Below this, there are triggers defined in the library object. At the bottom, the 'Object Triggers' section shows a threshold trigger for free space. The interface includes a top navigation bar with links like Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. A status bar at the top right shows 'New Log Entries' and various status icons. The footer contains the PRTG Network Monitor version (13.4.9.3728) and copyright information (© 2013 Paessler AG).

Example of Notification Trigger Settings

Note: Although the sensors activate a trigger, you can set notification triggers higher in the hierarchy (for example for groups or devices), thus defining triggers for multiple sensors using the [inheritance mechanism](#)^[87].

Note

This section describes one of three steps to set up the notification system in PRTG. A complete notification setup involves:

1. Check and set up the **Notification Delivery** settings. This will tell PRTG how to send messages.
For detailed information, see [System Administration—Notification Delivery](#)^[1815].
2. Check and set up several **Notifications**. This will define the kind of message and its content.
For detailed information, see [Account Settings—Notifications](#)^[1791].
3. Check and set up **Notification Triggers** for objects. These will provoke the defined notifications.
For detailed information, see [Sensor Notifications Settings](#)^[1690].

For background information, please see [Notifications](#)^[1723] section.

Available Notification Triggers Settings

On an object's detail page, click on the **Notifications** tab to change sensor notification triggers. The available options are the same for all objects. When defining triggers for probes, groups, or devices, they can be inherited down to sensor level.

Triggers that can be inherited from parent object(s)

You see a list of all notification triggers that are defined higher in the hierarchy. The list is empty when there are no triggers defined in groups or devices above the current object. You can see the type and the notifications that are executed once this trigger is activated.

Trigger Inheritance

Define whether the triggers shown above will be handed on to the current object. Choose between:

- **Inherit trigger(s) from parent object(s):** Use the triggers shown above.
- **Only use triggers defined for this object:** Do not use the triggers shown above; for this object only use the triggers defined below.

This setting is valid for all triggers shown above. It is not possible to only select some of them.

You can set up one or more of the following triggers, each with different setting options. Which trigger types will be visible depends on the kind of object you're editing:

- [Add State Trigger](#)  1691
- [Add Speed Trigger](#)  1693
- [Add Volume Trigger](#)  1695
- [Add Threshold Trigger](#)  1696
- [Add Change Trigger](#)  1698

All notification triggers can be created in a very easy way, forming natural sentences. There are different options for every type.

Add State Trigger

Define a trigger that is activated when a sensor changes its current status. This is the most common reason to send out notifications. Click on the **Add State Trigger** button to add a new trigger, or click on the **Edit** button next to an existing notification to change it. Then define settings as described below. Every trigger will provoke one or more [notification\(s\)](#)  1791 to be executed.

State Trigger	
When sensor is...	Select the condition that will trigger the notification. The trigger will be activated when a sensor enters the selected status. Choose from the drop down menu: ▪ Down: The trigger will be prompted if a sensor changes to a Down status. ▪ Warning: The trigger will be prompted if a sensor changes to a Warning status. ▪ Unusual: The trigger will be prompted if a sensor changes to an Unusual status. ▪ Partial Down: The trigger will be prompted if a sensor changes to a Down (Partial) status (available in a cluster^[81] configuration).
...for at least ... seconds	Define how many seconds will be waited before a notification is provoked. This can avoid false alarms in case a sensor 'flickers' and, for example, changes to a down status for just a few seconds. If the selected condition (i.e. the sensor status) persists after the defined time in seconds, the notification will be triggered. Please enter an integer value.
...perform...	Select a notification that will be triggered if the condition (i.e. the sensor status) selected is true and the latency time defined has elapsed. Choose a notification from the drop down menu. The menu shows all notifications defined in the Account Settings—Notifications^[1791] settings. You can also choose no notification in order to only use other conditions for this trigger.
When condition continues for at least ... seconds	Define an escalation latency in seconds. A second notification can be triggered if this number of seconds has passed since the sensor status has entered the defined condition. Use this to automatically escalate a notification in case a problem persists for a longer time. Please enter an integer value.
...perform...	Select a (second) notification that will be triggered if the condition (i.e. the sensor status) selected is true and the escalation latency time defined has elapsed. Choose a notification from the drop down menu. The menu shows all notifications defined in the Account Settings—Notifications^[1791] settings. You can also choose no notification in order to only use other conditions for this trigger.
...and repeat every ... minutes	Define an interval in minutes in which the escalation notification (defined above) will be sent repeatedly. The second (escalation) notification defined will be resent every x minutes. Please enter an integer value.

State Trigger	
When condition clears perform...	Select a notification that will be triggered if the condition (i.e. the sensor status) selected is not true any more because the sensor's status has changed again. Choose a notification from the drop down menu. The menu shows all notifications defined in the Account Settings—Notifications settings. You can also choose no notification in order to only use other conditions for this trigger.
Save	Click on the Save button to save your settings.
Delete	Click on the Delete button next to an existing notification trigger to delete it.

Add Speed Trigger

Define a trigger that is activated when a sensor (for example, a traffic sensor) changes its current speed. Click on the **Add Speed Trigger** button to add a new trigger, or click on the **Edit** button next to an existing notification to change it. Then define settings as described below. Every trigger will provoke one or more [notification\(s\)](#) to be executed.

Speed Trigger	
When ... channel	From the drop down menu, select the channel which's data will be regarded for this comparison. Select Primary to generally use a sensor's primary channel (this can be defined in the sensor's settings) or choose a specific channel name from the list (there are different channels for every sensor type). All following settings for this trigger will be based on the chosen channel.
...is...	Select the condition that will trigger the notification. Choose from the drop down menu: ▪ Above: The trigger will be prompted if the value of the selected channel overruns a defined value. ▪ Below: The trigger will be prompted if the value of the selected channel undercuts a defined value. ▪ Equal To: The trigger will be prompted if the value of the selected channel is the same as a defined value. ▪ Not Equal To: The trigger will be prompted if the value of the selected channel is different than a defined value.
[value]	Define the value the channel's data will be compared with. Please enter an integer value.

Speed Trigger	
[scale]	From the drop down menu, select the unit in which you entered the [value] above. [scale] and [time] together define the unit for the given value. If the channel's data is shown in a different unit PRTG will automatically convert values internally. Choose between: ▪ bit ▪ kbit ▪ mbit ▪ gbit ▪ tbit ▪ Byte ▪ KByte ▪ MByte ▪ GByte ▪ TByte
[time]	Select the time for the scale (so you create a scale per time designation). Choose from the drop down menu: ▪ second ▪ minute ▪ hour ▪ day [scale] and [time] together define the unit for the given value. If the channel's data is shown in a different unit PRTG will automatically convert values internally.
..for at least ... seconds	Define how many seconds will be waited before a notification is provoked. This can avoid false alarms in case a channel reaches a limit for just a few moments. If the combined channel condition of [value], [scale], and [time] persists after the defined time span, the notification will be triggered. Please enter an integer value.
...perform...	Select a notification that will be triggered if the combined channel condition of [value], [scale], and [time] is true and the latency time defined has elapsed. Choose a notification from the drop down menu. The menu shows all notifications defined in the Account Settings—Notifications settings. You can also choose no notification in order to only use other conditions for this trigger.

Speed Trigger	
When condition clears perform...	Select a notification that will be triggered if the combined channel condition of [value] , [scale] , and [time] is not true any more because the channel's value has changed again. Choose a notification from the drop down menu. The menu shows all notifications defined in the Account Settings—Notifications ¹⁷⁹¹ settings. You can also choose no notification in order to only use other conditions for this trigger.
Save	Click on the Save button to save your settings.
Delete	Click on the Delete button next to an existing notification trigger to delete it.

Note: No escalation notification and no repeat are available for this trigger type.

Add Volume Trigger

Define a trigger that is activated when a sensor (for example, a traffic sensor) reaches a certain volume limit in a specified time. Click on the **Add Volume Trigger** button to add a new trigger, or click on the **Edit** button next to an existing notification to change it. Then define settings as described below. Every trigger will provoke one or more [notification\(s\)](#) ¹⁷⁹¹ to be executed.

Volume Trigger	
When ... channel	From the drop down menu, select the channel which's data will be regarded for this comparison. Select Primary to generally use a sensor's primary channel (this can be defined in the sensor's settings ²⁹⁰) or choose a specific channel name from the list (there are different channels for every sensor type). All following settings for this trigger will be based on the chosen channel.
...has reached... [value]	Define the value the channel's data will be compared with. If the channel's data overruns this value, a notification will be triggered. Please enter an integer value.
[scale]	From the drop down menu, select the unit in which you entered the [value] above. [scale] and [time] together define the unit for the given value. If the channel's data is shown in a different unit PRTG will automatically convert values internally. Choose between: ▪ Byte ▪ KByte ▪ MByte ▪ GByte

Volume Trigger	
	▪ TByte
per [time]	Select the time for the scale (so you create a scale per time designation). Choose from the drop down menu: ▪ Hour ▪ Day ▪ Week ▪ Month [scale] and [time] together define the unit for the given value. If the channel's data is shown in a different unit PRTG will automatically convert values internally.
...perform...	Select a notification that will be triggered if the [value] in the combined unit of [scale] and [time] is overrun. Choose a notification from the drop down menu. The menu shows all notifications defined in the Account Settings—Notifications¹⁷⁹¹. You can also choose no notification in order to only use other conditions for this trigger.
Save	Click on the Save button to save your settings.
Delete	Click on the Delete button next to an existing notification trigger to delete it.

Note: No escalation notification, no repeat, and no notification when condition clears are available for this trigger type.

Add Threshold Trigger

Define a trigger that is activated when a sensor reaches specific values. Click on the **Add Threshold Trigger** button to add a new trigger, or click on the **Edit** button next to an existing notification to change it. Then define settings as described below. Every trigger will provoke one or more [notification\(s\)](#)¹⁷⁹¹ to be executed.

Threshold Trigger	
When ... channel	From the drop down menu, select the channel which's data will be regarded for this comparison. Select Primary to generally use a sensor's primary channel (this can be defined in the sensor's settings²⁹⁰) or choose a specific channel name from the list (there are different channels for every sensor type). All following settings for this trigger will be based on the chosen channel.

Threshold Trigger	
...is...	Select the condition that will trigger the notification. Choose from the drop down menu: ▪ Above: The trigger will be prompted if the value of the selected channel overruns a defined value. ▪ Below: The trigger will be prompted if the value of the selected channel undercuts a defined value. ▪ Equal To: The trigger will be prompted if the value of the selected channel is the same as a defined value. ▪ Not Equal To: The trigger will be prompted if the value of the selected channel is different than a defined value.
[value]	Define the value the channel's data will be compared with. It will be directly compared to the channel's data. Please enter values in the smallest possible (base) unit, for example, in bytes or seconds. Please enter an integer value.
..for at least ... seconds	Define how many seconds will be waited before a notification is provoked. This can avoid false alarms in case a channel reaches a limit for just a few moments. If the defined channel condition persists after the defined time span, the notification will be triggered. Please enter an integer value.
...perform...	Select a notification that will be triggered if the defined channel condition is true and the latency time defined has elapsed. Choose a notification from the drop down menu. The menu shows all notifications defined in the Account Settings—Notifications¹⁷⁹¹ settings. You can also choose no notification in order to only use other conditions for this trigger.
When condition clears perform...	Select a notification that will be triggered if the defined channel condition is not true any more because the channel's value has changed again. Choose a notification from the drop down menu. The menu shows all notifications defined in the Account Settings—Notifications¹⁷⁹¹ settings. You can also choose no notification in order to only use other conditions for this trigger.
Save	Click on the Save button to save your settings.
Delete	Click on the Delete button next to an existing notification trigger to delete it.

Note: No escalation notification and no repeat are available for this trigger type.

Add Change Trigger

Define a trigger that is activated by an 'on change' trigger. Some sensors offer the option to send such a trigger whenever sensor values have changed. Click on the **Add Change Trigger** button to add a new trigger, or click on the **Edit** button next to an existing notification to change it. Then define settings as described below. Every trigger will provoke one or more [notification\(s\)](#)^[1791] to be executed.

Change Trigger	
When sensor changes perform...	Select a notification that will be triggered whenever a compatible sensor sends a 'change notification'. You can enable this option in the settings ^[290] of some sensors. The notification trigger will be activated immediately whenever a sensor sends an 'on change' trigger. Choose a notification from the drop down menu. The menu shows all notifications defined in the Account Settings—Notifications ^[1791] settings.

Note: There are no other options available for this trigger type.

Sensor Settings Overview

For information about sensor settings, please see the following sections:

- [Sensor Settings](#)^[290]
- [List of Available Sensor Types](#)^[291]
- [Additional Sensor Types \(Custom Sensors\)](#)^[1680]
- [Sensor Channels Settings](#)^[1683]
- [Sensor Notifications Settings](#)^[1690]

Object Settings Overview

For more general information about object settings, please see section [Object Settings](#)^[141].

Part 7

Ajax Web Interface—Advanced Procedures

7 Ajax Web Interface—Advanced Procedures

The Ajax-based web interface is your access to PRTG. It is used to configure devices and sensors, and to set up notifications, as well as to review monitoring results and to create reports. This web interface is highly interactive, uses Asynchronous Java Script and XML (AJAX) to deliver a powerful and easy-to-use user experience. While the user is [logged in](#)^[102], the data on the screen is permanently refreshed (via Ajax calls) so it always shows the current monitoring results (refresh interval and method can be [set](#)^[102] by the user).

Because the web interface works as a **Single Page Application (SPA)**, you will rarely see a full page refresh to avoid this performance impact due to redundant processing. Only single page elements will be refreshed when necessary. All object setting dialogs are shown as pop-up layers, so you will never lose the current context. This speeds up the user experience appreciably and makes the configuration of objects in PRTG comprehensible.

The following sections introduce more advanced procedures in the Ajax Graphical User Interface (GUI).

Ajax Web Interface—Advanced Procedures—Topics

- [Toplists](#)  1702
- [Arrange Objects](#)  1707
- [Clone Object](#)  1708
- [Multi-Edit](#)  1710
- [Create Device Template](#)  1715
- [Geo Maps](#)  1718
- [Notifications](#)  1723
- [Libraries](#)  1733
- [Reports](#)  1749
- [Maps](#)  1768
- [Setup](#)  1784

Other Ajax Web Interface Sections

- [Ajax Web Interface—Basic Procedures](#)  100
- [Ajax Web Interface—Device and Sensor Setup](#)  188

Related Topics

- [Enterprise Console](#)  1860
- [Other User Interfaces](#)  1912

7.1 Toplists

Packet Sniffer and **xFlow** (NetFlow, jFlow, sFlow, IPFIX) sensor types can not only measure the total bandwidth usage, they can also break down the traffic by IP address, port, protocol, and other parameters. The results are shown in so-called **Toplists**. This way PRTG is able to tell which IP address, connection, or protocol uses the most bandwidth. PRTG looks at all network packets (or streams) and collects the bandwidth information for all IPs, ports, and protocols. At the end of the toplist period, PRTG stores only the top entries of each list in its database.

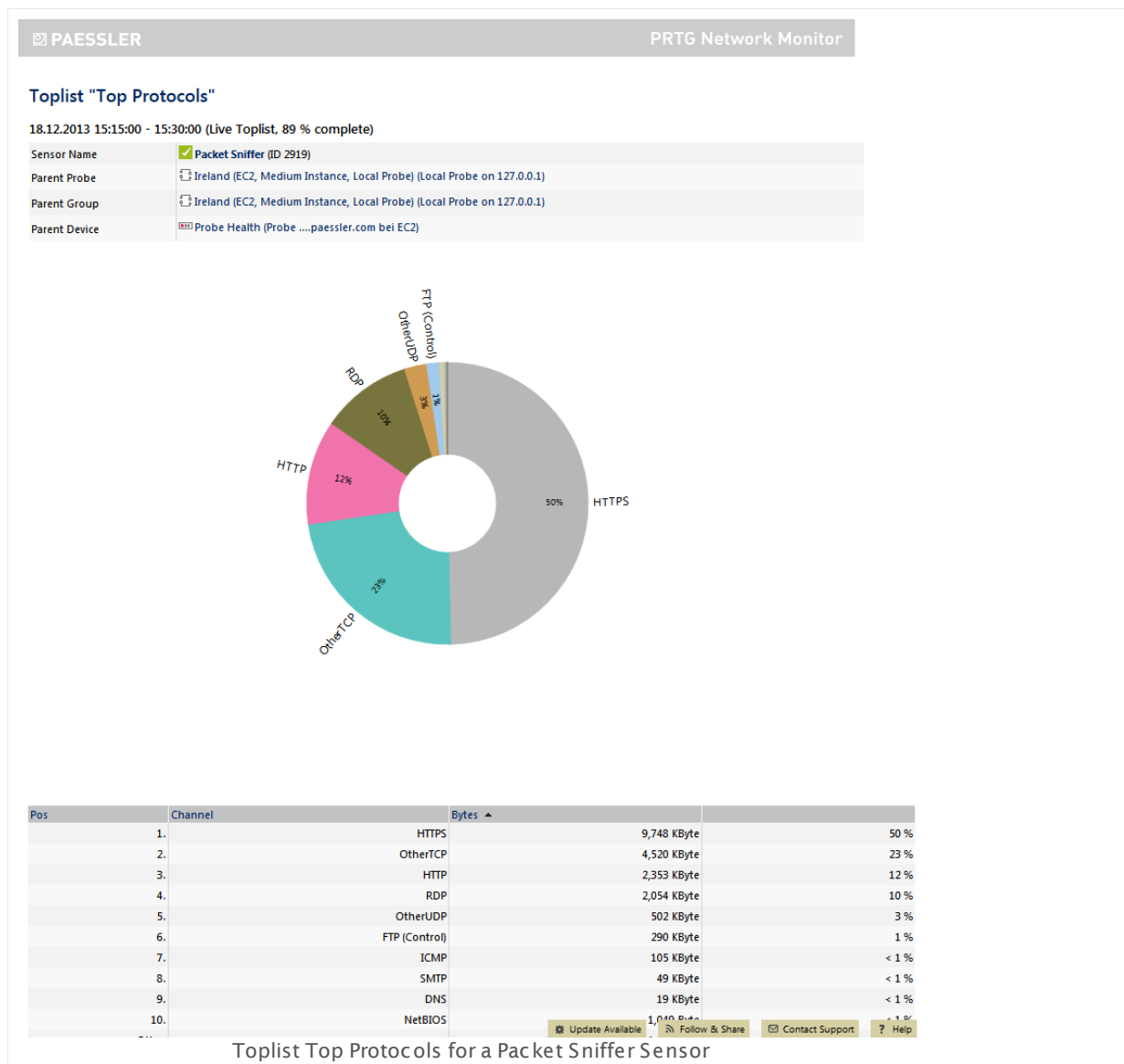
Only Top Entries are Stored

Storing all available analysis data in a database during the analysis process would create a huge amount of data which would be very slow to transfer between probe and core and also retrieving data would be too slow. By storing only the top 100 entries for short periods of time it is possible to reduce the amount of data to a minimum while still being able to identify devices with huge bandwidth usage.

Toplists Overview

Toplists are available for [xFlow, IPFIX, and Packet Sniffer sensors](#)^[291] only. Toplist graphs are displayed right on the sensor overview page. By default, there are three different toplist predefined for each sensor:

- **Top Connections:** Shows bandwidth usage by connection.
- **Top Protocols:** Shows bandwidth usage by protocol.
- **Top Talkers:** Shows bandwidth usage by IP address.



Click on one of these items to view a distribution chart and a list of source and destination IP and port, protocols, kind of traffic in different channels, etc. It depends on the selected list which information is available. Click on an entry in the **Toplist Periods** lists on the left side to view data for a certain time span. By default, a time span of 15 minutes is set. Additionally, several [table list options](#) are available.

In order to print a toplist, click on the **Print this toplist** button to view a printer-friendly version and then use the print option of your browser to send it to your printer. With **Sensor Overview** you will return to the current sensor's overview tab. For a quick selection of other toplist of the current sensor, click on one of the toplist icons at the top of the page.

In the sensor overview, you can add or delete new toplist, or edit existing ones.

Add

Click on the **Add Toplist** item in the sensor overview to create a new toplist. The available options are the same as for [editing](#) a list.

Edit

Click on the small **gear icon** of a toplist item in the sensor overview to modify it.

Toplist Settings	
Name	Enter a meaningful name to identify the toplist.
Type	▪ Top Talkers (Which IPs use the most bandwidth?): Shows bandwidth usage by IP address. ▪ Top Connections (Which connections use most bandwidth?): Shows bandwidth usage by connection. ▪ Top Protocols (Which protocols use the most bandwidth?): Shows bandwidth usage by protocol. ▪ Custom (Create your own toplist): Create your own list by selecting criteria below.
Toplist is based on	This setting is only available if a custom type is selected above. Select the fields you want to add to the toplist by adding a check mark in front of the respective field name. The available options depend on the type of sensor used. They're different for Packet Sniffer, NetFlow v5, v9 (and IPFIX), and sFlow. Note: For performance reasons, only select the field you really want to monitor. Please see Performance Considerations section below.
Period (Minutes)	Define the interval for the toplist in minutes. Please enter an integer value. Toplists always cover a certain time span. Once a time span has passed, the top results are stored and a new toplist is started. Note: In order to avoid load problems on your probe system, please do not set this interval too long. Default setting is 15 minutes. Please see Performance Considerations section below.
Top Count	Define the length of your toplist. Only this number of entries will be stored for each period. Please enter an integer value. Note: In order to avoid load problems on your probe system, please do not set this value as low as possible. Default setting is 100, in order to store the top 100 entries for each period. Please see Performance Considerations section below.

Toplist Settings	
Probe/Core Data Transfer	Define how the probe sends the toplist dataset to the core server. Choose between: ▪ According to sensor interval (default): Send data in the interval defined in the settings of the sensor this toplist is created for. This can create a lot of bandwidth and CPU load with many sniffer sensors, complex traffic, or long toplist. ▪ Wait until toplist period ends (less cpu&bandwidth h usage): Send data once a toplist period has finished. This will create less bandwidth usage and CPU load, but you cannot see the current toplist in the web interface, but only toplist with finished periods. For more information, please see Performance Considerations  section below.
Memory Limit (MB)	Define the maximal amount of memory in MB the probe will use for collecting the different connection information. Every toplist adds its amount to the probe's memory consumption. Increase this value if the number of captured connections is not sufficient. Please enter an integer value.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Delete

Click on the small **trashcan icon** of a toplist item in the sensor overview to delete it. Confirm with **Delete** to delete the list.

Details

Click on the **windows symbol** to show details of a toplist.

Performance Considerations

If you create toplist for data lines with considerable usage (for example, steady bandwidth over 10 Mbit/s) or if the traffic is very diverse (for example, many IPs/ports with only little traffic each) please consider the following aspects:

- The probe gathers all information needed for the toplist in RAM memory during each period. Only the top 100 entries are transferred to the core. Depending on the toplist type and traffic patterns the required memory can grow into many megabytes.
- Choose periods as short as desirable (especially important when traffic has a high level of diversity) to minimize memory usage.

- Memory requirements can grow almost exponentially with each field used in the toplist definition (depending on traffic pattern). Avoid complex toplist definitions for high and diverse traffic. For example, **Top Connections** (5 fields) needs a lot more memory than **Top Talkers** (1 field).
- If you experience high bandwidth usage between core and probe try to choose the **Wait until toplist period ends** option in the [toplist settings](#)¹⁷⁰⁶.
- If you experience **Data incomplete, memory limit was exceeded** messages try to increase the memory limit in the toplist settings but keep an eye on the probe process' memory usage.

Notes

- When working with toplist definitions be aware that privacy issues can come up for certain configurations of this feature. Using toplist definitions you can track all single connections of an individual PC to the outside world and you, as the administrator, must make sure that it is legal for you to configure PRTG like this.
- Keep in mind that toplist definitions can be viewed through the web interface. You may not want to show lists of domains used in your network to others. So you should restrict access to sensor types having toplist definitions.
- Note that diagrams, for example, for top connections are not meant to be used for detailed analysis. Rather they should indicate if there is an uncommon bigger change in this toplist.

More

- [Monitoring Bandwidth via Flows](#)¹⁹³⁴
- [Monitoring Bandwidth via Packet Sniffing](#)¹⁹³²

7.2 Arrange Objects

There are several possibilities to move objects within the device tree, or to move objects from one probe or group to another.

Manage Tab in Device Tree

While viewing the device tree (or parts of it), click on the **Manage** tab to switch to a tree view in which you can move monitoring objects using drag&drop in your browser window. For more information, see section [Manage Device Tree](#)^[222].

Device Details View: Arrange Sensors

When viewing the **Overview** tab of a device, you will see a list of all sensors on this device.

The screenshot shows the PRTG Network Monitor interface for a device named 'Exchange Mail Server'. The 'Overview' tab is selected, showing a status bar with 'OK' and a list of sensors. A large gauge displays 'IMAP 1' with a value of 14.030 msec. Below this, a table lists 14 sensors with columns for Position, Sensor Name, Status, Message, Graph, and Priority. To the right, a 'Geo Map' and three time-series graphs (2 days, 30 days, 365 days) are visible.

Pos	Sensor	Status	Message	Graph	Priority
1	PING 17	Up	OK	Ping Time 0 msec	★★★★★
2	WMI CPU Load 5	Up	OK	Total 36%	★★★★★
3	WMI Memory 5	Up	OK	Percent Available 50%	★★★★★
4	Intel(R) PRO 1000 MT Network Connection	Up	OK	Total < 0.01 Gb/s	★★★★★
5	MSExchange Store interface: RPC Requests failed_Total	Up	OK	RPC Requests fail 12,910	★★★★★
6	MSExchange Store interface: RPC Requests outstanding_Total	Up	OK	RPC Requests out 1	★★★★★
7	MSExchange Store interface: RPC Requests sent_Total	Up	OK	RPC Requests sent 111,800,410	★★★★★
8	MSExchange Store interface: RPC Slow requests_Total	Up	OK	RPC Slow requests 24,139	★★★★★
9	MSExchange Mailbox: Average Delivery Time_Total	Up	OK	Average Delivery 76,330 msec	★★★★★
10	MSExchangeS: RPC Averaged Latency	Up	OK	RPC Averaged Lat 3	★★★★★
11	MSExchangeS: RPC Operations/sec	Up	OK	RPC Operations/sec 222	★★★★★
12	MSExchangeS: RPC Requests	Up	OK	RPC Requests 0	★★★★★
13	MSExchangeS: RPC Averaged Latency	Up	OK	RPC Averaged Lat 2	★★★★★
14	MSExchangeS: Write Bytes RPC Clients/sec	Up	OK	Write Bytes RPC 401,771	★★★★★

Arrange Sensors on a Device

Click on the column headers **Pos**, **Sensors**, **Status**, or **Priority** to re-sort the sensor list. To change a sensor's position, simply click on the small grip at the beginning of the row, drag it to the position you like, and drop it. Changes take effect immediately.

Context Menu: Move

You can also right-click on any object to show the [Context Menu](#)^[162]. Select the **Move** entry to move sensors, devices, or groups up and down, or to move groups or devices into other groups or on other probes.

7.3 Clone Object

If you want to duplicate an object with the same settings, you can clone it. Cloning is available for groups, devices, and sensors. Unlike the results when using the [Create Device Template](#) ¹⁷¹⁵ option, a cloned device will contain all objects of the original device, regardless of whether they bring about working sensors or not (which often depends on the settings of the cloned device).

Note: You cannot clone 'fixed' objects, such as the root group or a probe device. You cannot clone the sensor types [QoS \(Quality of Service\) One Way Sensor](#) ⁸⁰¹ and [QoS \(Quality of Service\) Round Trip Sensor](#) ⁸⁰⁷.

Note: If you want to clone a **sensor**, a faster way will be to use the [Manage Device Tree](#) ²²² function.

To start, right click on an object in your device tree, and from the [context menu](#) ¹⁶², select **Clone...** An assistant will appear.

Clone Sensor IMAP 1

Duplicating Sensor by Cloning

To duplicate a sensor by creating a clone of a sensor you must choose a parent device and a new name for the sensor. Note: After creation the new sensor will be paused so you can edit its settings before monitoring is actually started.

SENSOR TO BE CLONED

Parent Probe: Local probe (Local Probe on 127.0.0.1)

Parent Group: Exchange

Parent Device: Exchange Mail Server

Sensor: IMAP 1

NEW SENSOR NAME

Choose a new name to describe the new sensor: Clone of IMAP 1

PLEASE CHOOSE A DEVICE TO ADD THE NEW SENSOR TO

Please select a device from the list

- Root
 - Local probe
 - Clone Staging
 - Clone_Source
 - Baseline
 - BUexec
 - Google Search Appliance
 - Probe Device
 - Networking
 - Firewalls
 - Cisco ASA Primary
 - Cisco ASA FO/Test
 - Switches
 - HP 2810-24G - Workgroup
 - GigabitSwitch Server
 - 3Com 2928 - Wireless/POE
 - Core Switch
 - Virtual Hosting
 - XenServer

Continue > Cancel

Clone Dialog for a Sensor

Clone Object Settings

Object To Be Cloned

Object

Several fields show information about the object that is to be cloned. The available information varies depending on whether you are about to clone a group, device, or sensor.

New Object Name

New Object Name

Enter a name for the cloned object. By default, the old name is filled in, preceded by **Clone of**.

New IP Address/DNS Name

This field is only available when cloning a device. Enter the IP address or DNS name for the new device.

Please choose a group/device to add the new object to

From the device tree shown, choose an object you want to add the cloned object to. When cloning a group or device, select a group. When cloning a sensor, select the device you want to add it to.

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

You will be redirected to the newly cloned object's [overview](#)^[124] page. By default, all sensors are initially paused to give you the chance to change settings before monitoring starts. Please check the [settings](#)^[141] and [resume](#)^[161] monitoring.

Related Topics

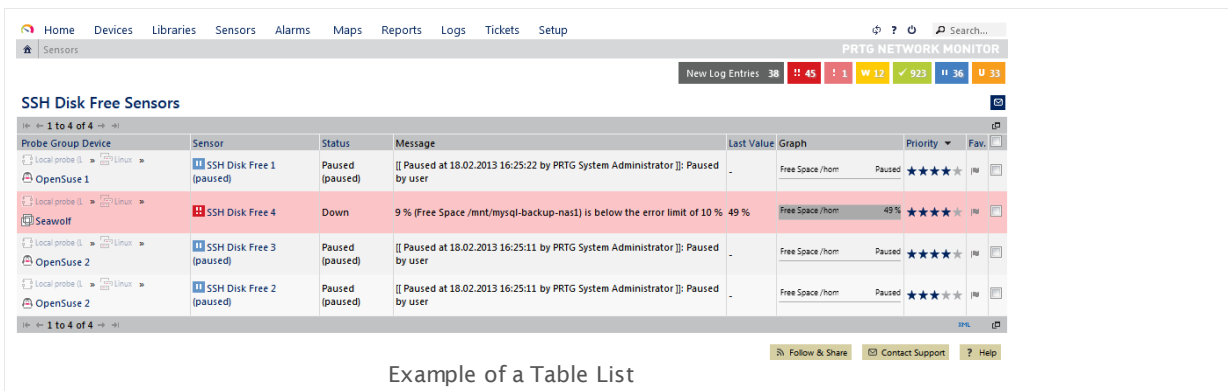
- [Create Device Template](#)^[1715]
- [Manage Device Tree](#)^[222]

7.4 Multi-Edit

Device and sensor table lists, as well as some other lists, offer multi-edit functionality. With this, you can bulk edit the properties of many objects at a time. Multi-edit is also available in the **Management** tab if you select multiple objects by holding down the **Ctrl** key (see [Manage Device Tree](#)^[223]).

Note: Using multi-edit, not all settings can be changed. PRTG will offer only settings which all selected objects have in common.

Note: The multi-edit option is not available for the standard [user groups](#)^[1829] PRTG Administrators and PRTG Users Group.



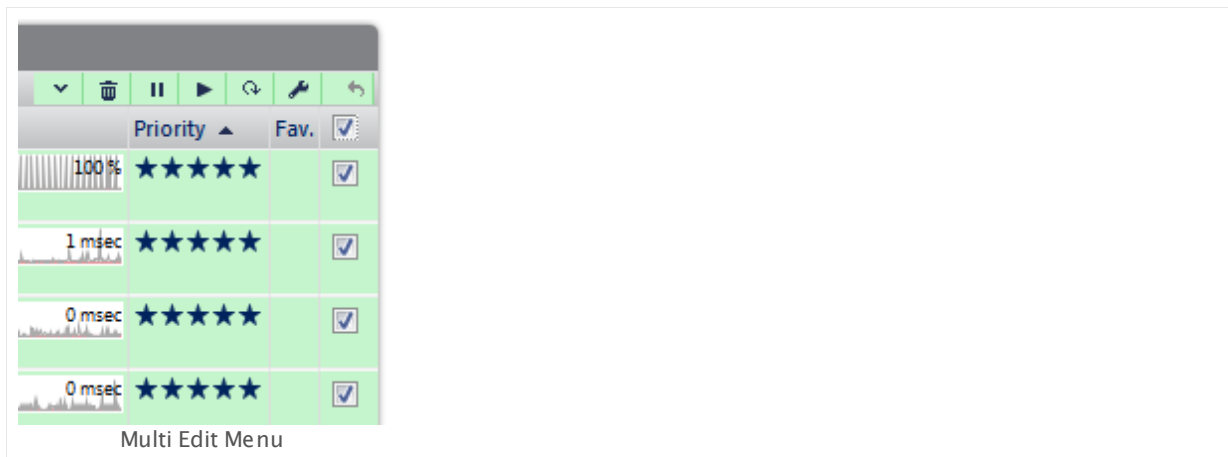
Example of a Table List

Probe Group Device	Sensor	Status	Message	Last Value	Graph	Priority	Fav.
OpenSuse 1	SSH Disk Free 1 (paused)	Paused (paused)	[[Paused at 18.02.2013 16:25:22 by PRTG System Administrator]]: Paused by user	-	Free Space /hom	★★★★☆	[X]
Seawolf	SSH Disk Free 4	Down	9% (Free Space /mnt/mysql-backup-nas1) is below the error limit of 10 %	49 %	Free Space /hom	★★★★☆	[X]
OpenSuse 2	SSH Disk Free 3 (paused)	Paused (paused)	[[Paused at 18.02.2013 16:25:11 by PRTG System Administrator]]: Paused by user	-	Free Space /hom	★★★★☆	[X]
OpenSuse 2	SSH Disk Free 2 (paused)	Paused (paused)	[[Paused at 18.02.2013 16:25:11 by PRTG System Administrator]]: Paused by user	-	Free Space /hom	★★★★☆	[X]

Start Multi-Edit in Lists

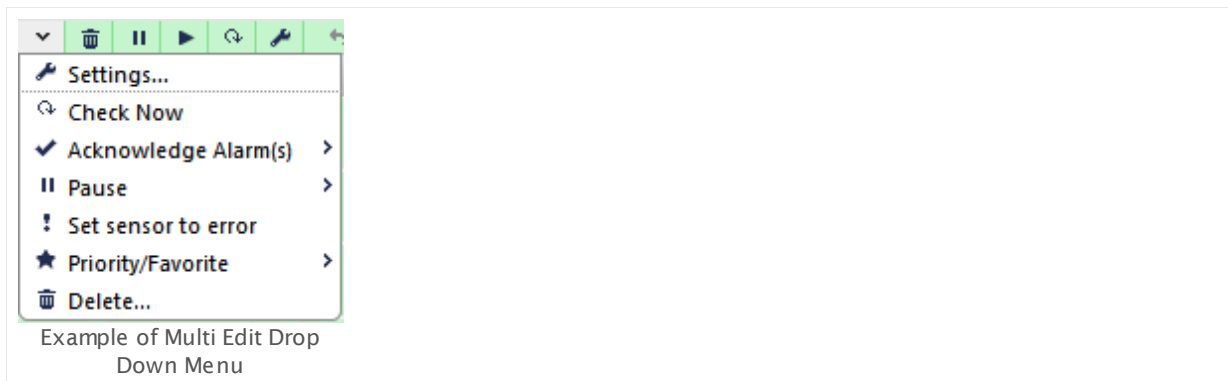
Start with viewing a table list. For example, choose **Sensors | By Type | ...** or **Devices | Device List | ...** from the main menu. Table lists are also available in the **Overview** tab of [Libraries](#)^[1733], [Maps](#)^[1768], [Reports](#)^[1749], [Notifications](#)^[1723], and [Schedules](#)^[1801].

In a table list, start multi-edit by selecting objects using the check boxes on the right. You can also select all objects of the current page at once by clicking the check box in the table header. Use the **Item Count** option to view more items per page. As soon as you select one or more objects, the multi-edit menu will appear at the top of the table and chosen objects are shaded in green.



Depending on the object type, different functions are available. For example, for sensor lists, some frequently used functions are available as quick buttons, such as **Delete**, **Pause**, **Resume**, **Check Now**, and **Settings**. If you click on one of those buttons, the respective function will be applied to all selected objects.

Other options are available in the drop down menu. **Hover** the arrow symbol to show it.



The options in this menu vary depending on the kind of objects selected. If you choose an entry, the respective function will be applied to all selected objects.

Once you have selected the objects you want to change settings for, click on the screwdriver symbol to enter the edit settings mode. For available settings, please see below.

Start Multi-Edit in Management Tab

In the device tree, start by clicking the **Management** tab.

You can use Multi-Edit for object settings:

- Hold down the **Ctrl** key and select multiple groups, devices, or sensors (one of a kind).
- In the appearing dialog, select the settings you would like to edit, change the according values and click on **Save**. The changes will be applied to all selected objects.

For available settings, please see below.

Edit Settings—Settings

In the multi-selected sensors' **Settings** tab within the **Edit Multiple Objects** popup, you can edit most of the sensors' properties which they have in common, respectively in the **Edit Multiple Objects** popup for devices. For example, for devices or sensors, edit the name, tags, priority, scanning interval, access rights, etc.

Editing 3 Objects

Edit Multiple Objects

This page allows to edit one or more settings for a selection of objects (groups, devices, sensors, etc.). First enable the checkbox in the first column for each setting that you want to change for all selected objects. Then enter/select your new value.

You are editing 3 objects ([Show all objects](#)):

BASIC DEVICE SETTINGS

- ☐ Device Name
- ☐ Status
 - ☒ Started
 - ☐ Paused
- ☐ IP Version
 - ☒ IPv4 device
 - ☐ IPv6 device
- ☐ IPv4 Address/DNS Name
- ☐ IPv6 Address/DNS Name
- ☐ Tags
- ☐ Priority
 - ★★★★★

ADDITIONAL DEVICE INFORMATION

- ☐ Device Icon
 - ☒ [Icon 1]
 - ☐ [Icon 2]
 - ☐ [Icon 3]
 - ☐ [Icon 4]
 - ☐ [Icon 5]
 - ☐ [Icon 6]
 - ☐ [Icon 7]
 - ☐ [Icon 8]
 - ☐ [Icon 9]
 - ☐ [Icon 10]
 - ☐ [Icon 11]
 - ☐ [Icon 12]
 - ☐ [Icon 13]
 - ☐ [Icon 14]
 - ☐ [Icon 15]
 - ☐ [Icon 16]
 - ☐ [Icon 17]
 - ☐ [Icon 18]
 - ☐ [Icon 19]
 - ☐ [Icon 20]

OK **Cancel**

Example of Device Settings in Multi-Edit Mode

The available options depend on the selected objects and will vary according to your selection. When editing multiple sensors, it may be useful to only choose one certain sensor type from the list, so that there are as much settings as possible available for multi-edit.

In order to change a property, add a check mark in front of the respective line and then change the settings. The new setting(s) will be applied to all objects you selected for multi-edit. All properties that are not activated with a check mark will remain unchanged.

Click on the **OK** button to store your settings. If you close the popup via the **X** or **Cancel** button, all changes to the settings will be lost!

Edit Settings—Channel Settings

The **Channel Settings** tab in the **Edit Multiple Objects** popup is only available when editing sensors. You can edit settings of all channels which the selected sensors have in common. Select a channel name from the **Channel** list. You can then edit, for example, channel name, ID, display settings, colors, scaling, limits, etc.

Editing 4 Objects

Edit Multiple Objects

This page allows to edit one or more settings for a selection of objects (groups, devices, sensors, etc.). First enable the checkbox in the first column for each setting that you want to change for all selected objects. Then enter/select your new value.

You are editing 4 objects (Show all objects):

Settings Channel Settings

SELECT CHANNEL

Channel

- Downtime (ID -4)
- Total (ID -1)
- Free Bytes /home (ID 2)
- Free Space /home (ID 3)

☐ Chart Rendering

- ☒ Show in Charts
- ☐ Hide from Charts

☐ Table Rendering

- ☒ Show in Tables
- ☐ Hide from Tables

☐ Line Color

- ☒ Automatic
- ☐ Manual

☐ Line Width

1

☐ Data

- ☒ Display actual values in GByte
- ☐ Display in percent of maximum

☐ Value Mode

- ☒ Average
- ☐ Minimum
- ☐ Maximum

☐ Decimal Places

- ☒ Automatic
- ☐ All
- ☐ Custom

☐ Vertical Axis Scaling

- ☒ Automatic Scaling
- ☐ Manual Scaling

☐ Limits

- ☒ Disable Limits
- ☐ Enable Limits

OK Cancel

Example of Sensor Channel Settings in Multi-Edit Mode

The available options depend on the selected sensors and will vary according to your selection. It may be useful to only choose one certain sensor type from the list, so that there are as much channel settings as possible available for multi-edit.

In order to change a property, add a check mark in front of the respective line and then change the channel settings. The new setting(s) will be applied to all sensors you selected for multi-edit. All properties that are not activated with a check mark will remain unchanged.

Click on the **OK** button to store your settings. If you close the popup via the **X** or **Cancel** button, all changes to the settings will be lost!

Related Topics

- [Working with Table Lists](#) ¹⁵⁵

- [Manage Device Tree](#) 

7.5 Create Device Template

If you want to add a certain device several times, you can create a device template from an existing device in your device tree. When creating a device template, information for nearly all sensors on this device will be saved to a template file which you can later use in combination with [Auto-Discovery](#)^[190] (restrictions apply for a few sensor types). From the sensors, all relevant settings will be saved, except those that refer to other objects, such as schedules, triggers, access rights, etc. They will automatically be reverted to **Inherit**.

To start, right click on a device in your device tree, and from the [context menu](#)^[162], select **Create Device Template....** An assistant will appear.

Create Device Template for Cisco ASA Primary

Creating Device Templates

To create a template that can be used for auto-discovery you have to provide a file name, as well as a clear text name which will be used in the appropriate select box for device templates. The template will contain an entry for every sensor of the selected device applicable for autodiscovery. That entry contains all relevant sensor settings except settings which refer to other objects (schedules, triggers, access rights, etc.). These settings will revert to 'inherited' when a sensor is created via a template.

CHOOSE TEMPLATE NAME

Choose a name which is used to store the template in the 'devicetemplate' folder of your PRTG installation. You can omit the file extension, it will be .odt anyway

File Name

Enter a clear name for display purposes

Template Name

Continue > **Cancel**

Create Device Template Assistant

Device Template Settings

File name for the template

File Name	Enter a name under which the file will be stored. It will be stored with the extension .odt in the \PRTG Network Monitor\devicetemplates sub-directory of your PRTG core installation (of the Master node, if in a cluster). The file may not exist in this directory, otherwise you will see an error message.
Template Name	Enter a meaningful display name for the template, as it will appear in the web interface.

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

You should see a success message indicating that your template file was saved. Finished! The device template is now stored in the program path of your PRTG core installation. Your device template file contains all sensors, including their settings, of the original device.

During your next auto-discovery, choose the **Automatic sensor creation using specific device template(s)** option and select the name of your newly created device template from the list. PRTG will then try to discover the stored sensor types on the new (or existing) device. If the physical device answers to a sensor request, the sensor is added to the PRTG device.

Note: Numbers will be added to the original sensor names. For detailed information, please see [Auto-Discovery](#) ¹⁹⁰ section.

Settings That Are Not Saved

There are a few settings which cannot be saved into a device template, and will therefore be set to default, such as the **Dependency Type** setting **Master object for parent** (in **Schedules and Dependencies** section), and **Result Handling** settings **Write result do disk** (as this is intended for debugging purposes only). Also, settings in the **Access Rights** section are not saved to avoid security flaws.

Furthermore, due to internal restrictions, the following sensor types will not be saved into a device template:

- **Core/Probe/Cluster Health**
- **DHCP**
- **HDD Health**
- **IPFIX**
- **IPFIX (Custom)**
- **jFlow V5**
- **jFlow V5 (Custom)**
- **NetFlow V5**
- **NetFlow V5 (Custom)**
- **NetFlow V9**
- **NetFlow V9 (Custom)**
- **Packet Sniffer**
- **Packet Sniffer (Custom)**
- **QoS (Quality of Service)**
- **Sensor Factory**
- **sFlow**
- **sFlow (Custom)**

- **SNMP Trap Receiver**
- **Syslog Receiver**
- **WMI Volume** (use [WMI Free Disk Space \(Multi Drive\) Sensor](#)¹⁵⁴⁷ instead)

No Update of Device Templates

Once a device template is created, it is not possible to add additional sensors to it. If you want to create a template with an extended set of sensors, please create a new one. **Note:** When saving a new device template, all internal IDs of the sensors contained in this template are updated. Therefore, when applying a new template to an existing device, all sensors contained in this template will be newly created on this device, even if those sensors were previously created using (another) device template!

Related Topics

- [Clone Object](#)¹⁷⁰⁸
- [Manage Device Tree](#)²²²

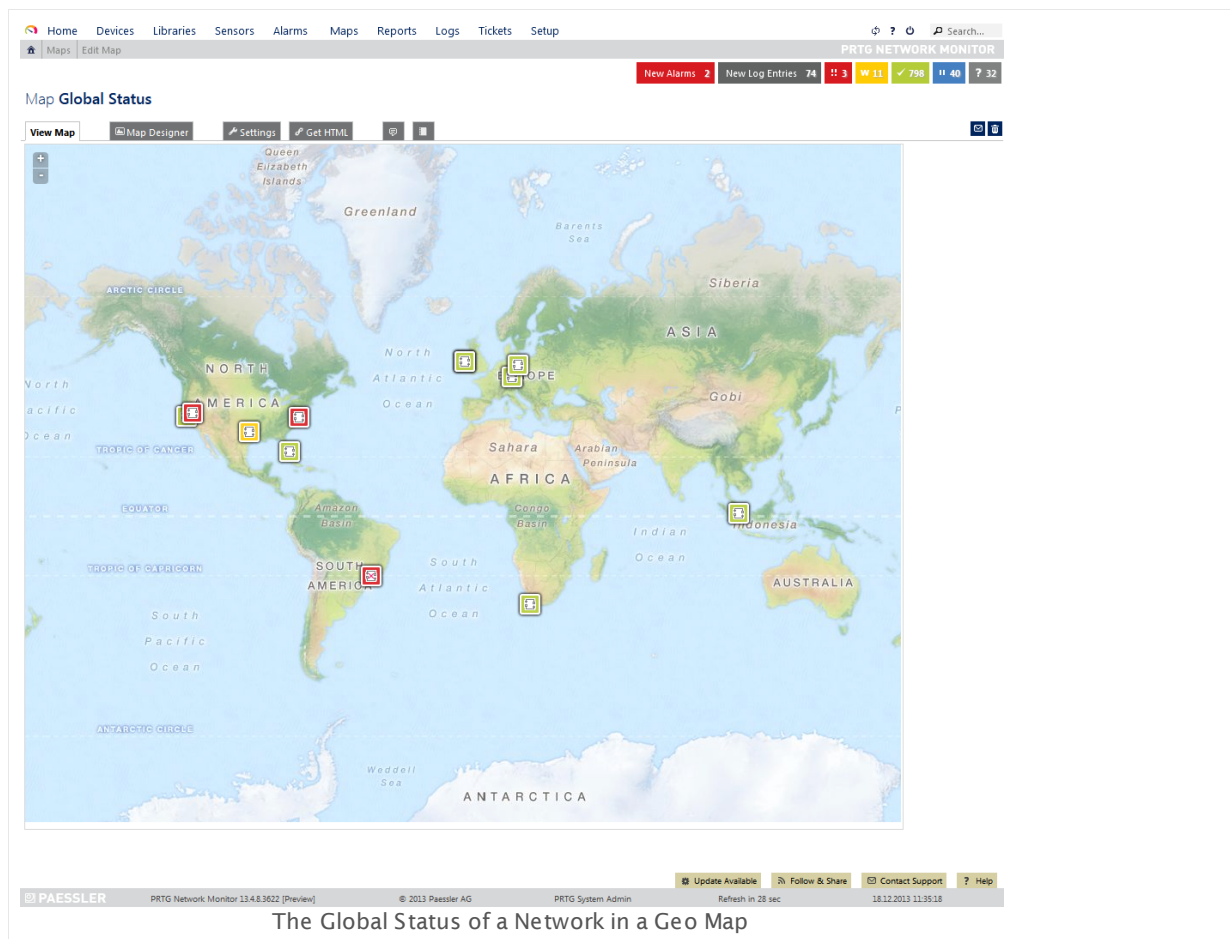
7.6 Geo Maps

With the PRTG Geo Maps feature you can visualize geographical information about your monitored objects. You can display the location of **probes**, **groups**, and **devices** in a graphical map on an object's details page, or on PRTG [Maps](#)¹⁷⁶⁸. This feature is especially useful when you monitor networks which are spread over different locations, for example, in various cities of a country or all over the globe.

For each probe, group, or device, you can enter **Location** information. PRTG will use the first line of this information to query a geographical map which shows your objects. Your location specification will be resolved to global geographical coordinates by the PRTG core server with the help of an external map service provider.

PRTG will connect to the specified maps provider to get **map tiles**. These are used to set up the graphical map. Then the defined locations will be marked with the corresponding object icons and their **status**¹⁷²¹ on the map. You can select your favorite map tiles provider in [System Administration—System and Website](#)¹⁸⁰⁶ (setting **Geo Maps**).

Geographical maps can be displayed on the device tree. PRTG will adjust the zoom of a map automatically such that all locations of a selected object can be displayed. You can also add geographical maps to PRTG [Maps](#)¹⁷⁶⁸. For this concern, go to the PRTG [Maps Designer](#)¹⁷⁷⁴ (either in an existing map or creating a new one) and choose the entry **Geo Maps** from the properties menu on the right.



The Global Status of a Network in a Geo Map

Using Geo Maps

In order to use geographical maps within the PRTG [web interface](#)^[100] or [Enterprise Console](#)^[1860], please make sure the following:

1. In the system administration (within the web interface), select the maps provider and type you want to view. There, you will also find an option to disable geo maps integration if you do not want to use it. See section [System Administration—System and Website](#)^[1806] (setting **Geo Maps**) for detailed information.
2. In your [objects' settings](#)^[141], add a city name, or address, or coordinates in the first line of the **Location** field. As soon as you view the details of such an object, a geographical map will be shown. The **Location** information will also be used when viewing objects in the [Enterprise Console](#)^[1800] or when adding **Geo Maps** objects to PRTG [Maps](#)^[1768].
3. Make sure your PRTG core server has access to the internet in order to obtain map tiles. If a proxy is mandatory in your network, please configure proxy settings accordingly. For details, please see [System Administration—System and Website](#)^[1811]. For details about tile server domains, please see [More](#)^[1722] section below.

Labeling Locations

You can define your own labels for locations of objects. For this concern, enter the desired label in the first line of the **Location** settings and provide the geo coordinates of the location in the second line. In PRTG's geo map, this object will be displayed with the defined label.

LOCATION

☐ Inherit from  Microsoft Servers (Location (for geo maps): Bucher Str. 79a, Nür...)

Location (for geo maps)

Big Apple
40.712778, -74.005833



Defining Location New York City with Geo Coordinates and Label
Big Apple

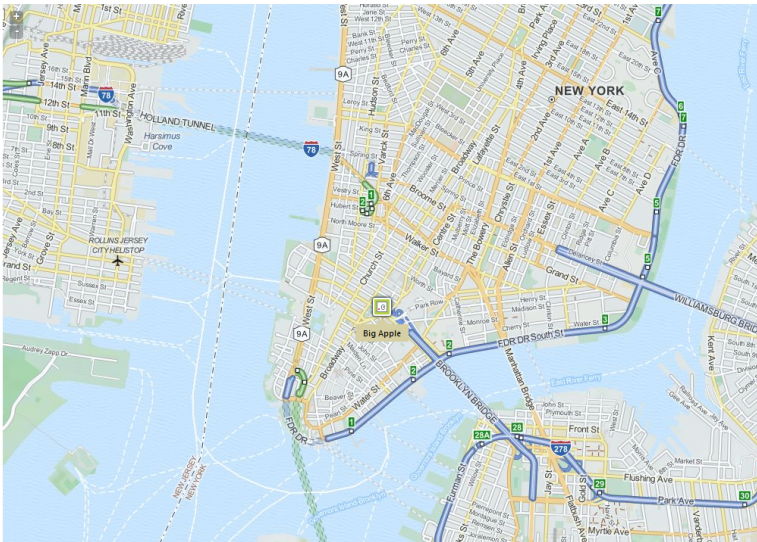
The location New York City will appear with the label Big Apple then:

Home Devices Libraries Sensors Alarms Maps Reports Logs Tickets Setup

Devices Local probe Microsoft Servers Exchange

New Alarms 1 New Log Entries 163 45 12 422 36 34

Geo Map for Exchange



Location New York City with Label Big Apple

It is also possible to define the same label for different locations. For example, imagine your company's headquarter is spread over several different locations. For each object representing a dedicated headquarter in the PRTG device tree, enter its coordinates in the second line of the respective **Location** settings and the label "Headquarter" in the first line. All corresponding objects will be displayed as "Headquarter". This way, you can easily find your desired objects on the map.

Map Icon Colors

On the geographical maps the different location icons will show the overall status at this location by using a color code. Following, all possible location states are listed ordered by their hierarchy:

Flag	Flag Color	Location Status	Meaning
	Red	Down	At least one sensor at this location shows a red Down status. Hover the circle with the letter symbol in the legend to view the total number of alarms at this location.
	Bright-Red	Down (Acknowledged)	At least one sensor at this location is Down and the status was acknowledged by a PRTG user, applying the Acknowledge Alarm function. The Down states of all sensors at this location have to be acknowledged—if at least one sensor is unacknowledged down, this location will be displayed as Down .
	Yellow	Warning	At least one sensor at this location shows a yellow Warning status. There is no sensor in a Down or Down (Acknowledged) status at this location.
	Orange	Unusual	At least one sensor at this location shows an orange Unusual status. There is no sensor in a Down , Down (Acknowledged) , or Warning status at this location.
	Green	Up	All sensors at this location are in a green Up status. There is no sensor in a Down , Down (Acknowledged) , Warning , Paused , or Unusual status at this location.
	Blue	Paused	All sensors at this location show a blue Paused status. There is no sensor in a Down , Down (Acknowledged) , Warning , Unusual , or Up status at this location.
	Black (Grey)	Unknown	All sensors at this location have an Unknown status. There is no sensor in a Down , Down (Acknowledged) , Warning , Unusual , Paused , or Up status at this location.

Note: For detailed information about sensor states, please see [Sensor States](#)¹²¹ section.

More

Knowledge Base: Which provider should I use for PRTG's "Geo Maps" feature?

- <http://www.paessler.com/knowledgebase/en/topic/34603>

Knowledge Base: Which domains and ports does the GeoMaps feature use?

- <http://www.paessler.com/knowledgebase/en/topic/35823>

Knowledge Base: Why does my street not appear on the Geo Map shown in PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/35653>

Knowledge Base: How do I get a Google Maps API key for use in PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/32363>

Knowledge Base: Which limitations apply when using the Google Maps API in PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/7913>

Knowledge Base: How can I change the way markers look like in PRTG's geo maps?

- <http://www.paessler.com/knowledgebase/en/topic/43153>

7.7 Notifications

Notifications are used to send alerts to the user whenever PRTG discovers a defined status, such as slow or failing sensors, or when threshold values are breached. You can define an unlimited number of notifications allowing to use one, or more, of several communication channels like email, text messaging, and many more. For video instructions, please see the [More](#)  section below.

Overview

Notifications can be triggered by:

- **Sensor status changes**
For example, when a sensor changes status to **Up** or **Down**, if responses are slow, or sensors show an **Unusual** status.
- **Sensor value threshold breaches**
For example, when a sensor shows a request time higher than 1,000 ms for more than 30 minutes.
- **Speed threshold breaches**
For example, when a traffic sensor shows more than 1 Mbit/s for more than 5 minutes.
- **Volume threshold breaches**
For example, when a traffic sensor shows more than 1 Gbyte transferred in 24 hours.
- **Sensor value changes**
For some sensors you can trigger a notification whenever the value changes, for example, when monitoring files on a hard disk drive.

A notification can be one of these actions:

- **Send Email**
- **Add Entry to Event Log**
- **Send Syslog Message**
- **Send SNMP Trap**
- **Send SMS/Pager Message**
- **Execute HTTP Action**
- **Execute Program**
- **Send Amazon Simple Notification Service (SNS) Message**
- **Assign Ticket**

For details, see section [Account Settings—Notifications](#) .

Note: Usually there are three successive attempts to deliver a notification. If all of these attempts fail, the notification is lost.

Notifications can contain valuable sensor information, such as:

- Last error message
- Last good/failed request
- Total downtime
- Total uptime
- Recent sensor history
- A direct link to the web interface

Notifications Setup

There are three steps to take in order to use notifications with PRTG. Please go through all of them:

1. Check and set up the **Notification Delivery** settings. This will tell PRTG how to send messages.
For detailed information, see [System Administration—Notification Delivery](#) ¹⁸¹⁵.
2. Check and set up several **Notifications**. This will define the kind of message and its content.
For detailed information, see [Account Settings—Notifications](#) ¹⁷⁹¹.
3. Check and set up **Notification Triggers** for objects. These will provoke the defined notifications.
For detailed information, see [Sensor Notifications Settings](#) ¹⁶⁹⁰.

See section [Setting Up Notifications Based on Sensor Limits: Example](#) ¹⁷²⁵ for a step-by-step guide describing a potential notifications setup.

More

Video Tutorial: There is a video available on the Paessler video tutorials page.

- http://www.paessler.com/support/video_tutorials

Knowledge Base: Notifications based on priorities

- <http://www.paessler.com/knowledgebase/en/topic/31243>

7.7.1 Setting Up Notifications Based on Sensor Limits: Example

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

This section will show you exemplarily how to set up a notification for exceeded disk free limits. The approach for this specific use case is examined step by step. You can easily adapt it to declare limits for other sensor types.

There are several steps to take in order to set up notifications based on limits:

- [Step 1:](#)  Provide necessary information about the delivery of notifications (SMTP and SMS).
- [Step 2:](#)  Create notifications, specifying the type of notification and its content.
- [Step 3:](#)  Define thresholds that will change a sensor's status (this is not necessary for every kind of notification).
- [Step 4:](#)  Add suitable triggers to objects which will evoke notifications if something is going wrong in your network.
- [Step 5:](#)  Test if the created notification will be triggered and delivered correctly.

Note: When you set up your own notifications, you will not necessarily need to go through all the steps described here. In this section, our main goal is to give you a general idea of the notifications concept.

Step 1: Setting up the Notification Delivery

Before creating notifications, you first have to define how those notifications actually will be delivered to your email account, mobile phone, or pager. To do so, choose **Setup | System Administration | Notification Delivery** from PRTG's main menu bar. Specify the mechanism of SMTP delivery, sender email and name, as well as the HELO ident. For SMS delivery, select your service provider and provide the corresponding credentials. You can find details about notification delivery in section [System Administration—Notification Delivery](#) .

Step 2: Setting up the Notification's Content

In order to get an informative message when a disk is running out of capacity, create a corresponding notification. Choose **Setup | Account Settings | Notifications** from PRTG's main menu bar and click on the button **Add New Notification**. Give the notification an explanatory name; in our case you could use **Disk Free Limit Notification**. However, if you want to trigger this notification on a global level (for example, for a probe or group) such that it would not only apply to breached disk free limits, a general name would be more suitable (like the predefined notification "Email to Admin"). If you leave the default text of the newly created notification, it will already contain all necessary information, like:

- which sensor is affected,
- since when the sensor is affected,
- last value of this sensor,

Part 7: Ajax Web Interface—Advanced Procedures | 7 Notifications

1 Setting Up Notifications Based on Sensor Limits: Example

- etc.

See section [More](#)¹⁷³¹ for the other options you have here.

After providing this basic information, select the delivery method. In our case, we choose **Send Email** for this notification by marking the corresponding checkbox. Specify who will receive the notification, its subject, the format, the content of the email, and its priority. By default, the email notification will contain several information parameters about the evoking sensor: its name, status, time, message, location in the device tree, etc. Feel free to adjust email messages to your needs (see section [More](#)¹⁷³¹). You can choose any other notification method, of course (see [Account Settings—Notifications](#)¹⁷⁹⁴).

☒ **SEND EMAIL**

Email Address
johnnpbublic@example.com, john.doe@example.com

Send to User Group
User Group X

Subject
[!sitename] %device %name %status %down (%message)

Format
☒ Text
☐ HTML

Message (Text)

```

=====
Sensor: %name
%homem/sensor.htm?id=%sensorid

Status: %status (%down)

=====
Date/Time: %datetime (%timezone)
Last Result: %lastvalue
Last Message: %message
=====
Probe: %probe
%homem/probenode.htm?id=%probeid
Group: %group
%homem/group.htm?id=%groupid
Device: %device (%host)
%homem/device.htm?id=%deviceid
=====
Last Scan: %lastcheck
Last Up: %lastup
Last Down: %lastdown
Uptime: %uptime
Downtime: %downtime
Cumulated since: %cumsince
Settings: %settings
=====

```

Priority
highest

Note: The mail footer can be changed in the System & Website settings of the System Administration.

Save Cancel

Creating an Email Notification

Once the notification is set up completely, click on **Save**. You will be redirected to the notifications overview page. You can now use this notification for every trigger on every object in your device tree.

Step 3: Define Limits

Before creating triggers that evoke notifications, first specify the limits which you want to apply to your disks. For example, if you want to be notified when a disk has exceeded 80% of its capacity, force the sensor into a **Warning** status at this utilization. You have several options to set limits for disk free sensors:

- Set limits checked against all disks in the settings of multi-drive sensors: [WMI Free Disk Space](#)¹⁵⁴⁷, [SNMP Linux Disk Free](#)¹¹⁰², [SSH Disk Free](#)¹²⁶⁰
- Enable limits in Channel settings of single sensors
- You can achieve both with [Multi-Edit](#)¹⁷¹⁰

Step 3.1: Define Limits in Sensor Settings (Multi-Disk Free Sensors Only)

You can set limits for sensors monitoring multiple disks directly via the **Settings** tab on a sensor's details page. [Multi-Edit](#)¹⁷¹² for existing sensors is also possible. Open the settings of the selected sensor(s) and go to section **Set limits checked against ALL disks**. There, for example, enable **Percentage Limit Check**. In the field **Lower Warning Limit**, enter the percentage suitable to your needs. In our example, this would be **20**. Alternatively, you can use bytes to define a limit. However, we recommend using percentage values for more flexibility. This limit will apply to all channels of this sensor representing disks.

SET LIMITS CHECKED AGAINST ALL DISKS

Please use the channel tab to set separate error/warning limits for each disk

Percentage Limit Check	☐ Disable Percentage Limits ☒ Enable Percentage Limits
Upper Error Limit	
Upper Warning Limit	
Lower Warning Limit	20
Lower Error Limit	10
Byte Limit Check	☒ Disable Byte Limits ☐ Enable Byte Limits
Alarm on Missing/Removed Disk	☒ Deactivate Alarm (default) ☐ Activate Alarm

SENSOR DISPLAY

Primary Channel	Free Space C: (%) ▼
Chart Type	☒ Show channels independently (default) ☐ Stack channels on top of each other

Setting Limits for All Disks

Note: This sensor setting is only available for multi-drive sensors. You can omit Step 3.1 for all sensors that are not from the type "disk free".

Step 3.2: Define Limits for Sensor Channels

In order to set specific limits for single disks, use the sensor's **Channel** settings. You can open channel settings via the gear icon in the respective channel gauge or in the channels table.

Enable Limits at the bottom of the channel settings dialog and specify your desired limits in the **Lower Warning Limit** field. This limit will only apply to the respective channel.

Note: If you define channel limits when using the sensor's limit setting in the sensor's **Settings** tab at the same time, the first limit that applies will be considered. This way, you can individually define harder limits for single disks in a multi-disk sensor. All defined limits are valid side-by-side.

You **have** to take the approach via channel settings for sensor types that monitor only one (logical) disk, for example, the [SNMP Disk Free Sensor](#)¹⁰⁰¹. For these sensor types, you can use [Multi-Edit](#)¹⁷¹³ if you want to apply the same limits for each of these sensors automatically.

- To see all sensors of this type at a glance, just filter for it: From PRTG's main menu bar, choose **Sensors | By Type | SNMP Disk Free**.
- Mark the checkboxes of the sensors you want to add a limit for.
- Click the screwdriver symbol in the multi-edit bar.
- Open the **Channel Settings** tab.
- Select the channel you want to add a limit for; in this case it would be most likely the channel **Free Space**.
- Then **Enable Limits** at the bottom of the dialog and enter the number in the correct field as described above.

Once done, save these settings—the new limit will apply to all channels with this name of the multi-edited sensors.

Part 7: Ajax Web Interface—Advanced Procedures | 7 Notifications

1 Setting Up Notifications Based on Sensor Limits: Example

Editing 17 Objects

Edit Multiple Objects

This page allows to edit one or more settings for a selection of objects (groups, devices, sensors, etc.). First enable the checkbox in the first column for each setting that you want to change for all selected objects. Then enter/select your new value.

You are editing 17 objects (Show all objects):

Settings

Channel Settings

SELECT CHANNEL

Channel

Total (ID -1)

Free Bytes C: (ID 4)

Free Space C: (ID 5)

☐ Chart Rendering

☒ Show in Charts

☐ Hide from Charts

☐ Table Rendering

☒ Show in Tables

☐ Hide from Tables

☐ Line Color

☒ Automatic

☐ Manual

☐ Line Width

1

☐ Value Mode

☒ Average

☐ Minimum

☐ Maximum

☐ Decimal Places

☒ Automatic

☐ All

☐ Custom

☐ Spike Filter

☒ Disable Filtering

☐ Enable Filtering

☐ Vertical Axis Scaling

☒ Automatic Scaling

☐ Manual Scaling

☒ Limits

☐ Disable Limits

☒ Enable Limits

☐ Upper Error Limit (%)

☐ Upper Warning Limit (%)

☒ Lower Warning Limit (%)

20

☐ Lower Error Limit (%)

Values above this value will set the 'Warning'.

OK

Cancel

Setting Limits for Channels with Multi-Edit

Step 4: Setting up the Notification Trigger

You have specified limits to define when a sensor will go into a **Warning** (or **Error**) status. Now you can create the according triggers. The trigger we use in this example is the **State Trigger**. For details about other possible notification triggers, see section [More](#)¹⁷³¹.

- You can set up a **State Trigger** on any level in your device tree. For example, open a group containing the device(s) representing your disks.
- Go on the **Notifications** tab.

Part 7: Ajax Web Interface—Advanced Procedures | 7 Notifications

1 Setting Up Notifications Based on Sensor Limits: Example

- Click **Add State Trigger**.
- Set the trigger to **"When sensor is Warning"** and choose the notification you have created before (**"Disk Free Limit Notification"** or a more general one) from the drop down list.
- Adjust the other notification settings to your needs and save this new object trigger.

Now you will be notified immediately when the capacity of one of your disks falls below the defined limit, in this case 20% free disk space.

Setting a Trigger for Disk Free Limit Notification

Step 5: Testing the Notification

Finally, test the notification which you have created. You can trigger this notification for test purposes immediately:

- From the [main menu bar](#)^[174], choose **Setup | Account Settings | Notifications**.
- For the respective notification, click on the corresponding **Test** button.

Then, check if the notification was triggered and delivered correctly, depending on what delivery method you defined before. If you do not get a notification (or a defined action is not executed) at all, check the notification logs: From the main menu bar, choose **Logs | System Events | Notifications**. Look for the triggered notification in the table list (verifying that the notification delivery is set up correctly in general) and consider the corresponding message. See section [Logs](#)^[146] for more information.

More

This section provides information about additional options you have when working with notifications.

- **Notification Settings:**

You can create schedules to activate notifications only at specific times, for example, only on weekdays. In section **Notification Summarization** you can choose between various options to avoid message floodings. Furthermore, define which user groups will have access to edit this notification. For details about notification settings, refer to section [Account Settings—Notifications](#)¹⁷⁹³.

- **Content of Emails:**

You can individually adjust the subject, content, header, and footer of emails to your needs. PRTG allows you to use placeholders here. See section [Account Settings—Notifications](#)¹⁷⁹⁴ for details about editing subject and message, and section [System Administration—Notification Delivery](#)¹⁸¹⁵ for details about editing header and footer of emails.

- **Other Triggers:**

An alternative to the state trigger would be to add a **Threshold Trigger**; then you would not need to set up limits explicitly, though, this trigger type would only be suitable for disk free sensors when using the trigger for single sensors, one by one. Free disk sensors have free space in **percent** as primary by default, other sensors have primary channels with the units bytes or seconds. However, threshold triggers only apply to the primary or total channel. General notification triggering by threshold might not work as expected for sensors of the "percentage" type. You can find all available triggers in section [Notifications](#)¹⁷²³.

- **Add a Threshold Trigger to a sensor directly:**

Go on a sensor's detail page and select the **Notifications** tab. Click on **Add Threshold Trigger**, select the desired channel, and provide the condition when this notification will be sent. In this example for free disk space, the setting would be "**When Free Bytes C: (%) channel is Below 20 for at least 60 seconds perform Disk Free Limit Notification**".

- **Notifications with Libraries:**

If your disk devices are spread over many groups, we recommend you to [use a PRTG library](#)¹⁷³³ for your disks. Choose **Libraries | All disk space sensors** from the main menu bar, go on the **Notifications** tab, and add a state trigger as described above. **Note:** Not all disk free sensor types might appear. You can add them to this library in the settings of the library node. There you can [filter by type or tag](#)¹⁷⁴² and add missing sensors this way. You can also filter by priority and other sensor properties.

Part 7: Ajax Web Interface—Advanced Procedures | 7 Notifications

1 Setting Up Notifications Based on Sensor Limits: Example

Settings

BASIC LIBRARY NODE SETTINGS

Library Node NameDiskspace sensors

Tags

NODE DISPLAY SETTINGS

Linked ObjectRoot

Node Type

- Show a subtree of the device tree in the library
- Show a collection of (filtered) sensors in the library

Filter By Type

- Show all sensor types
- Show specific sensor types only

Filter By Status

- Show all sensor states
- Show sensors with a specific status only

Filter By Tags

- Show all tags
- Show objects with specific tags only

Select Tags

Search...

	Name
☐	bandwidthsensor
☐	C_OS_VMware
☐	C_OS_Win
☐	cpu
☐	cpuloadsensor
☐	dell
☒	diskfree
☒	diskfreesensor
☒	diskspacesensor
☐	dnssensor

Filter By Priority

- Show all priorities
- Show objects with specific priority only

Save

Cancel

Settings of a Library with Diskspace Sensors

7.8 Libraries

With PRTG's **Libraries** feature you can create special views of your device tree with up-to-the-minute monitoring status information, arranged the way you want it.

The screenshot shows the PRTG Network Monitor interface. At the top, there's a navigation bar with links: Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, Setup. Below this is a status bar with 'New Alarms: 4', 'New Log Entries: 11', and various status icons. The main content area is titled 'Library All bandwidth sensors'. It has tabs for Overview, Management, Settings, and Notifications. Under the Overview tab, it shows 'Sensors: 186 (of 215)' and a search bar. Below this is a tree view of sensors categorized by type: jFlow, NetFlow, Packet sniffing, sFlow, SNMP, and Virtuozzo. The WMI category is expanded, showing a grid of various sensors like Broadcom BC..., Intel(R) B257..., MS TCP Loop..., VMware Acc..., etc., each with a status icon and a value. At the bottom right, there are links for 'Follow & Share', 'Contact Support', and 'Help'.

Example of a Library

In this section:

- [Introduction](#) ¹⁷³³
- [Start Libraries](#) ¹⁷³⁴
- [Libraries List](#) ¹⁷³⁴
- [Working with Libraries](#) ¹⁷³⁵

Introduction

Libraries is a powerful feature which enables you to create additional views of your device tree, which are updated with the same scanning interval as your device tree, showing the same monitoring data, but arranged in a way you want it. This is interesting if you want to show data in different ways, e.g. depending on target groups or use case. For example, you can create a library which contains an overview of all your bandwidth monitoring sensors, regardless of which device they're running on.

Library features include:

- Create libraries containing nodes with monitoring objects from all over your configuration
- Show data from different PRTG probes in one library
- Show different branches of your device tree right next to each other

- Arrange sensors in a tree-like view regardless of which device they are running on
- Filter your entire tree (or parts of it) for sensor type, state, or tag, showing only matching sensors

You can create libraries easily, using **drag&drop** right within your browser.

PRTG comes with several pre-configured standard libraries, which you can use right away. You can also change or delete them, if you like. The following libraries are automatically created when you install PRTG for the first time (visible for the PRTG Administrator user). Some of them will be initially empty, but as you add more sensors, they will be filled automatically according to the filter settings defined for the nodes of the libraries:

- All bandwidth sensors
- All CPU load sensors
- All diskspace sensors
- All memory sensors
- All VMware sensors
- Sensors grouped by priority
- Sensors grouped by state

Note: Sensors which are added to libraries are not counted against the maximum number of sensors of your license.

Start Libraries

Click the **Libraries** entry from the [main menu](#)¹⁷⁷ to view or add custom views of your network's status and monitoring data. **Hover** to show other menu items. Choose between:

- **All**
Calls the Libraries feature where you can view or add custom device tree views of your network's status and monitoring data.
- **Add Library**
Lets you directly [add](#)¹⁷⁸ a new library.
- **Select Library ›**
Show existing libraries. **Hover** to show other menu items. Follow the menu path (it is specific to your setup) to select a library.

Libraries List

In the **All** view, you see a list of all existing libraries. Using the links next to a library name, you can perform the following actions.

- Click on the name of a library to view it.
- **Delete:** Delete this library.

- **Clone:** Create a clone of this library.
- **Used by:** Show which other monitoring objects use this library.
- Click on the **Add Library** button to add a new library.

Please see also [Working with Table Lists](#)¹⁵⁵. Additionally, there is multi-edit available. This enables you to change properties of several objects at a time. For more details, please see [Multi-Edit Lists](#)¹⁷¹⁰ section.

Working with Libraries

For detailed information on how to create and edit libraries please see the following sections.

- [Libraries Step By Step](#)¹⁷³⁶
- [Management](#)¹⁷⁴⁰
- [Libraries and Node Settings](#)¹⁷⁴²
- [Context Menus](#)¹⁷⁴⁸

7.8.1 Libraries Step By Step

In order to create a new library, follow the steps in this section. In the web interface, click on the **Libraries** entry in the main menu to show the libraries main screen.

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

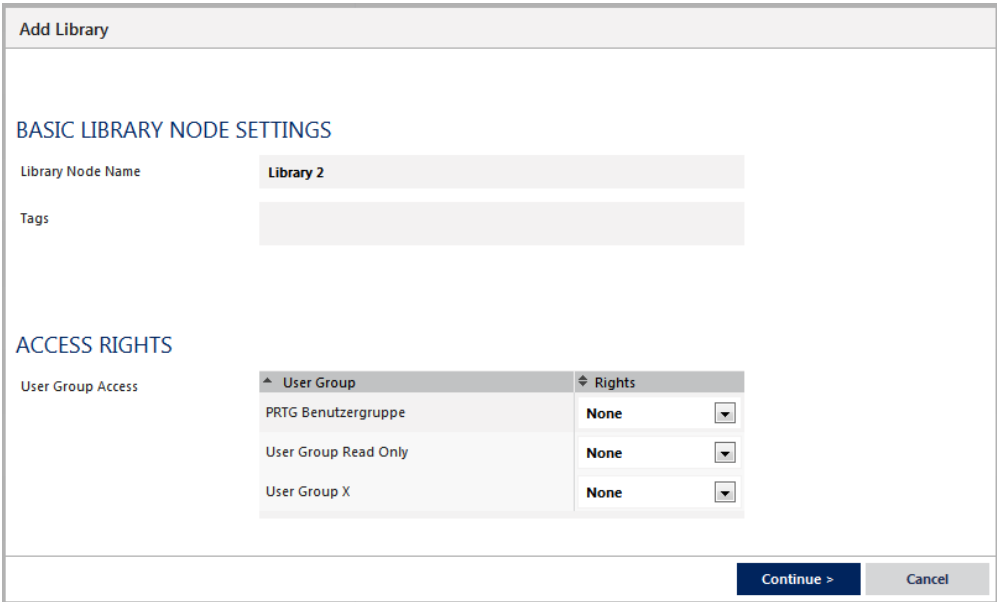
In this section:

- [Step 1: Add Library](#)  1736
- [Step 2: Add Library Nodes](#)  1737
- [Step 3: Set Library Node Display Settings](#)  1737
- [Step 4: View](#)  1738

Step 1: Add Library

Click on the **Add Library** button. An assistant is shown. Enter a **Library Name**, and define **Tags** and **Access Rights**, if you like. Click on **Continue**.

