

PRTG Network Monitor V7 User Manual

- Bandwidth monitoring
- Availability monitoring
- Usage monitoring

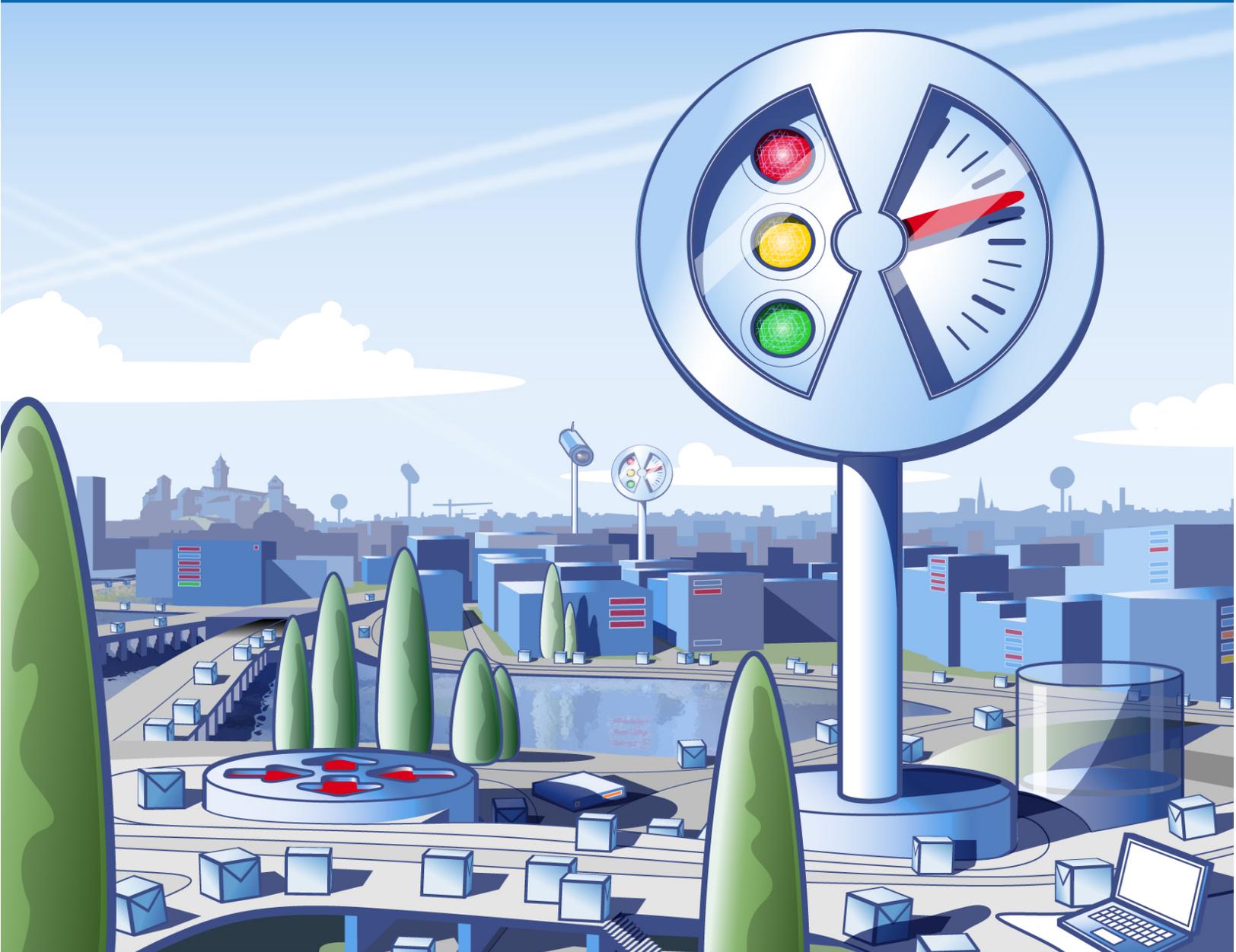


Table of Contents

Part I Introduction	6
1 Key Features.....	6
2 Available Licenses.....	7
3 About This Document.....	8
Part II System Requirements	10
1 Detailed System Requirements.....	10
Part III Installation	15
1 Downloading the Software.....	15
2 Upgrading to Version 7 from Previous Versions.....	15
3 Installation of a PRTG Core Server.....	16
4 Entering a License Key.....	18
5 Activating the Product.....	20
6 Installation of a PRTG Remote Probe.....	21
7 Installation of the Windows GUI.....	21
8 Uninstallation.....	22
Part IV Basic Concepts of PRTG Network Monitor	24
1 Architecture: PRTG Core Server, PRTG Probe and the User Interfaces	24
2 Object Hierarchy: Probes, Groups, Devices, Sensors, Channels.....	27
3 Inheritance of Settings.....	30
4 User Access Rights.....	31
5 Alarms Concept.....	31
6 Maps Concept.....	31
7 Reports Concept.....	31
8 Logs Concept.....	32
9 ToDos Concept.....	32
10 Notifications Concept.....	32
11 Schedules Concept.....	32
12 Dependencies Concept.....	33
Part V User Interfaces	35
1 Web Interface.....	37
2 Windows GUI.....	45

3	iPhone Interfaces.....	50
Part VI	Device and Sensor Setup	54
1	Reviewing Settings of the Root Group.....	54
2	Creating Groups, Devices and Sensors Manually.....	56
3	Creating Devices and Sensors Using the Auto-Discovery.....	59
4	Edit Sensor and Channel Settings.....	61
Part VII	Sensor Types	64
1	Common Sensors.....	64
2	Bandwidth Monitoring Sensors.....	64
3	Web Server (HTTP, HTTPS) Sensors.....	65
4	SNMP Sensors.....	68
5	Windows Systems (WMI) Sensors.....	71
6	Various Protocol Sensors.....	74
7	Mail Server Sensors.....	75
8	SQL Server Sensors.....	77
9	File Server Sensors.....	78
10	Virtual Server Sensors.....	79
11	VoIP and QoS Sensors.....	80
12	Custom Sensors.....	82
13	Packet Sniffer Sensors.....	83
14	xFlow (NetFlow and sFlow) Sensors.....	85
15	Comparison of Bandwidth Monitoring Sensors.....	87
16	Sensor Factory Sensors.....	88
Part VIII	Notifications	94
Part IX	Maps	100
Part X	Reports	109
Part XI	ToDoS	115
Part XII	User Management	117
Part XIII	System Settings and Administration	120
1	Account Settings - Edit My Account.....	121
2	Account Settings - Edit Schedules.....	121
3	Account Settings - Edit Notifications.....	123
4	System Administration - Edit System Setup.....	125
5	System Administration - Edit User Accounts and User Groups.....	128

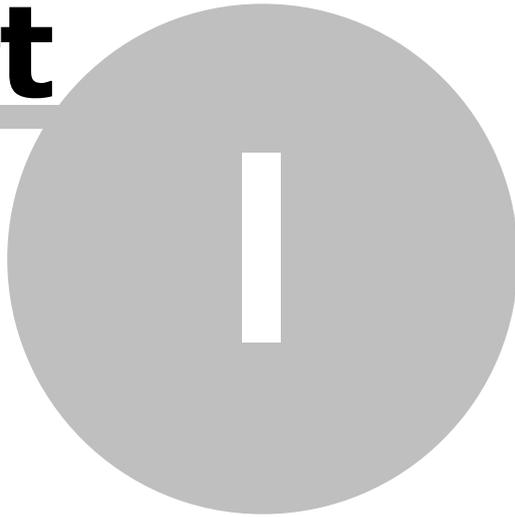
- 6 System Information and Optional Downloads..... 129
- 7 PRTG Server Administrator..... 129
- 8 PRTG Probe Administrator..... 135

Part XIV Advanced Topics 140

- 1 Toplists 140
- 2 Multiple Probes and Remote Probes..... 143
- 3 Copying Devices by Cloning or Using Device Templates..... 149
- 4 Importing Data from PRTG Traffic Grapher 6 or IPCheck Server
Monitor 5 150
- 5 Installing an SSL Certificate for the Web Server..... 150
- 6 Customizing the Web Interface..... 150
- 7 Using the PRTG API (Application Programming Interface)..... 151
- 8 Interface Definition for Custom EXE Sensors..... 151
- 9 Calculating Percentiles..... 153
- 10 Legal notices..... 153

Index 155

Part



Introduction

1 Introduction

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.

Why Network Monitoring is Important

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 mitigation 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. It 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 SNMP, WMI, packet sniffer, Cisco NetFlow as well as 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 Key Features

PRTG Network Monitor can be used to:

- Monitor and alert for uptimes/downtimes or slow servers.
- Monitor and account bandwidth and network device usage.
- Monitor system usage (CPU loads, free memory, free disk space etc.).
- 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.

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

- Paessler's own fast and efficient database system to store the raw monitoring results (outperforms SQL servers)

for monitoring data).

- Built-in web server with HTTP and HTTPS support for the user interface.
- Mail server for automatic email delivery.
- SQLite SQL Server for storage of events, toplist and ToDos.
- Report generator to create PDF reports.
- Graphics engine for user-friendly charts.
- Network analysis module to auto-discover devices and sensors.
- An application programming interface (API) allows users to program their own features.

PRTG Network Monitor can support thousands of sensors and can optionally work with multiple remote probes (agents) to monitor multiple sites or network segments from one central core installation. The software is based on Paessler's proven monitoring technology, which has been constantly improved since 1997 and is already used by more than 150,000 users around the world every day.

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.

1.2 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 with up to 4 probes.
- Supports all available sensor types (except NetFlow/sFlow/xFlow).
- Shortest available monitoring interval is one minute.

Starter Edition

The Starter Edition has all the features of the Freeware Edition, but it supports up to 20 sensors. By entering a Starter Edition key, you can extend your Freeware Edition.

Information on how to apply for a Starter Edition license key can be found on our website at <http://www.paessler.com/prtg/download>

Trial Edition

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

- Can monitor up to 500 sensors with up to 4 probes.
- Supports all available sensor types (including NetFlow/sFlow).
- Shortest available monitoring interval is one second.
- Temporary license key must be requested from Paessler's website.
- Trial period limited to 30 days (automatically reverts to Freeware Edition afterwards).

As default after installation, the Trial Edition runs with the functionality of the Freeware Edition only when no license key is entered. Free trial license keys are available on our website at <http://www.paessler.com/prtg/trial>

Commercial Editions

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

- Maximum number of sensors (100 or more), xFlow/NetFlow sensors (1 or more) and probes (4 or more) depend on the license.
- Supports all available sensor types (including NetFlow/xFlow).
- Shortest available monitoring interval is one second.

Editions overview

PRTG Network Monitor Version	Sensors	Probes	xFlow/NetFlow Sensors
Freeware Edition/Starter Edition	10/20	4	-
30-Days-Trial	500	4	2
Professional 100	100	4	2*
Enterprise 500	500	10	2*
Enterprise 1,000	1,000	20	2*
Enterprise Unlimited	unlimited	30	2*
Enterprise Unlimited Site**	unlimited	unlimited	2*

* Additional xFlow/NetFlow sensors can be purchased as add-on.

** The Enterprise Unlimited Site License allows multiple installations of the core server within one network.

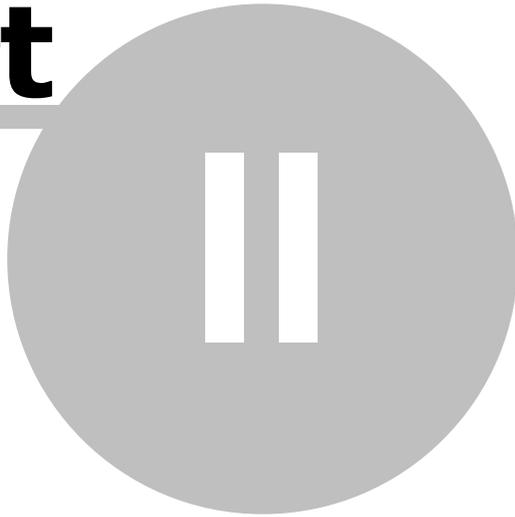
To learn more about pricing or to order licenses please visit: <http://www.paessler.com/order>

1.3 About This Document

This document introduces the reader to the system concepts of PRTG Network Monitor and explains how to set up the software to achieve the best results. You will learn how to plan your monitoring setup, how to set up your sensors, reports, notifications, maps and user accounts.

This document does not explain each and every edit field or button of the user interface. Detailed information is included in PRTG's web interface itself in the form of short contextual help texts and hints. Also, this document is not a technical in-depth documentation of file formats, APIs and other background information. This information is available online on the Paessler knowledge base at <http://www.paessler.com>.

Part



System Requirements

2 System Requirements

In order to install and work with PRTG Network Monitor you need:

- A PC, server or virtual machine with roughly the performance of an average PC built in the year 2007 or later.
- Operating system Microsoft Windows XP, Windows 2003, Windows Vista, Windows 7 or Windows 2008 (32-bit or 64-bit).
- Web browser to access the web interface (Google Chrome 3 is recommended; Firefox 3.5, Safari 4, and Internet Explorer 8 were also tested).

For more detailed information and if you plan a larger installation see [Detailed System Requirements](#).

Planing 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 for SNMP V3, WMI and packet sniffer apply).

For larger installations please refer to our knowledge base article "Planning Large Installations of PRTG Network Monitor 7": http://www.paessler.com/support/kb/prtg7/system_requirements

2.1 Detailed System Requirements

Operating Systems for PRTG Core Server and PRTG Probe

The 32-bit and 64-bit versions of the following operating systems are officially supported for PRTG "Core Service" and "Probe Service":

- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2

Hardware Requirements for PRTG Core Server and PRTG Probe

Hardware requirements mainly depend on the sensor types and intervals used. The following values are provided as reference for common usage scenarios of PRTG 7 (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).
- RAM: You will need about 150KB of RAM per sensor.
- Hard Disk: You will need about 200KB of disk space per sensor per day (for sensors with 60 second interval).
- An Internet connection is required for license activation (via HTTP or email).

There are also non-hardware dependent limitations for some sensor types, e.g. WMI and SNMP V3 sensors. These limitations can be overcome by distributing the sensors across multiple remote probes. If you plan installations with more than 500 to 1,000 sensors or more than 10 Packet Sniffer/xFlow (NetFlow/sFlow) sensors please consult the Knowledge Base article linked at the end of this section.

Sample Configurations

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

	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:

Technology	Client OS
VMware ESX/ESXi (version 3.5 and VSphere 4)	Windows XP, Windows 2003 (32/64 bit), Windows Vista, Windows 7 (32/64 bit), Windows 2008 (32/64 bit)

VMware Server 2.0	Windows XP, Windows 2003 (32/64 bit), Windows 2008
XEN Server 5.0	Windows XP
Parallels Virtuozzo Containers	Windows 2003 Server (32/64 bit)
Cloud Platforms (Amazon EC2, GoGrid, SoftLayer)	Windows Server 2003

Web Browser Requirements

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

- Google Chrome 3 (recommended)
- Mozilla Firefox 3.5
- Apple Safari 4
- Microsoft Internet Explorer 8
- Note: Microsoft Internet Explorer 7 is "deprecated" and may not be supported in future versions of PRTG.

A note on browser performance: PRTG's web interface makes heavy use of Javascript and AJAX. We found that for some functions Chrome and Safari are up to 10 times faster than Internet Explorer 8 and 3 - 5 times faster than Firefox 3.5.

Requirements for Monitored Devices

- **SNMP monitoring:** The monitored device(s) must be equipped with SNMP Version 1, 2c or 3 (i.e. a SNMP-compatible software must be installed on the device). SNMP must be enabled on the device and the machine running PRTG must be allowed 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
- **NetFlow, sFlow monitoring:** The device must be configured to send NetFlow data packets (NetFlow Version 5 or 9) or sFlow packets to the machine running a PRTG Probe.
- **Packet Sniffer:** 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.

Requirements for the Windows GUI

The optional PRTG Windows GUI runs under all Windows versions XP or later and requires Internet Explorer 7 or 8.

Requirements for the iPhone-based User Interfaces

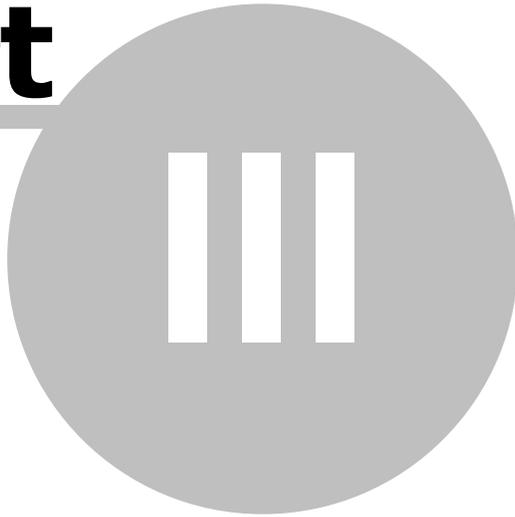
The optional iPRTG app for iPhones (must be purchased separately) requires iPhone firmware 3.0 (or later). The built-in web-browser based iPhone interface was created for iPhone firmware 2.0 (or later).

Planing 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 for SNMP V3, WMI and packet sniffer apply). For larger installations please refer to our knowledge base article "Planning Large Installations of PRTG Network Monitor 7":

http://www.paessler.com/support/kb/prtg7/system_requirements

Part



Installation

3 Installation

To use PRTG Network Monitor you need to download and install the software as described in the following sections:

- [Downloading the Software](#): How to get the latest version from Paessler
- [Upgrading to Version 7 from Previous Versions](#): Read this if you have used PRTG Traffic Grapher 6 or IPCheck Server Monitor 5 before
- [Installation of the PRTG Core Server](#): How to install the PRTG core server software on your PC/Server
- [Entering A License Key](#): How to enter a license key
- [Uninstallation](#): How to remove the software from your PC/Server

3.1 Downloading the Software

Please download the latest version of PRTG Network Monitor from the Paessler website. There are two different installers for PRTG, a public download for the Freeware and Trial editions, and another download for the commercial editions (which is only available for paying customers).

Downloading the Freeware Edition and Trial Edition

Please download the latest publicly available file from the Paessler website at www.paessler.com/prtg/download

Downloading the Commercial Editions

Updates are free to customers with an active maintenance contract. Please log into the Paessler website at www.paessler.com/login to get the latest download.

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

3.2 Upgrading to Version 7 from Previous Versions

Upgrading from Older Version 7.x Versions

If you have been running PRTG Network monitor with an earlier V7.x version number, simply install the latest version on top of the previous version.

Upgrading from PRTG Traffic Grapher 6 or IPCheck Server Monitor 5

If you have been running one of the two predecessor products of PRTG 7 (namely PRTG Traffic Grapher Version 6 or IPCheck Server Monitor Version 5), you can import most of your data (monitoring setup and historic data) into PRTG 7. Importing data from earlier versions is not possible.

Please refer to this Knowledge Base article on the Paessler website:
http://www.paessler.com/support/kb/prtg7/tricks/data_import_from_prtg6_or_ipcheck5/

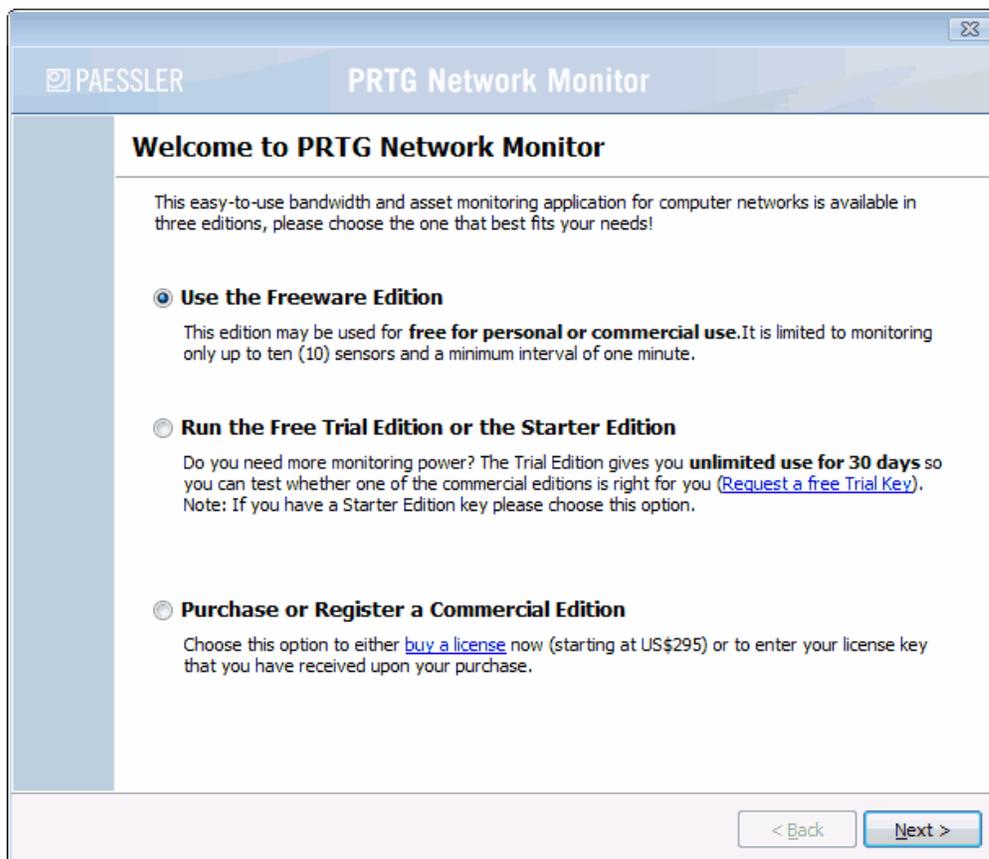
3.3 Installation of a PRTG Core Server

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

The usual software installation wizard will guide your through the installation process:



Please click "Next" to walk through the wizard. After accepting the license agreement, you can choose the folder you wish to install the software in. As soon as you click "Next", the necessary files will be copied to your disk and a dialog asking for your license type will appear.



Please select the proper option and enter the necessary data.

Afterwards you will see a dialog with some base settings:

The screenshot shows the 'Essential Settings for PRTG Network Monitor' window. It contains the following sections:

- Administrator Account:** Login Name: prtgadmin, Password: [masked], Email Address: [empty], Confirm Password: [masked].
- Web Server IPs:** Radio buttons for 'Localhost only (127.0.0.1, no external access)' and 'Specify IPs'. The 'Specify IPs' option is selected, and a text box contains '192.168.2.212'.
- Web Server Port:** Radio buttons for 'Standard Web Server Port 80 (recommended setting)', 'HTTPS/SSL on port 443', and 'Specify Port:'. The 'Standard Web Server Port 80' option is selected. The 'Specify Port' option has a text box with '80' and a refresh icon.
- Site Info:** Site Name: PRTG Network Monitor.

At the bottom right, there are '< Back' and 'Next >' buttons.

Usually the only edit field that you need to look at is the "Email Address" field. Please enter your email address here.

You may also want to review and edit the following settings (you can change all of these settings in the [PRTG Server Administrator](#) later):

- Optionally you can provide a "Login Name" and "Password" of your choice (the default is username "prtgadmin" and password "prtgadmin"). Selecting a private password is especially important if you plan to make your PRTG website available on the Internet.
- Please review the "Web Server IPs" and "Web Server Ports" settings. In most cases the default values should be fine.
- Optionally you can enter a custom "Site Name" for your PRTG website (e.g. "My Company Monitoring").

Please click "Next" one more time to finish the installation. When the installation is complete, the computer may ask you to restart the machine to properly complete the installation. Although you can choose to reboot later, it is strongly recommended to reboot the machine right away to fully complete the installation.

That's it. You can now work with PRTG Network Monitor!

3.4 Entering a License Key

A license key for PRTG Network Monitor consists of the name of the licensee and a string that contains 70 characters and numbers. This information is usually sent to customers via email:

- Sample Username: Paessler AG
- Sample License key: 0223515-FFSEJC-ZHGRDFM-UR1CS8-U73FGK-G645F2-YVF1DD-H8323N-D11HG9-M2DRG

You can either enter the license key during the installation process or you can use the PRTG Server Administrator tool to enter a license key later.

Step 1: Make Sure You Have Installed the Correct Edition

There are two different installers available for PRTG (see [Downloading the Software](#)):

- The publicly available installer only contains the Freeware, Starter and Trial Editions
- The Commercial installer is only available for download for paying customers

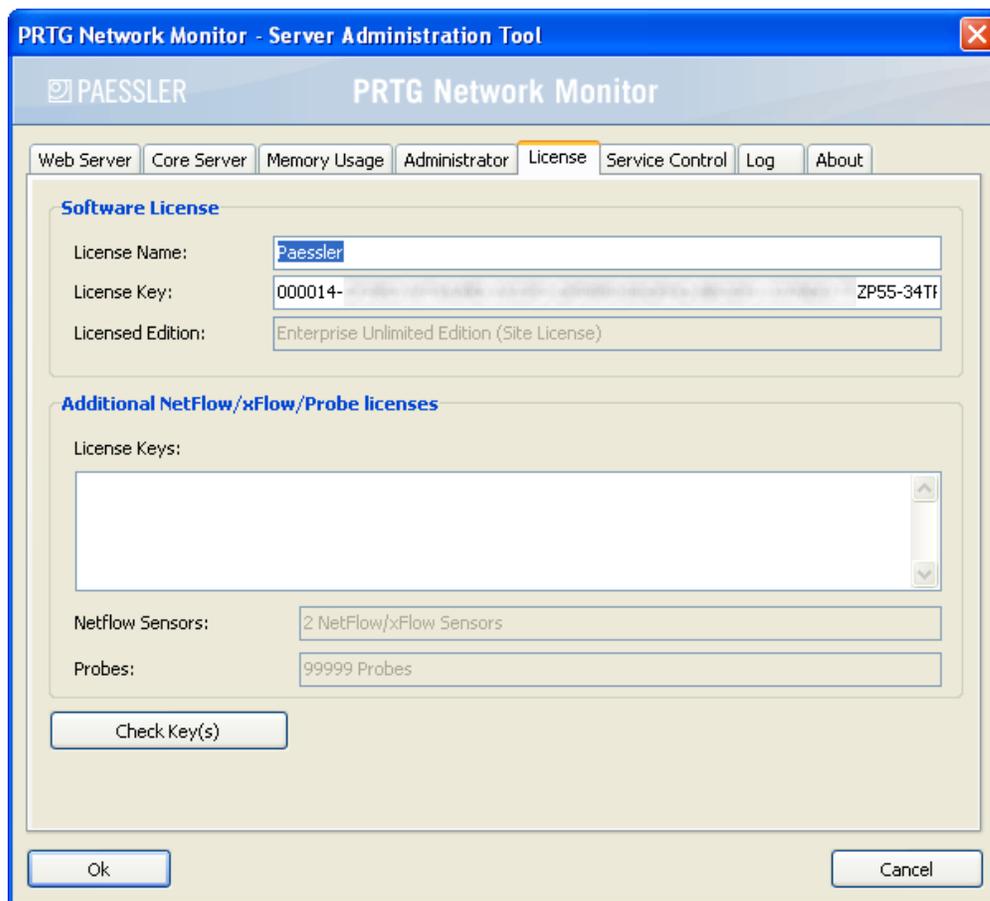
The Commercial Installer must be installed to run the commercial editions of PRTG Network Monitor. **If you have purchased a license key for PRTG you must download and install the latest Commercial Installer from the Paessler website in order to apply your license key.**

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

You must enter the license key into the server administrator program. To start the PRTG Server Administrator select or double click the respective icon:



Select the License tab and enter your license key. To avoid typos please copy and paste the name and the key from the license key email that you have received from Paessler AG:



To make sure your key has been entered correctly please click on "Check Key(s)". In the field "Licensed Edition" you will be able to see the accepted licence key

Entering an xFlow License Key (for NetFlow, sFlow)

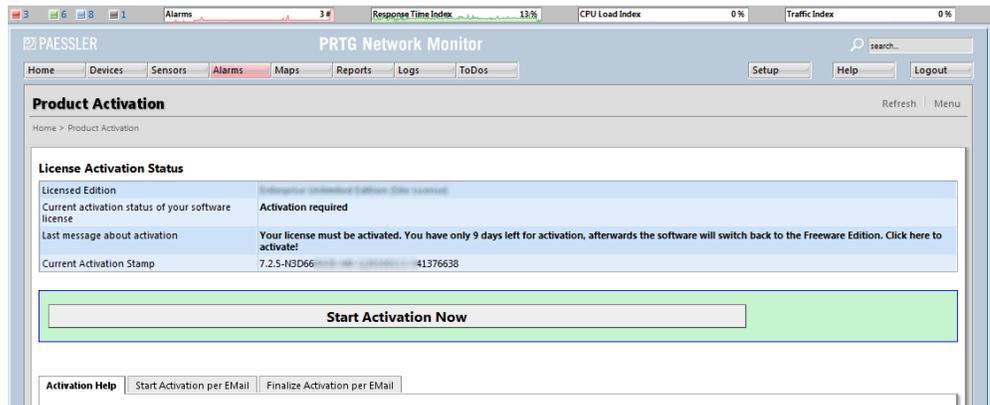
NetFlow/xFlow keys only consist of the code (70 characters and numbers) and are not specific to your company name. If you have purchased a NetFlow/xFlow license key you must also start the Server Administrator tool to enter the key. Select the License tab and paste the key(s) into the "Additional NetFlow Licenses" box. To make sure your key has been entered correctly please click on "Check Key(s)".

3.5 Activating the Product

After installing the PRTG software and entering a license key, you have to run through the Product Activation process in order to use it continuously (only Freeware and Trial Edition are 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 Freeware Edition (with a maximum of 10 sensors) until you activate. Login to the PRTG Web Interface to activate.

Activation via Internet

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



Click on the button "Start Activation Now" to start product activation. PRTG will now connect with Paessler to check your license. A few seconds later you should see "Activation OK" in the License Activation Status.

Activation via Email

In the PRTG Web Interface, choose "Setup | 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.
- Click on "Confirm Activation".

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

3.6 Installation of a PRTG Remote Probe

PRTG has two modules that perform the monitoring: The core server, which handles data storage, web server and a lot more, plus one or more "probes" which perform the actual monitoring. Please see [Multiple Probes and Remote Probes](#) for details and installation instructions.

3.7 Installation of the Windows GUI

The Windows GUI is a native Windows application that communicates with the core server using the PRTG API. All features for day-to-day use are implemented in the Windows GUI (for some features the web interface

is shown).

Please see [Windows GUI](#) for details and installation instructions.

3.8 Uninstallation

To uninstall PRTG Network Monitor:

- Select the Add/Remove Programs option from the computer's Control Panel.
- Select PRTG Network Monitor from the list of programs.
- Click the Remove button to uninstall the program.

Or select the "Uninstall PRTG Network Monitor" icon from the PRTG Network Monitor group in the Windows Start Menu.

Note: During uninstallation, your monitoring data will not be removed automatically.

After the completion of the uninstallation process of the software please check the PRTG Network Monitor installation folder and delete all remaining files that you do not want to keep. Also, please check the "\\Documents and Settings\\All Users\\Application Data\\Paessler\\PRTG Network Monitor\\V7" (Windows XP) folder for remaining data files which are not automatically removed.

Part



IV

Basic Concepts of PRTG Network Monitor

4 Basic Concepts of PRTG Network Monitor

There are a number of basic concepts that lay the foundation for the functionality and ease of use of the PRTG Network Monitor. We have made using our software as easy as possible. Nevertheless, there are some basic principles we would like to explain to you.

Please read this section carefully to make it easier for you to understand how best to use the software.

- [Architecture: PRTG Core Server, PRTG Probe and the User Interfaces](#)
- [Object Hierarchy: Probes, Groups, Devices, Sensors, Channels](#)
- [Inheritance of Settings](#)
- [User Access Rights](#)
- [Alarms Concept](#)
- [Maps Concept](#)
- [Reports Concept](#)
- [Logs Concept](#)
- [ToDos Concept](#)
- [Notifications Concept](#)
- [Schedules Concept](#)
- [Dependencies Concept](#)

4.1 Architecture: PRTG Core Server, PRTG Probe and the User Interfaces

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

Type	Name/Description	See also
System parts	PRTG Core Server This is the central part of a PRTG installation and includes data storage, web server, report engine, a notification system and more.	Below in this section.
	PRTG Probes The part of PRTG on which the actual monitoring is performed.	Below in this section.
Control interfaces	PRTG Web Interface The AJAX-based web interface is used for configuration of devices and sensors, as well as the review of monitoring results.	Section Web Interface .
	PRTG Windows GUI A native Windows application as web interface alternative.	Section Windows GUI .

	Supports the most important features.	
	PRTG iPhone interfaces Monitor your network on the go with the iPhone App for PRTG Network Monitor or the iPhone web interface.	Section iPhone Interfaces .
Basic administration interfaces	PRTG Core Administrator Used to configure very basic PRTG Core Server settings, such as administrator login, web server IPs and port, probe connection settings, system language, and more.	Section PRTG Server Administrator .
	PRTG Probe Administrator Used to configure very basic settings such as name of the probe, IP and server connection settings, and more.	Section PRTG Probe Administrator .

PRTG 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.
- 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.

The built-in, fast and secure web server (no 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 API calls (e.g. for the Windows GUI).

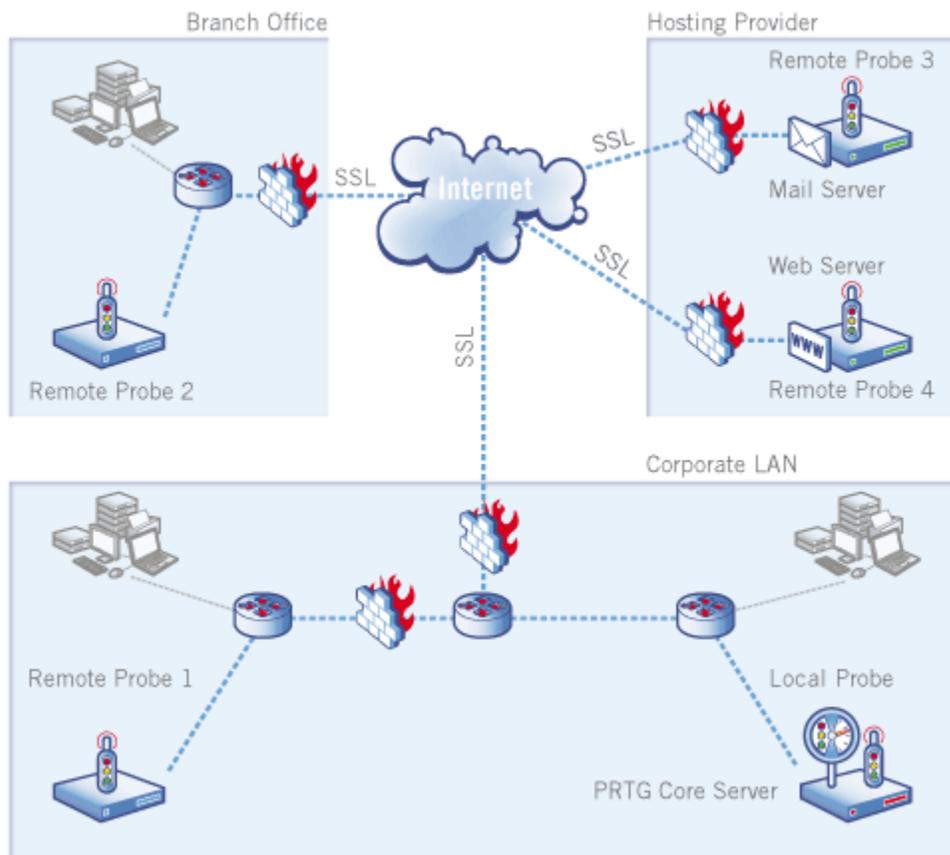
Note: Core server and probe(s) are running as Windows services which are permanently run by the Windows system without the requirement for a logged-in user.

PRTG Probes

On a "probe", the sensors for a device perform the actual monitoring. The probe receives its configuration from the Core Server, runs the monitoring processes and delivers monitoring results back to the Core Server. A Core Server always has a local probe running on the same server. Additionally a Core Server can manage an unlimited number of remote probes in order to achieve multiple location monitoring.

The actual monitoring is performed by PRTG Probe processes which run on one or more computers. During installation the so-called "local probe" is automatically created by the system. In a single-probe installation - which is the default setup - all monitoring is performed by the local probe. Additional so-called "remote probes" must be created by the user. 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. The

following chart shows an example:



To see a video of this, please go to http://www.paessler.com/support/video_tutorials

The PRTG Core Server inside the corporate LAN (bottom right) is able to monitor services and servers in remote offices, data centers and behind firewalls using remote probes. See [Multiple Probes and Remote Probes](#) for more information on remote probes.

After receiving their configuration from the core system, all probes are able to work independently of the core server for some time, e.g. in case the connection between probe and core is lost due to connectivity problems. 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.

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

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 "Probe Health", a "Disk Free" sensor, and a bandwidth sensor for all installed network cards:



It is recommended to keep these sensors, but you can optionally remove all except for the "Probe Health" sensor. It measures 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 sensor's channels for details.

4.2 Object Hierarchy: Probes, Groups, Devices, Sensors, Channels

All objects in PRTG 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, locations or services.

Devices, Sensors, Channels

In PRTG Network Monitor, you can add "Devices" that you want to monitor. These devices can be for example:

- A web or file server.
- A router or a network switch.
- A so called "Probe Device", which is a PRTG-internal system device. This device has access to the computer on which the probe is running on.
- Almost every device in your network that has its own IP address.

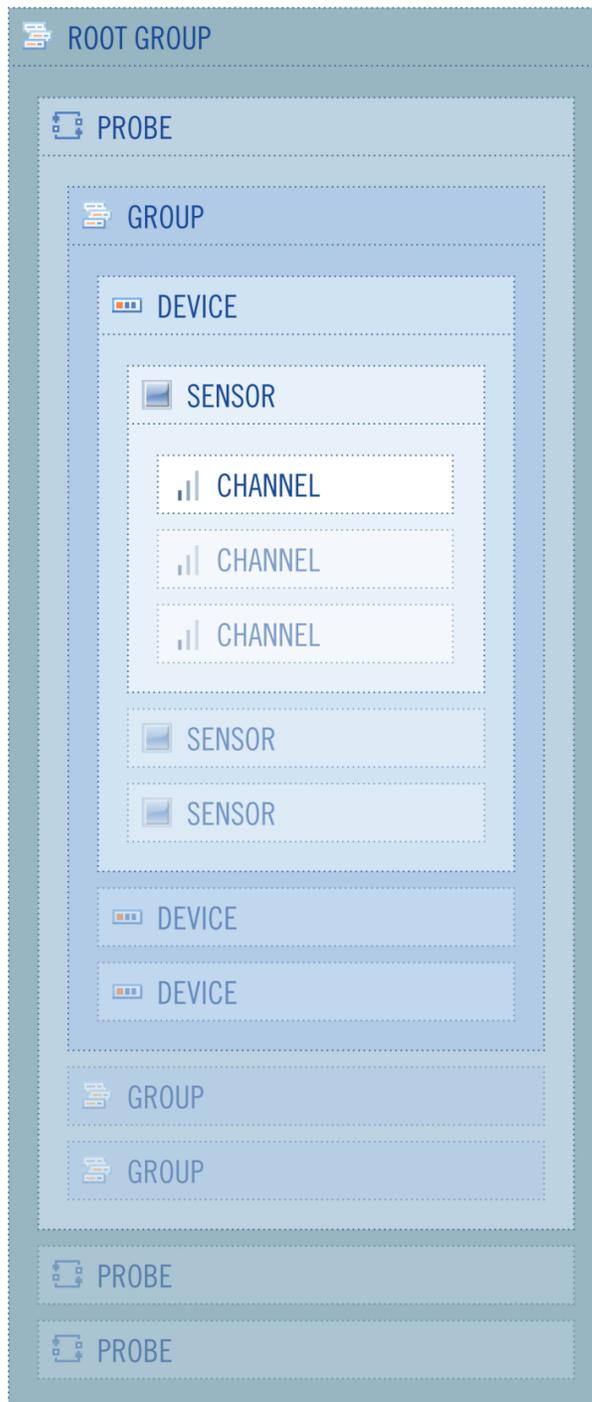
Each device has a number of "Sensors", where the actual monitoring is performed. Each of these sensors monitors one single aspect of a network device. For example:

- One network service like SMTP, FTP, HTTP, etc.
- The traffic of one port of a network switch.
- The CPU or memory load of a device.
- One network card's traffic.
- One NetFlow device, etc.

Each sensor has a number of "Channels" through which it receives the different data streams. Channels can contain, for example:

- Downtime and Total (for a WMI CPU Load sensor).
- Downtime, Percent Available Memory and Available Memory (for a WMI Memory sensor).
- Downtime, Average (for a PING sensor).
- Downtime, Loading time, Bytes received, Download Bandwidth and Time of first Byte (for a HTTP advanced sensor).
- Data for SMTP, HTTP, FTP, PING, etc. (for Packet Sniffer and xFlow sensor), etc.

Groups and Probes



Each device is part of a "Group". You can arrange your devices in different nested groups to reflect the structure of your network.

Each 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](#)).

Finally, the "Root" group is the topmost instance in PRTG, which contains all other objects.

