In order to improve the design or performance characteristics, MG-SOFT reserves the right to make changes in this document or in the software without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MG-SOFT Corporation. Permission to print one copy is hereby granted if your only means of access is electronic.

Depending on your license, certain functions described in this document may not be available in the version of the software that you are currently using.

Screenshots used in this document may slightly differ from those on your display.

MG-SOFT may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright © 2007-2018 MG-SOFT Corporation. All rights reserved.
TABLE OF CONTENTS

1 Introduction ......................................................................................................... 6
  1.1 Product Description ..................................................................................... 6

2 Installing SNMP Proxy Agent ............................................................................. 7
  2.1 System Requirements .................................................................................... 7
  2.1.1 Windows Operating System ........................................................................ 7
  2.1.2 Linux Operating System ............................................................................. 7
  2.2 Installing SNMP Proxy Agent for Windows .................................................... 8
    2.2.1 Migration from Previous Version Running on 32-bit Windows ..................... 8
  2.3 Installing SNMP Proxy Agent for Linux ......................................................... 9

3 Starting SNMP Proxy Agent ............................................................................. 10
  3.1 Windows Operating System .......................................................................... 10
    3.1.1 Starting SNMP Proxy Agent Configuration Utility .......................................... 10
    3.1.2 Starting SNMP Proxy Agent Service ............................................................. 11
  3.2 Linux Operating System ............................................................................... 11
    3.2.1 Starting SNMP Proxy Agent Configuration Utility on Linux ......................... 11
    3.2.2 Starting SNMP Proxy Agent Service on Linux ............................................ 12

4 Applying License Key .................................................................................... 13

5 Configuring SNMP Proxy Agent ..................................................................... 15
  5.1 About IP-Based and Port-Based Proxying .................................................... 15
    5.1.1 IP-Based Proxying ...................................................................................... 16
    5.1.2 Port-Based Proxying .................................................................................. 17
  5.2 Configuring SNMP Profiles ......................................................................... 19
    5.2.1 New/Edit SNMP Profile Dialog Box ............................................................ 19
  5.3 Configuring Proxy Forward Rules for SNMP Querying Operations ............... 21
    5.3.1 Creating a SNMP Query Forward Rule ......................................................... 22
    5.3.2 Creating Multiple SNMP Query Forward Rules .......................................... 25
      Creating Multiple SNMP Query Forward Rules for IP-Based Proxying ............ 25
      Creating Multiple SNMP Query Forward Rules for Port-Based Proxying .......... 30
    5.3.3 Testing SNMP Query Forward Rules ......................................................... 33
    5.3.4 Viewing Activity Status of Rules ............................................................... 34
    5.3.5 Enabling/Disabling SNMP Query Forward Rules ....................................... 34
    5.3.6 Deleting SNMP Query Forward Rules ....................................................... 36
  5.4 Configuring Proxy Forward Rules for SNMP Notifications ......................... 37
    5.4.1 Adding a SNMP Notification Forward Rule ............................................... 37
    5.4.2 Adding Multiple SNMP Notification Forward Rules .................................... 40
    5.4.3 Testing SNMP Notification Forward Rules ............................................... 43
    5.4.4 Enabling/Disabling SNMP Notification Forward Rules ............................. 44
    5.4.5 Deleting SNMP Notification Forward Rules .............................................. 45

6 Filtering Rules ............................................................................................... 46

7 Managing Local Network Interfaces and IP Addresses .................................. 48

8 Exporting and Importing Configuration ........................................................ 50
  8.1 Exporting Configuration to .ini File ............................................................. 50
8.2 Importing Configuration from .ini File .................................................................51
# TABLE OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Starting SNMP Proxy Agent Configurator in Windows 10</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>Starting SNMP Proxy Agent Service from Proxy Agent Configurator</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>Starting SNMP Proxy Agent Configurator on Ubuntu Linux</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>Selecting the license.key file</td>
<td>13</td>
</tr>
<tr>
<td>5</td>
<td>Applying the license.key file - restarting SNMP Proxy Agent</td>
<td>14</td>
</tr>
<tr>
<td>6</td>
<td>New SNMP Profile dialog box - SNMPv3 settings</td>
<td>20</td>
</tr>
<tr>
<td>7</td>
<td>Password For Authentication/Privacy Protocol dialog box</td>
<td>21</td>
</tr>
<tr>
<td>8</td>
<td>Adding a new SNMP query forward rule</td>
<td>22</td>
</tr>
<tr>
<td>9</td>
<td>New SNMP Proxy Rule dialog box</td>
<td>22</td>
</tr>
<tr>
<td>10</td>
<td>A new SNMP query forwarding rule in the Proxy Agent Configurator</td>
<td>24</td>
</tr>
<tr>
<td>11</td>
<td>Adding multiple SNMP query forward rules</td>
<td>25</td>
</tr>
<tr>
<td>12</td>
<td>New Multiple SNMP Query Rules dialog box (IPv4 listening address range)</td>
<td>26</td>
</tr>
<tr>
<td>13</td>
<td>New Multiple SNMP Query Rules dialog box (IPv6 listening address range)</td>
<td>27</td>
</tr>
<tr>
<td>14</td>
<td>Multiple new forward rules created for an IP-based proxy scenario</td>
<td>29</td>
</tr>
<tr>
<td>15</td>
<td>Multiple new forward rules created for a port-based proxy scenario</td>
<td>30</td>
</tr>
<tr>
<td>16</td>
<td>A list of enabled forwarding rules, where some of them are active and some idle</td>
<td>34</td>
</tr>
<tr>
<td>17</td>
<td>Disabling forwarding rules</td>
<td>35</td>
</tr>
<tr>
<td>18</td>
<td>A list of forwarding rules, where some of them are disabled</td>
<td>35</td>
</tr>
<tr>
<td>19</td>
<td>Adding a new SNMP notification forward rule</td>
<td>38</td>
</tr>
<tr>
<td>20</td>
<td>Configuring a new forward rule for SNMP notifications</td>
<td>38</td>
</tr>
<tr>
<td>21</td>
<td>A list of forwarding rules, where some of them are disabled</td>
<td>34</td>
</tr>
<tr>
<td>22</td>
<td>Adding a new SNMP notification forward rule</td>
<td>38</td>
</tr>
<tr>
<td>23</td>
<td>Multiple new notification forward rules</td>
<td>38</td>
</tr>
<tr>
<td>24</td>
<td>Filtering rules in the SNMP query list</td>
<td>40</td>
</tr>
<tr>
<td>25</td>
<td>Network Interface Manager dialog box</td>
<td>40</td>
</tr>
<tr>
<td>26</td>
<td>Adding a new IPv4 address</td>
<td>40</td>
</tr>
<tr>
<td>27</td>
<td>Adding a new IPv6 address</td>
<td>40</td>
</tr>
<tr>
<td>28</td>
<td>Multiple notification forward rules in the SNMP Notification tab</td>
<td>41</td>
</tr>
<tr>
<td>29</td>
<td>Deleting selected SNMP notification forward rules</td>
<td>41</td>
</tr>
<tr>
<td>30</td>
<td>Setting filter options</td>
<td>41</td>
</tr>
<tr>
<td>31</td>
<td>Filtering rules in the SNMP query list</td>
<td>47</td>
</tr>
<tr>
<td>32</td>
<td>Network Interface Manager dialog box</td>
<td>48</td>
</tr>
<tr>
<td>33</td>
<td>Adding a new IPv4 address</td>
<td>49</td>
</tr>
<tr>
<td>34</td>
<td>Adding a new IPv6 address</td>
<td>49</td>
</tr>
<tr>
<td>35</td>
<td>Selecting the Export Configuration command</td>
<td>50</td>
</tr>
<tr>
<td>36</td>
<td>Exporting configuration to .ini file</td>
<td>51</td>
</tr>
<tr>
<td>37</td>
<td>Selecting the Import Configuration command</td>
<td>51</td>
</tr>
<tr>
<td>38</td>
<td>Importing configuration from .ini file</td>
<td>51</td>
</tr>
<tr>
<td>39</td>
<td>Selecting the import method</td>
<td>52</td>
</tr>
<tr>
<td>40</td>
<td>Replacing the missing interface(s) while importing a configuration</td>
<td>53</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

This user manual contains instructions for completing basic operations in MG-SOFT SNMP Proxy Agent application. Majority of instructions are provided on a step-by-step basis, which should help the reader start using the software effectively.

