PAESSLER
the network monitoring company

SNMP Tester
User Manual

SNMP Tester Manual

Printed: Juli 2013 in Nuremberg

Table of Contents

Part 1

Introduction

1 Introduction

Welcome to SNMP Tester, a free network tool for PRTG Network Monitor! This tool is a test program indicated for debugging SNMP activities. It supports you in finding SNMP related issues when monitoring network devices with PRTG. The present document describes the underlying concepts and application fields for the SNMP tester, as well as it explains how to use the tester in detail.

Why SNMP Tester?

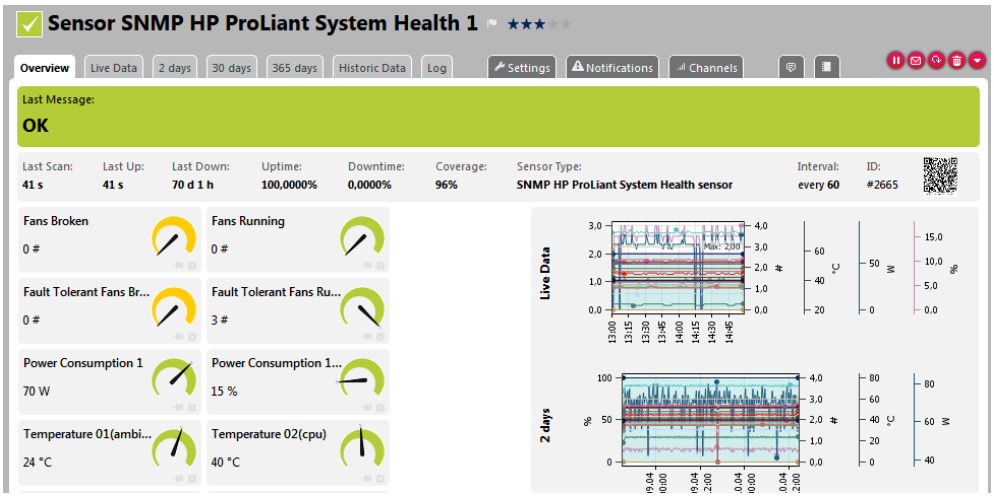
Monitoring via SNMP is the most basic method of gathering bandwidth and network usage data. However, SNMP as a base for extensive monitoring often comes not without problems. Reasons for these issues are not obvious in many cases.

The SNMP Tester is developed to support debugging steps for SNMP monitoring with PRTG. You can test various configurations to communicate with an SNMP device. Every step of this communication will be recorded to be able to investigate the functionality of your SNMP device and the corresponding SNMP settings.

1.1 About SNMP Tester

The SNMP Tester is a free network tool provided by Paessler for customers of PRTG Network Monitor. Mainly it is developed to have a tool available that enables you to debug SNMP activities down to the protocol level. The program is very useful if you encounter issues with PRTG and SNMP, especially when contacting PRTG support regarding this problems.

With the tester you can run simple SNMP requests against an SNMP supporting device in your network to debug your configuration. For this purpose, the tool tries to establish an SNMP connection with the target device—if this works, monitoring this device via SNMP will be achievable in PRTG as well.



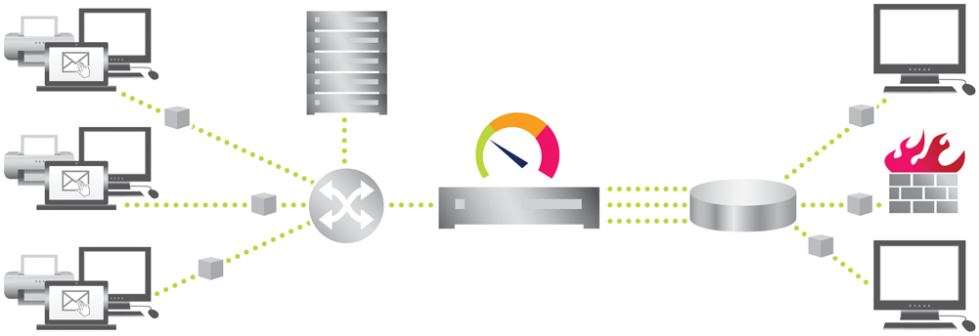
Monitoring via SNMP Works

The program is based on the SNMP technologies implemented in PRTG Network Monitor. It comes with various customizable settings so that you are able to test different configurations for SNMP monitoring.