The hierarchical order described is also used to define common settings for larger groups of objects, e.g. settings of the root group usually apply to all other objects below it (see section [Inheritance of Settings](#)).

Here is a sample configuration with one probe, several groups, devices and their sensors:

Root

- PRTG Monitoring Station (Local Probe on 127.0.0.1)**
 - Probe Device
 - Probe Health 100%
 - Disk Free 40%
 - Intel(R) PRO_1 150 kbit/s
 - Group 1**
 - Group 1a**
 - Mail Server 1
 - PING 1 1 msec
 - Messages in q 140 #
 - Queue Size 1 1 MByte
 - CPU Load 1 3%
 - Disk Free 1 65%
 - Memory 1 36%
 - Pagefile Usage 0%
 - IMAP 1 5 msec
 - POP3 1 4 msec
 - SMTP 1 7 msec
 - Web Server 1
 - PING 4 2 msec
 - HTTP 2 76 msec
 - IS Files Sent 2 0.03 Files/s
 - CPU Load 2 2%
 - Disk Free 2 65%
 - Memory 2 19%
 - HTTP 3 81 msec
 - Group 1b**
 - Firewall 1
 - PING 3 2 msec
 - Web Interface 413 msec
 - Port 1 24 kbit/s
 - Port 2 28 kbit/s
 - Port 3 48 kbit/s
 - Port 4 28 kbit/s
 - 48-port Switch 1
 - PING 2 2 msec
 - HTTP 1 884 msec
 - (001) to SW2 425 kbit/s
 - (002) to PC SW 795 kbit/s
 - (004) Ethernet 1.168 kbit/s
 - (005) Ethernet 8 kbit/s
 - (010) Service F 6 kbit/s
 - (011) Service F 6 kbit/s
 - (012) Service F 5 kbit/s
 - (013) PIP 164 kbit/s
 - (014) FRANK 501 kbit/s
 - (015) NAS1 708 kbit/s
 - (016) Ethernet 963 kbit/s
 - (022) Terastat 11 kbit/s
 - (025) to sw2 327 kbit/s
 - (026) to PC SW 657 kbit/s
 - (027) Temp Ra 8 kbit/s
 - (032) LENNY 804 kbit/s
 - (034) Service F 6 kbit/s
 - (035) Service F 6 kbit/s
 - (036) Service F 6 kbit/s
 - (037) POP 1.145 kbit/s
 - (038) HANK 482 kbit/s
 - (039) NAS2 27 kbit/s
 - (045) Mirror Pc 822 kbit/s
 - (046) Tape Lib 6 kbit/s
 - (047) VPN Dev 8 kbit/s
 - (048) Cisco Fir 820 kbit/s
 - (053) Uplink to 775 kbit/s
 - (054) Workstat 1.452 kbit/s
 - Group 2**
 - NAS 1
 - PING 5 3 msec
 - CPU Load 3 5%
 - Disk Free 3 34%
 - Memory 3 66%
 - NIC 1 180 kbit/s
 - NIC 2 441 kbit/s
 - NIC 3 180 kbit/s
 - Linux Server
 - PING 7 2 msec
 - CPU Load 4 11%
 - HTTP 4 27 msec
 - Network Traffic 64 kbit/s
 - ESX Server 1
 - PING 6 3 msec
 - ESX Server He 10%
 - VM 1 2%
 - VM 2 1%
 - VM 3 1%
 - VM 4 2%
 - VM 5 2%
 - CPU Load 0.33%
 - NIC 1 26 kbit/s
 - NIC 2 174 kbit/s
 - Processes 74 Processes
 - VoIP Server
 - PING 8 7 msec
 - IP SLA 1 msec
 - IP SLA 40 msec
 - CPU Load 5 7%
 - (001) BR10/1/0 < 0.01 kbit/s
 - (004) BR10/1/1 < 0.01 kbit/s
 - (021) FastEthe 95 kbit/s
 - (022) FastEthe 95 kbit/s
 - (024) FastEthe 95 kbit/s
 - (025) FastEthe 95 kbit/s
 - (026) FastEthe 95 kbit/s
 - (027) FastEthe 94 kbit/s
 - (028) FastEthe 94 kbit/s
 - (029) FastEthe 97 kbit/s
 - Free I/O Mem 65.231 kb

Priority

The basic idea of the priority concept is ensure that the most important sensors are always shown first in the sensors and alarms lists. This guarantees you never miss an important outage.

You can specify a priority for each object in the sensor tree, shown with 1 star ("*") for the lowest priority to 5 stars ("*****") for the highest priority. By default, PRTG sensors are sorted first by priority and then alphabetically by name in lists like "Alarms" or "Sensors". The default priority is three stars ("***") so you can prioritize objects in your configuration quickly. Simply left click an object and select the desired setting from the context menu:



You can also click on the stars directly in an object's detail view.

Favorite Sensors

Another method to highlight important sensors is to mark them as "Favorite Sensors", also accessible through a sensor's context menu. A list of the favorite sensors can be found in the Sensors menu ("Sensors | Favorite Sensors").

4.3 Inheritance of Settings

The hierarchical list is not only used to group sensors to organize them, 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).

You can override this inheritance on any level of the hierarchy by setting a different value for a specific group, device or sensor. All objects below will inherit these new settings, not the ones from levels above.

Settings that are inherited among all objects include:

- Monitoring interval.
- Notifications and Triggers.
- Windows authentication settings and WMI compatibility settings (for WMI sensors).
- ESX/ESXi Server authentication settings (for VMware servers)
- SNMP authentication settings and compatibility settings.
- Channel and unit configuration.
- User access rights.
- Paused status: If an object is paused by the user, by a schedule or by a dependency, all associated sensors are paused as well.

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

The actual overriding of the parent's settings takes place by deselecting the checkbox "Inherit ... from ..." on the object's settings page. As an example, this screenshot shows Windows authentication settings after deselecting the checkbox:

<input type="checkbox"/> Inherit Credentials for Windows Systems from parent object (Group) (Domain or Computer Name: <empty>, Username: <empty>)		
Domain or Computer Name	<input type="text"/>	Enter an authority for the Windows access (domain or computer name for the user account)
Username	<input type="text"/>	Enter a login name for the Windows access
Password	<input type="text"/>	Enter a password for the Windows access

Default values

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 "public" community string (default values for most devices).

- No entry in object "Schedules and Dependencies", no Windows authentication account.
- A set of schedules (in Setup).
- Various data purging settings.

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

Tip: Before sensor setup, go to the root group and set the defaults to values that suit your setup (including necessary credentials). This will make things easier later.

4.4 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 using an unlimited number of groups (which also control their security settings).

There are Administrator users, Read/Write Users and Read Only Users. With these tools, you can create a rights management that allows you to specify exactly what users will be able to see and edit. 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 he sees 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 group. Again, these settings are inherited.

See section [User Management](#) for more information.

4.5 Alarms Concept

Alarms are sensors in Error, Warning or Unusual state. The Alarm page shows the list of sensors that are in one of these states. If all your systems are running fine this page should not list any sensors at all. The Alarm overview is a good start if you want to solve problems in your network. Using the on-mouse-over main menu, you can select what kind of Alarms you want to see. The options are "All", "Errors only", "Warnings only", and "Unusuals only". Additionally to browsing the pages, you can also re-sort the data shown in the Alarm list just by clicking on the column headers or change the item count per page (available for big lists).

4.6 Maps Concept

Using "Maps" you can create personalized overviews and dashboards of your monitored network. A map can include a background image, such as a network drawing. You can place status icons, lists of sensors as well as graphs with your current monitoring status on the map.

You can define any number of maps and use them to create a NOC (Network Operation Center) Dashboard, an overview of the network status for your Intranet, a webpage with the graphs of your most important sensors and more. By setting the Access rights to "Public Access", you can provide others with URLs to a map so they can view the data without the need for a user account.

Read more about this in the section [Maps](#).

4.7 Reports Concept

"Reports" are used to analyze monitoring data, either once or at specified intervals. You can define any number of reports, specify the sensors for a report, select a template and run them at any interval you like, such as once,

daily, weekly or monthly.

Read more about this in the section [Reports](#).

4.8 Logs Concept

In the Log 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.

To support you when viewing the log files, there are several filters available. Move your mouse pointer over the "Logs" main menu item, and from the appearing menu, select a filter. Filters "By Group", "By Status Change" and "By System Events" are available. Select "All" to see all log entries unfiltered. Additionally to browsing the pages, you can also use the controls in the upper right corner of the list to change "Date Range" and "Item Count" of the currently shown list.

4.9 ToDos Concept

Whenever PRTG comes across an event or monitoring object that needs the administrator's attention, it will add an entry to the "ToDos" list and send an email to the admin user.

ToDos are created when:

- A new device or sensor has been created by the auto discovery process and should be acknowledged by the user.
- A new probe connects to the core 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, etc.

Read more about this in the section [ToDos](#).

4.10 Notifications Concept

Whenever PRTG discovers downtime, an overloaded system, threshold breach or similar situations, it will send a "notification". Notifications use various methods by which you can be notified (e.g. email, SMS, pager message and others). After creating notifications in the system settings, you can select them on the setting pages for a group, a device, and a sensor.

See [Notifications](#) for more details.

4.11 Schedules Concept

Group, device or sensor monitoring can be paused by user intervention or by a "schedule" (e.g. "don't monitor Sundays between 4 and 8 a.m."). Using schedules, you can limit the monitoring time. PRTG comes with a number of pre-defined schedules. You can activate schedules in the Settings menu of a group, a device or a sensor by changing the "Inherit Schedules and Dependencies" entry. Schedules are also used in [Reports](#) and for [Notifications](#).

To change the default pre-defined schedules or to add your own schedule, enter the account settings menu (via "Setup | Schedules").

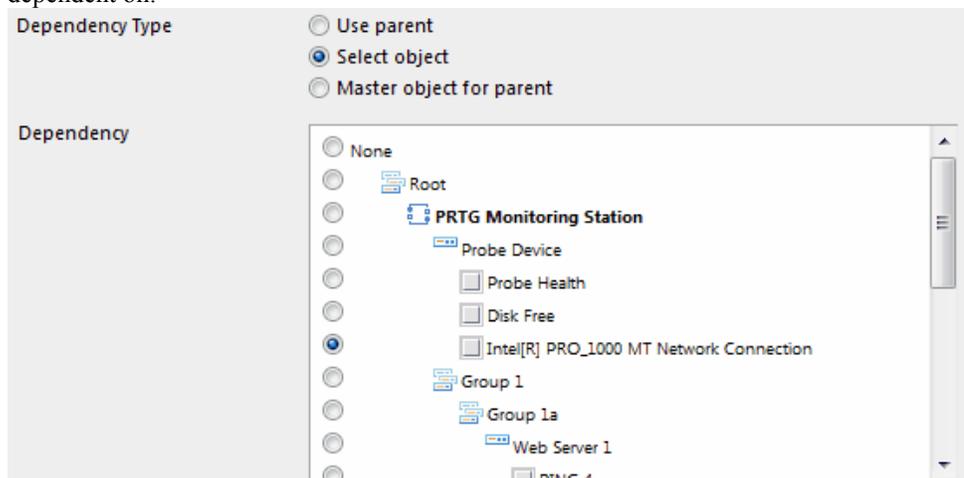
See [Account Settings - Schedules](#) for more details.

4.12 Dependencies Concept

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 down. This means, for example, you can stop monitoring remote network services when the corresponding firewall is down due to connection problems.

You can edit dependencies in the "Inherit Schedules and Dependencies" entry in an object's Settings menu. There are three options for dependencies:

- "Use parent": By default, all objects depend on their parent object. This means that if you specify a dependency for a group and the dependency sensor goes down, all sensors in the group will be paused.
- "Select object": With this option, you can select from a list the object from which your object shall be dependent on:

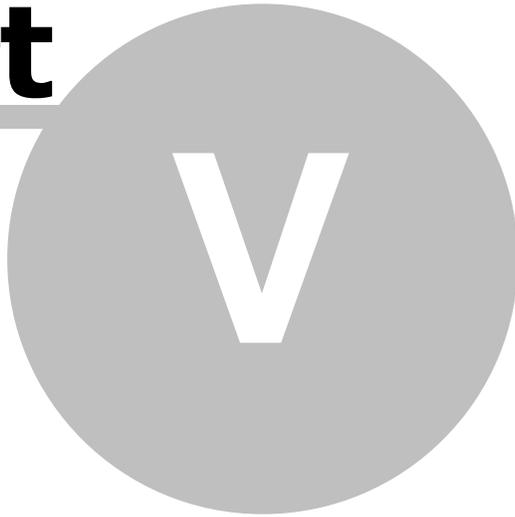


As soon as the object you have chosen from the list enters a "red" state (goes down), the monitoring for the dependent object (and all its child objects) will be paused and no notifications will be sent.

- "Master object for parent": This setting will make the current object the so-called "master object" for its parent device. All sensors of the parent device will be paused whenever this master sensor is down. It is recommended to set a basic sensor (e.g. PING) to be the master sensor (for example, the auto-discovery sets the PING sensors for each device as the master object).

Tip: Testing your dependencies is easy! Simply choose "Pause | Set sensor to error" from the context menu of a sensor that other objects depend on. A few seconds later all dependent sensors should be shown with a blue "paused" icon. Select "Pause | Resume" from the sensor's context menu to restart monitoring afterwards.

Part



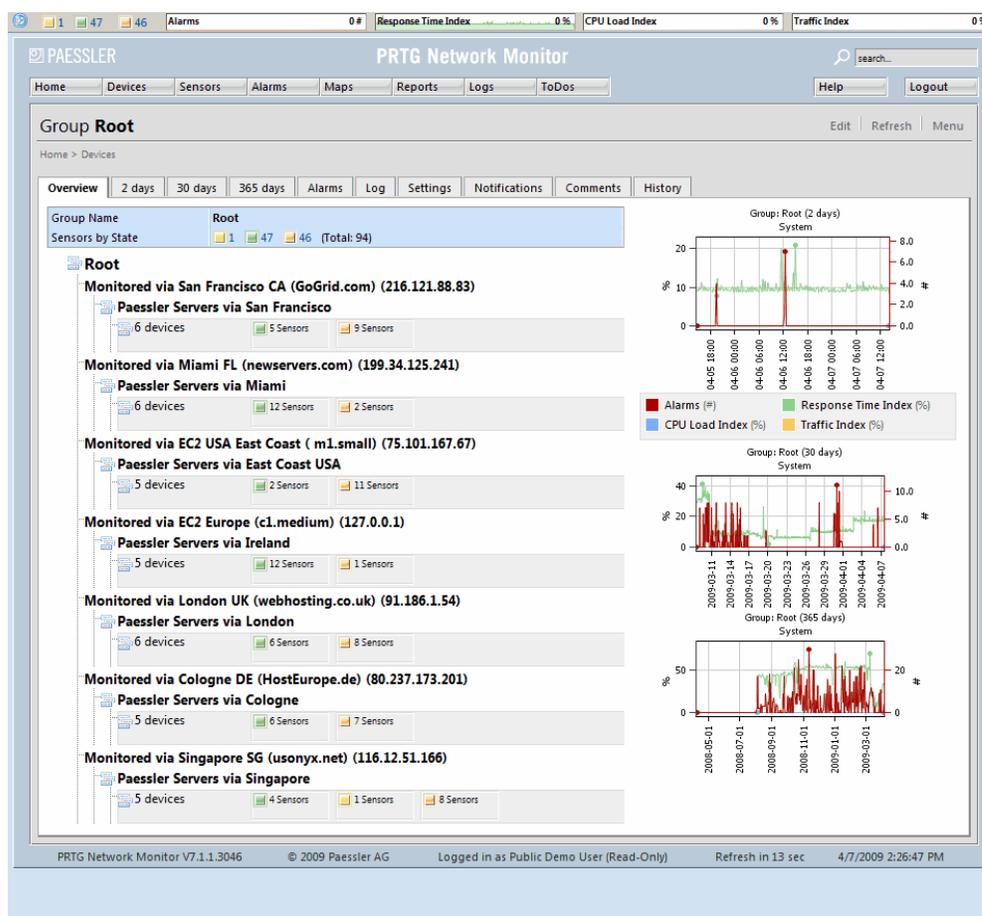
User Interfaces

5 User Interfaces

With PRTG Network Monitor you have several options for the user interface. You can use all of them at the same time and you can use multiple copies at the same time, too (e.g. by opening several browser windows or by running the Windows GUI on several computers).

Web Interface

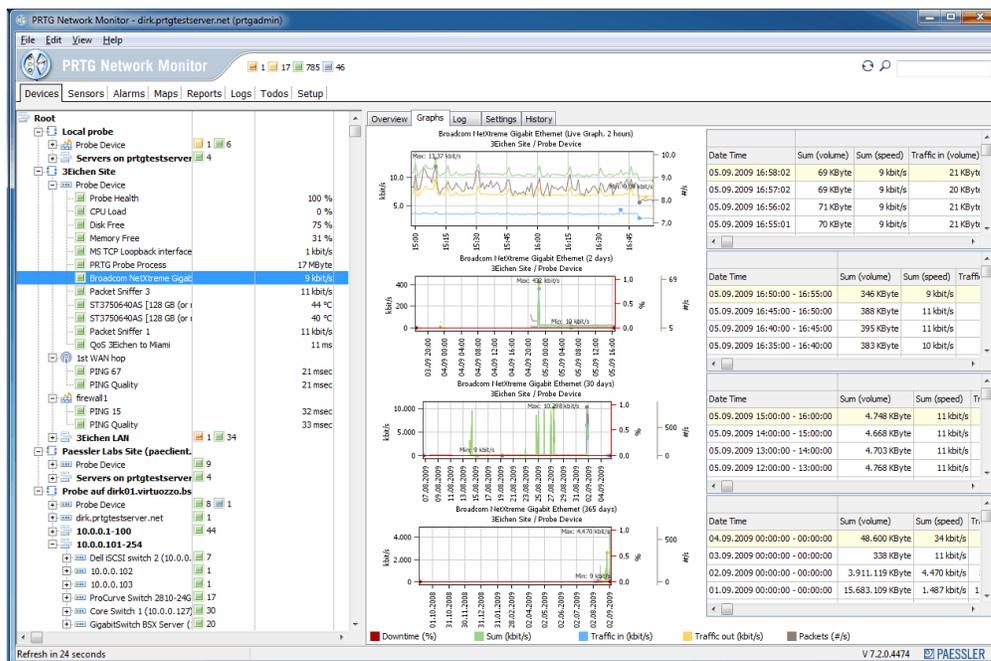
The main interface is a browser-based interface which is used to configure the software, set up sensors, review current status and create reports. Using an advanced control concept, it provides full functionality and is the first choice for new users. Here is a screenshot:



Read more about it in section [Web Interface](#).

Windows GUI

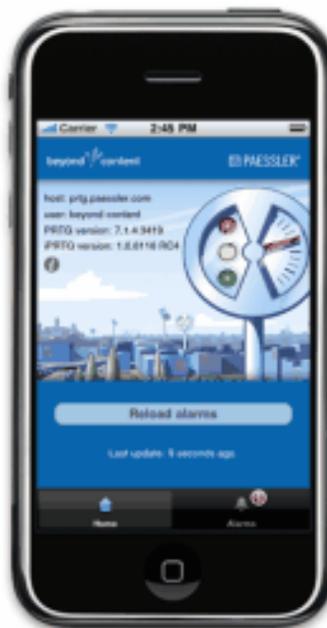
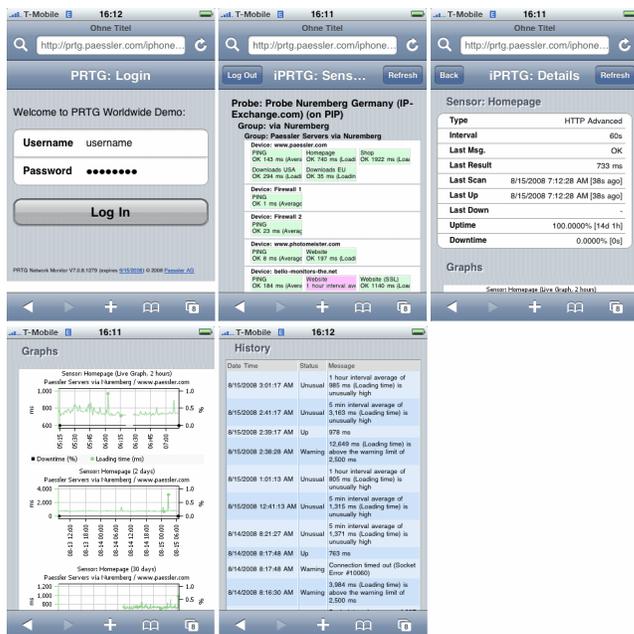
The Windows GUI allows you to completely control your PRTG installation using a native Windows application. When minimized it sits in your system tray and displays popups or plays alarm sounds whenever new alarms or events happen. When maximized you have access to the sensor tree, detailed information about groups, devices, sensors, maps, reports and logs:



Read more about it in section [Windows GUI](#).

iPhone Interfaces

If you have an iPhone, you can access a built-in web browser based user interface that is optimized for the iPhone or you can purchase the iPRTG app for PRTG:



Read more about it in section [iPhone Interfaces](#).

5.1 Web Interface

The AJAX-based web interface is used for the configuration of devices and sensors, as well as the review of monitoring results. The web interface is highly interactive and uses AJAX ("Asynchronous Javascript and XML") to deliver a powerful and easy-to-use user experience. While the user is logged in, 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 by the user).

Login

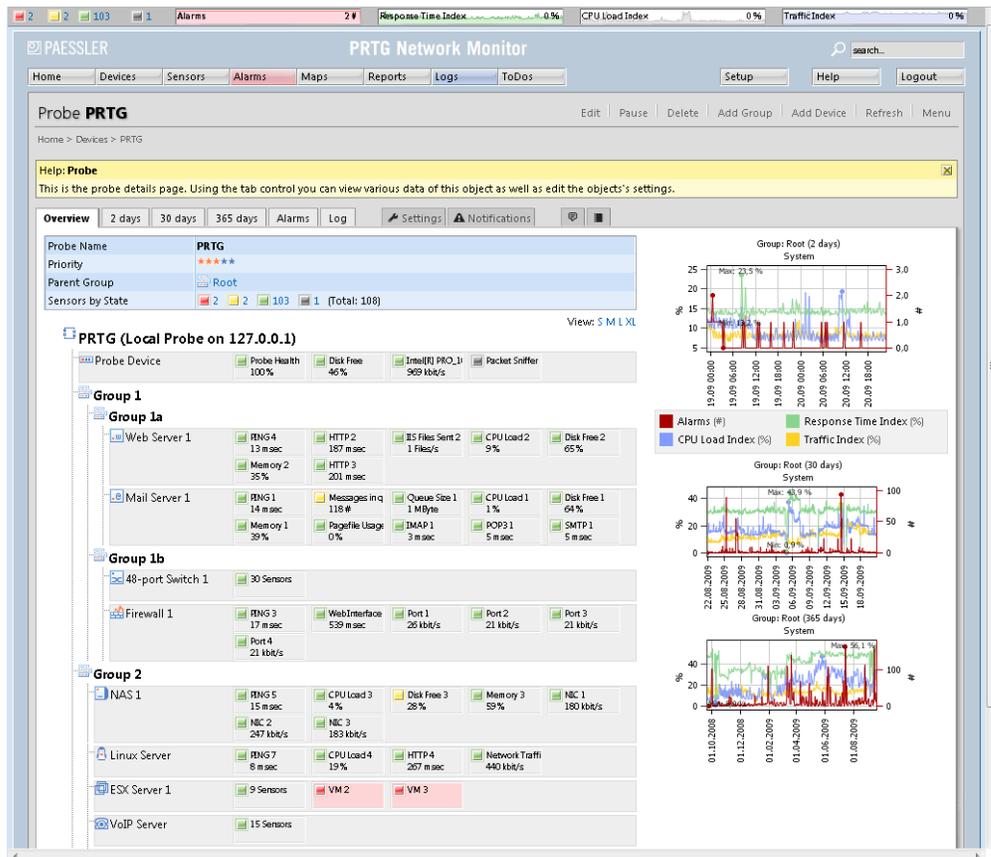
As default, login name and password are both "prtgadmin" (without the quotes), unless specified differently during setup. You can change login name and password any time using [PRTG Server Administrator](#).

The Interface

After logging into the web interface, you will see PRTG's welcome page as default. This page helps you to add sensors manually, perform an automatic network search, review results, download the Windows-GUI or iPhone applications and get further help and support.



By clicking on "Review Results", you enter the tree-like device view which will be your starting point for everyday use. Please have a look at this screenshot of PRTG's device page in the web interface:



The main layout consists of a status bar at the top, the header area with the main menu and quick-search box below it and, finally, the main page content (all these elements are described in the next section).

When you navigate through PRTG's web interface you will always use one of the following five 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.
- And, finally, you are able to drill down into the object hierarchy of probes, groups, devices and sensors in the object tree shown above by merely clicking a sub-object of the currently displayed object (e.g. a sensor on the device page).

These five 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.

Let's have a detailed look at PRTG's web interface -building blocks:

Global Status Bar and Sensor Colors



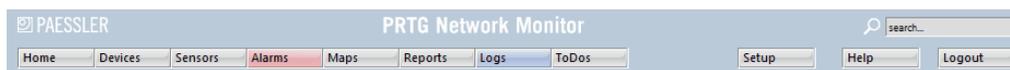
This bar is always shown above all pages. It shows the aggregated status of all sensors you have configured for monitoring. Depending on the sensors' status you will see colored squares with numbers which symbolize the sensors (in the screenshot above, 23 sensors are red, 3 are yellow, 95 sensors are green, 129 sensors are blue and 40 are orange).

The color of a sensor always shows it's current status:

Sensor Status		Meaning
	Red	Down
	Red (confirmed)	Down - this status is additionally verified
	Yellow	Warning
	Green	OK
	Blue	Paused
	Orange	Unusual
	Black	Unknown (sensor has not been checked yet)

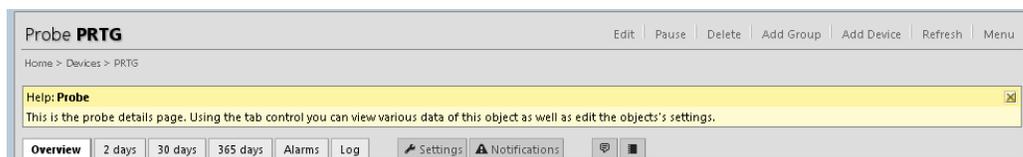
The four graphs in the global status bar show the number of alarms as well as three "Index" graphs for response time, CPU load and bandwidth traffic usage over the last 24 hours. These graphs are "index" graphs, similar to a stock index. The values are based on the readings of all sensors, groups or devices. They are computed by using statistical computations and by comparing the values to the highest and lowest readings ever recorded. For example, a CPU Load Index value of 90 % means that the average CPU load for all CPU sensors of your current configuration lies at 90 % of the highest ever measured CPU usage value.

Website Header Area, Search Box and Main Menu



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. Menu item "Alarms" is highlighted with red color whenever there is an alarm. "Logs" and "ToDos" are highlighted with blue color if new messages or new ToDos are available. To search for any monitoring object, simply 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.

Page Header and Tabs



The individual page content starts below the website header area. Depending on the page's content you will see a menu and a few action links on the right. "Breadcrumbs" that will always show the path back to the homepage can be found below the heading. The yellow boxes display context sensitive help which can be hidden by clicking the small "x" on the top right.

Many pages have a tab-like interface. Using these tabs you can navigate to various sub-pages for an object:

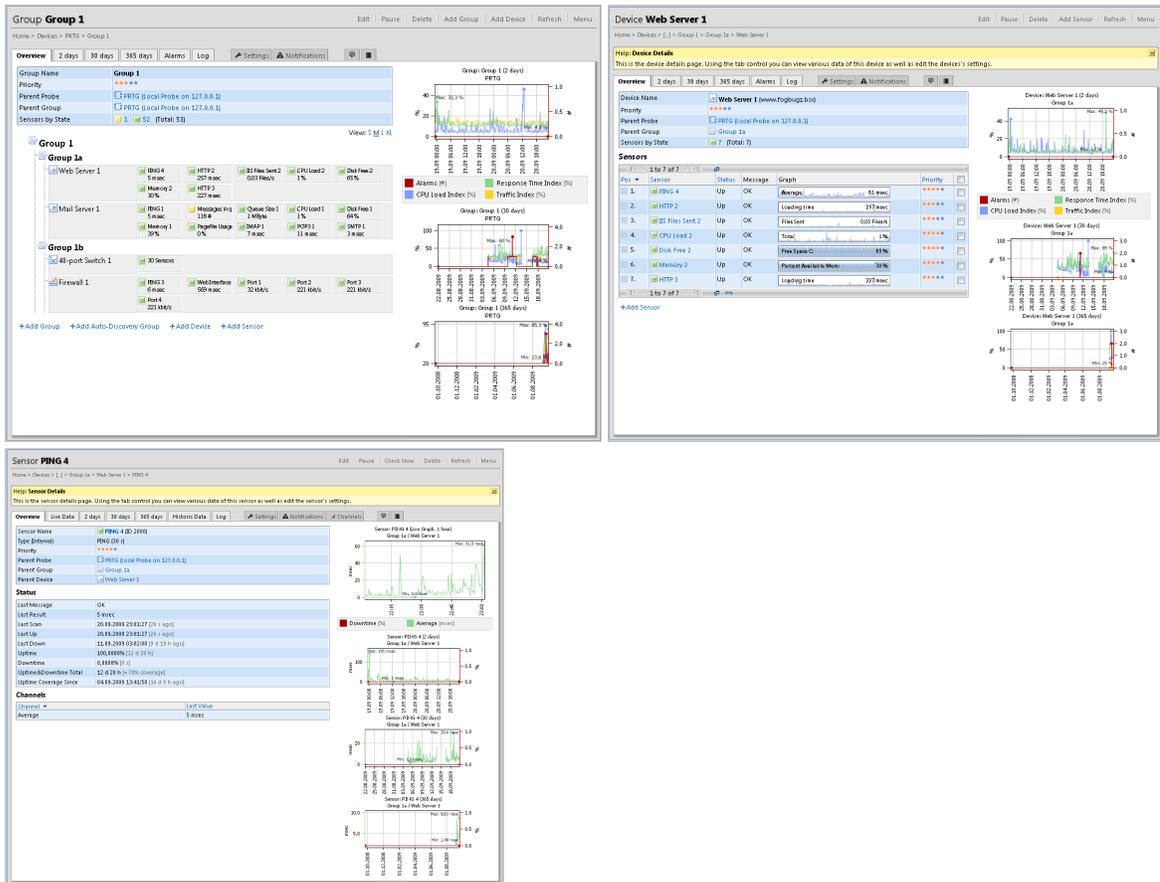
Tab(s)	Description
"Overview"	All monitoring objects offer this tab providing a quick overview of all parameters and statuses.
"Live Data", "48 Hours", "30 Days", "365 Days"	These three or four tabs show the group's, device's or sensor's historical graphs and data tables (note: live data is only available for sensors).
"Historic Data"	With this function, you can review or download historic sensor data. See below for further explanations ("Reviewing Historic Data").
"Alarms" and "Log"	Shows a list of current alarms and historic events for an object (and its child objects).
"Settings" and "Notifications"	Allows you to edit an object's settings and notifications. The available settings depend on the kind of object you are editing.
"Channels"	This tab is only available for sensors. Each sensor has one or more channels on which it stores data. In this tab, you can configure how a channel's values are processed. See section Edit Sensor and Channel Settings for more details.
"Comments"	Provides a notepad for your own comments.
"History"	Shows a lifetime log for each object (who created it, who edited it etc.).

These are the most common tabs. Please note that you will also see other tabs for other objects.

If you make any changes in a tab, please make sure you click on the "Save" button to save your changes. If you change tabs without saving, your changes will be discarded.

Overview Page for Groups, Devices and Sensors

Have a look at the following three screenshots showing the "Overview" tab of a group, a device and a sensor:



You can see that all three share a common layout:

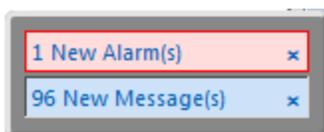
- On the upper left you have the object's name, basic settings and sensor status.
- Below that there is a list of child objects (devices for a group, sensors for a device and channels for a sensor).
- On the right there are three or four graphs showing recent history. To zoom into a graph, simply click on it (or choose the appropriate tab).

For sensors you will see four graphs that show all "channels" of the sensor for the last 2 days, last 30 days and last 365 days plus a live graph. For groups and devices there are three graphs that show the alarms, CPU load index, traffic index and response time index (explained above) for the last 2 days, last 30 days and last 365 days. Details about index calculation are available in the Paessler Knowledge Base at http://www.paessler.com/support/kb/prtg7/how_prtg_computes_index_graphs.

Note: Time frames can be changed in the [PRTG Server Administrator](#) ("Memory Usage" tab).

Box with Alerts

Every time a new event occurs while you are logged into the web interface of PRTG Network Monitor a box with alerts will show up in the lower right corner of your browser window:



Please keep an eye on these important messages which PRTG will display as it discovers changes in the network or requires your attention for other reasons. Simply click the text inside the colored bar to navigate to the detailed information page or click one of the "x" symbols to dismiss and hide the alert. In the user account settings you can control which events actually display the popup. There, you can also disable this feature.

Context Menus

Although context menus may seem unusual for a web-based application, they are the key to user interface's ease of use. Almost all objects that appear as links in the user interface will show a context menu when you right-click them. Using it, you can access every relevant function of an object. Here are three sample context menus (for group, device and sensor).

Group Menu	Device Menu	Sensor Menu
Details...	Details...	Details...
Settings...	Settings...	Settings...
Add Group...	Add Sensor...	Create Report...
Add Auto-Discovery Group...	Run Auto-Discovery	Check Now
Add Device...	Create Device Template...	Delete...
Run Auto-Discovery	Create Report...	Clone...
Create Report...	Check Now	Pause
Check Now	Delete...	Fold
Delete...	Clone...	Move
Clone...	Pause	Priority/Favorite
Pause	Fold	Historic Data
Fold	Move	Tools
Move	Priority/Favorite	
Priority/Favorite	Historic Data	
Historic Data	Tools	

Note: If you want to access the browser's own context menu, hold the CTRL key down when right-clicking.

Working with Lists and Multi Edit Menus

Throughout the web interface often you will see lists of items, e.g. sensors, devices, maps, reports etc. All these lists provide common functionality. Here are two sample lists (sensors and logs):

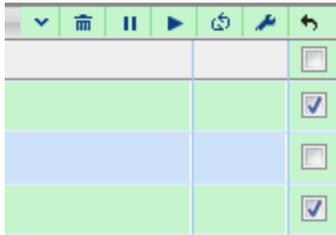
Pos	Sensor	Status	Message	Graph	Priority
1.	PING 1	Up	OK	Average 3 msec	★★★★★
2.	Messages in queue 1	Warning	139 # (Messages) is above the warning limit of 2 #	Messages 139 #	★★★★★
3.	Queue Size 1	Up	OK	Size 1 MByte	★★★★★
4.	CPU Load 1	Up	OK	Total 4 %	★★★★★
5.	Disk Free 1	Up	OK	Free Space C: 65 %	★★★★★
6.	Memory 1	Up	OK	Percent Available Mem 36 %	★★★★★
7.	Pagefile Usage 1	Up	OK	Total 0 %	★★★★★
8.	IMAP 1	Up	OK	Available 2 msec	★★★★★
9.	POP3 1	Up	OK	Response Time 3 msec	★★★★★
10.	SMTP 1	Up	OK	Available 3 msec	★★★★★

Date Time	Parent	Type	Object	Status	Message
04.09.2009 15:13:27	None	User	PRTG System Administrator	Edited	See history for details.
04.09.2009 14:21:00	Mail Server 1	Exchange Server 2003 (WMI)	Messages in queue 1	Warning	139 # (Messages) is above the warning limit of 2 #
04.09.2009 14:20:27	Group 1a	Device	Mail Server 1	Resuming	Resumed by Dependency
04.09.2009 14:20:27	Group 1a	Device	Mail Server 1	Active	
04.09.2009 14:20:27	Mail Server 1	Exchange Server 2003 (WMI)	Messages in queue 1	Resuming	Resumed by Dependency
04.09.2009 14:20:27	Mail Server 1	Exchange Server 2003 (WMI)	Queue Size 1	Resuming	Resumed by Dependency
04.09.2009 14:20:27	Mail Server 1	WMI CPU Load	CPU Load 1	Resuming	Resumed by Dependency
04.09.2009 14:20:27	Mail Server 1	WMI Memory	Memory 1	Resuming	Resumed by Dependency

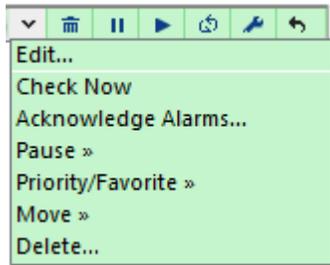
The following functions are available for lists:

Feature	Display	What it does
Paging		Use the small triangular icons at the top or bottom to walk through a list page by page.
Sorting		You can re-sort a list by clicking the header of the column you want to use as sorting index.
Date Range		When viewing log lists, you can click on "Date Range" to change the desired date range.
Item Count		Some lists offer the possibility to change the number of entries in the list by clicking on "Item Count".
New window		Opens the table in a new window.
Show XML		Views list as XML (your browser may offer you an XML file download).

Additionally some lists offer a column of checkboxes. The checkboxes are used to select two or more items from the list and work with the selected items. As soon as you select one or more checkboxes, an additional, green colored menu will show up:

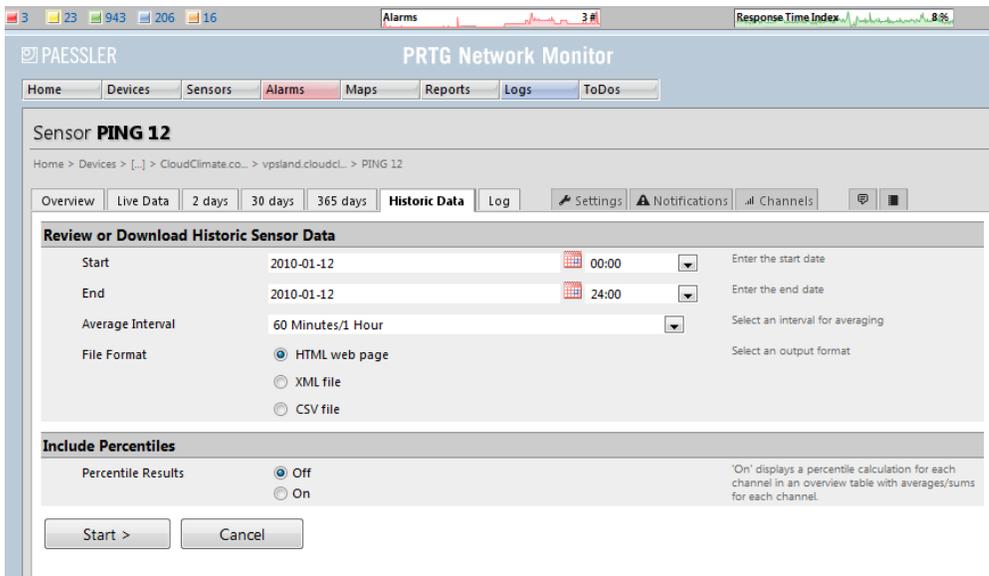


Depending on the object type different functions are available. Some frequently used functions are available as quick buttons, other functions are available in the drop down menu:



Reviewing Historic Data

Additionally to exhaustive reports that additionally can be scheduled for regular execution (see section [Reports](#)), 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 for further processing in external applications. To get to the Historic Data reports, choose a sensor, right-click on it and from the context menu, select "Details...". In the sensor's detail view, click on the "Historic Data" tab to start the review.



You can select the following options:

- Start: Enter the start date and time of the data you want to review.
- End: Enter the end date and time of the data you want to review.

- **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), a few seconds, minutes, hours, or a whole day. 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.
- **File Format:** This is the output format for the report. You can select between an HTML web page, an XML file and a CSV file (for import in Microsoft Excel, for example).
- **Include Percentiles:** Activate this option to add a percentile value to the report. See section [Calculating Percentiles](#) for more information.

Click on "Start" to generate the Historic Data report. Please note: Depending on the selected output format, either a new browser window or tab will open and show an HTML web page, or the browser will start the download of an XML or CSV file. If you just generated an HTML web page report and it is still opened while you are generating another, no new browser window or tab will open, but instead the existing HTML web page will be refreshed and it will show the most recent report.

During report calculation PRTG may allocate large amounts of RAM (depending on average interval and the report time span). To avoid system overload and ensure system stability PRTG automatically limits the minimum average interval depending on the time span automatically (selected via Start and End date):

Level of Detail	Maximum Timeframe in Historic Data Report
Raw Data (all single monitoring requests)	For up to 24 hours/1 day
Averages between 1 and 60 minutes	For up to 24 hours/1 day
Averages between 60 and 1440 minutes	For up to 30 days
Averages for one or more days	For up to 365 days/1 year

5.2 Windows GUI

This program is a native Windows application that communicates with the Core Server using the [PRTG API](#). All features for day-to-day use are implemented in the Windows GUI (for some features the web interface is shown).