It is supposed that you are familiar with using a graphical computer environment, such as choosing a main menu command or a pop-up command, selecting items, closing windows and dialog boxes, etc.

All program commands in this manual are written in bold and italic letters. Individual commands in combinations of commands are separated by the “/” character.

All hyperlinks in text are marked with blue colored letters, e.g., Configuring SNMP Proxy Agent. Clicking a hyperlink opens the page which the hyperlink points to.

The content of this guide is listed in the Table of Contents.

1.1 Product Description

MG-SOFT SNMP Proxy Agent software application can receive, optionally translate, and forward any valid SNMP messages to final targets, as well as receive, optionally translate, and send responses to these messages back to the message originators. In addition to SNMP Get, GetNext, GetBulk and Set requests, it can also forward and translate SNMP Trap and Inform messages. The software supports SNMPv1, SNMPv2c and SNMPv3 protocol versions and can translate SNMP messages between different versions of the protocol. It supports SNMP over IPv4 and IPv6 and can switch between these transport protocols while proxying SNMP messages. Furthermore, the software supports the so-called port-based proxying and IP-based proxying scenario. The former means that Proxy Agent listens for incoming SNMP packets on different ports on (typically) one IP address, while the latter means that Proxy Agent listens on a range of different IP addresses. In both cases, it forwards received SNMP messages to end destinations and received responses in the opposite direction, automatically performing the basic network address translation (NAT) where needed. All this can make MG-SOFT SNMP Proxy Agent fully transparent to the network management (NMS) applications and managed SNMP devices, which are not aware that the actual management is conducted through an SNMP proxy application.

A typical SNMP proxy agent application is located between one or more network management (NMS) applications and the managed SNMP devices (agents), for example, when NMS and agents do not support the same version of the SNMP protocol or when they are not in the same (sub)network.

The main components of the software are the proxy service and the management console. The SNMP Proxy Agent service runs as a system service application and receives, translates and forwards SNMP messages. The SNMP Proxy Agent Configurator is a management console that provides a graphical user interface (GUI) for configuring the proxy rules and controlling the service.

MG-SOFT SNMP Proxy Agent is available for 64-bit MS Windows and Linux operating systems (see the System Requirements section).
2 INSTALLING SNMP PROXY AGENT

2.1 System Requirements

MG-SOFT SNMP Proxy Agent is available for 64-bit Microsoft Windows operating systems and 64-bit Linux operating systems (Intel x86_64 architecture).

In order to install and use the software, your computer has to meet the following system requirements:

2.1.1 Windows Operating System

MG-SOFT SNMP Proxy Agent 2019 for Windows successfully runs on the following 64-bit Microsoft Windows operating systems:

- Windows Server 2008 R2,
- Windows 7,
- Windows Server 2012,
- Windows 8.x,
- Windows 10,

**Note:** Starting with 2019 (V5.0) release, MG-SOFT SNMP Proxy Agent software is available only in 64-bit build for x64 Microsoft Windows operating systems.

Additionally, **administrative user privileges** are required to successfully install SNMP Proxy Agent.

2.1.2 Linux Operating System

MG-SOFT SNMP Proxy Agent 2019 for Linux successfully runs on the following 64-bit Linux operating systems (Intel x86_64 architecture):

- RHEL / CentOS 6.6 or newer
- Debian 8 or newer
- Ubuntu 14.04, 16.04, 18.04, 18.10 or newer

For the most recent information about the supported distributions, please refer to the release notes (READ_ME.TXT) of the current software release.

Additionally, **root user privileges** are required to successfully install SNMP Proxy Agent.
2.2 Installing SNMP Proxy Agent for Windows

**Note:** Before installing the software, please make sure your computer meets the system requirements specified in the System Requirements section.

1. Use Windows Explorer to locate the MG-SOFT SNMP Proxy Agent software distribution (zip archive or setup file) that you have downloaded from MG-SOFT’s Website or obtained on a removable medium.

2. The software distribution contains the installer for 64-bit (x86_64) build of MG-SOFT SNMP Proxy Agent 2019. To start the SNMP Proxy Agent installation wizard on a supported 64-bit Windows operating system, run the installer executable (**setup-64.exe**).

3. Follow the installation guidelines on screen to complete the software installation. When prompted for the license, point the dialog box to the `license.key` file you have received from MG-SOFT, in order for the installer to apply the license to be used with the installed software.

   **Tip:** You can install the software also without providing a `license.key` file and apply the license later, as described in the Applying License Key section.

Once the installation is complete, you can start SNMP Proxy Agent program.

2.2.1 Migration from Previous Version Running on 32-bit Windows

MG-SOFT SNMP Proxy Agent 2019 and newer is available **only in 64-bit build (x64)**.

In case you are running a previous version of SNMP Agent Simulator on a 32-bit version of Windows, upgrade to version 2019 or newer on the same system is not possible. Instead, you can install version 2019 (or newer) on another, supported machine (see System Requirements) and transfer your existing proxy configuration(s) from old to new machine, as described in this section.

1. Install a fresh copy of SNMP Proxy Agent 2019 (or newer) on one of the supported 64-bit Windows operating systems. For installation instructions, please refer to Installing SNMP Proxy Agent for Windows section.

2. On the old machine, export the proxy configuration (forwarding rules and SNMP profiles), as described in the Exporting Configuration to .ini File section.

3. Copy the exported .ini file from the old to the new machine (e.g., to a temporary folder).

4. On the new machine, import configuration from the .ini file as described in the Importing Configuration section.
2.3 Installing SNMP Proxy Agent for Linux

**Note:** Before installing the software, please make sure your computer meets the system requirements specified in the System Requirements section.

Before the installation, please close all running MG-SOFT applications and uninstall any previous version of MG-SOFT SNMP Proxy Agent.

The software comes in two different distribution packages (rpm and deb). The complete installation procedure involves installing two components: MG-SOFT SNMP Trap daemon (mgtrapd) and MG-SOFT MIB Browser (mgSnmpProxy). Depending on your Linux distribution, run one of the following commands in a Terminal window to install the software:

a) On a 64-bit (x86_64) Linux distribution with the RPM package manager (e.g., RHEL, CentOS, etc), install the following RPM packages:

```
# rpm -ivh mgtrapd-X.X-X.x86_64.rpm
# rpm -ivh mgSnmpProxy_2019-X.X-X.x86_64.rpm
```

b) On a 64-bit (x86_64/amd64) Linux distribution with the DPKG package manager (e.g., Debian, Ubuntu, etc.), install the following DEB packages:

```
# dpkg -i mgtrapd_X.X-X_x86_64.deb
# dpkg -i mgSnmpProxy-2019_X.X-X_x86_64.deb
```

Where X.X-X is the version of the software included in the tarball.

If you have KDE or GNOME desktop environment installed on your machine, the installation will add an entry to the K Menu or Gnome Menu, respectively. Once the installation is complete, you can Start SNMP Proxy Agent.
3 STARTING SNMP PROXY AGENT

3.1 Windows Operating System

3.1.1 Starting SNMP Proxy Agent Configuration Utility

1. To start the MG-SOFT SNMP Proxy Agent configuration utility, select the SNMP Proxy Agent Configurator entry from the Windows Start menu (Figure 1).

![Figure 1: Starting SNMP Proxy Agent Configurator in Windows 10](image)

2. As the program starts, the MG-SOFT SNMP Proxy Agent splash screen appears, displaying the company name and announcing the program itself.

3. The SNMP Proxy Agent Configurator window will appear (Figure 2).
3.1.2 Starting SNMP Proxy Agent Service

By default, SNMP Proxy Agent Service is started automatically by the system. Should you need to start it manually, proceed as follows:

1. Select the **Service / Start** command from the main menu in SNMP Proxy Agent Configurator (Figure 2).

2. Depending on your operating system and user privileges, you may be prompted with a dialog to enter the administrator password or to permit the service starting operation. If prompted, enter the administrator password or permit the operation.

