



[MG-SOFT Corporation](http://www.mg-soft.com)

Trap Ringer 2014

Professional Edition

USER MANUAL

(Document Version: 5.5)

Document published on Wednesday, 19-March-2014

Copyright © 1995-2014 MG-SOFT Corporation

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 © 1995-2014 MG-SOFT Corporation. All rights reserved.

TABLE OF CONTENTS

| | | |
|-----------|--|-----------|
| 1 | Introduction | 7 |
| 1.1 | Product Description..... | 8 |
| 1.2 | About This Manual | 9 |
| 2 | Getting Started | 10 |
| 2.1 | System Requirements..... | 10 |
| 2.1.1 | Windows Operating System | 10 |
| 2.1.2 | Linux Operating System | 10 |
| 2.1.3 | Mac OS X Operating System | 11 |
| 2.1.4 | Solaris Operating System..... | 11 |
| 2.2 | Installing and Uninstalling Trap Ringer | 11 |
| 3 | Starting Trap Ringer | 12 |
| 3.1 | Starting Trap Ringer on Windows | 12 |
| 3.2 | Starting Trap Ringer on Linux..... | 12 |
| 3.3 | Starting Trap Ringer on Mac OS X | 13 |
| 3.4 | Starting Trap Ringer on Solaris..... | 14 |
| 3.5 | Trap Ringer Desktop..... | 16 |
| 3.5.1 | Trap List Window Panel..... | 17 |
| 3.5.2 | Trap Details Window Panel..... | 18 |
| 4 | Apply License Key | 21 |
| 5 | Configuring SNMPv3 Users | 23 |
| 6 | Configuring SNMP Notification Monitoring Options..... | 27 |
| 6.1 | Console Monitoring | 29 |
| 6.2 | Log-File Monitoring | 31 |
| 6.2.1 | Configuring Ring Log File Preferences | 31 |
| 6.2.2 | Configuring Daily Logging Preferences..... | 33 |
| 6.2.3 | Configuring Auto New File Logging Preferences | 34 |
| 6.3 | Running Commands | 37 |
| 6.4 | Sending E-Mails..... | 40 |
| 6.5 | Sending SMS Messages..... | 45 |
| 6.6 | Auditing with Windows Event Viewer..... | 48 |
| 6.7 | Logging Notifications to System Log Files (Syslog)..... | 51 |
| 6.8 | Web Monitoring..... | 53 |
| 6.9 | Forwarding and Translating SNMP Notifications | 56 |
| 7 | Filtering SNMP Notifications..... | 60 |
| 7.1 | Creating Filters from Received SNMP Notifications | 61 |
| 7.1.1 | Creating Filter from Notification | 61 |
| 7.2 | Creating Filters Manually | 63 |
| 7.2.1 | Adding Filters to Output Units..... | 64 |
| 7.2.2 | Configuring Filter Conditions | 66 |
| 7.2.3 | Example of Configuring Filter in Trap Ringer Output Manager..... | 70 |
| 8 | Searching for SNMP Notifications..... | 73 |
| 9 | Assigning Severity Levels and Colors to SNMP Notifications..... | 80 |
| 10 | Exporting Received SNMP Notifications..... | 83 |

| | |
|---|-----------|
| 11 Compiling and Loading MIB Files..... | 84 |
| 11.1 Compiling MIB Files | 84 |
| 11.2 Loading / Unloading MIB Modules in Trap Ringer | 85 |
| 12 Index..... | 87 |

TABLE OF FIGURES

| | |
|--|----|
| Figure 1: Starting Trap Ringer on Linux GNOME desktop environment..... | 13 |
| Figure 2: Launching Trap Ringer from the Finder on Mac OS X..... | 14 |
| Figure 3: Starting Trap Ringer on Solaris (JDS environment)..... | 15 |
| Figure 4: Trap Ringer desktop..... | 16 |
| Figure 5: Trap Details window panel..... | 19 |
| Figure 6: Selecting the license.key file..... | 21 |
| Figure 7: Applying the license.key file..... | 22 |
| Figure 8: Applying the license.key file - restarting Trap Ringer..... | 22 |
| Figure 9: Configuring SNMPv3 users..... | 23 |
| Figure 10: Entering the SNMPv3 authentication protocol password..... | 25 |
| Figure 11: Viewing properties of received SNMPv3 notifications in Trap Details window panel..... | 26 |
| Figure 12: The Output Manager Preferences dialog box..... | 28 |
| Figure 13: Configuring Console output unit options..... | 29 |
| Figure 14: Creating a new Log output unit..... | 31 |
| Figure 15: Configuring Log output unit options..... | 32 |
| Figure 16: Configuring daily logging options..... | 33 |
| Figure 17: Configuring auto new file logging options..... | 35 |
| Figure 18: Configuring Command output unit options..... | 37 |
| Figure 19: Reserved Words dialog box..... | 38 |
| Figure 20: A pop-up message displaying some linkDown Trap notification details..... | 39 |
| Figure 21: Configuring Mail output unit options..... | 40 |
| Figure 22: Mail Accounts dialog box..... | 42 |
| Figure 23: Mail Account preferences dialog box, General tab..... | 42 |
| Figure 24: Mail Account preferences dialog box, Mail Server tab..... | 43 |
| Figure 25: Configuring SMS output unit options..... | 46 |
| Figure 26: Configuring Event output unit options..... | 48 |
| Figure 27: Monitoring SNMP notifications in Event Viewer..... | 50 |
| Figure 28: Configuring syslog output unit options..... | 51 |
| Figure 29: Configuring Web output unit options..... | 53 |
| Figure 30: Viewing Web report in Web Browser..... | 55 |
| Figure 31: Configuring Forward output unit options..... | 56 |
| Figure 32: Starting Create Filter From Notification wizard..... | 61 |
| Figure 33: Create Filter From Notification wizard – first step..... | 62 |
| Figure 34: Create Filter From Notification wizard – second step..... | 63 |
| Figure 35: Adding a filter to output unit..... | 64 |
| Figure 36: Filter Preferences panel..... | 65 |
| Figure 37: Configuring a filter condition..... | 66 |
| Figure 38: Example of a variable binding filter condition..... | 68 |
| Figure 39: Example of a “coldStart SNMPv1 & SNMPv2c filter”..... | 71 |
| Figure 40: Example of a “warmStart SNMPv1 & SNMPv2c filter”..... | 71 |
| Figure 41: Search Parameters drop-down menu..... | 73 |
| Figure 42: Entering a search query into the Search box..... | 77 |
| Figure 43: Viewing the search results (the list of results is dynamic)..... | 78 |
| Figure 44: Setting criteria for a specific search operation..... | 79 |

| | |
|--|----|
| Figure 45: Severity levels and their default colors | 80 |
| Figure 46: Configuring display filters – assigning severity levels to notifications..... | 81 |
| Figure 47: Configuring display filters – assigning colors to severity levels | 82 |
| Figure 48: Exporting SNMP notifications to CSV file | 83 |
| Figure 49: MIB Compiler desktop..... | 84 |
| Figure 50: Loading MIB modules | 85 |

1 INTRODUCTION

Thank you for using MG-SOFT Trap Ringer Professional Edition with MIB Compiler.

MG-SOFT Corporation, established in March 1990, is the world's leading supplier of SNMP, SMI, NETCONF, YANG and general network management applications, toolkits and solutions for Windows, Linux, Mac OS X and Solaris platforms. MG-SOFT provides major IT companies worldwide with network management applications as well as with toolkits implementing core network management technologies. Furthermore, MG-SOFT provides customers with consulting services, custom made turn-key software products, solutions and/or services and network management integration solutions based on our extensive know-how and vast experience in network management technologies.

MG-SOFT has developed the world's first 32-bit SNMP protocol stack implementation for MS Windows operating systems and one of the first SNMPv3 implementations for Win32 platforms. As of today, MG-SOFT's SNMP stack implemented in [WinSNMP API](#), provides a solid base for all MG-SOFT's SNMP applications (as well as for thousands of third party applications, built by our clients who licensed our WinSNMP API) running on a number of operating system platforms: MS Windows (32-bit, 64-bit, embedded CE), Linux (32-bit and 64-bit), Mac OS X (PPC and Intel platforms, 32-bit and 64-bit), Mac iOS (iPad) and Solaris (Sparc and Intel platforms).

MG-SOFT is also active in the network configuration management area and offers a full line of NETCONF and YANG software products, ranging from a graphical YANG and YIN file explorer, over Visual YANG definition file designer up to full blown NETCONF configuration manager.

For additional information about MG-SOFT Corporation, please contact the following address:

MG-SOFT Corporation
Strma ulica 8
2000 Maribor
Slovenia

Phone: +386 2 2506565
Fax: +386 2 2506566
E-mail: info@mg-soft.com
URL: <http://www.mg-soft.com/>

1.1 Product Description

MG-SOFT Trap Ringer Professional Edition is a program for monitoring SNMPv1, SNMPv2c and SNMPv3 TRAP notification messages and SNMPv2c and SNMPv3 INFORM notification messages sent by arbitrary devices on the network. It lets you manage received notifications in various ways and includes mechanisms for informing users about the events reported by the received SNMP notifications.

Trap Ringer lets you monitor received SNMP notifications in the main window by viewing the Console log (used for real-time monitoring) or any other log file created by this application (e.g., a daily log file or a log file containing filtered notifications). The software can send information about received SNMP notifications in e-mail and SMS messages to any number of recipients, as well as log it to the system log files (using the syslog protocol on Linux, Mac and Solaris). Trap Ringer can also invoke external programs upon receiving SNMP notifications in order to start any number of specific actions by providing command line parameters for each of them, as well as generate and periodically update any number of HTML report files that let you monitor SNMP notifications by using a Web browser. The available monitoring/user-notifying options can all be used simultaneously.

In addition, Trap Ringer can also act as an SNMP notification proxy forwarder application, meaning that it can forward received SNMP notifications to other SNMP management stations on the network and optionally translate notification messages to the selected SNMP version (SNMPv1, SNMPv2c or SNMPv3) and type (Trap or Inform).

Trap Ringer incorporates advanced filtering capabilities, so that the notifications with particular attributes can be ignored. Furthermore, it provides a powerful and easy-to-use search tool that lets you search any existing log file and quickly find and display only those SNMP notifications that match the search criteria. Trap Ringer also lets you assign different severity levels and colors to SNMP notifications in order to emphasize their importance and provide a better overview of received notification messages.

Trap Ringer displays details for each notification message and decodes notification's attributes and included variable bindings by retrieving this information from the relevant MIB modules. The enclosed MG-SOFT MIB Compiler lets you compile any vendor specific MIB file for use with Trap Ringer. The information about received SNMP Trap and Inform notifications can also be exported from Trap Ringer to CSV (comma separated value) text files for the purpose of external viewing or post-processing.

Trap Ringer supports IPv4 and IPv6 transport protocol and can receive SNMP notifications on any IPv4/UDP and IPv6/UDP port.

Trap Ringer employs the client/server architecture in a sense that the notification receiving module (server) is separated from the application's GUI (client). The server module, which runs as a service/daemon application even when no user is logged on the operating system, receives SNMP notifications from the network and processes them according to applied configuration. Trap Ringer client, which runs on the same computer as Trap Ringer server, is a regular GUI application that, when started, connects to the server and lets you view and manage received SNMP notifications, as well as control and configure both parts of the application.

Trap Ringer Professional Edition is, apart from MS Windows operating systems, available also for Linux, Mac OS X and Solaris platforms. The Windows, Linux, Mac and Solaris versions of the software offer the same functions and features and share a common look-and-feel.

1.2 About This Manual


This manual contains instructions for completing the basic operations that can be performed by using MG-SOFT Trap Ringer Professional Edition software. Task-based instructions in this manual and many illustrative examples will help you understand how Trap Ringer works and how to use it efficiently.

It is supposed that you are familiar with basic actions in a graphical desktop environment, such as choosing a main menu command or a mouse pop-up command, dragging and dropping items, etc.

This manual consist of:

- ❑ The introductory part; containing the general information about the program, configuration requirements, installation instructions and other information you need to know before you start.
- ❑ The starting part; which will tell you how to start Trap Ringer and describe its desktop.
- ❑ The main part; providing the information on how to configure different options of monitoring SNMP trap and inform notifications in Trap Ringer, how to use and configure filters, how to search log files for particular SNMP notifications, how to assign severity levels and colors to SNMP notifications, etc.
- ❑ A section providing instructions on compiling MIB files in the enclosed MIB Compiler program and on loading compiled MIB files into Trap Ringer.
- ❑ Index

Almost all MG-SOFT Trap Ringer operations can be accessed in several possible ways. You can either use:

- ❑ Main menu commands (e.g., **View / Trap Ringer Preferences** - the construct “View / Trap Ringer Preferences” means: click the **View** command in the menu bar and select the **Trap Ringer Preferences** command from the sub-menu.)
- ❑ Toolbar buttons (e.g., )
- ❑ Keyboard shortcuts (e.g., **Ctrl+R** - hold down the **Ctrl** key and at the same time press the **R** key)
- ❑ Many operations can also be accessed via the pop-up menu (e.g., **Copy** - to use the “Copy pop-up command”, right-click inside the Trap Details window panel, and select the **Copy** command from the pop-up menu.)

Most of the procedures in this manual are described by using the main menu commands. However, you can use any of the above-mentioned shortcuts if they are available.

2 GETTING STARTED

This section presents the basic system requirements your computer has to meet to install and use MG-SOFT Trap Ringer Professional Edition for Windows, Linux, Mac OS X and Solaris operating systems.

2.1 System Requirements

MG-SOFT Trap Ringer Professional Edition is a program for monitoring SNMP Trap and SNMP Inform notification messages. Trap Ringer software is available for Microsoft 32-bit and 64-bit Windows operating systems, for Linux operating systems for Intel x86 hardware architecture (Red Hat, SUSE, Ubuntu,...), for Apple Mac OS X (universal binaries for Intel x86 and x86_64), as well as for Oracle Solaris 10 and 11 operating systems (Intel x86 and SPARC platforms).

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

2.1.1 Windows Operating System

The Windows version of MG-SOFT Trap Ringer has been successfully tested on the following 32-bit and 64-bit Microsoft Windows operating systems: Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2012 and Windows 8.

Note: To install the software on Windows, you need to have administrative privileges.

2.1.2 Linux Operating System

The Linux version of MG-SOFT Trap Ringer has been successfully tested on the following Linux distributions running on the Intel x86 and x86_64 architecture: Red Hat Enterprise Linux 4 or newer, Fedora Core 5 or newer, SUSE 10 or newer, Debian 4 or newer, Ubuntu 6.06 or newer and Slackware 12 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.

Note: To install the software on Linux, you need to have the root user privileges.

2.1.3 Mac OS X Operating System

MG-SOFT Trap Ringer Pro. for Mac OS X release contains universal binaries for Intel x86 and x86_64 platforms. It has been successfully tested by MG-SOFT on:

- ❑ Mac OS X v10.6.x Snow Leopard
- ❑ Mac OS X v10.7.x Lion
- ❑ Mac OS X v10.8.x Mountain Lion
- ❑ Mac OS X v10.9.x Mavericks

For the most recent information about the supported distributions, check the release notes (README.TXT) of the current software release.

Note: To install the software on Mac OS X, you need to have admin user privileges.

2.1.4 Solaris Operating System

MG-SOFT Trap Ringer Pro. for Solaris has been successfully tested on the following Solaris operating systems:

- ❑ Solaris v10 (Intel x86 and SPARC platforms)
- ❑ Solaris v11 (Intel x86)

For the most recent information about the supported distributions, check the release notes (README.TXT) of the current software release.

Note: To install the software on Solaris, you need to have the root user privileges.

2.2 Installing and Uninstalling Trap Ringer

Before you install MG-SOFT Trap Ringer Professional Edition with MIB Compiler on your computer, first make sure your computer meets the system requirements described in the [System Requirements](#) section.

For detailed installation instructions, please check the “Installing the software” section of the README.TXT file, which is bundled with the current software release.

For instructions on uninstalling Trap Ringer, please check the “Uninstalling the software” section of the README.TXT file, which is bundled with the current software release.

3 STARTING TRAP RINGER

Trap Ringer Professional Edition employs client/server architecture, where the server application receives SNMP notifications from the network and processes them according to applied configuration, while the client provides a graphical user interface for viewing received SNMP notifications and for configuring both Trap Ringer server and client.

On Windows operating system, the server module runs as a system service. Trap Ringer client, which runs on the same computer as Trap Ringer server, is a regular GUI application that, when started, connects to the server and lets you view and manage received SNMP notifications, as well as start, stop, and configure Trap Ringer server. Similarly, on Linux, Mac OS X and Solaris operating systems, Trap Ringer server module runs as a daemon application without a user interface, while the client runs as a regular GUI application, providing the same features and a similar look-and-feel as the Windows version of Trap Ringer client.

3.1 Starting Trap Ringer on Windows

1. Start the Trap Ringer client by selecting the **Trap Ringer Pro** entry from the system Start menu (i.e., using the **Start / Programs / MG-SOFT Trap Ringer Pro / Trap Ringer Pro** command).
2. As the program starts, the MG-SOFT Trap Ringer splash screen appears, displaying the company name and announcing the program itself.
3. The Trap Ringer client desktop will appear ([Figure 4](#)).
4. Trap Ringer client automatically starts Trap Ringer server application (if not already running), connects to it and displays received SNMP notifications in the main window (provided that the console or log-file monitoring option is enabled). In case the server does not start automatically, use the **Tools / Start Service** command to launch it manually.

Note: By default, Trap Ringer server is started automatically at the system startup. You can change this behavior by unchecking the **Start service at system startup** checkbox in Trap Ringer Preferences dialog box, General tab.

3.2 Starting Trap Ringer on Linux

1. Start the Trap Ringer client by selecting the **Trap Ringer Pro** entry from the system taskbar menu:
 - ❑ In the KDE desktop environment, click the **K** button and select the **MG-SOFT Trap Ringer Pro / Trap Ringer Pro** command.
 - ❑ Or, in the GNOME desktop environment, click the **GNOME** start button and select the **MG-SOFT Trap Ringer Pro / Trap Ringer Pro** command.

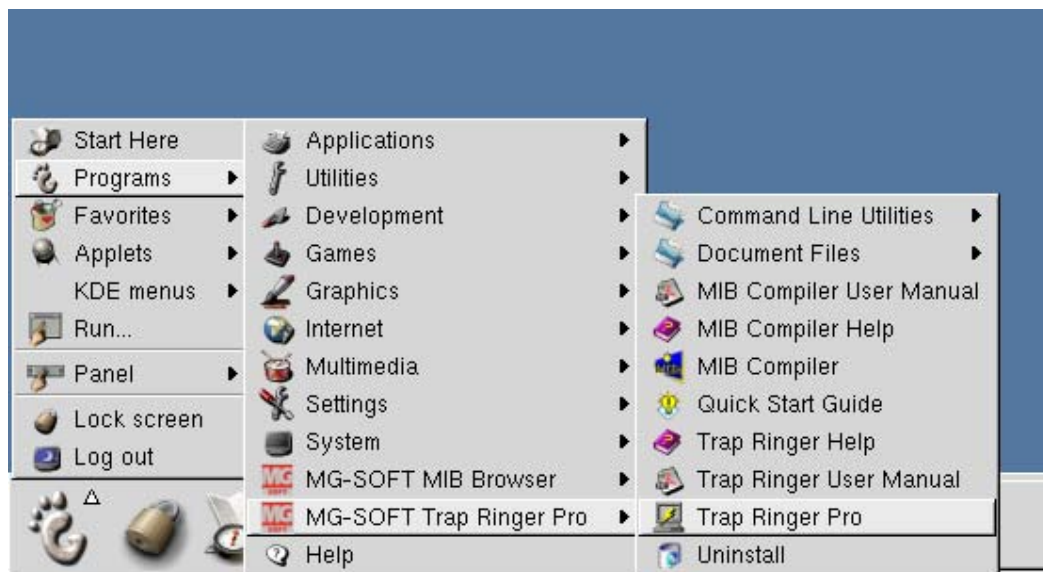


Figure 1: Starting Trap Ringer on Linux GNOME desktop environment

2. As the program starts, the MG-SOFT Trap Ringer splash screen appears, displaying the company name and announcing the program itself.
3. The Trap Ringer client desktop appears.
4. Trap Ringer client automatically connects to the Trap Ringer server application and displays received SNMP notifications in the main window (provided that the console or log-file monitoring option is enabled). If the Trap Ringer server is not running, use the **Tools / Start Service** command to launch it manually (requires root privileges).

Note: By default, Trap Ringer server daemon is started automatically at the system startup. You can change this behavior by unchecking the **Start service at system startup** checkbox in Trap Ringer Preferences dialog box, General tab.

3.3 Starting Trap Ringer on Mac OS X

1. Open the **Finder** and select the **Applications** folder in the panel on the left.
2. Expand the **MG-SOFT Trap Ringer Pro** folder in the Finder and double-click the **Trap Ringer Pro** entry to launch Trap Ringer (Figure 2).
3. As the program starts, the MG-SOFT Trap Ringer splash screen appears, displaying the company name and announcing the program itself.
4. The Trap Ringer client desktop appears.

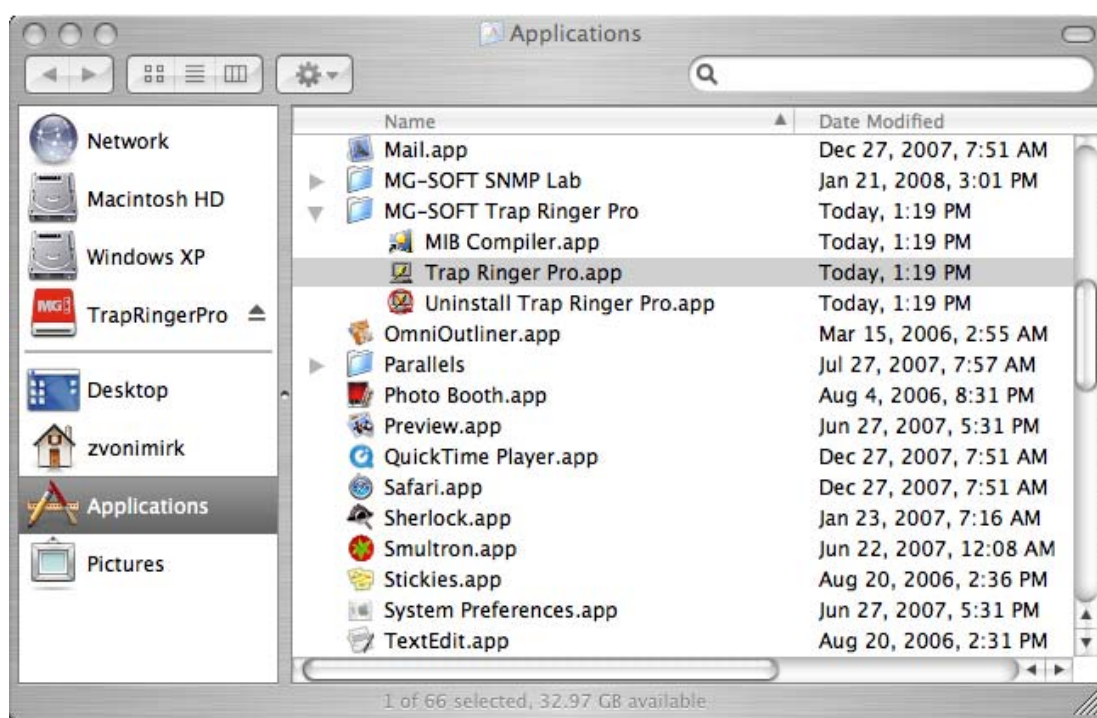


Figure 2: Launching Trap Ringer from the Finder on Mac OS X

5. Trap Ringer client connects to the Trap Ringer server application and displays received SNMP notifications in the main window (provided that the console or log-file monitoring option is enabled). If the Trap Ringer server is not running, use the **Tools / Start Service** command to launch it manually (requires admin privileges).

Note: By default, Trap Ringer server daemon is started automatically at the system startup. You can change this behavior by unchecking the **Start service at system startup** checkbox in Trap Ringer Preferences dialog box, General tab.

3.4 Starting Trap Ringer on Solaris

The easiest way to start Trap Ringer under Solaris operating system is to use the Java Desktop System (JDS) Launch menu or Gnome Applications menu. In the CDE desktop environment, Trap Ringer and other bundled applications can only be launched from a command line.

1. In JDS environment, display the **Launch** menu by clicking the taskbar **Launch** button (Figure 3).
2. To start Trap Ringer, use the **Applications / MG-SOFT Trap Ringer / Trap Ringer** command.
3. As the program starts, the MG-SOFT Trap Ringer splash screen appears, displaying the company name and announcing the program itself.
4. The Trap Ringer client desktop appears.



Figure 3: Starting Trap Ringer on Solaris (JDS environment)

5. Trap Ringer client connects to the Trap Ringer server application and displays received SNMP notifications in the main window (provided that the console or log-file monitoring option is enabled). If the Trap Ringer server is not running, use the **Tools / Start Service** command to launch it manually (requires root user privileges).

Note: By default, Trap Ringer server daemon is started automatically at the system startup. You can change this behavior by unchecking the **Start service at system startup** checkbox in Trap Ringer Preferences dialog box, General tab.

Tip: You can also start Trap Ringer from a terminal window by using the following command:

```
#/usr/local/mg-soft/mgtrapringer/bin/mgtrapringer.sh
```

In the CDE desktop environment, Trap Ringer can be launched only from a command line.

3.5 Trap Ringer Desktop

The Trap Ringer client desktop follows the conventions of the appearance and functionality of the general Windows graphical user interface in that it has a title bar, menu bar, toolbar, status bar, and minimize, maximize and close buttons, but it differs in specific areas.

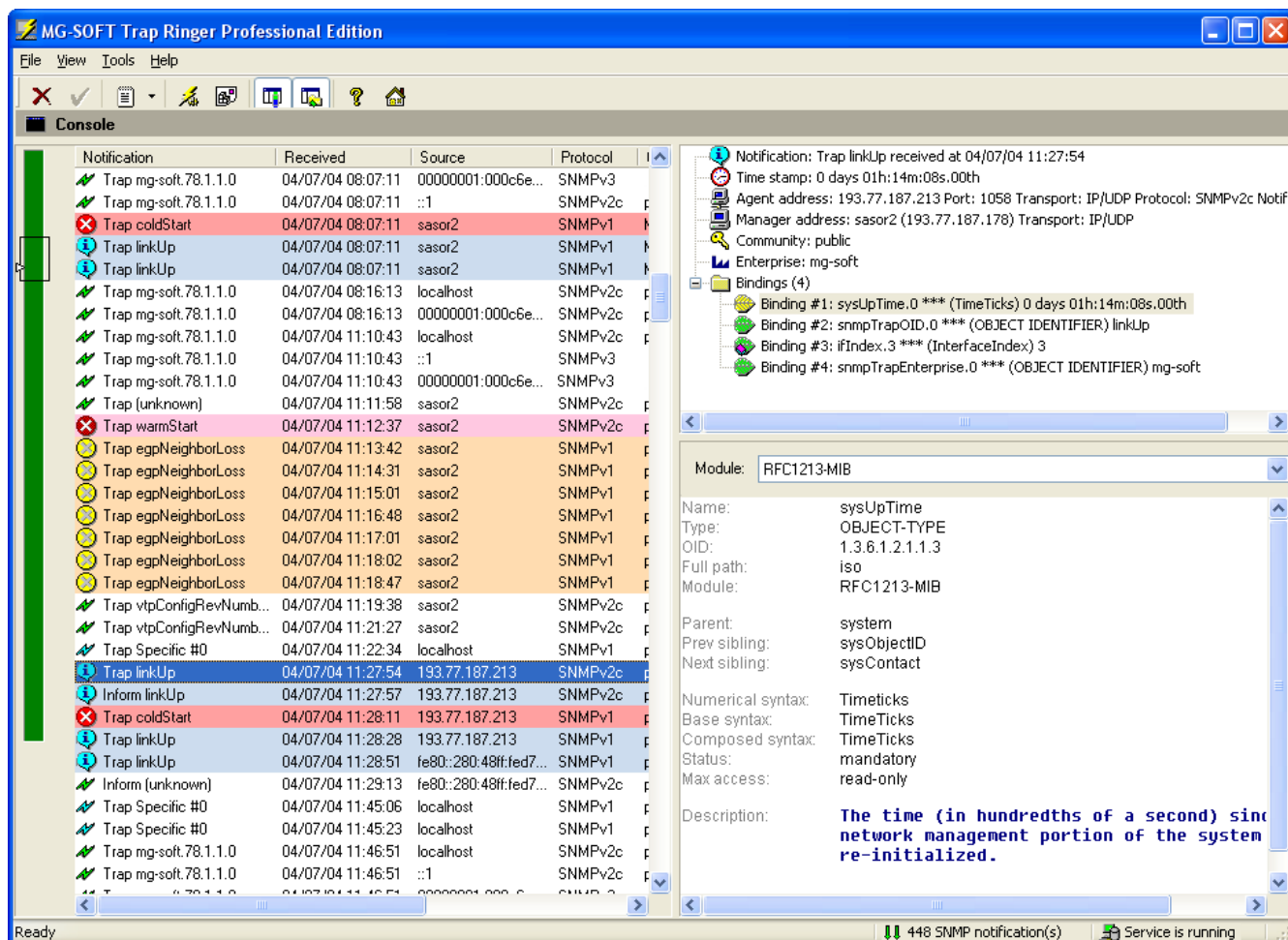


Figure 4: Trap Ringer desktop

Menu bar

Menu bar is the bar near the top of the application window that contains names of the program menus. It contains the menus such as File, View, Tools, etc.

Toolbar

The toolbar contains a group of buttons that provide quick access to a series of commands. To display or hide the toolbar, use the **View / Toolbars** command. You can get a brief description of a task behind each toolbar button either in a tooltip, or in the Status bar, by placing the mouse cursor on the toolbar button (without clicking).