For detailed information, see [Libraries Settings](#)  1742 section.



Add Library									
BASIC LIBRARY NODE SETTINGS									
Library Node Name	Library 2								
Tags									
ACCESS RIGHTS									
User Group Access	<table border="1"><thead><tr><th>User Group</th><th>Rights</th></tr></thead><tbody><tr><td>PRTG Benutzergruppe</td><td>None</td></tr><tr><td>User Group Read Only</td><td>None</td></tr><tr><td>User Group X</td><td>None</td></tr></tbody></table>	User Group	Rights	PRTG Benutzergruppe	None	User Group Read Only	None	User Group X	None
User Group	Rights								
PRTG Benutzergruppe	None								
User Group Read Only	None								
User Group X	None								
Continue > Cancel									

Add Library Assistant Step 1

Step 2: Add Library Nodes

Click to the **Management** tab. You will see a split screen: On the left side, your library is shown (empty in the beginning), and on the right side, you see a less colorful view of your device tree, as known from the device tree's [Management](#) tab.

The screenshot shows the PRTG Network Monitor interface in the Management tab. The top navigation bar includes Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. Below this, a status bar shows 'New Alarms: 3', 'New Log Entries: 21', and various status icons. The main area is titled 'Library All bandwidth sensors' and has tabs for Overview, Management, Settings, and Notifications. The Management tab is active, showing a split-screen view. On the left, there's a list of sensors categorized by type: 'All bandwidth sensors' (165 sensors), 'iFlow' (4 sensors), 'NetFlow' (12 sensors), 'Packet sniffing' (12 sensors), 'sFlow' (12 sensors), 'SNMP' (165 sensors), 'Virtuozzo' (4 sensors), and 'WMI' (12 sensors). On the right, there's a hierarchical tree of network devices. The tree starts with 'Root' and branches into 'Local probe', 'Clone Staging', 'Clone Source', 'Baseline', 'Bluevec', 'Google Search Appliance', 'Probe Device', 'Networking', 'Firewalls', and 'Switches'. Each node in the tree has a list of associated sensors. For example, 'Clone Source' has 'SNMP Custo', 'Baseline' has 'CPU Load', 'Service: Bad', 'Service: Bad', 'Service: Bad', 'Service: Bad', '% Free Space', '% Free Space', 'Avg. Disk se', 'Eventlog At', 'PING 27', 'Uptime 7', '0011 Io', '0021 eth0', 'Home Page', 'HTTP 18', 'GSA System', 'Probe Device' has 'Probe Health', 'Core/Probe', 'CPU Load', 'Memory', 'PRTG Server', 'PRTG Probe', 'IntelRI 8257', 'Packet Sniff', 'SNMP Trap f', 'Syslog Recei', 'Networking' has 'Firewalls' and 'Switches'. The bottom status bar shows 'PAESSLER', 'PRTG Network Monitor 13.4.9.3736+ [Canary]', '© 2013 Paessler AG', 'PRTG System Administrator', 'Refresh in 567 sec', 'Follow & Share', 'Contact Support', and 'Help'.

From the device tree on the right side, drag objects and drop them on the library on the left side. Each dropped object will be added immediately as a new **Library Node**. Repeat this procedure as often as you wish until you have added all desired items to the library. **Note:** When adding single sensors to the library, there can only be one sensor in one library node.

You can also create nested library nodes by adding a new node underneath an existing one.

Drag and drop nodes within the library to change their position. If you want to change the monitoring object that is associated with a library node, you can change the **Linked Object** in the node's settings.

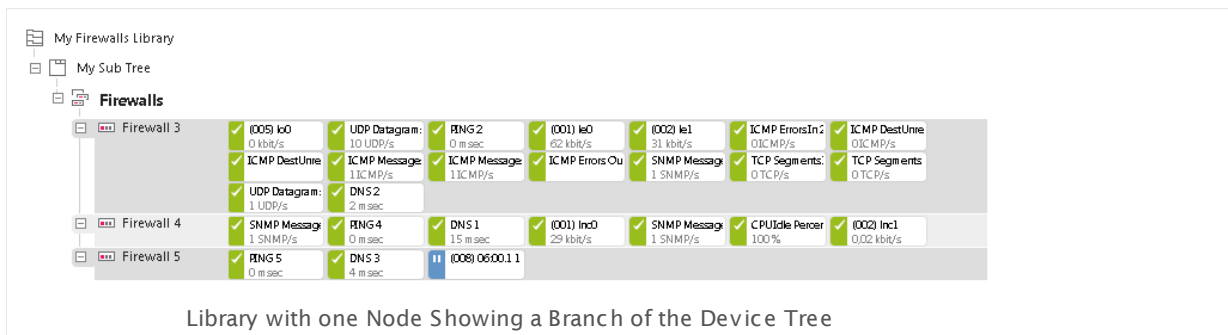
Step 3: Set Library Node Display Settings

You are still in the library **Management** tab.

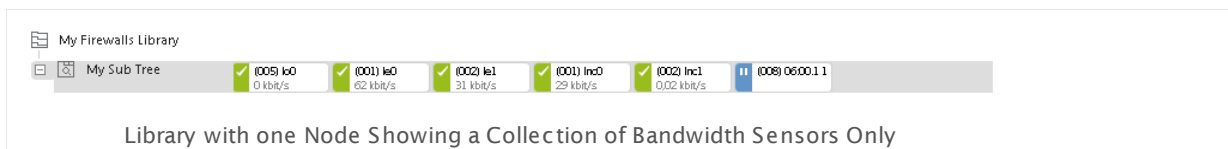
Right-click on the name of a **Library Node** and from the context menu, select **Edit | Settings...** to change the **Node Display Settings**. In this dialog, you can change the name of the library and its tags, as well as the linked object, node type, and filters.

These settings are available for each library node. You can choose to either show the **Linked Object** as a sub-tree of your device tree, or to view a collection of all sensors underneath the **Linked Object**.

When selecting the sub-tree view, the library node will just look like a branch in your device tree, as shown in the screen shot below for the library node names "My Sub Tree".



When selecting a sensor collection view, only the sensors underneath the **Linked Object** are shown, omitting probes, groups, and devices. You can additionally filter by certain sensor **Type**, **Status**, and **Tags**. Only matching sensors will be shown. The screen shot below shows the same **Linked Object** as above, but in sensor collection view, additionally filtered for sensors with a **bandwidthsensor** tag.



For detailed information, see [Libraries and Node Settings](#)^[1742] (Overview—Library Node Display Settings) section.

Step 4: View

Click on the **Overview** tab to see the final appearance of your library. You have the following options:

- Hover an object to view a popup window with recent monitoring and status data.
- Use the sensor state selection bar to select which sensors you want to see for the library: Simply remove check marks for sensor states you want to hide. **Note:** This function is the same you know from the device tree's [Sensor Status Bar](#)^[113]. The setting is reset the next time you open the library.
- Use the **Device Tree View** selection in the [page header bar](#)^[113] to change the size of the library display. **Note:** This function is the same you know from the [device tree](#)^[115].

- Use the **Search** box in the [page header bar](#)¹¹³ to search the library for a string in object names. Matching objects will be shown full-colored, all others will be grayed out while the filter is active. Click on the small **x** symbol in the search field to reset the filter. **Note:** This function is the same you know from the [device tree](#)¹¹³.

It depends on the library's access rights and the currently logged in user account if it will be visible to other PRTG users. Also, clicking on objects (for example, on sensors) will lead to more detailed information about the object or to an error message indicating insufficient access rights—depending on user account and access rights.

In libraries, you can right-click objects to access their [Context Menus](#)¹⁷⁴⁸.

7.8.2 Management

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Click to the **Management** tab. You will see a split screen: On the left side, your library is shown (empty in the beginning), and on the right side, you see a less colorful view of your device tree, as known from the device tree's [Management](#) tab.

The screenshot displays the PRTG Network Monitor Management interface. The top navigation bar includes tabs for Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. Below this, a status bar shows 'New Alarms: 3', 'New Log Entries: 21', and various status indicators. The main content area is titled 'Library All bandwidth sensors' and features a 'Management' tab. On the left, a list of sensors is shown, including 'iFlow', 'NetFlow', 'Packet sniffing', 'sFlow', 'SNMP', 'Virtuozzo', and 'WMI'. On the right, a tree view of the device hierarchy is visible, starting with 'Root' and branching into 'Local probe', 'Clone Staging', 'Probe Device', 'Networking', 'Firewalls', and 'Switches'. The 'Firewalls' section is expanded, showing details for 'Cisco ASA Primary' and 'Cisco ASA FO/Test'. The bottom of the interface includes a footer with the PRTG logo, version information, and a 'Bandwidth Library in Management Mode' label.

Add and Change Library Nodes

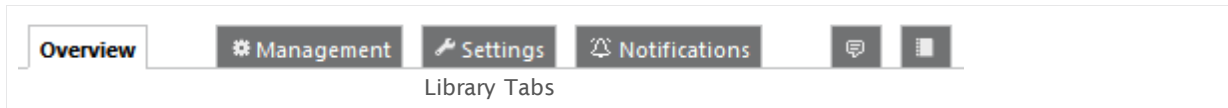
From the device tree on the right side, drag objects and drop them on the library on the left side. Each dropped object will be added immediately as a new **Library Node**. Repeat this procedure as often as you wish until you have added all desired items to the library. **Note:** When adding single sensors to the library, there can only be one sensor in one library node.

You can also create nested library nodes by adding a new node underneath an existing one.

Drag and drop nodes within the library to change their position. If you want to change the monitoring object that is associated with a library node, you can change the **Linked Object** in the node's settings.

7.8.3 Libraries and Node Settings

Using the libraries tabs you can access all functionalities and settings for a library.



Overview

Click on the **Overview** tab any time to show the current state of your library.

Library Node Display Settings

While in the **Overview** tab, click on a **library node**'s name to change its settings. Or, while in the **Management** tab, right-click a library node's name and select **Edit | Settings...** from the context menu. In both cases, the following settings are shown. **Note:** You can only change the settings of a node if it contains monitoring objects already, e.g. groups, devices, or sensors.

Basic Library Node Settings

Library Node Name	Enter a meaningful name for the library node.
Tags	Enter one or more tags, separated by space or comma. For example, you can use tags later to search for the library. Tags are not case sensitive.

Node Display Settings

Linked Object	Click on the reading-class symbol to change the object which is linked with this library node. A popup window will appear, showing the Object Selector ¹⁵⁸ .
Node Type	Select what you want to view for this library node. Choose between: ▪ Show a subtree of the device tree in the library: View all objects underneath the linked object as a device tree. ▪ Show a collection of (filtered) sensors in the library: View all sensors underneath the linked object (only sensors are shown). You can combine several filters with each other (see below).
Filter By Type	This option is visible only if collection of sensors is enabled above. Select if you want to filter the sensor list by a certain type. Choose between: ▪ Show all sensor types: Do not filter for a sensor type.

Node Display Settings	
	▪ Show specific sensor types only: Filter the sensor list of the linked object for certain sensor type(s). Note: This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.
Select Sensor Types	This option is visible only if filtering by type is enabled above. A list of all sensor types is shown, currently available sensor types are shown in bold letters for your convenience. Set a check mark in front of each sensor type you want to include in the library node view. You can also select and deselect all items by using the check box in the table head. Note: This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.
Filter By Status	This option is visible only if collection of sensors is enabled above. Choose between: ▪ Show all sensor states: Do not filter for a sensor status. ▪ Show sensors with a specific status only: Filter the sensor list of the linked object for sensors in certain states.
Select Sensor States	This option is visible only if filtering by sensor state is enabled above. A list of sensor states is shown. Set a check mark in front of each status you want to include in the library node view. Choose from: ▪ Unknown ▪ Up ▪ Warning ▪ Down ▪ Paused ▪ Unusual ▪ Down (Acknowledged) ▪ Down (Partial) You can also select and deselect all items by using the check box in the table head. Note: This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.

Node Display Settings	
Filter By Tags	This option is visible only if collection of sensors is enabled above. Choose between: ▪ Show all sensor tags: Do not filter for a tag. ▪ Show objects with a specific tag only: Filter the sensor list of the linked object for sensors with a certain tag. Note: The tag of a sensor can also be inherited^[87] by a parent object.
Select Tags	This option is visible only if collection of sensors is enabled above. A list of all available tags is shown. Set a check mark in front of each tag you want to include in the library node view. You can also select and deselect all items by using the check box in the table head. Note: This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.
Filter By Priority	This option is visible only if collection of sensors is enabled above. Choose between: ▪ Show all priorities: Do not filter for the priority setting^[159] of a sensor. ▪ Show objects with specific priority only: Filter the sensor list of the linked object for sensors with specific priority. Note: The priority setting of a group, device, or sensor is ignored here; only the priority setting of the sensor itself is regarded.
Select Priority	This option is visible only if collection of sensors is enabled above. Define which priority setting sensors must have to appear in this collection. Set a check mark in front of each priority you want to include in the library node view. Choose from: ▪ ***** (highest) ▪ ***** ▪ ***** ▪ *** ▪ ** ▪ * (lowest) Note: This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Note: After applying filters it might take several seconds for the changes to become visible. This is due to internal filter processes running in the background.

Management

Click on the **Management** tab to edit the contents of your library, for example, to add items to the library using drag&drop. For detailed descriptions, please see [Management](#)^[1740] section.

Settings

Click on the **Settings** tab to open a library's general settings.

Basic Library Settings	
Library Name	Enter a meaningful name for the library.
Tags	Enter one or more tags, separated by space or comma. For example, you can use tags later to search for the library. Tags entered here are inherited ^[87] to all library nodes underneath. Tags are not case sensitive.

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists and in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible. ▪ Read: Users in this group can see the object and review its monitoring results. ▪ Write: Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings. ▪ Full: Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings. You can create new user groups in the System Administration—User Groups¹⁸²⁹ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the Revert children's access rights to inherited option. For more details about access rights, please see section User Access Rights⁹⁴.

Note: When giving access rights to a user group, all members of this user group will be able to see the objects in the library just as seen by the user who originally created the library.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

You can define notification triggers for any kind of object libraries. This is even possible for dynamic libraries which can change with every scanning interval, for example, when you filter a library for the sensor status or priority. For details about how to use notifications, please see section [Notifications](#)¹⁷²³.

Comments

In the **Comments** tab you can enter free text for each object. This can be used for documentation purposes or to leave information for other users.

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the PRTG user which conducted the change, and a message. The history log keeps the last 100 entries.

Delete

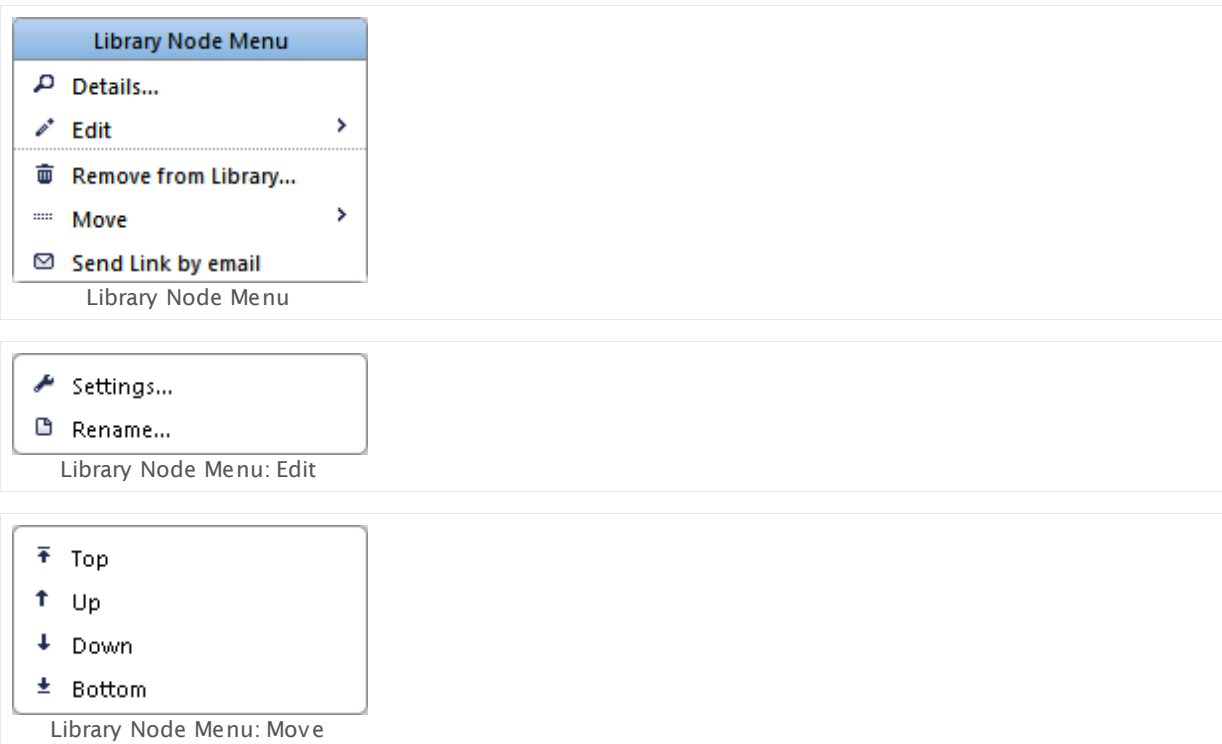
You can delete the entire library any time by clicking on the trash symbol on the right.

7.8.4 Context Menus

On right-click, there are different context menus available.

Library Node Menu

While in the **Overview** or the **Management** tab, right-click on any library node to show its context menu.



- Select either **Details...** or **Edit | Settings...** to get to the [Libraries and Node Settings](#)¹⁷⁴².
Note: While in the **Overview** tab, these settings are also accessible via left-click on the node's name.
- **Edit | Rename...** will give you an option to rename the library node quickly.
- **Remove from Library...** will remove this library node from the current library. **Note:** This will not delete any objects in your device tree.
- The **Move | ...** options will move the library node up and down within the library.
- Click on the **Send Link by email** entry to open a new email using your system's standard email client. It will contain a direct link to the page you're currently viewing.

Monitoring Objects Menus

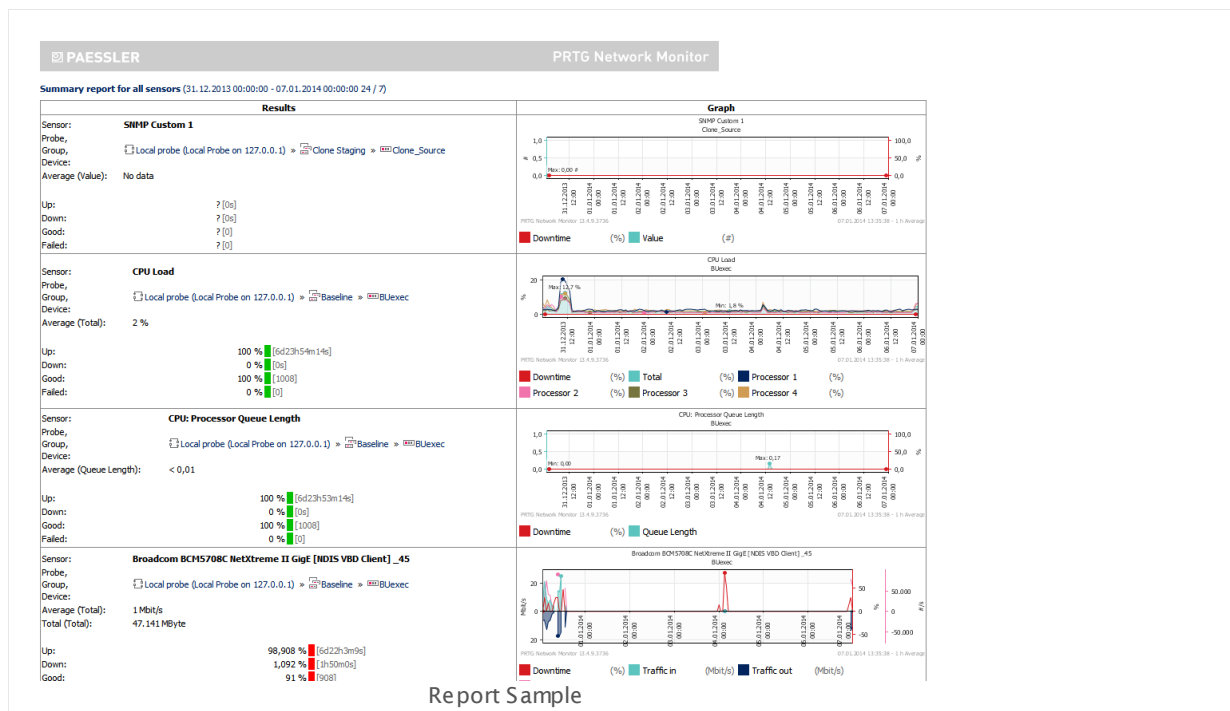
In libraries there are the same [Context Menus](#)¹⁶² available you already know from the device tree. With one exception: While accessing these menus within libraries, the **Move** and **Delete** options are disabled to avoid accidental changes to your device tree.

7.9 Reports

Reports are used to analyze historic monitoring results over a specified time such as one or more days, one month, or an entire year. You can create reports for all, or only for certain sensors.

Introduction

PRTG includes a powerful reporting engine for ad-hoc, as well as scheduled report generation in HTML and PDF format. Thus, reports can be run on demand or on a regular basis (for example, once a day). You can create reports for one single sensor, or you choose a range of sensors you want to create a report for. The content and layout of the report is controlled by the report template of your choice and is the same for all sensors in a report.



The sample report above shows a report data for devices on a local probe. You can see graphs for the preceding week, plus data tables with numeric results.

Start Reports

Click the **Reports** entry from the [main menu](#) ¹⁸¹ to view or add reports of your monitoring data. **Hover** to show other menu items. Choose between:

- **All**
Calls the Reports feature where you can view or add reports of your monitoring data.
- **Add Report**
Lets you directly add a new report.

▪ Select Report ›

Show existing reports. **Hover** to show other menu items. Follow the menu path (it is specific to your setup) to select a report.

Reports Overview

Reports Overview

Home Devices Libraries Sensors Alarms Maps Reports Logs Tickets Setup

PR TG NETWORK MONITOR

New Alarms 3 New Log Entries 32 45 1 12 929 36 27

Reports

1 to 20 of 20

Object	Template	Period	Schedule	Email	Status	Last Run	Next Run	Links
Active Directory	List of sensors (with 1h graph)	Week	None	Idle	17.12.2013 12:45:59 (63 Sensors)	-	Edit Clone Delete	
Exchange 2010	List of sensors (with 1h graph)	Week	None	Idle	16.12.2013 18:09:37 (21 Sensors)	-	Edit Clone Delete	
Firewall Report	Graph 1h interval, Table 24h interval	Week	None	Idle	17.12.2013 09:34:14 (28 Sensors)	-	Edit Clone Delete	
MS Systems - Iops	Graph 15 min interval, Table 15 min interval	Week	None	Idle	17.12.2013 10:05:55 (1 Sensors)	-	Edit Clone Delete	
NetApp	List of sensors (with 1h graph)	Week	None	Idle	17.12.2013 12:40:47 (24 Sensors)	-	Edit Clone Delete	
Ping	Data Table (24h interval)	Week	None	Idle	-	-	Edit Clone Delete	
SharePoint 2010	List of sensors (with 1h graph)	Week	None	Idle	17.12.2013 12:44:16 (99 Sensors)	-	Edit Clone Delete	
SNMP Traffic Benchmarking	Data Table (15 min interval)	Week	None	Idle	-	-	Edit Clone Delete	
SQL Server	Graph 1h interval, Table 24h interval	Week	None	Idle	16.12.2013 20:44:45 (20 Sensors)	-	Edit Clone Delete	
Summary report for all sensors	List of sensors (with 1h graph)	Day	None	Idle	-	-	Edit Clone Delete	
Top 100 Busy/Idle Processor Sensors	Highest and lowest 5 minute averages	Day	None	Idle	-	-	Edit Clone Delete	
Top 100 Fastest/Slowest HTTP Sens...	Highest and lowest 5 minute averages	Day	None	Idle	-	-	Edit Clone Delete	
Top 100 Fastest/Slowest PING Sens...	Highest and lowest 5 minute averages	Day	None	Idle	-	-	Edit Clone Delete	
Top 100 Free/Full Disk Space Sens...	Highest and lowest 5 minute averages	Day	None	Idle	-	-	Edit Clone Delete	
Top 100 Most/Least Used Bandwidth...	Highest and lowest 5 minute averages	Day	None	Idle	-	-	Edit Clone Delete	
Top 100 Most/Least Used Memory Se...	Highest and lowest 5 minute averages	Day	None	Idle	-	-	Edit Clone Delete	
Top 100 Uptime/Downtime Report	Top 100 Uptime/Downtime (based on uptime percent)	Day	None	Idle	25.11.2013 15:19:29 (1026 Sensors)	-	Edit Clone Delete	
vCenter VMs	Graph 5 min interval, Table 5 min interval	Week	None	Idle	16.12.2013 22:15:06 (130 Sensors)	-	Edit Clone Delete	
WAN Firewall1	Graph Only (15 min interval)	Week	None	Idle	-	-	Edit Clone Delete	
Windows_CPU	Data Table (15 min interval)	Quarter	None	Idle	-	-	Edit Clone Delete	

1 to 20 of 20

Add Report

PAESSLER PRTG Network Monitor 13.4.9.3726+ [Canary] © 2013 Paessler AG PRTG System Administrator Refresh in 591 sec 20.12.2013 13:26:30

Follow & Share Contact Support Help

List of Reports

In the **All** view, you see a list of all existing reports. Every line shows information about one report:

- **Period:** The time span covered by the report.
- **Schedule:** Shows if a schedule is set to regularly execute the report automatically.
- **Email:** If a schedule **and** an email address is set in the report settings, this shows the email address the report is automatically sent to.
- **Status:** Shows the current status of the report.
- **Last Run:** If a schedule is set in the report settings, this shows when the report was run the last time.
- **Next Run:** If a schedule is set in the report settings, this shows when the report will be run the next time.

Using the buttons at the end of a line, you can **Edit**, **Clone**, and **Delete** the respective report.

Please see also [Working with Table Lists](#)¹⁵⁵. Additionally, there is multi-edit available. This enables you to change properties of several objects at a time. For more details, please see [Multi-Edit Lists](#)¹⁷³⁰ section.

Click on the **Add Report** button to add a new report, or click on the name of an existing report to view and edit its settings. You can also run a pre-configured report easily by clicking on its name and then using the options in the **Run Now** tab. For both options, please see [Reports Step By Step](#)¹⁷⁵² section.

Working With Reports

For detailed information on how to create, edit, and schedule reports, please see the following sections:

- [Reports Step By Step](#)¹⁷⁵²
- [View and Run Reports](#)¹⁷⁵⁵
- [Reports Settings](#)¹⁷⁵⁸

Automatic Averaging

For performance reasons, PRTG automatically averages monitoring data when calculating data for large time spans. Data is then averaged regardless of the selected average interval.

Time Span in Report	Minimum Level of Detail (Average Interval)
Up to 40 days	Any
40 to 500 days	60 minutes/1 hour or larger

A report for a time span of more than 500 days is not possible. If you try to set a larger time span, it will be reduced to 365 days automatically.

Related Topics

- [Review Monitoring Data](#)¹²⁴
- [Historic Data Reports](#)¹³²

7.9.1 Reports Step By Step

In order to create a new report, or run an existing one, follow the steps in this section. In the web interface, click on the **Reports** entry in the main menu to show the reports main screen.

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Quick Start: Run an Existing Report

PRTG is delivered with several pre-configured reports. In order to use one of them, click on a report's name in the reports main screen, select the **Settings** tab. The other steps are the same as for new reports. Although some settings are already given, we recommend checking the settings. For example, check the sensors that will be included in the report. For some reports that come with PRTG there are no sensors added yet. Continue with [Step 3](#)¹⁷⁵² in this section.

Step 1: Add Report

Click on the **Add Report** button to add a new report. An assistant is shown where you can define various settings. First, enter a **Report Name**.

Add Report

BASIC REPORT SETTINGS

Report Name: Report

Template: <please select a file>

Security Context: PRTG System Administrator

Timezone: (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

Paper Size: ☐ A4 ☐ Legal ☒ Letter

SENSORS ("WHAT SENSORS WILL BE INCLUDED IN THE REPORT?")

Add Sensors Manually: There are too many sensors to show here. Please edit sensors and channels for this report on the tab "Select sensors manually" later

Add Sensors by Tag:

Filter Sensors by Tag:

SCHEDULE ("WHEN WILL THIS REPORT BE RUN?")

Report Schedule: ☒ No schedule (run interactive/on-demand only)
☐ Every full hour
☐ Every day at a specific hour
☐ Every specific day of a week
☐ Every specific day of a month
☐ The day after a quarter is finished (i.e. at 1. April for the 1. January - 31. March Quarter)
☐ Every specific date

PERIOD ("WHAT TIME SPAN WILL THE REPORT COVER?")

Reported Period: ☐ Current ☒ Previous

Report Period Type: ☐ Daily ☐ Weekly ☐ Quarterly (January-March, April-June, etc.)

Continue > Cancel

Add Report Assistant

Follow & Share Contact Support Help

Step 2: Select a Template

In the **Template** section, select one of the report templates from the list. This will define the overall look of your report and affect in which detail (interval) monitoring data is included. For a detailed description on the available options, please see [Reports Settings](#)¹⁷⁵⁸ section. If you are not sure, try a template that appears most suitable to you. You can change all settings later.

Step 3: Define Additional Settings

Select a **Security Context** (best choose **PRTG System Administrator**, if available), your **Timezone**, and **Paper Size** for PDF generation. For detailed information, please see [Reports Settings](#)¹⁷⁵⁸ section.

Step 4: Select Nodes and Sensors

Choose the sensors you want to include in the report. First, when running in a [cluster](#)⁸¹, define the **Cluster Node** the monitoring data will be taken from. Select a specific node from the list. If you select **All nodes**, a report with data from all of your cluster nodes will be created, but only the primary channel of every sensor will appear in the report.

Every report will show monitoring results from sensor data. There are two ways to include sensors in a report: You can either add sensors manually, or by tag. In the **Add Sensors by Tag** field, enter one or more tags that matches the sensor range you want a report for. For example, enter the tag **bandwidthsensor** to include all sensors that measure bandwidth (or select it from the list of tags which PRTG suggests). PRTG provides this tag as default when adding bandwidth sensors; so this tag typically gathers all bandwidth sensors, unless you have configured your system differently. You can enter several tags; hit the enter key, comma, or space after providing one tag and enter the next one. Use the **Filter Sensors by Tag** field to explicitly filter sensors with certain tags from the bulk of tags or manually selected sensors defined above.

Tagging is a great tool to group sensors or other objects. For more information, see [Tags](#)¹⁷⁵¹ section. You can also leave the tag fields empty and only choose specific sensors manually later.

Step 5: Decide on a Schedule and Additional Settings

In the **Report Schedule** section, choose if you want to run the report on a regular basis or on demand only. Also choose which time **Period** will be covered by the report, and if you want to show percentiles, add report comments, or special access rights. For detailed information, please see [Reports Settings](#)¹⁷⁵⁸ section.

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Step 6: Check and Adjust the Sensors Included

When settings are saved, switch to the **Sensors Selected by Tag** tab to see a list of all sensors that were added by the tag(s) you defined in step 4. To change tags, go back to the **Settings** tab. You can additionally add sensors manually. To do so, switch to the **Select Sensors Manually** tab. See [Reports Settings](#)¹⁷⁶⁵ section for detailed information. The final report will show sensors from both manual and by tag selection.

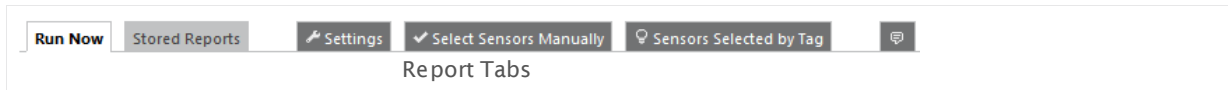
Step 7: Run Report

Switch to the **Run Now** tab, select the current or previous period, and in the **Processing Options** select **View Report as HTML**. Click the **Run Report** button. The report will be generated in a new browser window or tab immediately. Depending on the number of selected sensors and the used template, it may take a few minutes until you see the report. If you do not want to wait, close the newly opened browser window or tab and select a PDF option in the **Processing Options**. Click on the **Run Report** button again. The report will then be generated in the background and you will get a **ToDo ticket** or email once it is finished.

Note: For large PDF reports, PRTG will automatically split the output into separate files to avoid huge PDF files. You can change the number of sensors included into each PDF file by editing the report templates manually. See [More](#)¹⁷⁶⁷ section of [Reports Settings](#)¹⁷⁵⁸.

7.9.2 View and Run Reports

In the web interface, click on the **Reports** entry in the main menu to show the reports main screen. Click on a report's name to select it. Using the reports tabs you can access all functionalities and settings for this report. Click on the **Go to all reports** button at the bottom of the page to return to the list of Reports.



Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Run Now

In the **Run Now** tab you can execute a report immediately with the settings configured.

Run Report "[Name]"	
Report for	Define the time span covered by the report. Choose between: ▪ Current Period: Use monitoring data of the current period. The actual time span depends on the report period type defined in the report's settings¹⁷⁵⁸. It can be today, this week, this month, or this year. ▪ Previous Period: Use monitoring data of the last period. The actual time span depends on the report period type defined in the report's settings¹⁷⁵⁸. It can be yesterday, last week, last month, or last year. ▪ Select A Period: Use monitoring data of a period other than current or previous. Select below. ▪ Select Date Range Manually: Define a custom time span for the monitoring data that will be used. Set start and end date below.
Date Range	This selection is only visible if the period option is enabled above. From the list, select a data range for which the report will be generated. The actual time spans shown depend on the available monitoring data and on the report period type defined in the report's settings ¹⁷⁵⁸ . It can be days, weeks, months, or years.
Start Date	This selection is only visible if the date range option is enabled above. Define the begin of the time span for which the report will be generated. Click in the field and select a date from the calendar. Make sure you define a valid period.

Run Report "[Name]"	
End Date	This selection is only visible if the date range option is enabled above. Define the end of the time span for which the report will be generated. Click in the field and select a date from the calendar. Make sure you define a valid period.
Quick Range	This selection is only visible if the date range option is enabled above. Choose between different pre-defined ranges by simply clicking on it. With each click the Start and End Date fields above will be changed accordingly.
Processing Options	
File Format and Delivery	Define how you want to view the report. Choose between: ▪ View Report as HTML: Directly view the report in your web browser. It will be loaded in a new browser window or tab. ▪ Create and store PDF file: Create a PDF file of the report and store it. Once finished, you will find it in the Stored Reports tab and a ToDo ticket¹⁴⁹ will be created. By default, PRTG sends out a notification mail to the administrator in this case. ▪ Create PDF file, store it and send by email: Create a PDF file of the report, store it, and send it via email once it is finished. Note: For large PDF reports, PRTG will automatically split the output into separate files to avoid huge PDF files. You can change the number of sensors included into each PDF file by editing the report templates manually. See More¹⁷⁵⁷ section below.
Target Email Address	This option is only visible if sending by email is selected above. Please enter a valid email address the report will be sent to. Note: Configuration for outgoing email can be changed in the System Administration—Notification Delivery ¹⁸¹⁵ settings.
Compression	This option is only visible if sending by email is selected above. Specify if the attached report files will be compressed before sending. Choose between: ▪ Uncompressed: The report files will not be compressed before they are sent by email. ▪ Compressed: The report files will be compressed to a ZIP file before they are sent by email.

Click on the **Run Report** button to start report generation. Depending on the number of selected sensors, this may take a while. If you experience a long waiting time when generating HTML reports for immediate view, please consider using one of the PDF options. You can then view the report as soon as it's finished.

Note: Any sensor graphs in your report will only show the channels that are enabled via the **Show in Charts** option in the [Sensor Channels Settings](#)¹⁶⁸³ of the respective sensor.

Stored Reports

In the **Stored Reports** tab you can view PDF reports created in the past. Simply click on a name to open the report. Reports are stored until they are deleted according to the data purging settings of your PRTG configuration. You can set data purging limits for reports in the [System Administration—System and Website](#)¹⁸⁰⁵ settings.

Other Tabs

For all other tabs, please see [Reports Settings](#)¹⁷⁹⁸ section.

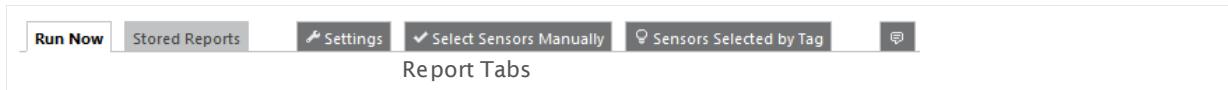
More

Knowledge Base: Can I change the number of PDFs created by a report?

- <http://www.paessler.com/knowledgebase/en/topic/11863>

7.9.3 Reports Settings

In the web interface, click on the **Reports** entry in the main menu to show the reports main screen. Click on a report's name to select it. Using the reports tabs you can access all functionalities and settings for this report. Click on the **Go to all reports** button at the bottom of the page to return to the list of Reports.



Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Run Now

In the **Run Now** tab you can execute a report immediately with the settings configured. Please see [View and Run Reports](#)¹⁷⁵⁵ section.

Stored Reports

In the **Stored Reports** tab you can view reports created in the past. Please see [View and Run Reports](#)¹⁷⁵⁷ section.

Settings

Click on the **Settings** tab to open a report's settings.

Basic Report Settings	
Report Name	Enter a meaningful name to identify this report.
Template	Select a template for the report. This will define the overall look of your report. There are several report templates delivered with PRTG. They also define in which detail (interval) monitoring data is included. You can choose from templates in the following categories: ▪ Data Table Only: Create a report with data tables only. Choose from several intervals. ▪ Graph Only: Create a report with graphs only. Choose from several intervals. ▪ Graph with Data Table: Create a report with graphs and data table. Choose from several intervals.

Basic Report Settings

	▪ List of Sensors: Create a report in a compact sensor list style. This is available with and without graphs. ▪ Top 10 Uptime/Downtime: Create a report with up to 10 objects with the highest uptime and downtime each. You can choose between data in percent and hours. ▪ Top 100 Highest and Lowest: Create a report with up to 100 objects with the highest and lowest average values. Choose from different intervals. ▪ Top 100 Uptime/Downtime: Create a report with up to 100 objects with the highest uptime and downtime each. You can choose between data in percent and hours. Monitoring data within an interval is averaged. See also the comment on data averaging in the Reports (Automatic Averaging) section. For information on how to modify templates, please see More section below.
Security Context	Define the user account that will be used for access to monitoring data. The report will only contain objects which the selected user is allowed to view. Please choose a user from the list. The available users depend on your configuration. By default, this is the user that created the report. PRTG Administrator users can change this setting.
Timezone	Define the time zone that will be used for all date-specific settings in this report (see below). Select a time zone from the dropdown list.
Paper Size	Define the paper size in which PDF reports will be created. Choose between: ▪ A4: Use German DIN A4 format. ▪ Legal: Use US legal paper format. ▪ Letter: Use US letter paper format.

Sensors

Cluster Node	This field is only visible when running PRTG in Clustering mode. Define the cluster node the report will take monitoring data from. Choose a cluster node from the list. The available options are specific to your configuration. Select All nodes to create a report with data from all of your cluster nodes. Note: A report for all nodes will include data of the primary sensor channels only, not for other sensor channels.

Sensors	
Add Sensors Manually	If you want to manually choose the sensors included in this report, please save settings and switch to the Select Sensors Manually  tab.
Add Sensors by Tag	Define the sensors included in this report by tag. Enter one or more tags; hit enter, space, or comma to confirm a tag. The report will cover all sensors that have at least one of the tags. Please enter a string or leave the field empty. Note: Tags are inherited  invisibly and automatically. So, for example, if you enter the tag of a group here, the report will include all sensors within this group. For detailed information, see Inheritance of Settings  section. For sensors that are added by tag, all sensor channels are included in the report automatically, except All nodes is selected in the Cluster Node selection above.
Filter Sensors by Tag	Further filter sensors. This is used in combination with sensors that are added manually, or added implicitly with their manually added parent objects. From those sensors, only the ones with the tags entered here will be included. Enter one or more tags to include sensors in the report; hit enter, space, or comma to confirm a tag. Please enter a string or leave the field empty.

Schedule	
Report Schedule	Define when the report will be run. Choose between: ▪ No schedule (run interactive/on-demand only): Only use the options in the Run Now tab to start generation of this report manually. ▪ Every full hour: Run this report every 60 minutes. ▪ Every day at a specific hour: Run this report every 24 hours. ▪ Every specific day of a week: Run this report every 7 days. Specify the day below. ▪ Every specific day of a month: Run this report on a specific day every month. Specify below. ▪ The day after a quarter is finished (i.e. at 1. April for the 1. January - 31. March Quarter): Run this report for every quarter of the year. ▪ Every specific date: Run this report on a specific date every year. Specify below.

Schedule	
Specify Hour	This setting is only visible if specific hour is selected above. From the list, please select the hour you want to run the report at. PRTG will automatically choose a suitable time within this hour, usually at the beginning of it.
Specify Day	This setting is only visible if the day of week or day of month option is selected above. From the list, please select a day of week or a date of the month you want to run the report. When selecting Last , the report will always run on the last day of the month, regardless of how many days the month has. When selecting a date that does not exist in every month, e.g. the 30th in May, PRTG will automatically run the report on the last day of this month.
Specify Date	This setting is only visible if the specific date option is selected above. Please enter a valid date in the form DD.MM , e.g. 31.12 . The report will be run annually on this date.
Scheduled Processing	This setting is only visible if one of the schedule options is selected above. Define what will be done when generating a report. Choose between: ▪ Save report to disk and send it by email: Create a PDF file of the report, store it, and send it via email. You will find the report in your emails and in the Stored Reports tab. Define an email address below. ▪ Save report to disk only: Create a PDF file of the report and store it. Once finished, you will find it in the Stored Reports tab and a ToDo ticket will be created. By default, PRTG will send out a notification mail to the administrator in this case. ▪ Send report by email only: Create a PDF file of the report and send it via email once it is finished. The report is not permanently stored, but only emailed. Define an email address below. Note: For large PDF reports, PRTG will automatically split the output into separate files to avoid huge PDF files. You can change the number of sensors included into each PDF file by editing the report templates manually. See More¹⁷⁶⁷ section below.
Email Address	This setting is only visible if a send by email option is selected above. Please enter a valid email address the report will be sent to. To enter more addresses, separate them by comma. PRTG will send a message with all recipients in the "To" field of the email. Note: Configuration for outgoing email can be changed in the System Administration—Notification Delivery ¹⁸¹⁵ settings.

Schedule	
Send to User Group	This setting is only visible if a send by email option is selected above. From the drop down list, please choose a user group to send an email with the report to all members of this group (you can edit user groups under System Administration—User Groups 1829). Note: If you define individual email addresses (see field above) and a user group, the report will be sent to the individual email addresses as well as to the members of the selected user group. In both cases, PRTG will send one message with all recipients in the "To" field of the email.
Compression	This setting is only visible if a send by email option is selected above. Specify if the attached report files will be compressed before sending. Choose between: ▪ Uncompressed: The report files will not be compressed before they are sent by email. ▪ Compressed: The report files will be compressed to a ZIP file before they are sent by email.
Period	
Reported Period	Define the time span covered by the report. Choose between: ▪ Current: Use monitoring data of the current period. Define the period type below. ▪ Previous: Use monitoring data of the last period. Define the period type below.
Report Period Type	Define the type of period you want to create a report for. Choose between: ▪ Day ▪ Week ▪ Month ▪ Quarter (January-March, April-June, etc.) ▪ Year Depending on your selection, different period selections are shown below.
Day Period	This setting is only visible if day period type is selected above. Define the hours when a day starts and ends. Choose from the list of hours. Default setting is 0:00-23:59.

Period	
Week Period	This setting is only visible if week period type is selected above. Define when a week starts and ends. Choose between: ▪ Monday-Sunday: A reported week will start on Monday. ▪ Saturday-Friday: A reported week will start on Saturday. ▪ Sunday-Saturday: A reported week will start on Sunday.
Month Period	This setting is only visible if month period type is selected above. Define when a month starts and ends. Choose between: ▪ 1.-last day: A reported month will start on the first and end on last of the month. ▪ 15.-14.: A reported month will start von 15th and end on 14th of the month.
Year Period	This setting is only visible if year period type is selected above. Define when a year starts and ends. Choose between: ▪ 1/1-12/31: A reported year will start on January 1st. ▪ 7/1-6/30: A reported year will start on July 1st.
Report only for specific hours-of-day (Schedule)	Include certain time spans within the defined period only. When a schedule is selected, only monitoring data for specified hours or weekdays within the defined period are included in the report. Select None to include all available monitoring data in the report, or choose a schedule. For example, select the schedule Weekdays to exclude all weekends from the report. The available schedules depend on your configuration. For more information, please see Account Settings—Schedules  section.

Percentile Settings	
Show Percentile	Define if percentiles  will be included in the report. Choose between: ▪ Off: Do not show percentiles ▪ On: Add a column to data tables, showing percentiles for every sensor channel. Note: Percentiles are not available for all report templates. If a template does not support percentiles, they will simply not show up in the report, even when you enable this setting.

Percentile Settings	
Show Percentile	This setting is only visible when showing percentiles. Enter the percentile number you want to calculate. If you choose, for example, to calculate the 95th percentile, enter "95" here and 5 % of peak values will be discarded.
Percentile Average (seconds)	This setting is only visible when showing percentiles. This is the averaging interval in seconds, which is used for percentile calculation. Default value is 300 which is equivalent to 5 minutes.
Percentile Mode	This setting is only visible when showing percentiles. Choose the mode for percentile calculation: ▪ Discrete: Discrete percentile chooses the next smaller discrete value. ▪ Continuous: Continuous percentile interpolates between discrete values. For details, see section Calculating Percentiles .

Report Comments	
Introduction	Define a custom text that will show up on the first page of the report. Please enter a string or leave the field empty.
Footer Comments	Define a custom text that will show up on the last page of the report. Please enter a string or leave the field empty.

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists. ▪ Read: Users in this group can see the object and review its settings. ▪ Write: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. ▪ Full: Users in this group can see the object, as well as review and edit its settings and edit access rights settings. You can create new user groups in the System Administration—User Groups ¹⁸²⁹ settings.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Select Sensors Manually

Click on the **Select Sensors Manually** tab to manually choose sensors that will be included in the report. You will see a split screen: On the left side, your list of objects is shown (empty in the beginning), and on the right side, you see a less colorful view of your device tree, as known from the device tree's [Management](#) ²²² tab. Adding objects to the report is very easy.

Part 7: Ajax Web Interface—Advanced Procedures | 9 Reports

3 Reports Settings

Manual Selection for Reports

■ Add Items

From the device tree on the right side, drag objects and drop them on the list on the left side. This can be entire probes, groups, devices, or single sensors. Each dropped object will be added immediately as a new list item. Repeat this procedure as often as you wish until you have added all desired items to the library. **Note:** Objects that already exist in the list on the left side will be grayed out in the device tree on the right side.

■ Select Sensor Channels

If in the report settings one specific cluster node is selected **and** if you are adding a sensor to the selection, you can specify the sensor channels that will be included in the report. By default, all channels are selected. To exclude a channel from the report, simply remove the check mark in front of a channel's name. **Note:** If **All nodes** is selected in the report's **Cluster Node** selection, the channel selection is not available, but only the primary channel of every sensor is included automatically.

■ Remove

To remove any objects from the report, click on the trash can symbol next the respective list item, or select several list items while holding down the **Ctrl** key and click on the green trash symbol appearing at the top of the list.

Your selection is saved automatically, and there is no undo function. **Note:** The final report will include both sensors selected manually and those selected by tag.

Sensors Selected by Tag

Click on the **Sensors Selected by Tag** tab to view all sensors that are added to the report depending on the report's **Add Sensors by Tag** setting. In the [table list](#)¹⁵⁵, you will see all sensors that are added by tag. This is for your information only, you cannot change sensors here. However, you can switch to the report's **Settings** tab and change the tabs that are used to add sensors. Additionally, you can also exclude sensors with certain tabs there. The final report will include both sensors selected manually and those selected by tag.

For sensors that are added by tag, all sensor channels are included in the report automatically, except **All nodes** is selected in the report's **Cluster Node** selection. In this case, only the primary channel of every sensor is included. **Note:** The final report will include both sensors selected manually and those selected by tag.

Comments

In the **Comments** tab you can enter free text for each object. This can be used for documentation purposes or to leave information for other users.

More

Knowledge Base: Can I change the number of PDFs created by a report?

- <http://www.paessler.com/knowledgebase/en/topic/11863>

Knowledge Base: How do I modify PRTG's report templates?

- <http://www.paessler.com/knowledgebase/en/topic/263>

Knowledge Base: How can I show full channel names below report graphs?

- <http://www.paessler.com/knowledgebase/en/topic/58913>

- [Calculating Percentiles](#)²⁰⁴⁰

7.10 Maps

With PRTG's **Maps** feature (some people might call this 'dashboards') you can create web pages with up-to-the-minute monitoring status information in a customizable layout. Using this unique concept, you can also make your overview pages of live data publicly available, if you like.



Example of a PRTG Map

In this section:

- [Introduction](#) ¹⁷⁶⁸
- [Start Maps](#) ¹⁷⁶⁹
- [Maps Overview](#) ¹⁷⁶⁹
- [Maps Rotation](#) ¹⁷⁷⁰
- [Working with Maps](#) ¹⁷⁷⁰

Introduction

There are countless possibilities for the implementation of maps. For example, this feature can be used to:

- Create network maps with status icons for each device on the map.

- Create quick views of your network that can be shown on network operations center screens.
- Create a quick network overview for publishing on the Intranet, allowing at-a-glance information for management of other employees.
- Create a custom view of the most important sensors in your monitoring setup.
- Create Top 10 lists of the sensors of a specific group or device.

Technically, a map is a usual HTML web page. You can build a schema of your network by choosing from hundreds of device icons and connect them with lines. A map can consist of the following elements:

- A set of map items, which can include device icons, sensor status icons, graphs, data tables, lists of sensors, connection lines, geographical maps, or custom HTML code.
- An optional background image (a JPG, PNG, or GIF file, for example, your company logo or a graphical view of your network).

You can also specify the size of the map. Using the AJAX-based map editor, you can place the items anywhere on the map and you can also change their size. Each map has a unique URL which can be used to link to the map. Users who want to access the map either need an account in your PRTG installation, or can access a public URL of the map if you allow the **Public Access** feature. Public maps contain a unique **Map ID** access key in the URL to block unwanted visitors.

Start Maps

Click the **Maps** entry from the [main menu](#)¹⁸¹ to view or add custom views of your network's status and monitoring data. **Hover** to show other menu items. Choose between:

- **All**
Calls the Maps feature where you can view or add custom views of your network's status and monitoring data.
- **Add Map**
Lets you directly [add](#)¹⁷⁷¹ a new map.
- **Select Map ›**
Show existing maps. **Hover** to show other menu items. Follow the menu path (it is specific to your setup) to select a map.

Maps Overview

In the **All** view, you see a list of all existing maps. Using the links next to a map name, you can perform the following actions.

- Click on the name of a map to view it.
- Click on the **Edit** button to adjust the settings of this map.
- Click on the **Clone** button to create an exact copy of this map. As soon as you click, the map is cloned and the cloned map's settings are shown.

- Click on the **Delete** button to remove this map.
- Click on the **Add Map** button to add a new map.

Please see also [Working with Table Lists](#)¹⁵⁵. Additionally, there is multi-edit available. This enables you to change properties of several objects at a time. For more details, please see [Multi-Edit Lists](#)¹⁷³⁰ section.

Map Rotation

To show several maps in a rotation, mark the desired maps using [multi-edit](#)¹⁷¹⁰ and then select **Map Rotation** from the multi-edit menu. You will be redirected to a page where the rotation is shown. This requires login credentials for PRTG.

It is also possible to set up a **public map rotation** without login: Allow public access in the [settings](#)¹⁷⁸⁰ of the desired maps. Use the corresponding map IDs with its secret keys to build a URL that calls a public map rotation. The URL must have this format: the address of your PRTG server, followed by `/public/mapshow.htm?ids=`. Then list the IDs of the desired maps, each separated by a comma. Each map ID has to be connected with its secret key using a colon:
`http://yourprtgserver/public/mapshow.htm?ids=mapid1:secretkey1,mapid2:secretkey2,mapid3:secretkey3`

While a map rotation is shown, you can change the refresh interval any time when hovering the arrows symbol in the lower right corner. Choose between **10**, **30**, or **60** seconds, **10** minutes or **Refresh** now.

Working with Maps

For detailed information on how to create and edit maps, and to learn how to make them accessible to others, please see the following sections.

- [Maps Step By Step](#)¹⁷⁷¹
- [Maps Designer](#)¹⁷⁷⁴
- [Maps Other Settings](#)¹⁷⁸⁰

7.10.1 Maps Step By Step

In order to create a new map, follow the steps in this section. In the web interface, click on **Maps** entry in the main menu to show the maps main screen.

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

In this section:

- [Step 1: Add Map](#)¹⁷⁷¹
- [Step 2: Add Map Items](#)¹⁷⁷²
- [Step 3: View and Share](#)¹⁷⁷²

Step 1: Add Map

Click on the **Add Map** button. An assistant is shown. Enter a **Map Name** and define **Map Layout** settings (size and optionally a background image). in the **Public Access** section, define whether your map will be visible without login.

For detailed information, see [Maps Other Settings](#)¹⁷⁸⁰ section (Settings).

Part 7: Ajax Web Interface—Advanced Procedures | 10 Maps

1 Maps Step By Step

Add Map (Step 1 of 2)

MAP NAME

Map Name:

MAP LAYOUT

Map Width:

Map Height:

Background Image (optional): Keine Datei ausgewählt.

PUBLIC ACCESS

Allow Public Access:

- ☒ No (map can not be viewed without login)
- ☐ Yes (map can be viewed by using a unique URL)

PAESSLER PRTG Network Monitor 13.4.9.3736+ [Canary] © 2013 Paessler AG PRTG System Administrator Refresh in 575 sec [Follow & Share](#) [Contact Support](#) [Help](#)

Add Maps Assistant Step 1

Step 2: Add Map Items

Click on the **Continue to step 2** button to open the **Map Designer**. **Drag&drop** an object from the items list on the right side, define further properties of the item (mark it in the main window of the map designer and see section **Properties** on the right), and confirm. The item will be added immediately. Repeat this procedure as often as you wish until you have added all desired items to the map. Drag items to change their position. Additionally, you can also draw connection lines between items or edit existing items.

For detailed information, see [Maps Designer](#)¹⁷⁷⁴ section.

Step 3: View and Share

Click on the **View Map** tab to see the appearance of your map. Later, it will be shown the way you see it there. If available for an object, most object names as well as all sensors can be clicked on. It depends on the object's access rights and the currently logged in user account if clicking the links will lead to more detailed information about the object or to an error message indicating insufficient access rights.

Click on the **Get HTML** tab to get the direct URL of your map that you can share with others. For detailed information, see [Maps Other Settings](#)¹⁷⁸² section.

While showing a map, the single map items will be refreshed in the refresh interval defined for this map.

7.10.2 Maps Designer

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

In this section:

- [Use a Proper Browser](#)  1774
- [Basic Design Concept](#)  1774
- [Device Tree Selection](#)  1775
- [Properties Selection](#)  1776
- [Edit Existing Map Items—Properties Box](#)  1777
- [Edit Existing Map Items—Hover Icons](#)  1777
- [Edit Existing Map Items—Using Cursor Keys](#)  1778
- [Draw Connection Lines Between Items](#)  1778
- [Snap To Grid](#)  1778
- [More](#)  1778

Use a Proper Browser

Due to the map designer's extensive scripting capability, it is important that you use a compatible browser when editing maps. We recommend using Google Chrome 31 or later (recommended) or Mozilla Firefox 25 or later. You can use Microsoft Internet Explorer 10 or 11 as well. The maps designer is **not** fully compatible with earlier versions of Internet Explorer or Opera browsers.

Basic Design Concept

Click on the **Map Designer** tab to open the editor. It might take a few moments to load (for **unresponsive script** warnings, please see [More](#)  1778 section below). Here, you can create your map by adding or changing items. The designer screen consists of three main parts: The **Device Tree** on the left side, the current **Map** in the middle, and the **Properties** on the right side.



Each map item takes attributes from both selections.

- **Device Tree** (left): Select the monitoring object which's data will be shown on the map
- **Properties** (right): Define how the map item will be shown

Simply **drag and drop** any object from either side onto the map, or **double-click** on an object. You will always see all changes immediately.

Device Tree Selection

Use the **Device Tree** to select the monitoring object which's data will be shown on the map (this can be a probe, a group, a device, or a single sensor). In order to find the right object, you have the following options:

- Use the arrow symbols at the beginning of each line to open nodes in the device tree to show objects underneath probes, groups, and devices.
- Enter a few characters into the **Search** box in the upper left corner to search for names (or part of names) of objects in your configuration. The search results will be shown immediately. Click on the red x icon to clear your search.

No matter which method you choose to find the desired object, you can always drag any object from the **Device Tree** on a free area of the map to create a new map item. If you drag it onto an existing map item, it will be replaced, while **Properties** and size will remain. You can also select a map item and double click on a **Device Tree** object to replace the map item. If no item is selected, a double-click on an object will add a new map item.

To gain more space for map editing, reduce the size of the **Device Tree** box by dragging its right border to left (or to the right to enlarge it again).

Properties Selection

Use the **Properties** selection to define how the map item will be shown (for example, as an icon, a map, a table, or a graph). Select the appearance in different categories. Hover a property object to get a live preview of it (in most cases). **Note:** If a certain **Properties** object is not available for the selected **Device Tree** object, you will see a corresponding text hint.

There are many different property object types available. Simply click a category's name to show all available types.

- **Icons A, Icons B, Icons C**

These three categories offer a variety of iconic symbols of typical network devices. Below each icon the object name and a sensor overview for the object is shown. This shows how many sensors are in which state. For some sensors, a mini graph is shown as well.

- **Icons A (Static), Icons B (Static), Icons C (Static)**

These three categories offer the same variety of iconic symbols of typical network devices as the category described above. Here, no object data displayed with them, but only the icon is shown.

- **Static Maps**

This category offers free or public domain geographical maps from different sources. For additional geographical maps, please see [More](#)¹⁷⁷⁶ section below. **Note:** The items in this section are independent from the selected **Device Tree** objects.

- **Status Icons**

This category shows options to insert status icons in different styles. These show the object name and an overview of how many sensors are in which state. There is also an object available for audible alert which will play a sound when the number of alarms of the monitored object are > 0. Please note that your browser must support playing embedded sounds (see [More](#)¹⁷⁷⁸ section below for further information).

- **Geo Maps**

In this category you can choose from different geographical map styles from Google: road map, satellite, hybrid, and terrain maps. The location of the currently selected object in the **Device Tree** will be shown on the map as a pin mark. To use this feature, Geo Maps integration must be enabled and you have to enter a **Location** in the settings of the monitoring object you want to use this with. For more information, please see [Geo Maps](#)¹⁷¹⁸ section. **Note:** If Geo Maps integration is disabled, you will only see white boxes instead of map previews.

- **Graphs**

This category offers different graph styles in several dimensions and detail. You can also select graphs including a legend or sensor states.

- **Objects**

Add some simple geometric shapes to your map. The items shown in this tab are always the same; the range displayed does not depend on the selected object in the **Object** field above.

- **Data Tables**

Choose from several tables showing sensor lists for the current selected object. You can also choose from several lists showing sensors in a certain state only.

- **Top 10**

Choose from several tables showing the top 10 of sensors with certain monitoring data, such as least used CPUs, highest bandwidth usage, best availability, slowest websites, etc.

Note: In order to provide live previews, PRTG calculates all top 10 lists from your monitoring data when opening this tab. It may take a few seconds before thumbnails are shown.

- **Custom HTML**

This can be used, for example, to add external images or applets to your map. In order to actually add custom HTML code to your map, please add this item and then click on it to [edit](#) . You can then copy your custom code into the **HTML Before** and **HTML After** fields in the **Properties** box on the right side.

No matter which object you choose, you can always drag any object from the **Properties** box on a free area of the map to create a new map item. If you drag it onto an existing map item, it will be replaced, while its **Device Tree** object attributes and size will remain. You can also select a map item and double click on an object in the **Properties** box to replace the map item. If no item is selected, a double-click on an object will add a new map item.

To gain more space for map editing, reduce the size of the **Properties** box by dragging its left border to right (or to the left to enlarge it again).

Edit Existing Map Items—Properties Box

Click on a map item to select it. You can then edit its attributes with the fields in the upper part of the **Properties** box on the right side:

- **Top, Left, Width, and Height** fields

Enter position and size values for direct positioning. Click the **Save** button to save your settings. Alternative: Use the mouse to move and resize a map item.

- **Layer** field

The layer number defines if an item will be shown on top of or behind another item, if overlapping. The item with the higher number will be shown on top. Enter a positive integer value and click the **Save** button to save your settings. Alternative: Use the arrow symbols in a map item's hover menu to **Bring to front** or **Send to back** an item one layer (see below).

- **HTML**

Click on the arrow symbol underneath to show the **HTML Before** and **HTML After** fields. Any HTML code you enter in these fields will be added before respectively after the map item. Please enter your custom HTML code that embeds an object and click the **Save** button. Your HTML object will be inserted. For example, you could enter the code `` to insert an image of the Paessler logo from the Paessler website.

Edit Existing Map Items—Hover Icons

Hover a map item to show the edit icons for it.

- **Bring to front (arrow up symbol)**

Move this item one layer to the front. This is useful when adding several items to a map that overlap each other.

- **Send to back (arrow down symbol)**
Move this item one layer to the back. This is useful when adding several items to a map that overlap each other.
- **Delete (trash symbol)**
Delete this item. **Note:** Be careful! The item will be deleted immediately without notice and you cannot undo this. Alternative: Select the item and press the **Del** button on your keyboard.
- **Drop Connections (scissors symbol)**
If you have drawn connection lines between two items, you can delete all lines starting from this item. Connection lines will be dropped immediately. **Note:** If a line between two items is not dropped, you've probably drawn it starting from the other item. Try the scissors symbol on the other item instead.

Edit Existing Map Items—Using Cursor Keys

While an object is selected, use the cursor keys to move it by one pixel. Hold the **Shift** key in combination with the cursor keys to move the object by 10 pixels.

Draw Connection Lines Between Items

You can draw connection lines between any map items via drag and drop. Simply click on the grey handles next to an item and drag a line to another item you want to draw a connection to. A line will be shown immediately. This can be useful to indicate network connections or logical coherences between two items. To delete connection lines, click the scissors symbol in the item's [edit icons](#)¹⁷⁷⁷.

Lines between objects are colored dynamically. They will turn red as long as one of the object's icons shows a red **Down** status. This will only affect half of the line, at the end where the red sensor is shown. If both objects connected show a red sensor, this will result in a line that is red all over.

Snap to Grid

Select whether to use **Snap To Grid** or **Don't Snap**, using the buttons underneath the **Device Tree** box. This will affect how map items will be positioned when adding or moving them via drag and drop. The setting is active immediately. With snap to grid enabled, you can place items aligned with the grid only.

More

Knowledge Base: Why does my browser show an unresponsive script warning while loading the Maps Designer?

- <http://www.paessler.com/knowledgebase/en/topic/19483>

Knowledge Base: Where can I download free political/topographical map images for use in PRTG map editor?

- <http://www.paessler.com/knowledgebase/en/topic/7463>

Knowledge Base: Which audible notifications are available in PRTG? Can I change the default sound?

- <http://www.paessler.com/knowledgebase/en/topic/26303>

Knowledge Base: How can I add "deep links" into PRTG's interface for map status icons?

- <http://www.paessler.com/knowledgebase/en/topic/3763>

Knowledge Base: How can I add or edit map objects used for PRTG's maps?

- <http://www.paessler.com/knowledgebase/en/topic/1703>

Knowledge Base: How to setup interactive maps?

- <http://www.paessler.com/knowledgebase/en/topic/2253>

Knowledge Base: Can you re-order or remove columns in sensor lists displayed in maps?

- <http://www.paessler.com/knowledgebase/en/topic/5523>

Knowledge Base: How can I show up-to-date weather information, webcam and radar images in PRTG's maps

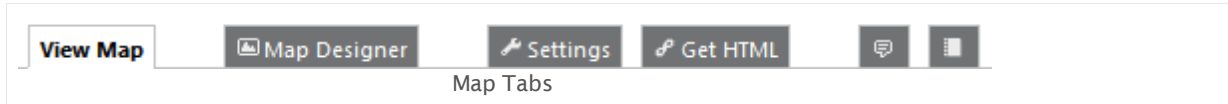
- <http://www.paessler.com/knowledgebase/en/topic/9263>

Knowledge Base: Can I use my own images/icons/logos in PRTG's map editor?

- <http://www.paessler.com/knowledgebase/en/topic/8043>

7.10.3 Maps Settings

Using the Map tabs you can access all functionalities and settings for a map.



View Map

Click on the **View Map** tab any time to show a preview of your map.

Map Designer

Click on the Map Designer tab to edit the contents of your map. Please see [Maps Designer](#)¹⁷⁷⁴ section.

Settings

Click on the **Settings** tab to open a map's general settings. **Note:** When using the **Add Map** dialog, not all of these settings are available. You can change them later by clicking on the **Settings** tab.

Basic Map Settings	
Map Name	Enter a meaningful name for the map.
Security Context	Define the user account that will be used for access to monitoring data. The map will only contain objects which the selected user ⁹⁴ is allowed to view. Please choose a user from the list. The available users depend on your configuration. By default, this is the user that created the map. PRTG Administrator users can change this setting.
Timezone	Define the time zone that will be used for all date-specific options in this map. Select a time zone from the list.
Tag Filter	This setting affects table maps objects. Enter one or more tags separated by space or comma to include sensors in tables. Only sensors with one of the tags entered here will appear in this map's data tables—including sensors which inherit ⁸⁷ tags from parent objects. Please enter a string or leave the field empty. Note: Use with care! This setting will affect all tables of the current map!

Map Layout	
Map Width	Define the width of the map in pixels. Please enter an integer value.
Map Height	Define the height of the map in pixels. Please enter an integer value.
Background Picture	Define if you want to use a background picture for the map. Choose between: ▪ On: Use a background image (define below). ▪ Off: Do not use a background image.
Background Image	This option is only visible if a background picture is enabled above. Click on the Choose File button and select an image from your computer or network. Note: Only images in the format JPG, PNG, and GIF are supported. The file size must be smaller than 2 MB. If you try to upload other images, you will get an error message. In a cluster, background images are not automatically deployed to the other nodes! In order to view maps on other nodes, please copy the background pictures manually to <code>\webroot\mapbackground</code> of the program directory on every node. For detailed information on how to find this path, please see Data Storage ²⁰³⁶ section.
Background Color	Select a background color for this Map. Either enter a hex color code or choose a color from the color selector. The hex color code field will always display the currently defined color.
Public Access	
Public Access	Define if others can see the map. Choose between: ▪ No Public Access: Do not allow public access to the map. Only users with both a login to the PRTG web interface and sufficient access rights can see the map. ▪ Allow Public Access: Allow access to the map using a unique address. The URL contains a key that you can change below.
Secret Key	This field is only visible if public access is enabled above. The key is automatically generated. It is part of the public URL for the map. You can also enter a customized string. We recommend using the default value. For more information on public access, please see the Get HTML ¹⁷⁸² section. Note: The characters comma "," and colon ":" are not allowed in the secret key field!

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists. ▪ Read: Users in this group can see the object and review its settings. ▪ Write: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. ▪ Full: Users in this group can see the object, as well as review and edit its settings and edit access rights settings. You can create new user groups in the System Administration—User Groups settings.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Get HTML

Your PRTG map is like a standalone HTML page. You can make it accessible to others, if you like. Depending on the **Public Access setting** of your map, a visitor will need to provide PRTG user account login data to view the map, or will see the map immediately using a URL containing a secret key. When using this unique key, you can also include your map on another webpage, embedding it via `<iframe>`.

- **Option 1: Link to a web page with the map that requires login credentials**
The shown URL requires login credentials in order to display the map. PRTG will ask the user trying to view the map via this URL for login credentials. **Note:** In the URL, usually the IP address is given via which the page is available. Maybe a NAT translation is set in your firewall, or you may want to use a domain name or a name from a dynamic DNS service for public access. Please customize URL you use for access to your needs.
- **Option 2: Link to a web page that displays the map without a login**
In order to get the shown URL working for public access without a login, enable **Allow Public Access** in the **settings tab** of your map. **Note:** In the URL, usually the IP address is given via which the page is available. Maybe a NAT translation is set in your firewall, or you may want to use a domain name or a name from a dynamic DNS service for public access. Please customize URL you use for access to your needs.

- **Option 3: Show a map inside other web pages using an IFRAME**

For your convenience, this shows source code for adding an **iframe** to another webpage. It includes a URL for direct access. Just copy the code and paste it into your webpage's code. Also enable **Allow Public Access** in the [settings tab](#)¹⁷⁸⁰. **Note:** In the URL, usually the IP address is given via which the page is available. Maybe a NAT translation is set in your firewall, or you may want to use a domain name or a name from a dynamic DNS service for public access. Please customize URL you use for access to your needs.

While a map is shown via these URLs, you can change the refresh interval any time by hovering the arrows symbol in the lower right corner. Choose between **10**, **30**, or **60** seconds, **10** minutes or **Refresh** now.

Comments

In the **Comments** tab you can enter free text for each object. This can be used for documentation purposes or to leave information for other users.

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the PRTG user which conducted the change, and a message. The history log keeps the last 100 entries.

Delete

You can delete the entire map any time by clicking on the trash symbol on the right.

More

Knowledge Base: How to disable links in public maps?

- <http://www.paessler.com/knowledgebase/en/topic/10283>
- [Data Reporting](#)⁹³¹

7.11 Setup

In the setup settings of the PRTG web interface, you can define almost all system settings for PRTG. However, some of the machine-oriented settings are defined using two Windows administration tools (see [Others](#)¹⁷⁸⁵ section below).

In the main menu, click on **Setup** to show the available options.

The screenshot shows the 'Setup Overview Page' of the PRTG Network Monitor web interface. The page is organized into several columns and sections:

- ACCOUNT SETTINGS:**
 - My Account:** Please choose this option to edit your personal account settings like email address, password, timezone, etc.
 - Notifications:** Notifications offer various notification methods through which you are informed in case a sensor trigger is activated.
 - Schedules:** Using Schedules you can pause monitoring for groups, servers or sensors (and notifications) based on time and day of week.
- SYSTEM ADMINISTRATION:**
 - System & Website:** Edit system settings for website, web server, automatic data purging, etc.
 - Notification Delivery:** Click here to manage notification delivery through SMTP, SMS, and HTTP proxy.
 - Probes:** Here you can edit settings for probe management (only necessary if you use remote probes).
 - User Accounts:** Use this link to manage user accounts for this PRTG installation. You can add as many user accounts as desired.
 - User Groups:** Access of users to monitoring objects is controlled using user groups.
 - Administrative Tools:** Perform administrative actions on core and probe systems. Use these tools when instructed by technical support.
 - Cluster (Not Enabled):** Edit the cluster nodes and their connections here (Use the Core Server Admin tool to enable Cluster Mode).
- PRTG STATUS:**
 - System Status:** Displays comprehensive system status information for your PRTG installation.
 - Auto Update:** Download and install the latest version of PRTG.
- OPTIONAL DOWNLOADS AND ADD-ONS:**
 - Client App for Windows (Enterprise Console):** PRTG's native Windows front end can connect to one or more PRTG servers.
 - Client Apps for iOS & Android:** Log into PRTG from your iOS based device (iPhone, iPad, iPod Touch) or Android based device (smartphone or tab).
 - Remote Probe Installer:** Required for installation of remote probes.
- SUPPORT:**
 - Contact Support:** Contact Paessler support to ask a question or to give us your feedback.

At the bottom of the page, there is a 'Setup Overview Page' label and a row of buttons: 'Follow & Share', 'Contact Support', and 'Help'.

Account Settings

- [Account Settings—My Account](#)¹⁷⁸⁶
- [Account Settings—Notifications](#)¹⁷⁹¹
- [Account Settings—Schedules](#)¹⁸⁰¹

System Administration

- [System Administration—System and Website](#)¹⁸⁰⁵
- [System Administration—Notification Delivery](#)¹⁸¹⁵
- [System Administration—Probes](#)¹⁸²¹

- [System Administration—User Accounts](#)  1824
- [System Administration—User Groups](#)  1829
- [System Administration—Cluster](#)  1823

PRTG Status

- [PRTG Status—System Status](#)  1837
- [PRTG Status—Auto Update](#)  1846
- [PRTG Status—Cluster Status](#)  1850

Optional Downloads and Add-Ons

- [Downloads—PRTG Enterprise Console](#)  1852
- [Downloads—Apps for iOS & Android](#)  1852
- [Downloads—Remote Probe Installer](#)  1852
- [Chrome Desktop Notifications](#)  1854

Support

- [Support—Contact Support](#)  1856

Others

There are some settings that have to be made in the [System Administration Tools](#)  1998, running as Windows applications. For more details, please see sections:

- [PRTG Server Administrator](#)  1959
- [PRTG Probe Administrator](#)  1979

7.11.1 Account Settings—My Account

In the **My Account** settings you can define values regarding your own PRTG user currently logged in. All settings in this section are user specific. Some account control options may not be available, but can only be defined by the administrator.

The screenshot displays the 'My Account Settings' page in the PRTG Network Monitor web interface. The page is divided into several sections:

- Account Settings:** Includes tabs for 'My Account', 'Notifications', and 'Schedules'. A QR code is visible on the right.
- USER ACCOUNT:**
 - Login Name: prtgadmin
 - Display Name: PRTG System Administrator
 - Email Address: john.q.public@paessler.com
 - Timezone: (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
 - Date Format: Use System Settings
 - Password: ☒ Don't change, ☐ Specify new password
 - Hash: (empty field)
- AUTO REFRESH AND ALERTING:**
 - Auto Refresh Type: ☒ Refresh page elements using AJAX (recommended), ☐ Refresh whole page, ☐ No auto refresh
 - Auto Refresh Interval (sec): 600
 - Play Audible Alarms: ☒ Never, ☐ On dashboard pages only, ☐ On all pages
 - Tickets as Emails: ☒ Yes, ☐ No
- WEB INTERFACE:**
 - Homepage URL: /welcome.htm
 - Max. Groups/Devices per Group: 10
 - Max. Sensors per Device: 20

At the bottom, there are 'Save' and 'Cancel' buttons, and a footer with 'My Account Settings', 'Follow & Share', 'Contact Support', and 'Help' links.

My Account Settings

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

User Account	
Login Name	Enter the login name for the user.
Display Name	Enter a name for the user for display purposes. This will not be used for login.

User Account	
Email Address	Enter the user's email address.
Timezone	Enter the time zone for the current user.
Date Format	Enter in what format dates will be displayed for the current user. Note: This setting will take effect after the next login.
Password	Define the user's password. For security reasons, the account settings page does not contain the password. Choose between: ▪ Don't change ▪ Specify new password If you choose to specify a new password, enter the old password, and the new password twice. Note: The new password must be at least 8 characters long; no character may occur more than 3 times. It must contain a number and a capital letter.
Hash	The hash (passhash) value can be used as password substitute when calling functions from PRTG's Application Programming Interface (API) that require an authentication. For more information please see Using the PRTG API (Application Programming Interface) section.

Auto Refresh and Alerting	
Auto Refresh Type	Specify how PRTG's web pages will be refreshed for the current user. Choose between: ▪ Refresh page elements using AJAX (recommended): Automatically refresh the single page elements on the web pages. ▪ Refresh whole page: Automatically reload the whole page with every refresh interval. ▪ No auto refresh: Do not automatically refresh web pages.
Auto Refresh Interval (sec)	This setting is only relevant when auto refresh is enabled above. Enter the number of seconds that will be waited between two refreshes. We recommend using 30 seconds or more. Minimum value is 20 seconds. Note: Shorter intervals create more CPU load on the server running the PRTG core server. If you experience load problems while using the web interface (or PRTG maps), please set a higher interval.

Auto Refresh and Alerting

Play Audible Alarms

Define when an audible alarm will be played for the current user on web pages whenever there are [alarms](#)^[143] in PRTG. Choose between:

- **Never:** Do not play sound files on any web pages.
- **On dashboard pages only:** When there are alarms, play a predefined sound on [dashboard](#)^[174] pages only. The sound will be replayed with every refresh of a dashboard page.
- **On all pages:** When there are alarms, play a predefined sound on all web pages. The sound will be replayed with every page refresh.

For more information about audible notifications and supported browsers, please see [More](#)^[1790] section below.

Ticket System

Email Notifications

Define if you want to get emails from the ticket system. Choose between:

- **I want to receive an email whenever a ticket changes:** You will receive an email each time a ticket is assigned to you or your user group, or if a ticket which is assigned to you or your user group is changed. **Note:** If you edit tickets which are assigned to you or your user group, or you assign a ticket to yourself or your user group, you will not get an email.
- **I do not want to receive any emails from the ticket system:** You will not get any emails about tickets.