3. SNMP Proxy Agent Configurator will automatically connect to the SNMP Proxy Agent Service.

3.2 Linux Operating System

3.2.1 Starting SNMP Proxy Agent Configuration Utility on Linux

1. Start the SNMP Proxy Agent Configurator by selecting the **SNMP Proxy** entry from the system launch menu:
   - In modern Linux desktop environments that feature a built-in search facility (GNOME 3+, KDE 4+, Unity,...), search for **SNMP Proxy** application by using the search tool and select the **SNMP Proxy** icon to start the application (Figure 3).
   - In Linux desktop environments without a search tool, click the **Applications** entry in launch menu and select the **MG-SOFT SNMP proxy Agent / SNMP Proxy** command.
2. As the program starts, the MG-SOFT SNMP Proxy Agent splash screen appears, displaying the company name and announcing the program itself.

3. The SNMP Proxy Agent Configurator window appears.

### 3.2.2 Starting SNMP Proxy Agent Service on Linux

By default, SNMP Proxy Agent Service (`mgsnmpproxyd`) is started automatically by the system. Should you need to start it manually, proceed as follows:

- Select the **Service / Start** command from the main menu in SNMP Proxy Agent Configurator (Figure 2).

  or

- Run the following command in a Terminal window (as root):
  ```
  # /etc/init.d/mgsnmpproxyd start
  ```

  Or, on recent Linux distributions with systemd service manager:
  ```
  # systemctl start mgsnmpproxyd
  ```
4 APPLYING LICENSE KEY

Without a valid `license.key` file in place SNMP Proxy Agent will operate in restricted mode. To apply a `license.key` file after the software has been installed, proceed as follows:

1. Select the **Help / Apply License** command from the main menu.
2. The empty Apply License dialog box (Figure 5) appears. Click the **Select** button in the Apply License dialog box to display the Select License dialog box (Figure 4).

![Figure 4: Selecting the license.key file](image)

3. Navigate to the drive and folder containing your `license.key` file for MG-SOFT SNMP Proxy Agent. Select the `license.key` file and click the **Open** button (Figure 4).

![Figure 5: Applying the license.key file](image)

4. Click the **Apply** button in the Apply License dialog box (Figure 5). The software will copy the specified `license.key` file to the proper location in order for SNMP Proxy Agent to read it and unlock its features accordingly (after a restart).
5. Click the **Yes** option in the dialog box that prompts you to restart SNMP Proxy Agent. Both parts of the application (SNMP Proxy Agent GUI and service) will be restarted. Allow restart if you are prompted for consent by the operating system during this process. After restart, the selected license should be applied and you can start using the software.

**Tip:** You can check if the license has been properly applied by verifying if the About SNMP Proxy Agent dialog box (accessible via the **Help / About** command) displays your license details correctly.
5 CONFIGURING SNMP PROXY AGENT

5.1 About IP-Based and Port-Based Proxying

MG-SOFT SNMP Proxy Agent can be configured in different ways. There are two main proxy configurations/scenarios:

- **IP-based proxying:**
  In this scenario, SNMP Proxy Agent listens on a number of different IP addresses for incoming SNMP requests (e.g., sent by a NMS). These IP addresses are from a certain range (e.g., IP range A) and are created locally by SNMP Proxy Agent. Actual managed devices behind the Proxy Agent have different IP addresses (e.g., IP range B). Proxy Agent performs basic network address translation (NAT), i.e., one-to-one translation of addresses between IP range A and IP range B. Typically, SNMP requests received on each IP address from range A will be forwarded to a different target device from IP range B, and responses from a target device will be sent back from the respective listening IP address (range A) to the request originator (e.g., a NMS). For illustration, please refer to the IP-Based Proxying diagrams.

  To configure SNMP Proxy Agent for this scenario, create one or more query forwarding rules, where each rule will have a different receive IP address (these IP addresses can be created by the SNMP Proxy Agent) and same receive port (e.g., 161). Each rule will have a different forward IP address. Rules can also have different receive and forward SNMP profiles, e.g., to translate SNMP messages between different version of the protocol (e.g., SNMPv1<->SNMPv3). Additionally, to enable proxying SNMP Trap and Inform notifications, create one notification forwarding rule for each NMS that will receive SNMP notifications sent by proxied devices.

- **Port-based proxying:**
  In this scenario, SNMP Proxy Agent listens on a number of different ports and a specific IP address or on all local IP addresses (Any) for incoming SNMP requests (e.g., sent by a NMS). Typically, SNMP requests received on each port will be forwarded to a different target device, and responses from a target will be sent back from the respective receive port to the request originator (e.g., a NMS). For illustration, please refer to the Port-Based Proxying diagrams.

  To configure SNMP Proxy Agent for this scenario, create one or more query forwarding rules, where each rule will have a different receive port and same IP address (either a specific one or Any). Each rule will have a different forward IP address. Rules can also have different receive and forward SNMP profiles, e.g., to translate SNMP messages between different version of the protocol. Additionally, to enable forwarding SNMP Trap and Inform notifications, create one notification forwarding rule for each NMS that will receive SNMP notifications sent by proxied devices.

There can be also combinations of the above scenarios. In all cases, there will be the same number of SNMP query forward rules as there are managed devices behind the Proxy Agent.
5.1.1 IP-Based Proxying

The following diagrams show an example of SNMP Proxy Agent configuration and SNMP message flow in IP-based proxying scenario.

**IP-based proxying - SNMP Requests**

**IP-based proxying - SNMP Responses**
5.1.2 Port-Based Proxying

The following diagrams show an example of Proxy Agent configuration and SNMP message flow in port-based proxying scenario.
Port-based proxying - SNMP Responses

```
[Diagram showing Port-based proxying - SNMP Responses]
```

Port-based proxying - SNMP Traps

```
[Diagram showing Port-based proxying - SNMP Traps]
```
5.2 Configuring SNMP Profiles

A SNMP profile contains SNMP protocol settings (SNMP version, community names or SNMPv3 user settings) that are used by SNMP Proxy Agent for receiving and sending SNMP messages. One can configure many different SNMP profiles in the SNMP Proxy Agent Configurator and assign them to forwarding rules.

To start configuring SNMP profiles, select the **Edit / SNMP Profiles** command from the main menu or click the **SNMP Profiles** toolbar button. The SNMP Profiles dialog box appears (Figure 7).

![Figure 7: SNMP profile management dialog box](image)

- To create a new SNMP profile, click the **New** button and the **New/Edit SNMP Profile** dialog box will appear.
- To remove an existing profile, select it on the list and click the **Delete** button.
- To edit an existing profile, select it on the list and click the **Edit** button and the **New/Edit SNMP Profile** dialog box will appear.
- To display only profiles that use a particular protocol version (SNMPv1, SNMPv2c, SNMPv3) or that are in use by rules or disabled, select the respective option(s) in the **Filter** frame in the SNMP Profiles dialog box.

### 5.2.1 New/Edit SNMP Profile Dialog Box

1. In the **Profile name** input line in the New/Edit SNMP Profile dialog box, enter the name of the SNMP profile.
2. Choose the **SNMP version** that will be supported by the simulated agent(s) by selecting the corresponding radio button.
3. If you have selected the **SNMPv1** or **SNMPv2c** protocol version, check the **Read Community checkbox** and into the accompanying input line enter the community name used for SNMP querying operations (SNMP Get, GetNext, GetBulk). To accept SNMP query messages with any community string (Receive profile) or to disable translating community string (Forward profile), leave the **Read community** checkbox unchecked.
4. If you have selected the SNMPv1 or SNMPv2c protocol version, check the Write Community checkbox and into the accompanying input line enter the community name used for SNMP Set requests. To accept SNMP Set messages with any community string (Receive profile) or to disable translating community string in outgoing SNMP Set messages (Forward profile), leave the Write community checkbox unchecked.

5. If you have selected the SNMPv3 protocol version, specify the following parameters:
   - Enter the name of the SNMPv3 USM user into the Security user name input line.
   - Enter the SNMPv3 context name into the Context name input line.
   - Select the SNMPv3 authentication protocol from the Authentication dropdown list and click the Change Password button next to it. The Password For Authentication Protocol dialog box appears (Figure 9).
Enter the authentication password into the **Password** and the **Password confirmation** input lines and click the **OK** button.

