Pro EMS

Element Management System for ZyXEL Enterprise Ethernet Switches and Wireless Access Points

User's Guide

Default Login Details

User Name	Administrator
Password	

Software Version 1.0
Edition 2, 8/2009

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the Pro EMS using the web configurator.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get your Pro EMS up and running right away. It contains information on setting up your network and configuring for Internet access.

- Support Disc

  Refer to the included CD for support documents.

- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.

- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your Pro EMS.

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

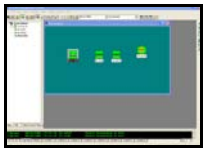
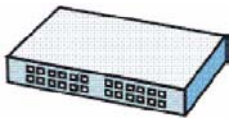
- The Pro EMS may be referred to as the "Pro EMS", the "server", the "system" or the "product" in this User's Guide.
- The ZyXEL Enterprise Ethernet Switches or Wireless Access Points may be referred to as the "managed device", the "device" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide use the following generic icons. The Pro EMS icon is not an exact representation of your Pro EMS.

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Table 1 Common Icons

Pro EMS 	Computer 	Notebook 
Server 	Internet Cloud 	Switch 
Router 	ZyXEL Enterprise Access Point 	ZyXEL Enterprise Ethernet Switch 

Contents Overview

Introduction 13

Introducing the Pro EMS 15

Pro EMS Manager and Troubleshooting 37

Tools 39

Troubleshooting 107

Appendices and Index 111

Table of Contents

About This User's Guide 3

Document Conventions 5

Contents Overview 7

Table of Contents 9

Part I: Introduction 13

Chapter 1
Introducing the Pro EMS 15

1.1 NMS Overview 15
1.1.1 Pro EMS 15
1.1.2 What You Need To Know 16
1.1.3 List of Devices the Pro EMS Can Manage 17
1.1.4 Pro EMS Hardware and Software Requirements 17
1.2 Installation 17
1.2.1 Procedure to Install NMS 17
1.2.2 Procedure to Install Pro EMS 21
1.3 Using NMS 23
1.3.1 Logging In 24
1.3.2 NMS Screen Overview 26
1.3.3 Device Discovery 27
1.3.4 Compiling MIBs 29
1.3.5 Viewing the Subnet Map 30
1.3.6 Disabling Automatic Startup 30
1.4 Pro EMS Menus 31
1.5 Uninstalling 33
1.5.1 Uninstall Pro EMS 34
1.5.2 Uninstall NMS 35

Part II: Pro EMS Manager and Troubleshooting 37

Chapter 2
Tools 39

2.1 Overview 39
2.2 What You Can Do in the Tools screens 39
2.3 The **Account Management** Screen 40
2.4 The **Configuration File Management** Screen 42
2.4.1 The Options Screen 43
2.4.2 The **Configure File Restore** Screen 44
2.4.3 The **Configure File Backup** Screen 47
2.4.4 The **Configure File Edit** Screen 49
2.5 The **Ethernet Status** Screen 52
2.6 The **Event Log** Screen 55
2.7 The **Firmware Upgrade** Screen 56
2.8 The **Group Management** Screen 58
2.8.1 Creating an **SNMPc Group** **60**
2.8.2 Associating a Device **with an SNMPc Group** **60**
2.8.3 **Example -** Adding a Device **from One Group to Another** **62**
2.9 The **Hardware Status** Screen 65
2.10 The **MAC Table** Screen 67
2.11 The **Port Status** Screen 69
2.12 The **RMON Configuration** Screen 71
2.12.1 The **History Config** Screen 73
2.12.2 RMON History Configuration Screens 74
2.12.3 The **Event Config** Screen 75
2.12.4 RMON Event Configuration Screens 77
2.12.5 The **Alarm Config** Screen 78
2.12.6 RMON Alarm Screens 80
2.12.7 RMON Alarm Event Log Screen 82
2.13 The **RMON Ethernet History Data** Screen 83
2.14 The **RMON Ethernet Statistics** Screen 85
2.15 The **Schedule Management** Screen 88
2.15.1 The **Schedule** Screen 90
2.15.2 The **History** Screen 96
2.16 The **Script Distribution** screen 97
2.17 The **System Information** Screen 100
2.18 The **System Management** Screen 101
2.19 The **VLAN Status** Screen 103

Chapter 3
Troubleshooting 107

3.1 Overview 107
3.2 Pro EMS Installation 107
3.3 Pro EMS Access and Login 108
3.4 Device Management 110

Part III: Appendices and Index 111

Appendix A SNMPc Network Manager 113

Appendix B Legal Information 119

Index 121

PART I
Introduction

Introducing the Pro EMS (15)

1

Introducing the Pro EMS

1.1 NMS Overview

A Network Management System (NMS), such as Castlerock's SNMPc network manager, is used to manage communication between network elements (NE). A network element is a device such as an Ethernet switch, wireless router, printer and so on, in a network that can be managed by the NMS. An Element Management System (EMS), such as the Pro EMS, is part of an NMS and is used to manage NEs of a specific type. Use the Pro EMS to manage ZyXEL Enterprise Ethernet switches and Enterprise access points.

1.1.1 Pro EMS

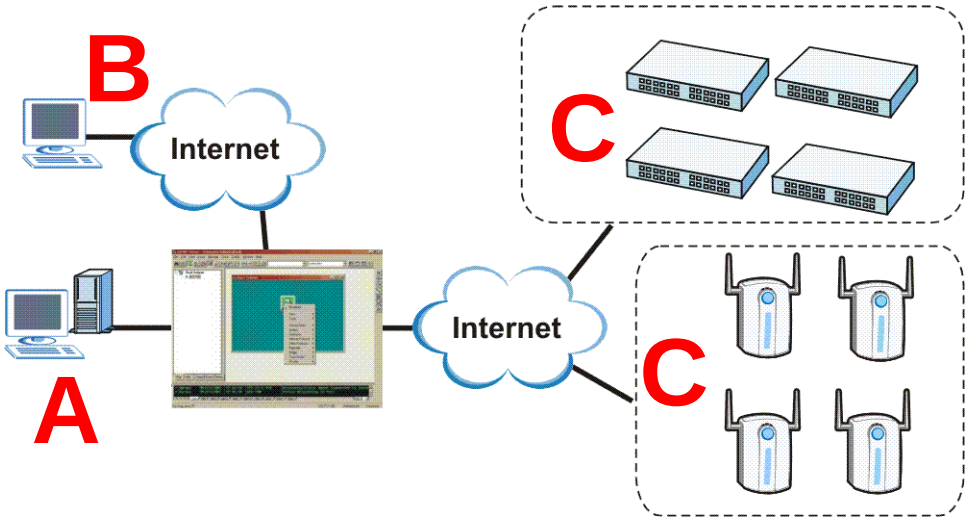
Pro EMS works with two types of NMS: Enterprise and Workgroup.

- With Enterprise, Pro EMS allows up to 20 network administrators to monitor and manage up to 25000 ZyXEL Enterprise Ethernet switches and Enterprise access points.
- With Workgroup, Pro EMS allows one administrator to monitor and manage up to 1000 ZyXEL Enterprise Ethernet switches and Enterprise access points.

The edition you install depends on the license you bought.

You can install an NMS console on a computer different to the one on which you installed the NMS server. In the example below, the server runs on server **A**, and uses SNMPc to communicate with the ZyXEL Enterprise Ethernet switches and Enterprise access points **C using** SNMP v1, SNMP v2 or SNMP v3. The console is installed on computer **B** and interacts with the server to manage devices.

Figure 1 NMS & EMS Overview



1.1.2 What You Need To Know

These are some terms that you need to know about SNMP-managed networks. In addition to NMS, EMS and NE an SNMP-managed network may consist of agents, polling agents, management consoles and a server.

- Simple Network Management Protocol (SNMP) is a TCP/IP protocol used for exchanging management information between network devices.
- An agent is a management software module that resides in a network element. An agent translates the local management information from the NE into a form compatible with SNMP.
- A polling agent helps collect management information from network elements.
- The server is the computer on which you install NMS and EMS server software. It executes applications that control and monitor network elements.
- Management consoles are computers on which you install NMS and EMS client software that allow other administrators to also control and monitor network elements in conjunction with the server.
- A Management Information Base (MIB) is a collection of variables that define each piece of information to be collected about an NE. Examples of variables include number of packets received, port status, device shutdown, device restart and so on.
- A trap is an SNMP message sent from an NE to the NMS.
- Community is the password used to encrypt messages between the NE and NMS.

1.1.3 List of Devices the Pro EMS Can Manage

This is the list of devices supported at the time of writing.

- NWA-3000 series
- ES-2000 series
- ES-3000 series
- GS-2000 series
- GS-4000 series
- XGS-4500 series

1.1.4 Pro EMS Hardware and Software Requirements

The following table lists the recommended minimum hardware and software you need in order to run Pro EMS.

Table 2 Minimum Pro EMS System Requirements

HARDWARE	SOFTWARE
• CPU: Intel Pentium(R) 4, 1.6 GHz • 1 GB RAM • 60 GB Hard Disk free space • 1024 by 768 Graphics Adapter • 10/100/1000 Mbps Ethernet Adaptor	• Win2003 server, Windows XP Professional • Castle Rock's SNMPc Network Manager 7.0.14a Enterprise or WorkGroup Edition

1.2 Installation

First install Castlerock's NMS software if you do not already have it installed. You then install the Pro EMS software that allows you to manage ZyXEL Enterprise Ethernet switches and Enterprise access points.

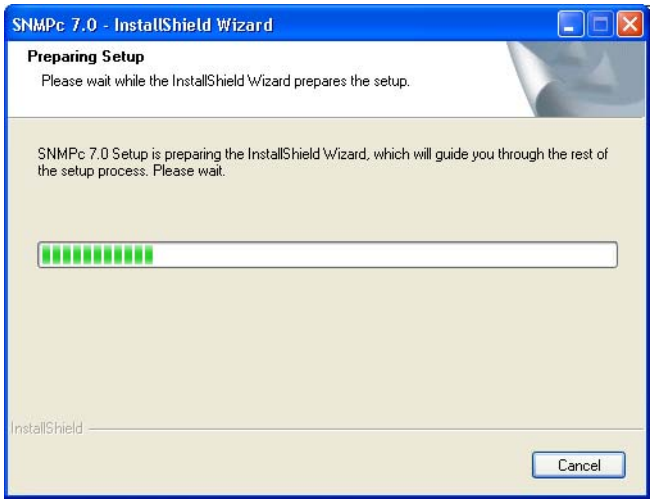
It is recommended you close all other applications on your computer before installing this software.

In the wizards, click **Next** to continue, **Back** to return to a previous screen and **Cancel** to exit the wizard without saving changes.

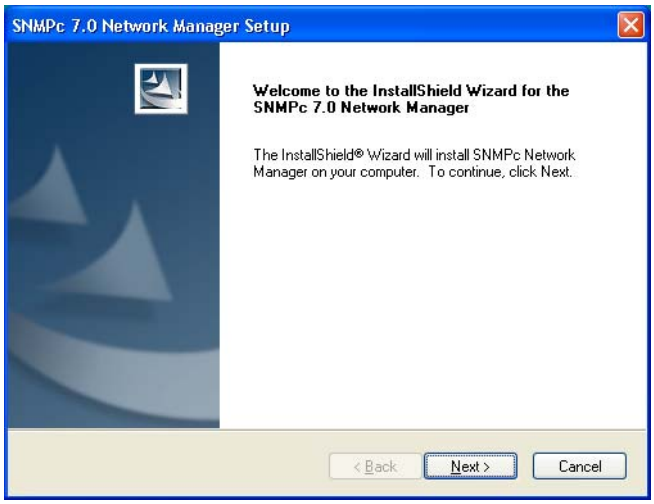
1.2.1 Procedure to Install NMS

You need to log on to Windows with Administrator permission.

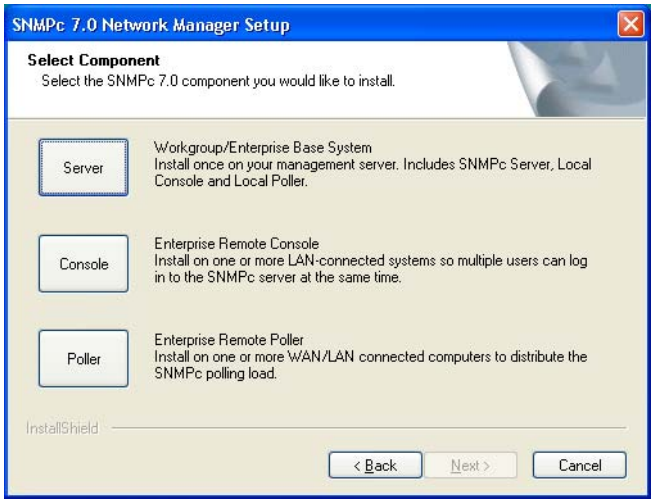
1 Castlerock's NMS software is on the Pro EMS disc or you can download it from www.castlerock.com. Double-click the installation program to run it.



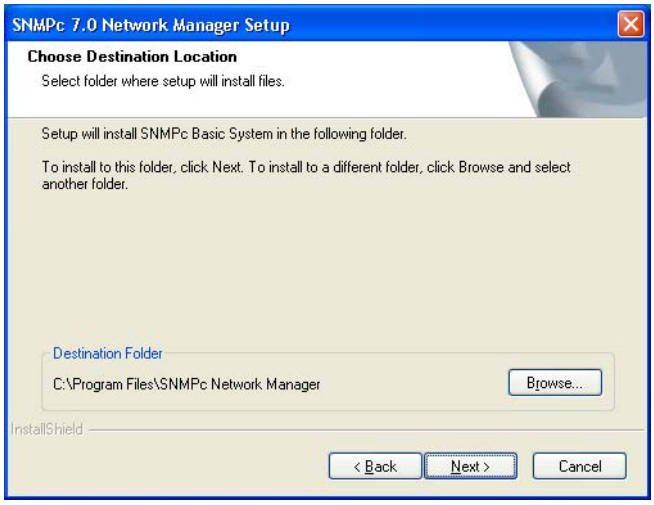
2 The **Welcome** screen appears after the files extract. Click **Next** to begin the installation wizard.



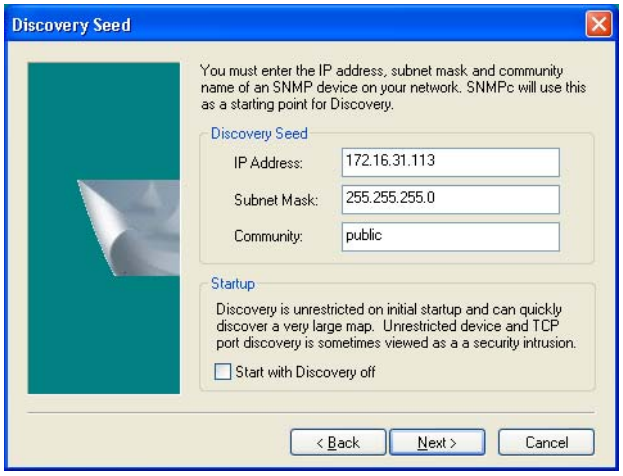
3 Select **Server** and click **Next**. **Server** includes the local console and polling agent. If you already installed **Server** on another computer in your managed network and you now want to set up another NMS management console, then select **Console** and click **Next**.



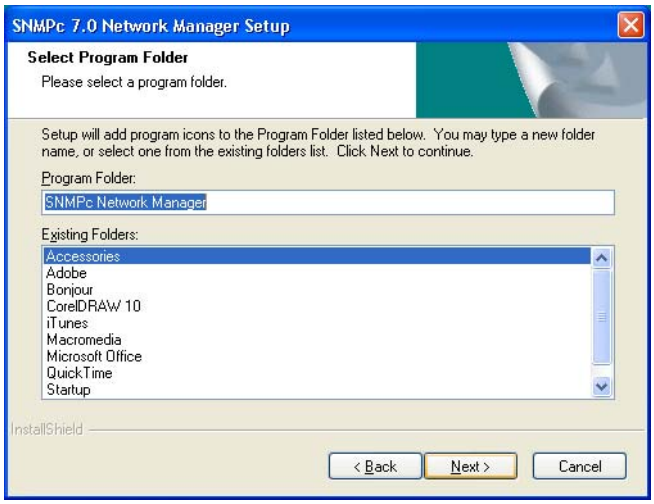
4 If you want to change the default installation folder, click **Browse**, navigate to a new folder, then click **Next**. If the default installation folder is OK, just click **Next** in this screen.



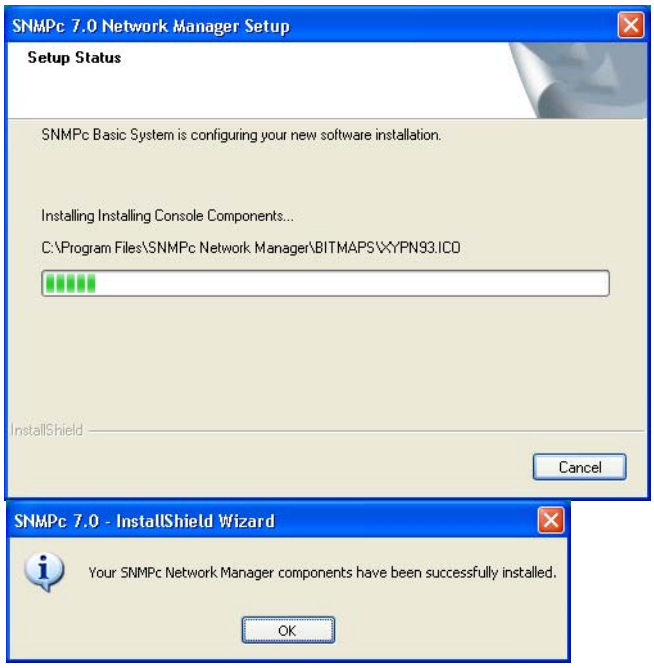
5 Type the IP address and subnet mask of an SNMP device that will be the starting point for device and port discovery. If you change the default **Community** password (public), make sure you make the same change on the managed devices. If this is not entered correctly, network discovery will not work.



6 Click **Next** to accept the default program name or type a new one.

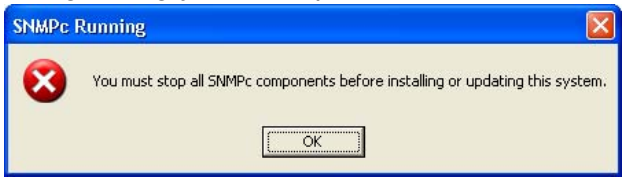


7 Wait while the program installs. You are notified when it finishes installation. Click **OK**.

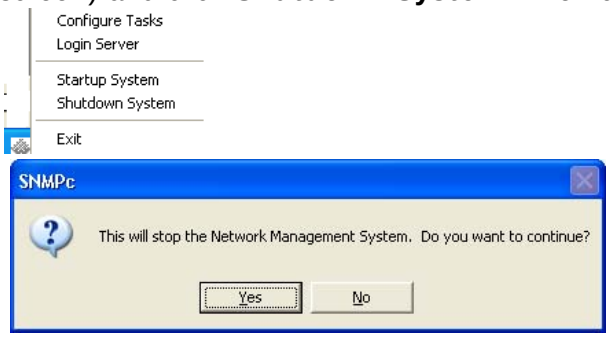


1.2.2 Procedure to Install Pro EMS

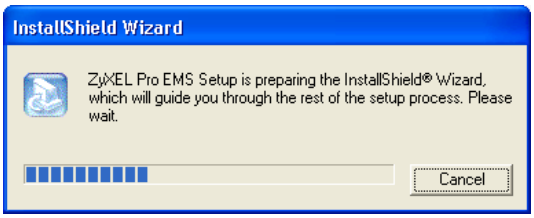
Do not run any NMS components yet. If they are running, you will see the next dialog telling you to stop them.



To stop them, right-click the NMS agent in the system tray (bottom right of your screen) and click **Shutdown System**. Then click **Yes** to confirm.

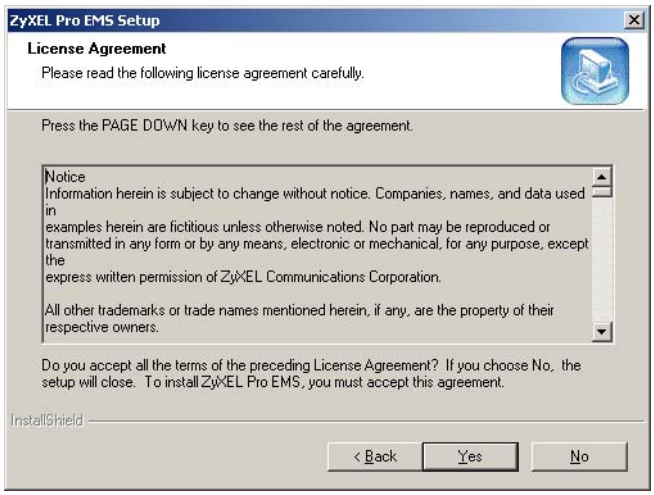


1 Find the Pro EMS executable file on the disc. Double-click it to run it.

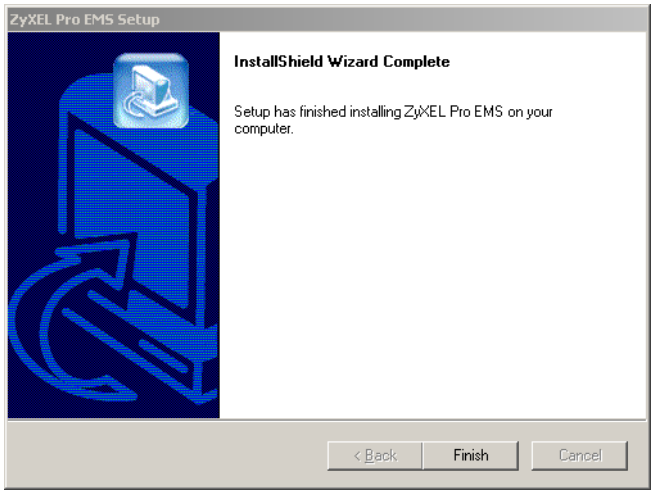


2 The **Welcome** screen appears after the files extract. Click **Next** to begin the installation wizard

3 Read the license agreement and then click **Yes** to continue the wizard.



4 Click **Finish** to complete the wizard.



5 You must restart your computer to complete the installation. After your computer restarts, NMS server will automatically start.

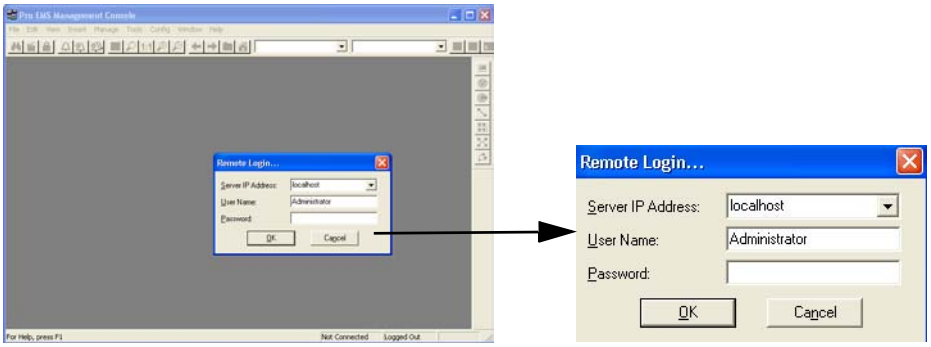
1.3 Using NMS

When your computer starts, NMS server will automatically start.

1.3.1 Logging In

A login screen displays. The default user name is **Administrator** and associated password is blank. Click **OK** to proceed.

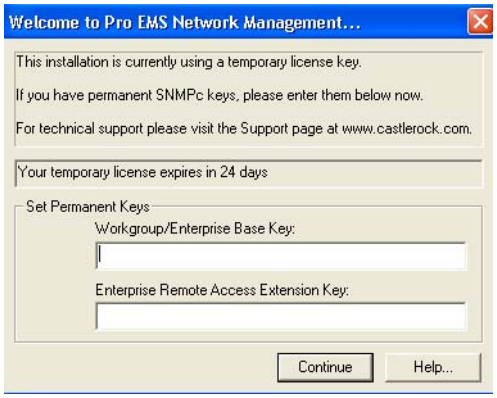
Figure 2 Logging In



6 If you're using the trial version of NMS, just click **Continue** in this screen. Otherwise, type the permanent key(s) found in the Pro EMS package and then click **Continue**.

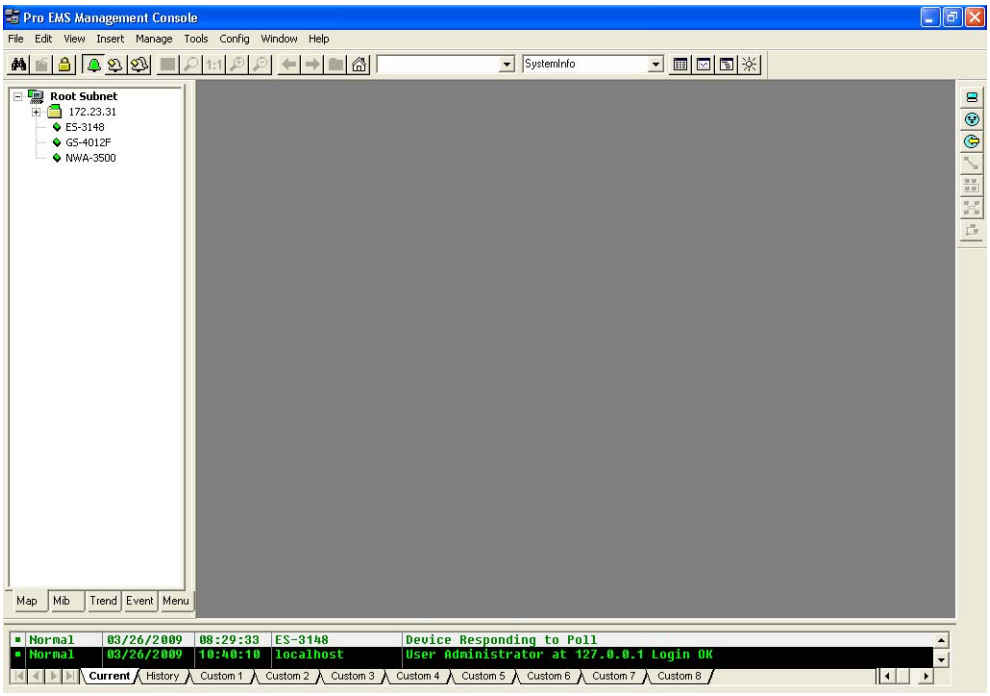
- With an Enterprise license, Pro EMS allows up to 20 network administrators to monitor and manage up to 500 ZyXEL Enterprise Ethernet switches and Enterprise access points.
- With a Workgroup license, Pro EMS allows one administrator to monitor and manage up to 150 ZyXEL Enterprise Ethernet switches and Enterprise access points.