Web Interface

Homepage URL

Define the user's default page loaded after login and when clicking on the [Home](#)^[174] button in main menu.

Max. Groups/Devices per Group

In order to provide you with a speedy user experience PRTG tries to keep the page size for the page showing the device tree small by automatically folding groups and devices with many items. Define how many groups and devices are shown at maximum before the automatic reduction is performed. We recommend using a value between **10** and **30**.

Web Interface	
Max. Sensors per Device	In order to provide you with a speedy user experience PRTG tries to keep the page size for the page showing the device tree small by automatically folding groups and devices with many items. Define how many sensors are shown at maximum before the automatic reduction is performed. We recommend using a value between 10 and 30 .
Account Control	
Account Type	This setting is only shown for administrator users. However, it is not shown if the user you modify the account settings for is a member of a group with administrative rights. Define the account type for the current user. Choose between: ▪ Read/Write User: The user may change settings. ▪ Read Only User: The user may not edit any settings. This is a good choice for public or semi-public logins. Note: This setting cannot be changed for the default administrator user.
Allow Acknowledge Alarms	This setting is only visible if read only user is enabled above. Acknowledging an alarm is an action which requires write access rights. However, you can explicitly allow this action to read-only users. If enabled, they still do not have write access, but may acknowledge alarms^[144]. Choose between: ▪ Allow: Allow acknowledging alarms for this user. ▪ Deny: The user will not be able to acknowledge alarms.
Primary Group	This setting is only shown for administrator users. Select the primary group for the current user. Every user has to be member of a primary group to make sure there is no user without group membership. Membership in other user groups is optional. For user experience, there is no difference between the primary and other user groups.
Status	This setting is only shown for administrator users. Define the status of the current user. Choose between: ▪ Active: The current user can login to the account. ▪ Inactive: The current user's login is disabled. Use this option to temporarily deny access for this user. Note: This setting cannot be changed for the default administrator user.

Account Control**Last Login**

Shows the time stamp of the user's last login. This setting is shown for your information only and cannot be changed here.

User Groups**Member of**

Shows the groups the current user is member of. Access rights to the device tree are defined on group level. This setting is shown for your information only and cannot be changed here.

Comments

In the **Comments** tab you can enter free text for each object. This can be used for documentation purposes or to leave information for other users.

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the PRTG user which conducted the change, and a message. The history log keeps the last 100 entries.

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: Which audible notifications are available in PRTG 9? Can I change the default sound?

- <http://www.paessler.com/knowledgebase/en/topic/26303>

7.11.2 Account Settings—Notifications

In the notifications settings you can define and change notifications for the currently logged in PRTG user. They can be triggered for certain sensor states and data.

Account Settings

NOTIFICATIONS

Object	Active/Paused	Links	Used by
Email to all members of group Interns	Active	Edit Clone Delete Test Pause	Used by
Email to all members of group PRTG Users Group	Active	Edit Clone Delete Test Pause	Used by
Email to all members of group Tech Staff	Active	Edit Clone Delete Test Pause	Used by
Email to all members of group Webinardemo	Active	Edit Clone Delete Test Pause	Used by
Mail to admin	Active	Edit Clone Delete Test Pause	Used by
Mail to support	Active	Edit Clone Delete Test Pause	Used by
SMS to Fabian via Kentix GSM	Active	Edit Clone Delete Test Pause	Used by
SMS to Tech Staff	Active	Edit Clone Delete Test Pause	Used by
Ticket Notification	Active	Edit Clone Delete Test Pause	Used by

[Add new notification](#)

PAESSLER PRTG Network Monitor 13.4.9.1736+ (Canary) © 2013 Paessler AG PRTG System Administrator Refresh in 320 sec 2012.2013 135617 [Follow & Share](#) [Contact Support](#) [Help](#)

Notification Settings

Note

This section describes one of three steps to set up the notification system in PRTG. A complete notification setup involves:

1. Check and set up the **Notification Delivery** settings. This will tell PRTG how to send messages.
For detailed information, see [System Administration—Notification Delivery](#)¹⁸¹⁵.
2. Check and set up several **Notifications**. This will define the kind of message and its content.
For detailed information, see [Account Settings—Notifications](#)¹⁷⁹¹.
3. Check and set up **Notification Triggers** for objects. These will provoke the defined notifications.
For detailed information, see [Sensor Notifications Settings](#)¹⁶⁹⁰.

For background information, please see [Notifications](#)¹⁷²³ section.

Notifications Overview

Click on the **Notifications** tab to show a list of all existing notifications. Using the links next to the notification name, you can perform the following actions:

- **Delete:** Delete this notification (not possible for predefined notifications)
- **Test:** Trigger this notification immediately for testing purposes. **Note:** When using placeholders, they will not be resolved in a test notification, but the variables will be sent instead.
- **Pause:** Pause this notification. If a notification is paused, no messages will be sent when it is triggered.
- **Clone:** Create an exact copy of this notification. It will be added to the notifications list as **Clone of ...**
- **Used by:** Show a list of objects using this notification.

Please see also [Working with Table Lists](#)^[155]. Additionally, there is multi-edit available. This enables you to change properties of several objects at a time. For more details, please see [Multi-Edit Lists](#)^[1730] section.

Notifications Settings

Click on the **Add new notification** button to add a new notification, or click on the name of an existing notification to edit it.

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Basic Notification Settings	
Notification Name	Enter a meaningful name for the notification, for example, SMS to service team or similar.
Status	Select the status of the notification. Choose between: ▪ Started: This notification will be active. ▪ Paused: Pause this notification. If a notification is paused, no messages will be sent when it is triggered.

Basic Notification Settings

Schedule	Define when this notification will be active. Please select None to set it to always active, or choose a schedule from the list. Usually schedules define when this notification will be active; schedules defined as period list set this notification to inactive at the corresponding time spans. The available options depend on your setup. To add or change existing schedules, please see Account Settings—Schedules section.
Postpone	Define if notifications triggered during Pause status will be sent later on. ▪ No: Discard all notification triggers received while the notification is paused. ▪ Yes: Collect all notification triggers received while the notification is paused. Send out notifications once the pause status ends.

Notification Summarization

Method	Define if and how notifications will be summarized if several notification triggers are received in a certain time span. Note : Regardless of the option chosen here, notifications of Execute HTTP Action and Execute Program are always sent ASAP; they are never summarized. Choose between: ▪ Always notify ASAP: Always send out one notification for each notification trigger received. ▪ Send first DOWN message ASAP, summarize others: When receiving several Down triggers, send the first notification immediately, but summarize other notifications into one message. ▪ Send first DOWN and UP message ASAP, summarize others: When receiving several Down or Up triggers, send each first notification immediately, but summarize other notifications into one message. ▪ Send all DOWN messages ASAP, summarize others: When receiving several Down triggers, send out one notification for each trigger received, but summarize notifications for all other triggers into one message. ▪ Send all DOWN and UP messages ASAP, summarize others: When receiving several Down or Up triggers, send out one notification for each trigger received, but summarize notifications for all other triggers into one message. ▪ Always summarize notifications: When receiving several notification triggers, summarize all notifications into one message, regardless of the kind of trigger received.

Notification Summarization	
Subject for Summarized Messages	Define a subject which will be used when sending summarized notifications. You can use the placeholder %SUMMARYCOUNT for the number of messages which are summarized. Note: The subject you define is only used for Send Email and Amazon Simple Notification Service Message notifications.
Gather Notifications For (Minutes)	Define a time span in minutes for which notifications will be collected for summarization. Please enter an integer value. Note: If you define a high value, for example, 60 minutes, PRTG will send out summarized notifications with a delay of up to one hour.

Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists. ▪ Read: Users in this group can see the object and review its settings. ▪ Write: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. ▪ Full: Users in this group can see the object, as well as review and edit its settings and edit access rights settings. You can create new user groups in the System Administration—User Groups settings.

Notifications Settings—Choose Notification Methods

With the following settings, you can add one or more methods by which a notification message will be sent out. From the list you can only choose one method or combine several methods. Whenever the notification is triggered, it will send out messages or perform actions for all configured methods at a time.

To choose a method, add a check mark symbol in front of the respective setting name. You will then see the options as described below.

Note: In your message, you can use various placeholders. Some are already filled in by default. For a complete list of available placeholders, please see the [More](#) section below.

Send Email

Note: The email **footer** can be set in the [System Administration—System and Website](#) settings. 

Email Address	Enter one or more recipient email addresses. If entering more addresses, separate them by comma. If you want to send to a PRTG user group only, leave this field empty!
Send to User Group	From the drop down list, please choose a user group to send an email with the report to all members of this group (you can edit user groups under System Administration—User Groups). Select None to not use this feature. Note: If you define individual email addresses (see field above) and a user group, the message will be sent to the individual email addresses as well as to the members of the selected user group. In both cases, PRTG will send one message with all recipients in the "To" field of the email.
Subject	Enter the subject of the email. Several placeholders (variables) are used here by default.
Format	Define the kind of email that will be sent. Choose between: ▪ Text ▪ HTML
Message	Depending on the format option selected above, you will see a text or HTML message in this field. A complete message about the sensor status is already predefined. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else). Click on the Reset to default link underneath the text box to do so.
Priority	Define the priority which will be set in the email. Some email clients can show this flag.

Add Entry to Event Log

Logfile	Define the log file the message will be written to. Choose between: ▪ Application: Use the Windows application log file in the event log. ▪ PRTG Network Monitor: Write messages to the PRTG Network Monitor log file in the Windows event log.

Add Entry to Event Log

Event Source	This setting is only relevant when using the Application log file. Enter the source for the event. Usually, this is the name of the application.
Event Type	Select the type of the event. Choose between: ▪ Error ▪ Warning ▪ Information
Event Log Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).

Send Syslog Message

Host/IP	Define the IP address or DNS name of the computer running the syslog server.
Port	Enter the port number on which syslog messages are sent. By default, this is port number 514. Note: Only User Datagram Protocol (UDP) is supported.
Facility	Define the facility information. There are several options available from the list.
Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).

Send Syslog Message—Syslog Message Severity Status

Depending on the status of the sensor triggering the syslog notification the **Severity** level of the message will be set automatically:

 OK	Severity level: Notice (5)
 Warning	Severity level: Warning (4)

Send Syslog Message—Syslog Message Severity Status

 Error	Severity level: Error (3)

Send SNMP Trap

For information about the OIDs used in the contents of the traps sent by PRTG, please see the SNMP Trap documentation in the [More](#)¹⁸⁰⁰ section below.

Host/IP	Define the IP address or DNS name of the computer running the trap receiver.
SNMP Port	Enter the port number on which trap messages are sent. By default, this is port number 162 .
Community String	Enter the device's community string. By default, this is set to public . Please enter a string or leave the field empty.
Specific Trap Code	Enter a code that can help you identify the purpose of the trap. Default value is 0 . Please enter an integer value.
Message ID	This ID helps you identify the origin of the trap. For example, enter 1.3.6.1.4.1.32446.1.1.1
Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).
Agent IP	Define the IP address of the agent. Leave this field blank to use the PRTG web server's IP address.

Send SMS/Pager Message

Note: This notification method needs to be set up in the [System Administration—Notification Delivery](#)¹⁸¹⁵ settings first.

Note: This notification method will use the central proxy settings defined for your PRTG core server. For details, please see [System Administration—System and Website](#)¹⁸¹¹ (section **Proxy Configuration**).

Send SMS/Pager Message

Recipient Number	Define the number the message will be sent to. The format depends on the SMS provider. Usually, you will use a plus sign, followed by country code and number. For example, enter +1555012345 .
Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).

Execute HTTP Action

Note: Regardless of the **Notification Summarization** method chosen above, notifications of **Execute HTTP Action** are always sent as soon as possible (ASAP); they are never summarized.

Note: This notification method will use the central proxy settings defined for your PRTG core server. For details, please see [System Administration—System and Website](#) ¹⁸¹¹ (section **Proxy Configuration**).

URL	Enter the URL the request will be sent to.
Postdata	If you want to send postdata to the URL, please enter it here. You can use placeholders here.

Execute Program

Note: Regardless of the **Notification Summarization** method chosen above, notifications of **Execute Program** are always sent as soon as possible (ASAP); they are never summarized.

Program file	Select an executable file from the list. It will be run every time the notification is triggered. In this list, files in the corresponding / Notifications/EXE sub-directory of the probe system's PRTG installation are shown. In order for the files to appear in this list, please store them as BAT, CMD, DLL, EXE, PS1, or VBS. In order to find the corresponding path, please see Data Storage ²⁰³⁹ section. Note: In a cluster setup, please copy your files to every cluster node installation manually. This makes sure the notification can be executed even when the master node fails. If your custom notification executes an external program, this has to be installed on all cluster nodes as well. Please see also Application Programming Interface (API) Definition ¹⁹⁹³ for detailed information.

Execute Program

Parameter

Enter parameters with which the program file will be started. You can use placeholders here. For example, when using a batch file containing a %1 variable, you can provide a value for this variable here.

Send Amazon Simple Notification Service Message

AWS Access Key ID

Enter your access key as shown in your login area at aws.amazon.com. Please enter a string.

AWS Secret Access Key

Enter your secret access key as shown in your login area at aws.amazon.com. Please enter a string.

Location

Define the location of your Amazon service. Choose between:

- **US-East**
- **US-West**
- **EU-West**

ARN

Enter the Amazon resource name. Please enter a string.

Subject

Enter the subject of the message.

Message

Define the message. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).

Assign Ticket

Note: Regardless of the **Notification Summarization** method chosen above, notifications of **Assign Ticket** are always sent as soon as possible (ASAP); they are never summarized.

For details about the ticket system, please see section [Tickets](#) ¹⁴⁸.

Assign to User or User Group

Specify whether to assign the notification ticket to a user group or to a single user. Choose between:

- **To User Group:** Define the user group which will get this ticket below.
- **To User:** Define the dedicated user who will get this ticket below.

Assign Ticket	
Assign Ticket to this User Group / User	Select the user group resp. user to which the notification ticket will be assigned to from the drop down menu.
Subject	Enter the subject of the ticket. Several placeholders (variables) are used here by default. You can change it to your liking.
Content	Define the message in the ticket. A message with information about the sensor status is already predefined. Several placeholders (variables) are used here. You can change it to your liking.
Close Ticket when Condition Clears	Specify if you want to have the ticket automatically closed when the defined trigger condition clears. Choose between: ▪ Yes: The ticket will be closed automatically. ▪ No: The ticket will remain open after the condition has cleared.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

- [Application Programming Interface \(API\) Definition](#) 

Knowledge Base: What placeholders can I use with PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/373>

Knowledge Base: Documentation of SNMP Traps Sent by PRTG

- <http://www.paessler.com/knowledgebase/en/topic/1133>

Knowledge Base: How can PRTG send instant messages to Jabber, ICQ, MSN, Yahoo, etc., using external software?

- <http://www.paessler.com/knowledgebase/en/topic/14803>

Knowledge Base: Which audible notifications are available in PRTG 9? Can I change the default sound?

- <http://www.paessler.com/knowledgebase/en/topic/26303>

7.11.3 Account Settings—Schedules

In the schedules settings you can define and change schedules for the currently logged in user. You can use schedules to [pause](#)¹⁶¹ monitoring/notify at certain times with the period lists option, respectively activate it at certain times with the time table option. You can also use schedules to define the time spans that are to be covered when creating [reports](#)¹⁷⁴⁹.

The screenshot displays the 'Account Settings' page in PRTG Network Monitor, specifically the 'Schedules' tab. The page header includes navigation links like Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. A status bar at the top right shows 'New Alarms: 3', 'New Log Entries: 118', and various status icons. The main content area is titled 'SCHEDULES' and shows a list of 8 predefined schedules. Each schedule row includes an 'Object' column with the schedule name and time range, a 'Links' column with 'Edit' and 'Delete' buttons, and a 'Used by' column with a 'Used by' button. The schedules listed are: Saturdays [GMT+0200], Sundays [GMT+0200], Weekdays [GMT+0200], Weekdays Eight-To-Eight (8:00 - 20:00) [GMT+0200], Weekdays Nights (17:00 - 9:00) [GMT+0200], Weekdays Nights (20:00 - 8:00) [GMT+0200], Weekdays Nine-To-Five (9:00 - 17:00) [GMT+0200], and Weekends [GMT+0200]. At the bottom of the list is an 'Add new schedule' button. The footer of the page includes the PAESSLER logo, version information (PRTG Network Monitor 13.4.9.3736+ [Canary]), copyright (© 2013 Paessler AG), user role (PRTG System Administrator), refresh interval (Refresh in 202 sec), and contact information (Follow & Share, Contact Support, Help).

Schedules Settings

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Click on the **Schedules** tab to show a list of all existing schedules. Using the links next to the notification name, you can perform the following actions:

- **Delete:** Delete this notification (not possible for predefined notifications)
- **Used by:** Show a list of objects using this notification.

Please see also [Working with Table Lists](#)¹⁵⁵. Additionally, there is multi-edit available. This enables you to change properties of several objects at a time. For more details, please see [Multi-Edit Lists](#)¹⁷¹⁰ section.

Click on the **Add new schedule** button or click on the name of an existing notification to edit.

Part 7: Ajax Web Interface—Advanced Procedures | 11 Setup
3 Account Settings—Schedules

Home Devices Libraries Sensors Alarms Maps Reports Logs Tickets Setup

[Search...](#)
PRTG NETWORK MONITOR

New Alarms: 3 New Log Entries: 143 !! 45 ! 1 W 12 ✓ 927 H 36 U 29

Add Schedule

BASIC SETTINGS

Schedule Name:

Edit Mode:

- ☒ Use weekday/hour time table
- ☐ Use list of period definitions

All	Mo	Tu	We	Th	Fr	Sa	Su	All off
00:00	✓	✓	✓	✓	✓	✓	✓	00:00 off
01:00	✓	✓	✓	✓	✓	✓	✓	01:00 off
02:00	✓	✓	✓	✓	✓	✓	✓	02:00 off
03:00	✓	✓	✓	✓	✓	✓	✓	03:00 off
04:00	✓	✓	✓	✓	✓	✓	✓	04:00 off
05:00	✓	✓	✓	✓	✓	✓	✓	05:00 off
06:00	✓	✓	✓	✓	✓	✓	✓	06:00 off
07:00	✓	✓	✓	✓	✓	✓	✓	07:00 off
08:00	✓	✓	✓	✓	✓	✓	✓	08:00 off
09:00	✓	✓	✓	✓	✓	✓	✓	09:00 off
10:00	✓	✓	✓	✓	✓	✓	✓	10:00 off
11:00	✓	✓	✓	✓	✓	✓	✓	11:00 off
12:00	✓	✓	✓	✓	✓	✓	✓	12:00 off
13:00	✓	✓	✓	✓	✓	✓	✓	13:00 off
14:00	✓	✓	✓	✓	✓	✓	✓	14:00 off
15:00	✓	✓	✓	✓	✓	✓	✓	15:00 off
16:00	✓	✓	✓	✓	✓	✓	✓	16:00 off
17:00	✓	✓	✓	✓	✓	✓	✓	17:00 off
18:00	✓	✓	✓	✓	✓	✓	✓	18:00 off
19:00	✓	✓	✓	✓	✓	✓	✓	19:00 off
20:00	✓	✓	✓	✓	✓	✓	✓	20:00 off
21:00	✓	✓	✓	✓	✓	✓	✓	21:00 off
22:00	✓	✓	✓	✓	✓	✓	✓	22:00 off
23:00	✓	✓	✓	✓	✓	✓	✓	23:00 off
All	Mo off	Tu off	We off	Th off	Fr off	Sa off	Su off	All off

Edit Schedule Time Table

[Follow & Share](#) [Contact Support](#) [Help](#)

Basic Settings

Schedule Name	Enter a meaningful name for the schedule that describes the defined time span(s) or purpose.
Edit Mode	Select how you want to define a schedule. Choose between: ▪ Use weekday/hour time table: Define a schedule with available checkboxes. Lowest increment is one hour. Note: The time table defines active time slots. ▪ Use list of period definitions: Define a schedule by entering text lines using a specific syntax (see below). Note: The period list defines inactive time slots.
Time Table	This selection is only visible if the time table option is enabled above. Define the schedule. It will be used for monitoring objects, reporting, and notifications. You can set time spans with a precision of one hour by setting check marks. If a box is checked, it means the object is active during this hour, if unchecked, the object will be paused during this hour. You can set check marks individually, or change complete ranges for certain days of the week or time spans.

Basic Settings	
	▪ To add ranges of check marks, use the buttons All, Mo, Tu, We, Th, Fr, Sa, and Su, as well as the time buttons on the left side. ▪ To remove ranges of check marks, use the buttons All Off, Mo Off, Tu Off, We Off, Th Off, Fr Off, Sa Off, and Su Off, as well as the time Off buttons on the right side.
Period List	This field is only visible if period definitions are enabled above. Define the date/time ranges in which the objects using this schedule will be inactive (i.e., paused). During other times, the objects will be active. Enter the ranges in the format ww:hh:mm-ww:hh:mm. For details and examples, see Schedules Settings—Period Definition Syntax below.
Access Rights	
User Group Access	Define which user group(s) will have access to the object you're editing. A table with user groups and right is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights: ▪ Inherited: Use the settings of the parent object. ▪ None: Users in this group cannot see or edit the object. The object does not show up in lists. ▪ Read: Users in this group can see the object and review its settings. ▪ Write: Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings. ▪ Full: Users in this group can see the object, as well as review and edit its settings and edit access rights settings. You can create new user groups in the System Administration—User Groups settings.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Schedules Settings—Period Definition Syntax

Define one or more periods of time during which the object using this schedule will be **inactive**. In each line, enter one range in the format **ww:hh:mm-ww:hh:mm**: weekday, hour, minute.

- **Possible values for ww**: mo, tu, we, th, fr, sa, su.

- **Possible values for hh:** Enter the hour in 24 hours format (no AM/PM allowed), i.e. a number between 00 and 23.
- **Possible values for mm:** Enter the minute, i.e. a number between 00 and 59.

Example

In the following, find an example of a schedule that pauses an object during the weekend as well as on Wednesday evenings.

```
fr:19:30-mo:06:05  
we:18:45-we:23:00
```

Any object using this schedule will be paused from Friday, 7:30 p.m. to Monday, 6:05 a.m. as well as on Wednesday from 6:45 p.m. to 11 p.m. It will be active during the other times.

7.11.4 System Administration—System and Website

In the system and website settings you can define global values regarding the PRTG system, web site appearance, web server settings and performance, auto update, etc.

System & Website Settings

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Web Server and Website Settings	
Web Server IP Address	This is the IP address the PRTG web server is running on. This setting is shown for your information only and cannot be changed here. To change this setting, please use the PRTG Server Administrator 1959 .
Web Server Port	This is the port number the PRTG web server is running on. This setting is shown for your information only and cannot be changed here. To change this setting, please use the PRTG Server Administrator 1959 .
PRTG Site Name	When using the web interface, the site name is shown in the title bar of your browser window. It is also used by default in notification emails. Please enter a string.
DNS Name	If your PRTG web interface is (additionally) reachable via a DNS name, please enter it here. It is e.g. used by default in notification emails to generate links. Please enter a string.
Active Directory Domain	In order to use Active Directory Integration 1991 , please enter the name of your local domain. Please enter a string or leave the field empty.
Active Directory Access	Define which user account will be used to configure Active Directory access. This account will be used to query the AD for existing groups. Choose between: ▪ Use the PRTG core service account (usually LOCAL SYSTEM): Use the same Windows user account configured for the "PRTG Core Server Service". In a default installation, this is the "local system" Windows user account. If this account does not have the right to query all groups of your Active Directory you should not use this option.

Web Server and Website Settings	
	▪ Use explicit credentials: Define a user account that will be used by PRTG to authenticate against the Active Directory. This should be a user account with full access to all of your Active Directory groups.
Active Directory Access User	This field is only visible if the use of explicit credentials is chosen above. Enter the Windows user account name which will be used to authenticate for Active Directory configuration.
Active Directory Access Password	This field is only visible if the use of explicit credentials is chosen above. Enter the password for the Windows user account which will be used to authenticate for Active Directory configuration.

Geo Maps	
Map Service Provider	Select if and how you want to integrate the Geo Maps feature into the web interface. If enabled, PRTG uses the first line of the location setting of an object¹⁴¹ to show it on a geographical map. Please choose a map provider: ▪ Do not show maps (disables Geo Maps integration): Disable Geo Maps integration and do not show geographical maps in the web interface. ▪ MapQuest: Use MapQuest to show geographical maps. This is the recommended option. ▪ Nokia Maps: Use Nokia Maps to show geographical maps. ▪ CloudMade (API key required): Use CloudMade to show geographical maps. Please sign up for an API key on their developer website to use this service. ▪ Google Static Maps (API key required): Use Google Static Maps to show geographical maps. Please sign up for a Google Maps API v2 key to use this service. Note: As of PRTG version 13 you will need to acquire a Google Maps API v3 key! For more information about the different map providers, please see the More¹⁸¹³ section below.
Map Type	This setting is only visible for some map providers. Depending on the chosen provider, several options are shown. Each will show map tiles in a different appearance. Please choose a map type from the list.

Geo Maps

API Key (required)

This field is only visible if you selected a provider that requires an API key. Please obtain your personal key and paste it here. For more information on how to get an API key, please see the [More](#)  section below. Please enter an alphanumeric string.

Scanning Intervals

Available Intervals

Define the intervals available in the drop down list of [every object's settings](#) . In the text field, enter one value in each line. Use **s**, **m**, **h**, and **d** for defining seconds, minutes, hours, and days. By default, there are following scanning intervals defined:

30s: 30 seconds

1m: 1 minute

5m: 5 minutes

10m: 10 minutes

15m: 15 minutes

30m: 30 minutes

1h: 1 hour

4h: 4 hours

6h: 6 hours

12h: 12 hours

1d: 1 day

Note: We recommend to not use intervals shorter than 10 seconds to prevent system overload. Intervals below 10 seconds are not officially supported!

Uptime Threshold

Minimum Allowed Uptime Threshold

Define which uptime in percent will be regarded as 100 percent. This setting affects the colors shown next to the sensor icons in reports. Select one of the predefined values between **90 %** and **99.999 %**.

Data Purging Limits: Select for how many days historic data remains accessible

Data purging enables you to automatically delete unnecessary data to free up disk space and improve system performance. You can define different time spans for several kinds of data. For further information on storage locations, please see [Data Storage](#) ^[2036] section.

Logfile Records	Define how long records in the system logfile Log Database.db will be kept. Enter a value in days. All entries older than this value will be deleted from the log file automatically. Keep this value as low as possible to enhance system performance.
Web Server Log Records	PRTG creates one web server log file every day. Define how many web server log files will be kept. Enter a value in days. All web server log files older than this value will be deleted automatically.
Historic Sensor Data	Define for how many days historic sensor data will be kept for all sensors. It is used to create reports ^[1749] of monitoring data. Enter a value in days. Depending on the used intervals and the number of sensors in your setup, the file containing this data can become large. For smaller installations (500 sensors or less) a value of 365 should be fine. Historic sensor data is the basis for reports on monitoring data. If you decrease this value, there will be less historic monitoring data available!
Toplist Records	Define how long toplist records for Flow ^[1934] and Packet Sniffer ^[1932] sensors will be kept. Enter a value in days. We recommend using 30 days here.
Closed Tickets	Define how long tickets which are in status closed will be kept. Enter a value in days.
Reports	Reports generated in PDF format are stored on disk for later reference. Define the maximum age for these reports. Enter a value in days. All reports older than this value will be deleted automatically.
Configuration Auto-Backups	PRTG creates one backup of your configuration every day. Define the maximum age for these backups. Enter a value in days. All configuration backup files older than this value will be deleted automatically.
Full HTTP Sensor (PhantomJS) Screenshots	Define how long the screenshots of the HTTP Full Web Page Sensor ^[526] (PhantomJS browser engine) will be kept. Enter a value in days. PRTG will delete older screenshots with every sensor scan.

Unusual Detection

The unusual detection can set sensors to an **Unusual status**^[121] when there are values that are untypical for the time span they're measured in, compared to historic monitoring results. When disabled (both settings to **Never**), sensors will never be shown as unusual. **Note:** You can enable and disable unusual detection for any object (e.g. for a device, or an entire group) in the **Object Settings**^[141].

Show Unusual When	Define when a sensor will be shown as unusual, comparing the weekday. Choose between: ▪ Never: Disable unusual detection for weekday average. ▪ 24h average is <80% or >120% of weekday average ▪ 24h average is <50% or >200% of weekday average ▪ 24h average is <20% or >500% of weekday average (recommended) ▪ 24h average is <10% or >1,000% of weekday average ▪ 24h average is <1% or >10,000% of weekday average
Show Unusual When	Define when a sensor will be shown as unusual, comparing the hour-of-day. Choose between: ▪ Never: Disable unusual detection for hour-of-day average. ▪ 24h average is <80% or >120% of hour-of-day average ▪ 24h average is <50% or >200% of hour-of-day average ▪ 24h average is <20% or >500% of hour-of-day average (recommended) ▪ 24h average is <10% or >1,000% of hour-of-day average ▪ 24h average is <1% or >10,000% of hour-of-day average
Logging	Define if unusual events will be written to the log file. Choose between: ▪ Do not log unusual events ▪ Write unusual events into the log

Similar Sensors Detection

Similar sensors detection enables PRTG to analyze sensor data for similarities. The detection will run in the background with low priority. The recommended setting for similar sensors detection is to let PRTG automatically decide how many channels will be analyzed. However, you can also override this setting. **Note:** When similar sensors analysis is turned off or you have exceeded 1,000 sensors and have chosen the automatic analysis depth option, the similar sensors entry will not be shown in the main menu bar.

Analysis Depth	Define the number of channels PRTG will analyze to detect similarities between sensors or turn the analysis off. Choose between: ▪ Manage automatically based on sensor count (recommended): The analysis depth depends on the total number of sensors you have configured. PRTG will analyze all channels for up to 500 sensors, and only the primary sensor channels for up to 1,000 sensors. If exceeding 1,000 sensors, the analysis will be turned off. ▪ Analyze primary channels only: Only the primary channels of sensors are analyzed. Be aware of potentially high CPU load of PRTG when choosing this setting for more than 1,000 sensors. ▪ Analyze all channels (higher CPU load): Similarity detection is applied to all channels. Be aware of potentially high CPU load of PRTG when choosing this setting for more than 500 sensors. ▪ Turn analysis off: No similarity detection will take place. Choose this option if you are not interested in the analysis results or you want to keep PRTG's CPU load at a minimum.

Auto-Discovery Settings

Specific Hour	Auto-discoveries can produce a certain load, so you can define at which hour of the day auto-discoveries ^[190] should be run when configured on a daily or weekly Discovery Schedule . Choose a full hour between 0:00 and 23:00 .

PRTG Software Auto-Update

When a New Version is Available	Define how PRTG will react to available software updates. This option will be used with the Auto Update ^[184] function. Choose between:

PRTG Software Auto-Update

- **Automatically download and install the latest version:** Any new PRTG version will be downloaded and installed automatically as soon as your installation detects that there is a newer version available (a check is performed once per day). **Note:** Without prior notice, installation will restart the PRTG Windows services and may also include a server restart.
- **Automatically download the latest version and alert the admin:** Any new PRTG version will be downloaded automatically as soon as your installation detects that there is a newer version available (a check is performed once per day). After successful download, PRTG will create a ToDo message for the administrator.
- **Alert the admin only:** When PRTG detects that there is a newer version available, it will not download updates automatically, but create a ToDo message only. You can still download updates manually on the [Auto Update](#) ¹⁸⁴⁶ page.

Release Channel

PRTG updates are delivered in different release channels. You can choose between maximum stability, or most early access to new features. Please choose between:

- **Stable: Updated about once per month (most conservative option, recommended):** These are our best tested versions. Choose this channel for live environments you have to depend on!
- **Preview: Updated about once per week:** Versions in this channel are already thoroughly tested in our labs, but may still contain limitations in certain monitoring configurations. Choose this channel if you are willing to take a little risk for the benefit of getting new features and bug fixes a little earlier.
- **Canary: Updated daily (testing only, should not be used on live systems):** Updated every night. Use with CAUTION! Software versions in this channel are not tested yet, might contain severe bugs, and are provided for testing purposes only. We strongly recommend to **not** use those versions in live environments you have to depend on!

For more information about the different release channels, please see the blog article linked in the [More](#) ¹⁸¹³ section below.

Proxy Configuration	
Use Proxy Server	We recommend using PRTG with a direct internet connection. However, if you need to use a proxy, you can configure according settings here. Choose between: ▪ No, use direct connection to the Internet: Do not use a proxy. Use this setting if there is a direct internet connection available to the server running the PRTG core server. ▪ Yes, in our network a proxy is mandatory: Define proxy settings below. Note: Proxy settings are valid for Auto-Update¹⁸⁴⁶, Activate the Product⁶⁰, obtaining Geo Maps¹⁷¹⁸ tiles, and for sending out HTTP and SMS text message Notifications¹⁷⁹⁴.
Proxy Server	This setting is only visible if proxy usage is enabled above. Enter the address of the proxy server that will be used for outbound connections. Please enter a valid address.
Port	This setting is only visible if proxy usage is enabled above. Enter the port of the proxy server that will be used for outbound connections. Please enter an integer value.
Use Proxy Credentials	This setting is only visible if proxy usage is enabled above. Determine whether the proxy server needs credentials. Choose between: ▪ Yes: Define credentials below. ▪ No: Do not use credentials for proxy connections.
Username	This setting is only visible if proxy credentials are enabled above. Enter a username for proxy authentication. Please enter a string.
Password	This setting is only visible if proxy credentials are enabled above. Enter a password for proxy authentication. Please enter a string.

User Interface	
Graph Type	Select how graphs are displayed throughout the web interface and in reports¹⁷⁴⁶. ▪ Use area charts (recommended): Display filled graphs. ▪ Use line charts: Display graphs using single lines only. We recommend using area charts, as they're better to read. Note: Graphs containing data from more than one cluster node will always be displayed with line charts automatically.

User Interface	
Performance Strategy	Select if you want to enable performance improvements for the web interface. ▪ All Features: Show all features and live data (recommended): Provide full functionality and show all menu items. ▪ More Speed: Limit features and delay display (experimental): Improve reaction time and speed of the web interface by delaying display of monitoring data and hiding some features. For more information on how to speed up the web interface, please see More ¹⁸¹³ section below.
Contact Support Links	In a PRTG installation running on a commercial license key, a link to the Contact Support ¹⁸⁵⁶ form is displayed in the lower right corner, enabling you to send us comments and/or support requests about our software at any time. You can switch this feature off and on. Choose between: ▪ Show 'Contact Support' links for all users (except read only users): Show support links for all users with write access. The links will never be shown for users set to read only. ▪ Hide 'Contact Support' links for all users: Do not show support links. This setting is valid for all user accounts.
Social Network Links	You can follow PRTG on your favorite social network if you want to. If you do not want to see the social network buttons in PRTG, you can hide these. Choose between: ▪ Show 'follow' links for social network to all users: Links to social networks will be displayed in PRTG (default). ▪ Hide 'follow' links for all users: Links to social networks will not be displayed in PRTG.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: What placeholders can I use with PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/373>

Knowledge Base: How can I speed up PRTG—especially for large installations?

- <http://www.paessler.com/knowledgebase/en/topic/2733>

Knowledge Base: Which provider should I use for PRTG's "Geo Maps" feature?

- <http://www.paessler.com/knowledgebase/en/topic/34603>

Knowledge Base: Which domains and ports does the GeoMaps feature use?

- <http://www.paessler.com/knowledgebase/en/topic/35823>

Knowledge Base: How do I get a Google Maps API key for use in PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/32363>

Knowledge Base: Which limitations apply when using the Google Maps API in PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/7913>

Knowledge Base: How and where does PRTG store its data?

- <http://www.paessler.com/knowledgebase/en/topic/463>

Paessler Blog: Version 12 of PRTG introduces "Continuous Rollout"

- <http://www.paessler.com/blog/2012/04/25/>

7.11.5 System Administration—Notification Delivery

In the notification delivery settings you can define global settings for notification delivery. If you do not want to use a specific notification method, just leave the respective fields empty.

Note

This section describes one of three steps to set up the notification system in PRTG. A complete notification setup involves:

1. Check and set up the **Notification Delivery** settings. This will tell PRTG how to send messages.
For detailed information, see [System Administration—Notification Delivery](#)  1815.
2. Check and set up several **Notifications**. This will define the kind of message and its content.
For detailed information, see [Account Settings—Notifications](#)  1791.
3. Check and set up **Notification Triggers** for objects. These will provoke the defined notifications.
For detailed information, see [Sensor Notifications Settings](#)  1690.

For background information, please see [Notifications](#)  1723 section.

Notification Delivery Settings

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Email Options	
Email Templates	Choose which templates will be used for all emails sent. ▪ Use standard email templates (Recommended): Use this option if you are not sure what to use. These templates offer the best compatibility with all email clients. ▪ Use templates from previous version (for upgrade installations from V7 only): This option is provided for update installations from V7 only. Use it if you have updated from PRTG version 7 and really want to continue using the old email templates. This can be useful when using custom HTML templates in PRTG 7 format. Depending on the option selected, the content of the other fields in this section changes.

Email Options	
Email Header (HTML)	Define the HTML text that will be used as the header for each HTML mail. To reset this field to its default value, click on the trash can icon left to the field or enter a single star symbol * (and nothing else).
Email Footer (HTML)	Define the HTML text that will be used as a suffix to every HTML mail. To reset this field to its default value, click on the trash can icon left to the field or enter a single star symbol * (and nothing else).
For Text Mails	Select if a footer will be added to plain text mails. Choose between: ▪ Append text footer (default): Add a text footer to all text mails. Define the text below. ▪ Do not append the footer Append text footer: Do not add a footer to text mails.
Email Footer (Text)	Define a text that will be used as a suffix to every plain text mail (if enabled above). You can use several placeholders in email templates. See the More ¹⁸¹⁶ section below for more information. To reset this field to its default value, click on the trash can icon left to the field or enter a single star symbol * (and nothing else).

SMTP Delivery	
SMTP Delivery Mechanism	Define how mails are sent using Simple Mail Transfer Protocol (SMTP). Choose between: ▪ Direct delivery using built-in mail relay server (default): Use the SMTP relay server built into PRTG. This server manages its own email queue. For each email, it will look up the target SMTP server via the MX record of the target domain, and send the email. ▪ Use SMTP relay server (recommended inside LANs/NATs): Set up your own SMTP relay server to send emails. Enter data below. ▪ Use two SMTP relay servers (primary and fallback server): Set up two own SMTP relay servers—one primary and one as fallback server. Enter data below. Note: When monitoring inside your NAT or LAN it is often a good idea to use your own LAN-based relay server to deliver notification emails quicker.

SMTP Delivery	
Sender Email	Enter an email address that will be used as sender of all emails. This setting is global and can only be changed centrally here.
Sender Name	Enter a name that will be used as sender of all emails. This setting is global and can only be changed centrally here.
HELO Ident	Enter the HELO Ident for SMTP. This must be a unique name, preferably the DNS name of the machine running PRTG. See SMTP RFC 2821: The sender-SMTP must ensure that the domain parameter in a HELO command is a valid principal host domain name for the client host.
SMTP Relay Server	This field is only visible if SMTP relay server is enabled above. Enter the IP address or DNS name of the SMTP relay server.
SMTP Relay SMTP Port	This field is only visible if SMTP relay server is enabled above. Enter the port number the SMTP relay server is running on. Standard value is 25.
SMTP Relay Authentication	This field is only visible if SMTP relay server is enabled above. Select the kind of authentication required for the SMTP server. Choose between: ▪ No authentication is required: Use SMTP without authentication. ▪ Use standard SMTP authentication: Use standard authentication. ▪ SASL authentication is required: Use secure authentication via Simple Authentication and Security Layer (SASL).
SMTP Relay Username	This field is only visible if SMTP authentication is enabled above. Enter a valid user name.
SMTP Relay Password	This field is only visible if SMTP authentication is enabled above. Enter a valid password.
Use Encrypted Connection	This field is only visible if SMTP relay server are enabled above. Enter the security level for SMTP connections. Choose between: ▪ Never: Use insecure connection with plain text transfer. ▪ If supported by server: Use a secure connection (default).

SMTP Delivery	
SSL Method	This setting is only visible if SMTP relay server and encryption are enabled above. It is only relevant for secure connections. Select the SSL or TLS version which is supported by your SMTP device. We recommend using the default value. If you do not get a connection, try with another setting.
SMTP Relay Server (Fallback)	These fields are only visible if the option for two SMTP relay servers is enabled above. Please see respective settings for primary SMTP relay server above.
SMTP Relay SMTP Port (Fallback)	
SMTP Relay Authentication (Fallback)	
Use Encrypted Connection (Fallback)	
SSL Method (Fallback)	
SMTP Relay Username (Fallback)	
SSL Method (Fallback)	
SMTP Relay Username (Fallback)	
SMTP Relay Password (Fallback)	
Security (Fallback)	

SMS Delivery
Note: Although PRTG has built-in support for the Application Programming Interface (API) of some SMS providers, we cannot officially provide support regarding these SMS service providers. If you have technical questions about SMS delivery beyond PRTG, please contact your SMS provider directly. Note: Instead of using a pre-configured provider you can always use a custom URL, enabling you to use extended parameters (this is also an alternative when using providers for which we offer pre-configured options).

SMS Delivery

You need an internet connection to send text messages via the HTTP API. For information about sending SMS via separate hardware using third party software, please see the [More](#)  section below.

Configuration Mode	Define how you want to select an SMS provider. Choose between: ▪ Select a SMS provider from a list of providers: Select a provider from a list below. ▪ Enter a custom URL for a provider not listed: Use another provider and enter the service URL manually below.
Service Provider	This field is only visible if the provider list is enabled above. Choose a service provider from the list. PRTG offers a small incomplete list of providers. Note: Some providers might require a port configuration in your firewall. See More  section below for more information.
Username	This field is only visible if the provider list is enabled above. Enter a user name for the service provider account.
Password	This field is only visible if the provider list is enabled above. Enter a password for the service provider account.
API ID / Account	This field is only visible if the provider list is enabled above. Some providers need an additional API ID or account information. If provided, enter it here. Please enter a string or leave the field empty.
Custom URL	This field is only visible if the custom provider option is enabled above. From the documentation of your SMS provider, please enter the service URL that is used to send SMS messages. Use the following placeholders for the recipient phone number and the text message: %SMSNUMBER, %SMSTEXT.
Maximum Length of Text	Some SMS providers will not allow SMS messages exceeding a certain amount of characters. PRTG will restrict the number of characters according to the length specified in this field. A value of 0 means the SMS is sent at its full length.

Note: The [notification](#)  methods "Send SMS/Pager Message" and "Execute HTTP Action" will use the central proxy settings defined for your PRTG core server. For details, please see [System Administration—System and Website](#)  (section **Proxy Configuration**).

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: How can I send SMS text message notifications via a modem or a mobile phone with PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/393>

Knowledge Base: Why do I get a connection timeout message when sending SMS via bulksms?

- <http://www.paessler.com/knowledgebase/en/topic/12253>

Knowledge Base: Which URLs does PRTG use for its preconfigured SMS providers?

- <http://www.paessler.com/knowledgebase/en/topic/13123>

Knowledge Base: How do I send SMS with PRTG using a Clickatell account?

- <http://www.paessler.com/knowledgebase/en/topic/34213>

Knowledge Base: How can PRTG send instant messages to Jabber, ICQ, MSN, Yahoo, etc., using external software?

- <http://www.paessler.com/knowledgebase/en/topic/14803>

Knowledge Base: Can GMail / Google Apps be used for SMTP relay?

- <http://www.paessler.com/knowledgebase/en/topic/2823>

Knowledge Base: How can I enable Notification Delivery Logging?

- <http://www.paessler.com/knowledgebase/en/topic/55363>

7.11.6 System Administration—Probes

In the probe management settings you can define the settings for probe connections.

Probes Settings

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

Probe Connection Settings	
Access Keys	Enter a list of access keys, one in each line. Every (remote) probe that want to connect to this PRTG installation has to use one of these keys. For information how to set this key for a probe, please see PRTG Probe Administrator ^[1979] (Probe Settings) section.
Allow IPs	Enter a list of remote probe IPs that will be accepted when connecting to this PRTG installation; each IP address in one line. The local probe (127.0.0.1) is always allowed automatically. Allowed IPs are checked first (before denied IPs). You can use PRTG's syntax for IP address ranges here (for information about the syntax please see Define IP Ranges^[2000] section). ▪ [Empty]: An empty field does not allow any remote probes (but only the local probe). Please enter IP addresses to allow remote probe connections. ▪ any: Enter the word any to automatically allow all remote probe connections. Note: This is recommended for use in Intranets only! Note: If the IP address of your remote probe changes regularly (e.g. due to an internet provider assigning IP addresses dynamically), please enter the potential IP range for this remote probe or use the any option.
Deny IPs	Enter a list of remote probe IPs that will not be accepted when connecting to this PRTG installation; each IP address in one line. This is useful to explicitly deny connections from certain remote probes you do not want to include in your setup any more (e.g., for a certain time). Access to IP addresses allowed above will be denied if you enter them here. This is useful to allow access to an IP range in the field above, but deny access to a single IP address. You can use PRTG's syntax for IP address ranges here (see Define IP Ranges ^[2000] section).

Probe Connection Settings

Deny GIDs

Enter a list of GIDs, each global ID (GID) in one line. The access to matching GIDs will be denied. If you remove a remote probe from the device tree or if you deny a remote probe after installation, its global ID (GID) will be automatically entered here. This specific remote probe will not be able to connect anymore. Denying GIDs is more precise than denying IPs, where other remote probes at the same location could be excluded too.

Settings from the PRTG Server Administrator program

IPs for Probe Connections

This is a list of the IP addresses on which the PRTG listens to incoming probe communication. **0.0.0.0** means that the server listens on all local network adapter IPs. This setting is shown for your information only and cannot be changed here. To change this setting, please use the [PRTG Server Administrator](#) .

Probe Connections Port

This is the port on which PRTG listens to incoming probe communication. This setting is shown for your information only and cannot be changed here. To change this setting, please use the [PRTG Server Administrator](#) .

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Remote Probe Setup

Find more information about setting up remote probes in the [Multiple Probes and Remote Probes](#)  section.

More

- [Define IP Ranges](#) 

7.11.7 System Administration—Cluster

In the cluster settings you can define the cluster settings. During [Failover Cluster Configuration](#)²⁰²⁰, the cluster settings were already pre-defined. See the [cluster status](#)¹⁸⁵⁰ to see if all nodes in your cluster are properly connected.

Cluster Settings

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

You can set up two, three, four, or five nodes in one cluster. In the table of the cluster settings, the information of each node is written in one line.

Node Settings	
Node Name	Enter the name of the node (for display purposes).
Node ID	The ID is unique for every node. We recommend using the default value.
Node State	You can set the state for every failover node. Choose between: ▪ Active: Set the node to be active. ▪ Inactive: Set the node to be not active. It will be disabled in the cluster configuration. It will then be not an active part of the cluster and will not appear in the cluster status¹⁸⁵⁰ any more. This setting is not available for the master node of a cluster. The master is always set to Active.
IPs/DNS Names used for Connections Between Nodes	Define the IP addresses or DNS names that will be used for the connections between the nodes. You can enter different values for every node-node connection. For example, in the field #2 => #1, enter the IP address that the second cluster member (this is a failover node) will use to connect to the master node server.

Click on the **Save** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

In order to put a cluster node to **Maintenance Mode**, please see [PRTG Status—Cluster Status](#)¹⁸⁵⁰.

The entire setup process for a cluster requires several different steps. For more information and step-by-step guidance, please see [Failover Cluster Configuration](#)²⁰²⁰ section.

7.11.8 System Administration—User Accounts

PRTG administrator users can change all users' account settings and add new users.

User Accounts Overview

- To change a user's settings, select it from the list by clicking on the user name. The available setting options are the same as shown in the [My Account](#)¹⁷⁸⁶ settings of the currently logged in user (plus some account control options).
- To add a new user, click on the **New User** button. The options are the same as for existing users (with slight differences).
- To batch-add several users at once in a simple way, please click the **Multiple New Users** button. In the dialog box appearing, select an existing [user group](#)¹⁸²⁰ from the drop down menu and enter or paste a list of email addresses. They can be separated by space, comma, semicolon, or a new line. Click the **Add** button to confirm. For each address, PRTG will create a new local user account within the selected user group, carrying the email address as value for **Login Name**, **Username**, and **Email Address**. A new password will be generated automatically and sent to the email address.
- To add a new user group, click on the **New User Group** button. The options are the same as for existing groups (with slight differences).
- Access rights in PRTG are given via user groups. Please make sure a user account is member of the right [user group](#)¹⁸²⁹ and give access to this group in your device tree [object's settings](#)¹⁴¹.

Note: Predefined objects cannot be deleted!

User Accounts Settings

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

User Account	
Login Name	Enter the login name for the user.
Display Name	Enter a name for the user for display purposes. This will not be used for login.
Email Address	Enter the user's email address.
Timezone	Enter the time zone for the current user.
Date Format	Enter in what format dates will be displayed for the current user. Note: This setting will take effect after the next login.

User Account	
Password	Define the user's password. For security reasons, the account settings page does not contain the password. Choose between: ▪ Don't change ▪ Specify new password If you choose to specify a new password, enter the old password, and the new password twice. Note: The new password must be at least 8 characters long; no character may occur more than 3 times. It must contain a number and a capital letter.
Hash	The hash (passhash) value can be used as password substitute when calling functions from PRTG's Application Programming Interface (API) that require an authentication. For more information please see Using the PRTG API (Application Programming Interface) ¹⁹⁹³ section.

Auto Refresh and Alerting	
Auto Refresh Type	Specify how PRTG's web pages will be refreshed for the current user. Choose between: ▪ Refresh page elements using AJAX (recommended): Automatically refresh the single page elements on the web pages. ▪ Refresh whole page: Automatically reload the whole page with every refresh interval. ▪ No auto refresh: Do not automatically refresh web pages.
Auto Refresh Interval (sec)	This setting is only relevant when auto refresh is enabled above. Enter the number of seconds that will be waited between two refreshes. We recommend using 30 seconds or more. Minimum value is 20 seconds. Note: Shorter intervals create more CPU load on the server running the PRTG core server. If you experience load problems while using the web interface (or PRTG maps ¹⁷⁸⁸), please set a higher interval.
Play Audible Alarms	Define when an audible alarm will be played for the current user on web pages whenever there are alarms ¹⁴³ in PRTG. Choose between: ▪ Never: Do not play sound files on any web pages.

Auto Refresh and Alerting

- **On dashboard pages only:** When there are alarms, play a predefined sound on [dashboard](#)^[174] pages only. The sound will be replayed with every refresh of a dashboard page.
- **On all pages:** When there are alarms, play a predefined sound on all web pages. The sound will be replayed with every page refresh.

For more information about audible notifications and supported browsers, please see [More](#)^[1790] section below.

Ticket System

Email Notifications

Define if you want to get emails from the ticket system. Choose between:

- **I want to receive an email whenever a ticket changes:** You will receive an email each time a ticket is assigned to you or your user group, or if a ticket which is assigned to you or your user group is changed. **Note:** If you edit tickets which are assigned to you or your user group, or you assign a ticket to yourself or your user group, you will not get an email.
- **I do not want to receive any emails from the ticket system:** You will not get any emails about tickets.

Web Interface

Homepage URL

Define the user's default page loaded after login and when clicking on the [Home](#)^[174] button in main menu.

Max. Groups/Devices per Group

In order to provide you with a speedy user experience PRTG tries to keep the page size for the page showing the device tree small by automatically folding groups and devices with many items. Define how many groups and devices are shown at maximum before the automatic reduction is performed. We recommend using a value between **10** and **30**.

Max. Sensors per Device

In order to provide you with a speedy user experience PRTG tries to keep the page size for the page showing the device tree small by automatically folding groups and devices with many items. Define how many sensors are shown at maximum before the automatic reduction is performed. We recommend using a value between **10** and **30**.

Account Control	
Account Type	This setting is only shown for administrator users. However, it is not shown if the user you modify the account settings for is a member of a group with administrative rights. Define the account type for the current user. Choose between: ▪ Read/Write User: The user may change settings. ▪ Read Only User: The user may not edit any settings. This is a good choice for public or semi-public logins. Note: This setting cannot be changed for the default administrator user.
Allow Acknowledge Alarms	This setting is only visible if read only user is enabled above. Acknowledging an alarm is an action which requires write access rights. However, you can explicitly allow this action to read-only users. If enabled, they still do not have write access, but may acknowledge alarms^[144]. Choose between: ▪ Allow: Allow acknowledging alarms for this user. ▪ Deny: The user will not be able to acknowledge alarms.
Primary Group	This setting is only shown for administrator users. Select the primary group for the current user. Every user has to be member of a primary group to make sure there is no user without group membership. Membership in other user groups is optional. For user experience, there is no difference between the primary and other user groups.
Status	This setting is only shown for administrator users. Define the status of the current user. Choose between: ▪ Active: The current user can login to the account. ▪ Inactive: The current user's login is disabled. Use this option to temporarily deny access for this user. Note: This setting cannot be changed for the default administrator user.
Last Login	Shows the time stamp of the user's last login. This setting is shown for your information only and cannot be changed here.
User Groups	
Member of	Shows the groups the current user is member of. Access rights to the device tree are defined on group level. This setting is shown for your information only and cannot be changed here.

Comments

In the **Comments** tab you can enter free text for each object. This can be used for documentation purposes or to leave information for other users.

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the PRTG user which conducted the change, and a message. The history log keeps the last 100 entries.

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: Which audible notifications are available in PRTG 9? Can I change the default sound?

- <http://www.paessler.com/knowledgebase/en/topic/26303>

7.11.9 System Administration—User Groups

PRTG administrator users can change existing user groups or add new ones, and define the users that are member of a certain group.

All the security settings as well as further rights management are conducted via the user groups. This means that group membership controls what a user may do and which objects the user will see when logged in. The actual rights for each object can be defined in an object's settings. There, you can define different rights for each user group.

- To change a user group's settings, select it from the list by clicking on the group name.
- To add a new user, click on the **New User** button. The options are the same as for existing users (with slight differences).
- To batch-add several users at once in a simple way, please click the **Multiple New Users** button. In the dialog box appearing, select an existing [user group](#)^[1826] from the drop down menu and enter or paste a list of email addresses. They can be separated by space, comma, semicolon, or a new line. Click the **Add** button to confirm. For each address, PRTG will create a new local user account within the selected user group, carrying the email address as value for **Login Name**, **Username**, and **Email Address**. A new password will be generated automatically and sent to the email address.
- To add a new user group, click on the **New User Group** button. The options are the same as for existing groups (with slight differences).
- By default, there aren't any rights set for a newly created PRTG user group. Initially, users in this group will not see any objects in the PRTG device tree. Please edit your device tree [object's settings](#)^[143] and set access rights for your newly created user group in the **Inherit Access Rights** section. **Note:** The easiest way is to set these rights in the [Root Group Settings](#)^[224].

Note: The multi-edit option is not available for the standard user groups PRTG Administrators and PRTG Users Group.

Note: Predefined objects cannot be deleted!

User Groups Settings

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

User Group Settings

User Group Name	Enter a name for the user group.

User Group Settings	
Administrative Rights	Define if the members of this group will be PRTG administrators. If you enable this option, all members of this group will have full access to all monitoring objects, maps, reports, user accounts and user groups, and they can change the PRTG monitoring configuration. Choose between: ▪ Yes: Give full PRTG administrator rights to all members of this group. ▪ No: Do not make members of this group administrators. Access to monitoring objects for users that are member of this group will be controlled by the Access Rights settings defined in the Object Settings^[141] of Probes, Groups, Devices, or Sensors. Note: This option is especially useful in combination with the Active Directory option below.
Default Homepage	Enter a PRTG internal web page. This will set the default homepage for all new users created with this group. A user will be redirected to this page after logging in. This concerns new users either added by an Active Directory login or by the Add multiple users feature.
Use Active Directory	Define if this PRTG user group will be connected to a group in your active directory. Choose between: ▪ Yes: Connect this group to an AD group. Choose below. For detailed information, please see Active Directory Integration^[199]. ▪ No: Do not use Active Directory integration for this group, but choose local user accounts instead.
Active Directory Group	If a valid Active Directory Domain is set in the System Administration—System and Website^[1805] settings and Active Directory integration is enabled above, a drop down menu will appear, showing the groups in your Active Directory. Choose the group whose members will be able to log in to PRTG using their Active Directory domain credentials. All of those AD users will be in the security context of the PRTG group you're about to create/edit. For detailed information, please see Active Directory Integration^[199]. If your Active Directory contains more than 1000 entries in total, PRTG will display an input field instead of a drop down menu. This is done due to performance reasons. In the input field, you can enter the group name only. PRTG will then add the prefix automatically.

User Group Settings	
New User Type	If Active Directory integration is enabled above, define the default rights for all new users in this user group. If a user logs in for the first time using Active Directory credentials, PRTG will automatically create a new local user account for this user, applying the user type defined here. Choose between: ▪ Read/Write User: The user may change settings. ▪ Read Only User: The user may not edit any settings. This is a good choice for public or semi-public logins.
Allowed Sensors	Define if members of this user group will be able to create all available sensor types or only specific ones. Choose between: ▪ Users may always create all sensor types: No restrictions for group members are applied. ▪ Users may create certain sensor types only: Choose the allowed sensor types below. This option is especially interesting for a Managed Service Provider (MSP).
Users May Create These Sensor Types	This field is only visible if you defined that the users in this group are only allowed to create certain sensor types. A list of all available types is shown with their name. Select the desired types by adding check marks in front of the respective lines. You can also select and deselect all items by using the check box in the table head.
Ticket System Access	Define if the members of this user group will be able to use PRTG's ticket system¹⁴⁶. Choose between: ▪ Members can use the Ticket System: No restrictions for group members are applied. ▪ Members can NOT use the Ticket System: The Tickets¹⁸² option in the main menu bar¹⁸² will not be visible to users in this group.
Members	
Members	This setting is available only if Active Directory integration is disabled above. Define which local user accounts will be a member of this group. To add a user account from the list, add a check mark in front of the user name. The user accounts available depend on your setup.

Primary Users

User List

Shows a list of all user accounts with this group set as primary group. This is shown for information purposes only. You can change it in a [user account's settings](#)  1824.

Comments

In the **Comments** tab you can enter free text for each object. This can be used for documentation purposes or to leave information for other users.

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the PRTG user which conducted the change, and a message. The history log keeps the last 100 entries.

Click on the **Continue** button to store your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

7.11.10 System Administration—Administrative Tools

With the administrative tools you can start system specific processes for debugging purposes. Use them if Paessler's technical support staff advises you to do so. You can start the respective processes by clicking on the **Go!** button on the right.

The screenshot shows the PRTG Network Monitor web interface. At the top, there's a navigation bar with links like Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. Below this is a status bar with 'New Alarms: 3', 'New Log Entries: 149', and various status icons. The main section is titled 'System Administration' and has a sub-tab 'Administrative Tools'. Under this, there are two categories: 'CORE ADMINISTRATIVE TOOLS' and 'PROBE ADMINISTRATIVE TOOLS'. Each category lists several tasks with a brief description and a 'Go!' button.

Task	Description	Action
Create Database Snapshot	Saves current configuration as ZIP file in folder 'Configuration Auto-Backups'.	Go!
Write Core Status File	Creates a debug file on the core system.	Go!
Clear Caches	Clears the webserver's internal caches for geomaps and Active Directory authentication.	Go!
Load Lookups	(Re)load the lookup files from the 'lookups/custom' folder.	Go!
Recalculate PRTG Graph Data Cache	Note: due to the recalculation the PRTG Core Server Service will be restarted.	Go!
Restart Core Server	Restarts the PRTG Core Server Service.	Go!
Write Probe Status Files	Creates a set of debug files on all probe systems.	Go!
Restart All Probes	Restarts all probe services.	Go!
Probe #1 "Local probe"	connected from: 127.0.0.1:62323 Last Data: 20.12.2013 14:06:47 (0 sec ago) (Mitteleuropäische Zeit)	Restart Probe

At the bottom of the page, there's a footer with 'PAESSLER', 'PRTG Network Monitor 13.4.9.3736+ [Canary]', '© 2013 Paessler AG', 'PRTG System Administrator', 'Refresh in 547 sec', and '20.12.2013 14:06:13'.

System Administrative Tools

Core Administrative Tools

Core Administrative Tools

Create Database Snapshot

This will create a snap shot of your PRTG configuration. This action can take up to 100 seconds. Once finished, you will find a ZIP file containing a *.dat file in the **Configuration Auto-Backups** sub folder of your [PRTG data directory](#). If you're running a PRTG cluster, this action is executed on the cluster node you're currently logged in to. The ZIP file follows the name pattern **PRTG Configuration (Snapshot YYYY-MM-DD HH-MM-SS).zip**.

Core Administrative Tools

Write Core Status File	This will create status files of your PRTG core server. You will find the two text files in the Logs (System) sub folder of your PRTG data directory ^[2036] . If you're running a PRTG cluster, this action is executed on the cluster node you're currently logged in to. The files are named Core Status.txt and Core Memory.txt . They are overwritten each time you click this button.
Clear Caches	PRTG caches tiles for Geo Maps ^[1718] and user data for Active Directory Integration ^[1991] . Use this button to delete the cache if you encounter broken geo map tiles, or if you changed a user's password in the Active Directory.
Load Lookups	This will (re)load the lookup files ^[2001] from the \lookups\custom folder. In this folder your customized lookup files are stored. If you have created a new lookup file or changed something in an existing lookup file, it might be necessary to load or to reload these files.

Probe Administrative Tools

Probe Administrative Tools

Write Probe Status Files	This will create status files of your PRTG probes. Status files will be written for the local probe running on the PRTG core server (if you're running a PRTG cluster, on the cluster node you're currently logged in to) as well as for all remote probes configured (if any). On the respective systems, you will find four text files in the Logs (System) sub folder of the PRTG data directories ^[2036] . The files follow the name pattern Probe Memory XX.txt , ProbeState XX.txt , ProbeState AXX.txt , and ProbeState BXX.txt . They are overwritten each time you click this button.
Restart All Probes	This will restart all PRTG probes as well as the local probe Windows service. If there are any remote probes ^[2011] configured, the probe Windows services on the respective remote systems will be restarted as well. In order to start single probes only, please see below. Note: If you're running a PRTG cluster, this action is executed on the cluster node you're currently logged in to. In this case, remote probes are only restarted if you're logged in to the primary master node. The cluster probe Windows service of failover nodes is not restarted if this action is executed on the master node. If you want to restart the cluster probe Windows service of a failover node, please log in to this failover node's web interface and click on the same button there.

Probe Administrative Tools

Probe [#Number]
"[Name]"

Information about the connection status is shown. If the probe is currently connected, the field shows the source IP address and port number used by the probe. For the "Local probe", the IP will always be IP 127.0.0.1. You will also see information about the date when the last data packet was received from the probe. If you want to restart a single probe, please click on the **Restart Probe** button. **Note:** Entries for every single probe are following.

Setup—Topics

- [Account Settings—My Account](#)  1786
- [Account Settings—Notifications](#)  1791
- [Account Settings—Schedules](#)  1801
- [System Administration—System and Website](#)  1805
- [System Administration—Notification Delivery](#)  1815
- [System Administration—Probes](#)  1821
- [System Administration—User Accounts](#)  1824
- [System Administration—User Groups](#)  1829
- [System Administration—Cluster](#)  1829
- [System Administration—Administrative Tools](#)  1833
- [PRTG Status—System Status](#)  1837
- [PRTG Status—Auto Update](#)  1846
- [PRTG Status—Cluster Status](#)  1850
- [PRTG Status—Activation Status](#)  1851
- [Downloads and Add-Ons](#)  1852
- [Chrome Desktop Notifications](#)  1854
- [Support—Contact Support](#)  1856

Others

There are some settings that have to be made in the [System Administration Tools](#)  1958, available as native Windows applications. For more details, please see sections:

- [PRTG Server Administrator](#)  1959
- [PRTG Probe Administrator](#)  1979

7.11.11 PRTG Status—System Status

System Status

Click on the **System Status** tab to view relevant system information you may need for debugging or when the support team asks you to provide system information in order to support you with PRTG.

Software Version and Server Information	
PRTG Version	Shows the exact version of the build your PRTG installation is currently running on.
Auto-Update Status	Shows the latest auto-update message available from Software Auto-Update ¹⁸⁴⁶ . For example, the message will indicate any PRTG updates ready to be installed.
Operating System	Shows the exact Windows version build and service packs, the number and kind of CPUs, and the computer name, of the system the PRTG core server is installed on. If you're running a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to. Note: When running PRTG on virtual systems, not all of the mentioned values may be available.
Server Time	Shows the date and time of the system the PRTG core server is installed on. If you're running a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.
Server CPU Load	Shows the current CPU load of the system the PRTG core server is installed on. If you're running a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.
Username	Shows the username ¹⁷⁸⁶ of the PRTG user you're currently logged in as.
Browser	Shows the name and user agent string of the browser you're currently viewing this page with.

Licensing	
Licensee	Shows the Name of the license ^[57] you're using for this installation of PRTG. Licensee (name) and license key together build your license information.
Key	Shows the beginning and the end of the license ^[57] key you're using for this installation of PRTG. Licensee (name) and license key together build your license information.
Edition	Shows the PRTG edition you're using for this installation of PRTG. This determines how many sensors you can use in your monitoring (see below).
Activation Status	Shows the activation status of this installation of PRTG. Usually, activation is done automatically on first start-up. Only if PRTG cannot connect directly to the internet, a manual activation is necessary. For details, please see Activate the Product ^[60] .
Software Maintenance	Shows the days remaining for your active maintenance contract. You can buy maintenance for each PRTG license. With an active maintenance contract you may download any available updates and use our premium email support, without additional costs.
Number of Sensors	Shows the number of sensors you can use in your monitoring, with your current edition of PRTG (see above). If you reach the limit, each new sensor that you create will be set to a Pause status automatically. In order to upgrade your license right now, click on the Need more sensors? Click here to upgrade! button to visit our web shop. Editions that allow an unlimited number of sensors do not restrict the number of possible sensors by license, so you can create sensors until the performance limit is reached. This means you can use about 20,000 sensors per core server (depending on your system's performance, sensor types, and scanning intervals); for details, see system requirements linked in the More ^[1845] section below.

System Startup Log

Shows the log information created during the last startup of the PRTG core server. If you're running a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

Cluster Status

This box is only visible if you're running a PRTG cluster. This section lists all cluster nodes configured in your monitoring.

Node [Number]	Shows the name of the cluster node as well as the node type (primary/secondary node) and status (current master/failover node). Additionally, all connections from this node to the other cluster nodes are shown, as illustrated on the PRTG Status—Cluster Status 1850 page.

Local Status

This box is only visible if you're running a PRTG cluster. This section lists information about the cluster node you're currently logged in to.

Server State Cluster Messages	Shows internal summary information about the current node and the communication between the nodes. You might be asked about this by Paessler's technical support staff.

Cluster Connections

This box is only visible if you're running a PRTG cluster. This section lists information about the connections between the different cluster nodes.

State of Local Node	Shows Treeversion and size of the Server Volume, both internal system information.
State of Cluster Members	For each cluster node, the name and IP address is shown, as well as a state CRC code, the time stamp of the last "keep alive" signal sent, the current size of the buffer, and the remote IP.
Message State of Cluster Members	For each cluster node, the name, IP address, and unique identifier is shown, as well as the connection state, and statistic information about the cluster message system which is used for the communication between the different nodes.

Auto-Discovery Tasks

Currently Running	Shows the number of auto-discovery tasks that are currently running. A high number of auto-discovery tasks can negatively influence system performance.

Background Tasks

Historic Data	Shows if PRTG is re-calculating the historic data cache in the background. If so, you will see the tasks to do until done. Usually, this calculation is done after every core server restart.
Toplist Buffer	When using xFlow ^[1934] or Packet Sniffer ^[1932] sensors, PRTG stores Toplist data. The data stream received is buffered and written to the data directory of the core system. Depending on the number and size of the data stream as well as the hard disk and system performance of the core system, the buffer size can rise. When reaching a buffer size of 500 , Toplist data is dropped which can lead to incorrect Toplist values for the sensors.
Toplist Upgrade	If you recently updated from an older PRTG version (7 or 8), Toplist data needs to run through a one-time conversion process. While conversion is running you may experience a considerably slow monitoring system. Usually, you will see n/a here.

Database Objects

Shows statistic information about your monitoring configuration. This information might be necessary when contacting Paessler's technical support staff.

Probes	Shows the total number of probes ^[238] configured.
Groups	Shows the total number of groups ^[253] in your configuration.
Devices	Shows the total number of devices ^[272] in your configuration.
Sensors	Shows the total number of sensors ^[290] in your configuration.
User Groups	Shows the total number of user groups ^[1829] in your configuration.
Users	Shows the total number of users ^[1824] configured.

Database Objects	
Notifications	Shows the total number of notifications  configured.
Schedules	Shows the total number of schedules  configured.
Requests/Second	Shows a value calculated from the total number of sensors and the average scanning interval configured. This number indicates how many monitoring requests per second are sent from the probe(s) to the devices in your network. There are no general guidelines what is a "good" value here. This depends on the sensor types used as well as on your system's performance.
Sensors	Shows a list with numbers and types of sensors used in your configuration. Note: In the list, internal short names are used for sensor types instead of the official designations.

Probes	
This section lists all probes configured in your monitoring. If there are no remote probes configured, only the "Local probe" appears in the list, which runs mandatorily on the PRTG core server. Note: If you're running a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to. Remote probes (if any) will only be shown when you're logged in to the primary master node. When logged in to a failover node, the cluster probe running on this node will appear as "Local probe".	
Probe [#Number] "[Name]"	Information about the connection status is shown. If the probe is currently connected, the field shows the source IP address and port number used by the probe. For the "Local probe", the IP will always be IP 127.0.0.1. You will also see information about the date when the last data packet was received from the probe. If you want to restart a single probe, please go to the Administrative Tools Settings .

System Settings	
Web Server URL	Shows the URL to access the PRTG web interface  . If you're running a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

System Settings	
Web Server IPs	Shows all IP addresses the PRTG web server is running at. If you're running a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.
Web Server Ports	Shows the port the PRTG web server is running at. If you're running a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.
Web Server Port Usage	Shows the number of ports used by the PRTG web server.
Incoming Probe Connection Binding	Shows a combination of the two values below.
Incoming Probe Connection IPs	Shows a list of all IP addresses on which your current PRTG installation listens to incoming remote probe connections. This is the same information as shown in the System Administration—Probes settings. 0.0.0.0 means that the core server listens on all local network adapter IPs. In order to change this setting, please open the PRTG Server Administrator on the system of the PRTG core server.
Incoming Probe Connection Port	Shows the port number on which your current PRTG installation listens to incoming remote probe connections. This is the same information as shown in the System Administration—Probes settings. Default port is 23560 . In order to change this setting, please open the PRTG Server Administrator on the system of the PRTG core server.
Probe Allow IPs	Shows all source IP addresses that will be accepted by the core server for incoming remote probe connections. This is the same information as shown in the System Administration—Probes settings and can be changed there. any means that all remote probe connections are accepted, regardless of the IP address of the remote probe system.
Probe Deny IPs	Shows all source IP addresses that will be denied by the core server for incoming remote probe connections. This is the same information as shown in the System Administration—Probes settings and can be changed there. Denied IPs are superior to allowed IPs. If this field is empty, there are no denied IPs. Note: PRTG automatically adds the IP address of a remote probe system to this list when you delete a remote probe from your device tree .

System Settings

DataPath	Shows the path where PRTG stores its configuration, monitoring database, etc. If you're running a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to. In order to change this setting, please open the PRTG Server Administrator 1999 on the system of the PRTG core server (or of the respective cluster node, if applicable).

Web Server Activity

Shows statistic information about the web server since last startup. All values are reset when the core server is restarted. If you're running a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

Time Since Startup	Shows the time that has passed since the PRTG web server was started.
Page Views	Shows the total number of page views on this core server.
Geo Maps	Shows the total number of geo maps shown on this core server.
HTTP Requests	Shows the total number of HTTP requests to this core server.
HTTP Requests > 500/1000/5000 ms	Shows for how many (percent) of the HTTP requests above the page delivery took longer than 500, 1,000, or 5,000 milliseconds.
Slow Request Ratio	Shows a calculated number of the HTTP request values above. The lower this number, the faster is your installation's web interface.

Synchronization

The core server holds the configuration of the entire monitoring and deploys it to the probes. This section shows statistic information about the synchronization of the core server with the local probe and all connected remote probes (if any), since last startup of the core server. All values shown here are reset when the core server is restarted. If you're running a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to. **Note:** Only when logged in to the primary master node you will see synchronization data for remote probe connections.

Synchronization	
Last Synchronization with a Probe	Shows the time stamp of the last probe synchronization, and if there is still something to do.
Probe/Core Message Count	Shows the total number of messages sent between core and probe(s), as well as a calculated message speed value.
Sync Cycle Speed	Shows the time necessary for a full synchronization, as well as an evaluation comment of this time (usually, this will be "OK").
Configuration Requests Sent	Shows the total number of configuration requests and the requests that still have to be sent.
Configuration Requests Deleted	Internal debug information. Usually, this value will be 0.
Configuration Requests With Response	Internal debug information. Usually, this value will be 0.

System Warnings
If there are any warnings they will be shown here. Usually "None" will be shown here.

Core System Memory
Shows machine-oriented information regarding the memory usage of the core server system. If you're running a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

Thread Information
Shows machine-oriented information regarding the threads running on the core server system. If you're running a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

More

Paessler Website: Detailed System Requirements for PRTG Network Monitor

- <http://www.paessler.com/prtg/detailed-requirements>

Knowledge Base: How can I speed up PRTG—especially for large installations?

- <http://www.paessler.com/knowledgebase/en/topic/2733>

7.11.12 PRTG Status—Auto-Update

Whenever a new version of the software is available from the Paessler website PRTG will download the setup file automatically if a direct internet connection is available. The administrator will then receive a [ToDo ticket](#)^[149] with instructions to initiate the update installation.

For customers using a [Freeware or Trial Edition](#)^[19], automatic software updates are available at any time. Customers using a [Commercial Edition](#)^[20] need to have an active maintenance contract so updates are available.

Using Auto-Update

Note: This documentation refers to the **PRTG System Administrator** user accessing the Ajax interface on a master node. For other user accounts, interfaces, or nodes, not all of the options might be available as described. When using a cluster installation, failover nodes are read-only by default.

To view the auto-update page of your PRTG installation, select **Setup | Software Auto-Update** from main menu.

If there is a new version available, you will see detailed information about the available version. Please read these notes carefully!

In order to install an available version, click the **Install Update [version number]** button. You will be asked to confirm installation and license—and that's it!

Click on the button **Show Auto-Update Log** to show corresponding log entries.

PRTG Network Monitor Auto-Update

Here you can automatically update your PRTG installation.

- If you are using the freeware or trial edition you can always update to the latest version for free
- If you are using a commercial edition your license key must be covered by a valid maintenance contract in order to download updates.
- You can always prolong your maintenance at <http://shop.paessler.com>

You can deactivate automatic downloading in the System & Website settings (section "Software Auto-Update Settings").

UPDATE STATUS FOR PRTG NETWORK MONITOR

Remaining Maintenance Days	4711
Latest Message from Auto-Update	[20.12.2013 11:38:26] Version 13.4.9.3736 has been downloaded and will be installed at: 7h 00m
Currently Installed Version	13.4.9.3728 [Canary]
Currently Selected Release Channel	Canary Select Other Release Channel
Latest Version Available from Paessler	13.4.9.3736 NEW! Check For Latest Update and Download
Latest Downloaded Version	13.4.9.3736 NEW! Install Update 13.4.9.3736

File: PRTG Network Monitor 13.4.9.3736 Setup Commercial (Canary).exe

RELEASE NOTES FOR VERSION: 13.4.9.3736

What's New In 13.4.8

- [Sensors] Completely rewritten high-performance Syslog Receiver and SNMP Trap Receiver sensors
- [Sensors] 9 new sensor types for monitoring of service, Cisco UCS, LenovoEMC systems, and NetApp Logical Unit, via SNMP; Volume Fragmentation via WMI; and a new HTTP Push Count sensor
- [GUI] Completely revised and updated look&feel of the Ajax Web GUI
- [Core] PRTG now includes its own ticket system
- Numerous other changes, improvements, and bugfixes

What Was New In Previous Version 13.x.7

- IMPORTANT!** Changed [Core]: When using a secure connection, the PRTG webserver now accepts SSLv3 and TLSv1 with AES or DES only. Note: In former versions, the only accepted encryption was RC4; this is not supported any more. Please make sure you use the latest browser version on your clients. For details, please see our [knowledge base article](#).
- [Sensors] 2 new sensor types for IPFIX monitoring
- [Sensors] Massive performance improvements for all VMware (SOAP) sensors
- [Sensors] Mass improvements and fixes to HTTP sensors and others

For detailed information please visit: [PRTG Release Notes and Version History](#)

[Show Auto-Update Log](#)

PAESSLER PRTG Network Monitor 13.4.9.3728 [Canary] © 2013 Paessler AG PRTG System Administrator Refresh in 21 sec 20.12.2013 14:09:18

Automatic Software Update Page

Manually Install an Interim Update

Not all available updates from Paessler will be pushed to all customers, but they are still available from the website. Sometimes Paessler support may ask you to update to the latest version.

