

Enterprise Network Center

Network Management System

User's Guide

DEFAULT LOGIN DETAILS

User Name	root
Password	root

Software Version 1.2
Edition 1, 3/2011

www.zyxel.com

ZyXEL

About This User's Guide

Intended Audience

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

Related Documentation

- Quick Start Guide

The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your software.

Note: It is recommended you use the web configurator to configure the ENC.

- Supporting 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.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. 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.

Disclaimer

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.

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 device.




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



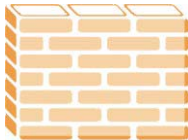


Syntax Conventions

- The Network Enterprise Center may be referred to as the "ENC", 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 may use the following generic icons. The ENC icon is not an exact representation of your device.

Computer	Notebook computer	Telephone
		

Server 	DSLAM 	Firewall 
Switch 	Router 	

Contents Overview

User's Guide	15
Web Configurator	17
Tutorials	47
Technical Reference	83
Dashboard	85
Configuration	93
Event	123
Tool	135
Report	177
Application	189
Maintenance	243
Troubleshooting	263

Table of Contents

About This User's Guide	3
Document Conventions	5
Contents Overview	7
Table of Contents	9
 Part I: User's Guide	 15
Chapter 1	
Web Configurator.....	17
1.1 Web Configurator Requirements	17
1.2 Web Configurator Access	18
1.3 Web Configurator Screens Overview	19
1.3.1 Title Bar	20
1.3.2 Main Menu Screens	21
1.3.3 OTV and Map	24
1.3.4 Main Window	33
1.3.5 Right-click Menus	33
1.3.6 Common Icons	43
1.3.7 Working with Tables	44
 Chapter 2	
Tutorials.....	47
2.1 Acknowledge Device Events	47
2.2 Firmware Upgrade for Multiple Devices	48
2.3 Configuration Backup for Multiple Devices	53
2.4 Configuration Restore to a Device	55
2.5 Script Distribution to Multiple Devices	58
2.6 ENC Backup and Performing a Complete Auto-Discovery with Filters	60
2.7 Event Actions Triggered By Received Events	63
2.8 Performance Monitoring for Interfaces	66
2.9 Configure VLAN Settings	70
2.10 Register Multiple NWA1300-N Series APs	74
2.10.1 Method 1	75
2.10.2 Method 2	77
2.10.3 Method 3	78
2.11 Different Map Views for Different Users	80

Part II: Technical Reference.....83**Chapter 3
Dashboard85**

3.1 Overview	85
3.2 The Dashboard Screen	85
3.2.1 Edit a Widget	90

**Chapter 4
Configuration93**

4.1 SNMP	93
4.1.1 MIB Browser	94
4.1.2 Custom Table	97
4.1.3 Custom Table Add/Edit	98
4.1.4 Table View	99
4.1.5 Graph View	100
4.2 Firmware Upgrade	100
4.2.1 Firmware List	101
4.2.2 Uploading Firmware to the ENC	102
4.2.3 Schedule List	102
4.2.4 Creating or Editing a Schedule List	103
4.3 Script Distribution	106
4.3.1 Script Distribution Add	107
4.4 Configuration File Update/Backup	111
4.4.1 Configuration File List	111
4.4.2 Uploading Configuration Files to the ENC	112
4.4.3 Backup Schedule List	114
4.4.4 Creating or Editing a Backup Schedule List	115
4.4.5 Update Schedule List	116
4.4.6 Creating or Editing an Update Schedule List	117
4.5 Default Performance Monitor Library	120
4.5.1 Customized Performance Monitor Library	120
4.5.2 Add a Performance Monitor	121

**Chapter 5
Event123**

5.1 Event Viewer	123
5.1.1 Events	125
5.2 Event Configuration	126
5.2.1 Edit Event Configuration	127
5.3 Customized Events	128
5.3.1 Customize an Event	128
5.4 Event Action	131

5.4.1 Add/Edit Event Action	132
-----------------------------------	-----

Chapter 6

Tool	135
-------------------	------------

6.1 Device Discovery	135
6.1.1 Automatic	135
6.1.2 Manual	135
6.1.3 Auto-Discovery	136
6.2 Inventory of Devices	140
6.2.1 Inventory Device Details - System	143
6.2.2 Inventory Device Details - Access	145
6.2.3 Inventory Device Details - Interface	148
6.2.4 Inventory Device Details - Routing	149
6.2.5 Inventory Device Details - ARP	151
6.2.6 Inventory Device Details - Port Analyzer	151
6.2.7 Inventory Device Details - MAC Table	152
6.2.8 Inventory Device Details - Wireless	153
6.3 Inventory of Networks	154
6.3.1 Inventory Network Details	155
6.4 Device Group	156
6.5 Device Group Add/Edit	157
6.6 PING/Trace Route	158
6.7 MIB Loader	159
6.7.1 User Loaded MIBs	159
6.7.2 Default MIBs	160
6.8 Performance Monitoring	161
6.8.1 Device Monitor	161
6.8.2 Example - Displaying Selected Performance Monitors	162
6.8.3 Example - Removing Selected Performance Monitors	163
6.8.4 Monitor Manager	163
6.8.5 Performance Monitor Add	164
6.8.6 Add a Threshold to the Performance Monitoring List	165
6.8.7 View the Performance Monitoring Report	166
6.9 Schedule Report	168
6.10 Schedule Report Add/Edit	169
6.11 Syslog Overview	170
6.11.1 Syslog View	170
6.11.2 Log Statistic	172
6.11.3 Settings	173

Chapter 7

Report	177
---------------------	------------

7.1 Default Reports Screen	177
----------------------------------	-----

7.2 Customized Reports Screen	178
7.2.1 Reports Add	179
7.2.2 A Report Example	184
7.3 Scheduled Report Summary Screen	185
7.4 Schedule Report Add/Edit Screen	185

Chapter 8

Application 189

8.1 Overview	189
8.1.1 What You Can Do in This Chapter	189
8.2 RMON Introduction	189
8.3 Statistics	190
8.3.1 Add/Edit an RMON Port	190
8.3.2 Viewing the Table	191
8.3.3 Viewing the Graph	193
8.4 History Config	196
8.4.1 Configuring an RMON History Entry	197
8.4.2 Viewing the Table	197
8.4.3 Viewing the Graph	199
8.5 Event/Alarm	201
8.5.1 Configuring an Event	203
8.5.2 View Alarm Logs	205
8.5.3 Alarm Parameters	206
8.5.4 Configuring an Alarm	206
8.6 VLAN Management	208
8.6.1 VLAN Management Configuration Examples	210
8.6.2 Edit a VLAN Group	214
8.6.3 Port Setting	217
8.7 Port Basic Settings	219
8.7.1 View Port Status	221
8.8 Bandwidth Control Overview	222
8.8.1 CIR and PIR	222
8.8.2 Bandwidth Control Setup	223
8.9 Broadcast Storm Control	224
8.10 Port Security	226
8.10.1 Static MAC Forwarding	226
8.10.2 MAC Address Learning	226
8.10.3 Port Security Configuration	227
8.10.4 Add Static MAC Forwarding	229
8.11 Authentication Overview	229
8.11.1 Local User Accounts	230
8.11.2 RADIUS and TACACS+	230
8.11.3 802.1x Authentication Overview	230

8.11.4 RADIUS Authentication Setup	231
8.11.5 TACACS+ Authentication Setup	232
8.11.6 802.1x Authentication Setup	234
8.12 AP Manager	235
8.12.1 The AP Profile Screen	235
8.12.2 Add/Edit an AP Profile	236
8.12.3 The AP Configuration Screen	238
8.12.4 The AP Monitor Screen	240
Chapter 9	
Maintenance	243
9.1 User Account Overview	243
9.2 Types of Accounts	243
9.3 User Account	244
9.3.1 User Account Add	246
9.4 Server	247
9.5 Customize Device Models	248
9.5.1 Device Model Add/Edit	249
9.6 Customize Images	251
9.6.1 Images Add/Edit	253
9.7 Backup/Restore	255
9.7.1 Backup	257
9.8 Data Export	258
9.9 Registration	258
9.9.1 Registration Screen	259
9.10 Log	260
9.11 About	261
Chapter 10	
Troubleshooting.....	263
10.1 Installation Problem	263
10.2 Problem Accessing the ENC	263
10.3 Problem Finding a Device	264
10.4 Map Problems	265
10.5 Script Problems	265
10.6 Event Action Problems	266
10.7 VLAN/Port Management Problems	266
10.8 Lose Connection Problems	266
10.9 Syslog Problems	267
10.10 Configuration Backup Problems	267
10.11 Other Problem	267
Appendix A Product Specifications	269

Appendix B IP Addresses and Subnetting	271
Appendix C Pop-up Windows, JavaScript and Java Permissions	281
Appendix D Open Software Announcements	291
Appendix E Legal Information.....	301
Index	303

PART I

User's Guide

Web Configurator

The ENC Web Configurator allows you to access the ENC that can manage devices through a web browser.

Note: This User's Guide shows example ENC Web Configurator screens. Available screens and fields vary depending on the managed device's model and firmware version.

1.1 Web Configurator Requirements

In order to use the Web Configurator, you must

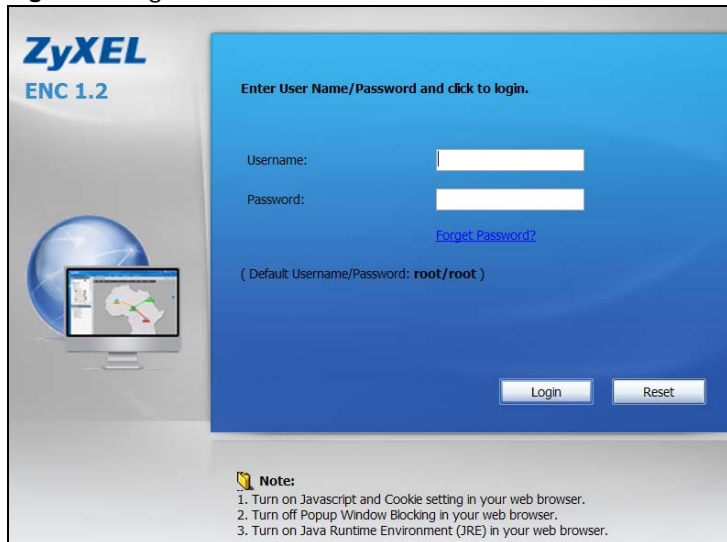
- Use Firefox 3.0 or later, or Internet Explorer 7 or later
- Allow pop-up windows (blocked by default in Windows XP Service Pack 2)
- Enable JavaScript (enabled by default)
- Enable Java permissions (enabled by default)
- Enable cookies

The recommended screen resolution is 1024 x 768 pixels.

1.2 Web Configurator Access

- 1 To access the ENC service on the ENC server itself, open a web browser and type `http://localhost/midas`. Otherwise, type `https://{ENC server's IP address}/midas`. The login screen displays.

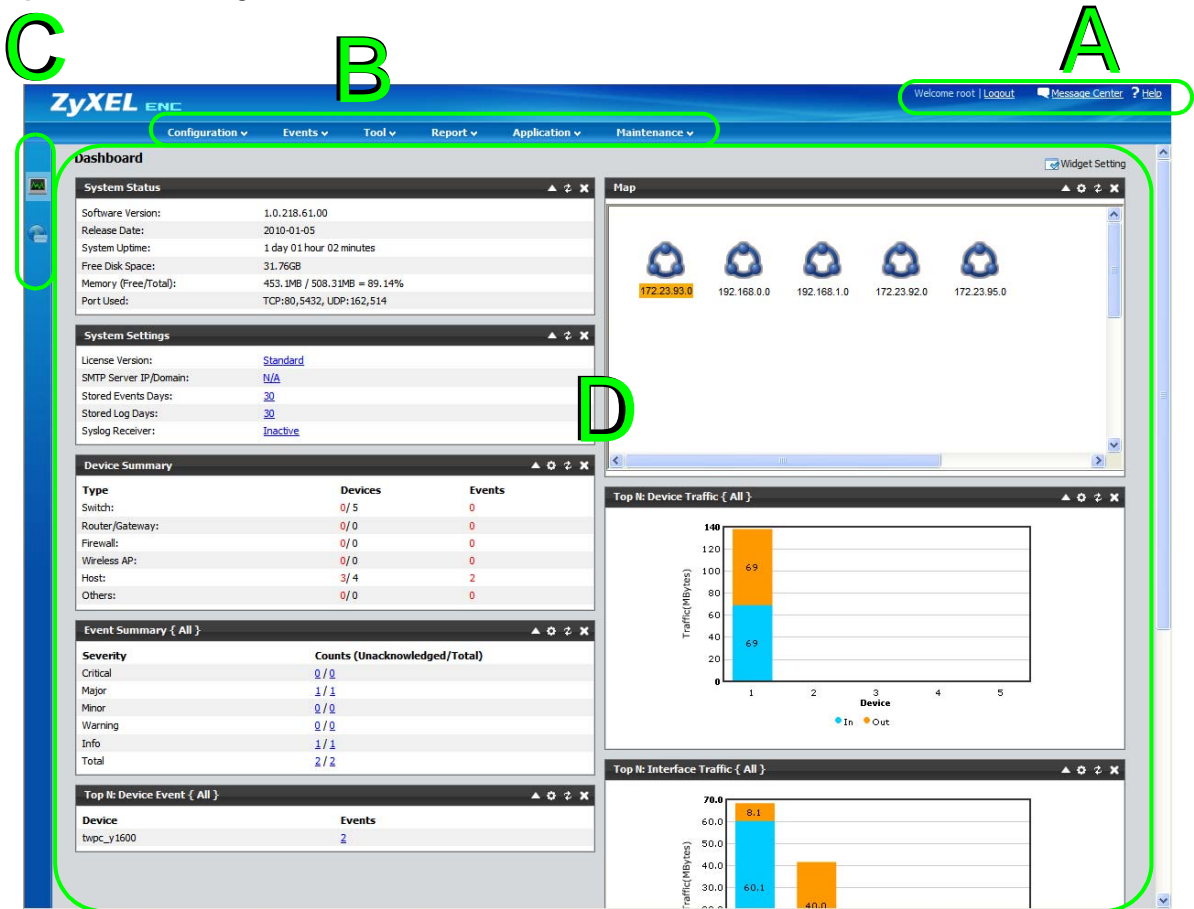
Figure 1 Login Screen

The image shows the login screen for the ZyXEL ENC 1.2 web configurator. On the left, there is a logo for 'ZyXEL ENC 1.2' and a small graphic of a globe with a computer monitor in front of it. The main area is a blue box with the text 'Enter User Name/Password and click to login.' Below this are two input fields: 'Username:' and 'Password:'. A link for 'Forgot Password?' is located below the password field. Below the input fields, it says '(Default Username/Password: root/root)'. At the bottom of the blue box are two buttons: 'Login' and 'Reset'. Below the blue box, there is a 'Note' section with three bullet points: 1. Turn on Javascript and Cookie setting in your web browser. 2. Turn off Popup Window Blocking in your web browser. 3. Turn on Java Runtime Environment (JRE) in your web browser.

- 2 Type the user name and password (see the cover page of this guide to get the default login information).

- 3 Click **Login**. The **Dashboard** screen appears as shown next. The dashboard displays general system status and settings information as well as information about the managed devices and their traffic in re-arrangeable widgets. See [Chapter 3 on page 85](#) for details on the dashboard.

Figure 2 Web Configurator: Dashboard



The Web Configurator automatically refreshes itself every 3 minutes.

Note: If there is no activity for more than 15 minutes, the Web Configurator automatically logs you out. If this happens to you, simply log back into the Web Configurator again.

1.3 Web Configurator Screens Overview

The Web Configurator screen is divided into these parts (as illustrated in [Figure 2 on page 19](#)):

- **A** - title bar
- **B** - main menus
- **C** - navigation panel
- **D** - main window

1.3.1 Title Bar

The title bar provides some links in the upper right corner.

Figure 3 Title Bar



The icons provide the following functions.

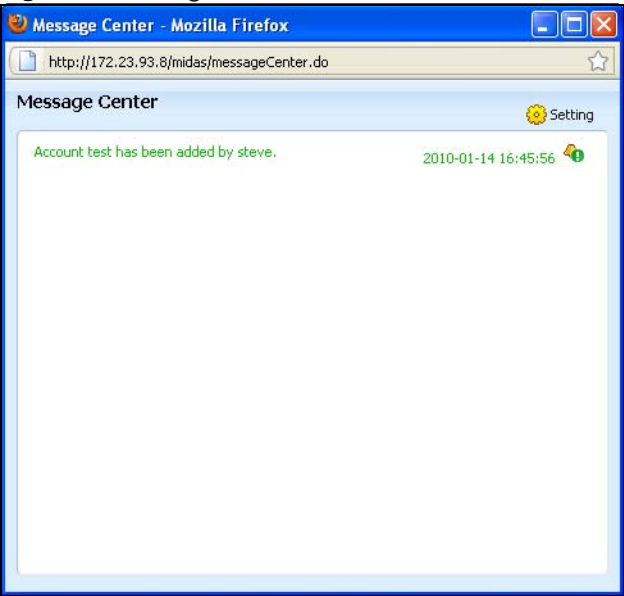
Table 1 Title Bar

LABEL	DESCRIPTION
Logout	Click this to log out of the Web Configurator.
Message Center	Click this to display the logs the ENC generates while you are logged in.
Help	Click this to open the help page for the current screen. If you have selected a node in the OTV tree (see Section 1.3.3 on page 24), you can see the node below the Help link.

1.3.1.1 Message Center

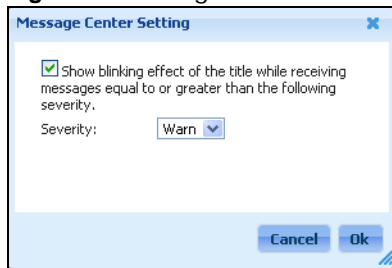
Click **Message Center** to display the logs the ENC generates while you are logged in.

Figure 4 Message Center



Click **Setting** to open a pop-up window where you can set the icons for the messages in the message center to blink for logs of a specific severity level or higher.

Figure 5 Message Center > Setting



1.3.2 Main Menu Screens

Use the Web Configurator main menu screens to manage and monitor devices and configure the ENC's settings.

Use the **Configuration** menu screens to configure devices.

Note: Not all menus are available for all user privilege levels.

Table 2 Main Menu Screens Summary

MENU	TAB	FUNCTION
Configuration		
MIB Browser		This menu is available when you select a device. Browse the currently selected device's MIB tree and get or set MIB object values.
Firmware Upgrade	Firmware List	Add firmware files that the ENC can upload to managed devices.
	Schedule List	Schedule the ENC to upload firmware files to managed devices.
Script Distribution		Create and maintain batch files of commands that you can apply to managed devices.
Update/Backup	Configuration File List	Maintain a list of device configuration files that the ENC can upload to devices. You can upload configuration files from your computer or devices.
	Backup Schedule List	Create schedules for backing up device configuration files to the ENC.
	Update Schedule List	Create schedules for uploading device configuration files saved in the ENC to devices.
Performance Monitor Library	Default Monitor Library	View a list of performance monitor templates that are defined by default.
	Customized Monitor Library	Manage (create, edit, and delete) a list of performance monitor templates that you configured.
Events		
Viewer		Receive and display events sent by the managed devices.
Configuration	Default	View and modify the default events including selecting an event action to use.
	Customize	Create and maintain non-default events including selecting an event action to use.

Table 2 Main Menu Screens Summary (continued)

MENU	TAB	FUNCTION
Event Action		Create and maintain profiles of event-triggerable operations such as program or script execution, sending e-mails or pages, or displaying a warning message popup, forwarding syslogs, or sending an SNMP trap.
Tool		
Auto-Discovery		Find devices in the ENC's network or a designated network segment or range of network segments.
Inventory	Device	Manage the database of managed devices for the currently selected map.
	Network	Manage the database of managed networks for the currently selected map.
Device Group		Create groups of similar devices to ease procedures such as upgrading firmware and applying scripts.
PING/Trace Route		Use ping to check if the ENC can connect to an IP address or web site and trace route to determine the network path from the ENC to an IP address or web site.
MIB Loader		Load and compile private MIB files for managing devices the ENC does not support by default.
Performance Monitoring	Device Monitors	View a device's monitored data in graphs.
	Monitor Manager	Select device performance information to monitor and display. You can also export raw data or reports.
	Schedule Report	Set a schedule to automatically generate device performance monitor reports and send them out by e-mail.
Syslog View	Log Viewer	Displays, clears, and exports the syslogs received from managed network devices.
	Log Statistic	Displays statistics based on the syslogs received from managed network devices.
	Settings	Set the ENC to receive and store syslogs. You can also have the ENC archive the syslogs.
Report		
Reports	Default Reports	View performance monitoring reports that were defined by default.
	Customized Reports	Generate, view, and export device inventory, event log, and/or performance monitoring reports.
Schedule Report		Set schedules for the ENC to generate and e-mail specific reports.
Application		
RMON	Statistics	This menu is available when you select an Ethernet Switch. Collect and display Ethernet port network traffic statistics for the selected managed device.
	History	Display historical Ethernet port network traffic statistics for the selected managed device.
	Event / Alarm	Configure the ENC to receive RMON events and alarms for the selected managed device.
VLAN Management		Configure the selected managed device's VLAN settings. A VLAN group tree also lets you view and edit VLANs in the managed devices.

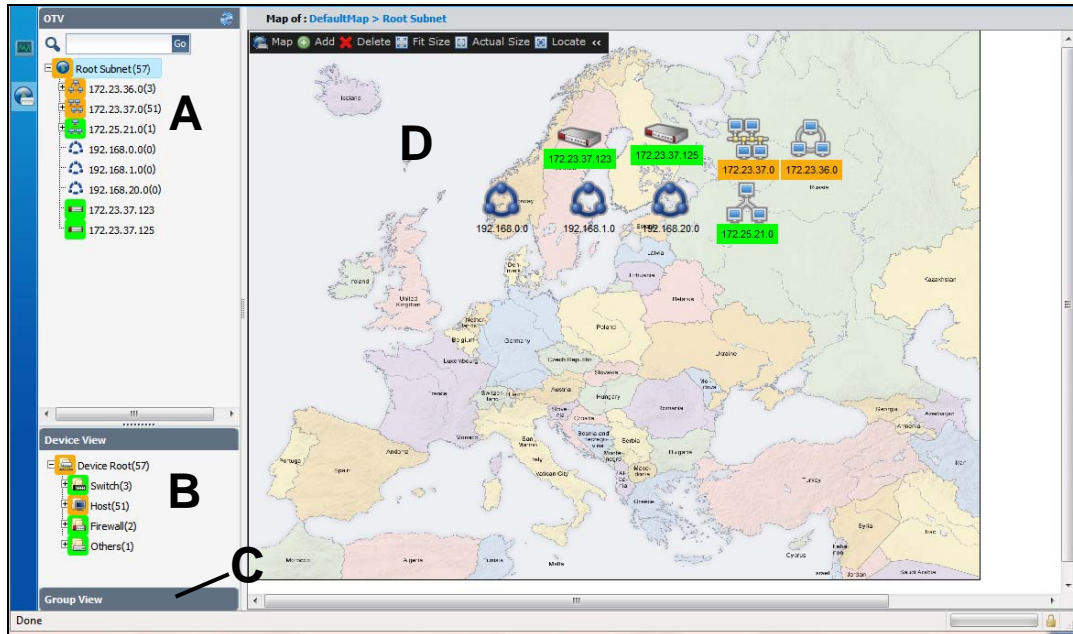
Table 2 Main Menu Screens Summary (continued)

MENU	TAB	FUNCTION
Port Management	Basic Setting	This feature is only available for devices which support port management. Configure a selected managed device's basic port settings.
	Bandwidth Control	Configure a selected managed device's bandwidth control settings.
	Broadcast Storm Control	Configure a selected managed device's broadcast storm settings.
	Security	Configure a selected managed device's security settings.
	Authentication	Configure a selected managed device's authentication settings.
AP Manager	AP Profile	Configure and view wireless AP profiles.
	AP Configuration	Search a wireless AP and view its basic settings.
	AP Monitor	View all managed wireless APs. Note: At the time of writings, this AP Manager function only supports ZyXEL NWA1300-N Series.
Maintenance		
User Account		Manage ENC user accounts.
Server		Configure the ENC's IP address or domain, login lockout, and mail relay settings.
Customize	Device	Create and manage a list of devices and set their representative icons.
	Image	Upload icons to use to represent devices.
Backup/Restore		Back up or restore the ENC's database.
Data Export		Export specific tables from the ENC's database.
Registration		View the licensed service status and upgrade licensed services.
Log		Display, search, export, and clear the ENC's system log.
About		Display version, release date, and copyright information.

1.3.3 OTV and Map

Click the **Map** icon on the left hand of the main screen to open the Object Tree View (OTV; **A**). The Device View (**B**), Group View (**C**) panels and main screen (**D**) are also shown.

Figure 6 OTV and Map



1.3.3.1 OTV

The OTV shows the current registered devices and networks and details such as their network topology, up or down status, and alarm status. Drag the OTV's right edge to re-size it or click the dotted section in the middle of the right edge to hide the OTV. Use the OTV to:

- Search for devices or networks
- View devices or networks and their status

Table 3 Device and Network Icon Colors

ICON	COLOR	DESCRIPTION
Device	green	The device is online and working normally.
	red	The device is offline.
	white	The device is temporarily not managed by the ENC. (Status polling for the device is disabled in the Tool > Inventory > Device screen.)
Network	green	All devices (except the devices that are temporarily not managed by the ENC) in the network are online and no events occurred from the devices.
	orange	Some devices in the network are offline.
	red	All devices (except the devices that are temporarily not managed by the ENC) in the network are offline.
Folder	green	All devices (except the devices with status Un-monitor or not registered yet) in the network are online.
	orange	Some devices in the network are offline.

Table 3 Device and Network Icon Colors

ICON	COLOR	DESCRIPTION
	red	All devices (except the devices with status Un-monitor or not registered yet) in the network are offline.
	white	All devices in the folder are with status Un-monitor or not registered yet.

- Add or remove devices and networks (right-click a device or network for options)
- Move devices between networks (drag and drop icons or right-click icons for cut and paste options)
- View all devices in the map (click **Root Subnet**)
- Log into devices (right-click a device and click **Device Web GUI**)
- View and edit device properties and settings (click a device icon)
- View a network in the map (click a network icon).
- View unacknowledged event details (click a ring bell with an exclamation mark icon). The color of the icons is determined by the highest severity level unacknowledged event on that device.
- View device performance information (click a performance monitor icon)
- View all unspecified devices which the ENC added passively according to received device traps (click the **Unspecified Device** folder)

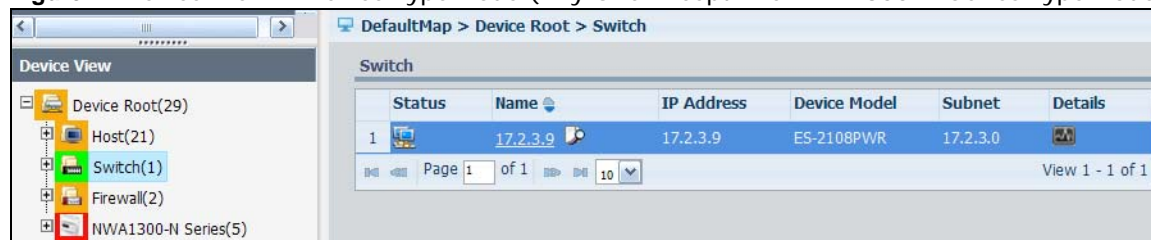
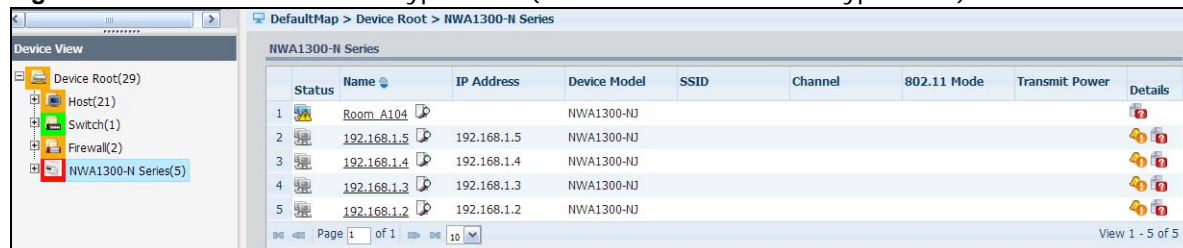
See [Section 1.3.6 on page 43](#) for more information about icons.

Note: Click the Plus Sign (+) next to an icon in the OTV, Device View or Group View to go to the next layer down. Click this Minus Sign (-) to hide the next layer objects.

Note: Some function menus are hidden until you select a device in the OTV, Device View or Group View such as MIB Browser, RMON, Performance Monitoring and Port Management.

1.3.3.2 Device View

The Device View shows managed devices by device type. Click a device type node to display the associated devices in the main screen. See [Table 51 on page 142](#) for similar description.

Figure 7 Device View > Device Type Node (Any One Except The NWA1300-N Series Type Node)**Figure 8** Device View > Device Type Node (The NWA1300-N Series Type Node)

Click a device node to display the device's inventory settings (see [Section 6.2 on page 140](#) for more information).

The ENC automatically updates this view every three minutes.

1.3.3.3 Group View

The Group View shows managed devices by group. Click the title bar to hide Device View and expand Group View. Click Device View again to hide Group View. By default, no group is available. You can configure device groups in the **Tool > Device Group** screen (see [Section 6.4 on page 156](#)).

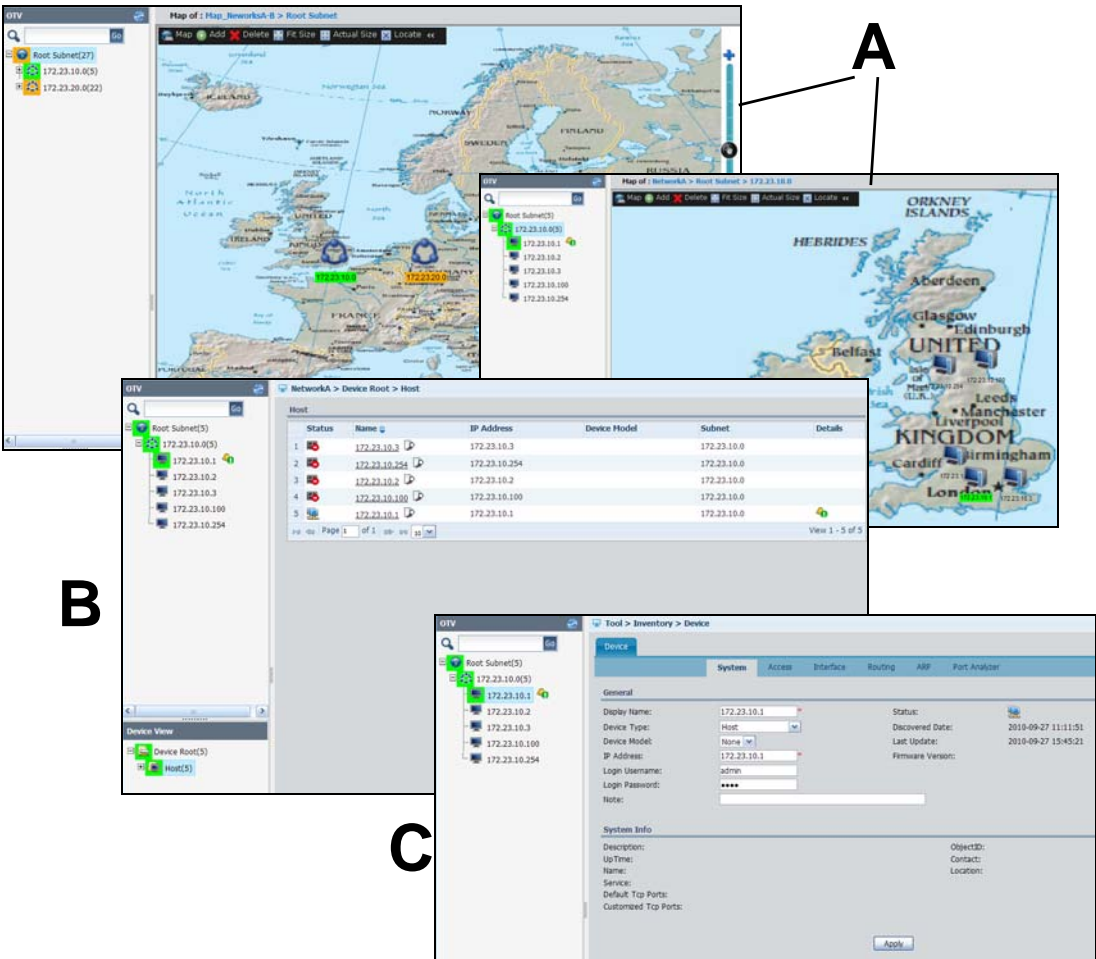
In Group View, click the icon for a single device to open the device's properties screen. Click the icon of a group folder to display all associated devices in the main screen (**D** in [Figure 6 on page 24](#)).

The ENC automatically updates this view every three minutes.

1.3.3.4 Map

The map screen displays icons for networks and shows their relationships in one map (A). The map screen displays a list of associated managed devices for device groups or types (B), and displays the inventory information for managed devices (C).

Figure 9 Map



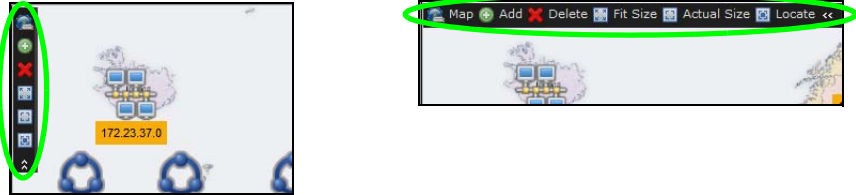

Administrators can create multiple maps and associate different devices with different maps for Operators and Users. See [Section 2.11 on page 80](#) for an example.

Administrators can also draw links on a map to show connections between devices and/or networks. See [Section 1.3.3.9 on page 32](#).

The following table describes the labels and submenus in the Map screen (A in [Figure 9](#)).

Table 4 Map	
LABEL	DESCRIPTION
Map of	This field displays the name of the Map image and the network path where the device is located in the ENC.
Map	
New	Click this to configure a new Map.
Open	Click this to an existing Map.

Table 4 Map

LABEL	DESCRIPTION
Manager	Click this to manage (add, duplicate, edit, remove) Maps.
Background	Click this to change the current Map image.
Add	
Network	Click this to add a network. See Section 1.3.5.1 on page 36 .
Folder	Click this to add a folder. See Section 1.3.5.2 on page 37 .
Device	Click this to add a device. See Section 1.3.5.3 on page 38 .
Devices	Click this to add multiple devices. See Section 1.3.5.4 on page 40 .
Link	<p>Use this function to monitor a connection between two nodes, either devices or networks.</p> <p>Hold the [Ctrl] key and select two nodes and then click this to create a connection between them. The Add Link screen appears. See Section 1.3.3.9 on page 32.</p> <p>You can also right-click the nodes and click Add Link to open the Add Link screen.</p>
Delete	Click this to remove the selected item(s)
Fit Size	Click this to resize the Map to fit this window.
Actual Size	Click this to display the actual size of the Map.
Locate	Click this to quickly find a device that you have selected in the Map if the Map is too big and you cannot easily find the device.
<<	<p>Click this to switch this menu bar location to display either horizontally on the top or vertically on the left hand of the window.</p> <p>Figure 10 Changing the Map Menu Bar Location</p> 
	Use this to zoom in and out by dragging the hand button up or down, or clicking the + and - icons.

1.3.3.5 Create a New Map

Use this screen to configure a new Map. To open this screen, click the **Map** icon on the left of the main window and then click **Map > New**.

Figure 11 Map > New

The following table describes the labels in this screen.

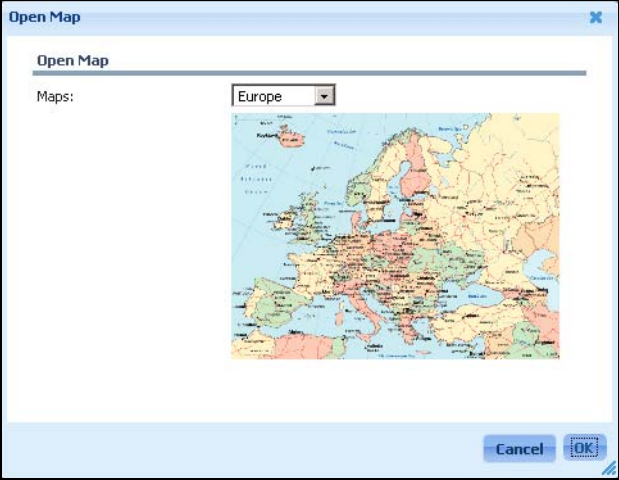
Table 5 Map > New

LABEL	DESCRIPTION
Map name	Enter up to 32 characters for the name of the Map. You can use alphanumeric characters (0-9, a-z, A-Z), colons (:), underscores (_), hyphens (-) and dots (.). Spaces are allowed.
Icon size	Select the size of device and network icons you want to display in this Map: 16 by 16 pixels or 48 by 48 pixels.
Background image	Select which image you want to display with the Map's root subnet.
Preview	This field displays the image preview.
Access Devices	This field displays the number of devices that have been associated with this Map. Click Select Devices to add or remove devices from a device list.
Description	Type additional information for this Map.
Access Setting	Select one or multiple users who are allowed to manage the devices in the Map from the Available Users list and click >> to move them to the Allowed Users list. Select the users who you disallow to access the Map from the Allowed Users list and click <<.
Cancel	Click this to discard the changes and exit this screen.
Ok	Click this to save the changes and exit this screen.

1.3.3.6 Open a Map

Use this screen to open an existing Map. To open this screen, click the **Map** icon on the left of the main window and then click **Map > Open**.

Figure 12 Map > Open



The following table describes the labels in this screen.

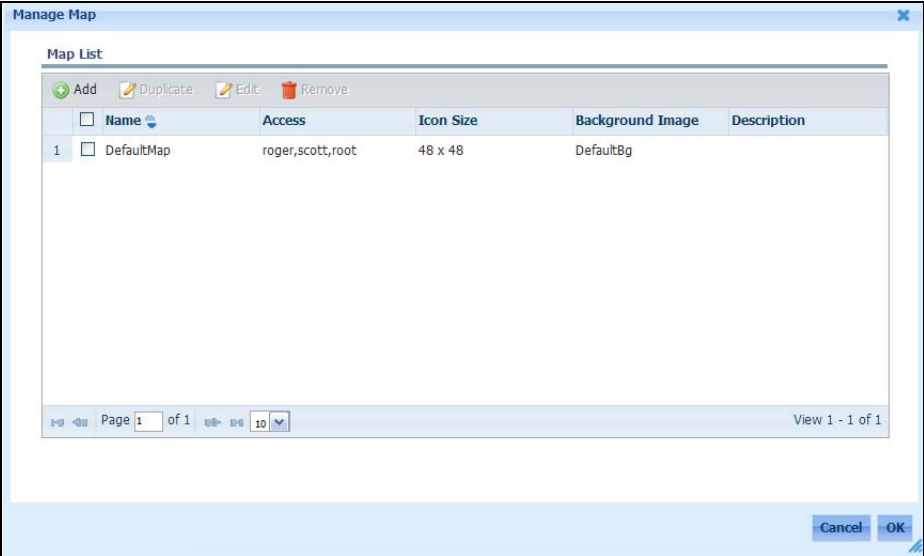
Table 6 Map > Open

LABEL	DESCRIPTION
Maps	Select the Map you want to open. The image preview appears.
Cancel	Click this to discard the changes and exit this screen.
Ok	Click this to save the changes and exit this screen.

1.3.3.7 Manage Maps

This screen lists a summary table of existing Maps. To open this screen, click the **Map** icon on the left of the main window and then click **Map > Manager**.

Figure 13 Map > Manager



The following table describes the labels in this screen.

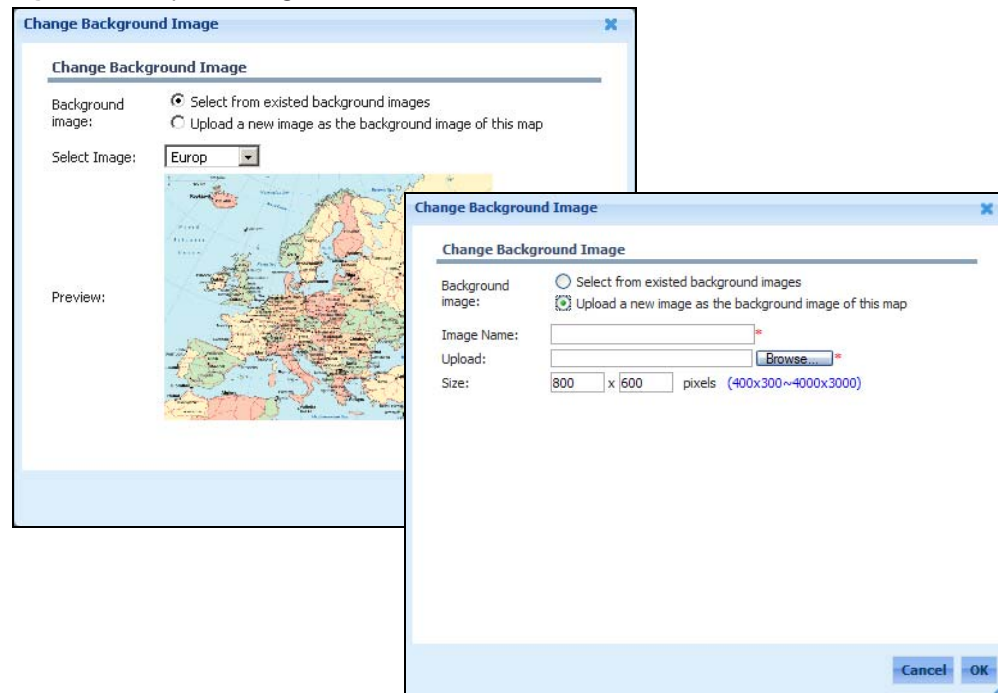
Table 7 Map > Manager

LABEL	DESCRIPTION
Add	Click this to create a Map. See Section 1.3.3.5 on page 29 .
Duplicate	Click this to duplicate a selected Map. The ENC adds a date and time that indicate when you performed the duplicate function for the new Map's name.
Edit	Click this to modify the settings for a selected Map. See Section 1.3.3.5 on page 29 for similar description.
Remove	Select one or multiple Map(s) and click this to delete them.
check box	Select the check box of an entry and click Duplicate , Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Name	This field displays the name of the Map.
Access	The field displays who can access the Map.
Icon Size	The field displays whether the ENC displays device icons at 16 by 16 or 48 by 48 pixels in this Map.
Maps	Select the Map you want to open. An image preview appears.
Cancel	Click this to discard the changes and exit this screen.
Ok	Click this to save the changes and exit this screen.

1.3.3.8 Change Background Image

Use this screen to change the background image of the map. To open this screen, click the **Map** icon on the left of the main window and then click **Map > Background**.

Figure 14 Map > Background



The following table describes the labels in this screen.