Figure 3 NMS Keys



7 The **Pro EMS Management Console** displays after a successful login.

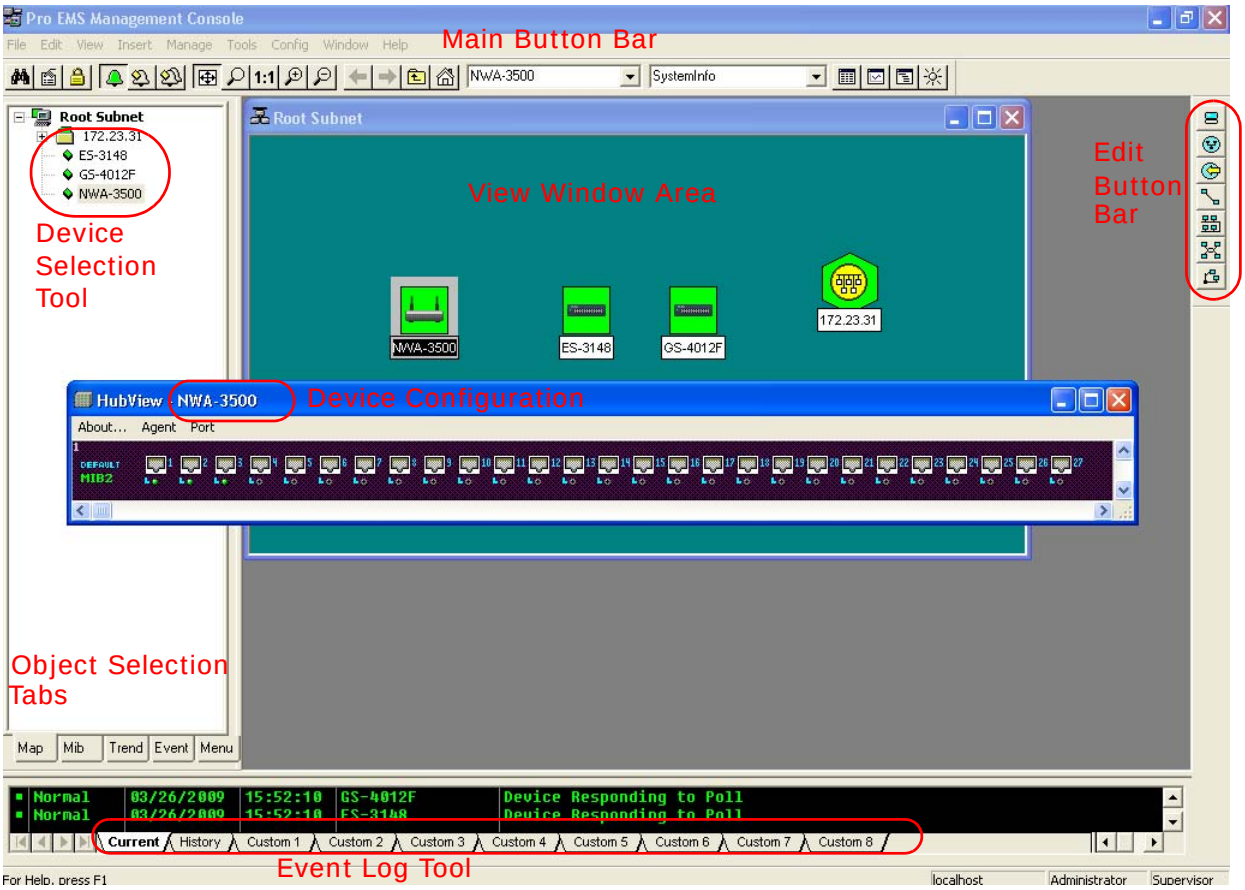
Figure 4 Management Console



1.3.2 NMS Screen Overview

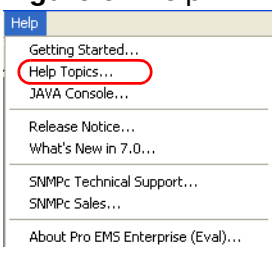
These are the major components of the main screen.

Figure 5 Major Components of NMS Management Console



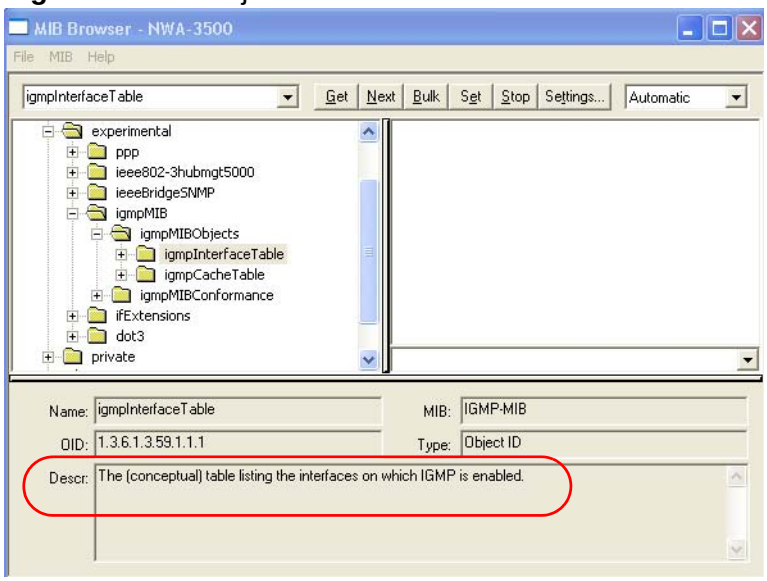
For more information on this screen and other NMS screens click **Help > Help Topics**.

Figure 6 Help



If you need help on a specific MIB (Management Information Base) object click **Tools > Mib Browser**, drill down to the desired MIB object and select it. Its description appears as shown.

Figure 7 MIB Object Details



1.3.3 Device Discovery

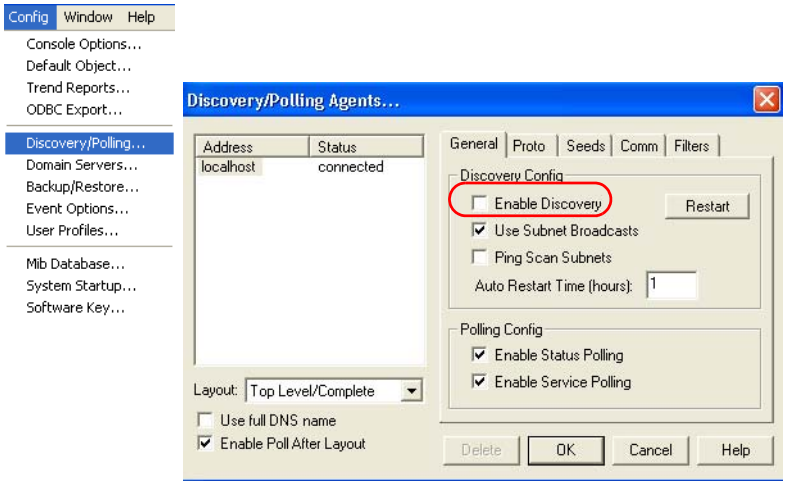
Devices can be discovered automatically or manually.

1.3.3.1 Automatic

Automatic discovery is enable by default. All devices automatically discovered are added to the top level of the discovery map. After a first discovery you could rearrange the map layout to reflect your network topology. Then, you may want to disable auto-discovery as further devices found will be automatically added to the top level of your map. To disable auto-discovery, click **Config > Discovery / Polling** and deselect **Enable Discovery**. After you do this, you will have to manually add new devices to your network; see Section 1.3.3.2 on page 28.

See the NMS help for information on other alternatives should you still want to know when new devices are added to your network, but you don't want them automatically added to the top of the map.

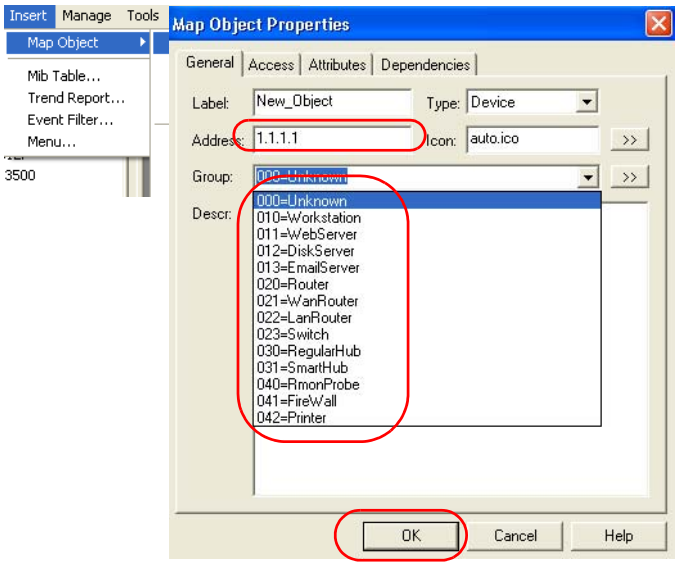
Figure 8 Disable Automatic Discovery



1.3.3.2 Manual

To manually add a device to your network, you must know what type of device it is and its IP address. Click **Insert > Map Object > Device**, configure the screen and click **OK**. For more information on this screen and other NMS screens click **Help > Help Topics**.

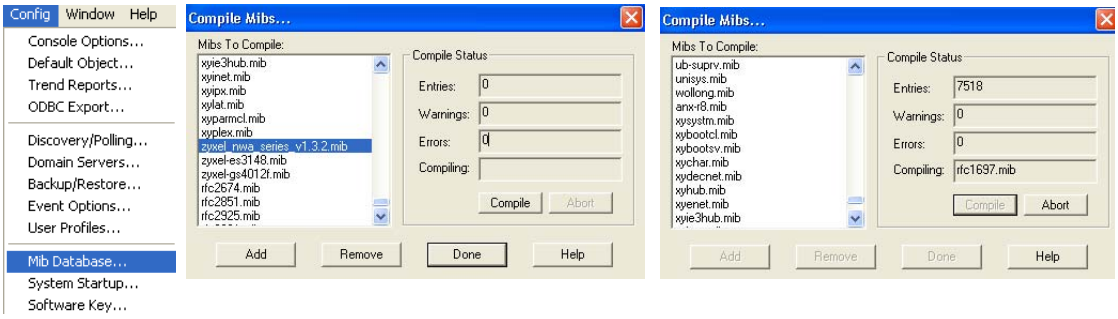
Figure 9 Manually Add a Device



1.3.4 Compiling MIBs

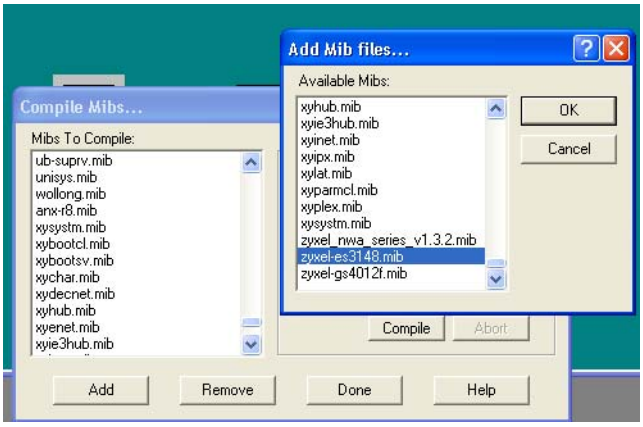
After a new type device is added to a network, you may need to add and compile its MIB (Management Information Base). Click **Config > Mib Database**, scroll down until you find the Mib for your device, then click **Compile**.

Figure 10 Compile MIBs



If you cannot find the MIB for your device, click **Add**, choose the MIB from the **Add Mib files** dialog box, click **OK** to return to the **Compile Mibs** screen, and then click **Compile**. If you cannot find the device MIB in the **Add Mib** files dialog, you will need to manually add it to C:\Program Files\SNMPc Network Manager\mibfiles (the default NMS installation path) and restart NMS.

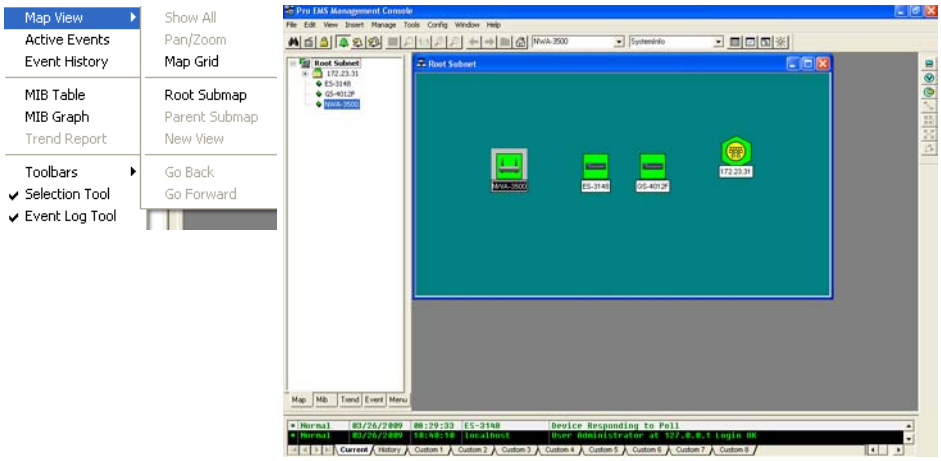
Figure 11 Add MIB File



1.3.5 Viewing the Subnet Map

To view the map of devices added to your network, click **View > Map View > Root Submap**.

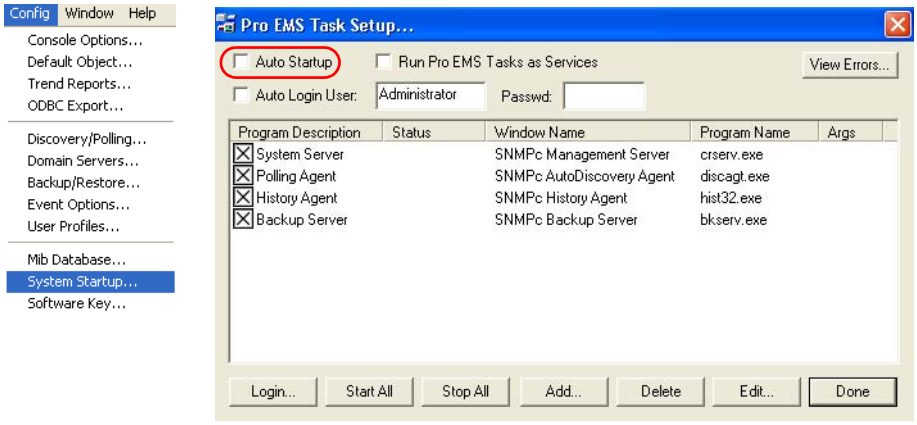
Figure 12 View Subnet Map



1.3.6 Disabling Automatic Startup

If you do not want NMS to start when you turn on your Windows computer, you must turn off automatic start-up. Click **Config > System Startup** and deselect **Auto Startup**.

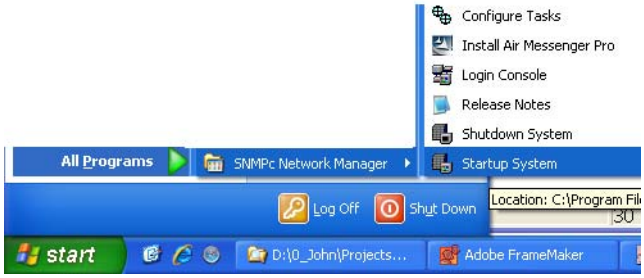
Figure 13 Disable Automatic Startup



To manually start NMS (in Windows XP), click **start > All Programs > SNMPc Network Manager > Startup System**. To log in, click **start > All Programs > SNMPc Network Manager > Login Console**. **Air Messenger Pro** is software

that allows the NMS to page you when an event occurs. It is not installed by default.

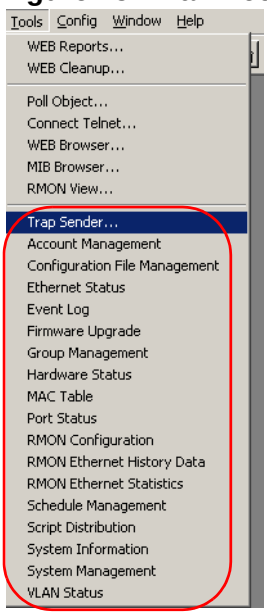
Figure 14 Manual Startup



1.4 Pro EMS Menus

This manual will focus on describing the following Pro EMS **Tools** menus. Information in the other menus can be found in the NMS help. To access these menus, select a managed ZyXEL device, then click the **Tools** menus.

Figure 15 Main Tools Menus



You may also view these menus by right-clicking on a managed ZyXEL device.

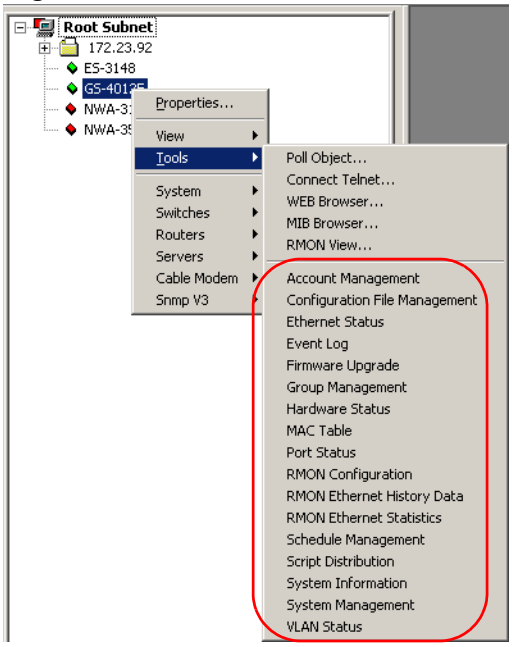
Table 3 Tools Menus

MENU	DESCRIPTION
WEB Reports	Use this screen to view Trend Micro reports
WEB Cleanup...	Use this screen to delete Trend Micro reports
Poll Object...	Use this screen to get SNMP traps from the selected device
Connect Telnet...	Use this screen to connect to the selected device using Telnet. You can configure the device using the command line interface via Telnet.
WEB Browser...	Use this screen to connect to the selected device using your web browser. Do this if you want to configure the device using its web configurator.
MIB Browser...	Use this screen to view detailed information on Mib objects.
RMON View...	Use this screen to view remote monitoring (RMON) statistics.
Trap Sender...	Use this screen to manually send traps to the selected device.
Account Management	Use this screen to change the default account user name and password for the selected device. Firmware and configuration files can be uploaded to or downloaded from the device using these settings.
Configuration File Management	Use this screen to back up, restore and edit the configuration file on the selected device.
Ethernet Status	Use this screen to view Ethernet statistics for the selected device.
Event Log	Use this screen to view historical and current logs for the selected device.
Firmware Upgrade	Use this screen to upload firmware to the selected device. Make sure you select the correct firmware for the device.
Group Management	Use this screen to group managed devices that have similiar configurations. You may distribute a script to a group of devices, for example.
Hardware Status	Use this screen to view temperature, fan and voltage information for the selected device.
MAC Table	Use this screen to view the MAC address table by MAC address, VLAN ID or port.
Port Status	Use this screen to view port statistics for the selected device.
RMON Configuration	Use this screen to configure remote network monitoring (RMON) on the selected device.
RMON Ethernet History Data	Use this screen to view historical remote networkmonitoring (RMON) Ethernet statistics for the selected device.
RMON Ethernet Statistics	Use this screen to view remote network monitoring (RMON) Ethernet statistics for the selected device.
Schedule Management	Use this screen to create schedules for backing up or restoring a configuration file on the selected device, upgrading firmware or resetting the selected device.
Script Distribution	Use this screen to send commands to one or multiple devices. First configure groups in the **Group Management** screen.

Table 3 Tools Menus (continued)

MENU	DESCRIPTION
System Information	Use this screen to view the status, device name, IP address and group of each managed device. Select a device in the screen to view more detailed information, such as system name, firmware version, serial number and hardware version.
System Management	Use this screen to save device configuration files, reload factory defaults or reboot the device.
VLAN Status	Use this screen to view VLAN settings for the selected device.

Figure 16 Shortcut to Tools Menus



See later chapters in this manual for more detailed information on these screens.

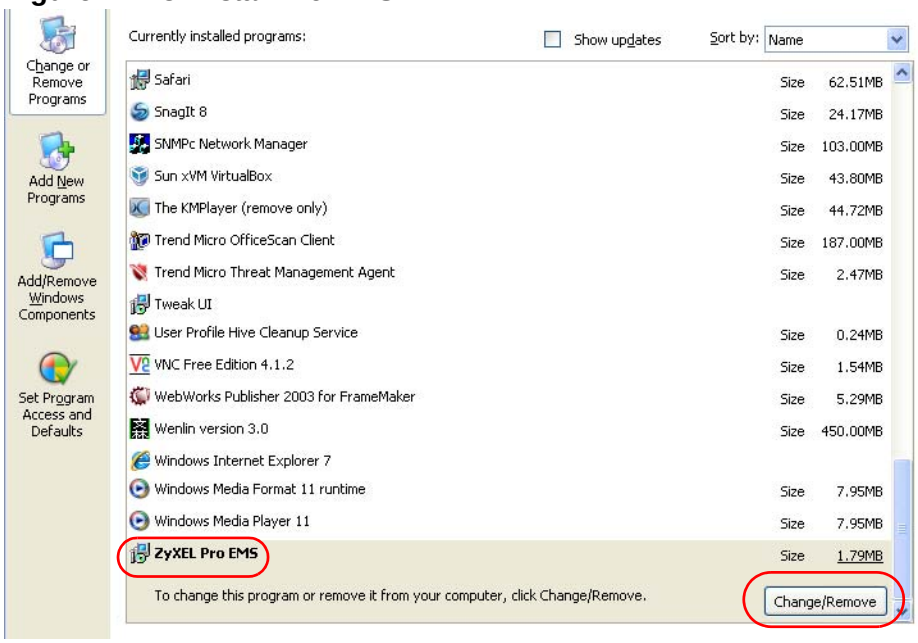
1.5 Uninstalling

This section shows you how to uninstall Pro EMS and NMS.

1.5.1 Uninstall Pro EMS

If you want to uninstall the Pro EMS, use the **Change/Remove Programs** function in the Windows **Control Panel**, and follow the directions on the screen.

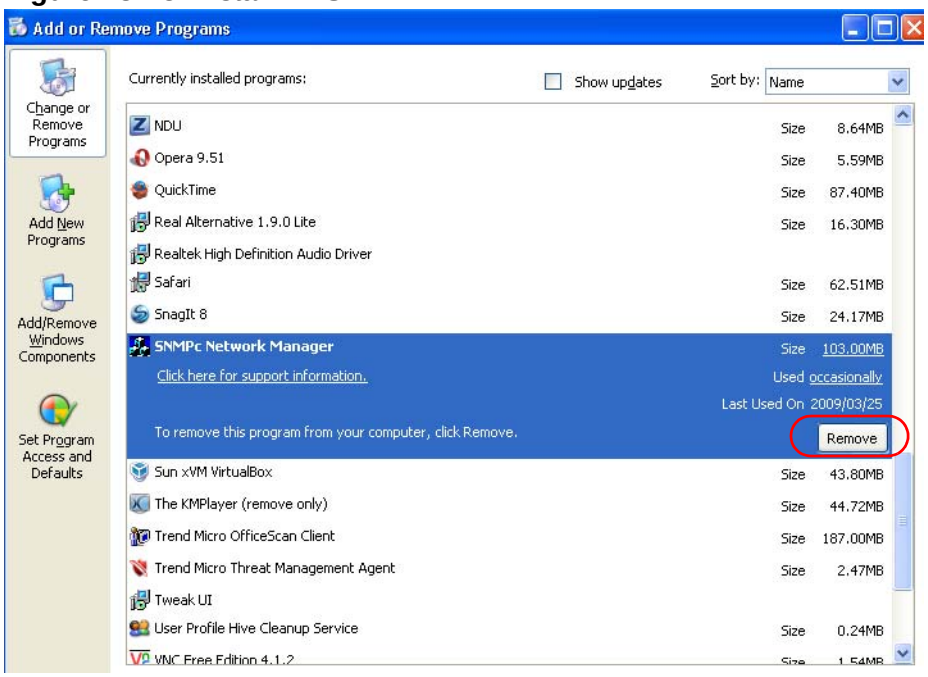
Figure 17 Uninstall Pro EMS



1.5.2 Uninstall NMS

If you want to uninstall the NMS, use the **Change/Remove Programs** function in the Windows **Control Panel**, and follow the directions on the screen.

Figure 18 Uninstall NMS



PART II
Pro EMS Manager and Troubleshooting

Tools (39)

Troubleshooting (107)

2

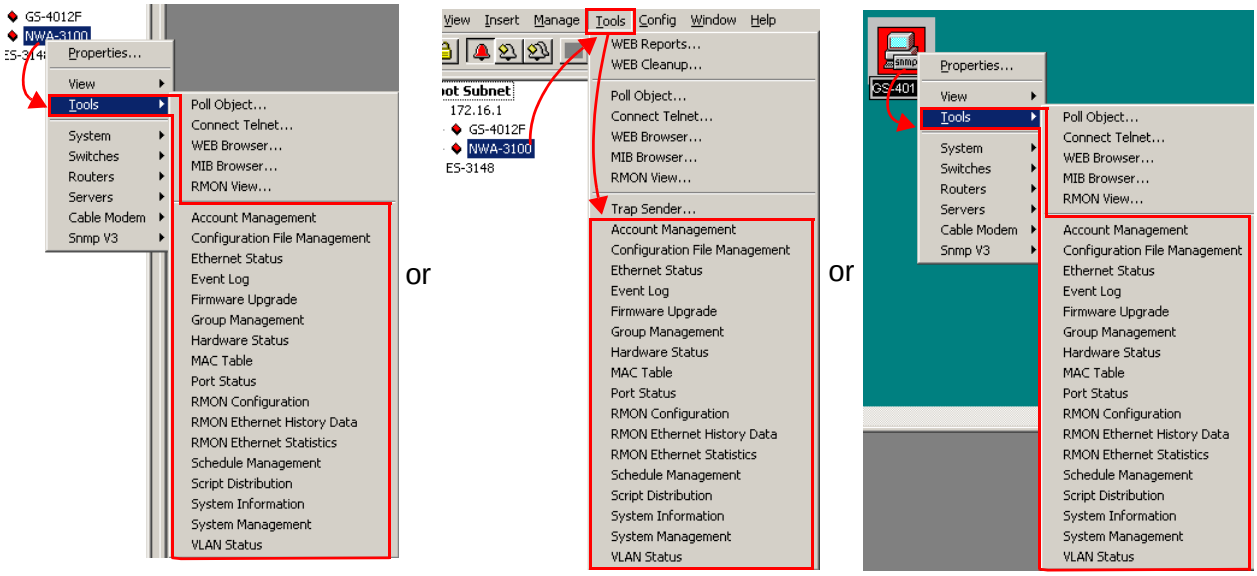
Tools

2.1 Overview

Pro EMS allows you to view or configure managed devices' settings and status through the submenus (from **Account Management** to **VLAN Status**) under the **Tools** menu. There are three ways to access these submenus:

- Right-click on a device in the Selection Tool panel and then select **Tools**.
- Select a device in the Selection Tool panel and then click **Tools** in the main menu bar.
- Right-click on a device in the View Window Area and then select **Tools**.

Figure 19 Three ways to Access the Tools Menu



2.2 What You Can Do in the Tools screens

- Use the **Account Management** screen (see Section 2.3 on page 40) to change the FTP account and/or password for managed device(s).
- Use the **Configuration File Management** screen (see Section 2.4 on page 42) to manage the configuration file for managed device(s).

- Use the **Ethernet Status** screen (see Section 2.5 on page 52) to view the status of Ethernet interfaces.
- Use the **Event Log** screen (see Section 2.6 on page 55) to view the logs of events generated on managed device(s).
- Use the **Firmware Upgrade** screen (see Section 2.7 on page 56) to upgrade firmware for managed device(s).
- Use the **Group Management** screen (see Section 2.8 on page 58) to logically group managed devices that can be configured together.
- Use the **Hardware Status** screen (see Section 2.9 on page 65) to view the status of hardware such as voltage, fan and temperature.
- Use the **MAC Table** screen (see Section 2.11 on page 69) to view the MAC table on managed device(s).
- Use the **Port Status** screen (see Section 2.11 on page 69) to view the status of ports on managed device(s).
- Use the **RMON Configuration** screen (see Section 2.12 on page 71) to configure RMON settings.
- Use the **RMON Ethernet History Data** screen (see Section 2.13 on page 83) to view historic RMON statistics on Ethernet interfaces.
- Use the **RMON Ethernet Statistics** screen (see Section 2.14 on page 85) to view RMON statistics on Ethernet interfaces.
- Use the **Schedule Management** screen (see Section 2.15 on page 88) to manage scheduled tasks such as firmware upgrade and configuration file backup and restore.
- Use the **Script Distribution** screen (see Section 2.16 on page 97) to execute a customized script containing one or multiple commands for device or group configuration.
- Use the **System Information** screen (see Section 2.17 on page 100) to view system information.
- Use the **System Management** screen (see Section 2.18 on page 101) to manage system.
- Use the **VLAN Status** screen (see Section 2.19 on page 103) to view status of each VLAN.