Working area

The working area is the area between the toolbar and the status bar. Each window or dialog box you open will be displayed in this working area. The Trap Ringer main window is used for viewing received SNMP Trap and Inform notifications. It consists of the Trap

List window panel, displaying the list of received SNMP notifications and the Trap Details Window panel, showing detailed information about SNMP notification messages.

Status bar

The Trap Ringer status bar contains the following fields:

- ❑ The leftmost field displays the operating status of Trap Ringer client and description of operations behind the toolbar buttons and menu commands.
- ❑ When the client is connected to the server, the middle field shows the number of SNMP notification in the log file currently displayed in the Trap List window panel. When a search operation is started, the middle field displays the "Opening query..." message and when search results are displayed, the middle field shows the number of found SNMP notifications and the total number of SNMP notifications in the given log file, separated by "/", e.g., "123 / 567 SNMP notification(s)". Furthermore, the status of the selected log file is indicated by one of the following icons:



- Indicates that currently displayed log file is not full and that information about received notifications is being appended to the existing information in that log file.



- Indicates that currently displayed log file is full and that the oldest logged notifications are being overwritten (log is rotating).

When the client is not connected to the server, the middle status bar field displays the "Disconnected" message.

- ❑ The rightmost field displays the current status of Trap Ringer server (i.e., "The service is running", "The service is not running" or the "Service is starting").

Thumbnail Scrollbar

The thumbnail scrollbar is the vertical scrollbar along the left edge of the main window that features a small frame with a pointer (thumbnail). When Trap Ringer client connects to the server, the thumbnail scrollbar visually indicates whether the SNMP notification data is being successfully transmitted from server to client by gradually coloring the portion of the thumbnail scrollbar that corresponds to the requested data from white to blue and, when the data is successfully transmitted, from blue to green. The black rectangular frame in the thumbnail scrollbar represents the portion of SNMP notifications currently displayed in the main window (Trap List window panel), and the small triangle-shaped pointer represents the line selected in the Trap List window panel. Click anywhere in the thumbnail scrollbar to quickly move the rectangular frame to that location and view other notifications. To display or hide the thumbnail scrollbar, use the **View / Thumbnail Scrollbar** command.

3.5.1 Trap List Window Panel

The Trap List panel occupies the left part of the Trap Ringer main window ([Figure 4](#)) and displays a list of received SNMP Trap and Inform notifications. SNMP notifications are listed top-down in the order they were received. By default, Trap List window panel displays SNMP notifications that are logged in the console log file. If the file-log monitoring option is used, you can also display the contents of the log files in the Trap List window panel.

To switch between viewing the contents of the console log file and other log files use the **View / Console** and **View / Log File** commands.

The Trap List window panel is updated every time a new SNMP Trap or Inform notification is received and the notification information is written to the currently viewed log file (console log or file log).

The Trap List window panel can display information about received SNMP notifications either in multiple columns or in a single (customizable) column. The preferred way of displaying the notification data can be configured in the Trap Ringer Preferences dialog box, Display tab

By default, the Trap List window panel displays trap information in multiple columns. These columns are (the last three columns can be displayed by checking their checkboxes on the Display tab of the Trap Ringer Preferences dialog box):

Notification

Displays the basic information about the received SNMP Trap or Inform notification, including the type of notification (“Trap” or “Inform”) and its name (e.g., “linkUp”) as resolved through loaded MIB modules.

Received

Shows the date and time of notification reception in MM/DD/YY hh:mm:ss format.

Source

Shows the IPv4 or IPv6 address or the hostname of the SNMP entity that issued the notification.

Protocol

Shows the SNMP protocol version of the received Trap or Inform (e.g., “SNMPv2c”).

Community

Displays the community name included in the received SNMPv1 or SNMPv2c notification message (e.g., “public”).

Enterprise

Displays the name or OID of the enterprise (organization) associated with the SNMP notification message (If this information is available).

Binding Count

Displays the number of variable bindings included in the SNMP notification message.

When notifications arrive and are displayed in the Trap List window panel, they are not acknowledged. To acknowledge all received notifications, select the **File / Acknowledge Notifications** command and all trap notifications will be acknowledged without clearing them from the Trap List.

More details of the selected notification can be seen in the [Trap Details Window Panel](#).

3.5.2 Trap Details Window Panel

The Trap Details window panel, when displayed, occupies the right part of Trap Ringer main window (with the Trap List window panel being displayed on the left). The Trap Details window panel shows detailed information about the received SNMP notification messages.

To view more information about a received SNMP Trap or Inform notification, do the following:

1. If the Trap Details window panel is not displayed, select the **View / Trap Details** command or click the **Trap Details** toolbar button to display it.
2. Click any notification in the Trap List window panel, to view all available information about it in the Trap Details upper window panel, like the notification's Time stamp, Agent address, Bindings, SNMPv3 Security parameters, etc.
3. If there is any variable binding listed under the Bindings item in the upper Trap Details window panel, click it to view its properties in the lower panel. For example, if the selected variable binding contains the `sysUpTime.0` variable, Trap Ringer will display the properties of the `sysUpTime` MIB object, e.g., its Name, Type, OID, Syntax, Description, etc. Trap Ringer retrieves this information from the loaded MIB modules.

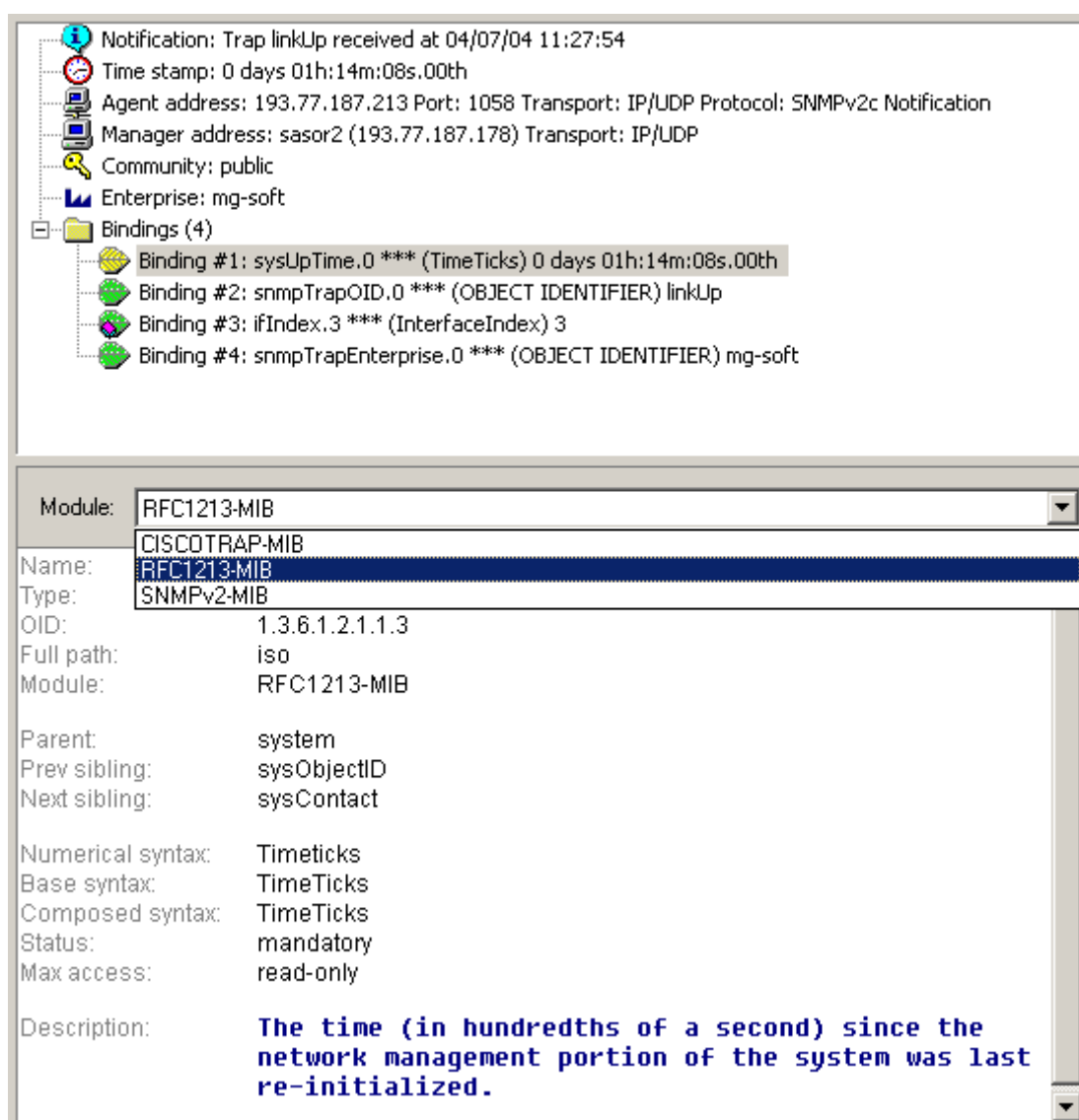


Figure 5: Trap Details window panel

The Module drop-down list in the lower Trap Details window panel lists the MIB module(s) that define the MIB object selected in the upper panel. If more than one MIB module is

listed, you can switch between them to view MIB object properties as defined by any of the listed MIB modules.

Note: If none of the loaded MIB modules contain the definition of the MIB object included in the notification's variable binding, such variable binding is displayed with a leaf icon with question mark (in the upper Trap Details window panel). This denotes that you should load the relevant MIB module in order to view the properties of this MIB object. MIB modules can be loaded in the Trap Ringer Preferences dialog box, [MIB Modules tab](#).

4 APPLY LICENSE KEY

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

1. If you have received your `license.key` file on a USB flash card (WalletFlash), insert the card into a free USB port on your computer and allow the operating system to install the necessary drivers to use the flash drive.
2. Select the **Help / Apply License** command from the main menu.
3. The Apply License dialog box (Figure 7) appears. Click the **Select** button in the Apply License dialog box to display the Open dialog box (Figure 6).

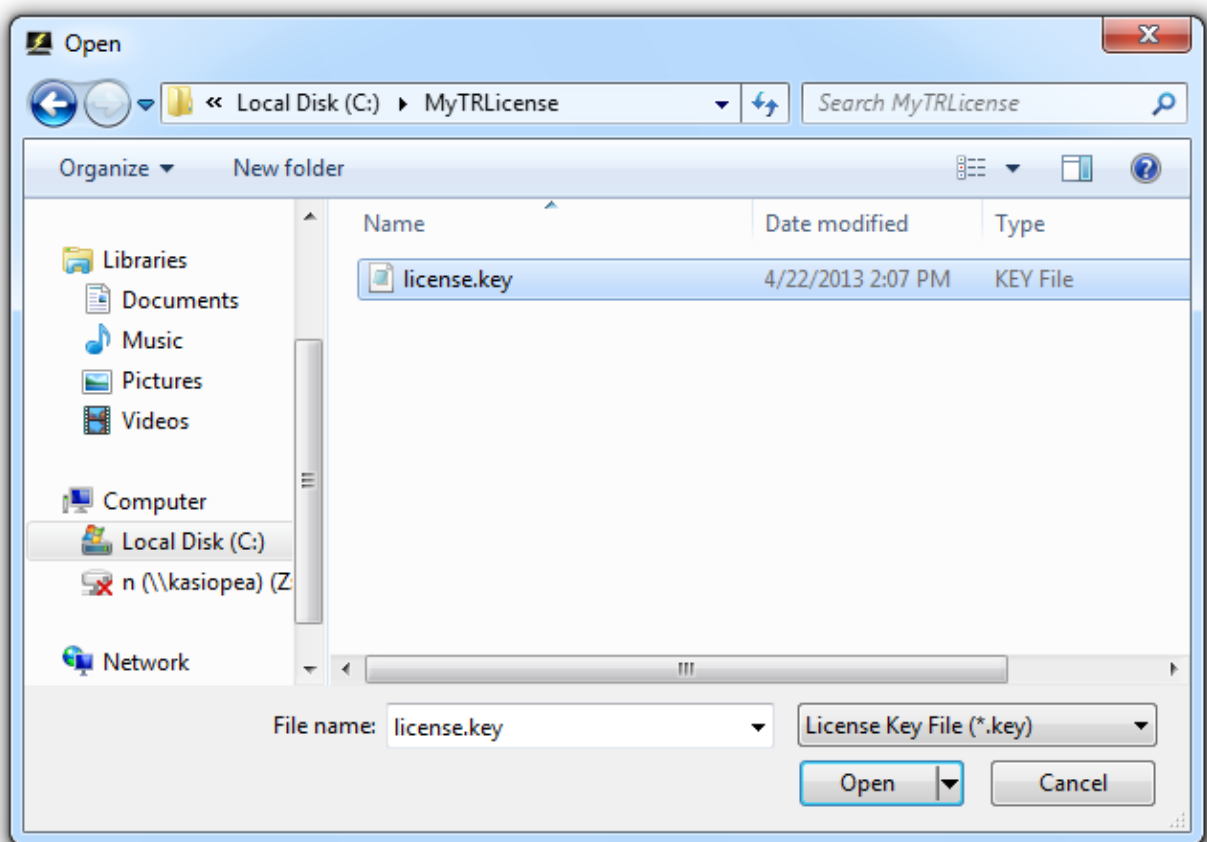


Figure 6: Selecting the license.key file

4. Navigate to the drive and folder containing your `license.key` file for MG-SOFT Trap Ringer Professional Edition. Select the `license.key` file and click the **Open** button (Figure 6).

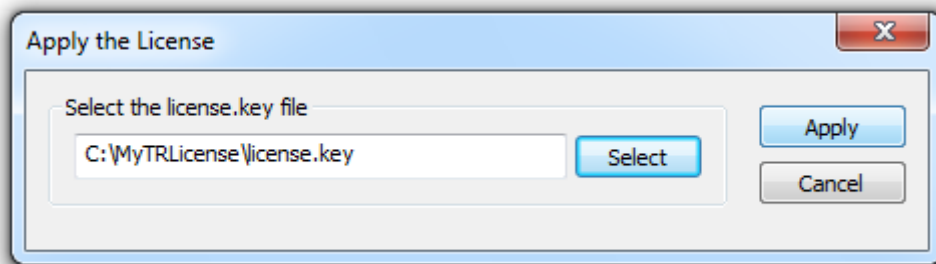


Figure 7: Applying the license.key file

5. Click the **Apply** button in the Apply License dialog box (Figure 7). The software will copy the specified `license.key` file to the proper location in order for Trap Ringer to read it and unlock its features accordingly (after a restart).

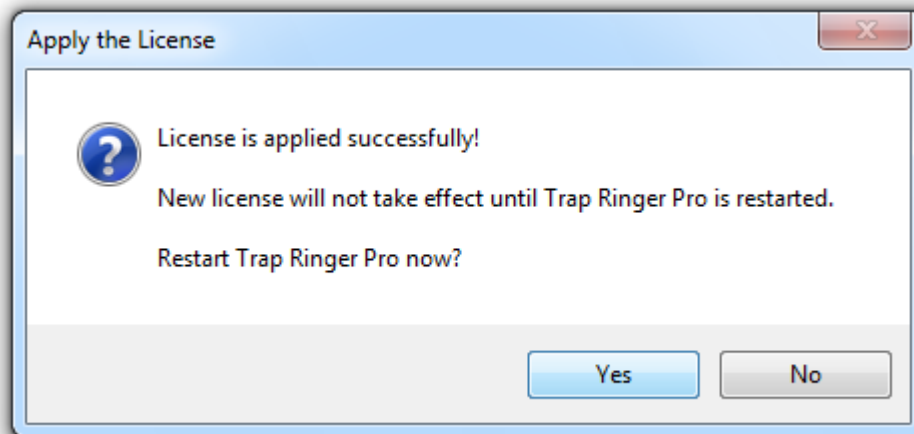


Figure 8: Applying the license.key file - restarting Trap Ringer

6. On Windows operating systems, click the **Yes** option in the dialog box that prompts you to restart Trap Ringer. Both parts of the application (Trap Ringer client and service) will be restarted. Allow the restart if you are prompted for consent by the operating system during this process. On Linux and other operating systems, restart Trap Ringer manually. After Trap Ringer restart, the selected license should be applied and you can start using the software.

Tip: You can check if the license key has been properly applied by verifying if the About Trap Ringer dialog box (accessible via the **Help / About** command) displays your license details correctly.

5 CONFIGURING SNMPV3 USERS

To enable receiving SNMPv3 Trap and Inform messages, or to make the forwarding of received notifications by means of the SNMPv3 protocol possible, you need to create and configure a corresponding SNMPv3 user profile in Trap Ringer. Trap Ringer lets you configure any number of SNMPv3 user profiles.

SNMPv3 user profiles are configured in the Trap Ringer Preferences dialog box, SNMPv3 Users tab. For detailed description of parameters available in this tab, consult the “User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)” specification ([RFC 3414](#)).

Note 1: You can skip reading this section if none of the monitored devices sends SNMPv3 notification messages to Trap Ringer and if Trap Ringer does not **forward** SNMPv3 notification messages to other network nodes.

Note 2: Out-of-the-box, Trap Ringer receives all SNMPv1 and SNMPv2c notification messages sent to the default trap ports of the PC running Trap Ringer. These ports are IPv4/UDP 162, and if the IPv6 protocol is installed, also IPv6/UDP 162 port. Ports on which Trap Ringer listens to for incoming SNMP notification messages can be configured in the Trap Ringer Preferences dialog box, Ports tab. For details on setting Trap Ringer preferences, please consult Trap Ringer Help documentation.

To create an SNMPv3 user profile and configure its SNMPv3 security parameters:

1. Select the **Tools / Trap Ringer Preferences** command to open the Trap Ringer Preferences dialog box and switch to the SNMPv3 Users tab.

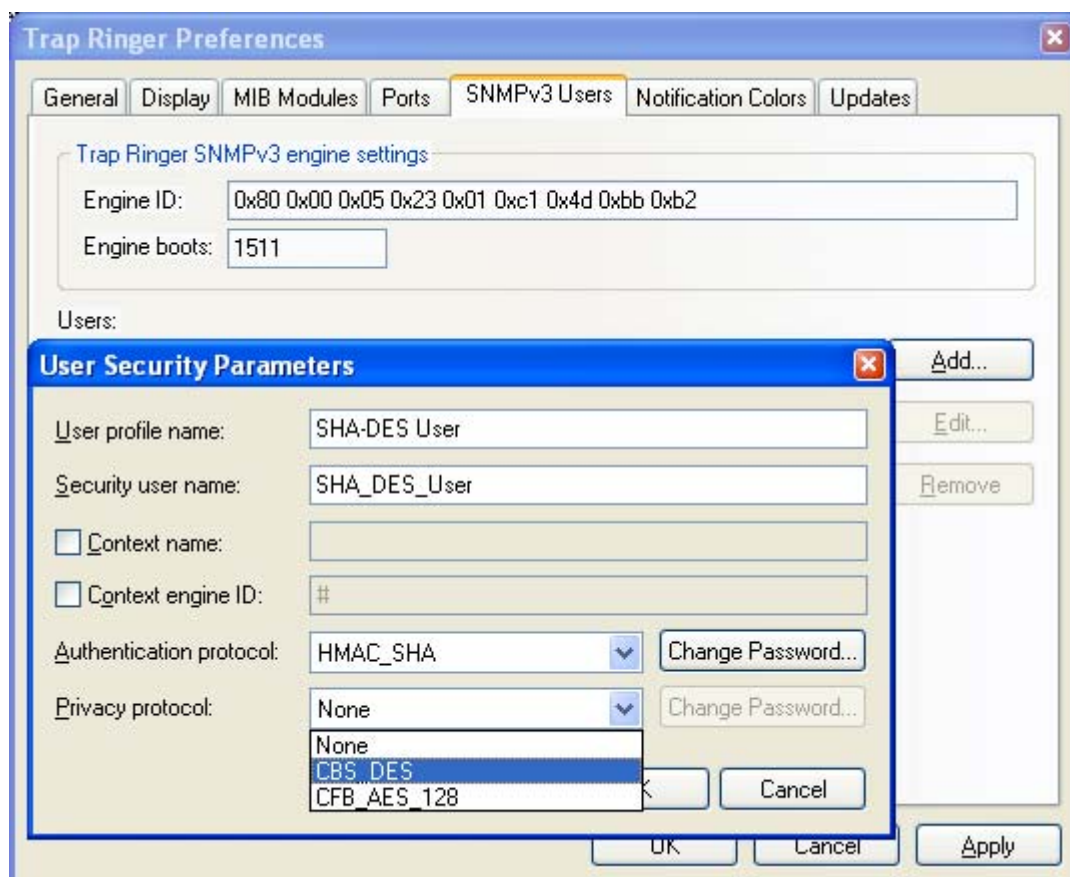


Figure 9: Configuring SNMPv3 users

2. The **Trap Ringer SNMPv3 engine settings** frame in the SNMPv3 Users tab displays two read-only Trap Ringer SNMPv3 engine parameters as read from the system registry - the **Engine ID** and **Engine boots** values (Figure 9). These values are provided for your reference only.
3. The Users list displays a list of registered SNMPv3 user profiles. Select a user profile and use the **Edit** button to view or edit SNMPv3 security parameters of the given SNMPv3 user. To remove the selected SNMPv3 user profile from the Users list, click the **Remove** button.

Note: An SNMPv3 user cannot be removed if it is being currently used by any **Forward output unit**.

4. Click the **Add** button to create a new SNMPv3 user profile. The User Security Parameters dialog box appears, where you can configure the following security parameters for the new SNMPv3 user (Figure 9):
 - ❑ Into the **User profile name** input line, enter a desired user profile name. The user profile name is only a label name, under which you store the current set of the SNMPv3 user security parameters in Trap Ringer (the entered value has no effect on the SNMPv3 protocol itself).
 - ❑ Into the **Security user name** input line, enter the name of the SNMPv3 user.
 - ❑ The **Context name** checkbox should normally be left unchecked. You should check this checkbox and enter a context name value into the accompanying input line only if you want to set the context name to a specific value in all outgoing SNMPv3 notification messages sent by a Trap Ringer **Forward output unit** that will use this SNMPv3 user profile. Note that this setting is not used for checking the context name in incoming SNMPv3 notification messages; it is used solely for setting the context name in outgoing (forwarded) SNMPv3 notifications. If the Context name checkbox is not checked and Trap Ringer is simply forwarding received SNMPv3 notification messages (no PDU translation occurs), the context name value from the original SNMPv3 notification message received by Trap Ringer will be inserted into outgoing (forwarded) SNMP notification messages. If the Context name checkbox is not checked and Trap Ringer is translating received SNMPv1 and SNMPv2c notification messages and forwarding them as SNMPv3 Trap or Inform messages, a blank (zero-length) context name will be used.
 - ❑ The **Context engine ID** checkbox should normally be left unchecked. You should check this checkbox and enter a value into the accompanying input line only if you want to set the context engine ID to a specific value in all outgoing SNMPv3 notification messages sent by a Trap Ringer **Forward output unit** that will use this SNMPv3 user profile. Note that this setting is not used for checking the context engine ID value in incoming SNMPv3 notification messages. Normally, you should configure the context engine ID value only in case Trap Ringer forwards SNMPv3 notifications to another SNMP proxy application. If the checkbox is not checked and Trap Ringer is simply forwarding received SNMPv3 notification messages (no PDU translation occurs), the context engine ID value from the original notification message received by Trap Ringer will be used. If the checkbox is not checked and Trap Ringer is translating received SNMPv1 and SNMPv2c notification messages and forwarding them as SNMPv3 Trap or Inform messages, the Trap Ringer's engine ID value or the Inform

receiver's engine ID value will be inserted into outgoing SNMPv3 notifications, respectively.

To set the context engine ID value for outgoing SNMPv3 notifications, enter a properly formatted binary value by starting the line with the '#' character and continue with any number of character codes in hexadecimal (prefix 0x) notation. For example, the following value:

```
# 0x12 0x34 0xef
```

will set the context engine ID field in outgoing SNMPv3 notification messages to value 1234EF (hex).

- ❑ Select the SNMPv3 authentication protocol from **the Authentication protocol** drop-down list. When selecting an entry other than **None** from this drop-down list, click the **Change Password** button to enter the authentication password. This will open the Password For Authentication Protocol dialog box.



Figure 10: Entering the SNMPv3 authentication protocol password

- ❑ Enter the authentication password into the **Password** input line and confirm it by reentering it into the **Password confirmation** input line below. To view the characters you type into both input lines, uncheck the **Hide typing** checkbox.
- ❑ Click the **OK** button. The Password For Authentication Protocol dialog box closes.
- ❑ Select the SNMPv3 privacy protocol from the **Privacy Protocol** drop-down list and click the **Change Password** button (except when selecting the **None** entry).
- ❑ The Password For Privacy Protocol dialog box appears (Figure 10).

Note: The Password For Authentication Protocol dialog box and the Password For Privacy Protocol dialog box have the same appearance.

- ❑ Enter the privacy password into the first **Password** input line and confirm it by reentering it into the **Password confirmation** input line. To view the characters you type into both input lines, uncheck the **Hide typing** checkbox. Close the dialog box by clicking the **OK** button.
5. After specifying all parameters, click the **OK** button. The User Security Parameters dialog box closes and the newly configured SNMPv3 user is added to the Users list in the Trap Ringer Preferences dialog box, SNMPv3 Users tab (Figure 9).

6. Click the **OK** button to close the Trap Ringer Preferences dialog box and apply new settings. From this moment on, Trap Ringer will receive SNMPv3 Trap and Inform notification messages issued by SNMPv3 agents on behalf of the configured SNMPv3 user (e.g., `SHA_DES_User`). Furthermore, the given user profile will be available for selection in the Forward Preferences panel's **User** drop-down list, meaning that it can be used for sending out (forwarding) SNMPv3 notification messages. To enable receiving or forwarding SNMPv3 notification messages on behalf of other SNMPv3 users, add additional user profiles to the Users lists in the SNMPv3 Users tab (Trap Ringer Preferences dialog box) by following the above procedure.
7. To view the SNMPv3 security parameters of a received SNMPv3 notification, select a notification in the **Trap List** (left) panel of the main window and expand the **Security parameters** tree in the upper **Trap Details** (right) window panel (Figure 11).

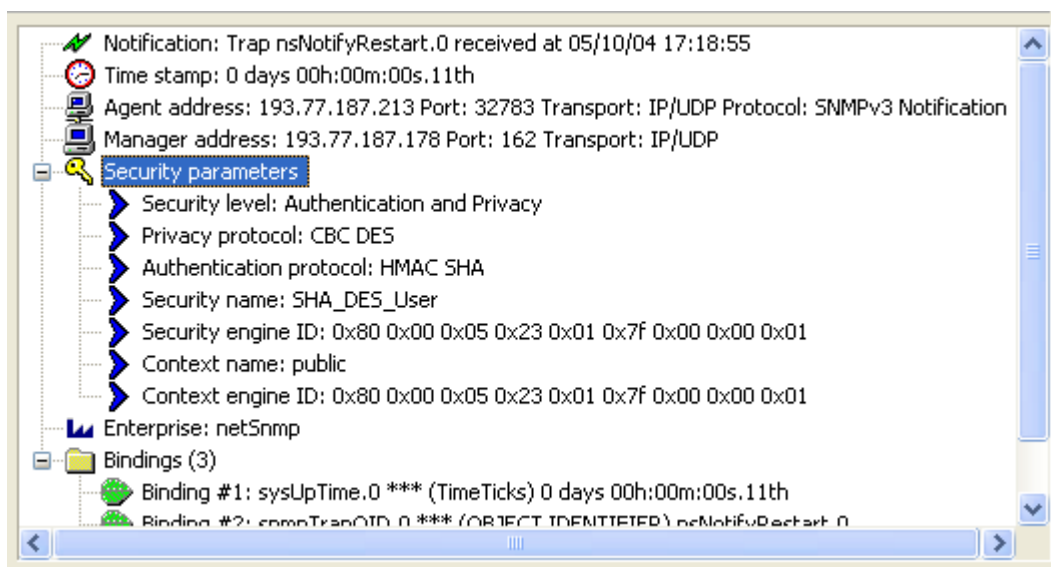


Figure 11: Viewing properties of received SNMPv3 notifications in Trap Details window panel

6 CONFIGURING SNMP NOTIFICATION MONITORING OPTIONS

MG-SOFT Trap Ringer lets you simultaneously monitor SNMP Trap and Inform notification messages in many ways. Different ways of notification monitoring are complementary. For example, the daily logging of SNMP notifications can be set (e.g., each day a new log file is created) in addition to other monitoring options. Received SNMP notifications can invoke external programs, or can be logged to the console log or to a continuous log file. Trap Ringer can also send e-mail or SMS messages whenever a new SNMP notification is received, generate and periodically update HTML report files (Web pages) containing information about received SNMP notifications, and/or create the event log messages (on Windows) or the syslog messages (on Unix-like operating systems).

In addition, Trap Ringer also incorporates the SNMP notification proxy forwarder application capabilities, meaning that it can forward received SNMP notifications to other SNMP management stations and optionally translate incoming SNMP notification messages to the selected SNMP version (SNMPv1 or SNMPv2c or SNMPv3) and type (Trap or Inform).

Options for monitoring SNMP Trap and Inform notifications are configured in the Output Manager Preferences dialog box. This section provides step-by-step instructions on how to configure available monitoring options in Trap Ringer.

In addition to using different monitoring options, the Output Manager Preferences dialog box lets you set up filters to allow only the notifications that match the filter conditions to pass through, as described in the [Filtering SNMP Notifications](#) section of this manual.

About monitoring options, output units and filters

The monitoring options and associated output units and filters are displayed as a tree structure in the left panel of the Output Manager Preferences dialog box (**Tools / Output Manager Preferences**). This gives you a clear overview of available and enabled output units and associated filters ([Figure 12](#)).

Monitoring options (Console, Command, Log, Mail, etc.) represent different ways (methods) of monitoring SNMP notifications. Every monitoring option can have zero, one or more subordinated output units (e.g., Command, Command (2), Log, Log(2), Log (3), etc.), except the Console monitoring option, which has exactly one output unit. For example, several Mail output units under the Mail monitoring option enable sending e-mails to different recipients.