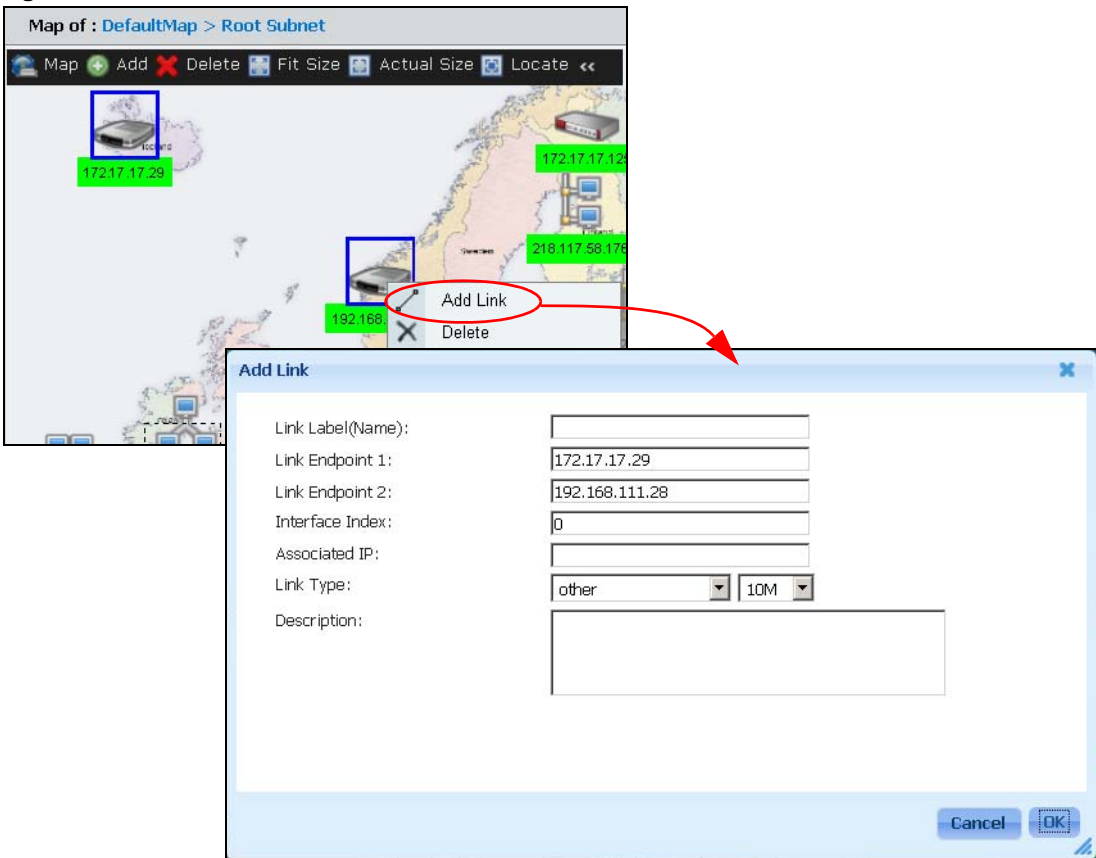
Table 8 Map > Background

LABEL	DESCRIPTION
Background image	Select whether to change the background image to an existing image or a new image.
Select Image	Select which image to which you want to change.
Preview	This field displays the selected image's preview.
Image Name	Enter up to 32 characters for the name of the image. You can use alphanumeric characters (0-9, a-z, A-Z), underscores (_), and hyphens (-). Spaces are not allowed.
Upload	Click the text box or Browse to specify the image file you want to upload from your computer to the ENC.
Size	Enter the size of background image in pixels that you want to display in the Map.
Cancel	Click this to discard the changes and exit this screen.
Ok	Click this to save the changes and exit this screen.

1.3.3.9 Add Link

Use this screen to monitor a connection between two nodes in a Map. To open this screen, click the **Map** icon on the left hand of the screen and select **Root Subnet** in the **OTV** panel. Hold the [Ctrl] key and select two nodes in the Map shown on the right, then right-click the nodes and click **Add Link**.

Figure 15 Add Link



The following table describes the labels in the **Add Link** screen.

Table 9 Map > Background

LABEL	DESCRIPTION
Link Label (Name)	Enter up to 32 characters for the link's name for identification purposes. You can use alphanumeric characters (0-9, a-z, A-Z), arrow brackets (<>), underscores (_), hyphen (-), dot (.) and spaces.
Link Endpoint 1	This field displays the first node's IP address that you selected.
Link Endpoint 2	This field displays the second node's IP address that you selected.
Interface Index	Enter the index number of a port or an interface on the device you specified in the Associated IP field. The ENC will monitor it to check the connectivity. Refer to the device's User's Guide for the number of the port or interface you should enter.
Associated IP	Enter the IP address of the endpoint 1 or 2 device. The ENC will use it to check and determine whether this link is up or down.
Link Type	Select the type and the maximum transmission speed of this link. If you are not clear about the settings, leave them to the defaults.
Description	Type additional information for this link in this field.
Cancel	Click this to discard the changes and exit this screen.
Ok	Click this to save the changes and exit this screen.

After you configure the link settings completely, a line displays between two nodes. The link becomes gray when the ENC is trying to send poll messages to the device. It is green when the connection between two nodes is up or red when they are disconnected.

1.3.4 Main Window

The main window shows the screen you select in the navigation panel (**D** in [Figure 6 on page 24](#)). The main window screens are discussed in the rest of this document.

Right after you log in, the **Dashboard** screen is displayed. See [Chapter 3 on page 85](#) for more information about the **Dashboard** screen.

1.3.5 Right-click Menus

In the **OTV** panel, right-click the **Root Subnet** network, a network under **Root Subnet** or a device, different menus display respectively. These menus provide a shortcut to execute a function for the network or device.

Note: Not all menus are available for all user privilege levels.

Figure 16 Right-click OTV: Select Root Subnet

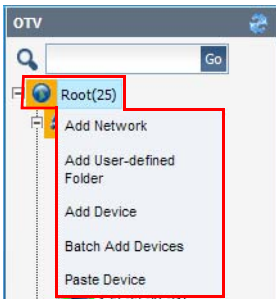


Figure 17 Right-click OTV: Select a Network

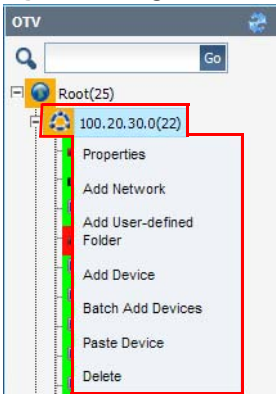
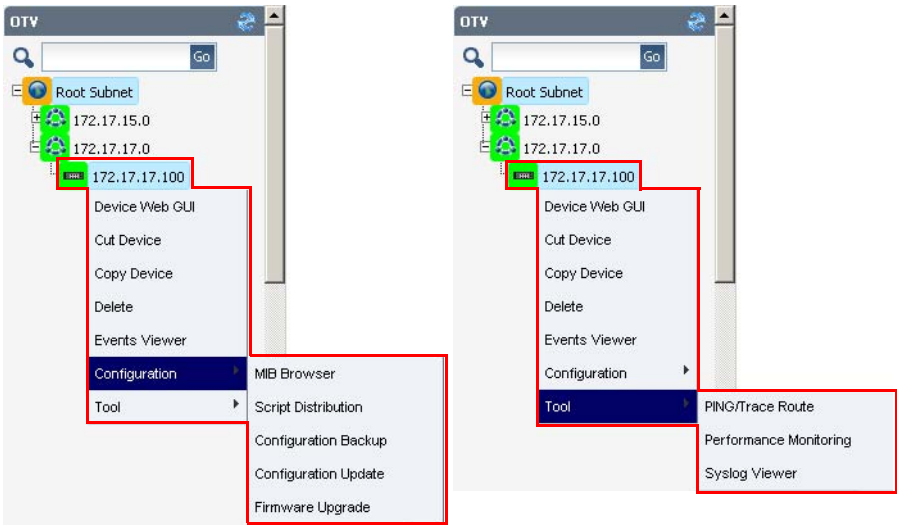


Figure 18 Right-click OTV: Select a Device



The following table describes the right-click menus.

Table 10 Right-click Menus

LABEL	DESCRIPTION
Add Network	Click this to create a new network node.
Add User-defined Folder	Click this to add a new folder which helps you to organize devices.
Add Device	Click this to register a new device.

Table 10 Right-click Menus

LABEL	DESCRIPTION
Batch Add Devices	Click this to register multiple devices at one time. Note: At the time of writing, this feature only supports the NWA1300-N Series devices.
Paste Device	Click this to paste a device node. You should first have cut from another network to the network.
Properties	Click this to modify the settings for the network or device.
Delete	Click this to remove the network or device from the ENC after you confirm the action.
Device Web GUI	Click this to access the device's Web Configurator.
Cut Device	Click this to remove the device from the current network in order to move it to another network.
Copy Device	Click this to duplicate the device configuration in order to give it to a similar device in another network.
Events Viewer	Click this to view events about this device. See Section 5.1 on page 123 .
Configuration	If you click Script Distribution , Configuration Backup/Update , or Firmware Upgrade function from the right-click menu, the main screen shows the related setting for the device only.
MIB Browser	Click this to view and configure MIB settings about this device. See Section 4.1.1 on page 94 .
Script Distribution	Click this to manage (add, edit, delete, execute) scripts on this device. See Section 4.3 on page 106 .
Configuration Backup	Click this to back up configuration for this device. See Section 4.4 on page 111 .
Configuration Update	Click this to restore configuration for this device. See Section 4.4 on page 111 .
Firmware Upgrade	Click this to upgrade firmware for this device. See Section 4.2 on page 100 .
Tool	
PING/Trace Route	Click this to test the network connectivity using ping or traceroute between the device and a host. See Section 6.6 on page 158 .
Performance Monitoring	Click this to configure performance monitors for this device, such as the CPU usage, bandwidth usage, memory usage, hardware temperature, incoming/outgoing traffic statistics, and so on. See Section 6.8 on page 161 .
Syslog Viewer	Click this to view system logs of the device. See Section 6.11.1 on page 170 .

1.3.5.1 Add Network

Use this screen to configure a new network in the ENC. To open this screen, right-click the **Root Subnet** or a network node and select **Add Network**.

Figure 19 Right-click Menus: Add Network

The image shows a screenshot of a web-based configuration window titled "Add Network". The window has a light blue header bar with the title and a close button. The main area contains several input fields: "Network Name:" with a text box and a red asterisk; "Network Address:" with a text box and a red asterisk; "Subnet Mask:" with a text box and a red asterisk; "Network Type:" with a dropdown menu currently showing "General" and a refresh icon; and "Description:" with a large text area. At the bottom right, there are "Cancel" and "OK" buttons. The "OK" button has a small blue icon next to it.

The following table describes the labels in this screen.

Table 11 Right-click Menus: Add Network

LABEL	DESCRIPTION
Network Name	Enter up to 32 characters for the name of a network. You can use alphanumeric characters (0-9, a-z, A-Z), underscores (_), hyphens (-) and/or dots (.).
Network Address	Enter the IP address of the network.
Subnet Mask	Enter the subnet mask of the network.
Network Type	Select the type of the network. The available options are General , Bus , Star , Ring and Tree . Each type associates an icon for your differentiation.
Description	Type additional information about the network in this field.
Cancel	Click this to exit this screen and go back to the previous screen.
OK	Click this to save the changes.

1.3.5.2 Add User-defined Folder

Use this screen to configure a new folder in the ENC. To open this screen, right-click the **Root Subnet** or a network node and select **Add User-defined Folder**.

Figure 20 Right-click Menus: Add User-defined Folder

The following table describes the labels in this screen.

Table 12 Right-click Menus: Add User-defined Folder

LABEL	DESCRIPTION
Folder Name	Type up to 32 characters for the folder's name. You can use alphanumeric (0-9, a-z, A-Z), underscores (_), hyphens (-), and dot (.). Spaces are not allowed.
Description	Type additional information for this folder.
Cancel	Click this to exit this screen and go back to the previous screen.
OK	Click this to save the changes.

1.3.5.3 Add Device

Use this screen to configure a new device in the ENC. To open this screen, right-click the **Root Subnet** or a network and select **Add Device**.

Figure 21 Right-click Menus: Add Device - Step 1

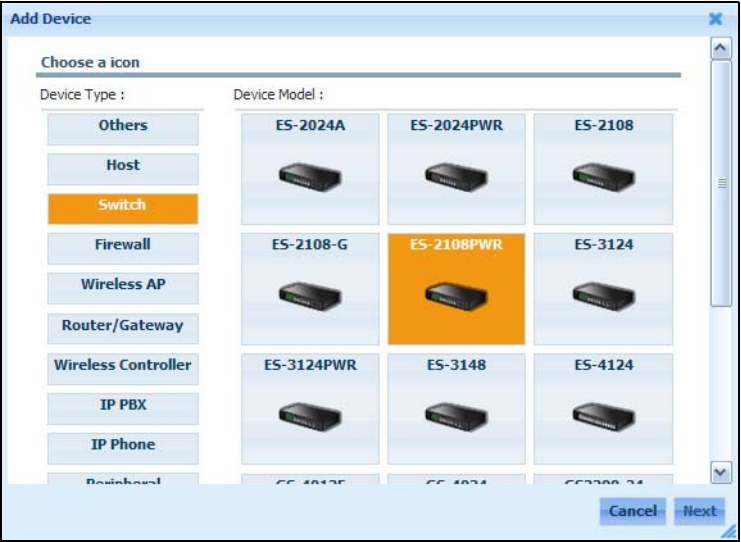
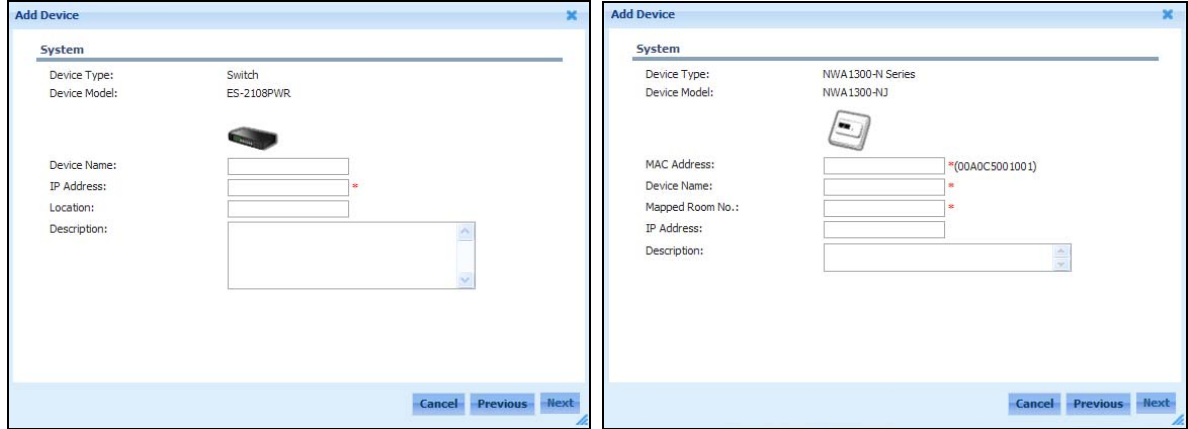


Figure 22 Right-click Menus: Add Device - Step 2



Note: At the time of writing, the step 2's screen for adding an NWA1300-N Series device is different than adding any other device.

Figure 23 Right-click Menus: Add Device - Step 3

The following table describes the labels in this screen.

Table 13 Right-click Menus: Add Device

LABEL	DESCRIPTION
Add Device - Step 1	
Device Type	Select the type of the device you want to add.
Device Model	Select the exact model name of the device if you can find it. If you cannot find an appropriate one, select device type Others , click Next and then fill it in the Device Name in the next screen.
Cancel	Click this to exit this screen and go back to the previous screen.
Next	Click this to proceed to the next screen.
Add Device - Step 2	
Device Type	This field displays the device type you just selected.
Device Model	This field displays the model name and the associated icon you just selected.
MAC Address	Enter the MAC address of the device.
Device Name	Enter up to 32 characters for the name of the device. You can use alphanumeric characters (0-9, a-z, A-Z), underscores (_), hyphens (-) and/or dots (.).
Mapped Room No.	Enter the number of the room where the device is located.
IP Address	Enter the IP address of the device.
Location	Type where you locate the device.
Description	Type additional information about the device.
Cancel	Click this to exit this screen and go back to the previous screen.
Previous	Click this to go back to the last screen.
Next	Click this to proceed to the next screen.
Add Device - Step 3	
SNMP Version	Select the version of the SNMP poll messages the ENC sends in order to communicate with the device.
Port	Enter the port number the ENC uses to transmit and receive SNMP messages to/from the device.

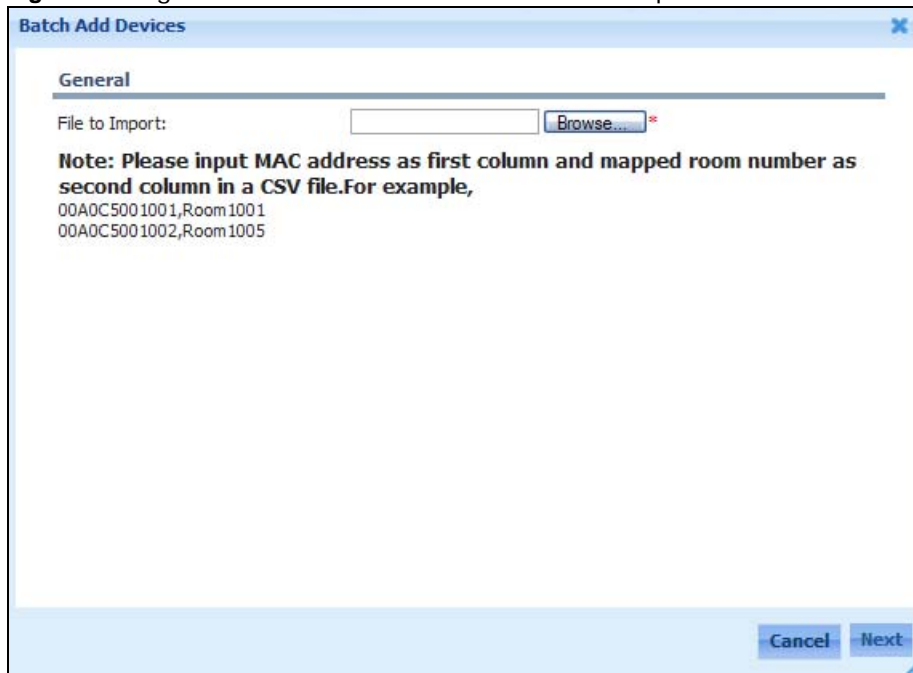
Table 13 Right-click Menus: Add Device

LABEL	DESCRIPTION
Read Community	Type the read-only community string the ENC uses to view information or settings on the device.
Write Community	Type the write community string the ENC uses to change settings on the device.
User Name	Enter the user name of the administrator account on the device.
Context Name	Enter the context name configured on the device. This setting should be the same on both the ENC and device in order to communicate with each other.
Authentication	Select which hash algorithm (None , MD5 or SHA1) to use to authenticate SNMP packets transmitted between the ENC and the device. SHA1 is generally considered stronger than MD5 , but it is also slower.
Auth. Password	<p>This field is available if you selected MD5 or SHA1 in the Authentication field.</p> <p>Enter the authentication key, which depends on the authentication algorithm you selected.</p> <p>MD5 - a key 16-20 characters long</p> <p>SHA1 - a key 20 characters long</p> <p>You can use any alphanumeric characters or ; ` ~ ! @ # \$ % ^ & * () _ + \ { } ' : . / < > = - ". If you want to enter the key in hexadecimal, type "0x" at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in "0123456789ABCDEF" is in ASCII format.</p>
Privacy	<p>This field is available if you selected MD5 or SHA1 in the Authentication field.</p> <p>Select which encryption algorithm to use for SNMP packets transmitted between the ENC and the device.</p> <p>None - no encryption key or algorithm</p> <p>DES - a 56-bit key with the DES encryption algorithm</p> <p>AES - a 128-bit key with the AES encryption algorithm</p>
Privacy Password	<p>This field is available if you selected DES or AES in the Privacy field.</p> <p>Enter the encryption key with the length according to the Privacy setting.</p>
Cancel	Click this to exit this screen and go back to the previous screen.
Previous	Click this to go back to the last screen.
OK	Click this to save the settings.

1.3.5.4 Batch Add Devices

Use this screen to add multiple devices to the ENC. To open this screen, right-click the **Root Subnet** or a network and select **Batch Add Devices**.

Note: At the time of writing, this feature is only for NWA1300 Series.

Figure 24 Right-click Menus: Batch Add Devices - Step 1


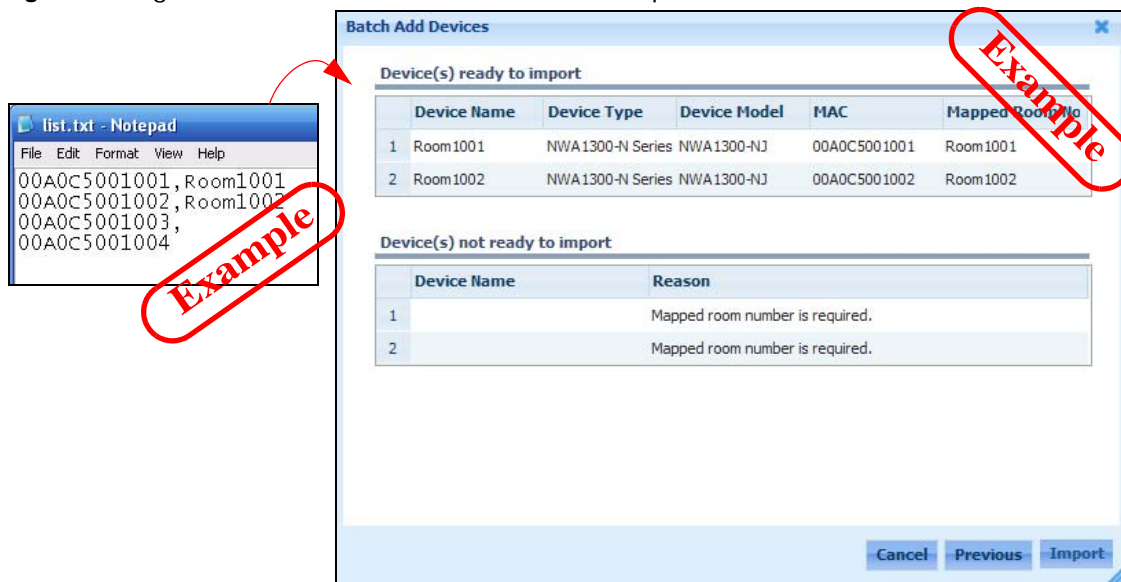
Batch Add Devices

General

File to Import: **Browse...**

Note: Please input MAC address as first column and mapped room number as second column in a CSV file. For example,
 00A0C5001001,Room1001
 00A0C5001002,Room1005

Cancel **Next**

Figure 25 Right-click Menus: Batch Add Devices - Step 2


list.txt - Notepad

```
File Edit Format View Help
00A0C5001001,Room1001
00A0C5001002,Room1002
00A0C5001003,
00A0C5001004
```

Batch Add Devices

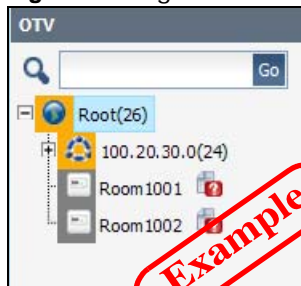
Device(s) ready to import

	Device Name	Device Type	Device Model	MAC	Mapped Room No
1	Room1001	NWA1300-N Series	NWA1300-NJ	00A0C5001001	Room1001
2	Room1002	NWA1300-N Series	NWA1300-NJ	00A0C5001002	Room1002

Device(s) not ready to import

	Device Name	Reason
1		Mapped room number is required.
2		Mapped room number is required.

Cancel **Previous** **Import**

Figure 26 Right-click Menus: Batch Add Devices - Step 3

The following table describes the labels in this screen.

Table 14 Right-click Menus: Batch Add Devices

LABEL	DESCRIPTION
Batch Add Devices - Step 1	
File to Import	Double click the field or click Browse to locate the text or CSV file you want to import. The file should contains devices' MAC address and room number mappings by following the format below: 00A0C5001001,Room1001 00A0C5001002,Room1002
Cancel	Click this to exit this screen and go back to the previous screen.
Next	Click this to proceed to the next screen.
Batch Add Devices - Step 2	
Device(s) ready to import	This section displays the list of devices that are ready to be imported.
Device Name	This field displays the name of a device.
Device Type	This field displays the device type you just selected.
Device Model	This field displays the model name and the associated icon you just selected.
MAC	Enter the MAC address of the device.
Mapped Room No.	Enter the number of the room where the device is located.
Device(s) not ready to import	This section displays the list of devices that are not ready to be imported because of insufficient information.
Device Name	This field displays the name of a device.
Reason	This field displays the reason why the ENC cannot import the device yet.
Cancel	Click this to exit this screen and go back to the previous screen.
Previous	Click this to go back to the last screen.
Import	Click this to start the import process.

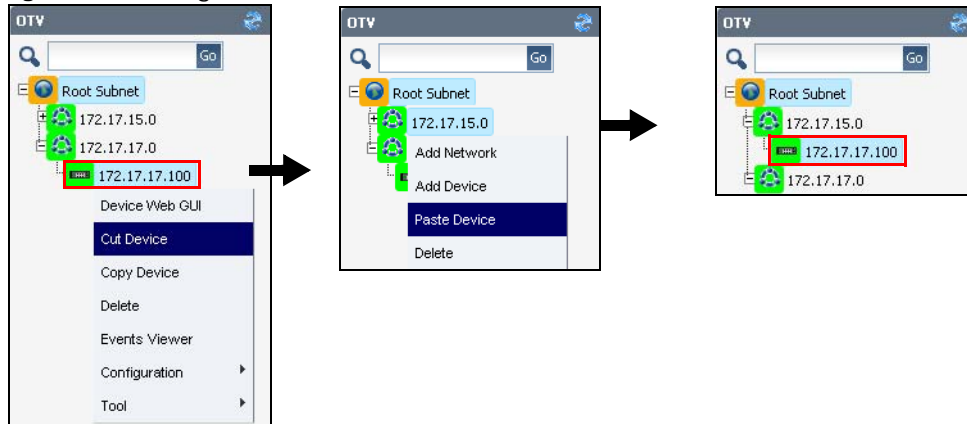
1.3.5.5 Cut/Paste Device

To disassociate a device from a network, log into the Web Configurator as an administrator or operator and do the following steps.

- 1 In the OTV panel, right-click on a device and click **Cut Device**.
- 2 Right-click on a network to which you want to move the device and click **Paste Device**.
- 3 The device re-associates to the network.

The following figure shows you an example of moving a device from one network to another. You may need to modify the device name and IP address by double-clicking the device.

Figure 27 Moving a Device



1.3.5.6 Copy/Paste Device

Copying a device and pasting it to another network in the OTV panel is similar to cutting and pasting a device. The difference is **Copy Device** does not remove the device from the original network. You may want to copy a device if you want to manually add a device and the device's configuration is similar to the one from which you want to copy.

1.3.6 Common Icons

This table describes the icons the ENC commonly uses.

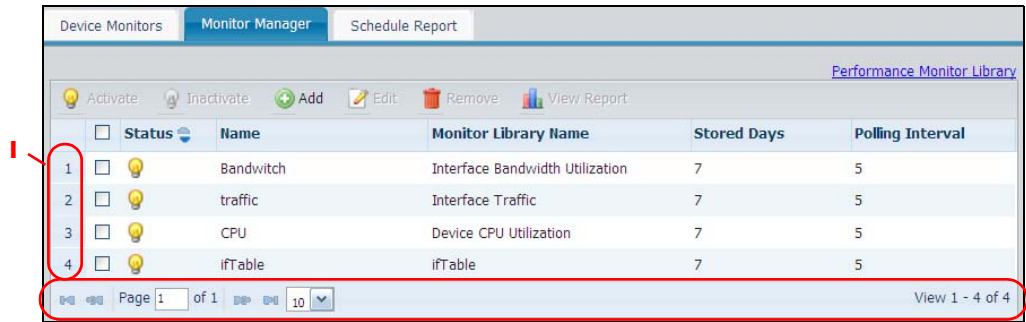
Table 15 Common Icons

ICON	DESCRIPTION
	An Info event occurred on the device and it has not been acknowledged. Click this to view the event details. An event is a log entry generated when an associated alarm occurs on a device. Use an event icon as a reminder that notifies you a to-do list. To clear the icon in the OTV, you have to acknowledge all the events on the device (see Section 2.1 on page 47).
	A Major event occurred on the device and it has not been acknowledged. Click this to view the event details.
	A Minor event occurred on the device and it has not been acknowledged. Click this to view the event details.
	The ENC is collecting the device's performance information. Click this to view raw data and reports.
	Online. The device or all devices in the network are online and accessible from the ENC.
	Partial Online. Some devices in the network are online but some are either off or not accessible from the ENC.
	Un-Monitored. The device or network is temporarily not managed by the ENC.
	Offline. The device or network is not accessible from the ENC.
	Edit AP Profile. The device has not yet been applied any wireless AP profile. Click this icon to configure it.

1.3.7 Working with Tables






Many screens in the Web Configurator contain tables to provide information or additional configuration options. This section describes the fields the ENC commonly uses in tables.

Figure 28 Common Fields in Tables



This table describes the highlighted part in the screen above.

Table 16 Common Fields in Tables

LABEL	DESCRIPTION
I	This indicates the index number of each entry in the table.
	Click this to display the first page.
	Click this to display the previous page.
Page X of X	This displays the page number and total number of pages.
	Click this to display the next page.
	Click this to display the last page.
	Select the maximum number of entries to display in one page.
View X - X of X	This displays the entry numbers and total number of entris. For example, "View 1 - 10 of 100" means the current page displays entries from 1 to 10 and there are 100 entries in total. No records to view displays if no entry to be displayed.

1.3.7.1 Manipulating Table Display

Here are some of the ways you can manipulate the Web Configurator tables.

- 1 Click a column heading to sort the table's entries in ascending alphabetical order according to that column's criteria. Click it again to sort the table's entries in descending (reverse) alphabetical order.

Figure 29 Sorting Table Entries by a Column's Criteria - Ascending

	Status	Name	Monitor Library Name	Stored Days	Polling Interval
1	<input type="checkbox"/>	Bandwitch	Interface Bandwidth Utilization	7	5
2	<input type="checkbox"/>	CPU	Device CPU Utilization	7	5
3	<input type="checkbox"/>	ifTable	ifTable	7	5
4	<input type="checkbox"/>	traffic	Interface Traffic	7	5

Page 1 of 1 View 1 - 4 of 4

Figure 30 Sorting Table Entries by a Column's Criteria - Descending

	Status	Name	Monitor Library Name	Stored Days	Polling Interval
1	<input type="checkbox"/>	traffic	Interface Traffic	7	5
2	<input type="checkbox"/>	ifTable	ifTable	7	5
3	<input type="checkbox"/>	CPU	Device CPU Utilization	7	5
4	<input type="checkbox"/>	Bandwitch	Interface Bandwidth Utilization	7	5

Page 1 of 1 View 1 - 4 of 4

- 2 Select a column heading cell's right border and drag to re-size the column.

Figure 31 Resizing a Table Column

	Status	Name	Monitor Library Name	Stored Days	Polling Interval
1	<input type="checkbox"/>	traffic	Interface Traffic	7	5
2	<input type="checkbox"/>	ifTable	ifTable	7	5
3	<input type="checkbox"/>	CPU	Device CPU Utilization	7	5
4	<input type="checkbox"/>	Bandwitch	Interface Bandwidth Utilization	7	5

Page 1 of 1 View 1 - 4 of 4

Application

8.1 Overview

Use the sub-menus under **Application** to look at and configure specific functions such as RMON (Remote Network Monitor), VLAN, port management and Wireless Access Point settings for ZyXEL Ethernet Switches.

8.1.1 What You Can Do in This Chapter

- Use the **Application > RMON** screens (see [Section 8.3 on page 190](#)) to configure RMON statistics, history, event and alarm settings.
- Use the **Application > VLAN Management** screens (see [Section 8.6 on page 207](#)) to configure VLAN settings for specific devices.
- Use the **Application > Port Management** screens (see [Section 8.7 on page 218](#)) to configure port management basic, bandwidth control, broadcast storm control, security, authentication settings for specific devices.
- Use the **Application > AP Manager** screen (see [Section 8.12 on page 234](#)) to configure wireless settings for specific devices which supports wireless access point function.

8.2 RMON Introduction

Similar to SNMP, RMON (Remote Network Monitor) allows you to gather and monitor network traffic.

Both SNMP and RMON use an agent, known as a probe, which are software processes running on network devices to collect information about network traffic and store it in a local MIB (Management Information Base). With SNMP, a network manager has to constantly poll the agent to obtain MIB information. With RMON, the probe is located on a remote device (ZyXEL Ethernet Switches), so a network manager (the ENC) does not need to constantly poll the probe for information. The probe communicates with the network manager via SNMP.

RMON groups contain detailed information about specific activities. The following table describes the RMON groups that the ZyXEL Ethernet Switches support.

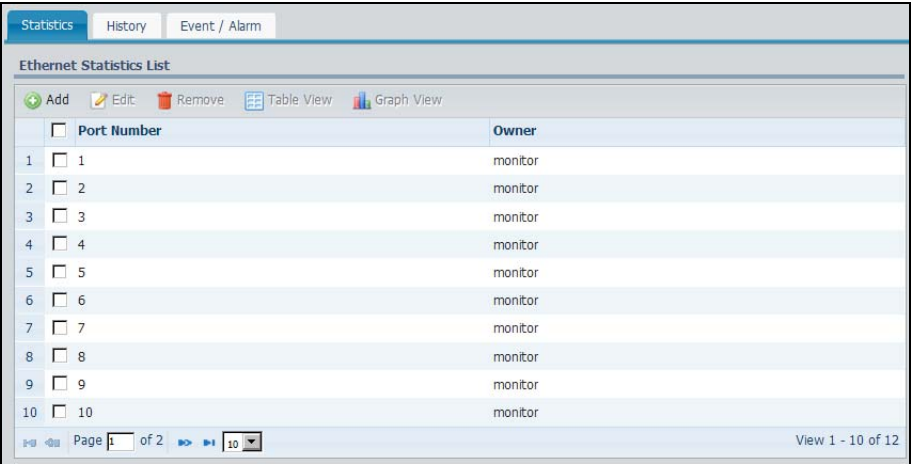
Table 81 Supported RMON Groups

GROUP	DESCRIPTION
Statistics	Defines event generation and resulting actions to be taken based on an alarm.
History	Records network traffic information on a specified Ethernet port.
Event/Alarm	Provides alerts when configured alarm conditions are met.

8.3 Statistics

Use this screen to look at network statistics on a selected device's ports. To open this screen, click a device that supports this feature in the OTV, Device View or Group View panel and click **Application > RMON > Statistics**. Then, select one or more ports or interfaces for which you want to view network statistics.

Figure 140 RMON > Statistics



The screenshot shows the 'Statistics' tab selected in the top navigation bar. Below it are 'History' and 'Event / Alarm' tabs. The main area is titled 'Ethernet Statistics List' and contains a toolbar with 'Add', 'Edit', 'Remove', 'Table View', and 'Graph View' buttons. A table lists 10 ports, each with a checkbox, a 'Port Number' column, and an 'Owner' column. All owners are listed as 'monitor'. At the bottom, there is a pagination control showing 'Page 1 of 2' and a 'View 1 - 10 of 12' indicator.

	<input type="checkbox"/>	Port Number	Owner
1	<input type="checkbox"/>	1	monitor
2	<input type="checkbox"/>	2	monitor
3	<input type="checkbox"/>	3	monitor
4	<input type="checkbox"/>	4	monitor
5	<input type="checkbox"/>	5	monitor
6	<input type="checkbox"/>	6	monitor
7	<input type="checkbox"/>	7	monitor
8	<input type="checkbox"/>	8	monitor
9	<input type="checkbox"/>	9	monitor
10	<input type="checkbox"/>	10	monitor

The following table describes the labels in this screen.

Table 82 RMON > Statistics

LABEL	DESCRIPTION
Add	Click this to create an entry. Note: At the time of writing, this function is only available for ZyXEL Ethernet Switches using 3.90 firmware version.
Edit	Select an entry in the table and click this to modify it.
Remove	Select an entry in the table and click this to delete it.
Table View	Select one or more ports or interfaces in the table and click this to display the network statistics as a table.
Graph View	Select one port or interface in the table and click this to display the network statistics as a graph.
check box	Select the check box of an entry and click Edit , Remove , Table View or Graph View to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Port Number	This field displays the number of the port or interface on the selected device.
Owner	This field displays the application name that created this entry.

8.3.1 Add/Edit an RMON Port

If you want to view network statistics on one port or interface but the port is not in the **Ethernet Statistics List** in the **Application > RMON > Statistics** screen, click **Add** to add the port or interface. To do this, select a device that supports this feature in the OTV, Device View or Group View panel and click **Add** in the **Application > RMON > Statistics** screen.

You can also change the RMON owner setting for the port or interface by selecting it and then clicking **Edit** in the **Application > RMON > Statistics** screen.

Note: At the time of writing, this screen is only available for ZyXEL Ethernet Switches using 3.90 version firmware.

Figure 141 RMON > Statistics > Add/Edit

The following table describes the labels in this screen.

Table 83 RMON > Statistics > Add/Edit

LABEL	DESCRIPTION
Port Number	Enter the number of one port or interface to add to the ENC for viewing network statistics. This field displays the port's number and is read-only when you are editing a port statistic entry.
Owner	Enter a descriptive name of the application that creates this entry. You can use 1-31 printable ASCII characters. Spaces are allowed.
Cancel	Click this to discard all changes and close the screen.
Ok	Click this to save the settings and close this screen.

8.3.2 Viewing the Table

This screen displays network statistics for the selected port(s) or interface(s) as a table. After selecting the data source(s) you wish to display, click **Table View** on the **Application > RMON > Statistics** screen to open this screen.

Figure 142 RMON > Statistics > Table View

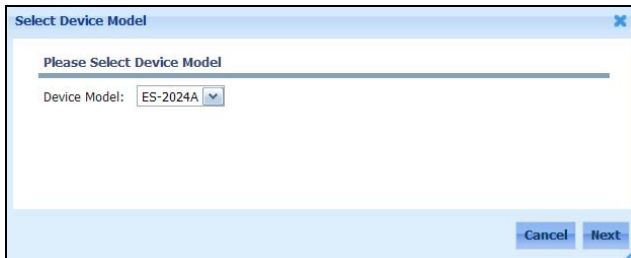
	Port Number	Octets	Total Packets	Broadcast Packets	Multicast Packets	Unicast Packets	U
1	6	645963257	6813328	2105017	4640592	67719	
2	8	0	0	0	0	0	
3	10	1609863972	21647380	2650594	6037526	12959260	

The following table describes the labels in this screen.

Table 84 RMON > Statistics > Table View

LABEL	DESCRIPTION
Device IP	This field displays the IP address of the selected device.
Port Number	This field displays the number of the selected port(s) or interface(s).
Polling Interval	Enter the number of seconds (5~3600) between data samplings the ENC retrieves from the selected device. Click Start Polling to have the ENC start to retrieve data from the device or Stop Polling to stop it. You have to stop pollings first if you want to change the settings for graphic display.
Delta Value	Select this to use Delta value as the method of obtaining the sample value. Clear this to use Absolute value as the method instead. Delta means the value is from the data sampled in each configured time interval. Absolute means the sampling value is accumulated since it started.
	The first column displays the index number of a data sampling. The number also indicates the order in which the port or interface (within all the selected ports or interfaces) is sampled.
Port Number	This is the number of the port or interface from which the ENC polled the data.
Octets	Select this to display the total number of octets received/transmitted on the port(s).
Total Packets	Select this to display the total number of all good packets received/transmitted on the port(s).
Broadcast Packets	This is the total number of good broadcast packets received/transmitted on the port(s).
Multicast Packets	This is the total number of good multicast packets received/transmitted on the port(s).
Unicast Packets	This is display the total number of good unicast packets received/transmitted on the port(s).
Undersize Packets	This is display the number of packets dropped by the port(s) because they were less than 64 octets long, and contained a valid FCS.
Fragments	This is display the number of packets received/transmitted on the port(s) because they were less than 64 octets long, and contained an invalid FCS, including non-integral and integral lengths.
Oversize Packets	This is display the number of packets dropped by the port(s) because they were longer than 1518 octets and contained an invalid FCS, including alignment errors in the graph of this section.
Jabbers	This is display the number of packets received/transmitted on the port(s) because they were longer than 1518 octets (non VLAN) or 1522 octets (VLAN) and contained an invalid FCS, including alignment errors.
64 Octets	This is the number of packets (including bad packets) received that were 64 octets in length in the graph of this section.
65~127 Octets	This is the number of packets (including bad packets) received that were between 65 and 127 octets in length in the graph of this section.
128~255 Octets	This is the number of packets (including bad packets) received that were between 128 and 255 octets in length in the graph of this section.
256~511 Octets	This is the number of packets (including bad packets) received that were between 256 and 511 octets in length in the graph of this section.
512~1023 Octets	This is the number of packets (including bad packets) received that were between 512 and 1023 octets in length in the graph of this section.
1024~1518 Octets	This is 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 in the graph of this section.

- 10 Select the device model (**ES-2024A**) and click **Next**.



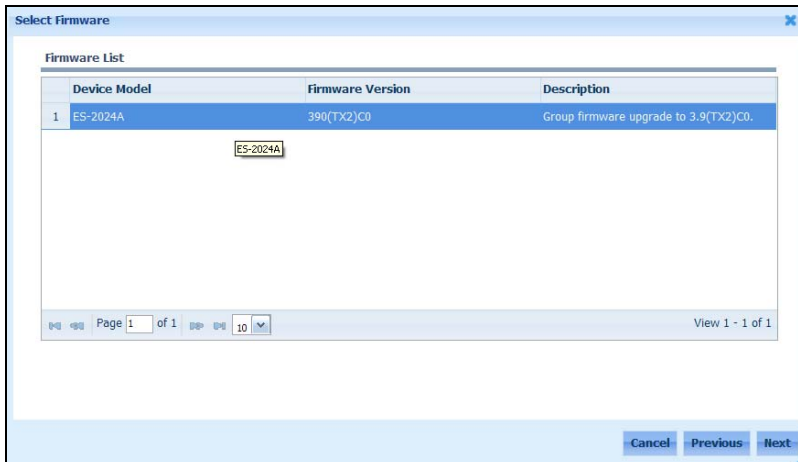
Select Device Model

Please Select Device Model

Device Model: ES-2024A

Cancel Next

- 11 The **Select Firmware** screen appears. Select the file for firmware upgrade and click **Next**.