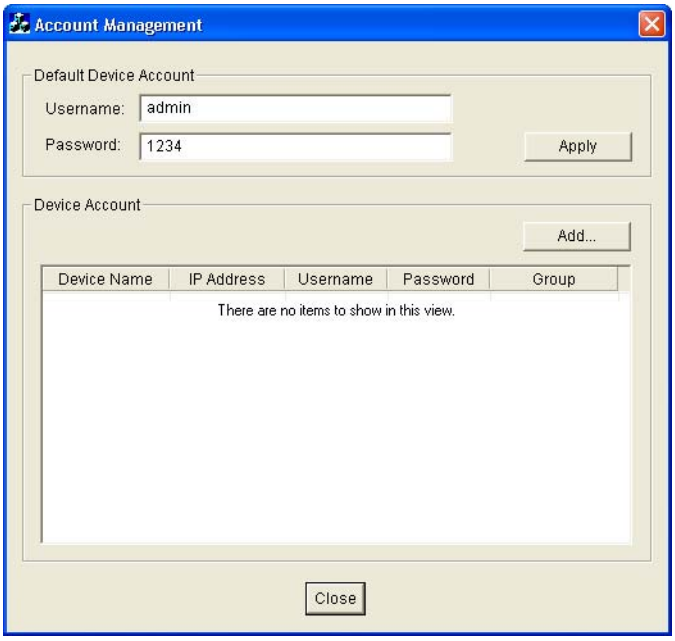
2.3 The Account Management Screen

Use this menu item to change the account name and/or password Pro EMS uses to communicate with the selected device for such as firmware upgrade or configuration backup. You can also add other devices in this screen if they also use the same account information.

Note: Make sure the same account information is configured on the select device(s).

Select a managed device. Select **Tools** > **Account Management** or right-click the managed device and then select **Tools** > **Account Management**. The screen appears as shown next.

Figure 20 Tool > Account Management



The following table describes the labels in this screen.

Table 4 Tools > Account Management

LABEL	DESCRIPTION
Default Device Account Select one or multiple device(s) in the **Device Account** section and then use this section to change the account setting that Pro EMS uses to communicate with the selected device(s).	
Username	Type up to 31 printable ASCII characters for the user name of the account. Spaces are allowed.
Password	Type up to 31 printable ASCII characters for the account's password. Spaces are allowed.
Apply	Click this to change the account setting stored on Pro EMS.
Device Account	
Add	Click this to add device(s) in the table below for further setting. A **Search Device** screen appears. See Figure 32 on page 61.
Device Name	This field displays the name of a device.
IP Address	This field displays the IP address of the device.
Username	This field displays the account name you have configured for the device on Pro EMS.
Password	This field displays the account password you have configured for the device on Pro EMS.

Table 4 Tools > Account Management (continued)

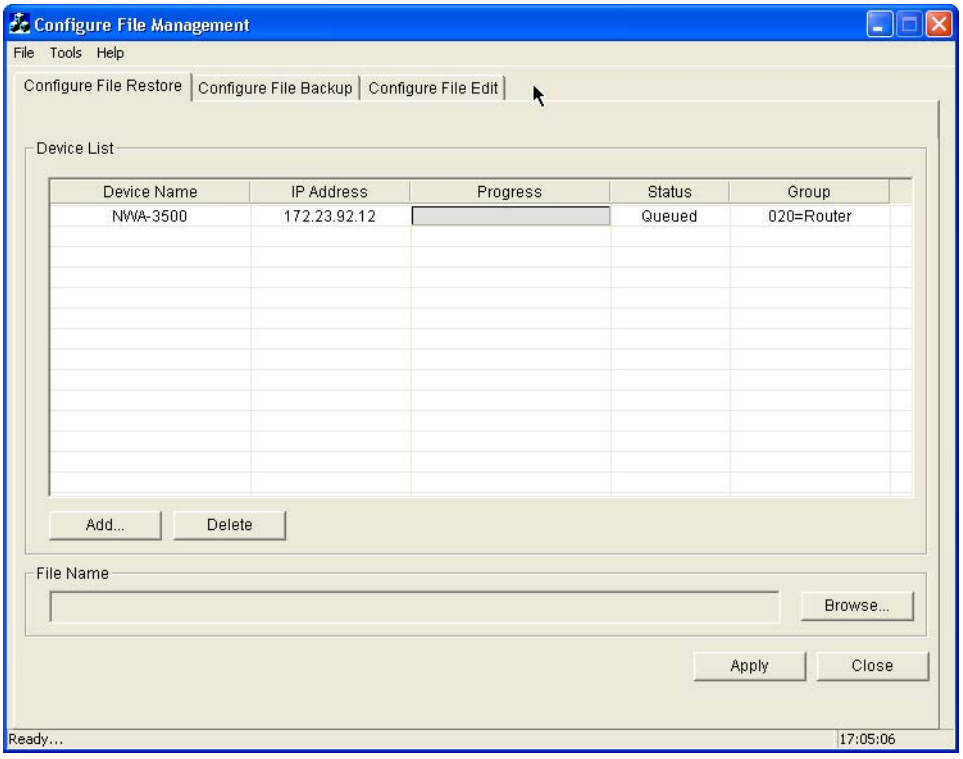
LABEL	DESCRIPTION
Group	This field displays the group with which the device is associated.
Close	Click this to discard all changes and exit this screen.

2.4 The Configuration File Management Screen

Use this menu item to manage (backup, restore, or edit) the configuration file of one or multiple managed devices. The backup here means to download the configuration file from the device(s) to Pro EMS while the restore is to upload a specified configuration file from Pro EMS to the device(s).

Select a managed device. Select **Tools** > **Configuration File Management** or right-click the managed device and Select **Tools** > **Configuration File Management**. The screen appears as shown next.

Figure 21 Tool > Configuration File Management



The following table describes the labels in this screen.

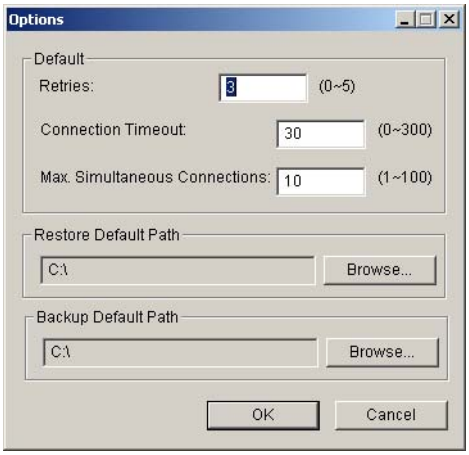
Table 5 Tools > Configuration File Management

LABEL	DESCRIPTION
File	
Exit	Select this to discard all changes and exit this screen.
Tools	
Options	Select this to configure the default values of parameters applied to the settings in this screen. See Section 2.4.1 on page 43.
Help	
About Configuration File Management	Select this to view the copyright information of this feature. The screen appears as shown next. **Figure 22** About Configuration File Management  Click **OK** to close this screen.
Configure File Restore	Use this tab screen to upload a specified configuration file to the selected device.
Configure File Backup	Use this tab screen to download the configuration file from the selected device.
Configure File Edit	Use this tab screen to edit the configuration file for the selected device.

2.4.1 The Options Screen

Select **Tools** > **Options** in the **Tools** > **Configuration File Management** screen, the screen appears as shown next.

Figure 23 Tools > Configuration File Management > Tools > Options



The following table describes the labels in this screen.

Table 6 Tools > Configuration File Management

LABEL	DESCRIPTION
Default	
Retries	Use this field to specify the number of retries (0~5) Pro EMS should do for a failed task. Enter **0** if you do not want Pro EMS to retry.
Connection Timeout	Use this field to specify the number of seconds (0~300) Pro EMS should wait before retrying a task if the task was failed. Enter **0** if you want Pro EMS to retry immediately for a failed task.
Max. Simultaneous Connections	Use this field to specify the maximum number of simultaneous connections Pro EMS allows when performing device configuration backup and restoring.
Restore Default Path	Click **Browse** to locate the default directory from which you restore a configuration file. This field then displays the specified directory.
Backup Default Path	Click **Browse** to locate the default directory to which you back up a configuration file. This field then displays the specified directory.
OK	Click this to save the changes and close this screen.
Cancel	Click this to discard all changes and exit this screen.

2.4.2 The Configure File Restore Screen

Use this screen to upload a specified configuration file to the selected device. You can also upload the file to other devices in this screen.

Select the **Configure File Restore** tab in the **Tools** > **Configuration File Management** screen, the screen appears as shown next.

Figure 24 Tools > Configuration File Management > Configure File Restore

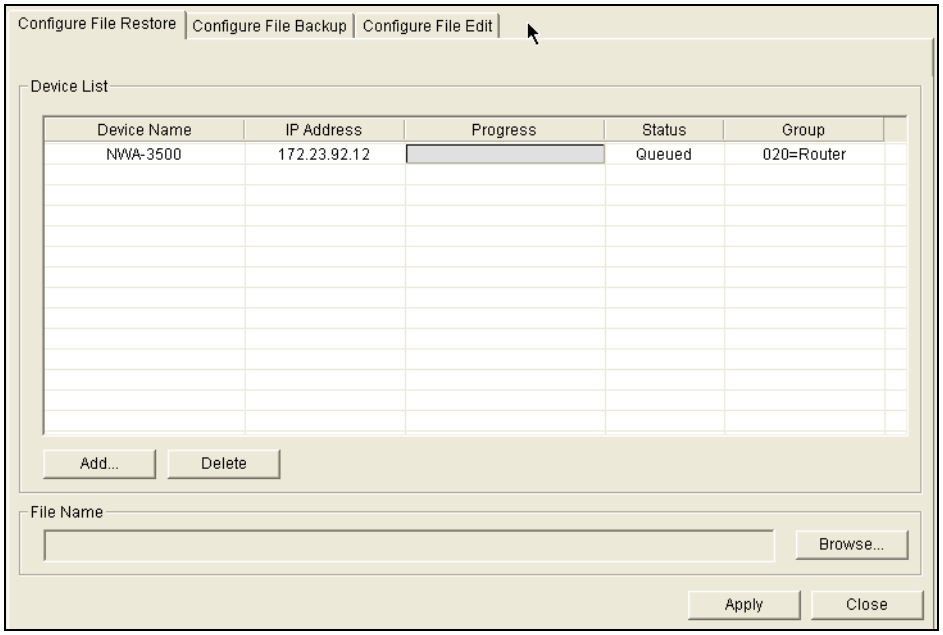


Table 7 Tools > Configuration File Management > Configure File Restore

LABEL	DESCRIPTION
Device List	
Device Name	This field displays the name of the selected device.
IP Address	This field displays the IP address of the device.
Progress	This field displays the percentage of a restoring task that has been completed.

Table 7 Tools > Configuration File Management > Configure File Restore

LABEL	DESCRIPTION
Status	This field displays the status of a device configuration restoring task. **Initializing**: Pro EMS is preparing for the configuration restoring task. **Connecting**: Pro EMS is attempting to upload the specified configuration file to the device. **Uploading**: Pro EMS is uploading the specified configuration file to the device. **Finished**: Pro EMS has successfully uploaded the configuration file to the device. **Queued**: The task is waiting in the queue because too many tasks are requested at the same time. You may try to adjust the **Max. Simultaneous Connects** value in **Tools** > **Options** in this screen. The higher the value the faster Pro EMS can handle tasks. **Retrying**: Pro EMS is attempting to connect to the device again because the configuration restoring task was failed last time. **Failed**: Pro EMS failed to connect to the device and the maximum number of retries has been reached (configured in **Tools** > **Options** in this screen). This could be because the network is disconnected between Pro EMS and the device.
Group	This field displays the group with which the device is associated.
Add	Click this to add more device(s) into the device list.
Delete	Click this to remove the selected device(s) from the device list.
File Name	Click **Browse** to locate the configuration file which Pro EMS will upload to the device.
Apply	Click this to upload the specified file to the selected device(s).
Close	Click this to discard all changes and exit this screen.

The following figure shows the

2.4.3 The Configure File Backup Screen

Select the **Configure File Restore** tab in the **Tools** > **Configuration File Management** screen, the screen appears as shown next.

Figure 25 Tools > Configuration File Management > Configure File Backup

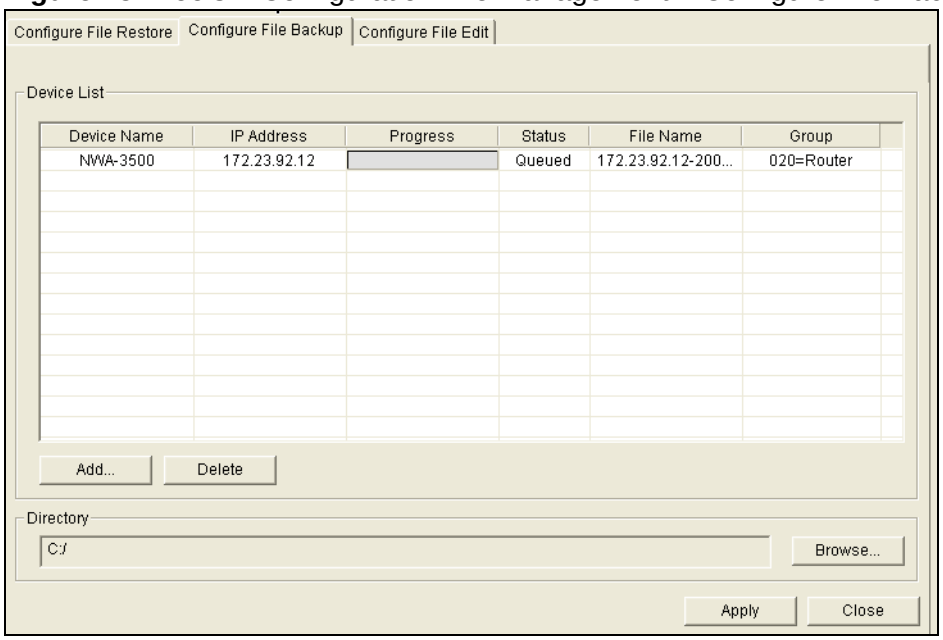


Table 8 Tools > Configuration File Management > Configure File Backup

LABEL	DESCRIPTION
Device List	Select one or multiple device(s) in this table you wish to download the configuration file(s).
Device Name	This field displays the name of a device.
IP Address	This field displays the IP address of the device.
Progress	This field displays the percentage of a backup task that has been completed.

Table 8 Tools > Configuration File Management > Configure File Backup (continued)

LABEL	DESCRIPTION
Status	This field displays the status of the device configuration backup task. **Initializing**: Pro EMS is preparing for the configuration backup task. **Connecting**: Pro EMS is attempting to download a configuration file from the device. **Downloading**: Pro EMS is downloading a configuration file from the device. **Finished**: Pro EMS has successfully downloaded a configuration file from the device. **Queued**: The task is waiting in the queue because too many tasks are requested at the same time. You may try to adjust the **Max. Simultaneous Connects** value in **Tools** > **Options** in this screen. The higher the value the faster Pro EMS can handle tasks. **Retrying**: Pro EMS is attempting to connect to the device again because the backup task was failed last time. **Failed**: Pro EMS failed to connect to the device and the maximum number of retries has been reached (configured in **Tools** > **Options** in this screen). This could be because the network is disconnected between Pro EMS and the device.
File Name	This is a combination of the device's IP address, current date, time and a random number generated automatically by Pro EMS. This will be the name of the device's configuration file downloaded from the device.
Group	This field displays the group with which the device is associated.
Add	Click this to add more device(s) in the device list.
Delete	Click this to remove the selected device(s) from the device list.
Directory	This field displays the default directory to store the configuration file downloaded from the selected device(s). Click **Browse** to locate another directory if you want to change it.
Apply	Click this to start the configuration backup task.
Close	Click this to discard all changes and exit this screen.

2.4.4 The Configure File Edit Screen

Select the **Configure File Edit** tab in the **Tools** > **Configuration File Management** screen, the screen appears as shown next.

Figure 26 Tools > Configuration File Management > Configure File Edit

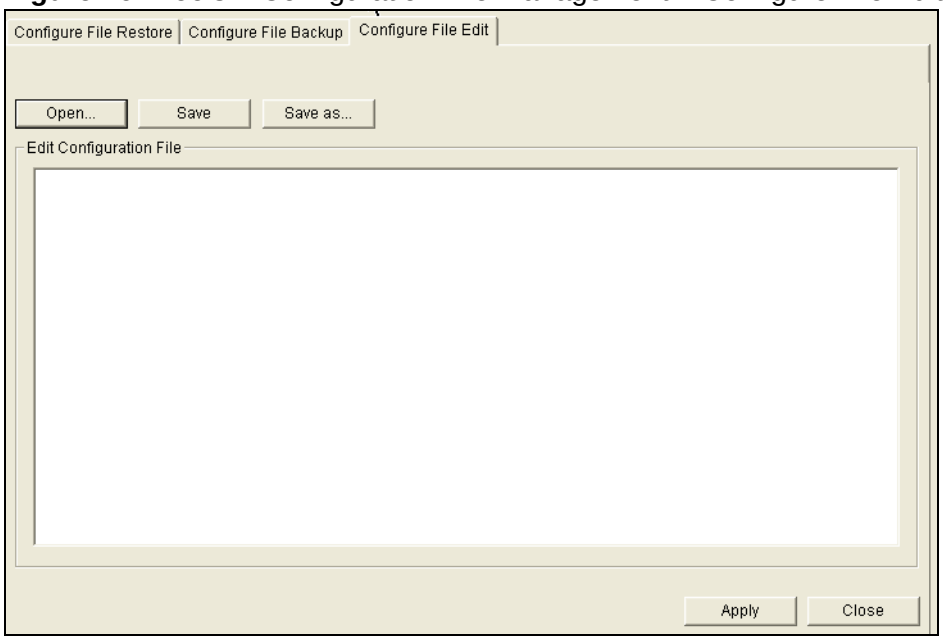


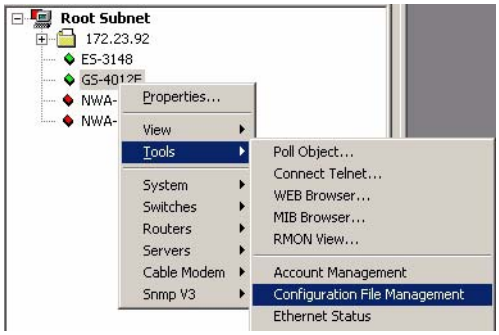
Table 9 Tools > Configuration File Management > Configure File Edit

LABEL	DESCRIPTION
Open	Click this to open a configuration file from your computer where Pro EMS is running. The configuration content is then displayed in the **Edit Configuration File** section.
Save	Edit the configuration file you opened and then click this to save all changes back to the original file.
Save as	Edit the configuration file you opened and then click this to save all changes to a specified file.
Edit Configuration File	This field displays the content of the opened configuration file. Scroll down the **Edit Configuration File** window to where you want to edit. Note: Only edit the text part of a configuration file. Editing the binary part and then uploading them to a device may damage the device.
Apply	Click this if you want to upload the edited configuration file to the original device or other device(s). An **Apply Devices** screen appears. See Section 2.4.2 on page 44 for similar field description. Note: You must save the changes to the original or another file before clicking **Apply**. Otherwise, the changes will not be applied to device(s).
Close	Click this to discard all changes and exit this screen.

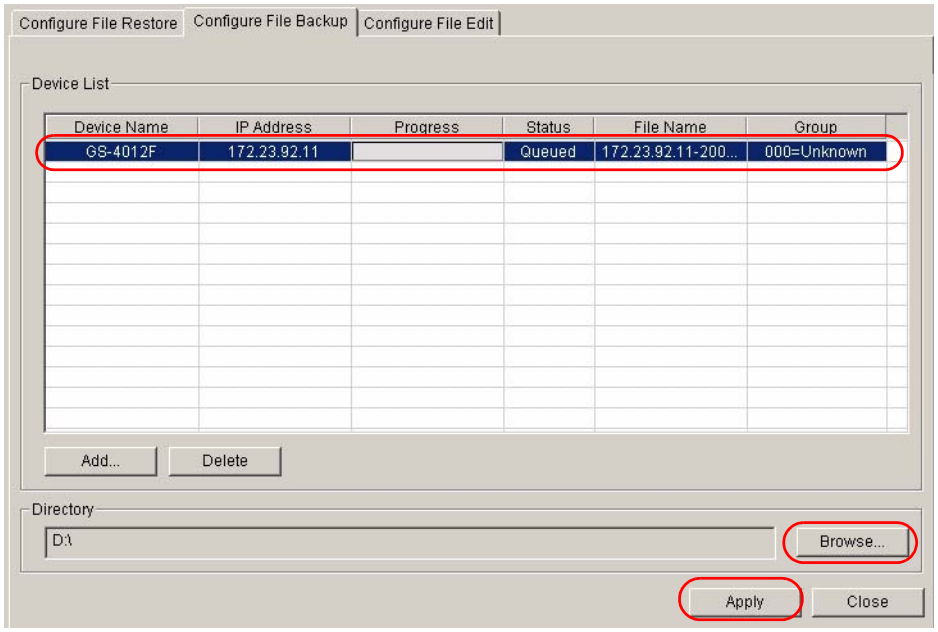
2.4.4.1 Editing a Configuration File Example

This section shows how to download the configuration file from a device, edit and then upload it back to the device.

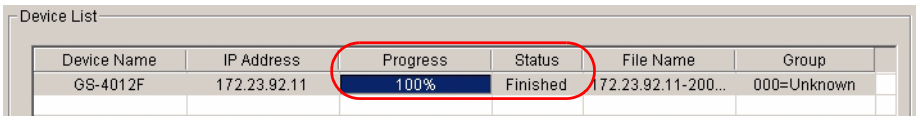
1 Right-click a device (**GS-4012F** in this example) and select **Tools** > **Configuration File Management**.



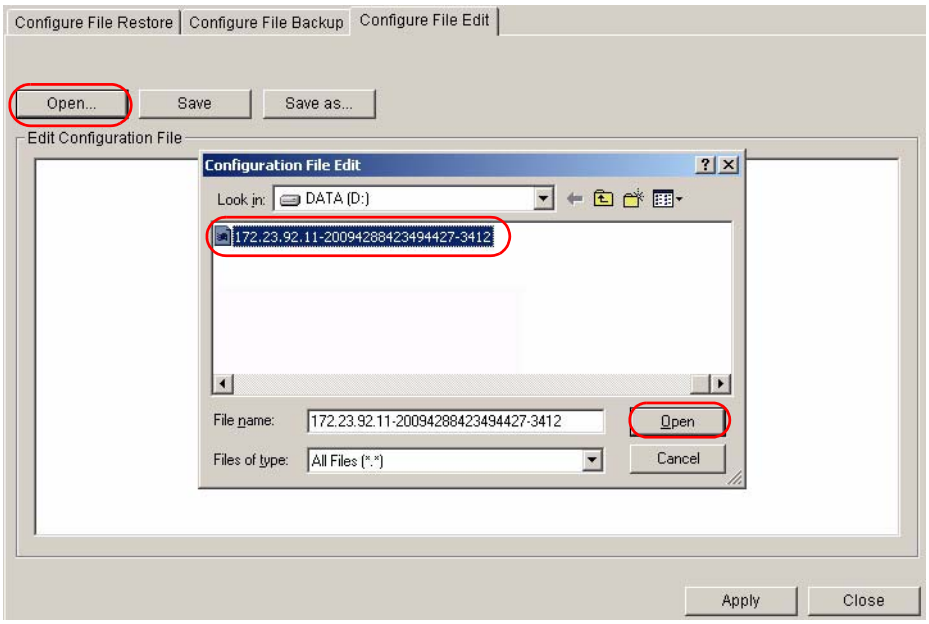
2 Select the **Configure File Backup** tab. Select the device and click **Browse** to locate the directory to which you want to store the downloaded configuration file. Then click **Apply**.



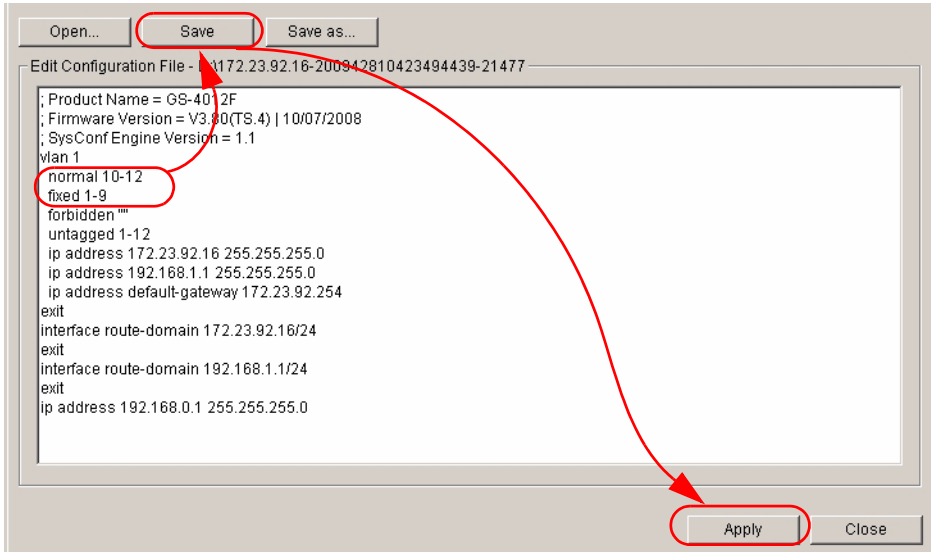
3 The backup starts to process until the **Progress** and **Status** display **100%** and **Finished**. Write down the file name that you will use later.



4 Select the **Configure File Edit** tab. Click **Open**. Select the file that you just downloaded and click **Open**.



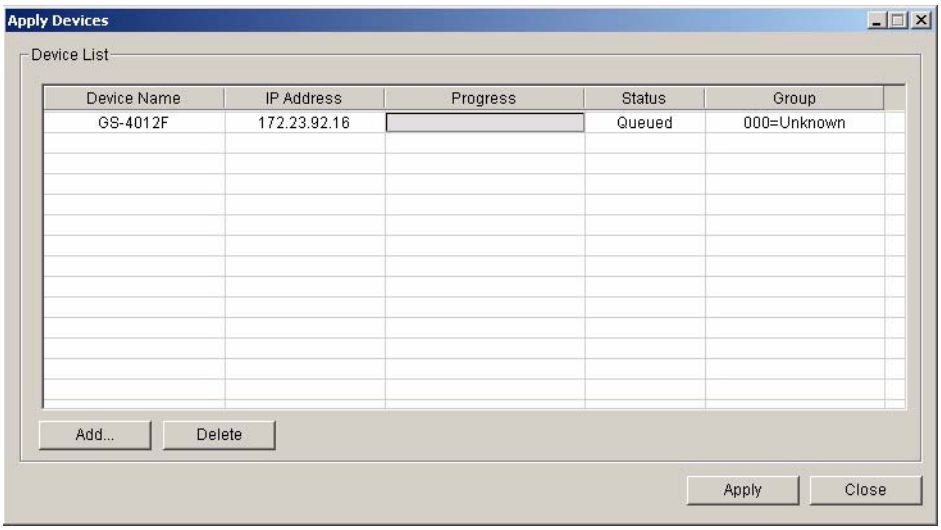
5 Edit the configuration content. This example edits the VLAN1 settings from **normal “”** to **normal 10-12** and **fixed 1-12** to **fixed 1-9**. Click **Save** or **Save as** to save the changes to the original or another file. Click **Apply**.