**Tip:** To see the entered characters, check the **Show typing** checkbox.

Select the SNMPv3 privacy protocol from the **Privacy** drop-down list and click the **Change Password** button next to it. The Password For Privacy Protocol dialog box appears, which has the same appearance as the Password For Authentication Protocol dialog box (Figure 9).

Enter the privacy password into the **Password** and the **Password confirmation** input lines and click the **OK** button to close the Password For Privacy Protocol dialog box.

**Tip:** To see the entered characters, check the **Show typing** checkbox.

6. Click the **OK** button at the bottom of the New/Edit SNMP Profile dialog box to create a new SNMP profile and close the dialog box.

### 5.3 Configuring Proxy Forward Rules for SNMP Querying Operations

This section describes how to add, configure and delete rules for forwarding SNMP requests (SNMP Get, GetNext, GetBulk, and Set requests). A forwarding rule is a configuration item that determines the IP address and port on which SNMP Proxy Agent listens for incoming SNMP requests, the target address and port which SNMP requests are forwarded to, as well as the SNMP protocol settings used for receiving and forwarding SNMP messages (the latter two control translation of SNMP messages between different versions of the protocol).

The software lets you configure multiple proxy forwarding rules to enable managing multiple devices through the proxy.

Every rule for forwarding SNMP requests must have a unique combination of receive IP address and receive port. SNMP Proxy Agent can be configured to either listen on a specific port on all (any) local network interfaces, or it can bind to a specific network interface and listen on an IP address and port specified by a user. A user can either select an IP address that already exists on the given interface or enter a new IP address, which will be created by the SNMP Proxy Agent and added to the system.

The next two sections describe how to create one SNMP query forwarding rule and how to create multiple SNMP query forwarding rules at a time (for IP-based and port-based proxying scenario). Then, the methods of testing, enabling and disabling
forwarding rules are explained. Finally, the procedure of deleting forwarding rules is described.

5.3.1 Creating a SNMP Query Forward Rule

1. In the SNMP Proxy Agent Configurator main window, select the **SNMP Query** tab.
2. Select the **Rule / New Rule** command from the main menu (Figure 10) or right-click inside the SNMP Query list and select the **New Rule** pop-up command.

![Figure 10: Adding a new SNMP query forward rule](image)

3. The New SNMP Query Proxy Rule dialog box appears (Figure 11).

![Figure 11: New SNMP Proxy Rule dialog box](image)
4. The **Receive** section of this dialog box lets you specify a network interface, IP address, subnet, port, and SNMP profile used by the SNMP Proxy Agent to listen for incoming SNMP requests, as follows:

- In the **Network interface** drop-down list, select the network interface the software will bind to when listening for SNMP requests. If you select the **Any** entry in this drop-down list, the software will listen on all (any) interfaces on the machine.

  **Note:** The **Network interface** drop-down list contains the currently connected Ethernet and Wi-Fi network interface controllers on the computer where the SNMP Proxy Agent runs. If you select an interface that is later disabled or removed from the system, the corresponding proxy rule will fail with the **Specified interface not available** message. To solve the problem, you need to select a valid interface in the **Network interface** drop-down list.

- In the **IP address** drop-down list, specify the IPv4 or IPv6 address the software will listen to for SNMP requests:
  - If you have selected a specific interface in the **Network interface** drop-down list, then you can select an IPv4 or IPv6 address that exists on the given interface or enter a new IPv4 or IPv6 address. If the entered IP address does not exist, it will be added to the system.
  - If you have selected the **Any** entry in the **Network interface** drop-down list, then you can select **0.0.0.0 (Any IPv4)** or **:: (Any IPv6)** address from this drop-down list to listen on all (any) existing local IPv4 or IPv6 addresses, respectively.

- If you have selected an IPv4 address other than **0.0.0.0** in the **IP address** drop-down list, the subnet mask of this IP address is displayed in the **Subnet mask** drop-down list by default. To use a different subnet mask, e.g., for an IP address you are creating, enter it into the **Subnet mask** drop-down list.

- Into the **Port** drop-down list, enter the UDP port number on which the SNMP Proxy Agent will listen for incoming SNMP requests (SNMP Get, GetNext, GetBulk (if applicable), Set).

  **Note:** the combination of IP address and port value must be unique in every SNMP query proxy rule.

- In the **SNMP profile** drop-down list, select the SNMP profile, whose settings the incoming SNMP requests must match in order to be forwarded by the given rule.

  **Tip:** To create a new SNMP profile, select the **<New SNMP profile...>** entry from the **Receive profile** drop-down list and configure its properties, as described in the **New/Edit SNMP Profile Dialog Box** section.

5. The **Forward** section of the New SNMP Proxy Rule dialog box lets you specify a forwarding destination (e.g., a managed device) and SNMP protocol settings used for forwarding SNMP requests to it, as follows:
- Into the **IP address** input line, enter the IP address or the fully qualified domain name (e.g., `myserver.mydomain.com`), which the SNMP requests will be forwarded to.

- Into the **Port** input line, enter the UDP port number, which the SNMP requests will be forwarded to.

- In the **SNMP profile** drop-down menu, select the SNMP profile to be used for forwarding SNMP requests. If the Receive and Forward profiles are different, all incoming SNMP requests will be translated to match the Forward profile's SNMP protocol settings (i.e., SNMP version, community name(s) or SNMPv3 settings) and then forwarded to the target address. Similarly, all SNMP Response messages received from the target address will be translated back to the original SNMP settings specified in the Receive SNMP profile, before being sent back to the request originator.

  *Tip:* To create a new SNMP profile, select the `<New SNMP profile...>` entry from the **Forward profile** drop-down list and configure its properties, as described in the New/Edit SNMP Profile Dialog Box

- Into the **Timeout** input line, enter the timeout value in seconds for forwarding SNMP requests.

- Into the **Retransmits** input line, enter a number that designates how many times the requests will be retransmitted after the first timeout.

6. Into the **Comment** input line, optionally enter a short comment, e.g., describing the rule or its target.

7. Click the **OK** button to close the New Forward Rule dialog box and create the new forwarding rule - a new line in the SNMP Query list (Figure 12).

Repeat the above steps to configure additional rules for forwarding SNMP requests. Alternatively, you can create multiple new rules at the same time, as described in the next section.
5.3.2 Creating Multiple SNMP Query Forward Rules

This section describes how to quickly create a number of rules for forwarding SNMP requests in **IP-based proxying** and **port-based proxying** scenario. For more information about these scenarios, refer to the About IP-Based and Port-Based Proxying section.

In both cases, the number of SNMP query forward rules should match the number of managed devices behind the proxy.

Creating Multiple SNMP Query Forward Rules for IP-Based Proxying

The **IP-based proxying** involves creating a range of IP addresses and accompanying query forwarding rules that will listen for SNMP requests on these IP addresses.

1. In the SNMP Proxy Agent Configurator main window, select the **SNMP Query** tab.
2. Select the **Rule / New Multiple Rules** command from the main menu (Figure 13) or right-click inside the SNMP Query list and select the **New Multiple Rules** pop-up command.

3. The New Multiple SNMP Query Rules dialog box appears (Figure 14).
4. Into the **Number of rules** input line in the General section of the dialog box, enter the number of SNMP query forwarding rules you would like to create.

5. The **Receive** section of this dialog box lets you specify a network interface, IP address(es), subnet, port(s), and SNMP profile used by the SNMP Proxy Agent to listen for incoming SNMP requests, as follows:
   - In the **Network interface** drop-down list, select a specific network interface the software will bind to when listening for SNMP requests. Do not select the **Any** entry.

   **Note:** The **Network interface** drop-down list contains the currently connected Ethernet and Wi-Fi network interface controllers on the computer where the SNMP Proxy Agent runs. If you select an interface that is later disabled or removed from the system, the corresponding proxy rules will fail with the **Specified interface not available** error. To solve the problem, select a valid interface in the **Network interface** drop-down list.

**Using IPv4 address range**

- Into the **IP address** drop-down list enter the first IPv4 address of the range you want to create. If IP addresses from the specified range do not exist, they will be added to the system. In order for each rule to listen on a different IP address, enable the **Auto increment** option next to the **IP address** drop-down list. This will create a number of forward rules, automatically incrementing the last octet of the specified receive IPv4 address by one in each consecutive rule. For example, if the Number of
rules is 100 and the given IP address is 10.0.0.1, then 100 rules will be created, first with the receive IP address of 10.0.0.1 and the last with the receive IP address of 10.0.0.100.