An output unit can have any number of filters attached in order to pass only those SNMP notifications that match the filter conditions to the output unit (filtering out all other notifications).

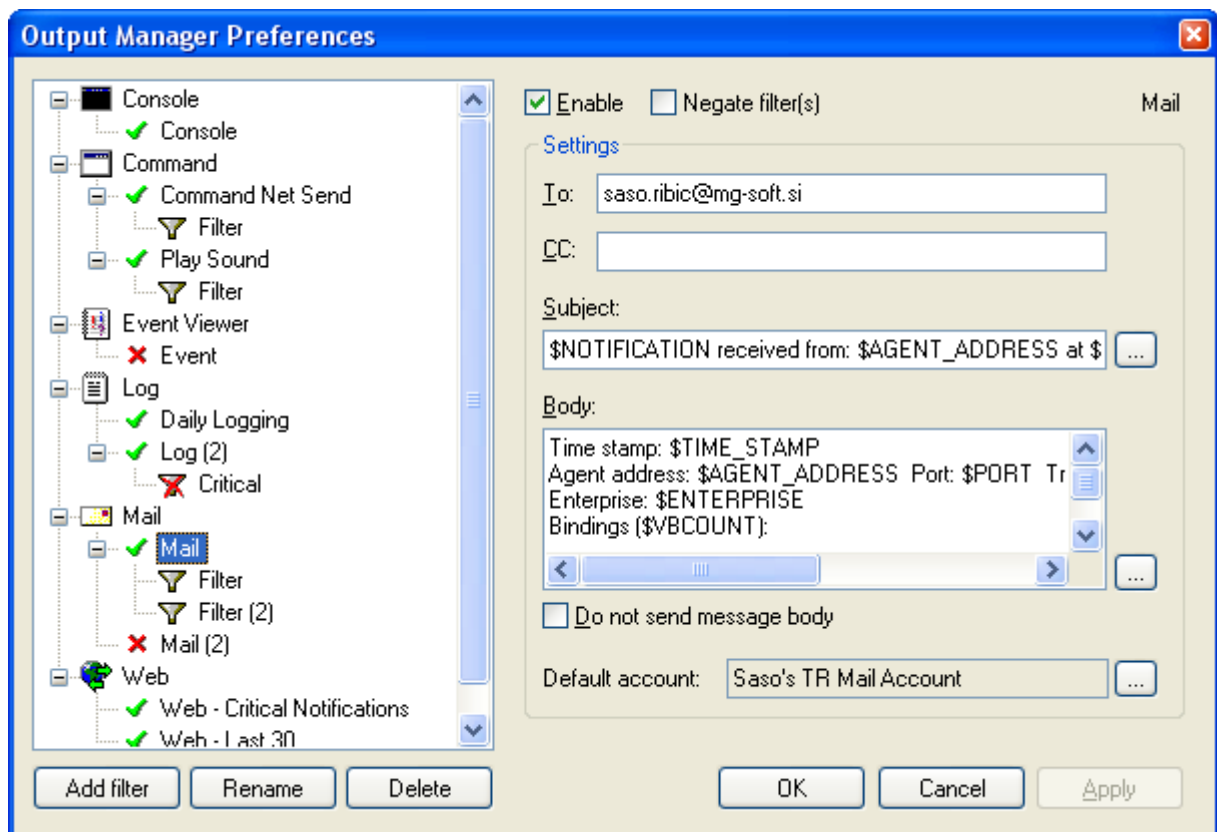


Figure 12: The Output Manager Preferences dialog box

Output units and filters can be enabled or disabled. Only enabled output units and filters are effective. The following icons in the tree structure of the Output Manager Preferences dialog box (Figure 12) indicate different states of output units and associated filters:

- ✓ - output unit is enabled
- ✗ - output unit is disabled
- 🔍 - filter is enabled
- ✗ - filter is disabled
- 🔍 - filter is enabled, but negated (its conditions are logically inverted)

6.1 Console Monitoring

The console monitoring option enables you to view received SNMP notification messages directly in the Trap Ringer main window. This option is typically used for on-line trap monitoring. The console monitoring is the only monitoring option that is enabled by default, meaning that by default all received SNMP notifications are logged to the console log file. On the first Trap Ringer client startup, the content of the console log is automatically displayed in the main window.

To configure the console monitoring preferences:

1. Open the Output Manager Preferences dialog box by selecting the **Tools / Output Manager Preferences** command or by clicking the **Output Manager Preferences** toolbar button.

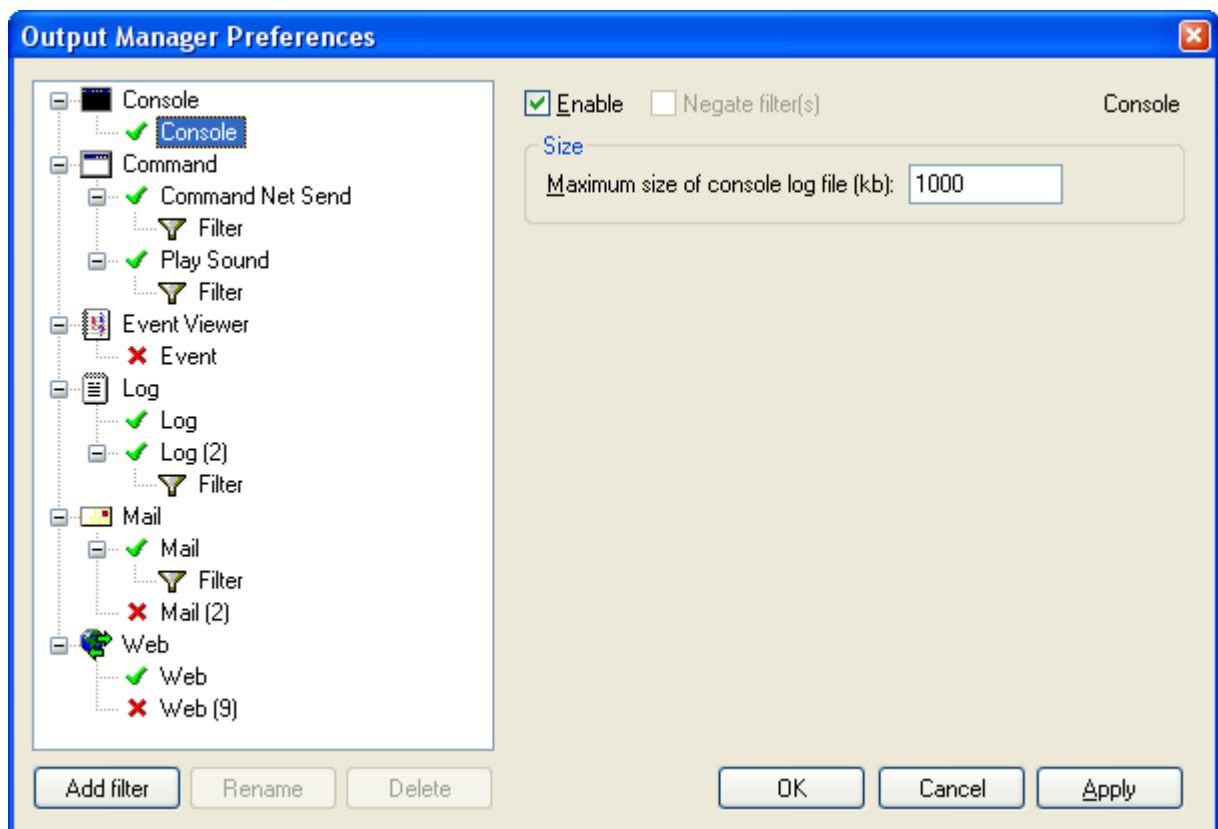


Figure 13: Configuring Console output unit options

2. Click the Console output unit in the Output Manager tree structure to display the Console Preferences window panel. If the Console output unit is not enabled, check the **Enable** checkbox to enable it.

Note: The **Negate Filter(s)** checkbox is enabled only if one or more filters are added to the output unit. This checkbox can be used to logically negate (invert) all filters associated with the output unit. For more information on filters, consult the **Filtering SNMP Notifications** section.

3. In the **Size** frame, set the maximum size (in kilobytes) of the console log file. This will limit the number of SNMP notifications being logged, automatically overwriting the oldest logged notifications.
4. Click the **OK** button to apply the settings and close the Output Manager Preferences dialog box.
5. Select the **View / Console** menu command to display the contents of the console log in the main window.
6. The received Trap and Inform notifications will be displayed in the Trap List panel in the main window.
7. Select a notification from the list to view its detailed information in the Trap Details panel of the main window. If this panel is not displayed, you can display it by using the **View / Trap Details** command.

Tip: If you do not want all received SNMP notification to be logged and displayed in the Console, you can add one or more filters to the Console output unit. See the [Filtering SNMP Notifications](#) section for more details on this.

6.2 Log-File Monitoring

The received SNMP Trap and Inform notifications can be logged to files. The log-file monitoring option is similar to the console monitoring option in a sense that the contents of log files can be viewed in the Trap Ringer main window. The main difference between both monitoring options is that there can be only one Console output unit, while you can configure any number of Log output units and that besides continuous (ring) log file a Log output unit can generate also daily log files, or automatically create a new log file whenever the existing one is full (i.e., when it reaches the max. file size limit).

6.2.1 Configuring Ring Log File Preferences


1. Open the Output Manager Preferences dialog box by selecting the **Tools / Output Manager Preferences** command or by clicking the **Output Manager Preferences** toolbar button. 
2. Select an existing Log output unit from the Output Manager tree structure to display the Log Preferences window panel. Alternatively, you can create a new Log output unit by selecting the Log monitoring option and clicking the **Add** button or choosing the **Add** pop-up command (Figure 14). The new “Log (2)” output unit appears as a child item of the Log monitoring option. To rename the output unit, use the **Rename** pop-up command and enter a new name for it.



Figure 14: Creating a new Log output unit

3. To enable configuring the selected Log output unit, check the **Enable** checkbox in the right panel of the Output Manager Preferences dialog box.

Note: The **Negate Filter(s)** checkbox is enabled only if one or more filters are added to the output unit. This checkbox can be used to logically negate (invert) all filters associated with the output unit. For more information on filters, consult the **Filtering SNMP Notifications** section.

4. Check the **Ring file** radio button in the Logging frame to enable continuous logging of notifications to the specified file until the Log output unit is disabled or the Trap Ringer server is stopped. This type of logging also starts automatically overwriting the oldest logged notifications when the max. ring log file is reached.

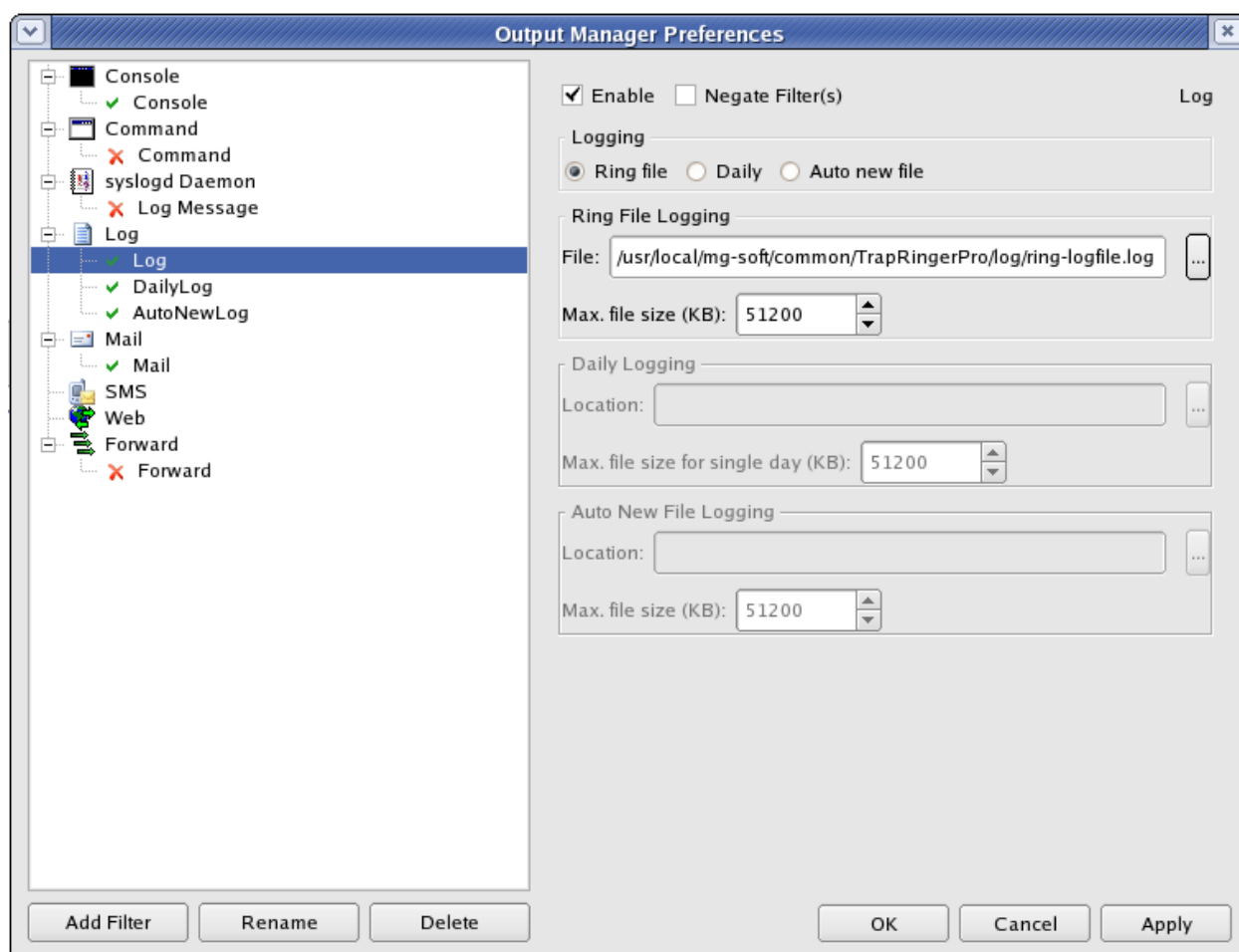



Figure 15: Configuring Log output unit options

5. Into the **File** input line in the Ring File Logging frame, enter the full path and the name of the log file to be created (e.g., on Windows: D:\Trap Ringer Logs\MyLog.log), or use the **Browse (...)** button to navigate to the desired folder and enter the log file name.
6. In the **Max. file size** input line, enter the maximum size of the log file (in kilobytes). This will limit the number of SNMP notifications being logged, automatically overwriting the oldest logged notifications (when the maximum file size is reached).
7. Click the **OK** button to apply the settings and close the Output Manager Preferences dialog box.
8. To display the contents of the ring log file in the main window, select the **View / Log / <Log Name>** menu command.
9. The Trap and Inform notifications logged in the ring log file will be displayed in the Trap List panel in the main window.
10. Select a notification from the list to view its detailed information in the Trap Details panel of the main window. If this panel is not displayed, you can display it by using the **View / Trap Details** command.

Tip: If you do not want all received SNMP notification to be logged to this log file, add one or more filters to the relevant log output unit. See the [Filtering SNMP Notifications](#) section for more details on adding and configuring filters.

6.2.2 Configuring Daily Logging Preferences

1. Open the Output Manager Preferences dialog box by selecting the **Tools / Output Manager Preferences** command or by clicking the **Output Manager Preferences** toolbar button. 
2. Select an existing Log output unit from the Output Manager tree structure to display the Log Preferences window panel. Alternatively, you can create a new Log output unit by selecting the Log monitoring option and using the **Add** pop-up command (Figure 14).
3. To enable configuring the selected Log output unit, check the **Enable** checkbox in the right panel of the Output Manager Preferences dialog box (Figure 16).

Note: The **Negate Filter(s)** checkbox is enabled only if one or more filters are added to the output unit. This checkbox can be used to logically negate (invert) all filters associated with the output unit. For more information on filters, consult the [Filtering SNMP Notifications](#) section.

4. Check the **Daily** radio button in the Logging frame to enable the daily logging type. Trap Ringer server will automatically create a new log file for each day and store log files to the location specified below.

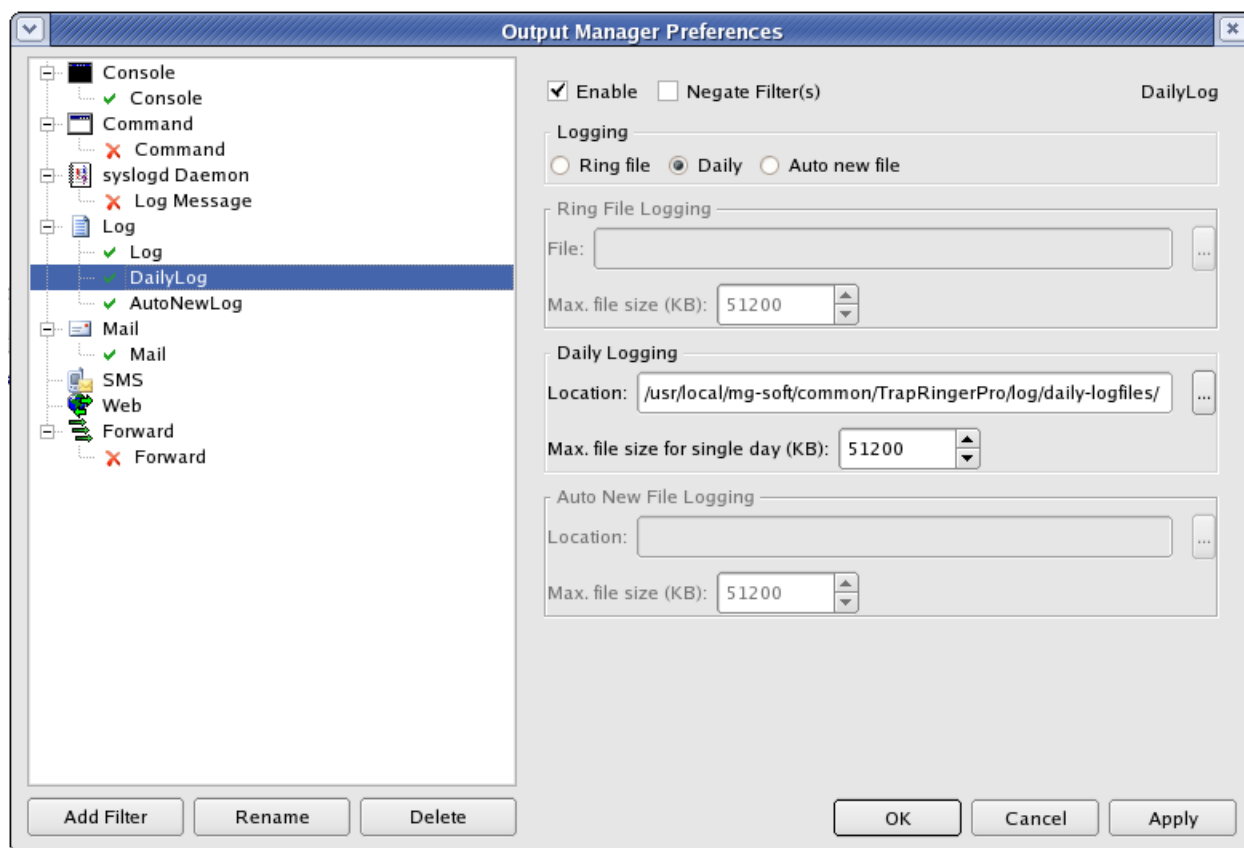


Figure 16: Configuring daily logging options

5. Into the **Location** input line, specify the full path of the folder where the daily log files will be saved. By default, this is the “Log” subfolder of the Trap Ringer installation folder. The generated log files will be named according to the following scheme:

TRDailyLog_YYYYMMDD.log

...where the characters following the underscore character (_) indicate the year, month and day of the daily log file, e.g., 20100422 stands for April 22nd 2010.


6. Into the **Max. file size for single day** input line, specify the maximum file size for the daily log file (in kilobytes). This will limit the number of notifications being logged in the daily log files; automatically disposing the oldest logged notifications in case log files exceed the maximum size given.
7. Click the **OK** button to apply the settings and close the Output Manager Preferences dialog box.
8. To display the contents of the daily log file in the main window, select the **View / Log / <Log Name>** menu command.
9. The contents of the daily log file for the current day will be displayed in the Trap List panel in the main window.

Tip: To view the daily log for any previous day, use the **File / Open** command and point the standard Open dialog box to the desired log file in the folder specified in the **Location** input line.

10. Select a notification from the list to view its detailed information in the Trap Details panel of the main window. If this panel is not displayed, you can display it by using the **View / Trap Details** command.

Tip: To enable logging only SNMP notifications that match the given criteria, add one or more filters to the log output unit, as described in the [Filtering SNMP Notifications](#) section.

6.2.3 Configuring Auto New File Logging Preferences

1. Open the Output Manager Preferences dialog box by selecting the **Tools / Output Manager Preferences** command or by clicking the **Output Manager Preferences** toolbar button. 
2. Select an existing Log output unit from the Output Manager tree structure to display the Log Preferences window panel. Alternatively, you can create a new Log output unit by selecting the Log monitoring option and using the **Add** pop-up command ([Figure 14](#)).
3. To enable configuring the selected Log output unit, check the **Enable** checkbox in the right panel of the Output Manager Preferences dialog box ([Figure 17](#)).

Note: The **Negate Filter(s)** checkbox is enabled only if one or more filters are added to the output unit. This checkbox can be used to logically negate (invert) all filters associated with the output unit. For more information on filters, consult the [Filtering SNMP Notifications](#) section.

4. Check the **Auto new file** radio button in the Logging frame to enable this type of logging. Trap Ringer server will automatically create a new log file and start logging notifications to it whenever the corresponding max. file size is reached.

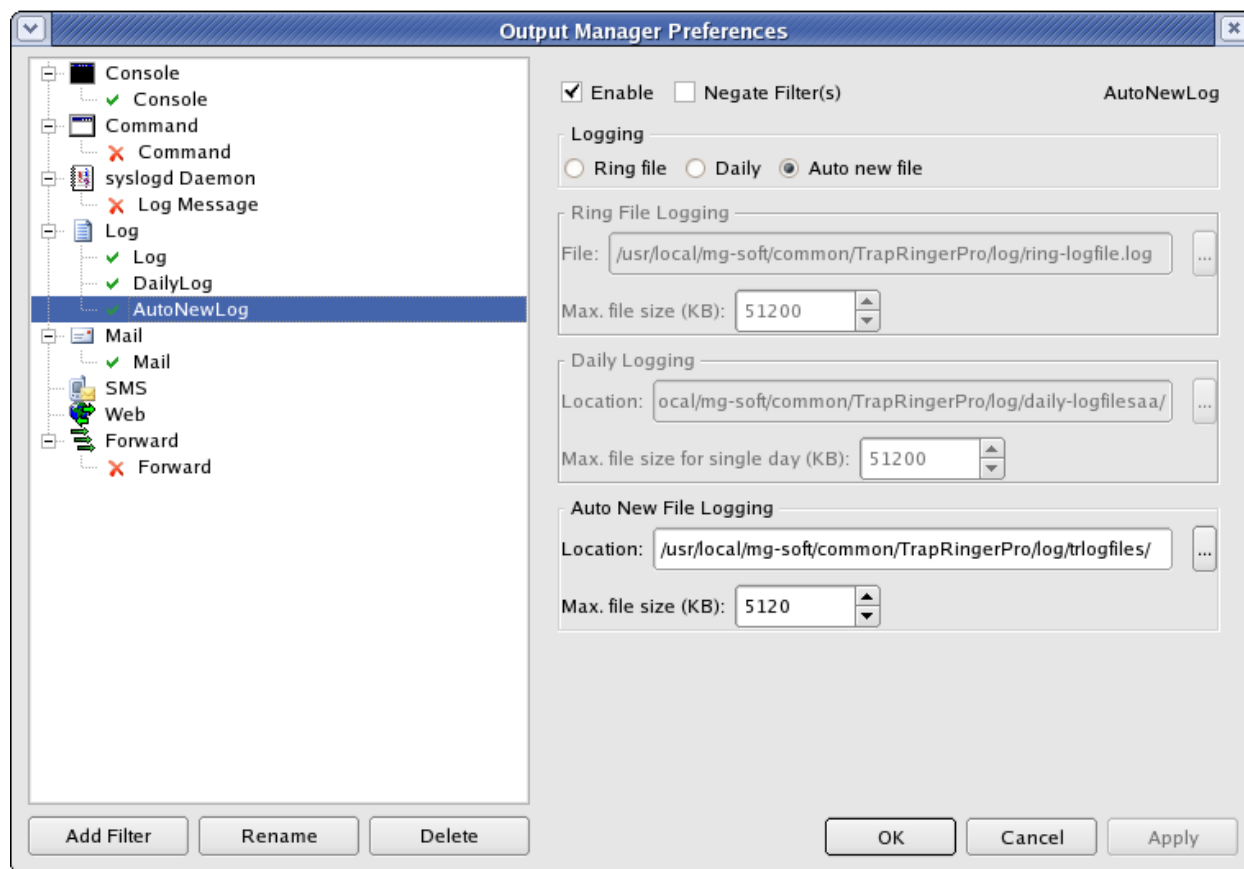


Figure 17: Configuring auto new file logging options

5. Into the **Location** input line, specify the full path of the folder where the log files will be saved. The generated log files will be named according to the following scheme:

UnixTimestamp_YYYYMMDD.log

...where the characters following the underscore character (_) indicate the year, month and day of the log file, e.g., 20100422 stands for April 22nd 2010.

6. Into the **Max. file size** input line, enter the maximum size of the log file (in kilobytes). When this limit is reached, a new log file is automatically created (using the file naming scheme described above) and Trap Ringer starts logging notifications to it.
7. Click the **OK** button to apply the settings and close the Output Manager Preferences dialog box.
8. To display the contents of the current log file in the main window, select the **View / Log / <Log Name>** menu command.
9. The contents of the last existing log file will be displayed in the Trap List panel in the main window.

Tip: If more than one log file exists, you can view the contents of any previous log file by using the **File / Open** command and pointing the standard Open dialog box to the desired log file in the folder specified in the **Location** input line.


10. Select a notification from the list to view its detailed information in the Trap Details panel of the main window. If this panel is not displayed, you can display it by using the **View / Trap Details** command.

Tip: To enable logging only SNMP notifications that match the given criteria, add one or more filters to the log output unit, as described in the [Filtering SNMP Notifications](#) section.

6.3 Running Commands

Trap Ringer can be configured to run a command to automatically invoke an external program or a batch/script file when an SNMP notification is received. Trap Ringer can also pass details about received SNMP notifications to the invoked program or script. Notification details can be passed as parameters appended to the command that runs the specified external program.

To configure the Command output unit preferences:

1. Open the Output Manager Preferences dialog box by selecting the **Tools / Output Manager Preferences** command or by clicking the **Output Manager Preferences** toolbar button. 
2. Select an existing Command output unit from the Output Manager tree structure to display the Command Preferences window panel. Alternatively, you can create a new Command output unit by selecting the Command monitoring option and using the **Add** button or pop-up command ([Figure 14](#)).

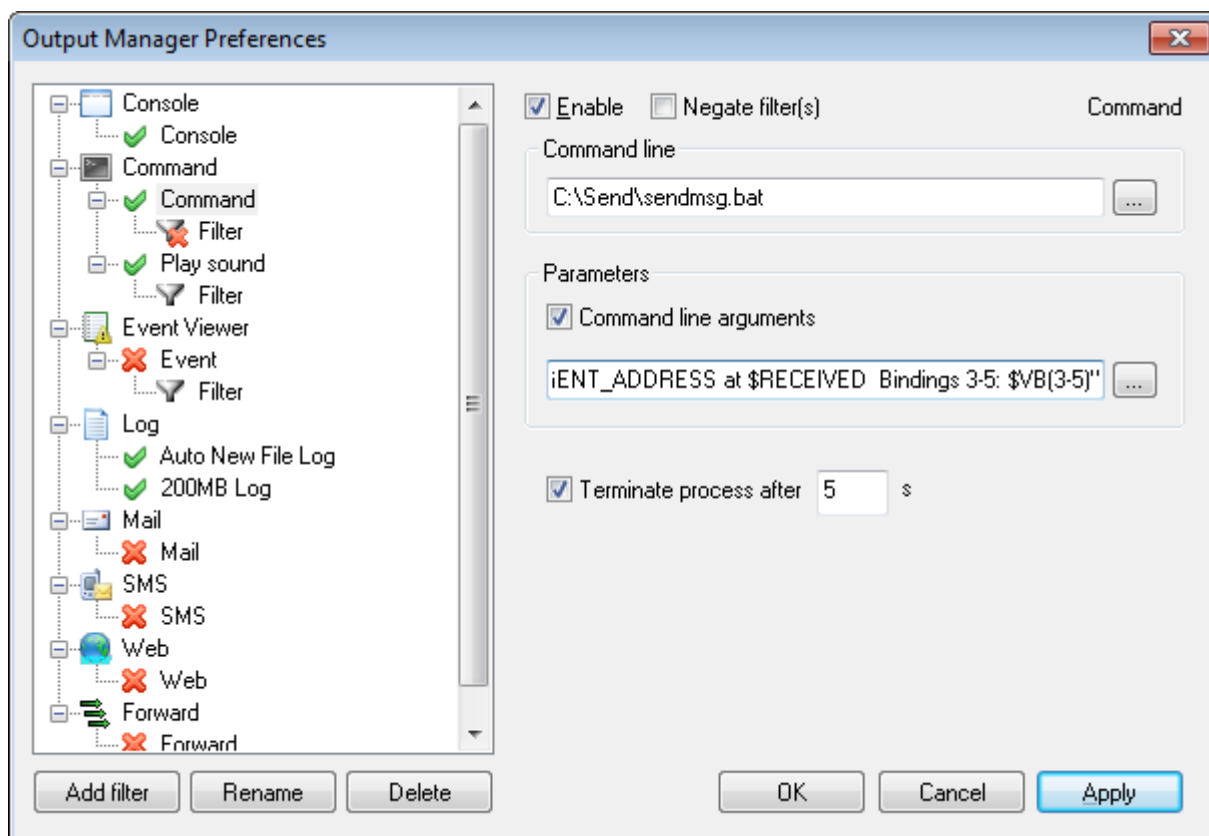


Figure 18: Configuring Command output unit options

3. To enable configuring the selected Command output unit, check the **Enable** checkbox in the right panel of the Output Manager Preferences dialog box ([Figure 18](#)).