In this case please click the **Download Update [version number]** button. PRTG will then connect to the Paessler servers and download the setup file, regardless of the status of the update-check. **Note:** In order to use this function, a direct internet connection is necessary on the computer running the PRTG core server.

Select Other Release Channel

PRTG is available in three different release channels. For details about continuous rollout and release channels, please see the blog article in the [More](#) ¹⁸⁴⁸ section below.

- **Stable:** Updated about once a month. Best tested versions. We recommended this channel for live environments you have to depend on!

- **Preview:** Updated about once a week. Thoroughly tested in our labs, but may still contain limitations in certain monitoring configurations
- **Canary:** Updated every night. Use with **caution!** Software versions in this channel are not tested yet, might contain severe bugs, and are provided for testing purposes only. We strongly recommend to **not** use those versions in live environments you have to depend on!

In order to change the release channel you receive updates from, please open the [System Administration—System and Website](#)¹⁸¹⁰ page by clicking on the **Select Other Release Channel** button and change settings in the **PRTG Software Auto-Update** section.

Notes

There are a few things we ask you to consider regarding automatic software updates:

- In order for auto-update to work the machine running the PRTG core server needs direct internet access. If a proxy connection is needed, please configure it in the [System Administration—System and Website](#)¹⁸¹¹ settings. For details about the update servers, see [More](#)¹⁸⁴⁸ section below.
- During installation the core server may be restarted without notice.
- Existing remote probes will be updated automatically, causing short downtimes in monitoring of remote locations. In rare cases a manual update of remote probes is required after you update the core server. In these cases you will be notified in the device tree, and monitoring of remote locations will be interrupted until you perform the manual update on the system(s) running the remote probe(s).
- In a cluster installation the update needs to be installed on one node only. The new version will then be deployed to all other cluster nodes automatically (causing a short downtime for the monitoring on the cluster nodes, one after another).
- If you run several individual PRTG core servers that are not in a cluster, for example, in combination with the [Enterprise Console](#)¹⁸⁹⁰, an update has to be initiated and confirmed for each single core server.
- You can disable automatic downloading in the [System Administration—System and Website](#)¹⁸¹⁰ settings. Updates will then only be downloaded on request, when you click on the **Download Update [version number]** button.

More

Knowledge Base: Which servers does PRTG connect to for Software Auto-Update and for Activation?

- <http://www.paessler.com/knowledgebase/en/topic/32513>

Knowledge Base: Which information does PRTG send back to Paessler?

- <http://www.paessler.com/knowledgebase/en/topic/28103>

Paessler Blog: Version 12 of PRTG will introduce "Continuous Rollout"

- <http://www.paessler.com/blog/2012/04/25/news/prtg-12-introduces-continuous-rollout>

7.11.13 PRTG Status—Cluster Status

Cluster Status

Click on the **Cluster Status** tab to view all nodes connected to the cluster. This tab is only available if you're running PRTG in [cluster mode](#)^[81]. Following information is shown:

- Cluster Status with all connected nodes as table and graphic
- Cluster Log with all log entries concerning cluster connections

CLUSTER STATUS

Node 1: PRTG Network Monitor (10.0.10.34)
Primary Node (Current Master) [Start Maintenance Mode](#)
Connection To IP State
→ Node 10.0.10.35 10.0.10.35 **Connected**

Node 2: Node 10.0.10.35
Secondary Node (Failover Node, Version: 28728) [Start Maintenance Mode](#)
Connection To IP State
→ PRTG Network Monitor (10.0.10.34) 10.0.10.34 **Connected**

CLUSTER LOG

Date Time	Parent	Type	Object	Status	Message	Cluster Node
20.12.2013 13:57:05	None	Probe	Cluster Probe	Cluster	Cluster: Access denied for node at "10.0.10.33:4741" (Incorrect cluster access key)	PRTG Network Monitor (10.0.10.34)
20.12.2013 13:41:58	None	Probe	Cluster Probe	Cluster	Cluster: Access denied for node at "10.0.10.33:2106" (Incorrect cluster access key)	PRTG Network Monitor (10.0.10.34)
20.12.2013 13:26:52	None	Probe	Cluster Probe	Cluster	Cluster: Access denied for node at "10.0.10.33:3424" (Incorrect cluster access key)	PRTG Network Monitor (10.0.10.34)
20.12.2013 13:11:46	None	Probe	Cluster Probe	Cluster	Cluster: Access denied for node at "10.0.10.33:4712" (Incorrect cluster access key)	PRTG Network Monitor (10.0.10.34)
20.12.2013 12:56:40	None	Probe	Cluster Probe	Cluster	Cluster: Access denied for node at "10.0.10.33:2071" (Incorrect cluster access key)	PRTG Network Monitor (10.0.10.34)
20.12.2013 12:41:33	None	Probe	Cluster Probe	Cluster	Cluster: Access denied for node at "10.0.10.33:3412" (Incorrect cluster access key)	PRTG Network Monitor (10.0.10.34)
20.12.2013 12:26:27	None	Probe	Cluster Probe	Cluster	Cluster: Access denied for node at "10.0.10.33:4745" (Incorrect cluster access key)	PRTG Network Monitor (10.0.10.34)
20.12.2013 12:11:21	None	Probe	Cluster Probe	Cluster	Cluster: Access denied for node at "10.0.10.33:2064" (Incorrect cluster access key)	PRTG Network Monitor (10.0.10.34)
20.12.2013 11:56:14	None	Probe	Cluster Probe	Cluster	Cluster: Access denied for node at "10.0.10.33:3408" (Incorrect cluster access key)	PRTG Network Monitor (10.0.10.34)
20.12.2013 11:41:08	None	Probe	Cluster Probe	Cluster	Cluster: Access denied for node at "10.0.10.33:4731" (Incorrect cluster access key)	PRTG Network Monitor (10.0.10.34)
20.12.2013 11:26:02	None	Probe	Cluster Probe	Cluster	Cluster: Access denied for node at "10.0.10.33:2098" (Incorrect cluster access key)	PRTG Network Monitor (10.0.10.34)
20.12.2013 11:10:55	None	Probe	Cluster Probe	Cluster	Cluster: Access denied for node at "10.0.10.33:3416" (Incorrect cluster access key)	PRTG Network Monitor (10.0.10.34)
20.12.2013 10:55:49	None	Probe	Cluster Probe	Cluster	Cluster: Access denied for node at "10.0.10.33:3416" (Incorrect cluster access key)	PRTG Network Monitor (10.0.10.34)

Example of a PRTG Cluster Status View

Click on the **Start Maintenance Mode** link to put a cluster node in maintenance mode. A node in this mode is still connected to the cluster, but its monitoring results are discarded until you click on the **Stop Maintenance Mode** link. You can use this functionality to explicitly exclude a node from monitoring if you know that the monitoring values will not be accurate, for example, because you're reconfiguring things, etc. During maintenance, a cluster node is displayed with a transparent color in the overview graphic.

For more information about cluster settings, please see [System Administration—Cluster](#)^[82] section.

7.11.14 PRTG Status—Activation Status

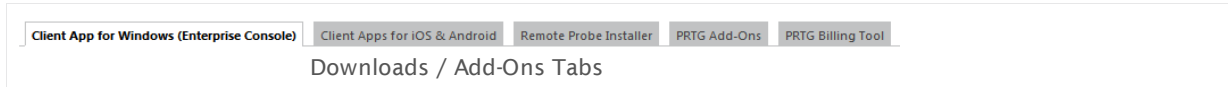
Activation Status

Click on the **Activation Status** tab to view information about the activation status of your PRTG Network Monitor license. For more details about activation, please see [Activate the Product](#)^[60] section.

License Activation Status	
Licensed Edition	Shows the edition of the license you are currently using for this installation of PRTG. This determines how many sensors you can use in your monitoring. If you are running a PRTG cluster, this will show information for the system of the cluster node you are currently logged in to.
Current activation status of your software license	Shows the activation status of your PRTG license. Usually, activation is done automatically on first start-up. The activation status is typically Activation OK . Only if PRTG cannot connect directly to the internet, a manual activation is necessary. For details, please see Activate the Product ^[60] .
Last message about activation	Shows the last message regarding the activation of your license.
Current activation stamp	Shows an internal activation stamp code.

7.11.15 Optional Downloads and Add-Ons

To see optional downloads, select **Setup | Downloads** from main menu. Click on the tabs to switch between different options.



There are the following downloads available:

- [PRTG Enterprise Console](#)  1852
- [Apps for iOS & Android](#)  1852
- [Remote Probe Installer](#)  1852
- [PRTG Add-Ons](#)  1852
- [PRTG Billing Tool](#)  1853
- [Chrome Desktop Notifications](#)  1853

PRTG Enterprise Console

Download the Windows Graphical User Interface (GUI) "Enterprise Console" to the current system. Using it, you can access the PRTG interface with a native Windows application. The version of the Enterprise Console must match your version of PRTG. For more information, please see [Install the Enterprise Console](#)  671 section.

Apps for iOS & Android

PRTG for iOS is a native iPhone application that enables you to use the PRTG web interface with the original iFeeling. You can download PRTG for iOS on iTunes for free. **PRTG for Android** gives you the possibility to monitor PRTG on the go. For more information, please see [More](#)  1853 section below.

Remote Probe Installer

With remote probes you can extend your monitoring to distributed networks that are not directly reachable from your PRTG core installation. The version of the remote probe installer must match your version of PRTG. For more information, please see [Install a PRTG Remote Probe](#)  621 section.

PRTG Add-Ons

This will display a link to the PRTG add-ons page on Google Code. There you will find a collection of various add-ons for PRTG Network Monitor and their source code. For more information, please see [More](#)  1853 section below.

PRTG Billing Tool

This will display a link to information and download of the PRTG Billing Tool. The PRTG Billing Tool is an application that can read PRTG sensor data and generate bills in PDF format. We provide this tool as a basis to develop your own billing applications. For more information, please see [More](#)¹⁸⁵³ section below.

Chrome Desktop Notifications

This tab is only visible if you're accessing the PRTG web interface with Google Chrome browser. For details, please see [Chrome Desktop Notifications](#)¹⁸⁵⁴ section.

More

Paessler Website: SmartPhone Apps for PRTG

- <http://www.paessler.com/apps>

Project Hosting on Google Code: PRTG AddOns

- <http://code.google.com/p/prtg-addons/>

Paessler Website: Billing Tool for PRTG

- <http://www.paessler.com/tools/billingtool>

7.11.16 Chrome Desktop Notifications

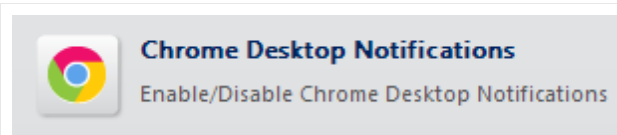
While you are logged in to the PRTG web interface with your Chrome browser, PRTG can use it to show notifications on your desktop whenever there are new alarms in your monitoring.

Desktop notifications will be shown (by default, in the lower right corner of your desktop) whenever there are new alarms after a page refresh. The notification will display the number of new alarms and the current number of each sensor status. Click on **X** to close the notification.



Example of a Chrome Desktop Notification

In Chrome's default configuration, you have to initially allow those notifications for each installation/profile of Google Chrome. To do so, in the PRTG web interface, please click on [Set up](#)¹⁷⁸⁴, then click on **Chrome Desktop Notifications**.



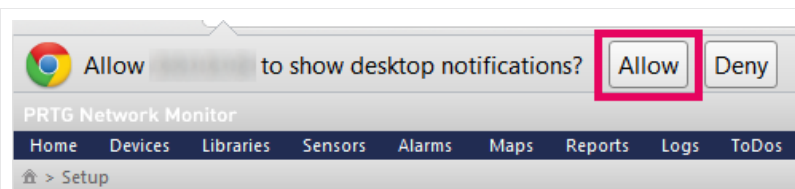
Chrome Desktop Notifications in Setup

Chrome Desktop Notifications Settings

On the settings page, you see one of the following status messages.

Status: Click button below to enable Desktop Notifications

- Click on the **Enable Chrome Desktop Notifications** button to add your PRTG URL to Chrome's list of allowed sites for desktop notifications.
- On top of your Chrome browser window a message will appear, asking you to allow desktop notifications. Click on **Allow** to add the web interface's URL to the allowed sites.



Click on 'Allow' to enable Chrome Desktop Notifications

Status: Sorry, Desktop Notifications cannot be enabled

- Desktop Notifications are explicitly blocked for the PRTG web interface's URL in the Chrome options. Please see [Notifications Settings in Google Chrome](#)¹⁸⁵⁴ below.

Desktop Notifications enabled

- Chrome Desktop Notifications are successfully activated. In order to disable them, please see [Notifications Settings in Google Chrome](#) below.

Notifications Settings in Google Chrome

To disallow or re-allow your web interface's URL for desktop notifications, please edit your Chrome browser's options:

Choose **Options | Under the Hood**, in the **Privacy** section, click on the button **Content settings....** In the **Notifications** section, change settings corresponding to your needs. For example, click on **Manage exceptions...** and remove the URL of your PRTG web interface to disable the feature. Or remove a blocked URL to re-enable the feature again.

7.11.17 Support—Contact Support

To open the **Contact Paessler Support / Send Your Feedback to Paessler** window in PRTG, choose **Setup | Contact Support** from the main menu. You can open this form also via the footer **Contact Support** on any page in PRTG.

On the one hand, you can adapt this page as **feedback** form. Help improve PRTG by providing criticism, praise, bug reports, and feature requests. Any comments are welcome! Your feedback will be handled directly by the Paessler support team.

On the other hand, you can use this function in order to ask for support regarding technical issues. To make the support contact more comfortable, PRTG can automatically attach a screenshot in combination with a **Support Bundle** which contains several selected PRTG log and status files. This information will help the support team a lot in order to analyze any issues you may have encountered with PRTG.

Once you are finished, click on **Submit to Paessler Support** to send your request, or click on **Cancel** to return to the page from which you opened the contact form. You can be sure that you will receive an answer by our support team within one or two business days, no matter whether you provide feedback or you have a question.

Note: PRTG will try to send your feedback / support question to Paessler as an email using Simple Mail Transfer Protocol (SMTP). Please ensure that your PRTG installation is able to send emails to external destinations!

Contact Paessler Support / Send Your Feedback to Paessler

Help us to improve PRTG! We look forward to your criticism, praise, feature requests. Anything. Your feedback will be handled by the Paessler support team and you can expect an email reply within 1-2 business days. Please note: Your PRTG server will try to send this information to Paessler as an email using SMTP (this means that your PRTG must be able to send emails to the outside world).

Having trouble with this feature? You can also open a support ticket on the Paessler website!!

ASK A QUESTION OR GIVE US YOUR FEEDBACK

Your Ticket ID PAExxxx
(if you have one)

Your Email Address

Your Comments

HELP US BY ATTACHING A SCREENSHOT AND/OR SUPPORT BUNDLE

It will be tremendously helpful for us if you attach a screenshot and/or analytical information about your PRTG installation. We call this a 'Support Bundle' and it contains selected log and status files of your PRTG installation which help our team to analyze any issues you may have encountered. The Base Pack contains system status, lists of red and black sensors, core state sensor data, probe health sensor data, and recent log entries (system and probe related), as well as the log files.

Screenshot

Support Bundle

☒ Do not attach screenshot
☐ Create and attach screenshot (recommended)

☒ Attach Base Pack with log files (recommended)
☐ Attach Base Pack with log files and PRTG configuration file
Please choose only when instructed by Paessler support
(Note: contains encrypted passwords legible by Paessler)
☐ Do not attach a Support Bundle

Submit

Cancel

The Support / Feedback Form

Ask a Question or Give Us Your Feedback

Provide the following information in this section of the contact form:

- **Your Ticket ID PAExxx:** If you have already opened a new ticket (either directly via email to support@paessler.com, or via the Knowledge Base, or via the support form on paessler.com), enter its ID here. You can find it in your confirmation email regarding the request we received. You can provide the ID with "PAE" in front or just the number. Otherwise, a new ticket will be created.
- **Your Email Address:** Enter your email address here. You can provide any of your addresses; however, recommended and default is the email address of your PRTG account.
- **Your Comments:** Leave your comments here. It can be feedback or support questions. Please describe your issue as detailed as possible!

Attach a Screenshot and/or Support Bundle

In order to provide as helpful information as possible, you can attach a screenshot of the current page and various support bundles with useful analytical data about your PRTG installation.

In section **Screenshot**, choose between:

- **Create and attach screenshot (recommended):** This will create a screenshot of the currently displayed page in PRTG. It will be sent with your ticket. A preview will be shown below the screenshot section. **Note:** If you encounter issues on a specific page in PRTG, call the contact support form on this page in order to get a screenshot of it.
- **Do not attach screenshot:** No screenshot will be taken. **Note:** We recommend to attach a screenshot in order to understand your request easier and faster.

In section **Support Bundle**, you can choose between several packages which differ in coverage of information:

- **Attach Base Pack with log files (recommended):** Contains log files of your PRTG installation and the following information:
 - System status
 - Lists of sensors regarding their current states
 - Core state data
 - Probe Health sensor data
 - Current log entries
- **Attach Base Pack with log files and PRTG configuration file:** Additionally contains the configuration file. **Note:** Send this package only if our support team told you so! This file contains encrypted passwords readable by Paessler support.
- **Do not attach a Support Bundle:** No files will be attached. Choose this option only when sending feedback.

Part 8

Enterprise Console

8 Enterprise Console

The Enterprise Console (formerly called "Windows GUI") is one alternative [interface](#)^[77] you can use to connect to the PRTG core server to configure your setup, view monitoring results and keep an eye on your network. It is a native Windows application for fast access to data and monitoring management.

The Enterprise Console provides extended popup window functionalities as well as a seamless link to the [Ajax web interface](#)^[100] where you can change your monitoring configuration and access further functionalities such as reporting, Maps, system setup, etc. Some of these functionalities are shown with an embedded webkit browser, for others an external browser window is opened.

Access Several Core Servers in One Console

As an additional functionality, you can configure access to several PRTG core servers in the Enterprise Console. The console will then show data of your independent core server installations at a glance (for example, the device tree and alarms list), so you can manage your monitoring centrally, also when it is spread across different servers.

Getting Started

With an installation of PRTG Network Monitor, the Enterprise Console is included and installed automatically on the computer running the PRTG core server. If you want to use the Enterprise Console on another computer, please download and install it there, as described in the [Install the Enterprise Console](#)^[67] section.

Note: The Enterprise Console is mainly designed to review and manage an existing installation of PRTG which has already been set up. If you just started monitoring, we recommend you use the [Configuration Guru](#)^[36] and the web interface's [auto-discovery](#)^[190] function and add your network's devices there.

For detailed instructions, please see [Quick Start Guide](#)^[32] section. Once finished, you can seamlessly switch to the Enterprise Console.

Requirements for Connections to PRTG Web Server(s)

In order to show monitoring data of your PRTG setup, the Enterprise Console must be able to establish a connection to your PRTG web server(s). For this purpose, please ensure the following:

- The following server settings in the Enterprise Console (see section [PRTG Servers](#)^[1893] for details) have to match the following settings in the [PRTG Server Administrator](#)^[1999]:

Enterprise Console Server Settings	PRTG Server Administrator Settings
Server IP / DNS name	IP address for PRTG's Web Server on the Web Server tab
Port	TCP Port for PRTG's Web Server on the Web Server tab Note: PRTG switches to port 8080 as a fallback after a restart when port 80 is already used. Because the EC does not recognize port 8080 automatically, enter this port manually in the EC settings. If you do not get a connection to the PRTG web server, check the currently used port in the Web Server and Website Settings of PRTG's web interface.
Login Name	Login Name on the Administrator tab
Password	Password on the Administrator tab

- No local software firewall blocks the connection
- No local virus protection program blocks the connection
- The specified port is not used by another application
- No (hardware) firewall blocks the connection when connecting through a network (LAN or WAN)
- The software versions of the Enterprise Console and the PRTG web server have to match

See section [More](#) for common issues with the Enterprise Console and their solutions.

More

Knowledge Base: Problems with the Enterprise Console: What can I do?

- <http://www.paessler.com/knowledgebase/en/topic/60091>

The following sections introduce the features and concepts of the Enterprise Console:

Enterprise Console—Topics

- [First Start](#)  1863
- [General Layout](#)  1864
- [Menu Tabs and Page Content](#)  1868
- [PRTG Servers](#)  1893
- [Options](#)  1896
- [Windows Menu Structure](#)  1902
- [Context Menus](#)  1907
- [Shortcuts Overview](#)  1908

Related Topics

- [Ajax Web Interface—Basic Procedures](#)  100
- [Ajax Web Interface—Device and Sensor Setup](#)  188
- [Ajax Web Interface—Advanced Procedures](#)  1700
- [Other User Interfaces](#)  1912

8.1 First Start

This section will help you start the Enterprise Console for the first time.

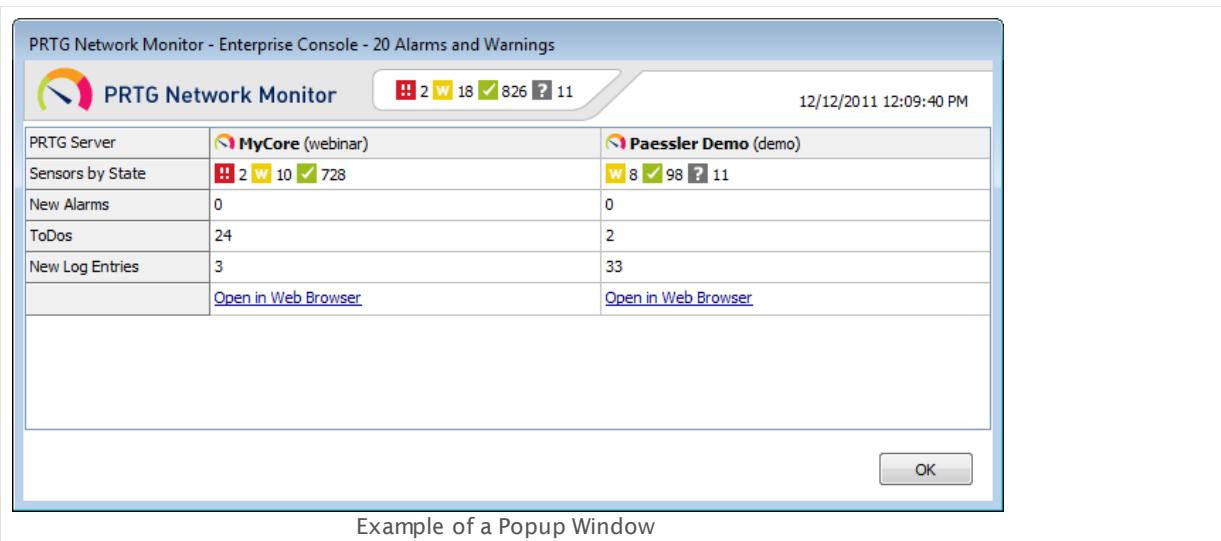
Opening the Enterprise Console

Double click the **PRTG Enterprise Console** icon in the Windows start menu to open it. As soon as it opens, the Enterprise Console will try to connect to your PRTG installation, according to the given PRTG server connection settings. In a fresh install of PRTG, the settings for the Enterprise Console installed on the computer running the PRTG core server are already predefined, so you can use the Enterprise Console right away. If you get an error message when opening the Enterprise Console, please check the connection settings. For example, editing the settings is necessary in case the IP address of the server has changed.

If you get an error message, please check your connection settings. For detailed information, please see [PRTG Servers](#)¹⁸⁹³ (**PRTG Server Connection**) section.

Popup Window

By default, the Enterprise Console runs in the background and shows a popup message whenever there are new alerts, new messages, or new tickets for your monitoring. The popup window will be one of the first things you see after opening the Enterprise Console.

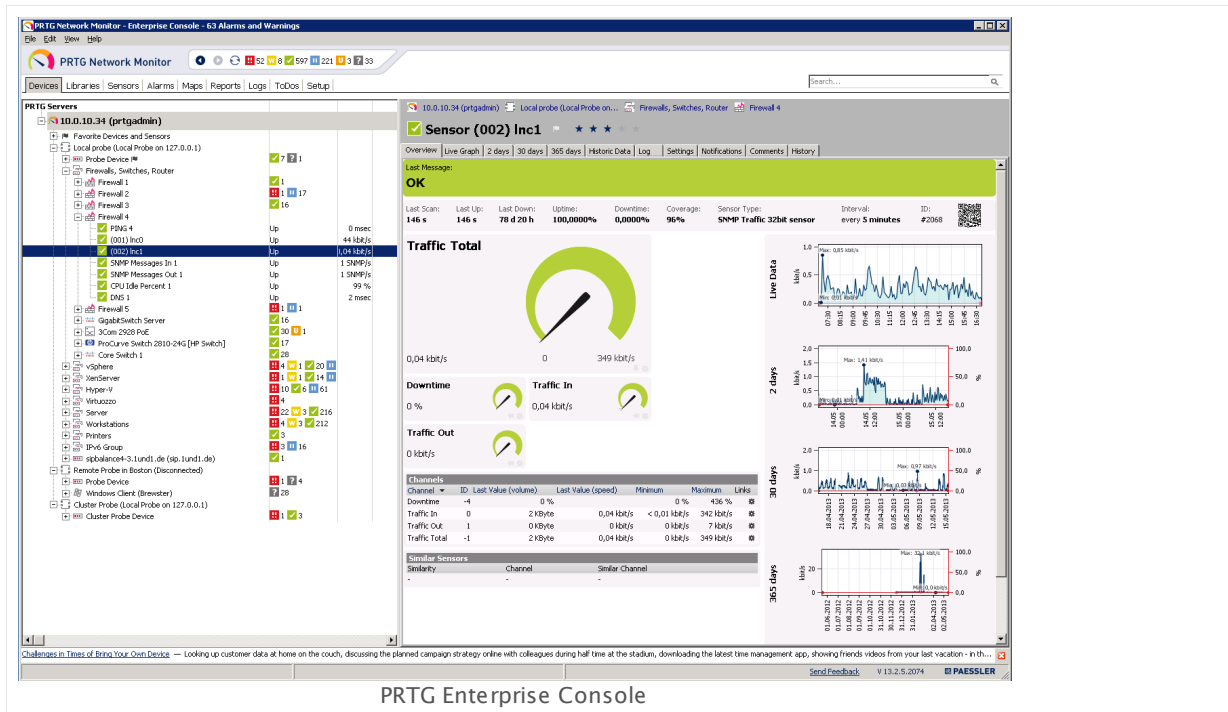


This window is shown as always on top. Click on the **OK** button to close it. You can change the popup behavior in the Enterprise Console settings.

For detailed information, please see [Options](#)¹⁸⁹⁷ settings (**System—Alerting**).

8.2 General Layout

The main layout of the Enterprise Console program consists of different elements which will be shortly described here.



From top to bottom, the main layout consists of:

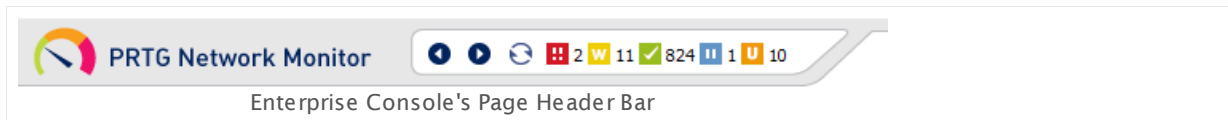
- The [Windows menu](#) ¹⁸⁶⁵.
- The [page header bar](#) ¹⁸⁶⁶ with the PRTG logo, the viewpoint arrow symbols, the refresh icon, and the sensor states overview.
- The [menu tabs bar and page content](#) ¹⁸⁶⁶ underneath.
- The [server selection](#) ¹⁸⁶⁶ and [search bar](#) ¹⁸⁶⁶ in the upper right corner.
- The [news feed](#) ¹⁸⁶⁶ underneath the page content.
- The [status bar](#) ¹⁸⁶⁷ at the bottom of the window.

Often, data and settings are displayed directly in the Enterprise Console. For some functionalities and extended setup, a new window of the system's default browser will be opened and the [web interface](#) ¹⁰⁰ will show up. In this case, you'll be logged in to the web interface automatically via username and [hash value](#) ¹⁷⁸⁶. In your browser, it might be necessary to confirm the certificate used by PRTG's web server. For more information, please see [SSL Certificate Warning](#) ¹⁰⁵ section. If you configure your Enterprise Console for a connection with more than one PRTG core server, keep an eye on the [server selection](#) ¹⁸⁶⁶ bar to choose which server's data you want to access.

Windows Menu

The Windows menu gives access to general configuration and settings. Find a detailed description in the [Windows Menu Structure](#) section.

Page Header Bar



The page header consists of the following parts:

- **PRTG Logo**

Click on the PRTG Network Monitor logo to open the [Ajax web interface](#) in the browser configured in the Enterprise Console's [Options](#). If several PRTG core servers are configured, the browser will load the web interface of the server currently selected in the [Devices](#) tab.

- **Previous Viewpoint / Next Viewpoint (Arrow Symbols)**

The enterprise stores the different views shown while you navigate through the application. Using these arrows (or using the shortcuts **Alt+Left** and **Alt+Right**) you can step back and forth in the history, just as known from your browser.

- **Refresh (Arrow Circle Symbol)**

Click on the refresh symbol (**F5**) any time to refresh the current screen. This will immediately query data for the current screen from all active PRTG core servers, just as the automatic refresh does, which can be configured in the [Options](#) settings.

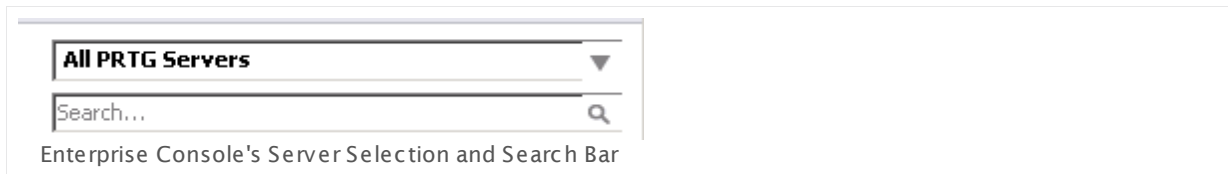
- **Global Sensor Status Symbols**

This area shows the aggregated status of all sensors from all active PRTG core servers, divided into different sensor states. Depending on the sensors' status you will see colored boxes with numbers which symbolize the sensors. For example, you can see how many sensors are in **Up**, **Down**, **Warning**, **Pause**, **Unusual**, or **Unknown** state. Click on a box to view a list of all sensors in the respective status. For a detailed description, please see [Sensor States](#) section. **Note:** When viewing sensor lists, you can show the sensors of one server at a time only. So, the global sensor overview shows the total number of sensors in a certain state on all active servers, but viewing a list of all sensors in a certain state from all servers is not possible for performance reasons.

Menu Tabs Bar and Page Content

You can navigate through your setup using the menu tabs bar. Please take a few minutes to familiarize yourself with all menu items. The page content underneath varies dependent on the selected menu tab. It shows various information about your monitored objects. For a detailed description of all tabs, please see the [Menu Tabs and Page Content](#) section.

Server Selection



In the server selection bar you see all active PRTG core server connections which are configured for the current Windows user account (saved in the registry).

The server you select here determines globally which information is shown in all [Menu Tabs](#) (except the **Devices** tab; the server selection does not apply there). Depending on your selection, **Libraries**, **Sensors**, **Alarms**, **Maps**, **Reports**, **Logs**, **Tickets**, and **Set up** options will be shown for the respective server only.

Select **All PRTG Servers** to show consolidated information for all active PRTG core servers which appear in the list. **Note:** For technical reasons, you cannot show consolidated information from all servers in the **Sensors**, **Set up**, and **Search Results** tab. In order to use those tabs, please decide on a single PRTG core server from the server selection bar.

Select **Manage PRTG Servers** to add or remove [PRTG Servers](#) from the list, or to edit an existing one.

Search Bar

Select a single PRTG core server from the [server selection](#) bar and enter a key word to search the respective server. In the **Search Results** tab, the Enterprise Console will display matching monitoring objects, help topics, and related objects. If you click on a monitoring object (for example, a sensor) in the search results, the Enterprise Console will open this object in the [Devices](#) tab, showing details in the device tree.

Note: If you start another search underneath the results within the **Search Results** tab, this will open a browser window, showing results.

Note: If you have configured a connection in the [PRTG Servers](#) options which uses a [Root ID](#) other than 0, this setting will be ignored while searching. In this case, **Search Results** for the entire server (starting at Root ID 0) will be shown.

News Feed Bar

The news feed bar shows latest news by Paessler. Click on the bar to open a popup with an overview about recent articles. You can open a specific article in the web browser by clicking on the particular header or on **More...** If you do not want to show the news feed in your Enterprise Console, click on the **X** besides the bar. You can enable it again via [View](#) in the main menu.

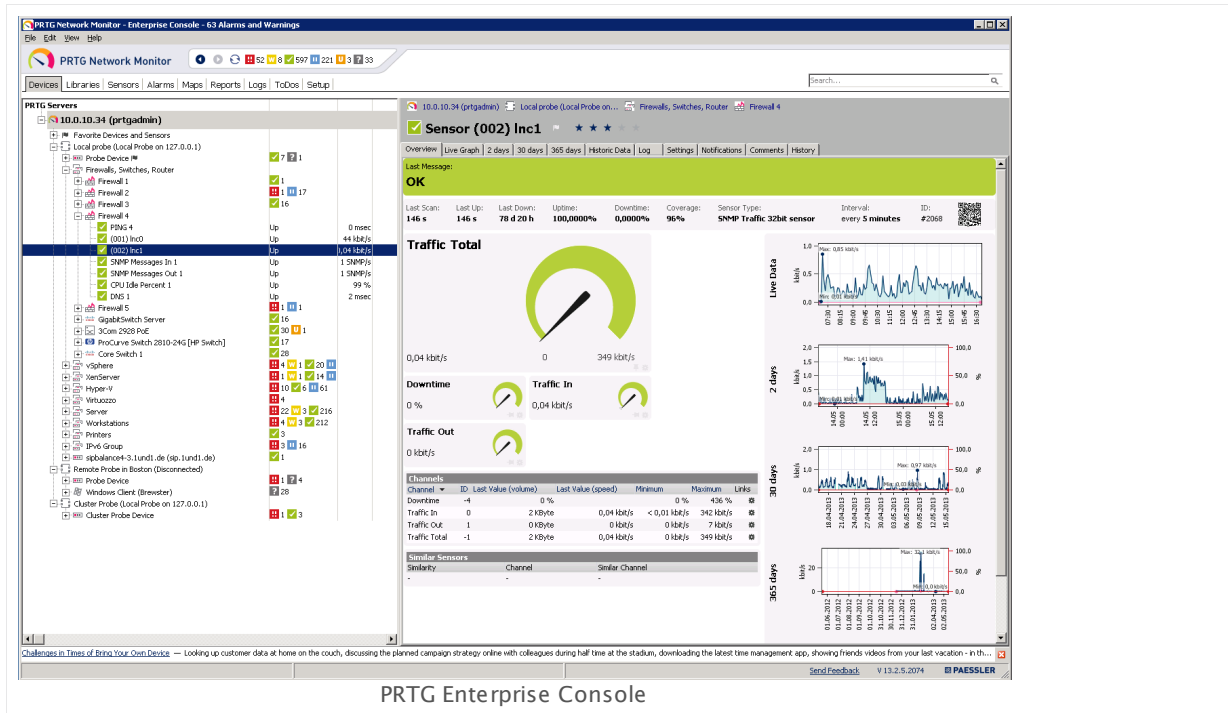
Status Bar



The status bar shows the version number of your PRTG Enterprise Console and the Paessler logo which leads you to the Paessler website when you click on it. Furthermore, the status bar contains a [Contact Support](#) link which will open a window to leave feedback or to ask for support.

8.3 Menu Tabs and Page Content

Under the different menu tabs of the Enterprise Console you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc.



The following sections introduce the available options within the different tabs:

- [Devices](#) ¹⁸⁶⁹
- [Libraries](#) ¹⁸⁷⁶
- [Sensors](#) ¹⁸⁷⁸
- [Alarms](#) ¹⁸⁸⁰
- [Maps](#) ¹⁸⁸²
- [Reports](#) ¹⁸⁸⁴
- [Logs](#) ¹⁸⁸⁶
- [Tickets](#) ¹⁸⁸⁸
- [Setup](#) ¹⁸⁹⁰
- [Search Results](#) ¹⁸⁹²

8.3.1 Devices

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.



There is documentation available for the following tabs:

- [Devices](#) ¹⁸⁶⁹
- [Libraries](#) ¹⁸⁷⁶
- [Sensors](#) ¹⁸⁷⁸
- [Alarms](#) ¹⁸⁸⁰
- [Maps](#) ¹⁸⁸²
- [Reports](#) ¹⁸⁸⁴
- [Logs](#) ¹⁸⁸⁶
- [Tickets](#) ¹⁸⁸⁸
- [Setup](#) ¹⁸⁹⁰
- [Search Results](#) ¹⁸⁹²

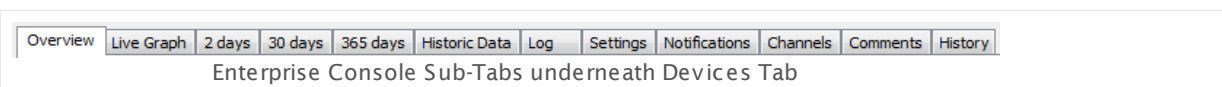
Devices Menu Tab

The **Devices** tab will be your starting point for everyday use. The page is split into two parts. On the left hand side, it shows the tree-like device view which lists all configured PRTG core servers with their probes, groups, devices, and the sensors on the devices, in a hierarchical order. Next to each object you see an overview of the number of sensors, grouped by their current status.

The first child node of the tree is called **Favorite Devices and Sensors**. It contains all devices and sensors that are marked as favorites. In order to add an object to the favorites list, right-click on it and select the **Add to Favorites** entry from the [context menu](#) ¹⁸⁶². For details, please see [Priority and Favorites](#) ¹⁸⁵⁹ section.

Note: For more information about the hierarchical order of the different objects in the device tree, please see [Object Hierarchy](#) ⁸³ section.

On the right side you see details about the object selected on the left. The information is spread over several tabs.



Edit Objects in the Device Tree

Using the **Edit** menu (or the object's [context menu](#)¹⁹⁰⁷) you can access different important functions of the items you have currently selected in the device tree on the left hand side, such as

- Add devices or sensors to the favorites list (or remove them from the list)
- Sort all sub nodes of an object alphabetically
- Move objects up and down in the tree
- Check now
- Pause monitoring
- Access tools
- and many more

For details about the available options, please see [Windows Menu Structure](#)¹⁹⁰².

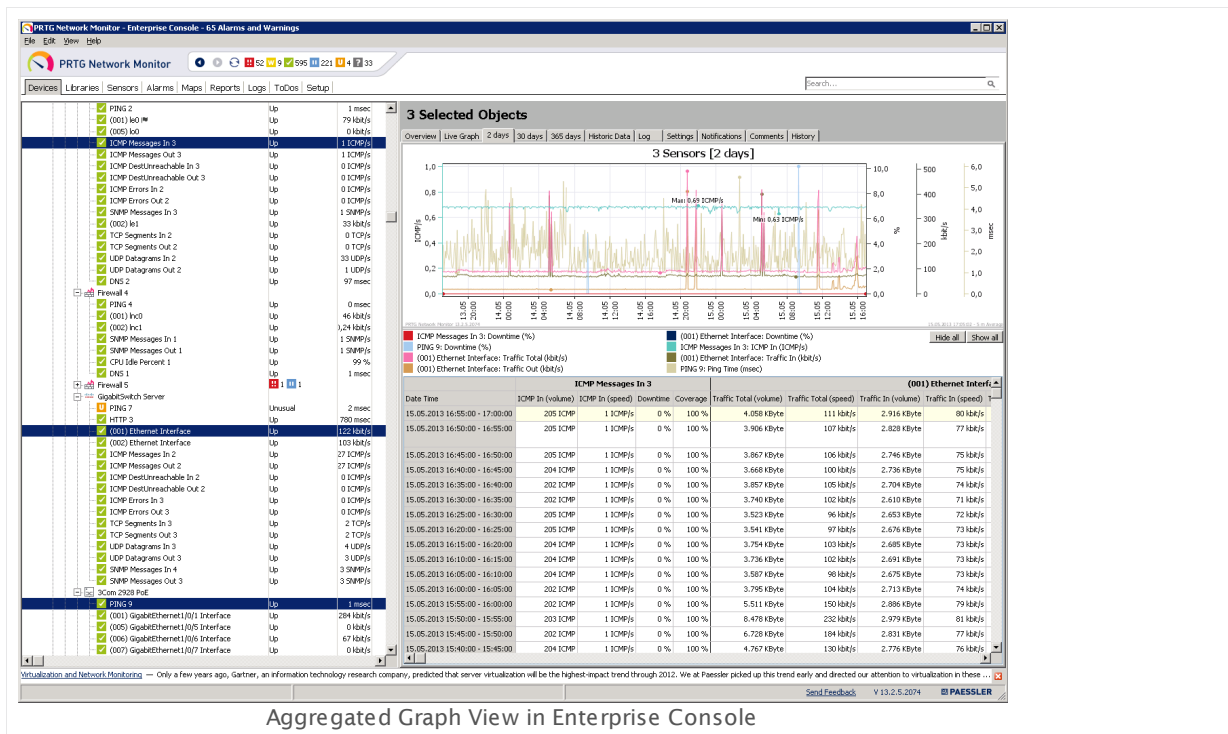
Select Multiple Items in Device Tree

In the device tree shown on the left, you can select one or more objects, even from different PRTG core servers. Hold down the **Ctrl** key to select more objects simultaneously. Usually, you will select more than one item in order to view combined graphs, or to apply a command from the [Windows Menu](#)¹⁹⁰² (for example, **Check Now** or **Pause**) to several objects.

When selecting multiple items, the sub-tabs on the right side will show data for **all** selected items at a glance. For example, when selecting two sensors, you will see their tables next to each other. Graphs will actually be shown combined! This is a great way to instantly show one chart containing the graphs of all selected objects. Each sensor channel will then be shown as one line. This aggregated view works for all kind of objects. **Note:** The tab **Live Graph** will show data for sensors only.

Note: Underneath each graph a legend is shown. Hover an entry in the legend to display the according line in the graph above in **bold**.

Part 8: Enterprise Console | 3 Menu Tabs and Page Content 1 Devices



Aggregated Graph View in Enterprise Console

Note: You may need to enlarge the Enterprise Console's window in order to see all tables and graphs.

Devices—Overview

The **Overview** tab shows general information about the selected object. Depending on the object selected, different information is displayed.

- For **servers**, **probes**, and **groups** the table shows information in the **Name** section only, such as priority and parent objects. On the right side, a geographical Map is shown, if enabled in your PRTG configuration as well as in the Enterprise Console's **View menu** ¹⁹⁰⁵. For detailed information about geographical maps, please see **Geo Maps** ¹⁷³¹⁰ section.
- For **devices**, the **Overview** tab shows device details and summary graphs for different time spans, as well as a list of all sensors on this device.
- For **sensors**, the **Overview** tab shows sensor details, current status, and the last value of all sensor channels, as well as sensor graphs for different time spans. You can also edit channel settings in this tab by clicking on a channel's gear icon (for details, please see section **Sensor Channels Settings** ¹⁶⁸³).

Devices—Live Graph, 2 days, 30 days, 365 days

These tabs are only available if the **Large Single Graph (Ctrl+L)** view is enabled in the **Windows Menu** ¹⁹⁰⁵ (**View**). For **Small Multiple Graphs** view please see **Devices—Graph** ¹⁸⁷² section below.

Select one of the tabs to display an object's monitoring results as **Live Graph** (content available for sensors only), or for different time spans in more or less detail (**2 days**, **30 days**, **365 days**). In every tab, you will see graphs as well as data tables.

While viewing a sensor graph you can hide single sensor channels individually. Simply remove the check mark symbol in front of a channel name underneath the graph, and the according channel's line will disappear. You can also **Show all** or **Hide all** channels by clicking on the buttons besides the channel names. The graph view will be reset immediately.

Note: The days mentioned here are the default setting. You can change the detail of the different graphs any time in the PRTG System Administrator program. See section [PRTG Server Administrator](#) (1999) (Memory Usage) for more details.

Note: Underneath each graph a legend is shown. Hover an entry in the legend to display the according line in the graph above in **bold**.

Devices—Graph

This tab is only available if the **Small Multiple Graphs** (**Ctrl+S**) view is enabled in the [Windows Menu](#) (1902) (**View**). For **Large Single Graphs** view please see above. This will show an overview with single graphs and data tables for live data, 2 days, 30 days, and 365 days. It might be necessary to enlarge the window in order to display all graphs. **Note:** The days mentioned here are the default setting. You can change the detail of the different graphs any time in the PRTG System Administrator program. See section [PRTG Server Administrator](#) (1999) (Memory Usage) for more details.

Note: Underneath each graph a legend is shown. Hover an entry in the legend to display the according line in the graph above in **bold**.

Devices—Historic Data

The **Historic Data** tab is available for sensors only (not for probes, groups, or devices). When calling the historic data reports via this tab, there is no sensor selection available, because you have already determined which sensor you would like to create a report for.

The screenshot displays the PRTG Network Monitor interface. At the top, there is a navigation bar with tabs: Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. Below this is a sub-navigation bar for the selected sensor, showing 'Sensor PING 8' with a status of '★★★★★'. The main content area is titled 'REVIEW OR DOWNLOAD HISTORIC SENSOR DATA'. It includes a 'Start' and 'End' date range selector, both set to '2013-12-09 11:42'. A 'Quick Range' section offers various time-based filters: 1 Day, 2 Days, 7 Days, 14 Days, Today, Yesterday, Last Week (Mo-Su), Last Week (Su-Sa), Last Month, 2 Months, 6 Months, and 12 Months. The 'Average Interval' is set to '60 Minutes/1 Hour'. The 'File Format' section has three options: 'HTML web page' (selected), 'XML file', and 'CSV file'. Below this is an 'INCLUDE PERCENTILES' section with 'Percentile Results' set to 'Off'. At the bottom of the form are 'Start' and 'Cancel' buttons. The footer of the interface shows the PAESSLER logo, version information (PRTG Network Monitor 13.4.9.3636+ [Canary]), copyright (© 2013 Paessler AG), user role (PRTG System Administrator), refresh interval (Refresh in 591 sec), and a timestamp (10.12.2013 11:42:09).

Historic Data Tab of a Ping Sensor

Depending on the **File Format** option you choose, the results will be shown:

- **HTML web page:** Open a new window, showing the historic data report
- **XML file:** A new browser window will open, showing the historic data report as XML file.
- **CSV file:** A new browser window will open, showing the historic data report as CSV file.

When you click on one of these items, a new window or tab of the external browser configured in the Enterprise Console's [Options](#)^[100] will open and PRTG will automatically login and redirect you to the respective web page. If your browser displays a certificate warning, please find more information in the [SSL Certificate Warning](#)^[105] section.

View and functionality are the same as in the web interface. For details about the available **Historic Data** report options please see [Historic Data Reports](#)^[132] section of the [Ajax Web Interface](#)^[100] documentation.

Devices—Log

Click on the **Log** tab to show a table list with all log information **on this object**. This is a subset of the entries available via the [Logs](#)^[108] menu tab.

In the list, one hundred entries are shown at a time. Use the arrow symbols above the list to show other items. You can jump to the beginning of the list, or browse through it hundred by hundred. If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click once or twice on the header of the column you want to sort by.

Devices—Settings

In the **Settings** tab the currently selected object's settings are loaded from the web interface and displayed. View and functionality are the same as in the web interface. For every type of object and for every sensor, different options are available. For detailed information, please see the following sections (depending on the selected object) in the [Ajax Web Interface](#)^[100] documentation:

- [Probe Settings](#)^[238]
- [Group Settings](#)^[253]
- [Device Settings](#)^[272]
- [Sensor Settings](#)^[290]

Devices—Settings—Multi-Edit

If you select several objects on the left side, the **Settings** tab will switch into multi-edit mode. Using multi-edit, you can set a check mark for one or more settings. All changes will be applied to all selected objects. The multi-edit dialog displays settings which are common among the selected objects only.

If you select sensors only on the left side, the **Settings** tab will display a new tab row with a **Channel Settings** tab. Using this tab you can multi-edit the settings of any channels which are common among the selected sensors, as long as the channels have the same name. Set a check mark for one or more channel settings. All changes will be applied to all selected sensors.

Note: You cannot use multi-edit for objects on different PRTG core servers.

Devices—Notifications

In the **Notifications** tab the currently selected object's settings are loaded from the web interface and displayed. View and functionality are the same as in the web interface. You can set different notification triggers.

For detailed information, please see the [Sensor Notifications Settings](#)^[1690] section in the [Ajax Web Interface](#)^[100] documentation.

Note: You cannot change notification settings for multiple objects at a time. We recommend using the [Inheritance of Settings](#)^[87] for easy configuration.

Devices—Comments

In the **Comments** tab the currently selected object's settings are loaded from the web interface and displayed. View and functionality are the same as in the web interface.

In the **Comments** tab you can enter free text for each object. This can be used for documentation purposes or to leave information for other users.

Devices—History

In the **History** tab all changes in the settings of an object are shown with a timestamp, the PRTG user which conducted the change, and a message.

Drag & Drop Sorting in Device Tree

In the device tree, you can also move probes, groups, and devices simply via drag and drop. Activate it in the [Windows menu](#)^[1902] **Edit | Drag & Drop Sorting** and then drag your objects as you like: You can move devices and groups, or add groups or devices to other groups. You can also move objects via the [context menu](#)^[1907].

Note: You cannot move objects in the following cases:

- You cannot move any objects from one PRTG core server to another.
- You cannot move sensors from one device to another. In order to clone sensors to other devices using drag&drop, please use the [Ajax Web Interface](#)^[100]. For detailed information, please see [Manage Device Tree](#)^[222] section.
- You cannot move devices from one group to another.
- You cannot move groups from one probe to another.
- You cannot move probes from one core server to another.

8.3.2 Libraries

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.



There is documentation available for the following tabs:

- [Devices](#)  1869
- [Libraries](#)  1876
- [Sensors](#)  1878
- [Alarms](#)  1880
- [Maps](#)  1882
- [Reports](#)  1884
- [Logs](#)  1886
- [Tickets](#)  1888
- [Setup](#)  1890
- [Search Results](#)  1892

Using Libraries is a great way to keep an eye on your network's status, as you can select which sensors you would like to see there. For a general introduction to Libraries, please see [Libraries](#)  1733 section.

Libraries Menu Tab

The page is split into two parts. On the left hand side you see all available libraries from one or several servers, on the right hand side the actual libraries are displayed.

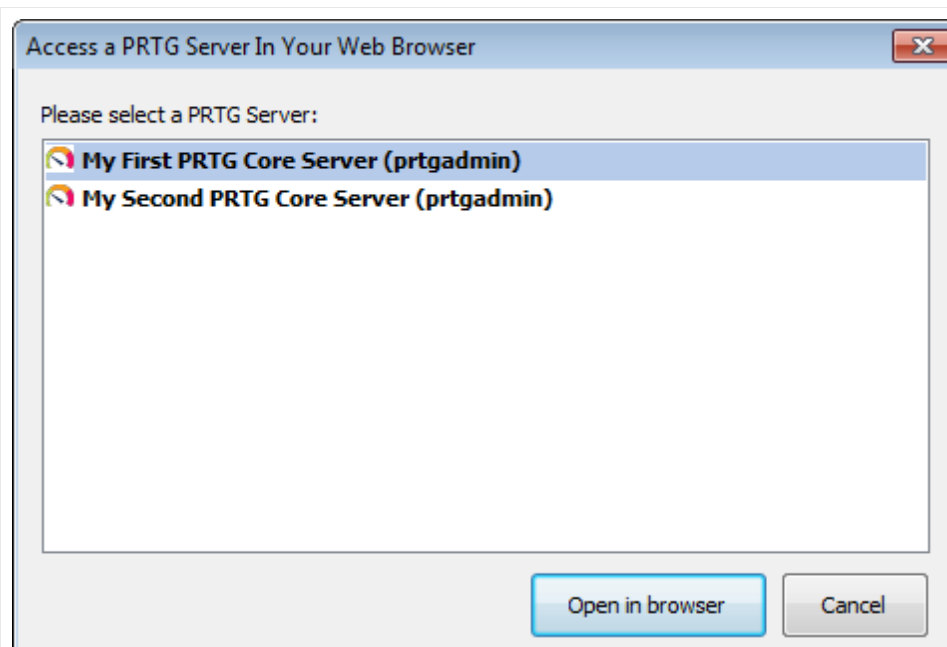
- Single-click on a library's name to display it. In the tabs above the library, select from [Overview](#)  1733, [Management](#)  1740, [Settings](#)  1742, [Comments](#)  1746, and [History](#)  1747. Each of these tabs loads the respective functionality of the [Ajax Web Interface](#)  100. Please remember to click the **Save** button in order to apply your settings. Please find detailed information in the [Libraries](#)  1733 section.
- Underneath the tabs bar, there are different options available to change the current library view: You can set sensor filters (set or remove check marks to include or exclude sensors in a certain state) and change the device tree view (for details about the tree view, please see [General Layout—Tree View Layout](#)  109 section).
- Double-click on a library's name to open the library in the configured external web browser. You can then edit it or add new libraries on this PRTG server. For more information see [Libraries](#)  1733 section.

- Right-click on a map's name to open a [context menu](#)¹⁹⁰⁷. The following options are available: **Add Library**, **Edit**, **Delete**, **Open in Web Browser**.

Libraries Menu Tab—Add Library

Click on the **Add Library** button to add a new library to a core server.

Depending on the current setting shown in the [server selection](#)¹⁸⁶⁶ bar in the upper right corner, an (embedded) browser window will be opened immediately (if one specific server is selected), or you will be prompted with a selection window, asking you to choose the core server you want to add the new item to. Choose an installation to open a browser window.



Enterprise Console Server Selection Dialog

For details about adding a library, please see [Libraries Step By Step](#)¹⁷³⁶.

8.3.3 Sensors

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.



There is documentation available for the following tabs:

- [Devices](#)  1869
- [Libraries](#)  1876
- [Sensors](#)  1878
- [Alarms](#)  1880
- [Maps](#)  1882
- [Reports](#)  1884
- [Logs](#)  1886
- [Tickets](#)  1888
- [Setup](#)  1890
- [Search Results](#)  1892

Viewing lists of sensors is a great way to keep an eye on your network's status, as you can select which kind of sensors you would like to see. You can filter by object, sensor type, and current sensor state.

Sensors Menu Tab

Note: For technical reasons, this function is available for one server at a time only. If you have configured more than one PRTG core server, please choose one server from the server list in the upper right corner.

Click on the **Sensors** entry in the menu tabs bar to show a table list of all sensors. You can enable a filter to only show certain sensors. To do so, choose from three different drop down menus to build a filter. With each filter you can further decrease the number of sensors shown.

- **By Type**
The second drop down menu shows all sensor types available in your monitoring setup. Select an entry to only show sensors of this type. The default value is **All Types**.

- **By State**

The third drop down menu shows all possible sensor states. Select an entry to only show sensors that currently show this status. Choose between **All States**, **Down**, **Down (Acknowledged)**, **Down (Partial)**, **Warning**, **Up**, **Paused**, **Unusual**, and **Unknown**. The default value is **All States**. **Note:** If you click on a sensor symbol in the [page header bar](#)¹⁸⁹⁵, you can directly view a sensor list filtered by the selected sensor state for the selected server.

If you have filtered out all sensors and the list below shows no entries, try removing some filters by reverting them to the default values. To disable all filters, remove the check mark in front of the **Filter by** option at the beginning of the line.

Note: In the column **Last Value** only the last value of the sensor's **primary channel** will be shown.

In the list, one hundred entries are shown at a time. Use the arrow symbols above the list to show other items. You can jump to the beginning of the list, or browse through it hundred by hundred. If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click once or twice on the header of the column you want to sort by.

From this list view, you can select multiple items in order to apply the same action to them, for example, **Edit** | **Check Now**.

You can select multiple items by the following means (you can also combine them):

- Click and hold your left mouse key while hovering the lines you want to select
- Hold the Ctrl key while clicking to toggle the selection status of a single line
- Click a line and hold the Shift key while clicking another line to select all lines in between.

8.3.4 Alarms

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.



There is documentation available for the following tabs:

- [Devices](#)  1869
- [Libraries](#)  1876
- [Sensors](#)  1878
- [Alarms](#)  1880
- [Maps](#)  1882
- [Reports](#)  1884
- [Logs](#)  1886
- [Tickets](#)  1888
- [Setup](#)  1890
- [Search Results](#)  1892

Alarms Menu Tab

In the **Alarms** tab the alarms of **all** active PRTG core servers can be displayed. To do so, select **All PRTG Servers** from the server selection in the upper right corner.

The Alarm list shows all sensors that are currently in a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. Sensors in other states (for example, **Up**, **Paused**, or **Unknown**) do not appear here. This is useful to keep track of all irregularities in your network.

Using the options **Error**, **Warning**, and **Unusual**, you can hide and show sensors in the respective status by removing and adding a check mark. When choosing **Error**, this includes sensors in the states **Down**, **Down (Partial)**, and **Down (Acknowledged)**.

If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click once or twice on the header of the column you want to sort by.

From this list view, you can select multiple items in order to apply the same action to them, for example, **Edit** | **Check Now**.

You can select multiple items by the following means (you can also combine them):

- Click and hold your left mouse key while hovering the lines you want to select
- Hold the Ctrl key while clicking to toggle the selection status of a single line
- Click a line and hold the Shift key while clicking another line to select all lines in between.

Acknowledge Alarm

An acknowledged alarm will show up in the alarms list as "acknowledged" (see [Sensor States](#)¹²¹) and will not [trigger](#)¹⁶⁹⁰ any more [notifications](#)¹⁷²³. **Note:** If the alarm condition clears, the sensor will usually return into an **Up** status immediately with the next sensor scan.

In order to acknowledge an alarm, right-click on a sensor and choose **Acknowledge Alarm...** from the context menu, enter a message and click the **OK** button. The message will appear in the sensor's last message value. You can choose between: **Acknowledge Indefinitely...**, **acknowledge For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Until...**

If you choose **Until...** a popup window will appear:

Acknowledge Alarm until	
Selected Objects	Shows the sensor(s) for which you want to acknowledge the alarm. You can acknowledge alarms for more than one sensor using multi-edit ¹⁷¹⁰ .
Message	Enter a text, for example, the reason why you acknowledge the alarm.
Until	Enter the date when the acknowledge status will end. Use the date time picker to enter the date and time. Note: If the alarm condition still persists after the specified date, the sensor will show a Down status again.

Only [users](#)¹⁸²⁴ with write access rights may acknowledge alarms. Read-only users can be given the right to acknowledge alarms, too. See section [User Accounts Settings](#)¹⁸²⁴, section **Account Control**.

8.3.5 Maps

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.



There is documentation available for the following tabs:

- [Devices](#) 
- [Libraries](#) 
- [Sensors](#) 
- [Alarms](#) 
- [Maps](#) 
- [Reports](#) 
- [Logs](#) 
- [Tickets](#) 
- [Setup](#) 
- [Search Results](#) 

Maps Menu Tab

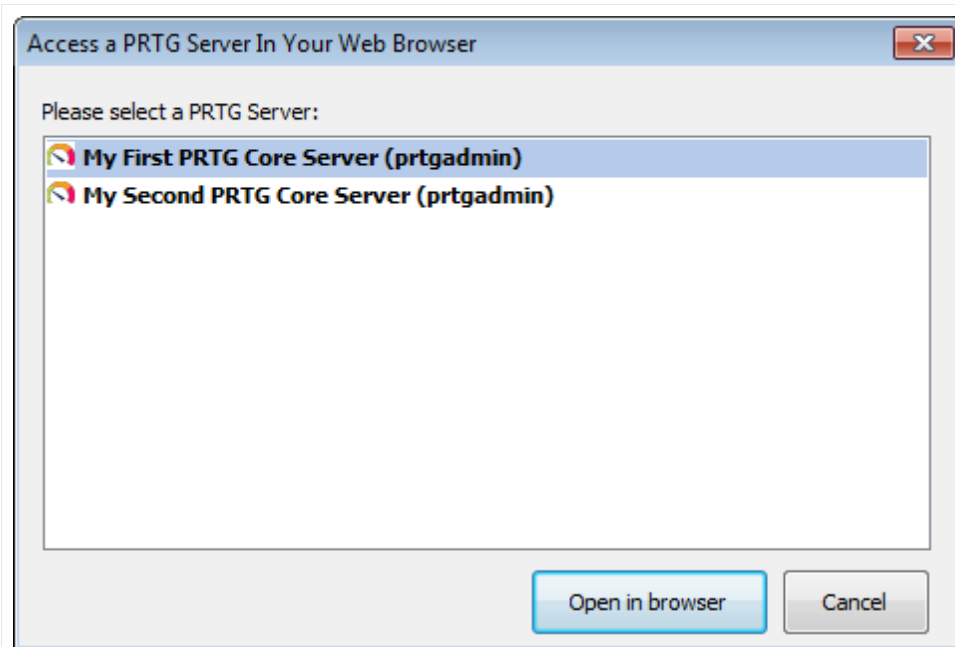
The page is split into two parts. On the left hand side you see all available maps from one or several servers, on the right hand side the actual maps are displayed.

- Single-click on a map's name to display it. In the tabs above the map, select from **View Map**, [Maps Designer](#) , [Settings](#) , [Get HTML](#) , and [Comments](#) . Each of these tabs loads the respective functionality of the [Ajax Web Interface](#) . Please remember to click the **Save** button in order to apply your settings. Please find detailed information in the [Maps](#)  section.
- Double-click on a map's name to open the map in the configured external web browser. You can then edit it using the [Maps Designer](#) , or add new maps on this PRTG server. For more information see [Maps](#)  section.
- Right-click on a map's name to open a [context menu](#) . The following options are available: **Add Map**, **Delete**, **Clone**, **Open in Web Browser**.

Maps Menu Tab—Add Map

Click on the **Add Map** button to add a new map to a core server.

Depending on the current setting shown in the [server selection](#) ¹⁸⁶⁶ bar in the upper right corner, an (embedded) browser window will be opened immediately (if one specific server is selected), or you will be prompted with a selection window, asking you to choose the core server you want to add the new item to. Choose an installation to open a browser window.



Enterprise Console Server Selection Dialog

For details about adding a map, please see [Maps Step By Step](#) ¹⁷⁷¹.

8.3.6 Reports

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.



There is documentation available for the following tabs:

- [Devices](#)  1869
- [Libraries](#)  1876
- [Sensors](#)  1878
- [Alarms](#)  1880
- [Maps](#)  1882
- [Reports](#)  1884
- [Logs](#)  1886
- [Tickets](#)  1888
- [Setup](#)  1890
- [Search Results](#)  1892

Reports Menu Tab

In the **Reports** tab you see all available reports from one or several servers, in one list.

If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click once or twice on the header of the column you want to sort by.

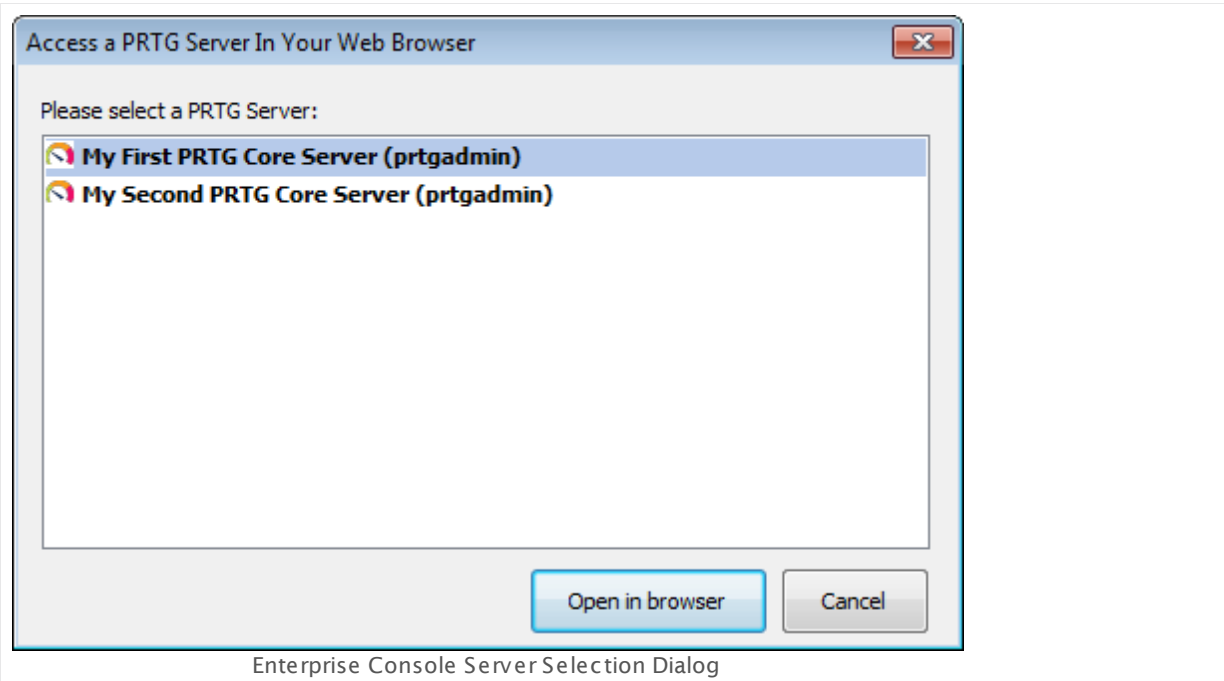
Choose one report and double click on it's name. The page will be split into two parts. On the left hand side you still see all available reports from one or several servers, on the right hand side the options for the currently selected report are displayed.

- Single-click on a report's name to display its options. In the tabs above the report, select from [Run Now](#)  1755, [Stored Reports](#)  1757, [Settings](#)  1758, [Select Sensors Manually](#)  1765, [Sensors Selected by Tag](#)  1767, and [Comments](#)  1767. Each of these tabs loads the respective functionality of the [Ajax Web Interface](#)  100. Please remember to click the **Save** button in order to apply your settings. Please find detailed information in the [Reports](#)  1749 section.
- Right-click on a report's name to open a [context menu](#)  1907. The following options are available: **Add Report**, **Delete**, **Clone**, **Open in Web Browser**.
- Double-click on any report's name on the left side to return to the initial list view of all reports.

Reports Menu Tab—Add Report

Click on the **Add Report** button to add a new report to a core server.

Depending on the current setting shown in the [server selection](#)¹⁸⁸⁶ bar in the upper right corner, an (embedded) browser window will be opened immediately (if one specific server is selected), or you will be prompted with a selection window, asking you to choose the core server you want to add the new item to. Choose an installation to open a browser window.



For details about adding a report, please see [Reports Step By Step](#)¹⁷⁵².

8.3.7 Logs

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.



There is documentation available for the following tabs:

- [Devices](#)  1869
- [Libraries](#)  1876
- [Sensors](#)  1878
- [Alarms](#)  1880
- [Maps](#)  1882
- [Reports](#)  1884
- [Logs](#)  1886
- [Tickets](#)  1888
- [Setup](#)  1890
- [Search Results](#)  1892

The Logs list shows all past activities and events of your PRTG monitoring setup. This is useful to keep track of all important activities and, for example, to check whether messages were sent, etc. In a typical setup, a huge amount of data is produced here. As the activity of every single object is minuted, you can use this data to check exactly if your setup works as expected.

PRTG Server	Date Time	Parent	Type	Name	Status	Message /
MyCore	12.12.2011 12:52:53	Core Switch 1 (10.0.255.2)	SNMP Custom	TCP Segments Out 4	Paused	Paused by dependency
MyCore	12.12.2011 12:53:03	Firewall 2	Ping	PING 1	Down	Request timed out (ICMP error # 11010)
MyCore	12.12.2011 12:53:00	Firewall 2	Ping	PING 1	Warning	Request timed out (ICMP error # 11010)
MyCore	12.12.2011 12:55:18	Core Switch 1 (10.0.255.2)	SNMP Custom	ICMP Messages In 4	Resuming	Resumed by Dependency
MyCore	12.12.2011 12:55:18	Core Switch 1 (10.0.255.2)	SNMP Custom	ICMP Messages Out 4	Resuming	Resumed by Dependency
MyCore	12.12.2011 12:55:18	Core Switch 1 (10.0.255.2)	SNMP Traffic	0x0 Ethernet Interface	Resuming	Resumed by Dependency
MyCore	12.12.2011 12:55:18	Core Switch 1 (10.0.255.2)	SNMP Custom	UDP Datagrams In 4	Resuming	Resumed by Dependency
MyCore	12.12.2011 12:55:18	Core Switch 1 (10.0.255.2)	HTTP	HTTP 5	Resuming	Resumed by Dependency

Enterprise Console Logs

There are two possibilities to call the logs list: Either you click on the **Log** tab while viewing an object's details in the [Devices](#)  1873 menu tab, or you choose the **Logs** entry from the menu tabs bar.

Logs Menu Tab

Click the **Logs** entry in the menu tabs bar to show a list of **all** log entries of a PRTG core server.

You can either view the entries of one or all servers. If you have configured more than one PRTG core server and you want to view entries from all servers in your [PRTG Servers](#) ¹⁸⁹³ setup, simply select **All PRTG Servers** from the server selection in the upper right corner.

The background color of a row indicates the value listed in the **Status** column. It is shown green for **Up**, yellow for **Warning**, red for **Down**, and white for all other values.

You can enable a filter to only show certain log entries of a certain event. The drop down menu shows all possible event types. Select an entry to only show events of the respective event type. Choose between **All Events**, **Up & Down**, **Down**, **Warning**, **Unusual**, **Up, Paused & Resumed**, **Probe Related**, **Auto Discovery**, **Notifications**, and **Status Messages**. The default value is **All Events**.

If you have filtered out all sensors and the list below shows no entries, try another filter or revert to **All Events**.

In the list, one hundred entries are shown at a time. Use the arrow symbols above the list to show other items. You can jump to the beginning of the list, or browse through it hundred by hundred. If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click once or twice on the header of the column you want to sort by.

8.3.8 Tickets

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.



There is documentation available for the following tabs:

- [Devices](#)  1869
- [Libraries](#)  1876
- [Sensors](#)  1878
- [Alarms](#)  1880
- [Maps](#)  1882
- [Reports](#)  1884
- [Logs](#)  1886
- [Tickets](#)  1888
- [Setup](#)  1890
- [Search Results](#)  1892

Tickets Menu Tab

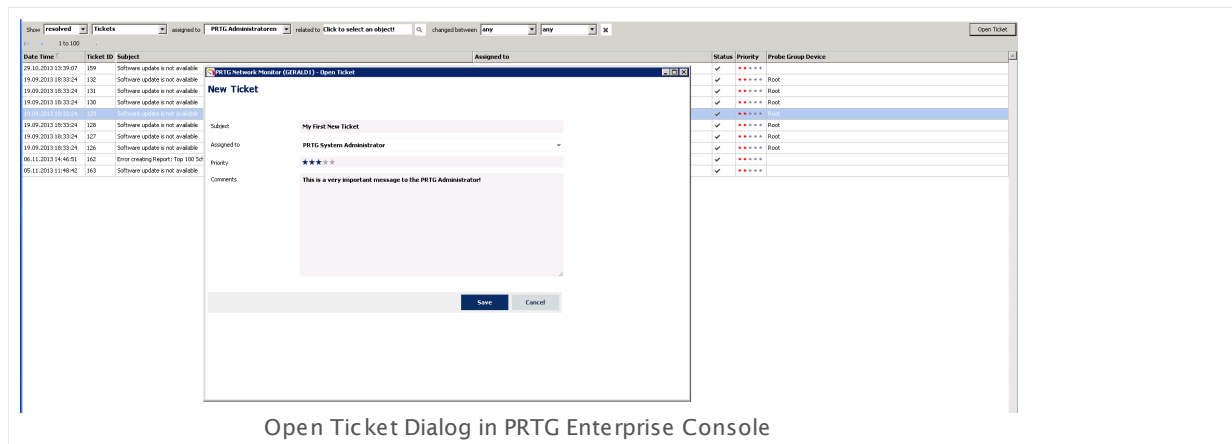
In the **Tickets** tab you can view all tickets on the currently selected PRTG core server. **Note:** You can only display tickets from one server at the same time, not from all PRTG servers.

In the header bar of the tickets list, you can choose several filters to find and display certain tickets: by status, type, concerned user or user group, related monitoring objects, and last edit. Click on the **X** to undo the date selection.

Double-click an entry in the tickets list to open a ticket in a popup window and to conduct ticket related actions (edit, assign, resolve, close, or reopen). You can also multi-edit tickets via the context menu: mark several tickets by holding **Ctrl** or **Shift** and clicking on the corresponding tickets. Then **right-click** to open the context menu.

Tickets Menu Tab—Open Ticket

In order to open a new ticket, click on the **Open Ticket** button in the upper right corner or in the context menu. Select a related object, click on **Continue**, and provide **Subject**, **Assigned to**, **Priority**, and **Comments**. Once finished, click on **Save** and the ticket will be created.

Part 8: Enterprise Console | 3 Menu Tabs and Page Content
8 Tickets

Open Ticket Dialog in PRTG Enterprise Console

For details about working with PRTG's ticket system, please see section [Tickets](#)¹⁴⁸ for PRTG's web interface.

8.3.9 Setup

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.



There is documentation available for the following tabs:

- [Devices](#)  1869
- [Libraries](#)  1876
- [Sensors](#)  1878
- [Alarms](#)  1880
- [Maps](#)  1882
- [Reports](#)  1884
- [Logs](#)  1886
- [Tickets](#)  1888
- [Setup](#)  1890
- [Search Results](#)  1892

Setup Menu Tab

Note: For technical reasons, this function is available for one server at a time only. If you have configured more than one PRTG core server, please choose one server from the server list in the upper right corner.

In the **Setup** tab you can access all options available in the [Setup](#)  1784 menu of the Ajax web interface. Please note that settings for user accounts and user groups are arranged a little different in the Enterprise Console.

For more information please refer to the respective section in the web interface's documentation.

Account Settings:

- [My Account](#)  1786
- [Notifications](#)  1791
- [Schedules](#)  1801

System Administration:

- [System & Website](#) 
- [Notification Delivery](#) 
- [Probes](#) 
- [Administrative Tools](#) 
- [Cluster](#)  (available in a [cluster](#)  setup only)

User Accounts:

- You see a list of configured user accounts. Select one to change settings. For details, please see [User Accounts](#)  section.

User Groups:

- You see a list of configured user groups. Select one to change settings. For details, please see [User Groups](#)  section.

PRTG Status:

- [System Status](#) 
- [Cluster Status](#)  (available in a [cluster](#)  setup only)
- [Auto Update](#) 

Optional Downloads and Add-Ons:

- [PRTG Enterprise Console](#) 
- [Apps for iOS & Android](#) 
- [Remote Probe Installer](#) 

8.3.10 Search Results

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network's status, monitoring results, etc., as well as access maps, reports, and settings.



There is documentation available for the following tabs:

- [Devices](#)  1869
- [Libraries](#)  1876
- [Sensors](#)  1878
- [Alarms](#)  1880
- [Maps](#)  1882
- [Reports](#)  1884
- [Logs](#)  1886
- [Tickets](#)  1888
- [Setup](#)  1890
- [Search Results](#)  1892

Search Results Menu Tab

Note: For technical reasons, this function is available for one server at a time only. If you have configured more than one PRTG core server, please choose one server from the server list in the upper right corner.

The **Search Results** tab is only visible if you did a search using the search box in the upper right corner. For your search, all matching objects on one PRTG core server are shown. Click on a monitoring object in the results to show it in the Enterprise Console's [Devices](#)  1869 tab.

Other objects, for example, chapters from the help file, are loaded in an external browser.

When you click on one of these items, a new window or tab of the external browser configured in the Enterprise Console's [Options](#)  1900 will open and PRTG will automatically login and redirect you to the respective web page. If your browser displays a certificate warning, please find more information in the [SSL Certificate Warning](#)  105 section.

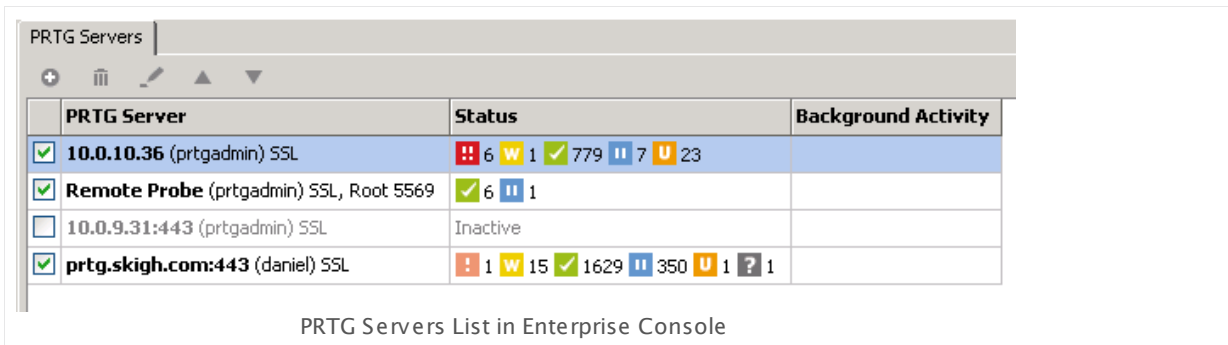
8.4 PRTG Servers

The Enterprise Console connects to the web server API running on every PRTG core server installation. It supports saving the configuration for a connection to one or more PRTG core servers. In a full PRTG installation, there is already a connection predefined.