- Into the **Subnet mask** drop-down list, enter a subnet mask for the IPv4 addresses you are creating.

An example of IPv4 address range settings is shown in Figure 14.

### Using IPv6 address range

- Into the **IP address** drop-down list enter the first IPv6 address of the range you want to create. If IPv6 addresses from the specified range do not exist, they will be created and added to the system. In order for each rule to listen on a different IPv6 address, enable the **Auto increment** option next to the **IP address** drop-down list. This will create a number of forward rules, automatically incrementing the selected varying part of the specified IPv6 address by one in each consecutive rule.

![New Multiple SNMP Query Proxy Rules dialog box (IPv6 listening address range)](image)

- In the **Varying IPv6 part** drop-down list, select the part of the IPv6 address you wish to increment.
In the **Start from** input line, enter the value you wish the incrementation to start from. The value must be in hexadecimal notation in the range of 0-ffff.

For example, if the number of rules is 10, the given IPv6 address is fe80::ac98:d82b:9c63:9601, the "varying part" of IPv6 address is the last part (9601), and the "start from" parameter contains the current value (9601), then ten rules will be created, first with the receive IP address of fe80::ac98:d82b:9c63:9601 and the last with the receive IP address of fe80::ac98:d82b:9c63:960a.

An example of IPv6 address range settings is shown in **Figure 15**.

- Into the **Port** drop-down list, enter the UDP port number on which the SNMP Proxy Agent will listen for incoming SNMP requests (SNMP Get, GetNext, GetBulk (if applicable), Set).

  **Note:** the combination of receive IP address and port must be unique in every SNMP query proxy rule.

- In the **SNMP profile** drop-down list, select the SNMP profile, whose settings the incoming SNMP requests must match in order to be forwarded by the given rule.

**Tip:** To create a new SNMP profile, select the <New SNMP profile...> entry from the **SNMP profile** drop-down list and configure its properties, as described in the New/Edit SNMP Profile Dialog Box section.

6. The **Forward** section of the New SNMP Proxy Rule dialog box lets you specify forwarding destinations (e.g., managed devices) and SNMP protocol settings used for forwarding SNMP requests to destinations, as follows:

- Into the **IP Address** input line, enter the IPv4 or IPv6 address, which the SNMP requests will be forwarded to. For each rule to forward SNMP requests to a different IP address, select the **Auto increment** option next to the **IP address** input line. This will create a series of forward rules, automatically incrementing the last octet of the specified forward IP address by one in each consecutive rule. For example, if the number of rules = 10 and Forward address = 10.0.0.1, then ten rules will be created, first with the forward address of 10.0.0.1 and the last with the forward address of 10.0.0.10. If you enter an IPv6 address, you need to specify also the "varying part" and "start from" parameters, as described above for receive IPv6 addresses.

- Into the **Port** input line, enter the UDP port number, which the SNMP requests will be forwarded to. For each rule to forward SNMP requests to a different port, select the **Auto increment** option next to the **Port** input line. This will create a series of forward rules, automatically incrementing the forward port number in each rule. For example, if the Number of rules = 10 and Forward port = 2001, then ten rules will be created, first rule with the forward port of 2001 and the last rule with the forward port of 2010.

- In the **SNMP Profile** drop-down menu, select the SNMP profile to be used for forwarding SNMP requests. If the Receive and Forward profiles are different, all incoming SNMP requests will be translated according to the Forward
profile’s SNMP protocol settings and then forwarded to the target address. Similarly, all SNMP Response messages received from the target address will be translated back to the SNMP settings specified in the Receive profile, before being sent back to the request originator.

Tip: To create a new SNMP profile, select the <New SNMP profile...> entry from the SNMP profile drop-down list and set its properties, as described in the New/Edit SNMP Profile Dialog Box section.

- Into the Timeout input line, enter the timeout value in seconds for forwarding SNMP requests.
- Into the Retries input line, enter a number that designates how many times the requests will be retransmitted after the first timeout occurs.

7. Into the Comment input line, optionally enter a short comment, e.g., describing the rules or target devices.

8. Click the OK button to close the New Multiple Rules dialog box and create the new forwarding rules (add new lines to the SNMP Query list).

Figure 16: Multiple new forward rules created for an IP-based proxy scenario
Creating Multiple SNMP Query Forward Rules for Port-Based Proxying

The **port-based proxying** involves creating a number of rules that open different listening ports on one local IP address or all (any) local IP addresses.

1. In the SNMP Proxy Agent Configurator main window, select the **SNMP Query** tab.
2. Select the **Rule / New Multiple Rules** command from the main menu (Figure 13) or right-click inside the SNMP Query list and select the **New Multiple Rules** popup command.
3. The New Multiple SNMP Query Rules dialog box appears (Figure 17).

![New Multiple SNMP Query Rules dialog box](image)

4. Into the **Number of rules** input line in the General section of the dialog box, enter the number \( n \) of SNMP query forwarding rules you would like to create.
5. The **Receive** section of this dialog box lets you specify a network interface, IP address(es), subnet, port(s), and SNMP profile used by the SNMP Proxy Agent to listen for incoming SNMP requests, as follows:
   - In the **Network interface** drop-down list, select the network interface the software will to bind to when listening for SNMP requests. If you select the **Any** entry in this drop-down list, the software will listen on all (any) interfaces on the machine.
In the **IP address** drop-down list, specify the IPv4 or IPv6 address the software will listen to for SNMP requests:

- If you have selected a specific interface in the **Network interface** drop-down list, then you can select an IPv4 or IPv6 address that exists on the given interface or enter a new IPv4 or IPv6 address. If the entered IP address does not exist, it will be created and added to the system.
- If you have selected the **Any** entry in the **Network interface** drop-down list, then you can select 0.0.0.0 (Any IPv4) or :: (Any IPv6) address from this drop-down list to listen on all (any) existing local IPv4 or IPv6 addresses, respectively.

Disable the **Auto increment** option next to the **IP address** drop-down list.

- If you have selected an IPv4 address other than 0.0.0.0 in the **IP address** drop-down list, the subnet mask of this IP address is displayed in the **Subnet mask** drop-down list by default. To use a different subnet mask, e.g., for an IP address you are creating, enter it into the **Subnet mask** drop-down list.

- Into the **Port** input line, enter the UDP port number on which the SNMP Proxy Agent will listen for incoming SNMP requests (SNMP Get, GetNext, GetBulk (if applicable), Set). For each rule to listen on a different port, select the **Auto increment** option next to the **Port** input line. This will create a series of rules, automatically incrementing the receive port number in each rule. For example, if the Number of rules = 10 and Receive port = 2001, then ten rules will be created, first rule with the receive port of 2001 and the last rule with the receive port of 2010.

**Note:** the combination of receive IP address and port must be unique in every SNMP query proxy rule.

- In the **SNMP profile** drop-down list, select the SNMP profile, whose settings the incoming SNMP requests must match in order to be forwarded by the given rule.

**Tip:** To create a new SNMP profile, select the **<New SNMP profile...>** entry from the **Receive profile** drop-down list and configure its properties, as described in the **New/Edit SNMP Profile Dialog Box** section.

6. The **Forward** section of the New SNMP Proxy Rule dialog box lets you specify a forwarding destination (e.g., a managed device) and SNMP protocol settings used for forwarding SNMP requests to it, as follows:

- Into the **IP Address** input line, enter the IPv4 or IPv6 address, which the SNMP requests will be forwarded to. For each rule to forward SNMP requests to a different IP address, select the **Auto increment** option next to the **IP address** input line. This will create a series of forward rules, automatically
incrementing the last octet of the specified forward IP address by one in each consecutive rule. For example, if the Number of rules = 10 and Forward address = 10.0.0.1, then ten rules will be created, first with the forward address of 10.0.0.1 and the last with the forward address of 10.0.0.10.