Select Firmware

Firmware List

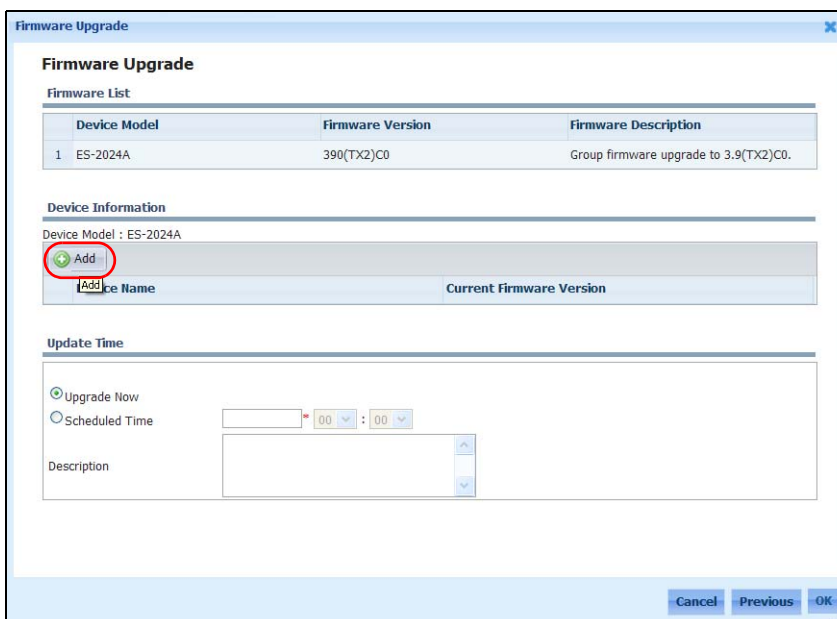
	Device Model	Firmware Version	Description
1	ES-2024A	390(TX2)C0	Group firmware upgrade to 3.9(TX2)C0.

ES-2024A

Page 1 of 1 View 1 - 1 of 1

Cancel Previous Next

- 12 Click **Add** in the **Device Information** section in the next screen.



Firmware Upgrade

Firmware List

	Device Model	Firmware Version	Firmware Description
1	ES-2024A	390(TX2)C0	Group firmware upgrade to 3.9(TX2)C0.

Device Information

Device Model : ES-2024A

Add

Add Name Current Firmware Version

Update Time

☒ Upgrade Now

☐ Scheduled Time

Description

Cancel Previous OK

- 13 The **Select Devices** screen appears. Select **Switches** from the **Group** field and click **Search**.

Select the device(s) you want to upgrade from the **Available List**, click > to make them appear in the **Selected List**. Click **Ok**.

Select Devices

By Search | By OTV

Device Type: Switch Device Model: ES-2024A

Display Name: IP Address:

Firmware: Group: Switches

Search

Available List

172.23.44.122

Showing 1 of 1

Selected List

--

Showing 0 of 0

> >> << <

Cancel Ok

- 14 Select **Upgrade Now** and click **OK** to start firmware upgrade immediately.

Firmware Upgrade

Firmware List

Device Model	Firmware Version	Firmware Description
1 ES-2024A	390(TX2)C0	Group firmware upgrade to 3.9(TX2)C0.

Device Information

Device Model : ES-2024A

+ Add

Device Name	Current Firmware Version
1 172.23.44.122	3.70

Update Time

☒ Upgrade Now

☐ Scheduled Time

Description

Cancel Previous **OK**

Do not turn off the devices while firmware upgrade is in process.

- 15 Wait a while until firmware upgrade is completed (**Success** displays in the **Status** field).

The screenshot shows the 'Schedule List' interface. At the top, there are tabs for 'Firmware List' and 'Schedule List'. Below the tabs is a search bar labeled 'Device Name:'. Underneath are three icons: 'Add' (green plus), 'Edit' (pencil), and 'Remove' (trash). The main part of the interface is a table with the following columns: Status, Update Time, Device Model, Firmware Versior, Total Device, Description, and Admin. There is one row in the table with the following data: Status is 'Success' (circled in red), Update Time is '2010-10-30 23:00:00', Device Model is 'ES-2024A', Firmware Versior is '390(TX2)C0', Total Device is '1', and Admin is 'admin'. At the bottom of the table, it says 'Page 1 of 1' and 'View 1 - 1 of 1'.

Status	Update Time	Device Model	Firmware Versior	Total Device	Description	Admin
Success	2010-10-30 23:00:00	ES-2024A	390(TX2)C0	1		admin

See [Chapter 10 on page 263](#) for how to troubleshoot if it fails.

2.3 Configuration Backup for Multiple Devices

The ENC allows you to back up remote devices according to a schedule. This tutorial shows you an example including the following:

- create a new backup schedule
- perform configuration backup
- check the result

The following shows how to configure step by step:

- 1 Click **Configuration > Update/Backup > Backup Schedule List**, click **Add**.

The screenshot shows the 'Backup Schedule List' interface. At the top, there are tabs for 'Configuration File List', 'Backup Schedule List', and 'Update Schedule List'. Below the tabs is a search bar labeled 'Device Name:'. Underneath are three icons: 'Add' (green plus, circled in red), 'Edit' (pencil), and 'Remove' (trash). The main part of the interface is a table with the following columns: Status, File Name, Total Device, Backup Time, Description, and Admin. The table is empty, and at the bottom, it says 'Page 1 of 0' and 'No records to view'.

Status	File Name	Total Device	Backup Time	Description	Admin
--------	-----------	--------------	-------------	-------------	-------

- 2 Enter the file name to which you want to save the device's configuration (**SwitchWeeklyBackup** in this example). Click **Add**.

The screenshot shows the 'Add Backup' form. It has a section titled 'Backup' with a 'File Name' field containing 'SwitchWeeklyBackup' (circled in red) and a 'Description' field. Below this is a 'Device List' section with an 'Add' button (green plus, circled in red) and a table with columns 'Device Name' and 'Device Model'.

- 3 Select the devices to back up the configuration. Click **Ok**.

Note: Configuration backup is not limited to devices of the same model.

- 4 Select **Scheduled Time** and click the text box to select a preferred date. Select a time using the drop list box and then click **OK**.

Do not turn off the devices while configuration backup is in process.

- 5 After the backup is completed, you should see **Success** in the **Status** field.

Backup Schedule List

Device Name:

Search

Add

Edit

Remove

<input type="checkbox"/>	Status	File Name	Total Device	Backup Time	Description	Admin
1	Success	SwitchWeeklyBackup	9	2010-10-30 10:00:00		admin

Page 1of 110

View 1 - 1 of 1









- 6 If you see **Partial Success** or **Fail** in the **Status** field at step 5, check the **Events > Viewer** screen for the details. See [Section 10.10 on page 267](#) for how to trouble the problem.

Figure 36 Configuration Backup Result in Event Viewer

Viewer

Show Search

Acknowledge

	<input type="checkbox"/>	Ack/UnAck	Name	Date/Time	Category	Severity	Source	Message
1	<input type="checkbox"/>		Configuration Backup Succeeded	2010-10-28 17:48:12	Configuration	Info	172.23.37.17 	Backup configuration from device 172.23.37.17 into test successfully.
2	<input type="checkbox"/>		Configuration Backup Succeeded	2010-10-28 17:48:11	Configuration	Info	172.23.26.121 	Backup configuration from device 172.23.26.121 into test successfully.
3	<input type="checkbox"/>		Configuration Backup Failed	2010-10-28 17:39:11	Configuration	Minor	172.23.26.106 	Backup configuration from device 172.23.26.106 into test failed. Download the file from FTP failed.
4	<input type="checkbox"/>		Configuration Backup Failed	2010-10-28 10:27:11	Configuration	Minor	172.25.27.220 	Backup configuration from device 172.25.27.220 into test failed. Download the file from FTP failed.

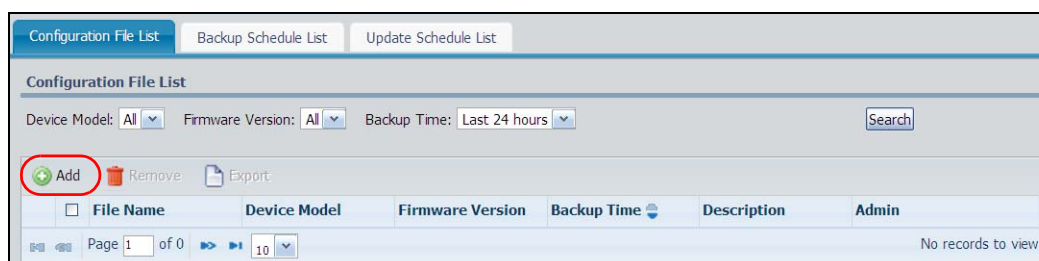
2.4 Configuration Restore to a Device

The ENC allows you to restore a configuration file to one or multiple devices with the same model according to a schedule. This tutorial shows you an example including the following:

- prepare a configuration file on the ENC through device backup or file upload
- create a new schedule for uploading the file to specified device(s)
- perform configuration upload
- check the result

The following shows how to configure step by step:

- 1 Click **Configuration > Update/Backup > Configuration File List** and then **Add**.



- 2 The **Add File** screen appears. Select **Backup From Device**, enter a name (**ES-2108_Conf**) for the backup file. Click **Add** to open **Select Devices** screen.

Note: You can also upload an existing configuration file to the ENC by selecting **Upload File** in this screen.

Add File

☒ Backup From Device ☐ Upload File

File Name: ES-2108_Conf

Description:

Device List

Device Name	Device Model	Firmware Version
172.23.26.19	ES-2108	3.80

Cancel OK

- 3 In the **Select Device** screen, select device(s) from which you want to get a configuration example. Click **OK**.
- 4 Click **OK** again in the next screen.
- 5 Click **Search** to update this screen or go to another screen and then back. If the file appears in the configuration file list, you have successfully backed up the configuration file from the device.

Configuration File List

Device Model: All Firmware Version: All Backup Time: Last 24 hours Search

Add Remove Export

	File Name	Device Model	Firmware Version	Backup Time	Description	Admin
1	ES-2108_Conf	ES-2108	3.70	2010-10-28 19:34:04		admin
2	ES-2108_Conf	ES-2108	3.60	2010-10-28 19:34:02		admin

Page 1 of 1 View 1 - 2 of 2

- 6 Click the **Update Schedule List** tab and then **Add** icon.

Configuration File List Backup Schedule List **Update Schedule List**

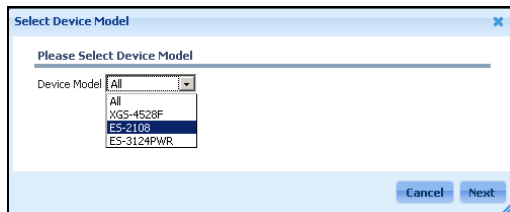
Device Name: Search

Add Edit Remove

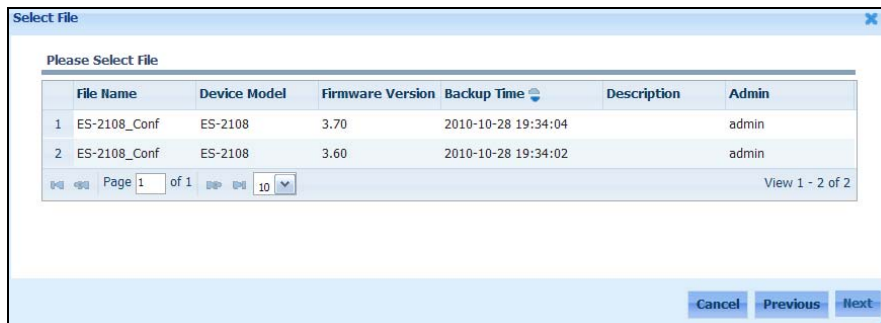
Status	File Name	Device Model	Total Device	Update Time	Admin
No records to view					

Page 1 of 0

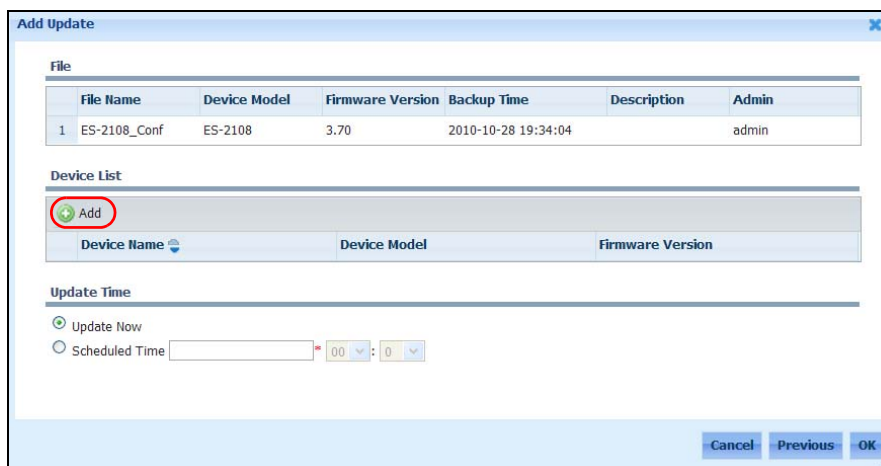
- 7 Select the device model (**ES-2108** in this example) you wish to upload the configuration file and then click **Next**.



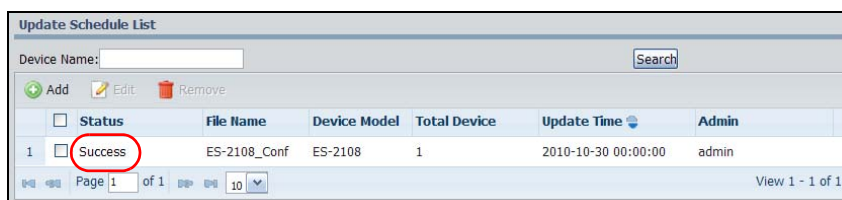
- 8 Select the configuration file you just uploaded and then click **Next**.



- 9 Click **Add**.



- 10 In the **Select Device** screen, select the device(s) to which you want to apply the configuration file. Click **OK**.
- 11 Select **Update Now** and then click **OK** to start configuration update.
- 12 After the configuration file is successfully uploaded, you should see **Success** in the **Status** field.



2.5 Script Distribution to Multiple Devices

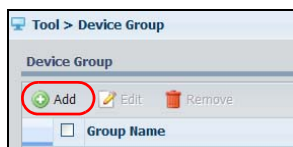
The ENC allows you to write CLI commands and apply them to multiple devices. This tutorial shows you an example including the following:

- group devices (optional)
- create a new script
- specify devices
- write CLI commands or load commands from a file
- configure a schedule
- perform script distribution
- check the result

Note: Make sure the ENC can access the devices via telnet before using this function. This includes enabling the Telnet service on the devices and configuring any firewall devices between the ENC and the devices to allow telnet access.

The following shows how to configure step by step:

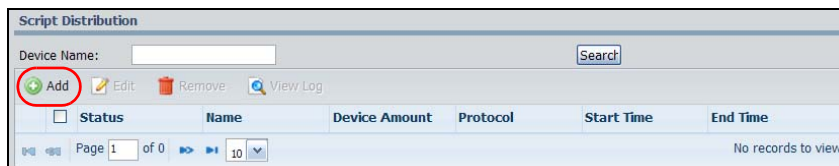
- 1 Click **Tool > Device Group**. Enter a name and the description for the group and then click **Add**.



- 2 In the **Select Devices** screen, select the device(s) to add to the group and click **Ok**.
- 3 Click **Ok** again in the next screen.
- 4 The group should be created successfully as shown next.

	Group Name	Total Device	Description
1	Switches	2	ZyXEL Ethernet Switches

- 5 Click **Configuration > Script Distribution** and then **Add**.



- 6 The **Add Script Distribution** screen appears. Select **Telnet** and enter the script name (**CollectBasicDeviceInfo** in this example). Leave the **Interval** to its default value. Click **Add**.

Add Script Distribution

General Setting

Protocol: ☒ Telnet ☐ SSH

Name:

Interval: 2~60 seconds

Device List

<input type="checkbox"/>	Device Name	IP Address	Model Name

Commands

```
#Usage:
# 1.use '#' for comments;
# 2.<command> | <keywords for response checking>;
#Example:
#show ip | ip interface
#It sends the 'show ip' command, and check response whether contains 'ip interface', otherwise, return fail.
```

- 7 In the **Select Device** screen, select the device(s) to which you want to apply the script. Click **OK**.
- 8 Type CLI commands in the **Commands** section. You can use a pound sign (#) to write a note in the script. Configure a schedule (select **Send Now** in this example). Click **Ok**.

Commands

```
#This script is to collect basic device information
show interface all
show firewall status
```

Schedule Time

☒ Send Now

☐ Schedule Time :

- 9 Wait a while until the script is successfully applied to the devices (**Success**, **Fail**, or **Partial Success** displays in the **Status** field). Select the script and then click **View Log**.

Script Distribution

Device Name:

<input type="checkbox"/>	Status	Name	Device Amount	Start Time	End Time
<input checked="" type="checkbox"/>	Success	CollectBasicDeviceInfo	2	2010-10-28 20:00:00	2010-10-28 24:24:03

Page 1 of 1

View 1 - 1 of 1

- 10 Then You can see the results of applying the CLI commands.

2.6 ENC Backup and Performing a Complete Auto-Discovery with Filters

Administrator Sam wants to clear all devices in the OTV and re-scan all ZyXEL firewall devices only in specific networks (for example, laboratory networks). This tutorial uses the following network topology and settings.

Figure 37 Network Topology in this Example

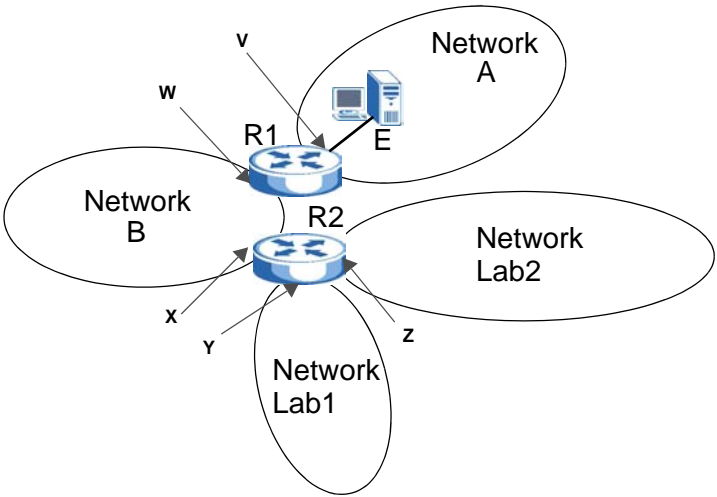


Table 17 IP Settings in this Example

LABEL	DESCRIPTION	IP ADDRESS
E	This is the ENC server.	1.1.1.250
Network A	A network where the ENC is located.	1.1.1.0/24
Network B	A network directly connected to the ENC.	2.2.2.0/24
R1	This router connects networks A and B.	v - 1.1.1.254 w - 2.2.2.254
R2	This router connects networks R and B.	x - 2.2.2.253 y - 3.3.3.254 z - 4.4.4.254
Network Lab1	The first network we want to scan in this example.	3.3.3.0/24
Network Lab2	The secondary network we want to scan in this example.	4.4.4.0/24

To do this, Sam has to know:

- how to back up the current ENC settings to a file
- how to perform a complete new auto-discovery
- how to configure seed settings
- how to configure discovery filter rules
- how to start auto-discovery
- how to update the OTV

The following shows you how to configure step by step:

- 1 Click **Maintenance > Backup/Restore** and configure to where to back up the current ENC's settings. In this example, you use **Local Host** and the default directory to store the backup file. Click **Apply** to save the settings.

Figure 38 Configure the Backup Location

Backup Location

Location: Local Host

Archive Location: C:\Program Files\ZyXEL\ENC\ENC\backup

Apply

- 2 Click the **BackUp** icon, the **BackUp** screen appears. Select **BackUp Database** and enter a name for the backup file (for example, **20100412ENCbackup**). Click **Ok**.

Figure 39 Back Up the ENC Database

Backup Location

Location: Local Host

Archive Location: C:\Program Files\ZyXEL\ENC\ENC\backup

Apply

Database Backup/Restore

BackUp Restore Remove

Name

Page 1 of 0

Schedule BackUp

Enable Schedule BackUp

Schedule Type

Time

Apply

BackUp

BackUp Type: BackUp Database Upload BackUp File

File Name: 20100412ENCbackup

Description:

Cancel Ok

No records to view

- 3 The ENC generates the file.

Figure 40 Back Up the ENC Database

Database Backup/Restore

BackUp Restore Remove

	Name	Time	Version	Note
1	20100412ENCbackup	2010-04-12 13:12:35	1.0.218.61.00	

Page 1 of 1

View 1 - 1 of 1

- 4 Click **Tool > Auto-Discovery** and select **Enable Ping** to use ping to detect ZyXEL firewall devices. Leave other settings not mentioned in the following steps to their defaults.

Figure 41 Enable Ping in the Auto-Discovery

General

Enable Ping

Enable resolve hostname / domain

- 5 Select **Root subnet / Complete** in the **Discover Option** field to clear all devices from the OTV and perform a brand-new scan.

Figure 42 Complete Discover

General

☒ Enable Ping

☒ Enable resolve hostname / domain

Timeout: *1~5 seconds

Retry: *0~3 times

Discover Option: **Root subnet / Complete**

- 6 Select **Entire Network** and enter **1** in the **Discover Type** and **Max. Hop Level** field. Click **Add** and enter the IP address and subnet mask of a device which is in network **Lab1** or **Lab2**. In this example, enter 3.3.3.254/255.255.255.0. You see the screen as shown next.

Figure 43 Seed Settings

Seeds

Discover Type: **Entire Network**

Max. Hop Level: **1**

Add

Seed	Net Mask
1 3.3.3.254	255.255.255.0

- 7 Select **v1** and **v2c** and enter a most commonly used community on the firewall devices in the **Read Community** field.

Figure 44 Seed Settings

SNMP

SNMP Version: ☒ v1 ☒ v2c ☐ v3

SNMP Port: *

Read Community: *

Note: The SNMP version selection depends on which SNMP versions your devices can support.

Note: The ENC will fail to get a device's information if the device uses a different read community.

- 8 Select the default discovery filter rule and click **Edit**, the **Edit Discovery Filter** screen appears. Select **Firewall** in the **Values** field. Then click **Ok**. This rule means the ENC only adds ZyXEL firewall devices to the OTV.

Figure 45 Discovery Filter Settings

Discovery Filters

Add **Edit**

Status	Property	Operation	Values
1	Device Type	equals	All

Edit Discovery Filter

Status: ☒ Active

Property: **Device Type**

Operation: **equals**

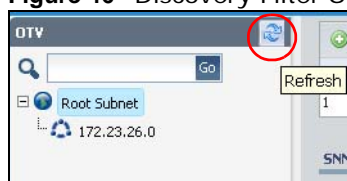
Values: **Firewall**

Cancel **Ok**

- 9 Click the **Discover** button to start finding devices.

- 10 Click the **Refresh** icon to update the OTV.

Figure 46 Discovery Filter Settings



2.7 Event Actions Triggered By Received Events

The ENC allows you to configure specific actions to notify administrators when it receives any or specific events. This tutorial shows an example including the following:

- configure mail relay settings on the ENC
- create a new event action (or configure the default event action)
- enable email notification and configure the mail subject and content
- associate the action to the Device Down event

The following shows you how to configure step by step:

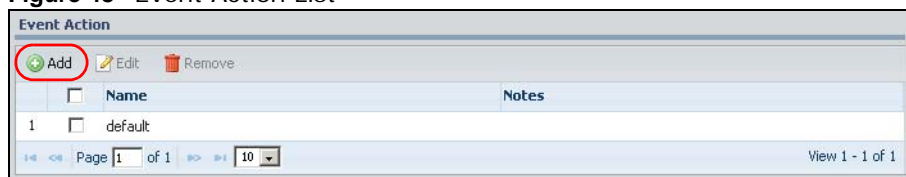
- 1 Click **Maintenance** > **Server**, configure the mail relay settings as shown next. Click **Apply**.

Figure 47 Mail Relay Settings

- 2 Click **Events** > **Event Action** and then **Add**.

Each default event (in **Events** > **Configuration** > **Default**) associates with the default event action (in **Events** > **Event Action**). You can also select the default event action and click **Edit** in this screen if you want the action to apply to all default events.

Figure 48 Event Action List



- 3 The **Add Event Action** screen appears. Configure the action name (**NotifyByMail**), enable e-mail notification, configure receiver e-mail addresses. Enter the mail subject and body using the variables provided in the list boxes. For example, type "A \$A event (\$B) occurred at \$C" where you click **Category of the alarm** for first variable \$A, **Severity of the alarm** for second variable \$B and **Time when alarm was generated** for third variable \$C. Click **Test Action** to make a test.

- 4 If you see **Send notification successfully**, you should receive a mail as shown. See [Section 10.6 on page 266](#) if you get an error message.



- 5 Click **Events > Configuration > Default**, select the **Device Down** event and click **Edit**.

Note: If you cannot find a particular event in this **Default** screen, click **Events > Configuration > Customize** and **Add** to customize an event.

Events Configuration				
<div> <div>Edit</div> <div>2</div> </div>				
	Category	Event Name	Severity	Action
1	Configuration	Configuration Backup Failed	Minor	default
2	Configuration	Configuration Backup Succeeded	Info	default
3	Configuration	Configuration Update Failed	Minor	default
4	Configuration	Configuration Update Succeeded	Info	default
5	Configuration	Firmware Upgrade Failed	Minor	default
6	Configuration	Firmware Upgrade Succeeded	Info	default
7	Configuration	Script Execution Failed	Minor	default
8	Configuration	Script Execution Succeeded	Info	default
9	SNMP Traps	Authentication Failure	Minor	default
10	SNMP Traps	Cold Start	Minor	default
11	SNMP Traps	egpNeighborLoss	Info	default
12	SNMP Traps	LinkDown	Minor	default
13	SNMP Traps	LinkUp	Info	default
14	SNMP Traps	Warm Start	Info	default
15	Threshold Crossing	Falling Threshold	Minor	default
16	Threshold Crossing	Raising Threshold	Minor	default
17	Topology	Device Down	Major	default
18	Topology	Device Up	Info	default

- 6 The **Edit Events Configuration** screen appears. Select the **NotifyByMail** action in the **Action** field. Click **OK**.

Edit Events Configuration

Event Name

Device Down *

Category

Topology

Trap OID

1.3.6.1.4.1.890.1.13.2.1.4.1.4

Severity

Major

Message

Device is down: \$1:\$2,\$3. *

\$1:Node

IP

\$2:Node

Name

\$3:Node

Type

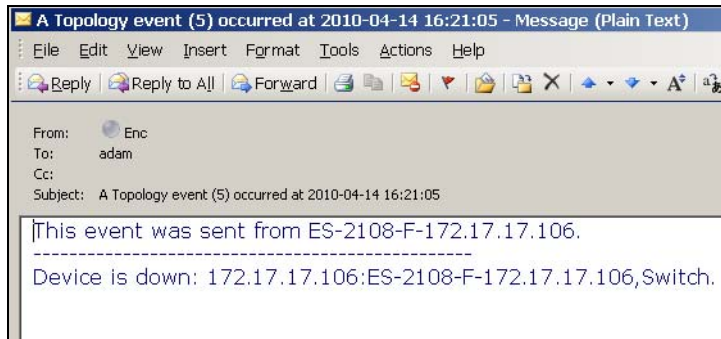
Action

NotifyByMail

Cancel

OK

- 7 If any managed device is down, you should receive a mail as shown next.



2.8 Performance Monitoring for Interfaces

You can monitor device status and display the changes in a graph through the ENC. This tutorial shows you how to configure settings to monitor traffic statistics on a device's interface. This tutorial includes the following:

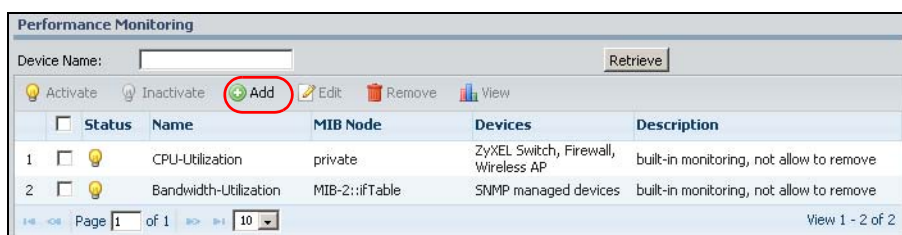
- choose the device to be monitored
- check if you can use any default performance monitor libraries (templates) or you need to customize one.
- configure a new performance monitor
- associate devices with the monitor
- configure the view to display statistics as a graph
- specify instances you wish to see in the graph
- monitor the changes over time

The following shows you how to configure step by step:

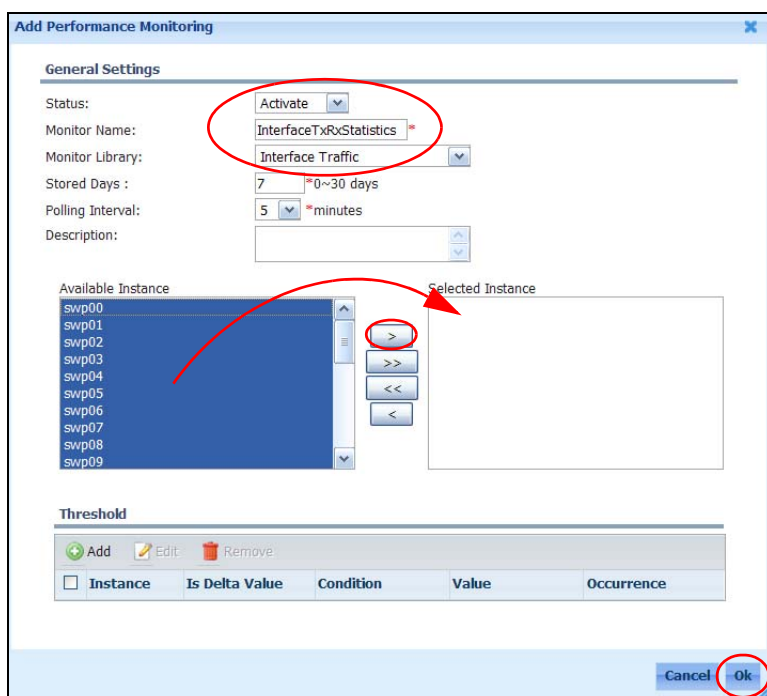
- 1 Click the device that you want to monitor the interface performance in the OTV panel.
- 2 Click **Configuration > Performance Monitor Library > Default Monitor Library**. See if you can use any default monitor library. If not, you can create a new one in the **Customized Monitor Library** screen. This example will use the **Interface Traffic** Monitor library.

Default Monitor Library		Customized Monitor Library	
Name	MIB Node	Description	
1 Device CPU Utilization	cpu	Monitor the device CPU utilization	
2 Memory Utilization	memory	Monitor the device memory utilization	
3 Interface Bandwidth Utilization	ifSpeed, ifOutOctets, ifInOctets	Monitor the interface bandwidth utilization	
4 Interface Traffic	ifOutOctets, ifInOctets	Monitor the traffic of all interfaces	
5 Interface Unicast Traffic	ifOutUcastPkts, ifInUcastPkts	Monitor the unicast traffic of all interfaces	
6 Interface Non-unicast Traffic	ifOutNUcastPkts, ifInNUcastPkts	Monitor the non-unicast traffic of all interfaces	
7 Interface Errors	ifOutErrors, ifInErrors	Monitor the errors of all interfaces	

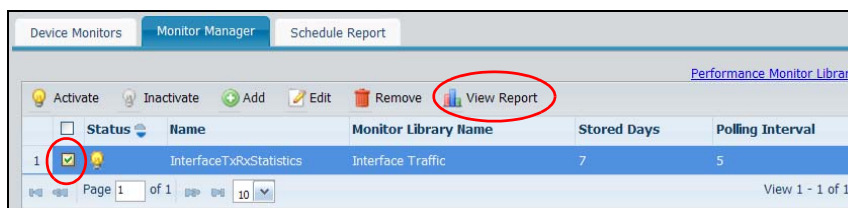
- 3 Click **Tool > Performance Monitoring > Monitor Manager** and then **Add**.



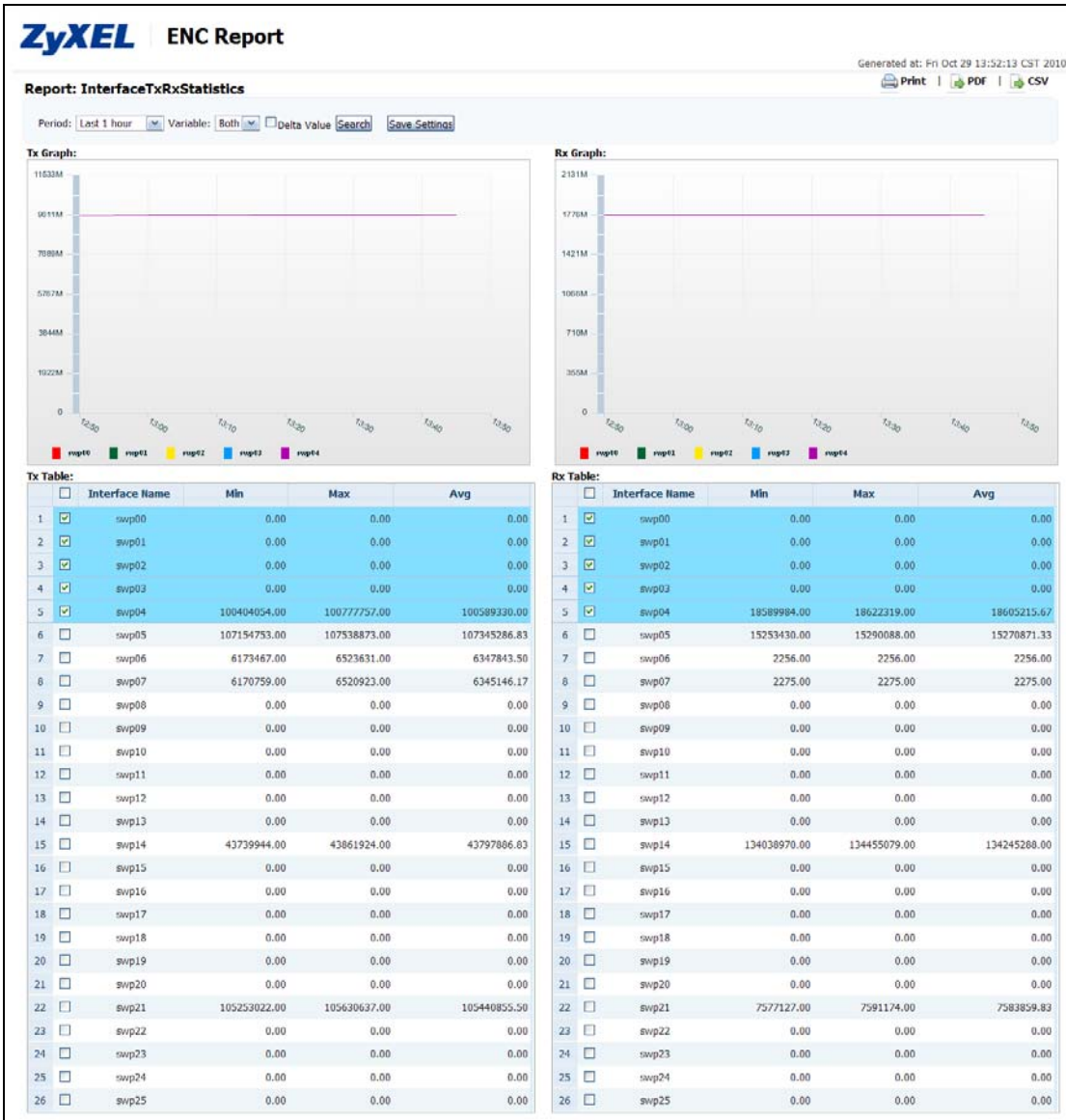
- 4 Activate this monitor and configure its name (**InterfaceTxRxStatistics**) and library (**Interface Traffic**). Select the instances you want to use (this example selects all) and click > to move them to the **Selected Instance** list. Click **Ok**.



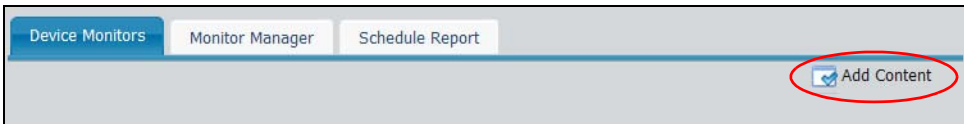
- 5 You will see the monitor has been created in the **Monitor Manager** screen. Select it and click **View Report**.



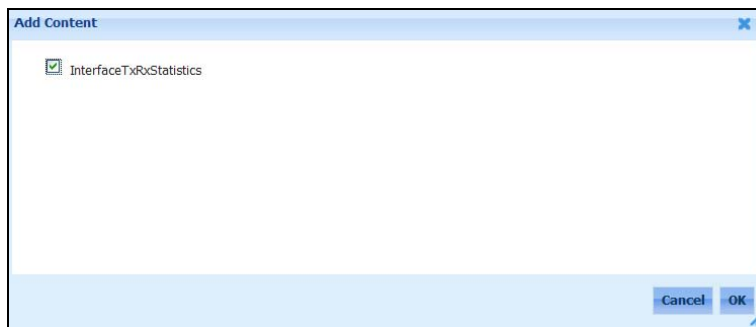
- 6 You will see the report. The following is an example. You can select up to 5 interfaces in the Tx and Rx tables at the bottom of the screen to display them in the graphics.



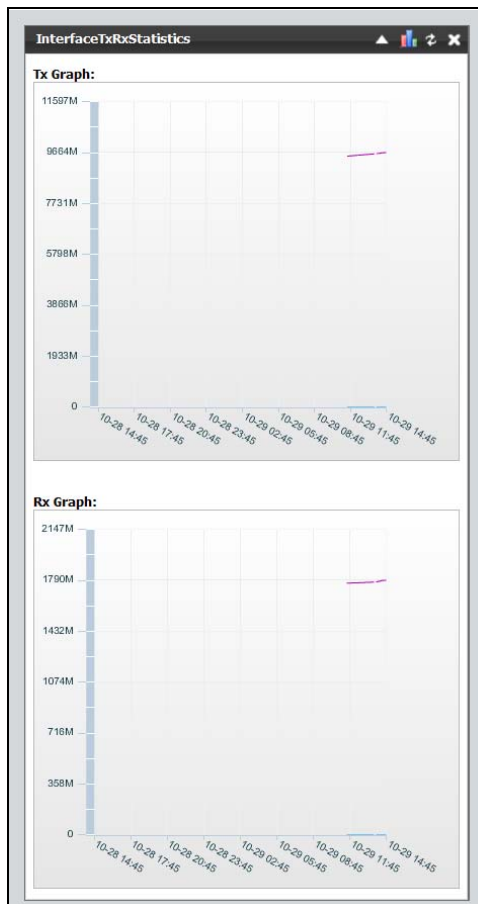
- 7 If you do not want to see the detailed report for each interface on the device, you can go to **Tool > Performance Monitoring > Device Monitors**. Click **Add Content**.



- 8 Select the monitor you just created. Click **Ok**.

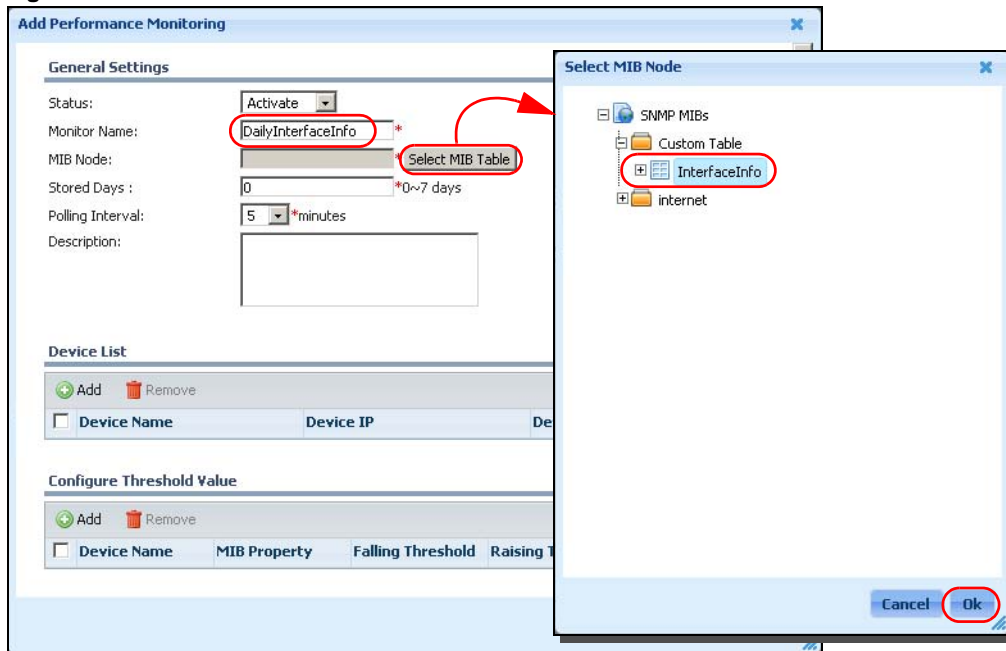


- 9 Then you can see the monitor as the example below.



- 10 The **Add Performance Monitoring** screen appears. Enter a name for the monitor (**DailyInterfaceInfo**) and then click **Select MIB Table**. Select **Custom Table > InterfaceInfo** that we just created and then click **Ok**.

Figure 49 Create a Performance Monitor



2.9 Configure VLAN Settings

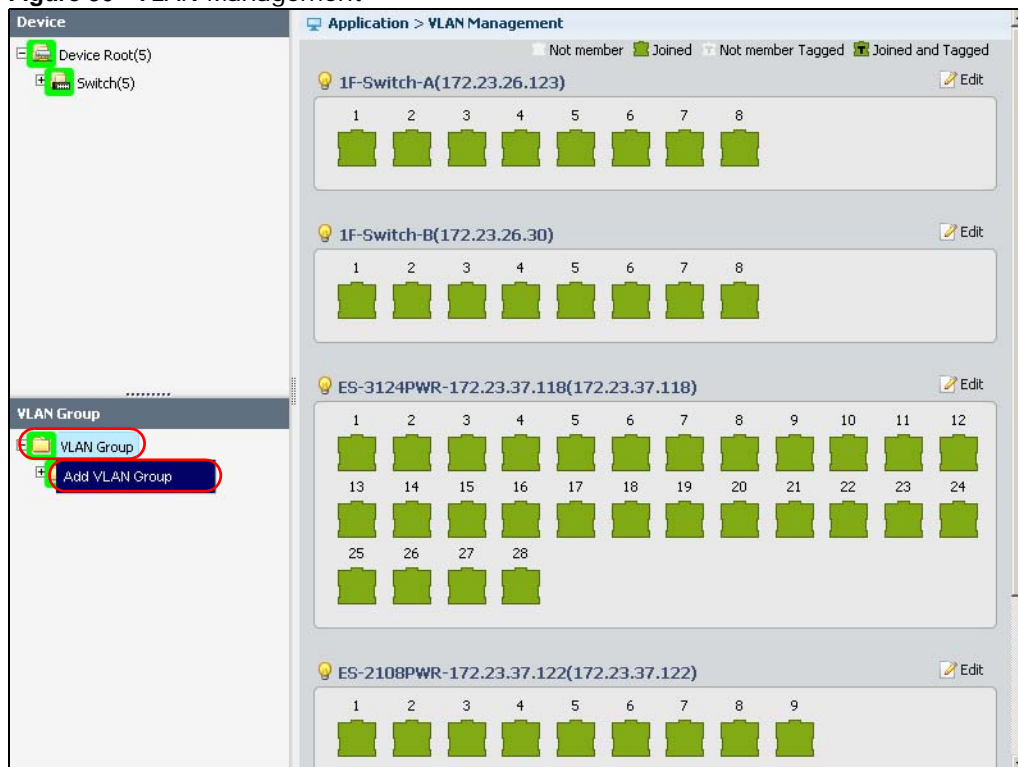
The ENC provides the VLAN management feature to help you easily configure VLAN settings on switches. This tutorial shows you how to configure VLAN settings (ports 1~4: VLAN 100, ports 5~8: VLAN 200) on switch **1F-Switch-A**, including the following:

- create VLAN groups
- add the device to the VLAN groups
- configure port VLAN settings
- configure additional VLAN settings

The following shows you how to configure step by step:

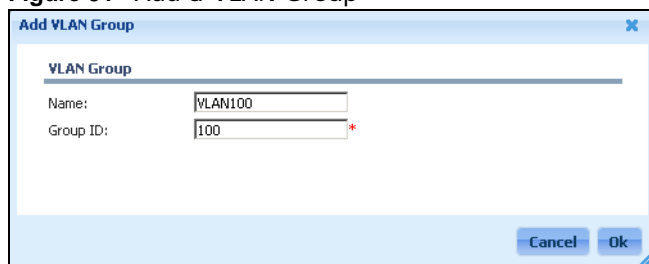
- 1 Click **Application > VLAN Management**. The screen displays as shown in [Figure 50](#). Click **VLAN Group** and then **Add VLAN Group** in the **VLAN Group** panel.