Note: You must save the file before you upload the changes back to the original device or other devices by clicking **Apply** in this screen.

Note: You can only edit the existing settings in the configuration content. The changes that adding new settings or editing the notes information (starting with a semicolon) will not be applied to device(s).

6 The Apply Devices screen appears. Click **Apply**.



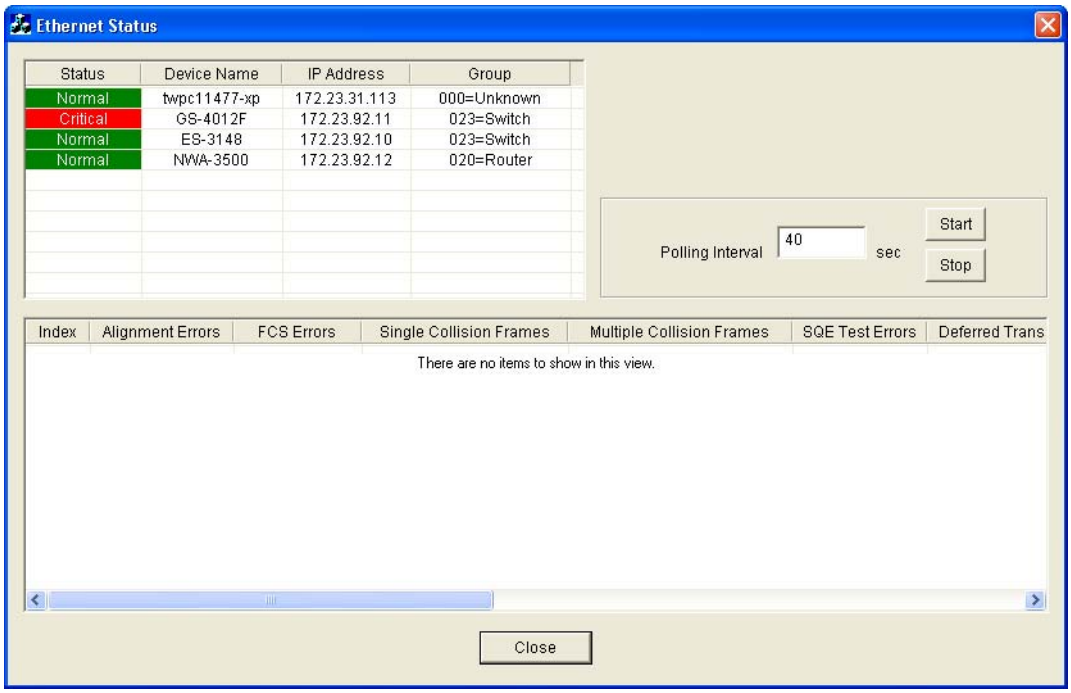
If you see that the **Progress** and **Status** display **100%** and **Finished then**, that means the changes have been successfully uploaded (/applied) to the device.

2.5 The Ethernet Status Screen

Use this menu item to view Ethernet packet statistics on all Ethernet interfaces of a managed device. Not all managed devices support this feature.

Select a managed device. Select **Tools** > **Ethernet Status** or right-click the managed device and select **Tools** > **Ethernet Status**. The screen appears as shown next.

Figure 27 Tool > Ethernet Status



The following table describes the labels in this screen.

Table 10 Tools > Ethernet Status

LABEL	DESCRIPTION
Status	This field indicates the presence of a most recent alarm/event log with one of the following severity levels (listed from high to low) on a managed device. • **Critical** • **Severe** • **Major** • **Minor** • **Warning** • **Normal** • **Info**
Device Name	This field displays the name of the device. Select the appropriate managed device.
IP Address	This field displays the IP address of the device.
Group	This field displays the SNMPc group code and name with which the device is associated. See Table 11 on page 54.
Polling Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Start**. Click **Stop** to halt statistic polling.

Table 10 Tools > Ethernet Status (continued)

LABEL	DESCRIPTION
Index	This is the index number of a port on the selected managed device.
Alignment Errors	This is the number of frames received/transmitted that were 64 to 1518 (non VLAN) or 1522 (VLAN) octets long but contained an invalid FCS and a non-integral number of octets.
FCS Errors	This is the number of frames received/transmitted with an integral length of 64 to 1518 octets and containing a Frame Check Sequence error.
Single Collision Frames	This field displays the number of frames received/transmitted containing one collision.
Multiple Collision Frames	This field displays the number of frames received/transmitted containing 2 to 15 collisions.
SQE Test Errors	This field displays the number of frames received/transmitted containing Signal Quality Error (SQC) errors.
Deferred Transmissions	This field displays the number of frames received/transmitted delayed due to deferred transmission.
Late Collisions	A late collision is counted when a device detects a collision after it has sent the 512th bit of its frame. This field displays the number of times such a collision is detected.
Excessive Collisions	This is the number of frames for which transmission failed due to excessive collisions.
Mac Transmit Errors	This field displays the number of packets with Internet MAC sublayer transmission error.
Carrier Sense Errors	This field displays the number of times a carrier senses an error occurred.
Frame Too Longs	This is the number of frames received/transmitted that were longer than 1518 octets (non VLAN) or 1522 octets (VLAN) and contained an invalid FCS, including alignment errors.
Mac Receive Error	This field displays the number of frames received with MAC address errors.
Ether Chip Set	This field identifies the Ethernet chipset used for the interface.
Close	Click this to discard all changes and exit this screen.

Table 11 Default SNMPc Group Codes and Names

CODE	DESCRIPTION
000	Unknown
002	Workstation
003	PC
011	WebServer
012	DiskServer
013	EmailServer
020	Router

Table 11 Default SNMPc Group Codes and Names

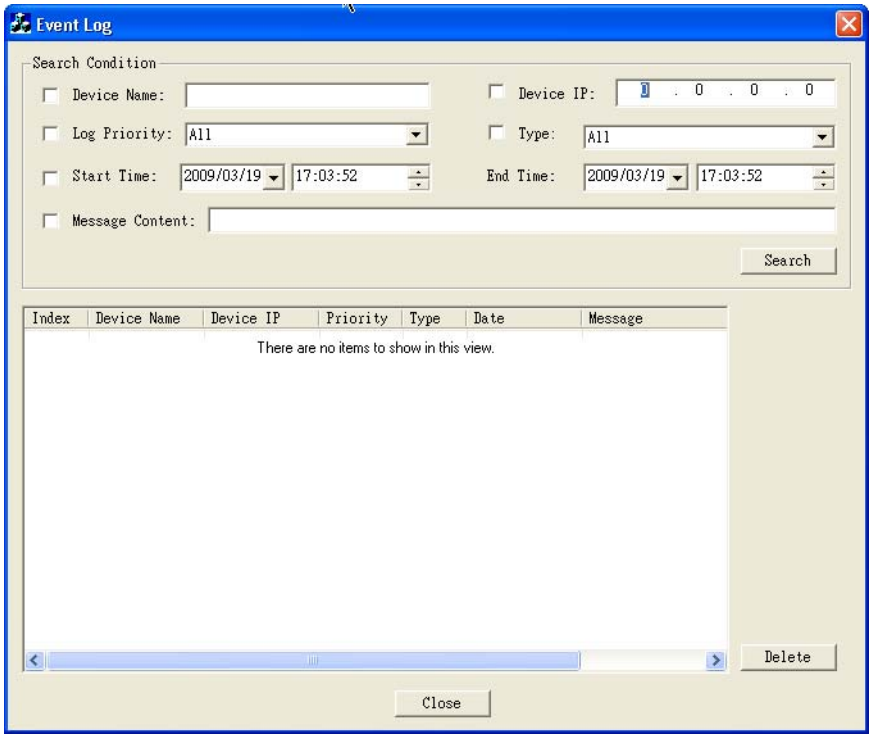
CODE	DESCRIPTION
021	WanRouter
022	LanRouter
023	Switch
030	RegularHub
031	SmartHub
040	RmonProbe
041	FireWall
042	Printer

2.6 The Event Log Screen

Use this menu item to search all or specific event logs stored on Pro EMS.

Select a managed device. Select **Tools** > **Event Log** or right-click the managed device and select **Tools** > **Event Log**. The screen appears as shown next.

Figure 28 Tool > Event Log



The following table describes the labels in this screen.

Table 12 Tools > Event Log

LABEL	DESCRIPTION
Search Condition These fields are criteria to select which events are displayed below. If you click the **Search** button without selecting any fields, this screen will display all event logs the Pro EMS stores.	
Device Name	Type the name of the device you wish to find.
Device IP	Type the IP address of the device.
Log Priority	Select this and the severity level of the event if you want this to be one of the search criteria. The choices are **All**, **Info**, **Normal**, **Minor**, **Major**, or **Critical**.
Type	Select this and the type of the event log(s) if you want this to be one of the search criteria. The choices are **All**, **History**, or **Current**.
Start Time End Time	All logs have a time-stamp. The time stamp depends on the time configured on the device. Select this if you want this to be one of the search criteria. Then select the start and end dates/times from which the device generated event log(s)
Message Content	Select this and type the keyword of the event you wish to find if you want this to be one of the search criteria.
Search	Click this to display the event logs based on the criteria in this section.
Index	This field displays the index number of an event log.
Device Name	This field displays the name of the managed device on which the event log was generated.
Device IP	This field displays the IP address of the device on which the log entry was generated.
Priority	This field displays the severity of the event log.
Type	This field displays the type of the event log.
Date	This field displays the date and time on which the event log was generated.
Message	This field displays some information about the event log.
Delete	Click this to remove the selected log message(s).
Close	Click this to discard all changes and exit this screen.

2.7 The Firmware Upgrade Screen

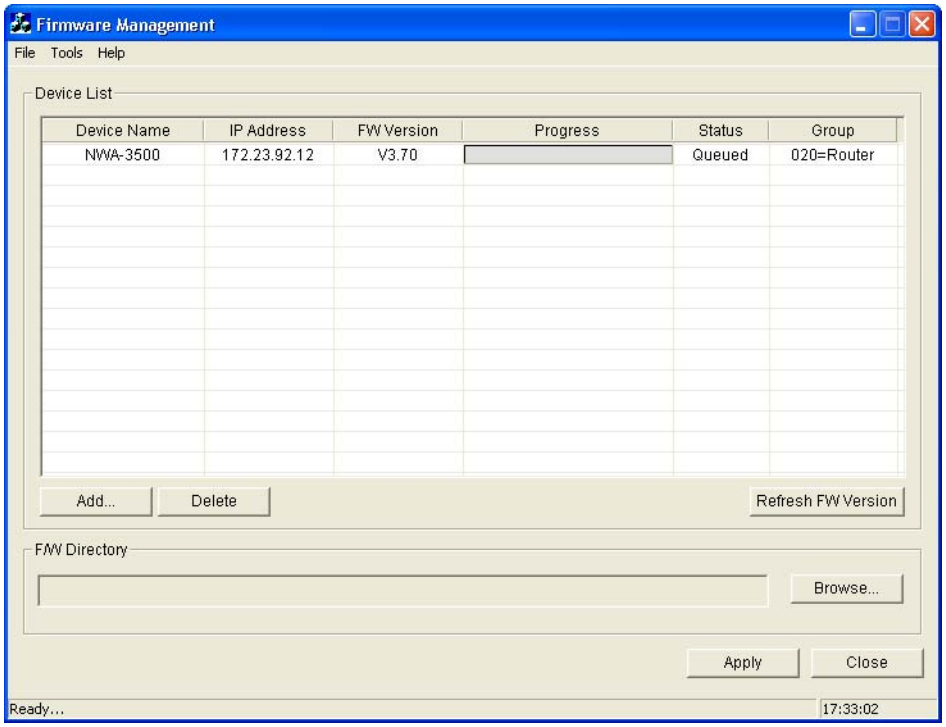
Use this menu item to upgrade firmware for one or multiple device(s). You have to check the following firmware file naming conversions and warnings before using this screen for device firmware upgrade.

- Notify device users before uploading firmware. The device must not be switched off during firmware upload. Otherwise the device may be damaged.

- Make sure to upload correct firmware for your device. For example, V3.80(TS.4). The firmware code (**TS** in this example) identifies a specific device (GS-4012F in this example). Only upload firmware with the same firmware code in the firmware file name to your device.

Select a managed device. Select **Tools** > **Firmware Upgrade** or right-click the managed device and select **Tools** > **Firmware Upgrade**. The screen appears as shown next.

Figure 29 Tool > Firmware Upgrade



The following table describes the labels in this screen.

Table 13 Tools > Firmware Upgrade

LABEL	DESCRIPTION
File	
Exit	Select this to exit this screen.
Tools	
Options	Select this to configure default values of parameters used in this screen.
Help	
About Firmware Upgrade	Select this to view the copyright information of this feature.
Device List	Select one or multiple device(s) in this section you wish to upgrade the firmware. Use [SHIFT] to select multiple entries in the table. Note: You must only select multiple devices that are identical.

Table 13 Tools > Firmware Upgrade (continued)

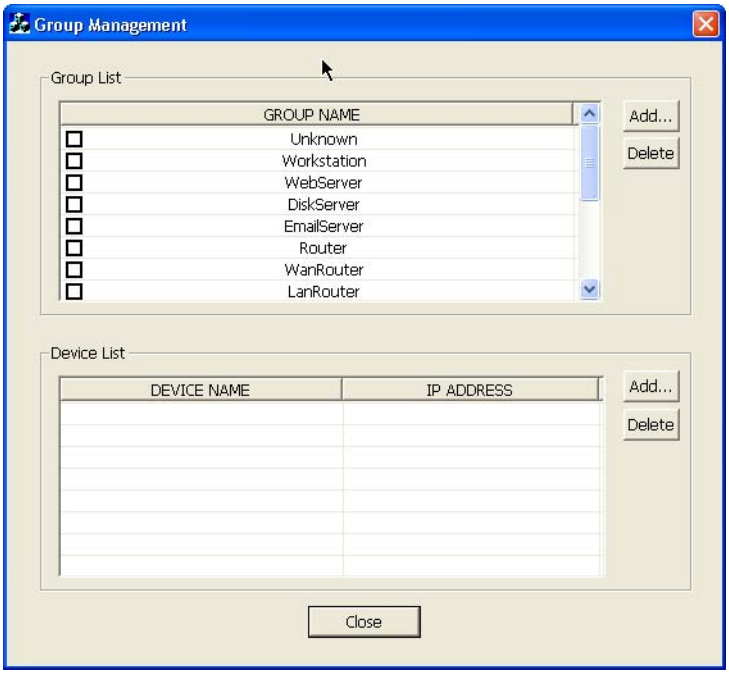
LABEL	DESCRIPTION
Device Name	This field displays the name of a device.
IP Address	This field displays the IP address of the device.
FW Version	This field displays the firmware version the device is currently using. This field also displays the date the firmware version was released.
Progress	This field displays the percentage of a firmware upgrading task that has been completed.
Status	This field displays the status of the firmware upgrade task. **Initializing**: Pro EMS is preparing for the firmware upgrade task. **Connecting**: Pro EMS is attempting to upload the specified firmware file to the device. **Uploading**: Pro EMS is uploading the specified firmware file to the device. **Finished**: The Pro EMS has successfully uploaded the firmware file to the selected device. **Queued**: The task is waiting in the queue because too many tasks are requested at the same time. You may try to adjust the **Max. Simultaneous Connects** value in **Tools** > **Options** in this screen. The higher the value the faster Pro EMS can handle tasks. **Retrying**: Pro EMS is attempting to connect to the device again because the firmware upgrade task was failed last time. **Failed**: Pro EMS failed to connect to the device and the maximum number of retries has been reached (configured in **Tools** > **Options** in this screen). This could be because the network is disconnected between Pro EMS and the device.
Group	This field displays the group with which the device is associated.
Add	Click this to add more device(s) to the device list.
Delete	Click this to remove the selected device(s) from the device list.
Refresh FW Version	Click this to retrieve the latest firmware information from devices and then update the **FW Version** field in this table above.
F/W Directory	Click **Browse** to locate the firmware file you want to upload to the selected device(s).
Apply	Click this to upload the specified firmware file to the selected device(s).
Close	Click this to discard all changes and exit this screen.

2.8 The Group Management Screen

Use this menu item to logically group managed devices that can be managed together. For example, a script that could be uploaded to ZyXEL enterprise layer-2 switches requires the same configuration settings.

Select a managed device. Select **Tools** > **Group Management** or right-click the managed device and select **Tools** > **Group Management**. The screen appears as shown next.

Figure 30 Tool > Group Management



The following table describes the labels in this screen.

Table 14 Tools > Group Management

LABEL	DESCRIPTION
Group List	
GROUP NAME	This field displays the name of an SNMPc group. Select a group to display the associated devices in the **Device List** table.
Add	Click this to take you to a screen where you can create an SNMPc group.
Delete	Click this to remove the selected SNMPc group(s).
Device List	
DEVICE NAME	This field displays the name of a device associated with the selected SNMPc group. Select one or more device(s) and click **Delete** if you want to remove them.
IP ADDRESS	This field displays the IP address of the device.
Add	Click this to add a device under the selected SNMPc group.
Delete	Click this to remove the selected device(s) from the selected SNMPc group.
Close	Click this to discard all changes and exit this screen.

2.8.1 Creating an SNMPc Group

Use this menu item to create an SNMPc group.

Click **Add** in the **Group List** section in the **Tool** > **SNMPc Group Management** screen. The screen appears as shown next.

Figure 31 Creating an SNMPc Group

The following table describes the labels in this screen.

Table 15 Creating an SNMPc Group

LABEL	DESCRIPTION
Group Name	Type up to 21 printable ASCII characters for the name of an SNMPc group you want to create.
Ok	Click this to save the changes and close this screen.
Cancel	Click this to discard all changes and exit this screen.

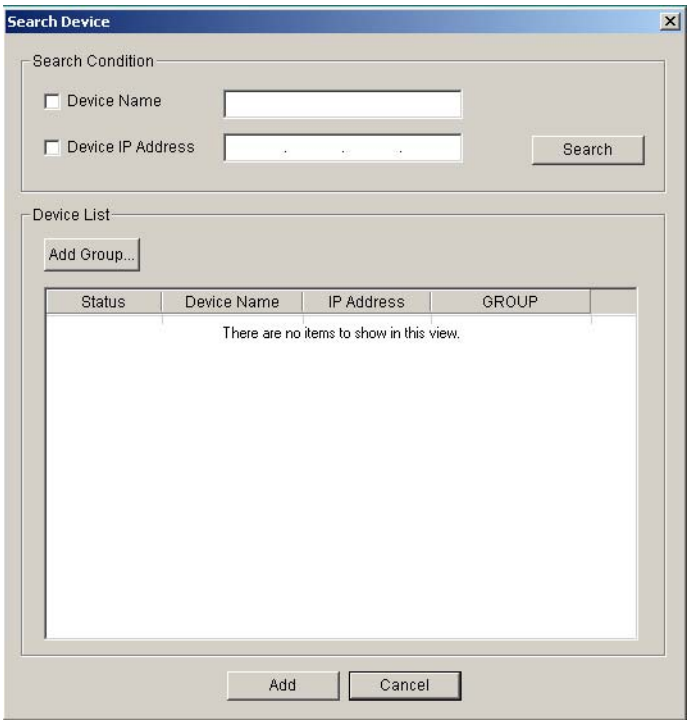
2.8.2 Associating a Device with an SNMPc Group

Use this menu item to associate device(s) with the selected groups.

Note: One device can be associated with one and only one SNMPc group.

Click **Add** in the **Group List** section in the **Tool** > **SNMPc Group Management** screen. The screen appears as shown next. The screen appears as shown next.

Figure 32 Associating a Device with an SNMPc Group



The following table describes the labels in this screen.

Table 16 Associating a Device with an SNMPc Group

LABEL	DESCRIPTION
Search Condition	Use this section to search device(s) from all managed devices by name or IP address.
Device Name	Select this and enter up to 31 printable ASCII characters for the name of a device you wish to search. This is the name you gave when you added the device in Pro EMS. You can also just enter a partial of the device name. For example, enter “NW” only to display all managed devices with NW starting in the names.
Device IP Address	Select this and enter the IP address of the device if you want to search a specific device. Unlike the **Device Name** field, you have to enter a complete IP address with four numbers, separated by dots.
Search	Click this to search device(s) according to the criteria you entered.
Device List	This section displays the device(s) you are looking for. You can also use this section to import devices from another SNMPc group.

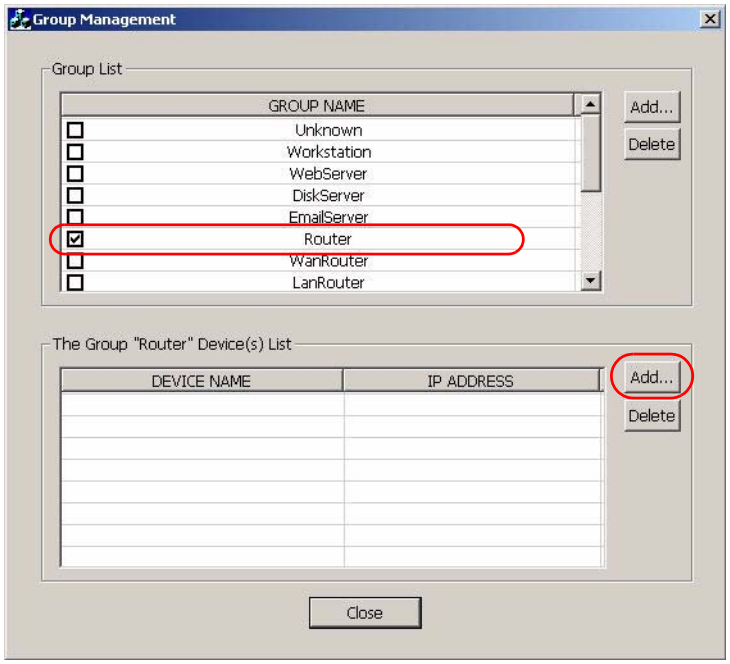
Table 16 Associating a Device with an SNMPc Group (continued)

LABEL	DESCRIPTION
Add Group	Click this to find device(s) from an SNMPc group. The screen appears as shown next. **Figure 33** Finding Devices from an SNMPc Group  1. Select a group from the **Group Name** field. 2. Click **OK**. 3. The available device(s) under the group will be shown in the **Device List** section of the **Search Device** screen. Note: After a device is associated from an SNMPs group to another, the device is removed from the original group.
Status	This field displays the current status of a device.
Device Name	This field displays the name of the device.
IP Address	This field displays the IP address of the device.
GROUP	This field displays the SNMPc group code and name with which the device is associated.
Add	Select one or multiple device(s) in the **Device List** and then click this to associate them with the previously selected SNMPc group in the **Group Management** screen (see Figure 30 on page 59). You can use the [SHIFT] key to select multiple devices.
Cancel	Click this to exit this screen without saving.

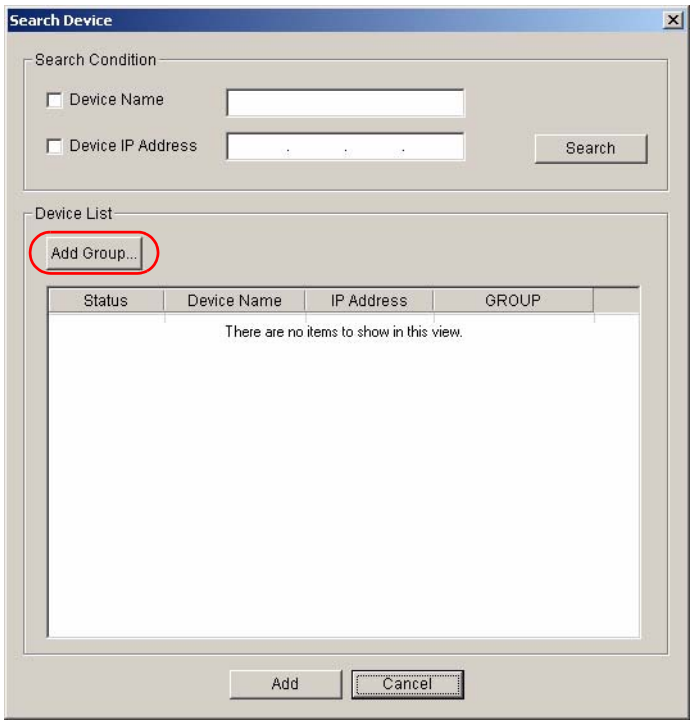
2.8.3 Example - Adding a Device from One Group to Another

A newly added device is associated with the **Unknown** SNMPc group by default. This example shows how to re-associate a device from the group **Unknown** to group **Router**.

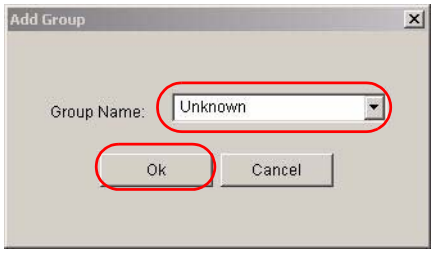
1 Select the group to which you want to be associated the newly added device in the **Group Management** screen. In this example, select **Router**. Click **Add** next to the device list table.



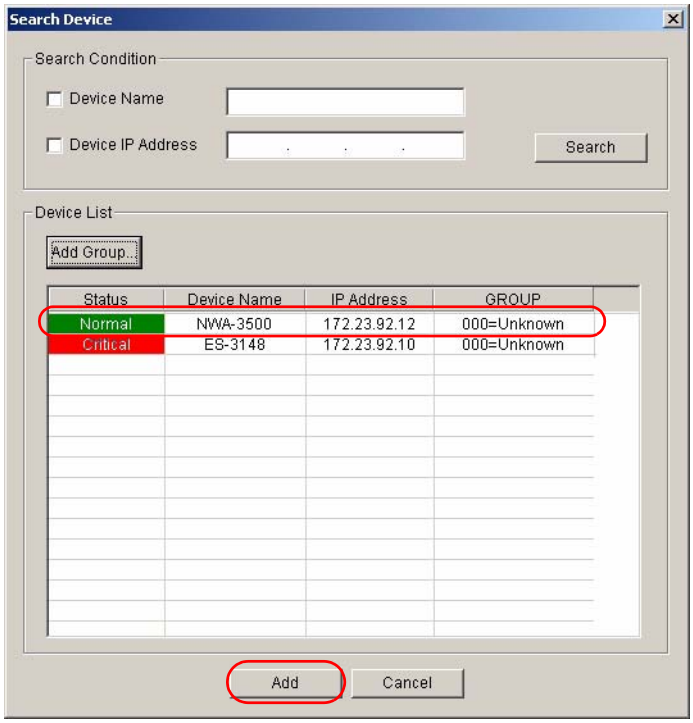
2 The **Search Device** screen appears. Click **Add Group** in the **Device List** section that is to find the group from which you want to add device(s).



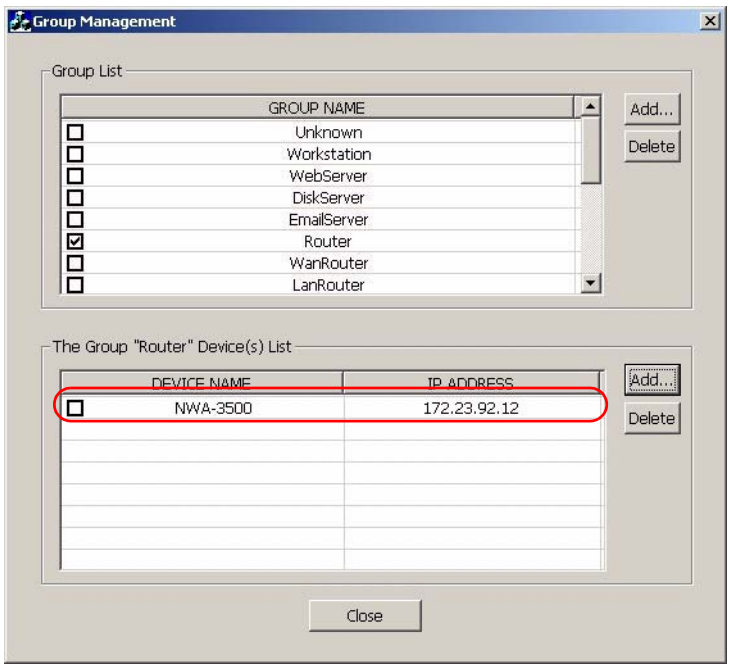
3 The **Add Group** screen appears. Select **Unknown** in the **Group Name** field and click **OK** to bring the devices under the group to the previous **Search Device** screen.