Note: For a successful connection, the program versions of Enterprise Console and PRTG core server have to match. When connecting to several servers please make sure they all run on the same software version.

PRTG Servers List

From the main menu, select **File | All PRTG Servers** to view a list of all servers configured for the currently logged in Windows user account. You can also access this list by clicking on the **PRTG Servers** entry above the device tree, or by selecting the **Manage PRTG Servers** option from the server selection in the upper right corner.



PRTG Server	Status	Background Activity
☒ 10.0.10.36 (prtgadmin) SSL	!! 6 W 1 ✓ 779 II 7 U 23	
☒ Remote Probe (prtgadmin) SSL, Root 5569	✓ 6 II 1	
☐ 10.0.9.31:443 (prtgadmin) SSL	Inactive	
☒ prtq.skigh.com:443 (daniel) SSL	! 1 W 15 ✓ 1629 II 350 U 1 ? 1	

PRTG Servers List in Enterprise Console

The list shows the server or display name, as well as login information used. In the **Status** column you see an overall sensor status for this server connection. If there is any **Background Activity** on the respective server, which can potentially affect performance and response times, this is displayed as well.

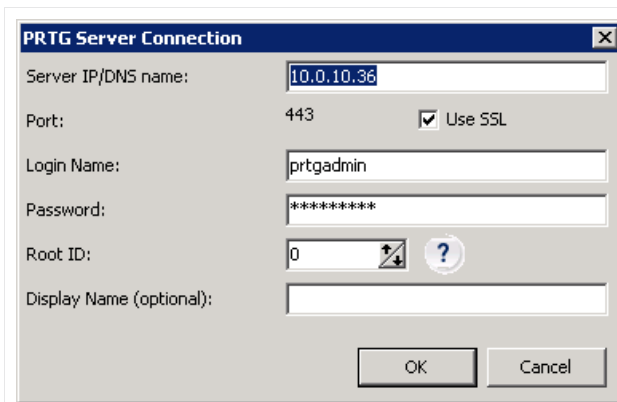
In the list, set a check mark for every PRTG server you want to poll with every update interval. If a server is not reachable, the Enterprise Console will deactivate it automatically after several unsuccessful connection attempts. When opening the Enterprise Console, it will automatically re-establish the connection to all active servers.

Add or Edit a PRTG Server Connection

In the icons bar above the server list, please click the **Add** button to add a new server connection configuration. Use the **Delete** button to remove an entry from the list. To change existing settings, choose an existing server from the list and click the **Edit** button.

When adding or editing, a dialog box will appear, allowing you to enter connection information.

Note: Connection settings are stored for each Windows user individually, in the registry, under the following node: HKEY_CURRENT_USER\Software\Paessler\PRTG Network Monitor\WinGUI



PRTG Server Connection Settings in Enterprise Console

Server IP/DNS name

- Enter the IP address or DNS name of the PRTG web server the Enterprise Console will connect to.
- This is the same address or name as defined in the web server settings for the core server. For detailed information please see [PRTG Server Administrator](#) ¹⁹⁵⁹ (Web Server) section. Please make sure that the set values match.
- Please make sure that the server is reachable (especially when using Network Address Translation (NAT)) and no firewall settings are blocking the connection.

Port

- Enter the port on which the PRTG web server is running.
- This is the same port as defined in the web server settings for the core server. For detailed information please see [PRTG Server Administrator](#) ¹⁹⁵⁹ (Web Server) section. Please make sure that the set values match.
- Please make sure that the server is reachable (especially when using Network Address Translation (NAT)) and no firewall settings are blocking the connection.

Login Name

- Enter the login name that will be used to login to the web server.
- This can be the administrator login or the login of another PRTG user.
- In a new installation, the login name is **prtgadmin** by default.
- For detailed information about user accounts please see [System Administration—User Accounts](#) ¹⁸²⁴ section.

Password

- Enter the password for the login name entered above.
- In a new installation, the password is **prtgadmin** by default.

Root ID

- Enter the ID of the object that will be considered the root of the device tree.
- Default value is **0**, which is the Root group of your configuration.
- If you enter an other object's ID here, the device tree will start at this object, only showing all other objects below in the hierarchy.
- This is useful to only view a part of the device tree, which is loaded much faster.
- You can create several connections that only differ in the **Root ID** value in order to quickly switch between different views within your configuration, choosing different PRTG core server connections in the Enterprise Console's [Devices](#)  tab.

Display Name (optional)

- Optionally enter a name that will be displayed in the **Server** list.
- If you leave this field blank, the **Server IP/DNS name** setting will be displayed there.

Click the **OK** button to save your settings.

8.5 Options

From the [Windows menu](#) of the Enterprise Console, select **File | Options...** to open the settings dialog.

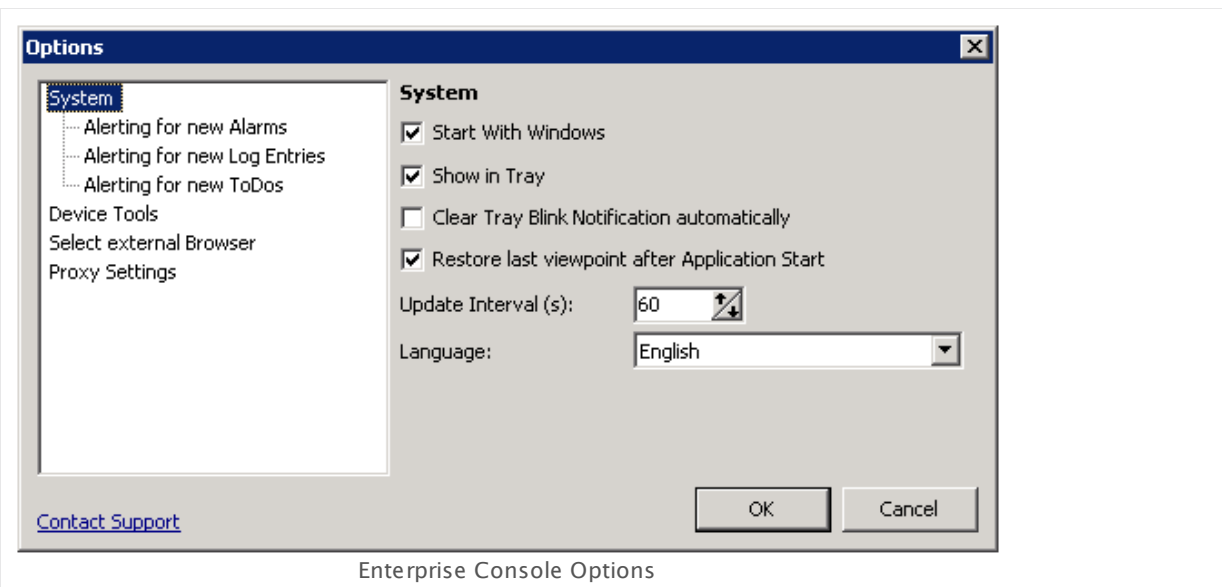
You can choose from these options on the left hand side:

- [System](#)
- [System—Alerting](#)
- [Tools](#)
- [Select External Browser](#)
- [Proxy Settings](#)

System

From the [Windows menu](#) of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

Change general system settings for the Enterprise Console.



Start With Windows

- By default this setting is enabled.
- With this setting enabled, the Enterprise Console will start up automatically when this computer is started.

Show in Tray

- By default this setting is enabled.
- With this setting enabled, a PRTG icon will be shown in the Windows tray.
- On mouse over, it will show a balloon info with the most important status information about your monitoring; with a right-click you can access a menu with access to the most important functions.
- In order to use any alerting functionalities (see [System—Alerting](#)¹⁸⁹⁷ section), you must enable this option. If the tray icon is not shown, no alerting from the Enterprise Console will be available.

Clear Tray Blink Notification automatically

- Whenever there are new entries in the [Alarms](#)¹⁸⁹⁰ list, the tray icon will start blinking. If you enable this option, the tray icon will stop blinking automatically as soon as there are no more alarms.
- With this option disabled, it will keep blinking, even if all alarms should be cleared meanwhile.

Restore last Viewpoint after Application Start

- If this option is enabled, the Enterprise Console saves information about the currently shown view (for example, sensor details, a certain graph, or a Map). It is written to the [registry](#)¹⁹⁰¹ when you close or exit the program. When you open the Enterprise Console again, it will try to restore the same view.
- Only if the object is not available any more (due to changes on the server, or due to unavailability of a server), the default view will be loaded.

Update Interval (s)

- Define the number of seconds that will be waited before the screen is refreshed.
- Default value is **60**.

Language

- Choose the language for this program from the drop down menu. Default is **English**. Depending on your installation, you may be able to choose other languages here.
- This setting will influence the language of the Enterprise Console only.

System—Alerting

From the [Windows menu](#)¹⁹⁰² of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

You can define what the Enterprise Console will do in case of new **Alarms**, **Log Entries**, or **ToDos**. The settings are the same for all of these three cases, but you can individually define them for each case. On the left side, please select either **Alerting for new Alarms**, **Alerting for new Log Entries**, or **Alerting for new ToDos** and define the settings as follows.

Note: All alerting options only take effect when the **Show in Tray** option is enabled in the [system](#)¹⁸⁹⁶ settings above; if the tray icon is disabled, there will be no alerting from the Enterprise Console.

Blink Tray Icon

- The tray icon will blink if there are new items to be alerted for.
- You can additionally set the **Clear Tray Blink Notification automatically** option in the [system](#)¹⁸⁹⁶ settings above.

Balloon Info in Tray

- Show a balloon info next to the PRTG tray icon if there are new items to be alerted for.

Popup Message

- Show a popup message window if there are new items to be alerted for.
- **Note:** The popup window will be always on top until it's closed.

Play Sound

- Play an audible notification if there are new items to be alerted for.
- There is a default sound defined. To change it, please click on the folder symbol and select any standard WAV file from your hard disk drive. PRTG already comes with a small set of sounds you can choose from.
- **Note:** The sound file will be played only on the computer running the Enterprise Console.

Open GUI

- Open the Enterprise Console if there are new items to be alerted for.

Device Tools

From the [Windows menu](#)¹⁹⁰² of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

In the **Device Tools** settings you can define commands that will be available in the [Windows Menu](#)¹⁹⁰² and [context menu](#)¹⁹⁰⁷ of groups, devices, and sensors. A command to initiate a remote desktop connection is already predefined.

Note: In order for the tool function to work with your Windows version, you may need to run the Enterprise Console as administrator.

Please click the **Add** button to add a new command, or choose an existing one from the list and click the **Edit** button to change the settings. Use the **Delete** button to remove an entry from the list.

Name

- Enter a custom name for your command as it will show up in the context menu.

Command

- Enter the command you want to execute on the local machine.
- This can be, for example the name of a program or script, with or without path, according to your system's configuration.

Parameters

- Enter the parameters with which the command will be called.
- You can use the placeholders (variables) shown in the window. Other placeholders are **not** possible. During runtime, these placeholders will be replaced by the respective values set for the object you have selected. For example, the **%id** placeholder will be replaced by the ID of a group, a device, or a sensor, depending on which object you're executing the command for.

Parameters—Available placeholders

The following placeholders (variables) are available in the Enterprise Console.

Placeholder	Available For Groups	Available For Devices	Available For Sensors	Will Be Resolved To
%id	X	X	X	The object's ID as shown in brackets behind the name
%name	X	X	X	The object's Name value.
%host	—	X	X	The sensor's or device's IP Address/DNS Name value
%message	—	—	X	The sensor's Last Message value
%value	—	—	X	The sensor's Last Result value
%type	—	—	X	The sensor's Type value

If a placeholder is used in combination with an object it is not available for, it will simply not be resolved, but the placeholder itself will be returned.

Note: To see the output of all placeholders for different objects you can create a simple test tool that displays the output in a command line window. Just create a tool with the command **cmd** and the following content in the **Parameters** field:

```
/K echo.id: %id && echo.name: %name
    && echo.host: %host && echo.message: %message
    && echo.value: %value && echo.type: %type
```

Then, click an object in the device tree and run the tool from the **Tools** option in the menu (either [Windows](#)¹⁹⁰² or [context menu](#)¹⁹⁰⁷).

Shortcut

- Select a key shortcut for the command. Choose an F-Key from the list or select **None** to not use a key.

Select External Browser

From the [Windows menu](#)¹⁹⁰² of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

With these settings you can define which browser the Enterprise Console will use when you select a command which requires opening an external browser window, for example when calling **View | Open Web GUI...** You can only select browsers installed on the system running the Enterprise Console; other browser options are disabled.

By default, the system's default browser is opened. To change the Enterprise Console's behavior, choose between:

- **Use system default browser (browser.exe)**
- **Use IE (Version: x)**
Note: Only Microsoft Internet Explorer 10 or 11 is supported by the Ajax web interface! Please do not use it with Internet Explorer 9 or earlier! We recommend using Google Chrome 31 or later (recommended) or Mozilla Firefox 25 or later as external browser.
- **Use Firefox (Version: x)**
- **Use Chrome (Version: x)**
- **Use Safari (Version: x)**

Proxy Settings

From the [Windows menu](#)¹⁹⁰² of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

If the connection to the PRTG core servers requires a proxy connection, you can set it here.

Choose between:

- **No Proxy**
Use a direct connection to the servers.
- **Use System Settings**
Use your Windows default settings, configured in Internet Explorer. To view these settings, open the Internet Explorer on your system and select **Tools | Internet Options** from the menu. Select the **Connections** tab and click on the **LAN settings** button.
- **Manual Proxy Configuration**
Manually enter a proxy configuration. Please enter the IP address/DNS name of the proxy, a port number, as well as username and password (if required by the proxy). **Note:** Only basic authentication is available!

Settings Storage

For each individual Windows user account, the settings of the Enterprise Console are stored in the Windows registry. For details, please see [Data Storage](#)²⁰³⁶.

8.6 Windows Menu Structure

The Windows menu of the Enterprise Console has four main menu items:

- [File](#) 
- [Edit](#) 
- [View](#) 
- [Help](#) 

File

- **All PRTG Servers**
Show a list of all configured PRTG core server connections. For detailed instructions, please see [PRTG Servers](#)  settings.
- **Options...**
Open the dialog to set options and to configure one or more PRTG core server connections. For detailed instructions, please see [Options](#)  settings.
- **Close or Exit**
This menu item appears as either **Close** or **Exit**, depending on whether the tray icon is enabled or disabled in the [Options](#)  settings. **Close** will close the Enterprise Console, but alerting will still be available via the tray icon. You can also double click on the tray icon to re-open the Enterprise Console. **Exit** will completely shut down the Enterprise Console. This option is only available if the tray icon is not running.
- **Close and Exit**
This menu item is only shown if the **Show in Tray** option is enabled in the [Options](#)  settings. It will completely shut down the Enterprise Console and tray icon, so no tray alerts are shown any more.

Edit

The content of the **Edit** menu varies, depending on whether and which objects are selected within the [Devices](#) , [Sensors](#) , or [Alarms](#)  tab.

Note: Some of the options will open the Ajax web interface.

When you click on one of these items, a new window or tab of the external browser configured in the Enterprise Console's [Options](#)  will open and PRTG will automatically login and redirect you to the respective web page. If your browser displays a certificate warning, please find more information in the [SSL Certificate Warning](#)  section.

- **Check Now**
This will perform an immediate scan for the selected object.
- **Detail**
This will call the overview tab for the selected object.

- **Edit**
Here you can access the pages for editing **Settings...**, **Notifications**, **Access Rights...**, and **Management** (not for sensors) of the selected object. In addition, you can **Rename...** this object.
- **Add Group...**
This option is available only when a probe or group (not the **Root** group) is selected. This will open the Ajax web interface which guides you through adding a new group to the selected probe or group. For detailed instructions, please see [Add a Group](#)^[205].
- **Add Auto-Discovery Group...**
This option is available only when a probe or group (not the **Root** group) is selected. This will open an assistant which guides you through adding such a group. For detailed instruction, please see section [Auto-Discovery](#)^[190].
- **Add Device...**
This option is available only when a probe or group (not the **Root** group) is selected. This will open the Ajax web interface which guides you through adding a new device to the selected probe or group. For detailed instructions, please see [Add a Device](#)^[211].
- **Add Sensor...**
This option is available only when a device is selected. This will open the Ajax web interface which guides you through adding a new sensor to the selected device. For detailed instructions, please see [Add a Sensor](#)^[220].
- **Run Auto-Discovery**
This option is available only when a device is selected. If you select this option, an automatic search is started, adding new sensors to the selected device. The search is running in the background. If found, you will see new sensors after a few minutes automatically. For more information, please see [Auto-Discovery](#)^[191] (**Run Auto-Discovery Now**).
- **Create Device Template...**
This option is available only when a device is selected. This will open the Ajax web interface which guides you through creating a device template; this will then be available in [auto-discovery](#)^[190]. For detailed instructions, please see [Create Device Template](#)^[1715].
- **Sort Alphabetically**
This option is available only when a probe, a single group, or a device is selected. This will sort direct children of the selected node such as groups, devices, or sensors in alphabetical order. The ordering will be stored in the monitoring configuration and cannot be revoked.
- **Check Now**
For all selected objects from the device tree (use the **Ctrl** key to select multiple objects), perform an immediate scan. This will poll all selected devices and query new data for all sensors on them. If you choose this option for a probe or a group, data for all sensors in the [object hierarchy](#)^[83] underneath will be queried.
- **Acknowledge Alarm...**
This option is available only when a sensor in a **Down** or **Down (Partial)** status is selected. For details on how to acknowledge an alarm, please see [Alarms](#)^[1881] section.
- **Delete**
This will delete the selected object(s). You will be asked for confirmation before anything is actually deleted.
- **Clone...**
This option is available only when a single group, device, or sensor is selected. This will open the Ajax web interface which guides you through cloning the selected object. For detailed instructions, please see [Clone Object](#)^[1708].

- **Move >**

This will move the selected object(s) of the device tree (use the **Ctrl** or **Shift** key to select multiple objects). Choose between **Top**, **Up**, **Down**, and **Bottom** to move the object(s) to the top or bottom of the mother node, resp. one entry up or down. If you have selected several objects which are not neighbors to move them, then the first object in the list will be moved up resp. down and the others will be attached below this object. You can also move the selected object(s) to another group with **To Other Group...** A popup will appear in this case with information about the selected object and the sub-objects which will also be moved. Please choose a target group from the list. **Note:** Please see section [Devices](#)^[1875] for details about allowed movements.

- **Pause >**

For all selected objects from the device tree (use the **Ctrl** key to select multiple objects), you can pause and resume monitoring, or set a sensor to error for testing purposes. **Hover** to see available options. You can choose between: **Pause Indefinitely**, **Resume** from pause, **pause For 5 Minutes**, **For 15 Minutes**, **For 1 Hour**, **For 3 Hours**, **For 1 Day**, **Pause Until...**, or **Set Sensor to Error**. The last option only takes effect when a sensor is chosen. If you choose **Pause Until...** a popup window will appear where you can define a date. Monitoring will be resumed after this date. You can also set up a **One-time maintenance window**: enter start and end date of the maintenance in the appearing popup window. You can also use the **date-time picker** for this purpose.

- **Rename...**

Rename the selected object. A popup will appear. Please enter a new name and confirm with the **OK** button.

- **Priority/Favorite >**

With this option you can set the priority for any object and you can add devices and sensors to favorites. For details, please see section [Priority and Favorites](#)^[159].

- **Historic Data >**

This will open the historic data tab of the selected object. You can choose between **Last 2 days...**, **Last 30 days...**, and **Last 365 days...**, or when selected one sensor **Live Data...** and **View Historic Data...**. You can also create a report. For detailed instructions, please see [Historic Data Reports](#)^[133] (**Menu**). When selected one or more sensors (hold the **Ctrl** or **Shift** key to select multiple items), it is possible to call the [Compare Sensors](#)^[129] function. The graphs of all chosen sensors will be added to comparison automatically. You can add additional sensors in the appearing comparison dialog.

- **Drag & Drop Sorting**

In order to use the option to sort all objects in the device tree via drag and drop, please enable this option. By default, this option is disabled to avoid accidental moves of objects. In this case, a dialog box appears when you try to drag an object. You can disable the dialog box message by clicking the respective check box which is shown together with the message. For details, please see section [Devices](#)^[1875].

- **Device Tools** ›

Call a tool command. All placeholders (variables) configured in a tool command will be resolved for the currently selected object. **Hover** to see all available tools configured in your [Options](#) settings (Device Tools). By default, a **Remote Desktop** tool is pre-configured which tries to initiate a remote desktop connection to the IP address or DNS name of the selected object (this will usually work for devices, of course). You can also add a device tool directly to the selected object: **Add Device Tool...** will open [Options—Device Tools](#).

For devices, additional options are available. They allow you to connect to the **Service URL** value defined in the device's [settings](#), or open the **IP address/DNS name** of the device via the protocols **HTTP**, **HTTPS**, and **FTP**. For each of these functions, your system's default programs will be used. Usually, this is your browser. You can also install a remote probe on a device via [Remote Probe Quick Setup](#).

Note: In order for the tool function to work with your Windows version, you may need to run the Enterprise Console as administrator.

- **Send link by email**

You can send the link to the selected probe by email. This will open a new email using your system's standard email client. It will contain a direct link to the selected probe's details page.

- **Open in Web Browser**

This will open the currently selected object in the Ajax web interface. This option is not available if multiple objects are selected. The default browser can be set in the [Options](#) settings. **Note:** This option is available in the [Context Menus](#) and under [View](#).

View

- **Refresh**

This will immediately query data for the current screen from the PRTG core server, just as the automatic refresh does, which can be configured in the [Options](#) settings.

- **Open Web GUI...**

This will open the start page of the Ajax web interface in the external browser. The default browser can be set in the [Options](#) settings.

- **Large Single Graph**

Change the view in [Devices](#) menu tab to large single graphs. This will display live graphs, and graphs for three other time spans, in different tabs.

- **Small Multiple Graphs**

Change the view in [Devices](#) menu tab to multiple small graphs. This will display live graphs, and graphs for three other time spans. This will display all graphs in one tab.

- **Show Geo Maps**

Choose if you want to show geographical maps in the Enterprise Console.

- **Show News Feed**

Choose if you want to show the news feed in the Enterprise Console.

- **Next Viewpoint**

Go forward to the next viewpoint (only available if you went back to a previous viewpoint before). This is similar to a browser's function to go forth in history.

- **Previous Viewpoint**

Go backwards to the previous viewpoint. This is similar to a browser's function to go back in history.

- **Open in Web Browser**

This will open the currently selected object in the Ajax web interface. This option is not available if multiple objects are selected. The default browser can be set in the [Options](#)  settings.

Help

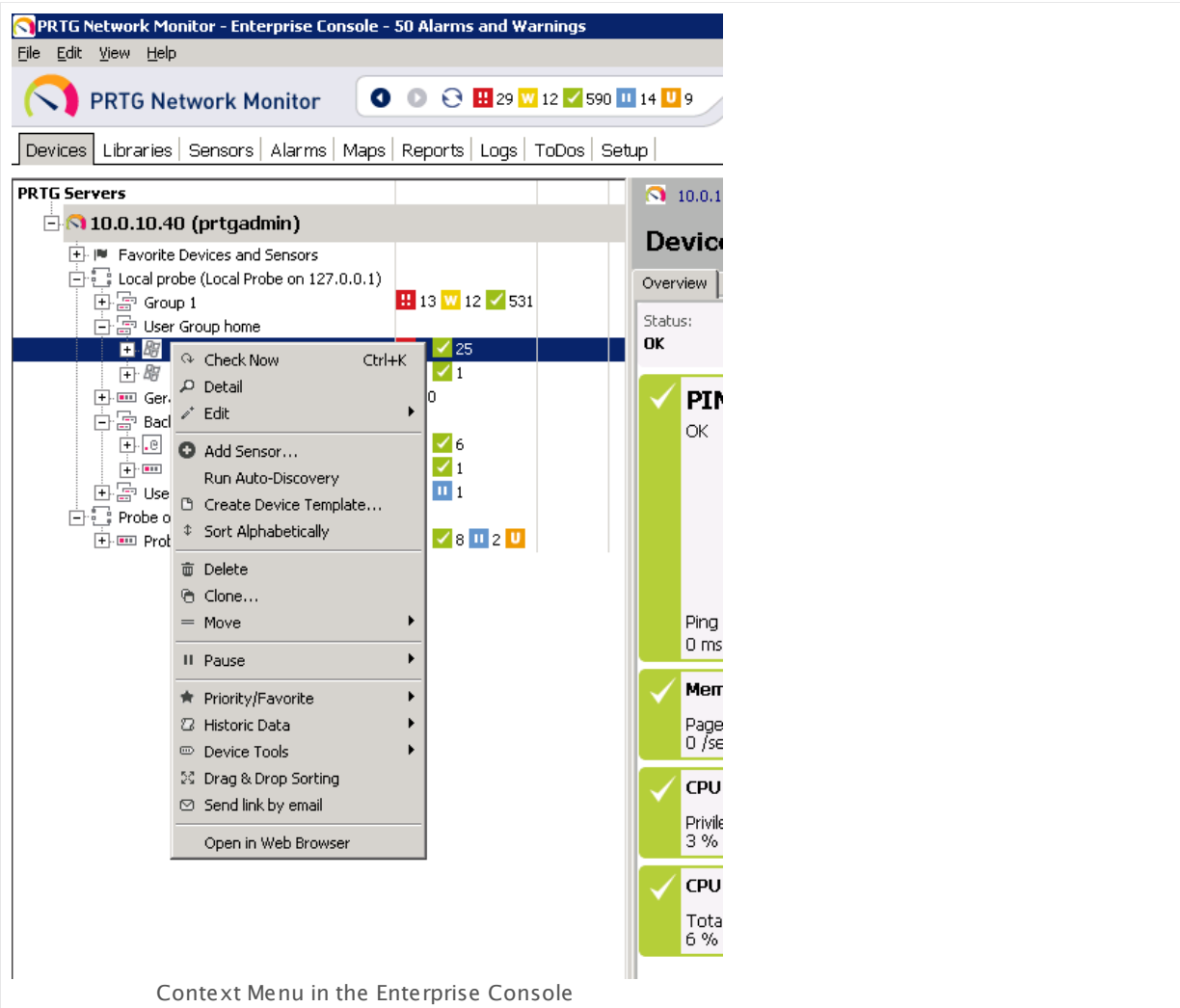
This menu provides web site links to the **HTML manual**, the **Paessler Knowledge Base**, and the **PRTG Network Monitor homepage**. You can start the [Configuration Guru](#)  and display program information when you select **About....**

See Also

- [Shortcuts Overview](#) 

8.7 Context Menus

For every object in the Enterprise Console, there are context menus available which appear when you right-click on object. These context menus vary depending on the selected object and always contain a sub-set of the options available in the Windows menu. For detailed explanations, please see [Windows Menu Structure](#) ¹⁹⁰².



8.8 Shortcuts Overview

The following shortcut keys are available in the Enterprise Console:

Alt+X: File | Close **or** Exit

With the **Show in Tray** option enabled in the [Options](#) 1896 settings, this will be **Close**; otherwise **Exit**.

Ctrl+Alt+X: File | Close and Exit

This menu item is only shown if the **Show in Tray** option is enabled in the [Options](#) 1896 settings.

Alt+Right: Next Viewpoint

Alt+Left:

Ctrl+C: Edit | Check Now

Ctrl+E: Edit | Pause | Set Sensor to Error

Ctrl+P: Edit | Pause | Indefinitely

Ctrl+R: Edit | Pause | Resume

Ctrl+L: View | Large Single Graph

Ctrl+S: View | Small Multi Graphs

Ctrl+H: View | Hide Google Map

Ctrl+Del: Edit | Acknowledge all ToDos (available only while in ToDos tab)

F5: View | Refresh

F6: [Context Menu] | Tools | **Custom tool command, if available**

F7: [Context Menu] | Tools | **Custom tool command, if available**

F8: [Context Menu] | Tools | **Custom tool command, if available**

F9: [Context Menu] | Tools | **Custom tool command** (default: **Remote Desktop**)

F10: [Context Menu] | Tools | **Custom tool command, if available**

F11: [Context Menu] | Tools | **Custom tool command, if available**

F12: [Context Menu] | Tools | **Custom tool command, if available**

See Also

- [Windows Menu Structure](#) 

Part 9

Other User Interfaces

9 Other User Interfaces

This chapter introduces other available user interfaces besides PRTG's Ajax web interface and Enterprise Console. There are special interfaces optimized for mobile access, including apps for mobile devices. Read more in the following sections.

Other User Interfaces—Topics

- [Mobile Web GUI](#)  1913
- [Smart phone Apps](#)  1916

Related Topics

- [Ajax Web Interface—Basic Procedures](#)  100
- [Ajax Web Interface—Device and Sensor Setup](#)  188
- [Ajax Web Interface—Advanced Procedures](#)  1700
- [Enterprise Console](#)  1860

9.1 Mobile Web GUI

The Mobile Web GUI is a slim interface to view your monitoring results while on the go. It is optimized for both small screens and low bandwidth usage in order to provide an easy and fast access to your PRTG core server when connecting with mobile devices. You can view sensor lists, data tables, and graphs with live data.

Compared to the [Ajax Web GUI](#)^[100], this interface comes with limited functionality and is primarily provided for quick review of data while on the go. Nevertheless, you can acknowledge alarms, pause or resume monitoring, and interactively view geo maps as well as sensors and other lists.

This interface is based on jQuery Mobile 1.0, supporting all major mobile operating systems and browsers.

Loading the Web Interface

Make sure your PRTG core installation is accessible via the internet. In your mobile device, enter the IP address or URL of the system PRTG is installed on. When using a cluster, you can connect to any node accessible.

If you see a certificate warning in your browser, you can usually just confirm it. For more information please see [SSL Certificate Warning](#)^[105].

Login Screen

After loading the web interface, the login screen is shown.

The screenshot shows the login interface for PRTG Network Monitor. On the left, there's a login form with fields for 'Login Name' and 'Password'. Below these are three radio button options: 'Use AJAX Web GUI (All features, optimized for desktop access)', 'Use Mobile Web GUI (Limited functionality, optimized for mobile access)' (which is selected), and 'Download Client Software (for Windows, iOS, Android)'. There are two buttons: 'Login' and 'Default Login'. A link 'Forgot password? Need Help?' is at the bottom left. On the right, the PRTG Network Monitor logo is displayed above a section titled 'NEWS FROM PAESSLER' which contains three short news items. At the bottom center, the text 'Mobile Web GUI Login' is visible.

Enter your credentials, choose the **Use Mobile Web GUI (Limited functionality, optimized for mobile access)** option, and click on **Login**. For detailed information about different credentials, please see the [Login](#)^[102] section for the Ajax Web GUI.

General Layout

The home screen of the Mobile Web GUI shows the sensor overview as well as all available main menu entries. Click/tab on menu items to get to groups, devices, and sensor data. You will be guided through a sequence of sub and sub-sub screens. Whenever you get lost, click/tab on the house symbol in the upper left corner to get back to the home screen.



There are also different sensor top lists available underneath the **Sensors** menu entry. **Note:** Most of the functionality is read-only, because this interface is intended for viewing data. In order to change your monitoring configuration or settings, please switch to the [Ajax Web Interface](#)^[100]. If you would like to have more options on your mobile devices, take a look at our [Smart phone Apps](#)^[101].

Using the Mobile Web GUI

The device tree and lists of sensors, alarms, logs, and tickets are available as usual, but in a view optimized for mobile screens. In addition, you can show monitoring data for all objects. This section will not explain the GUI in detail, because the concepts are the same as throughout the [Ajax web interface](#)^[100]. In the following, find a list with the main differences compared to the full Ajax interface:

- There are no context menus available, but actions such as acknowledge an alarm, scan now, pause, etc. can be initiated directly on an objects detail page, using the respective buttons.

- Reports and Maps are accessible in view only mode.
- You cannot edit system settings.
- To save bandwidth, an automatic page refresh is only activated after dedicated confirmation.
- You can switch from the Mobile Web GUI to the Ajax web interface at any time by using the **Switch to AJAX GUI** option.

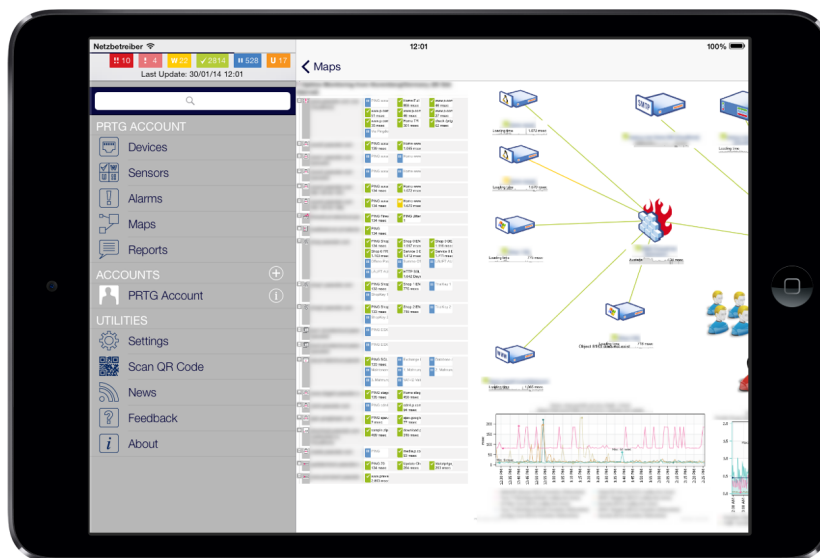
You will just need a few minutes to get familiar with this interface, because the structure is basically the same as you know it from PRTG's Ajax web interface. Have fun monitoring while on the go!

9.2 Smartphone Apps

There are PRTG apps for iOS and for Android devices. We also provide apps for BlackBerry and Windows Phone (currently in beta status; see section [More](#)¹⁹¹⁶). You can connect to your PRTG installation with these apps while on the go. If there is no PRTG app available for your mobile device, use the [Mobile Web GUI](#)¹⁹¹³ interface as an alternative.

PRTG for iOS

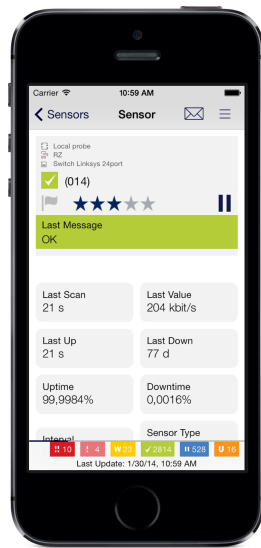
PRTG for iOS is the iOS app for PRTG Network Monitor. You can use it on iPhone, iPad, and iPod touch.



Maps on iPad

Don't let monitoring your network tie you to your desk! With PRTG for iOS, your network monitor is where your iPhone is. PRTG for iOS is an app for network administrators using the PRTG Network Monitor software to monitor and administrate their network. PRTG for iOS is a free app to have your entire network monitoring environment always with you. Your iOS device requests the monitoring data directly from your PRTG server(s) and displays it in the well-known iOS way. You can also perform several actions which you know from PRTG's Ajax WebGUI.

As of iOS 7, the app can check one or more PRTG servers in the background. It will notify you if something goes wrong in your network and you can call the affected sensor directly from your device's home screen to view details about the alarm.



PRTG for iOS on an iPhone

In order to use PRTG for iOS, your PRTG core server must be reachable from the network your device is connected to. You can view monitoring data and perform certain actions, such as acknowledge alarms, pause or resume monitoring, etc. **Note:** The app currently does not support PRTG [cluster](#) setups!

In order to get the app, please see [More](#) section below.

PRTG for Android

PRTG for Android is the Android app for PRTG Network Monitor. Use it on your phone, your tablet, or on a Kindle Fire.

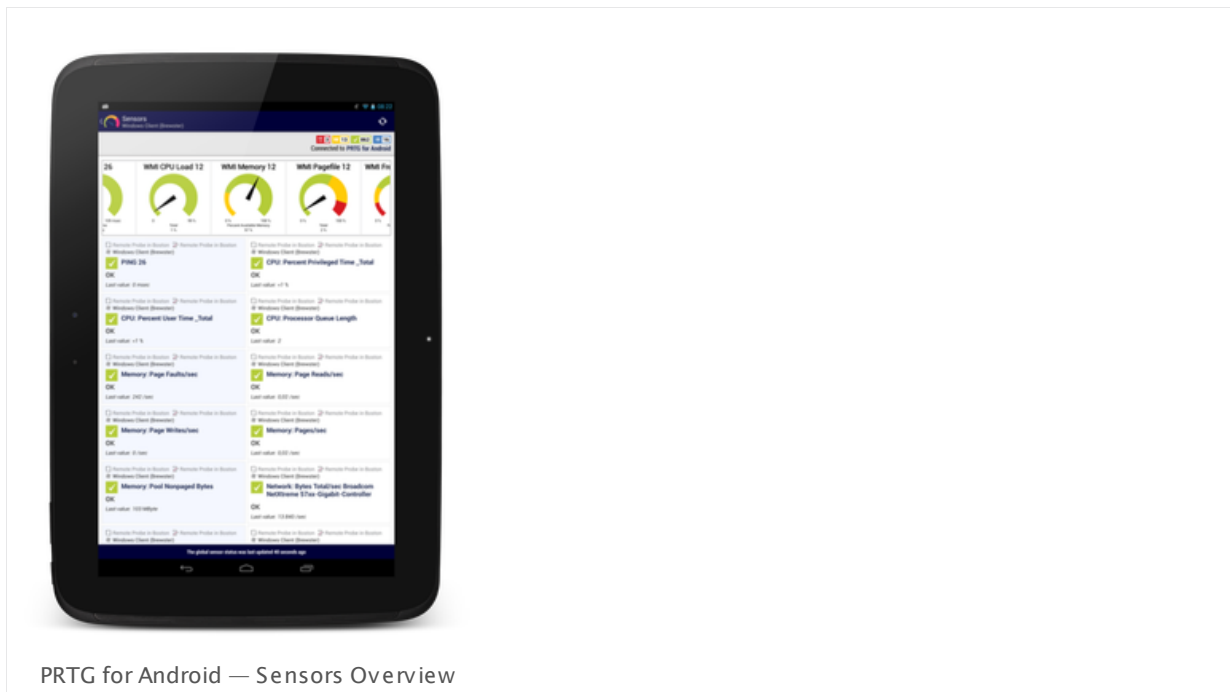


PRTG for Android — Main Menu Bar

The features include:

- Multiple accounts support to query different server/login combinations. Switch easily between different accounts to quickly view monitoring data of several installations and/or accounts.
- The app can check all accounts, or only specific ones, automatically in the configured polling interval and notify you in your device's status bar whenever there are alarms for one of them.
- Configure when you want to be notified: when Alarms > 0, or when there is a certain number of new alarms, or when alarms count raised since last check. Configure notifications via the system status bar with ringtone and/or vibration (triggered for new notifications). You can exclude "Warning" or "Unusual" states from alarms count, and set up notifications based on priority.
- PRTG for Android works with your PRTG core server to show you your device tree, sensor lists, sensor data, etc., in an Android familiar way. You can add sensor gauges as well as the global sensor status as widgets to your home screen. The data display automatically adapts to your screen size, so you can see as much information as possible at a glance.
- Many features of PRTG's web interface are available to perform actions with the app: acknowledging alarms, pausing and resuming monitoring, setting priorities and favorites, running device auto-discovery, scanning the network status instantly, etc. With QR code scanning, you can jump directly to sensor.
- The app provides additional network tools such as ping, traceroute, DNS, raw HTTP, and MAC address lookups. You can use these tools also without connecting to a PRTG server.

In order to use PRTG for Android (except for the additional network tools), your core server must be reachable from the network your device is connected to. For further information and the download link, please see section [More](#) ^{19/19} below.



More

More information about PRTG for iOS:

- <http://www.paessler.com/iosapp>

More information about PRTG for Android:

- <http://www.paessler.com/androidapp>

Blog Article: Are You Interested in a PRTG App for Windows Phone?

- <http://www.paessler.com/blog/2014/02/18/prtg/are-you-interested-in-a-prtg-app-for-windows-phone>

Knowledge Base: Is there a PRTG app for BlackBerry?

- <http://www.paessler.com/knowledgebase/en/topic/59382>

Part 10

Sensor Technologies

10 Sensor Technologies

This chapter introduces different technologies that PRTG uses for monitoring in order to give you more background information. Please read more in the following sections.

Sensor Technologies—Topics

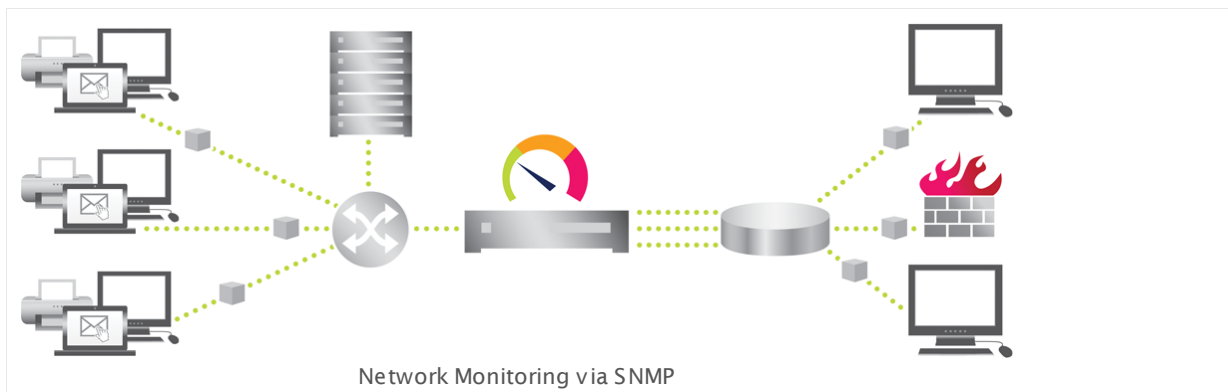
- [Monitoring via SNMP](#)  1923
- [Monitoring via WMI](#)  1927
- [Monitoring via SSH](#)  1930
- [Monitoring Bandwidth via Packet Sniffing](#)  1932
- [Monitoring Bandwidth via Flows](#)  1934
- [Bandwidth Monitoring Comparison](#)  1937
- [Monitoring Quality of Service](#)  1939
- [Monitoring Email Round Trip](#)  1943
- [Monitoring Backups](#)  1945
- [Monitoring Virtual Environments](#)  1946
- [Monitoring Databases](#)  1955

10.1 Monitoring via SNMP

Monitoring via Simple Network Management Protocol (SNMP) is the most basic method of gathering bandwidth and network usage data.

How SNMP Monitoring Works

SNMP can be used to monitor bandwidth usage of routers and switches on a port-by-port basis, as well as device readings such as memory, CPU load, etc. The queried devices must support SNMP.



When this technology is used, PRTG sends small data packets to devices, for example, querying routers, switches, and servers for the traffic counters of each port. These are triggering reply packets from the device. Compared to PRTG's other bandwidth monitoring technologies via flows, packet sniffing, or WMI, the SNMP option creates the least CPU and network load.

Reasons to Choose SNMP Monitoring

SNMP is the most commonly used method mainly because it is easy to set up and requires minimal bandwidth and CPU cycles. If your network devices support SNMP and/or if you want to monitor large networks with several hundred or thousands of sensors, we recommend you start with SNMP. Besides network usage monitoring, another well-known feature of SNMP is the ability to also watch other network parameters such as CPU load, disk usage, temperature, as well monitoring many other readings, depending on the queried device.

SNMP Network Issues

In order to use Simple Network Management Protocol (SNMP) for monitoring purposes, it is imperative that UDP packets are allowed to travel from the machine running PRTG to the device you want to monitor and back, which is usually the case in LANs and Intranets. For connections across the internet, to a Demilitarized Zone (DMZ), or for Wide Area Network (WAN) connections, some changes to the traversed firewalls may be necessary. Keep in mind that SNMP V1 and V2c are not secure protocols and should not be used across the internet or insecure data connections. Only SNMP version 3 supports encryption.

Understanding SNMP Sensors

To better understand and set up SNMP sensors, you may want to learn more about the principle of Object Identifiers (OID) and Management Information Base (MIB). For more information about this, please refer to the Knowledge Base article in the [More](#) ¹⁹²⁶ section below.

For an overview and details about all SNMP sensors, please see the [List of Available Sensor Types](#) ²⁹³ section.

SNMP Versions

PRTG supports three versions of the SNMP protocol: Version 1, version 2c, and version 3.

SNMP Version 1

This is the oldest and most basic version of SNMP.

- Pro: Supported by most SNMP-compatible devices; simple to set up.
- Contra: Limited security as it only uses a simple password (**community string**) and data is sent in clear text (unencrypted). It should therefore only be used inside LANs behind firewalls, not in WANs; only supports 32-bit counters which is not enough for high-load (gigabits/second) bandwidth monitoring.

SNMP Version 2c

This version adds 64-bit counters.

- Pro: Supports 64-bit counters to monitor bandwidth usage in networks with gigabits/second loads.
- Contra: Limited security (same as with SNMP V1).

SNMP Version 3

This version adds authentication and encryption to SNMP.

- Pro: Offers user accounts and authentication for multiple users and optional data packet encryption, increasing available security; plus all advantages of Version 2c.
- Contra: Difficult to configure. Not suitable for large networks (see below for more information).

It is important to know that if you select an SNMP version which is not supported by the server or device you want to monitor, you will receive an error message. Unfortunately, in most cases, these error messages do not explicitly mention the possibility that you could be using the incorrect SNMP version. These messages provide minimum information only, such as **cannot connect** or similar. Similar error occur when community strings, usernames, or passwords don't match.

SNMP Overload and Limitations of the SNMP System

SNMP V1 and V2 scale directly with the performance of the hardware and the speed of the network. In our labs we were able to monitor 30,000 SNMP V1 sensors at a 60 second interval with one PRTG server (core and local probe) plus two remote probes with 10,000 sensors each.

However, SNMP V3 has performance limitations due to the SSL encryption. The main limiting factor is CPU power (as well as the other general limits for PRTG). Because of this limitation, you can monitor only a limited number of sensors per second using SNMP V3. Currently, PRTG is able to handle roughly 40 requests per second and computer core, depending on your system. This means that, on a common 1.x GHz computer with two cores, you can run about 5,000 SNMP v3 sensors with a 60 seconds scanning interval; on a system with four cores, you can monitor around 10,000 sensors with 60 seconds interval. The CPU load is at about 50% then. We do not recommend more.

Furthermore, the PRTG core server and probes should run on different computers. If you experience increased values in the **Interval Delay SNMP** or **Open Requests** channels of the **Probe Health**⁷⁹⁷ sensor (values above 0 % indicate that the SNMP requests cannot be performed at the desired interval), you need to distribute the load over multiple probes. SNMP V1 and V2 do not have this limitation.

If you run into SNMP overload problems you have three options:

- Increase the monitoring interval of the SNMP V3 sensors.
- Distribute the SNMP V3 sensors over two or more probes.
- Switch to SNMP V1 or V2 if you can go without encryption.

What is the SNMP Community String?

The SNMP **Community String** is similar to a user ID or password that allows access to a router's or other device's statistics. PRTG Network Monitor sends the community string along with all SNMP requests. If the correct community string is provided, the device responds with the requested information. If the community string is incorrect, the device simply discards the request and does not respond.

Note: SNMP community strings are only used by devices that support SNMP V1 and SNMP V2c protocols. SNMP V3 uses safer username/password authentication, along with an encryption key.

By convention, most SNMP V1/V2c equipment ships with a read-only community string set to the value **public**. It is standard practice for network managers to change all the community strings to customized values during device setup.

More

Tools: Paessler MIB Importer and SNMP Tester

- <http://www.paessler.com/tools/>

Knowledge Base: How do SNMP, MIBs and OIDs work?

- <http://www.paessler.com/knowledgebase/en/topic/653>

Paessler White Papers: [Introducing SNMP](#) and [Putting SNMP into Practice](#)

- http://www.paessler.com/press/whitepapers/introducing_snmp

German: Paessler White Paper: [Einführung in SNMP](#) und [SNMP praktisch anwenden](#)

- http://www.de.paessler.com/press/whitepapers/introducing_snmp

Knowledge Base: My SNMP sensors don't work. What can I do?

- <http://www.paessler.com/knowledgebase/en/topic/46863>

10.2 Monitoring via WMI

Windows Management Instrumentation (WMI) is Microsoft's base technology for monitoring and managing Windows based systems. PRTG uses this technology to access data of various Windows configuration parameters and status values. However, sensors using the WMI protocol generally have a high impact on the system performance. In addition to strict WMI sensors, there are sensors which use another approach to monitor Windows systems with less influence on the system performance.

Monitoring Windows Systems: Performance Counters

Besides sensors which monitor Windows systems only via WMI, PRTG provides sensor types which use a **hybrid** approach. These sensors first try to query data via Windows **Performance Counters** using **Remote Registry Service**. Querying Performance Counters needs less system resources than monitoring via WMI. These Windows sensors use WMI as a fallback if Performance Counters are not available or cannot be read out. When running in fallback mode, PRTG re-tries to connect to Performance Counters after 24 hours. This is the default approach and can be changed in the **Windows Compatibility Options** in the [Device Settings](#)^[272]. Though, it can be the case sometimes that these Performance Counters differ from the direct method.

Note: You can identify these hybrid sensors by looking at their categories, for example, in the add sensor dialog. **Search directly** for "windows" and select "Performance Counters" as **Technology Used**. Among them are various sensors with "Windows" in the name, as well as some Hyper-V sensors.

How WMI Works

WMI allows accessing data of many Windows configuration parameters, as well as current system status values. Access can be local or remote via a network connection. WMI is based on **COM** and **DCOM** and is integrated in Windows 2000, XP, 2003, Vista, 2008, Windows 7, and Windows 8 (add-ons are available for Windows 9x and NT4). PRTG officially supports WMI for Windows XP or later.

In order to monitor remote machines, PRTG's WMI sensor needs Active Directory account credentials to have access to the WMI interface. You can enter these credentials in PRTG for the parent device or group, or in the [Root](#)^[224] group. The sensor will then inherit these settings.

Note: Sensors using the Windows Management Instrumentation (WMI) protocol generally have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[77]. Above this number, please consider using multiple [Remote Probes](#)^[2012] for load balancing.

For an overview and details about all WMI sensors, please see the [List of Available Sensor Types](#)^[294] section.

Limitations of WMI on Windows Vista and Windows Server 2008 R1

You should be aware that performance of WMI based monitoring is drastically limited when the monitoring station or the monitored client runs on Windows Vista or Windows Server 2008 R1. When it comes to network monitoring via WMI, Windows XP and Windows 2003 are up to 70 times faster than Windows 2008 or Vista.

Note: These are not limitations of PRTG, but arise from the WMI functionality built into the Windows operating systems mentioned.

The results of our tests are:

- On Windows XP/Windows 2003/Windows 7/Windows 2008 R2 you can run about 10,000 WMI sensors with one minute interval under optimal conditions (such as running the core and the target systems exclusively under Windows 2003 and being located within the same LAN segment). Actual performance can be significantly less depending on network topology and WMI health of the target systems - we have seen configurations that could not go beyond 500 sensors (and even less).
- On Windows Vista/Windows 2008 R1 you can run about 300 WMI sensors with one minute interval.
- The more Windows Vista/Windows 2008/Windows 7 client systems you have in your network the more WMI monitoring performance will be affected.
- System performance (CPU, memory etc.) of virtualization does not strongly affect WMI monitoring performance.

If you want to use WMI for network monitoring of more than 20 or 30 systems, please consider the following rules:

- Do not use Windows Vista or Windows 2008 R1 as monitoring stations for WMI-based network monitoring.
- If possible use Windows 2003 R2 Server for WMI based network monitoring (followed by XP and Windows 7/2008 R2).
- If you cannot run PRTG on Windows XP/Windows 2003 consider setting up a remote probe with XP for the WMI monitoring. (You still get far better WMI monitoring performance with a remote probe on a virtual machine running Windows XP or Windows 2003 than on any bare metal system running Windows Vista/Windows 2008 R1.)
- Consider switching to SNMP-based monitoring for large networks. Using SNMP you can easily monitor 10 times as many nodes as with WMI (on the same hardware).

More

Knowledge Base: General introduction to WMI and PRTG

- <http://www.paessler.com/knowledgebase/en/topic/1043>

Tool: Paessler WMI Tester. A useful freeware tool to test WMI connections. Tests the accessibility of WMI (Windows Management Instrumentation) counters in a quick and easy manner.

- <http://www.paessler.com/tools/wmitester>

CEO's Blog: Don't Use Windows Vista And Windows 2008 R1 for Network Monitoring via WMI!

- <http://www.paessler.com/blog/2010/09/22/>

10.3 Monitoring via SSH

Monitoring via Secure Shell (SSH) enables you to gather performance and system data from many Linux and Unix distributions, as well as from certain Mac OS X systems. If your system is supported this monitoring works natively without the need of additional software on the target systems.

How Monitoring via SSH Works

In order to monitor remote machines via SSH, PRTG needs credentials (preferably root access) of the devices. If you use PRTG's SSH sensors, you can enter the necessary credentials in PRTG for the parent device or group, or in the [Root](#)²²⁴ group, in the [Credentials for Linux \(SSH/WBEM\) Systems](#) section within the [Settings](#)¹⁴¹ tab. The sensors will then inherit these settings.

With each scanning interval, PRTG will login to your devices and query data by executing specific commands.

For an overview and details about all SSH sensors, please see the [List of Available Sensor Types](#)²⁹⁶ section.

Limitations When Using SSH Monitoring

Due to the plurality of Linux/Unix derivatives, PRTG's SSH sensors cannot support all distributions on the market. Also, only certain Mac OS systems are supported. For a detailed list please see the [More](#)¹⁹³¹ section below.

Authentication via SSH Private Key

PRTG supports authentication via password or via private key.

When using a private key, please ensure the following:

- Provide the key in [OpenSSH](#) RSA format.
- The key may **not** be encrypted! PRTG does **not** support password protected keys.
- The key must be provided as [RSA](#) key, you cannot use DSA keys with PRTG!

When providing an unencrypted RSA private key in OpenSSH RSA format, please copy the entire key, including the

```
-----BEGIN RSA PRIVATE KEY-----
```

and

```
-----END RSA PRIVATE KEY-----
```

lines, into the according text field in PRTG and **Save** your settings. Once pasted and saved, the private key will be shown as

```
*****
```

Please make sure there exists a corresponding public key on the target device.

For a detailed description how to convert and use an existing SSH key, please see the [More](#)  section below.

More

Knowledge Base: Which Linux or Mac OS distributions are supported by the Linux/Unix sensors (SSH, SNMP, WBEM)?

- <http://www.paessler.com/knowledgebase/en/topic/6733>

Knowledge Base: How can I use private keys for my SSH sensors with PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/32883>

Knowledge Base: How do I enable SSH on my Mac OS X system?

- <http://www.paessler.com/knowledgebase/en/topic/33113>

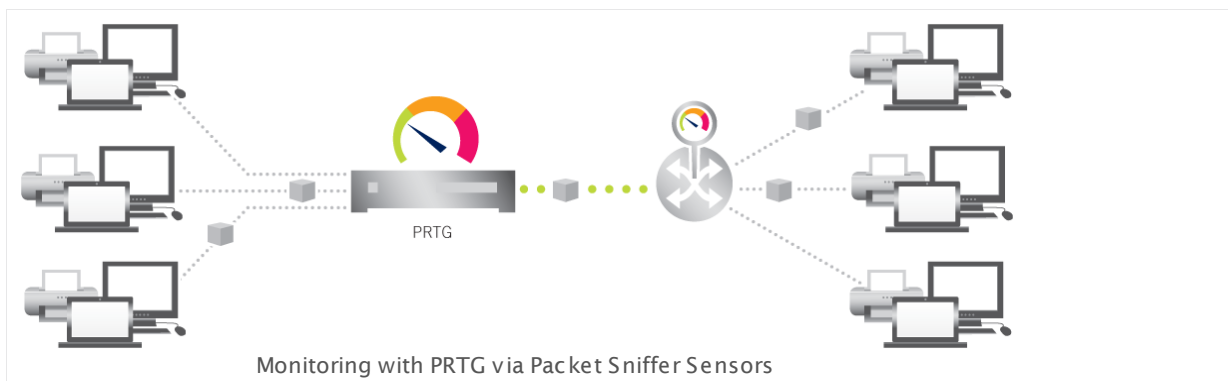
10.4 Monitoring Bandwidth via Packet Sniffing

Packet Sniffing should come into consideration if your network device(s) do not support SNMP or xFlow to measure bandwidth usage and if you need to differentiate the bandwidth usage by network protocol and/or IP addresses.

Note: Packet Sniffer Sensors support Toplists (Top Talkers, Top Connections, etc.), see [Toplists](#) ¹⁷⁰² section.

How Packet Sniffing works

If you need to know what applications or IP addresses are causing the traffic in your network, you can use a packet sniffer. This will look at every single data packet traveling through your network for accounting purposes.



PRTG can analyze the packets passing the network card of a PC or it can be connected to the so-called monitoring port of a switch. In order to calculate bandwidth usage, PRTG inspects all network data packets either passing the PC's network card (shown on the left side) or the data packets sent by a monitoring port of a switch (right side) with its built-in packet sniffer. Using remote probes you can set up packet sniffers anywhere in your network (see [Add Remote Probe](#) ²⁰¹¹ section).

Comparing the four bandwidth monitoring technologies provided by PRTG (SNMP, WMI, xFlow and packet sniffer) this one creates the most CPU and network load and should thus only be used in small to medium networks, on dedicated computers for larger networks or for individual computers.

Reasons To Choose Packet Sniffing

It is important to understand that the packet sniffer can only access and inspect data packets that actually flow through the network interface(s) of the machine running the PRTG probe software. This is fine if you only want to monitor the traffic of this machine (e.g. your web server). In switched networks, only the traffic for a specific machine is sent to each machine's network card, so PRTG can usually not discern the traffic of the other machines in the network.

If you also want to monitor the traffic of other devices in your network, you must use a switch that offers a "monitoring port" or "port mirroring" configuration (Cisco calls it "SPAN"). In this case the switch sends a copy to the monitoring port of all data packets traveling through the switch. As soon as you connect one of the PRTG probe system's network cards to the switch's monitoring port, PRTG is able to analyze the complete traffic that passes through the switch.

Another option is to set up the PC running PRTG as the gateway for all other computers in the network.

Set Up Packet Sniffer Sensors

Find details on how to set up the different flow sensors in the following sections:

- [Packet Sniffer Sensor](#) 722
- [Packet Sniffer \(Custom\) Sensor](#) 729

Header Based Packet Sniffing

For packet sniffing, PRTG looks at the IPs and ports of source and destination to assess the protocol. This is a very fast method which saves system resources. **Note:** At times, this method is not fully accurate. For example it is not possible to identify HTTP traffic on ports other than 80, 8080 and 443 as HTTP. HTTP traffic on non-standard ports would not be accounted as such.

More

Tool: Paessler Card Packet Counter: Shows short term statistics about the network data packets passing a local network card.

- <http://www.paessler.com/tools/>

10.5 Monitoring Bandwidth via Flows

Using Flow protocols you can monitor the bandwidth usage of all packets going through a device. In PRTG, you can view [Toplists](#) for all xFlow (including IPFIX) sensors.

How xFlow Monitoring works

You can measure bandwidth usage **by IP address** or **by application** in a network, using one of the xFlow (including IPFIX) protocols. They are the best choice especially for networks with high traffic (connections with 100s of megabit or gigabits). For xFlow monitoring the router gathers bandwidth usage data (**flows**), aggregates them and sends information about these flows to PRTG using UDP packets. When sampling is used (mandatory for sFlow) only information about every n-th packet is sent to PRTG which reduces CPU load a lot. Because the switch already performs a pre-aggregation of traffic data, the flow of data to PRTG is much smaller than the monitored traffic. This makes xFlow the ideal option for high traffic networks that need to differentiate the bandwidth usage by network protocol and/or IP addresses.

NetFlow and IPFIX Monitoring

The NetFlow (and IPFIX) protocol is mainly used by Cisco devices. Once configured, the router sends for each data flow a NetFlow or IPFIX packet to the monitoring system running on a PRTG probe. There the data can be filtered and evaluated. There are different NetFlow and IPFIX sensors available: The basic ones offer predefined channel definitions, the custom variants enable you to define your own channels.

The advantage of using NetFlow or IPFIX:

- Generates little CPU load on the router itself (according to Cisco 10,000 active flows create about 7% additional CPU load; 45,000 active flows account for about 20% additional CPU load).
- Generates less CPU load on the PRTG core system, compared to packet sniffer sensors.

Note: You must enable NetFlow or IPFIX export on the device you want to monitor. The device must send a flow data stream to the IP address of the PRTG probe system on which the NetFlow or IPFIX sensor is set up. Juniper **jFlow** monitoring is reported to work as well, using NetFlow v5 sensors.

sFlow Monitoring

sFlow works similar to NetFlow monitoring. The router sends data flow packets to the monitoring system running on a PRTG probe. The most obvious difference between the two flow protocols: With sFlow, not all of the traffic is analysed, but only every n-th packet. It is like having a river of traffic and you take a cup of water out of it ever so often and analyze it.

The advantage is clear: There is less data to analyze, there is less CPU load needed and less monitoring traffic is generated. Yet you can get a good insight into your network's bandwidth usage. **Note:** Currently, PRTG supports sFlow version 5.

Set Up Flow Sensors

Find details on how to set up the different flow sensors in the following sections:

- [NetFlow V5 Sensor](#)  682
- [NetFlow V5 \(Custom\) Sensor](#)  690
- [NetFlow V9 Sensor](#)  698
- [NetFlow V9 \(Custom\) Sensor](#)  706
- [IPFIX Sensor](#)  630
- [IPFIX \(Custom\) Sensor](#)  638
- [sFlow Sensor](#)  852
- [sFlow \(Custom\) Sensor](#)  860
- [jFlow V5 Sensor](#)  646
- [jFlow V5 \(Custom\) Sensor](#)  654

Limitations

On a powerful 2008 PC (Dual Core, 2.5 Ghz), you can process about 100,000 flows per second for one xFlow stream. Using sampling the number of actual flows can be much higher. When using complex filters, the value can be much lower. For example, with a router sending about 2,000 flows/second (which corresponds to mixed traffic at gigabit/sec level without sampling) you can expect to configure up to 50 NetFlow sensors operating properly. PRTG internally monitors its own NetFlow processing, and you will see a decreased values in the **Core/Probe Health** sensor's **Health** channel as soon as NetFlow packets are not processed due to an overload (you find this sensor on the Local Probe device).

If you experience an overload please consider using sampling or setting up multiple probes and distribute the NetFlow streams to them. We do not recommend adding more than 400 NetFlow sensors per PRTG probe.

This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

More

Knowledge Base: Can I add custom channels to standard Packet Sniffer and NetFlow sensors?

- <http://www.paessler.com/knowledgebase/en/topic/2143>

Knowledge Base: What filter rules can be used for custom Packet Sniffing or xFlow (NetFlow/sFlow) sensors?

- <http://www.paessler.com/knowledgebase/en/topic/483>

Knowledge Base: How do the channel definitions for custom Packet Sniffing or xFlow (NetFlow/sFlow) sensors work?

- <http://www.paessler.com/knowledgebase/en/topic/473>

Knowledge Base: Does my Cisco device (Router/Switch) support NetFlow Export?

- <http://www.paessler.com/knowledgebase/en/topic/5333>

Knowledge Base: Do you have any configuration tips for Cisco routers and PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/563>

Knowledge Base: Is it possible to monitor Cisco ASA Firewalls using Netflow 9 and PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/633>

Knowledge Base: How to monitor Cisco ASA Firewalls using NetFlow 9 and PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/1423>

Tools: NetFlow Generator and NetFlow Tester

- <http://www.paessler.com/tools/>

10.6 Bandwidth Monitoring Comparison

The following table shows the differences between PRTG's four methods available for bandwidth monitoring:

	WMI	SNMP	Packet Sniffer	xFlow (IPFIX, Netflow, sFlow, jFlow)
Setup	Medium	Easy	Easy to Complex (depending on filter rules used)	Can be complex (e.g. the switch must be configured)
Traffic can be filtered	No	No	Yes	Yes
Differentiate bandwidth usage by protocol or IPs	No	No	Yes	Yes
PRTG can show Toplists (Top Talker, Top Connections, Top Protocols etc.)	No	No	Yes	Yes
Filter bandwidth usage by IP	No	No	Yes	Yes
Filter bandwidth usage by MAC address	No	No	Yes	No
Filter bandwidth usage by physical network port	Yes	Yes	No	No

Part 10: Sensor Technologies | 6 Bandwidth Monitoring Comparison

	WMI	SNMP	Packet Sniffer	xFlow (IPFIX, Netflow, sFlow, jFlow)
Monitor network parameters other than bandwidth usage	Yes	Yes	No	No
CPU load on the machine running PRTG	Low	Low	Higher, depends on the amount of traffic	Higher, depends on the amount of traffic
Excess bandwidth usage of monitoring	Small	Small	None (except when monitoring switch ports are used)	Depends on the traffic

More

Knowledge Base: Should I use SNMP, xFlow (IPFIX/NetFlow/sFlow) or Packet Sniffing for my monitoring?

- <http://www.paessler.com/knowledgebase/en/topic/923>

Knowledge Base: How do I discern excessive bandwidth usage with PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/2923>

10.7 Monitoring Quality of Service and VoIP

PRTG can monitor the Quality of Service in a network with dedicated QoS sensors, as well as Cisco IP Service Level Agreement (SLA) and Cisco Class Based Quality of Service (CBQoS). Slight variations of network parameters like jitter, packet loss, or packet delay variation (PDV) usually have only little effect on TCP based services (e.g. HTTP, SMTP, etc.). But for UDP based services like Voice over IP (VoIP) and video streaming a steady stream of data packets is crucial. The sound quality of a VoIP call drops dramatically when UDP packets are not received in a timely fashion, or if packets are lost or out-of-order. As a rule of thumb for good quality of service (in a VoIP perspective) you would want low measurements for jitter (less than 20 to 50 ms) and PDV (less than 100 ms) and preferably **zero** measurements for packet loss, duplicated packets, or packets in wrong order.

For Quality of Service measurements, three sensors are available:

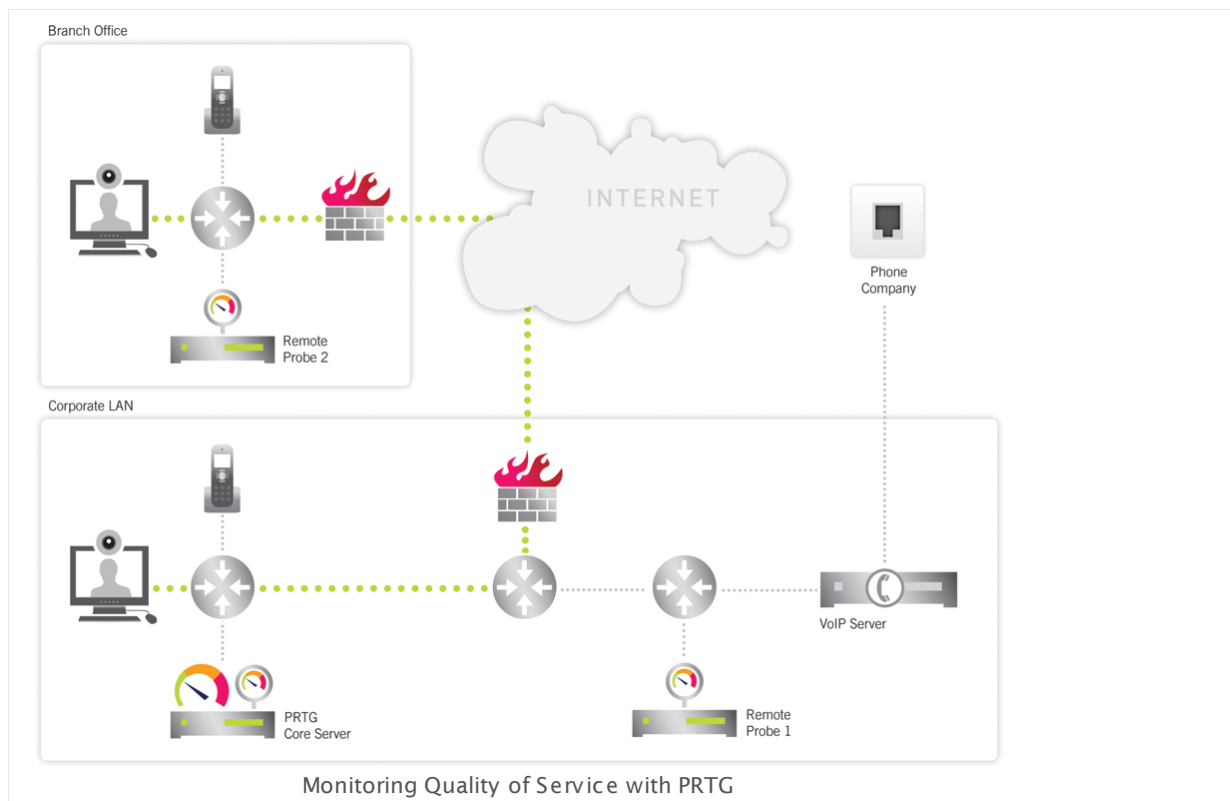
- [QoS \(Quality of Service\) Sensor](#)^[801]
Monitors VoIP relevant network parameters by testing network connection quality between two probes.
- [QoS \(Quality of Service\) Round Trip Sensor](#)^[807]
Monitors VoIP relevant network parameters by testing network connection quality between two probes. Traffic is measured bidirectional.
- [Cisco IP SLA Sensor](#)^[336]
Monitors VoIP relevant network parameters through IP SLA results from Cisco devices (via SNMP).
- [SNMP Cisco CBQoS Sensor](#)^[934]
Monitors VoIP relevant network parameters by using Cisco's CBQoS (via SNMP).

QoS (Quality of Service) Sensor

The QoS Sensor is used to monitor the quality of a network connection by measuring the following parameters:

- Jitter in ms according to RFC 3550
- Packet delay variation (PDV) in ms according to RFC 3393
- Lost packets in %
- Out-of-order packets in %
- Duplicated packets in %

The measurements are taken by sending UDP packets between two probes. This means that you can test any network connection in your network by simply placing a [remote probe](#)^[2011] on (or near) each 'end' of the connection and measuring the connection quality between them. This is the perfect tool to find network issues that can affect VoIP sound quality or video streaming 'hiccups'.



As mentioned before, measurements are taken between two probes. So the first step is to place two PCs running a remote probe on (or near) both ends of the connection that you want to monitor. As an alternative, the local probe on the PC running the PRTG core can also be used as one end. If any firewalls, packet filters or Network Address Translation (NAT) systems are en route, you must configure them as necessary so that the UDP packets can reach the target probe.

In PRTG, create a new QoS sensor on a **Probe Device**. Please find details about settings in the [QoS \(Quality of Service\) Sensor](#)^[801] section. With the settings for number and for size of the packets you can configure the test data stream. 1,000 packets of 172 bytes each is a good start, but if your applications use larger packets you may want to enter other values here. Try to configure the test streams with parameters similar to that of the UDP services you are using across this connection.

Cisco IP SLA Sensor

Wikipedia describes IP SLA as **a feature included in the Cisco IOS Software that can allow administrators the ability to Analyze IP Service Levels for IP applications and services. IP SLA uses active traffic-monitoring technology to monitor continuous traffic on the network. This is a reliable method in measuring over head network performance.** IP-SLA is mostly used to monitor the sound quality of VoIP traffic.

If you haven't done so already, please add a device in PRTG for the Cisco device that you want to monitor. Then create a new **Cisco IP SLA** sensor on this device. Please find details about settings in the [Cisco IP SLA Sensor](#)^[336] section.

This feature is only available in the more expensive Cisco devices. If you don't have IP SLA capable routers/switches you can still get similar information with PRTG's QoS sensor (see [above](#)¹⁹³⁹) which does not require any special hardware—just two PCs running Windows. If you do own hardware which supports IP SLA then PRTG brings you probably the least-cost monitoring solution for IP SLA. Most vendors charge extra for IP SLA support (a thousand bucks and more). Following Paessler's long term policy we simply include this as one of our sensor types. With PRTG you can even use the Freeware Edition to monitor IP SLA!

PRTG monitors the following parameters: Calculated Planning Impairment Factor (ICPIF), Mean Opinion Score (MOS), Average Jitter, Packets Lost, Packets Out Of Sequence, Packets Late, Average Round Trip Time (RTT), DNS RTT, TCP RTT, Transaction RTT. Especially two of these parameters are interesting for VoIP: Mean Opinion Score (MOS) and Calculated Planning Impairment Factor (ICPIF).

SNMP Cisco CBQoS Sensor

Cisco Class Based Quality of Service (CBQoS) provides information about QoS of Cisco network devices which support the **Modular QoS command line interface (MQC)**. With Class Based QoS, you can obtain monitoring data that includes summary counts and rates by traffic class before and after the enforcement of QoS policies, according to Cisco's CBQoS Management Information Base (MIB) definition. PRTG determines CBQoS data via Simple Network Management Protocol (SNMP). The corresponding sensor type is available out-of-the-box in PRTG version 13.x.5 or later. CBQoS is available in Cisco IOS by default as of version 12.4(4)T.

In order to monitor CBQoS, add a device to PRTG for the Cisco device that you want to monitor. Then create a new **SNMP Cisco CBQoS sensor** on this device. Please see section [SNMP Cisco CBQoS Sensor](#)⁹³⁴ for more details.

This sensor type supports the following CBQoS classes:

- **Class Map:** statistical data about class maps, such as pre- and post-policy packets and sizes, drop packets and size, as well as no-buffer drop packets
- **Match Statement:** statistical data about match statement specific information, such as pre-policy packets and size
- **Queueing:** statistical data about queuing actions, such as current and maximum queue depth, drop packets, and drop size

You can select the desired CBQoS entries which you want to monitor while creating the sensor in PRTG. The available entries are given with their particular connections, their descriptions, and class types.

Voice over IP

For Mean Opinion Score (MOS) measurements, Cisco conducted a panel test where a wide range of listeners judged the quality of voice samples sent using particular codecs, on a scale of 1 (poor quality) to 5 (excellent quality). The Cisco device calculated the corresponding value for the current network connection based on the network parameter measurements like jitter and packet loss. The values and their meanings are:

MOS	Quality	Expected Quality Impairment
5	Excellent	Imperceptible
4	Good	Perceptible, but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

The second interesting parameter ICPIF is the sum of measured impairment factors minus a user-defined access Advantage Factor that is intended to represent the user's expectations, based on how the call was placed (for example, a mobile call versus a land-line call) (quoted from Cisco's website).

Upper Limit for ICPIF	VoIP Call Communication Quality
5	Very good
10	Good
20	Adequate
30	Limiting case
45	Exceptional limiting case
55	Customers likely to react strongly (complaints, change of network operator)

More

Paessler Knowledge Base: Where can I find more information about Cisco IP SLAs, VoIP, and QoS?