- Into the **Port** input line, enter the UDP port number, which the SNMP requests will be forwarded to. For each rule to forward SNMP requests to a different port, select the **Auto increment** option next to the **Port** input line. This will create a series of forward rules, automatically incrementing the forward port number in each rule. For example, if the Number of rules = 10 and Forward port = 2001, then ten rules will be created, first rule with the forward port of 2001 and the last rule with the forward port of 2010.

- In the **SNMP Profile** drop-down menu, select the SNMP profile to be used for forwarding SNMP requests. If the Receive and Forward profiles are different, all incoming SNMP requests will be translated according to the Forward profile’s SNMP protocol settings and then forwarded to the target address. Similarly, all SNMP Response messages received from the target address will be translated to the SNMP settings specified in the Receive SNMP profile, before being sent back to the request sender.

**Tip:** To create a new SNMP profile, select the <New SNMP profile...> entry from the **SNMP profile** drop-down list and set its properties, as described in the New/Edit SNMP Profile Dialog Box section.

- Into the **Timeout** input line, enter the timeout value in seconds for forwarding SNMP requests.

- Into the **Retries** input line, enter a number that designates how many times the requests will be retransmitted after the first timeout occurs.

7. Into the **Comment** input line, optionally enter a short comment, e.g., describing the rules or target devices.

8. Click the **OK** button to close the New Multiple Rules dialog box and create the new forwarding rules (add new lines to the SNMP Query list).

Figure 18: Multiple new forward rules created for a port-based proxy scenario
5.3.3 Testing SNMP Query Forward Rules

1. To test a rule, select it in the SNMP Query list and choose the Rule / Test command from the main menu. Alternatively, right-click the rule and select the Test command from the pop-up menu (Figure 19).

   **Tip:** You can select and test several or all SNMP query forward rules at a time using the above procedure. To select a block of adjacent rules, click the first rule in the list, press and hold down the **SHIFT** key and click the last rule. To select non-adjacent rules, press and hold down the **CTRL** key while clicking the rules.

   ![Figure 19: Testing an SNMP query forward rule](image)

2. SNMP Proxy Agent sends an SNMP request to the forward destination specified by the selected rule. If it receives a valid SNMP response from the destination, the OK status icon (✔) and the test time stamp is displayed in the Test Status column of the respective rule. Otherwise, the Error status icon (❌) and error description is displayed (e.g., Timeout). Place your mouse cursor above the test status icon to see the detailed test result (retrieved value) in a tooltip.

   ![Figure 20: Viewing a rule’s test status details in a tooltip](image)
5.3.4 Viewing Activity Status of Rules

The SNMP Proxy Agent Configuration utility lets you view at any given time, which of the enabled forwarding rules are currently active and working as expected.

The software enables this by displaying a different rule status symbol, based on whether the rule is currently forwarding SNMP messages and receiving responses, or not:

- rule is enabled but idle (no forwarding is currently performed by this rule; probably no matching incoming SNMP messages are being received)
- rule is enabled and active (rule is currently forwarding SNMP messages to end destination and receiving responses from it)
- rule is enabled and semi-active (rule is currently forwarding SNMP messages to end destination, but is not receiving responses from it; test the rule for more information)

Example:

![Figure 21: A list of enabled forwarding rules, where some of them are active and some idle](image)

5.3.5 Enabling/Disabling SNMP Query Forward Rules

When a new forwarding rule is created, it is automatically enabled. If a rule is temporarily not needed, you can disable it. When a rule is disabled, SNMP Proxy Agent stops forwarding SNMP messages as specified by the given rule and releases the respective receive port.
To disable rules:

1. In the SNMP Proxy Agent Configurator main window, select the **SNMP Query** tab.
2. Select one or more forwarding rules you wish to disable and choose the **Rule / Disable** command from the main menu. Alternatively, right-click the selected rules and choose the **Disable** pop-up command (Figure 22).

3. The status of the selected rules changes to **Disabled** (Figure 23), meaning that the rules are not in effect (forwarding is disabled). The software also stops listening on the receive ports specified in the disabled rules.

![Figure 22: Disabling forwarding rules](image)

![Figure 23: A list of forwarding rules, where some of them are disabled](image)
To enable rules:
1. In the SNMP Proxy Agent Configurator main window, select the **SNMP Query** tab.
2. Select one or more forwarding rules you wish to enable and choose the **Rule / Enable** command from the main menu. Alternatively, right-click the selected rules and choose the **Enable** pop-up command.
3. The status of the selected rules changes to **Enabled** (Figure 22), meaning that the rules are in effect, i.e., the software listens on the specified receive port for incoming SNMP messages and is ready to forward SNMP requests according to the rule configuration.

5.3.6 Deleting SNMP Query Forward Rules

1. In the SNMP Proxy Agent Configurator main window, select the **SNMP Query** tab.
2. In the SNMP Query list, select one or more rules that you wish to delete and choose the **Rule / Delete** command from the main menu. Alternatively, right-click the selected rules and choose the **Delete** pop-up command (Figure 32).
3. Click the **Yes** button in the confirmation dialog that appears to confirm the rule deletion. The corresponding line(s) disappear from the list of forwarding rules in the SNMP Query tab.
5.4 Configuring Proxy Forward Rules for SNMP Notifications

This section describes how to add, configure and delete the rules for forwarding and optionally translating SNMP notifications (SNMP Trap and SNMP Inform messages). A notification forwarding rule is a configuration item that specifies the port on which SNMP Proxy Agent listens for incoming SNMP notification messages, the address and port to which SNMP notifications are forwarded, as well as the SNMP protocol settings used for receiving and forwarding SNMP messages (the latter two control translation of SNMP notification messages between different versions of the protocol).

SNMP-enabled devices send SNMP notification messages to one or more SNMP management applications when certain events occur, e.g., a device is restarted, device is queried with wrong credentials, link is lost or restored, etc.

SNMP Proxy Agent lets you configure multiple notification forwarding rules, for example, to enable forwarding SNMP notifications to more than one SNMP management application. This means that two or more rules for forwarding SNMP notifications can have the same receive port (of course, this port must not already be used by any of the SNMP query forwarding rules). This means that SNMP Proxy Agent can forward the same stream of incoming SNMP Trap and Inform messages to two or more destinations.

Typically, no more than one notification forward rule for each target (NMS) needs to be configured. If the matching query forward rules exist, SNMP Proxy Agent will automatically perform the basic network address translation (NAT) when forwarding SNMP notifications from different devices to target NMS, as depicted in the IP-based proxying - SNMP Traps diagram and in Port-based proxying - SNMP Traps diagram.

The next two sub-sections describe how to create a single notification forwarding rule and how to create multiple forwarding rules at a time, respectively. Then, the method of testing, enabling and disabling notification forwarding rules is explained. Finally, the procedure of deleting notification forwarding rules is described.

5.4.1 Adding a SNMP Notification Forward Rule

1. In the SNMP Proxy Agent Configurator main window, select the SNMP Notification tab.
2. Select the Rule / New Rule command from the main menu or right-click inside the SNMP Notification list and select the New Rule pop-up command (Figure 24).
3. The New SNMP Notification Proxy Rule dialog box appears (Figure 25).
4. Into the **Receive port** input line in the New SNMP Notification Proxy Rule dialog box, enter the UDP port number, which the Proxy Agent will listen for incoming SNMP Trap and SNMP Inform (if applicable) notification messages.

   **Tip:** You can create two or more SNMP notification rules that listen on the same port but forward SNMP notifications to different destinations.
5. In the **Receive SNMP profile** drop-down list, select the SNMP profile, whose settings the incoming SNMP notification messages must match in order to be forwarded by the given rule.

   **Tip:** To create a new SNMP profile, select the `<New SNMP profile...>` entry from the **Receive profile** drop-down list and set its properties, as described in the New/Edit SNMP Profile Dialog Box section.

6. Into the **Forward IP Address** input line, enter the IP address of the SNMP management application, which the SNMP requests will be forwarded to.

7. Into the **Forward port** input line, enter the UDP port number, which the SNMP notifications will be forwarded to.

8. In the **Forward SNMP Profile** drop-down menu, select the SNMP profile to be used for forwarding SNMP notification messages. If the Receive and Forward profiles are different, all incoming SNMP Trap and Inform notification messages will be translated to match the Forward profile SNMP protocol settings and then forwarded to the target address. Similarly, all SNMP Response to Inform messages received from the target address will be translated back to the initial SNMP settings that match the Receive profile parameters, before being sent back to the Inform sender.