Note: The **Negate Filter(s)** checkbox is enabled only if one or more filters are added to the output unit. This checkbox can be used to logically negate (invert) all filters associated with the output unit. For more information on filters, consult the [Filtering SNMP Notifications](#) section.

4. Into the **Command line** input line enter the command to be run on received SNMP Trap or SNMP Inform message. You can use the **Browse (...)** button to select the executable file and optionally add additional switches and parameters to the command line. For example, you can create a script/batch file that will invoke a program to send a pop-up message containing Trap details to administrator, etc.
5. To enable passing details about received SNMP notifications to the invoked program, check the **Command line arguments** checkbox. The accompanying input line becomes enabled.
6. Trap Ringer comes with a set of **reserved words** that can be inserted into the **Command line arguments** input line to pass desired notification details to the command line. All reserved words start with the “\$” character. The reserved words are replaced with the actual values when the command is executed, e.g., the “\$RECEIVED” reserved word is replaced with the time and date of notification reception, which is then passed to the above command as an ASCII string. By default, the Command line arguments input line contains a pre-configured expression, which can be freely edited (you can combine regular text with reserved words).

The following is the default command line arguments expression:

```
$NOTIFICATION received from: $AGENT_ADDRESS at $RECEIVED
```

An example set of parameters appended to the command line when using the above (default) settings would be:

```
Trap coldStart received from: sasor (192.168.100.15) at 02/23/13 15:37:16
```

- ❑ To view all available reserved words use the **Browse (...)** button to open the Reserved Words dialog box, listing available reserved words and their descriptions.

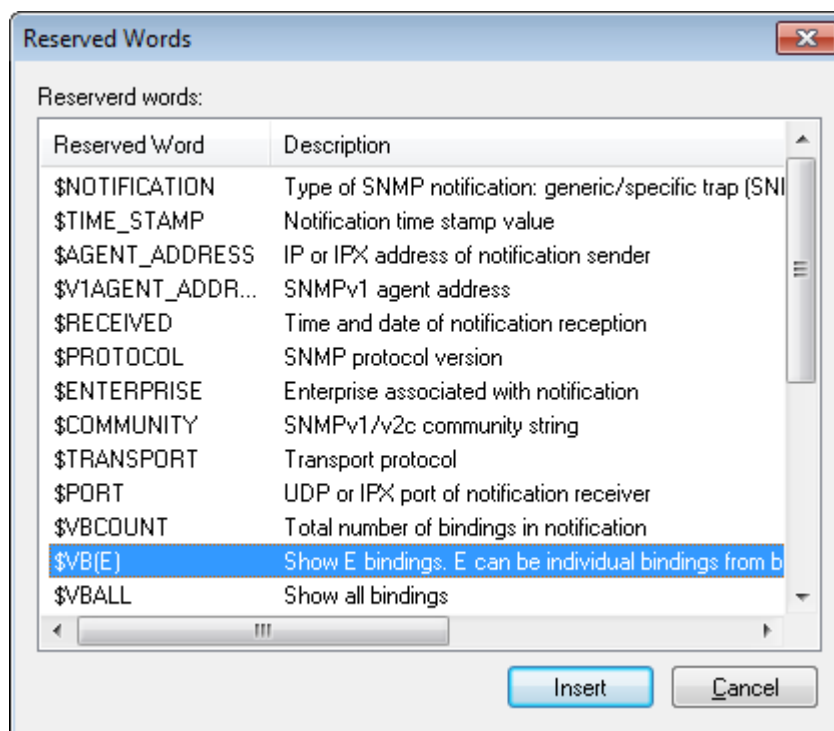


Figure 19: Reserved Words dialog box

- ❑ To add a reserved word to the **Command line arguments** input line, select it in the Reserved Words list and click the **Insert** button.
 - ❑ For example, to allow passing details about 3rd through 5th variable binding included in the received SNMP notification to the command line, select the \$VB(E) reserved word in the Reserved Words dialog box, and click the **Insert** button to insert the reserved word to the **Command line arguments** input line. Edit the expression in the **Command line arguments** input line to meet your requirements, e.g., \$VB(3-5) .
7. Check the **Terminate process after X s**, checkbox to limit the maximum running time of every process started by the given Command output to the specified number of seconds (X). Into the accompanying input line, enter the number of seconds after which each started process will be terminated. If this checkbox is not checked, Trap Ringer will not limit the running time of the processes it starts. You should leave this checkbox checked if the invoked processes do not (always) terminate by themselves in a timely fashion.

Tip: There are also global command execution limits that can be configured in the Trap Ringer Preferences dialog box, Advanced tab. These limits affect the performance of executing commands and aim to prevent the system overload in case of an incoming 'Trap storm'. The global command execution limits apply collectively to all enabled Command output units. They include the **Max. number of simultaneously running processes** setting that limits the total number of processes launched by all Command output units that can run simultaneously at any given time, and the **Number of processes to start in a set** setting that specifies how many pending processes Trap Ringer starts in one set. Namely, by default, Trap Ringer groups all pending commands into sets (e.g., 10 commands per set) and executes one set of commands after another in quick successions.

8. Click the **OK** button to apply the settings and close the Output Manager Preferences dialog box.
9. From this moment on, Trap Ringer server will run the above-specified command, e.g., to notify remote users about received SNMP Trap and Inform notifications. An example of such a pop-up message is shown in the picture below.




Figure 20: A pop-up message displaying some linkDown Trap notification details

Note: You should add one or more filters to the command output unit, as described in the **Filtering SNMP Notifications** section, to enable running commands only when SNMP notifications with particular attributes are received.

6.4 Sending E-Mails

Trap Ringer can be configured to automatically send an e-mail upon receiving an SNMP notification. The subject and body sections of such e-mails can be configured to include desired details about the received SNMP notification.

To configure the E-mail output unit preferences:

1. Open the Output Manager Preferences dialog box by selecting the **Tools / Output Manager Preferences** command or by clicking the **Output Manager Preferences** toolbar button. 
2. Select an existing Mail output unit from the Output Manager tree structure to display the Mail Preferences window panel. Alternatively, you can create a new Mail output unit by selecting the Mail monitoring option and using the **Add** button or pop-up command (Figure 14).

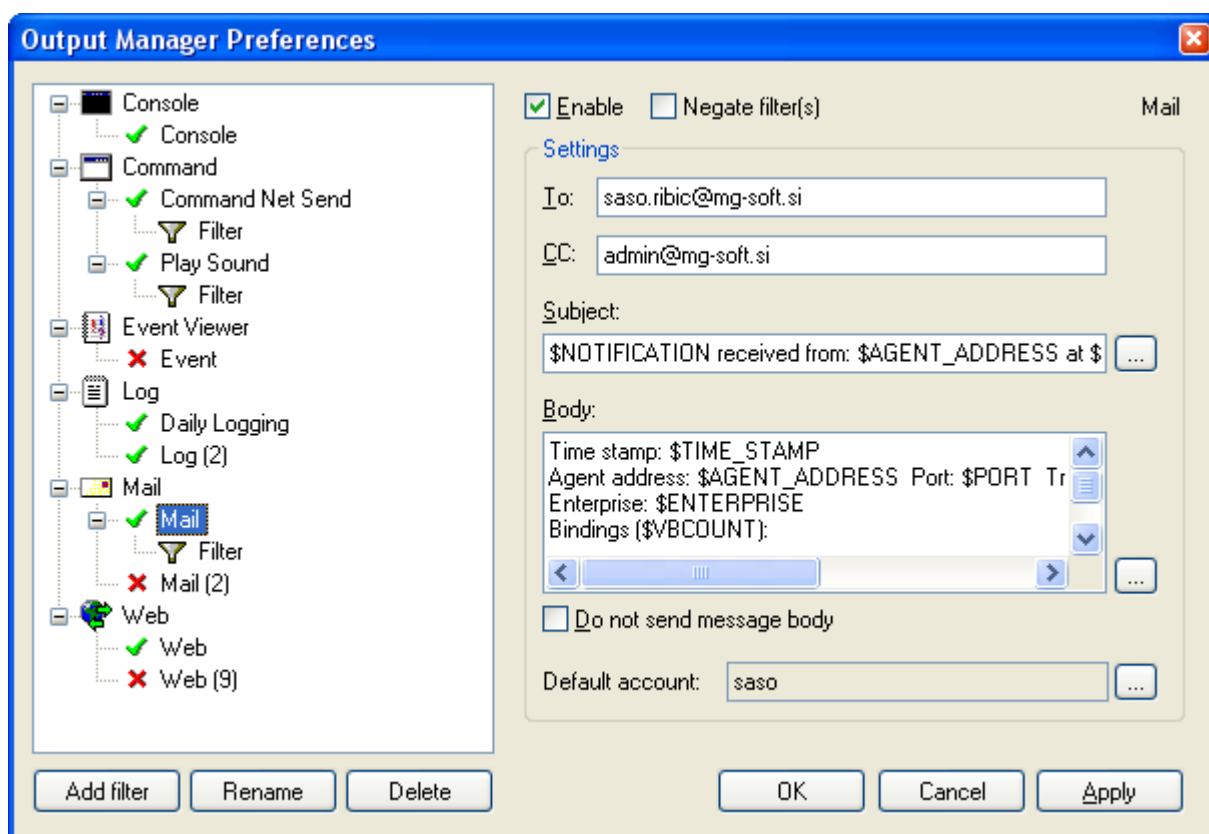


Figure 21: Configuring Mail output unit options

3. Check the **Enable** checkbox in the right panel of the Output Manager Preferences dialog box (Figure 21).

Note: The **Negate Filter(s)** checkbox is enabled only if one or more filters are added to the output unit. This checkbox can be used to logically negate (invert) all filters associated with the output unit. For more information on filters, consult the **Filtering SNMP Notifications** section.

4. Into the **To** input line enter the e-mail address of the e-mail recipient. Optionally, into the **CC** input line, enter the e-mail address to which the copies of e-mails will be sent.
5. Into the **Subject** input line, specify the contents of e-mail subject. To include desired details about received SNMP notification into the e-mail subject, use the reserved words. All reserved words start with the “\$” character. The reserved words are replaced with the actual notification values when the e-mail is sent, e.g., the “\$RECEIVED” reserved word is replaced with the time and date of notification reception. By default, the Subject input line contains a pre-configured expression, which can be fully customized.

The following is the default subject expression:

```
$NOTIFICATION received from: $AGENT_ADDRESS at $RECEIVED
```

An example of generated e-mail subject (using the default settings) would be:

```
Trap coldStart received from: sasor (192.168.100.15) at 02/15/09 15:37:16
```

- ❑ To view all available reserved words click the **Browse (...)** button next to the **Subject** input line to open the Reserved Words dialog box (Figure 19), listing available reserved words and their descriptions.
 - ❑ To add a reserved word to the **Subject** input line, select it in the Reserved Words list and click the **Insert** button.
6. If you do not want the e-mails to contain the e-mail message body section, check the **Do not send message body** checkbox. In this way, e-mails will contain only the e-mail subject section. This option is useful, for example, when using e-mail for sending SMS short messages in mobile telephone networks.
 7. If the **Do not send message body** checkbox is not checked, specify the contents of the e-mail body in the **Body** input field. To include desired details about received SNMP notification into the e-mail body, use the reserved words. By default, the Body input field contains the following pre-configured expression, which can be fully customized:

```
Time stamp: $TIME_STAMP
Agent address: $AGENT_ADDRESS Port: $PORT Transport: $TRANSPORT Protocol:
$PROTOCOL
Enterprise: $ENTERPRISE
Bindings ($VBCOUNT):
$VBALL
```

An example of the generated e-mail body (using the default settings) would be:

```
Time stamp: 2 days 09h:58m:14s.65th
Agent address: sasor (192.168.100.15) Port: 162 Transport: IP/UDP
Protocol: SNMPv2c
Enterprise: mg-soft
Bindings (4):
Binding #1: sysUpTime.0 *** (TimeTicks) 2 days 09h:58m:14s.65th
Binding #2: snmpTrapOID.0 *** (OBJECT IDENTIFIER) coldStart.0
Binding #3: ifIndex.1 *** (InterfaceIndex) 1
Binding #4: snmpTrapEnterprise.0 *** (OBJECT IDENTIFIER) mg-soft
```

- ❑ To view all available reserved words click the **Browse (...)** button next to the **Body** input field to open the Reserved Words dialog box (Figure 19), listing available reserved words and their descriptions.

- ❑ To add a reserved word to the **Body** input field, select it in the Reserved Words list and click the **Insert** button.
8. The **Default Account** field displays the default e-mail account. To configure an e-mail account, click the **Browse (...)** button next to the Default Account input line. The Mail Accounts dialog box appears, where you can configure a new e-mail account:

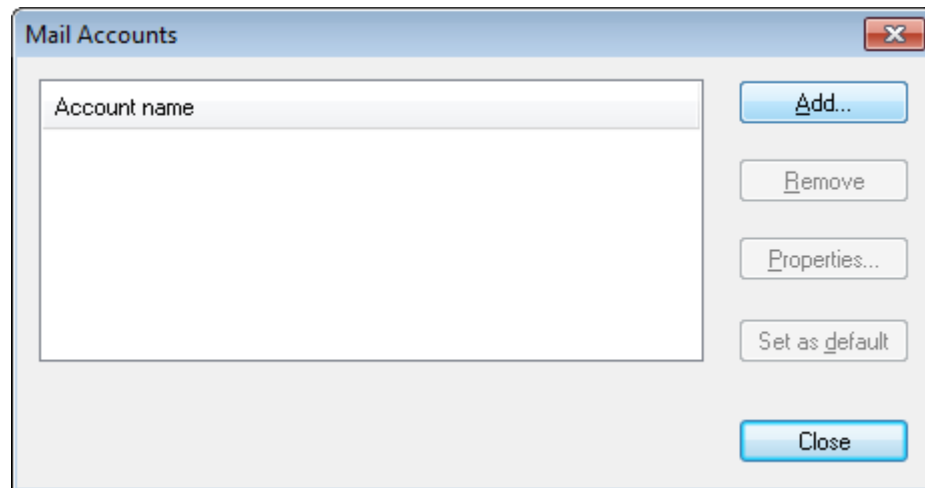


Figure 22: Mail Accounts dialog box

9. To add a new e-mail account, click the **Add** button in the Mail Accounts dialog box. The Mail Account Preferences dialog box appears, with the General tab selected (Figure 23).

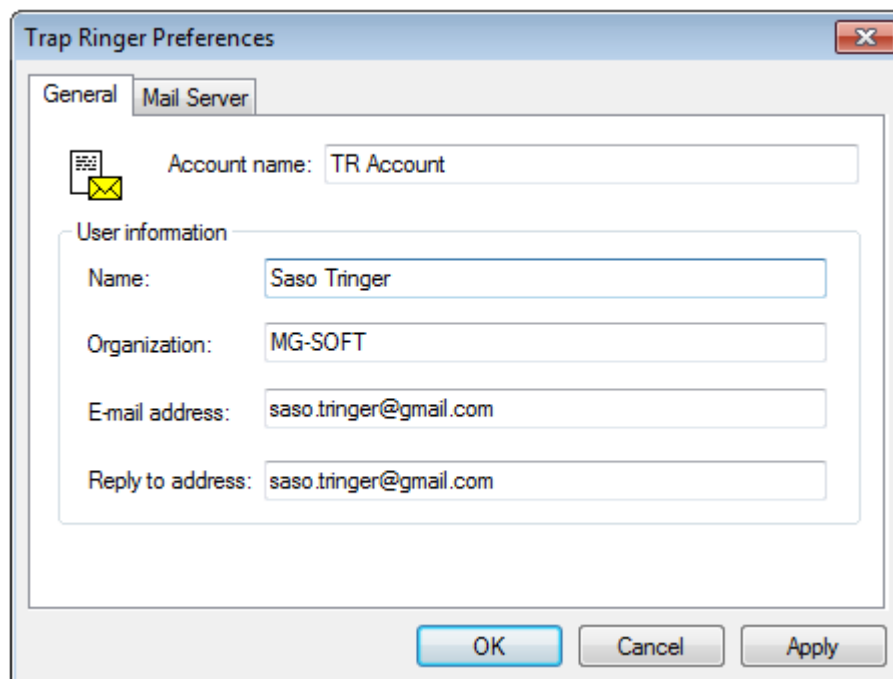


Figure 23: Mail Account preferences dialog box, General tab

- ❑ In the **Account name** input line, enter a name that will identify this e-mail account.
 - ❑ In the **Name** input line, enter the full name of the e-mail account holder.
 - ❑ In the **Organization** input line, enter the organization of the account holder.
 - ❑ In the **E-mail address** input line, enter the e-mail address of the account holder. Trap Ringer will send e-mail messages from this e-mail address.
 - ❑ Optionally, in the **Reply to address** input line, enter the “reply to” e-mail address that will be included into e-mail messages.
10. Click the **Mail server** tab to configure the e-mail server preferences (Figure 24).

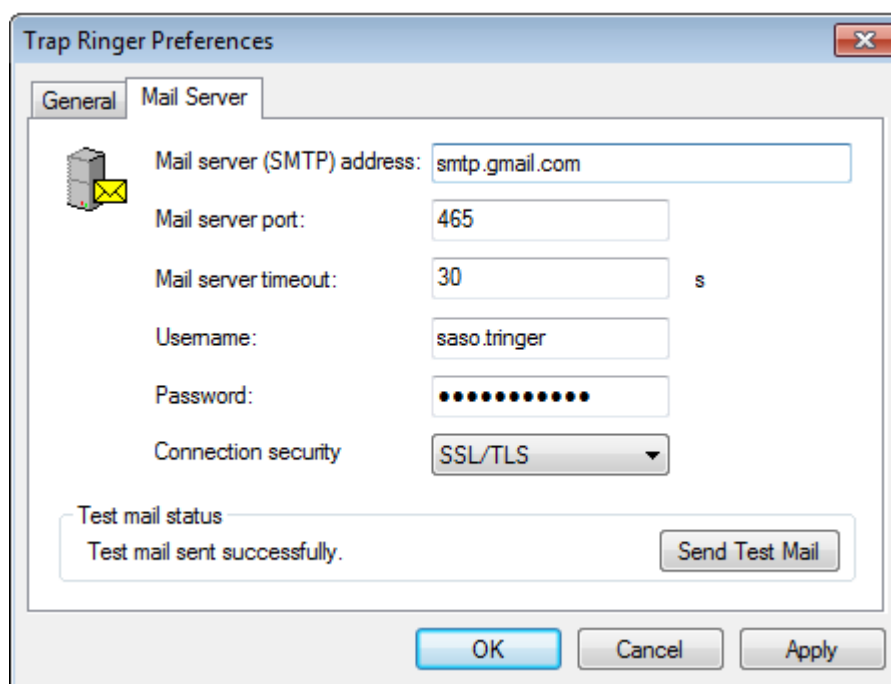


Figure 24: Mail Account preferences dialog box, Mail Server tab

- ❑ Into the **Mail server (SMTP) address** input line, enter the fully qualified domain name or IP address of the outgoing SMTP or ESMTP mail server.
- ❑ In the **Mail server port** input line, enter the TCP port on which the (E)SMTP server listens to for incoming e-mails. The default SMTP port number is 25. For secure SMTP connections over SSL or TLS, the default port numbers are 465 and 587, respectively.
- ❑ In the **Mail server timeout** input line, enter the timeout value (in seconds) when connecting to server.
- ❑ If the specified (E)SMTP server supports the AUTH LOGIN SMTP authentication mechanism, enter the username for authentication into the **Username** input line. Otherwise, leave this input line blank.
- ❑ If the specified (E)SMTP server supports the AUTH LOGIN SMTP authentication mechanism, enter the password for authentication into the **Password** input line. Otherwise, leave this input line blank.

- ❑ If the specified (E)SMTP server supports establishing secure connections over SSL or TLS protocol, select the **SSL/TLS** entry from this drop-down list. Otherwise, leave the **None** entry selected.
 - ❑ Click the **Send Test Mail** button to verify if Trap Ringer can successfully send e-mail messages using the configured settings. If everything is configured properly, the Test mail sent successfully message appears in the Test mail status frame (Figure 24). If an error message is displayed, check the mail account and mail server settings and enter the correct parameters. Make sure also that no firewall is blocking the specified port.
11. Click the **OK** button to close the Mail Account Preferences dialog box.
 12. The newly configured mail account will be displayed in the Mail Accounts list. Select the newly configured e-mail account and click the **Set as default** button to make the newly added account the default mail account. Close the Mail Accounts dialog by clicking the **Close** button.

Note: Trap Ringer always uses the default mail account for sending e-mails. More e-mail accounts can exist in the Mail Accounts list, but only one account at a time can be configured as the default mail account.

13. The **Default Account** selection field in the Output Manager Preferences dialog box displays the name of the newly added (default) e-mail account (Figure 21).
14. Click the **OK** button to apply the settings and close the Output Manager Preferences dialog box.
15. From this point on, Trap Ringer server will send an e-mail message to the specified recipient(s) whenever a new SNMP Trap or Inform notification is received.

Tip: To enable sending e-mails only when SNMP notifications that match the given criteria are received, add one or more filters to the mail output unit, as described in the [Filtering SNMP Notifications](#) section.

6.5 Sending SMS Messages

Trap Ringer now experimentally supports sending SMS (Short Message Service) text messages upon receiving SNMP notifications. The content of SMS messages can be configured to include desired information from the received SNMP notifications.


Short text messages are sent through the mobile (cellular) phone connected to a serial port or a virtual serial port of the computer that runs Trap Ringer. Such mobile phone must have a built-in modem supporting the AT instruction set.

Before setting the SMS preferences in Trap Ringer, please ensure that your mobile phone is correctly configured for sending SMS messages (try sending an SMS message from the given phone by using the phone's keypad) and that the phone is attached to a serial port of the computer with the appropriate serial data cable or otherwise properly connected to the applicable virtual serial port (e.g., via Bluetooth).

Note 1: Support for sending SMS messages is currently in **experimental** phase.

Note 2: All costs associated with sending SMS messages are subject to the policy of the mobile phone service provider. Hence, MG-SOFT cannot be responsible for any transmission costs. Please refer to your carrier's contract for billing information.

To configure the SMS output unit preferences:

1. Open the Output Manager Preferences dialog box by selecting the **Tools / Output Manager Preferences** command or by clicking the **Output Manager Preferences** toolbar button. 
2. Select an existing SMS output unit from the Output Manager tree structure to display the SMS Preferences panel. Alternatively, you can create a new SMS output unit by selecting the SMS monitoring option and using the **Add** button or pop-up command (Figure 14).
3. Into the **Phone number** input line, enter the phone number of the SMS message recipient. The phone number must include the international country code, the area code or mobile network code (without the leading zero), and the actual mobile phone number. Do not prefix the number with the international direct-dial prefix (which is 00 in most countries (011 in North America) and sometimes substituted with the plus (+) sign).

For example, to send SMS messages to the mobile phone number (415) 640-1939 in the USA, you should enter the following into the Phone number input line:

14156401939

...where the leading "1" is the international country code for the USA, "415" is the area code (for San Francisco) and the "6401939" is the local telephone number.

4. The **Message** input field lets you specify the contents of SMS messages. To include desired details of received SNMP notification into the short message, use the reserved words. All reserved words start with the "\$" character. The reserved words are replaced with the actual notification values when the short message is sent, e.g., the "\$RECEIVED" reserved word is replaced with the date and time of notification reception. By default, the Message input line contains a pre-configured expression, which can be freely edited.

The following is the default message expression:

```
$NOTIFICATION received from: $AGENT_ADDRESS at $RECEIVED
```

An example of generated SMS message text (using the default settings) would be:

```
Trap coldStart received from: router1 (192.168.100.1) at 07/15/09 14:39:16
```

- ❑ To view all available reserved words click the **Browse (...)** button next to the **Message** input field to open the Reserved Words dialog box (Figure 19), listing available reserved words and their descriptions.
- ❑ To add a reserved word to the **Message** input field, select it in the Reserved Words list and click the **Insert** button.

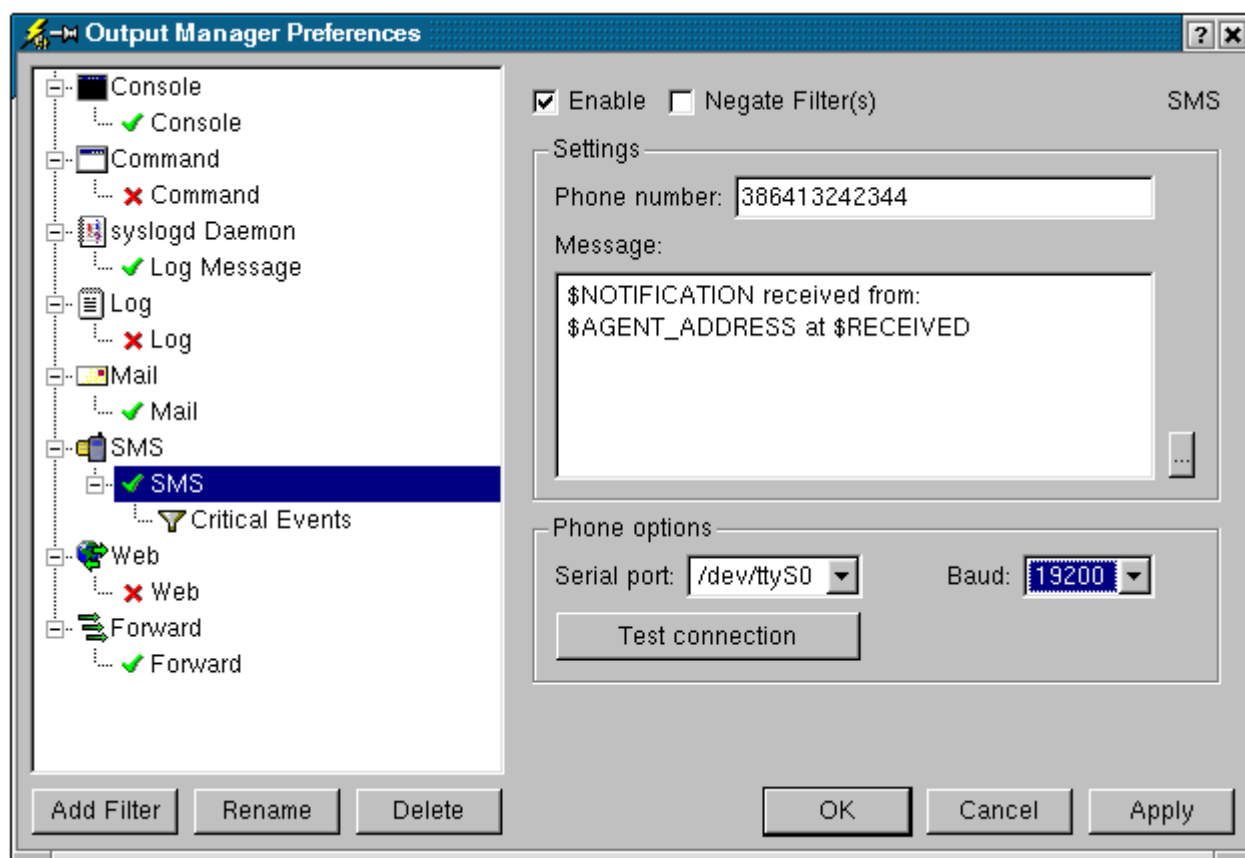


Figure 25: Configuring SMS output unit options

5. In the **Serial port** drop-down list in the Phone options frame, select the serial port to which the mobile phone is connected, e.g., COM1, COM2, etc. (on Windows) or /dev/ttyS0, /dev/ttyS1, etc. (on Linux). On Apple Macintosh computers that do not provide physical serial ports, enter the name of the virtual serial port (e.g., when connected via Bluetooth or USB) into this drop-down list (e.g., /dev/tty.PL2303-0000101D).
6. In the **Baud** drop-down list, select the desired baud rate (speed in bits per second) for communication with the mobile phone. If unsure, check with the device manufacturer for the best baud rate for your specific device. Some devices can only communicate at a particular speed, for example at 19200 bps.

7. Click the **Test connection** button to test the connection between the PC and the mobile phone. If you have configured everything correctly, the Connection succeeded message should appear. If the Connection failed message is displayed, please double-check if you have selected the correct serial port or change the baud rate value.
8. Click the **OK** button to apply the settings and close the Output Manager Preferences dialog box.
9. From this point on, Trap Ringer server will send an SMS message to the specified recipient whenever a new SNMP Trap or Inform notification is received.


Tip: To enable sending SMSes only when SNMP notifications that match the given criteria are received, add one or more filters to the SMS output unit, as described in the [Filtering SNMP Notifications](#) section.

6.6 Auditing with Windows Event Viewer

Trap Ringer Pro for Windows can generate event messages containing information about received SNMP notifications in the Application log of the event logging facility available in MS Windows operating systems. Event messages can be viewed with the Windows **Event Viewer** tool. For more information about the event logs and Event Viewer, please consult your Windows documentation.

Note: This feature is not available in Trap Ringer Pro for Linux, Mac and Solaris. Trap Ringer Pro for Linux, Mac OS X and Solaris incorporate the ability to generate **syslog messages** instead of Windows event log messages.

To configure the Event Viewer output unit preferences:

1. Open the Output Manager Preferences dialog box by selecting the **Tools / Output Manager Preferences** command or by clicking the **Output Manager Preferences** toolbar button. 
2. Select an existing Event Viewer output unit from the Output Manager tree structure to display the Event Viewer Preferences window panel. Alternatively, you can create a new Event Viewer output unit by selecting the Event Viewer monitoring option and using the **Add** button or pop-up command ([Figure 14](#)).