Figure 50 VLAN Management



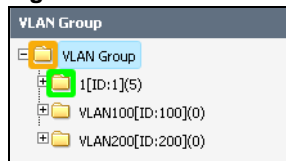
- 2 Create a VLAN 100. Click **Ok**.

Figure 51 Add a VLAN Group



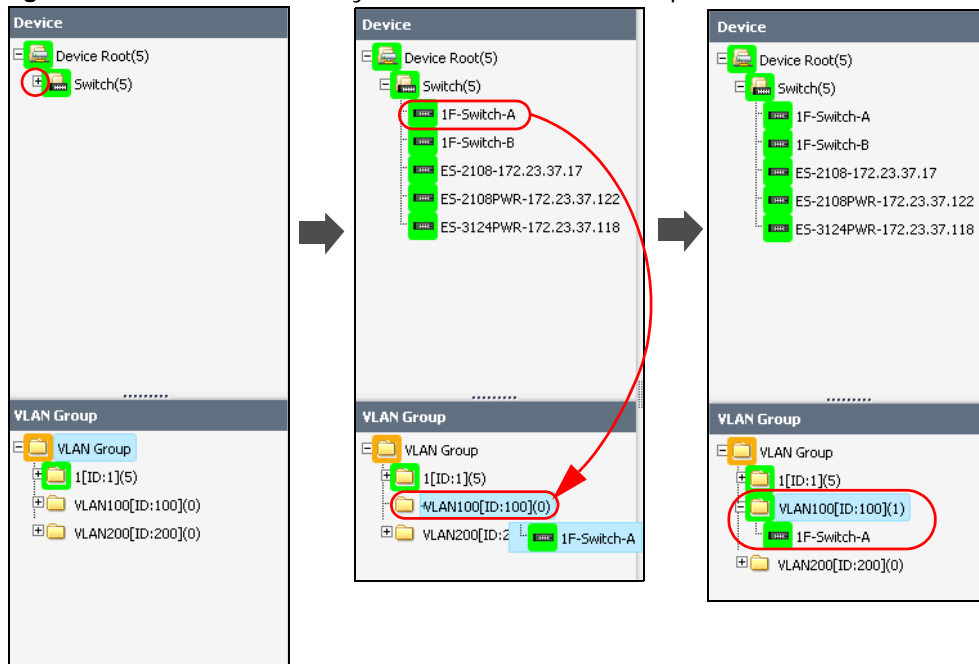
- 3 Repeat to create another VLAN 200. The created VLAN groups display in the **VLAN Group** panel.

Figure 52 Two VLAN Groups Created



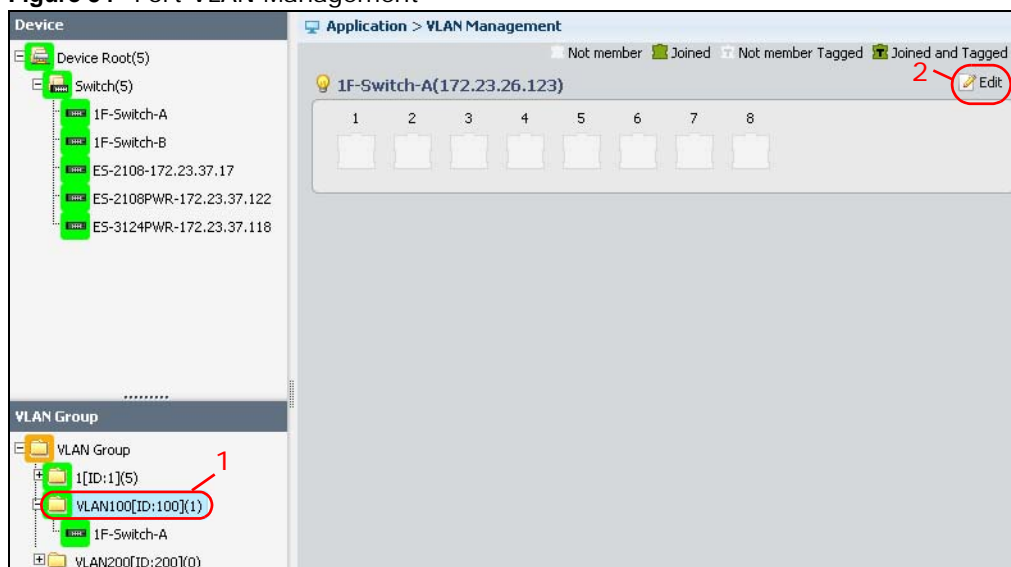
- Click the + mark to expand the **Switch** folder. Select and drag switch **1F-Switch-A** to the **VLAN100** folder. Release it when you see a + mark at the beginning of the **VLAN100** folder name. The ENC also configures a VLAN 100 on the switch.

Figure 53 The Device is Easily Added to the VLAN Group



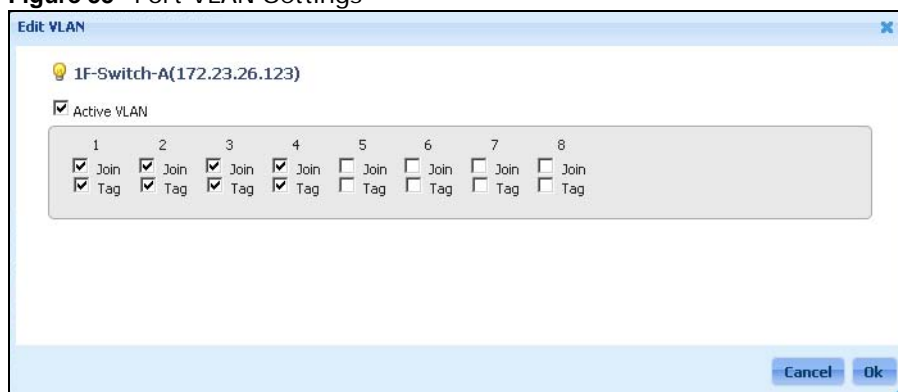
- Select **VLAN100** in the **VLAN Group** folder to display **1F-Switch-A**'s VLAN settings on the right hand of the screen. Click **Edit**.

Figure 54 Port VLAN Management



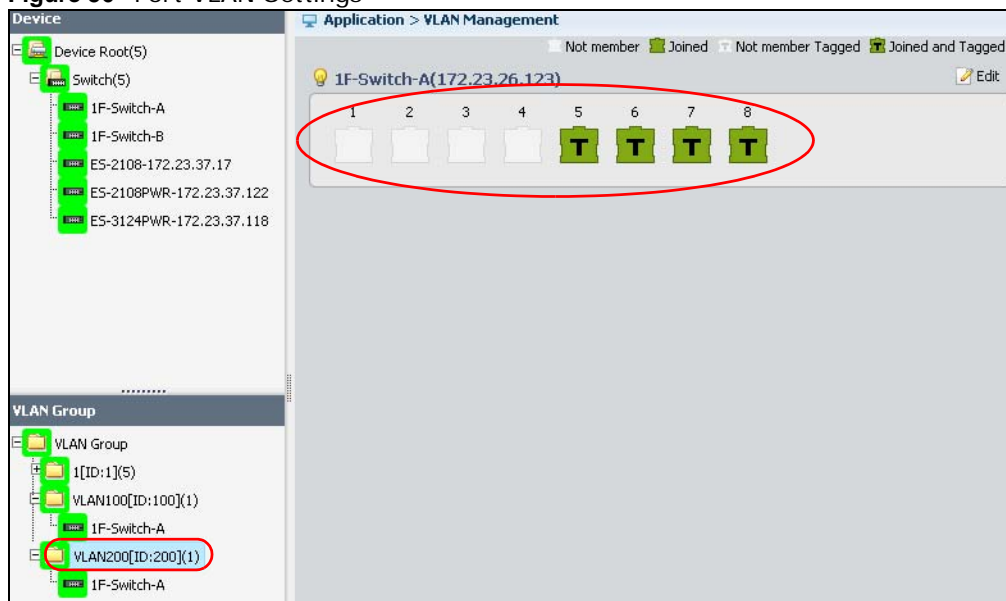
- 6 The **Edit VLAN** screen appears. Select **Join** and **Tag** on ports 1 to 4. Click **Ok**.

Figure 55 Port VLAN Settings



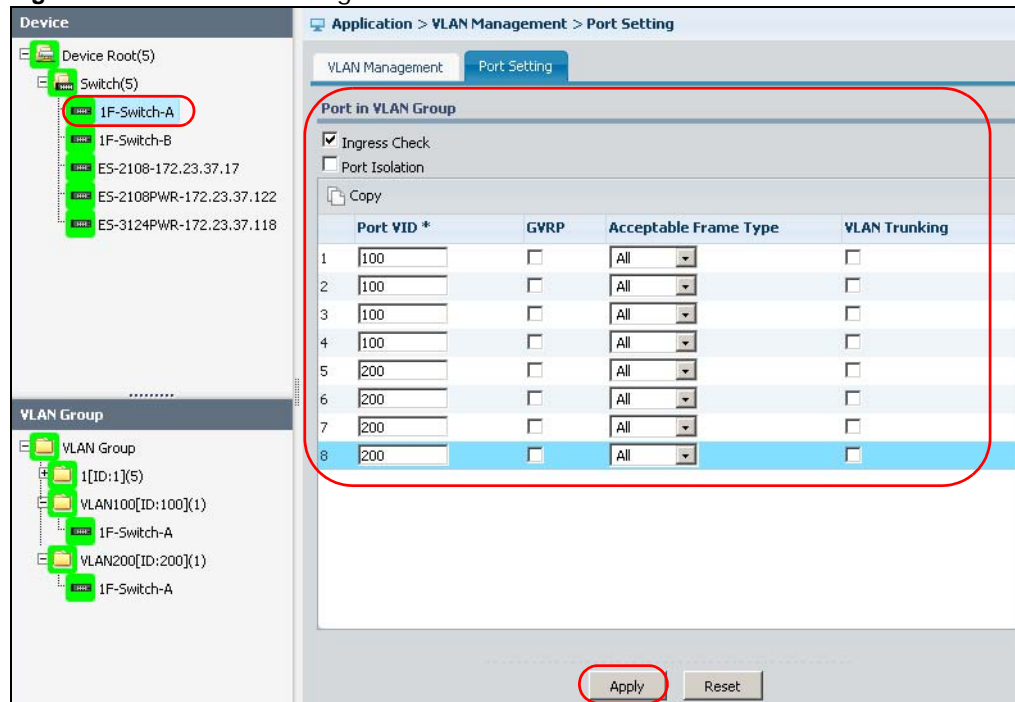
- 7 Repeat steps 4~6 to configure VLAN 200 on **1F-Switch-A**. The only difference is to add ports 5~8 to **VLAN200**.

Figure 56 Port VLAN Settings



- 8 Select **1F-Switch-A** in the **Device** panel and then click the **Port Setting** tab. Configure additional VLAN settings in this screen. For example, select **Ingress Check** and configure the **Port VID** for each port. Click **Apply**.

Figure 57 Port VLAN Settings



2.10 Register Multiple NWA1300-N Series APs

You can use the ENC and NWA1300-N Series for hotel management. There are three common methods for the device registration to the ENC. You can choose one of the following methods according to your condition.

Table 18 Methods of Registering NWA1300-N Series to the ENC

METHOD	DESCRIPTION	ADDITIONAL REQUIREMENTS
1	Devices use a dynamic IP address with DHCP option 224 and register to the ENC actively. See Section 2.10.1 on page 75 .	<ul style="list-style-type: none"> A DHCP Server which supports DHCP option 224 A mapping list between the device MAC addresses and room numbers
2	Devices use a static IP address and the administrator has to manually register them to the ENC. See Section 2.10.2 on page 77 .	
3	Devices use a dynamic IP address and the ENC adds them to the registration list through the Auto-Discovery function. See Section 2.10.3 on page 78 .	<ul style="list-style-type: none"> A DHCP Server without DHCP option 224 support

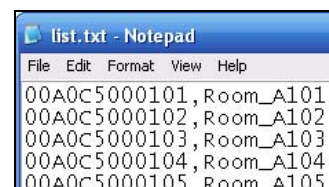
This example uses the following settings:

ITEM	SETTING		
The ENC's IP address	192.168.1.250		
Device's IP address, MAC address and room number mapping	device 1	192.168.1.1	00A0C5000101 <-> Room_A101
	device 2	192.168.1.2	00A0C5000102 <-> Room_A102
	device 3	192.168.1.3	00A0C5000103 <-> Room_A103
	device 4	192.168.1.4	00A0C5000104 <-> Room_A104
	device 5	192.168.1.5	00A0C5000105 <-> Room_A105

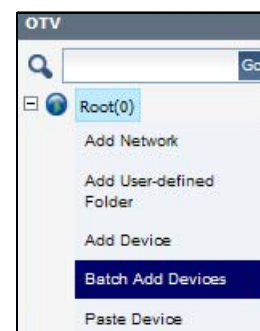
2.10.1 Method 1

First of all, make sure you have configured the ENC's IP address in the DHCP server's DHCP option 224 setting. Each of your NWA1300-N Series device will be able to obtain not only an IP address, subnet mask and gateway IP address but also the ENC's IP address. When an engineer installs an NWA1300-N series device in a room, he has to write down the device's MAC address and room number in a list. After installation, the engineer will pass the list to you, the ENC administrator. Then you can do:

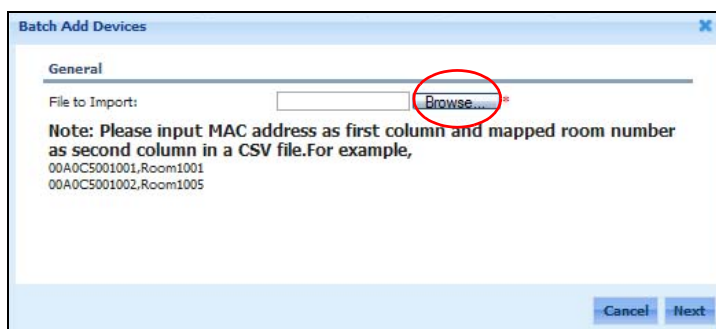
- 1 Prepare the mapping list and save it as a text file (list.txt in this example) for later upload. Follow the exact format as shown. Only use a comma (,) to separate the MAC address and room number without leaving any spaces in between.



- 2 In the ENC, right-click the **Root** node in the OTV tree and select **Batch Add Devices**.



- 3 Click **Browse** to locate the text file and then click **Next**.



- 4 Make sure all entries are in the **Device(s) ready to import** section. Click **Import**.

Batch Add Devices

Device(s) ready to import

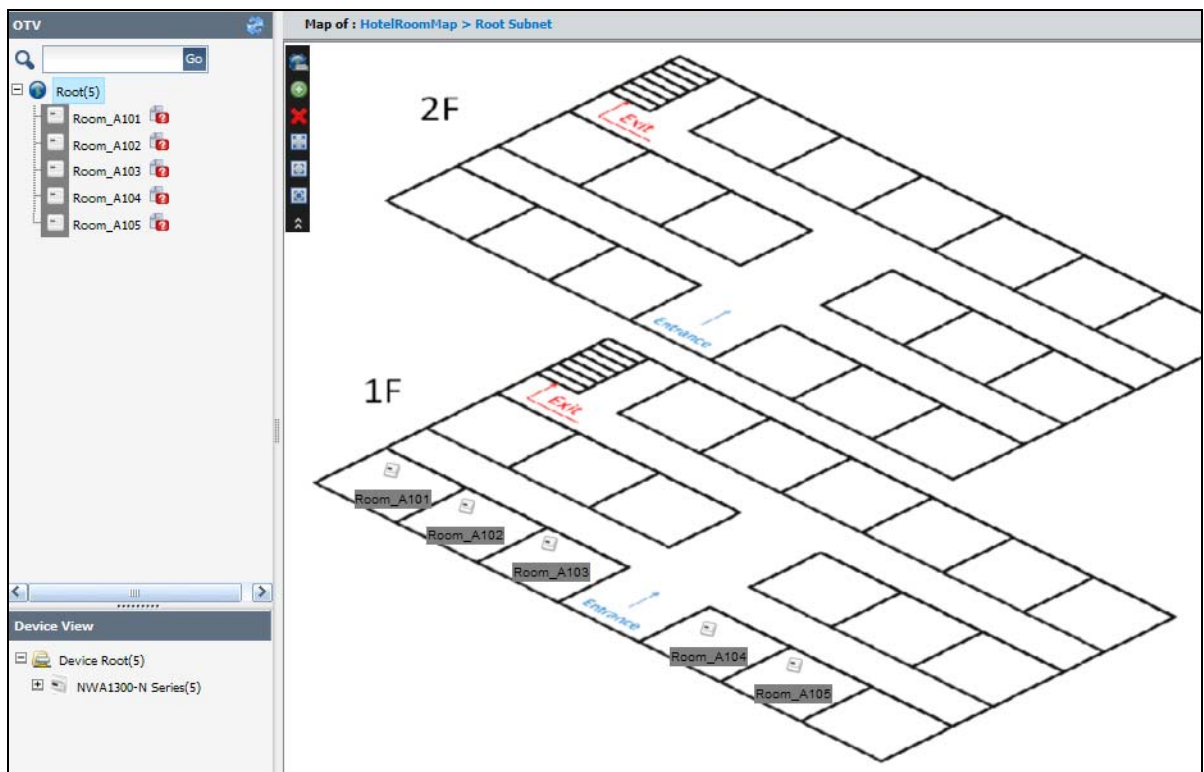
	Device Name	Device Type	Device Model	MAC	Mapped Room No.
1	Room_A101	NWA1300-N Series	NWA1300-NJ	00A0C5000101	Room_A101
2	Room_A102	NWA1300-N Series	NWA1300-NJ	00A0C5000102	Room_A102
3	Room_A103	NWA1300-N Series	NWA1300-NJ	00A0C5000103	Room_A103
4	Room_A104	NWA1300-N Series	NWA1300-NJ	00A0C5000104	Room_A104
5	Room_A105	NWA1300-N Series	NWA1300-NJ	00A0C5000105	Room_A105


Device(s) not ready to import

Device Name	Reason
-------------	--------

Cancel Previous **Import**

- 5 You will see all devices are added in the OTV tree. If you have prepared an appropriate Map image, move the device icons on the Map to the right places, which helps you check the location of each device.

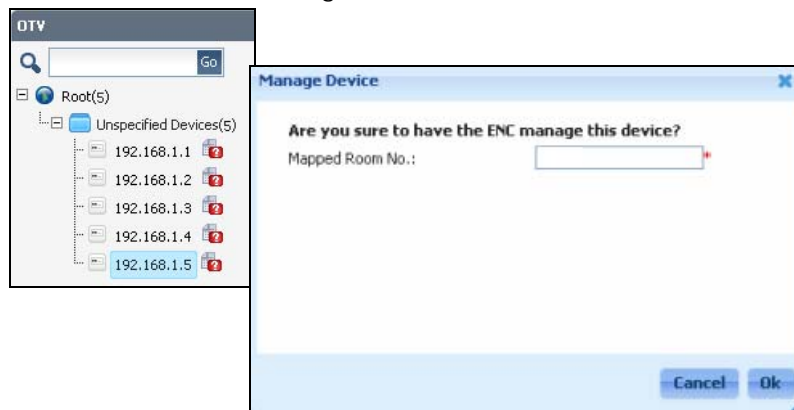


You have finished the registration. You can then click the **Edit AP Profile** icon () in the OTV tree to configure each device's wireless AP profile settings.

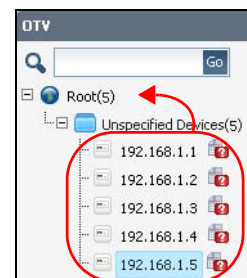
2.10.2 Method 2

If you want to configure a static IP address for your NWA1300-N Series devices, you have to configure them one by one when you install them in each room. You will have to go to a room and install an NWA1300-N as well as configure the IP address, subnet mask, gateway IP address and the ENC's IP address. See the device User's Guide for how to do these. After the installation and turning the devices on, the ENC will add the devices passively after receiving their traps. Then you can do:

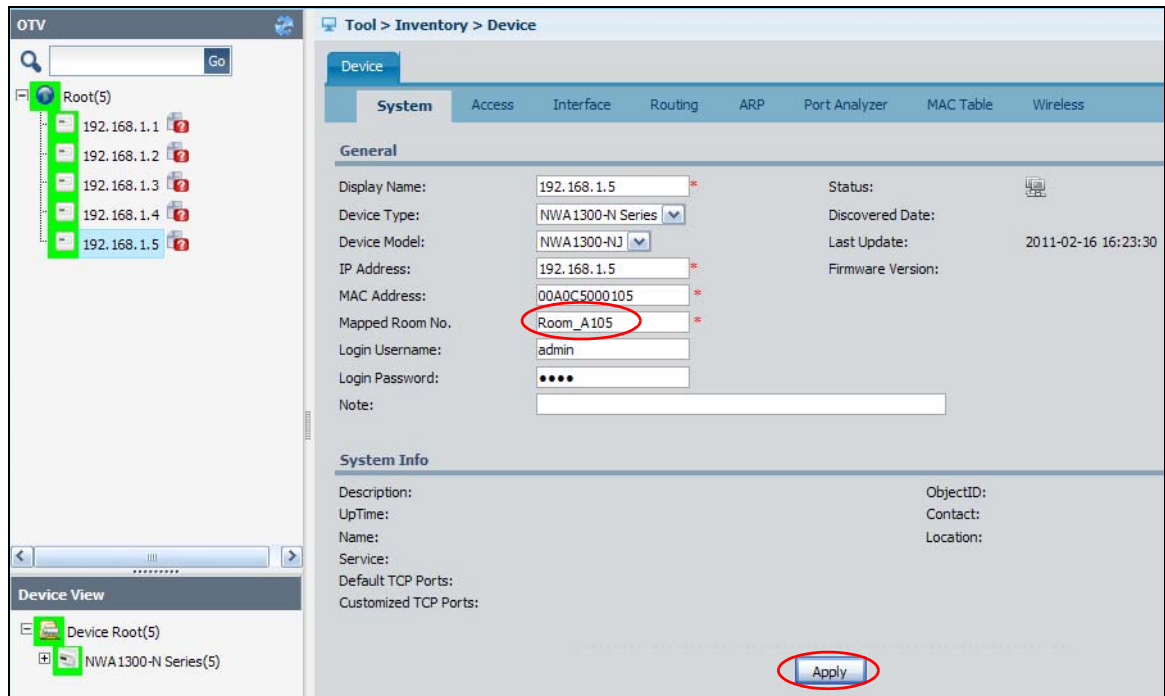
- 1 Click each device under the **Unspecified Devices** folder in the OTV tree and configure the room number. Click **Ok** to save the change.




- 2 Move the devices from the **Unspecified Devices** folder to an appropriate network or a folder node via drag and drop.



- Click each device to modify the number of the room where it is located. Click **Apply** to save the change.

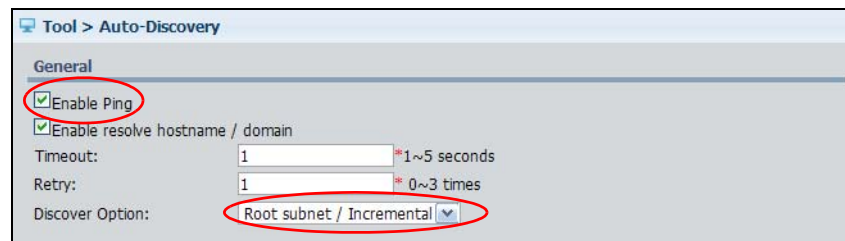


You have finished the registration. You can then click the **Edit AP Profile** icon () to configure the wireless AP profile settings.

2.10.3 Method 3

If you have a DHCP server in the network but it does not support DHCP option 224. You can use this method. After your NWA1300-N Series APs are turned on and obtain an IP address from the DHCP server, you can use the Auto-Discovery function to add them to the ENC. Do the following:

- In the ENC, click **Tool > Auto-Discovery**.
- Select **Enable Ping** and **Root subnet / Incremental** in the **Discover Option** field.



- 3 Select **Entire Network** in the **Discover Type** and enter **1** in the **Max. Hop Level** field. Click **Add** and enter the IP address and subnet mask of those devices. In this example, enter 192.168.1.0/255.255.255.0.

Seeds

Discover Type: Entire Network

Max. Hop Level: 1

Add Edit Remove

Seed	Net Mask
1 192.168.1.0	255.255.255.0

- 4 You may need to configure the SNMP community if you have changed the default settings on those devices. Leave this section as the defaults if you have no idea about them.

SNMP

SNMP Version: ☒ v1 ☒ v2c ☐ v3

SNMP Port: 161

Read Community: communityex

Note: The SNMP version selection depends on which SNMP versions your devices can support.

Note: The ENC will fail to get a device's information if the device uses a different read community.

- 5 Select the default discovery filter rule and click **Edit**, the **Edit Discovery Filter** screen appears. Select **NWA1300-N Series** in the **Values** field. Then click **Ok**. The ENC will only add NWA1300-N Series to the OTV through auto-discovery.

Discovery Filters

Add **Edit** **Remove**

Status	Property	Operation
1	Device Type	equals

Save Discover

Edit Discovery Filter

Status: ☒ Active

Property: Device Type

Operation: equals

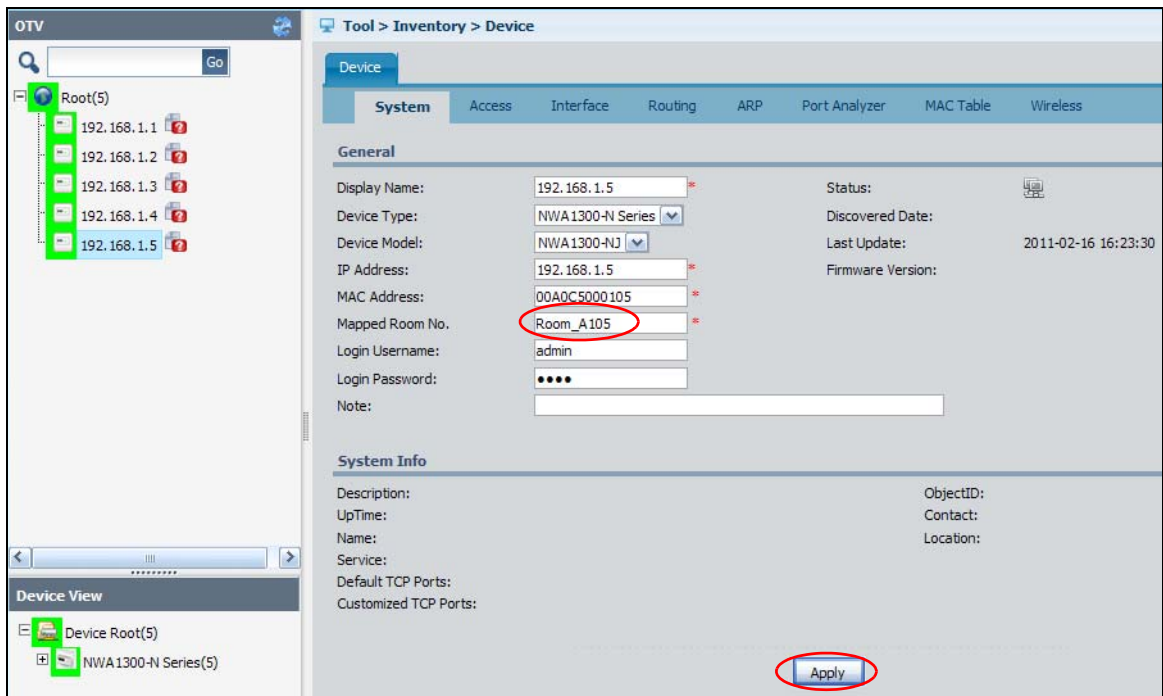
Values: **NWA1300-N Series**


Cancel Ok

- 6 Click the **Discover** button to start finding devices.

After the ENC finds an NWA1300-N Series device, the ENC will automatically configure the device's ENC IP address setting in order to receive the device's traps later.

- 7 Associate each device with their located room number. To do this for an amount of devices, see steps 1 ~ 4 in the Method 1 (Section 2.10.1 on page 75) to import a text file with the information. Alternatively, if you only need to do this for some devices, you can click each device in the OTV tree to input the room number. Click **Apply** to save the change.



You have finished the registration. You can then click the **Edit AP Profile** icon () to configure their wireless AP profile settings.

2.11 Different Map Views for Different Users

Depending on your management purpose, administrators can create different map views with different devices associated for different users with Operator and/or User types.

Note: By default, the “default map” is associated with all managed devices and is not editable or removable. Each map can be associated with only one background image.

Here is an example. You have registered 8 devices in the ENC. You want to use 5 maps to differentiate the device locations and show different users different map views. This example uses the following settings.

Table 19 Example - Different Maps

MAP	DEVICE INCLUDED	BACKGROUND IMAGE	ALLOWED USER ACCESS
Default MAP	All Devices (1 ~ 8)	Image1 (Global)	Administrators
EU-MAP	Devices 1 ~ 5	Image2 (Europe)	Operator1
EU-City1-MAP	Devices 1 ~ 3	Image3 (EU-Building 1)	Operator1, User1
EU-City2-MAP	Devices 4 ~ 5	Image4 (EU-Building 2)	Operator1, User2
US-MAP	Devices 6 ~ 8	Image5 (America)	Operator2

To do this:

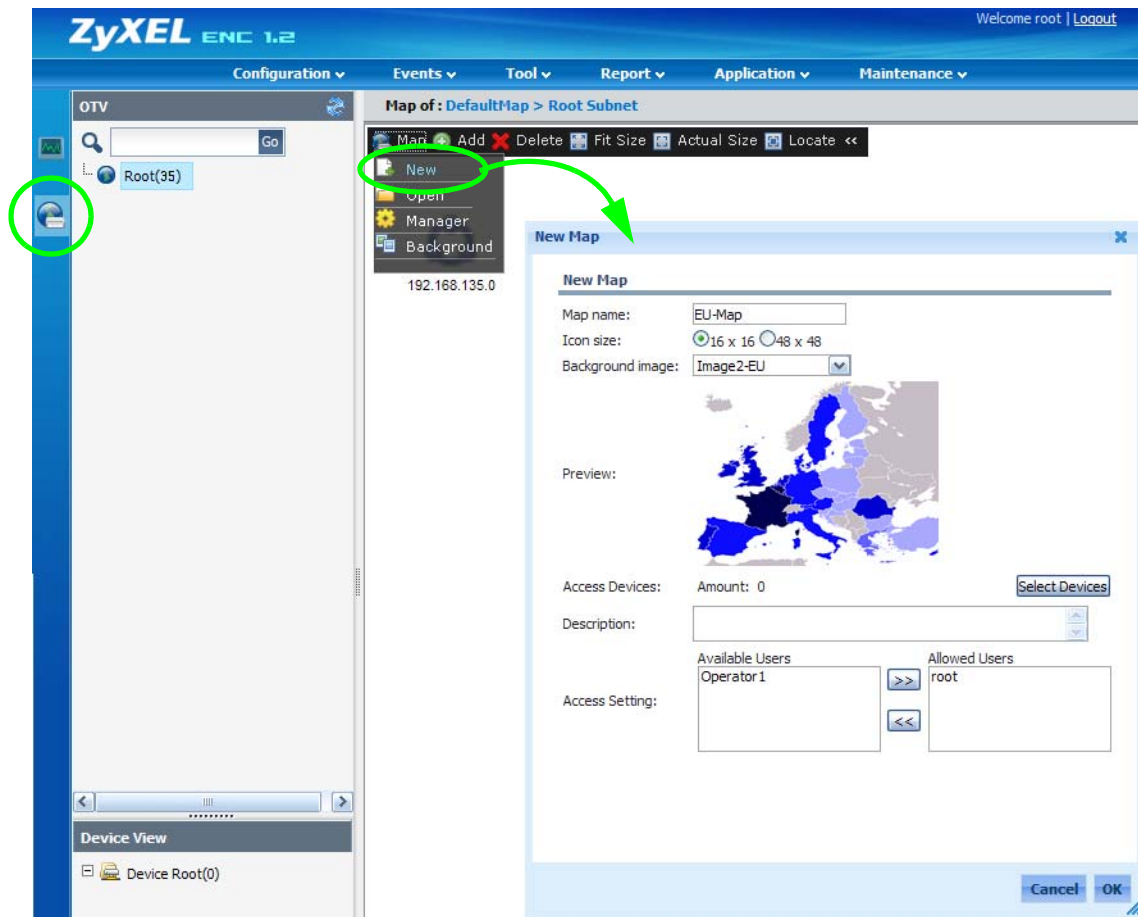
- 1 Upload background images in the **Maintenance > Customize > Image > Add** screen. You will need to upload 5 image files for this example.

The screenshot shows the 'Add Custom Image' dialog box. Under 'General Settings', the 'Image Type' is set to 'Background Image' (selected with a radio button). The 'Image Name' is 'Image1-Global', 'Device Type' is 'Background Image', and 'Size' is '800 x 600 pixels'. There is a 'Browse...' button next to the 'Image' field. The dialog has 'Cancel' and 'Ok' buttons at the bottom right.

- 2 Create user accounts in the **Maintenance > User Account > Add** screen. You will need to create 4 accounts (Operator1, User1, User2, Operator2). Leave the **Allowed Map Access** list empty since you have not created the other Maps yet except the default one.

The screenshot shows the 'Add Account' dialog box. Under 'General Settings', the 'Account Type' is 'Operator' (selected with a radio button). The 'Name' is 'Operator1', 'Password' and 'Verify Password' are masked with dots, and 'Email Address' is 'operator1@zyxel.com.tw'. There is a 'Description' field with up/down arrows. Under 'Map Access', the 'Available Maps' list contains 'DefaultMap', and the 'Allowed Map Access' list is empty. There are '>>' and '<<' buttons between the lists. The dialog has 'Cancel' and 'Ok' buttons at the bottom right.

- 3 Create Maps and associate them with background images, devices, and user accounts.



Log into the ENC using Operator1, Operator2, User1 and/or User2, you should see the corresponding map views.

PART II

Technical Reference

Dashboard

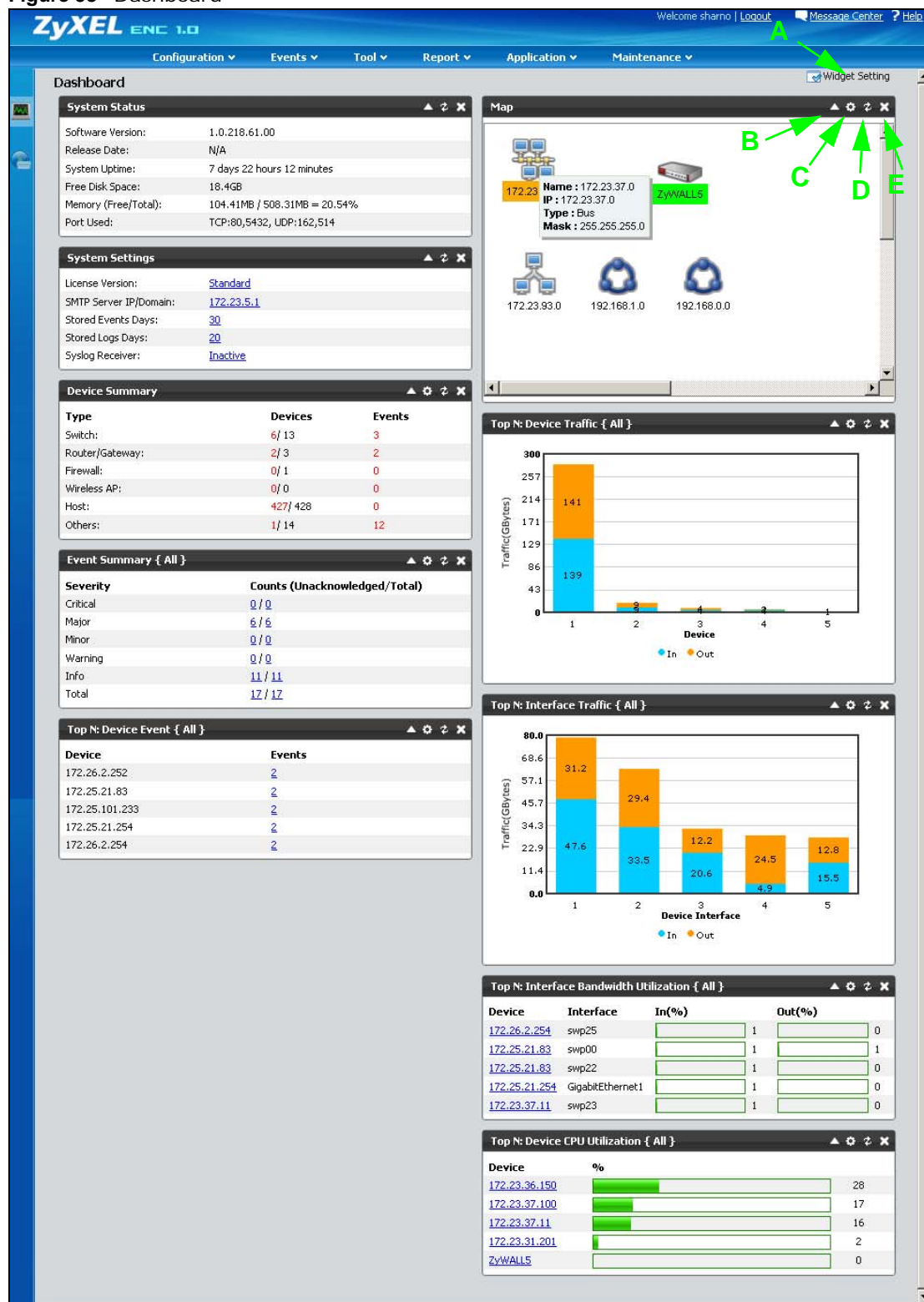
3.1 Overview

Use the **Dashboard** screens to check status information about the ENC.

3.2 The Dashboard Screen

The **Dashboard** screen displays when you log into the ENC or click **Dashboard** in the navigation panel. The dashboard displays general device information, system status, system resource usage, licensed service status, and interface status in widgets that you can re-arrange to suit your needs. You can also collapse, refresh, and close individual widgets.

Figure 58 Dashboard



The following table describes the labels in this screen.

Table 20 Dashboard

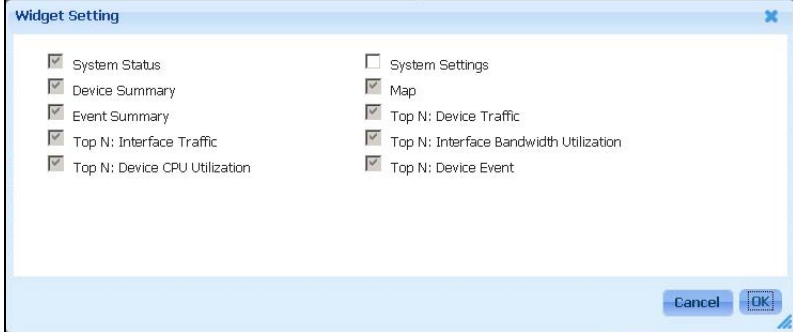
LABEL	DESCRIPTION
Widget Setting (A)	<p>Click this to open the Widget Setting screen.</p> <p>Figure 59 Dashboard - Widget Setting</p>  <p>This screen displays all available widget names. Widgets that are already opened appear grayed out in this screen. Otherwise, they were removed from the dashboard and are selectable in this screen. You can select a widget to re-open it in the dashboard.</p> <p>Note: Not all options on this screen are available for Operator and User accounts.</p>
Collapse/Expand (B)	Click this to hide (Collapse) or show (Expand) a widget.
Edit Widget (C)	<p>Not all widgets have this function.</p> <p>Click this if you want to change the widget's settings. The settings vary depending on widgets.</p>
Refresh Widget (D)	<p>Set the interval for refreshing the information displayed in the widget.</p> <p>Click this to update the widget's information immediately.</p>
Close Widget (E)	Click this to close the widget. Use Widget Setting to re-open it.
System Status	
Software Version	This field displays the version of the ENC.
Release Date	This field displays the date the ENC software version is released.
System Uptime	This field displays how long the ENC has been running since it last restarted or was turned on.
Free Disk Space	This field displays the available disk space in the computer where the ENC is installed.
Memory (Free/Total)	This field displays the available and total amount of memory the computer has allocated for the ENC.
Port Used	This field displays the TCP and UDP ports the ENC currently uses for the services.
System Settings	
License Version	This field displays whether you are using the Trial or Standard version of the ENC.
SMTP Server IP/Domain	This field displays the IP address or domain name of the mail server the ENC uses to send its notifications and alarms.
Stored Events Days	This field displays the number of days an event can be stored in the ENC before the ENC removes it.