4 Select a device (**NWA-3500** in this example) and then click **Add**.



5 Then you can see the **NWA-3500** has been added in the **Router** group.

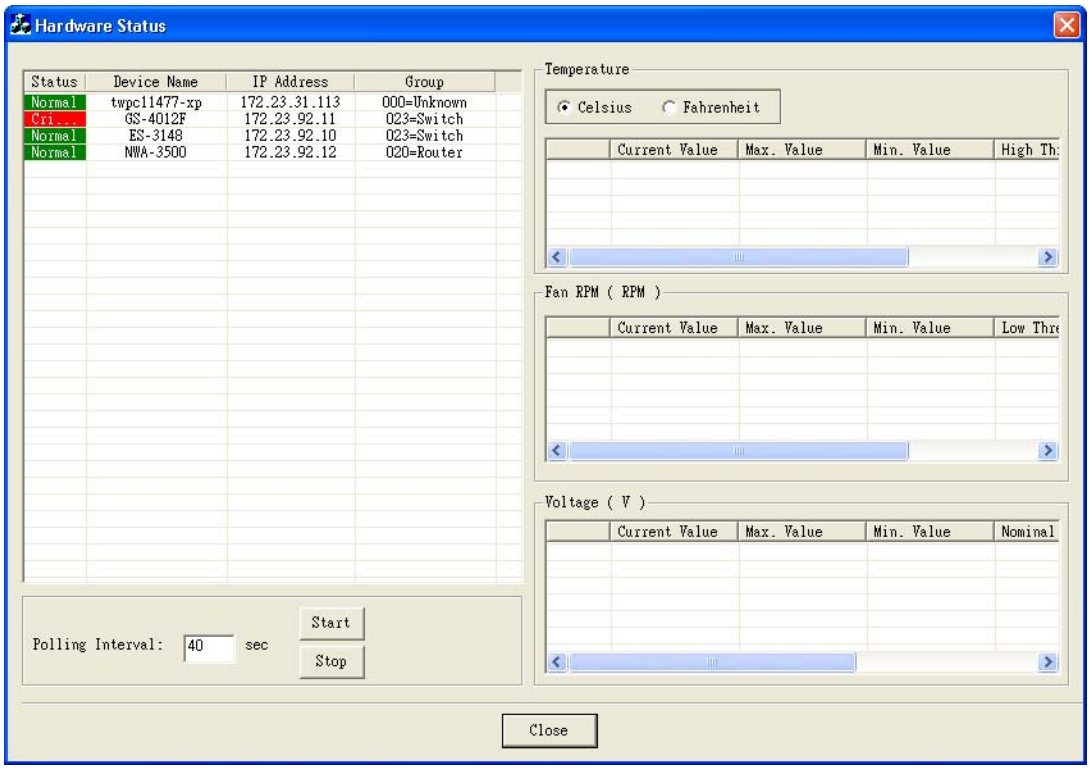


2.9 The Hardware Status Screen

Use this menu item to view hardware information such as temperature, fan and voltage.

Select a managed device. Select **Tools** > **Hardware Status** or right-click the managed device and select **Tools** > **Hardware Status**. The screen appears as shown next.

Figure 34 Tool > Hardware Status



The following table describes the labels in this screen.

Table 17 Tools > Hardware Status

LABEL	DESCRIPTION
Status	This field indicates the presence of a most recent alarm/event log with one of the following severity levels (listed from high to low) on a managed device. • **Critical** • **Severe** • **Major** • **Minor** • **Warning** • **Normal** • **Info**
Device Name	This field displays the name of the device. Select the appropriate managed device.
IP Address	This field displays the IP address of the device.
Group	This field displays the SNMPc group code and name with which the device is associated.

Table 17 Tools > Hardware Status (continued)

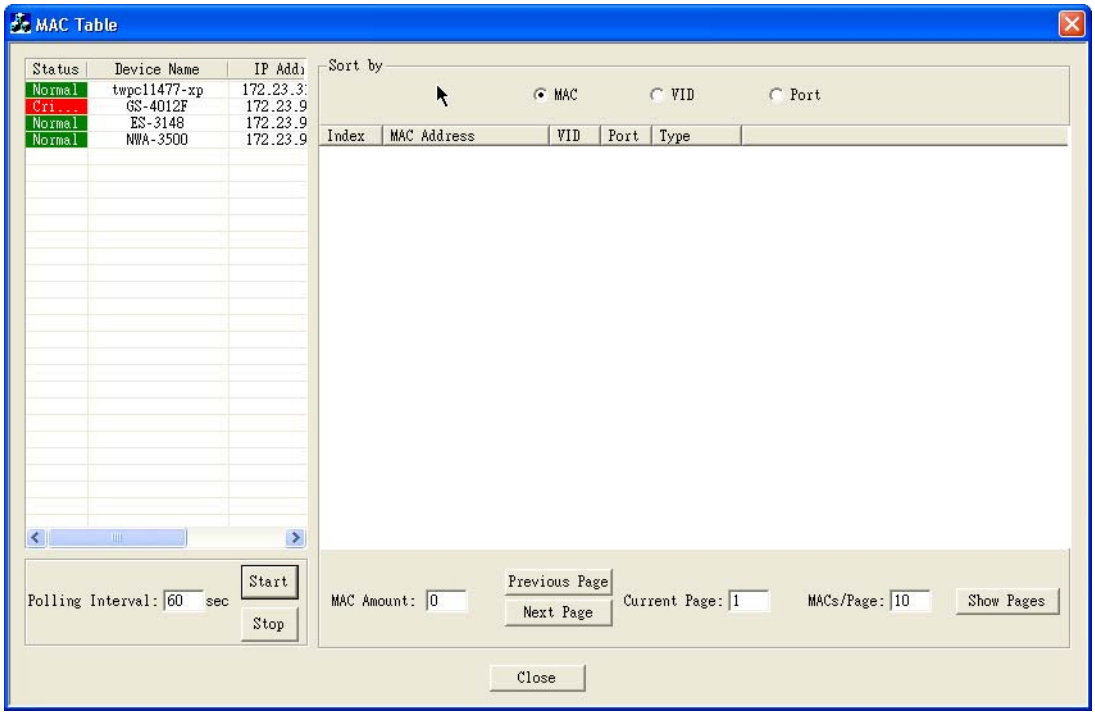
LABEL	DESCRIPTION
Polling Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Start**. Click **Stop** to halt statistic polling.
Temperature	Select **Celsius** to display all temperature measurements in degrees Celsius. Select **Fahrenheit** to display all temperature measurements in degrees Fahrenheit.
Max. Value	This field displays the maximum temperature measured at this sensor.
Min. Value	This field displays the minimum temperature measured at this sensor.
High Threshold	This field displays the highest temperature limit at this sensor.
Description	This field displays **Normal** for temperatures below the threshold and **Over** for those above.
Fan RPM (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that can detect and report the fan's RPM (Revolutions Per Minute).
Max. Value	This field displays the maximum RPM measured at this point.
Min. Value	This field displays the minimum RPM measured at this point.
Low Threshold	This field displays the lowest RPM limit at this sensor.
Description	**Normal** indicates that the RPM is within an acceptable operating range at this point; otherwise **Abnormal** is displayed.
Voltage (V)	The power supply for each voltage has a sensor that can detect and report the voltage.
Min. Value	This field displays the minimum voltage measured at this point.
Nominal Value	This field displays the average voltage in the operating voltage range that the device's vendor recommends.
Low Threshold	This field displays the lowest voltage limit at this sensor.
Description	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Abnormal** is displayed.
Close	Click this to exit this screen.

2.10 The MAC Table Screen

Use this menu item to view the MAC table of a managed device. You can sort the MAC addresses by MAC addresses, VLAN groups or ports.

Select a managed device. Select **Tools** > **MAC Table** or right-click the managed device and select **Tools** > **MAC Table**. The screen appears as shown next.

Figure 35 Tool > MAC Table



The following table describes the labels in this screen.

Table 18 Tools > MAC Table

LABEL	DESCRIPTION
Status	This field indicates the presence of a most recent alarm/event log with one of the following severity levels (listed from high to low) on a managed device. • **Critical** • **Severe** • **Major** • **Minor** • **Warning** • **Normal** • **Info**
Device Name	This field displays the name of the device. Select the appropriate managed device.
IP Address	This field displays the IP address of the device.
Group	This field displays the SNMPc group code and name with which the device is associated. See Table 11 on page 54 for the default SNMPc group codes and the names.
Polling Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Start**. Click **Stop** to halt statistic polling.

Table 18 Tools > MAC Table (continued)

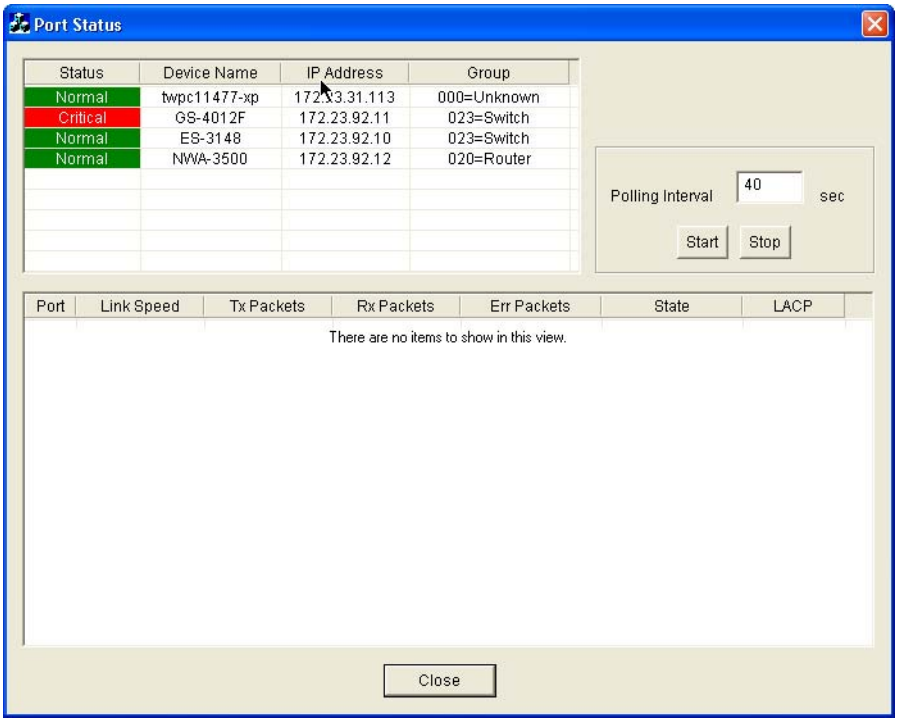
LABEL	DESCRIPTION
Sort by	Select one of the following options to display and arrange the data according to that option type. The information is then displayed in the summary table below. **MAC**: Select this to display and arrange the data according to MAC address. **VID**: Select this to display and arrange the data according to VLAN group. **Port**: Select this to display and arrange the data according to port number.
Index	This is the index number of a learned or static MAC address.
MAC Address	This is the MAC address of a computer or device that the device learned dynamically or is configured manually.
VID	This is the VLAN group to which the MAC address belongs.
Port	This field displays the number of each port from which the MAC address was learned if it is a dynamic MAC address. **CPU** displays when it is a static MAC address.
Type	This field displays whether the MAC address is **dynamic** (learned by the device) or **static** (manually configured on the device).
MAC Amount	This field displays the total number of MAC addresses listed in the table above.
Previous Page	Click this to display the previous page of the one that you entered in the **Current Page** field.
Next Page	Click this to display the next page of the one that you entered in the **Current Page** field.
Current Page	This field displays the page currently displayed in the table above.
MACs/Page	This field displays the maximum number of MAC addresses that can be displayed in one page.
Close	Click this to discard all changes and exit this screen.

2.11 The Port Status Screen

Use this menu item to view all port statistics and status of a managed device.

Select a managed device. Select **Tools** > **Port Status** or right-click the managed device and select **Tools** > **Port Status**. The screen appears as shown next.

Figure 36 Tool > Port Status



The following table describes the labels in this screen.

Table 19 Tools > Port Status

LABEL	DESCRIPTION
Status	This field indicates the presence of a most recent alarm/event log with one of the following severity levels (listed from high to low) on a managed device. • **Critical** • **Severe** • **Major** • **Minor** • **Warning** • **Normal** • **Info**
Device Name	This field displays the name of the device. Select the appropriate managed device.
IP Address	This field displays the IP address of the device.
Group	This field displays the SNMPc group code and name with which the device is associated. See Table 11 on page 54 for the default SNMPc group codes and the names.
Polling Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Start**. Click **Stop** to halt statistic polling.

Table 19 Tools > Port Status (continued)

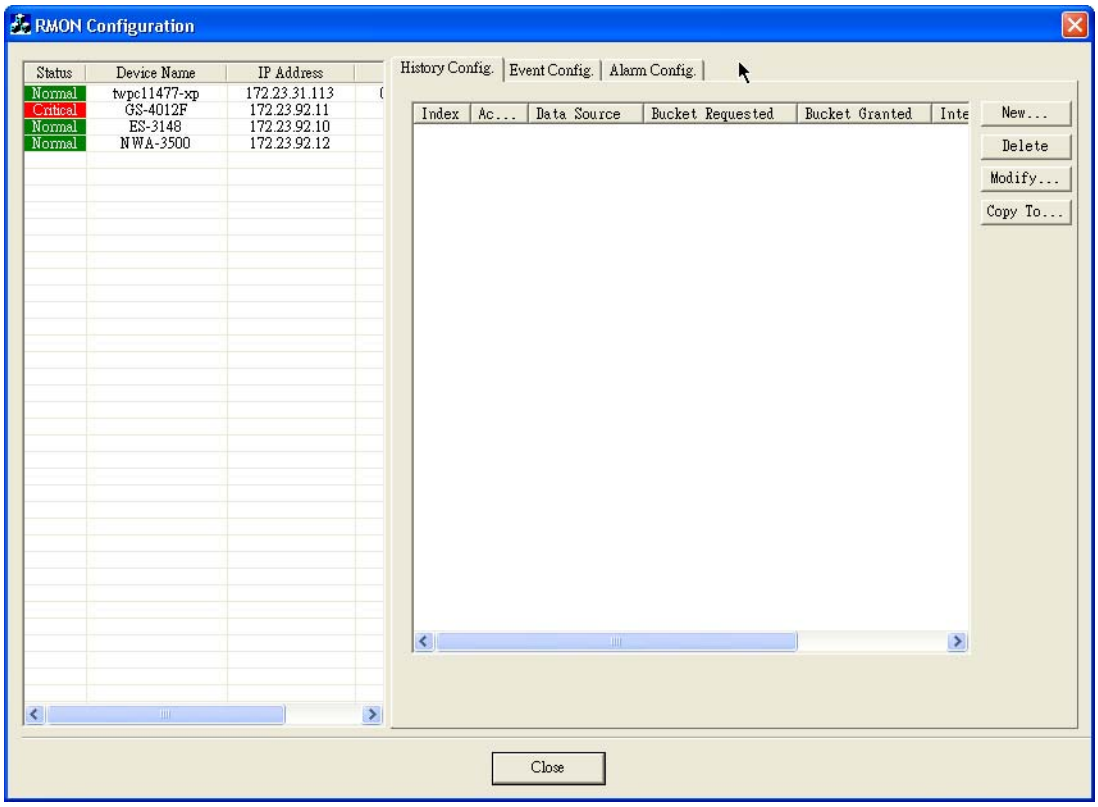
LABEL	DESCRIPTION
Port	This is the Ethernet port (**LAN**) or wireless LAN adaptor (**WLAN1** or **WLAN2**)
Link Speed	This shows the port speed and duplex setting if you are using Ethernet encapsulation for the Ethernet port. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect. This shows the transmission speed only for the wireless adaptors.
Tx Packets	This is the number of transmitted packets on this port.
Rx Packets	This is the number of received packets on this port.
Err Packets	This is the number of errors (collisions) occurred on this port.
State	This shows the current status of the port connection, which can be **Up** or **Down**.
LACP	This field displays whether Link Aggregation Control Protocol (LACP) is enabled on this port. When LACP is enabled on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention.
Close	Click this to exit this screen.

2.12 The RMON Configuration Screen

Use this menu item to view and configure RMON (Remote Network Monitoring) settings for managed device(s). RMON is a standard specification that provides information for a network administrator to monitor or analyze a network. RMON-supported devices use RMON probes to collect data according to the groups defined in the specification and then report it to Pro EMS.

Select a managed device. Select **Tools** > **RMON Configuration** or right-click the managed device and select **Tools** > **RMON Configuration**. The screen appears as shown next.

Figure 37 Tool > RMON Configuration



The following table describes the labels in this screen.

Table 20 Tools > RMON Configuration

LABEL	DESCRIPTION
Status	This field indicates the presence of a most recent alarm/event log with one of the following severity levels (listed from high to low) on a managed device. • **Critical** • **Severe** • **Major** • **Minor** • **Warning** • **Normal** • **Info**
Device Name	This field displays the name of the device. Select the appropriate managed device.
IP Address	This field displays the IP address of the device.
Group	This field displays the SNMPc group code and name with which the device is associated.

Table 20 Tools > RMON Configuration (continued)

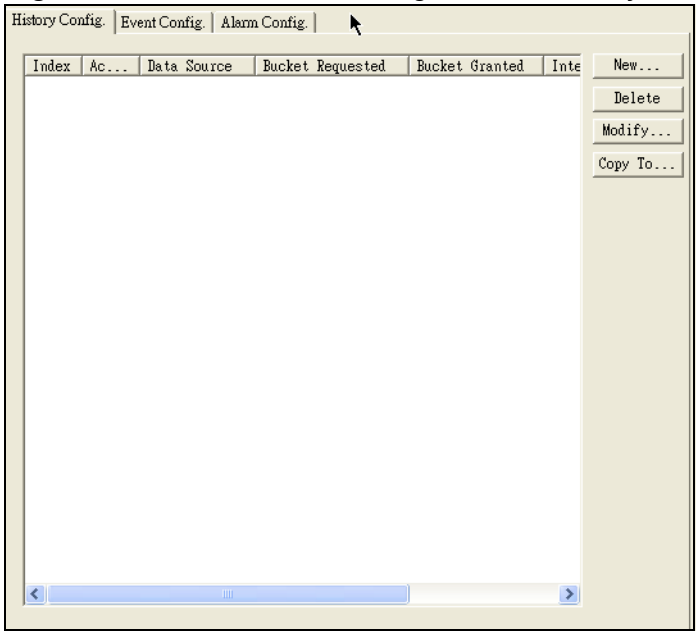
LABEL	DESCRIPTION
History Config	Use this tab screen to view and configure RMON history configuration settings for the selected device. See Section 2.12.1 on page 73.
Event Config	Use this tab screen to configure the actions that the selected device takes when an alarm is triggered. See Section 2.12.3 on page 75.
Alarm Config	Use this tab screen to configure alarms that occur when the sampled data exceeds the specified threshold. See Section 2.12.5 on page 78.
Close	Click this to exit this screen.

2.12.1 The History Config Screen

Use this screen to configure RMON historic data sampling settings that determine how to retrieve data samplings from historic RMON logs for the selected device. You will need to use the settings of this screen when configuring the **Tools** > **RMON Ethernet History Data** screen.

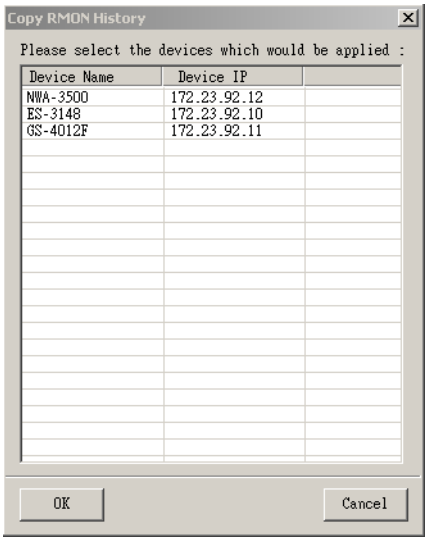
Select the **History Config** tab in the **Tools** > **RMON Configuration** screen, the screen appears as shown next.

Figure 38 Tool > RMON Configuration > History Config



The following table describes the labels in this screen.

Table 21 Tools > RMON Configuration > History Config

LABEL	DESCRIPTION
Index	This field displays the index number of a RMON historic data sampling setting.
Active	This field displays **Yes** if the historic configuration setting is enabled. Otherwise, it displays **No**.
Data Source	This is the port of the device that the Pro EMS will poll for data.
Bucket Requested	This field displays the number of data samplings the network manager requests the probe to retrieve.
Bucket Granted	This field displays the number of data samplings the probe allows to store.
Interval (sec)	This field displays the time between two data samplings.
Owner	This field displays the application that creates this setting.
New	Click this to add a new RMON historic data sampling setting.
Delete	Click this to remove the selected RMON historic data sampling setting.
Modify	Click this to change the setting of the selected RMON historic data sampling setting.
Copy To	Select one or multiple RMON historic data sampling setting(s) and then click this to copy it or them to another device. The screen appears as shown next. **Table 22** Copy To  Select one or multiple device(s) to where you want to duplicate the selected profile settings. Click **OK** to save the changes. An **Applied Results** screen displays then to show the result. Alternatively, you can click **Cancel** to exit this screen.

2.12.2 RMON History Configuration Screens

Use these screens to configure history configurations.

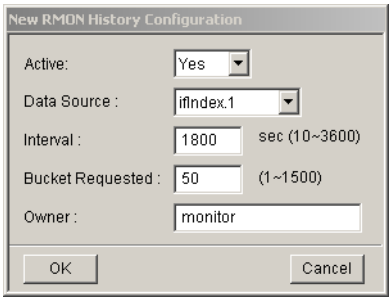
- **New RMON History Configuration**

This screen appears when you set up a new history configuration. To open this screen, select **Tools** > **RMON Configuration** > **History Config** > **New**. This screen appears in Figure 39 on page 75.

- **Modify RMON History Configuration**

This screen appears when you edit an existing history configuration. To open this screen, select **Tools** > **RMON Configuration** > **History Control** > **Modify**. Then, select the history configuration you want to edit, and click **Modify**. This screen is similar to the one below.

Figure 39 Tools > RMON Configuration > History Config > New



The following table describes the labels in this screen.

Table 23 Tools > RMON Configuration > History Config > New

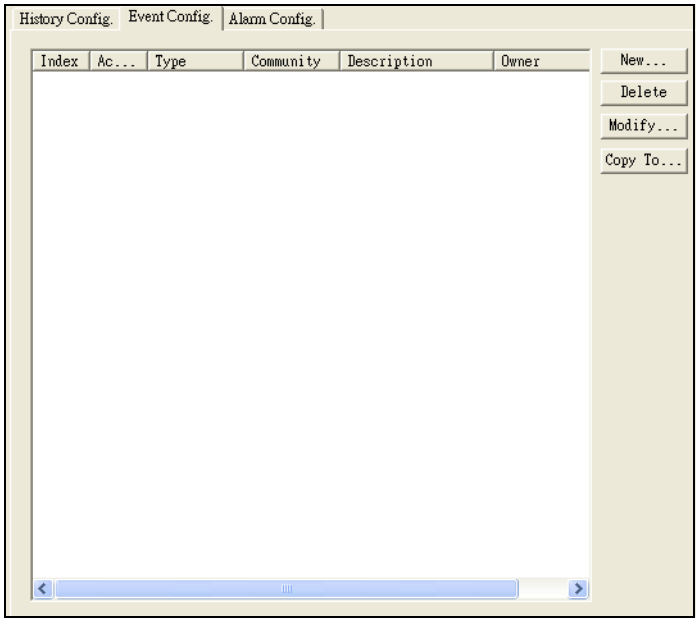
LABEL	DESCRIPTION
Active	Select **Yes** to enable this rule. Select **No** to disable this rule.
Data Source	Select the interface (/port) of the device that the Pro EMS polls for data. The probe sends data from this interface. **ifIndex.1**, for example, means port 1.
Interval	Enter the time (in seconds) between data samplings.
Bucket Requested	Specify the number of data samplings (between 1 and 1500) the network manager requests the probe to store.
Owner	Enter a descriptive name of the application that creates this entry. You can use 1-31 printable characters. Spaces are allowed.
OK	Click this to save the settings and close this screen.
Cancel	Click this to discard all changes and exit this screen.

2.12.3 The Event Config Screen

Use this screen to configure events. An event is the action a selected device takes when an alarm is triggered. You will need the settings of this screen when configuring the **Tools** > **RMON Configuration** > **Alarm Config** screen.

Select the **Event Config** tab in the **Tools** > **RMON Configuration** screen, the screen appears as shown next.

Figure 40 Tool > RMON Configuration > Event Config



The following table describes the labels in this screen.

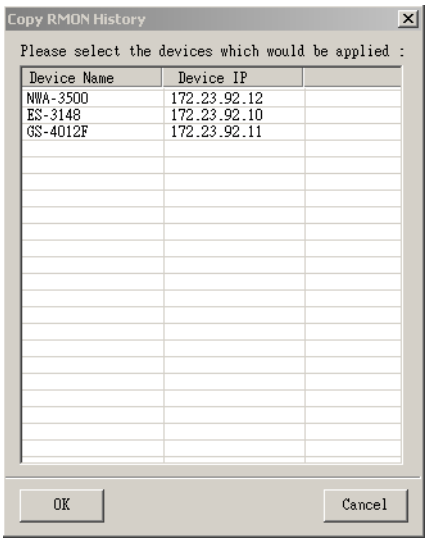
Table 24 Tools > RMON Configuration > Event Config

LABEL	DESCRIPTION
Index	This field displays the configuration index number.
Active	This field displays **Yes** if the event setting is enabled. Otherwise, it displays **No**.
Type	This field displays the event type (**log**, **snmp-trap** or **log&trap**).
Community	This field displays the community (or password).
Description	This field displays a description of the event.
Owner	Enter a descriptive name of the application that creates this entry.
New	Click this to add a new event configuration.
Delete	Click this to remove the selected event configuration.

Table 24 Tools > RMON Configuration > Event Config (continued)

LABEL	DESCRIPTION
Modify	Click this to change the setting of the selected event configuration.
Copy To	Select one or multiple event(s) and then click this to copy it or them to another device. The screen appears as shown next.

Table 25 Copy To



Select one or multiple device(s) to where you want to duplicate the event configuration. Click **OK** to save the changes. Otherwise, click **Cancel** to discard all changes and exit this screen.

2.12.4 RMON Event Configuration Screens

Use these screens to configure RMON events.

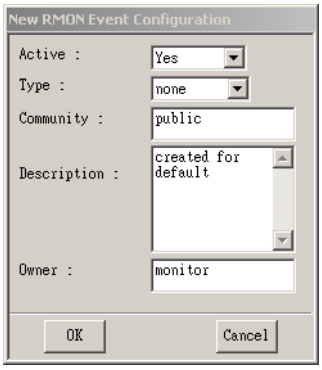
- **New RMON Event Configuration**

This screen appears when you set up a new RMON event. To open this screen, select **Tools** > **RMON Configuration** > **Event Config** > **New**. This screen appears in Figure 41 on page 78.

- **Modify RMON Event Configuration**

This screen appears when you edit an existing RMON event. To open this screen, select **Tools** > **RMON Configuration** > **Event Config**. Then, select the RMON event you want to edit, and click **Modify**. This screen is similar to the one below.

Figure 41 Tools > RMON Configuration > Event Config > New



The following table describes the labels in this screen.