Install

The Windows GUI is automatically installed on the computer where you have installed your PRTG Core Server. To use the Windows GUI on other computers, simply download and install the software from PRTG's web interface (select menu item "Setup | Downloads"). It can be installed on all Windows versions (XP or later).

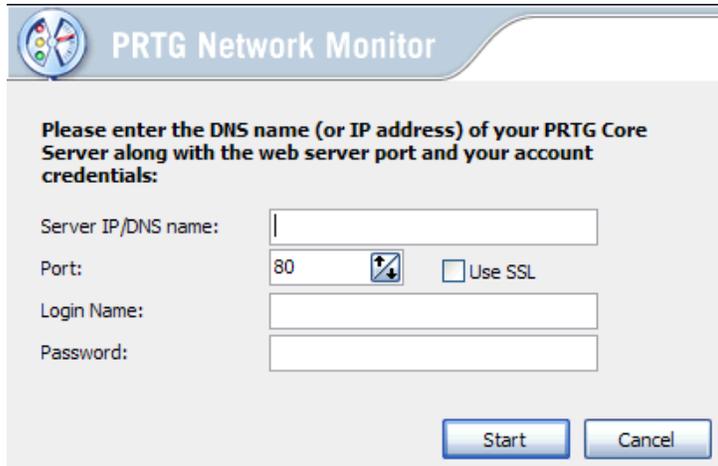
The Windows GUI runs in two modes:

- **Graphical user interface for PRTG:** You can add/edit groups, servers, devices and sensors (includes viewing sensor data and graphs as well as comparing sensor data). You can review and configure alarms, maps and reports.
- **Tray tool:** runs on your PC in the background and will notify you with popups, sounds etc. whenever PRTG discovers changes in your network.

The Windows GUI shares many concepts with the web interface and also opens a browser window for some features. For new PRTG users it is recommended to start with the [Web Interface](#) before using the Windows GUI.

Login Information

When you start the Windows GUI for the first time it will ask for "Server IP/DNS name" and your credentials. Please enter the same "Server IP address/DNS name", "Login Name" and "Password" that are set in the [PRTG Server Administrator](#).



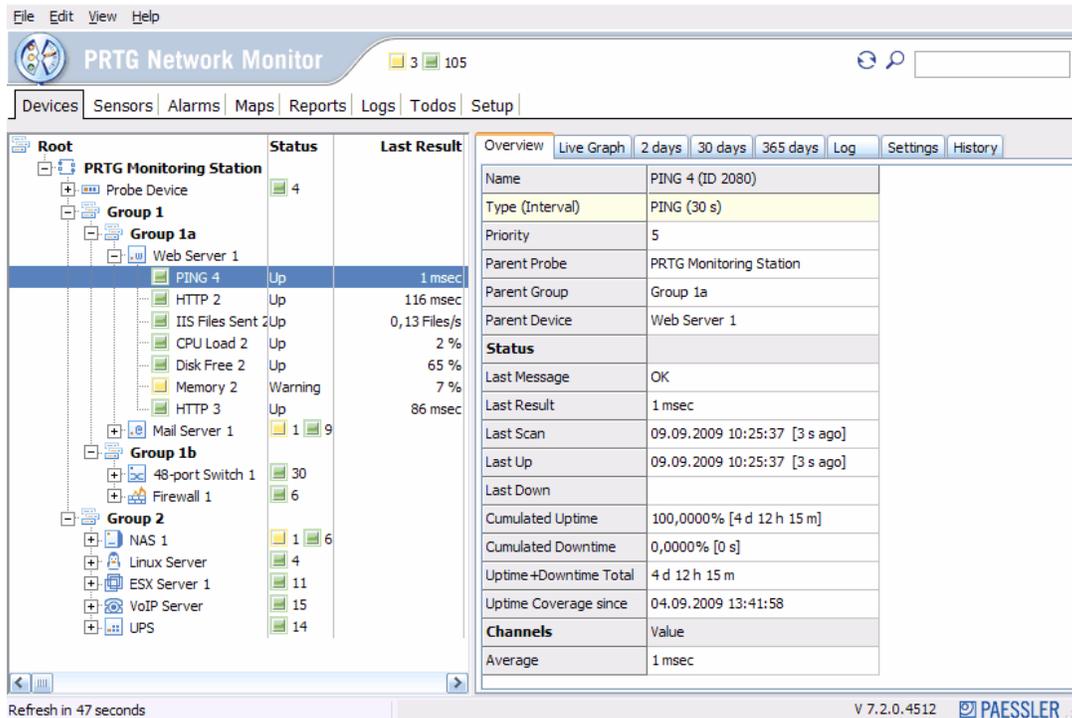
The screenshot shows a dialog box titled "PRTG Network Monitor". The text inside reads: "Please enter the DNS name (or IP address) of your PRTG Core Server along with the web server port and your account credentials:". Below this text are four input fields: "Server IP/DNS name:" (a text box), "Port:" (a spinner box with "80" and a "Use SSL" checkbox), "Login Name:" (a text box), and "Password:" (a text box). At the bottom right are two buttons: "Start" and "Cancel".

As soon as you click on "Start" it will contact the PRTG Core Server and the main window will show up.

Note: If you change one of these settings in [PRTG Server Administrator](#) later on, you will see an error message when starting the Windows GUI. In this case you have to enter the new settings for the Core Server: In the Windows GUI, click on "File | Options & Server Settings...", entry "PRTG Server Connection" and change the server settings to the new values.

Working with the Windows User Interface

Start the Windows GUI by clicking on the according entry in the Windows Start Menu.



At the top of the window you can find the summarized status for all sensors, a button to manually refresh the monitoring data and a search box:

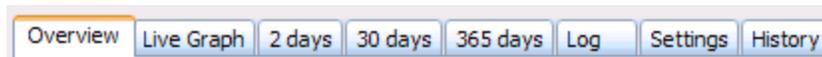


Using tabs the Windows GUI offers the same main module selection as the web interface:

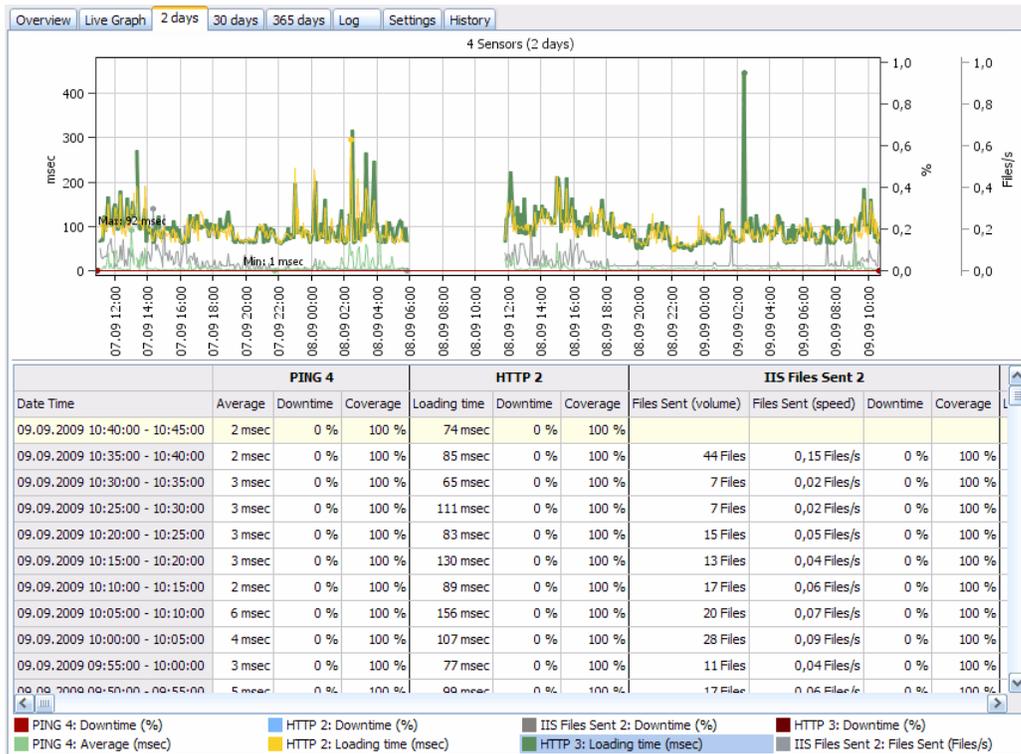


Module "Devices"

In the "Devices" module you will find a tree-like view of the groups, devices and sensors on the left side. You can select one or more items from the list (using CTRL and SHIFT while clicking with your mouse) and you will see detailed information about the selected items on the right side. Using a second row of tabs you can select what information you want to display:



The following screenshot shows the graph and data table for 3 sensors. In this sample the green line in the graph is shown thicker by hovering the mouse cursor over the respective entry in the legend at the bottom.



If you select the "Settings" tab you will see edit fields only for those object settings that are shared by all selected objects (e.g. the interval is shared by all sensors, tags are shared by all objects). Select the leftmost checkbox for the settings you want to edit for all objects (they will be shown with a green background), enter the desired value (s) and click "Save".

You are editing 3 objects

Basic Sensor Settings

Sensor Name: [] The sensor's name.

Tags: here_is_a_new_tag_for_all_objects Enter a list of tags (not case sensitive) for filtering purposes (e.g. the top 10 lists use these tags). Use space or comma as separators.

Priority: [***] Use this value in order to sort this object within lists.

Inherit Scanning Interval

Scanning Interval: 50 seconds Time between two scans

Inherit Schedules and Dependencies

Schedule: [None] Use schedules to pause monitoring for a specified time span (days, hours) throughout the week. You can edit schedule definitions under the system settings.

Inherit Access rights

User Group Access: User Group: PRTG Users Group, Rights: Inherited (None) Set user group access rights for this object. You cannot remove rights defined for a parent node. All rights are inherited to child nodes.

Save

Other Modules

The usage of other modules is straight forward. Lists show the sensors, alarms, maps, reports, logs and Todos.

You can navigate these lists as usual for a Windows application:

- Review the information by scrolling the content
- Resort the lists by clicking a column header
- Resize the columns by dragging column separators
- Edit the list items using their context menus (shown upon right click)

The Sensors and Alarms module also offer controls to filter the lists.

Working With the Tray Tool Functionality

When you close the Windows GUI main window you will still see a PRTG icon in the Windows System Tray in the lower right corner of your screen. The Tray Tool will now contact your Core server every 60 seconds and it will alert you in various ways when new events occur, sensors go down etc. (depending on your settings). For example, a popup showing the latest events looks like this:



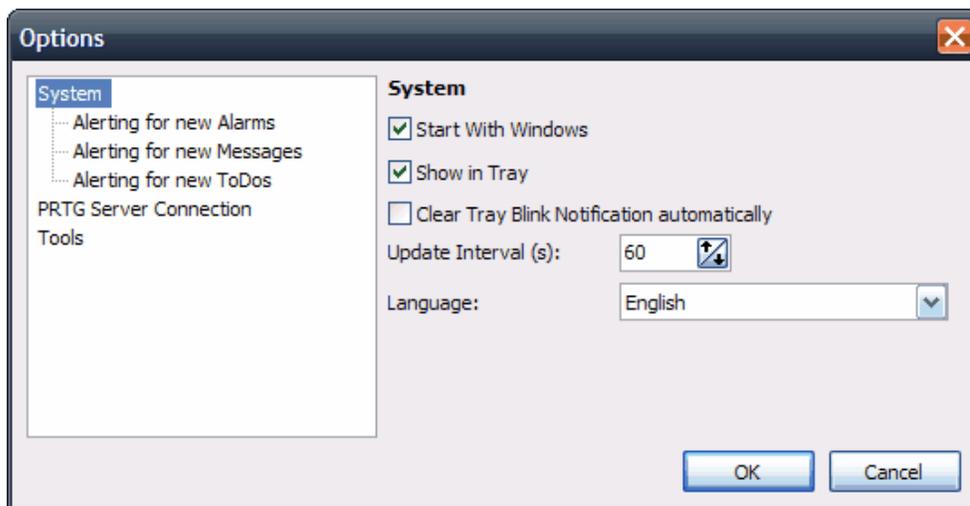
Date Time	Parent	Object	Status	Message
9/9/2009 10:07:54 AM	SNMP-1000 (sg.prtgtestserver.net)	PING 24	Up	283 msec
9/9/2009 10:07:54 AM	SNMP-1000 (sg.prtgtestserver.net)	HTTP 24	Resuming	Resumed by Dependency
9/9/2009 10:06:29 AM	prtgtestserver.net	SNMP-1000 (sg.prtgtestserver.net)	Paused	Paused by Dependency
9/9/2009 10:06:29 AM	SNMP-1000 (sg.prtgtestserver.net)	PING 24	Down	Request timed out (ICMP error # 11010)
9/9/2009 10:06:29 AM	SNMP-1000 (sg.prtgtestserver.net)	HTTP 24	Paused	Paused by Dependency
9/9/2009 10:06:26 AM	SNMP-1000 (sg.prtgtestserver.net)	PING 24	Warning	Request timed out (ICMP error # 11010)
9/9/2009 10:05:54 AM	prtgtestserver.net	SNMP-1000 (sg.prtgtestserver.net)	Resuming	Resumed by Dependency
9/9/2009 10:05:54 AM	prtgtestserver.net	SNMP-1000 (sg.prtgtestserver.net)	Active	
9/9/2009 10:05:54 AM	SNMP-1000 (sg.prtgtestserver.net)	PING 24	Up	286 msec
9/9/2009 10:05:54 AM	SNMP-1000 (sg.prtgtestserver.net)	HTTP 24	Resuming	Resumed by Dependency
9/9/2009 10:01:28 AM	prtgtestserver.net	SNMP-1000 (sg.prtgtestserver.net)	Paused	Paused by Dependency
9/9/2009 10:01:28 AM	SNMP-1000 (sg.prtgtestserver.net)	PING 24	Down	Request timed out (ICMP error # 11010)
9/9/2009 10:01:28 AM	SNMP-1000 (sg.prtgtestserver.net)	HTTP 24	Paused	Paused by Dependency
9/9/2009 10:01:26 AM	SNMP-1000 (sg.prtgtestserver.net)	PING 24	Warning	Request timed out (ICMP error # 11010)
9/9/2009 10:00:24 AM	prtgtestserver.net	SNMP-1000 (sg.prtgtestserver.net)	Resuming	Resumed by Dependency
9/9/2009 10:00:24 AM	prtgtestserver.net	SNMP-1000 (sg.prtgtestserver.net)	Active	

Alarms: 41 new
New Messages: 8
New Todos: 0

OK Open GUI

Configuring the Windows GUI

Select "File | Options & Server Settings..." to edit the settings for the Windows GUI:



Here you can set various alerting options, enter one or more PRTG server connections and you can configure command line tools.

The following settings are available for alerting (you can test the current settings by clicking "Test"):

- Blink the icon in the Windows system tray
- Show a balloon popup near the system tray
- Show a popup window
- Play a soundfile
- Open the main GUI window



5.3 iPhone Interfaces

If you have an Apple iPhone or iPod Touch you have the choice between two user interfaces optimized for your mobile device:

iPRTG: The iPhone App for PRTG Network Monitor

Don't let monitoring your network tie you to your desk! With iPRTG your network monitor is where your iPhone is. iPRTG is the iPhone App for network administrators using the PRTG Network Monitor software to monitor

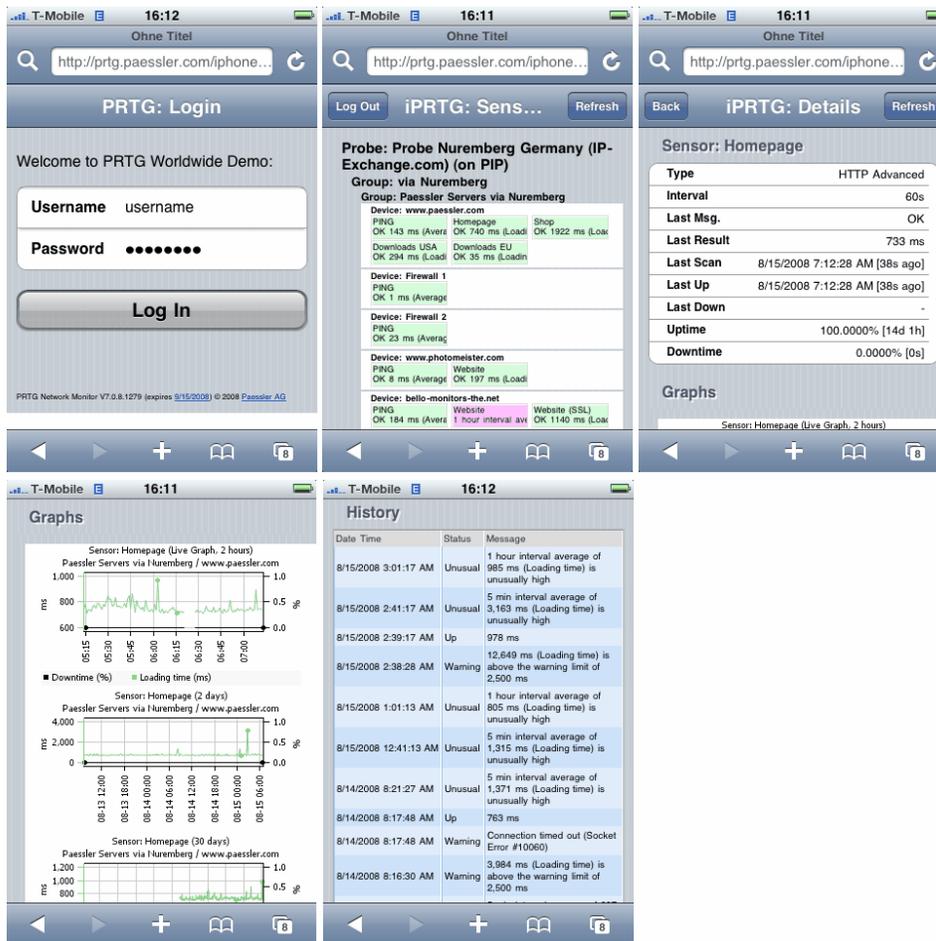
and administrate their network. iPRTG is the one and only clear and simple viewer for the entire network monitoring environment. Your iPhone requests the monitoring data directly from your PRTG server and displays it in an 'iPhonic' way. It looks like this:



iPRTG must be purchased separately, please see: <http://www.beyond-content.com/products/iphone-apps/>

Web-based iPhone Interface

PRTG offers also a read-only web browser based user interface that is optimized for the Apple iPhone. This feature enables the user to quickly check the status of the servers and sensors remotely. It looks like this:

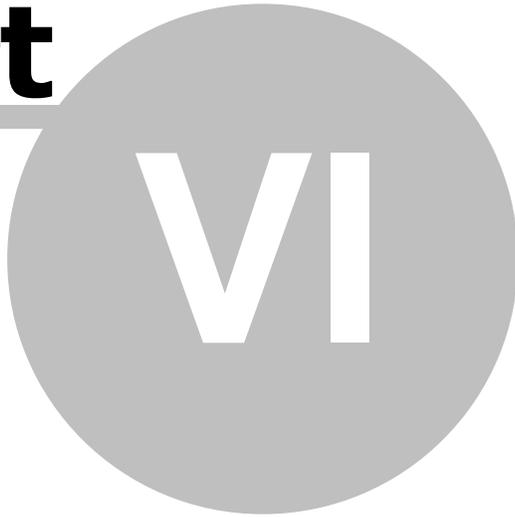


Simply point the Safari browser of your iPhone to the URL [https://\(your_prtg_server\)/iphone](https://(your_prtg_server)/iphone) and you will see the login dialog. Enter your credentials and a few seconds later you will see the sensor tree with groups, devices and sensors on the iPhone display. Tap on a sensor and you will receive a display with detailed information about the sensor, recent graphs logfile entries.

Please keep the following security aspects in mind:

- You could also use HTTP to connect to your server, but encrypted access with SSL/HTTPS is recommended in order to keep your password secure.
- As an added level of security you could create a user just for your iPhone logins that only has read access for the "Root Group" or for selected groups that you want to monitor remotely (in case you have more than a few sensors).

Part



Device and Sensor Setup

6 Device and Sensor Setup

Before starting to create sensors, review the "Root" group's settings that will be inherited by all other objects (see [Reviewing Settings of the Root Group](#)).

As soon as this step is completed you can start to create groups, devices and sensors to monitor your network. This can be done either manually or automatically. The following sections [Creating Groups, Devices and Sensors Manually](#) and [Creating Devices and Sensors Using the Auto Discovery](#) explain these steps.

Note: If you want to create a multi-probe setup, you need to add and configure the necessary probes first (see [Multiple Probes and Remote Probes](#)).

6.1 Reviewing Settings of the Root Group

Objects in the sensor tree inherit many settings from their parent objects as explained in the [Inheritance of Settings](#) section. Obviously, the "Root" group, which is the parent object to all other objects, is especially important in this regard.

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. Choose the "Devices" item from the main menu and click the "Settings" tab. There are several relevant settings:

Group Root
Edit | Pause | Refresh | Menu

Home > Devices

Overview | 2 days | 30 days | 365 days | Alarms | Log | Settings | Notifications

Basic Group Settings

Group Name: The group's name.

Status: started paused

Location: Use this field to enter the physical location of the object.

Schedules and Dependencies

Schedule: Use schedules to pause monitoring for a specified time span (days, hours) throughout the week. You can edit schedule definitions under the system settings.

Dependency Type: Use parent Select object Select the dependency behavior for this object. 'Use parent' will pause the object if the parent object is not 'UP'. 'Select object' allows to select an object from a drop-down list on which the current object will depend on.

Credentials for Windows Systems

Domain or Computer Name: Enter an authority for Windows access (domain or computer name for the user account)

Username: Enter a login name for the Windows access

Password: Enter a password for Windows access

WMI Compatibility Options

WMI Timeout (sec): Specify how long this sensor will wait for the return of its WMI query until it quits with a timeout error. Leave empty if you want to use the default mechanism (1.5 x scanning interval) or set to a specific value.

RPC server port: WMI uses DCOM for communication between computers. Therefore the RPC Server on the monitored machine has to be accessible, by default on Port 135. This port number, however, can be altered - if the hosts RPC server port has been changed, enter the new number here.

Credentials for VMware Servers

User: Enter a user name and password for authentication on VMware ESX and Virtual Center servers

Password:

Protocol: HTTPS (recommended) HTTP Please choose a protocol for access to the VMware server

Credentials for SNMP Devices

SNMP Version: v1 v2c v3 Depending on the target device you can use advanced features if you select SNMP v2c or SNMP v3. Standard is SNMP v1. Use SNMP v2c for 64bit counters and SNMP v3 if you want secure authentication and SNMP data encryption

Community String:

SNMP Port: The device's SNMP port. Standard is '161'.

SNMP Timeout (sec): If the reply takes longer than this value the request is aborted and you get an error message. If two consecutive requests fail (for whatever reason) the sensor enters a 'Down' state. This has consequences, e.g. on visual feedback or notifications.

SNMP Compatibility Options

SNMP Delay: Specifies the time between two SNMP requests. Some devices have problems with a fast sequence of SNMP requests. This option increases the delay time between SNMP requests to the selected value in ms.

SNMP Requests: Retry If a SNMP request fails, PRTG tries again. This helps with devices that fail to answer at times.

Overflow Values: Ignore Some devices handle overflows incorrectly. This behavior can cause false peaks in regular intervals.

Zero values: Ignore in delta sensors Some devices sometimes send incorrect 0 values, causing peaks.

32bit counters: Force The interface scan will search for 32bit traffic counters only, even if the device reports 64bit counters.

Request mode: Use multi get (recommended) Use single get Usually multiple SNMP requests such as traffic channels are bundled into one request. Check the 'single' option if you want a single request for each SNMP value (might be useful for older SNMP devices).

Port name template: Enter a single OID which is extended by the port number or a custom string with placeholders in brackets {port} for the port number, {alias} for the interface alias (oid 1.3.6.1.2.1.11.1.1.1), {descr} for the interface description (oid 1.3.6.1.2.1.1.2.1), {custom oid} for any custom oid extended by the port number

Scanning Interval

Scanning Interval: Time between two scans

Unusual Detection

Unusual Detection: Enabled Disabled Activate the detection and display of unusual sensor values (sensors turn orange), as specified in the system settings.

Access Rights

User Group Access:

User Group	Rights
PRTG Users Group	<input type="text" value="None"/>
User Group	<input type="text" value="None"/>

Revert children's access rights to inherited Set user group access rights for this object. You cannot remove rights defined for a parent node. All rights are inherited to child nodes.

Channel Unit Configuration

Channel Unit Types:

Channel Type	Unit
Bytes (Bandwidth)	<input type="text" value="KByte"/> / <input type="text" value="second"/>
Bytes (Memory)	<input type="text" value="kbit"/>
Bytes (Disk)	<input type="text" value="MByte"/>
Bytes (File)	<input type="text" value="Byte"/>

Configure the unit settings for each channel type.

Please review the settings and refer to the help texts on the right for detailed explanations for each of them. Remember that you can override these settings for all child objects later.

There are the following sections:

- **Credentials for Windows Systems:** The Active Directory user account provided here will be used to access different systems in your network, especially during the Auto-Discovery process. This includes WMI-based monitoring and Server Message Block (SMB, SAMBA) based monitoring (files, folders, disk shares), Remote Desktop Protocol (RDP) and Microsoft SQL (when Windows Authentication is activated in this sensor's settings). It is recommended to enter a user account with administrator privileges.
- **WMI Compatibility Options:** Here you can specify a WMI timeout and the RPC server port for WMI communication.
- **Credentials for VMware Servers:** If you want to work with VMware ESX/ESXi servers or VMware Virtual Centers please provide the necessary user account which will be used for auto discovery and for monitoring.
- **Credentials for SNMP Devices and SNMP Compatibility Options:** Please select the SNMP version and enter the necessary authentication strings used in your network. The defaults are "SNMP V1", community string "public" and port 161.
- **Scanning Interval:** Please select the default interval that shall be used for monitoring by all sensors.
- **Unusual Detection:** You can enable/disable the detection of unusual sensor activity.
- **Access Rights:** Use these settings to define which user group may view or edit objects.
- **Channel Unit Configuration:** Configure the unit settings for each channel type.

All of these predefinitions can later be overridden by disabling the "Inherit ..." setting in an object's settings further down in the device/sensor tree.

6.2 Creating Groups, Devices and Sensors Manually

Creating Groups Manually

To create a new group, go to the devices list ("Devices" in the main menu) and locate either a probe or group that shall contain the new group. Right click the object and then choose "Add Group..." from the context menu. As an alternative you can choose "Add Group" from the "Devices" menu - in the latter case you must then choose a parent group. The "Add Group" dialog appears.

Add Group to Group "Group 1"

Group Name and Tags

Group Name: ! The name of the Group.

Tags: Enter a list of comma separated tags (case insensitive) for filtering purposes

Inherit Credentials for Windows Systems from parent object (Group) (Domain or Computer Name: <empty>, Username: <empty>)

Inherit Credentials for SNMP Devices from parent object (Group) (SNMP Version: V1, SNMP Port: 161, SNMP Timeout (s): 5s)

Enter a name for the new group, optionally enter "Tags" or review the inherited credential settings and then click "Continue".

Creating Devices Manually

To create a new device, go to the devices list ("Devices" in the main menu) and locate either a probe or group

that is intended to contain the new device. Right click the object and then choose "Add Device..." from the context menu. As an alternative you can choose "Add Device" from the "Devices" menu - in the latter case you will be asked to either create a new parent group for the device or to choose an existing group as parent. The "Add Device" dialog appears.

Device Name and Address

Device Name: Device 1 ! Choose a new name to describe the device

Ip-Address/DNS Name: ! Enter a DNS name (e.g. "server.mycompany.com") or the IP address (e.g. "10.0.0.15")

Tags: Tags are keywords or descriptive terms associated with an object as means of classification.

Device Icon: Select an icon for the device.

Device Type

Sensor Management

- Manual (no auto-discovery) Choose "manual" if you want to create and manage sensors manually. All other settings will scan your network for available counters and create the corresponding sensors. "Automatic device identification" is mainly based on PING, SNMP and WMI counters. This option is intended for LANs only and is not suitable for WAN connections.
- Automatic device identification (standard, recommended)
- Automatic device identification (detailed, may create many sensors)
- Automatic sensor creation using specific device template(s)

Inherit Credentials for Windows Systems from 1st group (visible to all user accounts) (Domain or Computer Name: paesslergmbh, Username: admin)

Inherit Credentials for VMware Servers from 1st group (visible to all user accounts) (User: <empty>)

Inherit Credentials for SNMP Devices from 1st group (visible to all user accounts) (SNMP Version: V1, SNMP Port: 161, SNMP Timeout (sec): 5sec)

Continue > Cancel

There are two settings that you must enter for a device: The name and the IP address (or DNS name). Optionally, enter "Tags", choose a device icon or review the inherited credentials and then click "Continue". If you want to use one of the automatic options in the "Device Type" settings, please see section [Creating Devices and Sensors Using the Auto-Discovery](#) for more details.

Creating Sensors Manually

To create a new sensor, go to the devices list ("Devices" in the main menu) and locate a device where the new sensor is to be added. Right click the device and then choose "Add Sensor..." from the context menu. As an alternative you can choose "Add Sensor" from the "Sensors" menu - in the latter case you can choose if you want to add the sensor to a will be either asked to create a new parent device or to choose an existing device as parent.

The "Add Sensor" dialog appears. Creating new sensors involves two steps: First, you must select a sensor type, then - after some preparations by PRTG - you need to specify the sensor settings.

Sensor Type

- ▶ **Your Top 10 Sensors** The sensor types you are using the most
- ▼ **Common Sensors** The most common sensor types for network monitoring
 - PING** Performs PINGs to monitor the availability of a device. PINGs are used to check whether a device is reachable via the network at all. Optionally you can use this sensor to measure packet loss.
 - PORT** Checks the availability of TCP-based network services. Tries to connect to the specified TCP/IP port number of a device and waits for the request to be accepted.
 - HTTP** Monitors a web server via the HTTP protocol. You only need to supply an URL for this sensor.
 - SNMP Traffic** Monitors bandwidth and traffic via SNMP. Supports monitoring of bandwidth (bits/s) and volume (bytes), as well as number of packets and errors.
 - WMI Network Card** Monitors bandwidth usage and traffic through a network card via WMI.
- ▶ **Bandwidth Monitoring** Bandwidth usage monitoring (SNMP, Packet Sniffing, NetFlow, sFlow)
- ▶ **Web Servers (HTTP, HTTPS)** Sensors based on the HTTP protocol
- ▶ **SNMP** Sensors based on the Simple Network Management Protocol (SNMP)
- ▶ **Windows Systems (WMI)** Monitoring for computers running Windows using Windows Management Instrumentation (WMI)
- ▶ **Internet Protocols** Various sensor types for services used on the Internet (PING, PORT, FTP, DNS, RDP)
- ▶ **Mail Servers** Mail server sensors (SMTP, POP3, IMAP)
- ▶ **SQL Servers** SQL server monitoring (MySQL, MS-SQL and Oracle)
- ▶ **File Servers** Monitoring of file servers, NASs, etc.
- ▶ **Virtual Servers** Sensors for virtualized environments (VMWare, HyperV, and Amazon EC2)
- ▶ **VoIP and Infrastructure** Various sensor types used to monitor VoIP, QoS and network infrastructure
- ▶ **Custom Sensors** Various sensor types that enable you to define your own sensor scripts
- ▶ **All Sensors** A complete list of all sensors

Continue to step 2 > Cancel Haven't found what you need? Find more custom sensors online!

In step one you must select a sensor type from the available types list. There are more than 40 different types (see [Sensor Types](#) for detailed descriptions), so PRTG offers various groupings. Simply click one of the group headings and then select a sensor. Then click "Continue to Step 2".

Basic Sensor Settings

Sensor Name: HTTP 22 ! The sensor's name.

Tags: httpsensor Enter a list of tags (not case sensitive) for filtering purposes (e.g. the top 10 lists use these tags). Use space or comma as separators.

Priority: *** Use this value in order to sort this object within lists.

HTTP Specific

Timeout (sec): 60 ! If the reply takes longer than this value the request is aborted and an error message is triggered.

URL: http:// ! Enter a valid URL to monitor. The server part (e.g. www.paessler.com) may be different from the 'DNS Name' property in the settings of the associated server. If the protocol part (e.g. 'HTTP://') is omitted, 'HTTP' is used.

Request Method: GET, POST, HEAD HTTP request method

SSL Method: sslvSSLv23 Change this if you don't get a SSL connection.

Inherit Scanning Interval from Probe Device (Scanning Interval: 60sec)

Continue > Cancel

In step two, the settings available depend on the sensor type. Please review the settings and make any necessary changes, then click "Continue". The new sensor will start monitoring right away.

6.3 Creating Devices and Sensors Using the Auto-Discovery

PRTG's Auto-Discovery 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.

To see a video of this, please go to http://www.paessler.com/support/video_tutorials

How Auto-Discovery Works

PRTG's Auto-Discovery process has three stages:

- Step 1: Scanning a network segment for devices using PINGs (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 (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 [Copying Devices by Cloning or Using Device Templates](#))

The Auto Discovery can be used on a group level for a range of IP addresses, or for individual devices 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 "Todos" are created and mailed to the system admin.

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 (e.g. if a firewall blocks echo requests, a device behind it cannot be discovered).
- You must supply authentication settings for SNMP, Windows/WMI and VMware servers in order to fully exploit the power of this feature.
- 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.

Creating an Auto-Discovery Group

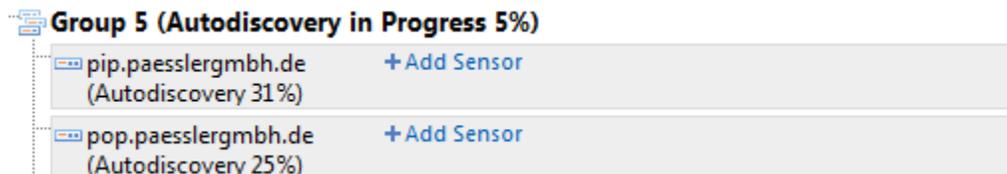
To create a new auto discovery group, go to the devices list ("Devices" in the main menu) and locate either a probe or group that is intended to contain the new group. Right click on the object and select "Add Auto-Discovery Group..." from the context menu.

Enter a name for the group (and optionally Tags) and choose the desired option for the "Sensor Management" setting:

You have three options:

- **Automatic Device Identification (Standard, recommended):** This recommended option should work fine for most installations.
- **Automatic Device Identification (Detailed, may create many sensors):** This option is only 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):** Choose this option if you do not want automatic device identification and would rather select the device templates manually, e.g. if you want to use a device template that you have created yourself. You will see a list of device templates from which you can select one or more templates.

Afterwards, enter the IP Base (the first 3 bytes of the IP Range) and the first and last 4th byte of the IP address range. As soon as you click on "continue", PRTG will start the discovery process, visible in the sensor tree ("Devices" menu item of the main menu):



If you keep looking at this page, you will see more and more devices and sensors showing up in the list. The Auto-Discovery process takes between 10 and 50 seconds per IP address, depending on configuration and network.

All sensors created by this process will start monitoring immediately and will notify failures as soon as they happen.

Creating an Auto-Discovery Device

Creating sensors for just one device using the Auto-Discovery function is quite similar to creating an Auto-Discovery Group. Go to the devices list ("Devices" in the main menu) and locate either a probe or group that is intended to contain the new device. Right click on the object and select "Add Device..." from the context menu.

Device Type	
Sensor Management	<input type="radio"/> Manual (No Autodiscovery) <input checked="" type="radio"/> Automatic Device Identification (Standard, recommended) <input type="radio"/> Automatic Device Identification (Detailed, may create many sensors) <input type="radio"/> Automatic Sensor Creation with specific Device Template(s)
Discovery Schedule	Once <input type="button" value="v"/>

Choose the "Manual" option if you want to create and manage sensors manually. The other settings will scan your network for available sensors and create the appropriate sensors. "Automatic Device Identification" is mainly based on PING, SNMP and WMI. It should only be used in LANs and is not suitable for WAN connections.

Enter a name and IP address (or DNS name) for the device and choose one of the options for "Sensor Management" (described above).

As soon as you click "Continue" the device assessment will begin and create the sensors that suit the device.

6.4 Edit Sensor and Channel Settings

In PRTG, it's the sensors which perform the monitoring. Each sensor has one or more channels through which it gets the actual data. For each sensor, you can configure general settings, notifications and the different channels. All of these settings are available in the tabs of a sensor's detail view.

To enter the sensor detail view, first click on "Sensors" in the main menu to view the sensor list and then click a sensor (or right-click a sensor and select "Details..." from its context menu) or select a sensor from the tree.

"Settings" Tab

In the "Settings" tab, you can enter/edit the following information:

- Basic settings, such as Name, Tags, Priority.
- Settings that configure the behavior of the sensor and that depend on the sensor type (e.g. the URL for an HTTP sensor).
- Various settings that can optionally be inherited from the parent object (e.g. SNMP settings, interval, authentication settings). See [Inheritance of Settings](#) for more details.
- Here you can also select the "Primary Channel" from the channels available to this sensor. The primary channel for this sensor will always be displayed in graphs and overviews. It can also be used to trigger notifications.
- Please note: Warning and Error Limits are based on the sensor's channels and can be changed in the "Channels" tab.

"Notifications" Tab

You can use a sensor to trigger many different notifications. Please see section [Notifications](#) for more details on creating notification triggers.

"Channels" Tab

In the "Channels" tab, you can specify the settings for every single channel of a sensor. First, choose the desired channel in the "Select Channel" area. The channels available in this selection box depend on the sensor you are editing. You can only choose one channel at a time.

The settings below the "Edit Channel" header are channel specific and vary slightly, depending on the selected channel. You can change the channel's name in the "Name" field. The "ID" is used as an internal channel identifier and cannot be changed.

With the check boxes available at "Display", you can select whether this channel should be displayed in charts, in tables, or both. This way, you can make your charts and tables clearer, by hiding the data of channels that do not interest you.

With the settings "Line Color", "Line Width", "Decimal Places", and "Vertical Axis Scaling", you can specify how the graphs for this channel are to be displayed. If you don't like the automatic settings, please change colors, line width, scaling, etc. to suit your needs.

The field "Spike Filter" is only available if applicable for the channel. If enabled, you can enter an upper and/or a lower limit. With the existing data, all values above the upper limit and below the lower limit will be ignored. This option is recommended only if you repeatedly receive obviously wrong data (e.g. enormously high or far too low values) due to an error in data transmission or due to incompatibilities with the device you are monitoring.

The field "Limits" is only available if applicable for the channel. If enabled, you can enter Upper and Lower values for both an Error and a Warning Limit. If one of these limits is reached for this channel, the whole sensor is then set to Error or Warning status (as specified). Additionally, you can also enter an Error Limit Message and a Warning Limit Message which will be added to the respective status. In combination with the settings in the "Notifications" tab you can setup PRTG to notify you when a sensor reaches a limit.

Remarks

For all other tabs in a sensor's details view, see table overview "Page Header and Tabs" in section [Web Interface](#).

Part



Sensor Types

7 Sensor Types

PRTG offers more than 40 different sensor types for various network services. All sensor types have a number of type-specific settings plus there are a number of common settings for all sensors. Please refer to the help text in the web interface for a detailed description of all settings.

Overview of Sensors

When creating new sensors you will see the following groups of sensor types. Note that some sensor types will show up several times in this list because they fit into more than one category:

- [Common Sensors](#): The most common sensor types for network monitoring.
- [Bandwidth Monitoring](#): Monitoring of bandwidth usage using [WMI](#), [SNMP](#), [Packet Sniffer](#) or [xFlow \(NetFlow/sFlow\)](#).
- [Web Server \(HTTP, HTTPS\)](#): Sensors based on the HTTP protocol.
- [SNMP](#): Sensors based on the Simple Network Management Protocol (SNMP).
- [Windows Systems \(WMI\)](#): Monitoring of Windows systems through Windows Management Instrumentation (WMI).
- [Various Protocols](#): Various sensor types for services used on the Internet and others (PING, PORT, FTP, DNS, RDP, HDD Health etc.).
- [Mail Servers](#): Sensors for mail servers (SMTP, POP3, IMAP, SMTP&IMAP Round Trip, SMTP&POP3 Round Trip etc.).
- [SQL Servers](#): Monitoring of SQL Servers (MySQL, MS-SQL and Oracle).
- [File Servers](#): Monitoring of File Servers, NASs, etc.
- [Virtual Servers](#): Sensors for VMware Servers, Hyper-V and Amazon CloudWatch.
- [VoIP and QoS](#): Quality-of-service monitoring and Cisco IP SLA monitoring via SNMP.
- [Custom Sensors](#): Various sensor types that enable you to define your own sensor scripts, including [Sensor Factory Sensors](#) for combination of measurement results. In this group, you'll find a user definable version of some sensors from other groups.

In the following sections, the most important sensors will be described.