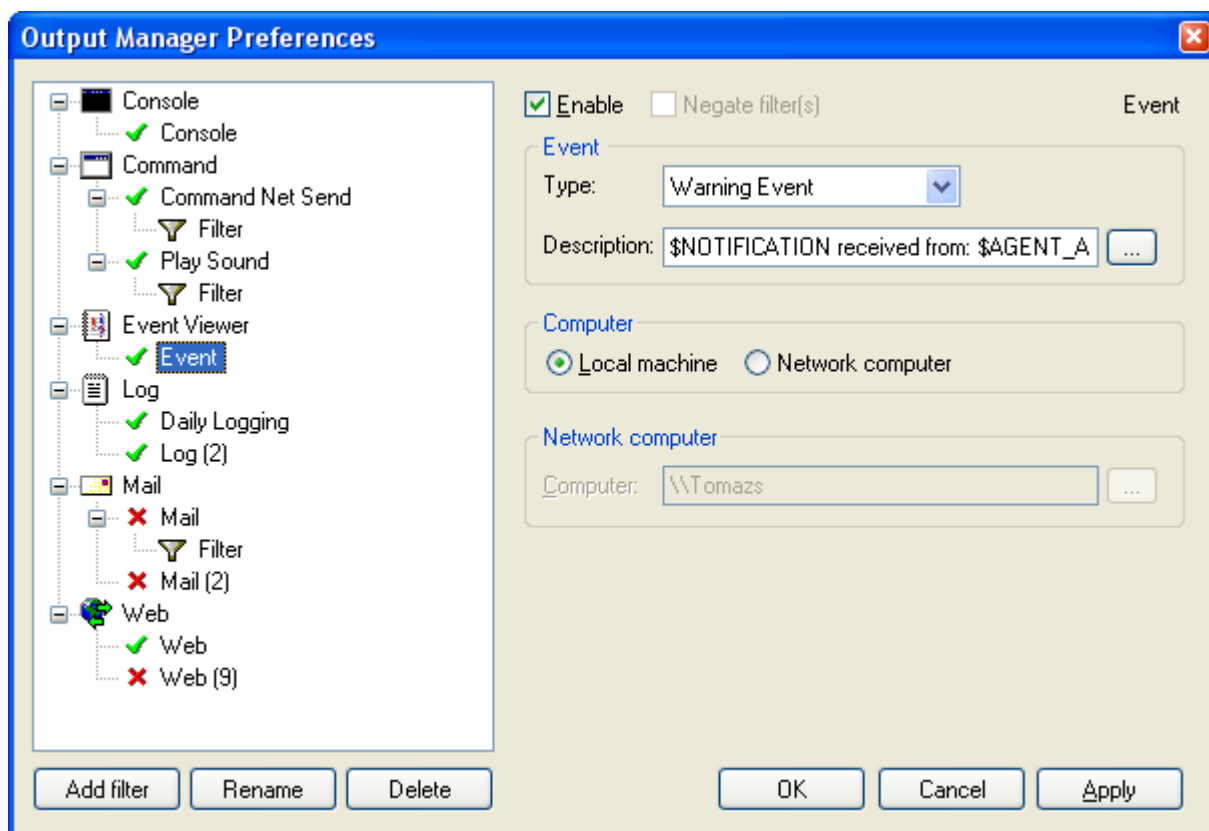


Figure 26: Configuring Event output unit options

3. Check the **Enable** checkbox in the right panel of the Output Manager Preferences dialog box (Figure 26).

Note: The **Negate Filter(s)** checkbox is enabled only if one or more filters are added to the output unit. This checkbox can be used to logically negate (invert) all filters associated with the output unit. For more information on filters, consult the [Filtering SNMP Notifications](#) section.

4. From the **Type** drop-down list in the Event frame, select the type of events that will be logged in the event log (Informational, Warning or Error event type).
5. Into the **Description** input line specify the event description contents. The event description can be viewed by double-clicking an event in the Event Viewer. To include information about received SNMP notification into the event description, use the reserved words. By default, the **Description** input line contains the following pre-configured expression, which can be freely edited:

```
$NOTIFICATION received from: $AGENT_ADDRESS at $RECEIVED
```

An example of generated event description (using the default settings) would be:

```
Trap coldStart received from: kasiopea (192.168.100.16) at 02/15/09 15:37:16
```

- ❑ To view all available reserved words click the **Browse (...)** button next to the **Description** input line to open the Reserved Words dialog box (Figure 19), listing available reserved words and their descriptions.
 - ❑ To add a reserved word to the **Description** input line, select it in the Reserved Words list and click the **Insert** button.
6. In the Computer frame, click the **Local machine** radio button if you want events to be logged in the event log on your local computer.
 7. Click the **Network computer** radio button if you want events to be logged in the event log on a remote computer on your LAN that runs MS Windows operating system. In such case, specify the name of the network computer into the **Computer** input line or use the **Browse (...)** button to select it.
 8. Click the **Apply** button to apply the settings or the **OK** button to apply the settings and close the Output Manager Preferences dialog box.
 9. From this point on, Trap Ringer server will log an event in the Windows event log whenever a new SNMP Trap or Inform notification is received.

Tip: To enable event logging only when SNMP notifications that match the given criteria are received, add one or more filters to the output unit, as described in the [Filtering SNMP Notifications](#) section.

To view events in Event Viewer:

To view event messages, start the Event Viewer tool (e.g., **Start / Control Panel / Administrative Tools / Event Viewer**) and select the **Application** log in the left panel of the Event Viewer window (Figure 27). Logged events are displayed in the right panel. Double-click an event or select it and choose the **Properties** pop-up command to view its properties, including the event description.

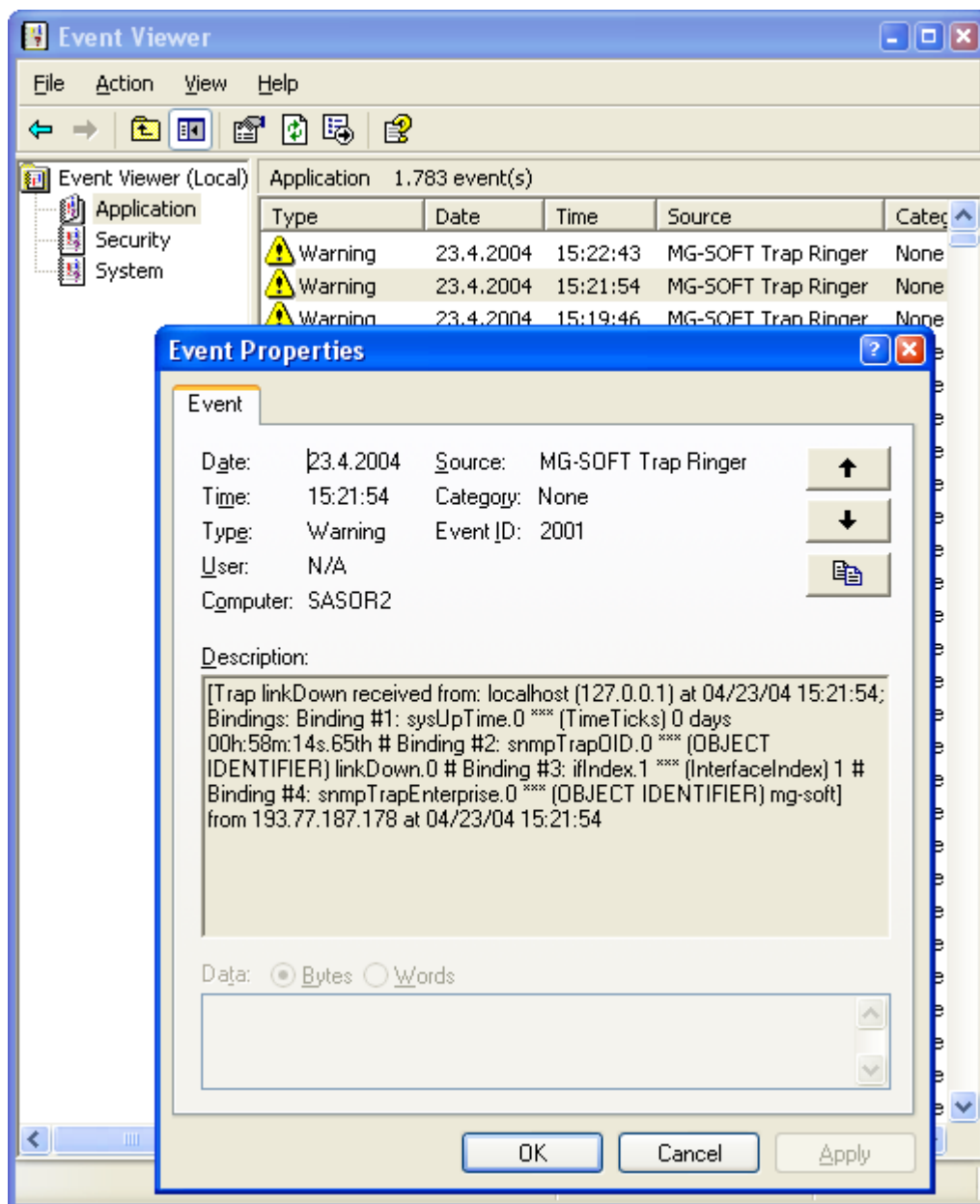


Figure 27: Monitoring SNMP notifications in Event Viewer


6.7 Logging Notifications to System Log Files (Syslog)

Trap Ringer Pro for Linux, Mac OS X and Solaris can generate syslog messages containing information about received SNMP notifications and send them to the local syslogd daemon, which logs messages to the system log files (typically located in the `/var/log` directory) and/or forwards them to remote syslog servers (depending on the syslogd configuration).

For more information about the system log files and the syslogd utility, please consult your operating system documentation.

Note: This feature is not available in Trap Ringer Pro for Windows. Trap Ringer Pro for Windows incorporates the ability to generate **Windows event log messages** instead of syslog messages.

To configure the syslog output unit preferences:

1. Open the Output Manager Preferences dialog box by selecting the **Tools / Output Manager Preferences** command or by clicking the **Output Manager Preferences** toolbar button. 
2. Select an existing Log Message output unit from the Output Manager tree structure to display the Log Message Preferences window panel. Alternatively, you can create a new Log Message output unit by selecting the syslog Daemon monitoring option and using the **Add** button or pop-up command ([Figure 14](#)).

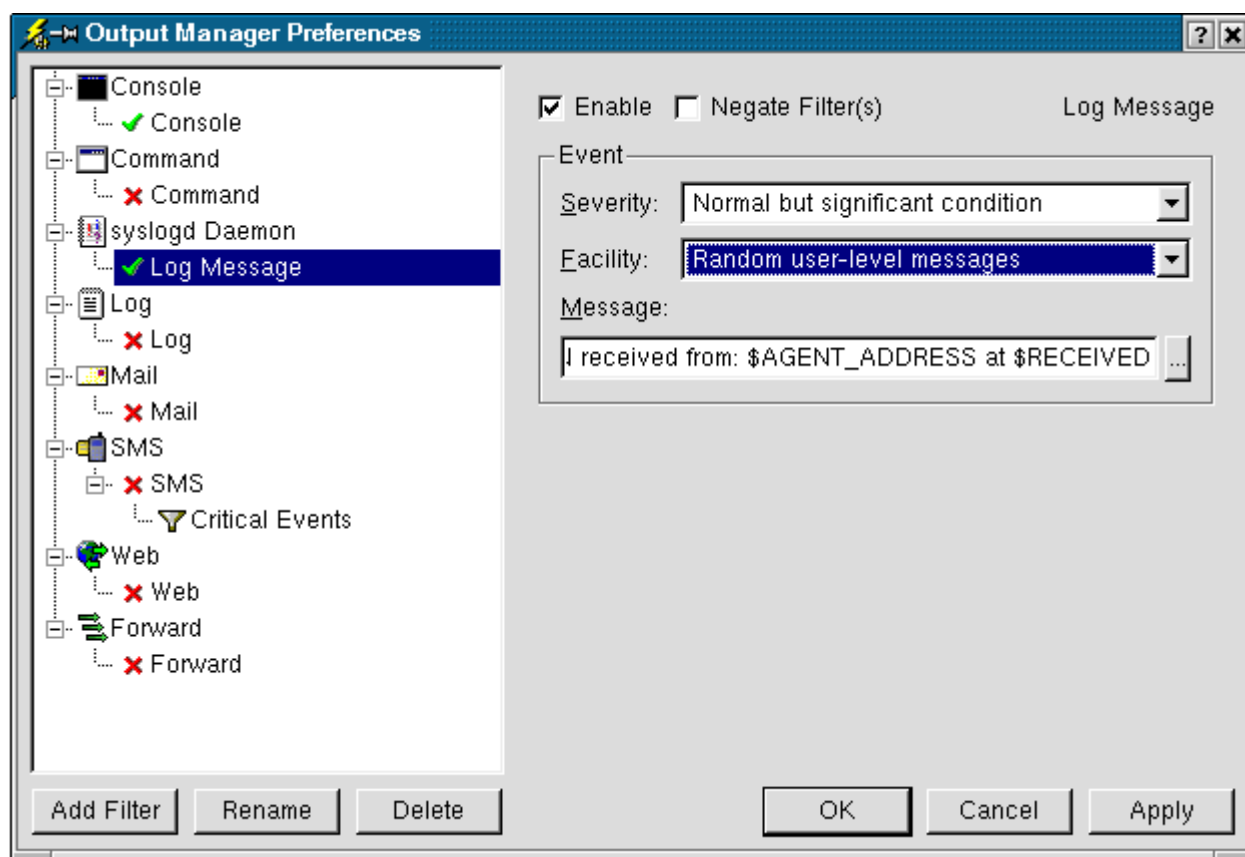


Figure 28: Configuring syslog output unit options

3. Check the **Enable** checkbox in the right panel of the Output Manager Preferences dialog box (Figure 28).

Note: The **Negate Filter(s)** checkbox is enabled only if one or more filters are added to the output unit. This checkbox can be used to logically negate (invert) all filters associated with the output unit. For more information on filters, consult the [Filtering SNMP Notifications](#) section.

4. From the **Severity** drop-down list in the Event frame, select the severity level for the syslog messages. Severity levels in the Severity drop-down list are listed top-down from most to least severe.
5. From the **Facility** drop-down list line, select the facility for the syslog messages. All outgoing syslog messages will have the selected severity and facility property.
6. Into the **Message** input line specify the attributes of received SNMP notifications that should be included into syslog messages by using the reserved words. All reserved words start with the “\$” character. The reserved words are replaced with the actual notification values when the message is sent. By default, the **Message** input line contains the following pre-configured expression, which can be freely edited:

```
$NOTIFICATION received from: $AGENT_ADDRESS at $RECEIVED
```

An example of generated syslog message contents (using the default settings) would be:

```
Trap coldStart received from: kasiopea (192.168.100.16) at 02/15/09 15:37:16
```

- ❑ To view all available reserved words click the **Browse (...)** button next to the **Message** input line to open the Reserved Words dialog box (Figure 19), listing available reserved words and their descriptions.
 - ❑ To add a reserved word to the **Description** input line, select it in the Reserved Words list and click the **Insert** button.
7. Click the **Apply** button to apply the settings or the **OK** button to apply the settings and close the Output Manager Preferences dialog box.
 8. From this point on, Trap Ringer server will send a syslog message to the local syslogd daemon whenever a new SNMP Trap or Inform notification is received.


Tip: To enable generating syslog messages only when SNMP notifications that match the given criteria are received, add one or more filters to the output unit, as described in the [Filtering SNMP Notifications](#) section.

6.8 Web Monitoring

Trap Ringer can automatically generate and update HTML report files containing information about received SNMP notifications. In this way, remote online Web monitoring of SNMP notifications can be set up (provided that your computer runs an HTTP server).

The Web monitoring option must be used together with the Log or Console monitoring option, because Trap Ringer uses information from a log file to generate HTML reports.

To configure the Web output unit preferences:

1. Open the Output Manager Preferences dialog box by selecting the **Tools / Output Manager Preferences** command or by clicking the **Output Manager Preferences** toolbar button. 
2. Select an existing Event Viewer output unit from the Output Manager tree structure to display the Event Viewer Preferences window panel. Alternatively, you can create a new Event Viewer output unit by selecting the Event Viewer monitoring option and using the **Add** button or pop-up command ([Figure 14](#)).

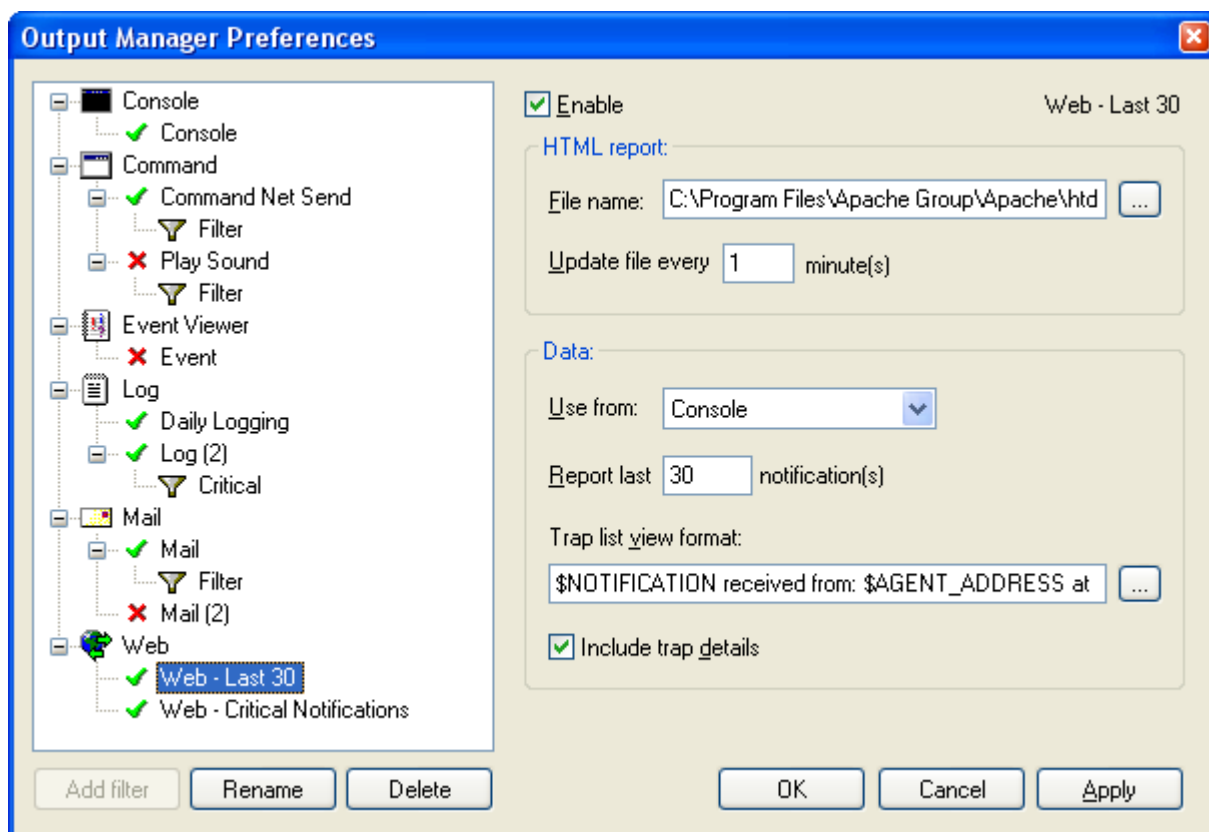


Figure 29: Configuring Web output unit options

3. Check the **Enable** checkbox in the right panel of the Output Manager Preferences dialog box ([Figure 26](#)).
4. Into the **File name** input line in the HTML Report frame, specify the path and the name and extension of the HTML file to be generated by Trap Ringer. By default, Trap Ringer generates Web report files to the “HTML” subfolder of the Trap Ringer installation folder.
5. Into the **Update file every ... minutes** input line enter the time interval specifying how often the HTML file should be updated (re-generated).
6. From the **Use from** drop-down list in the Data frame select the log file from which the HTML file will be generated (console log or any file log).
7. Into the **Report last ... notifications** input line specify the number of most recently received SNMP notifications that will be included into the HTML report file.
8. Into the **Trap list view format** input line specify the attributes of received SNMP notifications that should be listed in the HTML report by using the [reserved words](#). When viewing the HTML report in a Web Browser, every line in the report contains information about one SNMP notification. The “Trap list view format” input line defines what information is displayed for each notification.

By default, the **Trap list view format** input line contains the standard pre-configured expression, which can be freely edited:

```
$NOTIFICATION received from: $AGENT_ADDRESS at $RECEIVED
```

An example of a line displayed in the Web report (using the default settings) would be:

```
Trap linkUp received from: kasiopea (192.168.100.16) at 02/15/09 15:37:16
```

- ☐ To view all available reserved words use the **Browse (...)** button next to this input line. The Reserved Words dialog box appears, listing available reserved words and their descriptions.
 - ☐ To add a reserved word to the **Trap list view format** input line, select it in the Reserved Words list and click the **Insert** button.
9. Check the **Include trap details** checkbox if you want the generated HTML report to contain details about received SNMP notifications (same as displayed in the [Trap Details window panel](#)). In such case, trap details are displayed in the right frame when viewing the Web report in a (frame-capable) Web Browser, with the trap list being displayed in the left frame.
 10. Click the **Apply** button to apply the settings or the **OK** button to apply the settings and close the Output Manager Preferences dialog box.
 11. From this point on, Trap Ringer server will generate and periodically update HTML report files containing information about received SNMP notifications.

Tip: To enable reporting only those SNMP notifications that match the given criteria, add one or more filters to the web output unit, as described in the [Filtering SNMP Notifications](#) section.

To view Trap Ringer's Web report in a Web Browser:

1. To view the Web report page in your Web browser, search for the HTML index report file (e.g. `MyWebReport.html`) in the HTML report folder (e.g., `C:\Program Files\MG-SOFT\Trap Ringer Pro\Html`) and open it in a Web browser, such as MS Internet Explorer, Netscape Navigator, Mozilla, etc., by double-clicking the file or using the **Open With** pop-up command and selecting the desired Web browser application.
2. The Trap Ringer Web report page is displayed in the Web browser ([Figure 30](#)).

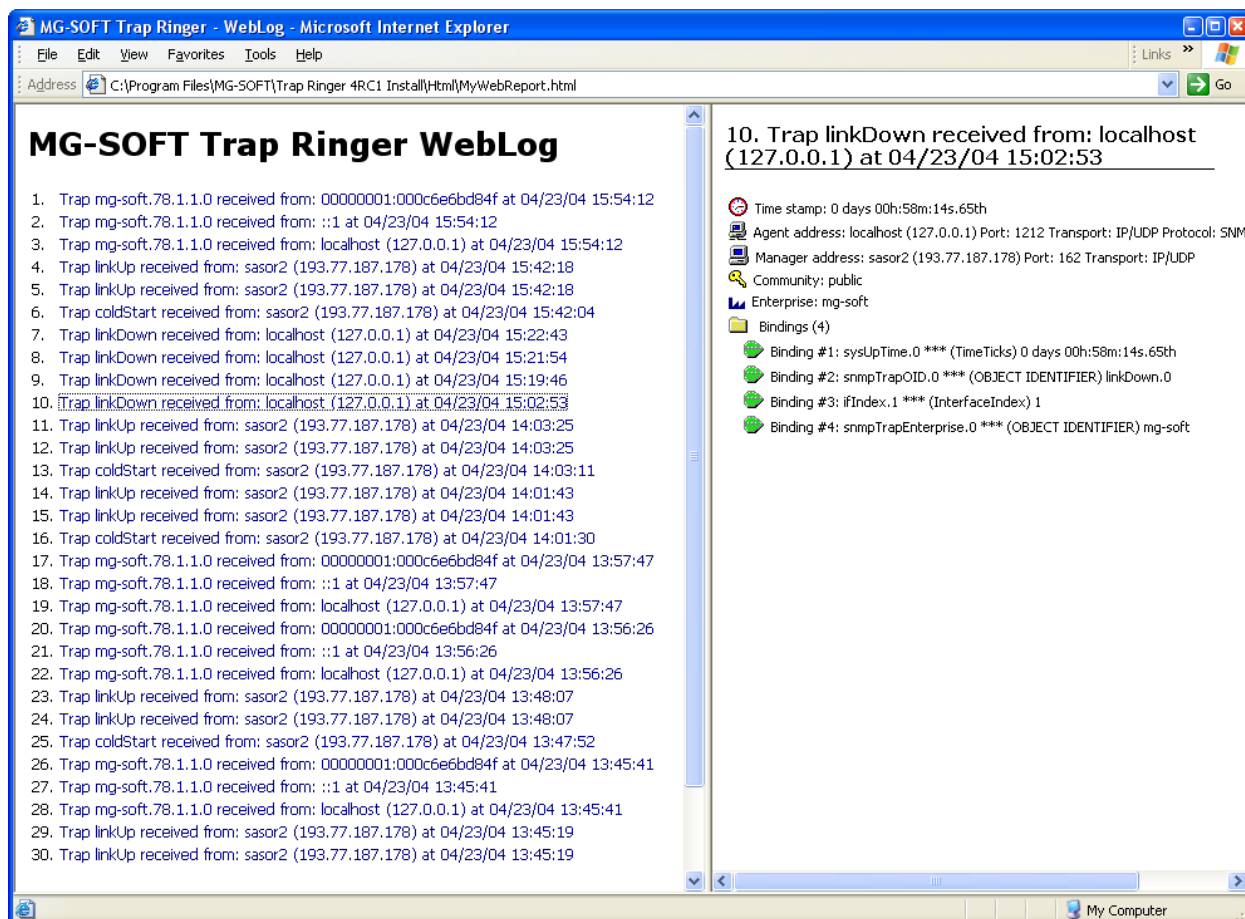


Figure 30: Viewing Web report in Web Browser


If the **Include trap details** checkbox is checked in the [Web Preferences panel](#), the generated HTML report will contain two frames. The left frame displays the list of last X received SNMP notifications (X is configurable) and the right frame displays details about SNMP notifications (the same as displayed in the [Trap Details window panel](#)). If the **Include trap details** checkbox is unchecked, the HTML report will contain only one frame displaying the list of received SNMP notifications.

Click an SNMP notification in the left frame to view its details in the right frame.

6.9 Forwarding and Translating SNMP Notifications

Trap Ringer can act as SNMP notification proxy forwarder application, meaning that it can forward received SNMP notification messages to other SNMP managers on the network. Moreover, it can also translate received SNMP notification messages and forward them as SNMPv1 or SNMPv2c or SNMPv3 Trap messages, or as SNMPv2c or SNMPv3 Inform messages.

To configure the Forward output unit preferences:

1. Open the Output Manager Preferences dialog box by selecting the **Tools / Output Manager Preferences** command or by clicking the **Output Manager Preferences** toolbar button. 
2. Select an existing Forward output unit from the Output Manager tree structure to display the Forward Preferences window panel. Alternatively, you can create a new Forward output unit by selecting the Forward monitoring option and using the **Add** button or pop-up command (Figure 14).

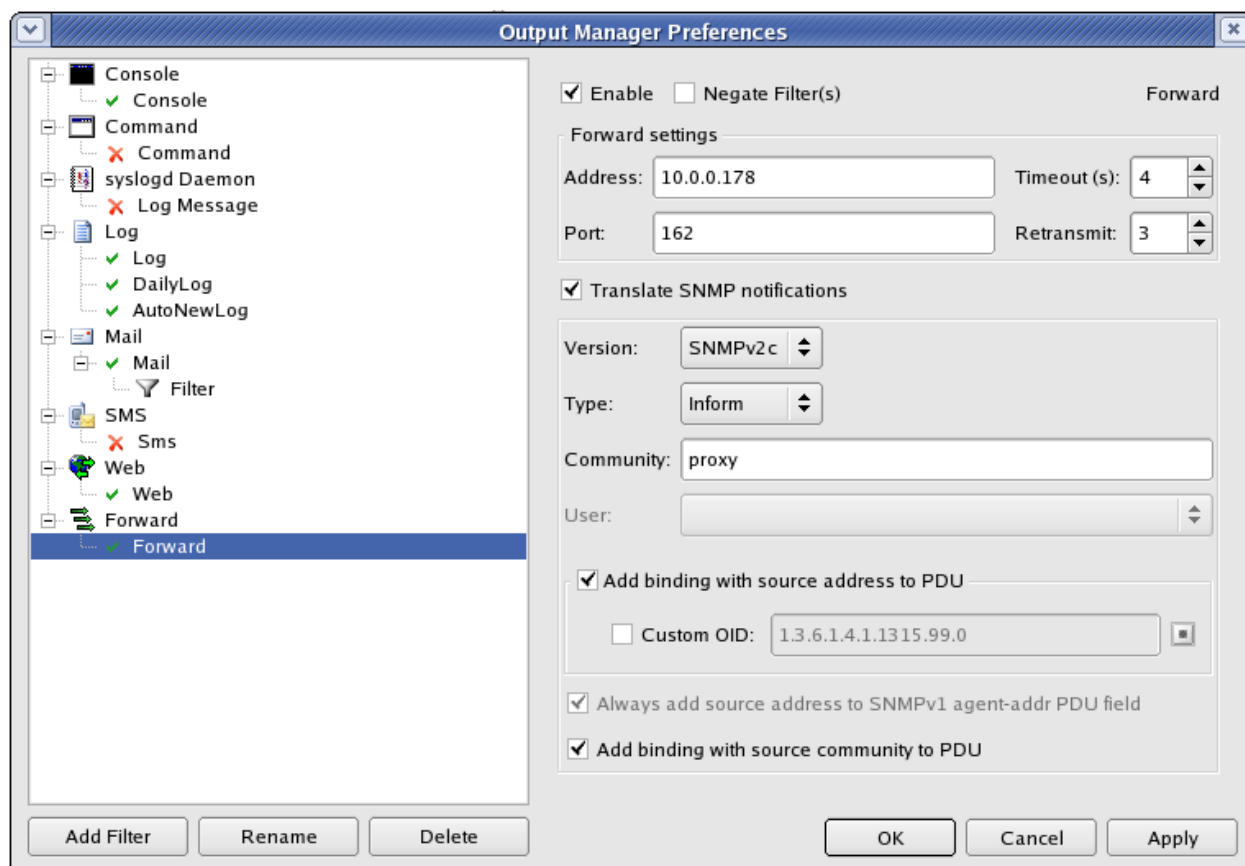


Figure 31: Configuring Forward output unit options

3. Check the **Enable** checkbox in the right panel of the Output Manager Preferences dialog box (Figure 31).
4. Into the **Address** input line, specify the IP address or hostname of the target host to which the SNMP notifications will be forwarded.