Table 26 Tools > RMON Configuration > Event Config > New

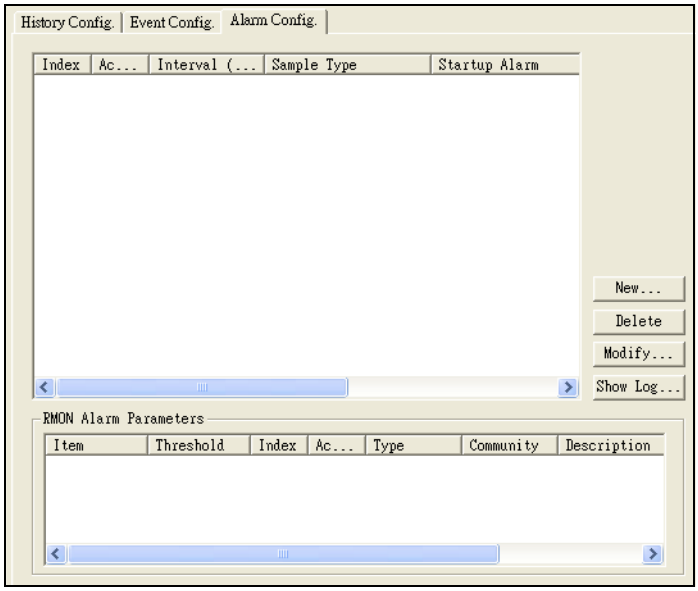
LABEL	DESCRIPTION
Active	Select **Yes** to enable this event. Otherwise, select **No**.
Type	Select an event type. Choices are **none**, **log, snmp-trap** and **log&trap**. Select **none** to not take any action when an associated alarm is generated. Select **Log** to generate a log when an associated alarm is generated. Select **snmp-trap** to send a trap when an associated alarm is generated. Select **log**&**trap** to generate a log entry and send a trap when an associated alarm is generated.
Community	This field displays the community (or password). You can use 1-31 printable ASCII characters. Spaces are allowed.
Description	Enter a description of the event. You can use 1-127 printable ASCII characters. Spaces are allowed. You can also leave this field blank.
Owner	Enter a descriptive name of the application that creates this entry. You can use 1-31 printable ASCII characters. Spaces are allowed.
OK	Click this to save the settings and close this screen.
Cancel	Click this to discard all changes and close the screen.

2.12.5 The Alarm Config Screen

Use this tab screen to configure alarms that occur when the sampled data exceeds the specified threshold. You have to at least create one event configuration in the **Tools** > **RMON Configuration** > **Event Config** screen before configuring an alarm.

Select the **Alarm Config** tab in the **Tools** > **RMON Configuration** screen, the screen appears as shown next.

Figure 42 Tools > RMON Configuration > Alarm Config



The following table describes the labels in this screen.

Table 27 Tools > RMON Configuration > Alarm Config

LABEL	DESCRIPTION
Index	This field displays the alarm configuration index number.
Active	This field displays **Yes** if an alarm configuration is enabled. Otherwise, it displays **No**.
Interval (sec)	This field displays the time interval (in seconds) between data samplings.
Sample Type	This field displays the method of obtaining the sample value. • **Absolute**: This means the sampling value is accumulated since it started. • **Delta**: This means the value is from the data sampled in each configured time interval.
Startup Alarm	This field displays the alarm type that can be sent when this alarm is first activated. • **Rising**: This means the probe triggers an alarm when a value that is greater or equal to the configured rising threshold. • **Falling**: This means the probe triggers an alarm when a value that is smaller or equal to the configured falling threshold. • **R/F**: This means Rising or Falling. That is, the probe triggers an alarm when either one of the above cases occur. Note: You can configure the rising and falling thresholds in the **Tools** > **RMON Configuration** > **Alarm Config** > **New** or **Modify** screen.
Port	This field displays the port number.
Variable	This field displays the name of the MIB field whose data is to be sampled.

Table 27 Tools > RMON Configuration > Alarm Config (continued)

LABEL	DESCRIPTION
Owner	This field displays the name of the application that creates this entry.
New	Click this to add a new alarm configuration.
Delete	Click this to remove the selected alarm configuration.
Modify	Click this to change the setting of the selected alarm configuration.
Show Log	Click this to view logs. You can see logs only when an alarm is triggered.
RMON Alarm Parameters	
Item	This field displays the index number of an alarm entry.
Threshold	This field displays the threshold value that indicates when the device should send an alarm.
Index	This field displays the event index number.
Active	This field display whether an alarm is enabled (**Yes**) or not (**No**).
Type	This field displays the alarm type (**log**, **snmp-trap** or **log&trap**).
Community	This field displays the community (or password).
Description	This field displays a description of the alarm.
Owner	This field displays the name of the application that creates this entry.

2.12.6 RMON Alarm Screens

Use these screens to configure RMON alarms.

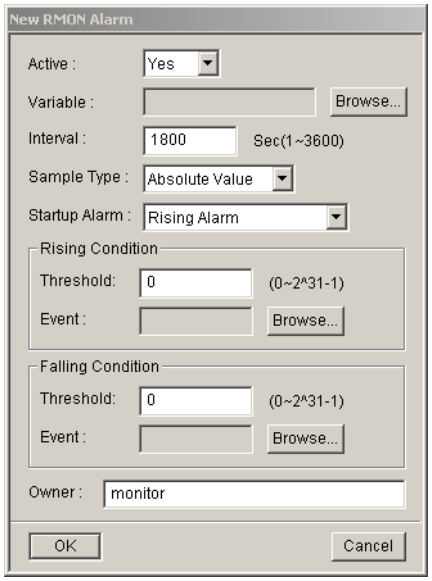
- **New RMON Alarm**

This screen appears when you set up a new RMON alarm. To open this screen, select **Tools** > **RMON Configuration** > **Alarm Config** > **New**. This screen appears in Figure 43 on page 81.

- **Modify RMON Alarm**

This screen appears when you edit an existing RMON alarm. To open this screen, select **Tools** > **RMON Configuration** > **Alarm Config**. Then, select the RMON alarm you want to edit, and click **Modify**. This screen is similar to the one below.

Figure 43 Tools > RMON Configuration > Alarm Config > New



The following table describes the labels in this screen.

Table 28 Tools > RMON Configuration > Alarm Config > New

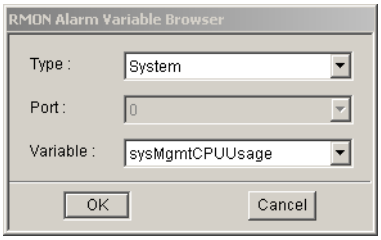
LABEL	DESCRIPTION
Active	Select **Yes** to enable this alarm. Otherwise, select **No**.
Variable	Click **Browse** to select the variable whose data is sampled. The following screen appears. **Figure 44** Tools > RMON Configuration > Alarm Config > New > Variable Browse  Select the type, port, and variable whose data should be sampled, and click **OK**.
Interval	Specify the time between data samplings in seconds.
Sample Type	Select the method of obtaining the sample value. • **Absolute**: This means the sampling value is accumulated since the data sampling was started. • **Delta**: This means the value is from the data sampled in each configured time interval.

Table 28 Tools > RMON Configuration > Alarm Config > New (continued)

LABEL	DESCRIPTION
Startup Alarm	Select the alarm type that can be sent when this alarm is first activated. • **Rising**: Select this to have the probe trigger an alarm only when a value that is greater or equal to the configured rising threshold. • **Falling**: Select this to have the probe trigger an alarm only when a value that is smaller or equal to the configured falling threshold. • **Rising or Falling Alarm**: Select this to have the probe trigger an alarm when either one of the above cases occur.
Rising Condition	
Threshold	Specify a rising threshold (between 0 and 2147483647). When a value that is greater or equal to this threshold, the probe triggers an alarm.
Event	Click **Browse** to select an index number of a rising event.
Falling Condition	
Threshold	Specify the falling threshold (between 0 and 2147483647). When a value that is smaller or equal to this threshold, the probe triggers an alarm.
Event	Click **Browse** to select an index number of a falling event.
Owner	Enter a descriptive name of the application that creates this entry. You can use 1-31 printable ASCII characters. Spaces are allowed.
OK	Click this to save the settings and close this screen.
Cancel	Click this to discard all changes and exit this screen.

2.12.7 RMON Alarm Event Log Screen

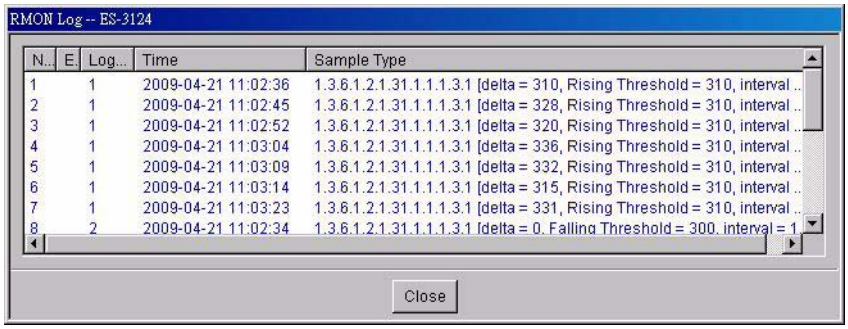
Use this screen to display alarm logs. To see logs in this screen, you have to do the following:

1 Create at least one event configuration profile (in **Tools** > **RMON Configuration** > **Even Config**) and select **log** or **log&trap** for the type.

2 Create a RMON alarm profile (in **Tools** > **RMON Configuration** > **Alarm Config**) with selecting the event configuration profile you just created.

To open this screen, select **Tools** > **RMON Configuration** > **Alarm Config** > **Show Log**. The screen appears as shown next.

Figure 45 Tools > RMON Configuration > Alarm Config > Show Log



The following table describes the labels in this screen.

Table 29 Tools > RMON Configuration > Alarm Config > Show Log

LABEL	DESCRIPTION
No.	This field displays the index number of an entry.
Event Index	This field displays an event index number.
Log Index	This field displays a log index number.
Time	This field displays the time the log was generated.
Sample Type	This field displays the method of obtaining the sample value.
Close	Click this to discard all changes and exit this screen.

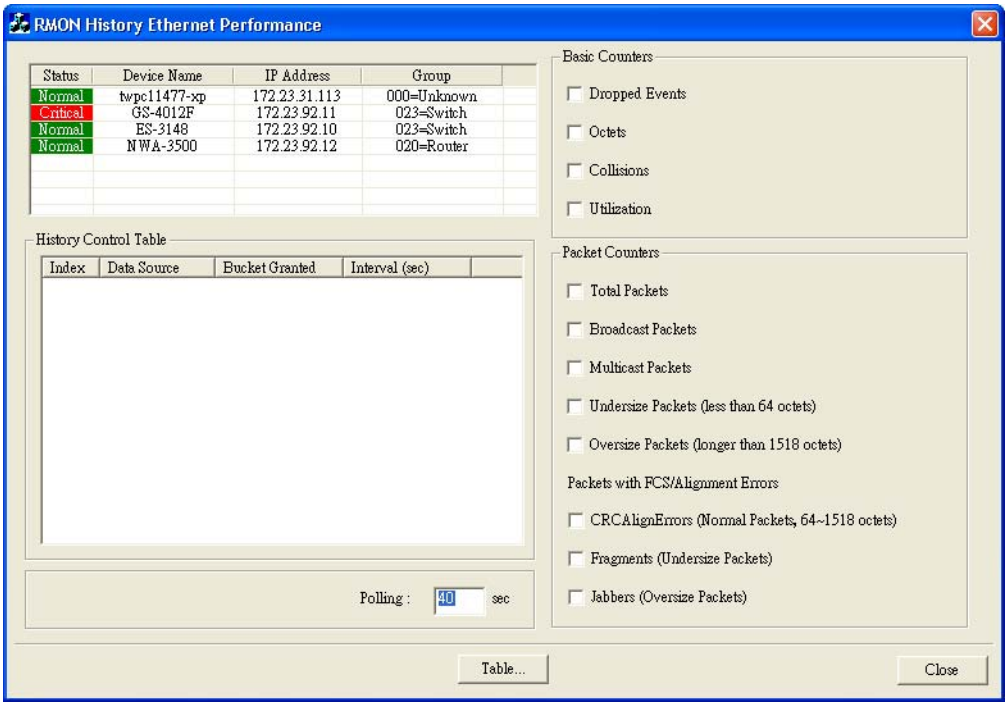
2.13 The RMON Ethernet History Data Screen

Use this menu item to view historical network traffic statistics on an Ethernet port. At the time of writing, only ZyXEL switches support this feature.

Note: You have to create at least one RMON history configuration entry in the **Tools** > **RMON Configuration** > **History Config** screen before using this screen.

Select a managed device. Select **Tools** > **RMON Ethernet History Data** or right-click the managed device and select **Tools** > **RMON Ethernet History Data**. The screen appears as shown next.

Figure 46 Tool > RMON Ethernet History Data



The following table describes the labels in this screen.

Table 30 Tools > RMON Ethernet History Data

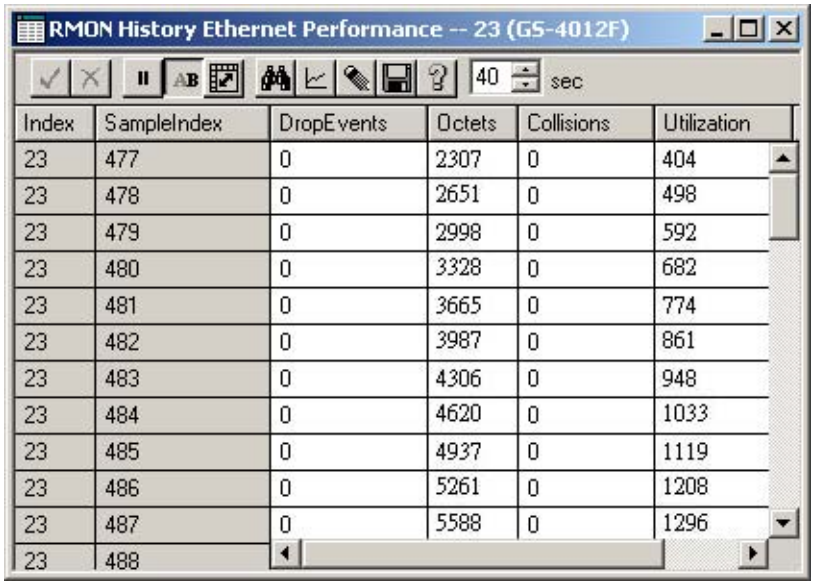
LABEL	DESCRIPTION
Status	This field indicates the presence of a most recent alarm/event log with one of the following severity levels (listed from high to low) on a managed device. • **Critical** • **Severe** • **Major** • **Minor** • **Warning** • **Normal** • **Info**
Device Name	This field displays the name of the device. Select the appropriate managed device.
IP Address	This field displays the IP address of the device.
Group	This field displays the SNMPc group code and name with which the device is associated. See Table 11 on page 54 for more information about the group code.
History Control Table	
Index	This field displays the index number of an entry.
Data Source	This field displays the port of the selected device that the Pro EMS will poll for data.
Bucket Granted	This field displays the number of data samplings the probe allows to store.
Interval (sec)	This field displays the time between data samplings.
Polling	This field displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number.
Basic Counters	
Dropped Events	Select this to display the total number of packets that were dropped.
Octets	Select this to display the total number of octets received.
Collisions	Select this to display the total number of collisions occurred.
Utilization	Select this to display the utilization of the LAN ports.
Packet Counters	
Total Packets	Select this to display the total number of all good packets received.
Broadcast Packets	Select this to display the total number of good broadcast packets received.
Multicast Packets	Select this to display the total number of good multicast packets received.
Undersize Packets (less than 64 octets)	Select this to display the number of packets dropped because they were too short (shorter than 64 octets).

Table 30 Tools > RMON Ethernet History Data (continued)

LABEL	DESCRIPTION
Oversize Packets (longer than 1518 octets)	Select this to display the number of packets dropped because they were too big (bigger than the maximum frame size).
Packets with FCS/ Alignment Errors	Select this to show the number of packets (between 64 ~ 1518 octets long) dropped because they either had bad Frame Check Sequence (FCS) or non-integral number of octets (alignment error).
Fragments (Undersize Packets)	Select this to display the number of frames dropped because they were less than 64 octets long, and contained an invalid FCS, including non-integral and integral lengths.
Jabbers (Oversize Packets)	Select this to display the number of frames dropped because they were longer than 1518 octets (non VLAN) or 1522 octets (VLAN) and contained an invalid FCS, including alignment errors.
Table	Select this to create a table based on the above selection(s).
Close	Click this to exit this screen.

The following figure shows an example of the statistics table.

Figure 47 Tools > RMON Ethernet History Data > Table

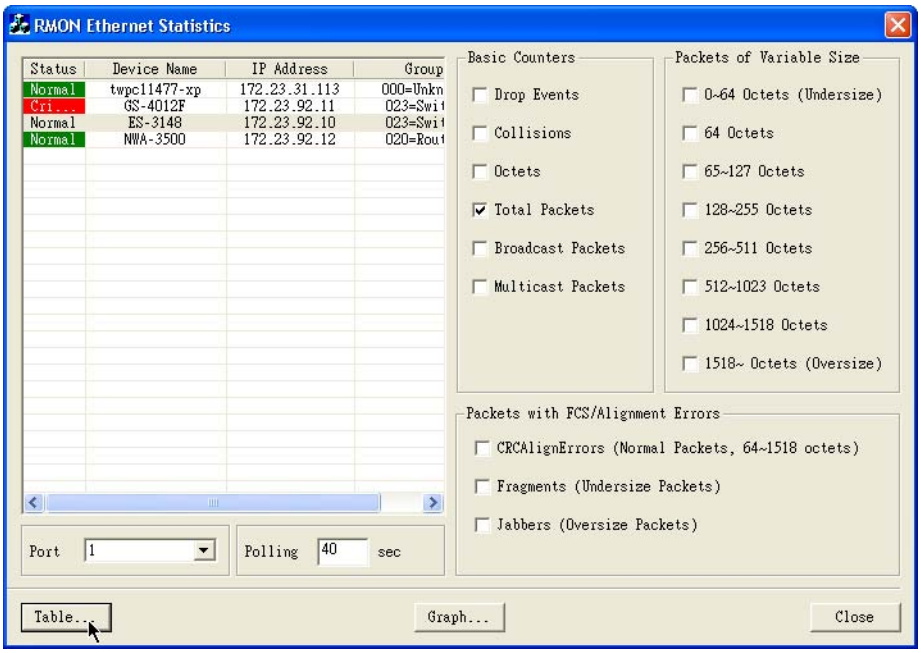


2.14 The RMON Ethernet Statistics Screen

Use this menu item to view the specified current packet statistics on a single port or all ports for the selected device. The statistics can be displayed in a table or in a graph.

Select a managed device. Select **Tools** > **RMON Ethernet Statistics** or right-click the managed device and select **Tools** > **RMON Ethernet Statistics**. The screen appears as shown next.

Figure 48 Tool > RMON Ethernet Statistics



The following table describes the labels in this screen.

Table 31 Tools > RMON Ethernet Statistics

LABEL	DESCRIPTION
Status	This field indicates the presence of a most recent alarm/event log with one of the following severity levels (listed from high to low) on a managed device. • **Critical** • **Severe** • **Major** • **Minor** • **Warning** • **Normal** • **Info**
Device Name	This field displays the name of the device. Select the appropriate managed device.
IP Address	This field displays the IP address of the device.
Group	This field displays the SNMPc group code and name with which the device is associated.
Port	Select **All** Ports or a single port on which you want to view the Ethernet traffic statistics.
Polling	This field displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number.

Table 31 Tools > RMON Ethernet Statistics (continued)

LABEL	DESCRIPTION
Basic Counters	
Drop Events	Select this to display the total number of packets that were dropped.
Collisions	Select this to display the total number of collisions occurred.
Octets	Select this to show the total number of octets received or transmitted.
Total Packets	Select this to display the total number of all good packets received.
Broadcast Packets	Select this to show the total number of broadcast packets received or transmitted.
Multicast Packets	Select this to show the total number of multicast packets received or transmitted.
Packets of Variable Size	
0~64 Octets (Undersize)	Select this to display the number of packets (including bad packets) received that were between 0 and 64 octets in length.
64 Octets	Select this to display the number of packets (including bad packets) received that were 64 octets in length.
65~127 Octets	Select this to display the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128~255 Octets	Select this to display the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256~511 Octets	Select this to display the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512~1023 Octets	Select this to display the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024~1518 Octets	Select this to display the number of untagged packets (including bad packets) received that were between 1024 and 1518 octets in length. This number also includes tagged packets received that were 1522 octets in size.
1518~ Octets (Oversize)	Select this to display the number of untagged packets (including bad packets) received that were greater than 1518 octets in length.
Packets with FCS/Alignment Errors	
CRCAlignErrors (Normal Packets, 64~1518 octets)	Select this to display the number of packets (between 64 ~ 1518 octets long) dropped because they had non-integral number of octets (alignment error).
Fragments (Undersize Packets)	Select this to display the number of frames dropped because they were less than 64 octets long, and contained an invalid FCS, including non-integral and integral lengths.
Jabbers (Oversize Packets)	Select this to display the number of frames dropped because they were longer than 1518 octets and contained an invalid FCS, including alignment errors.
Table	Select this to create a table based on the above selection(s).
Graph	Select this to create a graph based on the above selection(s).
Close	Click this to discard all changes and exit this screen.

The following figures are examples of displaying RMON Ethernet statistics in a graph and in a table.

Figure 49 Tools > RMON Ethernet Statistics > Graph

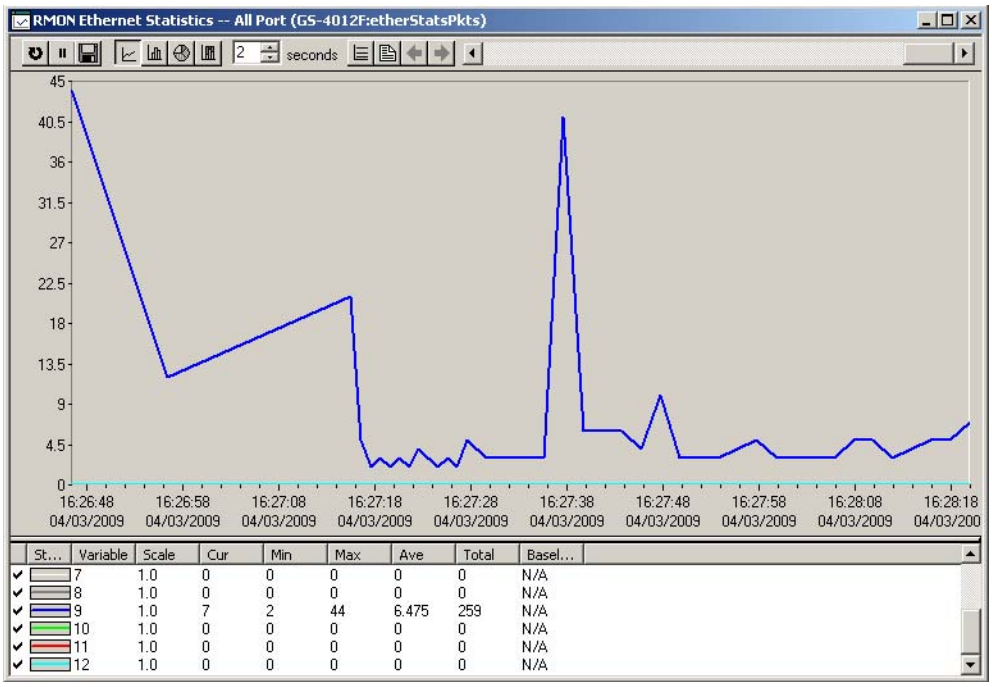
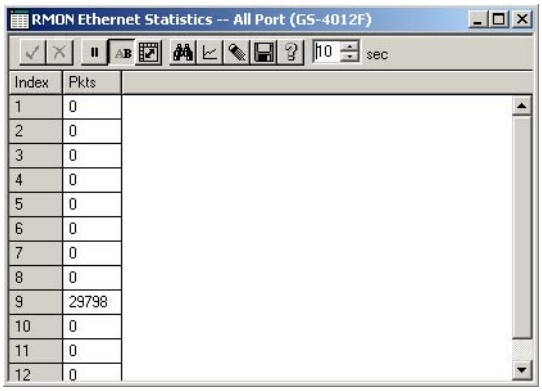


Figure 50 Tools > RMON Ethernet Statistics > Table

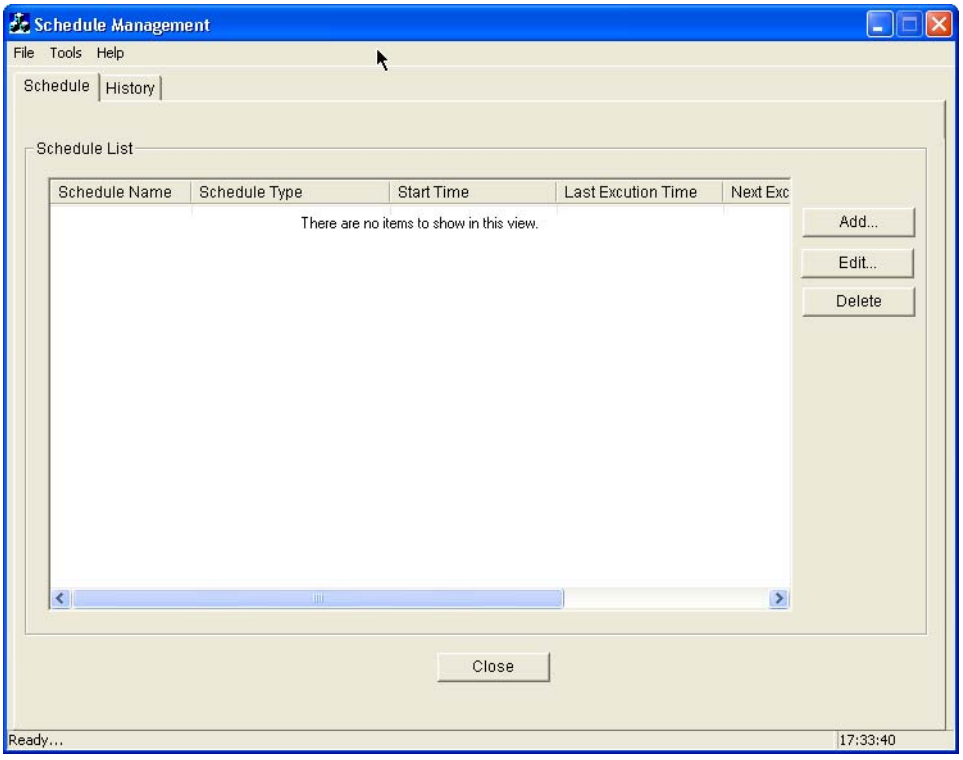


2.15 The Schedule Management Screen

Use this menu item to create schedules for firmware upgrade and configuration file backup and restore.

Select a managed device. Select **Tools** > **Schedule Management** or right-click the managed device and select **Tools** > **Schedule Management**. The screen appears as shown next.

Figure 51 Tool > Schedule Management



The following table describes the labels in this screen.