- <http://www.paessler.com/knowledgebase/en/topic/11093>

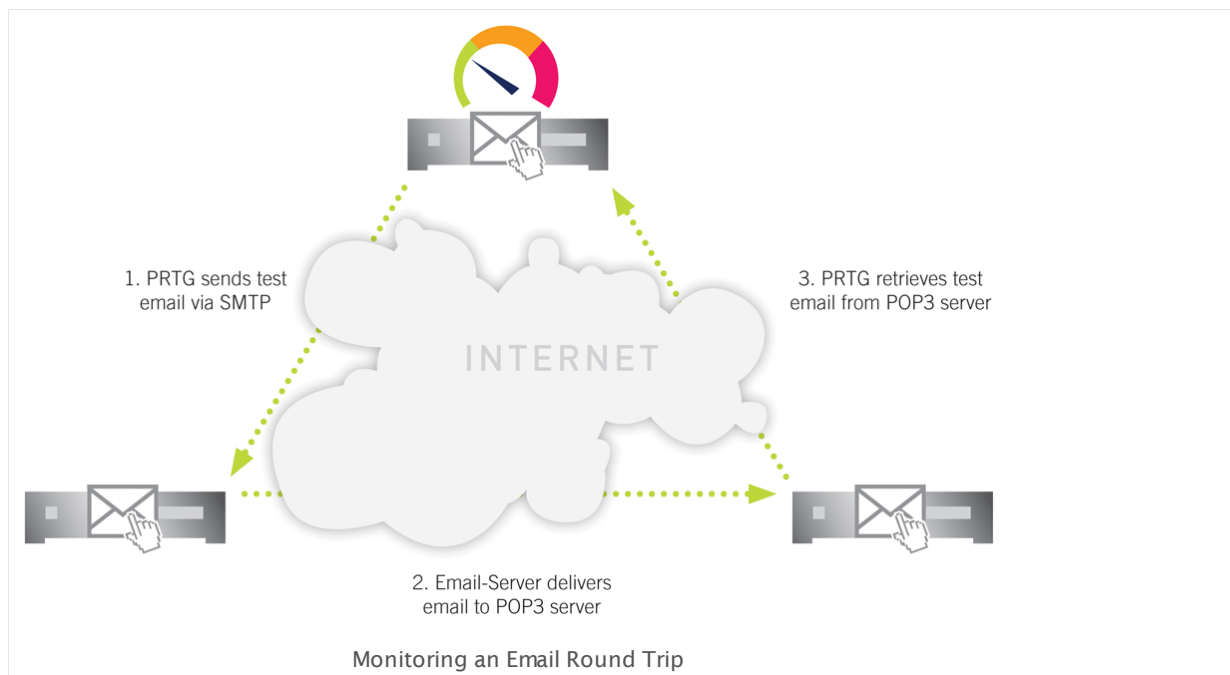
10.8 Monitoring Email Round Trip

Email Round Trip sensors ensure the end-to-end delivery of emails and make it possible to monitor availability and performance of a complete email delivery process. There are two sensor types for this task:

- [SMTP&POP3 Round Trip Sensor](#) 900
- [SMTP&IMAP Round Trip Sensor](#) 892

Both initially deliver an email to a mail server using SMTP. Afterwards the receiving mailbox is scanned using Post Office Protocol version 3 (POP3) or Internet Message Access Protocol (IMAP) until the email arrives. The test email contains a unique code in the topic which is used to identify the email, such as **PRTG Roundtrip Mail: {6D136420-5A3E-46CF-871A-1DAF0C4F3D5D}**.

When PRTG successfully received an email in this email round trip cycle, it marks the respective message for deletion on the mail server. Usually, a mail server will then delete this email. For best performance, we recommend using a dedicated email accounts for email round trip sensors.



In the scenario shown above, there are three steps in the round trip:

- **Step 1**
PRTG delivers an email via the SMTP protocol to a mail server (just like an email client).
- **Step 2**
The SMTP server delivers the email to a POP3/IMAP server (which can be located at a remote site, in your local LAN or on the same server as well).

- **Step 3**

Every few seconds PRTG connects to the POP3/IMAP server until the test email arrives.

Recommended Configuration

Here is a simple concept to check delivery of email out of and into your organization:

1. Create a dedicated email account for this test in your mail system.
2. Set up an external email account (hosted mail server, free mail service, etc.) and configure it to send all emails back to this dedicated email account in your organization (which you created in [Step 1](#)).
3. Set up PRTG's round trip sensor to send an email to the external email account (which you created in [Step 2](#)) using your LAN's mail server and then check for the email account on your mail system (which you created in [Step 1](#)) for arrival of the email.

With this technique you are testing multiple aspects of your email server setup. As long as the sensor shows a green light, this means:

- Your email server accepts emails via SMTP.
- Emails are being sent to the outside world (internet connection works, MX lookups work etc.).
- Emails from external mail server can be delivered into your mail system (this includes aspects like the fact that the MX records for your domain are correct, your mail server can be reached from the outside world, your email filtering is working etc.).
- Emails can be retrieved using POP3 (or IMAP).

Note: Please use dedicated email accounts with this sensor type. If you use more sensors of this type, please make sure that each sensor uses its own email accounts.

Conclusion

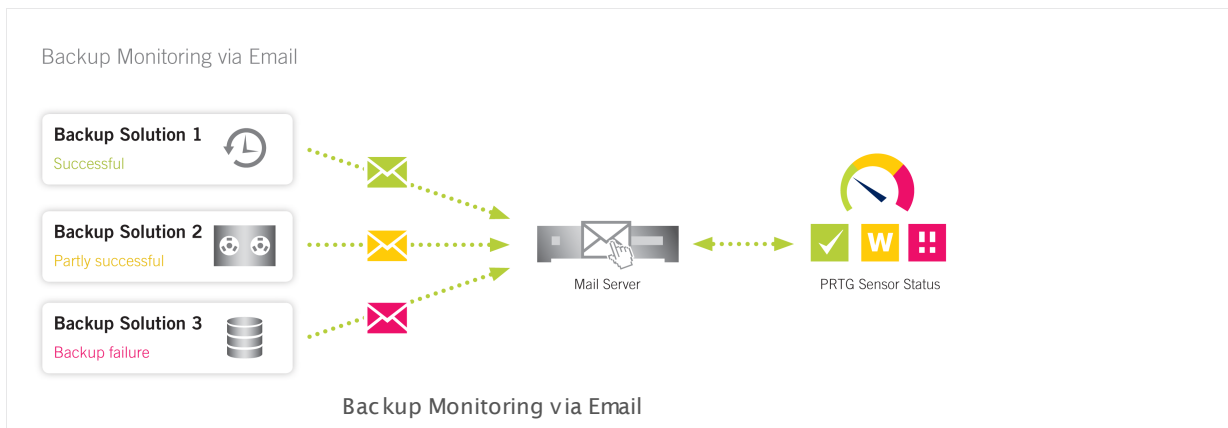
These two sensor types are a great tool to ensure delivery of email from and to your mail servers. Compared to the standard SMTP, POP3 and IMAP sensors - which only check the availability of these services - the two roundtrip sensor types actually monitor the complete transaction from accepting the mail on the first email server to delivery of the mail on the final POP3/IMAP server.

10.9 Monitoring Backups

Monitoring your backup software enables you to be sure that your recent backups succeeded. With PRTG you can check the email notifications of various backup jobs. You only need two things for backup monitoring:

1. Configure your backup software to send emails to a dedicated email account, and
2. configure PRTG's [IMAP Sensor](#)⁶⁰⁷ for backup monitoring.

PRTG will analyze the backup emails for you and set the status of the IMAP sensor accordingly. This way you will see the states of all your backup jobs at a glance.



Setting up Backup Monitoring

Please refer to our Knowledge Base for a step-by-step tutorial to monitor your backup jobs:

Monitoring Backup Solutions via Email

- <http://www.paessler.com/knowledgebase/en/topic/47023>

10.10 Monitoring Virtual Environments

A highly flexible IT infrastructure is a common need nowadays and virtualization has become an important pillar of the IT all over the world. Applications in your network might be distributed over many different servers, networks and locations. They might also be in the cloud, and your computations can take place in data centers spread over the whole world. So, if your network connection or any other corresponding hardware fails, hundreds of applications might be unavailable—an impact to your daily business processes which should be avoided at any costs.

Because of this, monitoring the physical infrastructure of your data center is still a must in times of virtual environments. With the layer of virtualization in addition to your physical equipment, your logical infrastructure needs also a close treatment. PRTG assists you to deal with these advanced requirements and enables you to react proactively to issues before they affect your whole system. With PRTG you can monitor all layers of your IT infrastructure in a comprehensible way so you will reduce issues related to dynamic IT environments significantly.

Monitoring All Layers of Your IT Infrastructure

In general, you can assume that with the layer of virtualization you have to monitor a total of four layers in your IT infrastructure:

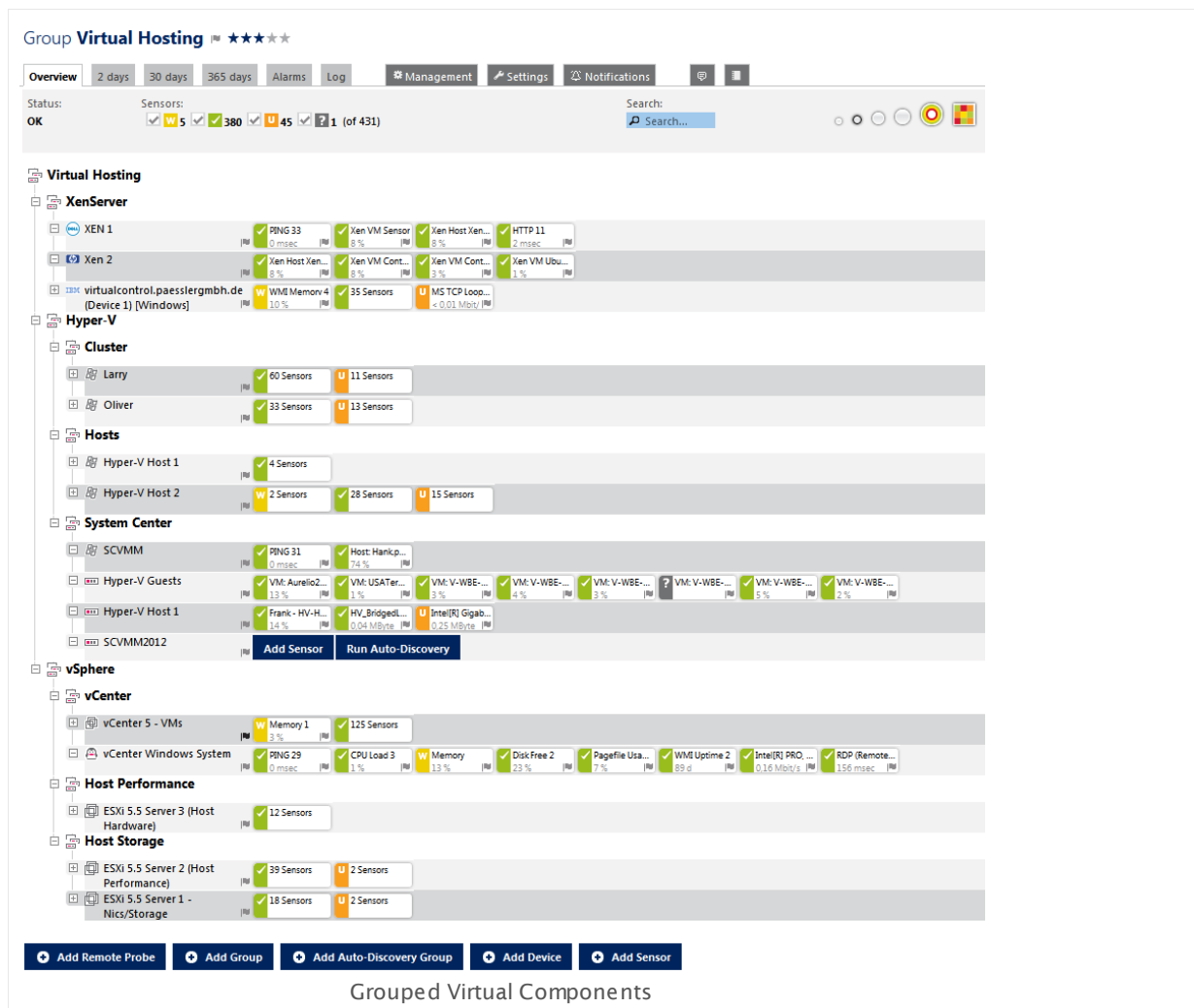
- **Hardware (Server Racks):** Usually you will set up your monitoring in the common way and monitor most of the hardware components in your network with [PRTG's SNMP sensors](#)²⁹³. You are able to gain monitoring data about many different device readings such as CPU load, memory, disk space, etc. with [this monitoring technology](#)¹⁹²³, as well as information about network traffic and bandwidth usage of your routers and switches. It is absolutely mandatory for a working IT environment to monitor all hardware components in order to be alerted if something fails or hardware resources are running out. In addition, you can identify potential bottlenecks affecting your virtualized infrastructure. You can set this monitoring up in usual way.
- **Host Server Hardware:** It is essential to monitor the host hardware of your virtualization solution explicitly. If you have issues with your virtual machines (VMs), the origin might be a host hardware failure. You should closely monitor your VM host servers to get alerted if the status is other than "normal". Besides the out of the box hardware sensors, PRTG provides specific sensors for various virtualization host servers; the following monitoring data of your host servers will help you prevent issues in virtualized environments:
 - VMware: current reading and health status (via WBEM), a general status as shown in vSphere (via SOAP), and disk space on ESX(i) (via SSH)
 - Hyper-V: host health critical values, deposited pages, network traffic, CPU usage of guests, hypervisor, and in total
 - Citrix XenServer: CPU, memory, and network usage, the number of running virtual machines on the host server, and load average
 - SCVMM: CPU usage, free memory (in bytes and percent), overall status, communication status, cluster node status, virtual server status, computer status, and the number of VMs

- **VMs from the "Out side":** The virtual machines run on their particular host servers. PRTG can show you the status of single virtual machines and several of their performance counters. It might be helpful to know which resources a single VM uses and needs, but monitoring single VMs is not advisable in every case because it has noticeable influence on the overall performance. Often it will be sufficient to monitor only VMs which are critical for your network. If a VM reaches its capacity limits, PRTG can alert you and you can conduct according resolution steps like enhancing this VM's resources. Indicators for a healthy virtual machine which you can monitor with PRTG out of the box are:
 - VMware: CPU and memory usage, disk read and write speed, read and write latency, and network usage
 - Hyper-V: CPU usage, disk read and write speed
 - Citrix XenServer: CPU usage and free memory
 - SCVMM: CPU usage, disk read and write speed, and the status of the VM
 - Virtuozzo: disk space and network usage
- **VMs from the "Inside" (Operating Systems):** You can monitor the Windows operating system of a single VM with PRTG's standard [WMI sensors](#)^[294], for example. [With this technology](#)^[1927] you can access data of various Windows parameters. Other operating systems like Linux/macOS can make data available via [SSH](#)^[1930] and [SNMP](#)^[1923]. The status of the operating systems on your VMs can indicate potential issues of the same, just like the operating systems on your physical machines which are important for a reliably working IT infrastructure: You can monitor these with the same attention, depending on your application scenario, but be careful due to performance considerations. Especially many WMI sensors can result in load problems, so monitor only really important systems "from the inside". Furthermore, you do not need to monitor every item multiple times. For example, it might be sufficient to monitor free disk space only from the outside of the actual VM.

Monitoring the Virtual Infrastructure

In order to monitor your IT infrastructure, best practice is to set up the monitoring of the hardware layer of your data center first in PRTG, especially in order to find potential bottlenecks which might have an impact on your virtual servers. Then you can start monitoring your virtual environment itself. If you use several solutions for virtual hosting, it is also a good idea to group related host servers, their virtual machines, and the operating systems together. The screenshot below will give you an idea about how to organize this.

Part 10: Sensor Technologies | 10 Monitoring Virtual Environments



The screenshot above shows you the particular group "Virtual Hosting" of an entire PRTG setup. This is an example how monitoring of virtual environments can look like. The sample group contains several subgroups for the virtualization solutions Citrix "XenServer", Microsoft "Hyper-V", and VMware "vSphere". The vSphere group, for example, has three subgroups: we monitor the vCenter VMs and the vCenter Windows system, the performance of the host server, and the storage system of the host.

Devices for Physical Hosts

In PRTG, set up devices which represent the physical hosts of your virtual machines. For example, for your VMware hosts, add devices which represent the ESX/ESXi servers, for Hyper-V add devices which represent your Hyper-V host servers, for Citrix add devices which represent your Xen servers. If you manage these hosts with a Microsoft System Center Virtual Machine Manager (SCVMM), you can also (or alternatively) add a device for the SCVMM.

Then you can add suitable and expressive sensors to the host server devices. Running PRTG's [auto-discovery](#)¹⁹⁰, many useful sensors will be created automatically. There are several pre-configured host hardware sensors available out of the box in PRTG:

- [VMware Host Hardware \(WBEM\) Sensor](#)^[1375]: monitors an ESX(i) server via Web-Based Enterprise Management (WBEM)
- [VMware Host Hardware Status \(SOAP\) Sensor](#)^[1381]: monitors a VMware host server via Simple Object Access Protocol (SOAP)
- [VMware Host Performance \(SOAP\) Sensor](#)^[1387]: monitors a VMware host server via Simple Object Access Protocol (SOAP)
- [Hyper-V Host Sensor](#)^[579]: monitors via Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device
- [Citrix XenServer Host Sensor](#)^[342]: monitors via Hypertext Transfer Protocol (HTTP)
- [SCVMM Host Sensor](#)^[823]: monitors, for example, a Hyper-V host, a VMware host, or a XenServer host which is managed by a System Center Virtual Machine Manager (SCVMM)

These sensor types monitor hardware specific counters to ensure that no hardware issues affect your actual virtual machines. Additional sensor types can monitor the host hardware via SNMP (for example, traffic and custom requests) and SSH (for example, disk space of VMware ESX(i) servers), as well as there are sensors for network adapters and storage devices which are connected to a Hyper-V host server. You can also monitor Virtuozzo host servers with sensors for network usage and disk space for each container.

Devices for Virtual Machines

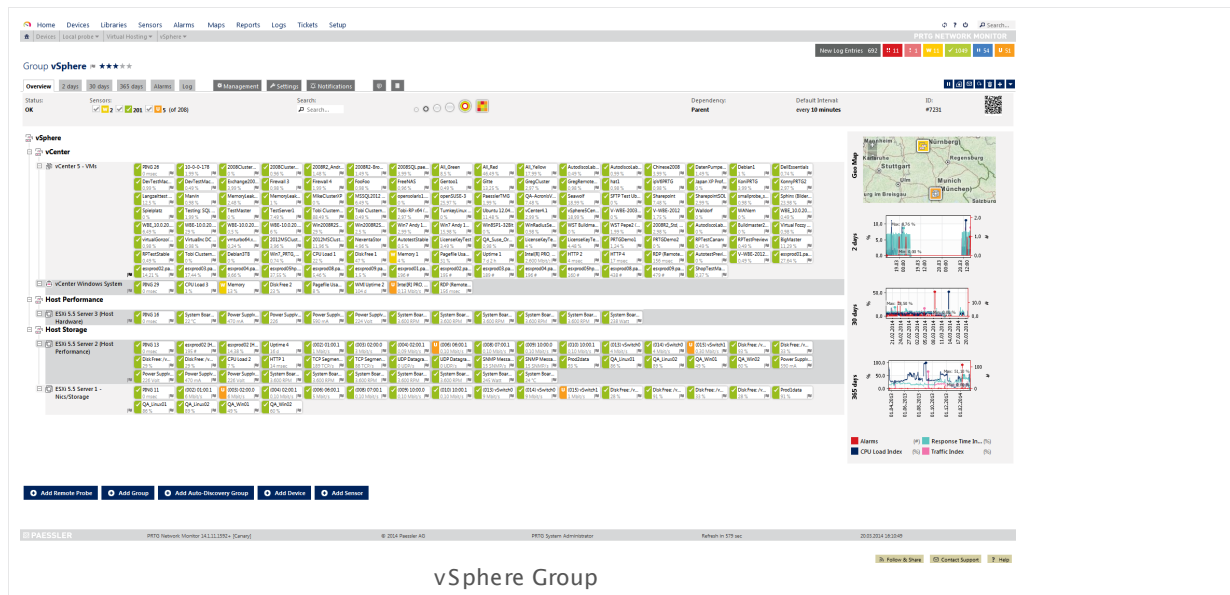
In order to monitor your actual virtual machines, add them to your host servers in PRTG. For a better overview, you might want to add another device to PRTG which represents your host server and add sensors for your VM to there. The according sensors for virtual machines will show you the performance of single VMs as well as their usage of resources. This will help you identify VMs with poor performance and react proactively before one or more VMs crash. As mentioned above, you can additionally monitor your particular VMs from the inside (i.e., the operating systems on your VMs) if necessary. See the sections below for details about particular virtualization solutions.

VMware Virtual Machine

PRTG's [VMware Virtual Machine \(SOAP\) Sensor](#)^[1393] monitors VMs on a VMware host server via Simple Object Access Protocol (SOAP). With the VMware system, the general idea is to add a **vCenter** server as a device to PRTG and use the vCenter as parent device where you add the sensors to for your virtual machines. So, in the case of **vMotion** when your VMs change their host server, PRTG will be able to follow these movements and will never lose the monitored VMs.

For this sensor type, you need the **Microsoft .NET Framework** with the latest update of version 4.0 running on the probe machine. If you use many VMware sensors, we also recommend adjusting the settings on your VMware host server to accept more incoming connections.

Part 10: Sensor Technologies | 10 Monitoring Virtual Environments

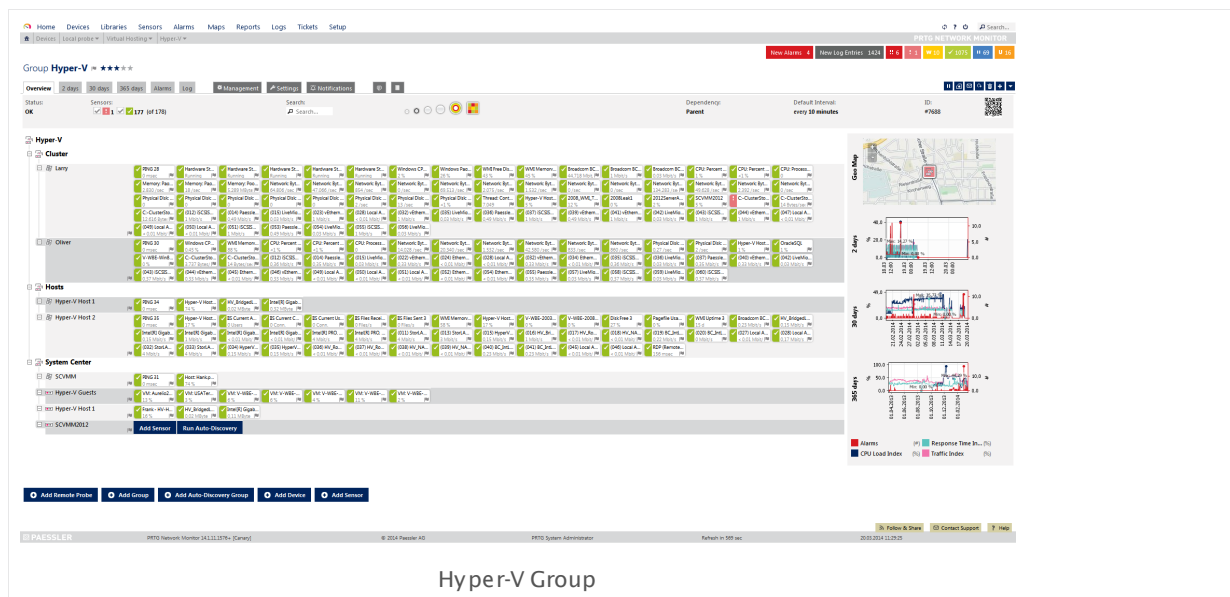


This screenshot shows a sample vSphere group in PRTG. As recommended, the VMware virtual machines are added to the vCenter device. There is also a dedicated device for the vCenter Windows operating system with common WMI sensors for CPU, memory, disk, and network usage. The ESXi host servers are organized in their own groups regarding performance and storage. In this example, PRTG monitors the hosts with the standard SNMP hardware sensors as well as with the specific VMware ESXi host sensors.

Microsoft Hyper-V Virtual Machine

PRTG's [Hyper-V Virtual Machine Sensor](#)^[585] monitors VMs via Windows Performance Counters or Windows Management Instrumentation (WMI), as configured in the "Windows Compatibility Options" of the parent device. With this hybrid approach, the sensor first tries to query data via performance counters and uses WMI as a fallback if there are no performance counters available. Performance counters in general need less system resources than WMI. We recommend using System Center Virtual Machine Manager (SCVMM) as parent device for this sensor type, because when your VMs change their physical host with **Live Migration**, this sensor will still be able to continue monitoring. You should also disable User Account Control (UAC) in the Windows operating system of the VM.

Part 10: Sensor Technologies | 10 Monitoring Virtual Environments



This screenshot shows a sample Hyper-V group in PRTG. There is a dedicated group for failover clustering where two nodes are monitored with several SNMP and WMI sensors, as well as [Hyper-V Host Server sensors](#)^[579] and sensors for the Hyper-V virtual machines. This ensures that Hyper-V and failover clustering works without any issues. The Hyper-V hosts are monitored the same way, organized in a dedicated group for hosts.

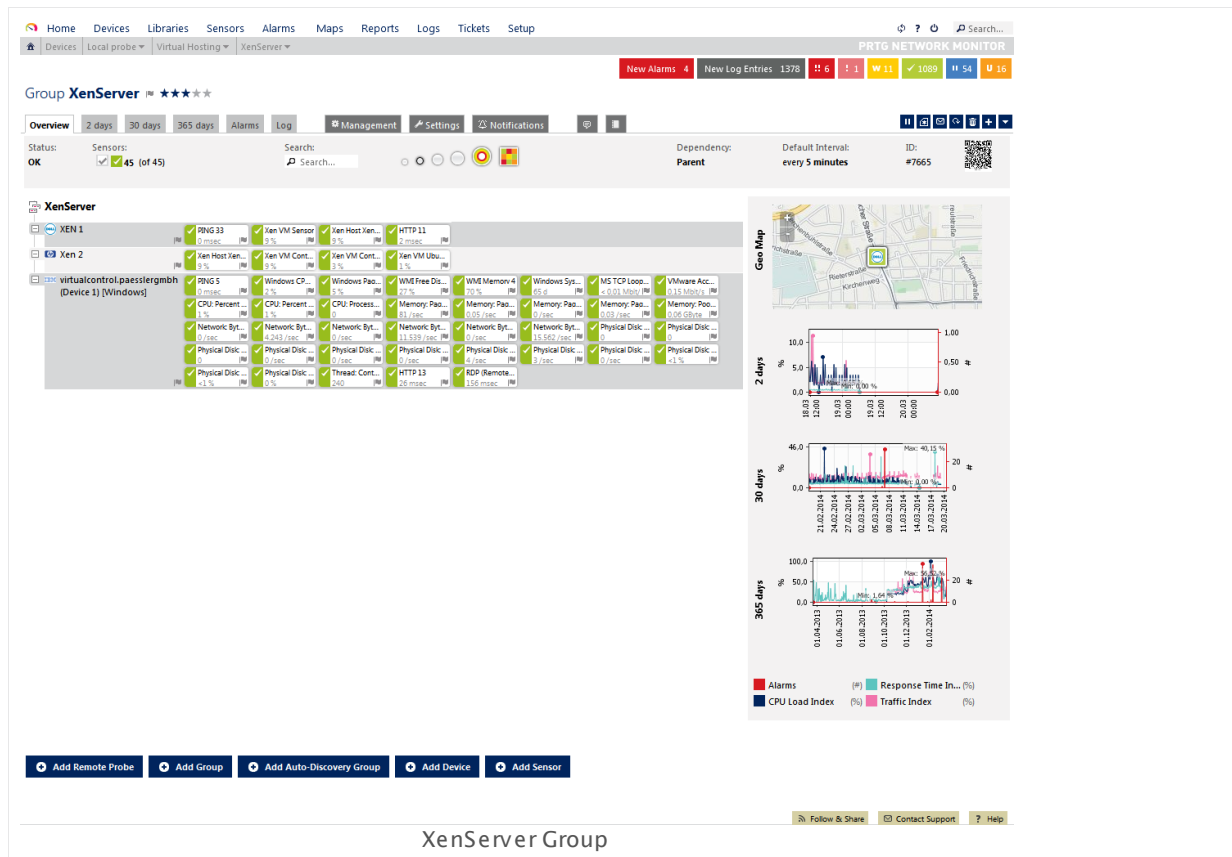
Note that we recommend adding the particular virtual machines to the SCVMM server if possible! We pointed out above that you should add the VMs to an SCVMM server to avoid issues with Live Migration. You can see this in the group "System Center". The particular VMs are added to the dedicated device "Hyper-V Guests". The SCVMM itself is monitored as described below.

Citrix XenServer Virtual Machine

PRTG's [Citrix XenServer Virtual Machine Sensor](#)^[348] monitors VMs via Hypertext Transfer Protocol (HTTP). For this sensor type, you have to add a device to PRTG which represents a Citrix XenServer with version 5.0 or later. Another requirement is the **Microsoft .NET Framework**: You have to run the latest update of version 4.0 on the probe machine where you add this sensor to.

In a XenServer pool, every host knows each running VM. Because of this, there is no central instance which provides all available data so it does not matter on which host you query your VMs. All queries on any host are automatically forwarded to the pool master which manages the XenServer pool. So it is sufficient to create the desired sensors for your XenServer VMs on a device that represents one host server of your pool. PRTG's XenServer sensors can figure out by themselves which host is running and retrieve the according data.

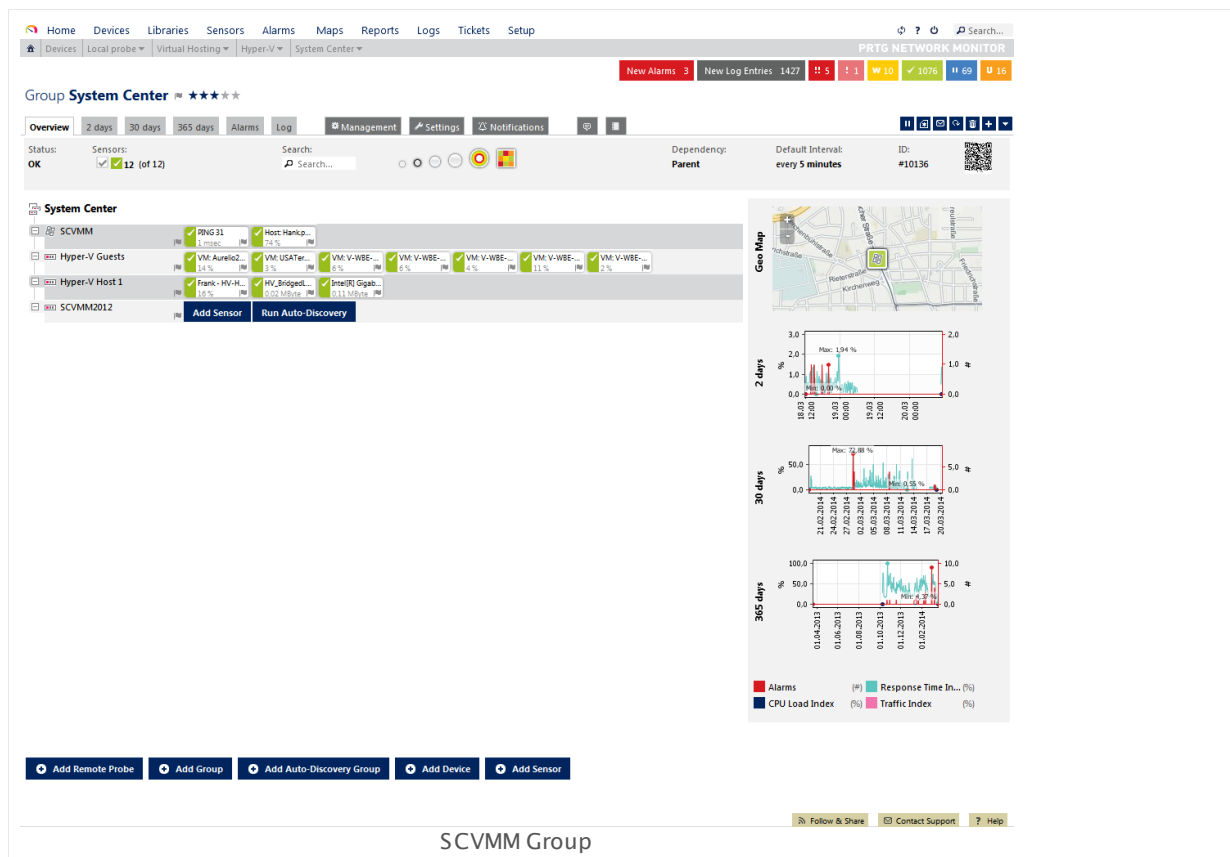
Part 10: Sensor Technologies | 10 Monitoring Virtual Environments



This screenshot shows a sample XenServer group in PRTG. There are two devices for XenServer hosts (Xen 1 and Xen 2), each with a [Citrix XenServer Host sensor](#)^[342] and several [Citrix XenServer Virtual Machine sensors](#)^[348] for the particular VMs on this host. Furthermore, the Windows operating system is represented as a dedicated device ("virtualcontrol") which is monitored with several WMI sensors regarding CPU, disk, memory, and network usage.

Microsoft SCVMM Virtual Machine

With the [SCVMM Virtual Machine Sensor](#)^[830] you can monitor VMs which are managed by a System Center Virtual Machine Manager (SCVMM), for example, Hyper-V or VMware. Requirements for this sensor type to work are the [Microsoft .NET Framework](#) with version 4.0 and the latest update, [Remote PowerShell 2.0](#), and the [VMM PowerShell Plugin](#). If you add your SCVMM server to PRTG, PRTG will be able to follow movements of your VMs automatically.



This screenshot shows a group for an SCVMM server in PRTG which manages Hyper-V virtual machines. The SCVMM server is monitored with the [SCVMM Host sensor](#)^[823] which shows several kinds of server states and usage parameters. Several virtual machines are added to the "Hyper-V Guests" device (as SCVMM Virtual Machine sensors) so that PRTG can automatically detect changed VM host devices.

The sensor types described in this section monitor virtual machine specific counters in order to ensure that all your VMs have enough resources available. If a VM is overloaded, PRTG can notify you immediately and you can proactively take care of issues before a particular VM has an outage or other failures. Additionally, we have shown an idea for a structured virtual monitoring with several recommendations.

You can find all available sensors for virtual servers and the according virtual machines in section [List of Available Sensor Types—Virtual Servers Sensors](#)^[296].

More

Knowledge Base: I run PRTG on VMware. How can I obtain best performance?

- <http://www.paessler.com/knowledgebase/en/topic/49193>

Paessler Blog: Virtualization and Network Monitoring

- <http://www.paessler.com/blog/2013/04/30/prtg/virtualization-and-network-monitoring>

Paessler Blog: Virtualization and Network Monitoring: PRTG Supports the new VMware ESXi 5.5!

- <http://www.paessler.com/blog/2013/10/01/prtg/virtualization-and-network-monitoring-prtg-supports-the-new-vmware-esxi>

Sensor Technologies—Topics

- [Monitoring via SNMP](#)  1923
- [Monitoring via WMI](#)  1927
- [Monitoring via SSH](#)  1930
- [Monitoring Bandwidth via Packet Sniffing](#)  1932
- [Monitoring Bandwidth via Flows](#)  1934
- [Bandwidth Monitoring Comparison](#)  1937
- [Monitoring Quality of Service](#)  1939
- [Monitoring Email Round Trip](#)  1943
- [Monitoring Backups](#)  1945
- [Monitoring Virtual Environments](#)  1946
- [Monitoring Databases](#)  1956

10.11 Monitoring Databases

Monitoring your databases enables you to ensure that, on the one hand, database queries are processed in time, and, on the other hand, that the database itself performs within the defined parameters. Furthermore, database monitoring with PRTG makes it possible to be alerted via a corresponding sensor status if database queries return an unexpected result value.

PRTG comes with built-in native sensors for the most common databases:

- Microsoft SQL servers
- MySQL servers
- Oracle SQL servers

However, it is possible to monitor many other database servers. For this concern, PRTG uses the ActiveX Data Objects (ADO) interface in combination with the PowerShell scripting language.

There are two types of database sensors:

- [Sensors monitoring databases directly](#)^[1995]: They monitor from the user perspective, sending a request to the database server and receiving values. These values can optionally be compared to the expected values to ensure they match.
- [Sensors monitoring database performance](#)^[1996]: They have a more abstract view on database servers and monitor performance counters via Windows Management Instrumentation (WMI).

Sensors Monitoring Databases Directly

PRTG provides several sensors which can "look into" the content of databases. Sensors of this type connect to the database server and show the response time. In addition, these sensors can read out the number of records and a value, depending on an SQL query.

The following sensors are available for this kind of monitoring:

- [Microsoft SQL Sensor](#)^[667]: can monitor Microsoft SQL servers (MSDE, SQL Server 7, 2000, 2005, 2008, and 2012).
- [MySQL Sensor](#)^[675]: can monitor MySQL servers (3.23, 4.0, 4.1, 5.0, and 5.1)
- [Oracle SQL Sensor](#)^[714]: can monitor Oracle SQL servers (7.3, 8.0, 8i, 9i, 10g, and 11g). **Note:** You have to provide all necessary information manually, in contrast to the other SQL sensors listed above.
- [ADO SQL Sensor](#)^[315]: can monitor almost all available database servers, as well as data files via an ActiveX Data Objects (ADO) connection and a PowerShell script.

For these sensors you can define a valid SQL statement that will be sent to the database server. With every scanning interval, the sensor will execute the query against the database and a corresponding value will be returned. You can indicate in the sensor settings whether you want to post-process this result and specify the intended sensor behavior for the received value ("Warning" status, "Down" status).

Sensors Monitoring Database Performance

Performance sensors for database servers have a more "abstract" view on databases and regard performance "from the outside". They do not read out any values of the database, neither do they send SQL queries to databases. This sensor type is only available for Microsoft SQL servers.

These sensors monitor Microsoft SQL servers' performance via Windows Management Instrumentation (WMI). You can manually set up different performance counters for your server instances, for example, general statistics, access methods, buffer and memory manager, locks, and SQL statistics.

Microsoft SQL Server performance sensors are available for Microsoft SQL Server 2008 and 2012:

- [WMI Microsoft SQL Server 2008 Sensor](#)  1501
- [WMI Microsoft SQL Server 2012 Sensor](#)  1509

Part 11

System Administration Tools

11 System Administration Tools

Using the two applications **PRTG Server Administrator** and **PRTG Probe Administrator** from the Windows start menu, you can edit administrative settings that affect your PRTG installation, the local probe running with it, or a remote probe installation. All settings will require a restart of the Windows services for changes to take effect. Please see these following sections.

System Administration Programs—Topics

- [PRTG Server Administrator](#)  1959
- [PRTG Probe Administrator](#)  1979

Related Topics

- [Setup](#)  1784
- [Failover Cluster Step by Step](#)  2029

11.1 PRTG Server Administrator

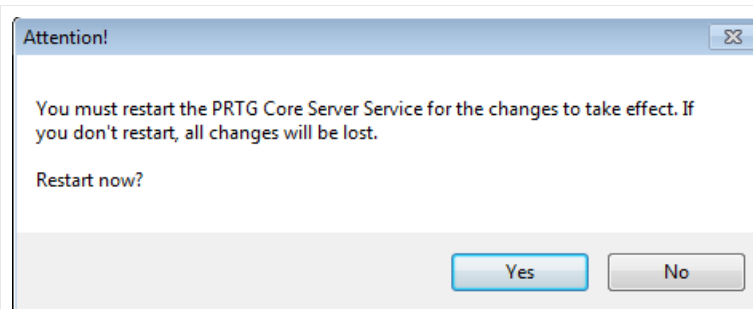
In the PRTG Server Administrator program you can define different system-oriented settings that affect your PRTG installation, as well as restart services and view log information. **Note:** To get familiar with the different components of PRTG, we recommend reading the [Architecture](#) section.

Note: All settings made here are only valid for the local installation running on the computer you're opening the program on. In order to change settings for another installation, for example, another cluster node installation, please log in to this computer and open the program there.

From the **PRTG Network Monitor** group in Windows start menu, please select **PRTG Server Administrator** to open the application. You can choose from these options in different tabs:

- [Web Server](#) 
- [Core Server](#) 
- [Cluster](#) 
- [Memory Usage](#) 
- [Administrator](#) 
- [License](#) 
- [Start/Stop](#) 
- [Logs](#) 
- [About](#) 

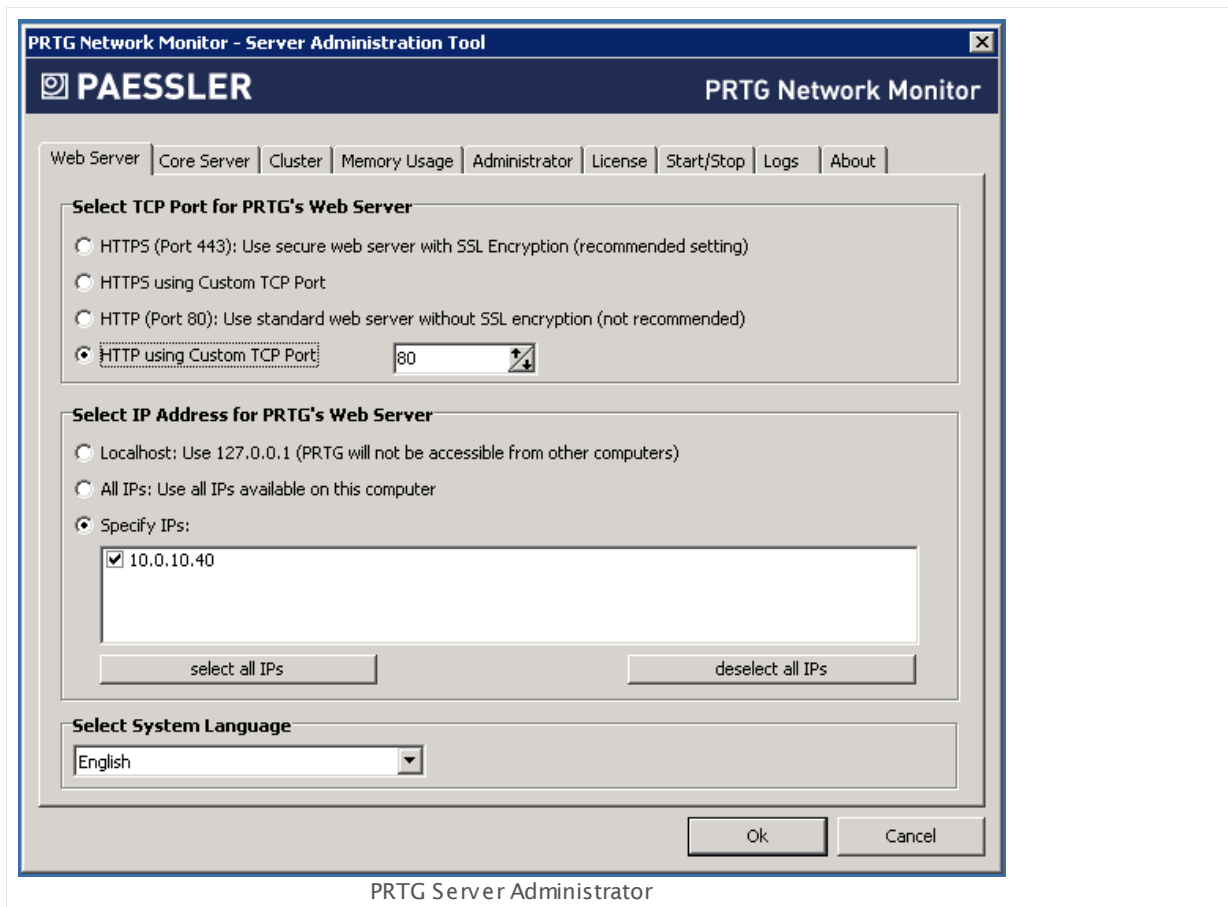
When closing the program using the **Ok** button, you are asked to restart the core server Windows service in order to save the settings. Please confirm by clicking the **Yes** button. Otherwise the changes are ignored.



PRTG Server Administrator

Web Server

Edit IPs, ports, access methods and language for the [Ajax](#)  and [Mobile Web GUI](#)  web interfaces.



Web Server—Select TCP Port for PRTG's Web Server

PRTG is running a web server in order to provide the web and Windows interface. Please specify on which port this web server will run.

HTTPS (Port 443)

- This is the recommended setting.
- Use a secure HTTPS connection that is encrypted via SSL on port 443.
- **Note:** Although the connection is secure, you will see an [SSL Certificate Warning](#)^[105] in your browser when logging in to the PRTG web interface, because the default certificate is unknown to your browser. You can install another SSL certificate for PRTG later. Please see [Using Your Own SSL Certificate](#)^[2030].
- **Note:** If port 80 is free, PRTG will reserve it as well. When users try to connect on port 80 via HTTP, they will then be redirected to port 443 via HTTPS. You can change this behavior using a registry setting.

HTTPS using Custom TCP Port

- Use a secure HTTPS connection that is encrypted via SSL on a custom port.

- This option is intended for systems with an existing web server on the standard port.
- Enter the desired TCP port number you want the PRTG web server to run on.
- **Note:** Although the connection is secure, you will see an [SSL Certificate Warning](#)^[105] in your browser when logging in to the PRTG web interface, because the default certificate is unknown to your browser. You can install another SSL certificate for PRTG later. Please see [Using Your Own SSL Certificate](#)^[2038].
- **Note:** If port 80 is free, PRTG will reserve it as well. When users try to connect on port 80 via HTTP, they will then be redirected to the custom port via HTTPS. You can change this behavior using a registry setting.

HTTP (Port 80)

- This setting is not recommended for WAN connections.
- Use a standard web server without SSL encryption on port 80.
- **Note:** If used on the internet, attackers could potentially spy on credentials you enter into PRTG. We strongly recommend using this option in a LAN only.

HTTP using TCP Port

- This setting is not recommended for WAN connections.
- Use a standard web server without SSL encryption on a custom port.
- This option is intended for systems with an existing web server on the standard port.
- Enter the desired TCP port number you want the PRTG web server to run on.
- **Note:** If used on the internet, attackers could potentially spy on credentials you enter into PRTG. We strongly recommend using this option in a LAN only.

Web Server—Select IP Address for PRTG's Web Server

PRTG is running a web server in order to provide access via the web and Windows interface. Please specify which IP address this web server will run on. **Note:** Later, you can log into PRTG by simply pointing your browser to the specified IP address.

Localhost

- Use **127.0.0.1** only.
- PRTG's web and Windows interface will only be accessible from the computer PRTG is installed on.
- **Note:** Either the selected port or at least one port in the range from **8080** to **8089** has to be available on **127.0.0.1**.

Note: If you run PRTG on localhost, please do not use the DNS name <http://localhost> to log in to the web server, as this may considerably slow down PRTG's web interface. Please use your local IP address or <http://127.0.0.1> instead.

All IPs

- Use all IP addresses available on this computer and enable access to the web server for all of these addresses.
- **Note:** The TCP port selected above must be free on every available IP address.

Specify IPs

- Select specific IP addresses on which the PRTG Web server will run on.
- A list specific to your system is shown.
- Add a check mark in front of every IP address you want the PRTG web server to be available at.
- **Note:** Either the selected port or at least one port in the range from **8080** to **8089** has to be available on the specified IP address.

Note: Regardless of the selected setting above, one port in the range from **8080** to **8180** has to be available on the specified IP address so PRTG can create reports. The report engine will try to connect to the core server on one of these ports.

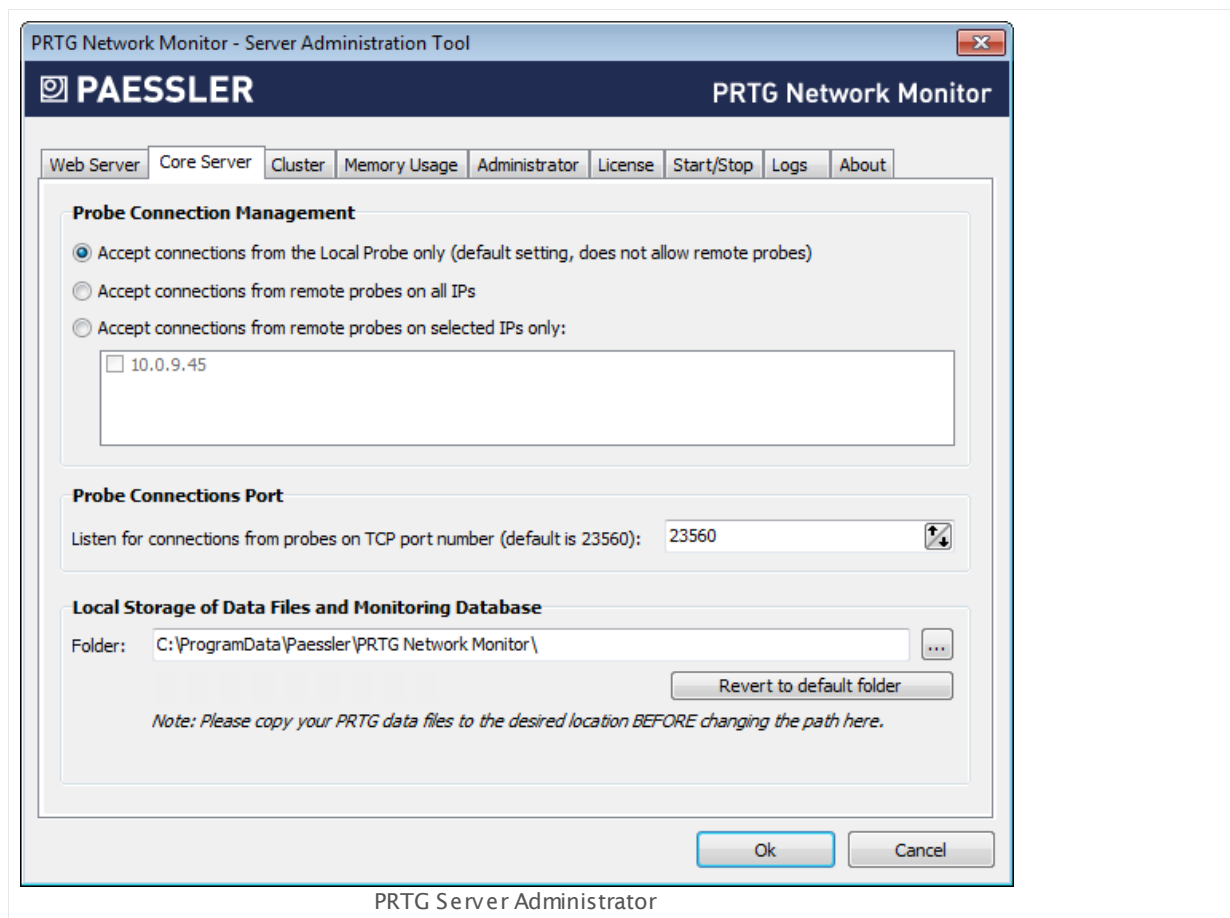
Note: If PRTG does not find a network card on startup it will switch the IP setting to **Localhost**. This setting will remain, even if a network card is available later on. If you disabled or removed the network card on the machine running the PRTG core server, please re-check this setting.

Select System Language

- Choose the language for this program from the drop down menu. Default is **English**. Depending on your installation, you may be able to choose other languages here.
- This setting will influence the language of this program, as well as the [Ajax](#)  and the [Mobile Web GUI](#)  web interfaces.

Core Server

Define settings for the core server.



Core Server—Probe Connection Management

In this section you can define how PRTG handles incoming connections from probes. Choose between several options.

Accept connections from the Local Probe only

- This is the default setting.
- Only local probe connections will be accepted by the PRTG core server.
- You cannot use [remote probes](#) with this setting enabled.

Accept connections from remote probes on all IPs

- Incoming connections from remote probes will always be accepted, no matter on which IP address of the core server they come in.

Accept connections from remote probes on selected IPs only

- Incoming connections from [remote probes](#) ²⁰²⁰ will only be accepted on the selected IP address(es) of the core server.
- In the list, select the IP addresses by adding a check mark in front the IPs.

Core Server—Probe Connections Port

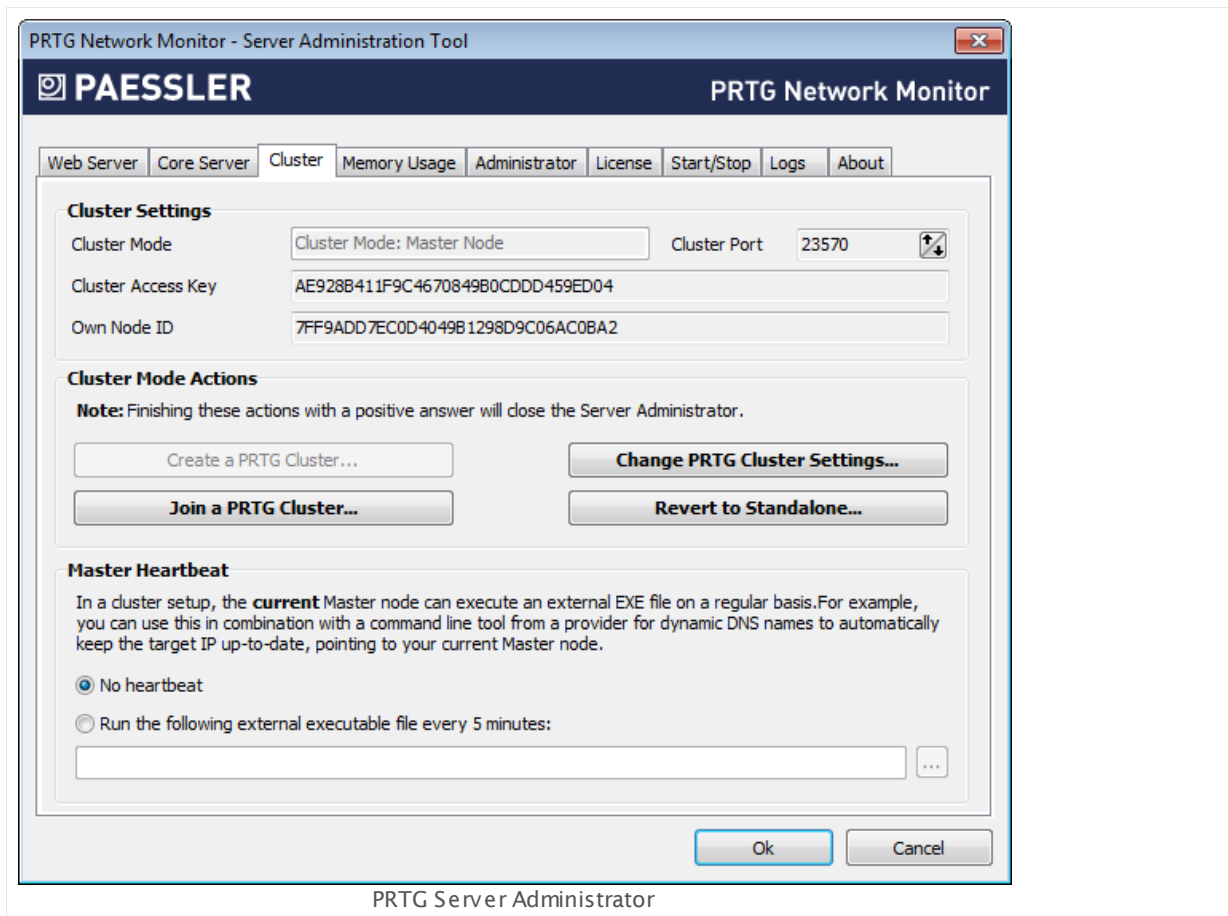
In this section you can define on which TCP port number PRTG listens to for incoming probe connections. Enter a port number. We recommend using the default value.

Core Server—Local Storage of Data Files and Monitoring Database

- Define the data folder to which PRTG will store configuration and monitoring data. Define a path or click on the **Revert to default folder** to reset to default. **Note:** Before changing the path, make sure you stop both services and copy all data to the new location.

Cluster

In the **Cluster** tab you can manually change how the current core installation will behave in a cluster. Before changing settings here, please read [Failover Cluster Configuration](#) ²⁰²⁰ section.



Cluster—Cluster Settings

Depending on the current cluster settings you will see different information here.

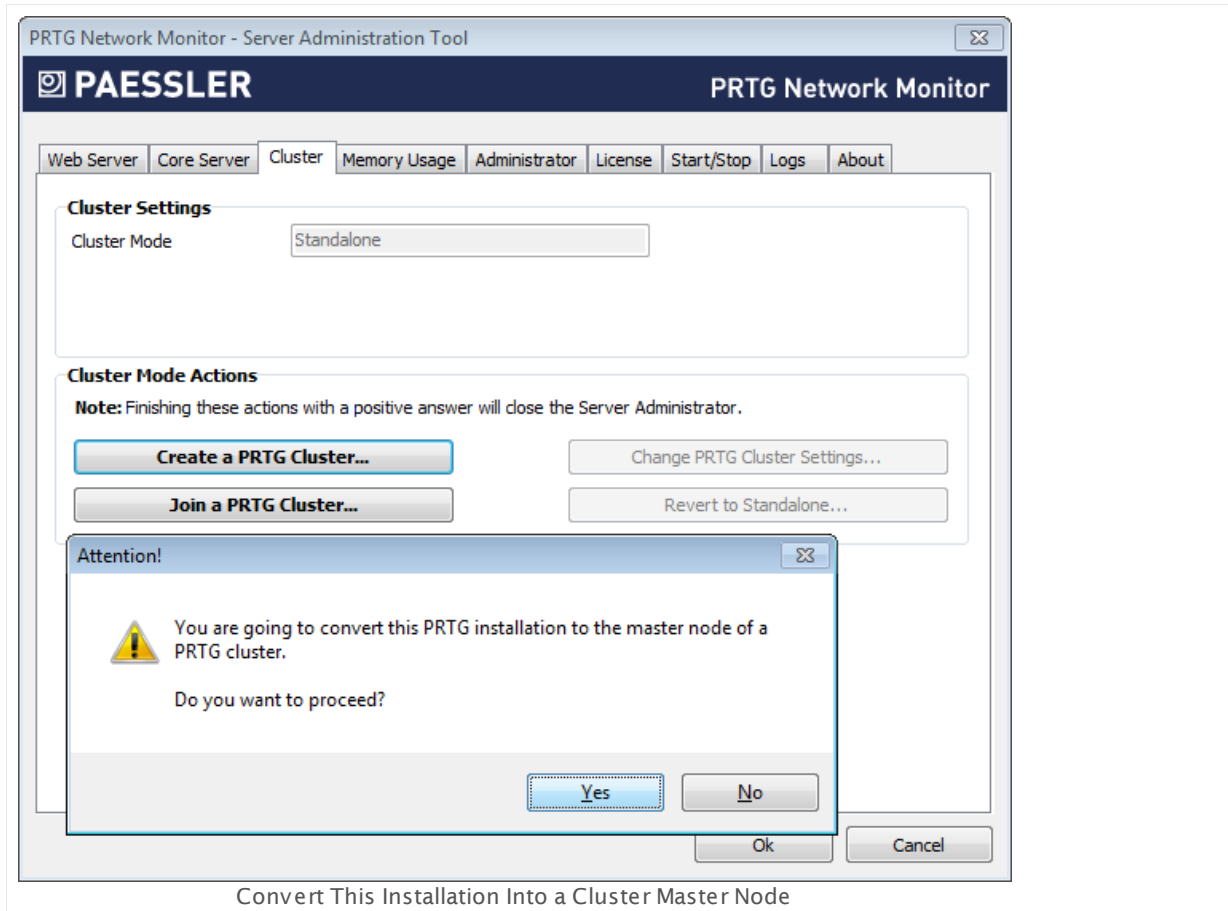
- In the **Cluster Mode** field shows which cluster mode the current installation is running. This setting is shown for your information only and cannot be changed here. Possible values are **Standalone** (no cluster mode), **Cluster Mode: Master Node**, or **Cluster Mode: Failover Node**.
- The **Cluster Access Key** field is shown only when running in a cluster mode. This setting is shown for your information only and cannot be changed here.
- The **Own Node ID** field is shown only when running in a cluster mode. This setting is shown for your information only and cannot be changed here.

Cluster—Cluster Mode Actions

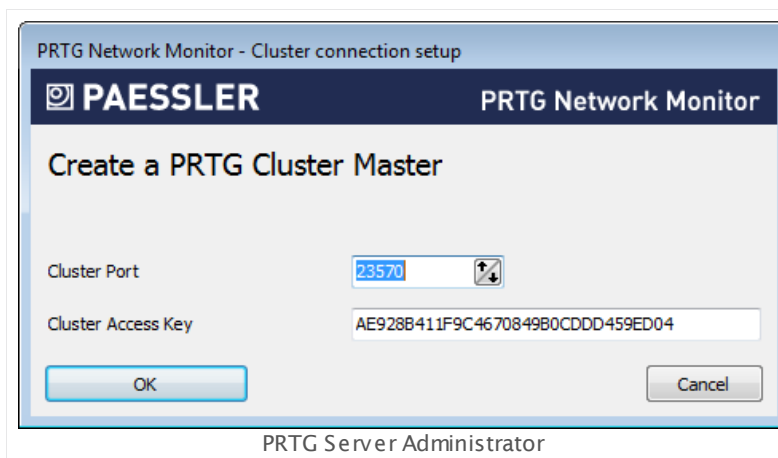
Depending on the current cluster settings you will see different buttons active here.

Create a PRTG Cluster...

- Start creating a cluster by clicking this button. The current PRTG core server will then be the **Master Node** of your cluster.
- After you click this button, please confirm converting this installation into a master node by clicking on the **Yes** button.



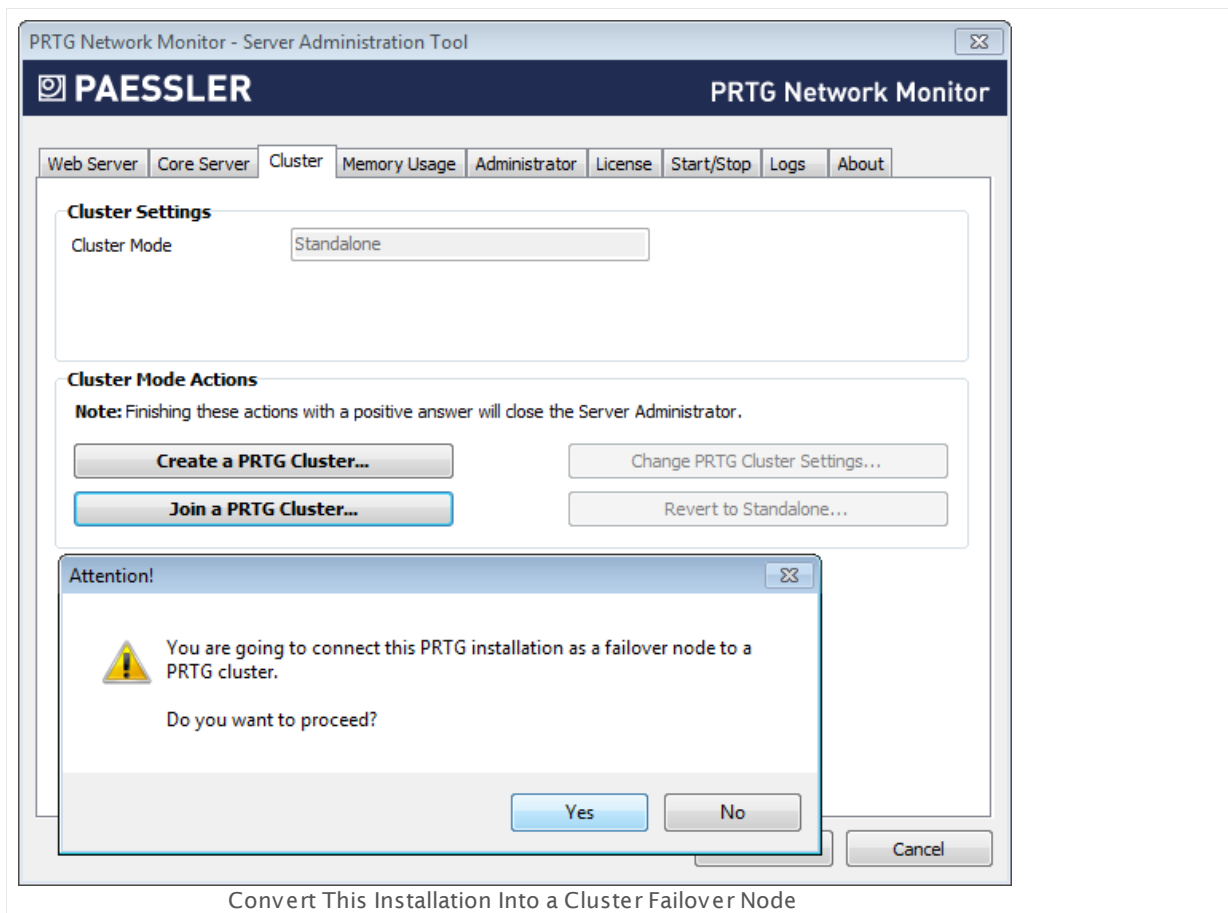
- A new popup window will appear.



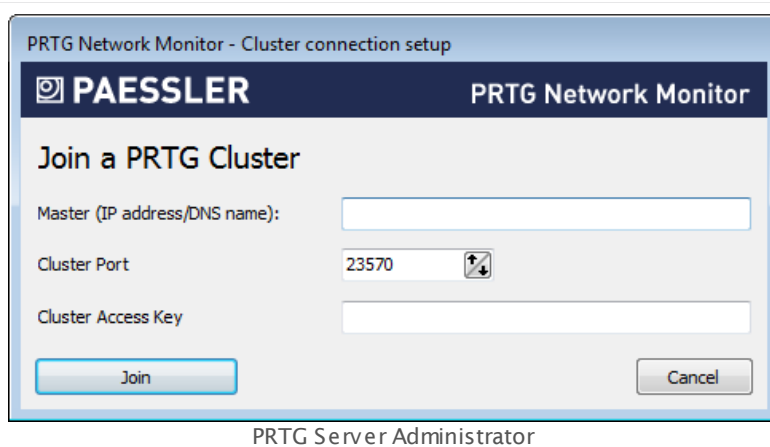
- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.
- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- We recommend using the default value.
- Save the **Cluster Access Key** so you have it at hand when configuring your Failover Node (s).
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

Join a PRTG Cluster...

- Add this installation to an existing cluster which already has a **Master Node**, by clicking this button. The current PRTG core server will then be a **Failover Node** in the cluster.
- **Note:** This button is also available if you're currently running your PRTG installation in **Cluster Mode: Master Node**. This option will then change your master node to a failover node!
- After you click this button, please confirm converting this installation into a failover node by clicking on the **Yes** button.

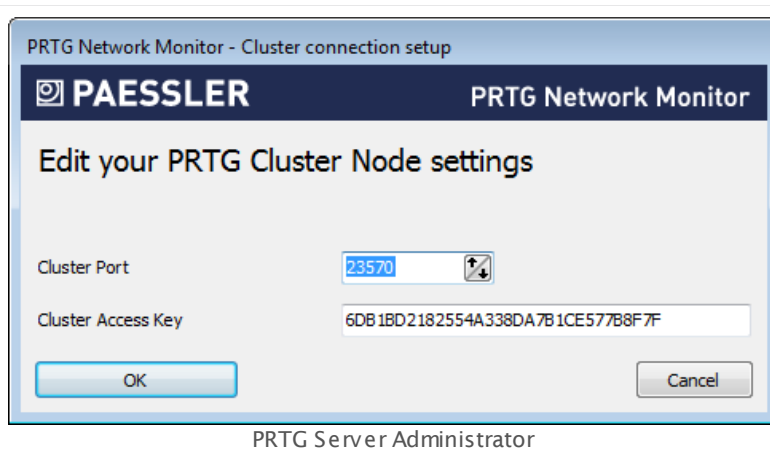


- A new popup window will appear.



- Enter the cluster's **Master IP address/DNS name**. It must be reachable from the machine running the failover node.
- Enter the other settings as defined in your **Master Node**'s settings. Please make sure you use the same settings on all nodes in your cluster.
- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.
- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

Change PRTG Cluster Settings...



- If you're running your PRTG installation in cluster mode, you can change the settings here. A new window will appear.

- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.
- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- Please make sure you use the same settings on all nodes in your cluster.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

Revert to Standalone...

- If you're currently running your PRTG installation in cluster mode, you can change it to **Standalone** mode. If you do so, this node will no longer be part of a cluster.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

Master Heartbeat

This section is only visible if you're running your PRTG installation in cluster mode. The **current** master can execute an external executable file on a regular basis. We call this a "heartbeat".

This can be used, for example, to report the IP address of the current master node to a dynamic DNS provider, so a DNS name is always redirected to the current PRTG master node in case the original master node fails and a failover node (running at a different IP address) takes over the master role.

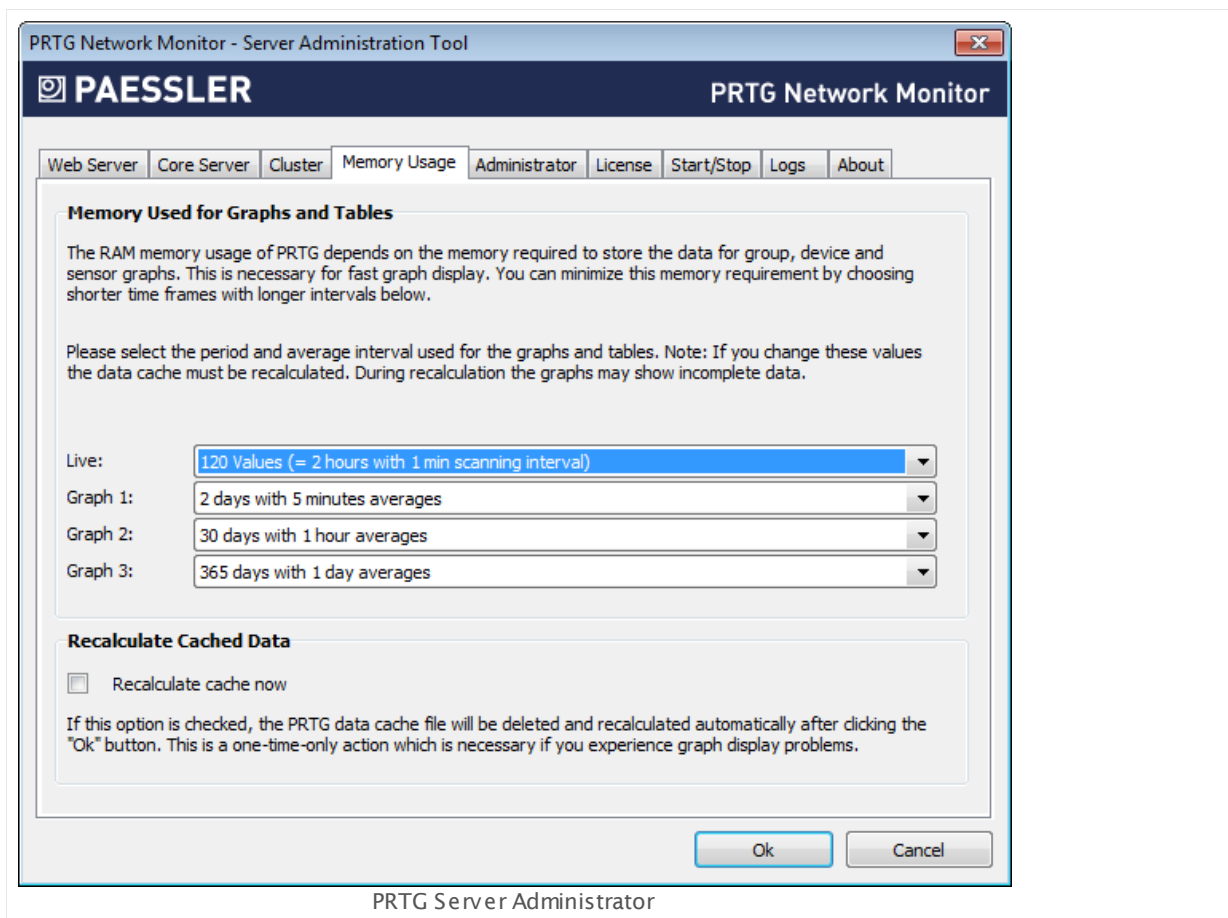
Choose between:

- **No heartbeat**: Do not execute a file on a regular basis.
- **Run the following external executable file every 5 minutes**: Click on the ... button to choose a file you want to execute. This can be, for example, a command line tool, or a batch file. It will be executed on the current master node only, with a fixed interval of five minutes. The interval cannot be changed.

Note: Please make sure the selected file is available under the same (local) path on all failover nodes. In case one of your failover nodes becomes current master, the heartbeat can only be executed reliably if the respective executable file exists on all of your failover nodes.

Memory Usage

PRTG shows several graphs in the [objects' detail pages](#)^[124] in the web interface. These are kept in RAM memory for fast display without causing extra CPU load or disk usage. The longer the time frames and the shorter the intervals are, the more memory will be used for this. You can adapt the details for all four graphs. This setting will also change the caption of the objects' tabs in the [web interface](#)^[100] and [Enterprise Console](#)^[106].



Live

The live graph is available for sensors only. For the live graph, no fixed time span is given, but you can define how many values will be displayed. The actual time span covered by the live graph depends on the scanning interval set for the sensor you're viewing and is calculated automatically. By default, **120 Values** is set, which results in a graph covering a time span of two hours, if a scanning interval of 60 seconds is set for the sensor. Other scanning intervals will result in graphs covering different time spans. Choose between:

- **60 Values:** This corresponds to a live graph covering a time span of one hour if a 1 minute scanning interval is set. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more.
- **120 Values:** This corresponds to a live graph covering a time span of two hours if a 1 minute scanning interval is set.
- **240 Values:** This corresponds to a live graph covering a time span of four hours if a 1 minute scanning interval is set.
- **480 Values:** This corresponds to a live graph covering a time span of eight hours if a 1 minute scanning interval is set.
- **960 Values:** This corresponds to a live graph covering a time span of 16 hours if a 1 minute scanning interval is set. Uses most RAM memory.

Graph 1

By default, this is the **2 days** graph in the web interface. You can change it to more or less detail by choosing a time span and a monitoring interval average associated with it. Monitoring results will be averaged regardless of the actual scanning interval set for the sensors. Choose between:

- **1 day with 1 minute averages:** Results in 1440 values.
- **1 day with 5 minutes averages:** Results in 288 values.
- **1 day with 15 minutes averages:** Results in 96 values. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more.
- **2 days with 1 minute averages:** Results in 2880 values. Uses most RAM memory.
- **2 days with 5 minutes averages:** Results in 576 values.
- **2 days with 15 minutes averages:** Results in 192 values.
- **4 days with 1 hour averages:** Results in 96 values. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more.

Graph 2

By default, this is the **30 days** graph in the web interface. You can change it to more or less detail by choosing a time span covered and a monitoring interval average associated with it. Choose between:

- **10 days with 1 hour averages:** Results in 240 values.
- **20 days with 1 hour averages:** Results in 480 values.
- **30 days with 1 hour averages:** Results in 720 values.
- **30 days with 6 hour averages:** Results in 120 values. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more.
- **40 days with 1 hour averages:** Results in 960 values.
- **40 days with 6 hour averages:** Results in 160 values.
- **60 days with 1 hour averages:** Results in 1440 values. Uses most RAM memory.
- **60 days with 6 hour averages:** Results in 240 values.

Graph 3

By default, this is the **365 days** graph in the web interface. You can change it to more or less detail by choosing a time span covered and a monitoring interval average associated with it. Choose between:

- **100 days with 1 day averages:** Results in 100 values. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more.
- **200 days with 1 day averages:** Results in 200 values.

- **365 days with 1 day averages:** Results in 365 values.
- **400 days with 1 day averages:** Results in 400 values.
- **750 days with 1 day averages:** Results in 750 values. Uses most RAM memory.

Recalculate Cached Data

PRTG writes monitoring data to the disk constantly and keeps the graphs for your graph tabs in memory. If PRTG is ended unexpectedly, the graph cache may get corrupted. In this case, graphs may be shown empty or show wrong data.

If you experience graph display problems, a graph recalculation will fix the problem. Enable the **Recalculate cache now** option. After you close the window with **Ok** and confirm restart of the Windows service, PRTG will delete the data cache file and recalculate it automatically.

Note: Directly after this action your graphs will be empty. They will be re-filled successively while recalculation in the background progresses. Until recalculation is finished, performance of the PRTG web interface may be affected due to high disk I/O activity.

Administrator

PRTG Network Monitor - Server Administration Tool

PAESSLER PRTG Network Monitor

Web Server Core Server Cluster Memory Usage Administrator License Start/Stop Log About

Login Credentials for the Administrator Account

Email Address: john.q.public@example.com

Login Name: prtgadmin

Password: ***** Confirm Password: *****

Ok Cancel

PRTG Server Administrator

Enter the administrator's contact email address and define login credentials for PRTG.

Email Address

- Enter a valid administrator's email address.
- By default, PRTG will send notifications and important messages to this address.