5. Into the **Port** input line, enter the number that specifies the UDP port on which the target host can receive SNMP notification messages.
6. Into the **Timeout [s]** input line, enter the timeout value in seconds for pending SNMP Inform messages.

The Timeout value specifies how many seconds the program waits for the Response to the outstanding Inform message. When this time is over, the program cancels or resends the Inform message, depending on the value of the Retransmits parameter.

7. Into the **Retransmits** input line, enter the number of retransmits for pending SNMP Inform messages.

The Retransmits value defines how many times the program resends the SNMP Inform messages after the first timeout.

Note: The **Timeout** and **Retransmit** settings apply only to **SNMP Inform** messages. These settings are ignored for SNMP Trap messages, as they are not retransmitted.

8. To enable translating SNMP notification messages, check the **Translate SNMP notifications** checkbox. If this checkbox is not checked, SNMP notification messages are forwarded unaltered. If this checkbox is checked, you can select the notification translation parameters, i.e., the SNMP version (SNMPv1 or SNMPv2c or SNMPv3) and type (Trap or Inform) of the outgoing notification messages. You can also configure Trap Ringer to add some additional information to the forwarded SNMP notifications, like the notification's source IP address and community string. When translation is enabled, all incoming notification messages are translated according to the configured translation preferences and then forwarded to the target address. Trap Ringer translates the notification parameters according to the SNMP Coexistence specification (RFC 3584).
9. In the **Version** drop-down list, select the version of SNMP to be used for sending the outgoing notification messages.

Tip: Do not select the **SNMPv1** from this drop-down list if the incoming SNMPv2c or SNMPv3 notifications contain variable bindings whose type is Counter64, as such notifications will not be forwarded (the Counter64 data type cannot be conveyed in SNMPv1 messages).

10. In the **Type** drop-down list, select the type of the SNMP notification message (Trap or Inform). All outgoing SNMP notification messages will be of selected type.

Note 1: SNMP Trap messages are unacknowledged notifications, meaning that they do not initiate any response from the receiver. The SNMP Inform messages, on the other hand, require that the receiver replies with a Response message, acknowledging that the notification has been received.

Note 2: SNMP Inform messages are not available in SNMPv1.

11. If you have selected the **SNMPv1** or the **SNMPv2c** entry from the **Version** drop-down list, enter the community name into the **Community** input line. The specified community name will be inserted into all outgoing SNMPv1 or SNMPv2c notification messages.

12. If you have selected the **SNMPv3** entry from the **Version** drop-down list, select an SNMPv3 user profile from the **User** drop-down list. The selected user profile will be used for sending out SNMPv3 notification messages.

Note: You can select among the SNMPv3 user profiles that are configured in the Preferences dialog box, SNMPv3 Users tab. For more information on adding and configuring SNMPv3 user profiles, see the [Configuring SNMPv3 Users](#) section.

13. To enable adding a variable binding carrying the original source address to each forwarded SNMP notification message, check the **Add binding with source address to PDU** checkbox. If this checkbox is checked, Trap Ringer 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 address from which Trap Ringer actually received the notification (if the notification was received as SNMPv2c or SNMPv3 Trap or Inform message). If you want the name (OID) portion of this variable binding to be other than **snmpTrapAddress.0** (1.3.6.1.6.3.18.1.3.0), check the **Custom OID** checkbox and into the accompanying input line specify the OID to be used instead of the **snmpTrapAddress.0** (1.3.6.1.6.3.18.1.3.0). This setting changes only the name (OID) portion of the variable binding, and does not affect the value portion in any way.

Note: The **snmpTrapAddress.0** variable binding will not be inserted into SNMP Trap or Inform PDUs, which already contain this variable binding.

14. If translation to SNMPv1 Trap messages is enabled, you can force inserting the notification source address into the SNMPv1 agent-addr PDU field of every outgoing SNMPv1 Trap. To enable this option, check the **Always add source address to SNMPv1 agent-addr PDU field** checkbox. If this option is disabled, the SNMPv1 agent-addr parameter will be set to 0.0.0.0 unless the original SNMP notification contained the **snmpTrapAddress.0** variable binding (as per RFC 3584).
15. To enable adding a variable binding carrying the original community name to each forwarded SNMP notification message, check the **Add binding with source community to PDU** checkbox. If this checkbox is checked, Trap Ringer appends an additional variable binding to the variable bindings list of every received SNMP notification PDU before forwarding it to the target address. The name portion of this variable binding is **snmpTrapCommunity.0** (1.3.6.1.6.3.18.1.4.0), and the value is either the community name from the original notification received by Trap Ringer (if the notification was received as SNMPv1 or SNMPv2c notification message), or a zero-length string (if the notification was received as SNMPv3 notification message).

Note: The **snmpTrapCommunity.0** variable binding will not be inserted into SNMP Trap or Inform PDUs, which already contain this variable binding.

16. Click the **Apply** button to apply the settings or the **OK** button to apply the settings and close the Output Manager Preferences dialog box.

17. From this point on, Trap Ringer server will forward the received SNMP notification messages to the specified target address.

Tip: To enable forwarding only those SNMP notifications that match the given criteria, add one or more filters to the Forward output unit, as described in the [Filtering SNMP Notifications](#) section.

7 FILTERING SNMP NOTIFICATIONS

The received SNMP Trap and Inform notifications can be filtered . Filters can be set up to allow only the notifications selected by the filter conditions to be displayed.

If an SNMP Trap or Inform message successfully passes through the filter, it is forwarded to the associated output unit. For example, one Mail output unit can be used for sending SMS messages via e-mail and can have a filter attached that will let through only notifications coming from a particular address, while another Mail output unit with another filter will send e-mails to other recipients on notifications coming from other sources, etc.

Filters can be added and configured either manually or by selecting an existing SNMP notification in the main window and running the Create filter from notification wizard. The second approach significantly speeds up the filter creation process as the wizard automatically creates filter conditions that match the properties of the selected SNMP notification for you. Of course, the wizard can create filters only from notifications that have been already received by Trap Ringer. The manual approach, on the other hand, can be used for creating filters for receiving or blocking any kind of SNMP notifications, regardless of whether they have been already received or not. This section describes both procedures of creating filters in Trap Ringer.

About Filters

Each output unit (e.g., Console, Log, SMS, Mail, etc.) can have any number of filters attached. Furthermore, a filter can contain any number of filter conditions.

Note: Filters attached to the same output unit are connected with the logical OR operator, while filter conditions within a filter are connected with the logical AND operator.

7.1 Creating Filters from Received SNMP Notifications

Trap Ringer lets you select a received SNMP notification displayed in the main window and run a wizard to create a filter for receiving or blocking SNMP notifications of the same type. The wizard automatically creates filter conditions that match the attributes of the selected SNMP notification. To complete the wizard, simply accept or modify the offered filter conditions and choose the output unit (e.g., Console, Mail, SMS, Log, etc.) to which you want to attach the filter.

7.1.1 Creating Filter from Notification

This method lets you select a notification listed in the Trap List panel and create a filter from it, as follows:

1. Right-click the SNMP notification in the Trap List window panel from which you want to create a filter and select the **Create Filter from Notification** pop-up command (Figure 32).

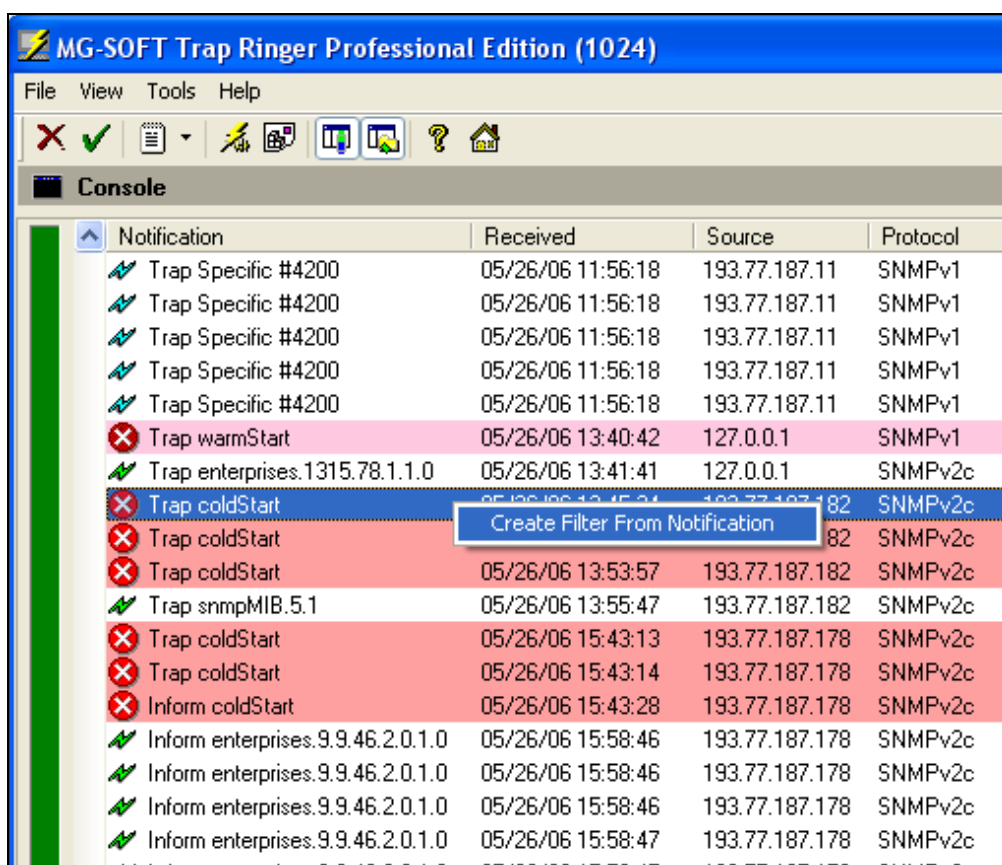


Figure 32: Starting Create Filter From Notification wizard

2. The first screen of the Create Filter From Notification wizard appears, listing filter conditions created from the selected notification. The wizard automatically selects (enables) the most commonly used conditions from the entire list of conditions (Figure 33). Disabled filter conditions are displayed in red color. To enable those conditions, click the checkboxes in front of them.

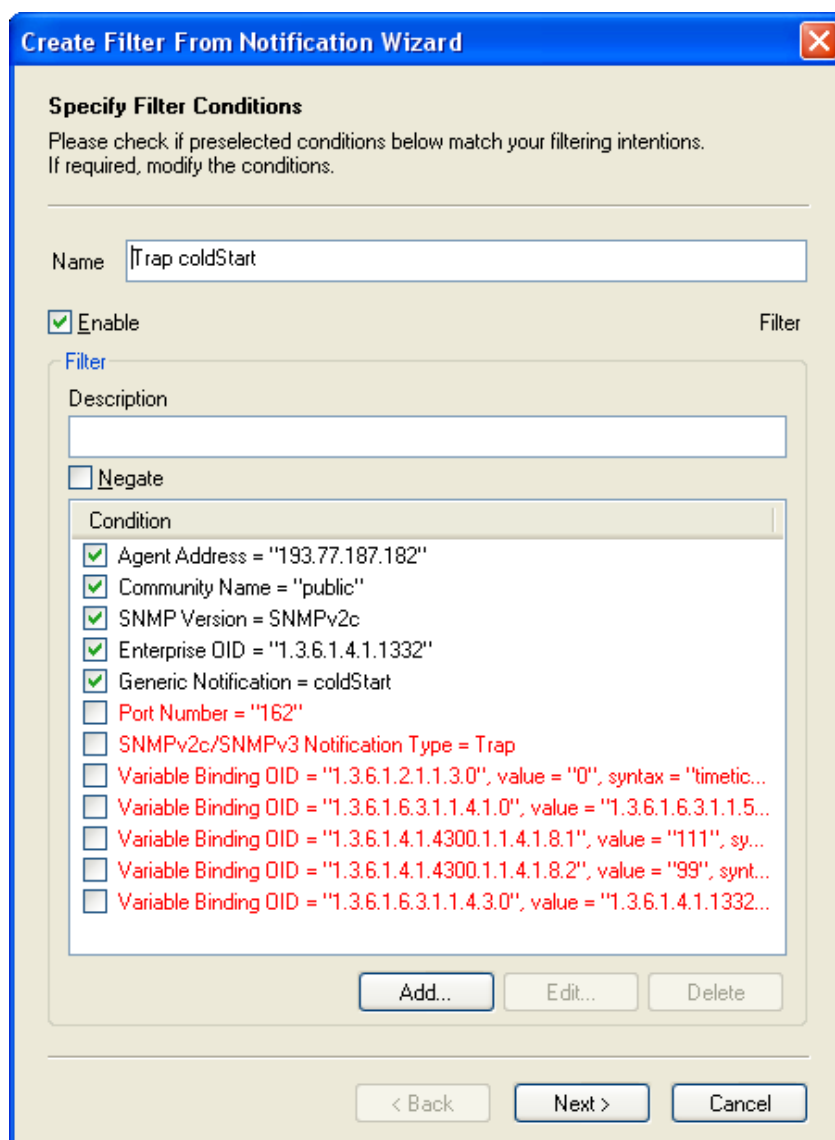


Figure 33: Create Filter From Notification wizard – first step

3. To modify a filter condition, select it in the Conditions list and click the **Edit** button. The Edit Condition dialog box appears where you can modify the selected filter condition. This dialog box has the same appearance and offers the same options as the [Add Condition](#) dialog box.
4. After selecting the desired filter conditions, click the **Next** button at the bottom of the Create Filter From Notification Wizard dialog box to proceed to the next screen.
5. The second and final screen of the Create Filter From Notification wizard displays all existing output units as available in the Output Manager Preferences dialog box ([Figure 34](#)). To attach the filter to an output unit, check the checkbox in front of it.
6. Click the **Next** button to finish the wizard and apply the changes. From that moment on, the filter will let through (and pass to the given output unit) only those SNMP notifications whose attributes match the (enabled) filter conditions.

Tip: Later, you can view, modify, enable/disable or remove the filter in the [Output Manager Preferences](#) dialog box.

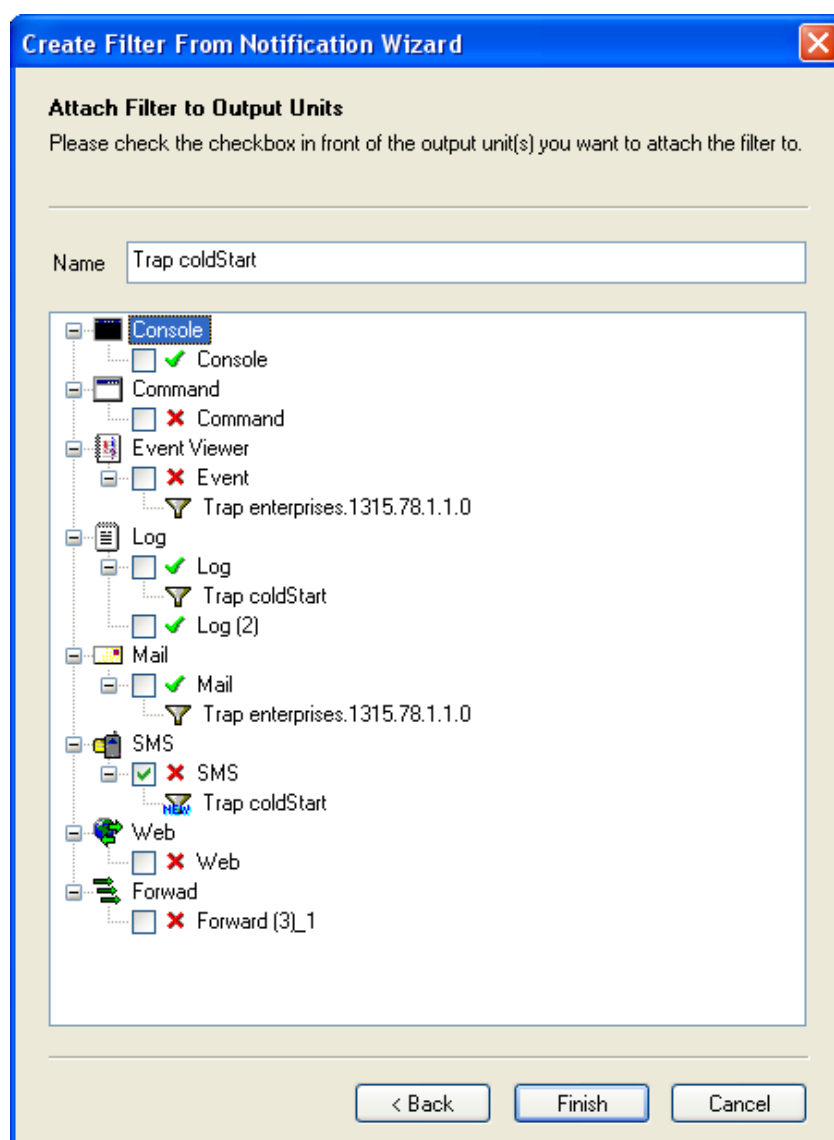


Figure 34: Create Filter From Notification wizard – second step

7.2 Creating Filters Manually


In addition to creating filters by running the **Create filter from notification** wizard, filters can also be created manually, as described in this section. To manually create a filter in the Output Manager Preferences dialog box, you need to add a filter to an output unit and configure filter conditions.

For detailed information on creating filters in the Output Manager Preferences dialog box, see the following sections:

1. [Adding Filters to Output Units](#)
2. [Configuring Filter Conditions](#)
3. [Example of Configuring Filter in Trap Ringer Output Manager](#)

7.2.1 Adding Filters to Output Units

To manually add a filter to an output unit:

1. Open the Output Manager Preferences dialog box by selecting the **Tools / Output Manager Preferences** command or by clicking the **Output Manager Preferences** toolbar button. 
2. To add a filter to the output unit (e.g., to Log(2), Mail, Console, etc.), select the output unit in the Output Manager tree structure and use the **Add Filter** button or the **Add Filter** pop-up command (Figure 35).

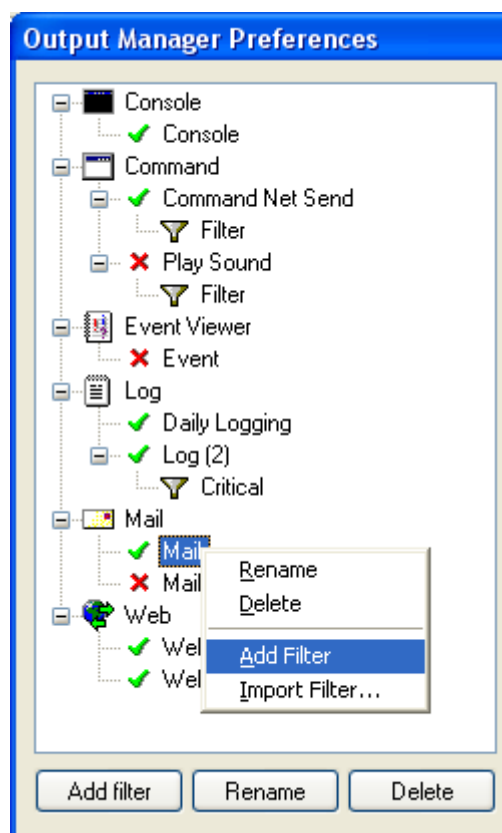


Figure 35: Adding a filter to output unit

3. A new, disabled filter icon will be added to the selected output unit as its child item. By default, all filters carry the name "Filter". To rename a filter, use the **Rename** pop-up command and enter a new name for it (e.g., "coldStart trap filter").
4. Select the filter icon to display its properties in the right panel of the Output Manager Preferences dialog box (Figure 36). Check the **Enable** checkbox to enable the filter and to configure its properties.
5. Into the **Description** input line enter optional filter description (e.g., "coldStart generic SNMPv1 trap filter").
6. The **Condition** list displays the existing filter conditions and lets you edit or remove them as well as add new filter conditions to the filter.

- ❑ To add a new filter conditions to the filter, click the **Add** button below the Condition list. For more information on adding and configuring filter conditions, see the next chapter.
 - ❑ To view or edit a filter condition, select it in the Condition list and click the **Edit** button. For more information on configuring filter conditions, see the next chapter.
 - ❑ To remove a filter condition, select it in the Condition list and click the **Delete** button. This removes the selected condition from the Condition list.
7. If you want to logically negate (invert) all conditions of the selected filter, check the **Negate** checkbox in the Filter frame of the Filter Preferences panel.

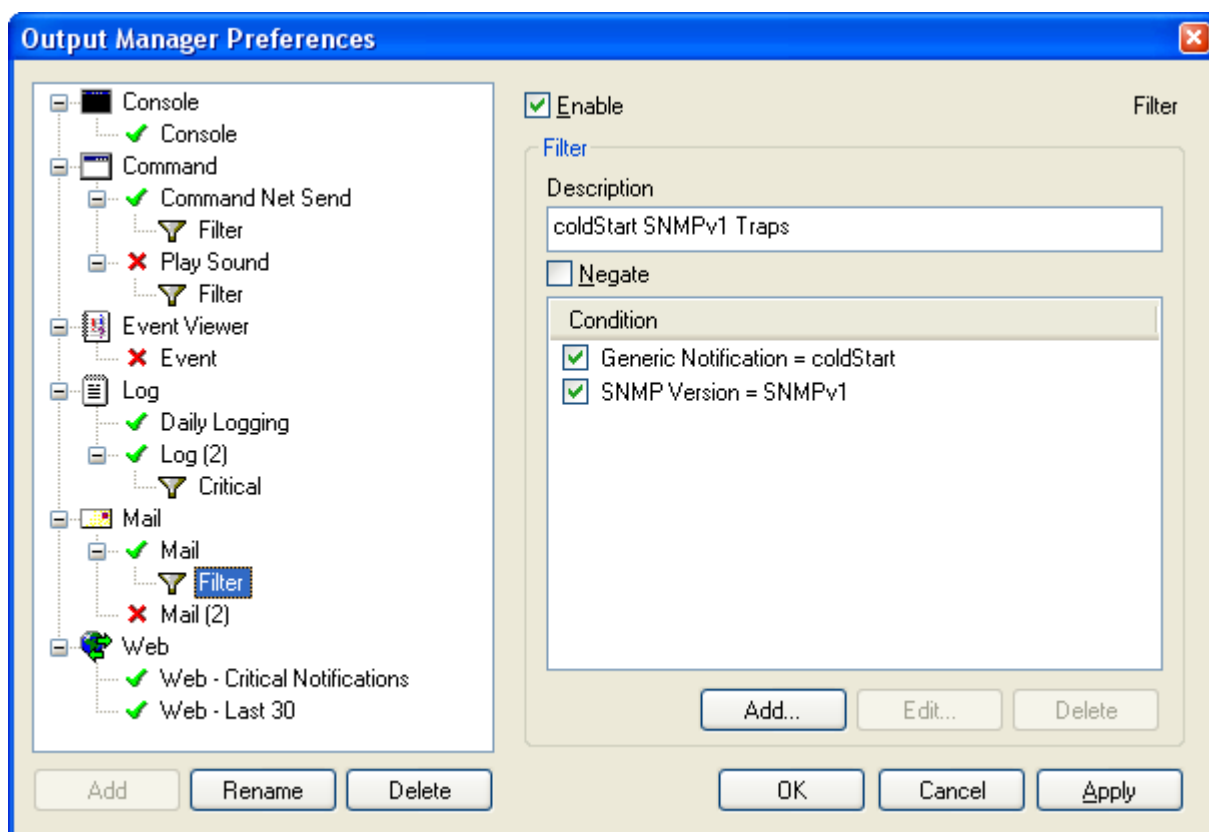


Figure 36: Filter Preferences panel

You can add any number of filters to the output unit and every filter can contain any number of filter conditions.

Note: Filters added to the output unit are connected with the **logical OR operator**, while filter conditions within a filter are connected with the **logical AND operator**.

Tip: To save a configured filter with all filter conditions for future use, select the filter in the Output Manager tree structure and use the **Save Filter** pop-up command. Specify the location and the file name for filter file. A saved filter can be easily added to another output unit by selecting the output unit and using the **Import Filter** pop-up command.

7.2.2 Configuring Filter Conditions

1. To manually add a filter condition to the filter, select the relevant filter icon in the Output Manager tree structure to display Filter Preferences panel and click the **Add** button in the Filter frame (Figure 36).
2. The Add Condition dialog box appears, where you can configure a filter condition.

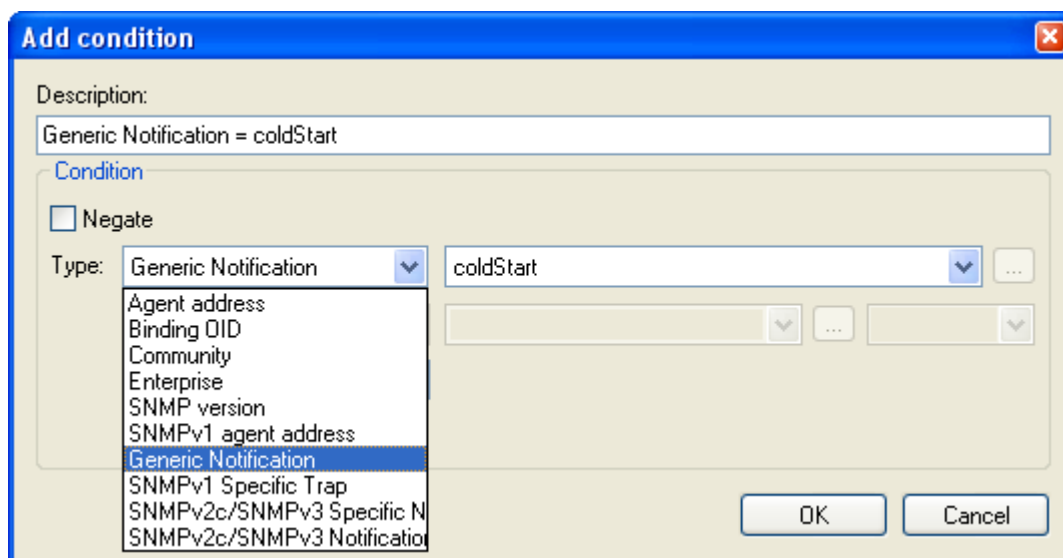


Figure 37: Configuring a filter condition

3. The **Description** input line automatically displays the condition description according to your selections made in the Condition frame. The description text can be freely edited.
4. If you want to logically negate (invert) the filter condition, check the **Negate** checkbox in the Condition frame.
5. Select the desired filter condition type from the **Type** drop-down list. The following types of filter conditions can be selected and configured:

❑ **Agent Address**

Lets you configure a filter condition that will let through only SNMP notifications coming from a particular address or from a **range** of IPv4 addresses (ignoring notifications coming from all other addresses). To configure an Agent Address filter condition, specify the IPv4 or IPv6 address of the SNMP agent (whose notifications you do not want to ignore) into the accompanying drop-down list. Alternatively, specify a range of IPv4 addresses using the following notation:

ip.ip.ip.ip-ip.ip.ip.ip For example, 10.0.0.1-10.0.0.254.

The SNMP notifications received from addresses that are part of the specified address range will be forwarded to the associated output unit (e.g., Console, Log(2), Mail(3), etc.).

❑ **SNMPv1 Agent Address**

Lets you configure a filter condition that will let through only SNMPv1 trap notifications having the value of the “agent-addr” field in the SNMPv1-Trap-PDU equal to the address you specify into the accompanying drop-down list.

Alternatively, specify a **range** of IPv4 addresses using the following notation:

ip.ip.ip.ip-ip.ip.ip.ip For example, 10.0.0.1-10.0.0.254.

The SNMP notifications received from addresses that are within the specified address range will be forwarded to the associated output unit (e.g., Console, Log(2), Mail(3), etc.).

Note that SNMPv1 Agent Address applies only to SNMPv1 traps and that this address can differ from the Agent Address.

❑ **Community**

Lets you configure a filter condition that will let through only SNMP notifications with the community name specified in the accompanying drop-down list (e.g., “public”).

❑ **Enterprise**

Lets you configure a filter condition that will let through only SNMP notifications with a particular enterprise OID (specified in the accompanying drop-down list). This OID will be compared with the value of the “enterprise” field in the SNMPv1 trap messages or with the value of the “snmpTrapEnterprise.0” variable binding included into SNMPv2c and/or SNMPv3 notification messages.

❑ **SNMP Version**

Lets you configure a filter condition that will let through only notifications of particular SNMP protocol version (i.e., SNMPv1 traps or SNMPv2c traps and informs or SNMPv3 traps and informs).

❑ **Generic Notification**

Lets you configure a filter condition that will let through only generic SNMP notifications (all or only particular generic notifications), by selecting the “[any]” or a particular generic notification type (e.g., “coldStart”, “warmStart”, “linkUp” etc.) from the accompanying drop-down list.

❑ **Binding OID**

Lets you configure a filter condition that will let through only SNMP notifications containing a particular variable binding. To configure a variable binding filter condition, select the “Binding OID” entry from the Type drop-down list and enter the OID of the variable binding into the accompanying drop-down list. Alternatively, click the **Browse** (...) button next to the OID drop-down list and select the desired object from the MIB tree. The OID of the selected object will be automatically inserted into the OID drop-down list. Additionally, you can refine the filter condition by specify the variable binding's value, syntax, and its position in the variable bindings list.