The SNMP Tester can optionally log packets of an SNMP request into a text file. This approach supports you in finding communication and/or data problems in SNMP monitoring configurations. With the created log file, SNMP communication issues can be analyzed in more detail. In addition, you can log raw data packets for debugging purposes.

1.2 SNMP—The Simple Network Management Protocol

SNMP stands for **Simple Network Management Protocol**. Monitoring with this technology is the most basic method of gathering bandwidth and network usage data. Using SNMP, PRTG sends small data packages to devices—for example, routers, switches and servers—to query for traffic counters of each port. Furthermore, SNMP makes PRTG able to monitor other network parameters, including CPU load, disk usage, temperature and many other readings, depending on your device.



Network Monitoring via SNMP

Introduction to SNMP

The Simple Network Management Protocol (SNMP) was developed to get a standard for monitoring various devices. This was necessary because of the huge amount of these devices on the market, supplied by many different manufacturers. For monitoring, all available SNMP objects must have clear addresses to be accessible—the **OIDs** which are stored in **MIBs**. SNMP requests are sent to these addresses to retrieve the desired information.

For detailed information about SNMP, please see section **More**.

About OIDs and MIBs

In order to access the values on a network device, the managing software needs to know their addresses. These addresses are called OIDs (Object Identifiers). They are organized in a hierarchical tree structure and defined in Management Information Base (MIB) files. The nodes are defined by decimal numbers, separated by dots. A typical OID looks like this: 1.3.6.1.2.1.10.20.1.3.1; this is an example from an ISDN-MIB. With the SNMP Tester you can access these addresses directly if you provide specific OIDs.

More

PRTG Manual: Monitoring via SNMP

- http://www.paessler.com/manuals/prtg/snmp_monitoring.htm

Knowledge Base: SNMP, MIBs and OIDs — an Overview

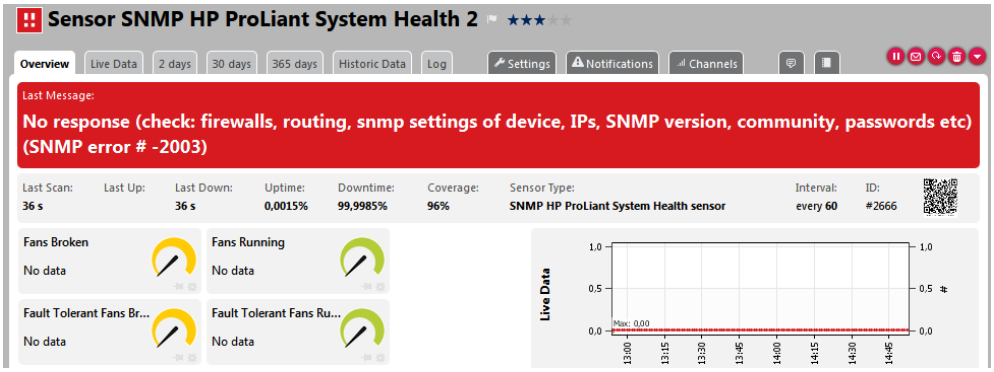
- http://www.paessler.com/knowledgebase/en/topic/653

White Paper: Quo Vadis SNMP?

- http://www.paessler.com/press/whitepapers/introducing_snmp

1.3 Monitoring SNMP Devices: Troubleshooting

Every so often customers using PRTG Network Monitor report issues when trying to monitor their systems using SNMP. In most cases, these issues result from a malfunctioning SNMP configuration or installation. The following section provides basics for monitoring via SNMP which should be checked in any case when problems with SNMP occur.



Malfunctioning SNMP Sensor

Note: Before going any deeper into troubleshooting, a good knowledge of the principles and functions of SNMP is necessary. For references, please see section **SNMP—The Simple Network Management Protocol**.

Basic Requirements

To get monitoring via SNMP to work with PRTG, and to receive any results with the SNMP Tester, please ensure the following:

- **Enable SNMP** on the target device.
- **Allow access to SNMP** for the machine running PRTG Network Monitor in the device's security settings.
- **Allow User Data Protocol (UDP) packages** to travel from the machine running PRTG to the device you want to monitor and back. If the device and PRTG are on different sides of a firewall, make sure that **UDP access to port 161** (SNMP) is allowed.
- **Important for firewall settings**: SNMP requires the use of UDP ports >1023 to the PRTG client side.
- PRTG supports SNMP V1, SNMP V2c, and SNMP V3. You have to select a version in PRTG (and the tester) which is supported by the device as well.
- **Authentication must match**: You have to provide the correct community strings (SNMP V1 and V2c), usernames (SNMP V3), and passwords (SNMP V3) in the tester respectively PRTG in order to connect to an SNMP device.