7.1 Common Sensors

The most common sensors for network monitoring are shown in this section:

- PING: Performs one or more PINGs to monitor the availability of a device and optionally measure packet loss in percent.
- PORT: Checks the availability of TCP based network services.
- HTTP: Monitors a web server via the HTTP protocol (see [Web Servers \(HTTP, HTTPS\) Sensors](#)).
- SNMP Traffic: Supports monitoring bandwidth (bits/s) and volume (bytes), as well as the number of packets and errors via SNMP for a port of a network card on a PC, server, switch, firewall, printer etc. (see [SNMP Sensors](#)).
- WMI Network Card: Measures traffic going through network cards (see [WMI Sensors](#)).

7.2 Bandwidth Monitoring Sensors

The following sensors can be used for bandwidth monitoring:

- WMI Network Card: Measures traffic going through network cards (see [WMI Sensors](#)).
- SNMP Traffic: Supports monitoring bandwidth (bits/s) and volume (bytes), as well as the number of packets

and errors via SNMP for a port or a network card on PCs, servers, switches, firewalls, printers (see [SNMP Sensors](#)).

- Packet Sniffer (Header): PRTG looks at the IPs and ports of source and destination to assess the protocol (see [Packet Sniffer Sensors](#)).
- Packet Sniffer (Content): PRTG captures the TCP packets, reassembles the data streams and then analyzes the content of the data using an internal set of rules to identify the type of traffic (see [Packet Sniffer Sensors](#)).
- NetFlow V5: Monitors Cisco switches using NetFlow V5 (see [xFlow \(NetFlow and sFlow\) Sensors](#)).
- NetFlow V9: Monitors Cisco switches using NetFlow V9 (see [xFlow Sensors \(NetFlow and sFlow\)](#)).
- sFlow: Monitors switches using sFlow (see [xFlow Sensors \(NetFlow and sFlow\)](#)).

To learn more about the four methods of bandwidth monitoring in PRTG, see section [Comparison of Bandwidth Monitoring Sensors](#).

7.3 Web Server (HTTP, HTTPS) Sensors

The HTTP protocol (Hypertext Transfer Protocol) is most commonly used for the World Wide Web. Web browsers request web pages, graphics etc. from web servers using this protocol. With PRTG, you can monitor your web server's performance and availability.

Overview: Different HTTP Sensors

PRTG offers the following HTTP-based sensors to monitor web servers:

- HTTP: Monitors a web server via the HTTP protocol. This is the easiest way to monitor if a website (or a specific website element) is reachable.
- HTTP Advanced: Monitors a web server via the HTTP protocol with various advanced settings (e.g. to check the content of a web page or to use authentication or a proxy server).
- HTTP Transaction: Monitors a web server using a set of URLs to monitor whether logins or shopping carts are working fine. You must supply a series of URLs (GET and/or POST requests) including the parameters to monitor a transaction.
- HTTP Content: Monitors a return value provided by a HTTP request. This sensor requests a HTTP URL and then parses the returned result for one or more values in square brackets. This is mainly used in combination with scripts running on a server.
- HTTP Full Web Page: Monitors the full download time of a webpage including images etc. (uses Internet Explorer to perform a full page download).

All sensors support HTTP and HTTPS.

Common Settings - HTTP Sensors

All HTTP sensors include basic sensor settings and these HTTP specific parameters:

- Timeout: Time in seconds after which the request is aborted.
- URL: The URL address of the web page to monitor (including the leading http://). Please see section "Smart URL replacement" below for other options. You can also enter the address of a specific web page element here, for example the URL to a JPG file.
- Request Method: The HTTP request mode to use (GET, POST, HEAD). GET requests the website directly, like browsing the web. If you want to monitor a URL for a POST form, you must select the POST method and enter the "Postdata". The HEAD method only requests 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: When using the POST request method, you can enter the data part here (no XML allowed).

- **SSL Method:** Relevant only when you're using HTTPS. If you are using a HTTPS URL and do not get a connection, please try with another SSL method.

For monitoring a simple web page, choose a simple "HTTP" sensor (for more advanced HTTP sensors see below). Enter the URL (with http:// at the beginning) and keep the default request method selection GET.

Smart URL Replacement

Instead of entering a complete address in the URL field, 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 device's IP address/DNS name in front of the third slash automatically. Whether this results in a valid URL or not, depends on the IP address/DNS name of the device where this HTTP sensor is running on.

For example, if you have a device with DNS name "paessler.com" and you put a HTTP sensor on it with the value "https:///" in the URL field, PRTG will automatically create the URL "https://paessler.com/" from that. Similarly, if you create a HTTP sensor on the same device using the value "/support" in the URL field, PRTG will automatically create and monitor the URL "http://paessler.com/support".

In combination with [cloning devices](#), the smart URL replacement makes it easy to create many like devices. (Please note that smart URL replacement does not work for sensors running on the "Probe Device".)

Notes For HTTP Advanced Sensors

For general settings, please refer to "Common Settings - HTTP Sensors" (above). Using the HTTP Advanced sensor, you can optionally enter the following advanced settings (you can also leave any of them blank):

- **Content:** Check "Monitor Changes" if you want to monitor any changes on the file at the given URL. You can combine this setting with a "On Change" notification trigger later (tab "Notifications" in sensor's settings).
- **Response must include:** If you enter a string here, the sensor will check if this string is part of the HTML page at the given URL. If so, the sensor status will be "OK". **Note:** 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). Therefore, a literal search for the characters * and ? is not possible.
- **Response must not include:** If you enter a string here, the sensor will check if this string is **not** part of the HTML page at the given URL. If so, the sensor status will be "OK". **Note:** 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). Therefore, a literal search for the characters * and ? is not possible.
- **Limit download:** To avoid exhaustive bandwidth usage, you can enter a kB limit for the data transferred per request. If you're using "Response must (not) include" options, only the part of the HTML page that is retrieved before reaching this download limit can be compared to your strings.
- **Authentication User/Password:** If the website at the given URL needs authentication, you can enter the credentials here. Please also choose if the website uses a HTTP-Basic or a Windows Integrated (NTLM) authentication.
- **Proxy:** If you want or need to access the given URL via a certain proxy, please enter the according information in these fields. We do not recommend using a proxy, because in case of a connection failure, you will not be able to determine if it's the web server or the proxy server causing it.

Notes For HTTP Transaction Sensors

This sensor is a special kind of HTTP Advanced Sensor. Instead of one single URL, it will check a series of URLs. For your HTTP Transaction Sensor, you can additionally configure the following settings:

- **Timeout:** This HTTP specific setting defines the time in seconds after which the complete series of transactions is aborted. If this happens, the sensor for the complete transaction series is set to "Failure".

- **Single URL Timeout:** With this HTTP specific setting you can define a timeout in seconds after which a single transaction step is aborted. If this happens, the sensor for the complete transaction series is set to "Failure".
- **Use cookies:** If cookies are needed for one of the transactions, check this option. If you are unsure, keep it checked.
- **Authentication User/Password:** If the websites at the given URLs (below) need authentication, you can enter the credentials here. Please also choose if the websites use a HTTP-Basic or a Windows Integrated (NTLM) authentication.
- **Proxy:** If you want or need to access the given URL via a certain proxy, please enter the according information in these fields. We do not recommend using a proxy, because in case of a connection failure, you will not be able to determine if it's the web server or the proxy server causing it.
- **Transaction URL #1 to #10:** In these fields, you can enter up to 10 different URLs that will be requested in a series. If all of them succeed, the sensor will be in "UP" status. To help you find the right transaction URLs, you can use the Paessler URL Recorder to build a suitable URL list (see "Tools" at the end of this section).
- Please see "Common Settings - HTTP Sensors" and "Notes For HTTP Advanced Sensors" (above) for information about the other fields.

For tips configuring Transaction Sensors, see Knowledge Base article:

<http://www.paessler.com/knowledgebase/en/topic/443>

Notes for HTTP Content Sensors

This sensor requests a URL with a script and in the result received, it searches for a certain values. In the script's results which are sent back, each value must be enclosed in square brackets ("["]"). The sensor then handles each value in a separate channel (this can be one or more). You can use this with a script running on a web server. Usually, your script won't give back a whole HTML page, but rather one line containing result values. However, this sensor parses the results and uses anything written between square brackets as a value for one sensor channel. Numbers are expected as values. Anything else will lead to a zero ("0") value for the channel.

The most common use is to monitor a particular value inside a web server for validity. For example, if you have a script or CGI running on the web server that merely publishes the free disk space of the server's hard disk and the current processor usage (e.g. "[10222][12]" as result) you can actually monitor these values in two different channels of the sensor. Of course many other usage concepts are possible.

For general settings, please refer to "Common Settings - HTTP Sensors" (above). Additionally, you can enter the following settings:

- **Script Url:** Enter the URL of the script you want to request the results from.
- **Value Type:** Enter the type of values that your script sends back as results. You can choose between Integer and Float values.
- **Number of channels:** Enter the number of values your script will send back. Remember: Each value must be enclosed in square brackets and each value is handled in an own sensor channel. So, if your script sends back e.g. "[10222][12]" as result, enter "2" for "Number of channels" to catch both values. If your script sends back less values than the number specified here, this will result in an error. The number of channels cannot be changed later.
- **Content:** Check "Monitor changes" to monitor any changes to the values your script sends back. In a second step, this can be combined with an "On Change" notification trigger (tab "Notifications" in sensor's settings).
- See the Paessler Knowledge Base for examples on how to use this sensor.

For examples on how to use the HTTP Content Sensor, see Knowledge Base articles:

<http://www.paessler.com/knowledgebase/en/tags/http-content-sensor/>

Notes for HTTP Full Web Page Sensor

This sensor uses Internet Explorer to load a full web page, including all images and page elements, and monitors the loading time. Please note that only the given URL is monitored and no links are followed.

What it Means When the HTTP Sensor is "Up"

The UP status of an HTTP sensor means that the web server delivers an HTTP result that is correct according to the HTTP protocol and that the URL is available. This means that the web server software is up and running but you do not know whether the results are correct, e.g. the webpage can contain error messages. So you don't know whether the CGI scripts etc. are working correctly or whether, for example, the database of the web server is ok. It is recommended to also check the content of a web page by using the HTTP Advanced Sensor, instead of the simple HTTP sensor, for added reliability.

What it Means When the HTTP Sensor is "Down"

There are numerous reasons for an HTTP sensor to fail. Besides normal connectivity problems, the most common problems are internal server errors (error codes 50x) and problems caused by an incorrect URL (error code 404, page not found).

Bandwidth Issues and Log File Analysis Issues

Important: Keep in mind that the HTTP sensor can create substantial bandwidth load since it is one of the sensors that transfers many bytes per requests (sometimes 1000 times more than a simple ping). So, choosing a URL that only provides a small HTML page in return is recommended if you have to pay for the bandwidth (either for your connection or for your web server). This is certainly not a major problem in most LANs and Intranets, but bandwidth usage should always be monitored. Requesting a 25 kb web page with an interval of one minute creates a traffic of 36 MB per day or more than one Gigabyte per month.

Also, keep in mind that the monitoring requests will show up in your web server log analysis (one month of monitoring with a one minute interval will create 43,200 requests). You should filter out the requests from PRTG when analyzing log files. Filtering can be done based on the IP address of the server running PRTG or by filtering requests from PRTG's browser agent:

```
Mozilla/5.0 (compatible; PRTG Network Monitor Vxxxx; Windows)
```

Tools

Paessler URL Recorder: Find out the URLs and the POSTDATA strings that a user sends to a web server while surfing a sequence of URLs - useful when setting up HTTP Transaction sensors.

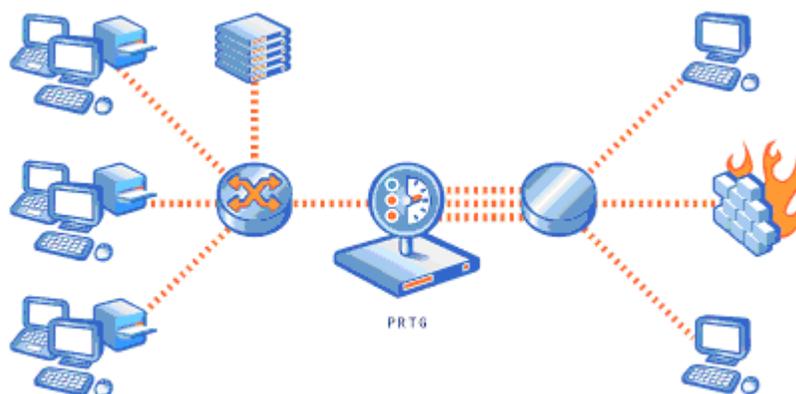
<http://www.paessler.com/tools/>

7.4 SNMP Sensors

The 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.



When this technology is used, PRTG queries the devices (e.g. routers, switches and servers) for the traffic counters of each port with quite small data packets. These are triggering reply packets from the device. Compared to PRTG's other bandwidth monitoring technologies (xFlow/NetFlow, Packet Sniffer and 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 loads, disk usage, temperatures, as well monitoring many other readings (depending on the device).

Important information about network issues: In order to use 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. This is not usually the case for Internet connections, DMZ and WAN connections. Here, 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.

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 linked below (section "See also").

The following sensors use the Simple Network Management Protocol (supports SNMP V1, V2c and V3):

- **SNMP Traffic:** Supports monitoring bandwidth (bits/s) and volume (bytes), as well as the number of packets and errors via SNMP for a port or a network card on PCs, servers, switches, firewalls, printers.
- **SNMP Custom:** Monitors one specific OID supplied by the user.
- **SNMP Library:** SNMP libraries make it easy to create system-specific sensors based on MIBs (some are

included and new ones can be created from standard SNMP MIB files using the free MIB importer tool, see below).

- **SNMP Uptime:** Monitors the uptime of a device (time since last reboot)
- **SNMP Custom:** Monitors a specific OID.
- **SNMP Custom String:** Monitors a string specified by an OID.
- **SNMP Trap Receiver:** Opens a UDP port on a probe and waits for SNMP Traps, then processes the information.

SNMP Version 1, 2c and 3

PRTG supports three versions of the SNMP protocol:

SNMP Version 1: The oldest and most basic version of SNMP.

- **Pros:** Supported by most SNMP-compatible devices; simple to set up.
- **Cons:** 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: Adds 64-bit counters.

- **Pros:** Supports 64-bit counters to monitor bandwidth usage in networks with gigabits/second loads.
- **Cons:** Limited security (same as with SNMP V1).

SNMP Version 3: Adds authentication and encryption.

- **Pros:** Offers user accounts and authentication for multiple users and optional data packet encryption, increasing available security; plus all advantages of Version 2c.
- **Cons:** 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, most of the time 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. The same situation exists if community strings, usernames or passwords are incorrect.

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 60 second interval with one PRTG server (core and local probe) plus two remote probes (10.000 sensors on each probe).

But SNMP V3 has software dependent performance limitations due to the SSL encryption. 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 3,000 SNMP V3 sensors for each probe. If you experience an increased "SNMP Interval Delay" or "Open Requests" reading of the probe health 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 live 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 forwards 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 "public". It is standard practice for network managers to change all the community strings to customized values within the device setup.

Tools

Paessler MIB Importer: Imports MIB (Management Information Base) files and converts them into OID libraries for use with PRTG Network Monitor.

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

Paessler SNMP Tester: SNMP Tester can run simple SNMP requests against a device in a network to debug SNMP requests down to the protocol level in order to find communication and/or data problems in SNMP monitoring configurations.

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

See also

- [Comparison of Bandwidth Monitoring Sensors](#)
- Knowledge Base article "SNMP, MIBs and OIDs - an Overview" on Paessler website:
<http://www.paessler.com/support/kb/questions/49>

7.5 Windows Systems (WMI) Sensors

Windows Management Instrumentation (WMI) is the base technology from Microsoft for monitoring and managing Windows-based systems. WMI allows access to data for 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 and Windows 7 (add-ons are available for Windows 9x and NT4). PRTG officially supports WMI for Windows XP or later.

In order to be able 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. The sensor will then inherit these settings.

WMI Sensors

PRTG supports the following WMI based sensor types:

- WMI CPU Load: Measures CPU load of a system (total and per CPU).
- WMI Memory: Displays free system memory (MB and %).
- WMI Disk Free: Free disk space on fixed drives (MB and %, per drive). Monitors all disks of a target system in one sensor (each volume in a different channel).

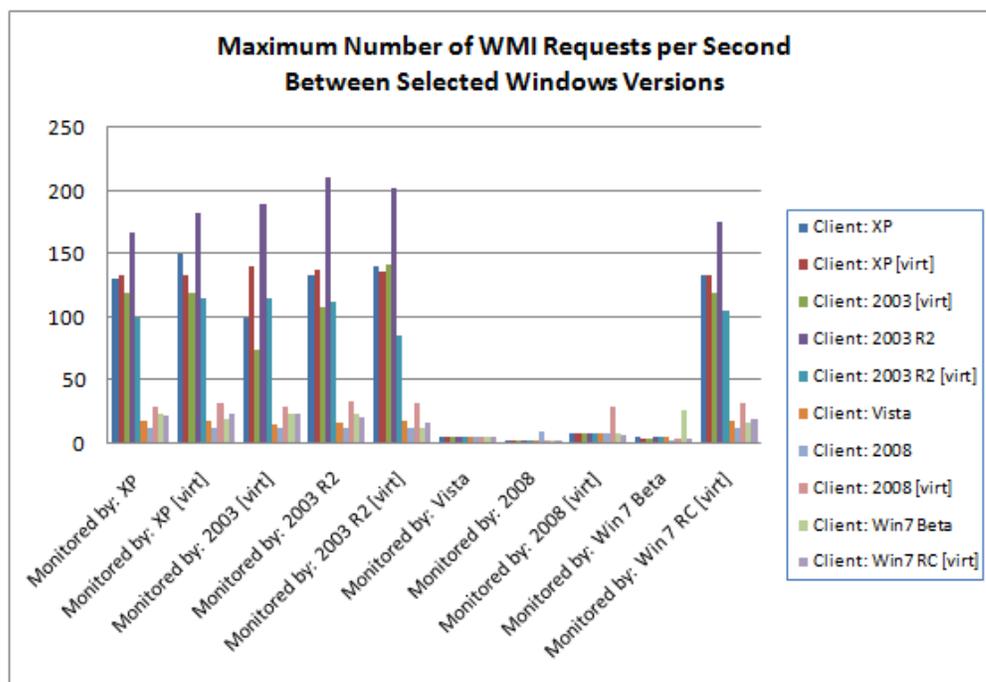
- WMI Network Card: Measures traffic going through network cards.
- WMI Volume: Monitors free disk space on Volumes. Monitors only one volume (one disk) per sensor (available for Windows Vista or higher). Preferred option to WMI Disk Free.
- WMI Pagefile: Checks the usage of the Windows page file.
- WMI Service: Checks if a service is running and optionally restarts a service if it is not running.
- WMI Process: Monitors a single process.
- WMI Event Log: Monitors a system's application, system and security event log for specific events.
- WMI File: Monitors file size and existence, as well as changes to a file.
- WMI Custom: Performs a custom WMI query.
- WMI Vital System Data: Users can select from more than 30 different vital Windows System parameters (CPU: Percent Processor Time, CPU: Processor Queue Length, CPU: Processor Percent Privileged Time, CPU: Processor Percent User Time, System: Thread Context Switches/sec, Memory: Free Physical Memory, Memory: Total Visible Memory, Memory: Pages/sec, Memory: Page Faults/sec, Memory: Page Reads/sec, Memory: Page Writes/sec, Memory: Percent Pagefile Usage, Memory: Pool Nonpaged Bytes, Memory: Pool Paged Bytes, Memory: Cache Bytes, Memory: Committed Bytes, Disk: Percent Disk Time (Windows 2000/XP/Server 2003 only), Disk: Current Disk Queue Length, Disk: Bytes/sec (Windows 2000/XP/Server 2003 only), Disk: Reads/sec (Windows 2000/XP/Server 2003 only), Disk: Writes/sec (Windows 2000/XP/Server 2003 only), Network: Bytes Total/sec, Network: Bytes Received/sec, Network: Bytes Sent/sec, Network: Packets Outbound Errors, Server: Bytes Total/sec, Server: Bytes Received/sec, Server: Bytes Sent/sec, CLR Memory: % Time in GC, CLR Memory: # Bytes in all Heaps, CLR Exceptions: # of Excepts Thrown / sec).

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.

These limitations are not limitations of PRTG, these limitations are coming from the WMI functionality built into the Windows operating systems.

Here are some detailed results of our WMI tests on selected Windows versions:



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 - 30 boxes 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 can't 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).

Links to WMI related articles

Paessler's Guide to Troubleshooting WMI Problems.
http://www.paessler.com/support/kb/prtg7/wmi_not_working/

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>

Microsoft: Windows Management Instrumentation Technical Articles: Managing Windows with WMI

<http://msdn2.microsoft.com/en-us/library/ms811533.aspx>

Microsoft: WMI Reference

<http://msdn.microsoft.com/en-us/library/aa394572.aspx>

See also

[Comparison of Bandwidth Monitoring Sensors](#)

7.6 Various Protocol Sensors

The following sensor types allow to monitor various TCP and UDP based services:

- PING: Performs one or more PINGs to monitor the availability of a device and optionally measure packet loss in percent.
- PORT: Checks the availability of TCP based network services.
- FTP: Monitors the availability of a FTP Server.
- DNS: Checks a DNS (Domain Name Service) server.
- RDP (Remote Desktop): Checks whether the RDP service of a device is available.
- HDD Health: Monitors the health of IDE disk drives via "SMART".
- RADIUS: Checks "Remote Authentication Dial In User Service" servers. It connects to a RADIUS server and checks if login credentials are accepted.
- Syslog Receiver: Receives and analyzes Syslog messages (can only be used in probe devices).
- SNMP Trap Receiver: Receives and analyzes SNMP Traps (can only be used in probe devices).

FTP Sensor

FTP (short for File Transfer Protocol) is used on the Internet for exchanging files (e.g. to upload content to a webpage or to download files from a server). The FTP sensor monitors a FTP server's availability.

Parameters include:

- Timeout: If the reply takes longer than this value the request is aborted and an error state is triggered.
- Port: The port number of the FTP service you want to monitor (usually port 21).
- FTP Mode: If you don't get a connection, use the passive mode.
- Username: The FTP username to log in with.
- Password: The FTP password for this username.
- TLS (Transport-Level Security): Select whether or not to use a secure connection. If you chose "Use", you can additionally select an SSL-Method. If you do not get a connection, try a different SSL method.

DNS Sensor Configuration

The DNS (Domain Name System or Service) is an Internet service that translates domain names (which are easier for humans to remember) into IP addresses (which computer use to address each other). Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For

example, the domain name `www.paessler.com` might translate to `62.146.51.168`.

The DNS sensor sends a request to resolve a specific domain name to an IP address to the server it is associated with. This is useful e.g. to ensure that a company's web server address can be resolved by the outside world or to check a DNS server in a LAN for availability.

Note: The device associated with this sensor has to be a DNS server and not the domain name of the server you want to monitor. As DNS server, the sensor will use the IP-Address/DNS Name of the device you're creating this sensor on.

If you only enter the Domain in the settings, PRTG will only check whether the name is resolved to an IP address at all (which simply means that the DNS server works correctly and the domain name is valid). If you also enter an IP address the resolved IP address will be compared to this and the sensor will show an error when the two addresses are different.

DNS Specific parameters include:

- Timeout: If the reply takes longer than this value the request is aborted and an error message is triggered.
- Port: Define the DNS port.
- Domain: Enter the domain name to look up (e.g. `www.yourcompany.com`).
- IP Address: Optionally enter an IP address to compare the result with.

7.7 Mail Server Sensors

Using a number of sensors for mail servers you can ensure that your mail systems are working.

Standard Email Sensors

- SMTP: Monitors availability of SMTP based email servers (Simple Mail Transfer Protocol).
- POP3: Monitors availability of POP3 based email servers (Post Office Protocol V3).
- IMAP: Monitors availability of IMAP based email servers (Internet Message Access Protocol).
- Exchange 2003: Monitors a Microsoft Exchange Server 2003.
- Exchange 2007: Monitors a Microsoft Exchange Server 2007.

Email Round Trip Sensors

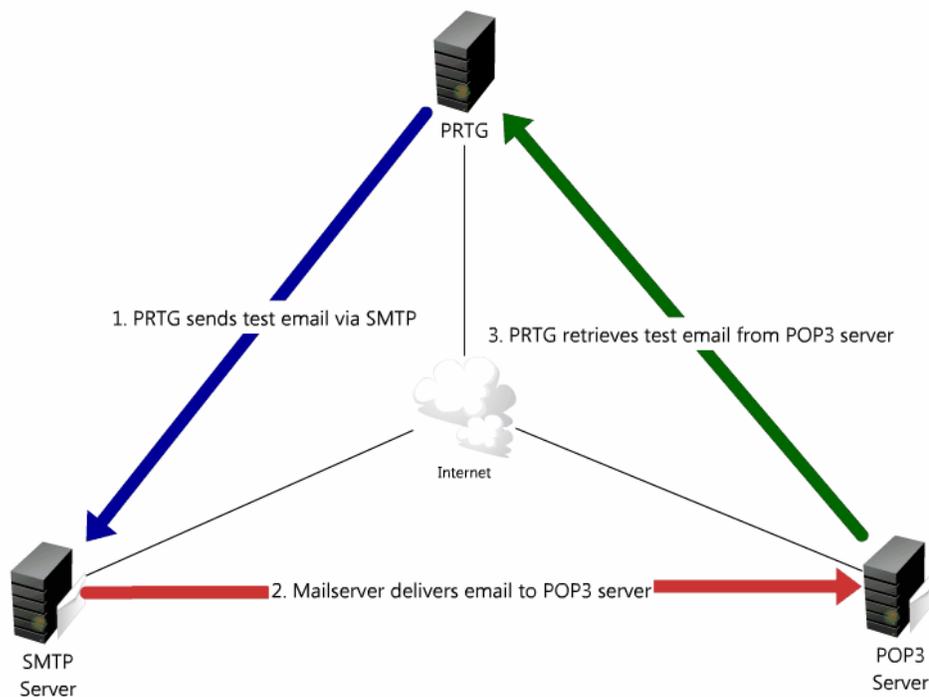
Email round trip sensors ensure the end-to-end delivery of emails and make it possible to monitor availability and performance of a complete email delivery process. There are two sensor types for this task:

- SMTP&POP3 Round Trip Sensor
- SMTP&IMAP Round Trip Sensor

Both initially deliver an email to a mail server using SMTP. Afterwards the receiving mailbox is scanned using POP3 or IMAP until the email arrives. The test email contains a unique code in the topic which is used to identify the email (e.g. "PRTG7 Roundtrip Mail: {6D136420-5A3E-46CF-871A-1DAF0C4F3D5D}").

The graph shows a sample configuration:

- 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 retrieves emails from 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, freemailer 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).

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.

7.8 SQL Server Sensors

Using the SQL Servers sensors you can natively monitor the most commonly implemented SQL servers: MySQL, Microsoft SQL, and Oracle SQL. The sensors monitor if the database server

- A: accepts connections and
- B: processes requests and
- C: returns an expected result when executing a custom SQL command.

PRTG supports native monitoring for the following SQL Servers:

- Microsoft SQL Server: Checks Microsoft SQL server connections.
- MySQL Server: Checks MySQL server connections.
- Oracle SQL Server: Checks Oracle SQL server connections.

General steps for setup

- Identify the IP address or the DNS name of your database server.
- Create a new device in PRTG Network Monitor. You can do this with the context menu of a group. If you already have an adequate device object created you can skip this step.
- In the configuration page of this device object locate the "DNS Name" property. Enter the IP address / DNS name from the first step. If you already have a device object with the correct address information you can use it and skip this step.
- Open the context menu of the device object from above and select "Add Sensor".
- Select the appropriate SQL Sensor type (Microsoft SQL, Oracle SQL, MySQL) and click on "Continue".

Common Settings for all SQL Sensors

Configuring the sensor consists of two steps:

- Setting connection relevant properties. This is mandatory to get a working sensor.
- Optional configuration of a SQL expression which the sensor should execute over the existing connection to the database server.

The following fields are particular to all of these sensors (there are others that appear with certain SQL Sensor types only - see below):

- Database: In this field, the name of the database or the path of the database can be entered in order to access the database information. Do not confuse this with the name of the database server (which is set in the corresponding device setting in PRTG Network Monitor).
- User/Password: Please enter your SQL server's credentials needed to log into the database.
- SQL-Expression: Provide an expression for querying or modifying database objects like tables, views, roles. When a cursor is returned (i.e. with a SELECT statement), only the first row of data will be fetched.
- Result Set: Select this checkbox if your SQL expression returns a result set. Then the value of the first column in the first row of the result set is used as the return value of the monitoring request (i.e. will be compared to the limits). Otherwise, the "number of affected rows" is regarded to be the return value of a monitoring request. The latter usually makes sense with a data modification statement like DELETE. **Note:** The Result Set has to be of type "integer".

Notes for Microsoft SQL Sensors

- Supports 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).
- Instance: This holds the name of the instance if you want to connect to a "named instance", otherwise this field should remain empty. **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).

- Port: If your SQL server runs the instance at a different static port than 1433, you can define the port number here. Select "Manual" and change the port number.
- Authentication: When using a Microsoft SQL server, you can also choose to use the Windows Authentication, if probe computer and the Microsoft SQL Server are in the same domain. You can change the Credentials for Windows Systems in the settings of the device on which you are creating the sensor. As default, these settings are inherited from the Root group, unless specified differently (see [Reviewing Settings of the Root Group](#) for more details).

For more configuration tips, see Paessler Knowledge Base article:

<http://www.paessler.com/knowledgebase/en/topic/1063>

Notes for Oracle SQL Sensors

- 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).
- Connections work through direct TCP/IP communication (SQL-NET). **Note:** OCI is not supported any more.
- Port: You need to supply the TCP/IP port for the connection in this field. Usually the default value "1521" is correct.

Notes for MySQL Sensors

- Supports MySQL server 5.1, 5.0, 4.1, 4.0 and 3.23.
- **Note:** For this sensor type, no port number can be set.
- The 'database' setting 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'.

7.9 File Server Sensors

In order to monitor file servers you can use the following sensors.

- WMI Disk Free: This sensor monitors free disk space on fixed drives via WMI. Monitors all disks of a target system in one sensor (each volume in a different channel). For more information see [Windows Systems \(WMI\) Sensors](#).
- WMI Volume: Monitors free disk space on Volumes via WMI. Monitors only one volume (one disk) per sensor (available for Windows Vista or higher). Preferred option to WMI Disk Free. For more information see [Windows Systems \(WMI\) Sensors](#).
- WMI File: Monitors file size and existence, as well as changes to a file via WMI. For more information see [Windows Systems \(WMI\) Sensors](#).
- Share Disk Space: Monitors free disk space of SMB shares (Windows/Samba).
- File: Monitors a file's existence, size and age and also discovers changes to the file via SMB.
- Folder: Monitors a folder's existence as well as the number of files and their ages/sizes and also discovers changes to the folder's content.

Note: The File Transfer Protocol (FTP) Sensor can be found in [Various Protocol Sensors](#).

7.10 Virtual Server Sensors

With PRTG you can monitor the vital parameters of VMware and Microsoft Hyper-V host servers and the virtual machines running on them. Also Amazon EC2 instances of Amazon AWS can be monitored via CloudWatch.

VMware Sensors

The sensor types for VMware are:

- VMware Host Server: Monitors a VMware ESX/ESXi Host Server (version 3.5 or vSphere 4.0)
- VMware Virtual Machine: Monitors a single virtual machine

While the Host Server sensor only works directly with an VMware ESX/ESXi server as its parent device you can use the Virtual Machine sensor in two ways:

- Use it to directly communicate with a VMware ESX/ESXi Host Server to monitor virtual machines running on this server.
- Use it to communicate with a VMware Virtual Center installation to monitor all virtual machines managed by this virtual center. Only this option supports virtual machines running on VMware Server 2.x and virtual machines that are under control of VMware's VMotion feature.

For VMware sensors PRTG needs an administrator login for the host server(s). You can enter these credentials in the VMware Credentials section for the parent device or group. The sensors will then inherit these settings.

Remarks

Due to performance limitations we recommend to keep the number of VMware sensors querying the same virtual server and using the same user account below 20. If you have more sensors you should use two or more user accounts or you should distribute the sensors across multiple probes.

VMware is a registered trademark of VMware Inc.

Microsoft Hyper-V Sensors

Hyper-V is the virtualization technology built into the latest Windows servers. With PRTG you can use two sensors to monitor Hyper-V Servers:

- Hyper-V Host Server: Monitors vital parameters of Hyper-V host servers.
- Hyper-V Virtual Machine: Monitors vital parameters of a single virtual machine on Hyper-V.

Amazon CloudWatch Sensor

If you are using Amazon EC2 (Elastic Compute Cloud) to host one or more servers then this new sensor is for you. Amazon offers the CloudWatch service for EC2 instances since May 2009 and it provides performance data for individual instances on EC2 (usage of this service costs a little extra).

1. Please use the Amazon AWS Management Console (<http://aws.amazon.com/console/>) to enable CloudWatch for the instance(s) that you want to monitor with PRTG.
2. In PRTG create a new device for your EC2 instance (if you don't have one already) and then add a new CloudWatch sensor to it. All you need to enter are your "AWS Access Key ID", "AWS Secret Access Key" and the "Instance ID". Click OK and your sensor will start automatically.
3. The Amazon CloudWatch sensors monitors CPU Utilization, Disk Read Ops, Disk Write Ops, Network In, Network Out.

You could also monitor the values "from the inside" by monitoring from the "guest operating system" itself. But using CloudWatch has two advantages:

- Operating system independence: You can monitor the vital system parameters regardless of the OS running on the instance.
- More security: You don't need to open any ports for monitoring requests to the instance.

7.11 VoIP and QoS Sensors

The sensors in this section can monitor Quality of Service using PRTG's own QoS sensor as well as Cisco IP-SLA. 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 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, 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 (< 20 - 50 ms) and PDV (< 100 ms) and "zero" measurements for packet loss, duplicated and out-of-order packets.

Two sensors are available:

- QoS (Quality of Service): Monitors VoIP relevant network parameters by testing network connection quality between two probes
- Cisco IP SLA: Monitors VoIP relevant network parameters through IP SLA results from Cisco devices (via SNMP)

QoS (Quality of Service) Sensor

The "QoS Sensor" is used to monitor the quality of a network connection by measuring the following "quality of service" 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 remote probes. This means that you can test any network connection in your network by simply placing a remote probe 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, measurement takes place 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 (the local probe on the PC running the PRTG Core can also be used as one end). If any firewalls, packet filters or NAT systems are en-route you must configure them as necessary so that the UDP packets can reach the target probe. In PRTG new QoS sensors must be created with a "probe device" as the parent device. The UDP packets will be sent from this probe to the target probe. During the creation of the sensor you are going to choose the target probe that the UDP packets shall be sent to for measurement. To get started right click a probe device, choose "Add Sensor" and then choose "QoS (Quality of Service)" from the "VoIP and QoS" group. On the next web page you can configure the sensor. Please choose a probe from the "Target probe" drop down. The list shows the probes with the IP address that is currently used by each probe to connect to the core. Nevertheless you must enter the IP address manually because the target probe's IP from the perspective of the sending probe may be different (e.g. due to NAT). You also have to choose a UDP port number (please use one port number per QoS sensor). With the settings for number and for size of the packets you can configure the test data stream, 1000 packets of 172 bytes is good for a 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 have a look at sound quality for VoIP traffic.

If you haven't done so already you must create a device for the Cisco device that you want to monitor. Remember to enter SNMP credentials because PRTG uses SNMP to get the data from the switch. The second step is to create a new sensor on that device, choose "IP SLA" from the "VoIP and Infrastructure" section and follow the instructions on the screen. A few moments later you will see the current measurements in PRTG's user interface.

This feature is only available in the more expensive boxes from Cisco. If you don't have IP SLA capable routers/switches you can still get similar information with PRTG's QoS sensor (see above) 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).

For MOS, Cisco conducted a panel test where a wide range of listeners have 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)

Notes

For more information about these measurements see "IP SLAs - Analyzing Service Levels Using the VoIP Jitter Operation" on the Cisco website: http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsvoipj.html

7.12 Custom Sensors

Custom sensors allow a number of monitoring tasks that go far beyond the standard sensor set to be performed. Apart from parameterized versions of SNMP, packet sniffer and NetFlow sensors you can create your own sensors using WQL (WMI Query Language) and by compiling an EXE file, using any Windows software development tool.

PRTG supports four custom sensor types:

- SNMP Custom: Monitors a specific OID (you must supply an OID for this sensor). See [SNMP Sensors](#).
- SNMP Custom String: Monitors a string returned by a specific OID.
- WMI Custom: Performs a custom WMI query written in WQL (WMI Query Language). See [Windows Systems \(WMI\) Sensors](#).
- EXE/Script: Runs a custom program (EXE, DLL) or script/batch file.
- Packet Sniffer (Custom): Accounts for data packets using user-specific rules, see [Packet Sniffer Sensors](#).
- NetFlow V5 and V9 (Custom): User configurable versions of the NetFlow sensor, see [xFlow Sensors \(NetFlow and sFlow\)](#).
- sFlow (Custom): User configurable version of the sFlow sensor, see [xFlow Sensors \(NetFlow and sFlow\)](#).
- Sensor Factory: see [Sensor Factory Sensors](#).

Custom EXE/DLL/BAT/CMD/VBS/PowerShell and WQL Sensors

You must create the sensor as a file and place it in a specific folder on the system running the PRTG probe (i.e. if you are using remote probes the files must be copied to the remote system!):

- Place executables (.EXE, .DLL), batchfiles (.CMD, .BAT), VBS scripts (.VBS), or PowerShell scripts (.PS1) into the "PRTG Network Monitor\Custom Sensors\EXE" subfolder.
- Place WQL scripts (.WQL) into the "PRTG Network Monitor\Custom Sensors\WMI WQL scripts" subfolder.

You will find a sample set of demo sensors in these folders, too. As soon as a file is placed into the folders mentioned above, you can create or edit your own Custom EXE sensor or WMI Custom sensor and select the new file from the list of files.

The local probe will run the file on the local PRTG Core Server system. But for remote probes, the file will actually run on the remote system. If your custom sensor code relies on other files (eg. DLLs, .NET framework, Windows PowerShell etc.) you must copy/install these files onto the probe machine manually! The probe (either

local or remote probe) will execute the file on the probe system using the user account configured for the "PRTG 7 Probe Service" (local "system" account is the default). You can change the account running this service in the Windows Computer Management console ("Services").

See [Interface Definition for Custom EXE Sensors](#) for detailed documentation. There, you will also find information about what placeholders are allowed in the "parameter" field.

Notes

- For PowerShell scripts, make sure that they may be executed by either code signing the files or changing the security policy for Powershell.exe accordingly.
- The API interface for custom EXE sensors is compatible to the custom EXE sensors provided by IPCheck Server Monitor 5.
- If you're looking for a sensor to work with scripts running on a remote web server, please see documentation for "HTTP Content" sensor (section [Web Server \(HTTP, HTTPS\) Sensors](#)) and also see the Paessler Knowledge Base at <http://www.paessler.com/kb>

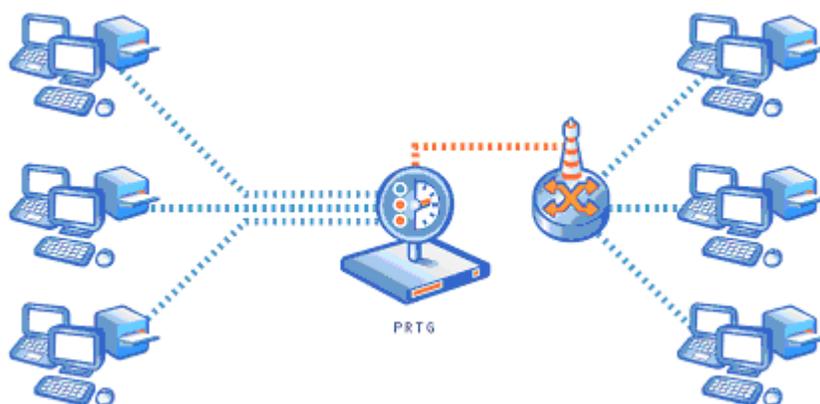
7.13 Packet Sniffer Sensors

Packet Sniffing should come into consideration if your network device(s) do not support [SNMP](#) or [xFlow](#) to measure bandwidth usage or 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](#).

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 [Multiple Probes and Remote Probes](#)).

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 of all data packets traveling through the switch to the monitoring port. As soon as you connect the PRTG core 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.

The Different Packet Sniffer Sensor Types

PRTG offers three sensor types that are based on Packet Sniffing:

- Packet Sniffer (Header): Looks at the headers of the data packets to account traffic by IP, by port, by protocol etc.
- Packet Sniffer (Content): Reassembles data packets to streams and looks into the payload data of the streams to assess the type of traffic (e.g. SMTP, HTTP, IMAP, file sharing, NETBIOS etc.).
- Packet Sniffer (Custom): Accounts for data packets using user-specific rules (header based). You find this sensor in the group "Custom Sensors".

In the sensor settings, you can enter Sniffer specific settings to specify the traffic that should be monitored (specific packets, IPs, ports, etc.). You can set Include or Exclude Filters and enter Channel Definitions. Please see the context help on the settings page for more details.