Table 32 Tools > Schedule Management

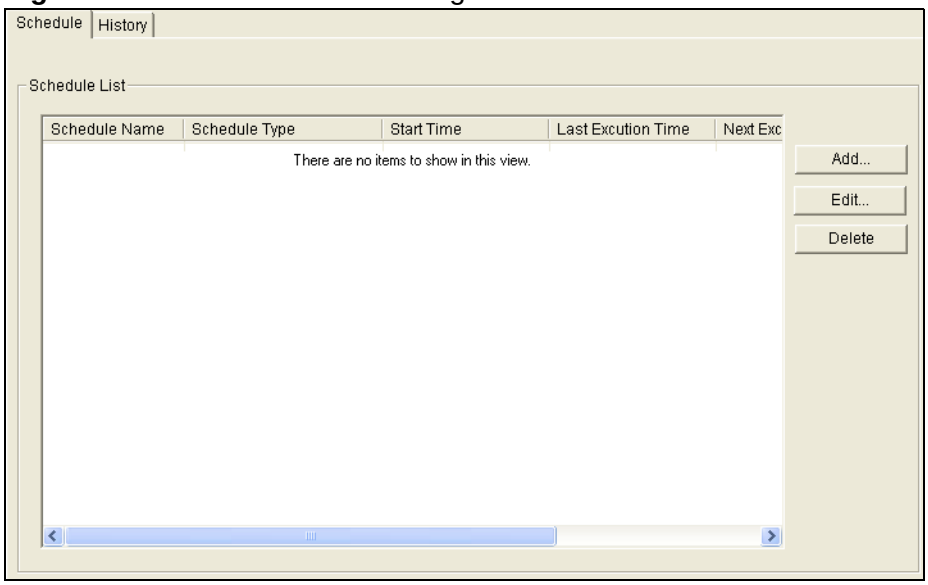
LABEL	DESCRIPTION
File	
Exit	Select this to exit this screen.
Tools	
Options	Select this to remove the selected entries.
Help	
About Schedule Management	Select this to view the copyright information of this schedule management feature.
Schedule	Use this tab screen to view or configure your scheduled tasks such as backing up the configure file or upgrading the firmware version according to a schedule.
History	Use this tab screen to view or manage your schedules tasks that have been completed.
Close	Click this to discard all changes and exit this screen.

2.15.1 The Schedule Screen

This screen provides a summary list after you create scheduled task(s) by clicking **Add** in this screen.

Select the **Schedule** tab in the **Tools** > **Schedule Management** screen, the screen appears as shown next.

Figure 52 Tool > Schedule Management > Schedule



The following table describes the labels in this screen.

Table 33 Tools > Schedule Management > Schedule

LABEL	DESCRIPTION
Schedule List	
Schedule Name	This field displays the name of a scheduled task.
Schedule Type	This field displays the type of the scheduled task.
Start Time	This field displays the date and time the scheduled task starts. This is based on the current date and time on the computer on which the Pro EMS, not based on the current date and time of the device(s).
Last Execution Time	This field displays the date and time the scheduled task last starts. **N / A** displays when the task has not started yet.
Next Execution Time	This field displays the date and time the scheduled task starts. **N / A** displays when the task has been completed.
Frequency	This field displays how often the Pro EMS performs the task.
Path	This field displays the full path of a file associated or used in this task.
Add	Click this to create a new task based on a schedule.

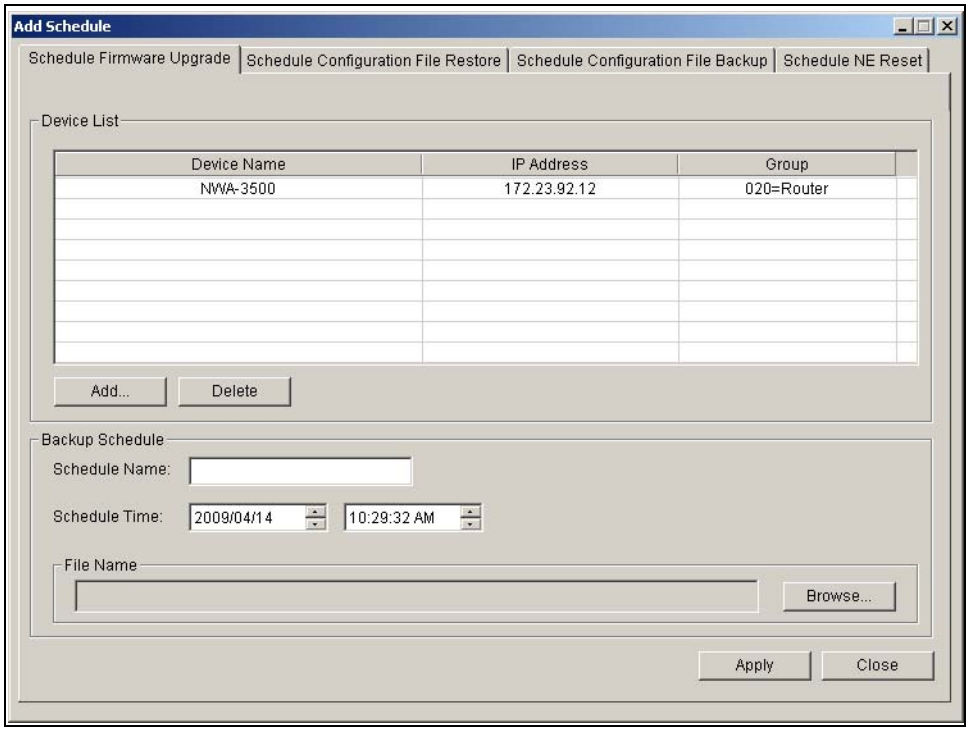
Table 33 Tools > Schedule Management > Schedule (continued)

LABEL	DESCRIPTION
Edit	Select a task and click this to modify it. Use this tab screen to view or manage your schedules tasks that have been completed.
Delete	Click this to remove the selected task(s).

2.15.1.1 The Schedule Firmware Upgrade Screen

Select **Add** in the **Tools** > **Schedule Management** > **Schedule** screen, the screen appears as shown next.

Figure 53 Tool > Schedule Management > Schedule > Add > Schedule Firmware Upgrade



The following table describes the labels in this screen.

Table 34 Tools > Schedule Management > Schedule > Add > Schedule Firmware Upgrade

LABEL	DESCRIPTION
Device List	
Device Name	This field displays the name of a device.
IP Address	This field displays the IP address of the device.
Group	This field displays the group with which the device is associated.
Add	Click this to add a device into the device list table.
Delete	Click this to remove an entry from the table.
Backup Schedule	

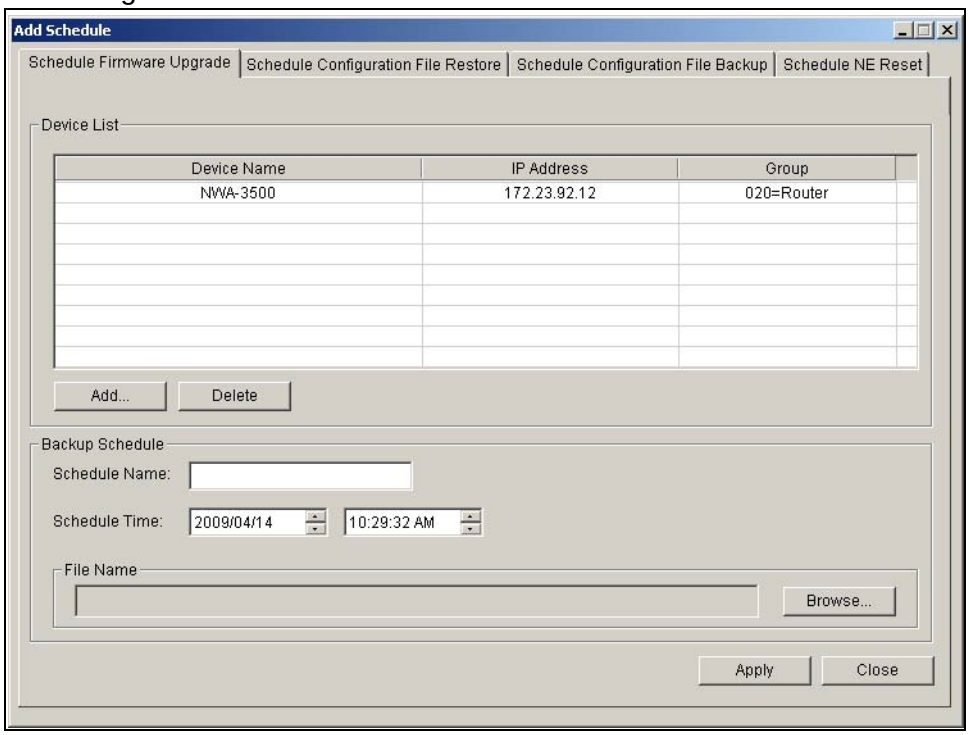
Table 34 Tools > Schedule Management > Schedule > Add > Schedule Firmware Upgrade (continued)

LABEL	DESCRIPTION
Schedule Name	Type up to 32 printable ASCII characters for the name of the scheduled task.
Schedule Time	Select the date and time the scheduled task starts. This is based on the current date and time on the computer on which the Pro EMS, not based on the current date and time of the device(s).
File Name	Click **Browse** to locate the firmware file that will be uploaded to the selected device(s)
Apply	Click this to save the change.
Close	Click this to discard all changes and exit this screen.

2.15.1.2 The Schedule Configuration File Restore Screen

Select **Schedule Configuration File Restore** in the **Tools** > **Schedule Management** > **Schedule** > **Add** screen, the screen appears as shown next.

Figure 54 Tool > Schedule Management > Schedule > Add > Schedule Configuration File Restore



The following table describes the labels in this screen.

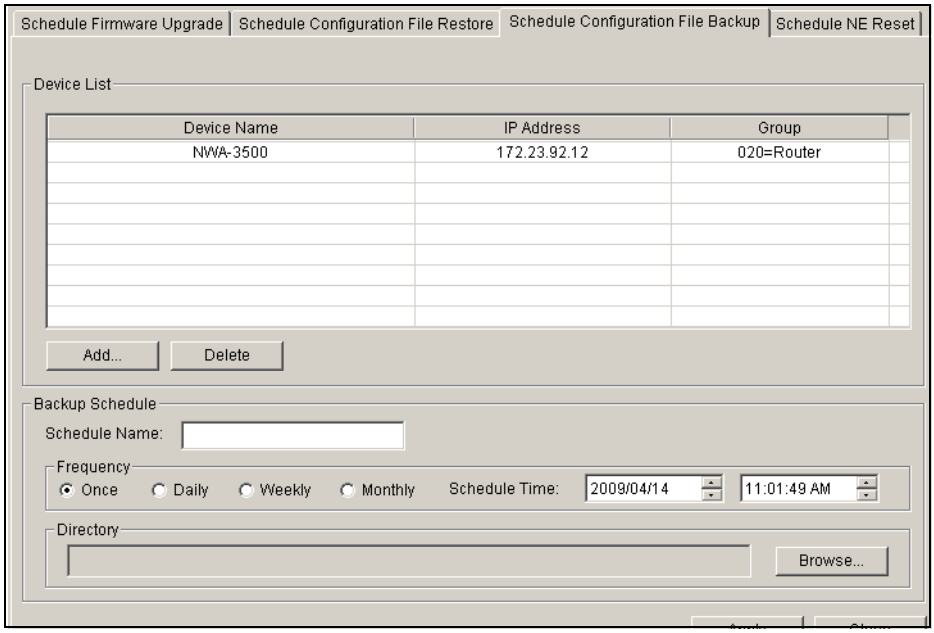
Table 35 Tools > Schedule Management > Schedule > Add > Schedule Configuration File Restore

LABEL	DESCRIPTION
Device List	
Device Name	This field displays the name of a device.
IP Address	This field displays the IP address of the device.
Group	This field displays the group with which the device is associated.
Add	Click this to add a device into the device list table.
Delete	Click this to remove an entry from the table.
Backup Schedule	
Schedule Name	Type up to 32 printable ASCII characters for the name of the scheduled task.
Frequency	Select how often to schedule firmware backup tasks for the selected device. Scheduled firmware upgrade can be performed **once**, **Daily**, **Weekly** or **Monthly**.
Schedule Time	Select the date and time the scheduled task starts. This is based on the current date and time on the computer on which the Pro EMS, not based on the current date and time of the device(s).
File Name	Click **Browse** to locate the firmware file that will be uploaded to the selected device(s)
Apply	Click this to save the change.
Close	Click this to discard all changes and exit this screen.

2.15.1.3 The Schedule Configuration File Backup Screen

Select **Schedule Configuration File Backup** in the **Tools** > **Schedule Management** > **Schedule** > **Add** screen, the screen appears as shown next.

Figure 55 Tool > Schedule Management > Schedule > Add > Schedule Configuration File Backup



The following table describes the labels in this screen.

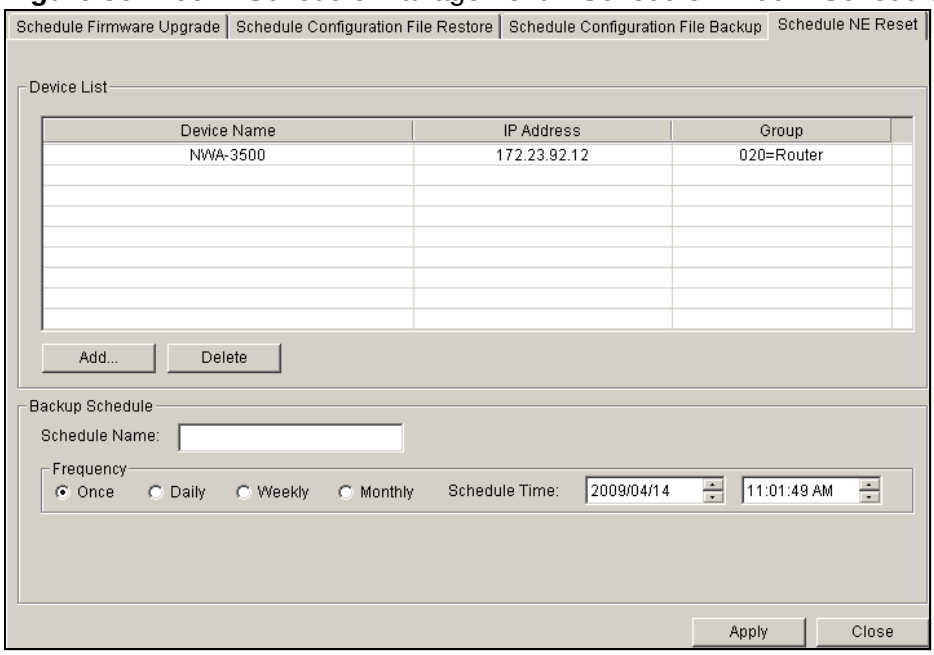
Table 36 Tools > Schedule Management > Schedule > Add > Schedule Configuration File Backup

LABEL	DESCRIPTION
Device List	
Device Name	This field displays the name of a device.
IP Address	This field displays the IP address of the device.
Group	This field displays the group with which the device is associated.
Add	Click this to add a device into the device list table.
Delete	Click this to remove an entry from the table.
Backup Schedule	
Schedule Name	Type up to 32 printable ASCII characters for the name of the scheduled task.
Schedule Time	Select the date and time the scheduled task starts.
Directory	Click **Browse** to locate the directory to which the Pro EMS will download the configuration file.
Apply	Click this to save the change.
Close	Click this to discard all changes and exit this screen.

2.15.1.4 The Schedule Configuration File Backup Screen

Select **Schedule NE Reset** in the **Tools** > **Schedule Management** > **Schedule** > **Add** screen, the screen appears as shown next.

Figure 56 Tool > Schedule Management > Schedule > Add > Schedule NE Reset



The following table describes the labels in this screen.

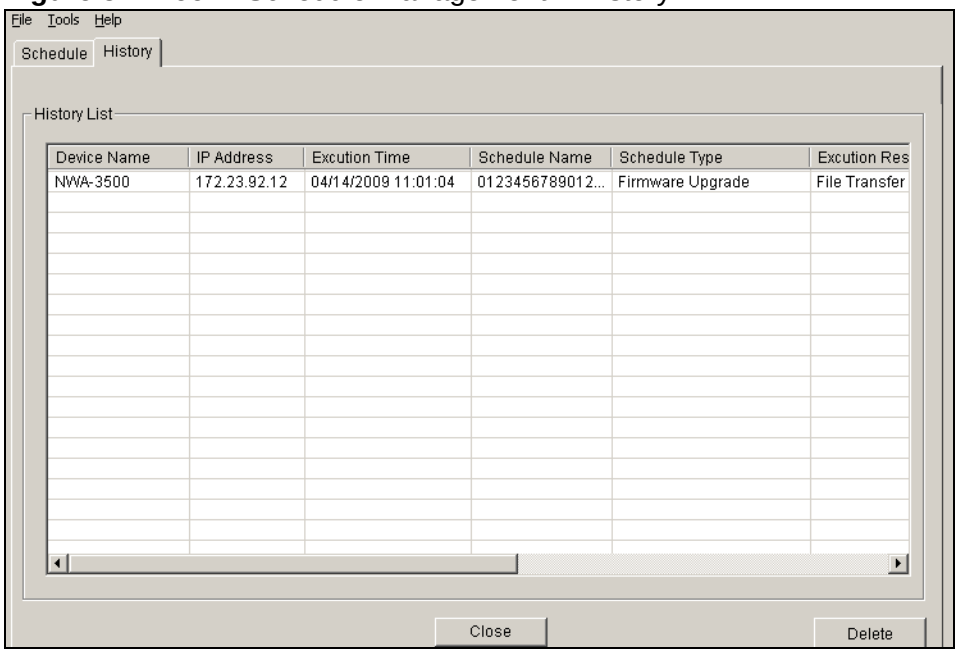
Table 37 Tools > Schedule Management > Schedule > Add > Schedule Configuration File Backup

LABEL	DESCRIPTION
Device List	
Device Name	This field displays the name of a device.
IP Address	This field displays the IP address of the device.
Group	This field displays the group with which the device is associated.
Add	Click this to add a device into the device list table.
Delete	Click this to remove an entry from the table.
Backup Schedule	
Schedule Name	Type up to 32 printable ASCII characters for the name of the scheduled task.
Schedule Time	Select the date and time the scheduled task starts.
Frequency	Select how often to schedule firmware backup tasks for the selected device. Scheduled firmware upgrade can be performed **once**, **Daily**, **Weekly** or **Monthly**.
Apply	Click this to save the change.
Close	Click this to discard all changes and exit this screen.

2.15.2 The History Screen

Select the **History** tab in the **Tools** > **Schedule Management** screen, the screen appears as shown next.

Figure 57 Tool > Schedule Management > History



The following table describes the labels in this screen.

Table 38 Tools > Schedule Management > History

LABEL	DESCRIPTION
History List	
Device Name	This field displays the name of a device related to a scheduled task.
IP Address	This field displays the IP address of the device.
Execution Time	This field displays the date and time the scheduled task was last time started.
Schedule Name	This field displays the date and time when the scheduled task last starts.
Schedule Type	This field displays the type of the scheduled task.
Execution Result	This field displays the result of this scheduled task.
Device Group	This field displays the group with which the device is associated.
Download File	This field displays the file path and name downloaded from the device. **N/A** displays if there is no any file downloaded in this task.
Close	Click this to discard all changes and exit this screen.
Delete	Click this to remove the selected task(s).

2.16 The Script Distribution screen

A script is a batch file of commands that can be sent to one or more devices. Use this menu item to write a script and execute it on specified device(s). You can save the script to a file for using it again in the future. This screen and view the result of executing the script.

One failed or invalid command does not stop a script. For example, if you upload a script to a device. The script contains 10 commands. Although the third command fails to execute, however, the script will continue to execute the rest of commands. Another example, if you upload a script to 10 devices and device 6 fails (maybe it's off), it will continue to devices 7,8,9 and 10.

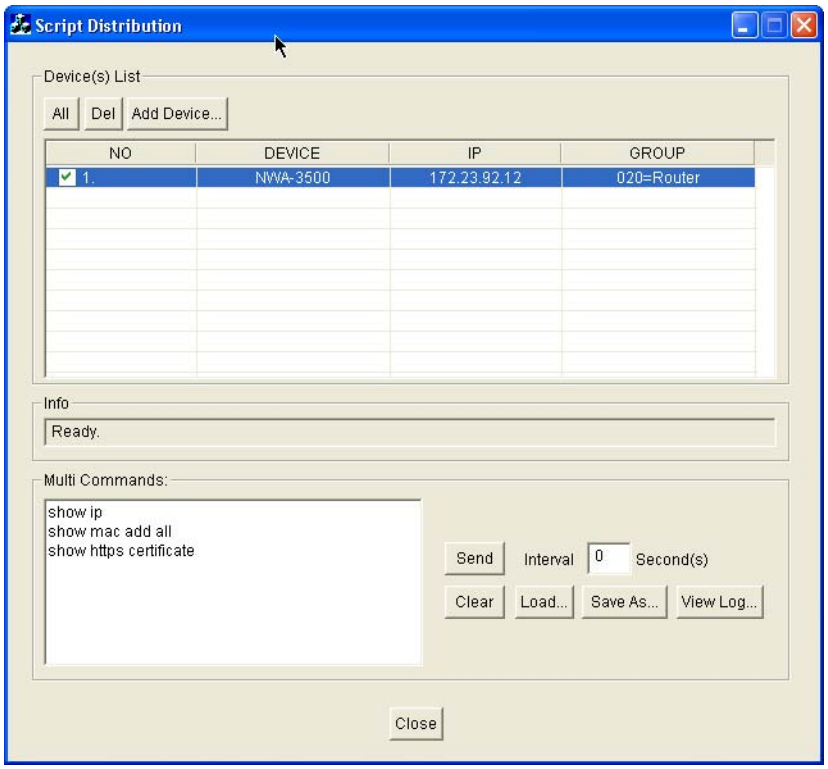
You must make sure the commands are supported by the device.

For Ethernet Switchs, you may refer to its command line reference guide. Telnet to an Ethernet Switch and log into the command line interface and type “?” to view all commands supported by the device.

For Access Points, telnet to an Access Point and log into the command line interface and type “help” to view all commands supported by the device.

Select a managed device. Select **Tools** > **Script Distribution** or right-click the managed device and select **Tools** > **Script Distribution**. The screen appears as shown next.

Figure 58 Tool > Script Distribution

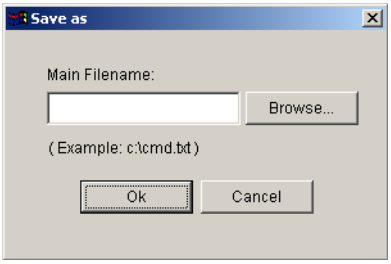


The following table describes the labels in this screen.

Table 39 Tools > Script Distribution

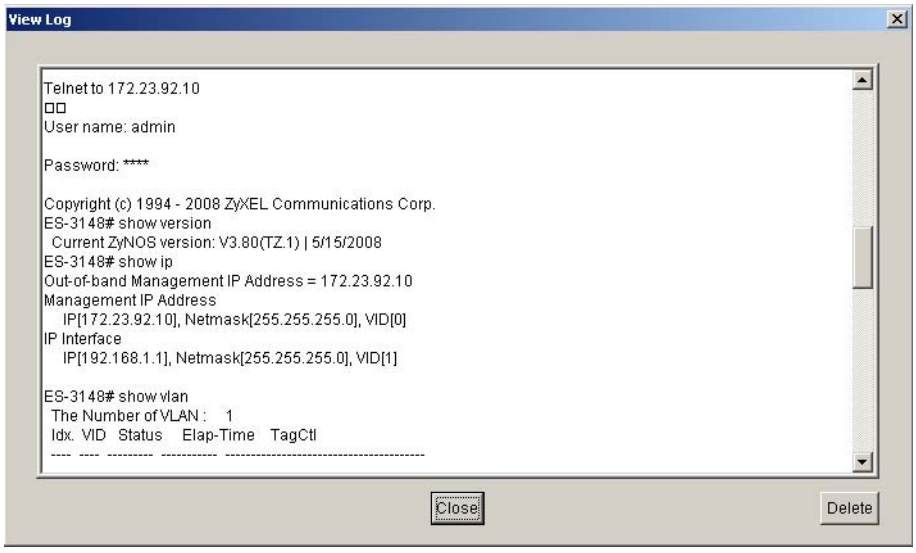
LABEL	DESCRIPTION
Device(s) List	
All	Click this to select or clear all entries in the table below.
Del	Click this to remove the selected entry or entries in the table below.
Add Device	Click this to add more device entries in the table below.
NO	This field displays the index number of an entry. Select one or more devices to which you want to send commands in this screen. This field displays **Running** when the Pro EMS is executing the specified commands on the selected device. This field displays **OK** when a script has been successfully executed on the selected device. This field displays **FAILED** when a script was failed to execute on the selected device.
DEVICE	This field displays the name of a device.
IP	This field displays the IP address of the device.

Table 39 Tools > Script Distribution (continued)

LABEL	DESCRIPTION
GROUP	This field displays the group with which the device is associated.
Info	This field displays status for the specified script uploading.
Multi Commands	Type one of multiple command(s) you want to execute on the selected device(s). Press [Enter] to separate two commands.
Send, Interval .. Second(s)	Enter the number of seconds and click **Send** to send the specified command(s) to the selected device(s) after the specified time interval. Enter **0** and click **Send** if you want to send the commands immediately.
Clear	Click this to clear the command(s) in the **Multi Commands** field.
Load	Click this to load a script file from your computer and display the content in the **Multi Commands** field.
Save As	Click this to save the command(s) to a file in your computer where the Pro EMS is running if you want to use it again in the future. The screen appears as shown next. **Table 40** Save As  Enter the full path of a file to which you want to save the script or click **Browse** to locate it. Click **OK** to save the file. Otherwise, click **Cancel** to exit this screen.
View Log	Click this to display the logs of scripts you executed recently. See Figure 59 on page 100.
Close	Click this to discard all changes and exit this screen.

The following figure shows an example of the **View Log** screen. You can click **Delete** to clear all logs. Click **Close** to exit this screen.

Figure 59 Tools > Script Distribution > View Log

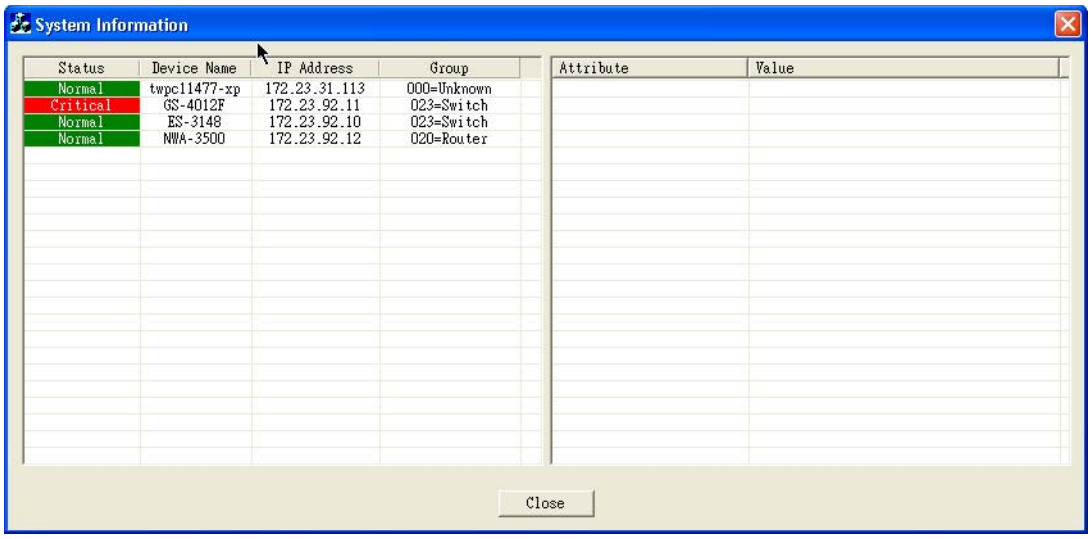


2.17 The System Information Screen

Use this menu item to view system information such as firmware version and serial number for the managed devices.

Select a managed device. Select **Tools** > **System Information** or right-click the managed device and select **Tools** > **System Information**. The screen appears as shown next.

Figure 60 Tool > System Information



The following table describes the labels in this screen.