Login Name

- Enter a name for the PRTG System Administrator login; this is your default login.
- It is used when logging in to the PRTG Web- or Windows interface.
- The default login name is **prtgadmin**

Password

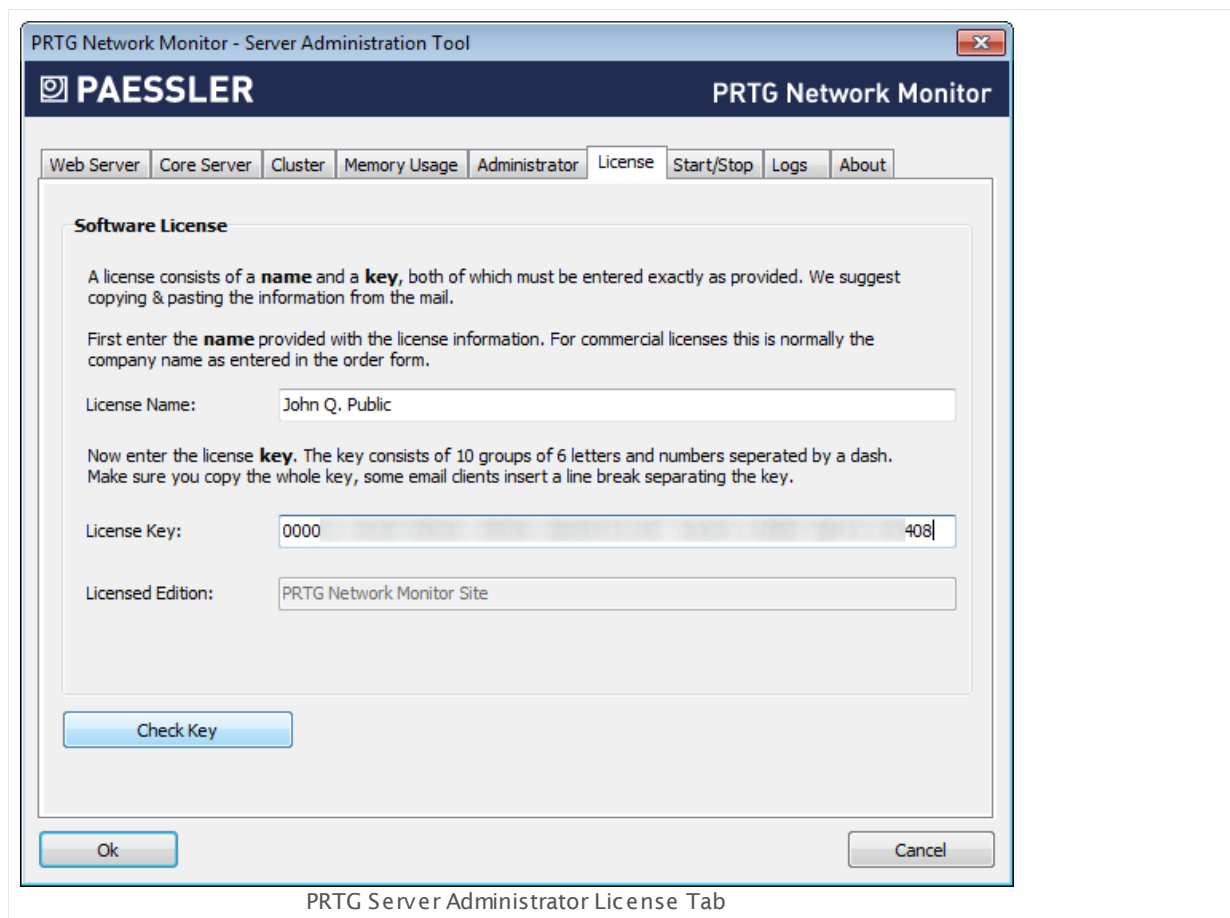
- Enter a password for the PRTG System Administrator login; this is your default login.
- It is used when logging in to the PRTG Web- or Windows interface.
- The default password is **prtgadmin**

Confirm Password

- Re-enter the password for the PRTG System Administrator login.
- The default password is **prtgadmin**

License

To use a PRTG license with this installation of PRTG, please enter the license information you have received from Paessler via email. To avoid typing errors, please copy and paste both the **License Name** and the **License Key** from the email. Both must be transferred exactly as shown in the email.

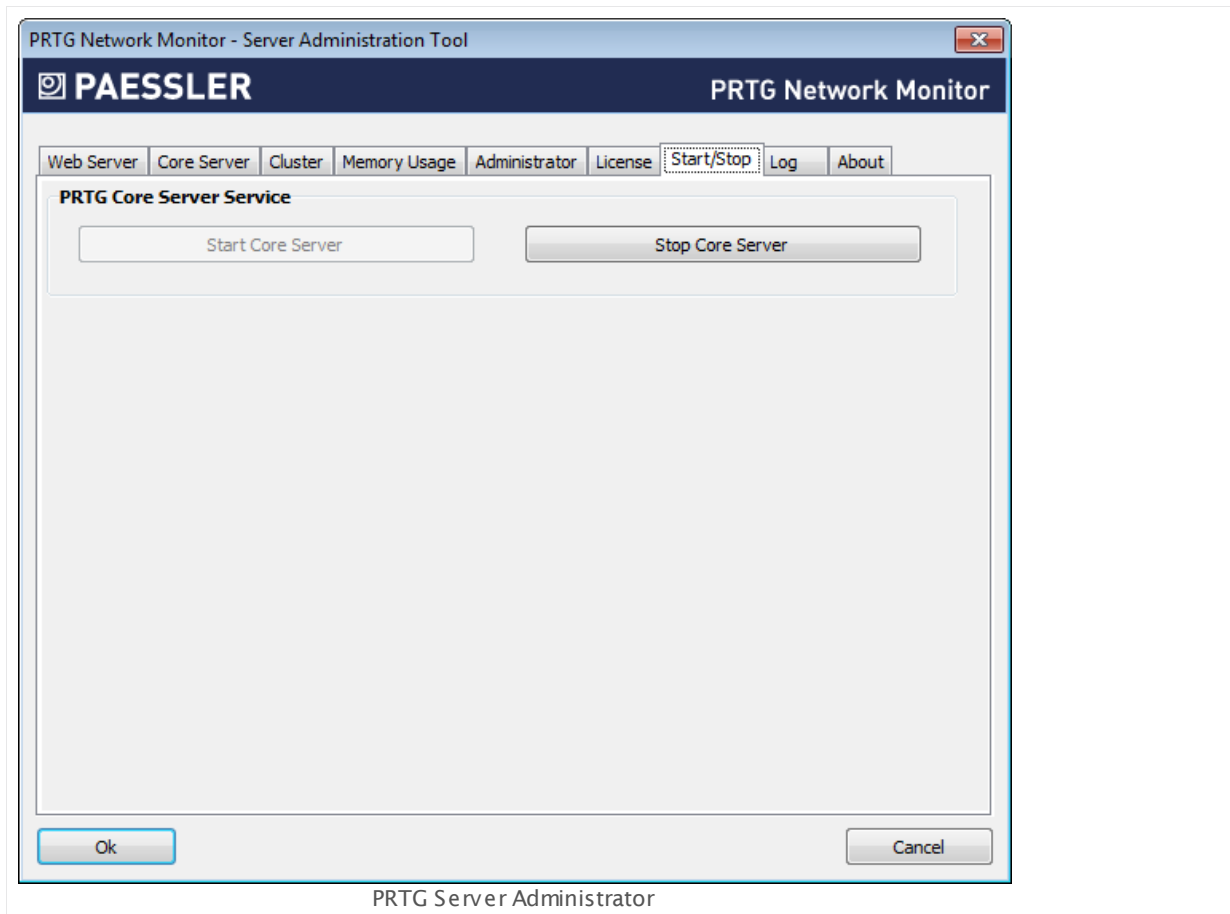


To make sure your key has been entered correctly please click on the **Check Key** button. A popup box will either show success or denial of your license information. License information is also checked if you change tabs.

In the **Licensed Edition** field you will see an accepted license key.

Note: You have to use the right edition for your license key. For example, the installer for trial and Freeware edition does not accept any commercial keys. For more information, please see [Enter a License Key](#) ^[57] section.

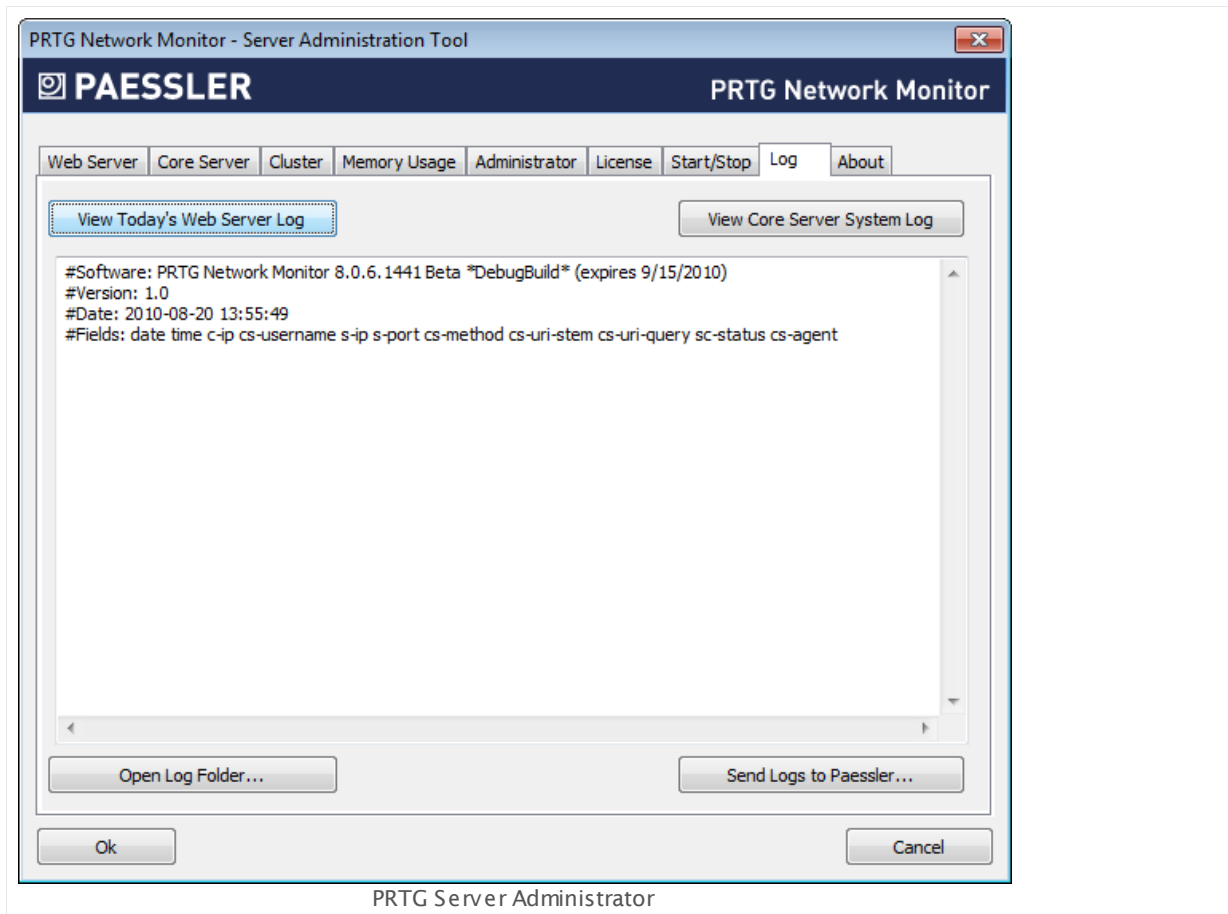
Start/Stop



You can stop and start the core server Windows service manually. Click the **Stop Core Server** button to stop the service, and **Start Core Server** to start it again. Both actions usually take from a few seconds up to several minutes to complete.

Note: If you want to schedule an automatic restart of Windows services for both core server and probe service, please do so using the **PRTG Probe Administrator**. For more details see [PRTG Probe Administrator](#) (Start/Stop) section.

Logs



You can view several logs of your PRTG installation. The following buttons are available:

- **View Today's Webserver Log**
Directly view the content of the web server log for the current date.
- **View Core Server System Log**
Directly view the content of the core server system log. Depending on the number of entries, it may take a few seconds until the logs are shown.
- **Open Log Folder...**
Open the log file directory on your hard disk drive to access older web log files, etc.
- **Send Logs to Paessler...**
Open an assistant to send log files to the Paessler support team. Please see below.

Logs—Send Logs to Paessler

Send Logs to Paessler

PAESSLER PRTG Network Monitor

Send Logs to Paessler

Name

Email

Ticket No.

Please supply your Paessler Ticket Number (PAEXXX) if you already have an open support ticket.

Configuration ☒ include Configuration file (may contain passwords)

Note: while passwords are usually encrypted the configuration file contains SNMP communities and hostnames in plain text.

If you click the "Send" button, this program will upload the relevant log files and, if selected, the configuration file of your PRTG installation to Paessler's FTP server and support ticketing system.

Please ensure that outgoing FTP and HTTP connections are enabled on this machine.

Send Logs to Paessler

When opening a support ticket, Paessler support may ask you to send log files for further analysis. Using the **Send Logs to Paessler...** button, PRTG will automatically collect, compress and send your log files. **Note:** This button is available when using a commercial license only.

Name

- Please enter your name.

Email

- Please enter your valid email address.

Ticket No.

- This field is optional.
- If you have already opened a ticket at Paessler support, please provide the ticket number you received. Your files will then be associated with your ticket automatically.
- Please enter the ticket number starting with **PAE** followed by four or more digits.
- If you do not have a ticket number, please leave the field empty. **Note:** You should usually contact the support team **before** sending any files.

Configuration

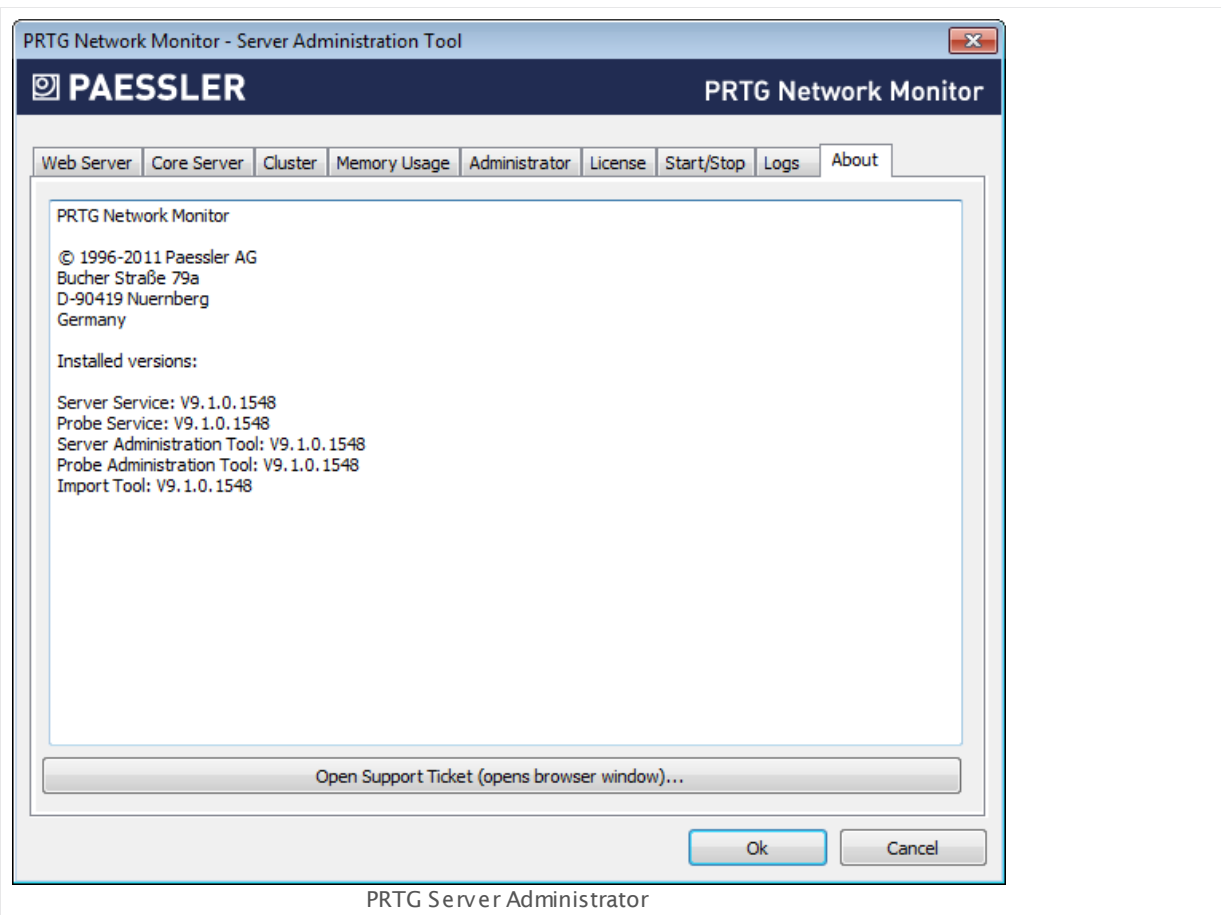
- Define if your configuration file will be included in the data. Passwords are usually encrypted, but there may be some passwords stored as plain text.

Shortened

- Define if your log files will be shortened (this is the default setting). Sometimes we will ask you to send full log files. In this case, please uncheck this box.

Click on the **Send** button to start data upload. Please make sure FTP and HTTP connections are allowed on this machine.

About



Displays version information for installed PRTG programs. Click on the **Open Support Ticket** button to ask the Paessler support team for help. This will open a new web browser window.

11.2 PRTG Probe Administrator

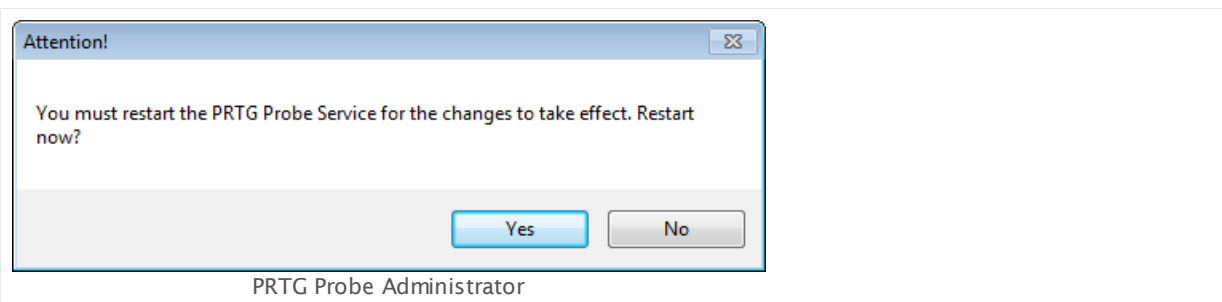
In the PRTG Probe Administrator program, you can define different system-oriented settings that affect your PRTG installation, as well as restart services and define the data storage location. **Note:** To get familiar with the different components of PRTG, we recommend reading the [Architecture](#) section.

Note: All settings made here are only valid for the local installation running on the computer you're opening the program on. In order to change settings for another installation, for example, another remote probe installation, please log in to this computer and open the program there.

From the **PRTG Network Monitor** group in Windows start menu, please select **PRTG Probe Administrator** to open the application. You can choose from these options in different tabs:

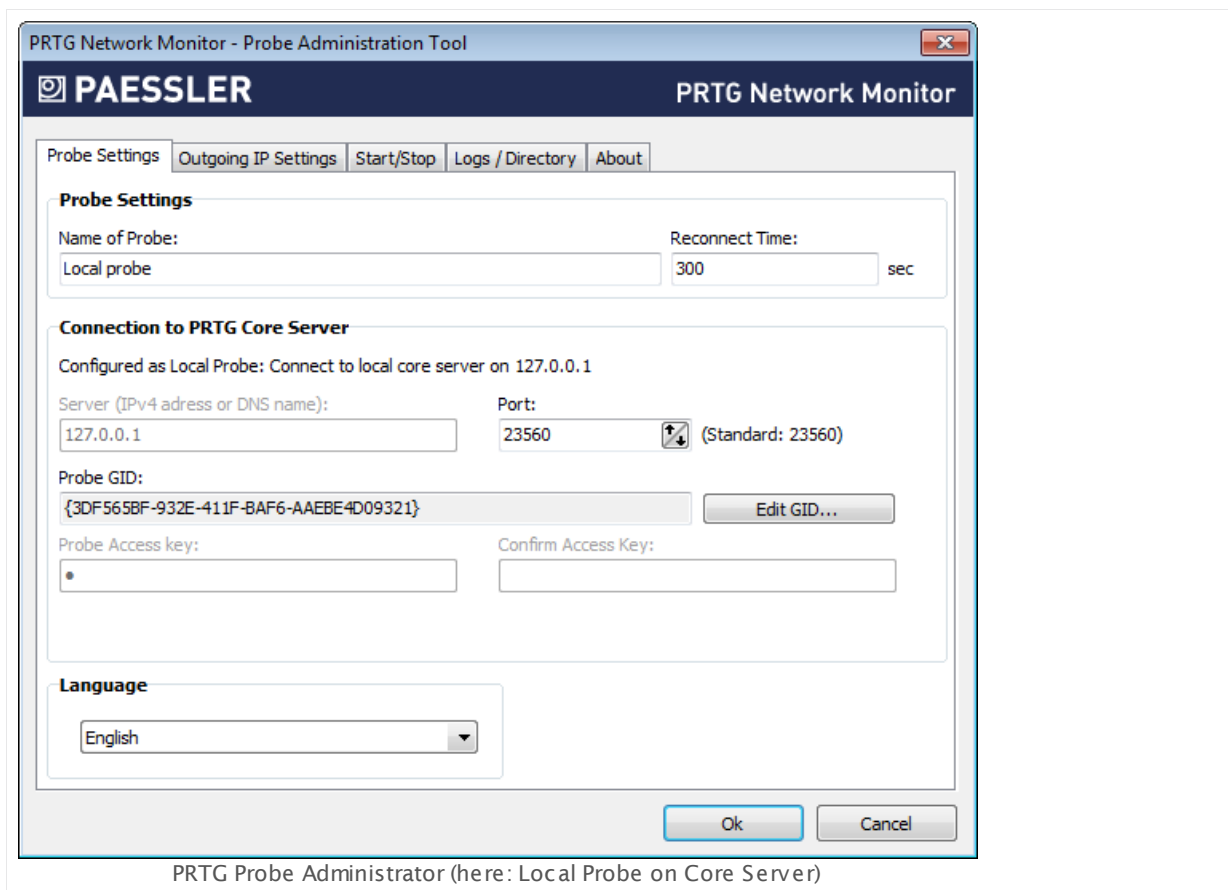
- [Probe Settings](#)
- [Outgoing IP Settings](#)
- [Start/Stop](#)
- [Logs / Directory](#)
- [About](#)

When closing the program using the **Ok** button, you are asked to restart the probe Windows service in order to save the settings. Please confirm by clicking the **Yes** button.



Probe Settings

Define general settings regarding the probe and probe connections.



Probe Settings—Probe Settings

Name of Probe

- Enter a name for the probe. It will appear in the device tree in the web interface.

Reconnect Time

- Define the time that will be waited until the probe tries to reconnect to the core server in case the connection fails.

Probe Settings—Connection to PRTG Core Server

These settings will affect how the probe will connect to the core server. A probe is either a local probe or a remote probe. PRTG will automatically detect the type of probe and show the correct setting options.

When you opened this tool on the PRTG core server

- This probe is configured as the local probe of the PRTG core installation.
- It will connect to the core via **127.0.0.1**.

- Define the **Port** number under which probe and core server will communicate. We recommend using the default value.
- The **Probe GID** is a unique identifier for the probe and should not be changed.
- No access key is needed for local probe connections.

When you opened this tool on a machine running a Remote Probe

- This probe is configured as remote probe.
- Enter the Server IP address or DNS name and the port for the connection to the core server.
- Define the **Port** number under which probe and core server will communicate. We recommend using the default value.
- The **Probe GID** is a unique identifier for the probe and should not be changed. Except when substituting an existing probe, you must change it to the old probe's GID. To do so, click on the **Edit GID...** button and confirm the warning with **Yes**. You can then change the value.
- The **Probe Access key** must match one of the access keys configured in your PRTG core server installation. If it doesn't, the remote probe will not be able to connect to the core server. Please see [System Administration—Probes](#)¹⁸²¹ (Probe Connection Settings) section for more information. **Note:** Also check the allowed and denied IPs there to make sure the core server accepts the IP address of the remote probe.

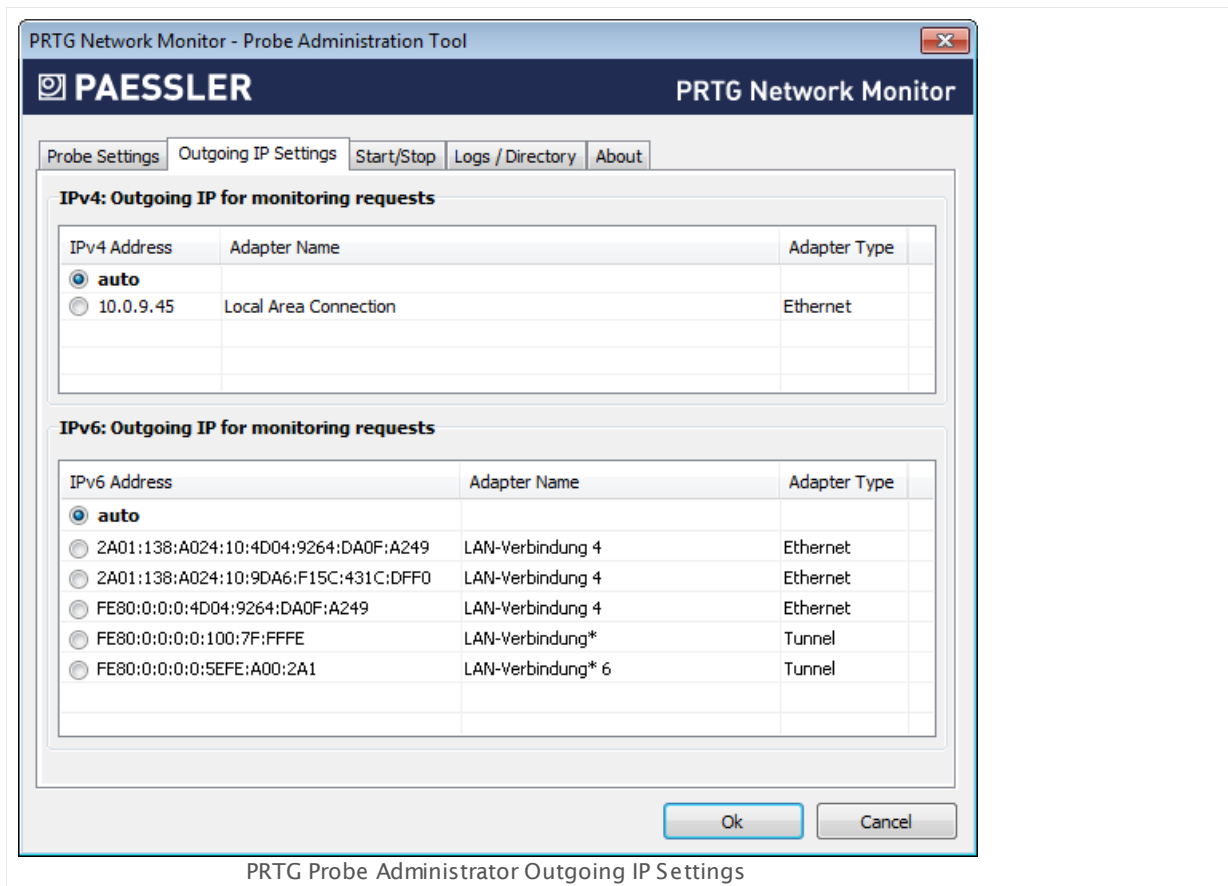
Probe Settings—Language

- Choose the language for this program from the drop down menu. Default is **English**. Depending on your installation, you may be able to choose other languages here.

Outgoing IP Settings

Define the IP address used for outgoing monitoring requests.

- If there is more than one IP on the current system available, you can specify the IP address that will be used for outgoing monitoring requests of certain sensor types.
- The setting is valid for all monitoring requests sent from this PRTG probe.
- This setting will be used for sensors using the following connection types: HTTP, DNS, FTP, IMAP, POP3, Port, Remote Desktop, SMTP, and SNMP.
- This is useful for devices that expect a certain IP address when queried.
- Default setting is **auto**. PRTG will select an IP address automatically.



Outgoing IP Settings—IPv4: Outgoing IP for Monitoring Requests

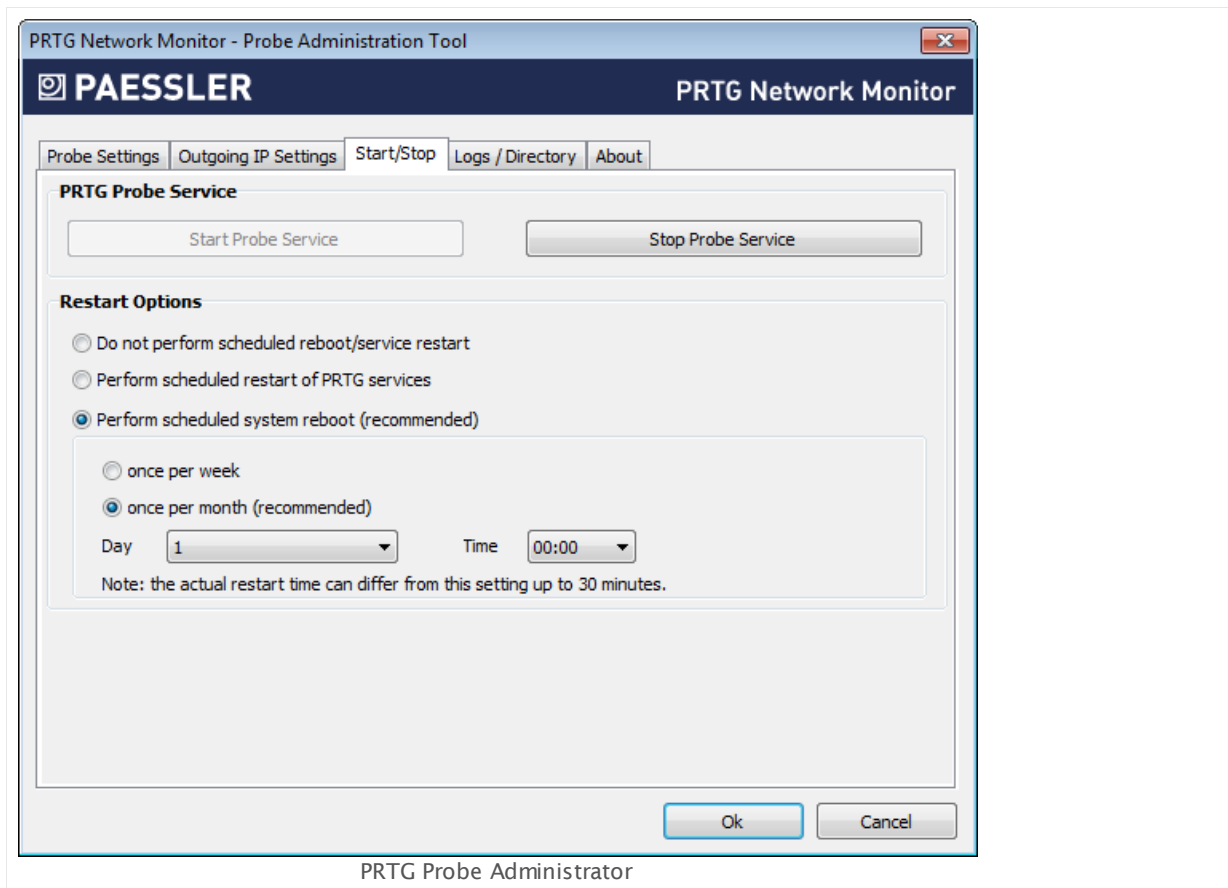
Define the IP address for outgoing requests using the IPv4 protocol. The list shows all IP addresses available on the current system. Choose a specific IP address or select **auto**.

Outgoing IP Settings—IPv6: Outgoing IP for Monitoring Requests

Define the IP address for outgoing requests using the IPv6 protocol. The list shows all IP addresses available on the current system. Choose a specific IP address or select **auto**. For details about the basic concept of IPv6 in PRTG, please see [IPv6](#) ⁹⁷ section.

Start/Stop

Start or stop the probe Windows service and schedule system restarts.



Start/Stop—PRTG Probe Service

You can stop and start the probe Windows service manually. Click the **Stop Probe Service** button to stop the service, and **Start Probe Service** to start it again. Both actions usually take from a few seconds up to several minutes to complete.

Start/Stop—Restart Options

For best performance we recommend to restart the Windows servers PRTG is running on from time to time. In order for PRTG to do this automatically you can schedule an automatic reboot. There are the following options:

Do not perform scheduled reboot/service restart

- Do not perform any scheduled reboot or restart of services automatically.
- We recommend a manual restart every few weeks.

Perform scheduled restart of PRTG services

- Restart both core server and probe service.

- Please enter a schedule below.

Perform scheduled system reboot (recommended)

- This is the recommended setting, although not set by default.
- Please enter a schedule below.
- We recommend restarting Windows servers once a month for best performance.

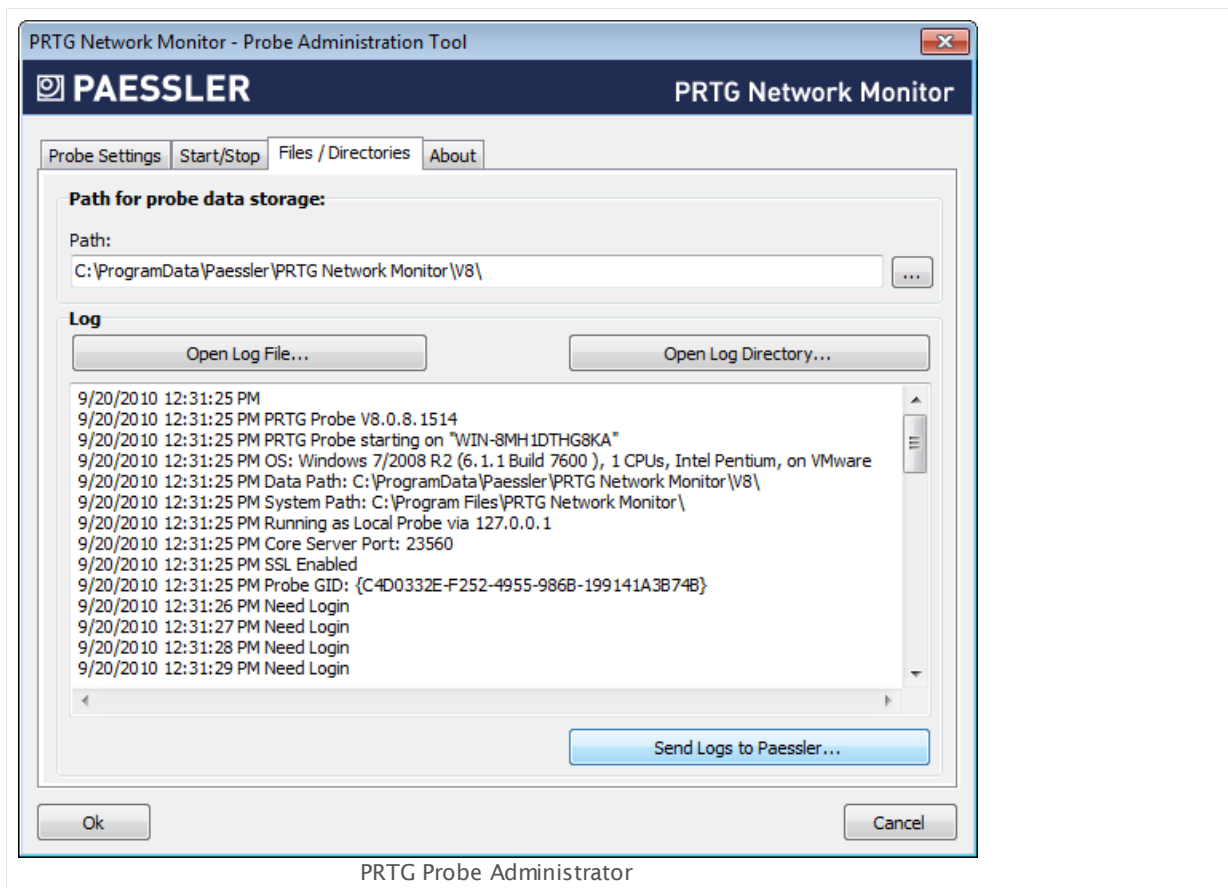
[Schedule]

When scheduling an automatic service restart or reboot, define a schedule. The options are:

- **Once per Week:** Select a weekday and time below.
- **Once per Month:** Select a day of month and time below. When selecting **Last**, the report will always run on the last day of the month, regardless of how many days the month has. When selecting a date that does not exist in every month, e.g. the 30th in May, PRTG will automatically run the report on the last day of this month.

Note: A Windows warning message will be displayed 10 minutes before reboot to inform a logged in user. The actual restart time can differ up to 30 minutes from the settings entered here!

Logs / Directory



Path for probe data storage

- **Note:** This setting is relevant merely for probe only installations, for example, when running a remote probe on the system. For an installation of PRTG core server and probe, i.e. a full PRTG installation, the path setting in this window is overridden by the path defined in the settings of [PRTG Server Administrator](#).
- Define the data folder to which PRTG will store configuration and monitoring data. **Note:** Before changing the path, make sure you stop both services and copy all data to the new location.

Log

You can view the log of your PRTG probe. The following buttons are available:

- **Open Log File...**
Directly view the content of the probe system log. Depending on the number of entries, it may take a few seconds until the logs are shown.

- **Open Log Directory...**
Open the log file directory on your hard disk drive.
- **Send Logs to Paessler...**
Open an assistant to send log files to the Paessler support team. Please see below.

Logs / Directory—Send Logs to Paessler

Send Logs to Paessler

PAESSLER PRTG Network Monitor

Send Logs to Paessler

Name

Email

Ticket No.

Please supply your Paessler Ticket Number (PAEXXXX) if you already have an open support ticket.

Configuration ☒ Include Configuration file (may contain passwords)

Note: while passwords are usually encrypted the configuration file contains SNMP communities and hostnames in plain text.

If you click the "Send" button, this program will upload the relevant log files and, if selected, the configuration file of your PRTG installation to Paessler's FTP server and support ticketing system.

Please ensure that outgoing FTP and HTTP connections are enabled on this machine.

Send Logs to Paessler

When opening a support ticket, Paessler support may ask you to send log files for further analysis. Using the **Send Logs to Paessler...** button, PRTG will automatically collect, compress and send your log files. **Note:** This button is available when using a commercial license only.

Name

- Please enter your name.

Email

- Please enter your valid email address.

Ticket No.

- This field is optional.

- If you have already opened a ticket at Paessler support, please provide the ticket number you received. Your files will then be associated with your ticket automatically.
- Please enter the ticket number starting with **PAE** followed by four or more digits.
- If you do not have a ticket number, please leave the field empty. **Note:** You should usually contact the support team **before** sending any files.

Configuration

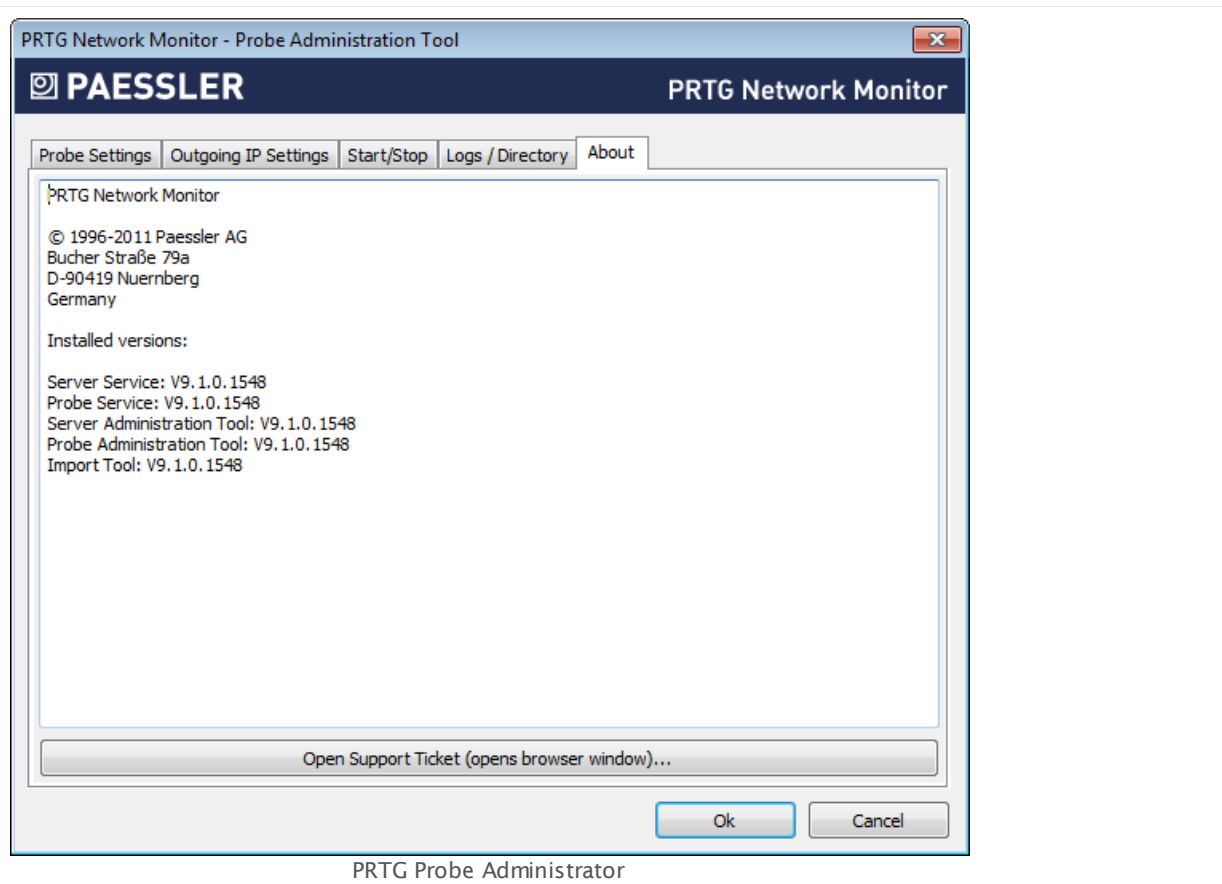
- Define if your configuration file will be included in the data. Passwords are usually encrypted, but there may be some passwords stored as plain text.

Shortened

- Define if your log files will be shortened (this is the default setting). Sometimes we will ask you to send full log files. In this case, please uncheck this box.

Click on the **Send** button to start data upload. Please make sure FTP and HTTP connections are allowed on this machine.

About



Displays version information for installed PRTG programs. Click on the **Open Support Ticket** button to ask the Paessler support team for help. This will open a new web browser window.

Part 12

Advanced Topics

12 Advanced Topics

In this section topics are covered that address more advanced PRTG users. If you already gained some experience with PRTG, you might want to learn more about the topics following.

Advanced Topics

- [Active Directory Integration](#)  1991
- [Application Programming Interface \(API\) Definition](#)  1993
- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)  1994
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)  1998
- [Define IP Ranges](#)  2000
- [Define Lookups](#)  2001
- [Regular Expressions](#)  2010
- [Add Remote Probe](#)  2011
- [Failover Cluster Configuration](#)  2026
- [Data Storage](#)  2036
- [Using Your Own SSL Certificate](#)  2038
- [Calculating Percentiles](#)  2040

12.1 Active Directory Integration

PRTG offers a detailed rights management via different user groups. For detailed information please see [User Access Rights](#)^[94].

In order to make user management easier, you can integrate an existing Active Directory into PRTG in four steps. During this process, you will connect an Active Directory (AD) group with a user group in PRTG. All members of your AD group will then be able to log into PRTG using their AD domain credentials. **Note:** You cannot add single AD users to PRTG, but only allow access for entire groups. A PRTG user will be created automatically for each AD user who logs in to PRTG successfully.

Step 1: Prepare Your Active Directory

- In your Active Directory, please make sure that users you want to give access to PRTG are member of the same AD group.
- You can also organize users in different groups, for example, one group whose members will have administrator rights within PRTG, and another one whose members will have read-only rights within PRTG.

Step 2: Prepare Your PRTG Server

- Make sure that the computer running PRTG is member of the domain you want to integrate it to. You can check this setting in your machine's **System Properties** (for example, **Control Panel | System and Security | System**, click on **Change settings** link).

Step 3: Add Domain and Credentials (optional) to System Settings

- In the PRTG [web interface](#)^[100], switch to the [System Administration—System and Website](#)^[105] settings.
- In the **Active Directory Domain** field, enter the name of your local domain. **Note:** You can only integrate one AD domain into PRTG.
- **Optional:** PRTG will use the same Windows user account used to run the "PRTG Core Server Service". By default, this is the "local system" Windows user account. If this user does not have sufficient rights to query a list of all existing groups from the Active Directory, you should provide credentials of a user account with full AD access by using the **Use explicit credentials** option.
- **Save** your settings.

Step 4: Add a New User Group

- Switch to the **User Groups** tab (see [System Administration—User Groups](#)^[102]).
- Click on the **Add User Group** button to add a new PRTG user group.
- In the dialog appearing, enter a meaningful name and set the **Use Active Directory** setting to **Yes**.

- From the **Active Directory Group** drop down menu, select the group of your Active Directory whose members will have access to PRTG. If you have a very large Active Directory, you will see an input field instead of a drop down. In this case, you can enter the group name only; PRTG will add the prefix automatically.
- With the **New User Type** setting, define the rights a user from the selected Active Directory group will have when logging in to PRTG for the first time. You can choose between **Read/Write User** or **Read Only User** (latter is useful to show data only to a large group of users).
- **Save** your settings.

Done

That's it. All users in this Active Directory group can now log in to PRTG using their AD domain credentials. Their user accounts will use the PRTG security context of the PRTG user group you just created.

Notes and Limitations

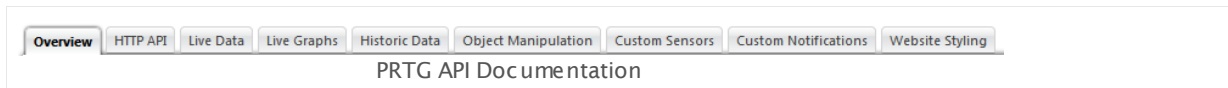
- Active Directory users can [log in to the web interface](#)^[102] using their Windows username and password (please do not enter any domain information in PRTG's **Login Name** field). When such a user logs in, PRTG will automatically create a corresponding local account on the PRTG core server. Credentials are synchronized every hour.
- All requests to the Active Directory servers are cached for one hour, for performance reasons. If a password is changed in the Active Directory, you must either wait for 1 hour or clear the cache manually by clicking on the **Clear Caches** button on the [System Administration—Administrative Tools](#)^[1833] page in the [Setup](#)^[1784] menu).
- By default, there aren't any rights set for the new PRTG user group. Initially, users in this group will not see any objects in the PRTG device tree. Please edit your device tree [object's settings](#)^[141] and set access rights for your newly created user group in the **Inherit Access Rights** section. **Note:** The easiest way is to set these rights in the [Root Group Settings](#)^[224].
- PRTG only supports explicit group rights. If your AD uses groups which are member of another group, PRTG will **not** regard inherited implicit rights of the parent group and therefore refuse login for members of those groups.
- PRTG will ignore AD information about Organizational Units (OUs). These values cannot be read by PRTG.
- PRTG does not support SSO (single sign-on).

12.2 Application Programming Interface (API) Definition

The PRTG Application Programming Interface (API) enables you to access monitoring data and manipulate objects using HTTP requests, run your own written sensors and notifications, and customize the web interface.

Detailed HTTP API Documentation

An interactive documentation of the API is integrated into your PRTG installation: [Login to the web interface](#)¹⁰² and select **Set up | PRTG API** from the main menu.



In different tabs, the documentation provides information about:

- **HTTP API:** Access monitoring data and manipulate monitoring objects using HTTP requests (includes an interactive query builder)
- **Custom Sensors:** Create your own sensors for customized monitoring
- **Custom Notifications:** Create your own notifications to send alarms to external systems
- **Website Styling:** Customize the look and feel by adding your own CSS statements

You can also have a look at Paessler's PRTG demo installation's API documentation. But only the documentation that comes with your PRTG installation fits exactly the PRTG version you are using.

More

API Documentation in Paessler's PRTG Demo Installation

- <http://prtg.paessler.com/api.htm?username=demo&password=demodemo>

12.3 Filter Rules for xFlow, IPFIX and Packet Sniffer Sensors

Filter rules are used for the include, exclude, and channel definition fields of Packet Sniffer, xFlow, and IPFIX sensors. They are based on the following format:

```
field[filter]
```

Valid Fields for All Sensors

- **IP**
Possible values: IP address or DNS name (see [Valid Data Formats](#) 1997 below)
- **Port**
any number
- **SourceIP**
Possible values: IP address or DNS name (see [Valid Data Formats](#) 1997 below)
- **SourcePort**
any number
- **DestinationIP**
Possible values: IP address or DNS name (see [Valid Data Formats](#) 1997 below)
- **DestinationPort**
any number
- **Protocol**
Possible Protocol values: **TCP**, **UDP**, **ICMP**, **OSPF**, **IGMP**, or any number
- **TOS**
Type Of Service (any number)
- **DSCP**
Differentiated Services Code Point (any number)

Additional Fields for Packet Sniffer Sensors Only

- **MAC**
physical address (see [Examples](#) 1997 below)
- **SourceMAC**
physical address
- **DestinationMAC**
physical address
- **EtherType**
Possible EtherType values: **IPv4**, **ARP**, **RARP**, **APPLE**, **AARP**, **IPv6**, **IPX**, **old**, **IPX**, or any number
- **VlanPCP**
IEEE 802.1Q VLAN Priority Code Point

- **VlanID**
IEEE 802.1Q VLAN Identifier
- **TrafficClass**
IPv6 Traffic Class (corresponds to TOS used with IPv4)
- **FlowLabel**
IPv6 Flow Label

Additional Fields for NetFlow v5 and jFlow v5 Sensors Only

- **Interface**
any number
- **ASI**
any number
- **InboundInterface**
any number
- **OutboundInterface**
any number
- **SenderIP**
IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see [Valid Data Formats](#) below)
- **SourceASI**
any number
- **DestinationASI**
any number

Additional Fields for NetFlow v9 and IPFIX Sensors Only

- **Interface**
any number
- **ASI**
any number
- **InboundInterface**
any number
- **OutboundInterface**
any number
- **SenderIP**
IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see [Valid Data Formats](#) below)
- **SourceASI**
any number

- **DestinationASI**
any number
- **MAC**
physical address
- **SourceMAC**
physical address
- **DestinationMAC**
physical address
- **Mask**
"Mask" values represent subnet masks in the form of a single number (number of contiguous bits).
- **DestinationMask**
"Mask" values represent subnet masks in the form of a single number (number of contiguous bits).
- **Next Hop (IP address)**
Possible values: IP address or DNS name (see [Valid Data Formats](#)¹⁹⁹⁷ below)
- **VLAN**
"VLAN" values represent a VLAN identifier (any number).
- **SourceVLAN**
"VLAN" values represent a VLAN identifier (any number).
- **DestinationVLAN**
"VLAN" values represent a VLAN identifier (any number).

Additional Fields for sFlow Sensors Only

- **Interface**
any number
- **InboundInterface**
any number
- **Out boundInterface**
any number
- **SenderIP**
IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see [Valid Data Formats](#)¹⁹⁹⁷ below)
- **MAC**
physical address
- **SourceMAC**
physical address
- **DestinationMAC**
physical address

Valid Data Formats

- IP fields support wildcards (*), range (10-20) and hostmask (/10, /255.255.0.0) syntax, as well as DNS names.
- Number fields support range (80-88) syntax.
- Protocol and EtherType fields support numbers and a list of predefined constants.

For detailed information on IP ranges, please see [Define IP Ranges](#)^[2000] section.

Examples

All of the following filter rules are valid examples:

```
SourceIP[10.0.0.1]
SourceIP[10.*.*.*]
SourceIP[10.0.0.0/10]
DestinationIP[10.0.0.120-130]
DestinationPort[80-88]
Protocol[UDP]
MAC[00-60-50-X0-00-01]
DSCP[46]
```

Complex expressions can be created using parentheses () and the words **and**, **or**, or **and not**. For example, this is a valid filter rule:

```
Protocol[TCP] and not (DestinationIP[10.0.0.1] or SourceIP[10.0.0.120-130])
```

Related Topics

- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)^[1998]
- [Monitoring Bandwidth via Packet Sniffing](#)^[1932]
- [Monitoring Bandwidth via Flows](#)^[1934]

12.4 Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors

When adding Custom xFlow sensors, Custom IPFIX, or Custom Packet Sniffing sensors, you will notice a field entitled **Channel Definition**. In this field you need to provide the channel definitions in the following syntax (one entry per channel):

```
#<id>:<Name>  
<Rule>
```

Syntax

- **<id>** needs to be 1 or greater and must be unique for the sensor (i.e., each channel definition must have a unique ID). **Note:** The maximum channel ID you can use is 2147483648 (2³¹). Higher IDs are not supported. We recommend using channel IDs 1, 2, 3, etc.
- The **<id>** is linked to the historic data: As soon as it has been changed, the history for this particular channel is lost.
- One rule can span multiple lines.
- The next rule starts with a # as first character in a line.
- **<name>** is the channel's display name.
- The rules are processed top to bottom (the number doesn't matter) and the data is accounted to the first match.
- One **Other** channel is added automatically.
- Behind the name a optional [**<unit>**] can be used to override the automatic unit based on the source sensors.

The **<Rule>** syntax is identical to the one described in the [Filter Rules for xFlow and Packet Sniffer Sensors](#) ¹⁹⁹⁴ section. Since data is accounted to the first match, please make sure to start with the most specific rule at the top getting less specific to the bottom.

Note: We recommend writing the rule list in an external editor and paste it into the respective PRTG field. Otherwise, if the rules contain an error, the entries will be removed when adding the rules in case!

Example

General example:

```
#5:HTTP  
Protocol[TCP] and  
(SourcePort[80] or DestinationPort[80] or SourcePort[8080] or  
DestinationPort[8080])
```

Channel definition example for differentiating by protocol:

```
#1:TCP
Protocol[TCP]

#2:UDP
Protocol[UDP]

#3:ICMP
Protocol[ICMP]
```

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#) 1994
- [Monitoring Bandwidth via Packet Sniffing](#) 1932
- [Monitoring Bandwidth via Flows](#) 1934

More

Knowledge Base: Can I add custom channels to standard Packet Sniffer and NetFlow sensors?

- <http://www.paessler.com/knowledgebase/en/topic/2143>

12.5 Define IP Ranges

In some setting fields, you can either enter a host name or single IP address, or you can define IP ranges. PRTG follows a common syntax for this. IP ranges are available, for example, for [xFlow and Packet Sniffer sensors](#)^[291], and for [probes settings](#)^[1821].

Note: For the syntax available for PRTG's automatic network discovery, please see [Auto-Discovery](#)^[192] (**IP Selection Method** setting).

Available Options

Option	Description	Syntax	Example(s)
Simple	Enter a fixed IP address.	a.b.c.d	10.0.10.9
Hostname	Enter a hostname. PRTG will resolve it to an IP address in your network.	hostname	device-xyz
Hostmask	Enter a hostmask. A hostmask defines the relevant bits of the IP address.	a.b.c.d/h or a.b.c.d/e.f.g.h	10.0.0.0/255
Range	Enter an IP address range. Please replace each of a , b , c , d by either * (asterisk) for any value; corresponds to 0-255 —or— x-y for any range between 0 and 255.	a.b.c.d	10.0.0.1-20 or 10.*.0.* or 10.0.0-50.*

12.6 Define Lookups

PRTG uses **lookups** for some sensor types with custom channels. In general, lookups map status values as returned by a device (usually integers) to more informative expressions that show you the status of a monitored device as a clear message. Additionally, lookups can define the [sensor status](#) that will be shown for certain status codes (similar as [sensor channel limits](#) can define a sensor status, too). For example, for a printer, PRTG can show a sensor in a yellow **Warning** status with channel values like "Toner Low" instead of simple status codes.

Lookups can be customized individually; you can define your own texts that will be shown in a sensor's channel. See section [Customizing Lookups](#) below.

Note: If a channel uses lookups, we strongly recommend you to control the sensor status only via the lookup definition and not to use channel limits! See also section [Sensor Channels Settings](#).

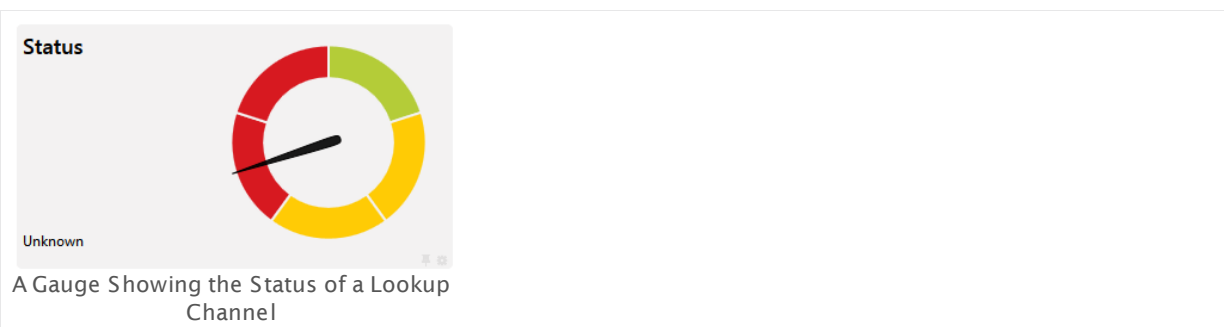
Note: Lookups do not change data in PRTG's database, but they merely change the way sensor channels are shown. Any change to lookup definition files will apply to historic data as well as to live data.

Requirement: Channel Unit "Custom"

All channels with enabled **Value Lookup** need to use the channel Unit **"Custom"**. For details, refer to section [Sensor Channels Settings](#).

Gauges of Lookup Channels

PRTG can display gauges for channels which use lookups. We recommend staying below 120 lookup values in order to display informative gauges for primary channels. Non-primary channels have an upper limit of around 40 lookup values.



Lookups Directory and Format

Lookups are defined in XML format in files ending in **.ovl**. PRTG's standard lookup files are located in the [PRTG program directory](#)^[2036] in a sub folder named **lookups**. These files are maintained by PRTG itself. In each of the files lookups are defined for one or more sensors. Furthermore, the lookups folder contains a sub folder named **custom** to store your customized lookups.

The files follow a basic principle. For each numeric value you can define:

- A message that will be looked up and shown instead of the value
- The status the sensor will show

Example

The following code illustrates the lookup definition for the toner status of the [SNMP HP LaserJet Hardware](#)^[1017] sensor:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="oid.paessler.hp.laserjet.tonerstatus" desiredValue="1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Lookups>
    <SingleInt state="Ok" value="0">
      Toner Okay
    </SingleInt>
    <SingleInt state="Warning" value="1">
      Toner Low
    </SingleInt>
    <SingleInt state="Error" value="2">
      No Toner Cartridge Loaded
    </SingleInt>
  </Lookups>
</ValueLookup>
```

The schema in the example provides an insight how lookups are defined:

- The **<?xml>** tag in the first line defines the content as XML.
- The **<ValueLookup>** tag in the second line contains:
 - The **ID** which will be shown in the [Sensor Channels Settings](#)^[1063].
 - The **desiredValue**^[2007] attribute contains the value which will be used for the calculation of the "Coverage". In this example, 1 is defined.
 - The **xsi** attributes refer to PRTG's predefined XML schema definitions (which allow easy editing of lookup files with supported editors). We recommend using the default value.

- Between the tags **<Lookups>** and **</Lookups>** the particular lookups for the sensor data are defined:
 - A lookup entry starts with a tag containing the type of the status value, the **lookup type** (in this example, this is always **<SingleInt>**).
 - Separated by whitespace, the **state** attribute defines the status the sensor will show. Allowed values are: **Ok**, **Warning**, **Error**, and **None** ("None" will not trigger a status change).
 - The **value** attribute defines which numeric value will trigger the lookup. This is the value that PRTG will receive from the device.
 - The **text** defines the substitution text that will be shown instead of the value. For example, this can be a status message.
- The same way all other possible lookups are defined. The lookup definitions are closed by the tag **</Lookups>**. The file closes with **</ValueLookup>**.

In our example, the lookup file will have the following effect:

Value as Reported from HP Printer	Value Shown in PRTG (Sensor Channel)	Sensor Status Shown by PRTG
0	Toner Okay	Up
1	Toner Low	Warning
2	No Toner Cartridge Loaded	Down

The XML Schema

An overall schema of the XML files containing the lookups definitions can be sketched like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="..." desiredValue="..." xmlns="..." xsi="...">
  <Lookups>
    <SingleInt state="..." value="...">
      status text
    </SingleInt>
    <BitField state="..." value="...">
      status text
    </BitField>
    <Range state="..." from="..." to="...">
      status text
    </Range>

    [several other lookup definitions]

  </Lookups>
</ValueLookup>
```


Element	Description	Attributes, Value Assignment, and Content
<code><?xml></code> <code>content</code>	This is the XML declaration. Every XML file begins with it.	▪ version and encoding are "1.0" resp. "UTF-8" ▪ content: <code><ValueLookup>contentValueLookup</ValueLookup></code>
<code><ValueLookup></code> <code>contentValueLookup</code> <code></ValueLookup></code>	Defines the ID of the channel, what desiredValue is used, and links to PRTG's predefined schema definitions, which allow easy editing of lookup files with supported editors.	▪ id: specifies how the name of the lookup file is shown in the Sensor Channels Settings ▪ desiredValue: please see below ▪ xmlns:xsi/xsi: refers to predefined XML schema definition ▪ contentValueLookup: lookup definitions <code><Lookups>contentLookups</Lookups></code>
<code><Lookups></code> <code>contentLookups</code> <code></Lookups></code>	Defines the particular lookups for the sensor data.	▪ contentLookups: one or more lookup entries, see below
<code><SingleInt></code> <code>status text</code> <code></SingleInt></code> <code><BitField></code> <code>status text</code> <code></BitField></code> <code><Range></code> <code>status text</code> <code></Range></code>	Each element defines one lookup entry. There can be one or more entries in this format. SingleInt , BitField , and Range are lookup types .	▪ state: defines the state the sensor will show; allowed values: Ok, Warning, Error, None ▪ value: defines the value which triggers the lookup. Please enter an integer value. Note: Range needs always both values "from" and "to". ▪ status text: defines a status text that will be used as substitution text and shown instead the integer value. For example, a status message.

Since all the XML files containing lookup definitions are delivered in a pre-given schema as indicated above, it will be easy and comprehensible for you to customize lookups.

Customizing Lookups

There is a subfolder named `\lookups\custom` located in the [PRTG program directory](#)²⁰⁰⁶. In order to customize existing lookups, copy the desired lookup file from the `lookups` folder to the `custom` folder or create a new `.ovl` file there. When using the same ID in the `ValueLookup` tag, the files in the `\lookups\custom` folder will have a higher priority than the original files in the `lookups` folder. This way, your customizations will be handled preferably by PRTG instead of the original lookup settings. If you want to use custom lookup definitions **in addition** to the existing lookups, define a new ID in the lookup file which is not used by another lookup file. PRTG identifies lookup definitions via this ID, it does **not** use the file name.

Open the file with an XML or text editor and adjust the lookups to your personal preferences. You can define your own messages as well as you can customize sensor states for the particular return values. For example, if you do not want an "Error" status (i.e. a sensor **Down** status) for the return value "2" but only a warning, then you can replace "Error" with "Warning".

Note: The possible states are given in the `LookupState.xsd` file in the custom directory. Following the schema of the XML files that are delivered with PRTG enables you to edit the lookups in a safe way.

Example for Lookups Customization

For example (just for illustration purposes), imagine you would like to add the status "None" to the [example](#)²⁰⁰² above and change the status for the return value "2" from "Down" to "Warning". Then do the following:

- Copy the file `oid.paessler.hplaserjet.tonerstatus` to the `\lookups\custom` subfolder of your PRTG installation.
- Open this file with an editor.
- Leave the ID value unchanged to prioritize the customized lookup to the original file.
- Replace "Error" with "Warning" for value "2".
- Add a "SingleInt" element with status "None" for the (hypothetical) return value "3".
- Save the file and [reload](#)²⁰⁰⁸ the custom lookup folder in PRTG.

The customized lookup file will finally look like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="oid.paessler.hplaserjet.tonerstatus" desiredValue="1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Lookups>
    <SingleInt state="Ok" value="0">
      Toner Okay
    </SingleInt>
    <SingleInt state="Warning" value="1">
      Toner Low
    </SingleInt>
    <SingleInt state="Warning" value="2">
      No Toner Cartridge Loaded
    </SingleInt>
    <SingleInt state="None" value="3">
      Unknown status of toner
    </SingleInt>
  </Lookups>
</ValueLookup>
```

desiredValue Attribute

It is necessary to define a **desiredValue** in the lookup files. The **desiredValue** corresponds to a status value triggering a lookup. PRTG calculates the percentage of time this specific state has been monitored. The result is displayed for all data tables and graphs that show averaged values.

Considering the example above where the **desiredValue** is "1", PRTG will calculate the percentage of time the toner status has been "Warning". If in a time span of five minutes four of five sensor scans returned a "Warning" status, PRTG would show an average of 80% for this time span, because in 80% of the time the sensor showed a "Warning".

Lookup Types: SingleInt, BitField, Range

Beside the lookup type **SingleInt** as seen above, there are two other lookup types: **BitField** and **Range**. Using these types you can define lookup values beyond simple integers.

Lookup Type	Description	Syntax
SingleInt	Uses an integer to define a lookup for one status value.	value="int"
BitField	Uses a bit field for multiple status values.	Should only be used if you have basic knowledge about bitmasks. Please see More below for a general introduction. Note: Every value has to equal a power of two (e.g., 1, 2, 4, 8, 16, 32, 64, etc.).
Range	Uses an inter range from-to to define a lookup for several status values.	from="int" to="int" Note: Using ranges, the parameters "from" and "to" always have to be defined. If you want to query only one single value in a range file, this value must be set as parameter for "from" and "to" (e.g., from="2" to="2").

Note: You can use only one kind of lookup type in one lookup file. For example, only **SingleInts**, **BitField**, or **Ranges**. Different lookup types in one file are not allowed.

Define Lookup Files in Sensor Channel Settings

For each sensor with a custom channel you can define a lookup file that will be used. This is done in a sensor's channel settings with an option called "Value Lookup". This option is visible for many **SNMP sensors**, some **application sensors**, and always for the following sensor types:

- [EXE/Script Sensor](#) ⁴³⁰
- [EXE/Script Advanced Sensor](#) ⁴³⁹ (if a **Custom** unit is defined)
- [SNMP Custom Sensor](#) ⁹⁶⁸

For details, please see the [Sensor Channel Settings](#) ¹⁶⁸⁰ section.

Loading Lookups

You can (re)load the defined lookups in the custom folder by clicking the **Load Lookups** button. This button can be found in PRTG under **Set up | System Administration | Administrative Tools** ¹⁸³⁰.

Debugging—What will happen if...?

- A return value is defined in the lookups that never will be returned by a device because the value is not assigned: The value will never be triggered, so PRTG will simply ignore this entry.
- PRTG receives a return value that is not defined for lookups: No substitution message can be found. PRTG will just show the return value.
- Different lookup types are in one lookup file: This is not allowed and PRTG will discard this lookup definition. If you use miscellaneous lookup types in one file, for example, ranges and singleInts together, the PRTG system will create a ticket when loading lookups or restarting the PRTG server with the following error message: **Value lookup file "[...]" could not be loaded (" " is not a valid integer value)**.
- Incorrect XML code: PRTG will create a new ticket when loading lookups or restarting the PRTG server with a corresponding error message and discard this lookups definition.

More

Wikipedia: Masks (computing)

- http://en.wikipedia.org/wiki/Bit_mask

12.7 Regular Expressions

For some sensors, you can use regular expressions to match a search pattern. PRTG will use PCRE-RegExp. In the following, we will provide examples for the most common patterns.

Common Search Patterns

Find matches containing the word **error** or **alarm**:

```
\b(error|alarm)\b
```

Find matches containing the words **error** and **alarm** in any order:

```
(?=.*\berror\b)(?=.*\balarm\b).*
```

Find matches containing all of the words **t**ree, **f**lower, **l**ea**f**, and **b**ug, in any order:

```
(?=.*\btree\b)(?=.*\bflower\b)(?=.*\bleaf\b)(?=.*\bbug\b).*
```

Example

The search pattern