Table 20 Dashboard (continued)

LABEL	DESCRIPTION
Stored Logs Days	This field displays the number of days a log entry can be stored in the ENC before the ENC removes it.
Syslog Receiver	This field displays whether the syslog server is enabled (Active) or not (Inactive) in the ENC.
Device Summary	
Type	The field displays a type of device.
Devices	The field displays how many managed devices of that type are online and the total amount of devices managed by the ENC.
Events	The field displays how many events that devices of the related type have generated.
Event Summary	
The title bar also displays for which device type this widget displays in brackets {}. They are All , Switch , Router/Gateway , Firewall , Wireless AP , Host , or Others .	
Severity	This is a severity level of events. The severity levels from high to low are Critical , Major , Minor , Warning , Info .
Counts (Unacknowledged/Total)	This field displays the number of events that have not been acknowledged (removed) and the total number of events the ENC has received from managed devices. Click a number to go to the Events > Viewer screen where you can view details about the events as well as acknowledge events. An acknowledged event means the event has been known and dealt with by an administrator or operator.
Top N: Device Event	
The title bar also displays for which device type this widget displays in brackets {}. They are All , Switch , Router/Gateway , Firewall , Wireless AP , Host , or Others .	
Device	This field displays the name of a device that generated most events.
Events	This field displays the number of events the device has generated.
Map	
This widget displays the managed networks and devices that you are allowed to view and/or manage as well as a Map image as the background (the default is blank). The devices and Map image that you can see here may vary depending on the account you used to log in.	
When you move your mouse over a network icon, you can see the following information:	
<ul style="list-style-type: none"> • Name: This is the network's name. • IP: This is the network's IP address. • Type: This is the network type that is configured when the device is added to the ENC. • Mask: This is the subnet mask of the network. 	
When you move your mouse over a device icon, you can see the following information:	
<ul style="list-style-type: none"> • Name: This is the device's name. • IP: This is the device's IP address. • Category: This is the device type. • Mask: This is the subnet mask of the network. 	
See Section 1.3.3.4 on page 27 for more information.	
Top N: Device Traffic	
This widget displays the incoming (In) and outgoing (Out) traffic statistics in a graph. The title bar also displays for which device type this widget displays in brackets {}. They are All , Switch , Router/Gateway , Firewall , Wireless AP , Host , or Others .	
When you move your mouse over a bar on the graph, you can see more detailed information such as the IP address of the computer and traffic statistic.	

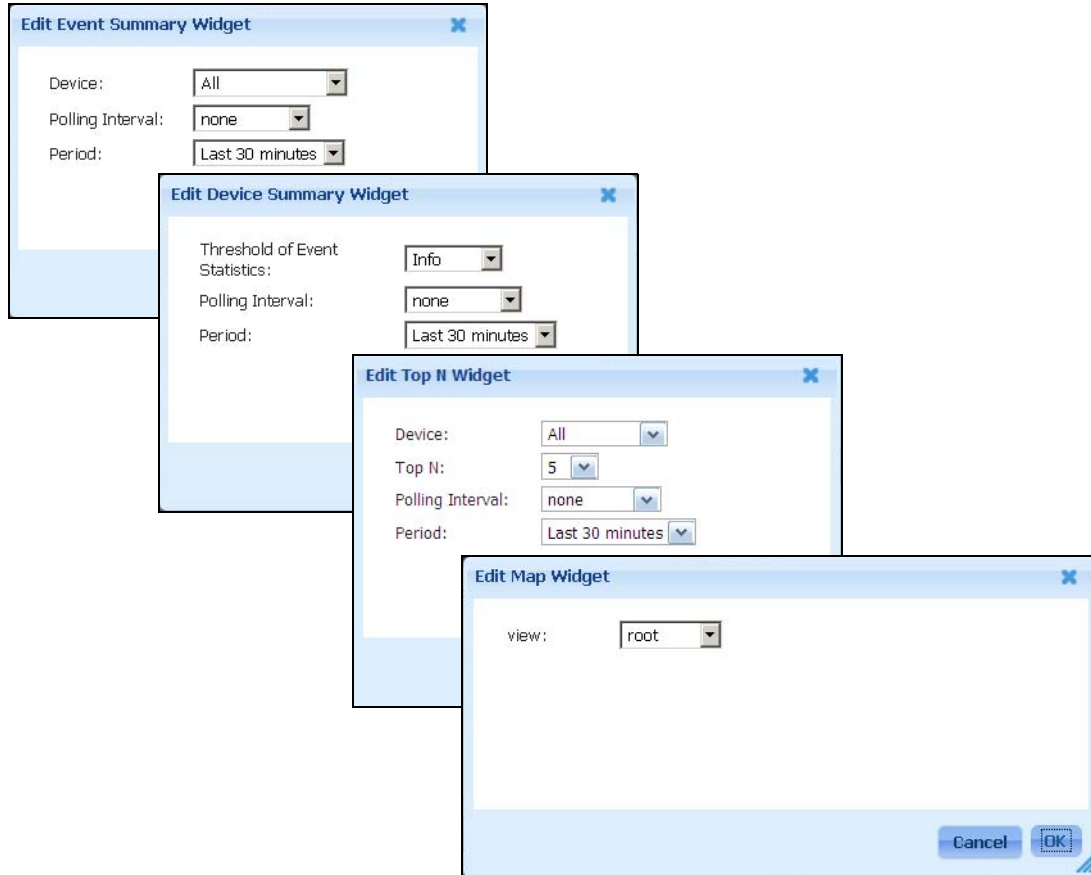
Table 20 Dashboard (continued)

LABEL	DESCRIPTION
<p>Top N: Interface Traffic</p> <p>This widget displays the incoming (In) and outgoing (Out) traffic statistics in a graph. The title bar also displays for which device type this widget displays in brackets {}. They are All, Switch, Router/Gateway, Firewall, Wireless AP, Host, or Others.</p> <p>When you move your mouse over a bar on the graph, you can see more detailed information such as the IP address of the computer, the interface name about the traffic statistic.</p>	
<p>Top N: Interface Bandwidth Utilization</p> <p>The title bar also displays for which device type this widget displays in brackets {}. They are All, Switch, Router/Gateway, Firewall, Wireless AP, Host, or Others.</p>	
Device	This field displays the name of a device that uses the most highest bandwidth.
Interface	This field displays the name of an interface on the device. swp means a switch port.
In(%)	This field displays what percentage of incoming traffic out of total incoming traffic amount the device has received.
Out(%)	This field displays what percentage of outgoing traffic out of total outgoing traffic amount the device has received.
<p>Top N: Device CPU Utilization</p> <p>The title bar also displays for which device type this traffic statistic displays in brackets {}. They are All, Switch, Router/Gateway, Firewall, Wireless AP, Host, or Others.</p>	
Device	This field displays the name of a device that uses most highest CPU resources.
%	This field displays what percentage of CPU resource that device is currently using.

3.2.1 Edit a Widget

Use this screen to change a widget's settings for display. To open this screen, click the **Edit Widget** icon on the top right corner of a widget. The settings vary depending on widgets.

Figure 60 Edit a Widget - Event Summary/Device Summary/Top N/Map



The following table describes the labels in this screen.

Table 21 Edit a Widget

LABEL	DESCRIPTION
Device	Select what type of devices to display or to be used for the widget's statistics. The available options are All, Switch, Router/Gateway, Firewall, Wireless AP, Host, Others.
Top N	Select how many top number of entries about events or traffic amount to display in the widget.
Polling Interval	Select how often you want the ENC to update the widget information it displays. Select none to have the ENC stop updating the widget information.
Period	Select the length of time interval you want to use to look at the statistics. These values are updated based on the Polling Interval setting.
Threshold of Event Statistics	Select the severity level of the event logs as a threshold for the statistics the Device Summary widget displays. The choices and the severity level from low to high are Info , Warning , Minor , Major , and Critical . For example, select Major to display statistics about event logs with severities Major and Critical .

Table 21 Edit a Widget (continued)

LABEL	DESCRIPTION
view	<p>Select which devices to display in the Map.</p> <ul style="list-style-type: none">• root: Select this to display all devices.• Segment: Select this and a specific network segment to only display devices in the segment.
Cancel	Click this to discard the changes and close this screen.
OK	Click this to save the changes and close this screen.

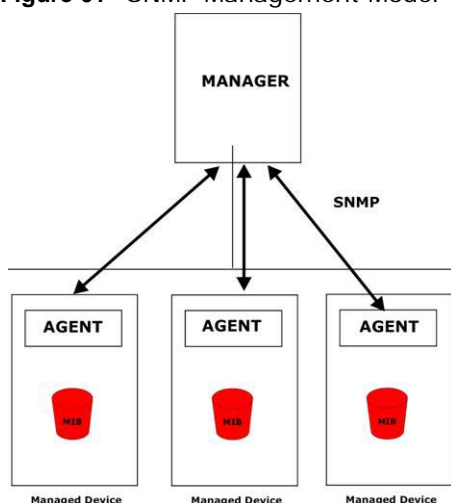
Configuration

This chapter shows you how to use the ENC's configuration menus.

4.1 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network switches. SNMP is a member of TCP/IP protocol suite. A manager station can manage and monitor the switch through the network via SNMP version 2c. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 61 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (your Ethernet switch). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 22 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMP, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

See the switch User's Guide for a list of supported traps.

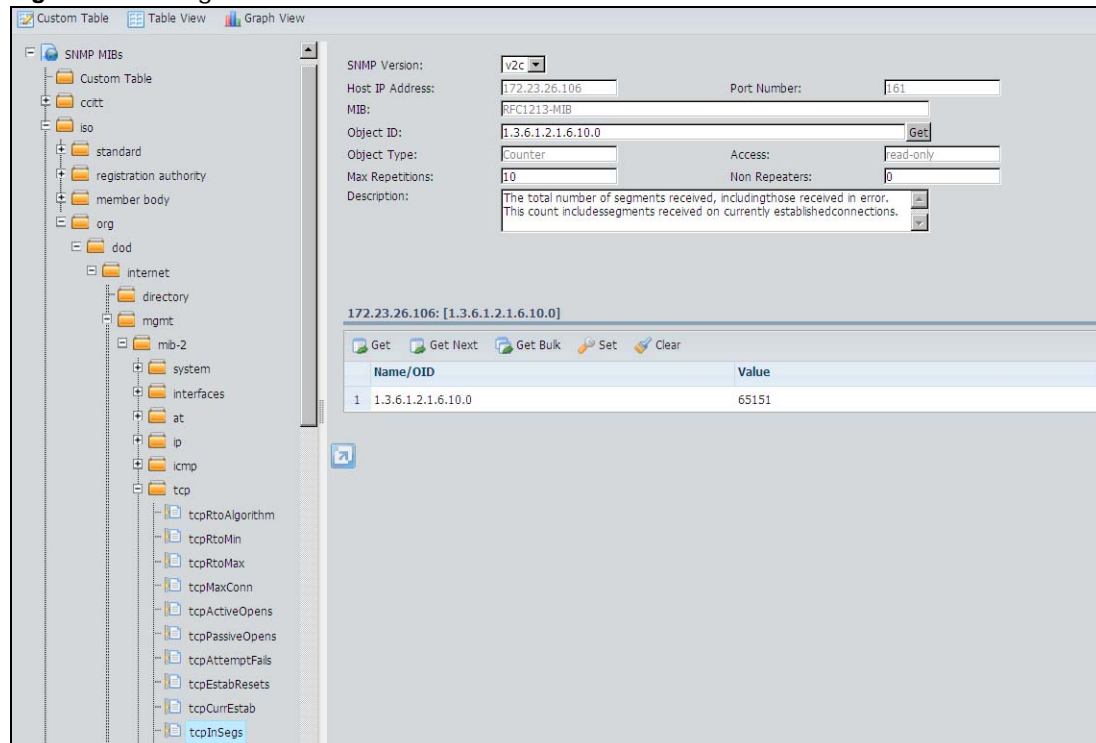
4.1.1 MIB Browser

To open the **MIB Browser** screen, select a device in the OTV and click **Configuration > MIB Browser** to display the MIB browser screen. Then select an object from the SNMP MIB tree to display its details to the right. Use this screen to do the following SNMP operations:

- Retrieving Data - Get, GetNext, GetBulk
- Altering Variables - Set

Note: Click the Plus Sign (+) next to a MIB object in the SNMP MIB tree to go to the next layer down.

Figure 62 Configuration > MIB Browser

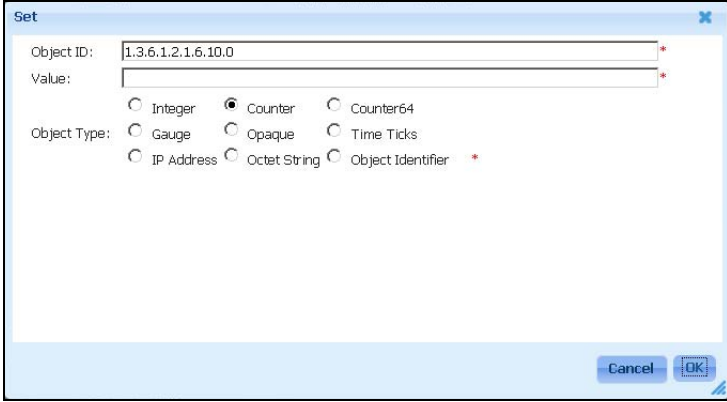


The following table describes the labels in this screen.

Table 23 Configuration > MIB Browser

LABEL	DESCRIPTION
Custom Table	Click this to open a screen where you can specify various objects in one table for which to display their values at one time in the table or graph view.
Table View	Click this to display the object's information in a table in a separate screen. Not all objects support this.
Graph View	Click this to display the object's information as a graph in a separate screen. Not all objects support this.
SNMP Version	Select the SNMP version to use with the selected device. The supported versions vary by device. The fields available vary based on the selected version.
Host IP Address	This field displays the managed device's IP address.
Port Number	This field displays the port number the ENC uses to use SNMP with the device.
MIB	This field displays the object's name.
Object ID	Select a leaf object from the MIB tree on the left or enter a leaf object's ID here. You can also select a folder in the MIB tree on the left and type the rest of a leaf object's ID. Enter a leaf object's ID or Object identifier. Data is formatted in MIB dot format, optionally with a leading text identifier, for example sysObjectID.0 or 1.3.6.1.2.1.1.2.0.
Get	Click Get to retrieve the latest recorded value or setting for the selected object.
Object Type	This field identifies what kind of value the object uses.
Access	This field identifies what kind of access is available for this object.
Description	This field displays any descriptive information recorded for the object.
Max Repetitions	This field displays with SNMP version v2c or v3. When you use the get-bulk command for this object, this setting determines up to how many get-next operations to attempt in order to retrieve the remaining objects
Non Repeaters	This field displays with SNMP version v2c or v3. When you use the get-bulk command for this object, this setting determines how many objects can be retrieved with a simple get-next operation.
Get	Click this to retrieve the object's value.
Get Next	Click this to retrieve the next object's value.
Get Bulk	This is available with SNMP version v2c or v3. Click this to retrieve the values of objects in the specified object's sub-tree.

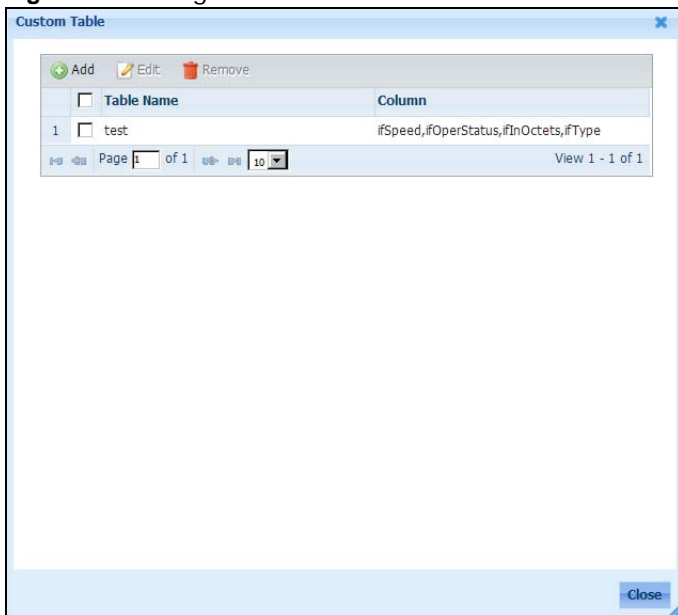
Table 23 Configuration > MIB Browser (continued)

LABEL	DESCRIPTION
Set	<p>Click this to change the value of a managed object. The Set screen appears.</p> <p>Figure 63 Set</p>  <p>The following describes the fields in the Set screen.</p> <ul style="list-style-type: none"> • Object ID: This field displays the selected MIB object's ID. • Value: Enter a new value for the MIB object. • Object Type: Select an appropriate type for the MIB object. • Cancel: Click this to discard the changes and exit this screen. • OK: Click this to save the changes and exit this screen.
Clear	Click this to remove the information displayed in the table.
Name/OID	This is the object's name or object ID.
Value	This is the object ID's setting. For some objects you can set this. For other objects you can only retrieve the setting.

4.1.2 Custom Table

To open the **Custom Table** screen, select a device in the OTV and click **Configuration > MIB Browser > Custom Table**. Use this screen to create and manage custom tables (lists) of MIB objects.

Figure 64 Configuration > MIB Browser > Custom Table



The following table describes the labels in this screen.

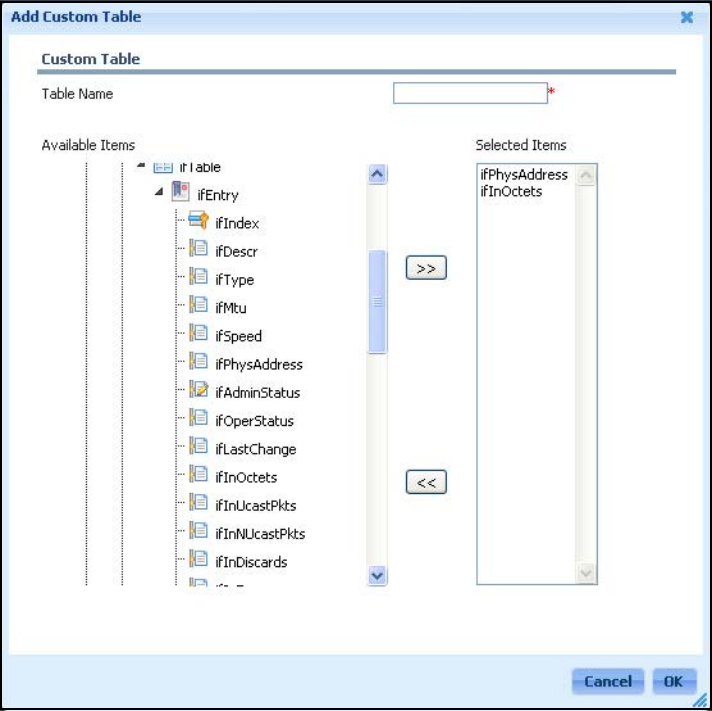
Table 24 Configuration > MIB Browser > Custom Table

LABEL	DESCRIPTION
Add	Click this to open a screen where you can create a new custom table.
Edit	Select a custom table and click this to modify it.
Remove	Select a custom table and click this to delete it.
check box	Select the check box of an entry and click Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Table Name	This name identifies the custom table.
Column	This field displays the custom table's objects.
Close	Click Close to close the screen.

4.1.3 Custom Table Add/Edit

To open the **Custom Table** screen add or edit screen, select a device in the OTV and click **Configuration > MIB Browser > Custom Table > Add** (or select a custom table and click **Edit**). Use this screen to name the custom table and select its member objects.

Figure 65 Configuration > MIB Browser > Custom Table > Add



The following table describes the labels in this screen.

Table 25 Configuration > MIB Browser > Custom Table > Add

LABEL	DESCRIPTION
Table Name	Enter up to 20 characters to identify the custom table. You can only edit this when adding a custom table, it is read-only when editing a custom table.
Available Items	Select the objects (leaf nodes) under the same parent in the MIB tree to include in this table and use the >> arrow to move them to the Selected Items list.
Selected Items	This section lists the objects included in this custom table. Select an object and click the << arrow if you need to remove it from the custom table.
Cancel	Click Cancel to discard all changes and close this screen.
OK	Click OK to save the changes and close this screen.

4.1.4 Table View

If an object in the **MIB Browser** screen supports displaying information as a table, click **Table View** to display a table view screen.

Figure 66 Configuration > MIB Browser > Table View

Table View

Polling Setting

Polling Interval: * second(s)

SNMP Table

Table view on 172.23.93.15

ifLastChange
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
0
4200
0
4100
6300
0

The following table describes the labels in this screen.

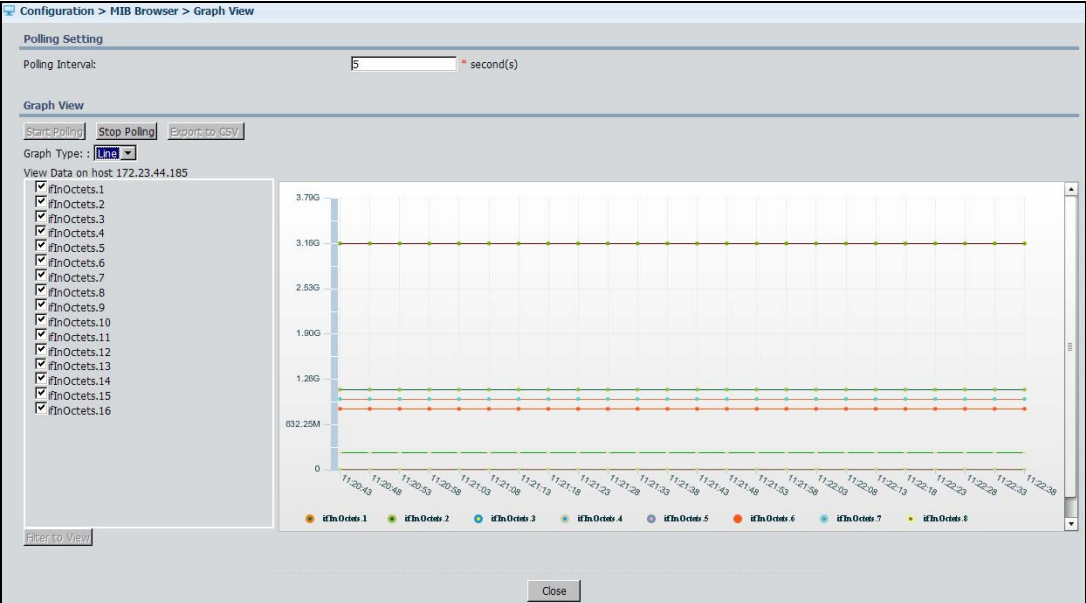
Table 26 Configuration > MIB Browser > Table View

LABEL	DESCRIPTION
Polling Interval	Set how often (5 to 3600 in seconds) the ENC should query the monitored device for the value of the object.
Start Polling	Click this to have the ENC start querying the monitored device for the value of the object.
Stop Polling	Click this to have the ENC halt querying the monitored device for the value of the object.
Switch to Graph View	Click this to view the results for the object as a graph. Switch to graph view can be used for TimeTicks, Counter, Counter64, Gauge, or Integer objects.
Export to CSV	Click this to save the results as a Comma Separated Values Excel file.
Close	Click Close to close the screen.

4.1.5 Graph View

If an object in the **MIB Browser** screen supports displaying information as a graph, click **Graph View** to display a graph view screen. You can also click the table view's **Switch to Graph View** button to display this screen.

Figure 67 Configuration > MIB Browser > Graph View



The following table describes the labels in this screen.

Table 27 Configuration > MIB Browser > Graph View

LABEL	DESCRIPTION
Polling Interval	Set how often (5 to 3600 in seconds) the ENC should query the monitored device for the value of the object.
Start Polling	Click this to have the ENC start querying the monitored device for the value of the object.
Stop Polling	Click this to have the ENC halt querying the monitored device for the value of the object.
Export to CSV	Click this to save the results as a Comma Separated Values Excel file on your computer.
Graph Type	Select whether to display a line, bar, or pie graph.
View Data on host	This read-only field identifies from which managed device the object values came. Select the items you want in the graph and click Filter to View to display a graph with the selected items.
Filter to View	
Close	Click Close to close the screen.

4.2 Firmware Upgrade

Use these screens to upload firmware files to the ENC and have the ENC use them to upgrade the firmware on managed devices.

You must be logged in with system administrator rights to use this function.

Note: Do NOT turn off the switch during the updating process, as it may corrupt the firmware and make the selected device unusable.

4.2.1 Firmware List

Click **Configuration > Firmware Upgrade** to list the firmware files uploaded to the ENC.

Figure 68 Configuration > Firmware Upgrade

	Device Model	Firmware Version	Description
1	ES-2108-LC	3.9	fireware file

The following table describes the labels in this screen.

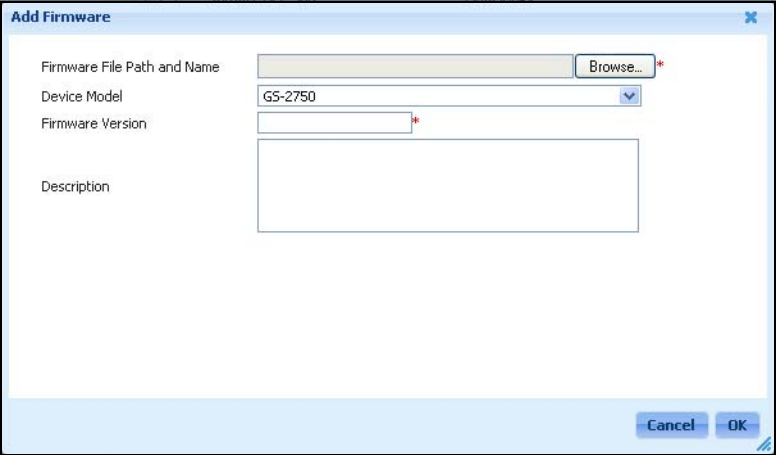
Table 28 Configuration > Firmware Upgrade

LABEL	DESCRIPTION
Device Model	To only display firmware for a specific model, select the model here and click Retrieve .
Firmware Version	To only display firmware of a specific version, select the model in the Device Model field and then select the firmware version and click Search .
Add	Click this to upload a firmware file to the ENC.
Remove	Select one or more entries and click this to delete them.
check box	Select the check box of an entry and click Remove to delete it. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Device Model	This field displays the name of the device model for which the firmware file was uploaded.
Firmware Version	This field displays the version of the firmware file.
Description	This field displays any special information that you specified about the firmware file.

4.2.2 Uploading Firmware to the ENC

Click **Configuration > Firmware Upgrade > Add** to display the screen for uploading firmware files to the ENC. To upload firmware, first download the firmware, unzip it, and store it on your computer.

Figure 69 Configuration > Firmware Upgrade > Add



The following table describes the labels in this screen.

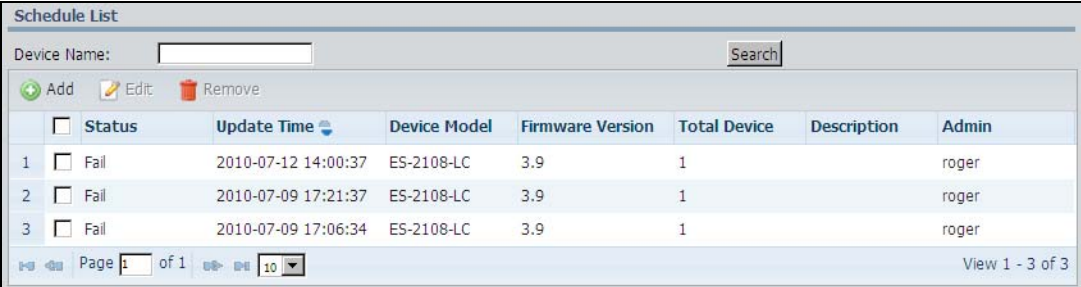
Table 29 Configuration > Firmware Upgrade > Add

LABEL	DESCRIPTION
Firmware File Path and Name	Type the path and file name of the firmware file you wish to upload to the ENC in the text box or click Browse to locate it.
Device Model	Select the model to which the firmware applies.
Firmware Version	Specify the version of the firmware.
Description	List any special information that you want to record about the firmware file.
Cancel	Click Cancel to discard all changes and close this screen.
OK	Click OK to save the changes and close this screen.

4.2.3 Schedule List

Click **Configuration > Firmware Upgrade > Schedule List** to display the list of firmware upgrade schedules. Before you can do this you need to use the **Configuration > Firmware Upgrade > Firmware List** screen to upload the firmware to the ENC (see [Section 4.2.2 on page 102](#)).

Figure 70 Configuration > Firmware Upgrade > Schedule List



	Status	Update Time	Device Model	Firmware Version	Total Device	Description	Admin
1	Fail	2010-07-12 14:00:37	ES-2108-LC	3.9	1		roger
2	Fail	2010-07-09 17:21:37	ES-2108-LC	3.9	1		roger
3	Fail	2010-07-09 17:06:34	ES-2108-LC	3.9	1		roger

The following table describes the labels in this screen.

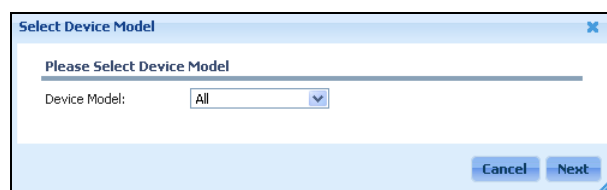
Table 30 Configuration > Firmware Upgrade > Schedule List

LABEL	DESCRIPTION
Schedule List	
Device Name	Enter a part of a device name or the full name you wish to find in this field and click Search .
Add	Click this to create a new schedule for having the ENC upgrade firmware on managed devices.
Edit	Select an entry that has a status of Waiting and click this to edit the entry's update time.
Remove	Select an entry that has a status of Waiting , Success , Fail , or Partial Success and click this to delete it.
check box	Select the check box of an entry and click Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Status	This shows the status of the scheduled firmware upgrade: Waiting , Running , Success , Fail , or Partial Success .
Update Time	This is the date and time the schedule has for upgrading device firmware.
Device Model	This field displays the name of the device model for which the schedule has the ENC upgrade firmware.
Firmware Version	This field displays the version of the firmware file.
Total Device	This is the number of devices the ENC will upgrade the firmware according to the predefined schedule.
Description	This field displays any special information specified about the firmware file.
Admin	This is the name of the administrator who created the firmware upgrade schedule.

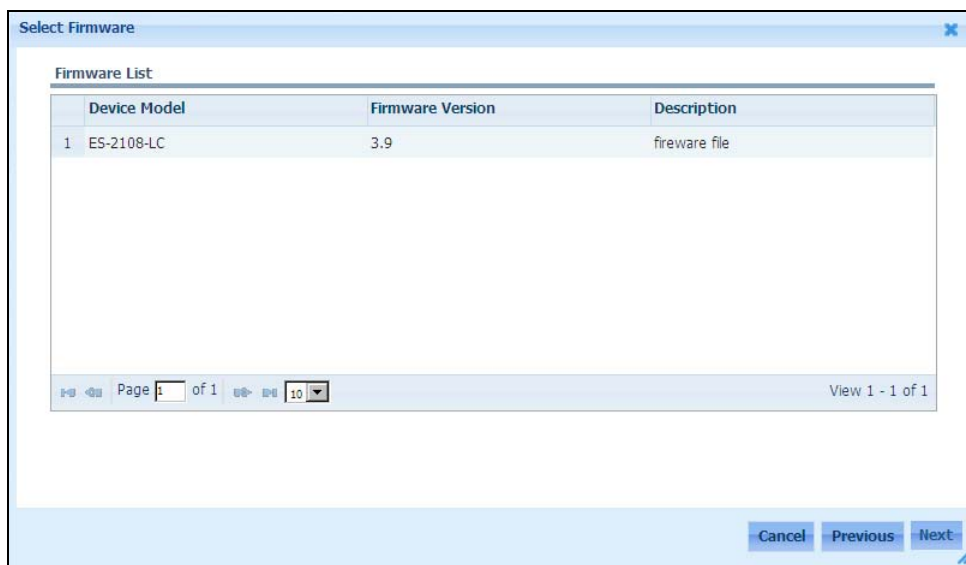
4.2.4 Creating or Editing a Schedule List

Click **Configuration > Firmware Upgrade > Schedule List > Add** (or select a schedule and click **Edit**) and use the following steps to create or edit a firmware upgrade schedule. If you are editing an upgrade schedule you can only edit the update time; skip to the last step for details.

- 1 Select the model for which you want to upgrade firmware and click **Next**.



- 2 Select the firmware version to use to upgrade the managed devices and click **Next**.

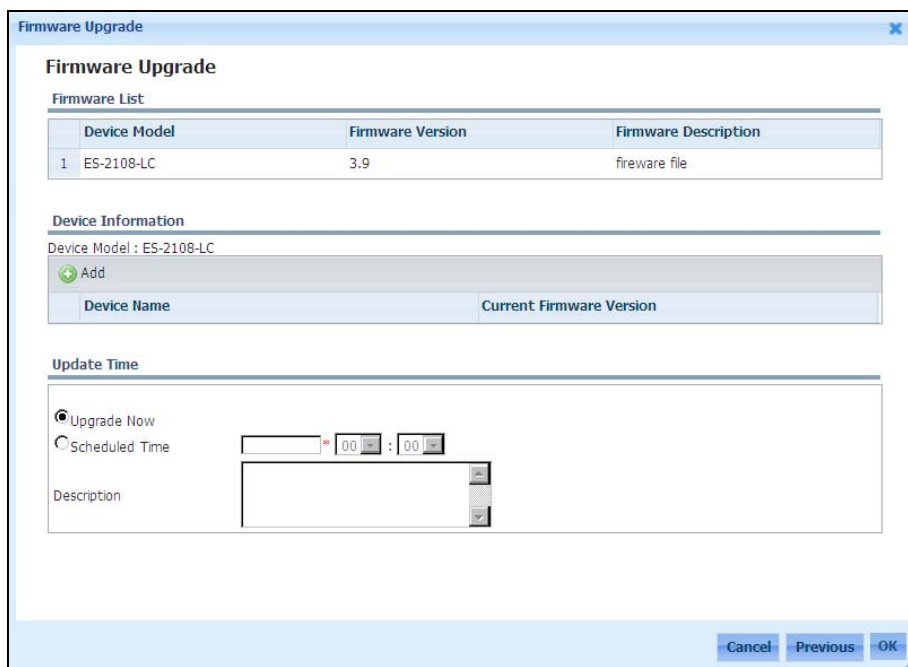


The 'Select Firmware' dialog box displays a 'Firmware List' table with the following data:

	Device Model	Firmware Version	Description
1	ES-2108-LC	3.9	fireware file

At the bottom of the dialog, there are navigation buttons: 'Cancel', 'Previous', and 'Next'. The 'Next' button is highlighted.

- 3 Under **Device Information** click **Add**.



The 'Firmware Upgrade' dialog box contains the following sections:

- Firmware List:** A table with the same data as the 'Select Firmware' dialog.
- Device Information:** Shows 'Device Model : ES-2108-LC' and an 'Add' button (a green circle with a plus sign).
- Update Time:** Includes radio buttons for 'Upgrade Now' (selected) and 'Scheduled Time'. The 'Scheduled Time' section has a time picker set to 00:00:00. There is also a 'Description' text area.

At the bottom, there are 'Cancel', 'Previous', and 'OK' buttons. The 'OK' button is highlighted.

- 4 Make a search according to your specified criteria. Select the individual managed devices that you want to upgrade with the selected firmware. Click **OK**. (You can also use the **By OTV** screen to choose the devices for firmware upgrade.)

The screenshot shows a 'Select Devices' dialog box with two tabs: 'By Search' (active) and 'By OTV'. Under 'By Search', there are input fields for 'Device Type' (set to 'Switch'), 'Device Model' (set to 'ES-2108-LC'), 'Display Name', 'IP Address', 'Firmware', and a 'Group' dropdown menu (set to 'All'). A 'Search' button is located below these fields. Below the search fields are two lists: 'Available List' and 'Selected List'. The 'Available List' contains two IP addresses: '172.23.39.129' and '172.23.49.49'. The 'Selected List' is currently empty. Between the two lists are four arrow buttons: '>', '>>', '<<', and '<'. At the bottom of the dialog are 'Cancel' and 'Ok' buttons. Status text at the bottom of each list indicates 'Showing 2 of 2' for the available list and 'Showing 0 of 0' for the selected list.

- 5 Set a time for the ENC to perform the upgrade or leave **Upgrade Now** selected to do it right away. You can also optionally add a descriptive note. Click **OK**.

Make sure the ENC and the managed devices do NOT get turned off during the upgrade process, as it may corrupt the firmware on the managed device and leave it unusable.

Edit Schedule List

Firmware Upgrade

Firmware List

	Device Model	Firmware Version	Firmware Description
1	ES-2108-LC	3.9	fireware file

Device Information

Device Model : ES-2108-LC

	Device Name	Current Firmware Version
1	172.23.49.49	3.60
2	172.23.39.129	3.80

Update Time

☐ Upgrade Now

☒ Scheduled Time

2010-09-15 * 00 : 00

Description

Cancel

OK

4.3 Script Distribution

Use script files to apply commands that you specify. Use the ENC to create the script files.

Click **Configuration > Script Distribution** to open the **Script** screen. Use the **Script** screens to create and manage script distribution entries. Use script distribution entries to create, store, name, and run script files. You can store multiple script files on the ENC at the same time.

Figure 71 Configuration > Script Distribution

Script Distribution

Device Name:

☒ Add

☐ Edit

☐ Remove

☐ View Log

	Status	Name	Device Amount	Protocol	Start Time	End Time
1	<input type="checkbox"/> Success	scriptTest	1	Telnet	2010-07-07 14:37:38	2010-07-07 14:37:56

Page 1 of 1

10

View 1 - 1 of 1

Each field is described in the following table.

Table 31 Configuration > Script Distribution

LABEL	DESCRIPTION
Device Name	To only display scripts for a specific model, enter a part of the device name or the full name here and click Search .
Add	Click this to create a new script distribution entry for having the ENC apply a script to managed devices.
Edit	Select an entry with a status of Waiting and click this to edit the entry.
Remove	Select an entry and click this to delete it. You cannot delete an entry that has a status of Running .
View Log	Select an entry and click this to display a log of the script's distribution history.
check box	Select the check box of an entry and click Edit , Remove or View Log to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Status	This shows whether the script distribution is Running , waiting to start (Waiting), has failed (Fail), has all completed (Success) or has partial completed (Partial Success).
Name	This field displays the name of the entry.
Device Amount	This is to how many devices this script distribution entry applies.
Protocol	This shows the protocol (Telnet or SSH) which the ENC uses to connect to the specified device(s) and execute this script.
Start Time	This is the date and time that the script distribution entry was (or is scheduled to be) applied.
End Time	This is the date and time the ENC stopped applying the script distribution. This is N/A if the script distribution has not yet been applied.

4.3.1 Script Distribution Add

Use script files to apply commands that you specify.

Click **Configuration > Script Distribution > Add** to open the following screen. Use this screen to create a script distribution entry to create, store, name, and run script files.

Note: For some device models, you may need to include `write` commands in your scripts. If you do not use the `write` command, the changes will be lost when the device restarts. You could use multiple `write` commands in a long script.

Figure 72 Configuration > Script Distribution > Add

Add Script Distribution

General Setting

Protocol ☒ Telnet ☐ SSH
Name
Interval * 2~60 seconds
Device List

+ Add - Remove

<input type="checkbox"/>	Device Name	IP Address	Model Name

Commands

#Usage:
1.use '#' for comments;
2.<command> | <keywords for response checking>;
#Example:
#show ip | ip interface
#It sends the 'show ip' command,and check response whether contains 'ip interface',otherwise,return fail.

Schedule Time

☒ Send Now
☐ Schedule Time O'clock

Cancel Ok

Each field is described in the following table.

Table 32 Configuration > Script Distribution > Add

LABEL	DESCRIPTION
Protocol	Select the protocol (Telnet or SSH) which the ENC uses to connect to the specified device(s) and execute this script.
Name	Enter up to 32 characters to specify a name for the script distribution entry.
Interval	Specify how long the ENC is to wait (in seconds) between sending two commands to the entry's listed devices. Note: You can put commands that need a longer time to process in a separate script file and set a longer interval for it.
Device List	Use this table to select the devices to which you want to apply the script.

Table 32 Configuration > Script Distribution > Add (continued)

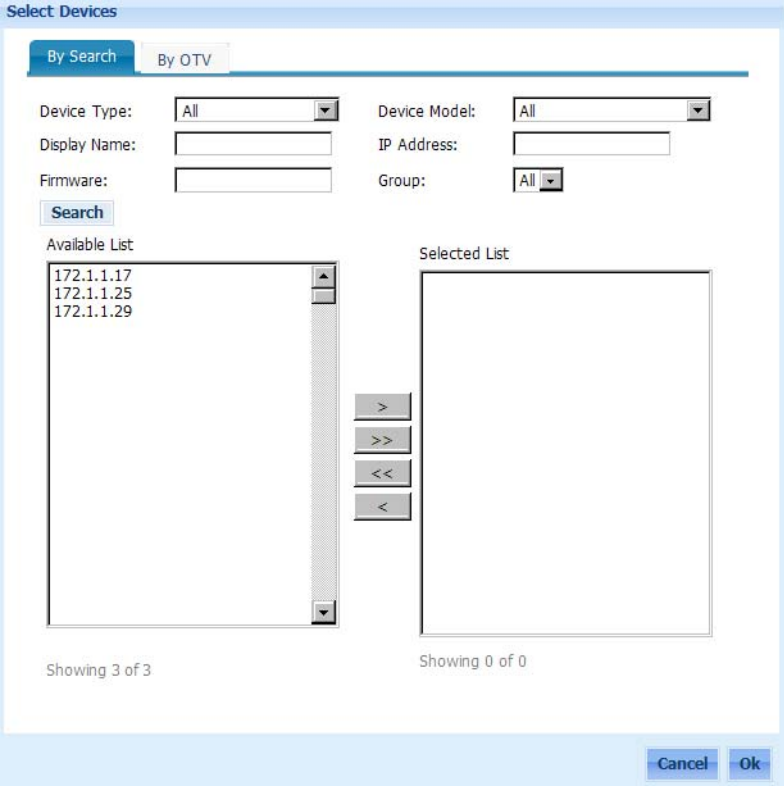
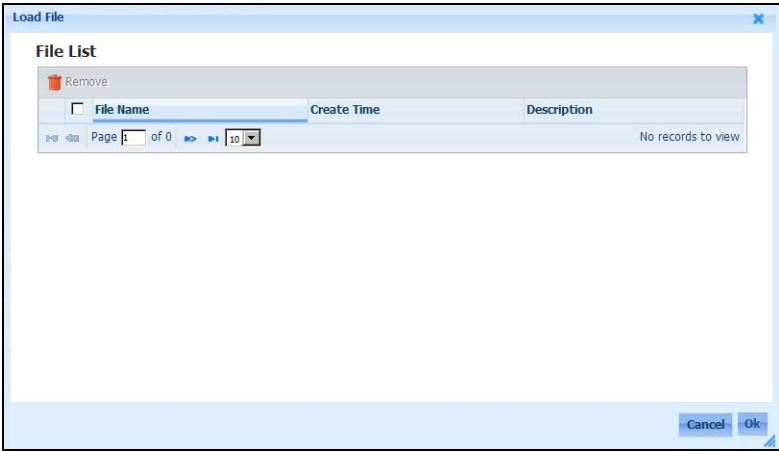
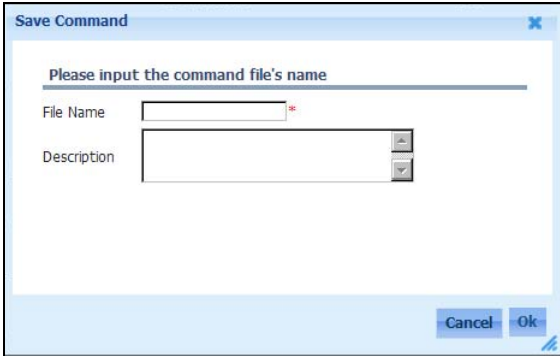
LABEL	DESCRIPTION
Add	<p>Click this to open screens where you can add devices to the list.</p> <p>In the By Search screen, select the individual managed devices to which you want to apply the script. You can display the list of available devices by OTV, device view, or group view. Click OK.</p> <p>Figure 73 Select Devices - By Search</p> 
Remove	Select an entry and click this to delete it from the list.
check box	Select the check box of an entry and click Remove to delete it. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Device Name	This field displays the name of each managed device to which you want to apply the script.
IP Address	This field displays the corresponding IP address of each listed managed device.
Model Name	This field displays the name of the device model for each listed managed device.
Commands	<p>Use this section to list the commands you want to run on the selected managed devices.</p> <p>Use a pound sign '#' in the beginning of a line for a note. Use a pipe character ' ' followed by keywords that identify whether the script has failed or not. If the entire keywords can be found in the command output, the script continues. Otherwise, the ENC terminates the script and returns "failed".</p> <p>This is an example:</p> <pre>show ip ip interface</pre> <p>#A command of 'show ip' is included in this script. The ENC will check whether the command output contains 'ip interface'. If it does not, it stops this command and returns 'failed'. The script continues if there is the next command.</p>

Table 32 Configuration > Script Distribution > Add (continued)

LABEL	DESCRIPTION
Load Commands	<p>If you have already created and saved command list files, you can click this Load Commands icon to be able to select which of them you want to use. The following screen appears.</p> <p>Figure 74 Load Commands</p>  <p>Select a file and click Ok to load commands from the file to the ENC. Select one or more files and click Remove if you want to delete them. Click Cancel to exit this screen without loading any commands.</p>
Save Commands	<p>Click this icon to save the commands listed in the text frame below as a command list file. The Save Command screen appears.</p> <p>Figure 75 Save Command</p>  <p>The fields in this Save Command screen are described as following:</p> <ul style="list-style-type: none"> • File Name: Enter up to 32 characters for the name of the command list file. You can use alphanumeric characters (0-9, a-z, A-Z), underscores (_) and hyphen (-). • Description: Type additional information for the file in this field. • Cancel: Click this to discard the changes and exit this screen. • Ok: Click this to save the changes and exit this screen.
Clear	Click this icon to clear the text frame.
Schedule Time	Use this section to either apply the commands to the selected managed devices immediately (Send Now) or schedule it for a specific date and time (Schedule Time). This time is based on the ENC server's time.
Cancel	Click this to discard all changes and close this screen.
Ok	Click this to save the changes and close this screen.