❑ **Value** (checkbox and drop-down lists)

If checked, you can specify the value and the syntax of variable binding by using the accompanying drop-down lists. To do this, select the desired operator from the leftmost drop-down list (e.g.: =, >, contains, etc.) and enter the corresponding value into the middle drop-down list. The rightmost drop-down list lets you select the variable bindings syntax (e.g., Integer, Octet

String, Counter32, etc.). According to the selected syntax, different operators are available in the leftmost drop-down list.

- ❑ **Position** (checkbox and input line) business
If checked, you can specify the variable binding's position in the variable bindings list included in the notification's PDU. For example the number "1" means that this variable binding should be the first binding in the variable bindings list.
- ❑ **Include sub-identifiers** (checkbox)
If checked, the condition will let through notification with variable bindings that have zero, one or more sub-identifier(s) appended to the OID. For example, if the binding OID is 1.3.6.1.2.1.2.2.1.1 (ifIndex), and this checkbox is checked; all variable binding OIDs that start with 1.3.6.1.2.1.2.2.1.1 will be passed through (e.g., 1.3.6.1.2.1.2.2.1.1.1 (ifIndex.1), 1.3.6.1.2.1.2.2.1.1.10.5.3 (ifIndex.10.5.3), etc.).
This option is useful when creating conditions that apply to columnar OIDs, whose object instances dynamically change (rows are being created and destroyed in the corresponding SNMP table).

The screenshot shows a dialog box titled "Add condition" with a description field containing: "Variable Binding OID = '1.3.6.1.2.1.2.2.1.8.*', value = '2', syntax = 'integer', binding position = 5th". Below this is a "Condition" section with a "Negate" checkbox (unchecked). The "Type" is set to "Binding OID" with a dropdown menu. The value "1.3.6.1.2.1.2.2.1.8" is entered in the text field, followed by a dropdown menu and an ellipsis button. Below this, there are three checked checkboxes: "Value", "Position", and "Include sub-identifiers". The "Value" checkbox has a dropdown menu set to "=", a text field containing "2", a dropdown menu set to "Integer32", and an ellipsis button. The "Position" checkbox has a text field containing "5" and a spin button. The "Include sub-identifiers" checkbox is checked. At the bottom right are "OK" and "Cancel" buttons.

Figure 38: Example of a variable binding filter condition

The example in [Figure 38](#) shows a variable binding filter condition that, when applied, will let through only those SNMP notifications that include the variable binding with OIDs of 1.3.6.1.2.1.2.2.1.8.* (ifOperStatus.*), where the syntax of this binding must be Integer32 and the value of this OID must be 2 (down(2)). Additionally, this variable binding must be the 5th binding in the variable bindings list included in the SNMP trap or inform notification message. Note that because the **Include sub-identifiers** checkbox is checked, this condition will let through all object instances of the ifOperStatus columnar object. The variable binding shown in the picture above can be found in (some) SNMPv2c/v3 linkDown and linkUp notification messages.

- ❑ **SNMPv1 Specific Trap**
Lets you configure a filter condition that will let through only SNMPv1 specific trap notifications with the trap number specified in the accompanying drop-down list (e.g., “1”).
 - ❑ **SNMPv2c/SNMPv3 Specific Notification**
Lets you configure a filter condition that will let through only SNMPv2c and SNMPv3 notifications, whose value (OID) of the “snmpTrapOID.0” variable binding matches the one specified in the accompanying drop-down list.
 - ❑ **SNMPv2c/SNMPv3 Notification Type**
Lets you configure a filter condition that will let through only SNMPv2c and SNMPv3 trap notifications or only SNMPv2c and SNMPv3 inform notifications.
 - ❑ **Port**
Lets you configure a filter condition that will let through only SNMP notifications received on a particular IPv4/UDP or IPv6/UDP port.
6. After configuring a filter condition, click the **OK** button to add condition to the filter.

Note: You can add any number of filter conditions to a filter. Filter conditions are connected with the logical AND operator.

Tip: To save a configured filter (with all filter conditions) to a file, select the filter in the Output Manager tree structure and use the **Save Filter** pop-up command. Specify the location and the name for the filter file. A saved filter can later easily be added to another output unit by selecting the output unit, choosing the **Import Filter** pop-up command and pointing the dialog that appears to the relevant filter file.

7.2.3 Example of Configuring Filter in Trap Ringer Output Manager

Example: How to configure a filter that will pass through only coldStart and warmStart generic SNMPv1 and SNMPv2c notifications?

First, let us consider using a single filter and adding the following conditions to it:

```
Generic Notification = coldStart
Generic Notification = warmStart
```

This would connect both filter conditions with logical AND operator and thus create a criteria, which is never true because no SNMP notification can be coldStart and warmStart notification at the same time. Note that conditions within a filter are always connected with **logical AND operator**. On the other hand, filters that are added to the same output unit are connected with **logical OR operator**. Therefore, we need to add and configure two filters, one for each type of generic notification.

To configure both filters, do the following:

1. Add the first filter to the output unit by selecting the output unit in the Output Manager tree structure and using the **Add Filter** pop-up command (Figure 35).
2. Select the newly created filter icon in the Output Manager tree structure and use the **Rename** pop-up command to rename the filter (e.g., “coldStart SNMPv1 & SNMPv2c filter”).
3. Select the filter icon to display its properties in the right panel of the Output Manager Preferences dialog box (Figure 36). Check the **Enable** checkbox to enable the filter.
4. Optionally, enter a filter description into the **Description** input line (e.g., “coldStart SNMPv1 & SNMPv2c notification filter”).
5. Click the **Add** button in the Filter frame (Figure 36) to add the first filter condition to the filter. The Add Condition dialog box appears.
 - ❑ Configure the following condition by selecting appropriate entries from the **Type** drop-down list and the drop-down list next to it:


```
Generic Notification = coldStart
```
 - ❑ Click the **OK** button to add condition to the filter.
6. Click the **Add** button in the Filter frame to add the second filter condition to the filter. The Add Condition dialog box appears.
 - ❑ Configure the following condition by selecting the entries from the **Type** drop-down list and the drop-down list next to it:


```
SNMP version = SNMPv3
```
 - ❑ Click the **Negate** checkbox to logically invert the condition.
 - ❑ Click the **OK** button to add condition to the filter.

The first filter is now configured and should look like this:

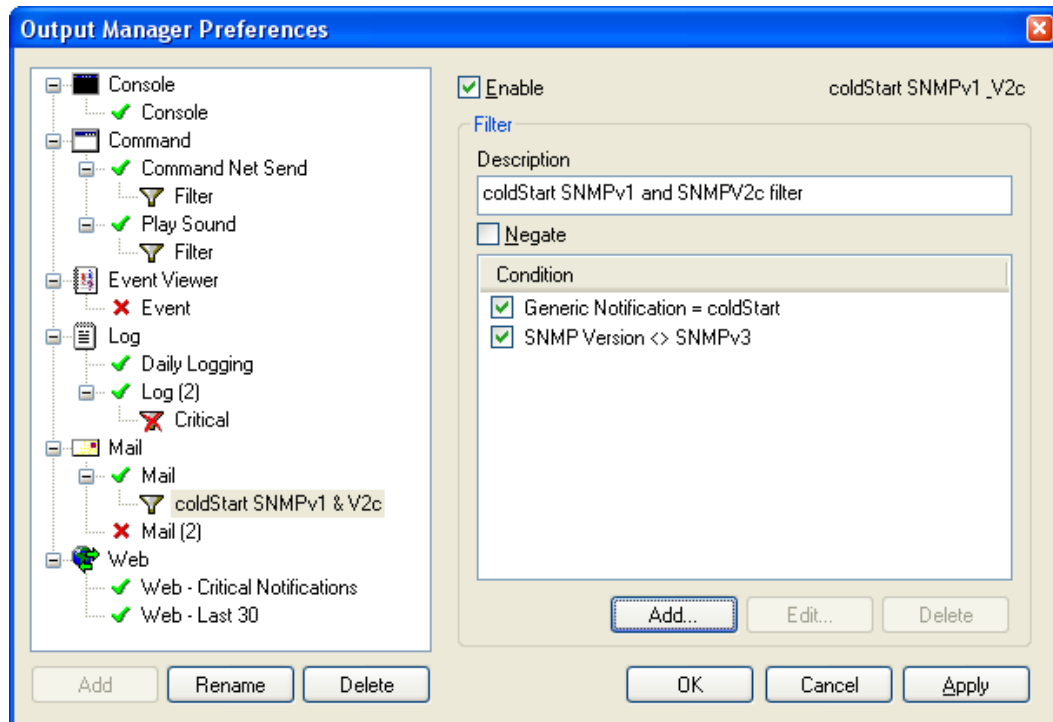


Figure 39: Example of a “coldStart SNMPv1 & SNMPv2c filter”

7. Repeat the above procedure to add the second filter to the output unit, but instead of the Generic Notification = coldStart, configure the Generic Notification = warmStart condition in [step 5](#).
8. The second filter should look like this:

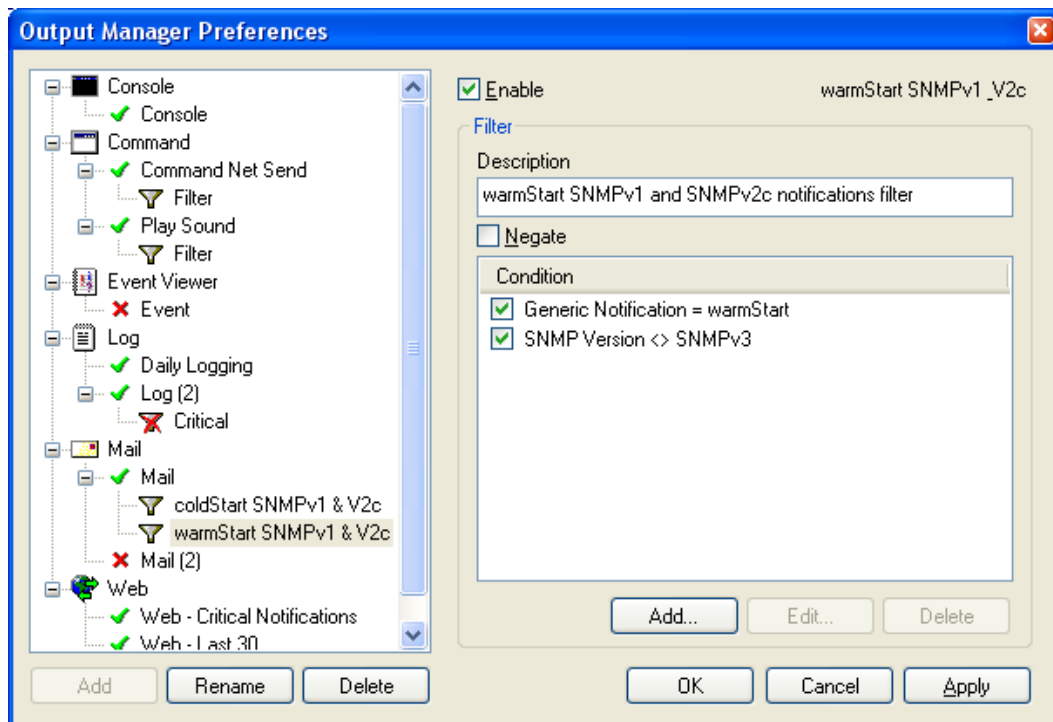


Figure 40: Example of a “warmStart SNMPv1 & SNMPv2c filter”

9. Click the **Apply** button in the Output Manager Preferences dialog box to apply the filters or the **OK** button to apply the filters and close the dialog box.

From this point on, Trap Ringer server will send an e-mail to the specified recipient(s) whenever it receives an SNMPv1 coldStart or warmStart Trap message or SNMPv2c coldStart or warmStart Trap or Inform message.

8 SEARCHING FOR SNMP NOTIFICATIONS

Trap Ringer toolbar contains a convenient search tool that lets you search console or the currently displayed log file for those SNMP Trap and Inform notification messages that match the search criteria.


SNMP notifications can be searched for by virtually any category (property), like the notification type (name), reception date and time, source address, included variable bindings, etc.

When you select the search options, enter a search term and press the **Enter** key or click the **Search** button, the search is started and the SNMP notifications that match the search conditions are displayed in the [Trap List window panel](#). Note that once a search is started, it remains active until you cancel it. Active search behaves as a continuous display filter, meaning that only those newly received SNMP notifications that match the search criteria are added to the list.

To search for specific SNMP notifications in the Console log:

1. To display the contents of the console log in the main window, select the **View / Console** menu command. All SNMP notifications logged in the console log file are displayed in the main window ([Trap List window panel](#)).

Tip: To display the contents of a log file in the main window, select the respective **View / Log / <Log Name>** command.

2. In the Trap Ringer toolbar locate the search tool and click the down arrow () button next to the **Search** button to display the **Search Parameters** drop-down menu ([Figure 41](#)).

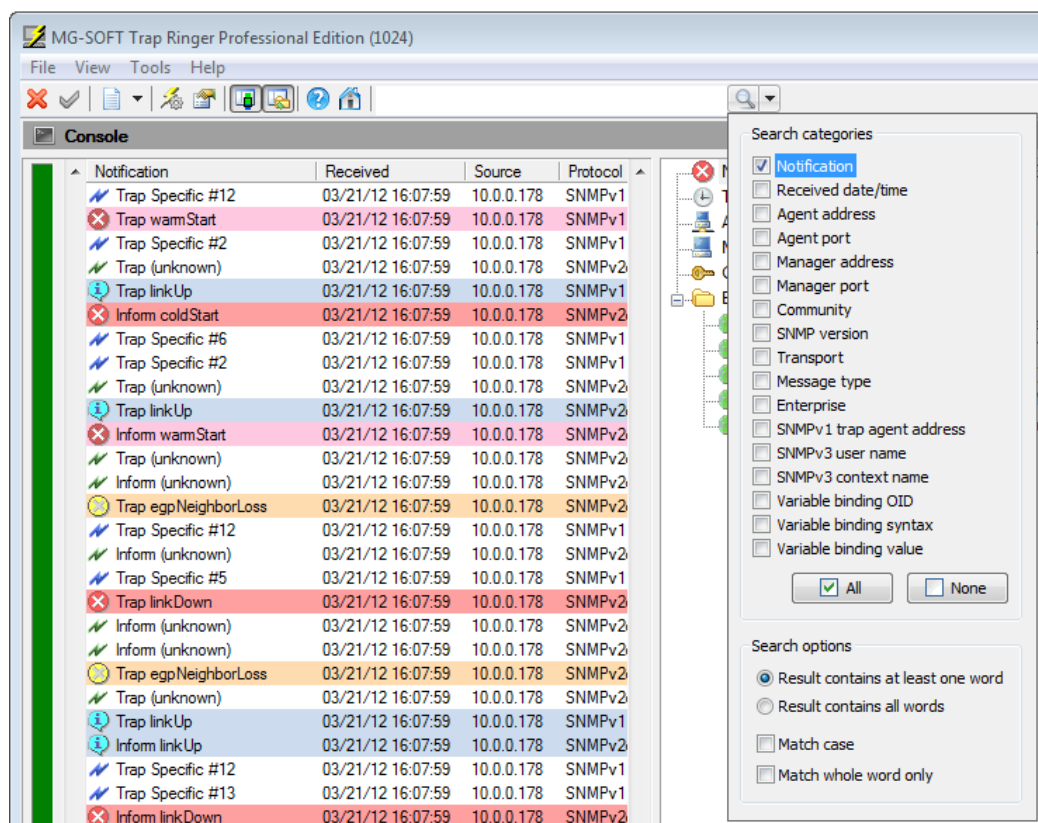


Figure 41: Search Parameters drop-down menu

3. In the **Search Parameters** drop-down menu, check the checkboxes in front of the **categories** (notification properties) you want to search, e.g., Notification, Received date/time, Agent address, etc. and optionally set the search options (Match case, Match whole words only). The **Search Parameters** drop-down menu contains the following components:

Search categories

Contains the list of categories (SNMP notification properties) that you can search:

Tip: You can significantly speed up the initial search query by deselecting the categories that do not need to be searched in the given case. The search performance is most notably increased if you disable the variable binding categories.

Notification (checkbox)

The SNMP notification name or OID (e.g., "Trap coldStart", "Trap Specific #2", "Inform 1.3.4.5.6.7.4.5.6.2.0", etc.). For example, to find all SNMP notifications that contain word "link" in its resolved name (e.g., linkDown, linkUp, etc.), use the following search query: `link`

Note: A notification can be found by its name only if the MIB module that defines the given SNMP notification is currently loaded in Trap Ringer.

Received date/time (checkbox)

The date and time of SNMP notification reception in MM/DD/YY hh:mm:ss format (e.g., "03/29/12 16:49:10"). For example, to find all SNMP notifications received in March 2012, use the following search query: `03/*/12`

To find all SNMP notification received on March 29th, 2012 at 16:xx hours, use the following search query: `"03/29/12 16"` (with quotes).

Agent address (checkbox)

The SNMP notification source address, i.e., IPv4 or IPv6 address from which the notification has been sent (e.g., "10.0.100.1", "fe80::cd4b:2292:3e04:2cc6", "::1", etc.). For example, to find all SNMP notifications sent from the 10.0.x.x subnet, use the following search query: `10.0.`

Agent port (checkbox)

The SNMP notification source port, i.e., the UDP port number from which the notification has been sent (e.g., "161", etc.).

Manager address (checkbox)

The SNMP notification destination address, i.e., IPv4 or IPv6 address on which the notification has been received (e.g., "10.0.12.3", "fe80::cd4b:2232:3e04:2cc8", etc.).

Manager port (checkbox)

The SNMP notification destination port, i.e., the UDP port number on which the notification has been received (e.g., "162", etc.).

Community (checkbox)

The community name included in the SNMP notification message (e.g., "public", etc.).

SNMP version (checkbox)

The version of the SNMP protocol used to convey the notification message (e.g., "SNMPv1", "SNMPv2c" or "SNMPv3").

Transport (checkbox)

The SNMP notification transport protocol, i.e., the IPv4/UDP or IPv6/UDP port number on which the notification has been received (e.g., "IPv4/UDP", etc.).

Message type (checkbox)

The SNMP notification message type, i.e., Trap or Inform (e.g., "Trap", etc.).

Enterprise (checkbox)

The enterprise OID or name associated with the SNMP notification (e.g., "1.3.6.1.4.1.1315", "mgSoft", etc.). This is the value of the "enterprise" field in SNMPv1 Trap messages and the value of the "snmpTrapEnterprise.0" variable binding included in SNMPv2c and SNMPv3 Trap and Inform messages.

Note: The enterprise name can only be found if the MIB module that defines the given MIB object (OID) is currently loaded in Trap Ringer.

SNMPv1 trap agent address (checkbox)

The agent address specified in the "agent-addr" field of the SNMPv1 Trap PDU (e.g., "10.0.12.3", etc.). Note that this address applies only to SNMPv1 Trap messages and that this address can differ from the Agent address.

SNMPv3 user name (checkbox)

The name on the user on behalf of which the SNMPv3 Trap or Inform message has been sent (e.g., "joe", "NoAuthUser", etc.).

SNMPv3 context name (checkbox)

The name on the SNMP context in which the SNMPv3 Trap or Inform message has been sent (e.g., "", "public", etc.).

Variable binding OID

The OID or name of the variable binding included in the SNMP notification message (e.g., "syUpTime.0", "1.3.6.1.2.1.1.3.0", etc.). For example, to find all SNMP notifications that contain a variable binding, whose name portion is ifOperStatus.x (1.3.6.1.2.1.2.2.1.8.x), use the following search query:
`ifOperStatus` or `1.3.6.1.2.1.2.2.1.8`

Note: The name can only be found if the MIB module that defines the given MIB object (OID) is currently loaded in Trap Ringer.

Variable binding syntax (checkbox)

The base or composed syntax of the variable binding included in the SNMP notification message (e.g., "INTEGER", "Counter32", "DisplayString", etc.).

Note: The composed syntax can only be found if the MIB module that defines the given MIB object (OID) is currently loaded in Trap Ringer.

Variable binding value (checkbox)

The value of the variable binding included in the SNMP notification message (e.g., "1", "down(2)", "20 port converter chassis", etc.). If a value is of a type that can be resolved through MIB (e.g., OBJECT IDENTIFIER, Integer enumeration, etc.) one can search also by the resolved value (e.g., for an enumerated integer, use search string `down` instead of the integer value `2`).

Note: The resolved value can only be found if the MIB module that defines the given MIB object (OID) is currently loaded in Trap Ringer.

Tip: You can significantly speed up the initial search query by deselecting the categories that do not need to be searched in the given case. The search performance most notably increases if you deselect the variable binding categories, especially the **Variable binding value** category.

All (button)

Quickly selects all categories.

None (button)

Quickly deselects all categories.

Search options**Result contains at least one word** (radio button)

If selected, the words in the query are connected with **logical OR operation**, meaning that all SNMP notifications that **contain either** the first or the second (or third, etc.) word or any combination of entered words in any of the selected categories will be found and displayed as results. (e.g., the query `inform coldstart` (two words separated by white space) will find all SNMP notifications that contain either string `inform` or string `coldstart` or both in the Notification category (provided that only the Notification search category is selected). This is the default search option.

Result contains all words (radio button)

If selected, the words in the query are connected with **logical AND operation**, meaning that all SNMP notifications that **contain all words** in the selected categories will be found and displayed as results. (e.g., the query `inform coldstart` (two words separated by white space) will find all SNMP notifications that contain both words `inform` and `coldstart` (in any order) in the Notification category (provided that only the Notification search category is selected).

Match case (checkbox)

If checked, the search is case sensitive, meaning that search operation distinguishes between uppercase and lowercase letters. If this option is enabled, the search will find only those strings in which the capitalization matches the one used in the search query (e.g., `link` will find `linkDown`, but not `LinkDown`).

Match whole word only (checkbox)

If this option is enabled, the search will find only those strings that are whole words and not part of a larger word (e.g., `link` will find `link Down`, but not `linkDown`).

4. Into the Search box enter the search query containing one or more words you are searching for (Figure 42). For example, enter the `linkDown` word to find all generic `linkDown` notification messages, or enter the `linkDown linkUp` query (two words separated by white space) to find all `linkUp` and `linkDown` generic notifications (provided that the `Notification` search category is selected, and the `Result contains at least one word` search option is selected). Alternatively, you can enter only the word `link` to find all SNMP notifications that contain word “link” in the selected search categories (e.g., `Notification` category).

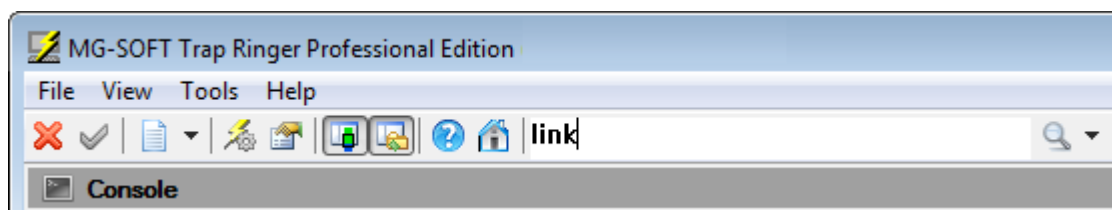





Figure 42: Entering a search query into the Search box

The following **rules** apply to search queries:

- ❑ A search query contains one or more words.
- ❑ A word in this context is a sequence of one or more printable characters. Words are separated by white space characters.
- ❑ If only one word is entered into the search box, all SNMP notifications that **contain** the entered word in any of the enabled categories will be found and displayed.
- ❑ If two or more words are entered into the search box, the words are combined with **logical OR operation** by default (i.e., when the **Result contains at least one word** search option is selected). This means that all SNMP notifications that contain either the first or the second (or third, etc.) word or any combination of entered words in any of the selected categories will be found and displayed as results. This search behavior can be changed by selecting the **Result contains all words** search option, which combines the words with **logical AND operation**, meaning that SNMP notifications that contain all words in the selected search categories will be found and displayed as results.
- ❑ The **asterisk (*)** is a wildcard character that replaces any set of characters. For example, use the `03/*/12` string (`Received date/time` category enabled) to find all notifications received in the third month of the year 2012. To search for the asterisk (*) character, prefix the asterisk with backslash (\), i.e., `*`.
- ❑ To find the exact sequence of words, put the words in **double-quotes (")**. For example, the `trap coldstart` search query will find all SNMP Trap messages and all `coldStart` Trap and Inform messages, while the `"trap coldstart"` search query will find only SNMP Trap `coldStart` messages.

- After entering the search query into the Search box, press the **Enter** key or click the **Search** button () to start the search operation. Trap Ringer performs the initial search query in the given log file using the search criteria you specified (the **Abort Search** button () is displayed in the Search tool during the initial search query). When the initial search query finishes, the SNMP notifications that match the search conditions are displayed in the main window ([Figure 43](#)). The **status bar** displays the number of SNMP notifications that match the search criteria and the total number of SNMP notifications in the file, separated by “/”, e.g., 9000/66390 ([Figure 43](#)).

Tip: If the initial search query takes a long time to complete (it depends on the number of SNMP notifications in the given log file and the complexity of the search), you can click the **Abort Search** button () displayed in the Search tool to stop the initial search query before it finishes and view partial results. Even if you abort the initial search query, the search filter will still apply to all newly received SNMP notifications messages (until you cancel the search operation).

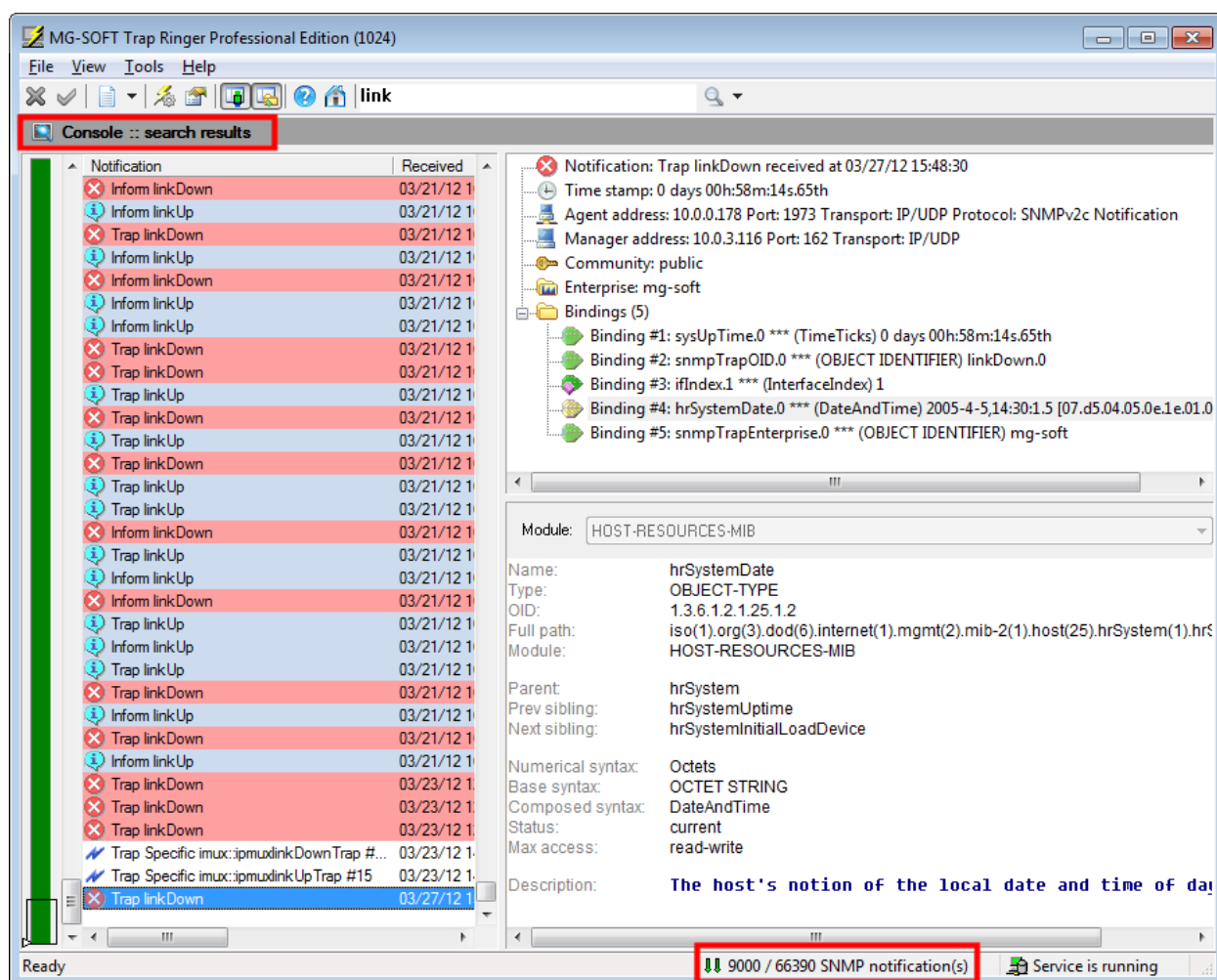



Figure 43: Viewing the search results (the list of results is dynamic)

Note: Once a search is started, it remains active until you cancel it. Active search behaves as a continuous display filter, meaning that the list of results changes over time, i.e., the newly received SNMP notifications that match the search criteria are being automatically added to the list and the SNMP notifications that are deleted from the log file (if any) automatically disappear from the list.

To cancel the search, press the **Esc** keyboard key. This will clear the Search box and display all SNMP notifications in the given log file. Alternatively, you can manually clear the Search box and press the **Enter** key or click the **Search** button.

Search Example: How to find all SNMPv2c Inform notification messages

1. In the search tool click the down arrow () button to display the **Search Parameters** drop-down menu.
2. In the Search Parameters drop-down menu, select the **SNMP version** and **Message type** categories and deselect (uncheck) all other search categories (Figure 44).
3. In the Search Parameters drop-down menu, select the **Result contains all words** search option and deselect (uncheck) all other search options (Figure 44).