Table 41 Tools > System Information

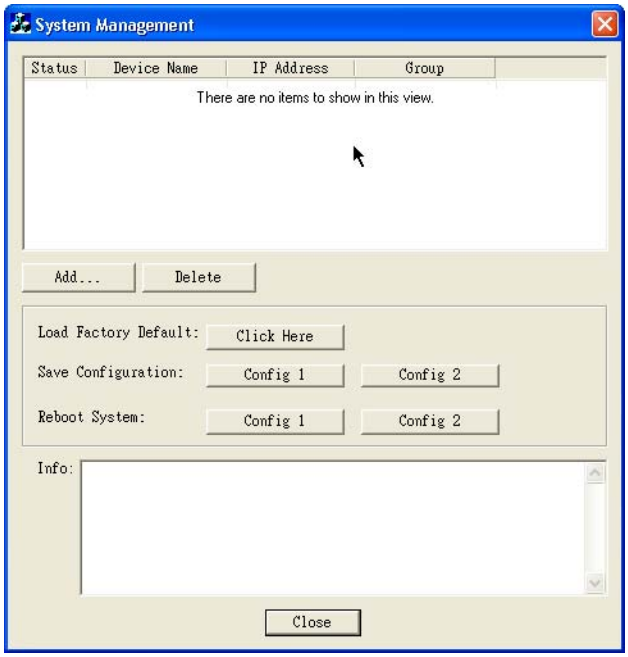
LABEL	DESCRIPTION
Status	This field indicates the presence of a most recent alarm/event log with one of the following severity levels (listed from high to low) on a managed device. • **Critical** • **Severe** • **Major** • **Minor** • **Warning** • **Normal** • **Info**
Device Name	This field displays the name of the device. Select the appropriate managed device.
IP Address	This field displays the IP address of the device.
Group	This field displays the SNMPc group code and name with which the device is associated.
Attribute	Select a managed device from the left to have this field display the available attributes for it.
Value	This field displays the information of an attribute for the managed device.
Close	Click this to exit this screen.

2.18 The System Management Screen

Use this menu item to view the system information or perform basic system maintenance (such as load factory defaults and reboot the system) for the managed devices.

Select a managed device. Select **Tools** > **System Management** or right-click the managed device and select **Tools** > **System Management**. The screen appears as shown next.

Figure 61 Tools > System Management



The following table describes the labels in this screen.

Table 42 Tools > System Management

LABEL	DESCRIPTION
Status	This field displays the status of each managed devices that you may use in this screen.
Device Name	This field displays the name of the managed devices. Select the appropriate managed device.
IP Address	This field displays the IP address of the device.
Group	This field displays the SNMPc group code and name to which the device currently belongs.
Add	Click this to add managed device(s) to this table.
Delete	Select one or multiple entries and then click this to remove them from the table.
Load Factory Default	Select one or multiple entries and then click **Click Here** to load their factory defaults.

Table 42 Tools > System Management (continued)

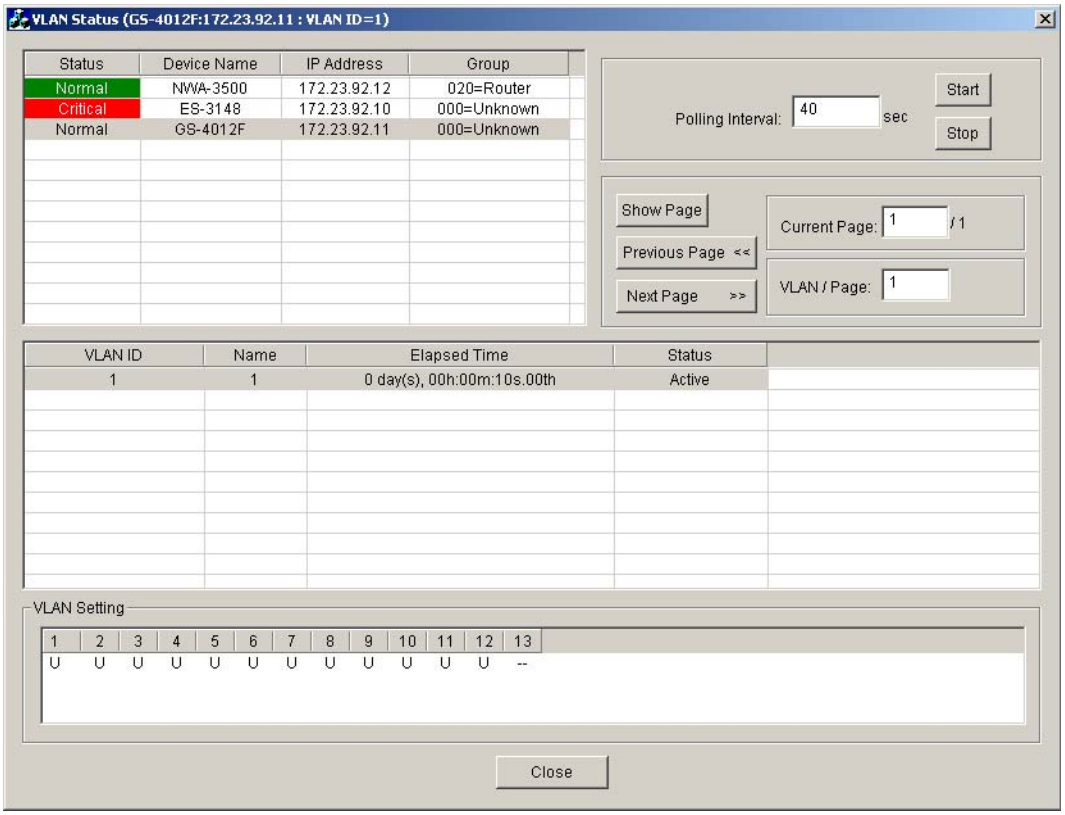
LABEL	DESCRIPTION
Save Configuration	Select one or multiple entries and then click **Config 1** or **Config 2**. This specifies to which configuration file the device should save the running configuration. Note: At the time of writing, not all devices support dual configuration files that allow you to store different settings in different files, rom-0 and rom-1. Check your device User's Guide for the related information.
Reboot System	Select one or multiple entries and then click **Config 1** or **Config 2**. This specifies which configuration file the managed device should use when next time it boots up.
Info	This field displays whether the actions were successful or failed that you performed in the screen.
Close	Click this to discard all changes and exit this screen.

2.19 The VLAN Status Screen

Use this menu item to view the current VLAN status of a managed device.

Select a managed device. Select **Tools** > **VLAN Status** or right-click the managed device and select **Tools** > **VLAN Status**. The screen appears as shown next.

Figure 62 Tool > VLAN Status



The following table describes the labels in this screen.

Table 43 Tools > VLAN Status

LABEL	DESCRIPTION
Status	This field indicates the presence of a most recent alarm/event log with one of the following severity levels (listed from high to low) on a managed device. • **Critical** • **Severe** • **Major** • **Minor** • **Warning** • **Normal** • **Info**
Device Name	This field displays the name of the device. Select the appropriate managed device.
IP Address	This field displays the IP address of the device.
Group	This field displays the SNMPc group code and name with which the device is associated.

Table 43 Tools > VLAN Status (continued)

LABEL	DESCRIPTION
Polling Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Start**. Click **Stop** to halt statistic polling.
Show Page	Click this to display the page that you entered in the **Current Page** field.
Previous Page	Click this to display the previous page of the one that you entered in the **Current Page** field.
Next Page	Click this to display the next page of the one that you entered in the **Current Page** field.
Current Page	This field displays the page currently displayed in the table located in the middle of the screen.
VLAN / Page	This field displays the maximum number of VLANs can be displayed in one page.
VLAN ID	This is the VLAN identification number of a VLAN on the selected device.
Name	This field displays the descriptive name of the VLAN.
Elapsed Time	This field displays how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows status of the VLAN.
VLAN Setting	Select an appropriate VLAN from the table located in the middle of the screen to display the VLAN settings on ports here. A tagged port is marked as **T**, and untagged port is marked as **U** and port not participating in a VLAN are marked as "**-**".
Close	Click this to exit this screen.

3

Troubleshooting

3.1 Overview

This chapter offers some suggestions on how to solve problems you might encounter. The potential problems are divided into the following categories.

- Pro EMS Installation
- Pro EMS Access and Login
- Device Management

3.2 Pro EMS Installation

I failed to install Pro EMS.

- Make sure you're logged in as the Windows administrator on the computer on which you're installing Pro EMS.
- Make sure your computer meets the Pro EMS system requirements. See Section 1.1.4 on page 17.

The computer on which I installed Pro EMS crashed and is not usable.

1 Install Pro EMS on another computer that has SNMPc already installed. You may have to add all devices and configure them again.

3.3 Pro EMS Access and Login

I forgot the password.

1 The default password of the **Administrator** account is blank.

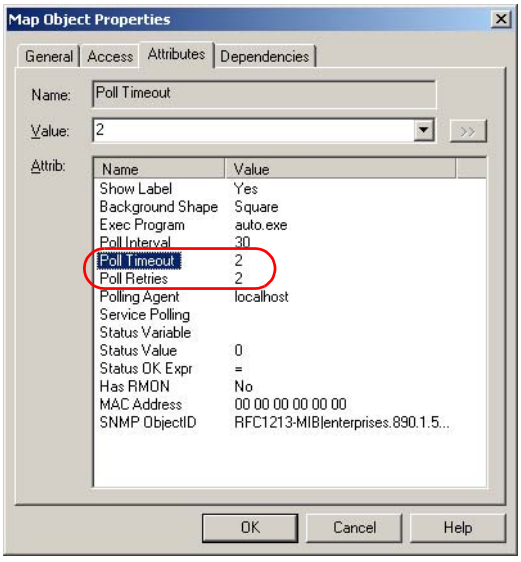
2 If you are the administrator and you forget your password, you cannot log into the Pro EMS any more. Uninstall Pro EMS and reinstall it. Alternatively, install Pro EMS on another computer.

I see this warning pop-up message: "SNMP Operation Timout".

1 The warning message also instructs you how to check this problem. First, check the timeout setting by right-clicking the device and select **Properties**. Select the **Attributes** tab and then check the **Poll Timeout** and **Poll Retries** settings.

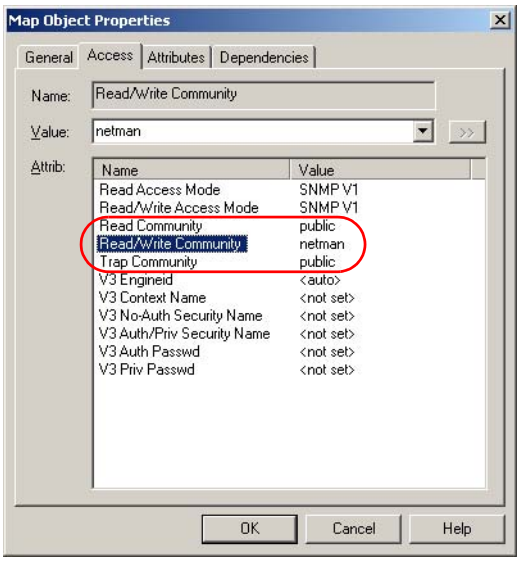
Select **Poll Timeout** and enter the number of seconds Pro EMS should wait before sending another Get request in the **Value** field.

Select **Poll Retries** and enter the maximum number of times Pro EMS should resend the same request before failing in the **Value** field.



2 Select the **Access** tab in the screen above to switch to the screen as shown next.

Check the settings of **Read**, **Read/Write** and **Trap** communities. Change the settings if they do not match the settings on the device.



By default, ZyXEL Enterprise Ethernet Switchs and Access Points use `public` as the SNMP communities. You can use the `show snmp` command to check them on the device. In the following example, the device uses `public`.

```
ras# show snmp

[General Setting]
SNMP Version    : v2c
Get  Community  : public
Set  Community  : public
Trap Community  : public

[ Trap Destination ]
Index  Version       IP  Port  Username
-----  -------  -------  ----  --------
    1      v2c  0.0.0.0   162
    2      v2c  0.0.0.0   162
    3      v2c  0.0.0.0   162
    4      v2c  0.0.0.0   162

[ User Information ]
Index   Name  SecurityLevel  Authenticaion  Privacy
-----  -----  -------------  -------------  -------
    1  admin         noauth            md5      des
```

3 Check your network connection. Make sure you can ping to the device from the computer where your Pro EMS is installed.

3.4 Device Management

Why do I always get "FAILED" after I execute a script?

1. Click the **View Log** button in the **Tools** > **Script Distribution** screen.
2. Scroll down the **View Log** screen to the end, find the corresponding logs. The log should show you the reason.
3. Make sure you set the user name and password Pro EMS uses to telnet the device in the **Tools** > **Account Management** screen.
4. Use ping to check the connection between the device and Pro EMS. Make sure they are connected.
5. Check the device status using the **Tools** > **Hardware Status** screen. Make sure the device is operating correctly. Try to execute your script again. Contact your local support if it still fails.

PART III
Appendices and Index

SNMPc Network Manager (113)

Legal Information (119)

Index (121)

A

SNMPc Network Manager

This appendix gives a brief overview of the SNMPc Network Manager.

Starting the SNMPc Network Manager

You must have SNMPc properly installed before you can use the Pro EMS; please refer to the Castle Rock web site at www.castlerock.com or see your SNMPc user's guide.

You may start the SNMPc Network Manager manually or automatically each time you turn on your computer.

Manual Startup

Click **Start**, **Programs**, **SNMPc**, **Startup System** to manually start the SNMPc Network Manager. This is the default location of the SNMPc Network Manager.

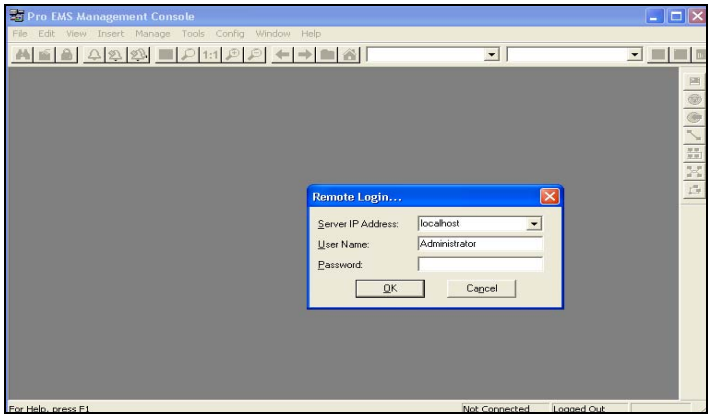
Automatic Startup

To automatically start the SNMPc Network Manager each time you turn on your computer:

1 In the SNMPc main window, click **Config**, **System Startup**.

2 Select the **Auto Startup** check box, and click **Done**.

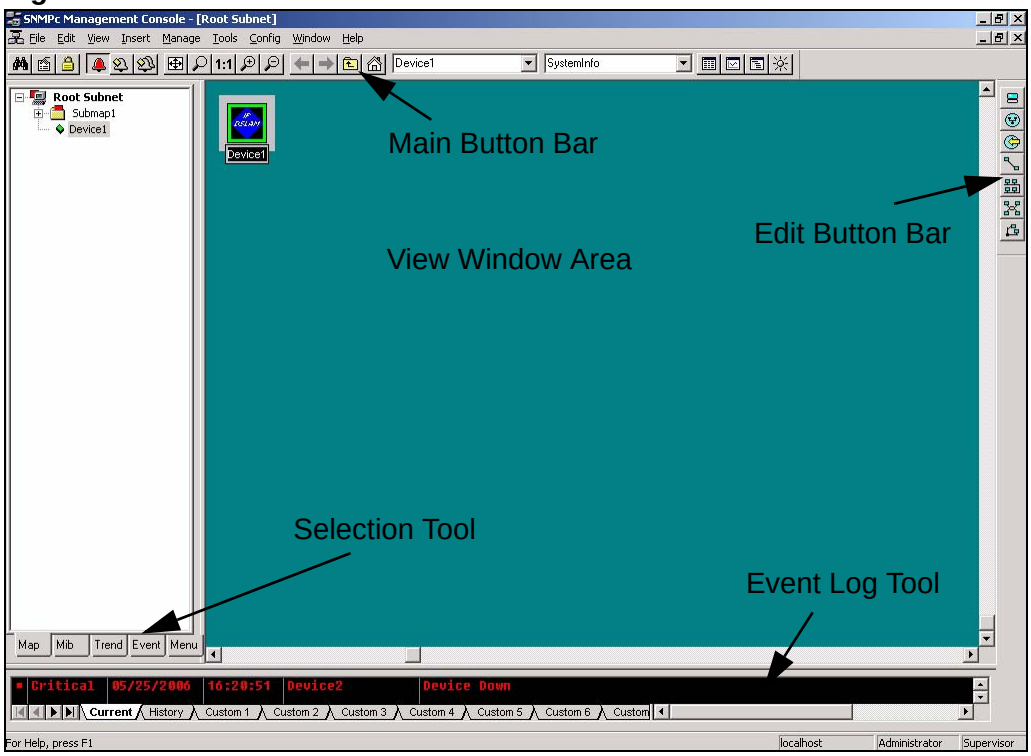
Figure 63 SNMPc: Automatic Startup



SNMPc Main Window

The following figure and table show the elements of the SNMPc main window.

Figure 64 SNMPc: Main Window



The following table describes the labels in this screen.

Table 44 SNMPc: Main Window

ELEMENT	FUNCTION
Main Button Bar	These are buttons and controls to execute common commands quickly. Hold the cursor over an icon to see a tool tip.
Edit Button Bar	These are buttons to quickly insert map elements. Hold the cursor over an icon to see a tool tip.
Selection Tool	This is a tabbed control for selection of objects within different SNMPc functional modules.
Event Log Tool	This is a tabbed control for display of filtered event log entries.
View Window Area	Map View, Mib Tables and Mib Graph windows are shown here.

Selection Tool

If you can't see the selection tool, click **View**, **Selection Tool** to display it. Use the selection tool to manipulate objects from one of several databases. Use the drag control at the right of the selection tool to change its size. Select one of the selection tool tabs to display a tree control for the database. Right-click on an icon inside a selection tree for database-specific commands.

Table 45 Selection Tool

TAB	DESCRIPTION
Map	Map Object database, including devices and subnets.
Mib	Compiled SNMP Mibs, Custom Tables and Custom Mib Expressions.
Trend	Report profiles that define long-term polling procedures and scheduled reports.
Event	Event filters used to determine what happens when an event is received.
Menu	Custom menus that appear in the Manage, Tools and Help SNMPc menus.

Event Log Tool

The event log tool displays different filtered views of the SNMPc event log. If you can't see the event log tool, click **View**, **Event Log Tool** to display it.

- Select the **Current** tab to show unacknowledged (current) events. These events have a colored box at the left side of the log entry. The color of map objects is determined by the highest priority unacknowledged event for that object.
- Select the **History** tab to show all events, including acknowledged and unacknowledged events.
- Select one of the **Custom** tabs and use the right-click **Filter View** menu to specify what events should be displayed for that tab.
- Double-click an event entry to display a **Map View** window with the corresponding device icon visible.

- To quickly view events for a particular device, first select the device and then use one of the **View Events** buttons (or the **View**, **Active Events** and **View**, **History Events** menus). This will show the device events in a separate window in the View Windows area.
- To remove one or more events, select the events and press the **Delete** key.
- To acknowledge (remove current status of) an event, right-click on an event entry and click **Acknowledge**.
- To completely clear the event log, click **File** and **Clear Events**.

View Window Area

The View Window Area is the main interface for viewing the SNMPc map and command results. This area uses the Multi-Document-Interface (MDI) specification to display multiple windows at the same time. Click **Window** and select **Cascade**, **Tile Horizontally** or **Tile Vertically** to rearrange the windows in the View Window Area in a way that makes them all visible.

Windows in this area can be in one of several states:

- A **Maximized** window uses the entire area and hides any other windows behind it. If you close a maximized window, the next top-most window will still be displayed in the maximized state. You need to be careful when using maximized windows because it is easy to lose track of how many windows you have open and there is an upper limit. Use the Windows menu to see a list of windows. Click **Windows** and select either **Tile Horizontally** or **Tile Vertically** to view all windows at the same time.
- An **Overlapped** window does not take up the entire area. One window will be completely visible and other windows are partially hidden behind it. This is the most common situation for the View Window area because it lets you view maps, tables and graphs at the same time and quickly move between them. Click **Windows** and select **Cascade**.
- A **Minimized** window is displayed as a small title bar with window open/close buttons. Windows are not typically minimized within the View Window Area because, as with the maximized case, they can easily be lost behind other windows.

Main and Edit Button Bar Icons

The following figure is a brief overview of the SNMPc main button and edit button bar icons.

Figure 65 SNMPc Main Button Bar Icons

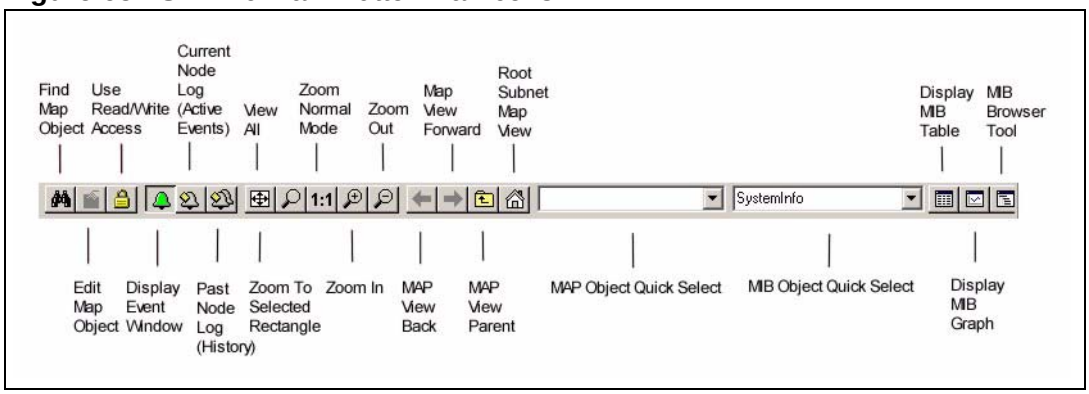
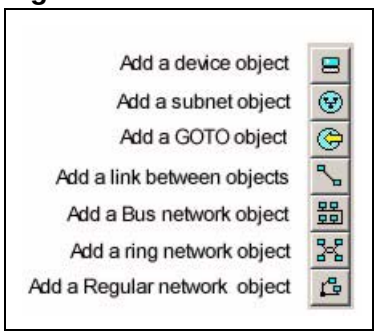


Figure 66 SNMPc Edit Button Bar Icons



Note: For more detailed information, please see www.castlerock.com.

B

Legal Information

Copyright

Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index

A

about
configuration file management 43
schedule management 89
account for device configuration backup 40
account for device firmware upgrade 40
Account Management 32
administrator
password 24
agent 16
alarm and alarm log
severity levels 53
alarm configuration 78
alarm type
Falling 79
Rising 79
alignment errors 54
associating device with an SNMPc group 60
auto-start-up
disable 30
average voltage 67

B

bucket granted 74
bucket requested 74

C

carrier sense errors 54
Castlerock 15
Celsius 67
certifications
viewing 119
communities
default 109
Community
public 20
community 16, 76, 78
Compiling MIB databases 29
computer crash 107
Configuration File Management 32
configuring actions for alarms 75
configuring alarms 78
Connect Telnet 32
connection timeout 44
copyright 119
configuration file management 43
creating schedules
firmware and configuration management 88

D

data sampling value
absolute 79
default communities 109
default directory
configuration backup 44
configuration restore 44
default password 24
Deferred 54
Deferred Transmissions 54
definition of script 97
device configuration file
editing 49
device configuration file management 42
Device Discovery
automatic 27
manual 28
device group 58
device hardward startus 65
device hardware status 62
device MAC table 67
device selection tool 26

device temperature 67
device VLAN status 103
devices supported 17
disable auto-start-up 30
disclaimer 119
downloaded configuration file name 48
dual configuration 103

E

edit button bar 26
editing configuration file example 50
editing device configuration file 49
Element Management System (EMS) 15
Element Management System. See EMS.
EMS 15
Ethernet packet statistics 52
Ethernet Status 32
event 75
Event Log 32
event log tool 26
excessive collisions 54
executing a script 97

F

Fahrenheit 67
fail to install 107
Failed 48
failed task retry times 44
Falling alarm type. 79
fan RPM 67
FCS errors 54
Firmware Upgrade 32
forget password 108
frame too longs 54

G

Group Management 32
grouping devices 58

H

Hardware Requirements
  CPU 17
  Disk space 17
  ethernet adapter 17
  graphics adapter 17
  RAM 17
Hardware Status 32
historical network traffic statistics 83

I

Installation
  NMS 17
  Pro EMS 21
Internet MAC sublayer 54

L

LAN 71
late collision 54
Licenses
  Enterprise 15, 24
  Trial 24
  Workgroup 15, 24
Link Aggregation Control Protocol (LACP) 71
load device factory defaults 101
login 24

M

MAC Table 32
MAC table of devices 67
main button bar 26
managed devices 17
Management Console
  Pro EMS 25

management console 16
Management Information Base (MIB) 16
managing device configuration file 42
Menus
  Tools 31
MIB (Management Information Base) 27
  compiling 29
MIB Browser 27, 32
MIB files 29
multiple collision frames 54

N

network elements (NE) 15
Network Management System (NMS) 15
Network Management System. See NMS.
NMS 15
  Console 19
  Server 19
  uninstalling 35
NMS console 15
NMS Keys 24
NMS screen overview 26
NMS server 15
no retry for failed task 44
nominal voltage value 67
note
  editing configuration file 49
  saving edited configuration file 49
note of account management 40
notes for firmware upgrade 56

O

object selection tabs 26

P

Poll Object 32
poll retries 108
poll timeout 108
polling agent 16
polling interval 53
Port Status 32
Pro EMS 15
  Enterprise 15
  Tools menus 31
  uninstalling 34
  Workgroup 15
Pro EMS Management Console 25
product registration 120

Q

Queued status 46, 48, 58

R

read/write community 109
reboot devices 101
registration
  product 120
related documentation 3
restoring configuration file 44
restoring device configuration status 46
retries for failed task 44
Revolutions Per Minute, see fan RPM 67
Rising alarm type 79
RMON 71
RMON Configuration 32
RMON Ethernet History Data 32
RMON Ethernet Statistics 32
RMON Ethernet statistics graph example 88
RMON Ethernet statistics table example 88
RMON history configuration 74
RMON probes 71
RMON View 32
RPM (Revolutions Per Minute) 67

S

saving script to a file 97

Schedule Management 32
script definition 97
Script Distribution 32
script execution 97
script failed 110
searching device event logs 55
Simple Network Management Protocol (SNMP) 16
simultaneous connections 44
single ccollision frames 54
SNMP
  v1 15
SNMP communities
  default 109
SNMP operation timeout 108
SNMP v2 15
SNMPc 15, 113
SNMPc group
  default codes and names 54
SNMPv3 15
Software Requirements
  Castlerock 17
  database system 17
  operating systems 17
  Postgres 8.0 17
SQE test errors 54
startup alarm 79
status
  Connecting 46, 48, 58
  device restoring task 46
  Downloading 46, 48
  Failed 46, 48, 58
  Finished 46, 48
  Queued 46, 48, 58
  Retrying 46, 48, 58
subnet map 30
summary
  tools menu 39
summary of scheduled tasks 90
syntax conventions 5
System Information 32
System Management 32

T

temperature limit 67
threshold for alarm falling 82
threshold for alarm rising 82
time-stamp of logs 56
Tools menus 31
trademarks 119
trap 16
Trap Sender 32
Troubleshooting
  communities 109
  crash 107
  fail to install 107
  forget password 108
  operation timeout 108
  script failed 110
troubleshooting
  EMS crashes 107
  fail to connect EMS 108
  fail to install EMS 107
  forget password 108

U

uninstall 33

V

View Log 110
view subnet map 30
view window area 26
viewing script execution result 97
VLAN Status 32
VLAN status on devices 103

W

warranty 120
  note 120
ways for accessing the Tools menu 39

WEB Browser 32
WEB Cleanup 32
WEB Reports 32
Windows Administrator permission 17
Wizard
  Pro EMS 21