4.4 Configuration File Update/Backup

Use these screens to upload configuration files to the ENC and have the ENC use them to configure managed devices.

You must be logged in with system administrator rights to use this function.

Note: Do NOT turn off the switch during the updating process, as it may corrupt the firmware and make the selected switch unusable.

4.4.1 Configuration File List

Click **Configuration > Update/Backup** to display the list of configuration files.

Figure 76 Configuration > Update/Backup

The following table describes the labels in this screen.

Table 33 Configuration > Update/Backup

LABEL	DESCRIPTION
Device Model	To only display configuration files for a specific model, select the model here and click Search .
Firmware Version	To only display configuration files of a specific firmware version, select the model in the Device Model field and then select the firmware version and click Search .
Backup Time	Select a time period to limit up to how long ago the configuration files were saved to the ENC and click Search .
Add	Click this to upload a configuration file to the ENC.
Remove	Select an entry and click this to delete it.
Export	Select an entry and click this to view the configuration file or save it to the computer you are using to access the ENC.
check box	Select the check box of an entry and click Remove or Export to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
File Name	This is the file name of the configuration file saved on the ENC.
Device Model	This field displays the name of the device model for which the configuration file was uploaded.
Firmware Version	This field displays the version of the firmware file.
Backup Time	This is when the configuration file was saved to the ENC.
Description	This field displays any special information that you specified about the configuration file.
Admin	This is the name of the administrator who uploaded the configuration file or set the ENC to back up the configuration file from a managed device.

4.4.2 Uploading Configuration Files to the ENC

Click **Configuration > Update/Backup > Add** to upload configuration files to the ENC. You can get the configuration files from managed devices or from your computer if you have them stored there.

Figure 77 Configuration > Update/Backup > Add > Backup From Device

The 'Add File' dialog box has two tabs: 'Backup From Device' (selected) and 'Upload File'. Under 'Backup From Device', there are fields for 'File Name' (containing '2010-9-21_batch-bk') and 'Description'. Below these is a 'Device List' table with an 'Add' button. The table has columns for 'Device Name', 'Device Model', and 'Firmware Version'. At the bottom right are 'Cancel' and 'OK' buttons.

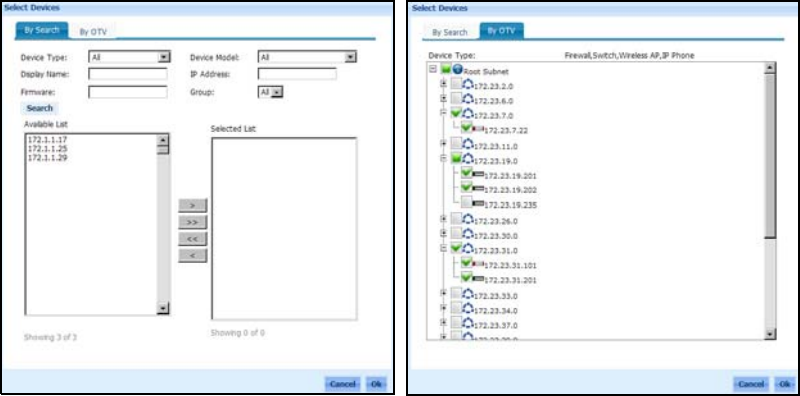
	Device Name	Device Model	Firmware Version
1	172.23.7.22	ZyWALL USG 100	No such object
2	172.23.11.12	NWA-3163	V3.71(AAN.0) 11/25/2009
3	172.23.19.202	IES-5005	
4	172.23.11.13	NWA-3163	V3.71(AAN.0) 11/25/2009
5	172.23.11.11	NWA-3163	V3.71(AAN.0) 11/25/2009
6	172.23.19.201	IES-6000	

Figure 78 Configuration > Update/Backup > Add > Upload File

The 'Add File' dialog box has two tabs: 'Backup From Device' and 'Upload File' (selected). Under 'Upload File', there are fields for 'Device Model' (a dropdown menu showing 'ES-3124'), 'Firmware Version', 'Description', and 'File Path and Name' (with a 'Browse...' button). At the bottom right are 'Cancel' and 'OK' buttons.

The following table describes the labels in this screen.

Table 34 Configuration > Update/Backup > Add

LABEL	DESCRIPTION
Backup From Device	Select this to get a configuration file from a managed device.
Upload File	Select this to upload a configuration file saved on your computer.
Backup	The following fields appear when you select Backup From Device .
File Name	Enter up to 20 characters to specify a name for the configuration file. You can use letters, numbers, underscores, and dashes.
Description	List any special information that you want to record about the configuration file.
Device List	If you will backup configuration files from managed devices, use this table to select the managed devices from which you want the ENC to save copies of their configuration files.
Add	<p>Click this to open a screen where you can add devices to the list. The ENC will get the configuration files from the devices.</p> <p>You can display a list of available devices by search or by the OTV view. In the By Search screen, enter the criteria such as device model and group and click Search to filter the available devices. Select one or more devices from which you want to back up the configuration files. Click > or >> to move them to the Selected List. Click OK.</p>  <p>In the By OTV screen, select device(s) from the OTV list and then click OK.</p>
Device Name	This field displays the name of each selected managed device.
Device Model	This field displays the model name of each selected managed device.
Firmware Version	This field displays the version of the firmware file.
Upload File	The following fields appear when you select Upload File .
Device Model	Select the model to which the configuration file applies.
Firmware Version	Specify the version of the firmware the device is using.
Description	List any special information that you want to record about the configuration file.
File Path and Name	Type the path and file name of the configuration file you wish to upload to the ENC in the text box or click Browse to locate it.
Cancel	Click Cancel to discard all changes and close this screen.
OK	Click OK to save the changes and close this screen.

4.4.3 Backup Schedule List

Click **Configuration > Update/Backup > Backup Schedule List** to have the ENC save backup copies of the configuration files on managed devices.

Figure 79 Configuration > Update/Backup > Backup Schedule List

The screenshot shows the 'Backup Schedule List' interface. At the top, there is a 'Device Name' search field with a 'Search' button. Below this are three action buttons: 'Add' (green plus icon), 'Edit' (yellow pencil icon), and 'Remove' (red trash icon). A table with the following columns is displayed: 'Status' (with a checkbox), 'File Name', 'Total Device', 'Backup Time' (with a clock icon), 'Description', and 'Admin'. At the bottom of the table area, it says 'Page 1 of 0' and 'No records to view'.

The following table describes the labels in this screen.

Table 35 Configuration > Update/Backup > Backup Schedule List

LABEL	DESCRIPTION
Device Name	To narrow down the list of displayed results, specify the name or partial name of a managed device.
Add	Click this to create a new schedule for having the ENC back up configuration files from managed devices.
Edit	Select an entry that has a Status of Waiting and click this to edit the entry.
Remove	Select an entry that is not running and click this to delete it.
check box	Select the check box of an entry and click Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Status	This shows whether the scheduled configuration download is Running , waiting to start (Waiting), has failed (Fail), has all completed (Success), or has partially completed (Partial Success).
File Name	Enter up to 20 characters to specify a name for the configuration file. You can use letters, numbers, underscores, and dashes.
Total Device	This is how many devices this schedule is to have the ENC back up configuration files from.
Backup Time	This is the date and time the schedule will have the ENC back up the selected managed devices' configuration files.
Description	This field displays any special information specified about the backup schedule.
Admin	This is the name of the administrator who created the configuration backup schedule.

4.4.4 Creating or Editing a Backup Schedule List

Click **Configuration > Update/Backup > Backup Schedule List > Add** (or select a schedule and click **Edit**) to create or edit a configuration backup schedule.

Figure 80 Configuration > Update/Backup > Backup Schedule List > Add

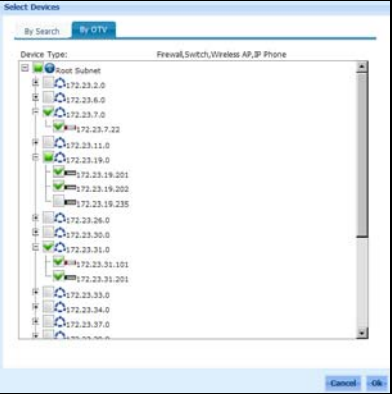
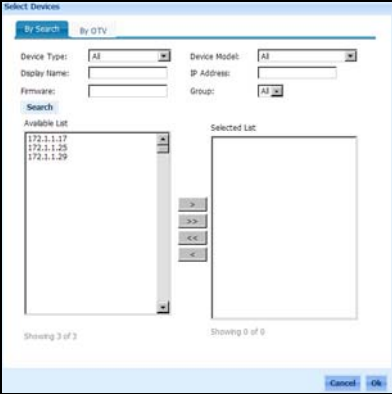
The screenshot shows the 'Add Backup' configuration window. It includes a 'Backup' section with 'File Name' and 'Description' fields. Below is a 'Device List' section with an 'Add' button and a table with columns 'Device Name', 'Device Model', and 'Firmware Version'. The 'Backup Time' section has radio buttons for 'Backup Now' (selected) and 'Scheduled Time' (with a time picker). The window has 'Cancel' and 'OK' buttons at the bottom right.

The following table describes the labels in this screen.

Table 36 Configuration > Update/Backup > Backup Schedule List > Add

LABEL	DESCRIPTION
File Name	Enter up to 20 characters to specify a name for the configuration file. You can use letters, numbers, underscores, and dashes.
Description	List any special information that you want to record about the configuration file.
Device List	If you will backup configuration files from managed devices, use this table to select the managed devices from which you want the ENC to save copies of their configuration files.

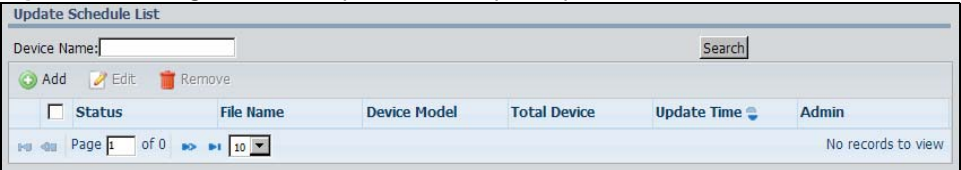
Table 36 Configuration > Update/Backup > Backup Schedule List > Add (continued)

LABEL	DESCRIPTION
Add	<p>Click this to open a screen where you can add devices to the list. The ENC will get the configuration files from the devices.</p> <p>You can display a list of available devices by search or by the OTV view. In the By Search screen, enter the criteria such as device model and group and click Search to filter the available devices. Select one or more devices from which you want to back up the configuration files. Click > or >> to move them to the Selected List. Click OK.</p> <div></div> <p>In the By OTV screen, select device(s) from the OTV list and then click OK.</p>
Device Name	This field displays the name of each selected managed device.
Device Model	This is the model of the selected managed device.
Firmware Version	This field displays the version of the firmware the device is using.
Backup Time	Use this section to have the ENC back up the configuration files of the selected managed devices immediately or schedule it for a specific date and time.
Cancel	Click Cancel to discard all changes and close this screen.
OK	Click OK to save the changes and close this screen.

4.4.5 Update Schedule List

Click **Configuration > Update/Backup > Update Schedule List** to display the following screen. Use this screen to have the ENC upload configuration files to managed devices. Before you can do this you need to use the **Configuration > Update/Backup > Configuration File List** screen to upload the configuration files to the ENC (see [Section 4.4.1 on page 111](#)) or use the **Configuration > Update/Backup > Backup Schedule List** screen to back up the configuration files to ENC (see [Section 4.4.3 on page 114](#)).

Figure 81 Configuration > Update/Backup > Update Schedule List



The following table describes the labels in this screen.

Table 37 Configuration > Update/Backup > Update Schedule List

LABEL	DESCRIPTION
Device Name	To narrow down the list of displayed results, specify the name or partial name of a managed device.
Add	Click this to create a new schedule for having the ENC upload configuration files to managed devices.
Edit	Select an entry that has a Status of Waiting and click this to edit the entry.
Remove	Select an entry that is not running and click this to delete it.
check box	Select the check box of an entry and click Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Status	This shows whether the scheduled configuration upload is Running , waiting to start (Waiting), has failed (Fail), has all completed (Success) or has partial completed (Partial Success). Note: Some devices may need a manual system restart to complete the whole configuration restore process. Check the User's Guide of your device for the related information.
File Name	Enter up to 20 characters to specify a name for the configuration file. You can use letters, numbers, underscores, and dashes.
Device Model	This is the model of the selected managed device.
Total Device	This is how many devices this schedule is to have the ENC upload configuration files to.
Update Time	This is the date and time that the configuration file update was (or is scheduled to be) performed.
Admin	This is the name of the administrator who created the configuration file update schedule.

4.4.6 Creating or Editing an Update Schedule List

Click **Configuration > Update/Backup > Update Schedule List > Add** (or select a schedule and click **Edit**) and use the following steps to create or edit a waiting configuration update schedule. For an existing update schedule you can only edit the update time; skip to the last step for details.

- 1 Select the model for which you want to update the configuration file and click **Next**.

- 2 Select the configuration file to upload to the managed devices and click **Next**.

Select File

Please Select File

	File Name	Device Model	Firmware Version	Backup Time	Description	Admin
1	config01	ES-2108-LC	3.60	2010-07-01 11:51:43		root
2	config01	ES-2024A	3.60	2010-07-01 11:51:41		root

Page 1 of 1

View 1 - 2 of 2

Cancel Previous Next

- 3 Under **Device List** click **Add**.

Add Update

File

	File Name	Device Model	Firmware Version	Backup Time	Description	Admin
1	config01	ES-2024A	3.60	2010-07-01 11:51:41		root

Device List

Add

Device Name	Device Model	Firmware Version
-------------	--------------	------------------

Update Time

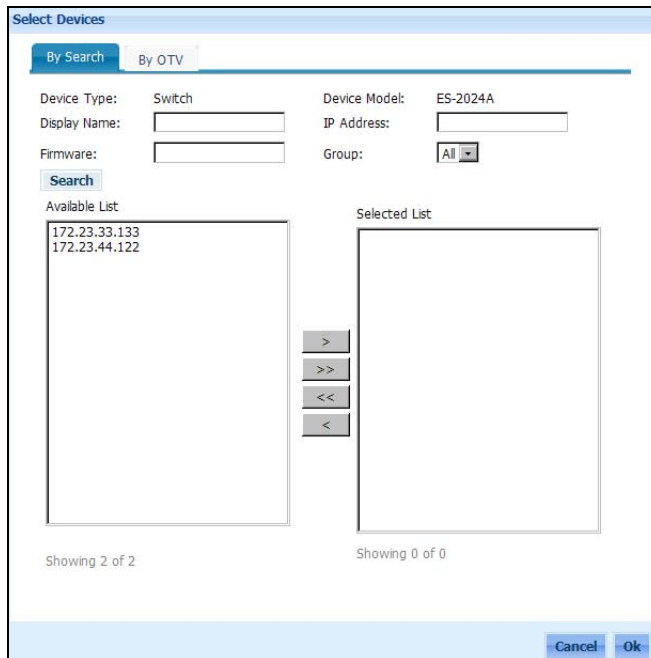
☒ Update Now

☐ Scheduled Time

00:00

Cancel Previous OK

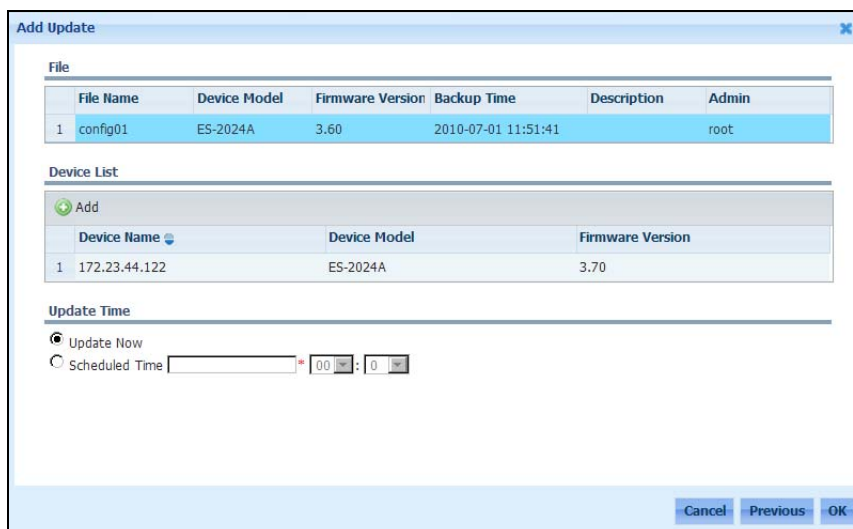
- 4 Select the individual managed devices to which you want to upload the selected configuration file. You can display the list of available devices by OTV, device view, or group view. Click **OK**.



The **Select Devices** dialog box has two tabs: **By Search** (selected) and **By OTV**. Under **By Search**, there are input fields for **Device Type** (Switch), **Device Model** (ES-2024A), **Display Name**, **IP Address**, **Firmware**, and **Group** (All). A **Search** button is below these fields. Below the search fields are two lists: **Available List** and **Selected List**. The **Available List** contains two IP addresses: 172.23.33.133 and 172.23.44.122. The **Selected List** is empty. Between the lists are four arrow buttons: >, >>, <<, and <. At the bottom right are **Cancel** and **Ok** buttons. Status text at the bottom indicates 'Showing 2 of 2' for the available list and 'Showing 0 of 0' for the selected list.

- 5 Set a date and time for the ENC to perform the update or leave **Update Now** selected to do it right away. Click **OK**.

Make sure the ENC and the managed devices do NOT get turned off during the update process, as it may leave the managed device unusable.



The **Add Update** dialog box contains three sections. The **File** section has a table with the following data:

	File Name	Device Model	Firmware Version	Backup Time	Description	Admin
1	config01	ES-2024A	3.60	2010-07-01 11:51:41		root

The **Device List** section has an **Add** button and a table with the following data:

	Device Name	Device Model	Firmware Version
1	172.23.44.122	ES-2024A	3.70

The **Update Time** section has two radio buttons: **Update Now** (selected) and **Scheduled Time**. The **Scheduled Time** field is empty, with a time picker showing 00:00.

4.5 Default Performance Monitor Library

Click **Configuration > Performance Monitor Library** to open the **Default Monitor Library** screen. Use this screen to view the default performance monitors that you can use in the **Tool > Performance Monitoring** screens (see [Section 6.8 on page 161](#)).

Figure 82 Configuration > Performance Monitor Library > Default Monitor Library

Default Monitor Library		Customized Monitor Library	
	Name	MIB Node	Description
1	Device CPU Utilization	cpu	Monitor the device CPU utilization
2	Memory Utilization	memory	Monitor the device memory utilization
3	Interface Bandwidth Utilization	ifSpeed, ifOutOctets, ifInOctets	Monitor the interface bandwidth utilization
4	Interface Traffic	ifOutOctets, ifInOctets	Monitor the traffic of all interfaces
5	Interface Unicast Traffic	ifOutUcastPkts, ifInUcastPkts	Monitor the unicast traffic of all interfaces
6	Interface Non-unicast Traffic	ifOutNUcastPkts, ifInNUcastPkts	Monitor the non-unicast traffic of all interfaces
7	Interface Errors	ifOutErrors, ifInErrors	Monitor the errors of all interfaces

Each field is described in the following table.

Table 38 Configuration > Performance Monitor Library > Default Monitor Library

LABEL	DESCRIPTION
Name	This field displays the name of a performance monitor.
MIB Node	This field displays the MIB node(s) this monitor uses.
Description	This field displays additional information for the monitor.

4.5.1 Customized Performance Monitor Library

Click **Configuration > Performance Monitor Library > Customized Monitor Library** to open the **Default Monitor Library** screen. Use this screen to configure more performance monitors that you can use in the **Tool > Performance Monitoring** screens (see [Section 6.8 on page 161](#)).

Figure 83 Configuration > Performance Monitor Library > Customized Monitor Library

Default Monitor Library

Customized Monitor Library

Add

Edit

Remove

	<div><input type="checkbox"/> Name</div>	MIB Node	Description
1	<div><input type="checkbox"/> monitorTest-template-1</div>	ifEntry	
2	<div><input type="checkbox"/> monitorTest2-template-2</div>	ifIndex	

Page 1 of 1

10

View 1 - 2 of 2

Each field is described in the following table.

Table 39 Configuration > Performance Monitor Library > Customized Monitor Library

LABEL	DESCRIPTION
Add	Click this to create a performance monitor.
Edit	Select a performance monitor and click this to modify it.
Remove	Select one or more performance monitors and click this to remove them.
check box	Select the check box of one or more entries and click Edit or Remove to take the action for the entries respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Name	This field displays the name of a configured performance monitor.

Table 39 Configuration > Performance Monitor Library > Customized Monitor Library (continued)

LABEL	DESCRIPTION
MIB Node	This field displays the MIB node this monitor uses.
Description	This field displays additional information for the monitor.

4.5.2 Add a Performance Monitor

Click **Add** in the **Configuration > Performance Monitor Library > Customized Monitor Library** screen to open the following screen. Use this screen to configure more performance monitors that you can use in the **Tool > Performance Monitoring** screens (see [Section 6.8 on page 161](#)).

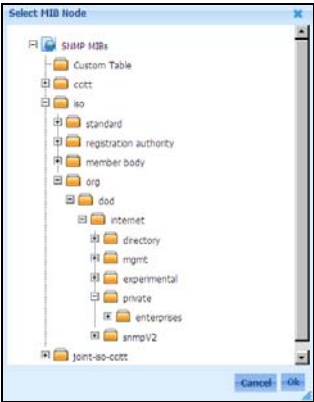
Figure 84 Configuration > Performance Monitor Library > Customized Monitor Library > Add

Each field is described in the following table.

Table 40 Configuration > Performance Monitor Library > Customized Monitor Library > Add

LABEL	DESCRIPTION
Monitor Library Name	Type up to 32 alphanumeric characters for the name of the performance monitor. You can also use underscores (_) and hyphens (-). Spaces are not allowed.

Table 40 Configuration > Performance Monitor Library > Customized Monitor Library > Add

LABEL	DESCRIPTION
MIB Node	<p>Click Select MIB Node to open the following screen.</p>  <p>Choose the MIB node this monitor will use and click Ok.</p> <p>This field will then display the object ID of the selected MIB node.</p>
Description	Type additional information for the monitor in this field.

This chapter describes the event log settings on the ENC.

5.1 Event Viewer

A managed device sends traps to the ENC when an event occurs. To display device and system event logs, click **Events** > **Viewer**.

Figure 85 Event Viewer

The screenshot shows the 'Viewer' interface with the following search filters:

- Time: Last 24 hours
- Severity: >= Info
- Category & Event: All
- Status: All
- Source: (empty)

Buttons: Acknowledge, PDF, CSV, Search, Hidden Search.

	<input type="checkbox"/> Ack/UnAck	Name	Date/Time	Category	Severity	Source	Message
1	<input type="checkbox"/>	Device Up	2011-01-26 14:03:12	Topology	Info	DIVINE-PC	Device is up: 172.23.41.6:DIVINE-PC,Host.
2	<input type="checkbox"/>	Device Down	2011-01-26 11:42:12	Topology	Major	DIVINE-PC	Device is down: 172.23.41.6:DIVINE-PC,Host.
3	<input type="checkbox"/>	Device Up	2011-01-26 11:12:12	Topology	Info	DIVINE-PC	Device is up: 172.23.41.6:DIVINE-PC,Host.
4	<input type="checkbox"/>	Device Down	2011-01-25 19:39:11	Topology	Major	DIVINE-PC	Device is down: 172.23.41.6:DIVINE-PC,Host.

Page 1 of 1 | View 1 - 4 of 4

The following table describes the labels in this screen.

Table 41 Event Viewer

LABEL	DESCRIPTION
Show Search Hide Search	Click Show Search to display further fields for you to search specific event logs stored in the ENC. Click Hide Search to hide those fields.
Time	<p>All logs have a time-stamp. The time stamp depends on the time configured on the device.</p> <p>Specify the time (since how many hours or days ago) to display the event logs. Select Custom and specify the start and end dates from which the device generated event logs.</p>

Table 41 Event Viewer (continued)

LABEL	DESCRIPTION
Severity	<p>Set your filters according to what severity levels of the logs are being displayed for the search criteria. For the first drop-down list box, the following parameters can be used.</p> <ul style="list-style-type: none"> • >= - Select this if you want to display event logs with the severity level higher than or equal to the severity you set. • = - Select this if you want to display event logs with the severity level equal to the severity you set. • <= - Select this if you want to display event logs with the severity level lower than or equal to the severity you set. <p>Select the severity level of the event logs in the second drop-down list box. The choices and the severity level from low to high are Info, Warning, Minor, Major, and Critical.</p> <p>For example, select >= and Major to display the matched event logs with severities Major and Critical.</p>
Category & Event	Specify an event category and/or event to make a search. Select All to specify a category and/or event. See Section 5.1.1 on page 125 for more details.
Status	Specify whether to display Acknowledged , Unacknowledged or All events.
Source	Type the name of the device(s) you wish to find. You can type a part of the device name for the search criteria.
Search	Click this to display the matched event logs.
Acknowledge	Click Acknowledge to acknowledge any selected log messages.
PDF	Click this to export the table to a PDF file on the computer you are using to access the ENC.
CSV	Click this to export the table to a CSV file on the computer you are using to access the ENC.
check box	Select the check box of an entry and click Acknowledge to take the action for the entry. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Ack/UnAck	This field displays whether a log has been acknowledged by an administrator. If you have configured to clear the correlated events for an event (in the Events > Configuration > Customize > Add/Edit screen), the latest correlated event will be unacknowledged automatically first, the others will be acknowledged later.
Name	This field displays the name of the event.
Date/Time	This field displays the date and time when the event log was generated.
Category	This field displays the name of the category to which this event log belongs.
Severity	<p>This field displays the severity level of the event log. Each severity level color is defined as the follows:</p> <ul style="list-style-type: none"> • Critical - red • Major - orange • Minor - grass green • Warning - cyan • Info - forest green • Unknown - blue
Source	This field displays the device name. Click the device name to view the detailed device settings (see Section 6.2 on page 140 for more information). Click the Locate It in OTV icon to quickly find the device in the OTV panel.
Message	This field displays some information about the event log.

5.1.1 Events

The following table describes the events by categories.

Table 42 Event Categories and Events

EVENT	DESCRIPTION
Configuration	
These events are about the results of options performed through the ENC.	
Configuration Backup Failed	Configuration file download failed.
Configuration Backup Succeeded	Configuration file download was successful.
Configuration Update Failed	Configuration file upload failed.
Configuration Update Succeeded	Configuration file upload was successful.
Firmware Upgrade Failed	Firmware upload failed.
Firmware Upgrade Succeeded	Firmware upload was successful.
Script Execution Failed	Failed to execute the script.
Script Execution Succeeded	The script was successfully executed.
SNMP Traps	
These events are about device traps received by the ENC.	
Authentication Failure	The ENC failed to access a managed device because of a wrong community setting.
Cold Start	The device was powered on.
egpNeighborLoss	Failed to receive a neighbor's response to the device's polls through EGP. The device will then assume that the neighbor is down and remove the neighbor's routes from its database. Exterior Gateway Protocol (EGP) is a routing protocol used for exchanging routing information with gateways in other autonomous systems. Computers communicating via EGP are called EGP neighbors. EGP uses Hello and I-Heard-You (I-H-U) message exchanges to monitor neighbors' reachability.
LinkDown	An interface of the device went down.
LinkUp	An interface of the device went up.
Warm Start	The device performed a software restart.
Threshold Crossing	
These events are about a variable that has went out of the set thresholds.	
Failling Threshold	A variable fell below the set "falling" threshold.
Raising Threshold	A variable went over the set "rising" threshold.
Topology	
These events are about topology changes detected by managed devices.	
Device Down	A network device is disconnected or powered off and causes the STP topology to change.
Device Up	A network device is available or powered on and causes the STP topology to change.
Link Down	The connection is down.
Link Up	The connection is up.
Service Available	The service is functioning normally.
Service Not Available	The service is not available.

5.2 Event Configuration

This screen shows a list of events that devices or the ENC may generate. By default, each event has a priority (severity level) and the corresponding action that the ENC should take when it receives the event. You can use this screen to modify the severity and action.

To change the severity level and/or action of a default event, click **Events > Configuration**.

Figure 86 Events > Configuration > Default

DefaultCustomize

General

Stored Events Days:301~90 days

Events Configuration

ActivateDeactivateEdit

	Status	Category	Event Name	Severity	Action
1	<input type="checkbox"/>	Configuration	AP Profile Set Failure	Minor	default
2	<input type="checkbox"/>	Configuration	AP Profile Set Success	AP Profile Set Failure	default
3	<input type="checkbox"/>	Configuration	Configuration Backup Failure	Minor	default
4	<input type="checkbox"/>	Configuration	Configuration Backup Success	Info	default
5	<input type="checkbox"/>	Configuration	Configuration Update Failure	Minor	default
6	<input type="checkbox"/>	Configuration	Configuration Update Success	Info	default
7	<input type="checkbox"/>	Configuration	Firmware Upgrade Failure	Minor	default
8	<input type="checkbox"/>	Configuration	Firmware Upgrade Success	Info	default

ApplyReset

The following table describes the labels in this screen.

Table 43 Events > Configuration > Default

LABEL	DESCRIPTION
General	
Stored Events Days	Specify the number of days you wish to store event logs in ENC before removing them.
Events Configuration	
Activate	Select one or more disabled events and click this button to enable them.
Deactivate	Select one or more enabled events and click this button to disable them.
Edit	Select an event and click this to modify the settings.
Status	This field displays whether the event is currently enabled or disabled.
Category	This field displays the category to which the event belongs.
Event Name	This field displays the name of the event.
Severity	This field displays the severity level of the event.
Action	This field displays the action the ENC takes when the event was generated.
Apply	Click this to save the changes.
Reset	Click this to discard the changes and reset the fields to their last saved settings.

5.2.1 Edit Event Configuration

To modify an event's setting, select an event and click **Edit** in the **Events > Event Configuration**.

Figure 87 Event Configuration > Default > Edit

The following table describes the labels in this screen.

Table 44 Event Configuration > Default > Edit

LABEL	DESCRIPTION
Event Name	This field displays the name of the selected event.
Category	This field displays the category to which the event belongs.
Trap OID	This field displays the object identifier (OID) of the event. An OID identifies a trap (an event).
Severity	Select the severity level for the event you want to display in the ENC. The choices and the severity level from low to high are Info , Warning , Minor , Major , and Critical .
Message	Type the information you wish to display for the event in the ENC. You can use the variables defined on the right hand of the screen. For example, use "\$2" to display the device name that generates this event.
Action	Select the action profile to apply to this event. The ENC takes the action when it receives this event. Select None to not apply this event any action.
Clear Correlated Events	
Clear correlated events	Select this to have the ENC automatically acknowledge any selected correlated events.
Available Events	This field displays all available correlated events that you can select. Select one or more events (select while pressing [Ctrl]) and press the right arrow button (>) to add them into the selected list at the right field. Use the double right arrow button (>>) to add all available events to the right field.

Table 44 Event Configuration > Default > Edit (continued)

LABEL	DESCRIPTION
Selected Correlate Events	This field displays the event(s) you selected to make a correlation with this event. Select one or more events (select while pressing [Ctrl]) and press the left arrow button (<) to remove them from this field. Use the double left arrow button (<<) to remove all events except the default one from this field.
Cancel	Click this to discard the changes and close this screen.
OK	Click this to save the changes and close this screen.

5.3 Customized Events

This screen displays a list of customized events. To open the screen, click **Events > Configuration > Customize**.

Figure 88 Events > Configuration > Customize

Custom Events Configuration			
Add Edit Remove			
<input type="checkbox"/> Category	Event Name	Severity	Action
1 <input type="checkbox"/> SNMP Traps	EventEx1	Info	default

The following table describes the labels in this screen.

Table 45 Events > Configuration > Customize

LABEL	DESCRIPTION
Add	Click this to create an event.
Edit	Click this to modify a selected event.
Remove	Click this to delete the selected event(s).
check box	Select the check box of an entry and click Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Category	This field displays the category to which the event belongs.
Event Name	This field displays the name of the selected event.
Severity	This field displays the severity level of the event.
Action	This field displays the name of the action profile this event applies. The ENC takes the action when it receives this event.

5.3.1 Customize an Event

Use this screen to configure an event that has managed devices notify the ENC without being requested when the event occurs. It does this by sending a message known as a trap.

To open this screen, click **Add** or **Edit** in the **Events > Configuration > Customize** screen. A customized event must belong to the SNMP traps category.

Figure 89 Events > Configuration > Customize > Add/Edit

The following table describes the labels in this screen.

Table 46 Events > Configuration > Customize > Add/Edit

LABEL	DESCRIPTION
General Settings	
Event Name	Type a descriptive name (up to 32 characters) for this event for identification purposes. You can use alphanumeric characters (0-9, a-z, A-Z), hyphen (-), and underscore (_). Spaces are allowed. This field is read-only if you are editing an existing event.
Category	This field displays the category to which the event belongs.
SNMP Trap Version	Select the version of the SNMP trap messages. Select SNMP version 1 (v1) or both SNMP version 2c and version 3 (v2c/v3). SNMP v2c and v3 traps use different format comparing to SNMP v1. Note: SNMP version 2c is backward compatible with SNMP version 1.

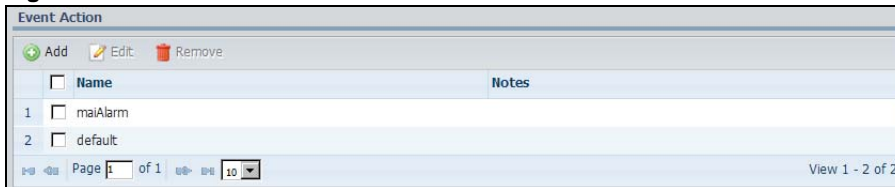
Table 46 Events > Configuration > Customize > Add/Edit (continued)

LABEL	DESCRIPTION
Generic Type	This field is available if you select v1 in the SNMP Trap Version field. Select a trap from the drop-down list box in order to associate it with this event. You can select a standard generic trap (coldStart , warmStart , linkDown , linkUp , authenticationFailure , egpNeighborLoss) or a vendor specific trap (enterpriseSpecific).
Specific Type	This field is available and mandatory if you select enterpriseSpecific(6) in the Generic Type field. Enter a code number that identifies a specific trap supported by a vendor's devices.
Enterprise OID	This field is available if you select v1 in the SNMP Trap Version field. Type a MIB object identifier (OID) or click the magnifier icon next to this field to find the object you are looking for.
Trap OID	This field is available if you select v2c/v3 in the SNMP Trap Version field. Type a MIB object identifier (OID) or click the magnifier icon next to this field to find the object you are looking for.
Severity	Select the severity level for the event you want to display in the ENC. The choices and the severity level from low to high are Info , Warning , Minor , Major , and Critical .
Message	Type the information you wish to display for the event in the ENC. You can select variables from the drop-down list box to include in the message. The available variables are System Name , System OID , System Description and SNMP Varbinds . SNMP Varbinds - This is variable bindings. Each variable binding associates a particular MIB object's instance with its current value.
Action	Select the action profile to apply to this event. The ENC takes the action when it receives this event.
Clear Correlated Events	
Clear correlated events	Select this to have the ENC automatically acknowledge any selected correlated events.
Available Events	This field displays all available correlated events that you can select. Select one or more events (select while pressing [Ctrl]) and press the right arrow button (>) to add them into the selected list at the right field. Use the double right arrow button (>>) to add all available events to the right field.
Selected Correlate Events	This field displays the event(s) you selected to make a correlation with this event. Select one or more events (select while pressing [Ctrl]) and press the left arrow button (<) to remove them from this field. Use the double left arrow button (<<) to remove all events from this field.
Cancel	Click this to discard the changes and close this screen.
OK	Click this to save the changes and close this screen.

5.4 Event Action

This screen shows a list of configured event actions that the ENC takes when it receives associated events. To open this screen, click **Events** > **Event Action**.

Figure 90 Event Action



The following table describes the labels in this screen.

Table 47 Event Action

LABEL	DESCRIPTION
Add	Click this to create a new event action.
Edit	Select an entry from the table in this screen and click this to modify it.
Remove	Select one or multiple entries from the table and click this to remove them.
check box	Select the check box of an entry and click Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Name	This is the name of the event action.
Notes	This is more information about the event action.

5.4.1 Add/Edit Event Action

Use this screen to configure an event action. The actions include sending an e-mail, SMS, forwarding the received syslogs, or excuting a file on the ENC. To open this screen, click **Add** or **Edit** in the **Events > Event Action** screen.

Figure 91 Event Action > Add/Edit

Add Event Action

General

Event Action Name

Notes

Email Notification

Enable ☐

Mail To
(seperated by comma,')

Message Subject
Select Message Variables
Message of the alarm
Source of the alarm

Message Body
Select Message Variables
Message of the alarm
Source of the alarm
Category of the alarm
Severity of the alarm
Time when alarm was generated

HTTP-POST Notification

Enable ☐

Server URL

Post Data
Select Message Variables
Message of the alarm
Source of the alarm
Category of the alarm
Severity of the alarm
Time when alarm was generated

Syslog Forward

Enable ☐

Server URL

SNMP Trap

Enable ☐

Trap Destination

Destination Port

Community

Run System Command

Enable ☐

Command Name Example:
C:\WINDOWS\system32\cmd.exe

Command Attributes

Cancel Test Action OK

The following table describes the labels in this screen.

Table 48 Event Action > Add/Edit

LABEL	DESCRIPTION
General	
Event Action Name	Enter a descriptive name for the new event action profile. This field displays the profile name if you are modifying an existing profile.
Notes	Enter further information about the event action.
Email Notification	
Enable	Select this to have the EMS send an e-mail to the specified e-mail address when it receives the events. Clear this to disable it.
Mail To	Enter one or multiple valid e-mail addresses of the person who should receive matched events. Use a comma (,) to separate e-mail addresses.
Message Subject	This is the mail subject. You can include one or more variables by clicking them in the list box. The available variables are Message of the alarm and Source of the alarm .
Message Body	This is the mail content. You can include one or more variables by clicking them in the list box. The available variables are Message of the alarm , Source of the alarm , Category of the alarm , Severity of the alarm , Time when alarm was generated .
HTTP-POST Notification	
Enable	Select this to have the EMS send an HTTP POST request to a web server when it receives the events. Clear this to disable it. An HTTP POST request sends additional data to the web server. The additional data is specified after the URL.
Server URL	Enter the domain name or IP address of the web server to which the EMS will forward the matched events.
Post Data	Enter the additional data you wish to send to the web server.
Syslog Forward	
Enable	Select this to have the ENC forward devices' system logs to the specified IP address when it receives the events. Clear this to disable it.
Server URL	Enter the IP address or domain name of a host to which the ENC will forward devices' system logs.
SNMP Trap	
Enable	Select this to have the ENC send an SNMP trap to the specified IP address when it receives the event. Clear this to disable it.
Trap Destination	Enter the IP address of a host to which the ENC will send the SNMP trap.
Destination Port	Enter the port number the specified host uses to receive the SNMP traps sent by the ENC.
Community	Enter the SNMP Get/Set community string which is the password the ENC uses to communicate with the specified host.
Run System Command	
Enable	Select this to have the ENC execute a file when it receives the matched events. Clear this to disable it.
Command Name	Specify the full path of the file on the ENC that you want to execute. For example, C:\WINDOWS\system32\cmd.exe.
Command Attributes	Specify the attributes of the specified file if any. Otherwise, leave this field blank.
Cancel	Click this to discard the changes and close this screen.

Table 48 Event Action > Add/Edit (continued)

LABEL	DESCRIPTION
Test Action	Click this to perform the action(s) you have enabled and configured in this screen for a test.
OK	Click this to save the changes and close this screen.

The tool help to find devices, check device connectivity, group devices that have similar configurations, upload private MIBs to the ENC, monitor specific performance on devices, and manage device logs.

6.1 Device Discovery

Devices can be discovered automatically or manually.

6.1.1 Automatic

Automatic discovery lets you search devices or networks from the specified seeds that you configured. A seed is the IP address of a host in the ENC's network or a remote network. The ENC can learn other networks through a router's routing table if you configure the same SNMP community on both the ENC and the router. By clicking the **Discover** button in the **Tool > Auto-Discovery** screen, you can start an automatic discovery process. All devices automatically discovered are added to the networks to which they belong in the **OTV** panel.

You can perform automatic discovery through SNMP messages, and/or ping (ICMP). The **Auto-Discovery** screen also allows you to configure status and service polling to update the latest status of managed devices and the list of different services managed devices provide.

The ENC adds all subnets and then devices according to your seed/IP range settings. The ENC stops an auto-discovery process if it has reached the maximum number of devices it can supports according to the license the ENC is using.

The ENC uses the SNMP GET method to differentiate a device's type (**Host**, **Switch**, **Firewall**, **Wireless AP**, **Router/Gateway**, **Wireless Controller**, **IP PBX**, **IP Phone**, **Peripheral**, and **Others**). If the ENC does not receive a device's SNMP response (for example, when you configure a different SNMP community on the ENC) but the ENC receives a ping response from the device, the ENC will assign the device to the **Host** type. If the ENC receives the device's SNMP messages but fails to get the device's type, the ENC will assign the device to the **Others** type.