Packet sniffing can differentiate between the following protocols (in the sensor's "Channel Configuration"):

- Web/WWW Traffic: HTTP, HTTPS
- File Transfer: FTP
- Mail Traffic: IMAP, POP3, SMTP
- Chat, Instant Messaging: IRC, AIM
- Remote Control: RDP, SSH, Telnet, VNC
- Network Services: DHCP, DNS, Ident, ICMP, SNMP
- NetBIOS: NETBIOS
- Various: Socks, SSL, OtherUDP, OtherTCP

Header Based vs. Content Based Packet Sniffing

PRTG provides two base technologies for packet sniffing:

- Header based: PRTG looks at the IPs and ports of source and destination to assess the protocol. This is very fast but, at times, not very accurate. For example it is not possible to identify HTTP traffic on ports other than 80, 8080 and 443 as HTTP.

- Content based: PRTG captures the TCP packets, reassembles the data streams and then analyzes the content of the data using an internal set of rules to identify the type of traffic. This is quite accurate (e.g. HTTP traffic on any port number is accounted for as HTTP) but requires much more CPU and memory resources, especially when a lot of traffic passes the network card.

To summarize, header based sniffing is much faster but the accounting is less reliable (e.g. HTTP packets on non-standard ports are not accounted as HTTP traffic). Content based sniffing is quite accurate, but creates more CPU load.

Tools

Paessler Card Packet Counter: Shows short term statistics about the network data packets passing a local network card.

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

See also

- [Comparison of Bandwidth Monitoring Sensors](#)
- [Toplists](#)

7.14 xFlow (NetFlow and sFlow) Sensors

Some routers and switches can capture and export bandwidth usage data using the NetFlow and sFlow protocols. Both options are specially suited for bandwidth monitoring in high traffic networks.

Both technologies are quite similar and are commonly referred as "xFlows" in PRTG.

- NetFlow is a network protocol developed by Cisco Systems for collecting IP traffic information. Many of the larger Cisco IOS-enabled routers and switches support this feature. Besides Cisco devices also some routers from other vendors support NetFlow export (e.g. Juniper jFlow can export NetFlow data).
- sFlow is a cross-vendor standard and alternative to Netflow

xFlow sensors support Toplists (Top Talkers, Top Connections etc.), see [Toplists](#).

How xFlow Monitoring works

You can measure bandwidth usage "by IP address" or "by application" in a network by using one of the xFlow 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 NetFlow the ideal option for high traffic networks that need to differentiate the bandwidth usage by network protocol and/or IP addresses.



NetFlow Monitoring

PRTG supports flow monitoring using NetFlow with the following sensors types:

- NetFlow 5: Monitors switches using NetFlow V5.
- NetFlow 9: Monitors switches using NetFlow V9.
- NetFlow 5 (Custom): User configurable version of the NetFlow sensor.
- NetFlow 9 (Custom): User configurable version of the NetFlow sensor.

Before you can create NetFlow sensors, you must configure the NetFlow export on your switch/router. Configure the switch to send the NetFlow packets to the computer running a PRTG probe (either the local probe or a [remote probe](#)). The NetFlow port (port number that the UDP packets are sent to) and the flow timeout must be set to the same value in the router and in PRTG. Finally don't forget to open the NetFlow port in the PRTG system's firewall. Paessler supplies two test tools for debugging NetFlow installations as well as tips for the router setup (see below).

sFlow Monitoring

PRTG supports flow monitoring using sFlow with the following sensors types:

- sFlow: Monitors switches using sFlow.
- sFlow (custom): User configurable version of the sFlow sensor.

Before you can create sFlow sensors, you must configure the sFlow export on your switch/router. Configure the switch to send the sFlow packets to the computer running a PRTG probe (either the local probe or a [remote probe](#)). The sFlow port (port number that the UDP packets are sent to) must be set to the same value in the router and in PRTG. Finally don't forget to open the sFlow port in the PRTG system's firewall.

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 probe health reading as soon as NetFlow packets are not processed due to an overload (see Probe Health sensor on the 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.

Tools

Paessler NetFlow Generator: NetFlow Generator creates artificial NetFlow Version 5 data streams without the need for NetFlow compatible hardware. It is a perfect tool to test the NetFlow functionality of PRTG or other NetFlow compatible programs.

<http://www.paessler.com/tools/netflowgenerator>

Paessler NetFlow Tester: NetFlow Tester simply dumps the data of all NetFlow 5 packets that a computer receives from a Cisco router - useful when debugging bandwidth monitoring configurations based on NetFlow protocol.

<http://www.paessler.com/tools/netflowtester>

See also

- [Comparison of Bandwidth Monitoring Sensors](#)
- [Toplists](#)
- Paessler Knowledge Base: Configuration Tips for Cisco Routers and PRTG
<http://www.paessler.com/support/kb/questions/20/>
- Cisco Netflow information: <http://www.cisco.com/go/netflow>
- sFlow website: <http://www.sflow.org>

7.15 Comparison of Bandwidth Monitoring Sensors

The following table shows the differences between PRTG's four methods available for bandwidth monitoring:

	WMI	SNMP	Packet Sniffer	xFlow (Netflow, sFlow)
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	No	No	Yes	Yes

	WMI	SNMP	Packet Sniffer	xFlow (Netflow, sFlow)
Connections, Top Protocols etc.)				
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
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

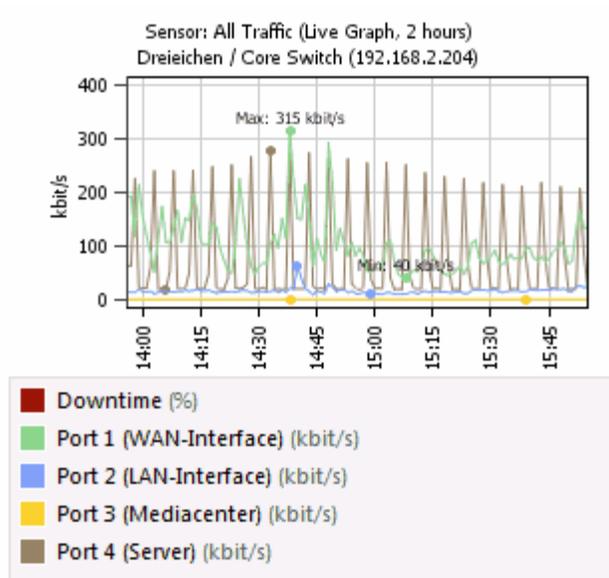
7.16 Sensor Factory Sensors

A sensor with special capabilities is called "Sensor Factory". It allows combining measurements from two or more sensors into one new sensor.

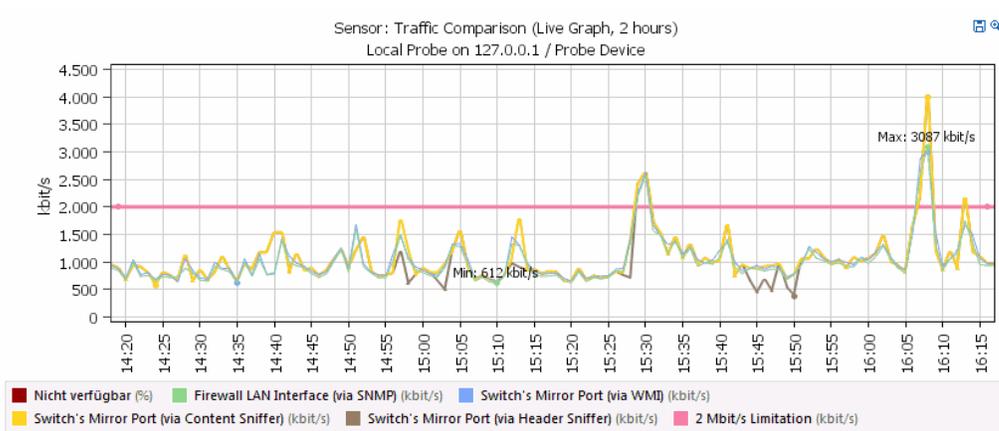
Samples for usage are:

- Show two or more channels from one or more sensors in one graph.
- Add the value from two or more channels from one or more sensors into a new value (you can also subtract, multiply and divide values).
- Create charts with one or more graph lines and one or more horizontal lines at specific vertical positions.

This is the graph of a Sensor Factory with 4 channels that use data from 4 different sensors:



Here is second sample: A sensor factory which compares the results of an SNMP sensor, a WMI sensor and two packet sniffer sensors for one data line. And there is a horizontal line at 2 Mbit/s.



The Sensor Factory can be found in the "Custom Sensors" section when creating a new sensor.

Channel Definition Basic Syntax

The behaviour of a Sensor Factory sensor is controlled by a text field called "Channel Definition". The basic syntax for a channel definition looks like this:

```
#<id>: <name>[ <unit>]
<formula>
```

For each channel one section is used. A section begins with the # sign. Here is an example with two channels:

```
#1: Sample
Channel(1000,0)
#2: Response Time[ ms]
Channel(1001,1)
```

The parameters are:

- <id> must be a unique number (1 or greater).
- <name> is the name of the channel (displayed in graphs and tables).
- [<unit>] is optional (e.g. bytes). If it is not provided a fitting unit string is automatically selected (recommended).
- <formula> contains the formula to calculate the channel.

In the formula the following elements are allowed:

- Basic operations: + - * / -
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 1, otherwise 0, for delta sensors the speed is compared.
- Functions: channel, min, max, avg, percent.

channel() Function

The channel() function allows to read the data from a channel of a different sensor. The syntax is:

```
channel( <SensorId>, <ChannelId>)
```

- The SensorId is displayed on the sensor details page, in the "Overview" tab behind the sensor name.
- The ChannelId is displayed on the sensor details page, in the "Channels" tab for each channel behind the channel name.

Example: Read the data of sensor ID 2001, channel ID 2:

```
channel( 2001, 2)
```

Channels can be gauge values (e.g. PING ms) or delta values (e.g. traffic kbit/s) values. Not all combinations are allowed in a formula. There are calculations you **cannot** do:

- You cannot add/subtract a delta from a gauge channel (and vice versa).
- You cannot multiply two delta channel.
- You cannot compare a delta with a gauge channel.
- You cannot use a channel of (another) Sensor Factory channel in the formula.

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 b are either numbers or channel() functions, see this example:

```
min( 10, 5 )
min( channel( 2001, 1 ), channel( 2002, 1 ) )
```

The first one returns "5", the latter one returns the minimum of channel 1 of the sensors with IDs 2001 and 2002.

avg() Function

avg() returns the average of the two values. This equals: (a+b) / 2. The syntax is:

```
avg( <a>, <b> )
```

Example:

```
avg( 20,10)
```

This function returns "15".

percent() function

Calculates the percent value of a value (e.g. a channel) compared to a given fixed value. The syntax is:

```
percent( <source>, <maximum>[ , <unit>])
```

"Source" is the value the percent is calculated for. This is usually a "channel()" function. "Maximum" is the limit value used for the percent calculation. This value is multiplied with the maximum value. "Unit" is optional and is the unit the maximum is provided in. You can use constants with this function (see below for a list). This can be used for gauge (e.g. PING) sensors and delta (e.g. Traffic Sensors).

The following example shows how to display a traffic sensor as % of maximum bandwidth (100 kilobit/second):

```
#1: Usage IN
percent( channel( 2001,0) , 100, kilobit)
#2: Usage OUT
percent( channel( 2001,1) , 100, kilobit)
```

Another example shows how to display the values of a sensor as percentage of 200ms:

```
#1: Ping %
percent( channel( 2002,0) , 200)
```

Horizontal Lines

You can add lines to the graph using a formula without a channel() function (returning a fixed value). In this case you have to provide the unit of the axis the line is used for. You can use constants here. Examples:

```
#1: Line at 100ms [ms]
100
#2: Line at 50 kbit [kbit/s]
50
#3: 2 Mbit/s [kbit/s]
2000
```

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

Channel Settings

The color, line thickness, warning/error limits, etc. can be edited on the "Channels" tab after creating the sensor. This works like with any other sensor. You can also use triggers to send notifications. See section [Edit Sensor and Channel Settings](#) for more details.

Tips and Infos

- The data is always calculated on the fly using the Historic Data of the sensors if available.
- The display of live data for Sensor Factory sensors can be delayed since it has to wait for data in all used channels.
- You can use channels from sensors with different scanning intervals to create a new channel, but it is recommended to use the same interval for the source sensors and the Sensor Factory.
- There is no uptime/downtime totals calculation for Factory Sensors.
- The coverage of the Sensor Factory is defined as the minimum coverage of all Sensor Factory channels.
- The coverage of a Sensor Factory channel is the weighted average coverage of the sensors used in the calculation.
- The downtime channel of Sensor Factory sensors is defined as the average of the downtime of all used channels.

Part



Notifications

8 Notifications

"Notifications" are used to send alerts to the user whenever PRTG discovers a defined state, such as slow or failing sensors, or when thresholds are reached. You can define an unlimited number of notifications allowing to use one, or more, of several communication channels like email, pager, SMS messaging, and many more.

To see a video of this, please go to http://www.paessler.com/support/video_tutorials

Overview

Notifications can be triggered by:

- Sensor status changes (a sensor goes down or up, responses are slow or the sensors show an unusual status).
- When the measured value reaches a specific threshold (e.g. higher than 1,000 ms request time for more than 30 minutes).
- Reaching a specific speed threshold (e.g. more than 1 Mbit/s for more than 5 minutes. Traffic sensors only).
- Reaching a specific data volume threshold (e.g. more than 1 Gbyte transferred in 24 hours. Traffic sensors only).

Notifications can be sent by:

- Send Email: PRTG provides a built-in mail server (uses MX records to deliver emails) or can use an available SMTP relay. Please see "Check Notification Delivery Settings" in this section.
- Add Entry to Event Log: Write an entry into the local system event log.
- Send Network Broadcast (NET SEND): Send a message using Windows' NET SEND command (Note: NetSend is no longer supported on computers running Windows Vista, Windows Server 2008 or Windows 7).
- Send Syslog Message: Send a message to a Syslog server.
- Send SNMP Trap: Send a message to a computer running a trap receiver.
- Send ICQ or MSN Message: Send a message via instant messenger. Please see "Check Notification Delivery Settings" in this section.
- Send SMS/Pager Message: Send SMS or pager message through third party services. Please see "Check Notification Delivery Settings" in this section.
- Execute HTTP Action: Send postdata to a URL.
- Execute Program: Run an external program or batch file.
- Play Sound File: Play a sound via external speakers of the system running the PRTG core (sound card required).

Notifications contain valuable sensor information, such as:

- Last error message.
- Last good/failed request.
- Total downtime.
- Total uptime.
- Recent sensor history.

You can use various placeholders in your message. Some are already filled in by default. For a list of all placeholders, please refer to the Knowledge Base article at the end of this section ("More").

Using Notifications

There are three steps to take in order to use notifications with PRTG:

1. In the "System Setup", check the "Notification Delivery Settings".

2. In the "Account Settings", create/edit notifications for later use.
3. In an object's settings, create triggers that invoke your notifications.

Check Notification Delivery Settings

Before using certain notification methods, a general one-time administrator setup is required. Please refer to the section "Notification Delivery Settings" in [System Administration - Edit System Setup](#).

Creating Notifications

To create or edit notifications, choose "Setup | Notifications" from the main menu. Click a name to edit a notification or click on "Add new notification" to create a new one:

Edit Notification

Home > @notifications > (new object)

Basic Notification Settings

Notification Name: ! The name of the notification.

Status: started paused

Schedule: Using Schedules you can pause notification at specific days and hours throughout the week. You can edit schedules in the system settings.

Postpone: No Yes 'Yes' means when this notification is triggered during a scheduled pause it will be sent after the scheduled pause ends. With 'No' it will be discarded.

Access Rights

User Group Access	User Group	Rights
	PRTG Users Group	<input type="text" value="None"/>
	readonly user	<input type="text" value="None"/>
	testusers	<input type="text" value="None"/>

Set user groups access rights for this object. You cannot remove rights defined for a parent node. All rights are inherited to child nodes

Send Email

Add Entry to Event Log

Send Network Broadcast (NET SEND)

Send Syslog Message

Send SNMP Trap

Send ICQ Message

Send MSN Message

Send Yahoo Message

Send SMS/Pager Message

Execute HTTP Action

Execute Program

Play sound file

You can enable one or more communication types by checking the respective checkboxes. Then, fill out the specific settings for each type. Refer to the help messages next to the form fields for more information. Be sure to enter a meaningful name for the notification to make it easier for you to find it later in the notification trigger settings.

How To Trigger Notifications

A notification is sent by a trigger. These connect sensors and notifications. PRTG supports five different trigger types:

- **State Triggers:** Trigger a notification when a sensor enters an UP, DOWN, WARNING or UNUSUAL state. For state triggers, there are also escalation notifications available (see below).
- **Speed Triggers:** Trigger a notifications when a traffic sensor reaches a certain bandwidth limit for a specified time.
- **Volume Triggers:** Trigger a notification when a traffic sensor has reached a certain volume limit in a specified time.
- **Threshold Triggers:** Trigger out notifications when certain values are measured by a sensor.
- **Change Triggers:** Change triggers are triggered by some sensors whenever the content of a file or the event log has changed.

It is recommended to define triggers for notifications on a group or device level. Sensors will then inherit these settings (see [Inheritance of Settings](#)). The advantage is that you can change notifications for multiple sensors by merely editing the notification settings on the group level.

Editing of the notification triggers takes place under the "Notifications" tabs in the detail view of probes, groups, devices or sensors:

The screenshot displays the 'Notifications' configuration window. At the top, there are navigation tabs: Overview, 48 Hours, 30 Days, 365 Days, Alarms, Log, Settings, **Notifications**, Comments, and History. The main content area is divided into four sections, each with a title and a brief description:

- State Trigger(s)**: State Triggers are triggered when a sensor enter or leaves a DOWN, WARNING or UNUSUAL state. This is the most common reason to send out notifications. Below this is a table with columns: Condition, Latency (sec.), On Notification, Off Notification, Esc. Latency (sec.), Esc. Notification, Repeat every (min.), and a Delete button. One trigger is listed with Condition 'Down', Latency '60', On Notification 'Mail to Admin', Off Notification 'Mail to Admin', Esc. Latency '300', Esc. Notification 'Mail to Admin', and Repeat every '0'. An 'Add State Trigger' button is below the table.
- Speed Trigger(s)**: Using Speed Triggers you can send out notifications when a traffic sensor reaches a certain bandwidth limit for a specified time. Below is a table with columns: Channel, Condition, Value, Scale, Time, Latency (sec.), On Notification, and Off Notification. The table is empty with '(no triggers defined)'. An 'Add Speed Trigger' button is below.
- Volume Trigger(s)**: Using Volume Triggers you can send out notifications when a traffic sensor has reached a certain volume limit in a specified time. Below is a table with columns: Channel, Value, Scale, Period, and On Notification. The table is empty with '(no triggers defined)'. An 'Add Volume Trigger' button is below.
- Threshold Trigger(s)**: Threshold Triggers are flexible means of sending out notifications when certain values are measured by a sensor. Below is a table with columns: Channel, Condition, Value, Latency (sec.), On Notification, and Off Notification. The table is empty with '(no triggers defined)'. An 'Add Threshold Trigger' button is below.

At the bottom of the window, there are 'Save' and 'Cancel' buttons.

You can add as many triggers of each type as desired (e.g. one trigger for "DOWN" events and another one for "UNUSUAL" events). This even includes several triggers for one single sensor channel (e.g. you can create a

bunch of Threshold Triggers for several different thresholds of one sensor channel). Click on Add Trigger, fill out the edit fields and click on Save.

State Trigger(s)

When editing state triggers you will see the following settings:

- Condition: Select the condition under which a notification is triggered (e.g. Down, Warning, Unusual).
- Latency: Latency is used to defer a notification for a specified time, e.g. to give a server or service the chance to recover from failure or to avoid being spammed with notifications just because a data line was offline for three seconds. For example, if you set the latency for a trigger to 60 seconds, the notification will only be sent if the failure situation remains active for 61 seconds.
- On Notification: This notification will be sent when the trigger becomes active (e.g. a sensor goes down for a state trigger with condition "Down").
- Off Notification: This notification will be sent when the trigger becomes inactive (e.g. a sensor goes up for a state trigger with condition "Down").

State Trigger(s) Escalation Notifications

If an error situation remains unsolved for some time, it is a good idea to send additional notifications (e.g. with a more aggressive recipient list) called Escalation Notifications. You can set the latency time to control when escalations are sent and you can also choose to repeat escalation mails every X minutes.

- Esc. Latency: This is the latency time after which escalation notifications will be sent.
- Esc. Notification: The notification that will be sent.
- Repeat Every: If this value is unequal to zero the notification will be re-sent at the specified interval.

Speed Trigger(s)

When editing speed triggers you will see the following settings:

- Channel: Select a channel which is used to compare the given values with (e.g. Primary, Sum, Traffic In, Traffic Out).
- Condition: Select the condition under which a notification is triggered (e.g. Above, Below, Equal, Not Equal).
- Value: The value you want to compare with.
- Scale: The scale for the value entered.
- Time: The time after which the counter is reset (e.g. second, minute, hour, day). Together with "Scale", you can enter notations like "bit per second" or "MByte per day" etc.
- Latency: Latency is used to defer a notification for a specified time, e.g. to give a server or service the chance to recover from failure or to avoid being spammed with notifications just because a data line was low for three seconds. For example, if you set the latency for a trigger to 60 seconds, the notification will only be sent if the failure situation remains active for 61 seconds.
- On Notification: This notification will be sent when the trigger becomes active (e.g. a sensor goes over a specified speed with condition "Above").
- Off Notification: This notification will be sent when the trigger becomes inactive (e.g. a sensor goes back below a specified speed with condition "Above").

Volume Trigger(s)

When editing volume triggers you will see the following settings:

- Channel: Select a channel which is used to compare the given values with (e.g. Primary, Sum, Traffic In, Traffic Out).

- Value: The value you want to compare with.
- Scale: The scale for the value entered.
- Period: The time after which the counter is reset (e.g. Hour, Day, Week, Month). Together with "Scale", you can enter notations like "KByte per Hour" or "GByte per Month" etc.
- On Notification: This notification will be sent when the trigger becomes active (e.g. a sensor goes above a specified volume).

Threshold Trigger(s)

When editing threshold triggers you will see the following settings:

- Channel: Select a channel which is used to compare the given values with (e.g. Primary, Sum).
- Condition: Select the condition under which a notification is triggered (e.g. Above, Below, Equal, Not Equal).
- Value: The value you want to compare with.
- Latency: Latency is used to defer a notification for a specified time, e.g. to give a server or service the chance to recover from failure or to avoid being spammed with notifications just because a data line was low for three seconds. For example, if you set the latency for a trigger to 60 seconds, the notification will only be sent if the failure situation remains active for 61 seconds.
- On Notification: This notification will be sent when the trigger becomes active (e.g. a sensor goes over a specified threshold with condition "Above").
- Off Notification: This notification will be sent when the trigger becomes inactive (e.g. a sensor goes below a specified threshold with condition "Above").

Change Trigger(s)

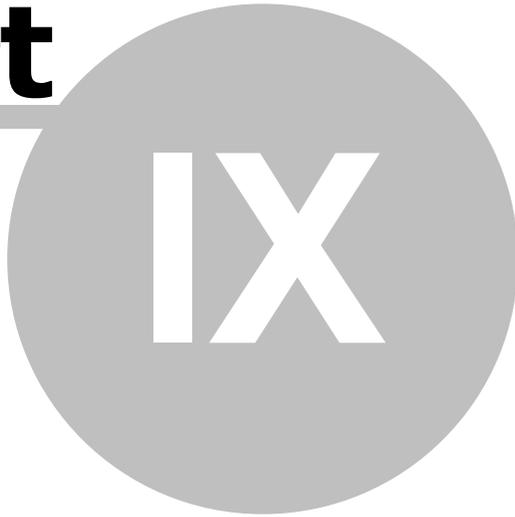
When editing change triggers you will see the following settings:

- Notification: Only the notification can be selected here. Change triggers are triggered by some sensors themselves.

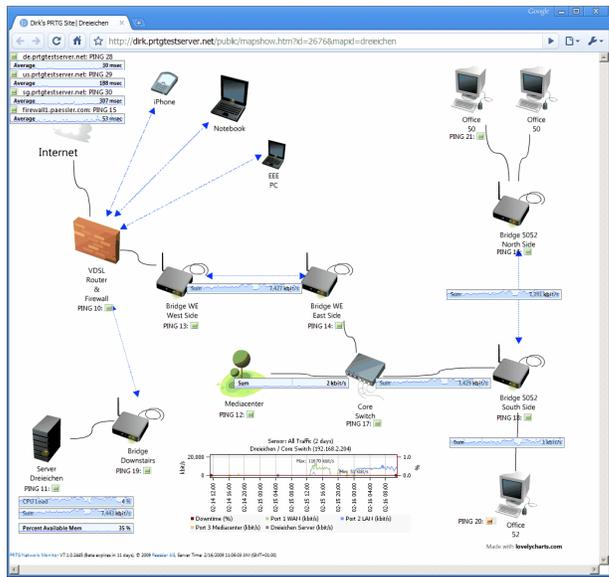
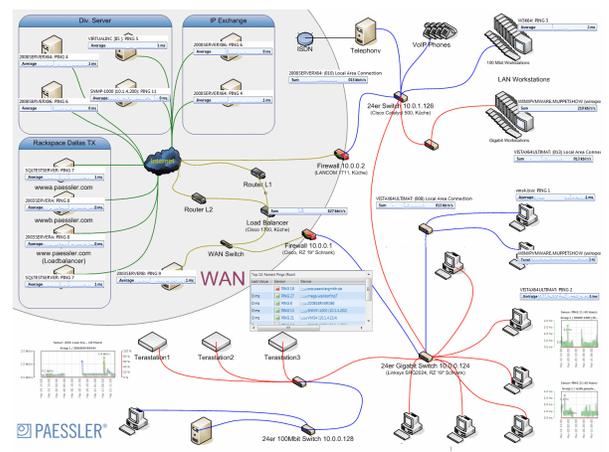
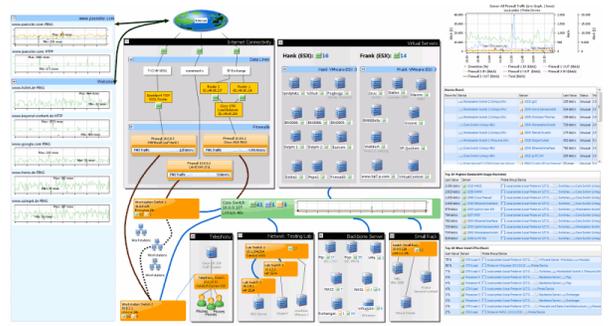
More

- Section "Notification Delivery Settings" in [System Administration - Edit System Setup](#)
- [Account Settings - Edit Notifications](#)
- Paessler Knowledge Base: PRTG 7 Placeholder Overview
http://www.paessler.com/support/kb/prtg7/placeholder_overview/

Part



Maps



Step 1: Create a New Map

To get started select "Maps | Add Map" from the main menu:

Add **Map** (Step 1 of 2)

Map Name	
Map Name	Map 6 ! Choose a new name of your choice to describe the Map

Map Layout	
Map Width	800 ! Please specify the width of the map in pixels.
Map Height	600 ! Please specify the height of the map in pixels.
Background-Image (optional)	<input type="button" value="Choose File"/> No file chosen Choose a file to be used as background for your map. This can be a .JPG, .PNG or .GIF image (filesize must be below 2 MB)

Public Access	
<input checked="" type="radio"/> No Public Access	This map will not be accessible without a login You can choose between two options: Only allow users that are logged into PRTG to view the map or allow any user to access the map, if he knows the correct URL.
<input type="radio"/> Allow Public Access	This map will be viewable without a login if the user enters the correct URL

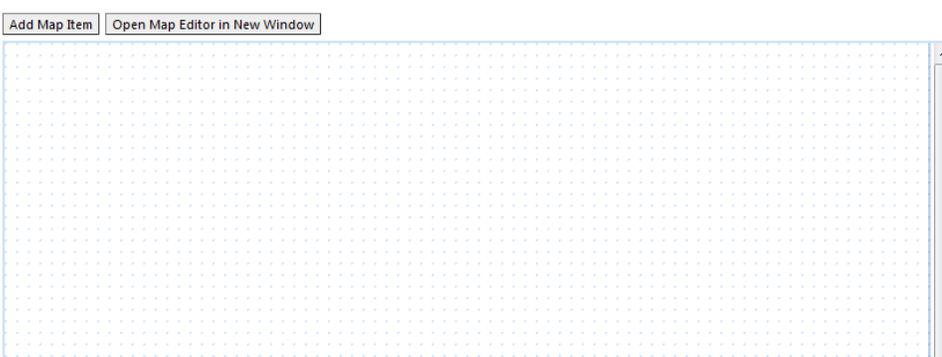
Fill out the fields and optionally select a map background image. Enable "Allow Public Access" if you want users without a PRTG user account to be able to view the map. Click "Continue to Step 2" and you will be taken to the new map.

Step 2: Add Items to the Map

Click on the "Map Editor" tab to enable the Map Editor:

Map **Map 1** Map Editor | Edit | Delete | Refresh | Menu

Home > Maps > Edit Map



To add an item to the map click on the button "Add Map Item":

Add Item(s) to Map

Choose one or more groups, devices or sensors from the device tree on the left and select a map item template from the template list on the right. You can optionally specify the size in pixels and add your own HTML code before and after the map element, too. PRTG will try to arrange the objects on the map automatically.

There are over 50 different map item templates available, the basic types are:

<p>Status Icons and Minigraphs</p>	
<p>Graphs</p>	

Sensor: Packet Sniffer 1 (2 days)
Local probe / Probe Device

Legend:

- Downtime (%)
- WWW (Ibit/s)
- Chat (Ibit/s)
- Various (Ibit/s)
- Sum (Ibit/s)
- FTP/P2P (Ibit/s)
- Infrastructure (Ibit/s)
- Other (Ibit/s)
- Mail (Ibit/s)
- NetBIOS (Ibit/s)

Group: Root (2 days)
System

Tables

Sensors (48-port Switch 1)						
Probe Group Device	Sensor	Status	Message	Last Value	Graph	
PRTG (Local Probe on 127.0.0.1) .. Group 1b 48-port Switch 1	PING 2	Up	OK	16 msec	Average	16 msec
PRTG (Local Probe on 127.0.0.1) .. Group 1b 48-port Switch 1	HTTP 1	Up	OK	847 msec	Loading time	764 msec
PRTG (Local Probe on 127.0.0.1) .. Group 1b 48-port Switch 1	(001) to SW2	Up	OK	817 kbit/s	Sum	817 kbit/s
PRTG (Local Probe on 127.0.0.1) .. Group 1b 48-port Switch 1	(002) tp PC SW	Up	OK	471 kbit/s	Sum	471 kbit/s
PRTG (Local Probe on 127.0.0.1) .. Group 1b 48-port Switch 1	(004) Ethernet Interface	Up	OK	970 kbit/s	Sum	970 kbit/s
PRTG (Local Probe on 127.0.0.1) .. Group 1b 48-port Switch 1	(005) Ethernet Interface	Up	OK	9 kbit/s	Sum	9 kbit/s
PRTG (Local Probe on 127.0.0.1) .. Group 1b 48-port Switch 1	(010) Service POP	Up	OK	5 kbit/s	Sum	5 kbit/s

Top 10: Highest Bandwidth Usage (PRTG Monitoring Station)		
Last Value	Sensor	Probe Group Device
78,426 kbit/s	(053) Uplink to SW2	PRTG Monitoring Station (Local Pr... .. Group 1b 48-port Switch 1
78,055 kbit/s	(025) to sw2	PRTG Monitoring Station (Local Pr... .. Group 1b 48-port Switch 1
77,485 kbit/s	(015) NAS1	PRTG Monitoring Station (Local Pr... .. Group 1b 48-port Switch 1
2,644 kbit/s	NIC 1	PRTG Monitoring Station (Local Pr... .. Group 2 NAS 1
2,544 kbit/s	NIC 3	PRTG Monitoring Station (Local Pr... .. Group 2 NAS 1
1,594 kbit/s	(054) WorkstationSwitch	PRTG Monitoring Station (Local Pr... .. Group 1b 48-port Switch 1
1,179 kbit/s	(004) Ethernet Interface	PRTG Monitoring Station (Local Pr... .. Group 1b 48-port Switch 1
1,088 kbit/s	(026) to PC SW	PRTG Monitoring Station (Local Pr... .. Group 1b 48-port Switch 1
1,038 kbit/s	(039) NAS2	PRTG Monitoring Station (Local Pr... .. Group 1b 48-port Switch 1
1,028 kbit/s	(028) LAN1	PRTG Monitoring Station (Local Pr... .. Group 1b 48-port Switch 1

Packet Sniffer 1		
Channel	Last Value (volume)	Last Value (speed)
Chat	0 KByte	0 kbit/s
FTP/P2P	1 KByte	0,08 kbit/s
Infrastructure	5 KByte	1 kbit/s
Mail	3 KByte	0,41 kbit/s
NetBIOS	15 KByte	2 kbit/s
Other	21 KByte	3 kbit/s
Remote Control	478 KByte	65 kbit/s
Sum	3,683 KByte	503 kbit/s
Various	2,506 KByte	342 kbit/s
WWW	654 KByte	89 kbit/s

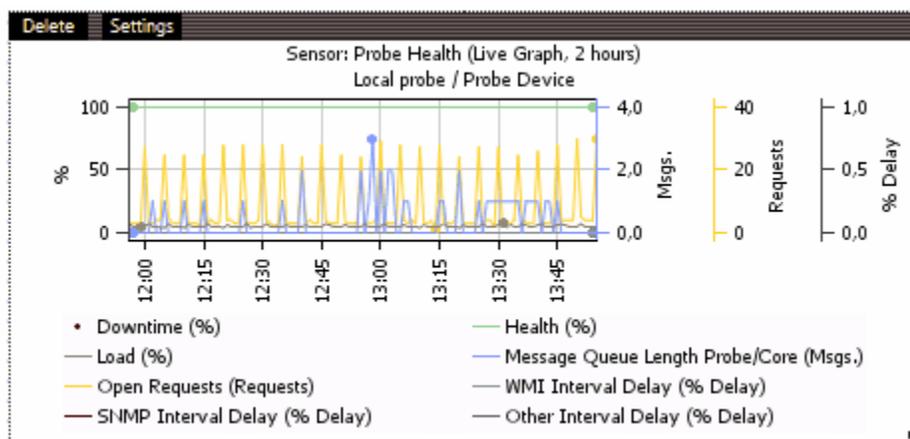
Tree Views

PRTG Monitoring Station

- Probe Device
 - Group 1
 - Group 1a
 - Web Server 1
 - PING 4: 2 msec
 - HTTP 2: 61 msec
 - IIS Files Sent: 0.13 Files/s
 - CPU Load 2: 3 %
 - Disk Free 2: 65 %
 - Memory 2: 42 %
 - HTTP 3: 111 msec
 - Mail Server 1
 - PING 1: 2 msec
 - Messages in c: 112 #
 - Queue Size 1: 1 MByte
 - CPU Load 1: 2 %
 - Disk Free 1: 64 %
 - Memory 1: 41 %
 - Pagefile Usag: 0 %
 - IMAP 1: 2 msec
 - POP3 1: 2 msec
 - SMTP 1: 3 msec
 - Group 1b
 - 48-port Switch 1
 - 30 Sensors
 - Firewall 1
 - PING 3: 2 msec
 - Web Interface: 452 msec
 - Port 1: 37 kbit/s
 - Port 2: 155 kbit/s
 - Port 3: 170 kbit/s
 - Port 4: 155 kbit/s
 - Group 2
 - NAS 1
 - Linux Server
 - ESX Server 1
 - VoIP Server
 - UPS

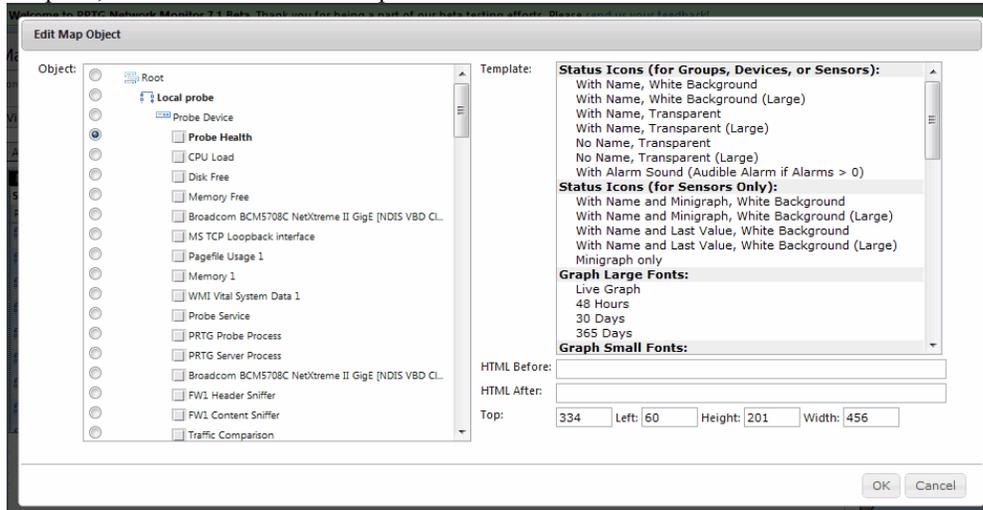
Step 3: Move and Edit Map Items

As soon as you have added an item to the map you can modify it as follows:



- Move the item by clicking and dragging the black "grip bar" at the top. If you move an item outside the map area, the Map Editor will move it back in automatically. Remark: If you click on an object's name instead of the black "grip bar" (e.g. the name of an IP sensor), you will leave the Map Editor and enter the object's details page.

- Resize the item by dragging the small arrow at the bottom right corner.
- Delete the item by clicking the "Delete" link in the black "grip bar" at the top.
- Edit item settings by clicking the "Settings" link in the black "grip bar" at the top: A dialog will appear, similar to the one you already saw while adding a new map item. You can then change the associated monitoring item, template, the HTML as well as the position and size:



Please note that you **cannot** do the following in the Map Editor:

- You cannot draw any lines between items or put any additional pictures or graphics except for a background image.
- You cannot insert customized icons from outside PRTG.

However, if you want to create a scheme that shows the devices of your network and how they are connected to each other or if you want a world map, please use your own images and insert them as background image for your map. As second step, you can then spread the map items across your image as described above.

Step 4: Edit Map Settings

Click on the "Settings" tab to edit the general settings of a map. You can edit the following settings:

- Map Name: Enter the name of the map.
- Timezone: Select the timezone for a user who views the map via the public URL.
- Tag Filter: You can enter one or more "Tag Filters" (separated by spaces). If filters are entered here, only sensors carrying one of the tags (themselves or inherited) will appear in the table map views, and others will be hidden. This filter takes effect immediately after saving the settings and has only effect on table view elements (not on status icons, graphs, or tree views).
- Map Width/Height: Enter the size of the map in pixels.
- Background Picture: If you want to use your own background picture, click "On" and select a picture from your hard disk drive.
- User Group Access: Select which rights each user group has for this map (None, Read Only, Write, Full).
- Public Access: Here you can allow or disallow the public access to your map.
- Map ID: If public access is allowed, this string will be used to create the URL for this map. A proper ID is generated automatically and can be changed if necessary. As the ID works similar to a public password, it's a good idea to keep it hard to guess.

To enter any comments for your map (visible within PRTG only), please click on the tab "Comments", write down your notes and click "Save".

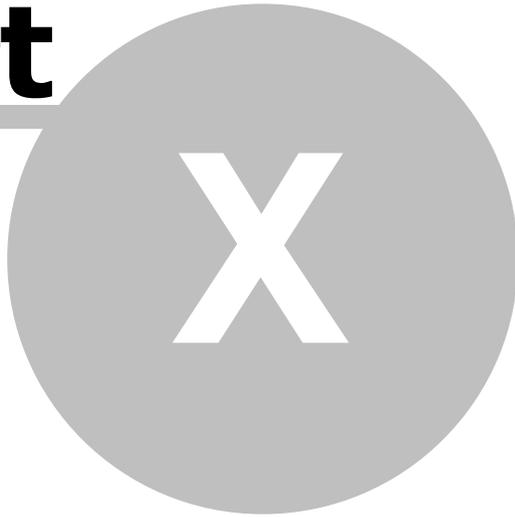
Step 5: View a Map and Share a Map

Click on the tab "View Map" to look at the final layout. To use the map outside of PRTG you have to two options:

- Option 1: Link directly to a web page with the map.
- Option 2: Show a map inside other webpages using an IFRAME.

Click on the tab "Get HTML" in order to discern the necessary URLs and HTML codes as well as additional instructions. Please note that further changes in your firewall settings may be necessary if you want the map to be accessible from the outside world.

Part



Reports

10 Reports

Reports are used to analyze historic monitoring results over a specified time such as one or more days, one month, or one year.

PRTG includes a powerful reporting engine for ad-hoc, as well as scheduled report generation in PDF format. Reports can be run on-demand or can be run on a regular basis (e.g. once a day). A report can be created for one or more sensors. 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.