```
(?=.*\berror\b)(?=.*\balarm\b).*
```

will match the following expressions:

- alarm error
- error alarm
- I am an error and I evoke an alarm
- I am an alarm and I indicate an error
- An alarm combined with an error indeed!
- An error combined with an alarm, too!

More

Regex Tester: Test Regular expressions interactively

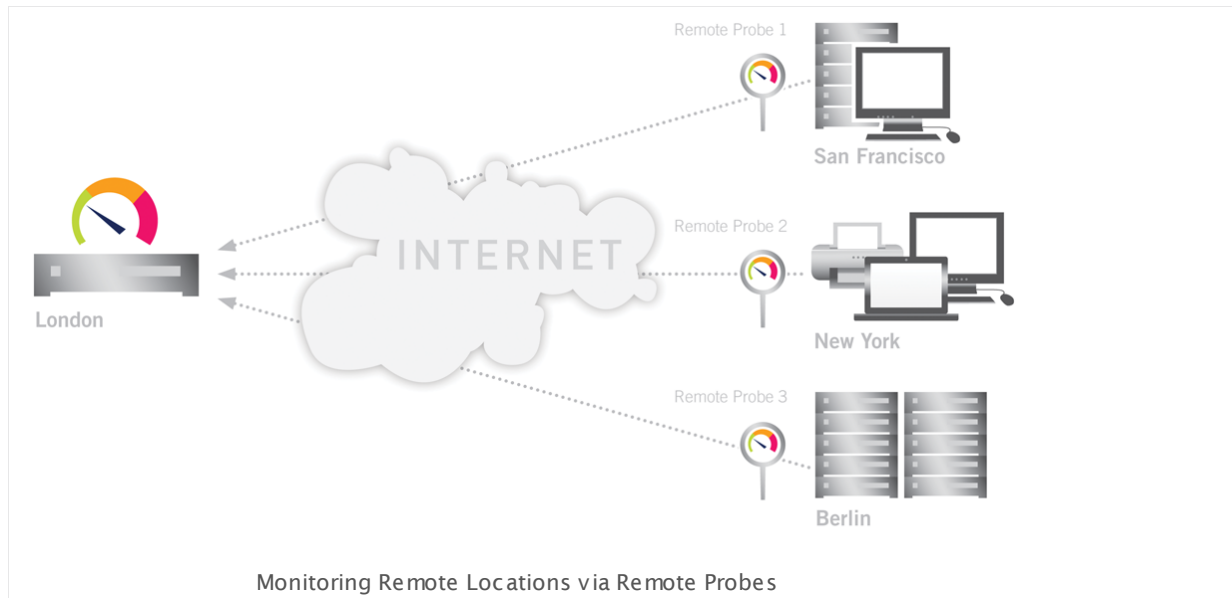
- <http://www.regexpal.com>

Wikipedia: Regular expression

- http://en.wikipedia.org/wiki/Regular_expression

12.8 Add Remote Probe

To monitor different sub-networks that are separated by a firewall, to keep an eye on remote locations, or for several other scenarios, you can extend your monitoring by installing one or more **Remote Probes**.



Extend Your Monitoring Now

Installing remote probes is easy and done in a few minutes. Please see the sections linked below for further instructions.

- Background: [Remote Probes and Multiple Probes](#) 2012
- Installing: [Remote Probe Quick Install](#) 2015
- Step by Step: [Remote Probe Set up](#) 2020

More

Video Tutorial: Core Server and Remote Probes

- http://www.paessler.com/support/video_tutorials/distributed_monitoring

12.8.1 Remote Probes and Multiple Probes

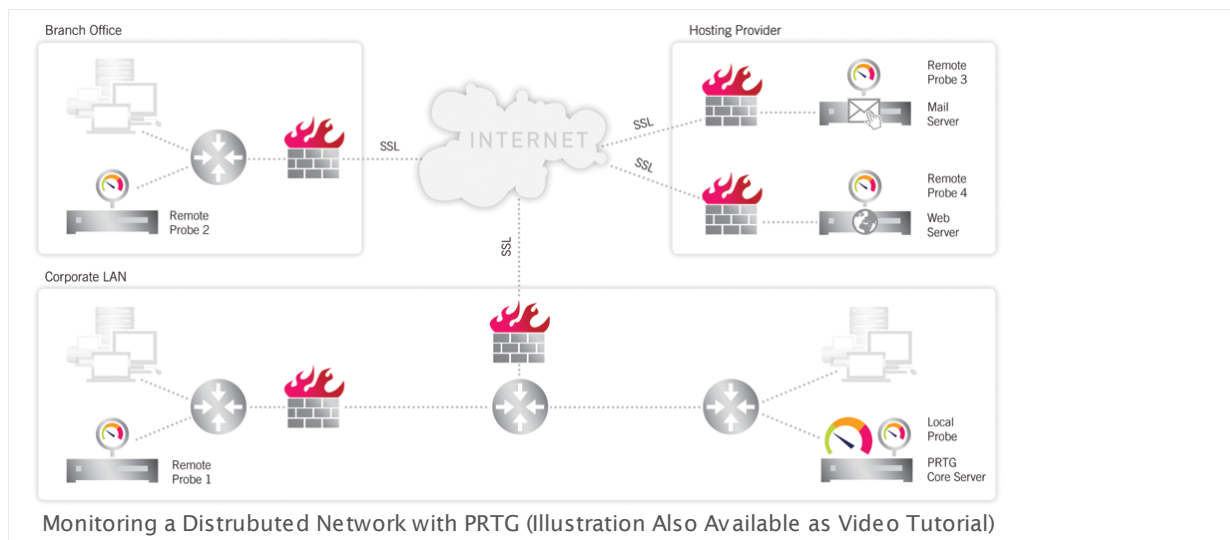
Upon installation, PRTG creates the first probe automatically, called the **Local Probe**. It runs on the same machine as the PRTG core server and monitors all devices from this system, using the sensors you have configured. Working with only one local probe should suffice for Local Area Network (LAN) monitoring and if you want to monitor one location only.

Scenarios Requiring Remote Probes

However, there are several situations making it necessary to work with **Remote Probes** in the same LAN or in remote locations. Among these situations are the following:

- You have more than one location and you need to make sure that services are available from all locations.
- Your network is separated in several LANs by firewalls, and the local probe cannot monitor specific services across the firewalls.
- You need to monitor systems in a Virtual Private Network (VPN) across public or in-secure data lines.
- You want to sniff packets on another computer.
- You want to monitor NetFlow data on another computer.
- You experience performance issues with CPU intensive sensors like packet sniffer or NetFlow sensors and need to distribute the load over more than one PC.

The following chart shows an example for a remote probe scenario.



The PRTG core server inside the **Corporate LAN** (bottom right) is able to monitor:

- Services inside the **Corporate LAN** using the **Local Probe**.
- Services behind a firewall in the **Corporate LAN** using **Remote Probe 1**.
- Secured services inside the **Branch Office** (top left) using **Remote Probe 2**.

- Secured services on **Mail Server** and **Web Server** using **Remote Probe 3** and **Remote Probe 4** installed directly on these servers.
- Public services on the internet using any of the probes.

How Probes Work

As soon as a probe is started, it automatically connects to its [core server](#)^[78], downloads the sensor configuration, and begins its monitoring tasks. The core server sends new configuration data to a probe as soon as the monitoring configuration is changed by the user. Probes monitor autonomously and send the monitoring results back to the core server for each check they have performed.

If the connections between core and probe fails for any reason (for example, a reboot of the computer running the core server) the probe continues its monitoring and stores the results. During a connection loss a buffer stores a maximum of 500,000 sensor results in RAM memory of the remote probe system (up to 50 - 200 MB). This means that for 100 sensors with one minute interval the monitoring results of up to 3 days can be buffered (or 52 minutes for 10,000 sensors with one minute interval). The probe automatically reconnects to the core as soon as it is available again and transmits all monitoring results gathered during the connection loss.

The connection between probe and core is initiated by the probe, secured using Secure Sockets Layer (SSL). This means that the data sent back and forth between core and probe is not visible to someone capturing data packets. The core server provides an open TCP/IP port and waits for connection attempts from probes. If a new probe connects for the first time, the administrator will receive a **ToDo** [ticket](#)^[148] and will then see the new probe in the device tree.

As a security precaution, the probe must be manually acknowledged by the administrator in the device tree before any sensors can be created and monitored. The administrator can also deny a probe which will then be disconnected. No further connection attempts will be accepted and the probe IP is added to the **Deny IPs** list in the probes system settings (see [System Administration—Probes](#)^[182] section). This ensures that unauthorized probes cannot connect to a core server.

Because the probe initiates the connection, you must ensure that a connection can be established from the outside world onto your core server. For example, you may need to open any necessary ports in your firewall and you may need to specify a Network Address Translation (NAT) rule for your network. The process is the same as if you wanted to allow access to the web server provided by the PRTG core server via port 443, for example. Usually it is sufficient to open or forward TCP port **23560** (default) on the machine that runs the core server; on probe side it is **not** necessary to open any port in most cases.

Automatic Probe Update

Whenever a new version of PRTG is installed on the core server, all remote probes will automatically download and install the updated version of the probe as soon as they reconnect to the updated core installation.

The local probe has already been updated during the core installation. All remote probes are automatically downloading the new binaries using the SSL-secured probe/core connection. The download of the 4 MB file takes between a few seconds (in a LAN) and a few minutes (via internet connections), depending on the available bandwidth. As soon as the update has been downloaded the probe disconnects, installs the update and reconnects to the core server. This takes between 20 and 100 seconds. Please note that during the update phase the monitoring of the local probe can be affected due to the bandwidth required for the downloads.

More

- [Remote Probe Quick Install](#)  2015
- [Remote Probe Setup](#)  2020

Video Tutorial: There is a video available on the Paessler video tutorials page.

- http://www.paessler.com/support/video_tutorials

12.8.2 Remote Probe Quick Setup

PRTG provides an easy, semi-automatic install mechanism for a new Remote Probe. You can perform a remote installation of a probe directly in PRTG's web interface by right-clicking on a device in the PRTG device tree. **Note:** This is an experimental feature. It is possible that direct installation does not work in all situations. In this case, please see [Debugging](#)^[2019] and [Remote Probe Setup Using Installer](#)^[2020].

In order to install a Remote Probe directly from the web interface, follow the steps below:

- [Step 1: Meeting Requirements](#)^[2015]
- [Step 2: Preparing Core Server](#)^[2015]
- [Step 3: Providing Credentials](#)^[2017]
- [Step 4: Installing Remote Probe](#)^[2017]
- [Step 5: Approving New Remote Probe](#)^[2018]

Please look carefully at the requirements in the first three steps.

Step 1: Meeting Requirements

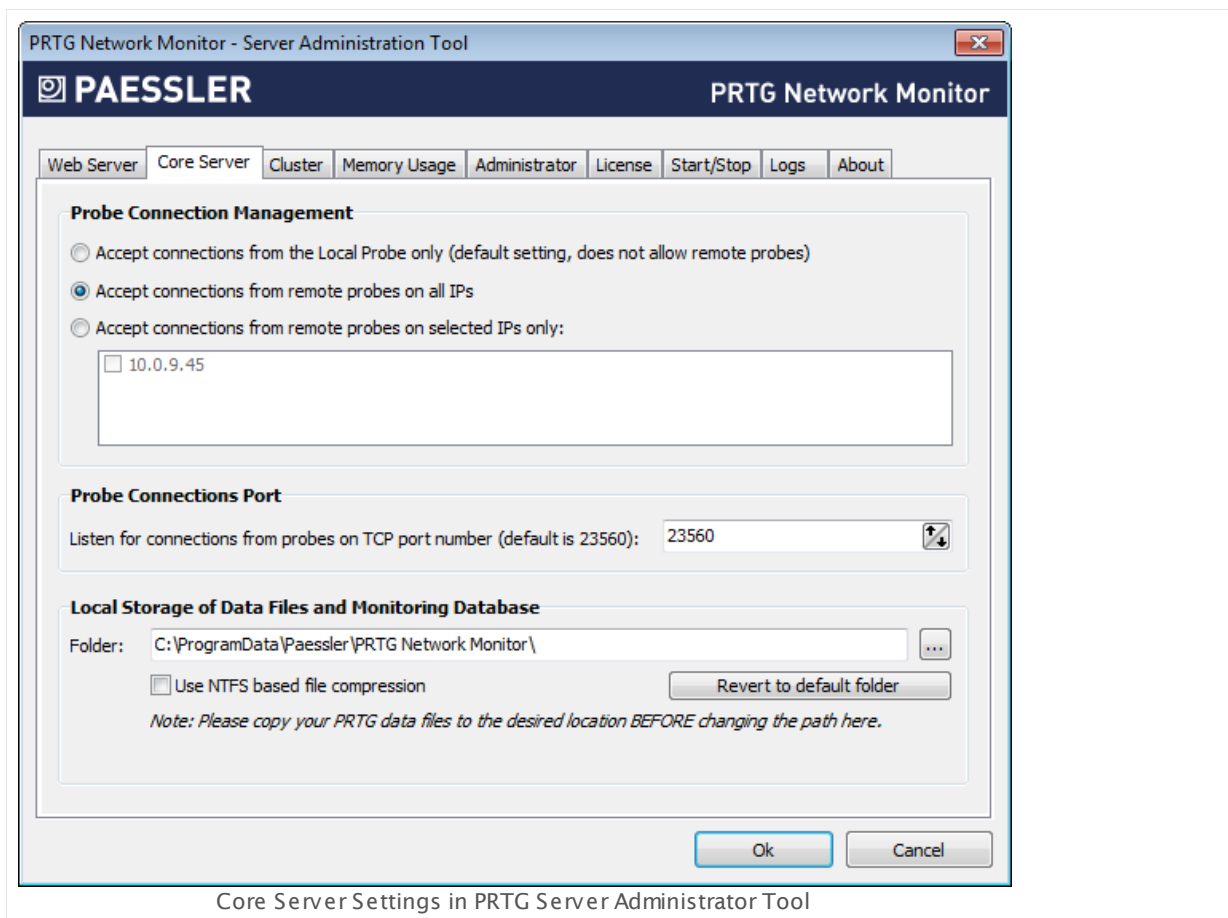
There are some conditions which have to be met in order to install a probe remotely on another computer. Please ensure the following:

- The target computer must be running with operating system Windows (XP or later).
- The target computer must be accessible through Remote Procedure Call (RPC). This is usually the case when your PRTG server and the target computer are located in the same LAN segment. Otherwise, open Windows **services.msc** on the target computer. Start the Remote Procedure Call (RPC) service.
- You cannot install a remote probe on a probe device.
- You have to permit programs to communicate through your Windows Firewall. Open the settings of your Firewall and choose **Allow programs to communicate through Windows Firewall**. Mark the checkbox for **Remote Service Management**, and the checkbox **Public** in the corresponding line.
- You cannot install a remote probe on the computer where PRTG's Core Server runs.
- The IP address setting for probe connections to the core server must not be **127.0.0.1**. Please see [Step 2](#)^[2015] how to prepare the **Core Server**.

Step 2: Preparing Core Server

Before remote probes can connect to the core server, you have to edit the relevant settings in the [PRTG Server Administrator](#)^[1959].

Part 12: Advanced Topics | 8 Add Remote Probe
2 Remote Probe Quick Setup



Core Server Settings in PRTG Server Administrator Tool

By default, a core server accepts connections **from the Local Probe only** (this is, IP address **127.0.0.1**). This setting does not allow for remote probes. It is the most secure setting. In order to allow external probes to connect, please change to the **Core Server** tab, and in the **Probe Connection Management** section, choose one of the following options:

- **Accept connections from remote probes on all IPs:** We recommend using this setting for easy setup (this is, IP address **0.0.0.0**).
- **Accept connections from remote probes on selected IPs only:** Specify the IP addresses that will accept incoming connections.
- As **Probe Connections Port**, you can leave the standard port number, even when configuring several probes. Please make sure this port is not blocked by firewall rules on your core server's side.

When you are done, click **OK** to save your settings. The core server process must be restarted so that the changes take effect.

For detailed information about these settings, please see [PRTG Server Administrator](#) ¹⁹⁰² (**Core Server**) section.

Step 3: Providing Credentials

If not done yet, [add a device](#)^[272] to PRTG that represents the target computer where you want to install the remote probe on. You have to set the correct Windows credentials for this device.

- Open the [Device Settings](#)^[272].
- In the **Credentials for Windows Systems** section, provide **Domain or Computer Name**, **Username**, and **Password** for the target computer.
- You can also [inherit](#)^[87] the credentials from its parents' settings.

Please make sure that this user account has administration rights on the target computer.

Step 4: Installing Remote Probe

- In the device tree overview, open the [context menu](#)^[167] of the target device.
- Choose **Device Tools > Install Remote Probe....**
- The install assistant will appear on a new page.

PRTG Network Monitor

Home Devices Libraries Sensors Alarms Maps Reports Logs ToDos Setup

Devices > Install Remote Probe on Device

Install Remote Probe on Device Example Device

Please note: This is an experimental feature, it may not work in all possible situations. Please send your feedback to support@paessler.com.

You are about to install a Remote Probe of PRTG on the computer "Example Device". This will allow PRTG to monitor this computer locally instead of using remote monitoring features which can sometimes be a good workaround for performance or authentication problems (e.g. for WMI sensors). Additionally this will allow you to use some probe-only sensors like Packet Sniffing, xFlow/NetFlow and others.

Details	
Device Name	Example Device (example.com)
Status	OK
Priority	★★★★☆
Parent Probe	Local probe (Local Probe on 127.0.0.1)
Parent Group	User Group home
Sensors by State	(Total: 0)

Prerequisites

Please make sure the following conditions are met:

- The target computer must be a Windows PC (Windows XP or later).
- The target computer must be accessible through RPC (this is usually the case when your PRTG server and the target computer are located in the same LAN segment).
- Windows credentials must be set in the device settings or its parents' settings (Current user name: examplecom\johnpublic) and the user account must have administration rights on the target machine.
- IP address setting for probe connections to the core server must not be 127.0.0.1 (Current setting: 0.0.0.0). You can change this setting in the Core Server Administrator.

Start Probe Installation

The installation will take between 10 and 100 seconds.

Install Remote Probe on "Example Device"

Remote Probe Install Assistant

Part 12: Advanced Topics | 8 Add Remote Probe

2 Remote Probe Quick Setup

The install assistant is divided into four sections:

- Experimental feature notice and short introduction
- **Details:** overview about the device, this is, name, status, priority, parent probe, parent group, and sensor states in place with their number
- **Prerequisites:** for details, see [Step 1](#) ²⁰¹⁵
- **Start Probe Installation:** time estimation for installation and installation start button

If prerequisites are not met, you cannot start the installation process. Open requirements will be highlighted in red. Please correct these to continue!

Prerequisites

Please make sure the following conditions are met:

- The target computer must be a Windows PC (Windows XP or later).
- The target computer must be accessible through RPC (this is usually the case when your PRTG server and the target computer are located in the same LAN segment).
- You can not install a remote probe on a probe device.
- **Please correct before proceeding: Windows credentials must be set in the device settings or its parents' settings (Current user name: \) and the user account must have administration rights on the target machine.**
- IP address setting for probe connections to the core server must not be 127.0.0.1 (Current setting: 0.0.0.0). You can change this setting in the Core Server Administrator.

Start Probe Installation

Sorry, you can not continue. Please correct the highlighted items above!

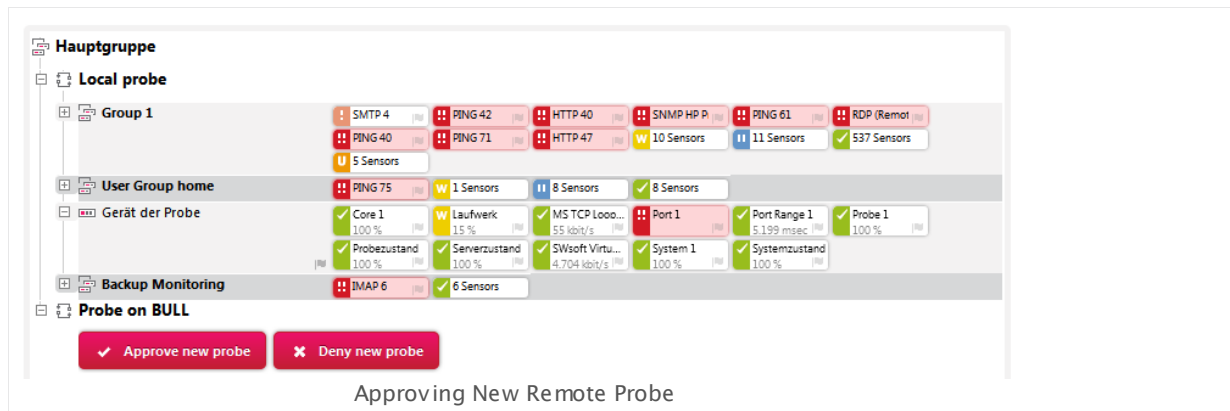
Installation Unable to Start due to Unmet Prerequisites

If all prerequisites are met, you can install the remote probe on the target computer by clicking the button **Install Remote Probe on "[device name]"**. Wait until the process has ended. If installation was successful, the following message will appear in the **Start Probe Installation** section: **Done. Result is: OK.**

Note: Every time you start an installation, no matter if it is successful or not, a key will be added automatically to **Access keys** in [Probes Settings](#) ¹⁸²¹.

Step 5: Approving New Remote Probe

If installation was successful, further instructions are given after the result message. As indicated, go back to the [device tree](#) ¹⁰⁹ and acknowledge the new probe. The approval button will appear at the bottom of the devices list. You will also get a new [ToDo ticket](#) ¹⁴⁹.



Click on **Approve new probe** to acknowledge the created remote probe. You can also discard the new probe by clicking **Deny new probe**.

Note: When denying or removing a remote probe, this device's global ID (GID) will be entered to **Deny GIDs** in [Probes Settings](#).

Note: Denying the remote probe in the PRTG device tree does **not** uninstall the probe, but only denies access to the core server. The probe will continue to run on the target system until you uninstall it manually.

After approving, the approval button will turn into a **Working** status. Please wait while the probe connects. Once approved, PRTG automatically creates a set of sensors for the probe to ensure that bottle-necks on the probe will always be noticed. We recommend keeping these sensors. You are able now to create groups, devices and sensors for monitoring via the new probe.

Debugging

Please be aware that installing a remote probe from PRTG's web interface is an experimental feature. Thus, it can be the case that this approach is not possible in all situations.

However, please follow the steps of this chapter closely when encountering problems with the Remote Probe Quick Install. Especially consider the conditions as described in [Step 1](#) of this chapter like Windows Firewall settings.

If the quick installation procedure described in this section does not work with your setup, please install your remote probes manually; see section [Remote Probe Setup Using Installer](#).

12.8.3 Remote Probe Setup Using Installer

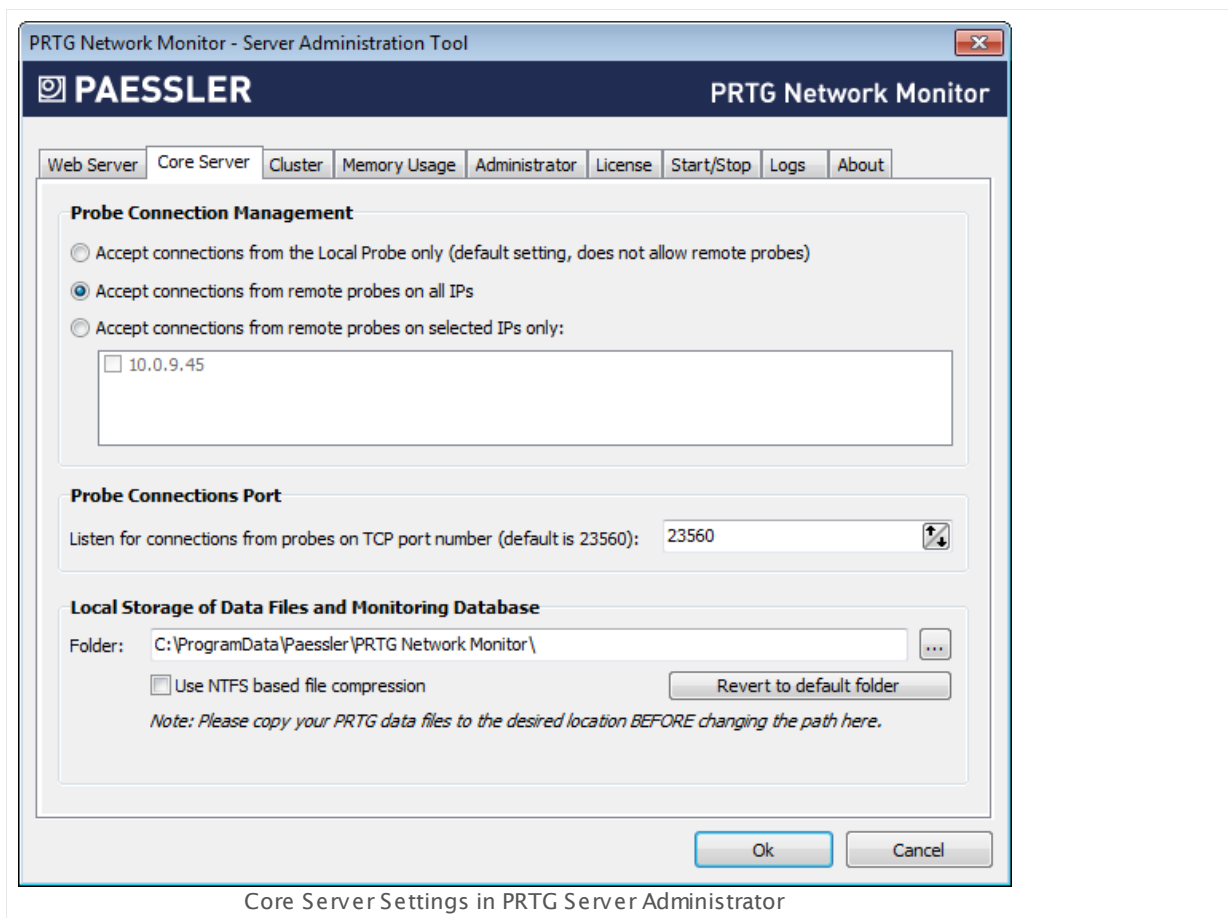
This section will guide you through the steps to set up a remote probe using the **Remote Probe Installer**. For a semi-automatic installation of a Remote Probe directly from PRTG's web interface, see section [Remote Probe Quick Setup](#)²⁰¹⁵.

- [Step 1: Prepare Core Server](#)²⁰²⁰
- [Step 2: Settings in Web Interface](#)²⁰²²
- [Step 3: Download and Install Remote Probe](#)²⁰²²
- [Step 4: Configure Remote Probe Connection](#)²⁰²³
- [Step 5: Approve New Probe and Start Monitoring](#)²⁰²⁴
- [Debugging Probe Connection Problems](#)²⁰²⁴

There are preparations to do on the core server, so it accepts incoming remote probe connections. Then you log in to the computer you want to install the remote probe on, download the installer from your PRTG web interface, and install it.

Step 1: Prepare Core Server

Before remote probes can connect to the core server you must edit the relevant settings in the [PRTG Server Administrator](#)¹⁹⁶².



By default, a core server accepts connections **from the Local Probe only**. This setting does not allow remote probes, which is the most secure setting. In order to allow external probes to connect, please change to the **Core Server** tab, and in the **Probe Connection Management** section, choose one of the following options:

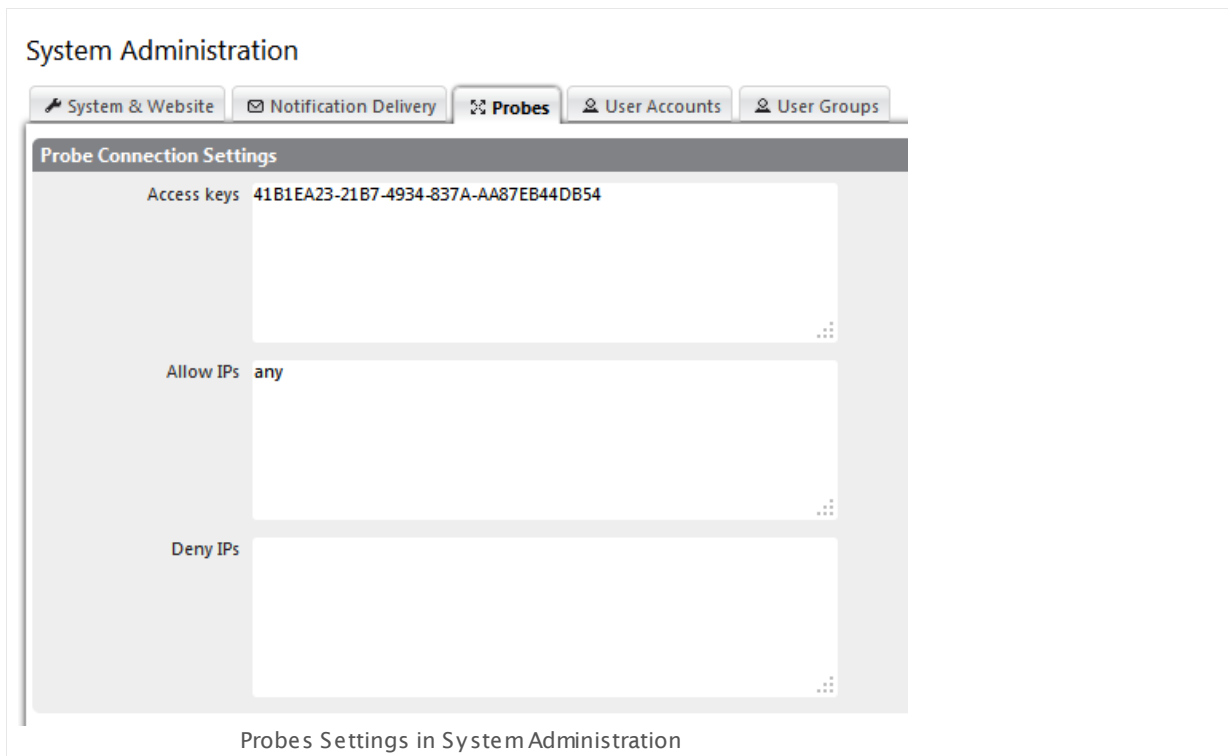
- **Accept connections from remote probes on all IPs:** We recommend using this setting for easy setup.
- **Accept connections from remote probes on selected IPs only:** Specify the IP addresses that will accept incoming connections.
- As **Probe Connections Port**, you can leave the standard port number, even when configuring several probes. Please make sure this port is not blocked by firewall rules on your core server's side. You have to configure the same port number in your remote probe's settings, so please save it for later use.

When you are done, click **OK** to save your settings. The core server process must be restarted so that the changes take effect.

For detailed information about these settings, please see [PRTG Server Administrator](#) ¹⁹⁶² (Core Server) section.

Step 2: Settings in Web Interface

Login to the [Ajax web interface](#)^[102]. From the main menu, select **Setup | System Administration | Probes** to access the probes settings.



- From the **Access keys** field, copy one access key you will use for the remote probe connection. You can also enter a new access key with arbitrary signs and length if you like. In any case save the correct access key for later use.
- In the **Allow IPs** field, enter the IP address of the computer you will install a remote probe on. To make things easier, you can also enter the word **any**; this will set the core server to accept remote probes connecting from any IP address. **Note:** If you use **any**, please make sure you write the word in lower case only! Any other variations will not be recognized!
- Make sure the IP address of the computer you will install a remote probe on is not listed in the **Deny IPs** field.

For detailed information about these settings, please see [System Administration—Probes](#)^[1821] section.

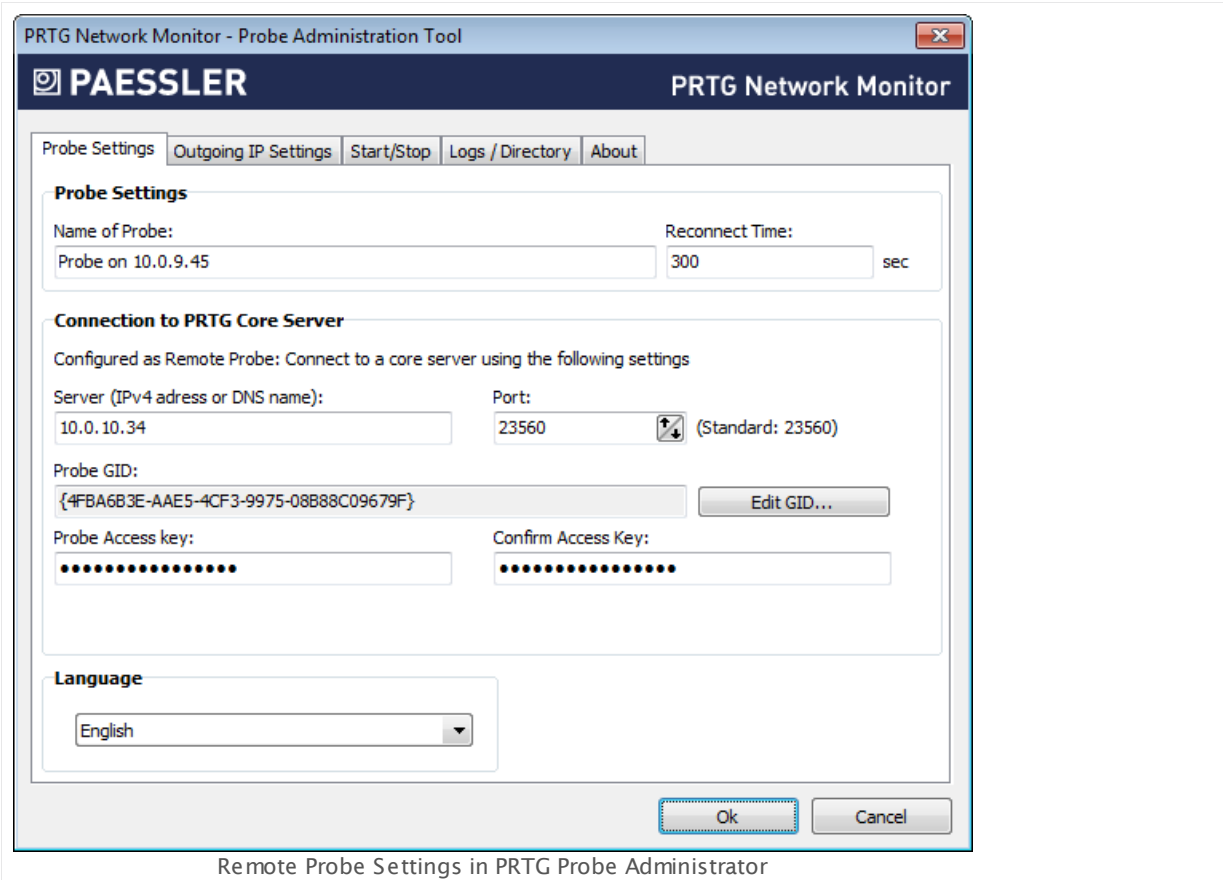
Step 3: Download and Install Remote Probe

From the computer you want to install a remote probe on, connect to the [Ajax web interface](#)^[102], download the setup file and install it. For detailed instructions, please see [Install a PRTG Remote Probe](#)^[62] section. **Note:** You cannot install a remote probe on a system already running a PRTG core installation.

At the end of the remote probe installation the **PRTG Probe Administrator** will be started (or you can start it manually from the Windows start menu later).

Step 4: Configure Remote Probe Connection

In the [PRTG Probe Administrator](#) ¹⁹⁷⁹ on the Windows system you have installed the remote probe on, please configure the connection to the core server.



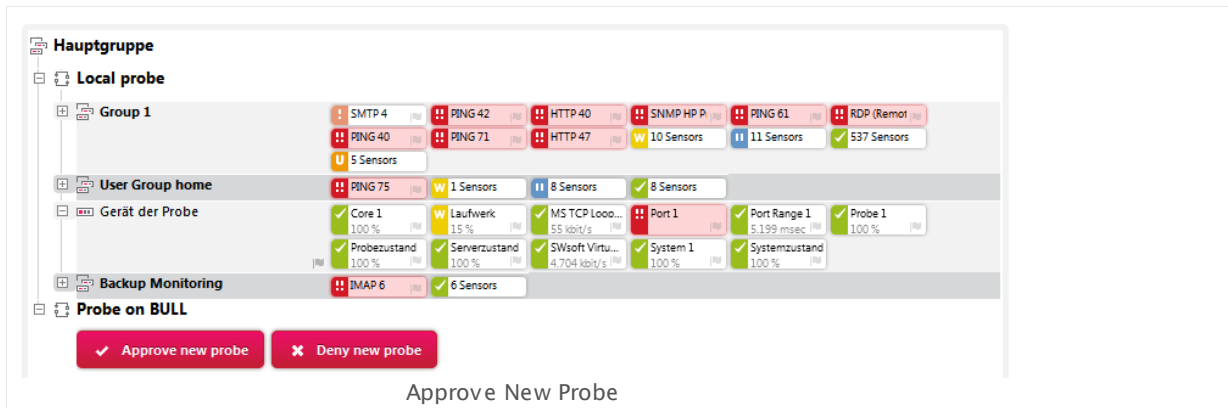
In the **Connection to PRTG Core Server** section, you can then edit the following settings:

- **Server:** Enter the IP address or DNS name of the core server the remote probe will connect to. If Network Address Translation (NAT) is used, this must be the IP address that is externally visible, as the remote probe will connect from outside of your network.
- **Port:** Enter the port number the remote probe will connect to on the core server. This number must match the one set in [Step 1](#) ²⁰²⁰.
- **Probe Access Key** and **Confirm Access Key:** Enter the access key the probe will send to the core server. You have saved this key in [Step 2](#) ²⁰²². This key has to match exactly the one shown in the web interface's probes settings, so a connection can be established.

For detailed information about these settings, please see [PRTG Probe Administrator](#) ¹⁹⁷⁹ section. Click the **Ok** button to confirm your settings and to start the probe service.

Step 5: Approve New Probe and Start Monitoring

When a new probe connects to the core server for the first time, a new [ToDo ticket](#)¹⁴⁹ will be created and the probe will show up as a new object in the device tree of your setup.



Please click on **Approve new probe** to fully enable the probe. You have to do this once for every new probe. Once approved, PRTG automatically creates a set of sensors for the probe to ensure that bottle-necks on the probe will always be noticed. We recommend keeping these sensors. You can now create groups, devices and sensors for monitoring via the new probe.

You can also discard the new probe by clicking **Deny new probe**.

Note: When denying or removing a remote probe, this device's global ID (GID) will be entered to **Deny GIDs** in [Probes Settings](#)¹⁸²¹.

Note: Denying the remote probe in the PRTG device tree does **not** uninstall the probe, but only denies access to the core server. The probe will continue to run on the target system until you uninstall it manually.

Debugging Probe Connection Problems

If you have trouble with the setup of remote probes please look at the probe's log files.

The probe process writes log files with a file name in the format **PRTG Probe Log (x).log**. Please open the one with the most recent date.

For a correct connection the probe log should look similar to this:

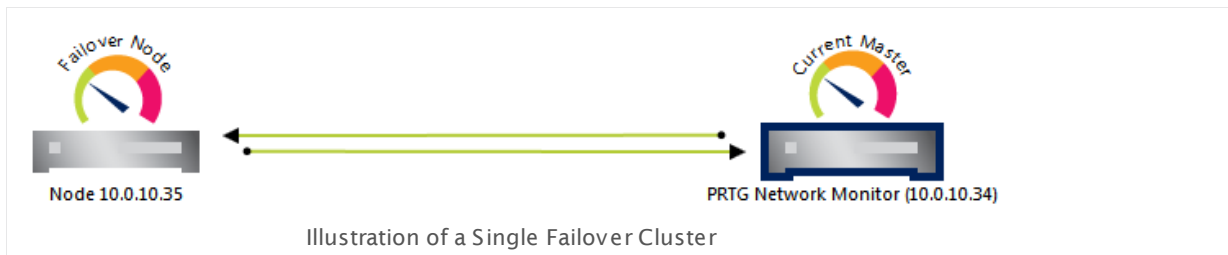
```
11.08.2012 16:15:15 PRTG Probe Server V12.3.2.5101
11.08.2012 16:15:15 Starting Probe on "WINXPVMWARE"
11.08.2012 16:15:15 Data Path: C:\documents and settings\All Users\A[...]
11.08.2012 16:15:15 Local IP: 0.0.0.0
11.08.2012 16:15:15 Core Server IP and Port: 10.0.2.167:23560
11.08.2012 16:15:15 Probe ID: -1
11.08.2012 16:17:01 Connected to 10.0.2.167:23560
11.08.2012 16:17:06 Login OK: Welcome to PRTG
```

If the connection fails, for example, due to an incorrect **Access Key**, or due to incorrect **IP** settings (see [Step 2](#) ²⁰²²), you will see:

```
11.08.2012 16:31:02 Try to connect...
11.08.2012 16:31:02 Connected to 10.0.2.167:23560
11.08.2012 16:31:07 Login NOT OK: Access key not correct!
```

12.9 Failover Cluster Configuration

PRTG offers single failover clustering in all licenses—even using the freeware edition. A single failover cluster consists of two servers ("Current Master" Node and "Failover Node"), each of them running one installation of PRTG. They are connected to each other and exchange configuration and monitoring data.



For setting up a cluster you need two or more servers and there is one [core installation](#)^[51] necessary on each of them—with different settings configured for each type of node. In return, you benefit from seamless high-available monitoring with automatic failover and/or multi-location monitoring.

In a cluster, you can run:

- **1 Master Node**
On the master node, you set up your devices and configuration. Also notifications, reporting, and many other things are handled by the master node.
- **Up to 4 Failover Nodes**
You can install one, two, three, or four additional nodes for fail-safe, gapless monitoring. Each of these nodes can monitor the devices in your network independently, collecting their own monitoring data. The data can be reviewed in a summarized way, enabling you to compare monitoring data from different nodes.

Note: During an outage of one node, you will see data gaps for the time of the outage on that node. However, data for that time span will still be available on all other cluster nodes.

Before Getting Started

Configuring a cluster with one failover node is the most common way to set up a seamless network monitoring with PRTG. You will need two servers running any Windows version (XP/2003 or later); your servers can be real hardware (**recommended!**) or virtual machines.

Please make sure the following:

- Your servers must be up and running.
- Your servers must be similar in regard to the system performance and speed (CPU, RAM memory, etc.).

- In a cluster setup, each of the cluster nodes will individually monitor the devices added to the **Cluster Probe**. This means that monitoring load will increase with every cluster node. Please make sure your devices and network can handle these additional requests. Often, a larger scanning interval for your entire monitoring is a good idea. For example, you could set a scanning interval of 5 minutes in the [Root Group Settings](#)²²⁴.
- We recommend installing PRTG on dedicated real-hardware systems for best performance.
- Please bear in mind that a server running a cluster node may in rare cases be rebooted automatically without notice (e.g. for special software updates).
- Both servers must be visible for each other through the network.
- Communication between the two servers must be possible in **both directions**. Please make sure that no software- or hardware firewall is blocking communication. All communication between nodes in the cluster is directed through one specific TCP port. You will define it during cluster setup (by default, it is **TCP port 23570**).
- A Failover Master will send notifications in case the Primary Master is not connected to the cluster. In order for mails to be delivered in this case, please make sure you configure the [Notification Delivery](#)¹⁸¹⁵ settings in a way they can be used to deliver emails from your Failover Node as well (for example, using the option to set up a secondary Simple Mail Transfer Protocol (SMTP) server).
- Make your servers safe! From every cluster node, there is full access to all stored credentials as well as other configuration data and the monitoring results of the cluster. Also, PRTG software updates can be deployed through every node. So, please make sure you take security precautions to avoid security attacks (hackers, Trojans, etc.) You should secure every node server the same careful way as the master node server.
- Run the nodes in your cluster either on 32-bit or 64-bit Windows versions only. Avoid using both 32-bit and 64-bit versions in the same cluster, as this configuration is not supported and may result in an unstable system. Also, ZIP compression for the cluster communication will be disabled and you may encounter higher network traffic between your cluster nodes.
- If you run cluster nodes on Windows systems with different timezone settings and use [Schedules](#)¹⁸⁰¹ to pause monitoring of defined sensors, schedules will apply **at the local time of each node**. Because of this, the overall status of a particular sensor will be shown as **Paused** every time the schedule matches a node's local system time. Please use the same timezone setting on each Windows with a cluster node in order to avoid this behavior.

Start Now!

Ready to get started? Please go to [Failover Cluster Step by Step](#)²⁰²⁹!

More

Knowledge Base: What's the Clustering Feature in PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/6403>

Knowledge Base: What are the bandwidth requirements for running a PRTG Cluster?

- <http://www.paessler.com/knowledgebase/en/topic/8223>

Knowledge Base: What is a Failover Master and how does it behave?

- <http://www.paessler.com/knowledgebase/en/topic/7663>

Knowledge Base: I need help with my PRTG cluster configuration. Where do I find step-by-step instructions?

- <http://www.paessler.com/knowledgebase/en/topic/41913>

Knowledge Base: PRTG Cluster: How do I convert a (temporary) Failover Master node to be the Primary Master node?

- <http://www.paessler.com/knowledgebase/en/topic/34853>

12.9.1 Failover Cluster Step by Step

This section will guide you through a step-by-step process to set up a failover cluster. Please follow these instructions carefully, in order to successfully integrate two or more PRTG installations into one failover cluster.

Note: Before getting started, please make sure you've read the information in section [Failover Cluster Configuration](#) .

Step 1: Install Core Servers

We will start with setting up a single failover cluster, consisting of two PRTG core server installations, each running on an individual server. Please use your license key twice to install the PRTG core server on two different computers.

If you already run an installation of PRTG, this will be your future Master Node. In this case, please install a second core server on another computer only. Make sure you use the same license key for both installations.

Before you begin to set up a cluster, please make sure you run exactly the same PRTG version (build number) on all (future) nodes (install updates for existing installations, if necessary).

Note: Once the cluster is established, any updates you install on one node will be deployed to all other cluster nodes automatically.

For details about the installation process, please see [Install a PRTG Core Server](#) .

Step 2: Configure Master Node

Decide which of your PRTG core server installations will be your future Master Node. If you already run an installation of PRTG in your network for some time, this should be your master, so your existing monitoring configuration is being kept.

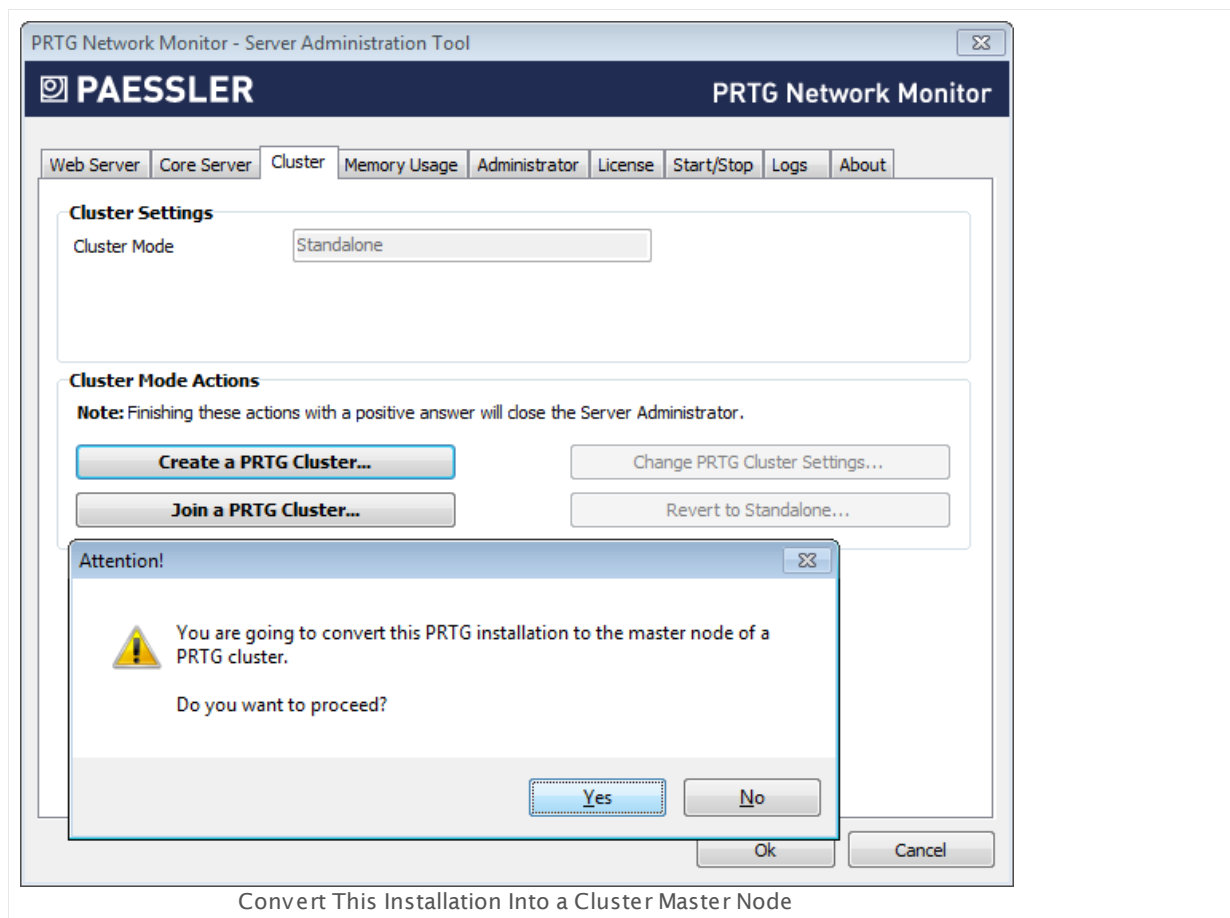
On the Master Node server, from the Start menu, open the [PRTG Server Administrator](#)  program. In the Cluster tab, click on the following button:

Create a PRTG Cluster...

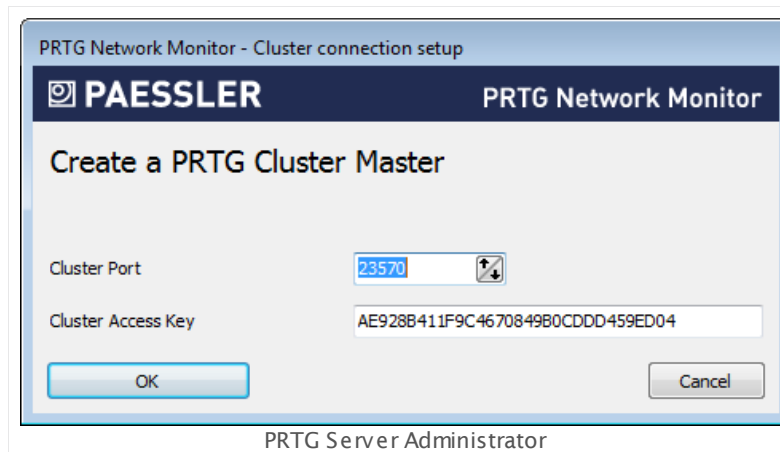
- Start creating a cluster by clicking this button. The current PRTG core server will then be the **Master Node** of your cluster.
- After you click this button, please confirm converting this installation into a master node by clicking on the **Yes** button.

Part 12: Advanced Topics | 9 Failover Cluster Configuration

1 Failover Cluster Step by Step



- A new popup window will appear.



- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.

- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- We recommend using the default value.
- Save the **Cluster Access Key** so you have it at hand when configuring your Failover Node(s).
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

Step 3: Configure Failover Node

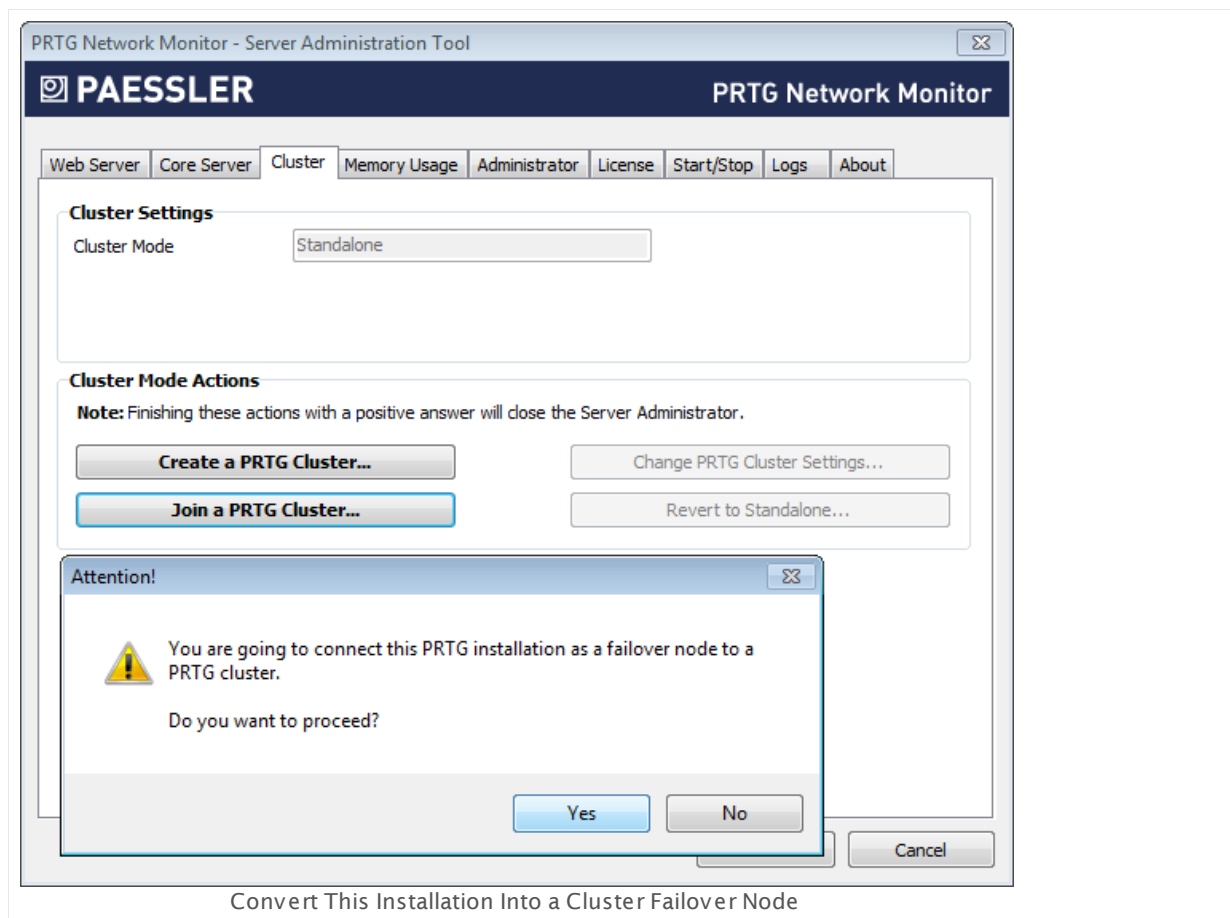
On the server that will be your Failover Node, from the Start menu, open the [PRTG Server Administrator](#)  program. In the Cluster tab, click on the following button:

Join a PRTG Cluster...

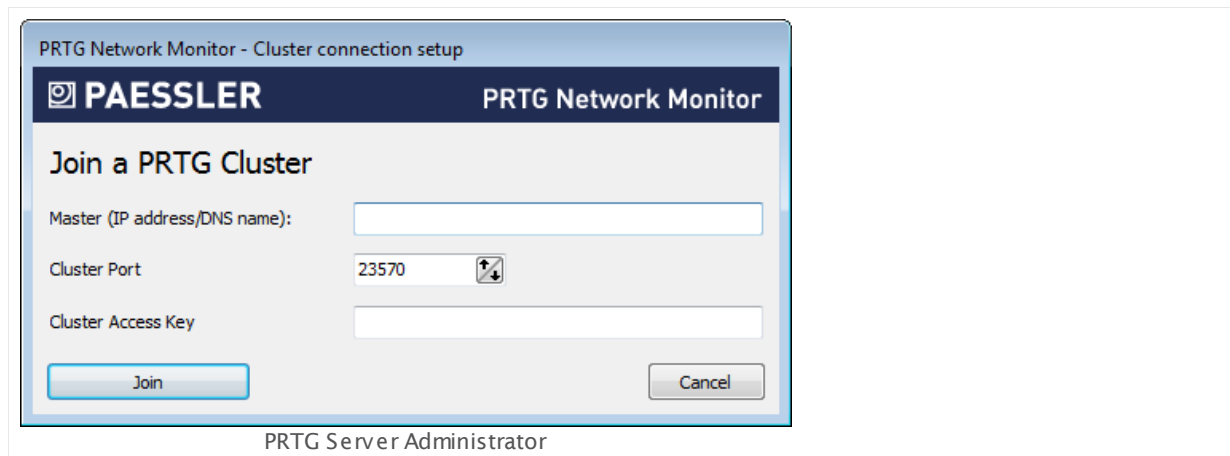
- Add this installation to an existing cluster which already has a **Master Node**, by clicking this button. The current PRTG core server will then be a **Failover Node** in the cluster.
- **Note:** This button is also available if you're currently running your PRTG installation in **Cluster Mode: Master Node**. This option will then change your master node to a failover node!
- After you click this button, please confirm converting this installation into a failover node by clicking on the **Yes** button.

Part 12: Advanced Topics | 9 Failover Cluster Configuration

1 Failover Cluster Step by Step



- A new popup window will appear.



- Enter the cluster's **Master IP address/DNS name**. It must be reachable from the machine running the failover node.
- Enter the other settings as defined in your **Master Node's** settings. Please make sure you use the same settings on all nodes in your cluster.

- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.
- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

Step 4: Confirm Failover Node

Now you need to confirm the new failover node by setting it to **Active** in the master node's settings.

In a browser window, log into PRTG's [web interface](#)^[102] of the **Master Node** server.

In the [System Administration—Cluster](#)^[182] settings, you will see your “Master Node” server in the first line of the cluster list and your “Failover Node” server below.

System Setup

System, Website, and Web Server Settings | Notification Delivery Settings | Probe Management | **Cluster Settings**

Node Name	Node ID	Node State	IP/DNS Names used for Connections Between Nodes
1 PRTG Network Monitor IP: CBC	25C	Active	#2 = #1 #3 = #1 #4 = #1 #5 = #1
2 PRTG Network Monitor IP: 276	7D5	☒ Active ☐ Inactive	#1 = #2 #3 = #2 #4 = #2 #5 = #2
3		☐ Active ☒ Inactive	#1 = #3 #2 = #3 #4 = #3 #5 = #3
4		☐ Active ☒ Inactive	#1 = #4 #2 = #4 #3 = #4 #5 = #4
5		☐ Active ☒ Inactive	#1 = #5 #2 = #5 #3 = #5 #4 = #5

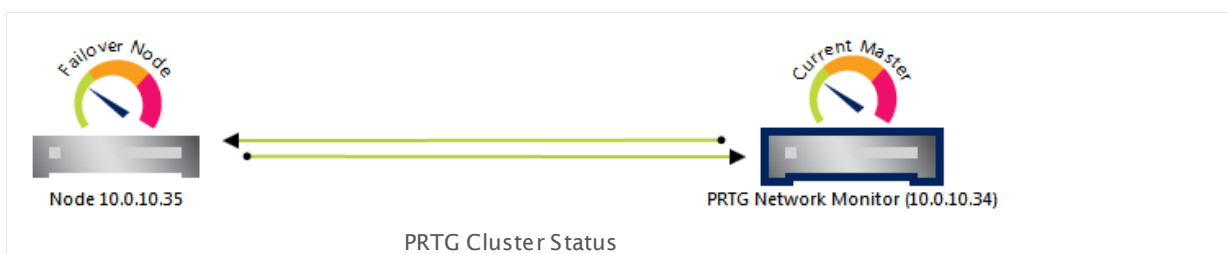
Save Changes

SystemSetup Cluster Settings

For the “Failover Node”, set the radio button for **Node State** to **Active** and **Save** the changes. The nodes will now connect and exchange configuration data. This may take a few minutes.

Step 5: Check Cluster Connection

In two browser windows, log into PRTG's web interfaces of **both** of your PRTG installations. Open the cluster status page in both windows by clicking on the narrow cluster information bars at the top of each window. You should see a cluster status with your two nodes in a **Connected** state after a few minutes.



CLUSTER STATUS		
Node 1: PRTG Network Monitor (10.0.10.34)		
Primary Node (Current Master)		Start Maintenance Mode
Connection To	IP	State
⇒ Node 10.0.10.35	10.0.10.35	Connected
Node 2: Node 10.0.10.35		
Secondary Node (Failover Node, Version: 28665)		Start Maintenance Mode
Connection To	IP	State
⇒ PRTG Network Monitor (10.0.10.34)	10.0.10.34	Connected
PRTG Cluster Status		

Step 6: Trouble Shooting

Having any problems? If your nodes cannot connect, please see

- the Cluster Log entries on the [PRTG Status—Cluster Status](#) ¹⁸⁵⁰ page of the web interface
- the core server log file, a text file in the logs directory of your PRTG data folder (see [Data Storage](#) ²⁰³⁶).

In the latest entries of these logs, you can see messages about any errors that might have occurred. These will give you hints on where to find a solution.

If you encounter connection problems between the two cluster nodes, please make sure that no software- or hardware firewall is blocking communication on the cluster port defined during cluster setup. Communication between the nodes must be possible in **both directions** in order for the cluster to work properly.

Step 7: Done! Move Sensors to the Cluster Probe Now

That's it. You've now successfully set up your failover cluster. All devices that are created or moved under the **Cluster Probe** will be monitored by both servers.

In order to monitor your existing configuration via all cluster nodes, on your master node, please move your groups, devices, and sensors from the local probe to the cluster probe! Objects, including their settings, will then be transferred to all cluster nodes automatically.

Add More Failover Nodes

If you want to add an additional failover node to your cluster, you will need an additional license key for two and three failover nodes, and two additional license keys to run four failover nodes. **Note:** In a cluster, only core servers running on the same size of [license](#)¹⁹ can be combined. For example, you can use several "PRTG Unlimited" licenses or several "PRTG 1000" licenses in one cluster.

To add another failover node to your cluster, please set up a new PRTG core server installation on a new server, using an additional license key. Then proceed with [Step 3](#)²⁰³¹ and following. **Note:** Use a second license key to set up both your second and third failover node, and use a third license key to set up your fourth failover node. The licenses "Site" and "Corporate" can be used to install an unlimited number of core servers.

Each failover cluster is technically limited to five cluster nodes: As a maximum, you can run one master node and four failover nodes in one cluster.

More

Knowledge Base: My PRTG Cluster is messed up. How can I start over?

- <http://www.paessler.com/knowledgebase/en/topic/41903>

Advanced Topics

- [Active Directory Integration](#)¹⁹⁹¹
- [Application Programming Interface \(API\) Definition](#)¹⁹⁹³
- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁴
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)¹⁹⁹⁸
- [Define IP Ranges](#)²⁰⁰⁰
- [Define Lookups](#)²⁰⁰¹
- [Regular Expressions](#)²⁰¹⁰
- [Add Remote Probe](#)²⁰¹¹
- [Failover Cluster Configuration](#)²⁰²⁶
- [Data Storage](#)²⁰³⁶
- [Using Your Own SSL Certificate](#)²⁰³⁸
- [Calculating Percentiles](#)²⁰⁴⁰

12.10 Data Storage

PRTG stores the monitoring configuration, monitoring data, logs, tickets, and reports, as well as support and debug data into different folders on the core server or the system running a [Remote Probe](#)^[2031]. Additionally, there is data from PRTG in the program directory and the Windows registry.

Data can be found in different locations. For a detailed information please see the article linked in the [More](#)^[2037] section below.

PRTG Program Directory

32 bit systems:

```
%programfiles%\PRTG Network Monitor
```

64 bit systems:

```
%programfiles(x86)%\PRTG Network Monitor
```

Note: These are the default paths. If you specified another installation directory, you will find your data there.

PRTG Data Folder

On Windows Vista, Windows 7, Windows 2008, Windows 8, and Windows 2012:

```
%programdata%\Paessler\PRTG Network Monitor
```

On Windows XP and Windows 2003:

```
%ALLUSERSPROFILE%\Application data\Paessler\PRTG Network Monitor
```

Note: These are the default paths, depending on your Windows version. If you specified a custom path for data storage, please look it up in the [PRTG Server Administrator](#)^[1962]. Open this application and switch to the **Core Server** tab. You will find the path there.

Windows Registry

System settings on 32 bit systems:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Paessler\PRTG Network Monitor
```


System settings on 64 bit systems:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Paessler\PRTG Network Monitor
```

Enterprise Console settings:

```
HKEY_CURRENT_USER\Software\Paessler\PRTG Network Monitor\WinGUI
```

More

Knowledge Base: How and where does PRTG store its data?

- <http://www.paessler.com/knowledgebase/en/topic/463>

12.11 Using Your Own SSL Certificate with PRTG's Web Server

This section will give you a brief overview on how to use your own trusted SSL certificate files with the PRTG web server.

What is SSL?

PRTG supports Secure Sockets Layer (SSL) to encrypt all data entered and shown in the [Web Interface](#)^[100], in the [Enterprise Console](#)^[106], or in the [Smartphone Apps](#)^[1916]. That ensures that no sensitive information can be intercepted when sending data between the PRTG core server and your client software.

By default PRTG is already delivered with an SSL certificate so you can use secure connections to your PRTG core server. However, these certificate files are not signed by a valid authority, which is why browsers show an [SSL Certificate Warning](#)^[105] when you try to access the web interface. Despite this warning your connection is still encrypted successfully.

To remove the browser warning you can obtain a certificate that is valid for your own domain name and signed by a valid authority. The certificate must be provided in the correct format and can then be copied to your PRTG program directory (see [Data Storage](#)^[2036]).

PRTG Needs PEM Encoded Format and Unencrypted Key

There are many different issuers for certificates, and there are different formats certificates can be provided in.

PRTG needs three different files, named correctly, containing data in the expected encoding and format:

- **prtgcrt**: This is the certificate for your PRTG server. It has to be stored in **PEM** encoded format.
- **prtkey**: This is the private key matching your server certificate. It has to be stored in **PEM** encoded format and may not be encrypted! Please make sure that you provide this file in **decrypted** format! The best way to check this is to open the file in a text editor. If you find a line containing the word "ENCRYPTED", the file still needs to be decrypted before you can use it with PRTG. Please decrypt using an SSL tool (e.g. OpenSSL) and your key password.
- **root.pem**: This is the public root certificate of your certificate's issuer. It has to be stored in **PEM** encoded format and must contain all necessary root certificates of your issuer in one file. If there is more than one PEM encoded root certificate, please use a text editor to copy all of them into a single file (the order does not matter).

Once ready, copy these three files to the **/cert** sub folder of your PRTG program directory (please backup existing files) and restart your PRTG core server service (see [PRTG Server Administrator](#)^[1975]). **Note:** PRTG services won't restart if the files are not provided in exactly the expected format!

For detailed instructions and examples, installation descriptions for various certificates (including **Wildcard** certificates), as well as links to certificate tools and converters, please see the [More](#) 2039 section below.

More

Knowledge Base: How can I establish a secure web interface connection to PRTG?

- <http://www.paessler.com/knowledgebase/en/topic/273>

Knowledge Base: How can I use a trusted SSL certificate with the PRTG web interface?

- <http://www.paessler.com/knowledgebase/en/topic/283>

12.12 Calculating Percentiles

Wikipedia describes a percentile as **the value of a variable below which a certain percent of observations fall**. Providers often use it in their billing models, e.g. when determining the used bandwidth. With percentile calculation, you can cut off an x percent of peak values from an amount of values.

In PRTG, you can calculate percentiles when creating general reports (see [Reports](#)¹⁷⁴⁹ section), or creating historic data reports of a certain sensor (see [Historic Data Reports](#)¹³² section). If you activate the **Percentile Results** option in your reports' settings, the according values will be added to the tables. You can customize the following settings:

- **Percentile:** Enter the percentile number you want to calculate. If you choose, for example, to calculate the 95th percentile, enter "95" here and 5 % of peak values will be discarded.
- **Percentile Average:** This is the averaging interval in seconds, which is used for percentile calculation. Default value is 300 which is equivalent to 5 minutes.

Percentile Mode: Choose between **Discrete** and **Continuous**. Continuous percentile interpolates between discrete values, whereas discrete percentile chooses the next smaller discrete value.

- **Discrete** percentile means that the value must be a member of the data set. For this kind of calculation you require a discrete distribution. The median of a discrete distribution can not be defined, as such, meaning that the 50th discrete percentile may not necessarily be the median if the value does not belong to an odd number of measurements. Discrete percentiles, as such, should not be used for billing applications.
- **Continuous** percentile basically means that the measurements are treated as a statistical population and the value is determined by interpolating a value when it isn't present. This means that values are interpolated between actual measurements that are varying around the "perfect" center of the measurements.

More

Knowledge Base: What are percentiles?

- <http://www.paessler.com/knowledgebase/en/topic/9563>

Part 13

Appendix

13 Appendix

Please find further information in the following sections.

- [Glossary](#)  2043
- [List of Abbreviations](#)  2047
- [Support and Troubleshooting](#)  2050
- [Legal Notices](#)  2051

13.1 Glossary

This section explains special words used in the context of PRTG Network Monitor. **Note:** Here, only explanations are given. For information on where to find detailed instructions for a specific key word, please see the **Index** section.

Channel

The monitoring data of a [sensor](#)^[2046] is shown in sensor channels. For example, for sensors that measure network traffic, there is one channel each for traffic **in** and traffic **out**. You can set various triggers for each channel, enabling you to set sensor status changes or notifications based on the monitoring data received.

Cluster

PRTG can be configured as a failover cluster for fail-safe monitoring. In a cluster, one or more [core servers](#)^[2043] work together in one configuration. Every node can monitor all devices in a network for gapless monitoring, additionally enabling you to compare monitoring results measured from different perspectives.

Cluster Node

Sometimes used as synonym for [Node](#)^[2045].

Cluster Probe

When running PRTG in cluster mode, a cluster probe is automatically created. All [objects](#)^[2045] created on the cluster probe, or below it in the [device tree](#)^[2044], are monitored by all nodes in the cluster. Create or move [objects](#)^[2045] there to monitor them fail-safely. If one node fails, the other nodes will continue to monitor them. You can add [groups](#)^[2044] and [devices](#)^[2044] to the probe. On a PRTG installation, the cluster probe runs as part of this installation's [local probe](#)^[2044]. [Remote probes](#)^[2045] cannot be connected to a cluster probe, but only to one local probe of one PRTG installation.

Core Server

The central unit of PRTG. It receives monitoring data from the [probe\(s\)](#)^[2045] and handles reporting and notifications, provides the web server for the user interfaces, and many other things. In a [cluster](#)^[2043], one core server is installed on every node.

Dashboard

In the Home menu of the web interface there are several pre-configured dashboards available which show a quick overview of the overall status of your monitoring configuration. Custom dashboards can be created using the [Maps](#)^[2045] function.

Device

A device in PRTG represents a physical device in the network. For an easily understandable tree structure, you usually create one PRTG device for each physical device you want to monitor (exceptions apply to some sensors that can only be created on the [local probe](#)^[2044] device, and for sensor types that are not bound to a certain device, such as HTTP sensors, which are also usually created on the local probe). You can add one or more [sensors](#)^[2046] on every device.

Device Tree

PRTG's configuration is represented in a hierarchical tree structure, called device tree, containing all [objects](#)^[2045]. While building the tree, you can relate to your network's topology to make your monitoring setup easy to understand.

Failover Master (Node)

If the [primary master](#)^[2045] node fails, a [failover node](#)^[2044] is promoted to current failover master and takes over the master role until the primary master node re-joins the [cluster](#)^[2043].

Failover Node

In a [cluster](#)^[2043] a failover node monitors all [sensors](#)^[2046] on the [cluster probe](#)^[2043], providing monitoring data for the [core server](#)^[2045]. Additionally, it serves as a backup in case the [master node](#)^[2045] fails.

Group

A group is an organizational unit in your PRTG tree structure that helps to arrange your devices. To existing groups, you can add devices, or additional sub-groups. This way you can model your physical network's topology within the PRTG configuration.

Library

Libraries are a way to show parts of your [device tree](#)^[2044] in a different layout or with different filters enabled. There is an editor available that allows creating libraries directly in your browser.

Local Probe

The local probe is installed together with the [core server](#)^[2043]. All [objects](#)^[2045] created on the local probe, or below it in the [device tree](#)^[2044], are monitored by the local core system. You can add [groups](#)^[2044] and [devices](#)^[2044] to the probe.

Map

Maps (sometimes referred to as "[dashboard](#)"^[2043]) are a way to present monitoring the way you want to arrange it. There is an editor available that allows creating maps directly in your browser.

Master Node

In a [cluster](#)^[2043], the master node controls the settings and cluster management. It also takes over notifications. All changes to the monitoring configuration are made on the master node.

Node

In a [cluster](#)^[2043] there is one [master node](#)^[2045] and one or more [failover nodes](#)^[2044]. On each node, one PRTG [core server](#)^[2043] installation is running independently. All nodes are connected to each other, exchanging configuration and monitoring data.

Object

All different items in the [device tree](#)^[2044] are generally referred to as objects. An object can be a [probe](#)^[2045], a [group](#)^[2044], a [device](#)^[2044], or a [sensor](#)^[2046].

Primary Master (Node)

The **primary** master node in a [cluster](#)^[2043] is the [node](#)^[2045] that is master by configuration. Only if it fails, one of the [failover nodes](#)^[2044] becomes [failover master](#)^[2044] and takes over the master role until the primary master node re-joins the cluster.

Probe

On a probe, the actual monitoring takes place. A probe can run as [local probe](#)^[2044] on the local system where the [core server](#)^[2043] is installed. There are also [cluster probes](#)^[2043] and [remote probes](#)^[2045].

Remote Probe

A remote probe is a small piece of software installed on a computer in the local or remote network. It scans the network from there and sends monitoring results to the [core server](#)^[2043]. Once the connection is established, the remote probe is shown in the PRTG tree structure. All [objects](#)^[2045] created on the remote probe, or below it in the [device tree](#)^[2044], are monitored by the remote system running the remote probe. You can add [groups](#)^[2044] and [devices](#)^[2044] to the probe. In [cluster](#)^[2043], remote probes can only be connected to the [master node](#)^[2045], not to one of the [failover nodes](#)^[2044].

Sensor

A sensor monitors one aspect of a [device](#)^[2044]. For example, monitoring if a device responds to a Ping request is done by one sensor. Monitoring the traffic of one ethernet port of a router device is done by another sensor. For monitoring the CPU load of the local system yet another sensor is set up, and so on. A sensor's data is shown in [channels](#)^[2043].

Sensor Tree

Sometimes used as synonym for [device tree](#)^[2044].

Tickets

[Tickets](#)^[148] are created by the system or a PRTG user and contain important messages or action steps to take for the administrator or another specific user. Every ticket should be viewed to take appropriate actions. You can access the list of tickets from the main menu.

xFlow

Paessler designates all kinds of flow protocols as xFlow. Currently, PRTG supports NetFlow V5 and V9, sFlow V5, and jFlow V5.

13.2 List of Abbreviations

In the following, please find a list of the most common abbreviations used in this documentation.

ADO: ActiveX Data Objects (ADO)

ADSL: Asymmetric Digital Subscriber Line (ADSL)

AJAX: Asynchronous Java Script and XML (AJAX)

API: Application Programming Interface (API)

CoS: Class of Service (CoS)

CSV: Comma Separated Values (CSV)

DHCP: Dynamic Host Configuration Protocol (DHCP)

DMZ: Demilitarized Zone (DMZ)

DSCP: Differentiated Services Code Point (DSCP)

DNS: Domain Name Service (DNS)

GUI: Graphical User Interface (GUI)

GUID: Globally Unique Identifier (GUID)

HTTP: Hypertext Transfer Protocol (HTTP)

ICMP: Internet Control Message Protocol (ICMP)

IMAP: Internet Message Access Protocol (IMAP)

IPsec: Internet Protocol Security (IPsec)

JSON: JavaScript Object Notation (JSON)

LAN: Local Area Network (LAN)

LDAP: Lightweight Directory Access Protocol (LDAP)

MoID: Managed Object ID (MoID)

MIB: Management Information Base (MIB)

MOS: Mean Opinion Score (MOS)

NAT: Network Address Translation (NAT)

NTLM: NT LAN Manager (NTLM)

PDF: Portable Document Format (PDF)

PDV: Packet Delay Variation (PDV)

POP3: Post Office Protocol version 3 (POP3)

QoS: Quality of Service (QoS)

RADIUS: Remote Authentication Dial-In User Service (RADIUS)

REST: Representational State Transfer (REST)

RMON: Remote Monitoring (RMON)

RPC: Remote Procedure Call (RPC)

SASL: Simple Authentication and Security Layer (SASL)

SLA: Service Level Agreement (SLA)

S.M.A.R.T.: Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.)

SMB: Server Message Block (SMB)

SMTP: Simple Mail Transfer Protocol (SMTP)

SNMP: Simple Network Management Protocol (SNMP)

SNTP: Simple Network Time Protocol (SNTP)

SOAP: Simple Object Access Protocol (SOAP)

SPAN: Switched Port Analyzer (SPAN)

SQL: Structured Query Language (SQL)

SSH: Secure Shell (SSH)

SSL: Secure Sockets Layer (SSL)

TFTP: Trivial File Transfer Protocol (TFTP)

UNC: Uniform Naming Convention (UNC)

UPnP: Universal Plug and Play (UPnP)

UUID: Universally Unique Identifier (UUID)

VoIP: Voice over IP (VoIP)

VPN: Virtual Private Network (VPN)

WAN: Wide Area Network (WAN)

WBEM: Web-Based Enterprise Management (WBEM)

WMI: Windows Management Instrumentation (WMI)

WQL: Windows Management Instrumentation Query Language (WQL)

WSUS: Windows Server Update Services (WSUS)

XML: Extensible Markup Language (XML)

13.3 Support and Troubleshooting

Need help with PRTG? There are several ways to get support and trouble shooting.

Video Tutorials

A video says more than a thousand words—watch tutorials for PRTG from Paessler and other PRTG users.

- http://www.paessler.com/support/video_tutorials

Paessler Knowledge Base

In the Knowledge Base you can search in hundreds of articles about PRTG. You can post your own questions and answers, too!

- <http://www.paessler.com/knowledgebase/>

Open a Support Ticket

Users that have purchased a license can open support tickets which will usually be answered by Paessler's staff in less than 24 hours on business days.

- <http://www.paessler.com/support/openticket>

13.4 Legal Notices

Build using Indy Internet Direct (<http://www.indyproject.org/>). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). Uses the net-SNMP library, see "netsnmp-license.txt". Uses the DelphiZip library distributed under the GNU LESSER GENERAL PUBLIC LICENSE (<http://www.delphizip.net/>). Uses FastMM (<http://sourceforge.net/projects/fastmm/>), TPLockBox (<http://sourceforge.net/projects/tplockbox>) and Delphi Chromium Embedded (<http://code.google.com/p/delphichromiumembedded/>) under the Mozilla Public License 1.1 (MPL 1.1, available from <http://www.mozilla.org/MPL/MPL-1.1.html>). Soundfiles from <http://www.soundsnap.com>. Uses Public Domain regional maps from the "CIA World Factbook" webpage of the CIA (<https://www.cia.gov/library/publications/the-world-factbook/docs/refmaps.html>). Uses the "wkhtmltopdf" (<http://code.google.com/p/wkhtmltopdf/>) library distributed under the GNU LESSER GENERAL PUBLIC LICENSE (see [wkhtmltopdf_lgpl-3.0.txt](#)). Icons from <http://www.androidicons.com>.

All trademarks and names mentioned herein belong to their respective owners.

Last manual export: Freitag, 4. April 2014 11:14:55

Index

- 2 -

2 days tab 124

- 3 -

30 days tab 124
365 days tab 124

- A -

Account Settings 1786, 1824
Account Type 1786
Activation 60
Add
 Device 211
 Group 205
 Sensor 220
Ajax Web Interface 100
Alarm
 Acknowledge 1880
 List 1880
Alarms 174
Android App
 PRTGdroid 1916
API 1993
Architecture
 Basic Concept 77
Audible Alarms 1786
Auto-Discovery
 Quick Start 36
 Settings 190
Automatic
 Folding 1786
 Refresh 1786
 Restart Options (Probe System) 1979
Automatic Software Update 1846
Averaging 132, 1749

- B -

Bandwidth Monitoring Overview 1937

Basic Concepts 76
Billing Tool 1852
Bulk edit 1710

- C -

Certificate
 Trusted SSL 2038
Change Trigger 1690
Check Now
 Context Menu 162
Chrome
 Desktop Notifications 1854
Clone
 Context Menu 162
Cluster
 Basic Concept 81
 Maintenance Mode 1837
 Status 1837
Cluster Connection 1823
Configure
 Cluster 56, 1823
 Dependencies 90
 Device 272
 Geographical Map 1718
 Group 253
 License Key 57
 Map 1768
 Notification 1723, 1791
 Notification Delivery 1815
 Notification Trigger 1690
 Object Arrangement 1707
 Probe 62, 238, 1821, 1979
 PRTG Server 1959
 Reboot (automatic) 1979
 Report 1749
 Root Group 224
 Schedule 1801
 Sensor 290
 Sensor Channel 1683
 System 1784, 1805
 User Account 1786, 1824
 User Group 1829
 Website 1805
Continuous (Percentiles) 2040
Create Device Template
 Context Menu 162
Create Objects 204

- D -

Data

- Folder 2036
- Reporting 93
- Storage 2036

Data Purging 1805

Date Format 1786

Decimal Places 1683

Dependencies 90

Device

- add 211
- arrange 1707
- clone 1708
- Multi-Edit 1710
- Template 1715

Device Tools

- Context Menu 162

Devices 174

Discrete (Percentiles) 2040

Down 121

Down (Acknowledged) 121

Down (Partial) 121

Download 45

Downloads

- Add-Ons 1852
- Apps for iOS & Android 1852
- Billing Tool 1852
- Google Chrome 1852
- Remote Probe Installer 1852
- Windows Enterprise Console 1852

- E -

Edit

- Context Menu 162

Email Address 1786

Email Round Trip
Technology 1943

Email Templates 1805

Enterprise Console 1860

Error Limit 1683

Escalation 1690

- F -

Favorites

- Context Menu 162

Flow

- Channel Definitions 1998
- Filter Rules 1994
- IP Ranges 2000
- Technology 1934
- Toplists 1702

- G -

General Web Interface Layout 108

Geo Map Type 1805

Geographical Map 1718

Google

- Chrome Desktop Notifications 1854
- Code 1680
- Maps 1718

Graph

- Settings 1805
- Type 1805

Group

- add 205
- arrange 1707
- clone 1708

- H -

Hash 1786

Header 108

Help Center 174

Historic Data

- Context Menu 162

Home 174

Homepage 1786

HTML GUI 1913

HTTP Proxy 1815

- I -

ICMP Echo 756

Inheritance of Settings 87

Install

- Core Server 51

Index

Install

- Download 45
- Enterprise Console 67
- Uninstall 71
- Update 47

Intervals 1805

iPhone App

iPRTG 1916

- L -

Latency 1690

Libraries 1733

Context Menus 1748

Management 1740

Multi-Edit 1710

Node 1742

Settings 1742

Limits

Error 1683

Warning 1683

Line

Color 1683

Width 1683

Live Data tab 124

Login Name 1786

Logout 174

Logs 174

Lookups 2001

- M -

Maintenance Mode 1837

Management

Tab 222

Maps 174, 1768

audible alert 1774

automatic rotation 1768

Designer 1774

edit 1774

Line Color 1774

Multi-Edit 1710

Mini HTML 1913

Monitoring Data 2036

Move

Context Menu 162

Multi-Edit 1710

- N -

None 121

Notification 1723, 1791

Delivery 1815

Escalation 1690

Multi-Edit 1710

Trigger 1690

Notifications

Chrome Desktop 1854

Notifying 92

- O -

Object Hierarchy 83

Off Notification 1690

OK 121

On Notification 1690

Overview tab 124

- P -

Packet Sniffer

Channel Definitions 1998

IP Ranges 2000

Packet Sniffing

Filter Rules 1994

Technology 1932

Toplists 1702

Passhash 1786

Password 1786

Pause

Context Menu 162

Paused 121

Peak Filter (Spike Filter) 1683

Percentile 2040

Percentiles 132, 1749

Performance Strategy 1805

Priority

Context Menu 162

Probe

arrange 1707

Probe Administrator 1979

Probe Connection 1821

Probes

IP Ranges 2000

- R -

- Refresh 174, 1786
- Registry
 - Data 2036
- Remote Probe 2011
- Remote Registry 1431
- Rename
 - Context Menu 162
- Reports 174, 1749
 - Data 93
 - Multi-Edit 1710
- Restart Options (Probe System) 1979

- S -

- Schedule 1801
 - Multi-Edit 1710
- Scheduled Reboot (Probe System) 1979
- Scheduling 91
- Search Box 174
- Send Link by email
 - Context Menu 162
- Sensor
 - add 220
 - arrange 1707
 - Behavior 121
 - Channel Settings 1683
 - clone 1708
 - compare 129
 - Multi-Edit 1710
 - Notification Trigger 1690
 - Settings 290
 - Status 121
 - Type 291
- Sensors 174
- Server Administrator 1959
- Session Expiry 1805
- Settings
 - Context Menu 162
- Setup 174
- Shift 1774
- SMART 1555
- Smart Phone Apps
 - iPRTG 1916
 - PRTGdroid 1916

- SMS Delivery 1815
- SMTP Delivery 1815
- SNMP
 - Lookups 2001
 - Technology 1923
- Sort Alphabetically
 - Context Menu 162
- Sound Alarms 1786
- Speed Trigger 1690
- Spike Filter 1683
- SSL 2038
- State Trigger 1690
- System
 - Status 1837

- T -

- Tags 89
- Threshold Trigger 1690
- Ticket Email Address 1805
- Tickets 174
- Timezone 1786
- Toplists 1702
- Tree View
 - Zoom 108
- Trigger
 - Change 1690
 - Latency 1690
 - Speed 1690
 - State 1690
 - Threshold 1690
 - Volume 1690

- U -

- Unknown 121
- Unusual 121
- Unusual Detection 1805
- Update 47
- Uptime Threshold 1805
- User Access Rights 94
- Username 1786

- V -

- Value Mapping
 - Lookups 2001

Index

Vertical Axis Scaling 1683

VoIP

Technology 1939

Volume Trigger 1690

- W -

Warning 121

Warning Limit 1683

Web Interface 100

Web Server

Certificate 2038

IP Address 1805

Port 1805

Windows GUI 1860

Menu Structure 1902

Menu Tab 1868

Options 1896

WMI

Technology 1927

Last change to this manual (YYYY-MM-DD): 04.04.2014