Debugging SNMP Activities

If you encounter any problems with your SNMP sensors, the first step after checking basic requirements is to debug SNMP activities. For this concern, Paessler provides the SNMP Tester. Please see the following sections of the present manual about the usage of this program.

More

We also recommend you to refer to this article for further details about troubleshooting:

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

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

Part 2

Download and Getting Started

2 Download and Getting Started

Getting the SNMP Tester started is straightforward:

- Download the ZIP file SNMP Tester v5 on http://www.paessler.com/tools/snmptester.
- Extract all files into one folder of your choice on the system where your PRTG core server is running.

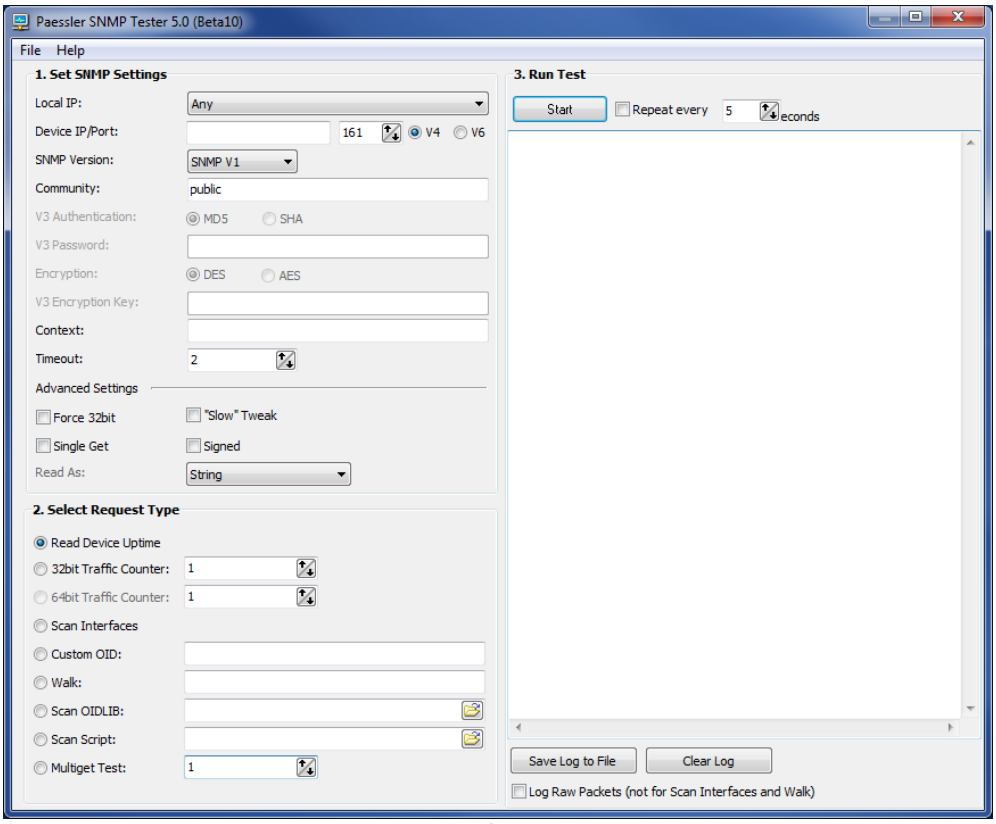
No further installation steps are required. You can launch the SNMP Tester by opening **snmptest.exe**.

Part 3

Using SNMP Tester

3 Using SNMP Tester

Launch the SNMP Tester by opening **snmptest.exe**. The main window will appear.



SNMP Tester after First Launch

General Layout

The general layout of the SNMP Tester is organized as follows:

- At the top: the global header bar containing the main menu.
- On the left: SNMP settings and request type for a test run.
- On the right: start button for a test run and log section.