After using Auto-Discovery, the ENC uses devices' IP addresses as their display name in the ENC.

6.1.2 Manual

To manually add a device or network to your network, you must know what type of device it is and its IP address. Right-click the **Root Subnet** or a network in the **OTV** and then click **Add Network** or **Add Device**. See the Quick Start Guide for a configuration example.

6.1.3 Auto-Discovery

Use this screen to find devices in the ENC's network or a designated network segment or range of network segments.

To open this screen, click **Tool > Auto-Discovery**.

Figure 92 Tool > Auto-Discovery

General

☒ Enable Ping

☒ Enable resolve hostname / domain

Timeout: * 1~5 seconds

Retry: * 0~3 times

Discover Option:

Seeds

Discover Type:

Max. Hop Level: *

AddEditRemove

Seed	Net Mask
------	----------

SNMP

SNMP Version: ☐ v1 ☒ v2c ☐ v3

SNMP Port: *

Read Community: *

Polling

☒ Enable Status Polling

Polling Interval: minutes

☐ Enable auto-remove obsolete devices

Auto remove after offline period: * 1~30 days

Schedule

☐ Enable schedule discover

Schedule Type:

Time: :

Discovery Filters

AddEditRemove

Status	Property	Operation	Values
1	Device Type	equals	All

Save

Discover

The following table describes the labels in this screen.

Table 49 Tool > Auto-Discovery

LABEL	DESCRIPTION
General	
Enable Ping	Click this to enable ping from the ENC in order to find devices. You may also need to disable anti-probing on devices. Clear this to disable this feature.
Enable resolve hostname/domain	Click this to have the ENC automatically resolve device names from their IP addresses. Clear this to disable this feature.

Table 49 Tool > Auto-Discovery (continued)

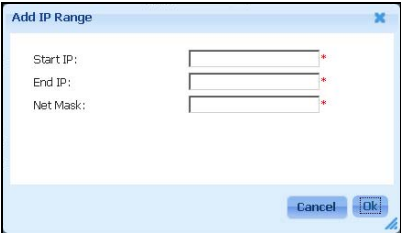
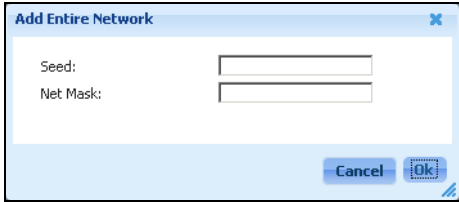
LABEL	DESCRIPTION
Timeout	Set the number of seconds (1–5) the ENC has to wait for a device's response, before the ENC polls the device again. If the device does not respond after the number of retries you set, then it is deemed to be down.
Retry	Set the number of times (0–3) the ENC resends a poll message to a device if the device does not respond. 0 means the ENC will not poll the device again if a response is not received the first time.
Discover Option	Select whether the ENC performs a scan afresh (Root subnet / Complete) or a scan for devices that have not been added to the OTV panel yet (Root subnet / Incremental).
Seeds	
Discover Type	<p>Select whether to scan devices on a basis of networks or IP addresses.</p> <p>Entire Network - Select this to scan devices in the ENC's network or a designated network(s) depending on the seed settings you will configure later.</p> <p>IP Range - Select this to scan devices in an IP address range.</p>
Max. Hop Level	This field is available if you selected Entire Network in the Discover Type field. Enter the number of gateways to across from the specified seed(s). 0 means to scan the network where the specified seed host is located.
Add	<p>Click this to add a seed for auto-discovery.</p> <p>If you selected IP Range in the Discover Type field, the following screen appears. Enter the starting and ending IP addresses for the ENC to find devices in this IP range. You have to also enter the subnet mask. You can use the subnet mask to specify an IP range across subnets. For example, an IP range starting from 172.17.1.1 to 172.17.2.254 with a subnet mask of 255.255.0.0. Click Ok to save the changes and close this screen or Cancel to exit this screen.</p> <p>Figure 93 Add IP Range</p>  <p>If you selected Entire Network in the Discover Type field, the following screen appears. Enter the IP address of a host and its subnet mask. The ENC will scan the device and the other devices in the same network. In addition, if the value in the Max. Hop Level field is not 0 and a router found in the network has other network information, the ENC will scan devices in the neighbor network(s). Click Ok to save the changes and close this screen or Cancel to exit this screen.</p> <p>Figure 94 Add Entire Network</p> 
Edit	Click this to modify a selected seed's settings.
Remove	Click this to delete a selected seed.
Seed	This field is available if you select Entire Network in the Discover Type field. This field displays the IP address of the seed.

Table 49 Tool > Auto-Discovery (continued)

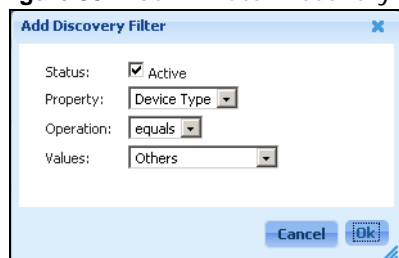
LABEL	DESCRIPTION
Net Mask	This field displays the subnet mask of the IP address(es).
Start IP	This field is available if you select IP Range in the Discover Type field. This field displays the starting IP address of the IP range.
End IP	This field is available if you select IP Range in the Discover Type field. This field displays the ending IP address of the IP range.
SNMP	
SNMP Version	Select the version of the SNMP poll messages the ENC sends in order to communicate with managed devices. You can select more than one check box if your devices support different SNMP versions.
SNMP Port	Enter the port number the ENC uses to transmit and receive SNMP messages to/from managed devices.
Read Community	Type the read-only community string the ENC uses to view information on managed devices.
User Name	This field is available if you selected v3 in the SNMP Version field. Enter the user name of the administrator account on the device.
Context Name	This field is available if you selected v3 in the SNMP Version field. Enter the context name configured in the device that you are looking for.
Authentication	This field is available if you selected v3 in the SNMP Version field. Select which hash algorithm (MD5 or SHA1) to use to authenticate SNMP packets transmitted between the ENC and the device. SHA1 is generally considered stronger than MD5 , but it is also slower. Select None if no authentication is required.
Auth. Password	This field is available if you selected MD5 or SHA1 in the Authentication field. Enter the authentication key, which depends on the authentication algorithm you selected. MD5 - a key 16-20 characters long SHA1 - a key 20 characters long You can use any alphanumeric characters or ; ` ~ ! @ # \$ % ^ & * () _ + \ { } ' : . / < > = - ". If you want to enter the key in hexadecimal, type "0x" at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; "0123456789ABCDEF" is in ASCII format.
Privacy	This field is available if you selected MD5 or SHA1 in the Authentication field. Select which encryption algorithm to use for SNMP packets transmitted between the ENC and the device. None - no encryption key or algorithm DES - a 56-bit key with the DES encryption algorithm AES - a 128-bit key with the AES encryption algorithm
Privacy Password	This field is available if you selected DES or AES in the Privacy field. Enter the encryption key with the length according to the Privacy setting.
Polling	
Enable Status Polling	Select this to have the ENC poll its managed devices periodically to update their status in the ENC. Clear this to disable it.
Polling Interval	Select how often in minutes the ENC sends a poll message to a managed device.
Enable auto-remove obsolete devices	Select this to allow a device to remain offline for the specified number of days before the ENC removes it from the OTV panel. You can configure the days in the Auto remove after offline period field. Clear this if you want to disable this feature.

Table 49 Tool > Auto-Discovery (continued)

LABEL	DESCRIPTION
Auto remove after offline period	Enter the number of days (1~30) a device is allowed to be offline before the ENC removes it from the OTV panel.
Schedule	
Enable schedule discover	Select this to have the ENC perform automatic discovery according to a schedule. Clear this to disable it.
Schedule Type	Select whether to perform automatic discovery daily or weekly.
Time	For a weekly schedule, select the week day, hour and second for the schedule. Otherwise, select the hour and second for a daily schedule.
Discovery Filters	Use this section to configure filter rules. The ENC only finds devices that match the criteria you set in the table. By default, the ENC finds all devices. You must delete this default rule if you want the ENC to only find devices that you specified in the table. See Section 2.6 on page 60 for a configuration example. Note: Make sure you have configured correct SNMP settings (versions and community) to use device type (see Table 51 on page 142 for all available device types) as the filters in this screen.
Add	Click this to add a filter rule. Note: Each rule is independent. The ENC finds devices according to the order of filter rules you configured.
Edit	Click this to modify a selected filter rule.
Remove	Click this to delete a selected filter rule.
	The first column displays the index number of each entry in the table. This number is also the order the ENC uses to find devices.
Status	This field displays whether the rule is activated or not.
Property	This field displays the parameter's name this rule is based on.
Operation	This field displays the comparison operator of the criteria for the rule; equals , contains , starts with or ends with .
Values	This field displays the value of the criteria for the rule.
Save	Click this to save the settings.
Discover/Stop	Click Discover to begin scanning. Click Stop to halt the current scanning process. Note: It will take a while to stop the process.

6.1.3.1 Adding a Discovery Filter

Use this screen to create a rule that the ENC can use to find matching devices. To open the screen, click **Add** in the **Discovery Filters** section of the **Tool > Auto-Discovery** screen.

Figure 95 Tool > Auto-Discovery > Add Discovery Filter

The following table describes the labels in this screen.

Table 50 Tool > Auto-Discovery > Add Discovery Filter

LABEL	DESCRIPTION
Status	Select Active to enable this filter rule or clear this to disable it.
Property	Select the parameter of this rule. The available options are Device Type , Model Name , Host Name , IP Address and sysOid . sysOid means the SNMP object identifier of a MIB object. Note: Make sure you have configured correct SNMP settings (versions and community) to use device type (see Table 51 on page 142 for all available device types) as the filters.
Operator	Select the comparison operator for the rule. The available options vary depending on the Property you selected. They are equals , contains , starts with or ends with .
Values	Select or enter the corresponding value according to the Property you selected.
Cancel	Click Cancel to close this screen without saving the settings.
Ok	Click Ok to save the settings.

6.2 Inventory of Devices

Use this screen to look for devices in the **OTV** panel and their information such as IP address, current status, firmware version, and so on.

To open this screen, click **Tool > Inventory**. Input the search criteria and click **Search**.

Figure 96 Tool > Inventory > Device

Search filters:

- Name:
- IP Address:
- Firmware:
- Device Group:
- Discovered Date:
- Device Type:
- Status:
- Device Model:
- Enable Status Polling:
- Support SNMP:

Buttons: View Events, Remove, Activate Status Polling, Deactivate Status Polling, Customize Columns, PDF, CSV

	Status	Name	IP Address	Device Model	Last Update	Device Type	Firmware Version	Details
1	<input type="checkbox"/>	DIVINE-PC	172.23.41.6		2011-01-26 15:12:12	Host		
2	<input type="checkbox"/>	10.50.1.254	10.50.1.254		2011-01-25 18:27:36	Host		
3	<input type="checkbox"/>	10.50.1.2	10.50.1.2		2011-01-25 18:27:36	Host		
4	<input type="checkbox"/>	172.23.41.221	172.23.41.221	ZyWALL USG 2000	2011-01-25 18:27:31	Firewall		
5	<input type="checkbox"/>	172.23.41.254	172.23.41.254		2011-01-25 18:27:30	Host		
6	<input type="checkbox"/>	172.23.41.226	172.23.41.226	ZyWALL USG 2000	2011-01-25 18:27:30	Firewall		
25	<input type="checkbox"/>	172.23.40.41	172.23.40.41	NWA1300-NJ	2011-01-24 13:48:11	NWA1300-N Series	v1.00(UJF.0)b01_alpha5	

Page 1 of 1 | View 1 - 25 of 25

Figure 97 Tool > Inventory > Device (NWA1300-N Series)

Search filters:

- Name:
- IP Address:
- Firmware:
- Device Group:
- Discovered Date:
- Device Type:
- Status:
- Device Model:
- Enable Status Polling:
- Support SNMP:

Buttons: View Events, Remove, Activate Status Polling, Deactivate Status Polling, Customize Columns, PDF, CSV

	Status	Name	IP Address	Device Model	MAC Address	SSID	Channel	Profile Name	Transmit Power
1	<input type="checkbox"/>	192.168.1.4	192.168.1.4	NWA1300-NJ	00A0C5000104				
2	<input type="checkbox"/>	192.168.1.5	192.168.1.5	NWA1300-NJ	00A0C5000105				
3	<input type="checkbox"/>	192.168.1.3	192.168.1.3	NWA1300-NJ	00A0C5000103				
4	<input type="checkbox"/>	192.168.1.2	192.168.1.2	NWA1300-NJ	00A0C5000102				
5	<input type="checkbox"/>	Room A104		NWA1300-NJ	00A0C5000104				

Page 1 of 1 | View 1 - 5 of 5

The following table describes the labels in this screen.

Table 51 Tool > Inventory > Device

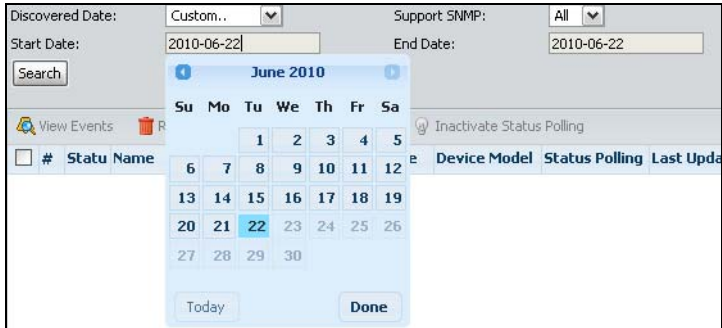
LABEL	DESCRIPTION
Name	Enter a partial or full name of a device for which to search.
Device Type	<p>Select the type of the device for the search criteria. The available options are Host, Switch, Firewall, Wireless AP, Router/Gateway, Wireless Controller, IP PBX, IP Phone, Peripheral, NWA1300-N Series, Others and All.</p> <p>Host: such as a computer or a device that does not respond to the ENC through SNMP but the ENC can ping to it.</p> <p>Others: these are devices that support SNMP but for which the ENC cannot find a matching device type in its database or the ENC fails to get the device's type. For example, a non-ZyXEL switch.</p> <p>Peripheral: such as a printer or digital photo frame. This type of device must be manually added to the ENC.</p> <p>Wireless Controller: such as ZyXEL NXC-8160. At the time of writing, the ENC does not support the device.</p>
IP Address	Enter a partial or full IP address for the search criteria. This field does not support asterisks as wildcards. Leave this field blank to not specify the criteria.
Status	Select the device status (Online , Offline , Un-monitored or All) for the search criteria.
Firmware	Enter a partial or full firmware version of the device for the search criteria. Leave this field blank to not specify the criteria.
Device Model	Select the device model name for the search criteria.
Device Group	Select a device group (configured in the Tool > Device Group screen) or All device groups for the search criteria.
Enable Status Polling	Select whether status polling is enabled (true) or not (false) or both (All) for the search criteria.
Discovered Date	<p>Select within the number of hours or days in the past the device was discovered by the ENC for the search criteria. The options are Last 24 hours, Last 48 hours, Last 5 days, Last 7 days and Last 30 days. Select All to not specify the criteria. Select Custom to display additional fields if you want to customize a period for the search criteria. Click the text box next to Start Date or End Date, a calendar displays as shown next.</p> <p>Figure 98 Customize a Period</p>  <p>Choose a date (or click Today) and click Done to close the calendar. The ending date must not be earlier than the starting date.</p>
Support SNMP	Select whether the device enables SNMP (Yes or No) or both (All) for the search criteria.
Search	Click this to perform the search.
View Events	Select one or multiple table entries and click this to view the events about the devices. See Section 5.1 on page 123 for more information.
Remove	Select one or multiple table entries and click this to delete them.

Table 51 Tool > Inventory > Device (continued)

LABEL	DESCRIPTION
Activate Status Polling	Select one or multiple table entries and click this to have the ENC poll the device status periodically and update it in this screen.
Deactivate Status Polling	Select one or multiple table entries and click this to have the ENC stop polling the devices status periodically.
Customize Columns	Select this to customize the table columns that you want to display in this table.
PDF	Click this to export the search device list to a PDF file on the computer you are using to access the ENC.
CSV	Click this to export the search device list to a CSV file on the computer you are using to access the ENC.
check box	Select the check box of an entry and click View Events , Remove , Activate Status Polling or Inactivate Status Polling to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Status	This field displays whether the device is Online , Offline , Un-register or Un-monitored .
Name	This field displays the name of the device. Click the name to view the device's detailed settings and information.
IP Address	This field displays the IP address of the device.
Device Type	This field displays the type of the device.
Device Model	This field displays the model name of the device.
Firmware Version	This field displays the firmware version the device is currently using.
Last Update	This field displays the date and time this entry's information was last updated.
Details	This field displays icon(s) that represent additional information for the device. Refer to Section 1.3.6 on page 43 for icon descriptions.
MAC Address	This field displays the MAC address of the device.
SSID	This field displays the SSID the device uses for wireless client association.
Channel	This field displays the operating frequency the device uses for the wireless network.
Profile Name	This field displays the name of the wireless AP profile with which the device was applied.
Transmit Power	This field displays the transmitting power (in percentage) device uses for transmitting and receiving wireless data.

6.2.1 Inventory Device Details - System

Use this screen to configure a device's general settings and view its system information. The settings are stored on the ENC and might be different than the settings on the device. Clicking **Apply** will save the changes on the ENC.

To open this screen, click a device in the **Name** field in the **Tool > Inventory > Device** screen.

Figure 99 Tool > Inventory > Device Details > System

The screenshot shows the 'System' tab of the 'Device Details' screen. It is divided into two main sections: 'General' and 'System Info'. The 'General' section contains fields for 'Display Name', 'Device Type', 'Device Model', 'IP Address', 'Login Username', 'Login Password', and 'Note'. The 'System Info' section contains fields for 'Description', 'UpTime', 'Name', 'Service', 'Default Tcp Ports', 'Customized Tcp Ports', 'ObjectID', 'Contact', and 'Location'. At the bottom, there are 'Apply' and 'Back' buttons.

The following table describes the labels in this screen.

Table 52 Tool > Inventory > Device > System

LABEL	DESCRIPTION
General	
Display Name	This field displays the descriptive name of the device. Enter a new name (up to 32 printable character; spaces are not allowed) if you want to modify it.
Status	This field displays whether the device is reachable (Online), not reachable (Offline) or temporarily not managed by the ENC (Un-monitored).
Device Type	This field displays the type of the device. Select a more appropriate one if necessary.
Discovered Date	This field displays the date and time this device was discovered and added to the ENC.
Device Model	This field displays the model name of the device. Select a more appropriate one if necessary.
Last Update	This field displays the date and time the device's information in this screen was last updated.
IP Address	This field displays the IP address of the device. Enter another IP address if you want to change it without re-scanning the device using auto-discovery. Then the ENC will use the updated IP address to communicate with the device. Note: Changing the IP address here will not change the device's IP address.
Firmware Version	This field displays the firmware version the device is using.
MAC Address	This field displays the MAC address of the device. Enter a new MAC address if you want to change it.
Mapped Room No.	This field is available if you selected NWA1300-N Series in the Device Type field. This field displays the number of the hotel room where the device is located especially for the hotel management application. Enter a new room number if you want to change it.
Login Username	This field displays the user name of an administrator account on the device.
Login Password	This field displays the password of the administrator account, which is displayed using several stars (*) in order to prevent the password from being exposed.
Note	This field displays additional information about the device.

Table 52 Tool > Inventory > Device > System (continued)

LABEL	DESCRIPTION
System Info	<p>This section displays the device's information the ENC retrieves from the device.</p> <p>Note: This section displays the selected device's information only when the device supports SNMP and it is reachable from the ENC (the device's icon color is green).</p>
Description	This field displays descriptive information about the device.
ObjectID	This field displays the MIB object identifier of sysObjectID for this device. The ENC uses this ID to get the device's name that comes with the device when it is produced.
Up Time	This field displays how long the device has been available since the last time it started or restarted.
Contact	This field displays e-mail address(es) to contact if this device has a problem.
Name	This field displays the changeable system name of the device.
Location	This field displays the device location that you configured when you added this device to the ENC.
Service	This field displays MIB object identifier of sysServices for this device. The ENC uses this ID to differentiate what services the device provides.
Apply	Click this to save the changes.
Default Tcp Ports	<p>This field displays the number of each default service port the device allows to access, detected by the ENC. The default service ports include 80 for web, 21 for FTP, 23 for Telnet, and 25 for SMTP services.</p> <p>To view the information, you have to enable TCP port scanning and select default service(s) you want to scan for the device in the Tool > Inventory > Device > Access screen.</p>
Customized Tcp Ports	<p>This field displays the number of each customized service port the device allows to access, detected by the ENC.</p> <p>To view the information, you have to enable TCP port scanning and configure TCP port(s) you want to scan for the device in the Tool > Inventory > Device > Access screen.</p>
Back	Click this to exit this screen and go back to the previous screen.

6.2.2 Inventory Device Details - Access

Use this screen to configure the default SNMP and polling settings used by the ENC to communicate with the device. The settings are stored on the ENC and might be different from the settings on the device.

To open this screen, click a device in the **Name** field in the **Tool > Inventory > Device** screen, then click the **Access** tab.

Figure 100 Tool > Inventory > Device > Access

The following table describes the labels in this screen.

Table 53 Tool > Inventory > Device > Access

LABEL	DESCRIPTION
SNMP	
SNMP Version	Select the version of the SNMP poll messages the ENC sends in order to communicate with the device.
Port	Enter the port number the ENC uses to transmit and receive SNMP messages to/from the device.
Read Community	Type the read-only community string the ENC uses to view information or settings on the device.
Write Community	Type the write community string the ENC uses to change settings on the device.
User Name	Enter the user name of the administrator account on the device.
Context Name	Enter the context name configured on the device. This setting should be the same on both the ENC and device in order to communicate with each other.
Authentication	Select which hash algorithm (None , MD5 or SHA1) to use to authenticate SNMP packets transmitted between the ENC and the device. SHA1 is generally considered stronger than MD5 , but it is also slower.
Auth. Password	<p>This field is available if you selected MD5 or SHA1 in the Authentication field.</p> <p>Enter the authentication key, which depends on the authentication algorithm you selected.</p> <p>MD5 - a key 16-20 characters long</p> <p>SHA1 - a key 20 characters long</p> <p>You can use any alphanumeric characters or ; ` ~ ! @ # \$ % ^ & * () _ + \ { } ' : . / < > = - . If you want to enter the key in hexadecimal, type "0x" at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in "0123456789ABCDEF" is in ASCII format.</p>

Table 53 Tool > Inventory > Device > Access (continued)

LABEL	DESCRIPTION
Privacy	<p>This field is available if you selected MD5 or SHA1 in the Authentication field.</p> <p>Select which encryption algorithm to use for SNMP packets transmitted between the ENC and the device.</p> <p>None - no encryption key or algorithm</p> <p>DES - a 56-bit key with the DES encryption algorithm</p> <p>AES - a 128-bit key with the AES encryption algorithm</p>
Privacy Password	<p>This field is available if you selected DES or AES in the Privacy field.</p> <p>Enter the encryption key with the length according to the Privacy setting.</p>
Polling	
Enable Status Polling	Select this to have the ENC poll its managed devices periodically to update their status in the ENC. Clear this to disable it.
Polling Method	Select which method (SNMP , Ping) the ENC uses to poll the device's status.
Polling Interval	Select how often the ENC sends a poll message to the device.
Status Variable	<p>You can use this and the following two Status fields to customize a threshold the ENC uses to determine whether the device is running normally or not. Type the MIB object ID of the variable for the criteria. This is an example for the threshold.</p> <p>"1.3.6.1.4.1.890.1.6.1.1.1.0 (sysCPUUsage) < 98" means the device is running normally when the CPU usage is less than 98%. If the CPU usage goes to 98% or above, the device is overloaded.</p> <p>You can also click the magnifier icon and find the object to have the ENC automatically display the object ID in this field.</p>
Status OK Exp	Select the comparison expression for the threshold. The available options are greater than (>), equal to (=), and less than (<).
Status OK Value	Enter the value for the threshold. If the variable's value stays within the set threshold, the device is online to the ENC. Otherwise, the ENC changes the device's status to offline.
TCP Port Scan	
Enable TCP Port Scan	Select this to enable TCP port scan for the device, if you want to track whether a service is available for access.
Web: 80	Select this to have the ENC detect whether web service is available on the device.
FTP: 21	Select this to have the ENC detect whether FTP service is available on the device.
Telnet: 23	Select this to have the ENC detect whether Telnet service is available on the device.
SMTP: 25	Select this to have the ENC detect whether mail service (SMTP) is available on the device.
#1 ~ #4	Select this and configure the service's name and port number to have the ENC detect whether the service is available on the device.
Apply	Click this to save the changes.
Back	Click this to exit this screen and go back to the previous screen.

6.2.3 Inventory Device Details - Interface

Use this screen to view the current port information of the selected device.

To open this screen, click a device in the **Name** field in the **Tool > Inventory > Device** screen, then click the **Interface** tab.

Figure 101 Tool > Inventory > Device > Interface

The screenshot displays the 'Interface' tab with three data tables for host 172.17.17.118. Each table includes a 'Refresh' icon and a 'Back' button at the bottom.

Interface Info Table

Index	Description	Type	Mtu	Speed	PhysAddress
1	swp00	ethernetCsmacd	1500	0	0x00:13:49:00:00:F1
2	swp01	ethernetCsmacd	1500	100000000	0x00:13:49:00:00:F1
3	swp02	ethernetCsmacd	1500	0	0x00:13:49:00:00:F1
4	swp03	ethernetCsmacd	1500	0	0x00:13:49:00:00:F1

Interface Usage Table

Index	Description	InBPS	OutBPS	TotalBPS
1	swp00	0	0	0
2	swp01	116824	111648	228472
3	swp02	0	0	0
4	swp03	0	0	0

Interface Utilization Table

Index	Description	InUtil	OutUtil	TotalUtil	ErrorsPercent
1	swp00	0.0	0.0	0.0	0.0
2	swp01	0.117	0.112	0.229	0.0
3	swp02	0.0	0.0	0.0	0.0
4	swp03	0.0	0.0	0.0	0.0

The following table describes the labels in this screen.

Table 54 Tool > Inventory > Device > Interface

LABEL	DESCRIPTION
Interface Info/Usage/Utilization Table on host ...	
The line displays the Display Name of the device for which these corresponding information and statistics are generated. These tables display basic port information and incoming/outgoing traffic statistics.	
Refresh	Click this in each table to update the table information respectively.
Index	This field displays the index number of an entry in each table.
Description	This field displays the name of a port or an interface on the device. swp means a switch port.
Type	This field displays the type of the port or interface. See ifType in RFC1213 for more information.
Mtu	This field displays the Maximum Transmission Unit (MTU) which is the maximum size (in bytes) of a packet the port is allowed to receive and transmit.

Table 54 Tool > Inventory > Device > Interface (continued)

LABEL	DESCRIPTION
Speed	This field displays the speed (in bytes) of the Ethernet connection on this port.
PhysAddress	This field displays the MAC address of this port.
InBPS	This field displays the packet receiving rate (in bits per second) on this port.
OutBPS	This field displays the packet transmission rate (in bits per second) on this port.
TotalBPS	This field displays the total packet receiving and transmission rate (in bits per second) on this port.
InUtil	This field displays the bandwidth utilization (as a percentage) of incoming packets received on this port.
OutUtil	This field displays the bandwidth utilization (as a percentage) of outgoing packets transmitted on this port.
ErrorsPercent	This field displays the bandwidth utilization (as a percentage) of errors received on this port.
Back	Click this to exit this screen and go back to the Tool > Inventory > Device screen.

6.2.4 Inventory Device Details - Routing

Use this screen to view the current routing information on the device. The device uses static routes to send data and respond to remote devices that are not reachable through the default gateway. For example when sending SNMP traps or using ping to test IP connectivity.

To open this screen, click a device in the **Name** field in the **Tool > Inventory > Device** screen, then click the **Routing** tab.

Figure 102 Tool > Inventory > Device > Routing

Dest	Index	Metric1	Metric2	Metric3	Metric4	NextHop	Type	Proto	Age	Mask	Metric5	Info
1 0.0.0.0	1	1	-1	-1	-1	172.23.2.6.254	invalid	local	0	0.0.0.0	-1	0.0
2 127.0.0.0	1	1	-1	-1	-1	127.0.0.1	direct	local	0	255.255.0.0	-1	0.0
3 172.23.2.6.0	1	1	-1	-1	-1	172.23.2.6.106	direct	local	0	255.255.255.0	-1	0.0

The following table describes the labels in this screen.

Table 55 Tool > Inventory > Device > Routing

LABEL	DESCRIPTION
Refresh	Click this to update the information in the table below.
Dest	This field displays the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Index	This field displays the index number of the route. Click a number to edit the static route entry.

Table 55 Tool > Inventory > Device > Routing (continued)

LABEL	DESCRIPTION
Metric1	This field displays the primary routing metric which indicates the cost of transmission for routing purposes. IP routing uses hop count as the measurement of cost, 1 displays if the final destination is a direct-connected network or device. -1 displays if this metric is not used.
Metric2~4	These fields display the alternative routing metrics for the route. -1 displays if this metric is not used.
NextHop	This field displays the IP address of the gateway. The gateway is an immediate neighbor of the device, that will forward the packets to the destination.
Type	This field displays the type of route the device supports. See ipRouteType in RFC1213 for more information.
Proto	This field displays local if the route is added to the table manually. Otherwise, the field displays a particular routing protocol via which this route was learned.
Age	This field displays the remaining time (in seconds) before the route is removed from this table (for dynamic routes). 0 means the route does not age out (for static routes).
Mask	This field displays the subnet mask for this destination.
Metric5	This field displays the alternative routing metric for the route. -1 displays if this metric is not used.
Info	This field displays additional information for the routing protocol shown in the Proto field above. 0.0 means no additional information.
Back	Click this to exit this screen and go back to the Tool > Inventory > Device screen.

6.2.5 Inventory Device Details - ARP

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. Use this screen to view current IP-to-MAC address mapping(s) on the device.

To open this screen, click a device in the **Name** field in the **Tool > Inventory > Device** screen, then click the **ARP** tab.

Figure 103 Tool > Inventory > Device > ARP

Device		Network	
System		Access	Interface
Routing		ARP	Port Analyzer
MAC Table			

ARP Table

ARP Table on host 172.23.26.106

Refresh

Index	IP Address	MAC Address	Type
1 1	172.23.26.254	00:04:80:9B:78:00	dynamic
2 1	172.23.26.255	FF:FF:FF:FF:FF:FF	static
3 1	192.168.1.255	FF:FF:FF:FF:FF:FF	static

Back

The following table describes the labels in this screen.

Table 56 Tool > Inventory > Device > ARP

LABEL	DESCRIPTION
Refresh	Click this to update the information in the table below.
Index	This field displays the index number of a port or an interface on the device, via which the device can access the host shown in the NetAddress field of this entry.
IP Address	This is the IP address of a device connected to a port on the device.
MAC Address	This is the MAC address of the device.
Type	This shows whether the MAC address is dynamic (learned by the device) or static (manually configured on the device).
Back	Click this to exit this screen and go back to the Tool > Inventory > Device screen.

6.2.6 Inventory Device Details - Port Analyzer

Use this screen to view which TCP and UDP ports are currently in use on the selected device.

To open this screen, click a device in the **Name** field in the **Tool > Inventory > Device** screen, then click the **Port Analyzer** tab.

Figure 104 Tool > Inventory > Device > Port Analyzer

Device

Network

System

Access

Interface

Routing

ARP

Port Analyzer

MAC Table

TCP Port Table

TCP Port Table on host 172.23.26.106

Refresh

	LocalAddress	LocalPort	RemoteAddress	RemotePort	State
1	0.0.0.0	21	0.0.0.0	0	listen
2	0.0.0.0	22	0.0.0.0	0	listen
3	0.0.0.0	23	0.0.0.0	0	listen
4	0.0.0.0	80	0.0.0.0	0	listen

UDP Port Table

UDP Port Table on host 172.23.26.106

Refresh

	Address	Port
1	0.0.0.0	53
2	0.0.0.0	67
3	0.0.0.0	68
4	0.0.0.0	69

Back

The following table describes the labels in this screen.

Table 57 Tool > Inventory > Device > Port Analyzer

LABEL	DESCRIPTION
Refresh	Click this to update the information in each table respectively.
LocalAddress	This field displays the IP address of the device.
LocalPort	This field displays the number of a TCP port on the device, which is in use.

Table 57 Tool > Inventory > Device > Port Analyzer (continued)

LABEL	DESCRIPTION
RemoteAddress	This field displays the IP address of a remote device which is trying to connect or has connected to the device. 0.0.0.0 displays if no remote device is accessing the port on the local device.
RemotePort	This field displays the number of a port on the remote device, which is used to communicate with the local device for the service. 0 displays if no remote device is accessing the port on the local device.
State	This field displays the connection status between the local and remote ports. listen displays if the local port is listening to a connection request. established displays if the connection has been successfully established.
Address	This field displays the IP address of the device.
Port	This field displays the number of a UDP port the device uses to send UDP packets.
Back	Click this to exit this screen and go back to the previous screen (Tool > Inventory > Device).

6.2.7 Inventory Device Details - MAC Table

Use this screen to view all the MAC table entries on the selected device.

To open this screen, click a device in the **Name** field in the **Tool > Inventory > Device** screen, then click the **MAC Table** tab.

Figure 105 Tool > Inventory > Device > MAC Table

Port	MAC Address	Status
1 24	00:00:AA:04:56:5A	learned(3)
2 24	00:00:1D:79:08:63	learned(3)
3 24	00:04:80:98:04:00	learned(3)
4 24	00:08:02:1D:1D:67	learned(3)
5 24	00:0C:29:04:83:64	learned(3)

The following table describes the labels in this screen.

Table 58 Tool > Inventory > Device > MAC Table

LABEL	DESCRIPTION
MAC Table on host	This field displays the selected device's IP address.
Port	Enter a port number here if you want to search any MAC address entries to which the port is connected.
MAC Address	Enter a MAC address here if you want to search the specified MAC address entry.
Status	Select a status from the drop-down list (All, other, invalid, learned, self, or mgmt) for a search criteria.

Table 58 Tool > Inventory > Device > MAC Table (continued)

LABEL	DESCRIPTION
Search	Click this button to search the matched entries from the selected device's MAC table.
Refresh	Click this to update the MAC table.
Port	This field displays the number of a port the MAC entry is related.
MAC Address	This field displays a MAC address which indicates you can access the host through the port.
Status	This field displays how this MAC entry was added.

6.2.8 Inventory Device Details - Wireless

Use this screen to view the wireless settings of the selected device which supports the wireless AP feature.

To open this screen, click a wireless AP in the **Name** field of the **Tool > Inventory > Device** screen, then click the **Wireless** tab.

Note: At the time of writing, this feature is only available for NWA1300-N Series.

Note: You may see **N/A** on this screen, if the wireless function is disabled on the device.

Figure 106 Tool > Inventory > Device > Wireless

Device	System	Access	Interface	Routing	ARP	Port Analyzer	MAC Table	Wireless
Wireless Setting								
SSID:	N/A	802.11 Mode:	N/A					
Channel:	N/A	Transmit Power:	N/A					

The following table describes the labels in this screen.

Table 59 Tool > Inventory > Device > Wireless

LABEL	DESCRIPTION
SSID	This field displays the wireless SSID the selected device is using.
802.11 Mode	This field displays which wireless mode (such as 802.11 a/b/g/n) the selected device is using.
Channel	This field displays which operating frequency/channel the selected device is using.
Transmit Power	This field displays the transmission power the selected device is using for transmitting data wirelessly.

6.3 Inventory of Networks

Use this screen to look for networks in the **OTV** panel and their information such as the network IP address, current status, type, etc.

To open this screen, click a device in the **Name** field in the **Tool > Inventory > Network** screen.

Figure 107 Tool > Inventory > Network

	Status	Name	IP Address	Type	Last Update
1	<input type="checkbox"/>	172.23.11.0	172.23.11.0	General	2010-09-13 12:48:13
2	<input type="checkbox"/>	172.23.7.0	172.23.7.0	General	2010-09-03 17:24:20
3	<input type="checkbox"/>	172.23.10.0	172.23.10.0	General	2010-09-02 09:54:21
4	<input type="checkbox"/>	172.23.45.0	172.23.45.0	General	2010-09-01 08:27:20
5	<input type="checkbox"/>	172.23.24.0	172.23.24.0	General	2010-08-26 13:45:24
6	<input type="checkbox"/>	172.23.15.0	172.23.15.0	General	2010-08-26 13:45:24
7	<input type="checkbox"/>	172.23.6.0	172.23.6.0	General	2010-08-26 13:42:26
8	<input type="checkbox"/>	172.23.3.0	172.23.3.0	General	2010-08-26 13:42:26
9	<input type="checkbox"/>	172.23.1.0	172.23.1.0	General	2010-08-26 13:42:26
10	<input type="checkbox"/>	172.23.2.0	172.23.2.0	General	2010-08-26 13:42:26

The following table describes the labels in this screen.

Table 60 Tool > Inventory > Network

LABEL	DESCRIPTION
Name	Enter a partial or full name of a network for the search criteria.
Type	Select the type of the network for the search criteria. The options are All , General , Bus , Star , Ring , Tree . All means any.
IP Address	Enter a partial or full IP address of a network for the search criteria. You cannot use an asterisk as a wildcard or a hyphen to search an IP range.
Status	Select the device status in the network that you want to find. Online - all managed devices in the network are reachable. Partial Online - some of the managed devices in the network are not reachable. Offline - all managed devices in the network are not reachable. Un-monitored - no device is found in the network. This might be caused by a NAT device that exists between the network and the ENC. All - select this to include all the status above for the criteria.
Search	Click this to perform the search.
View Events	Select one or multiple table entries and click this to view the events about the networks. See Section 5.1 on page 123 for more information.
Remove	Select one or multiple table entries and click this to delete them.
check box	Select the check box of an entry and click View Events or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.

Table 60 Tool > Inventory > Network (continued)

LABEL	DESCRIPTION
Status	<p>This field displays whether the ENC can detect the devices in the network.</p> <p>Online - all managed devices in the network are reachable.</p> <p>Partial Online - some of the managed devices in the network are not reachable.</p> <p>Offline - all managed devices in the network are not reachable.</p> <p>Un-monitored - no device is found in the network. This might be caused by a NAT device that exists between the network and the ENC.</p>
Name	Click the name to view the network's detailed settings and information.
IP Address	This field displays the IP address of the network.
Type	This field displays the type of the network.
Last Update	This field displays the date and time this entry's information was last updated.

6.3.1 Inventory Network Details

Use this screen to view the device information. You can also change the device name and/or device type for display in the ENC.

To open this screen, click a device in the **Tool > Inventory > Network** screen.

Figure 108 Tool > Inventory > Network Details

The following table describes the labels in this screen.

Table 61 Tool > Inventory > Network Details

LABEL	DESCRIPTION
Display Name	This field displays the descriptive name of the network. Enter a new name (up to 32 printable character; spaces are not allowed) if you want to modify it.
Status	<p>This field displays whether the ENC can detect the devices in the network.</p> <p>Online - all managed devices in the network are reachable.</p> <p>Partial Online - some of the managed devices in the network are not reachable.</p> <p>Offline - all managed devices in the network are not reachable.</p> <p>Un-monitored - no device is found in the network. This might be caused by a NAT device that exists between the network and the ENC.</p>
IP Address	This field displays the IP address of the network.
Network Mask	This field displays the subnet mask of the network.
Discovered Member	This field displays the number of devices that the ENC has discovered on the network.

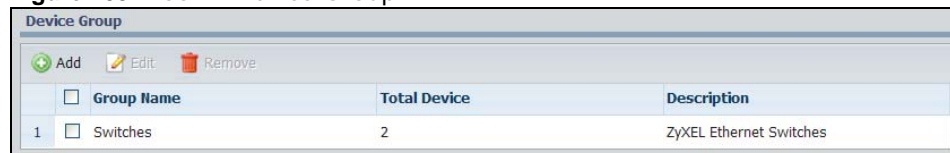
Table 61 Tool > Inventory > Network Details (continued)

LABEL	DESCRIPTION
Discovered Date	This field displays the date and time this network was discovered and added to the ENC.
Type	This field displays the type of the network (General , Bus , Star , Ring or Tree . Select an appropriate one if you want to change it.
Last Update	This field displays the date and time the device's information in this screen was last updated.
Apply	Click this to save the changes.
Back	Click this to exit this screen and go back to the previous screen.

6.4 Device Group

Use this screen to logically group managed devices that can be configured together. You may distribute a script to a group of devices, for example.

To open this screen, click **Tool > Device Group**.

Figure 109 Tool > Device Group

The following table describes the labels in this screen.

Table 62 Tool > Device Group

LABEL	DESCRIPTION
Add	Click this to create a device group.
Edit	Click this to modify a selected device group.
Remove	Click this to remove selected device group(s).
check box	Select the check box of an entry and click Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Group Name	This field displays the descriptive name of the group. Select one or more device(s) and click Remove if you want to remove them.
Total Device	This field displays the number of devices associated with the group.
Description	This field displays additional information of the group.

6.5 Device Group Add/Edit

Use this screen to configure a device group.

To open this screen, click **Add** or **Edit** in the **Tool > Device Group** screen.

Figure 110 Tool > Device Group Add/Edit

Device List			
	Device Name	Device Model	Device IP
1	172.23.5.69		172.23.5.69
2	172.23.5.67		172.23.5.67

The following table describes the labels in this screen.

Table 63 Tool > Device Group Add/Edit

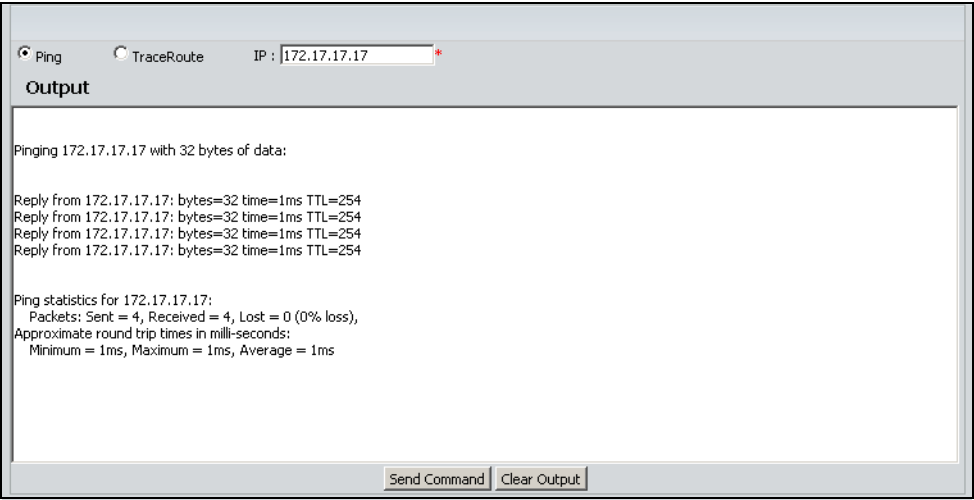
LABEL	DESCRIPTION
Group Name	Type up to 20 alphanumeric characters (0-9, a-z, A-Z), underscores (_), and/or hyphens (-) for the name of the group. Spaces are not allowed.
Description	Type up to 80 printable characters for additional information about this group.
Add	Click this to add device(s) to this group.
Device Name	This field displays the name of the device being associated with this group.
Device Model	This field displays the model name of the device.
Device IP	This field displays the address of the device.