   **Tip:** To create a new SNMP profile, select the `<New SNMP profile...>` entry from the **Forward profile** drop-down list and set its properties, as described in the New/Edit SNMP Profile Dialog Box section.

9. Into the **Timeout** input line, enter the timeout value in seconds for forwarding SNMP Inform messages. Note that this setting applies only to SNMP Inform messages (Trap messages are not retransmitted).

10. Into the **Retransmits** input line, enter a number that controls how many times the SNMP Inform messages will be retransmitted after the first timeout. Note that this setting applies only to SNMP Inform messages (Trap messages are not retransmitted).

11. To enable adding a variable binding carrying the original source address to each forwarded SNMP notification message, check the **Add source address variable binding to PDU** checkbox. If this checkbox is checked, SNMP Proxy Agent appends an additional variable binding to the variable bindings list of every received SNMP notification PDU before forwarding the notification to the target address. The name (OID) portion of this variable binding is `snmpTrapAddress.0` (1.3.6.1.6.3.18.1.3.0), and the value is either the value of the SNMPv1 agent-addr field (if the notification was received as SNMPv1 Trap message), or the IP address from which SNMP Proxy Agent actually received the notification (if the notification was received as SNMPv2c or SNMPv3 Trap or Inform message).

12. Into the **Comment** input line, optionally enter a short comment describing the rule.

13. Click the **OK** button to close the New SNMP Notification Proxy Rule dialog box and create the new forwarding rule (a new line appears in the SNMP Notification list - Figure 26).
Repeat the above steps to configure additional rules for forwarding SNMP notification messages.

5.4.2 Adding Multiple SNMP Notification Forward Rules

This section describes how to quickly create a number of rules for forwarding SNMP Trap and Inform notification messages. Each rule created in this procedure uses a different receive port and can forward SNMP requests to a different IP address and/or port.

1. In the SNMP Proxy Agent Configurator main window, select the **SNMP Notification** tab.

2. Select the **Rule / New Multiple Rules** command from the main menu or right-click inside the SNMP Query list and select the **New Multiple Rules** pop-up command (Figure 27).

3. The New Multiple SNMP Notification Rules dialog box appears (Figure 28).
4. Into the **Number of rules** input line in the New Multiple SNMP Notification Rules dialog box, enter the number of SNMP notification forwarding rules you would like to create \((n)\).

5. Into the **Receive port** input line, enter the UDP port number on which SNMP Proxy Agent will listen for incoming SNMP Trap and Inform notification messages. There are two options:

   - To create rules that will have different (incrementing) receive port; select the **Auto increment** checkbox next to the **Port** input line. If this option is selected, the software will automatically listen for incoming SNMP notifications also on the additional \(n-1\) ports, starting from the specified receive port. For example, if the **Number of rules** is 10 and **Receive port** is 2000, then ten rules will be created, each with a different receive port starting with port 2000 and ending with port 2009 (the software will listen for SNMP notifications on UDP port range 2000-2009).

   - To create rules that will have the same receive port, but different forward destinations, uncheck the **Auto increment** checkbox next to the **Port** input line. In this case SNMP Proxy Agent will listen on one port for incoming SNMP Trap and Inform messages and forward them to \(n\) destinations specified in the Forward IP address and Port controls.
6. In the **Receive SNMP profile** drop-down list, select the SNMP profile, whose settings the incoming SNMP notification messages must match in order to be forwarded by the given rules.

   **Tip:** To create a new SNMP profile, select the `<New SNMP profile...>` entry from the **Receive profile** drop-down list and set its properties, as described in the **New/Edit SNMP Profile Dialog Box** section.

7. Into the **Forward IP Address** input line, enter the IP address, which the SNMP notification messages will be forwarded to. If you wish that each rule forwards SNMP notifications to a different IP address, select the **Auto increment** option next to the Forward IP address input line. This will create a series of rules, where the last octet of the specified forward IP address will be incremented by one in each consecutive rule. For example, if the *Number of rules is* 10 and *Forward address is* 10.0.0.1, then ten rules will be created, first with the forward address of 10.0.0.1 and the last with the forward address of 10.0.0.10.

8. Into the **Forward port** input line, enter the UDP port number, which the SNMP requests will be forwarded to. For each rule to forward SNMP requests to a different port, select the **Auto increment** option next to the Forward Port input line. This will create a series of rules with the increasing Forward port number, starting with the entered value. For example, if the *Number of rules is* 10 and *Forward port is* 8001, then ten rules will be created, first rule with the forward port of 8001 and the last rule with the forward port of 8010.

9. In the **Forward SNMP Profile** drop-down menu, select the SNMP profile to be used for forwarding SNMP notification messages. If the Receive and Forward profiles are different, all incoming SNMP Trap and Inform notification messages will be translated to match the Forward profile’s SNMP protocol settings and then forwarded to the target address. Similarly, all SNMP Response to Inform messages received from the target address will be translated back to the initial SNMP version according to the Receive profile settings before being sent back to the Inform sender.

   **Tip:** To create a new SNMP profile, select the `<New SNMP profile...>` entry from the **Forward profile** drop-down list and set its properties, as described in the **New/Edit SNMP Profile Dialog Box** section.

10. Into the **Timeout** input line, enter the timeout value in seconds for forwarding SNMP Inform messages. Note that this setting applies only to SNMP Inform messages (Trap messages are not retransmitted).

11. Into the **Retransmits** input line, enter a number that controls how many times the SNMP Inform messages will be retransmitted after the first timeout. Note that this setting applies only to SNMP Inform messages (Trap messages are not retransmitted).

12. To enable adding a variable binding carrying the original source address to each forwarded SNMP notification message, check the **Add source address variable binding to PDU** checkbox. If this checkbox is checked, SNMP Proxy Agent appends an additional variable binding to the variable bindings list of every received SNMP notification PDU before forwarding the notification to the target address. The name (OID) portion of this variable binding is `snmpTrapAddress.0`
(1.3.6.1.6.3.18.1.3.0), and the value is either the value of the SNMPv1 agent-addr field (if the notification was received as SNMPv1 Trap message), or the IP address from which SNMP Proxy Agent actually received the notification (if the notification was received as SNMPv2c or SNMPv3 Trap or Inform message).

13. Into the **Comment** input line, optionally enter a short comment describing the rules.

14. Click the **OK** button to close the New SNMP Notification Proxy Rule dialog box and create the new forwarding rules (new lines appear in the SNMP Notification list).

![MG-SOFT SNMP Proxy Agent Configurator](image)

**Figure 29: Multiple notification forward rules in the SNMP Notification tab**

### 5.4.3 Testing SNMP Notification Forward Rules

1. To test a notification forwarding rule, select it in the SNMP Notification list and choose the **Rule / Test** command from the menu. Alternatively, right-click the rule and select the **Test** command from the pop-up menu (Figure 30).

**Tip:** You can select and test several or all SNMP notification forward rules at a time using the above procedure. To select a block of adjacent rules, click the first rule in the list, press and hold down the **SHIFT** key and click the last rule. To select non-adjacent rules, press and hold down the **CTRL** key while clicking the rules.
2. SNMP Proxy Agent will send an SNMP Trap message (if the forward profile uses SNMPv1 protocol version) or SNMP Inform message (if the forward profile uses SNMPv2c or SNMPv3 protocol version) to the forward destination.

Note: SNMP Trap sending represents an unconfirmed event reporting mechanism, while SNMP Inform sending is a confirmed event reporting mechanism. In other words, in case of a SNMP Trap message no response is sent back by the Trap receiver, while in case of an SNMP Inform message the receiver is required to send a response message back to the sender to confirm the Inform reception.

3. If SNMP Proxy Agent receives a valid SNMP response to Inform message from the destination, the **OK** status icon (✔) and the test time stamp is displayed in the **Test Status** column. Otherwise, the **Error** status icon (❗) and error description is displayed (e.g., Timeout). Hover your mouse cursor over the test status icon to see the detailed test result in a tooltip (Figure 31).