Main Menu

From the main menu you can access general functions:

- **File**
  - **Exit**: Closes the SNMP Tester.
- **Help**

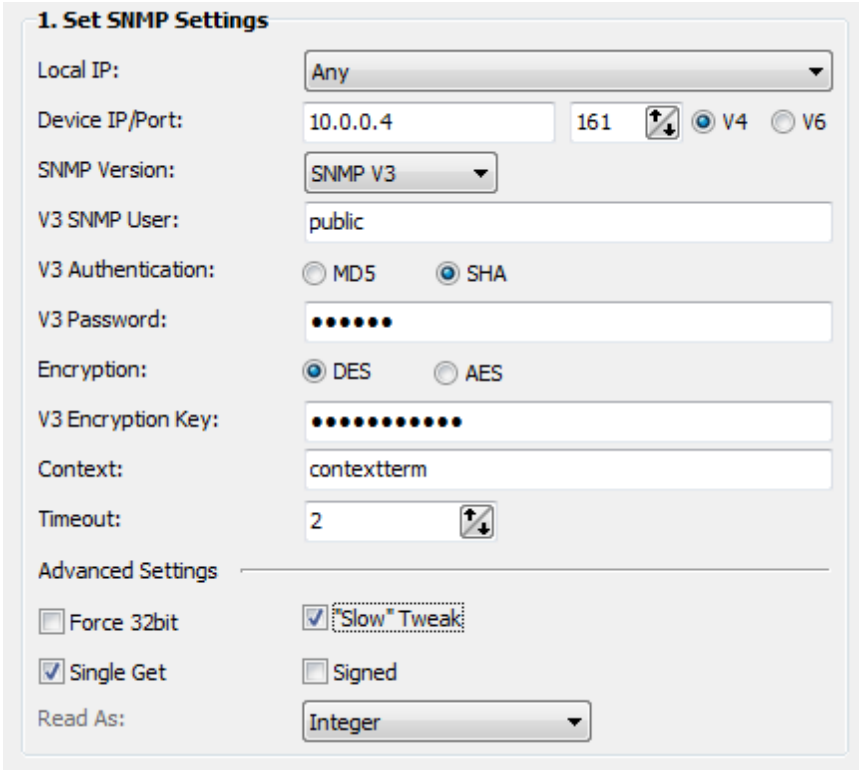
- **Online Help...**: Opens this manual.
- **About...**: Opens a popup with general information about the SNMP Tester.

How to Use

Before performing a test run, you have to set **SNMP Settings**, such as IP addresses and credentials. Furthermore, you can specify a **Request Type**, such as uptime, specific counters, and walks. After this you can **Run SNMP Tester** and analyze the log.

3.1 SNMP Settings

In this section of the SNMP Tester you can define the SNMP settings for a test run.



Settings Section — SNMP V3 Enabled

Provide the settings which you want to test in order to communicate with your SNMP device. Try several different settings for debugging SNMP issues. Check if there is any communication with the target device at all and analyze the returning data.

Set SNMP Settings

The settings you provide here are the general SNMP settings for connecting to a specific device, such as credentials and SNMP version.

- **Local IP**: In some cases—usually concerning multi-homed systems—it is necessary to select a specific local IP address for the SNMP request. Default is Any.
- **Device IP/Port**: Enter the IP address of the device you want to communicate with. Define the port used for SNMP communication. This is usually port 161. Specify whether IPv4 or IPv6 is used.
- **SNMP Version**: Select the SNMP version. Ensure that the target device supports this version! Choose between:
  - **SNMP V1**: This is the standard and most common version with limited security.
  - **SNMP V2c**: In addition to SNMP V1, 64bit counters are supported.

  - **SNMP V3**: Authentication and encryption are supported.
- **Community**: This setting is only visible for SNMP V1 and V2c. Enter the SNMP community string. A community string is similar to an ID or clear-text password, allowing access to a device's statistics.
- **Context**: If required by the configuration of the device, enter a context name.
- **Timeout**: Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the request is aborted.

SNMP V3 Specific Settings

The following configuration steps need only to be performed if SNMP v3 is enabled above. The values you provide here have to be the same as on the target device.

- **V3 SNMP User**: Provide the username for the SNMP device.
- **V3 Authentication**: Specify the authentication type. Choose between:
  - **MD5** (Message-Digest Algorithm 5)
  - **SHA** (Secure Hash Algorithm)
- **V3 Password**: Enter the password for the SNMP device.
- **Encryption**: Select the encryption type. Choose between:
  - **DES** (Data Encryption Standard)
  - **AES** (Advanced Encryption Standard)
- **V3 Encryption Key**: Enter the encryption key. If you provide an encryption key, SNMP packets will be encrypted using the algorithm chosen above.