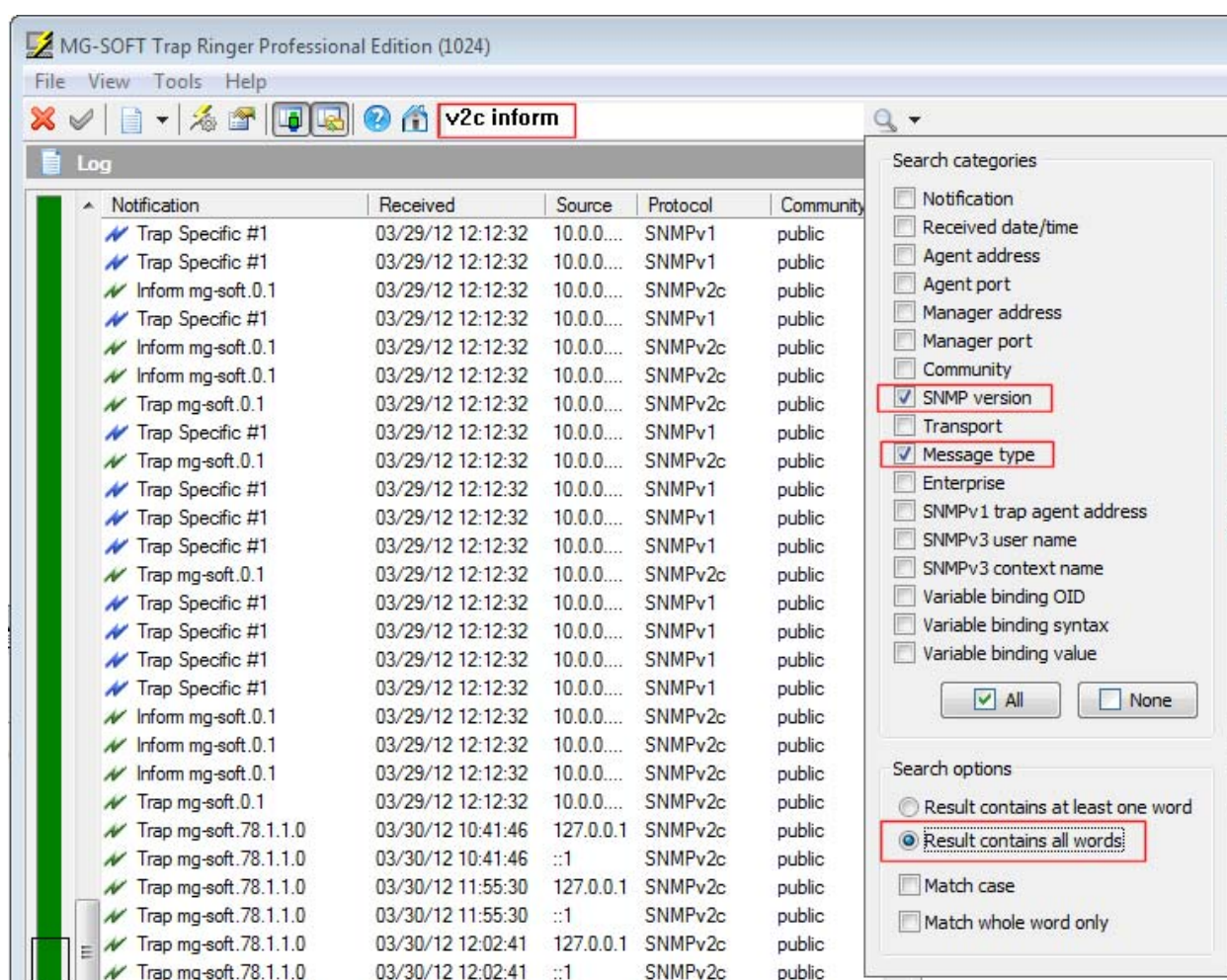



Figure 44: Setting criteria for a specific search operation

4. Into the Search box, enter the **v2c inform** query and click the **Search** button () to start the search operation.
5. When the initial search query finishes, only the *SNMPv2c Inform notification message* are displayed in the main window.
6. To cancel the search operation, press the **ESC** keyboard key.

9 ASSIGNING SEVERITY LEVELS AND COLORS TO SNMP NOTIFICATIONS

Trap Ringer supports assigning severity levels and colors to SNMP Trap and Inform notifications to indicate their importance and to provide a better overview of received SNMP notification messages displayed in Trap Ringer main window. The software comes with pre-configured severities and colors for generic SNMP notifications (e.g., the `coldStart` generic notifications have `Critical` severity level assigned and such notifications are colored red when displayed in the [Trap List window panel](#)). You can modify the severity levels and/or colors assigned to generic SNMP notifications, as well as assign a severity level and color to any other type of SNMP notification by adding and configuring a display filter for it.

The following are the severity level icons and associated colors used for representing different severity levels of SNMP notifications (listed from the most to the least severe):



Figure 45: Severity levels and their default colors

To assign a severity level and display color to SNMP notifications:

1. Select the **Tools / Trap Ringer Preferences** command to open the Trap Ringer Preferences dialog box and switch to the Notification Colors tab.
2. In the tree structure in the left panel of the Notification Colors tab, right-click the severity level (e.g., **Warning**) you want to assign to a particular type of SNMP notification (e.g., mg-soft SNMPv1 specific trap #2) and use the **Add Filter** pop-up command.
3. A new display filter icon is displayed in the left panel of the Notification Colors tab. Optionally; use the **Rename** pop-up command to rename it.
4. Click the filter icon and check the **Enable** checkbox in the right panel displaying filter preferences.
5. Into the **Description** input line enter optional filter description, e.g., "MG-SOFT SNMPv1 specific trap #2 display filter".
6. Click the **Add** button in the Filter frame to add the first filter condition to the filter. The Add Condition dialog box appears.
7. From the **Type** drop-down list select the **SNMPv1 Specific Trap** entry and enter the number **2** into the accompanying drop-down list. Leave the **Negate** checkbox unchecked.
8. Click the **OK** button to add this filter condition to the filter.

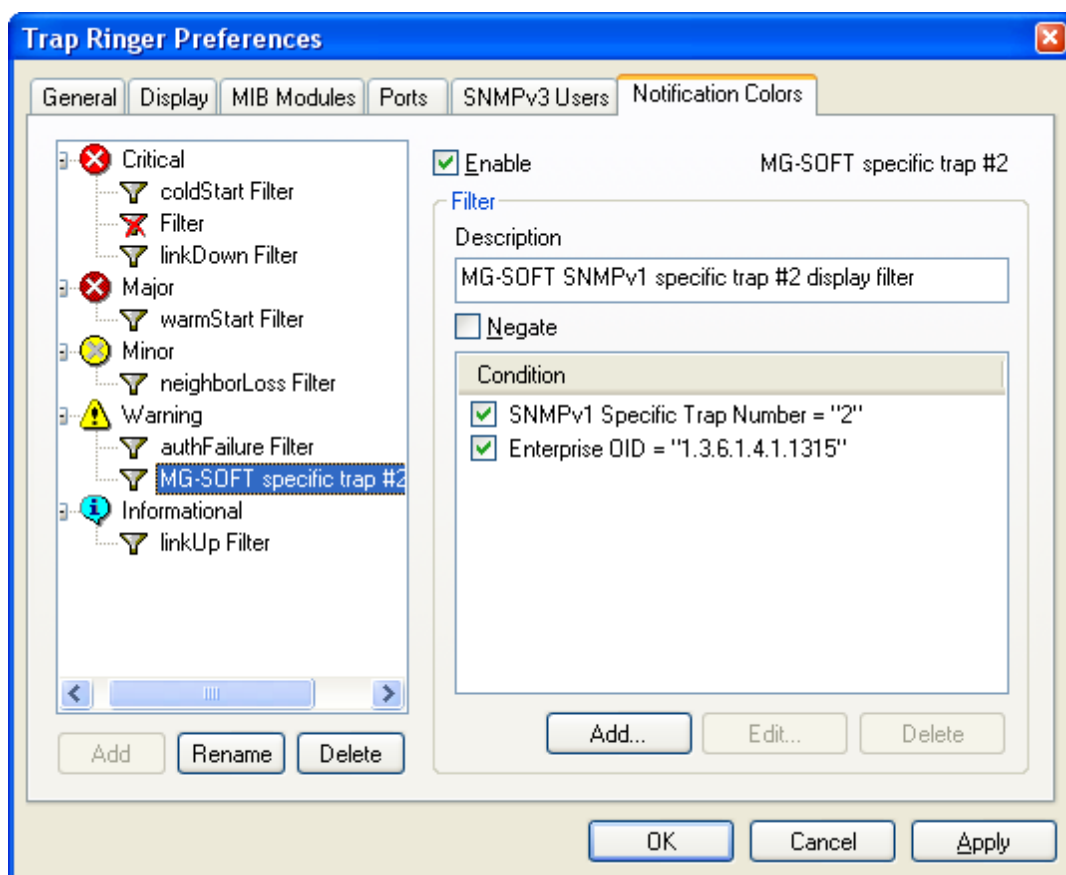


Figure 46: Configuring display filters – assigning severity levels to notifications

9. Click the **Add** button in the Filter frame to add the second filter condition to the filter. The Add Condition dialog box appears.
10. From the **Type** drop-down list select the **Enterprise** entry and enter the OID assigned to MG-SOFT (1.3.6.1.4.1.1315) into the accompanying drop-down list. Alternatively, you can click the **Browse** (...) button next to this input line to select the **mgSoft** node from the MIB tree. Leave the **Negate** checkbox unchecked.

Tip: For more information on configuring filter conditions, see the [Configuring Filter Conditions](#) section.

11. Click the **OK** button to add the second filter condition to the filter. The display filter is now configured (Figure 46).
12. If you want to change the color assigned to all SNMP notifications of the given severity level (e.g. **Warning**), click any severity level node in the tree structure of the Notification Colors tab to view available severity levels and colors assigned to them in the right panel (Figure 47).
13. Click the **Change color** button next to the relevant severity level (e.g. **Warning**), and choose another color from the Color dialog box.
14. Click the **OK** button to close the Color dialog box. The new color is displayed in the color field next to the **Warning** severity level.

15. Click the **Apply** button to apply the new settings. Observe the results of the applied settings in the main window.

Tip 1: Click the **Set default colors** button to apply the default colors to severity levels.

Tip 2: Click the **Disable coloring** checkbox to disable applying severity level colors and icons to SNMP notifications.

Tip 3: Click the **Set default filters** button if you want to restore the default filters and remove all user-defined filters from this dialog.

16. Click the **OK** button to close the Trap Ringer Preferences dialog box.
17. The Trap Ringer main window will display all received SNMPv1 specific traps with trap number “2” and with the Enterprise field value of “mgSoft” (i.e.: 1.3.6.1.4.1.1315) with the assigned severity level icon and color.

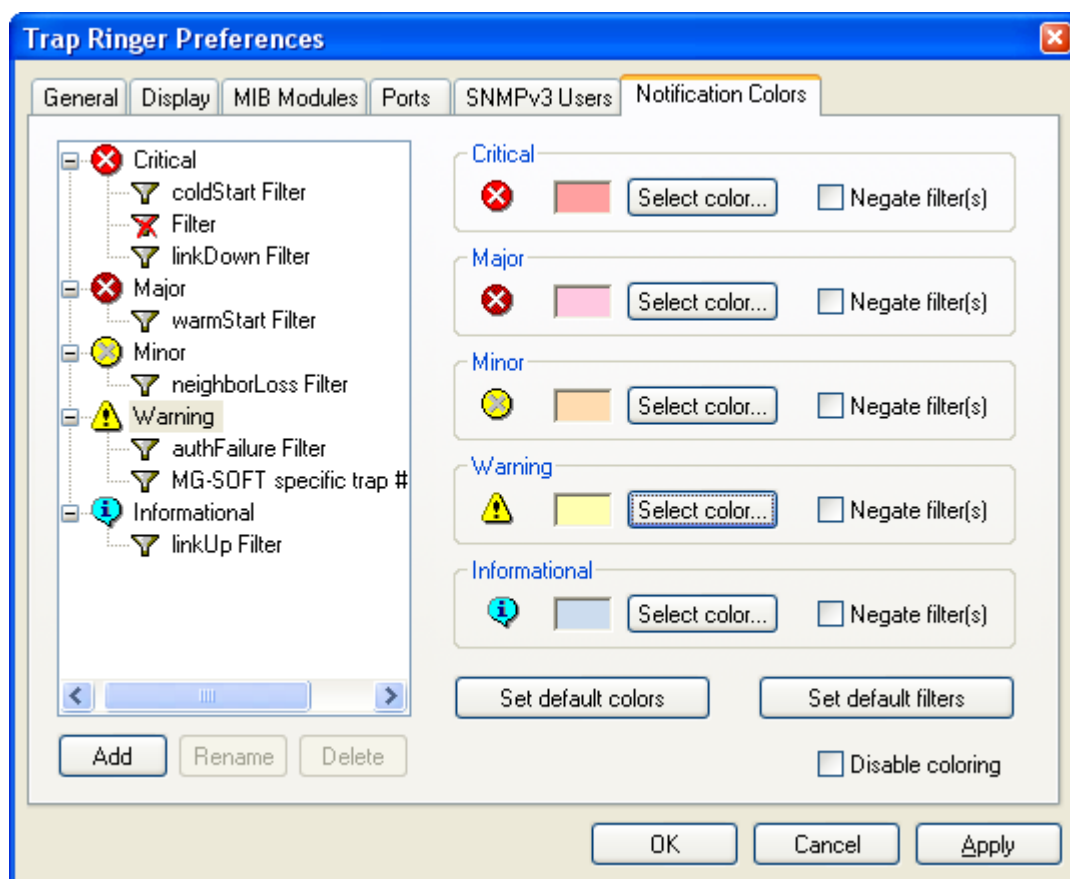


Figure 47: Configuring display filters – assigning colors to severity levels

Note 1: A higher severity level has priority over lower severity levels. For example, if the “coldStart” filter is added to both “Critical” and “Minor” severity levels, the settings of the higher severity level apply (i.e., “coldStart” generic notifications will be displayed with the “Critical” icon and color).

Note 2: The properties of filters and filter conditions that can be configured in the Notification Colors tab of the Trap Ringer Preferences dialog box are the same as those in the **Output Manager Preferences dialog box**. You can save a filter in one of these dialog boxes and then import it to another.

10 EXPORTING RECEIVED SNMP NOTIFICATIONS

Trap Ringer lets you export information about received SNMP Trap and Inform notifications to CSV (comma separated value) text files for the purpose of external viewing or post-processing. You can export received SNMP Trap and Inform notifications either from the Console log file or any other log file displayed in the main window.

To export SNMP notifications to a CSV file:

1. Use the **View / Console** or **View / Log / <LogName>** command to select and display the log file from which you want to export logged SNMP notifications.
2. Select the **File / Export / To CSV File** command. The Export To CSV File dialog box will appear.

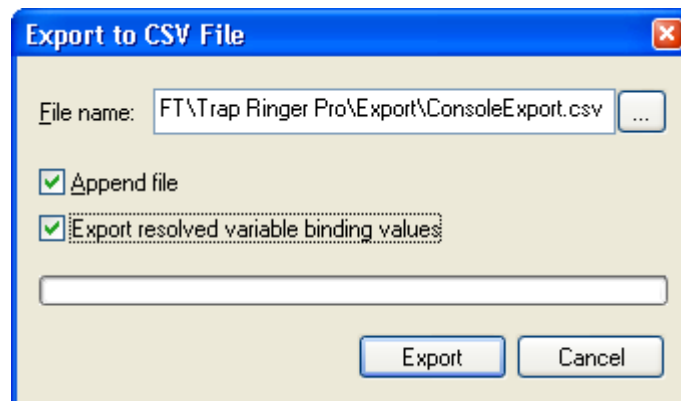


Figure 48: Exporting SNMP notifications to CSV file

3. Into the **File name** input line, specify the full path of the file you wish export SNMP notifications to. By default, Trap Ringer generates exported files to the “Export” subfolder of the Trap Ringer installation folder (e.g., “C:\Program Files\MG-SOFT\Trap Ringer Pro\Export”). To create a CSV file in the default folder, enter only a file name with the .csv extension into this input line (e.g., ConsoleExport.csv). Alternatively, use the **Browse (...)** button next to this input line to browse your computer and specify the desired export folder and file.
4. Check the **Append file** checkbox if you wish to append exported information to an existing file.
5. Click the **Export resolved variable binding values** checkbox if you wish to export the resolved OIDs (i.e., names) and values of variable bindings included in the received SNMP notifications. The OIDs and values (where applicable) can be resolved only if the relevant MIB modules are loaded in Trap Ringer.
6. Click the **Export** button to export information about SNMP notifications currently displayed in the main window into the specified CSV file.

Note: The **Export** command includes all SNMP notification details into the specified CSV file (including variable bindings data).

11 COMPILING AND LOADING MIB FILES

The enclosed MG-SOFT MIB Compiler lets you compile any standard or vendor specific MIB file. A compiled MIB file can then be loaded and utilized by Trap Ringer to identify received SNMP trap and inform notifications by their names, to resolve variable binding's OIDs and certain values to names, to display properties of OIDs in the Trap Details lower window panel, etc.

While the standard MIB files come pre-compiled, MIB files supplied by the vendors of SNMP manageable devices first have to be compiled into a data format that can be utilized by MG-SOFT's products.

11.1 Compiling MIB Files

In this section, you will learn how to compile vendor specific MIB files with the enclosed MIB Compiler, and load compiled MIB files into Trap Ringer.

To compile a MIB file, you have to use the enclosed MG-SOFT MIB Compiler that can be launched from within Trap Ringer client application. MIB Compiler is a program that converts ASN.1 MIB files into binary files, which can then be loaded and utilized by Trap Ringer.

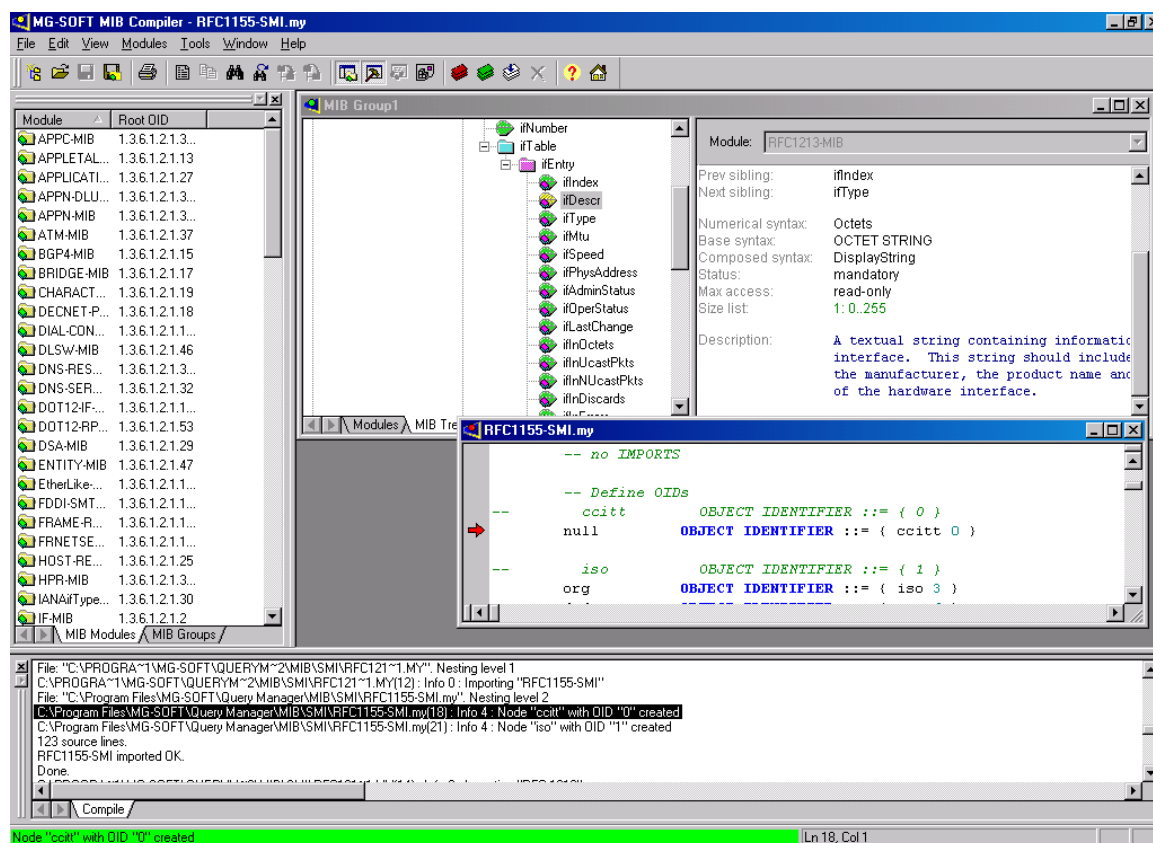


Figure 49: MIB Compiler desktop

To start MG-SOFT MIB Compiler and compile a MIB definition file, do the following:

1. To start MG-SOFT MIB Compiler, click the **MG-SOFT MIB Compiler** toolbar button or the **Tools / MG-SOFT MIB Compiler** command. The MIB Compiler desktop appears (Figure 49).
2. In the MIB Compiler main menu, select the **File / Compile** command or click the **Compile MIB file** toolbar button. The standard Open dialog box appears.
3. Select the MIB definition file that you wish to compile and click the **Open** button. The Open dialog box closes.
4. MIB Compiler compiles the selected file. The compiled MIB module is displayed in the Compiled MIB Modules dialog box.
5. To save the compiled MIB module, select its name from the list of compiled MIB modules and click the **Save** button.
6. The Save As dialog box appears. Specify the file name and save it to the SMIDB file format by clicking the **Save** button.

Tip: For more information on compiling MIB files, consult the MIB Compiler User Manual.

11.2 Loading / Unloading MIB Modules in Trap Ringer

Once you have compiled and saved a MIB file, you can load it in Trap Ringer:

Use the **Tools / Trap Ringer Preferences** command to open the Trap Ringer Preferences dialog box. Switch to the MIB Modules tab (Figure 50).

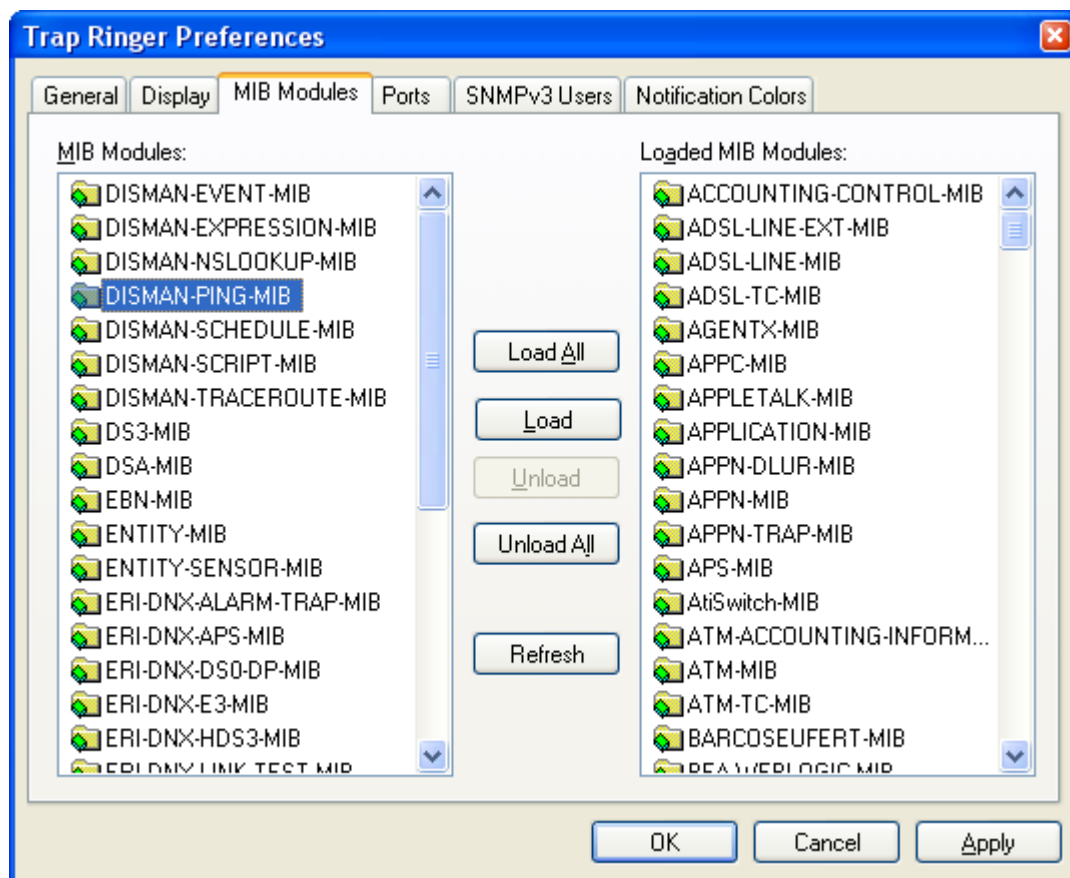


Figure 50: Loading MIB modules

To Load MIB Modules

1. The **MIB Modules** list contains registered MIB modules that are currently not loaded and the **Loaded MIB Modules** list displays all currently loaded MIB modules.
2. To load a MIB module, select a MIB module from the **MIB modules** list and click the **Load** button. The selected MIB module will be removed from the MIB Modules list and added to the Loaded MIB Modules list.
3. To load all registered MIB modules, simply click the **Load All** button. All registered MIB modules will be cleared from the MIB Modules list and added to the **Loaded MIB Modules** list.

Tip: Before loading MIB modules refresh the contents of the Registered MIB Modules list by clicking the **Refresh** button. If any new modules were compiled in the meanwhile, they will appear in the Registered MIB Modules list.

4. Close the Trap Ringer Preferences dialog box by clicking the **OK** button.

To Unload MIB Modules

1. To unload a MIB module, select a MIB module from the **Loaded MIB Modules** list and click the **Unload** button. The selected MIB module will be cleared from the Loaded MIB Modules list and added to the MIB Modules list.
2. To unload all MIB modules, just click the **Unload All** button. All MIB modules will be cleared from the Loaded MIB Modules list and added to the MIB Modules list.

12 INDEX

A

| | |
|---------------------------|----|
| about | |
| filters | 27 |
| MG-SOFT Corporation | 7 |
| monitoring options | 27 |
| output units | 27 |

C

| | |
|---|---|
| coloring SNMP notifications | 80 |
| commands | |
| executing | 37 |
| compiling MIB files | 84 |
| contacting | |
| MG-SOFT Corporation | 7 |
| Create filter wizard | 61 |
| creating filters from notifications | <i>See</i> Create filter wizard |
| CSV file | <i>See</i> Exporting SNMP notifications |

D

| | |
|----------------------------|----|
| desktop | |
| MIB Compiler desktop | 84 |
| Trap Ringer desktop | 16 |

E

| | |
|------------------------------------|----|
| e-mail messages | |
| sending | 40 |
| Event Viewer monitoring | 48 |
| exporting SNMP notifications | 83 |

F

| | |
|--------------------------------------|----------------------------|
| filtering SNMP notifications | |
| adding filters to output units | 64 |
| configuring filter conditions | 66 |
| Create filter wizard | 61 |
| forwarding SNMP notifications | <i>See</i> proxy forwarder |

L

| | |
|--|----|
| loading and unloading MIB modules | 86 |
| logging SNMP notifications to file | 31 |

M

| | |
|-----------------------------|----|
| mail messages | |
| sending | 40 |
| menu bar | 16 |
| MG-SOFT Corporation | |
| about | 7 |
| MIB Compiler | |
| about MIB Compiler | 84 |
| compiling MIB files | 84 |
| starting MIB Compiler | 84 |
| MIB modules | |
| loading MIB modules | 86 |
| unloading MIB modules | 86 |

O

| | |
|---|----|
| Output Manager Preferences dialog box | 27 |
|---|----|

P

| | |
|-----------------------|----|
| proxy forwarder | 56 |
|-----------------------|----|

R

| | |
|----------------------|----|
| reserved words | 38 |
| retransmits | 57 |

S

| | |
|--|------------------------|
| search box | <i>See</i> search tool |
| search tool | 73 |
| searching for SNMP notifications | 73 |
| cancel search | 79 |
| search categories | 74 |
| search options | 76 |
| search queries | 77 |
| sending | |
| e-mail messages | 40 |
| SMS messages | 45 |
| syslog messages | 51 |
| severity level | 80 |
| SMS messages | |
| sending | 45 |
| SNMP notifications | |
| assigning severity levels and colors | 80 |
| auditing with Event Viewer | 48 |
| console monitoring | 29 |
| e-mail monitoring | 40 |

| | | | |
|--|---|--|---|
| filtering – adding filters to output units | 64 | syslog monitoring | 51 |
| filtering – configuring filter conditions | 66 | System requirements | |
| filtering – example | 70 | Linux version of Trap Ringer | 10 |
| filtering – in general | 60 | Mac OS X version of Trap Ringer | 11 |
| forwarding notifications | 56 | Solaris version of Trap Ringer | 11 |
| logging to file – auto new file logging | 34 | Windows version of Trap Ringer | 10 |
| logging to file – continuous (ring file) logging | 31 | | |
| logging to file – daily logging | 33 | T | |
| logging to Linux system log files | 51 | text search | <i>See</i> searching for SNMP notifications |
| proxy forwarder | 56 | timeout | 57 |
| running commands | 37 | toolbar | 16 |
| searching for | <i>See</i> searching for SNMP notifications | translating SNMP notifications | <i>See</i> proxy forwarder |
| SMS monitoring | 45 | Trap Ringer client | |
| translating notifications | 56 | desktop | 16 |
| Web monitoring | 53 | status bar | 17 |
| SNMPv3 | | thumbnail scrollbar | 17 |
| authentication protocol | 25 | Trap Details window panel | 18 |
| context engine ID | 24 | Trap List window panel | 17 |
| context name | 24 | working area | 16 |
| privacy protocol | 25 | Trap Ringer Preferences dialog box | 23, 80 |
| profile | 24 | | |
| user name | 24 | | |
| users | 23 | | |