4. In case of an error (e.g., a timeout), please verify that the SNMP manager at the end destination is up and running and that no firewall is blocking SNMP Trap and SNMP Inform messages, as well as SNMP Response messages.

### 5.4.4 Enabling/Disabling SNMP Notification Forward Rules

When a new forward rule is created, it is automatically enabled. If one or more rules are temporarily not needed, they can be disabled for the SNMP Proxy Agent to stop forwarding SNMP messages according to these rules and to free the respective listening ports.
SNMP notification forward rules can be disabled and enabled in the same manner as SNMP query forward rules. For the detailed instructions, please refer to the section Enabling/Disabling SNMP Query Forward Rules.

5.4.5 Deleting SNMP Notification Forward Rules

1. In the SNMP Proxy Agent Configurator main window, select the SNMP Notification tab.

2. In the SNMP Notification list, select one or more rules that you wish to delete and choose the Rule / Delete command from the main menu. Alternatively, right-click the selected rules and choose the Delete pop-up command (Figure 32).

3. Click the Yes button in the confirmation dialog that appears to confirm the rule deletion. The corresponding line(s) disappear from the list of forwarding rules in the SNMP Notification tab.

![Figure 32: Deleting selected SNMP notification forward rules](image)
6 FILTERING RULES

MG-SOFT SNMP Proxy Agent Configurator implements a convenient filtering feature that lets you find and display only those rules that contain a user-specified text string in any of the selected columns.

To filter forwarding rules:

1. Select the tab in the Proxy Agent Configurator main window where you wish to filter the rules, i.e., **SNMP Query** tab or **SNMP Notification** tab.

2. Click the **Filter Options** button (●) next to the **Filter** input line to display the **Filter Options** drop-down list (Figure 33).

3. In the **Filter Options** drop-down list, select the desired filtering options and the columns that you wish to search in.

![Figure 33: Setting filter options](image)

**Filter Options:**

- **Dynamic filter**: Select the **Dynamic filter** option to make the filter behave as a continuous search and filter tool, meaning that any subsequent changes you make to the rules are automatically put through the filter and only those rules that match the filtering criteria are displayed. This process continues until you remove (clear) the filter. If **Dynamic filter** option is not selected the filter functions as a one-time search.

- **Match case**: Select the **Match case** option to make the filter case sensitive. If this option is enabled, the search will find only those strings in which the letter capitalization matches the one used in the **Filter** input line (e.g., `SNMPv1` will find `SNMPv1`, but not `Snmpv1`).

- **Match whole word only**: Select the **Match whole word only** option to find only those strings that are whole words and not part of a larger word (e.g., `SNMP` will find `SNMP`, but not `SNMPv1`).
4. Enter characters that will serve as a filter condition into the **Filter** input line.

5. Only the rules (rows) that contain the entered text in one or more of the selected columns will be displayed in the list of forwarding rules. The number of hits, i.e., rules that match the filter condition, is displayed next to the **Filter** input line (Figure 34). For example, indication *(6/106)* means that 6 rules out of 106 satisfy the filter condition.

6. Click the **Clear** button next to the **Filter** input line to remove the filter and display all forwarding rules.

Figure 34: Filtering rules in the SNMP query list
7 MANAGING LOCAL NETWORK INTERFACES AND IP ADDRESSES

This section describes how to view local network interfaces and IP addresses assigned to them. It also explains how to manually add and delete IPv4 and IPv6 addresses and how the software handles unused IP addresses.

1. In the SNMP Proxy Agent Configurator main window, select the **Edit / Network Interfaces** command from the menu.

2. The Network Interface Manager dialog box appears (Figure 28).

3. From the **Network Interface** drop-down list at the top of the dialog box, select a desired network interface.
   - The **IPv4 addresses** and **IPv6 addresses** tabs display a list of all IPv4 and IPv6 addresses that exist on the given interface, respectively. For IPv4 addresses, the corresponding subnet masks are also listed.
   - The column **In Use** denotes if the IP address is currently in use by any proxy rule.
   - The column **Custom** denotes if the address has been added by SNMP Proxy Agent (Yes) or not (No).
   - Check the **Automatically remove unused custom IP addresses** checkbox in order for SNMP Proxy Agent to automatically delete the IP addresses that are currently not in use by any of the proxy rules.
To create a new IPv4 address:
1. Select the **IPv4 addresses** tab in the Network Interface Manager dialog box.
2. Click the **Add** button in the right section of the Network Interface Manager dialog box. The Add IPv4 Address dialog box appears.

![Add IPv4 Address dialog box](image1)

Figure 36: Adding a new IPv4 address

3. Enter the desired IPv4 address and subnet mask into the corresponding input line and click the **Add** button to add the new IP address to the system and assign it to the selected network interface.

To create a new IPv6 address:
1. Select the **IPv6 addresses** tab in the Network Interface Manager dialog box.
2. Click the **Add** button in the right section of the Network Interface Manager dialog box. The Add IPv6 Address dialog box appears.

![Add IPv6 Address dialog box](image2)

Figure 37: Adding a new IPv6 address

3. Enter the desired IPv6 address into the **IP address** input line and click the **Add** button to add the new IPv6 address to the system and assign it to the selected network interface.

To delete an IPv4 or IPv6 address:
1. Select the custom IPv4 or IPv6 address you would like to remove and click the **Remove** button in the right section of the Network Interface Manager dialog box.
2. The address is removed from the system and from the list of available addresses.

**Note:** An address cannot be removed if it is currently being used by any of the proxy rules.
8 EXPORTING AND IMPORTING CONFIGURATION

MG-SOFT SNMP Proxy Agent Configurator lets you export the entire configuration, i.e., all SNMP query and notification forward rules and SNMP profiles, and save it to a configuration .INI file. This .INI file can later be imported into (the same or different copy of) SNMP Proxy Agent Configurator in order to either replace its current configuration or append the rules and profiles from the .ini file to the current configuration.

8.1 Exporting Configuration to .ini File

1. In the Proxy Agent Configurator select the **File / Export Configuration** command from the main menu (**Figure 38**).

![Figure 38: Selecting the Export Configuration command](image)

2. The Export dialog box appears (**Figure 39**). Navigate to the location where you want to save the configuration file and enter the name of the configuration .ini file into the **File name** input line and click the **Save** button to write the file to disk.
8.2 Importing Configuration from .ini File

1. In the Proxy Agent Configurator select the **File / Import Configuration** command from the main menu (Figure 40).

2. The Import dialog box appears (Figure 41). Navigate to the location that contains the previously exported configuration .ini file, select the file and click the **Open** button to start importing the configuration.
3. The Proxy Agent Configurator displays the dialog box prompting you to select whether to replace or supplement the current configuration (Figure 42).

![Figure 42: Selecting the import method](image)

- Select the **Replace** button to replace the current configuration (rules and profiles) with the one from the selected .ini file, or
- Select the **Append** button to append the configuration (rules and profiles) from the .ini file to the current configuration.

4. The Proxy Agent Configurator reads the configuration from the .ini file and either replaces the current configuration or appends data to it, based on your selection.

5. While importing the configuration, the software may detect one or more network interfaces (MAC addresses) in the .ini file that are not available on the local machine. In such case, it displays the following dialog box that lets you resolve the issue (Figure 43).
To replace the missing interfaces and import the configuration:

1. The **Configuration Network Interface** column in the Import dialog box displays the MAC address(es) of the missing interface(s). In the **Local Network Interface** column, select the desired interface to be used instead of the missing one by choosing it from the corresponding drop-down menu, as shown in Figure 43.

2. Click the **Import and Change** button in the Import dialog box to import the configuration and modify the rules to utilize selected interface(s) instead of the missing one(s).

To import the unchanged configuration:

Click the **Import Unchanged** button in the Import dialog box to import the configuration without modifying it. Note that the proxy rules that utilize the missing interface(s) will be in the error state until the missing interface(s) become available again (e.g., by enabling the interface in the OS) or until you manually edit the rules to use a different local interface(s).
c) To import the configuration but skip rules with the missing interface(s):

   Click the **Import and Skip** button in the Import dialog box to import the configuration but skip importing those rules that utilize the missing interface(s).

d) To cancel the import operation:

   Click the **Cancel Import** button in the Import dialog box to cancel the import operation. If you select this option, nothing will be imported.