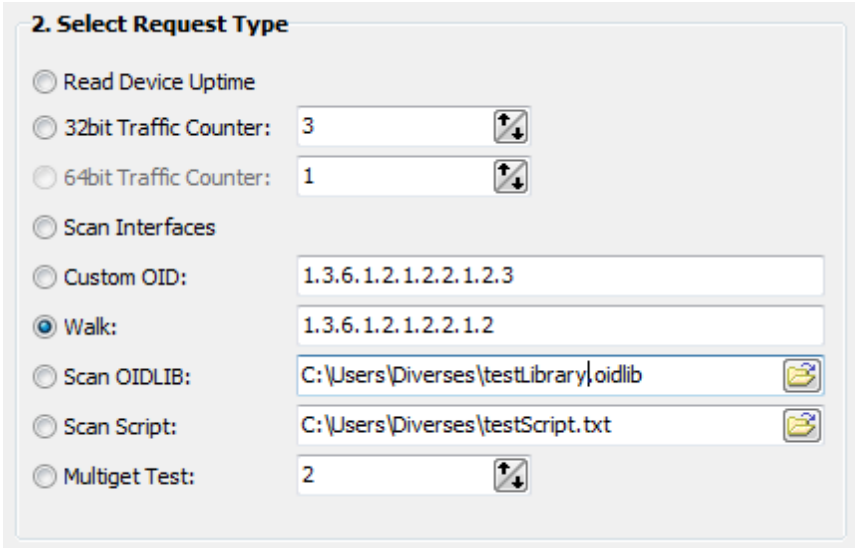
Advanced Settings

These settings allow you to test several more detailed aspects of an SNMP connection.

- **Force 32bit**: Check this option to search for 32bit counters only, even if the device reports 64bit counters. For some devices monitoring is more reliable when using 32bit counters only.
- **"Slow" Tweak**: Requests are sent less fast. Some devices might have problems with the speed requests are usually sent. Check this option to slow down requesting.
- **Single Get**: Check this option to send a single request for each SNMP value. This can be useful for older devices.
- **Signed**: Check this option to interpret returning numbers as signed.
- **Read As**: Select the format in which the returning values will be interpreted. Choose between **String**, **Integer**, and **Float**.

3.2 Request Type

In this section of the SNMP Tester you can select the request type of your test run. SNMP request types are used to describe the nature of the request.