Here is a sample report page for one sensor: You can see two graphs (one for the current month and one for the sensors history over the last 365 days) plus a data table with the numerical results:

PAESSLER
PRTG Network Monitor

Sample Report: IPX Leitung (ASA WAN Interface)

Report Time Span:	15.09.2008 00:00:00 - 22.09.2008 00:00:00				
Sensor Type:	SNMP Traffic (60s Interval)				
Probe, Group, Device:	Local probe > BSX Firewalls and DSL Infrastructure > firewall1.hp7 (Firewall 1 (Cisco ASA 5510)) [Cisco IOS Cisco Switch]				
Average:	464 kbit/s				
Uptime Stats:	Up:	100 %	[6d23h41m21s]	Down:	0 % [0s]
Request Stats:	Good:	100 %	[1,2820]	Failed:	0 % [0]

IPX Leitung (ASA WAN Interface)

firewall1.hp7 (Firewall 1 (Cisco ASA 5510)) [Cisco IOS Cisco Switch]

■ Traffic in (lbit/s) ■ Traffic out (lbit/s)

IPX Leitung (ASA WAN Interface)

firewall1.hp7 (Firewall 1 (Cisco ASA 5510)) [Cisco IOS Cisco Switch]

Date Time	Traffic in (Volume)	Traffic in (Speed)	Traffic out (Volume)	Traffic out (Speed)	Coverage
21.09.2008	2.993.862 KByte	284 kbit/s	899.783 KByte	85 kbit/s	100 %
20.09.2008	2.716.966 KByte	258 kbit/s	770.235 KByte	73 kbit/s	100 %
19.09.2008	3.719.085 KByte	353 kbit/s	1.868.967 KByte	178 kbit/s	100 %
18.09.2008	3.450.011 KByte	327 kbit/s	1.122.424 KByte	106 kbit/s	100 %
17.09.2008	4.314.449 KByte	409 kbit/s	1.122.875 KByte	106 kbit/s	100 %
16.09.2008	3.927.667 KByte	374 kbit/s	1.205.807 KByte	115 kbit/s	100 %
15.09.2008	4.392.578 KByte	418 kbit/s	1.674.498 KByte	159 kbit/s	100 %
Sums (of 7 values)	25.514.618 KByte		8.664.589 KByte		
Averages (of 7 values)	3.644.945 KByte	346 kbit/s	1.237.798 KByte	118 kbit/s	100 %

Creating reports involves 3 steps:

Step 1: Setting up a Report

Select choose "Reports | Add Report" from the main menu to get started:

Add Report

Home > Reports > (new object)

Basic Report Settings

Report Name	<input type="text" value="Report"/>	Please choose a descriptive name
Template	<please select a file>	Please choose a report template from the list of available templates. There are templates that offer optional data tables to the graphs. You also specify the graph/calculation intervals by selecting a template. Note: You can edit the HTML templates in the "website/reporttemplates" subfolder of your PRTG Installation.
Timezone	(GMT+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien	Timezone setting for all dates regarding this report. This includes schedule dates, report timespan and dates in tables/graphs
Paper size	Letter	Please specify the paper size for which the report shall be formatted.
Orientation	Landscape	Please specify the paper orientation for which the report shall be formatted.

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	When selecting sensors manually you can also select/deselect individual channels of each sensor.
Add Sensors by Tag	<input type="text"/>	Enter tags to add all sensors from the sensor tree to the report which have one of the tags. Tip: Tags are inherited from parent objects, i.e. if you enter a specific tag into a group's tag setting and into this report setting, all sensors of that group will be included in the report - additionally to the sensors selected manually. Use spaces to separate the filter tags.

Schedule ("When will this report be run?")

Report Schedule	<input checked="" type="radio"/> No schedule (Run interactive/on-demand only) <input type="radio"/> Every Full Hour <input type="radio"/> Every day at a specific hour <input type="radio"/> Every specific day of a week <input type="radio"/> Every specific day of a month <input type="radio"/> Every specific date	You can create reports just for manual "on-demand use" or automatically every hour, day, day of week, day of month or a specific date. If you choose scheduled processing you will receive a ToDo email everytime the report is run.
Scheduled Processing	<input type="radio"/> Save report to disk and send it by email <input checked="" type="radio"/> Save report to disk only <input type="radio"/> Send report by email only	When PRTG runs this report due to a schedule it can simply email the report to an email address or write the PDF file to the disk or both.

Period ("What time span will the report cover?")

Reported Period	<input type="radio"/> Current <input checked="" type="radio"/> Previous	Specify which period is to be reported. Please choose between daily, weekly, monthly or yearly reports. Examples: Current is "today" for daily reports, "current month" for monthly reports. Previous means "yesterday" for daily reports, "last month" for monthly reports.
Report Period Type	<input type="radio"/> Day <input checked="" type="radio"/> Week <input type="radio"/> Month <input type="radio"/> Year	
Week Period	Monday-Sunday	

Click on "Save" when you are done with the settings. Please see "Editing Report Settings" further down for more detailed information.

Step 2: Select Sensors Manually

In the "Select Manuals Manually" tab, you can then edit the list of probes, groups, devices, sensors and channels which are included in the report. Adding a probe, group or device will include all associated sensors (and their channels), too.

Run Now | Stored Reports | Settings | **Select Sensors Manually** | Sensors Selected by Tag | Comments

Probe Group Device	Object	Sensor Channel Selection	Actions
Root	Root		Delete
Local Probe on 127.0.0.1 (127.0.0...)	Memory Free	<input checked="" type="checkbox"/> Percent Av <input checked="" type="checkbox"/> Available M <input checked="" type="checkbox"/> Downtime	Delete
Local Probe on 127.0.0.1 (127.0.0...)	Broadcom BCM5708C NetXtreme II Gi...	<input checked="" type="checkbox"/> Traffic in <input checked="" type="checkbox"/> Traffic out <input checked="" type="checkbox"/> Packets <input checked="" type="checkbox"/> Sum <input checked="" type="checkbox"/> Downtime	Delete
Local Probe on 127.0.0.1 (127.0.0...)	MS TCP Loopback interface	<input checked="" type="checkbox"/> Traffic in <input checked="" type="checkbox"/> Traffic out <input checked="" type="checkbox"/> Packets <input checked="" type="checkbox"/> Sum <input checked="" type="checkbox"/> Downtime	Delete
Local Probe on 127.0.0.1 (127.0.0...)	Pagefile Usage 1	<input checked="" type="checkbox"/> Total <input checked="" type="checkbox"/> Downtime	Delete
Local Probe on 127.0.0.1 (127.0.0...)	Memory 1	<input checked="" type="checkbox"/> Percent Av <input checked="" type="checkbox"/> Available M <input checked="" type="checkbox"/> Downtime	Delete
Local Probe on 127.0.0.1 (127.0.0...)	Probe Service	<input checked="" type="checkbox"/> Running <input checked="" type="checkbox"/> Downtime	Delete
Local Probe on 127.0.0.1 (127.0.0...)	PRTG Probe Process	<input checked="" type="checkbox"/> Working S <input checked="" type="checkbox"/> Commit Siz <input checked="" type="checkbox"/> Processor: <input checked="" type="checkbox"/> Downtime	Delete
Local Probe on 127.0.0.1 (127.0.0...)	PRTG Server Process	<input checked="" type="checkbox"/> Working S <input checked="" type="checkbox"/> Commit Siz <input checked="" type="checkbox"/> Processor: <input checked="" type="checkbox"/> Downtime	Delete
Local Probe on 127.0.0.1 (127.0.0...)	Header Packet ASA	<input checked="" type="checkbox"/> Andere <input checked="" type="checkbox"/> WWW <input checked="" type="checkbox"/> FTP/P2P <input checked="" type="checkbox"/> Mail <input checked="" type="checkbox"/> Chat <input checked="" type="checkbox"/> Remote Co <input checked="" type="checkbox"/> Infrastruct <input checked="" type="checkbox"/> NetBIOS <input checked="" type="checkbox"/> Various <input checked="" type="checkbox"/> Summe	Delete

Add Sensors Manually

1 to 20 of 364

Probe Group Device	Object	Actions
Local Probe on 127.0.0.1 (127.0.0...)	Probe Device	Add
Local Probe on 127.0.0.1 (127.0.0...)	Probe Health	Add
Local Probe on 127.0.0.1 (127.0.0...)	CPU Load	Add
Local Probe on 127.0.0.1 (127.0.0...)	Disk Free	Add
Local Probe on 127.0.0.1 (127.0.0...)	Memory Free	Add
Local Probe on 127.0.0.1 (127.0.0...)	Broadcom BCM5708C NetXtreme II Gi...	Add
Local Probe on 127.0.0.1 (127.0.0...)	MS TCP Loopback interface	Add
Local Probe on 127.0.0.1 (127.0.0...)	Pagefile Usage 1	Add
Local Probe on 127.0.0.1 (127.0.0...)	Memory 1	Add
Local Probe on 127.0.0.1 (127.0.0...)	WMI Vital System Data 1	Add
Local Probe on 127.0.0.1 (127.0.0...)	Probe Service	Add

You can enable/disable individual channels of a sensor using the checkboxes. Use the "Delete" links in the "Actions" column to remove an object from the report. To add more objects to a report choose one from the list of all objects in the lower half and click the "Add" link. To find a specific object either use the paging function of the table or enter a search term in the search box and click "Search". All changes to the sensor list are saved automatically and immediately.

Step 3: Run the Report

Click on the "Run Now" tab to create a report immediately:

Run Now | Stored Reports | Settings | **Select Sensors Manually** | Sensors Selected by Tag | Comments

Run Report "Bericht" for

Current Period This week (16/02/2009 - 22/02/2009) Choose a period to run the report for
 Previous Period Last week (09/02/2009 - 15/02/2009)
 Quick Select 16/02/2009 - 22/02/2009
 Manual Select
 Start Date: 2009-02-16
 End Date: 2009-02-22

Processing Options

View Report as HTML Choose a target file format for this report
 Create and store PDF file (You will receive a ToDo when report has been created)
 Create PDF file, store it and send by email

Run Report

Select the desired settings and click on "Run Report".

- HTML Reports will be shown immediately.
- PDF reports will be created in the background and you will receive an email with a ToDo when the report is finished.

In the Report Settings, you can also set an automatic schedule to run the report on a regular basis.

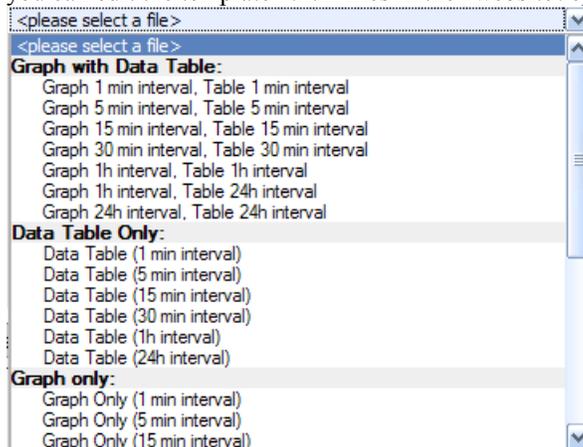
Step 4: Accessing Historic Reports

On the "Stored Reports" tab you can access former reports that are stored on the disk.

Editing Report Settings

In the "Settings" tab, you can configure the following settings for the current report:

- Report Name: Please choose a descriptive name.
- Template: You can choose from the list of available templates. There are templates that offer graphs, data tables, or both and there are "Top x" reports. You also specify the graph/calculation intervals by selecting a template. Note: In this PRTG version, we do not officially support customizing report templates. However, you can edit the template *.htm files in the "website\reporttemplates" subfolder of your PRTG Installation.



- Timezone/Paper size/Orientation: Please select the appropriate settings for your needs.
- Add Sensors Manually: If you want to add or remove sensors for this report manually, please use the "Select Sensors Manually" tab. You will find the according options there. See "Step 2: Select Sensors Manually" above.
- Add Sensors by Tag: Enter one or more tags. Every sensor from the sensor tree which has one of the tags will then be added to the report. Note: The concept of inheritance also works with tags (see section [Inheritance of Settings](#)).
- Filter Sensors by Tag: Use this field to further filter all sensors added to this report (either manually or by the "Add Sensors by Tag" option). Enter one or more tags and only sensors with one of these tags will be visible in the report. Works best if used in combination with a manual selection of probes, groups or devices.
- Report Schedule: You can choose between no schedule and several different schedules. This report will be run automatically on the scheduled dates. According to your settings, you will be asked to additionally specify an hour, a day, or date. If you choose automatic processing you will receive a new message in your "ToDos" every time the report is run.
- Scheduled Processing: Select what should be done when an automatic report is run. Options are: Save report to disk, email it, or both.
- Reported Period/Report Period Type/... Period: Please select if you want a report with data of the current or previous day, week, month or year. According to your settings, you will be asked to select a day, week, month

or year period, too.

- Report only for specific hours-of-day (Schedule): You can select a schedule to narrow the monitor data for the report. Only sensor data monitored during the specified time will be used then. Please note: The items in the drop down selection are inserted by the central Schedules engine. To change these settings or to add a new schedule, please select "Setup | Schedules" from main menu (see section [Account Settings - Edit Schedules](#) for more details).
- Show Percentile: For some report templates, you can activate a percentile calculation here for each sensor channel. See section [Calculating Percentiles](#) for more details.
- Report Comments: You can enter a customized introduction and footer comments which will be added at the beginning and the end of your report.
- Access Rights: For each User Group, you can specify access rights for this report. Options are "None", "Read", "Write" and "Full".

Remarks

To get a quick and easy report of one single sensor, its best to use the "Historic Data" report function. See section "Reviewing Historic Data" in chapter [Web Interface](#).

More

If you want to further adapt the look of your reports, you can change report templates. Please refer to the Paessler Knowledge Base article "HowTo Change Report Templates" at http://www.paessler.com/support/kb/prtg7/prtg_change_report_templates

Part



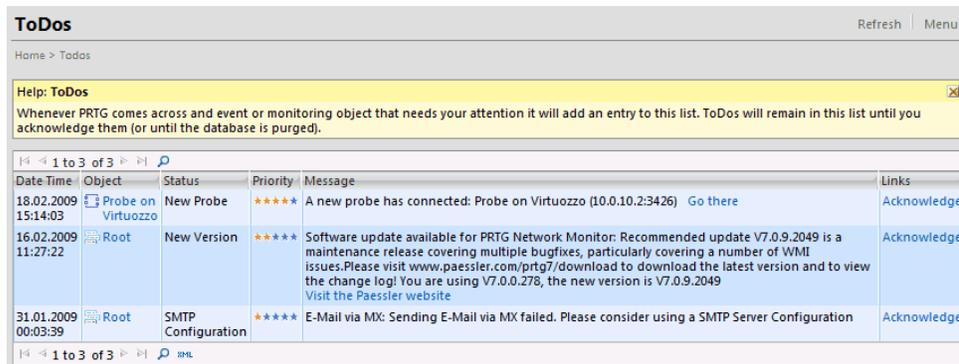
XI

ToDoS

11 ToDos

ToDos ("to do" tasks) are PRTG's way to hand over tasks to you as the administrator, when an event occurs that PRTG cannot handle without your attention.

Click on "ToDos" in the main menu to see a list of all ToDos:



Date Time	Object	Status	Priority	Message	Links
18.02.2009 15:14:03	Probe on Virtuozzo	New Probe	*****	A new probe has connected: Probe on Virtuozzo (10.0.10.2:3426) Go there	Acknowledge
16.02.2009 11:27:22	Root	New Version	*****	Software update available for PRTG Network Monitor: Recommended update V7.0.9.2049 is a maintenance release covering multiple bugfixes, particularly covering a number of WMI issues. Please visit www.paessler.com/prtg7/download to download the latest version and to view the change log! You are using V7.0.0.278, the new version is V7.0.9.2049 Visit the Paessler website	Acknowledge
31.01.2009 00:03:39	Root	SMTP Configuration	*****	E-Mail via MX: Sending E-Mail via MX failed. Please consider using a SMTP Server Configuration	Acknowledge

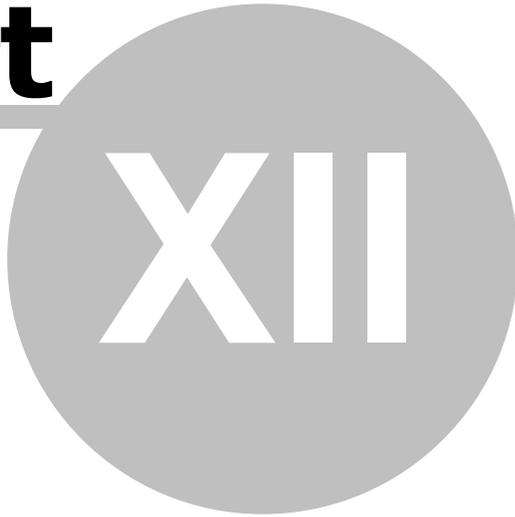
You will see a new ToDo whenever any of the following situations arise:

- The auto discovery has discovered a new device and has created new sensors and you should acknowledge them.
- A probe which had never connected before has connected and this new probe must be acknowledged by the administrator.
- PRTG's built-in check for new versions has found a new version of the software available from Paessler.
- A PDF report has been created and is now ready for review.
- A critical situation has shown up on the server system (e.g. system runs out of disk space, licensing issues, etc.).

Whenever a new ToDo is created by PRTG, the administrator user will receive an email asking to take care of the issue. You can disable this automatic email in the system settings (see section [System Administration - Edit System Setup](#)). ToDos remain in the list until they are acknowledged (by clicking on "Acknowledge").

Note: You can acknowledge all ToDos at once by choosing the corresponding item from the "ToDos" menu in the main menu bar.

Part



User Management

12 User Management

In PRTG, you can control the access rights for every user with a smart User Management.

Overview

The default administrator can use the PRTG installation as the only user or can create an unlimited number of users. Users are organized using an unlimited number of groups (which also control their security settings).

There are three types of users:

- Administrator Users: Only members of the "PRTG Administrators" group can create and edit user accounts and they can see and edit all monitoring objects and system settings.
- Read/Write Users: These users can see all menus and links needed to edit the monitoring configuration (regardless of whether they are allowed to change it).
- Read Only Users: These users will not see any editing links or menus and thus will not be able to edit anything in the configuration.

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 he sees 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 probe, group, device, sensor, and other objects.

Managing Users and Access Rights

To manage users and access rights, there are basically three steps to follow:

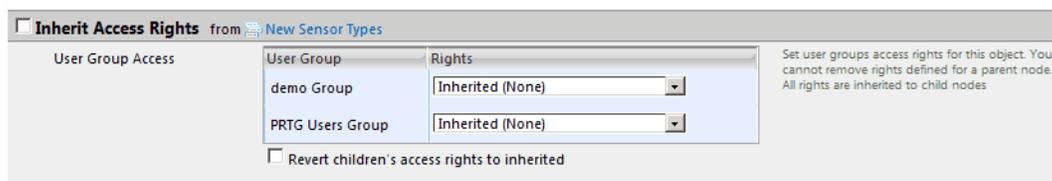
1. Create new users and set the user account's rights.
2. Create user groups and define users as members of this group.
3. For each object in your device tree, define access rights (inheritance applies; see section [Inheritance of Settings](#)).

Create New Users and Groups

Step 1 and 2 are done in the System Administration Settings. See section [System Administration - Edit User Accounts and User Groups](#) for more details.

Controlling User Rights

Step 3: Throughout the web interface of PRTG you can control access to the monitoring objects (e.g. groups, devices, sensors, maps, reports, etc.) using the following settings in the according object's setting page:



User Group Access	Rights
demo Group	Inherited (None)
PRTG Users Group	Inherited (None)

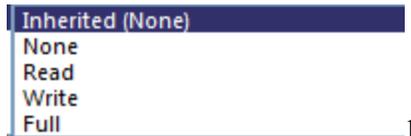
Revert children's access rights to inherited

Set user groups access rights for this object. You cannot remove rights defined for a parent node. All rights are inherited to child nodes.

For sensor tree objects the default setting is "Inherit Access Rights", which means that a user has the same

access rights to all child objects if one has access to the object itself (see section [Inheritance of Settings](#)).

This can be overridden by disabling the checkbox in front of "Inherit Access Rights" and setting the "User Group Access" options. You can specify the access rights to the current object for each user group by choosing an option from the drop down list:



The options are:

- Inherited: Uses the setting of the parent object
- None: User cannot see or edit the object. The object does not show up in lists and in the sensor tree - unless a child object is visible to the user, then the object is visible in the sensor tree, though not accessible.
- Read: User can see the object and review its monitoring status.
- Write: User can see the object, review its monitoring status and edit the object's settings - except for group access settings.
- Full: Same as "Write", but the User can additionally control the group access settings.

A user can only add and delete objects if the user has "Write" or "Full" access to the parent object.

You will see an additional checkbox for groups and devices, "Revert children's access rights to inherited". If you select this box, the access right of all child objects will be reset to "inherited" which actually deletes all individual right settings for the underlying objects. This is the quick way to reset all access rights and should be used with caution.

Part



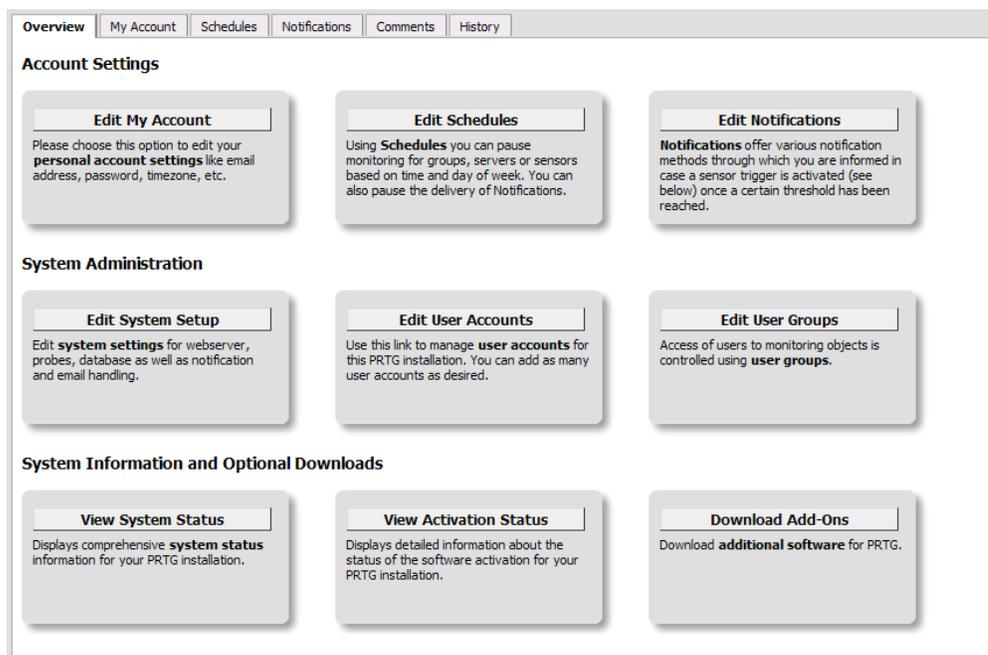
System Settings and Administration

13 System Settings and Administration

Basically, you can make settings at two different locations: In the web interface and in the Windows administrator programs.

The settings for your account, the system settings and most of the system administration settings are available from the "Setup" menu in the web interface. Some settings that "dig deeper" into the system (e.g. web server IP and port, entering the license key or changing the system language) are located in the PRTG Server Administrator and PRTG Probe Administrator.

This is a screenshot of the web interface's "Setup" screen:



Please read on in the following sections.

Web interface:

- [Account Settings - Edit My Account](#)
- [Account Settings - Edit Schedules](#)
- [Account Settings - Edit Notifications](#)
- [System Administration - Edit System Setup](#)
- [System Administration - Edit User Accounts and User Groups](#)
- [System Information and Optional Downloads](#)

Administrator programs (Windows applications):

- [PRTG Server Administrator](#)
- [PRTG Probe Administrator](#)

Note: Only for a PRTG Administrator User all settings are visible. If you're logged in as another user, you may not see all options described in this manual.

13.1 Account Settings - Edit My Account

In the web interface, click on "Setup | My Account" in the main menu to open the "My Account" settings. Here you can change various settings specific to your user account:

The screenshot shows the 'My Account' settings page. It features a navigation bar with tabs: Overview, My Account, Schedules, Notifications, Comments, and History. The 'My Account' tab is selected. The page is divided into two main sections: 'User Account Settings' and 'Auto Refresh Settings'.
User Account Settings:
- Login Name: prtgadmin
- Username: PRTG System Admin
- Email Address: support@paessler.com
- Timezone: (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
- Password: Don't change (selected)
Auto Refresh Settings:
- Auto Refresh Type: Refresh Page Elements (recommended) (selected)
- Auto Refresh Interval (sec): 60
A help text on the right side of the form explains the refresh options: 'PRTG automatically refreshes the content in your browser. Here you can choose between two different refresh methods and you can specify the refresh time (30s recommended).'

This page allows to define the following information in detail:

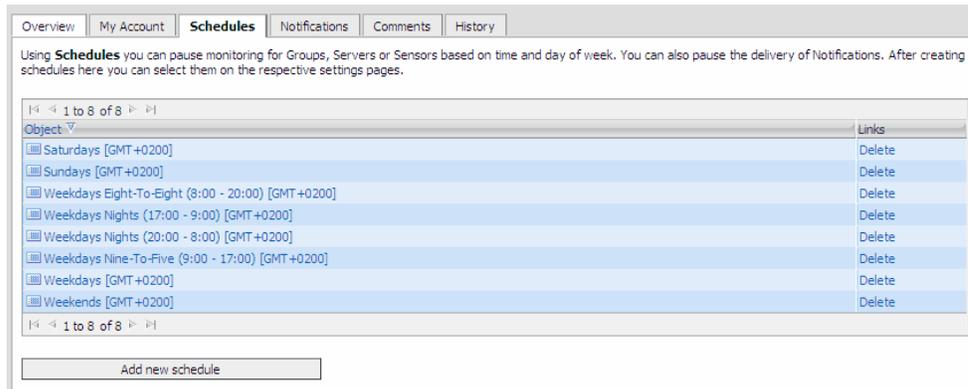
- **User Account:** These fields allow you to define the login name, the user name, the email address for the user, time zone and data format, and it allows you to set a new password. The Hash value cannot be changed and can be used for certain API calls.
- **Auto Refresh and Alerting:** Using these fields you can select whether you want the content of your browser to be refreshed automatically or not, if you want to merely refresh page elements or the entire page, and what refresh interval (in seconds) you want to use. You can also specify when Pop-up Alerts are shown or an Audible Alarm should be played.
- **Web Interface:** Here you can enter the URL which the web interface will use as homepage. As default, "/welcome.htm" is used which is the welcome page you have already seen after logging in. Also, you can set the charts display mode: Select static images for faster graph processing or Flash for increased interactivity. You can further specify a delay for Flash graphs to better support slow clients.
- **Auto-folding:** PRTG tries to keep the page size for the pages with the sensor tree small by automatically "folding" groups and devices with many items. In these fields you can define how many groups/devices or how many sensors maximum are to be shown before the specific branch is reduced (folded).
- **Account Control:** These fields allow you to define to what group(s) the user in case belongs to, among other defining the user's access rights. Non-admin users can also be set to active or inactive by selecting the respective radio button (available for the admin only).
- **User Groups:** Shows a list of all groups the user is a member of.

13.2 Account Settings - Edit Schedules

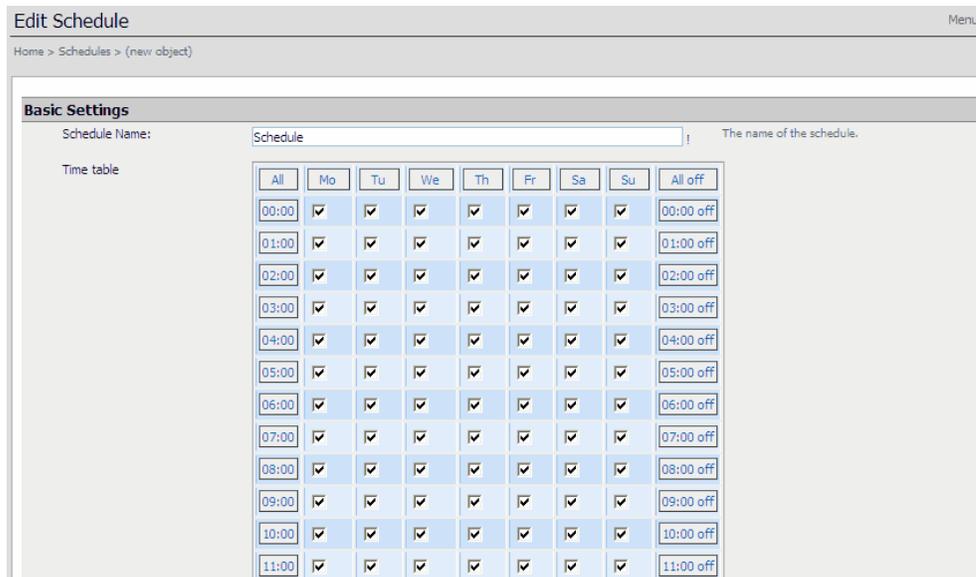
In the web interface, click on "Setup | Schedules" in the main menu to open the "Schedules" settings. Here you can define timetables that can be used later to pause monitoring for groups, servers or sensors based on time and day of week, as well as pause the delivery of notifications.

In the account settings, schedules are managed centrally. Once a schedule has been created, you can use it in the object settings (for either a probe, group, device or sensor) at the "Inherit Schedules and Dependencies" entry.

Various common schedules are available by default, further schedules can be added using the "Add new schedule" button.



By either selecting an existing schedule or when adding a new schedule, the following window appears:



Here you can provide a schedule name for identification purposes, as well as check the respective checkboxes to determine the time range of the schedule. Clicking on the daily icons at the top or at the daily "off" icons at the bottom allow to select/deselect entire daily ranges. Clicking on the hourly icons on the left, or on the hourly "off" icons on the right, allow to select/deselect entire hourly ranges.

At the very bottom of the window, you can also assign user group access rights for the selected schedule. The following rights can be assigned:

- None: This user group has no access to the schedule whatsoever. As such, this user group cannot see or edit the specific schedule.
- Read: This user group has read access to the schedule. The group can see, but not edit, the specific schedule.
- Write: This user group has read and write access to the schedule. The group can see and edit the specific schedule.
- Full: This user group has read and write access to the schedule, plus it can assign schedule access rights to other user groups.

13.3 Account Settings - Edit Notifications

Under "Notifications" you can discern an overview of all configured notifications (see [Notifications](#)).



The screenshot shows a web interface with a navigation bar at the top containing tabs for Overview, My Account, Schedules, Notifications (selected), Comments, and History. Below the navigation bar, there is a text block explaining that notifications offer various methods by which you are notified when a sensor has fired a trigger. Below this text is a table with three columns: Object, Content, and Links. The table contains one row with the value 'Mail to Admin' in the Object column and 'Delete | Test' in the Links column. Below the table is a button labeled 'Add new notification'.

Object	Content	Links
✉ Mail to Admin		Delete Test

Clicking on any particular notification will direct you to the its configuration page. You can add a new notification by clicking on the "Add new notification" button. Use the "Delete" link to remove any particular notification or use the "Test" link to test any particular notification.

The edit page looks like this:

Basic Notification Settings

Notification Name ! The name of the notification.

Status started paused

Schedule Using schedules you can pause notifications at specific days and hours throughout the week. You can edit schedules under the system settings.

Postpone No Yes "Yes" means when this notification is triggered during a scheduled pause, it will be sent after the scheduled pause ends. With "No" it will be discarded.

Access Rights

User Group Access	User Group	Rights	
	PRTG Users Group	None	<input type="text"/>
	User Group	None	<input type="text"/>

Set user group access rights for this object. You cannot remove rights defined for a parent node. All rights are inherited to child nodes.

Send Email

Add Entry to Event Log

Send Network Broadcast (NET SEND)

Send Syslog Message

Send SNMP Trap

Send ICQ Message

Send MSN Message

Send SMS/Pager Message

Execute HTTP Action

Execute Program

Play sound file (Windows XP/2003 only)

You can also assign user group access rights for the selected notification. The following rights can be assigned:

- **None:** This user group has no access to the notification whatsoever. As such, this user group cannot see or edit the specific notification.
- **Read:** This user group has read access to the notification. The group can see but not edit the specific notification.
- **Write:** This user group has read and write access to the notification. The group can see and edit the specific notification.
- **Full:** This user group has read and write access to the notification, plus it can assign notification access rights to other user groups.

First you can enter a name for the notification and you can set the user group rights (e.g. if you want to enable or

disable the use of a specific notification by some users).

Using the checkboxes you can activate various methods of notification. For each method you must enter the receiver address. Optionally, you can also change the notification texts (the available placeholders are explained on the right).

Note: For notifications with instant messengers, it is important to understand that in order to use instant messaging for notifications you always need two accounts - One account that sends the messages and another one that receives the messages.

Important: For some notification methods, you must enter the sender information in the Notification Delivery Settings (see section [System Administration - Edit System Setup](#)).

13.4 System Administration - Edit System Setup

System, Website, and Web Server Settings

Select "Setup | System Setup" in the main menu. In the "System, Website, and Web Server Settings" tab, you can define following specifics:

The screenshot shows the 'System, Website, and Web Server Settings' configuration page. It has three tabs: 'System, Website, and Web Server Settings' (selected), 'Notification Delivery Settings', and 'Probe Management'. The main content is organized into three sections:

- Site Information:**
 - Site Name: PRTG Network Monitor (XP-PRO)
 - DNS Name: [Empty field]
 - Language Selection: Please use the PRTG Server Administrator program to select the user interface language.
- Scanning Intervals:**
 - Available Intervals: 30s, 1m, 5m, 10m, 15m, 30m, 1h, 4h
 - Intervals available in the interval drop down list. Use s/m/h/d for defining seconds/minutes/hours/days and append them to a number. So 5m is means five minutes. Only add one setting per line.
- Uptime Threshold:**
 - Minimum Allowed Uptime Threshold: 99.99 %
 - This value controls the colors shown next to sensor icons in reports. If the uptime or number of good requests falls below this value, the sensor will show a red icon
- E-Mail Options:**
 - Email Footer (Text):


```
=====
This email was sent to %toaddress at %systemdatetime.
Access the web interface for "%sitename" at %home
=====
%programname %programversion %company
```

 - Text that will be appended to each plain text mail
 - Email Header (HTML):


```
<html>
<head>
<title>
```

 - HTML text that will be used as the header for each HTML mail

- **Site Information:** Here you can define a site name (used in the web interface and in the subject of emails), as well as the URL for the site (used for building links in emails). If you want to use a symbolic (DNS-) name to access PRTG's web server you must enter the name here.
- **Scanning Intervals:** Here you can define intervals which will in turn become selectable when adding objects to the installation. In order to add a new interval value merely add a numerical value followed by a time span enumerator (s/m/h/d for defining seconds/minutes/hours/days respectively).
- **Uptime Threshold:** With this option, you can define when a sensor goes to a red Down state. If you experience repeated fail alarms, you can expand the failure tolerance here.

- **Email Options:** Here you can edit the footer (for text-only mails) and HTML template that will be used for outgoing emails (placeholders allowed - more information in the "More" section below) and define whether "ToDo" emails are to be forwarded to the administrator, a specific email address or to no one at all. If "specific email" is selected, a new field appears allowing to define the email address in case.
- **Data Purging Limits:** Here you can select for how many days historic data remains accessible. Enter the number of days to retain historic data for each of the available entries.
- **Unusual Detection:** Here you can define the sensitivity of the "unusual" state detection mechanism.
- **User Login Timeout:** Specify the time after which a user is automatically logged out the web interface when idle.
- **Settings from the PRTG Server Administrator program:** These entries are "for your information" only. These entries can be edited from the PRTG Server Administrator applet under Start | PRTG program group (see [PRTG Server Administrator](#)).

Notification Delivery Settings

Select "Setup | System Setup" in the main menu. Under the "Notification Delivery Settings" tab you can define specifics relevant to notifications (see [Notifications](#)):

The screenshot shows the 'Notification Delivery Settings' configuration page. At the top, there are three tabs: 'System, Website, and Web Server Settings', 'Notification Delivery Settings' (which is active), and 'Probe Management'. Below the tabs, the 'SMTP Delivery' section is visible. It has three radio button options for the 'SMTP Delivery Mechanism': 'Automatic (uses MX records for direct delivery, recommended)' (which is selected), 'Via SMTP Relay Server (recommended inside LANs/NATs)', and 'Two SMTP Relay Servers (Primary and fallback server)'. To the right of these options is a detailed explanation. Below the mechanism options are three text input fields: 'Sender E-Mail' with the value 'support@paessler.com', 'Sender Name' with 'System Admin', and 'HELO Ident' with 'XP-PRO'. Each field has a small exclamation mark icon to its right. Below these fields are two more input fields: 'Merge notifications if more than' with the value '3' and 'Maximum number of merged notifications' with the value '50'. The 'SMS Delivery' section is partially visible at the bottom, showing two radio button options: 'Select a SMS provider from a list of providers' and 'Enter a custom URL for a provider not listed'.

Note: It is important to understand that in order to use instant messaging for notifications you always need two accounts: One account that sends the messages and another one that receives the messages.

This page allows to define the following information in detail.

- **SMTP Delivery:** Here you can define the SMTP delivery mechanism (either use PRTG's automatic relay or

define your own SMTP server or even two servers), as well as all relevant information for email forwarding. If you select to define your own SMTP server(s), you will need to provide your server's information, including the server itself (use either IP address or DNS name), the SMTP port, as well as the relay authentication type (none, standard or SASL). If you require authentication, username and password need to be provided. If you choose to set up two SMTP Relay Servers, the second server is used when the first server is not reachable (fallback server). Furthermore, it is possible to define when PRTG should start merging individual notifications, as well as provide a maximum number of notifications to be merged at any given time (this will reduce the number of mails that you will receive).

- **SMS Delivery:** Please choose whether to select a SMS provider from a list (and choose a provider) or choose to enter a custom URL (and enter a URL). If you have chosen a provider from the list, enter your gateway's access username and password (and API ID if necessary). Please note: Although PRTG has built-in APIs 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.
- **ICQ Delivery:** Provide your ICQ number ("Sender Number") and Password for the ICQ account intended to relay (not receive!) ICQ notifications.
- **Windows Live Messenger (MSN Messenger) Delivery:** Provide your MSN ID ("Sender Number") and Password for the MSN account intended to relay (not receive!) MSN notifications.

Probe Management

Select "Setup | System Setup" in the main menu. Under the "Probe Management" tab you can define specifics relevant to probes:

The screenshot shows the 'Probe Management' configuration page. At the top, there are three tabs: 'System, Website, and Web Server Settings', 'Notification Delivery Settings', and 'Probe Management'. The 'Probe Management' tab is active. Below the tabs, there are two main sections:

- Probe Connection Settings:**
 - Access keys:** E049FF3F-05B9-48B6-9791-69F4D917F718. Description: Enter a list of access keys, each of which every single probe has to use to connect to this PRTG installation.
 - Allow IPs:** any. Description: Enter all IPs that are allowed.
 - Deny IPs:** (empty). Description: Enter all IPs that are not allowed.
- Settings from the PRTG Server Administrator program:**
 - IPs for Probe Connections:** 127.0.0.1. Description: IP list of this machine where PRTG listens to incoming probe communication, using the specified Port. 0.0.0.0 means that the Server listens on all local network: adapter IPs. Notice that these settings cannot be edited in the Web GUI. They are editable in the PRTG Server Administrator program only as the service needs to be restarted for the changes to take effect.
 - Probe Connections Port:** 23560.

- **Probe Connection Settings:** Here you can define access keys, as well as allow / deny specifics IPs access to the probe(s). See [Multiple Probes and Remote Probes](#).
- **Settings from the PRTG Server Administrator program:** These entries are "for your information" only. These entries can be edited from the PRTG Server Administrator applet under Start | PRTG program group (see [PRTG Probe Administrator](#)).

More

For an overview of allowed placeholders, see our Knowledge Base article "PRTG 7 Placeholder Overview": http://www.paessler.com.stage.bsx/support/kb/prtg7/placeholder_overview/

13.5 System Administration - Edit User Accounts and User Groups

This section shows how user accounts can be managed. For a general introduction see section [User Management](#).

Note: Only for a PRTG Administrator User all settings are visible. If you're logged in as another user, you may not see all options described in this manual.

Creating New Users

For each new user the administrator user must specify a login name and an email address. New users can be created by selecting "Setup | User Accounts" from the main menu and clicking on "Add new user". Please see next section "User Account Settings" for details about the options.

Tip: If you want to control the rights of each user individually, you must create a user group for each user. This can be automated by choosing "Create new user group for this user" from the "Primary Group" drop-down when creating a new user account. This will create a new user and a new user group with the same name. In turn, you can use this user group to control the user's rights individually.

User Account Settings

Each user account has a number of settings that can be changed by the user (choose "Setup | My Account" from the web interface's main menu) or by the administrator (choose "Setup | User Accounts" from the web interface's main menu). These settings are:

- **User Account:** Enter user specific data, such as a Login Name, a Username for display purposes, Email Address, Timezone, Date Format and Password. The Hash value cannot be changed. It can be used for identification in certain API calls.
- **Auto Refresh and Alerting:** PRTG automatically refreshes the content in your browser. Here you can choose between different refresh methods, you can disable the refreshing and you can specify the refresh time (30 seconds recommended). You can also specify which Pop-up Alerts are shown and where an Audible Alarm should be played if there are alarm messages.
- **Web Interface:** You can specify the URL of the Homepage that is shown after login and when clicking on the Home button. You can also choose a Chart Rendering method (whether or not to use the more interactive Flash Graphs) and specify a Flash Graph Delay to improve browser performance in case of using Flash Graphs.
- **Auto-folding:** In order to provide you with a speedy user experience, PRTG tries to keep the page size for the pages with the sensor tree small by automatically "folding" groups and devices with many items. The two settings "Max. Groups/Devices per Group" and "Max. Sensors per Device" control how many groups/devices or how many sensors are shown at max before the automatic reduction is performed. Recommended values are 10 - 30 for both settings. If you do not want to see any individual sensors in the tree view enter a zero for "Max. Sensors per Device".

Account Control (only PRTG Administrator Users can edit settings here):

- **Account Type:** Choose between "Read/Write User" or "Read Only User". Read Only User can only view objects and values and cannot edit any configuration settings. All editing functions are disabled and hidden in

the user interface. Of course, this user can only see objects that are enabled for this user. A Read/Write User can also edit every object that is write enabled for this user.

- **Primary Group:** Each user is mandatorily member of a "Primary Group". User access rights for objects and settings are controlled on group level.
- **Status:** The administrator can set a user to Inactive, meaning the user can not log on.

Creating New User Groups

This is for Administrator Users only. To create a new user group, select "Setup | User Groups" from the main menu and click on "Add new user group". See next section "User Group Settings" for details about the options.

User Group Settings

This is for Administrator Users only. To edit a user group's settings, select "Setup | User Groups" from the main menu and select a group. You have these options:

- **User Group Settings:** Here, you can enter the name of the group.
- **User List:** Select which users from the user list should be member of this group. Please note: Every user already is member of a primary group by default. Here you can add all marked users to the current group additionally. In the object settings, access rights are defined on group level only (not on user level).
- **Primary Users:** Shows a list of all users that have assigned the current group as Primary Group.

13.6 System Information and Optional Downloads

There are three buttons you can choose for system information or optional downloads.

View System Status

On this page, you can view exhaustive information about your system's status. You can find information about the software version you are using, about hardware and system resources, licensing information and an overview of your settings - to name a few. When contacting the Paessler support team, they will need these vital information to help you.

View Activation Status

Your PRTG Network Monitor license must be activated by the Paessler Licensing System. You can view your license's activation status or start an activation via email.

See section [Activating the Product](#) for more details.

Download Add-Ons

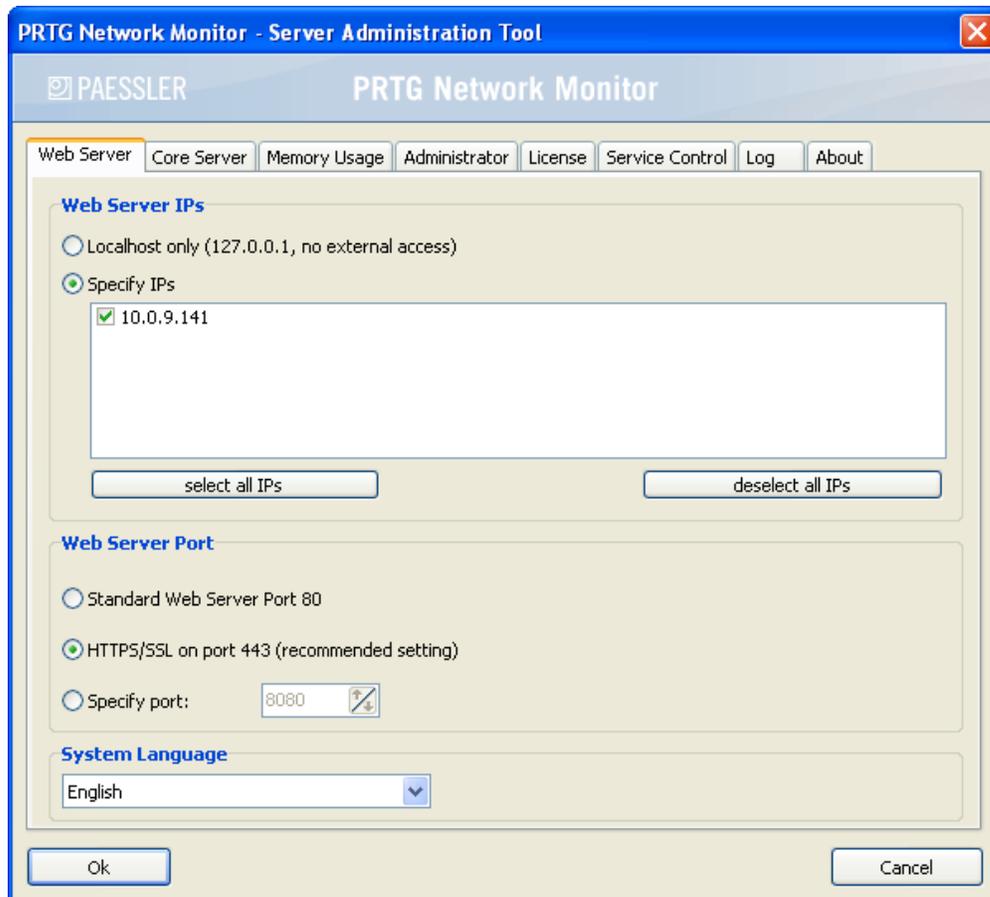
This is the starting point for you to get additional software you might need to set up your network monitoring. You can download the Windows GUI or the Remote Probe Installer, buy the iPhone App or visit the Paessler website.

13.7 PRTG Server Administrator

The "PRTG Server Administrator" can be started from the "PRTG Network Monitor" program group in the Start

Menu and allows configuring basic server settings. It is divided into eight tabs:

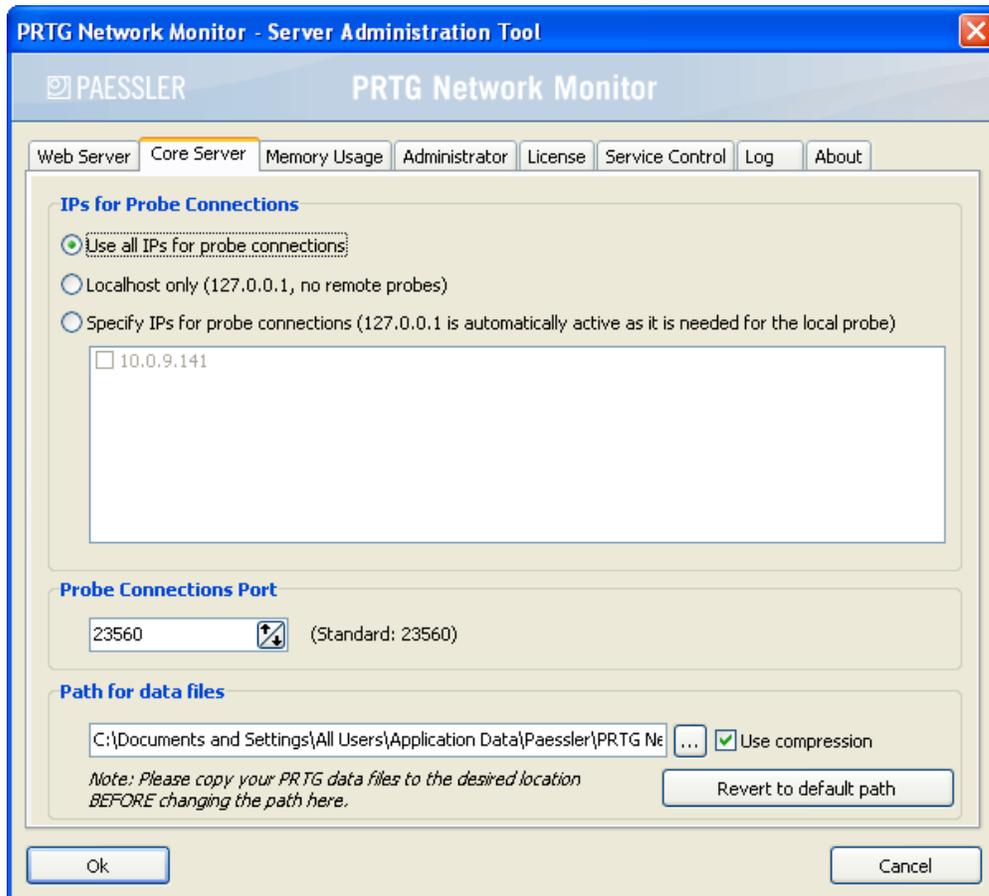
Web Server



Under the "Web Server" tab you can define the web server IP addresses. You can select to use local host only. This means that no external access will be possible and is the most secure setting. Alternatively, you can specify individual IPs from a list provided. You can further define the web server port to use. The options are:

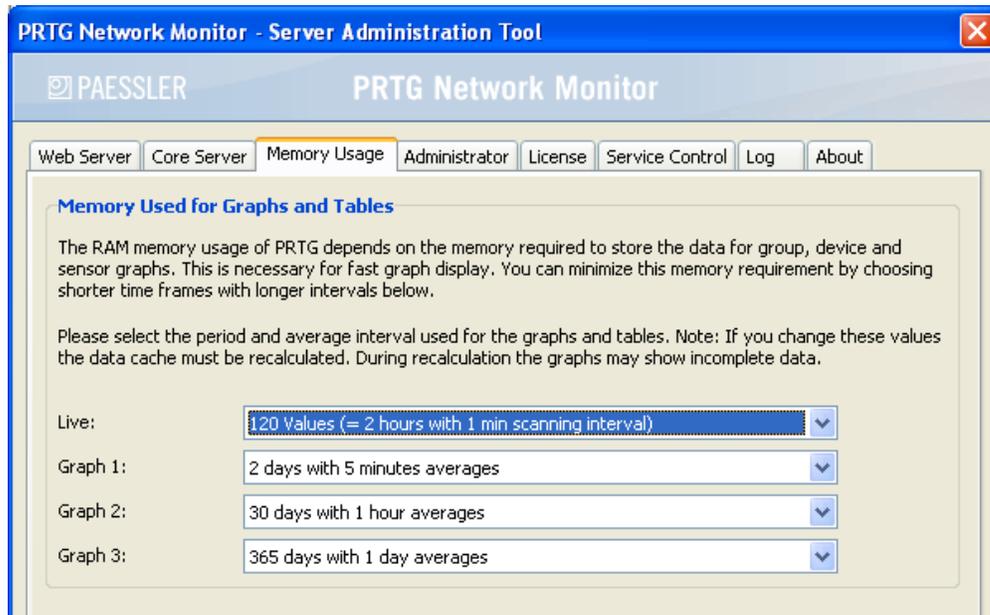
- Standard Web Server Port 80: Unencrypted connection via standard HTTP port 80 is used to access the web interface.
- HTTPS/SSL on port 443: The web interface can only be accessed using a secure SSL connection ("https://your_IP"). This is the default setting and recommended for most installations. **Note:** If you are using the PRTG Web Interface via an Internet (WAN) connection, we strongly recommend using an SSL encrypted connection! Please see "See also" at the end of this section.
- Specify Port: Enter a port number of your choice.
- System Language: With this setting you can change the language of the web interface and the PRTG Server Administrator. Select a language of your choice (German, English, Spanish, French, Japanese). A restart of server services will be necessary.

Core Server



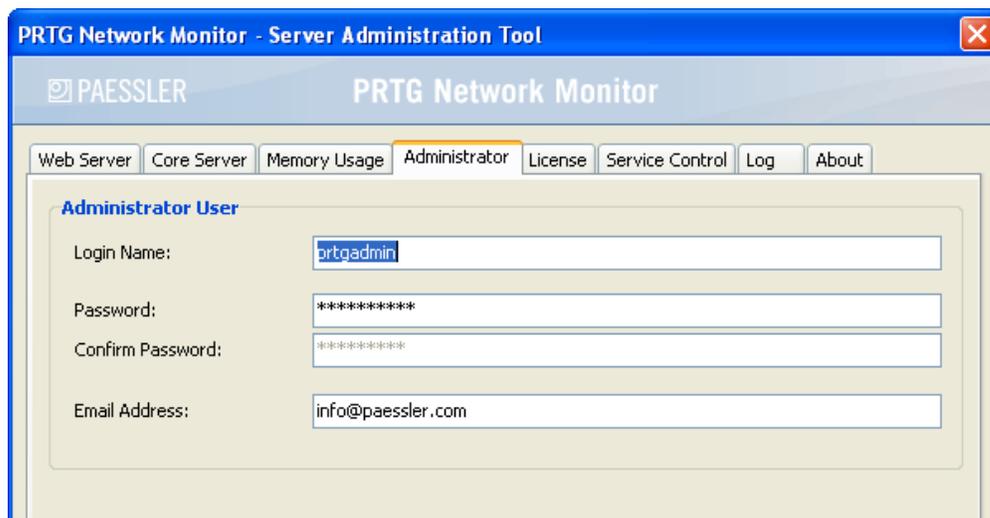
Under the Core Server tab you can define the IPs for probe connections. The connection between Core and probe is initiated by the probe (see section [Multiple Probes and Remote Probes](#)). You can select to use all IPs for connections, localhost only or individual IPs from the list provided. You can further define the port for probe connections, as well as define a path for all Core Server data files (you can optionally turn on compression and revert to the default path by clicking on the respective element).

Memory Usage



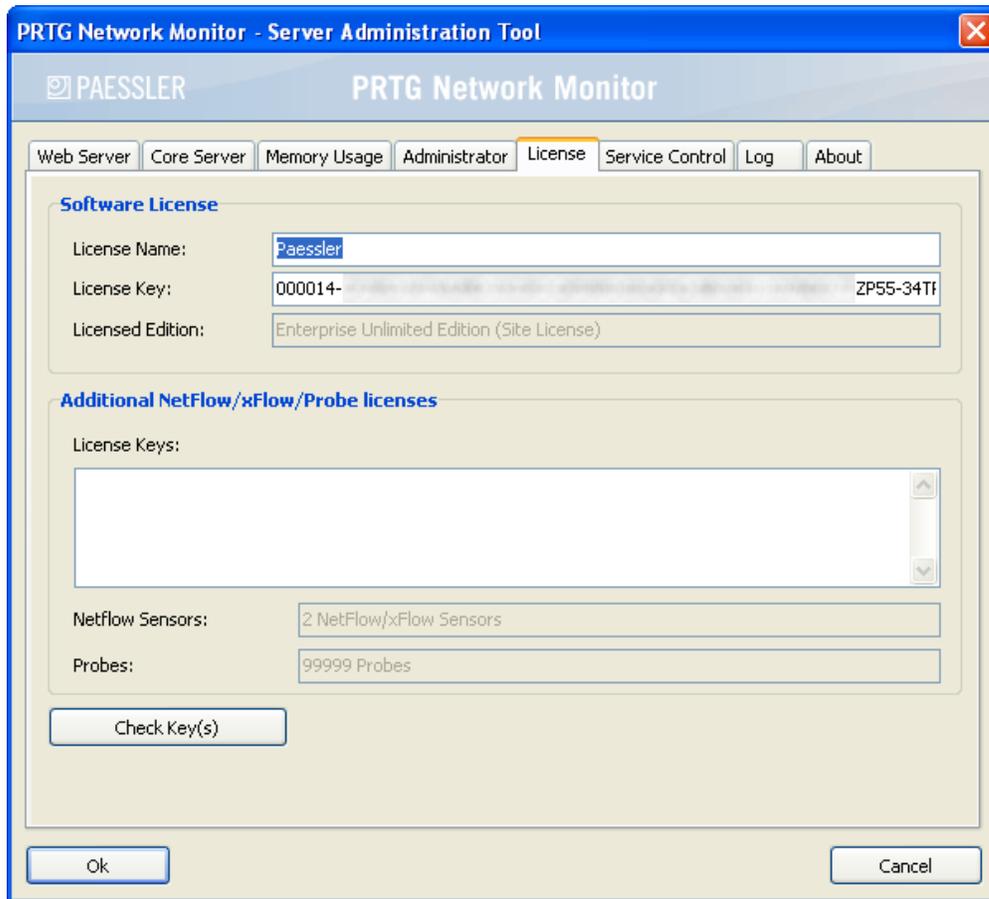
Under the "Memory Usage" tab you can define PRTG's memory usage for graphs and tables. To do so, you can define timeframes for live graphs, as well as the other three standard graphs displayed under PRTG. You can reduce memory usage by decreasing the graph time frame and increasing the intervals.

Administrator



Under the "Administrator" tab you can define the login name, the password and the email address of the administrator user. We strongly recommend to use a save password, especially when the web interface is accessible from the Internet.

License



Under the "License" tab you can enter your program license information (name and key, which will return a license edition value), as well as Netflow/xFlow add-on licenses. Once the licensing information has been entered click on the "Check Key(s)" button to check and activate them.

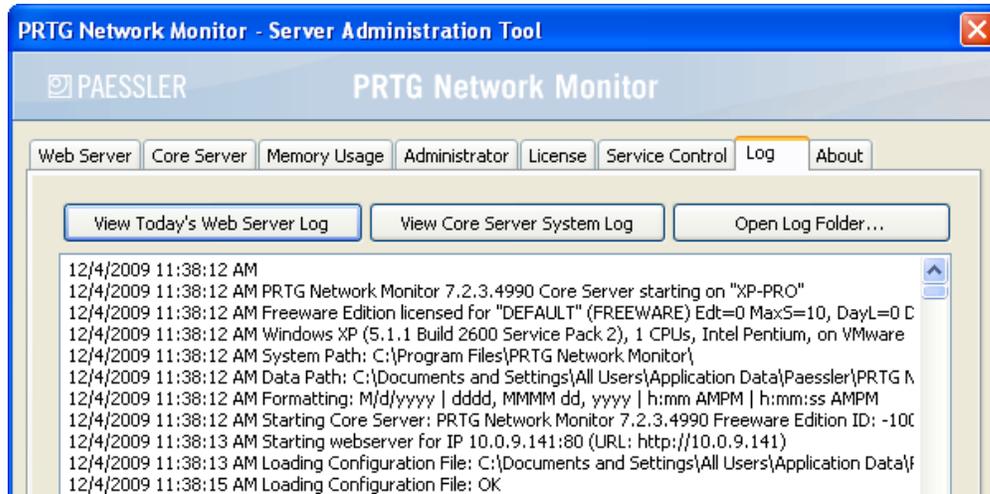
See section [Entering A License Key](#) for more detailed instructions.

Service Control



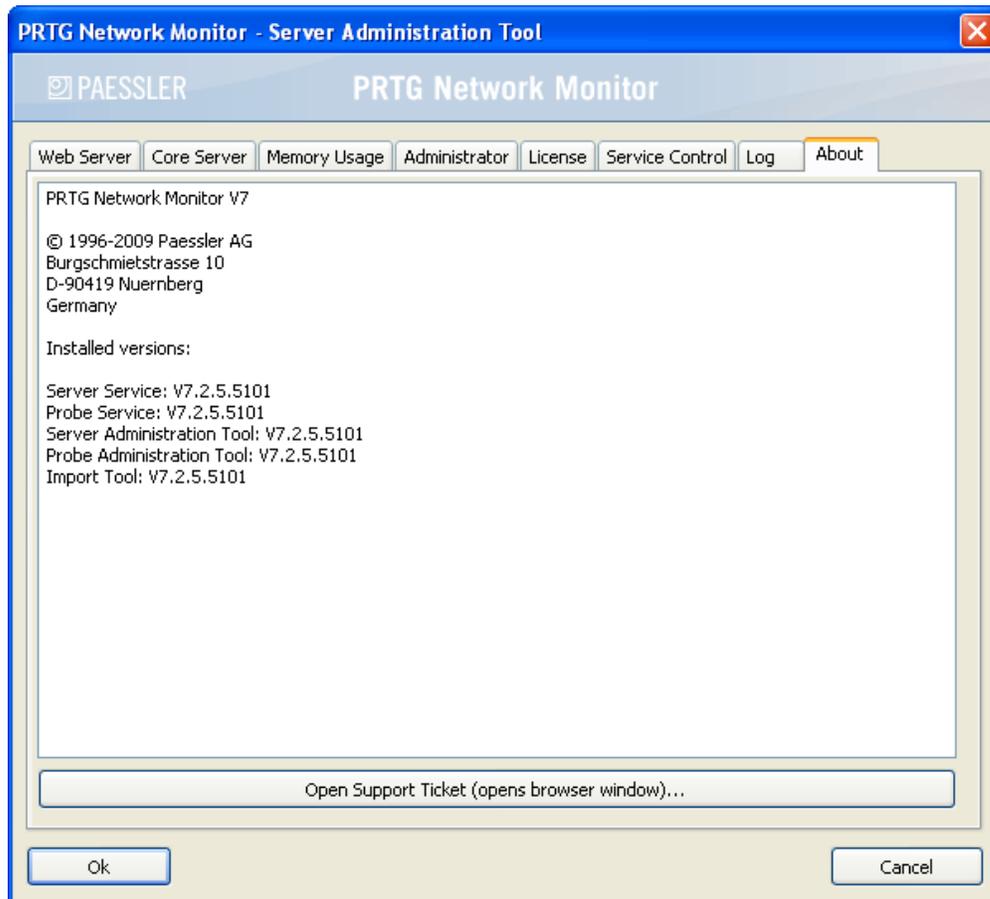
Under the "Service Control" tab you can install/uninstall, as well as start/stop the Core service.

Log



Under the "Log" tab you can view the current day's web server log and the Core Server system logs, or directly open the core's log file directory.

About



The information written under this tab contains details about the installed program versions. This tab also offers an option to directly open a ticket for our technical support.

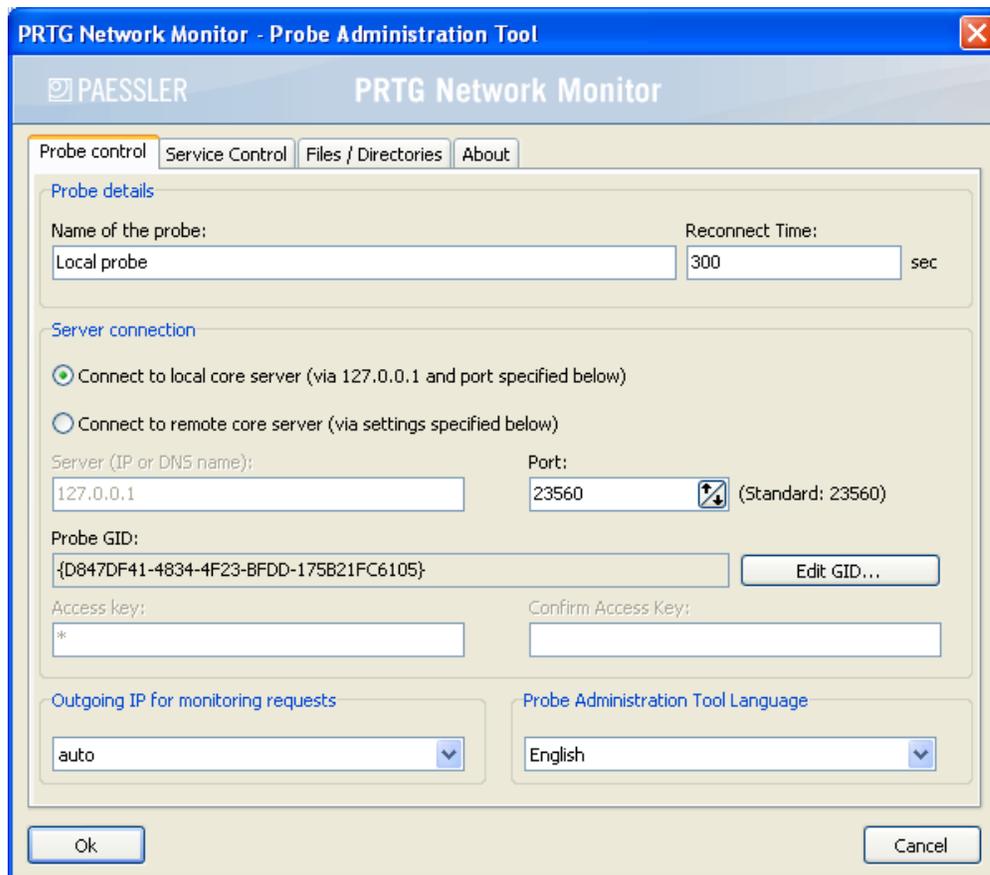
See also

- If you are using a HTTPS connection to the PRTG Web Interface and want to get rid of the browser security warning, you can install a trusted certificate. Please see our Knowledge Base article "Installing a Trusted SSL Certificate for PRTG for Free":
http://www.paessler.com/support/kb/categories/prtg7/install_ssl_certificate_for_free
- For a general introduction of the PRTG security options, see our Knowledge Base article "Secure PRTG Web Interface Connection":
http://www.paessler.com/support/kb/categories/prtg/secure_prtg7_web_interface_connection

13.8 PRTG Probe Administrator

The PRTG Probe Administrator can be started from the "PRTG Network Monitor" program group in the Start menu and allows configuring a probe running on the local PC. This can be the "Local Probe" for a PC running a full PRTG installation, or one of the remote probes when only the probe installer was used on a PC. The PRTG Probe Administrator is divided into four tabs:

Probe Control



Under the Probe Control tab you can define:

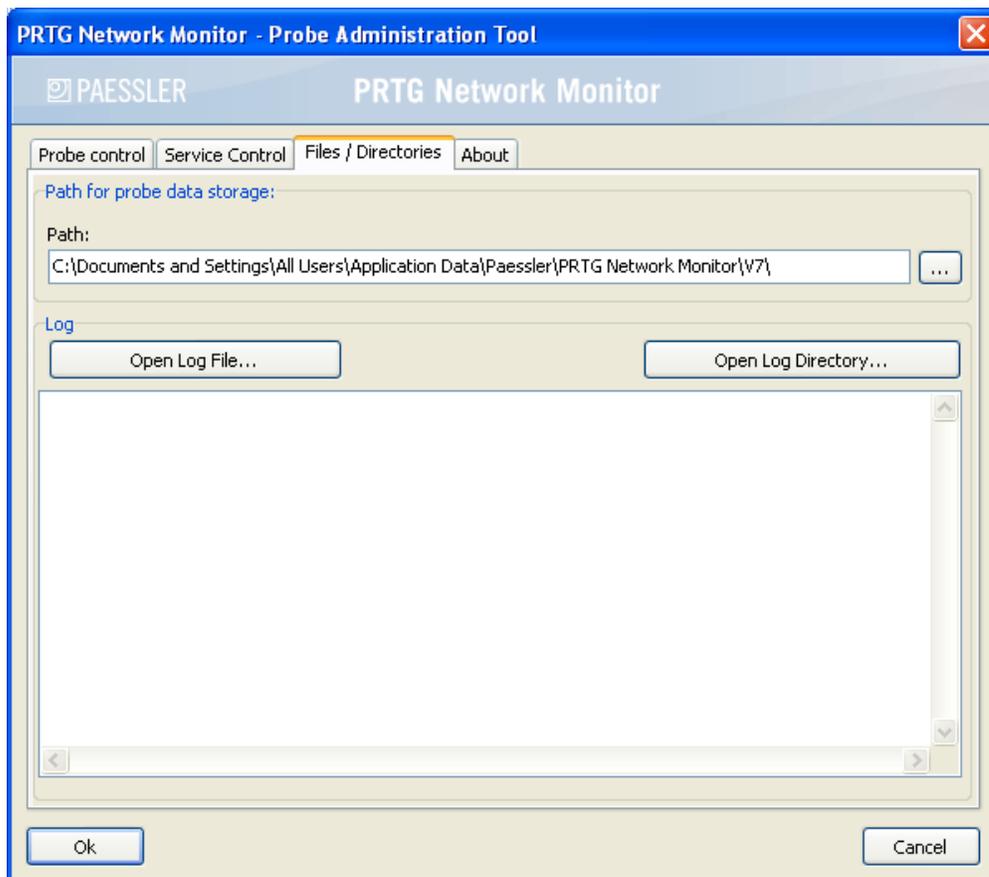
- Name of the probe (the name will be shown in the web interface).
- Reconnect Time (in seconds) which is the time between two connection attempts when the Core can't be reached.
- Server Connection: The server's IP address or DNS name, as well as the server's port and the probe's access key (these settings must match the settings in the PRTG Server Administrator, see also section [Multiple Probes and Remote Probes](#)).
- Probe GUID, the unique identifier for each probe (use with extreme caution!).
- Outgoing IP for monitoring requests: Choose the IP address that all outgoing monitoring requests should use. The setting "auto" is recommended (e.g. it automatically chooses the right IP on multi-homed systems).
- Probe Administration Tool Language: With this setting you can change the language of the PRTG Probe Administrator. Select a language of your choice (English, German, French, Spanish, Japanese). A restart of the probe service will be necessary. Please note: You can set the language of the PRTG web interface in the [PRTG Server Administrator](#).

Service Control



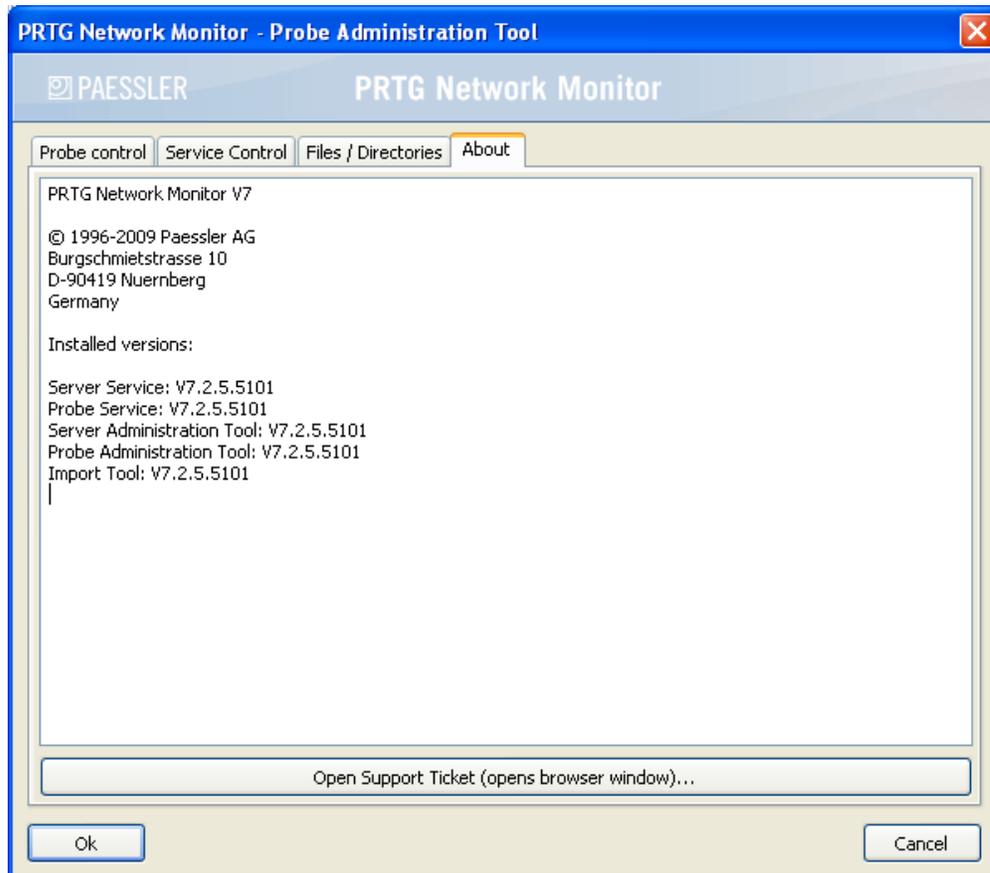
Under the Service Control tab you can install/uninstall, as well as start/stop the probe service.

Files/Directories



Under the "Files/Directories" tab you can select a path specifying where probe data is to be stored. You can further show the probe log files and open the probe's log file directory.

About



The information written under this tab contains details about the installed program versions. This tab also offers an option to directly open a ticket for our technical support.

Part



Advanced Topics

14 Advanced Topics

The chapter covers various advanced topics for PRTG Network Monitor:

- [Toplists](#)
- [Multiple Probes and Remote Probes](#)
- [Copying Devices by Cloning or Using Device Templates](#)
- [Importing Data from PRTG Traffic Grapher 6 or IPCheck Server Monitor 5](#)
- [Installing an SSL Certificate for the Web Server](#)
- [Using the PRTG API \(Application Programming Interface\)](#)
- [Interface Definition for Custom EXE Sensors](#)
- [Calculating Percentiles](#)

14.1 Toplists

[Packet Sniffer](#) and [xFlow](#) 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 in its database.

Why Are Only the Top Entries Stored?

Storing all the data in a database that becomes available 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 find bandwidth hogs.

Accessing Toplists

To access the Toplists for a Packet Sniffer or NetFlow sensor click the "Toplists" tab on the sensor's detail page:

Sensor Header Packet ASA

Home > Devices > Local probe > Probe Device > Header Packet ASA

Overview | Live Data | 2 days | 30 days | 365 days | **Toplists** | Log | Settings | Notifications | Channels | Comments | History

Please select a toplist

- Top Connections
- Top Protocols
- Top Talkers

Toplist "Top Connections"

Available Periods: 27.02.2009 14:45:00 - 15:00:00

1 to 49 of 1876

Pos	Source IP	Source Port	Destination IP	Destination Port	Protocol	Bytes	Item Count
1.	192.168.2.104	49739	192.168.2.104	22	TCP	56 MByte	70 %
2.	192.168.2.104	80	POP.paesslergmbh.de (10.0.0.202)	2093	TCP	1.116 KByte	1 %
3.	192.168.2.104	80	POP.paesslergmbh.de (10.0.0.202)	4438	TCP	1.116 KByte	1 %
4.	192.168.2.104	80	POP.paesslergmbh.de (10.0.0.202)	5435	TCP	1.116 KByte	1 %
5.	192.168.2.104	80	POP.paesslergmbh.de (10.0.0.202)	4935	TCP	1.116 KByte	1 %
6.	192.168.2.104	23560	192.168.2.104	3137	TCP	775 KByte	< 1 %
7.	192.168.2.104	443	192.168.2.104	13073	TCP	699 KByte	< 1 %
8.	192.168.2.104	22	192.168.2.104	49739	TCP	575 KByte	< 1 %
9.	192.168.2.104	49708	192.168.2.104	443	TCP	481 KByte	< 1 %
10.	192.168.2.104	54321	192.168.2.104	1796	TCP	435 KByte	< 1 %
11.	192.168.2.104	80	192.168.2.104	1997	TCP	365 KByte	< 1 %
12.	192.168.2.104	80	192.168.2.104	51499	TCP	309 KByte	< 1 %
13.	192.168.2.104	49841	192.168.2.104	25	TCP	271 KByte	< 1 %
14.	192.168.2.104	80	192.168.2.104	24787	TCP	231 KByte	< 1 %
15.	192.168.2.104	80	192.168.2.104	1993	TCP	213 KByte	< 1 %
16.	192.168.2.104	5665	192.168.2.104	25	TCP	212 KByte	< 1 %
17.	192.168.2.104	80	192.168.2.104	27561	TCP	211 KByte	< 1 %
18.	192.168.2.104	80	192.168.2.104	27565	TCP	200 KByte	< 1 %
19.	192.168.2.104	80	192.168.2.104	24788	TCP	184 KByte	< 1 %
20.	192.168.2.104	1449	192.168.2.104	23560	TCP	181 KByte	< 1 %
21.	192.168.2.104	80	192.168.2.104	55435	TCP	172 KByte	< 1 %
22.	192.168.2.104	80	192.168.2.104	1239	TCP	170 KByte	< 1 %
23.	192.168.2.104	80	192.168.2.104	4521	TCP	170 KByte	< 1 %
24.	192.168.2.104	80	192.168.2.104	4864	TCP	170 KByte	< 1 %
25.	192.168.2.104	80	192.168.2.104	27570	TCP	170 KByte	< 1 %
26.	192.168.2.104	80	192.168.2.104	1979	TCP	167 KByte	< 1 %
27.	192.168.2.104	80	192.168.2.104	2131	TCP	163 KByte	< 1 %
28.	192.168.2.104	80	192.168.2.104	27568	TCP	150 KByte	< 1 %
29.	192.168.2.104	80	192.168.2.104	4911	TCP	157 KByte	< 1 %
30.	192.168.2.104	80	192.168.2.104	3775	TCP	150 KByte	< 1 %

You can select a Toplist in the list at the beginning of the page. You can select the time period on the left.

2/27/2009 2:45:00 PM - 3:00:00 PM

1 to 100 of 100

Pos	Source IP	Source Port	Destination IP	Destination Port	Protocol	Bytes	
Other						807 KByte	24 %
1.	backup (192.168.2.104)	1208	[65.75.243.170]	23560	TCP	357 KByte	10 %
2.	mail2.myzms.com (62.146.10.41)	80	backup (192.168.2.104)	3932	TCP	203 KByte	6 %
3.	mail2.myzms.com (62.146.10.41)	80	backup (192.168.2.104)	4497	TCP	203 KByte	6 %
4.	mail2.myzms.com (62.146.10.41)	80	backup (192.168.2.104)	4220	TCP	201 KByte	6 %
5.	www.t-online.de (217.6.164.162)	80	backup (192.168.2.104)	4254	TCP	132 KByte	3 %
6.	www.t-online.de (217.6.164.162)	80	backup (192.168.2.104)	4529	TCP	131 KByte	3 %
7.	www.t-online.de (217.6.164.162)	80	backup (192.168.2.104)	3964	TCP	129 KByte	3 %
8.	www.t-online.de (217.6.164.162)	80	backup (192.168.2.104)	3929	TCP	120 KByte	3 %
9.	www.t-online.de (217.6.164.162)	80	backup (192.168.2.104)	4492	TCP	120 KByte	3 %
10.	www.t-online.de (217.6.164.162)	80	backup (192.168.2.104)	4216	TCP	120 KByte	3 %
11.	noname (192.168.2.102)	1036	[239.255.255.250]	8082	UDP	98 KByte	2 %

PRTG tries to show a DNS name for each IP address by performing reverse DNS requests. Each entry of the list shows the IPs, Ports, etc. (depending on the Toplist type) and the total number of bytes for this entry during the Toplist period. The last column displays the bandwidth of each entry as a percentage of the total bandwidth.

Configuring Toplists

In order to edit an existing Toplist or to add a new Toplist click the respective buttons next to the list of Toplists.

Add toplist

Name	<input type="text"/>	<small>Enter a name for the toplist</small>
Type	<input checked="" type="radio"/> Top Talkers (Which IPs use most bandwidth?) <input type="radio"/> Top Connections (Which connections use most bandwidth?) <input type="radio"/> Top Protocols (Which protocols use most bandwidth?) <input type="radio"/> Custom (Create your own toplist)	<small>Select a preconfigured toplist type or choose "Custom" to create your own toplist.</small>
Period (minutes)	<input type="text" value="15"/>	<small>Toplists always cover a specified period of time (e.g. 15 minutes). Afterwards the toplist is stored on disk and a new toplist is started from scratch.</small>
Top Count	<input type="text" value="100"/>	<small>Select the number of entries in the toplist. Performance tip: Keep this value as low as possible!</small>
Probe/Core Data Transfer	<input checked="" type="radio"/> According to sensor interval (default) <input type="radio"/> Wait until toplist period ends (less cpu&bandwidth usage)	<small>By default the probe sends the toplist dataset with the sensor's interval to the core. This can create a lot of bandwidth and cpu load for setups with 1. many sniffer sensors, 2. complex traffic, or 3. long toplists with many entries. Performance tip: Disable this option for such situation. But you will not be able to see the data of the current toplist in the web interface, only historic ones will be visible.</small>
Memory limit (MB)	<input type="text" value="10"/>	<small>Set the maximal amount of memory in MB the probe will use for collecting the different connection informations. Every toplist adds its amount to the probe's memory consumption. Increase this value if the number of captured connections is not sufficient.</small>

For the Toplist type you have 4 options:

- Top Talkers (Which IPs use most bandwidth?).
- Top Protocols (Which protocols use most bandwidth?).
- Top Connections (Which connections use most bandwidth?).
- Custom (Create your own Toplist).

For the "Custom" option you can select the parameters used while creating the Toplists. The fields available depend on the sensor type and include Source IP, Source Port, Destination IP, Destination Port, Source MAC, Destination MAC, Protocol, Ether Type, ToS, Channel, IP (combined), Port (combined), MAC (combined). Apart from the list type you can also set the period and number of entries in the list.

Toplists for Connections With a Lot of Traffic

If you create Toplists for data lines with considerable usage (e.g. steady bandwidth over 10 Mbit/s) or if the traffic is very diverse (i.e. 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 Toplists definition (depending on traffic pattern). Avoid complex Toplists for high and diverse traffic (e.g. "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 "Wait until Toplist period ends" (data is only transferred to the core once per period).
- If you experience "Data incomplete, memory limit was exceeded" messages try to increase the memory limit in the Toplist's settings but keep an eye on the probe process' memory usage.