Request Type Section

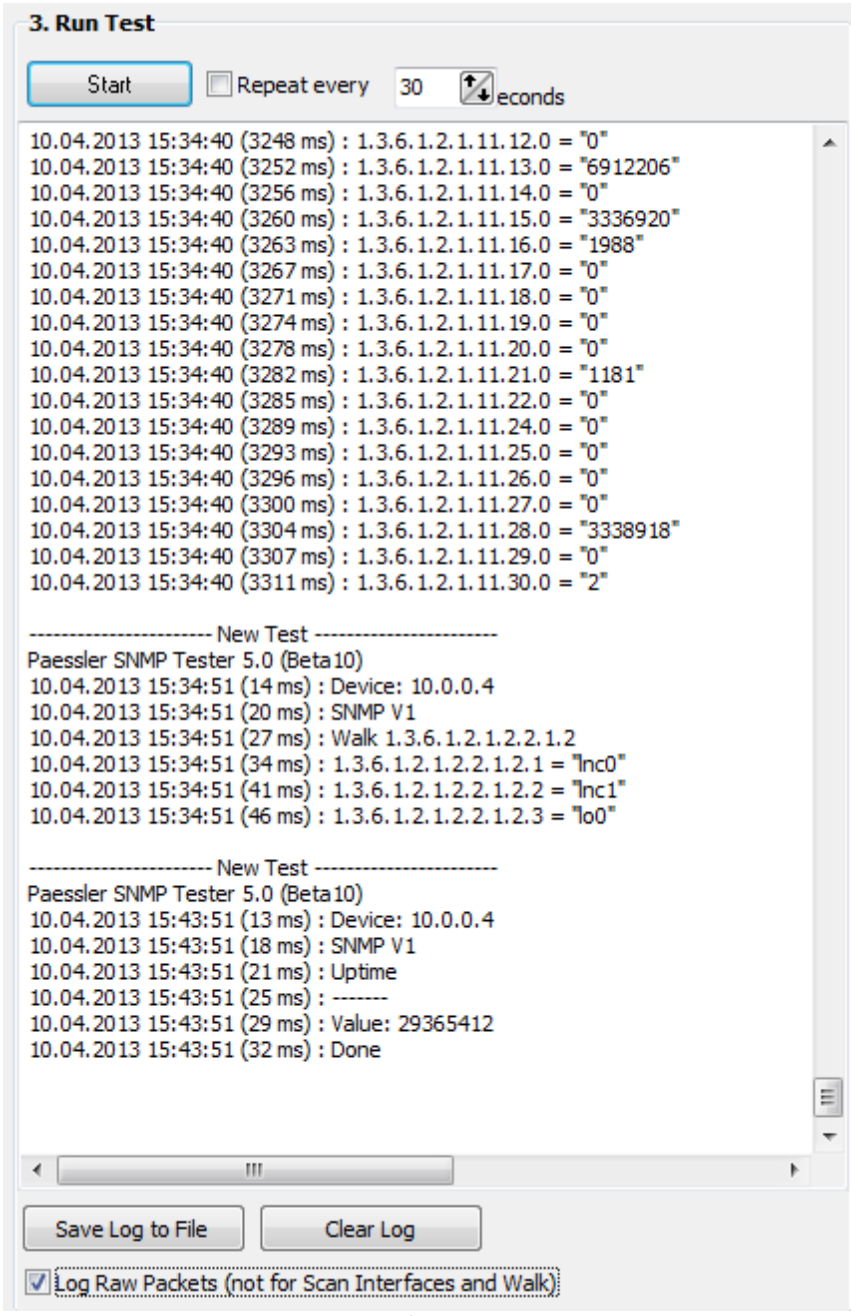
Select Request Type

- **Read Device Uptime**: Reads the standard system uptime value from the device.
- **32bit Traffic Counter**: Reads the traffic counter of a port according to the MIB-II OID. Enter an integer number to specify the interface (port).
- **64bit Traffic Counter**: The 64bit traffic counter is only available for SNMP V2c and SNMP V3. Enter an integer number to specify the interface (port).
- **Scan Interfaces**: Enumerates all interfaces (ports) of the device.
- **Custom OID**: Enter a custom OID value to access a specific OID value on the device.
- **Walk**: In general, a walk sends an SNMP request to all OIDs starting with the OID part you enter here. This retrieves a subtree of the values using SNMP getnext requests.
- **Scan OIDLIB**: Loads a Paessler SNMP Library file and checks all OIDs from this library. You can create an SNMP library by using Paessler's free MIB Importer tool.
- **Scan Script**: With a script you can test a number of OIDs without entering them individually. A script is a common text file with commands. Create such a file and provide the path to it by clicking on the folder symbol. Currently the following commands are supported (replace the brackets and included terms by the corresponding desired value):
  - get = [OID]
  - multiget = [OID],[OID],[...]
  - walk = [startOID]
  - sleep = [milliseconds]

    - **Comments**: Everything else than a command will be handled as a comment.
- **Multiget Test**: Sends multiple SNMP requests bundled into one request to the device. Enter an integer number to specify the counter.

3.3 Run SNMP Tester

In this section of the SNMP Tester you can start a test run with your individual configuration. In order to debug SNMP communication, the results in the log section show if a connection to a specific device is possible with the current settings, as well as returning values are printed if these can be read out. The resulting log can be stored for further analysis.



Run Section with Log of a Walk and Device Uptime

Run Test

Click on the **Start** button to send requests against the SNMP device according to your settings. If you want to run the test continuously, mark the checkbox in front of **Repeat every** and enter the number of seconds to define the time interval of the test run repetitions.

After starting the test run, the tester will communicate with the SNMP device. We recommend you to scan for device uptime first, later on for other values. The results will be displayed in the log section, depending on the specified request type. Check if any values are returned.

Below, click on **Save Log to File** to save the log for detailed debugging purposes. This way you are also able to send the log to Paessler support later. In the appearing popup, specify the folder where the text file containing the log will be stored.

Click on **Clear Log** to discard the scanning results.

Log Raw Packets

You can also log raw data packets to a text file. These raw binary data packets will be registered by the Net-SNMP library directly and stored on the hard disk. You can find the corresponding log file **packets.log** in the SNMP Tester folder.

This approach is a further debug option, for example, to investigate corrupted data as returned by a device.

The result can be imported to Wireshark, a network protocol analyzer, for a more detailed analysis. If username and password are known, Wireshark is also able to decode SNMP v3 in a way that you can analyze these packets.

Note: You cannot use this log option for the request types Scan Interfaces and Walk.

Part 4

Notes

4 Notes

SNMP Tester is a freeware program provided for Paessler customers. It is mainly developed as a diagnostic tool for users of PRTG Network Monitor. Please note that Paessler does not provide support for this free program.

However, when contacting Paessler's support regarding SNMP sensor issues, then it is very useful to send log files created by the SNMP Tester—using the configuration as set up in PRTG—with your support request.