Notes

- Note 1: When working with Toplists be aware that privacy issues can come up for certain configurations of this feature. Using Toplists 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.

- Note 2: Keep in mind that Toplists 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 sensors having Toplists.

14.2 Multiple Probes and Remote Probes

PRTG has two system modules: The Core Server, which handles data storage, web server and a lot more, as well as one or more "Probes" which perform the actual monitoring.

How Probes Work

As soon as a probe is started it automatically connects to its Core Server, 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 (e.g. a reboot of the Core) the probe continues its monitoring and stores the results.

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 and will then see the new probe in the sensor tree. As a security precaution, the probe must be manually acknowledged by the administrator (in the "ToDos" list) before any sensors can be created and monitored. The admin 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 probe system settings (see section [System Administration - Edit System Setup](#)). This ensures that unauthorized probes can not connect to a Core Server.

Since the probe initiates the connection, you must ensure that a connection can be established from the outside world onto your Core Server, e.g. you may need to open any necessary ports in your firewall and you may need to specify a NAT rule for your network. The process is the same when you want to allow access to the web server of the Core Server via port 80.

Note: The local probe is automatically configured and approved and connects to the Core via localhost (127.0.0.1) and SSL.

Situations That Require Monitoring Using Remote Probes

Upon installation, PRTG creates the first probe automatically called the "Local probe". The Local probe runs on the same machine as the Core Server and monitors all sensors from this system. Working with only one Local probe should suffice for LAN monitoring and if you have just one location that you need monitoring for.

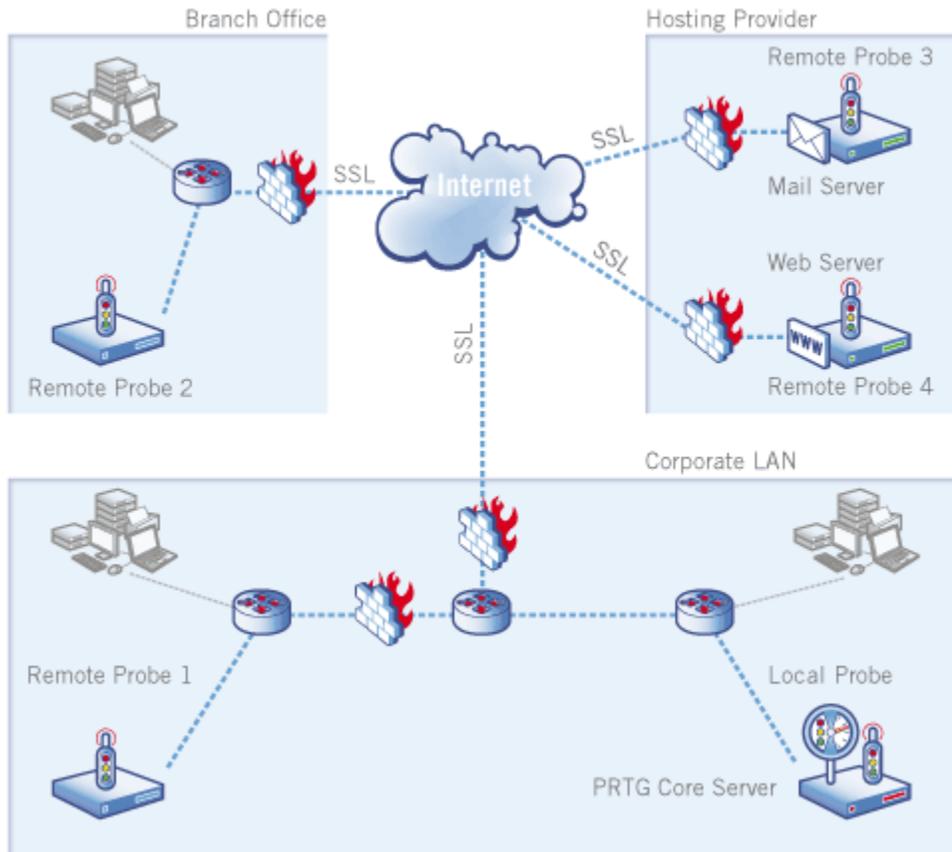
However, there are several situations that make it necessary to work with multiple probes or remote probes:

- If you have more than one location and you need to make sure that services are available from all locations.
- If your network is separated in several LANs by firewalls and the local probe can not monitor specific services across the firewalls.
- If you need to monitor systems in VPNs across public or in-secure data lines.
- If you want to sniff packets on another computer.
- If you want to monitor NetFlow data on another computer.
- If you experience performance issues with CPU intensive sensors like packet sniffer or NetFlow sensors and need to distribute the load onto more than one PC.

The following chart shows an example: The PRTG Core Server inside the "Corporate LAN" (bottom right) is

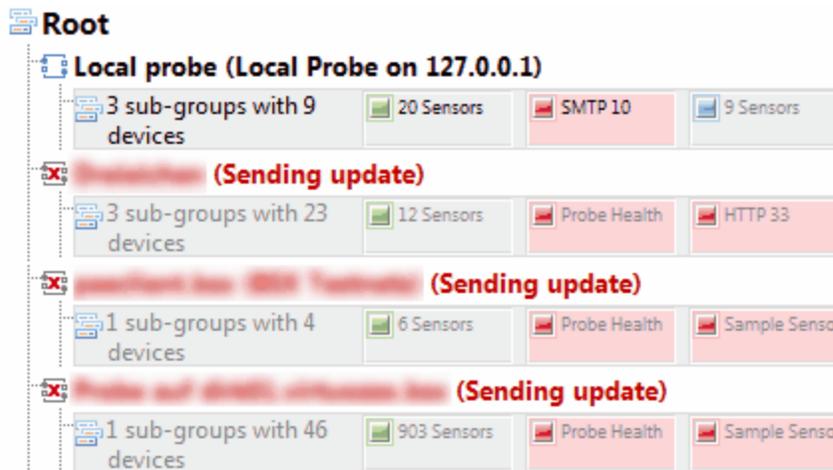
able to monitor:

- 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 a "Remote Probe 2" installed on a dedicated probe server.
- 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.



Automatic Probe Updating

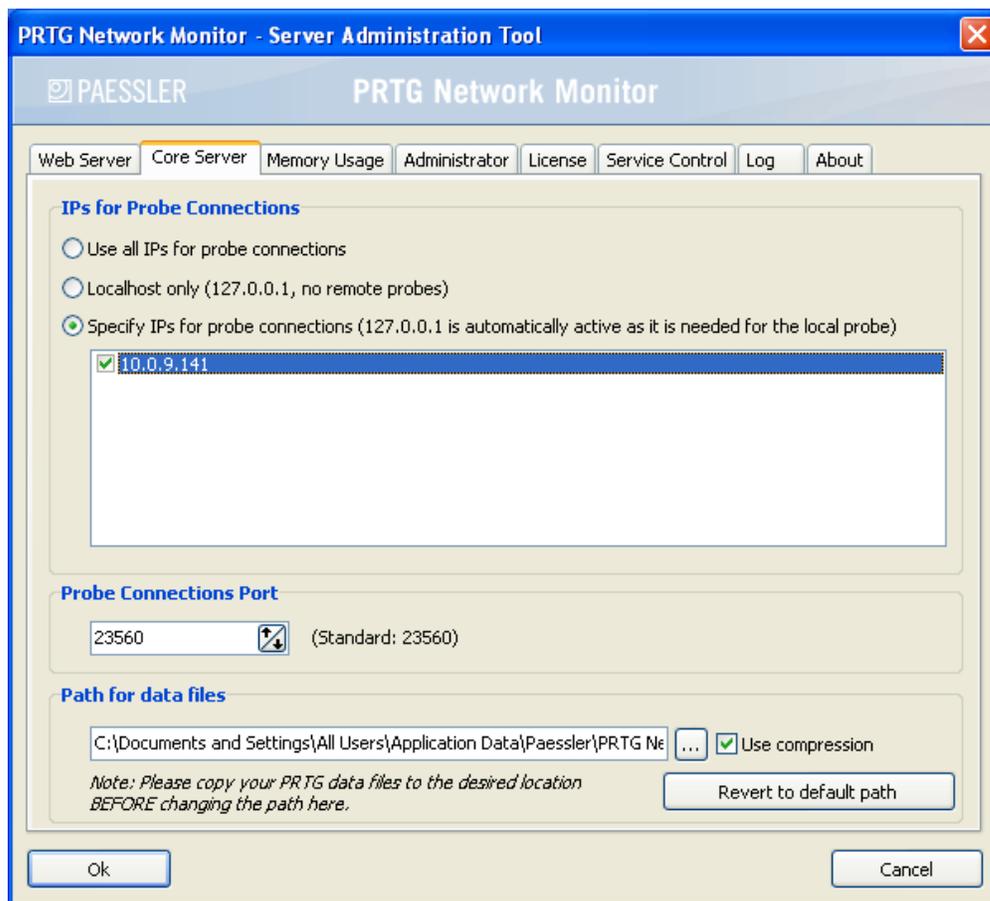
Whenever a new version of PRTG is installed on the Core Server all remote probes will automatically download and install the updated version of the probe as soon as they reconnect to the updated Core. Here is a screenshot of the "Devices" page of a PRTG installation shortly after the restart of a Core Server that has been updated to the latest PRTG version:



The Local probe has already been updated during the Core installation. All other probes are automatically downloading the new binaries of the "PRTG probe" using the SSL-secured probe/Core connection. The download of the 4 MB file takes between a few seconds (in LANs) and a few minutes (over WAN 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.

Step 1: Preparing a Core Server for Remote Probes

Before remote probes can connect to a Core Server you must edit the relevant settings in the PRTG Server Administrator which you can find in PRTG's Start menu group (see section [PRTG Server Administrator](#)):



By default, a Core Server only accepts connections via localhost (127.0.0.1) which means that only the Local probe can connect. This is the most secure setting. In order to allow external probes to connect you must check "Use all IPs..." or "Specify IPs..." and select one of the IPs of the server. You can also specify the TCP/IP port number.

When you are done, click "OK" to save your settings. The Core Server process will be restarted so that the changes take effect.

Step 2: Setting up Remote Probes

To install a remote probe, open a browser window on the machine you want to install the probe on and go to the PRTG web interface of the Core Server installation. In the interface, go to "Setup | Download", download the Remote Probe Installer and run it. **Note:** You cannot install a remote probe on a system where a PRTG Core Server is installed.

At the end of the installation the Probe Administrator will be started (or you can start it manually from the Windows Start Menu later) and you can enter the settings:

PRTG Network Monitor - Probe Administration Tool

PAESSLER PRTG Network Monitor

Probe control Service Control Files / Directories About

Probe details

Name of the probe: Local probe Reconnect Time: 300 sec

Server connection

Connect to local core server (via 127.0.0.1 and port specified below)

Connect to remote core server (via settings specified below)

Server (IP or DNS name): 127.0.0.1 Port: 23560 (Standard: 23560)

Probe GUID: {D847DF41-4834-4F23-BFDD-175B21FC6105} Edit GUID...

Access key: * Confirm Access Key:

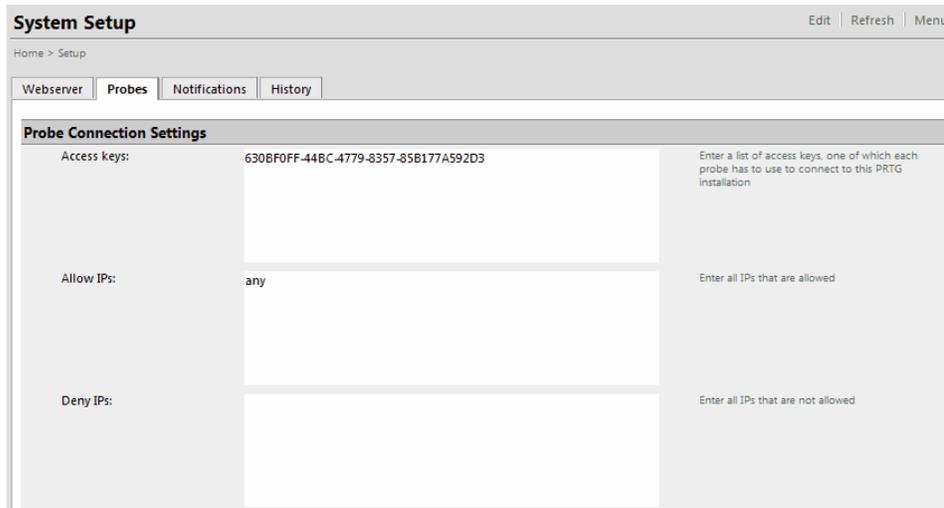
Outgoing IP for monitoring requests: auto Probe Administration Tool Language: English

Ok Cancel

The important settings are (see [PRTG Probe Administrator](#) for more details):

- Name of the probe: A name of your choice that will be visible in the sensor tree later.
- Server Connection: Please choose "Connect to remote core server".
- Server (IP or DNS name). Please enter the server's IP address or DNS name (the one that you have specified in the core server administrator tool above). Note: If the core server resides in a NAT-ed network behind a firewall you must edit your firewall NAT settings and supply the external mapped IP address.
- Port: Please enter the same port number that you have set up in your Core Server above.

You can edit the access keys on the server through the web interface: Choose "Setup | System Setup" from the main menu and you will see this screen:

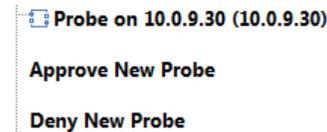


You can enter one or more access keys in the web interface (one for each probe is recommended) and the exact same string must be entered into the probe's setup, otherwise the core server will not accept a connection. By default PRTG accepts connections from any IP. Using the two settings you can make your configuration even more secure, especially by only allowing authorized IPs. Simply enter these IPs in the "Allow IPs" setting. If you ever need to hard block a probe from a specific IP, please enter the IP in the "Deny IPs" settings.

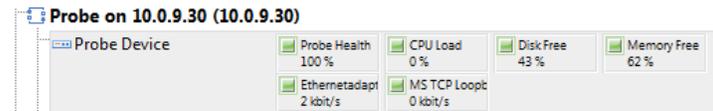
When you are done with the probe setup, the probe service is started automatically and the it tries to connect to the core server.

Step 3: Approving a New Probe

When a new probe has connected to the Core Server you must approve it in the web user interface:



Click on "Approve New Probe" to fully enable the probe. PRTG automatically creates a set of sensors for the probe to ensure that bottle-necks on the probe will always be noticed. It is recommended to keep these sensors.



Now you can create groups, devices and sensors for monitoring via the new probe.

Debugging Probe Connection Problems

If you have trouble with the setup of remote probes please look at the probe's log files which usually reside in the following folder on the probe system:

Windows XP and Windows Server 2003:

```
C:\Documents and Settings\All Users\Application Data\Paessler\PRTG Network Monitor\V7\Logs (System)
```

Windows Vista, Windows Server 2008, and Windows 7:

```
C:\ProgramData\Paessler\PRTG Network Monitor\V7\Logs (System)
```

The probe process writes the two log files "PRTG Probe Log (1).log" and "PRTG Probe Log (2).log" alternatively. Please open the one with the most recent date.

For a correct connection the probe log should look similar to this:

```
11.01.2010 16:15:15 PRTG Probe Server V7.2.5.5101
11.01.2010 16:15:15 Starting Probe on "WINXPVMWARE"
11.01.2010 16:15:15 Data Path: C:\documents and settings\All Users\...
11.01.2010 16:15:15 Local IP: 0.0.0.0
11.01.2010 16:15:15 Core Server IP and Port: 10.0.2.167:23560
11.01.2010 16:15:15 Probe ID: -1
11.01.2010 16:17:01 Connected to 10.0.2.167:23560
11.01.2010 16:17:06 Login OK: Welcome to PRTG
```

For example if the connection fails due to an incorrect Access Key password you will see:

```
11.01.2010 16:31:02 Try to connect...
11.01.2010 16:31:02 Connected to 10.0.2.167:23560
11.01.2010 16:31:07 Login NOT OK: Access key not correct!
```

14.3 Copying Devices by Cloning or Using Device Templates

After configuring a device with one or more sensors there are two options to copy it:

- Cloning a device: Is the best option to simply duplicate a device only a few times with all its sensors and settings.
- Using device templates: Is the preferred option if you have many similar devices and if you do not want to create all devices manually through the web interface. This is also the better option if the devices do not have the same number of ports.

Cloning a Device

Choose the context menu item "Clone" from the device's context menu. PRTG will ask you for the new parent group and well as a new name for the device. The new device will be initially be paused to give you the chance to edit sensor settings if necessary. When all sensors are configured correctly you can resume monitoring for the device with all its sensors.

Using Device Templates

In order to create a device template PRTG stores the definitions of the sensors of a device in a device template file. Later this template file can be used to recreate all sensors that can successfully be recreated for the a device. To create a device template choose the "Create Device Template" item from the device's context menu and PRTG will ask you for a filename and a template name. The template file will be stored in the 'devicetemplate' subfolder of your PRTG installation. To create new devices with the same set of sensors you now have two options:

- Create an auto-discovery group, select option "Automatic sensor creation using specific device template(s)" and choose this specific device template from the list of templates.
- Create a new device, select option "Automatic sensor creation using specific device template(s)" and choose

this specific device template from the list of templates.

Limitations of Device Templates

Copying devices using device templates has the following limitations (cloning a device does not have these limitations):

- Only the following devices are supported: Generic Device (PING only), Generic Device (SNMP-enabled, Detailed), Generic Device (SNMP-enabled), VMware ESX Server, Hyper V Host Server, Printer (HP), DNS Server, FTP Server, Server (Compaq/HP agents), HTTP Web Server, Mail Server (MS Exchange 2007), Mail Server (MS Exchange 2003), Mail Server (Generic), Switch (Cisco Catalyst), Switch (Cisco Generic), Switch (Cisco IOS Based), Switch (HP Procurve), UNIX/Linux Device, UPS (APC), Windows (Detailed via WMI), Windows (via WMI), Windows IIS (via SNMP).
- Only the following sensor types can be stored in a device template: DNS, EXE, FTP, HTTP, HTTP Advanced, HTTP Full Web Page, IMAP, Ping, POP3, Port, RemoteDesktop, SMTP, SNMP Custom, SNMP Helper (discontinued), SNMP Library, SNMP Traffic, WMI Custom, WMI Disk Free, WMI Event Log, WMI File, WMI Memory, WMI Network, WMI Pagefile, WMI Process, WMI Processor, WMI Service, WMI Vital System Data, HyperV Virtual Machine.
- Credentials settings of the device are not stored in the device template file. You should enter credentials on the group level before you create devices using a device template.
- Sensors that are created based on available objects (e.g. SNMP Traffic and WMI Network Card sensors which look at available ports of a device) will be recreated from scratch for all available ports on the new device.
- Schedules, triggers, dependencies and channel settings are not stored in device templates.

14.4 Importing Data from PRTG Traffic Grapher 6 or IPCheck Server Monitor 5

You can import your sensor configuration and historic monitoring data from PRTG 7's predecessor products - PRTG Traffic Grapher V6 or IPCheck Server Monitor 5 - into your PRTG Network Monitor 7 installation using the Import tool.

Please see this Knowledge Base article on the Paessler website for details:

http://www.paessler.com/support/kb/prtg7/tricks/data_import_from_prtg6_or_ipcheck5/

14.5 Installing an SSL Certificate for the Web Server

PRTG Network Monitor comes with a default SSL certificate so you can securely use the web interface through HTTPS out-of-the-box. But because it is not an official certificate that matches the domain name or IP address of your PRTG installation a web browser will always show an alert ("the certificate is not correct") when it connects to this server (although the transmission is already secure).

Please see the Paessler Knowledge Base for details:

http://www.paessler.com/support/kb/prtg7/tricks/install_ssl_certificate/

14.6 Customizing the Web Interface

There are different possibilities how you can customize the PRTG Web Interface. By changing the surface of the web interface, you can re-brand the look and feel to fit into your company's corporate design. **Note:** A good knowledge of HTML and CSS is necessary to perform these changes.

Please see the following articles from Paessler's Knowledge Base:

- HowTo: Customize PRTG Login Screen:
http://www.paessler.com/support/kb/categories/prtg7/customize_prtg_login_screen
- HowTo: Re-Brand and Customize the PRTG Web Interface Using CSS:
http://www.paessler.com/support/kb/prtg7/branding_and_customizing_prtg_web_interface_using_css

14.7 Using the PRTG API (Application Programming Interface)

PRTG Network Monitor includes an API that enables access to internal data for external programs. This means that you can create your own programs or scripts that have access to information from the monitoring database and are able to manipulate the object database of PRTG. The API is HTTP based and uses a set of URLs to access the data.

Please see the menu item "PRTG RESTful API" in the "Help" menu for details.

14.8 Interface Definition for Custom EXE Sensors

Note: Please read the general introduction to [Custom Sensors](#) first.

This section will give you an overview of the usage of "Custom EXE/Script" sensors. Every time the sensor is run, the selected EXE, script or DLL file is executed.

The EXE/Script sensor supports following file types:

- EXE
- DLL
- VBScript
- Powershell script
- CMD/BAT script

EXE Sensors

The string entered in the parameter field of the sensor's settings is placed in the command line. The EXE file must send the results to the Standard OUT. The data must be in the following format:

```
value: message
```

Value has to be a 32 bit integer and will be used as the resulting value for this sensor (e.g. bytes, milliseconds, etc.), message can be any string and will be stored in the database.

The EXE's exit code has to be one of the following values:

- 0: ok
- 1: warning
- 2: system error (e.g. a network/socket error)
- 3: protocol error (e.g. web server returns a 404)
- 4: content error (e.g. a web page does not contain a required word)

If the EXE does not return control to the PRTG process it is killed as soon as the timeout value set for this sensor is reached.

You can test the EXE file you want to use for the sensor very easily on the command line (cmd.exe). Simply start the EXE file and pipe the results into a file, e.g.:

```
sensorexex parameter > result.txt
```

The results are then written into the file result.txt and you can check the results with notepad or any other text editor.

As "parameter" variable you can also use the following placeholders:

- "%host": Device IP/DNS.
- "%device": Device name.
- "%probe": Probe name.
- "%name": Sensor name.

Please make sure you write the placeholders in quotes to ensure that they are working properly if their values contain blanks.

CMD/BAT files

The CMD/BAT file must send the results to the Standard OUT. The data must be in the following format:

```
value: message
```

Value has to be a 32 bit integer and will be used as the resulting value for this sensor (e.g. bytes, milliseconds, etc.), message can be any string and will be stored in the database.

The script's exit code has to be one of the following values:

- 0: ok
- 1: warning
- 2: error

If the EXE does not return control to the PRTG process it is killed as soon as the timeout value set for this sensor is reached.

A simple sample batch file would look like this:

```
echo 100: Everything OK
exit 0
```

DLL sensors

Every time the sensor is to be checked the selected DLL file is called. The DLL must export one function:

```
function perform( para, msg: pchar): integer; stdcall;
```

para and msg are zero terminated strings. The allocated buffer for msg is 255 bytes, the DLL must make sure that fewer bytes are returned. Msg must be in the following format:

```
value: message
```

Value has to be an 32 bit integer and will be used as the resulting value for this sensor (e.g. bytes, milliseconds, etc.), message can be any string and will be stored in the database.

The integer return value of the perform function has to be one of the following values:

- 0: ok
- 1: warning
- 2: system error (e.g. a network/socket error)
- 3: protocol error (e.g. web server returns a 404)
- 4: content error (e.g. a web page does not contain a required word)

Warning: If the function call in the DLL does not return control it could block the whole PRTG system. Make sure to handle your own timeouts and build in a reliable error management. For this reason EXE sensors are recommended.

Links

Sample projects for these Custom sensors can be found:

- In the "PRTG Network Monitor\custom sensors\EXE" subfolder of your PRTG installation.
- In the Knowledge Base on the Paessler website at <http://www.paessler.com/kb>
- On the prt7addons website on the open source platform Google Code: <http://code.google.com/p/prtg7addons/>

14.9 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 a certain amount of values.

In PRTG, you can calculate percentiles when creating general Reports (see section [Reports](#)) or performing Historic Data reports of a certain sensor (see section [Web Interface](#)). Activating the Percentile Results for your reports, 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

A good source for more information regarding these percentiles can be found on this page:

http://www.servicelevel.net/rating_matters/newsletters/issue13.htm

14.10 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 the Info.Zip library, license info in the provided "info-zip-license.txt". Uses FastMM (<http://sourceforge.net/projects/fastmm/>) and TPLockBox (<http://sourceforge.net/projects/tplockbox>) under the Mozilla Public License 1.1 (MPL 1.1, available from <http://www.mozilla.org/MPL/MPL-1.1.html>). Soundfiles from www.soundsnap.com.

Legal notice: All trademarks mentioned herein belong to their respective owners.

Last change (DD.MM.YYYY): 03.03.2010

Index

- A -

Access Concept 31, 117
 Access Key 129, 135
 Access Keys 125
 Access Rights 117
 Account 121
 Account Settings 120, 121, 123, 128
 Account Setup 120
 Activate Product 20
 Activation Status 20
 Add a User 128
 Add Devices 54
 Add Notification 123
 Add Schedule 121
 Add Sensors 54
 Add-On 129
 Administration 120
 Administrator 129
 Advanced Topics 140
 Aggregate Sensor Values 88
 Aggregation Sensor 88
 Alarm 31
 Alarm Concept 31
 Alert 32, 94, 123
 Alert Box 37
 Allow IP 125
 Amazon 79
 Amazon Web Services 79
 Analyse Network Usage 140
 Analysis 32
 Analyze Data 140
 Analyze Monitoring Data 109
 API 82, 151
 Apple iPhone 50
 Application programming interface 82, 151
 Approved Certificate 150
 Architecture 24
 Auto Discovery 59
 Auto Folding 121, 128
 Auto Refresh 121, 128
 Autocreate 59
 Automatic Device Creation 59, 149
 Automatic Sensor Creation 59

AWS 79

- B -

Bandwidth Monitoring 64, 87
 Bandwidth Usage Analysis 140
 Basic Concepts of PRTG 24
 Basic Principle 24
 Basic Sensor Settings 61
 Basics 6
 BAT 82, 151
 Black Sensor 37
 Blue Sensor 37
 Board 31
 Browser 10
 Browser Type 10

- C -

Calculated Planning Impairment Factor 80
 Change Channel Settings 61
 Change Language 135
 Change Logins 117
 Change Password 117, 121, 128
 Change Sensor Settings 61
 Change Settings 61
 Change System Language 129
 Change User Settings 128
 Change Web Site Title 125
 Change Website DNS Name 125
 Channels 27, 30, 61
 Charts 31, 109
 Chrome 10
 Cisco 64
 Cisco Switch 68, 80, 85
 Cisco Switches 140
 Client 79
 CMD 82, 151
 COM 71
 Combine Sensor Values 88
 Commercial Edition 7, 18
 Common Sensors 64
 Configuration 10
 Content Based Packet Sniffing 83
 Context Menu 37
 Core 129
 Core Server 24

Core Server Admin Tool 129
 Core System Memory Usage 129
 Create Devices Automatically 59, 149
 Create Devices Manually 56
 Create Network Overview 100
 Create Sensors Automatically 59, 149
 Create Sensors Manually 56
 Custom 82, 151
 Custom Layouts 100
 Custom Sensor 88, 151
 Customize Web Interface 150

- D -

Dashboard 31, 100
 Data 153
 Data Extraction 31, 109
 Data Folder 135
 Data Folders 129
 Data Purging Limit 125
 Database Objects 129
 DCOM 71
 Deinstall PRTG 22
 Deny IP 125
 Dependencies Settings 61
 Dependency Concept 33
 Depending on 33
 Deutsch 129, 135
 Device 27, 30, 56, 59
 Device Settings 33
 Device Template 149
 Device Tree 33
 Diagram 100
 Diary 32
 Distribute Network Load 143
 Distributed Component Object Model (DCOM) 71
 DNS 74
 Domain Name System 74
 Download 15, 129
 Download iPRTG 129
 Download Windows GUI 129

- E -

EC2 Instance 79
 Edit Schedule 121
 Edit Sensor 61

Edition 18
 EMail 75, 94, 123
 Enterprise Edition 7, 18
 Error Log 32
 Error Settings 61
 Español 129, 135
 ESX 79
 ESXi 79
 Evaluate Data 31, 109
 Events 32
 EXE 82, 94, 123, 151
 Execute 123

- F -

Factory Sensor 88
 Features 6
 File Monitoring 78
 File Transfer Protocol 74
 Firefox 10
 Flash Graphs 121, 128
 Folder 135
 Folder Monitoring 78
 Folders 129
 Français 129, 135
 Freeware 7
 Freeware Edition 18
 French 129, 135
 FTP 74

- G -

German 129, 135
 GET 65
 Get Software 15
 Global Status Bar 37
 Google Chrome 10
 Graph Intervals 129
 Green Sensor 37
 Grey Sensor 37
 Group 27, 30, 56, 59
 GUI 21

- H -

Hard Disk Drive 78
 Hardware Requirements 10

- Hash 128
- Header Based Packet Sniffing 83
- Hierarchy 27
- High Speed Switched Networks 85
- Historic Data 37
- Host 79
- How Alarms Work 31
- How Logs Work 32
- How PRTG Architecture works 24
- How PRTG Works 24
- How the Object Hierarchy works 27
- How to Access System Information 129
- How to Activate Software 20
- How to Change Probe System Language 135
- How to Change Schedules 121
- How to Change Settings of Sensors and Channels 61
- How to Change System Language 129
- How to Choose the Right License 7
- How to Choose the Right Sensor 64
- How to Choose the Right Sensor Technology for Bandwidth Monitoring 87
- How to Choose the Right User Interface 35
- How to Create Devices and Sensors Automatically 59
- How to Create Devices and Sensors Manually 56
- How to Create Devices Automatically 149
- How to Create Interactive Maps of Your Network 100
- How to Create Reports From Your Monitoring Data 109
- How to Customize the Web Interface 150
- How to Define How Notifications are Being Sent 125
- How to Define Settings for the Root Group 54
- How to Determine System Requirements 10
- How to determine the Quality-of-Service of your network 80
- How to Download Software 15
- How to Edit a User's Account Settings (Admins only) 128
- How to Edit Basic Probe System Settings 135
- How to Edit Basic System Settings 129
- How to Edit Notification Delivery Settings 125
- How to Edit System, Website, and Web Server Settings 125
- How to Edit Your Account Settings 121
- How to Enter a License Key 18
- How to Import Data From Older Program Versions 150
- How to Install 15
- How to Install a PRTG Remote Probe 21
- How to Install a Validated SSL Certificate for Your Web Server Connection 150
- How to Install PRTG Core Server 16
- How to Install Windows GUI 21
- How to Manage a Probe Connection 125
- How to Manage Users and Define Access Rights 117
- How to Obtain Additional Software 129
- How to Set Up a Remote Probe 143
- How to Set Up Devices and Sensors 54
- How to Set Up New Notifications 123
- How to Understand Basic PRTG Concepts 24
- How to Understand Schedules 32
- How to Uninstall PRTG 22
- How to Upgrade From Previous Versions 15
- How to Use Bandwidth Monitoring Sensors 64
- How to Use Common Sensors Sensor 64
- How to Use Custom Sensors 82
- How to Use Dependencies 33
- How to Use File Server Sensors 78
- How to Use Mail Server Sensors 75
- How to Use Multiple Probes in Your Network 143
- How to Use NetFlow Sensors 85
- How to Use Notifications 94
- How to Use Packet Sniffer Sensors 83
- How to Use PRTG on the iPhone 50
- How to Use Quality-of-Service (QoS) Sensors 80
- How to Use sFlow Sensors 85
- How to Use Simple Network Management Protocol (SNMP) Sensors 68
- How to Use SQL Database Server Sensors 77
- How to Use the Application Programming Interface (API) 151
- How to Use the Different Program Interfaces 24
- How to Use the Inheritance of Settings 30
- How to Use the PRTG Probe Administrator 135
- How to Use the PRTG Server Administrator 129
- How to Use the Web Interface 37
- How to Use the Windows GUI 45
- How to Use This Document 8
- How to Use Toplists für xFlow and Packet Sniffer Sensors 140
- How to Use Various Protocol Sensors 74
- How to Use Virtual Server Sensors 79
- How to Use Voice-over-IP (VoIP) Sensors 80
- How to Use Web Server Sensors 65

How to Use Windows Management Instrumentation (WMI) Sensors 71
 How to Use xFlow Sensors 85
 How to Work With the ToDos List 115
 HTTP 65
 HTTP Request 94, 123
 HTTP Sensor 64
 HTTPS 65, 150
 Hypertext Transfer Protocol 65
 Hypertext Transfer Protocol Sensor 64
 HyperV 79

- I -

ICPIF 80
 ICQ 94, 123
 ICQ Delivery 125
 Images 121, 128
 IMAP 75
 Import Data 150
 Inherit 30
 Inherit Rights 61
 Inheritance 30, 54, 61
 Install 21
 Install Remote Probe 21, 129, 143
 Installation 10, 15, 16
 Instant Messenger 94
 Internet Explorer 10
 Internet Message Access Protocol (IMAP) 75
 Internet Page 65
 Internet Provider 153
 Internetserver 65
 Internetworking Operating System (IOS) 85, 87
 Introduction 6, 7
 IOS 85, 87
 IP 129, 135
 IPCheck Server Monitor 5 150
 IPCheck Server Monitor V5 Upgrade 15
 iPhone 10, 35, 50
 iPRTG 35, 50
 IP-SLA 80

- J -

Japanese 129, 135
 Jitter 80
 Journal 32

- K -

Key 18

- L -

Language Settings 129, 135
 LED 37
 License 7, 18, 129
 Licenses 7
 Limit User Access 31, 117
 Limits Settings 61
 Lineup 32
 Lists 37
 Live Graphs 129
 Local IP 135
 Local Probe 24, 143
 Log 32, 129, 135
 Log File 32
 Logbook 32
 Login Name 37, 45, 121, 128, 129

- M -

Mail 75
 Mail Server 75
 Main Menu 37
 Management Information Base 68
 Manual Device Creation 56
 Manual Sensor Creation 56
 Map 31
 Map Concept 31
 Maps 100
 Mean Opinion Score 80
 Memory Usage 129
 Merge Sensors 88
 Messenger 94, 123, 125
 MIB 68
 MIB Import 68
 Microsoft Exchange 75
 Microsoft SQL 77
 Microsoft Windows 71
 Mobile 50
 Monitor Bandwidth 64
 Monitor Cisco Switch 68
 Monitor Disk Share 78

Monitor Disk Space 78
 Monitor Disk Volume 78
 Monitor File 78
 Monitor Folder 78
 Monitor Hard Disk Drive 78
 Monitor Mail Server 75
 Monitor PING 64
 Monitor Port 64
 Monitor SAMBA 78
 Monitor SMB 78
 Monitor SQL Server 77
 Monitor via SNMP 68
 Monitor via WMI 71
 Monitor Web Servers 65
 Monitor Website 64
 Monitoring Bandwidth 87
 Monitoring Switch 85
 MOS 80
 MS SQL 77
 MSN Messenger 94, 123, 125
 Multi Edit 37
 Multiple Selection 37
 My Account 121
 MySQL 77

- N -

Net Send 94, 123
 NetFlow 64, 85, 87, 140
 Network Broadcast 94, 123
 Network Provider 153
 Network Sketch 100
 New User 128
 News 32, 94
 Notice 32
 Notification 31, 94, 123
 Notification Delivery 125
 Notifications 61
 Notifications Concept 32

- O -

Object 27
 OIDLIB 68
 Operating System Requirements 10
 Oracle SQL 77
 Orange Sensor 37

Order of Objects 27
 Overview of Sensor Types 64
 Own Application 151

- P -

Packet Delay Variation 80
 Packet Loss 80
 Packet Sniffer 64, 83, 87, 140
 Packet sniffing 64, 83, 140
 Paessler 18
 Pager Message 94
 Password 37, 45, 121, 128, 129
 PDF 109
 PDV 80
 Percentile Calculation 153
 PING 74
 PING Sensor 64
 Plan 32
 Play Sound 94, 123
 POP3 75
 Popup Messages 37, 45
 Port 74, 129, 135
 Port Sensor 64
 POST 65
 Post Office Protocol (POP3) 75
 Powershell 82
 Probe 21, 24, 27, 129, 135, 143
 Probe Access Key 129, 135
 Probe Administrator 135
 Probe Connection 129, 135
 Probe Management 125
 Probe Server Admin Tool 135
 Probes 30
 Product Activation 20
 Professional Edition 7, 18
 Program 82, 151
 Proxy 65
 PRTG 18, 21
 PRTG Probe Administrator 135
 PRTG Server Administrator 129
 PRTG Traffic Grapher 6 150
 PRTG Traffic Grapher V6 Upgrade 15
 PS1 82, 151
 Public Access 100, 117
 Public URL 100

- Q -

QoS 80
 Quality of Service 80
 Quick Search 37

- R -

RDP 74
 Re-Brand Web Interface 150
 Records 32
 Red Sensor 37
 Remote Desktop Protocol 74
 Remote Probe 24, 143
 Remote Probe Installer 129
 Remove PRTG 22
 Report 109
 Report Concept 31
 Reporting 31, 109
 Reports 153
 Requirements 10
 Root Group 54
 Root Group Settings 30
 Round Trip 75

- S -

SAMBA 78
 Sample configuration 10
 Scanning Interval 61
 Schedule 121
 Scheduled Report 109
 Schedules Concept 32
 Schedules Settings 61
 Schematic 100
 Search Box 37
 Secure Sockets Layer 150
 Secure User 117
 Security 117
 Sensor 56, 59, 64, 65, 68, 71, 74, 75, 77, 78, 79, 80, 82, 83, 85, 87, 88
 Sensor Chart 100
 Sensor Color 37
 Sensor Meaning 37
 Sensor Setup 54
 Sensor Status 31

Sensor Types Overview 64
 Sensors 27, 30
 Server 79
 Server Administrator 129
 Server Message Block 78
 Service Control 129, 135
 Service Level Agreement 80
 Set for All 30
 Set Probe Access Key 125
 Set Up 54
 Set Up Devices 54
 Set Up Sensor 61
 Set Up User accounts 128
 Set Up User Groups 128
 Settings 33, 54, 61, 129, 135
 Setup 16, 24, 120, 143
 sFlow 64, 85, 87, 140
 Share Disk Space Monitoring 78
 Sharing Monitoring Data 100
 Short Message Service 94, 123
 Short Message Service Delivery 125
 Show System Information 129
 Show System Settings 129
 Show Traffic Usage 140
 Simple Mail Transfer Protocol 75
 Simple Network Management Protocol 64, 68, 87
 Simple Network Management Protocol Sensor 64
 Site Information 125
 Site License 18
 SMB 78
 SMS 94, 123
 SMS Delivery 125
 SMTP 75, 123
 SMTP Delivery 125
 SMTP Relay 123
 Sniffing 64, 83
 SNMP 64, 68, 87
 SNMP Helper 68
 SNMP Library 68
 SNMP Sensor 64
 SNMP Traps 68
 Software Requirements 10
 Software Version 129
 Sound 94, 123
 Sound Notification 94, 123
 Spanish 129, 135
 SSL 150
 Static Images 121, 128

Statistic 153
Status Bar 37
Status Information 129
Stop Sensor 33
Synchronization Information 129
Syslog 94, 123
System Administration 125
System Events Log 32
System Log 94
System Requirements 10
System Settings 125
System Setup 120
System Startup Log 129
System Tray 45

- T -

Tables 31, 109
Tabs 37
Take Over Settings 30
Tasks 32, 115
Timetable 32
Timezone 121, 128
To Do 32, 115
To Dos 32, 115
ToDo Concept 32
Todos 115
Toplist 140
Traffic Sensor 68, 83
Transaction 65
Tray 35, 45
Trial 7
Trigger 123
Triggers 94

- U -

Uninstallation 22
Unlimited License 18
Unusual Detection 125
Upgrading From 15
Use Secure Connection 150
User Access Concept 31, 117
User Account 117
User Concept 31
User Defined 151
User Defined Program 82

User Interface 37, 45, 50, 117
User interfaces 35
User Login Timeout 125
User Management 31, 117
Users 31

- V -

View Activation Status 129
View System Status 129
Virtual Machine 10, 79
Virtual Server 79
Virtualization 79
VM 10, 79
Voice over IP 80
VoIP Quality 80
Volume (Disk) 78
VPN 143

- W -

Warning 32, 94
Warning Settings 61
Web browser 10
Web Interface 35, 37, 150
Web Interface Credentials 117
Web Server 65, 125, 129
Webinterface 37
Website 65
Website Settings 125
What Do I Need 10
Windows 71, 78
Windows Graphical User Interface 35, 45
Windows GUI 35, 45
Windows Live Messenger 94, 125
Windows Management Instrumentation 64, 71, 78, 82, 87
Windows Management Instrumentation Sensor 64
Windows Server 71
Windows System Tray 45
Windows-GUI 21
WMI 64, 71, 78, 82, 87
WMI Sensor 64
WMI Troubleshooting 71
WMware 79
WQL 82, 151
Write Code 151

WWW 65

- X -

xFlow 85, 87, 140

XML 151

- Y -

Yellow Sensor 37