6.6 PING/Trace Route

Use this screen to test the connection from the device to a specified IP address. The **Ping** function only tests whether the specified device responds. The **Trace Route** function additionally tests how

a packet is transmitted and routed through devices between the ENC and the device. To open this screen, click **Tool > PING/Trace Route**.

Figure 111 Tool > PING/Trace Route



The following table describes the labels in this screen.

Table 64 Tool > PING/Trace Route

LABEL	DESCRIPTION
Ping	Select this and enter the IP address of a device (in the IP field) to which you want to test the connection from the ENC. Enter the IP address of the device to which you want to send a traceroute packet from the the ENC.
TraceRoute	Select this and enter the IP address of a device (in the IP field) to which you want to test the connection from the ENC.
IP	Enter a valid IP address.
Send Command	Click this to begin the ping or traceroute connection test.
Clear output	Click this to clear the output content from your last test.

6.7 MIB Loader

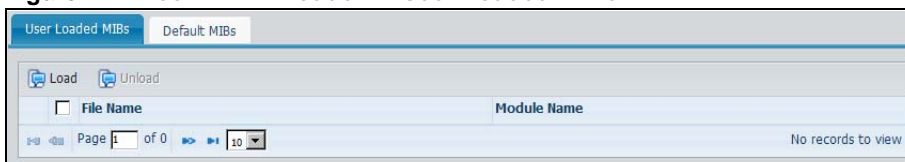
By default, the ENC stores some standard Management Information Bases (MIBs) and specific ZyXEL devices' MIBs (listed in the **Tool > MIB Loader > Default MIBs** screen). The ENC allows you to upload your private MIBs if you cannot find them in the **Default MIBs** screen through the **Tool > MIB Loader > User Loaded MIBs** screen.

6.7.1 User Loaded MIBs

You may need to upload a device's private MIBs to the ENC if you want the ENC to support a specific function for your device. Use this screen to upload a MIB file to the ENC.

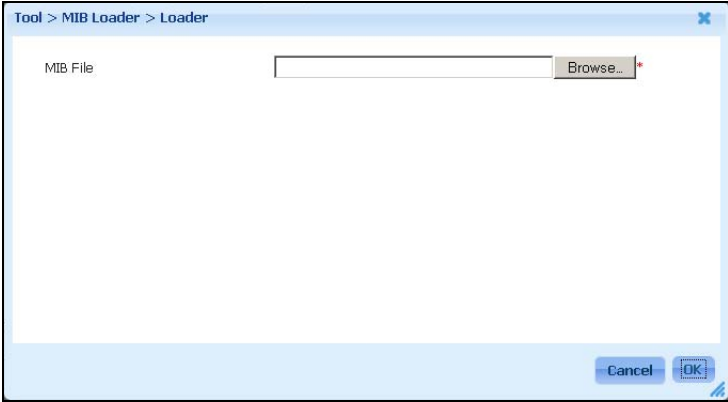
To open this screen, click **Tool > MIB Loader > User Loaded MIBs**.

Figure 112 Tool > MIB Loader > User Loaded MIBs



The following table describes the labels in this screen.

Table 65 Tool > MIB Loader > User Loaded MIBs

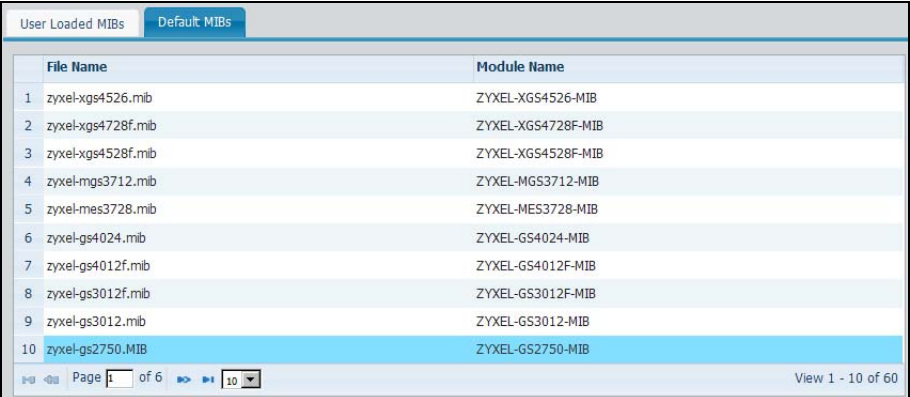
LABEL	DESCRIPTION
Load	<p>Click this to upload a MIB file. The following screen appears.</p> <p>Figure 113 MIB Loader</p>  <p>You have to download the MIB file you want to upload to the computer that you are using to access the ENC first. Then specify the full path of the MIB file (for example, c:\Download\example.mib) in the MIB File field or click Browse to locate the file. Click OK to start the upload. Otherwise, click Cancel to exit this screen.</p>
Unload	Select an existing MIB file in the table and click this to delete it from the ENC database.
check box	Select the check box of an entry and click Unload to delete it. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
File Name	This field displays the name of the MIB file.
Module Name	This field displays the MIB module name retrieved from the MIB file.

6.7.2 Default MIBs

Use this screen to view the default MIBs the ENC stores view default MIBs that came with the ENC when the ENC was installed.

To open this screen, click **Tool > MIB Loader > Default MIBs**.

Figure 114 MIB Loader > Default MIBs



User Loaded MIBs	
Default MIBs	
File Name	Module Name
1 zyxel-xgs4526.mib	ZYXEL-XGS4526-MIB
2 zyxel-xgs4728f.mib	ZYXEL-XGS4728F-MIB
3 zyxel-xgs4528f.mib	ZYXEL-XGS4528F-MIB
4 zyxel-mgs3712.mib	ZYXEL-MGS3712-MIB
5 zyxel-mes3728.mib	ZYXEL-MES3728-MIB
6 zyxel-gs4024.mib	ZYXEL-GS4024-MIB
7 zyxel-gs4012f.mib	ZYXEL-GS4012F-MIB
8 zyxel-gs3012f.mib	ZYXEL-GS3012F-MIB
9 zyxel-gs3012.mib	ZYXEL-GS3012-MIB
10 zyxel-gs2750.MIB	ZYXEL-GS2750-MIB

The following table describes the labels in this screen.

Table 66 Tool > MIB Loader > Default MIBs

LABEL	DESCRIPTION
File Name	This field displays the name of the MIB file.
Module Name	This field displays the MIB module name retrieved from the MIB file.

6.8 Performance Monitoring

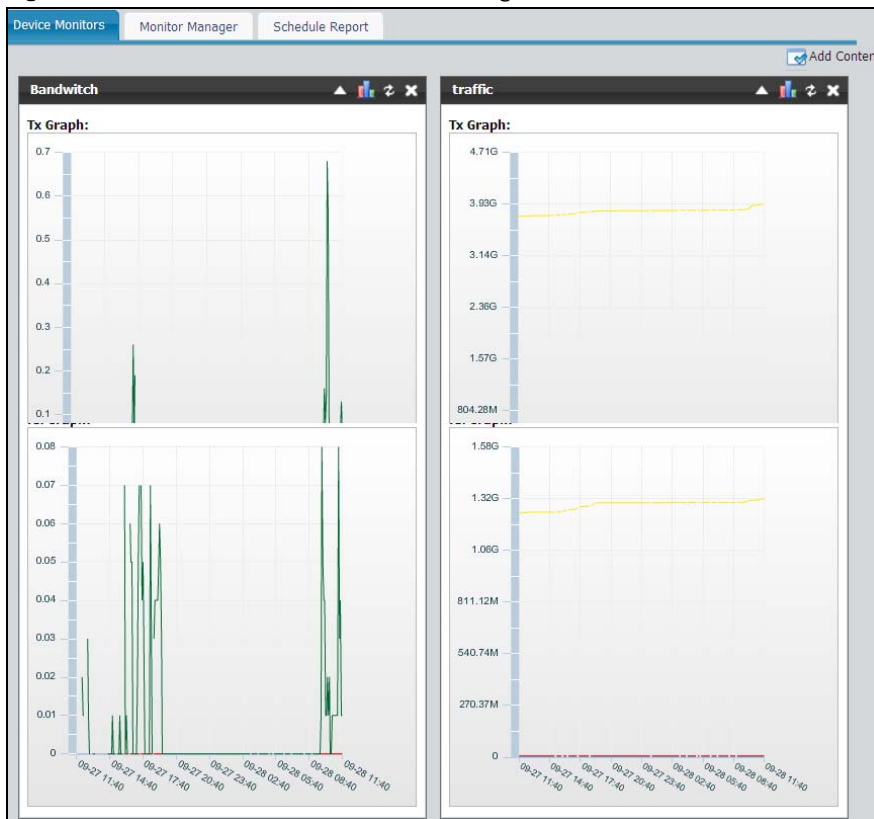
Use these screens to view or configure performance monitors for an individual device. You must select a device first before using this menu.

6.8.1 Device Monitor

Use this screen to view the performance statistics in graphs for the selected device. Before using this screen, make sure that you configure at least a performance monitor in the **Monitor Manager** screen for the device first.

To open this screen, click **Tool > Performance Monitoring**. The screen varies depending on the monitor(s) you selected to display.

Figure 115 Tool > Performance Monitoring > Device Monitors



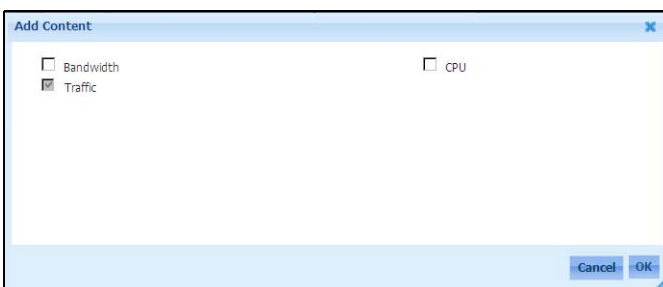
6.8.2 Example - Displaying Selected Performance Monitors

To add performance monitor(s):

- 1 Click **Add Content** on the top-right corner.



- 2 Select the monitor(s) to display. Click **OK**.

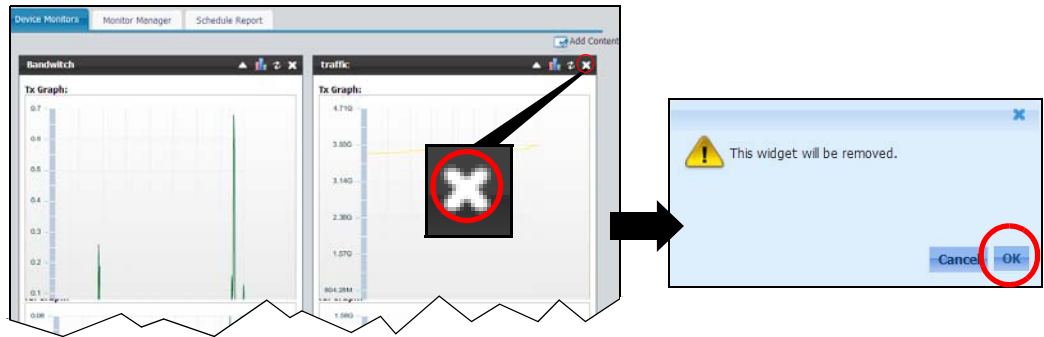


- 3 The selected performance monitor(s) appear.

6.8.3 Example - Removing Selected Performance Monitors

To not display a performance monitor in this screen:

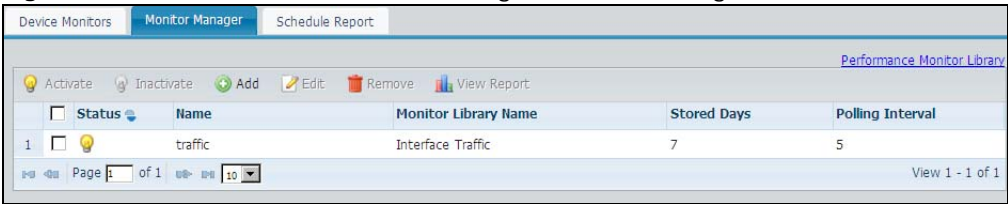
- 1 Click the **Close Widget** icon on the top-right corner of the widget.
- 2 Click **OK** to confirm the action.



6.8.4 Monitor Manager

Use this screen to configure performance monitor(s) for the selected device. To open this screen, click **Tool > Performance Monitoring > Monitor Manager**.

Figure 116 Tool > Performance Monitoring > Monitor Manager



The following table describes the labels in this screen.

Table 67 Tool > Performance Monitoring > Monitor Manager

LABEL	DESCRIPTION
Performance Monitor Library	Click this link to display the Configuration > Performance Monitor Library screen, if you want to view default performance monitor templates or customize more performance monitor templates.
Activate	Click this to activate the selected performance monitor(s).
Inactivate	Click this to deactivate the selected performance monitor(s).
Add	Click this to create a new performance monitor for the selected device.
Edit	Select a performance monitor and click this to configure it.
Remove	Click this to delete the selected performance monitor(s).
View Report	Select a performance monitor and click this to display the statistics in a graph.
check box	Select this check box and click Activate , Inactivate , Edit , Remove or View Report to take the action respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Status	This field displays whether the monitor is active or not.
Name	This field displays the name of the performance monitor.

Table 67 Tool > Performance Monitoring > Monitor Manager (continued)

LABEL	DESCRIPTION
Monitor Library Name	This field displays the name of the performance monitor template this monitor uses.
Stored Days	This field displays the number of days the ENC keeps the monitor data before removing it from the ENC.
Polling Interval	This field displays how often (in seconds) the ENC retrieves the monitor data from the device.

6.8.5 Performance Monitor Add

Use this screen to configure performance monitor(s) for the selected device and the threshold(s) of the monitor. To open this screen, click **Add** in the **Tool > Performance Monitoring > Monitor Manager** screen.

Note: The available fields in this screen vary depending on the monitor library option you selected.

Figure 117 Tool > Performance Monitoring > Monitor Manager > Add

The following table describes the labels in this screen.

Table 68 Tool > Performance Monitoring > Monitor Manager

LABEL	DESCRIPTION
General Settings	
Status	Select whether to Activate or Inactivate this performance monitor.
Monitor Name	Type up to 32 alphanumeric characters (0-9, a-z, A-Z) for the monitor's name. Underscores (_) and hyphens (-) are also allowed.
Monitor Library	Select a performance monitor template to apply to this monitor.

Table 68 Tool > Performance Monitoring > Monitor Manager (continued)

LABEL	DESCRIPTION
Stored Days	Select the number of days the ENC will store the monitor data before the ENC deletes it.
Polling Interval	Select the number of minutes the ENC sends a poll message for the performance monitor.
Description	Enter additional information for the performance monitor in this field.
Available Instance	Select the item(s) you want to monitor and use the > arrow to move them to the Selected Instance list. You can use the >> arrow to move all the available items to the Selected Instance list.
Selected Instance	This section lists the items to monitor for this performance monitor. Select item(s) and click the < arrow to remove them from this list. You can use the << arrow to remove all the items from this list.
Threshold	
Add	Click this to create a new threshold rule.
Edit	Select a threshold rule and click this to configure it.
Remove	Click this to delete the selected threshold rule(s).
check box	Select this check box and click Edit or Remove to take the action respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Instance	This field displays the MIB object to which this threshold rule is related.
Is Delta Value	This field displays whether the method used to obtain the sample values is delta (true) or absolute (false). Delta means the value is from the data sampled in each configured time interval. Absolute means the sampling value is accumulated since it started.
Condition	This field displays the comparison operator (above , below , equal , not equal or status change) for the threshold.
Value	This field displays the value for the threshold.
Occurrence	This field displays the number of times the monitored value has to continuously fall into the threshold's condition before the ENC takes the corresponding action.
Cancel	Click this to discard the changes and close this screen.
Ok	Click this to save the changes and close this screen.

6.8.6 Add a Threshold to the Performance Monitoring List

Use this screen to configure a threshold for the performance monitor.

To open this screen, click **Add** in the **Configure Threshold Value** section of the **Tool > Performance Monitoring > Monitor Manager > Add** screen.

Note: The available fields on this screen may vary depending on the monitor library you selected.

Figure 118 Tool > Performance Monitoring > Monitor Manager > Add > Add

The following table describes the labels in this screen.

Table 69 Tool > Performance Monitoring > Monitor Manager > Add > Add

LABEL	DESCRIPTION
Instance	Select the MIB object (you may also need to select the instance number) for this threshold. The instance numbers vary depending on the MIB object you specified. You can set a different threshold for each instance in this screen.
Is Delta Value	Select whether to use the delta or absolute method to obtain the sample values. Delta means the value is from the data sampled in each configured time interval. Absolute means the sampling value is accumulated since it started.
Condition	Select the comparison operator (above , below , equal , not equal or status change) for the threshold to determine when the ENC will take the corresponding action configured in the Events > Configuration screen.
Value	Enter a value for the threshold.
Occurrence	Enter how many times the monitored value has to continuously fall into the threshold's condition before the ENC takes the corresponding action.
Cancel	Click this to discard the changes and close this screen.
Ok	Click this to save the changes and close this screen.

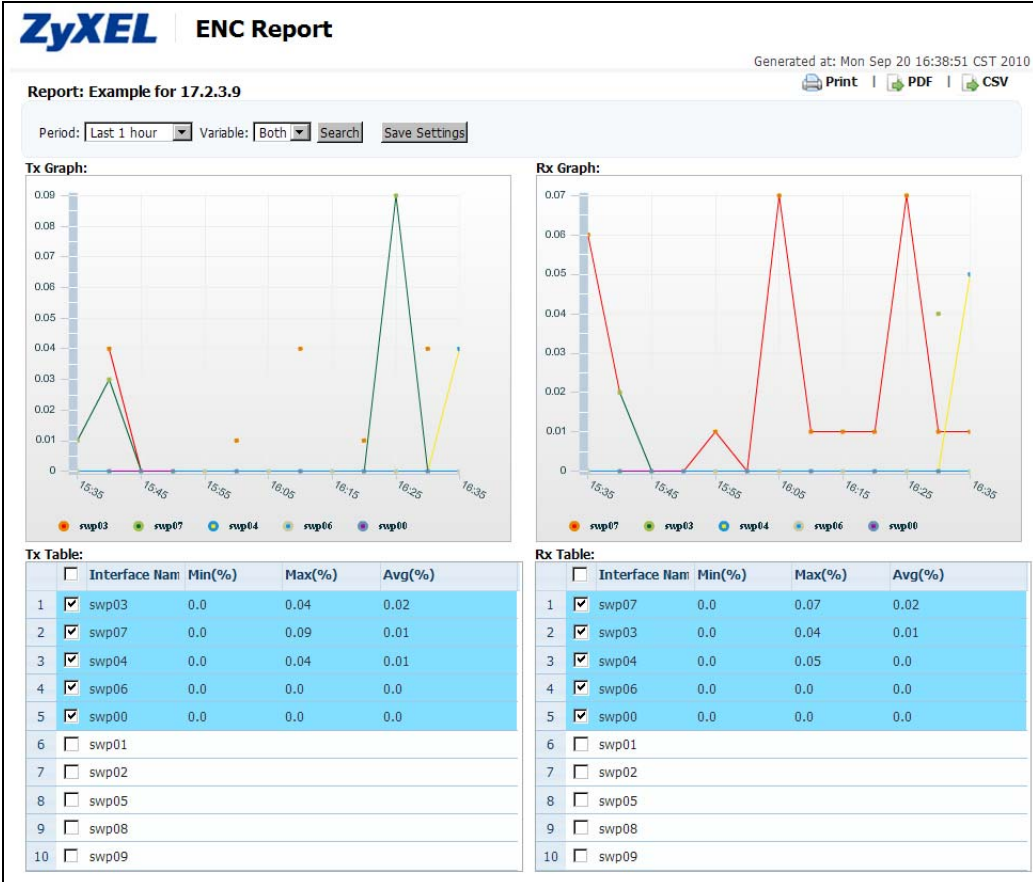
6.8.7 View the Performance Monitoring Report

Use this screen to view and/or print the performance monitor data in a graph. You can also export the data to a CSV and/or PDF file.

To open this screen, select a performance monitor and click **View Report** in the **Tool > Performance Monitoring > Monitor Manager** screen.

Note: Fields vary depending on the report you selected. The following figure is an example.

Figure 119 Tool > Performance Monitoring > Monitor Manager > View Report



The following table describes the labels in this screen.

Table 70 Tool > Performance Monitoring > Monitor Manager > View Report

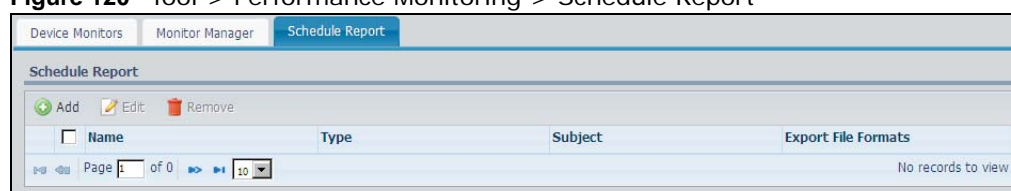
LABEL	DESCRIPTION
Generated at	The field displays when this report was generated.
Report:	This field displays the name of the report you are viewing and the selected device's name.
Print	Click this to print this report out.
PDF	Click this to export the report to a PDF file on the computer you are using to access the ENC.
CSV	Click this to export the report to a CSV file on the computer you are using to access the ENC.
Period	Select how long ago the monitor's data that you are looking for was added to the ENC.
Variable	Select whether to show statistics about outgoing traffic only (Tx), incoming traffic only (Rx) or both incoming and outgoing traffic (Both) for the report.
Search	Click this to generate the monitor data based on your selected criteria.
Save Settings	Click this to save the customized settings for the graph being displayed in this screen.

Table 70 Tool > Performance Monitoring > Monitor Manager > View Report (continued)

LABEL	DESCRIPTION
Tx/Rx Graph	The graph shows statistics of the monitor based on the specified criteria.
Tx/Rx Data Table	
check box	Unselect this check box to not display the related statistic data in the graph. Select it again to display the data in the graph. Select or clear the check box at the table heading line to select or clear all check boxes in this column. Note: A graph can display up to five interfaces' data.
Interface Name	This field displays the name of an instance on the device.
Min	This field displays the minimum value of this instance during the sampling period.
Max	This field displays the maximum value of this instance during the sampling period.
Avg	This field displays the average value of this instance during the sampling period.

6.9 Schedule Report

Click **Tool > Performance Monitoring > Schedule Report** to view the list of existing scheduled performance monitor reports for the device. Click **Add** to create a new schedule report.

Figure 120 Tool > Performance Monitoring > Schedule Report

Each field is described in the following table.

Table 71 Tool > Performance Monitoring > Schedule Report

LABEL	DESCRIPTION
Add	Click this to create a daily, weekly or monthly report in a time interval.
Edit	Click this to modify an existing scheduled report.
Remove	Click this to delete the selected scheduled report.
check box	Select the check box, and click Edit to modify the settings or Remove to delete the scheduled report. Select or clear the check box at the table heading line to select or clear all check boxes in this column. Clear it to have all the check boxes being cleared.
Name	This field displays the name of the scheduled report. Click it and Edit to edit the scheduled report next to it. The Customize Scheduled Report screen appears. Otherwise, this field is a sequential value, and it is not associated with a specific scheduled report. For example, if you delete a scheduled report, the remaining scheduled reports are re-numbered.
Type	This field displays whether this is a daily, weekly or monthly report.
Subject	This field displays the subject line in the e-mail message the ENC sends.
Export File Formats	This field displays the format(s) of files that the ENC will send through e-mail when the scheduled report is generated.

6.10 Schedule Report Add/Edit

Click **Add or Edit in the Tool > Performance Monitoring > Schedule Report** screen to configure a scheduled report. You can check whether the schedule report is successfully generated or not later in the **Maintenance > Log** screen.

Figure 121 Tool > Performance Monitoring > Schedule Report > Add/Edit

Each field is described in the following table.

Table 72 Tool > Performance Monitoring > Schedule Report > Add/Edit

LABEL	DESCRIPTION
Name	Enter the name of the schedule report. Only numbers (0-9), letters (a-z, A-Z), hyphen (-) and the underscore (_) are allowed. Spaces are not allowed.
Type	Select how often (daily , weekly or monthly) to generate the schedule report.
Send Time	<p>Select when to start generating the report. The ENC sends the report after it finishes generating it. The report generation time depends on the amount of information in the report. Having the ENC generate too many reports at the same time can affect performance. It is recommended that you vary the times for your reports.</p> <p>For a daily report, select the time (hour:minute) to generate the report.</p> <p>For a weekly report, select which week day (Sunday~Saturday) and time (hour:minute) to generate the report.</p> <p>For a weekly report, select which date (1~31) and time (hour:minute) per month to generate the report.</p>
Receiver Email Address List	Enter a valid e-mail address to which the ENC sends the report and click Add to add it in the list below. You can enter as many valid e-mail addresses as you want. Select one or multiple entries and click Remove to delete them from the list. The ENC provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.

Table 72 Tool > Performance Monitoring > Schedule Report > Add/Edit

LABEL	DESCRIPTION
Subject	Enter the subject line in the e-mail message the ENC sends. Only numbers (0-9), letters (a-z, A-Z), characters ('+', '/', '=', '?', '!', '*', '#', '@', '\$', '_', '%', '-'), carriage returns (\n), line breaks (\r) and spaces are allowed. The ENC provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.
Export File Formats	Select the format(s) of the report(s) that you see. The available options are CSV, PDF and HTML. The ENC will send you an e-mail with a URL (Uniform Resource Locator). Click the URL to see the report(s).
Available Items	Select the reports to include in this schedule report and use the >> arrow to move them to the Selected Items list. You can configure more reports for the device in the Tool > Performance Monitoring > Monitor Manager screen.
Selected Items	This section lists the reports included in this schedule report. Select a report and click the << arrow if you want to remove it from the schedule report.
Cancel	Click this to discard the changes and exit this screen.
Ok	Click this to save your settings and close the screen.

6.11 Syslog Overview

These screens provide information for all log entries of devices being monitored by ENC.

Note: The logs screens, fields and menus can vary according to which device the logs are collected for.

6.11.1 Syslog View

Use this screen to search for specific logs that devices sent to the ENC.

To open this screen, click **Tool > Syslog View**.

See [Section 6.11.3 on page 173](#) for more information about update frequencies for log entries. See [Section 6.11.2 on page 172](#) for more information about the source data used by the report.

Figure 122 Tool > Syslog View > Log Viewer

The screenshot shows the 'Log Viewer' window with tabs for 'Log Viewer', 'Log Statistic', and 'Settings'. The 'Log Viewer' tab is active. It contains search filters: 'Time' (Last 24 hours), 'Facility' (All), 'Severity' (All), 'Source' (empty), and 'Keyword' (empty). A 'Search' button is below these filters. Below the search filters are 'Export' and 'Remove' buttons. At the bottom, there is a table with columns: Time, Facility, Severity, Source, and Message. The table is empty, and a message at the bottom right says 'No records to view'.

The following table describes the labels in this screen.

Table 73 Tool > Syslog View > Log Viewer

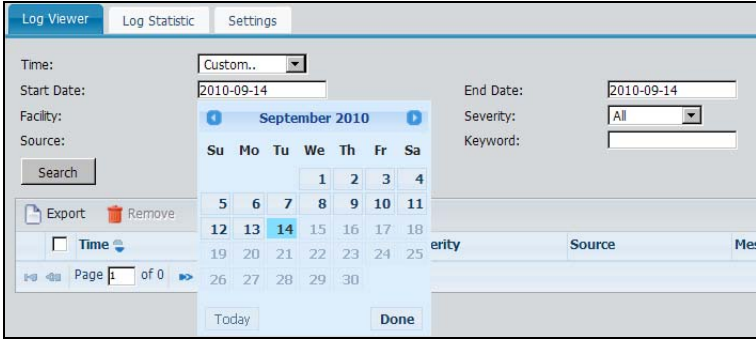
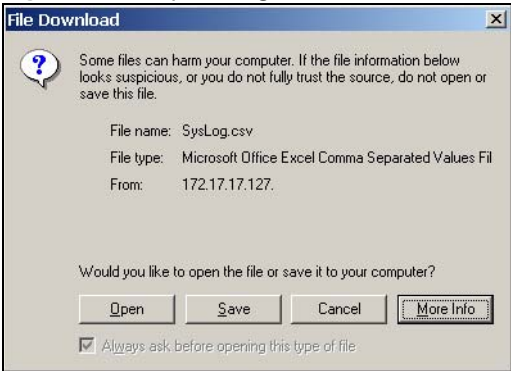
LABEL	DESCRIPTION
Time	<p>Select within the number of hours or days in the past the log you are looking for was received by the ENC for the search criteria. The options are Last 24 hours, Last 48 hours, Last 5 days, Last 7 days and Last 30 days. Select Custom to display additional fields if you want to customize a period for the search criteria. Click the text box next to Start Date or End Date, a calendar displays as shown next.</p> <p>Figure 123 Customize a Period</p>  <p>Choose a date (or click Today) and click Done to close the calendar. The ending date must not be earlier than the starting date.</p>
Facility	<p>Select a location (local0–local7) from the drop down list box. The log facility allows you to display the logs in different files in the syslog server of the ENC. Select All to display all messages in all the files on the ENC.</p>
Severity	<p>Select which severity level of log entries you want to see. You can also select All.</p> <p>Severity ranking follows RFC 3164 of the SYSLOG protocol and is defined as follows.</p> <ul style="list-style-type: none"> • Emergency - System is unusable • Alert - Action must be taken immediately • Critical - Critical conditions • Error - Error conditions • Warning - Warning conditions • Notice - Normal but significant condition • Info - Informational messages • Debug - Debug-level messages
Source	<p>Enter the source IP address that generated the log entry.</p>
Keyword	<p>Enter part or all of any value you are looking for in the Message field. You can use any printable ASCII character. The search is not case-sensitive.</p>
Search	<p>Click this to display the log entries based on the current search criteria.</p>

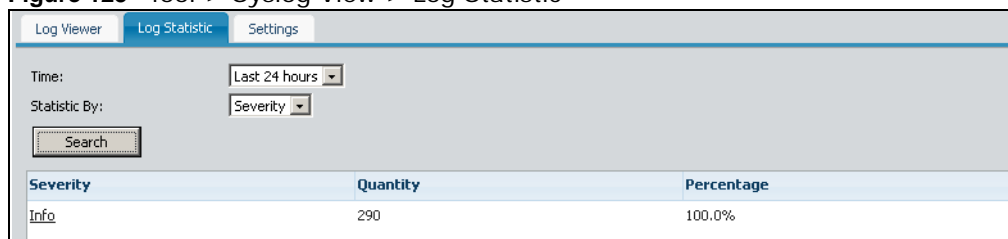
Table 73 Tool > Syslog View > Log Viewer (continued)

LABEL	DESCRIPTION
Export	<p>Click this to export the search results to a CSV file. The screen pops up as shown next.</p> <p>Figure 124 Export Logs</p>  <ul style="list-style-type: none"> Click Open to open the file directly. Click Save to save the file to the computer that you are currently using to access the ENC server, then exit this screen. Click Cancel to exit this screen without saving any changes. Select More Info to view an on-line help page about downloading files.
Remove	Select one or more log entries in the table and click this to delete them.
Time	This field displays the date and time the ENC received the log entry, not the time the log entry was generated.
Facility	This field displays the name of the location where the log entry is stored in the ENC.
Severity	This field displays the severity level of the log entry.
Source	This field displays the source IP address that generated the entry.
Message	This field displays the reason the log entry was generated.

6.11.2 Log Statistic

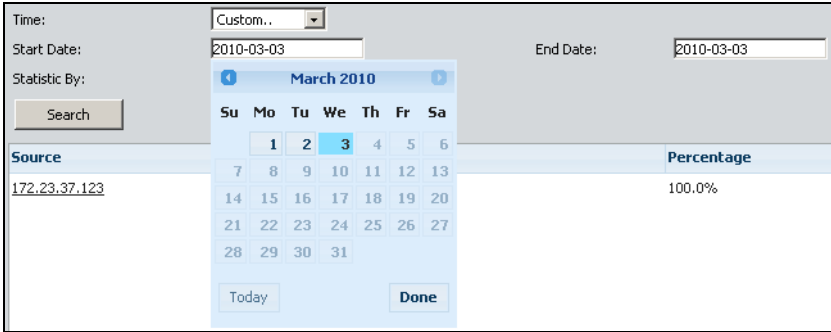
Use this screen to view log statistics by date, source IP address or severity level.

To open this screen, click **Tool > Syslog View > Log Statistic**.

Figure 125 Tool > Syslog View > Log Statistic

The following table describes the labels in this screen.

Table 74 Tool > Syslog View > Log Statistic

LABEL	DESCRIPTION
Time	<p>Select within the number of hours or days in the past the log you are looking for was received by the ENC for the search criteria. The options are Last 24 hours, Last 48 hours, Last 5 days, Last 7 days and Last 30 days. Select Custom to display additional fields if you want to customize a period for the search criteria. Click the text box next to Start Date or End Date, a calendar displays as shown next.</p> <p>Figure 126 Customize a Period</p>  <p>Choose a date (or click Today) and click Done to close the calendar. The ending date must not be earlier than the starting date.</p>
Statistic By	<p>Select this to display the log statistics shown by:</p> <p>Date - the date the ENC received the log entries</p> <p>Source - the source IP address that generated the log entries</p> <p>Severity - the severity level of the log entries</p> <p>The fields of the table below vary depending on the option you select in this field.</p>
Search	Click this to display the log entries based on the current search criteria.
Date	This field displays each date of the matched log entries received by the ENC.
Source	This field displays each source IP address that generated the matched log entries.
Severity	This field displays each severity level of the matched log entries.
Quantity	<p>If you selected Statistic By Date, this field displays the number of the day's log entries.</p> <p>If you selected Statistic By Source, this field displays the number of the log entries generated by the IP address.</p> <p>If you selected Statistic By Severity, this field displays the number of the log entries that are in the severity level.</p>
Percentage	This field displays what percent of the log entries came from each category.

6.11.3 Settings

Use this screen to archive past logs to a preferred location (local directory or FTP/storage server) as a ZIP file.

To open this screen, click **Tool > Syslog View > Settings**.

The screen display varies according to your storage location preference.

Figure 127 Tool > Syslog View > Settings

The following table describes the labels in this screen.

Table 75 Tool > Syslog View > Settings

LABEL	DESCRIPTION
General	
Syslog Receiver	Select this check box to enable (Active) or disable (Inactive) syslog server on the ENC.
Stored Logs Days	Enter the number of days the ENC stores a log entry before it removes the log from the database.
Archiving Setting	This section allows you to archive past logs to a preferred location (local directory, FTP or storage server) as a ZIP file. You can set the day(s) or time interval when ENC performs this task.
Enable Archiving	Click this to enable ENC to archive log files.
Archive: every... 1~7days	Set every how many days (1~7) the ENC archives the generated log entries.
Location	<p>Local Host: Select this to store the archive to a local folder in the computer where the ENC is installed. This is the default storage setting for the ENC.</p> <p>FTP Site: Select this to store the archive to an FTP site. Additional fields appear when you choose this option.</p> <p>Storage Server: Select this to store the archive to a storage server, such as a Network Attached Storage (NAS) server. Additional fields appear when you choose this option.</p> <p>Note: If the storage server's space is not enough for the size of the log archive, the ENC sends out an alert e-mail and generates a system log.</p>
Archive Location	This field is available if you selected Local Host in the Location field. Specify where you want the ENC to store log archives in the local directory of the ENC.
FTP Host/IP	<p>This field is available if you selected FTP Site in the Location field.</p> <p>Enter the IP address or domain name of the File Transfer Protocol (FTP) server you want to use.</p>
Port	<p>This field is available if you selected FTP Site in the Location field.</p> <p>Enter another port number if the FTP server does not use port 21 for the service.</p>

Table 75 Tool > Syslog View > Settings (continued)

LABEL	DESCRIPTION
User Name	This field is available if you selected FTP Site in the Location field. Enter the User Name for your FTP account.
Password	This field is available if you selected FTP Site in the Location field. Enter the Password for your FTP account.
FTP path	This field is available if you selected FTP Site in the Location field. You can specify in which FTP folder you want to store the archive.
Network Folder	This field is available if you selected Storage Server in the Location field. Enter the full path of a server folder where you want to store the archive.
Authentication	This field is available if you selected Storage Server in the Location field. Select this if authentication is required to use the specified directory. Click Authentication if your server prompts for identification before allowing access.
User Name	This field is available if you selected Storage Server in the Location field. Enter the user name that has the privilege to upload files to the specified directory.
Password	This field is available if you selected Storage Server in the Location field. Enter the corresponding Password .
Apply	Click this to save your settings.
Reset	Click this to change the settings in this screen to the last-saved values.

Report

Use the **Report** screens to start or stop data collection and view various statistics about traffic passing through managed devices or the devices themselves. You can also set up and generate reports according to a set period. Scheduled reports can be sent daily, weekly, and/or monthly through e-mails.

Note: To send scheduled reports by e-mail, you have to enter the SMTP mail server settings in the **Maintenance > Server** screen. See [Section 9.4 on page 247](#) for more information.

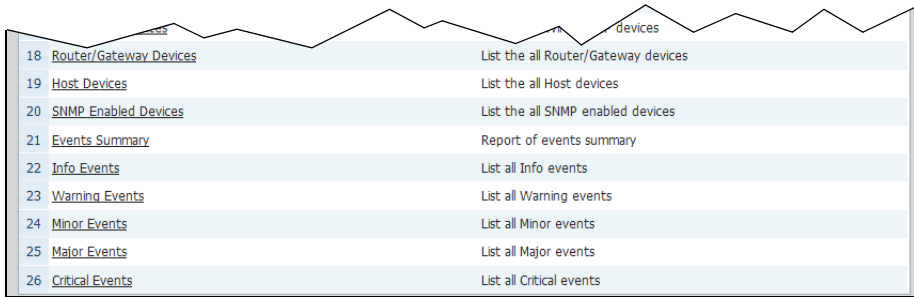
The ENC server backs up all scheduled reports in the {ENC_home}\ENC\data\report\{schedule_report_name}\ folder. The file name includes the schedule report name and the date and time the report is generated, for example, "WeeklyPerfReport_20100121014001.zip".

7.1 Default Reports Screen

Use this screen to view reports that are defined by default. Click **Report > Reports** to open the screen as shown next.

Figure 128 Report > Reports > Default Reports

Default Reports		Customized Reports
Report Name	Description	
1 Top N Device CPU Utilization	Top N report of Device CPU Utilization	
2 Top N Device Memory Utilization	Top N report of Device Memory Utilization	
3 Top N Interface Rx Bandwidth Utilization	Top N report of Interface Rx Bandwidth Utilization	
4 Top N Interface Tx Bandwidth Utilization	Top N report of Interface Tx Bandwidth Utilization	
5 Top N Device Rx Traffic	Top N report of Device Rx Traffic	
6 Top N Device Tx Traffic	Top N report of Device Tx Traffic	
7 Top N Interface Rx Traffic	Top N report of Interface Rx Traffic	
8 Top N Interface Tx Traffic	Top N report of Interface Tx Traffic	
9 Top N Interface Rx Unicast Traffic	Top N report of Interface Rx Unicast Traffic	
10 Top N Interface Tx Unicast Traffic	Top N report of Interface Tx Unicast Traffic	
11 Top N Interface Rx Non-unicast Traffic	Top N report of Interface Rx Non-unicast Traffic	
12 Top N Interface Tx Non-unicast Traffic	Top N report of Interface Tx Non-unicast Traffic	
13 Top N Interface Rx Errors	Top N report of Interface Rx Errors	
14 Top N Interface Tx Errors	Top N report of Interface Tx Errors	
15 Switch Devices	List the all Switch devices	
16 Firewall Devices	List the all Firewall devices	
17 Wireless AP Devices	List the all Wireless AP devices	



18	Router/Gateway Devices	List the all Router/Gateway devices
19	Host Devices	List the all Host devices
20	SNMP Enabled Devices	List the all SNMP enabled devices
21	Events Summary	Report of events summary
22	Info Events	List all Info events
23	Warning Events	List all Warning events
24	Minor Events	List all Minor events
25	Major Events	List all Major events
26	Critical Events	List all Critical events

Each field is described in the following table.

Table 76 Report > Reports > Default Reports

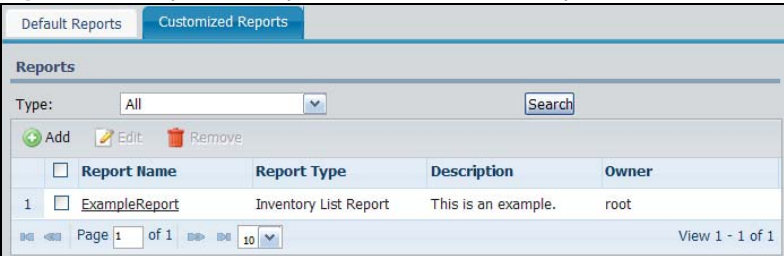
LABEL	DESCRIPTION
Report Name	This field displays the descriptive name of a default report. Click this to generate and view the report.
Description	This field displays more information about the report.

7.2 Customized Reports Screen

Click **Report > Reports > Customized Reports** to view and manage (add, edit, delete) a list of configured reports.

Note: The ENC allows a maximum size of 300 MB for a scheduled report. When the ENC server's disk space is not enough, the ENC sends out an alert e-mail to administrators. Remove unused reports to free up some disk space.

Figure 129 Report > Reports > Customized Reports



Each field is described in the following table.

Table 77 Report > Reports > Customized Reports

LABEL	DESCRIPTION
Type	Select the type of reports you want to display in this screen and click Retrieve . You have to add at least a report by clicking Add to use this filter.
Search	Click this to perform the filter.
Add	Click this to create a report.
Edit	Select a report and click this to configure it.
Remove	Click this to delete the selected report(s).

Table 77 Report > Reports > Customized Reports

LABEL	DESCRIPTION
check box	Select this check box and click Remove to delete the report. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Report Name	This field displays the descriptive name of the report. Click this to generate and view the report.
Report Type	This field displays the type of the report. Either Inventory, Events or Performance related and either a list view, summary or TopN report.
Description	This field displays more information about the report.
Owner	This field displays a person's name who creates this report.

7.2.1 Report Add

Use this screen to add a report. To open the screen, click **Add** in the **Report > Reports > Customized Reports** screen. The fields in the **Add Reports** screens vary depending on the **Report Type** you select.

Figure 130 Report > Reports > Add (Inventory List Report)

The figure illustrates the three-step process for adding an Inventory List Report:

- Step 1: General Properties** (labeled with a red '1'). The 'Report Name' field contains 'ExampleReport' and the 'Descriptions' field contains 'This is an example.' Buttons for 'Cancel' and 'OK' are at the bottom.
- Step 2: Settings for Inventory List Report** (labeled with a red '2'). This screen includes dropdown menus for 'Device Type', 'Device Model', 'Status', and 'Discovered Date', along with text input fields for 'Display Name', 'IP Address', and 'Firmware Version'. Buttons for 'Cancel', 'Previous', and 'Next' are at the bottom.
- Step 3: List View Report Customized Columns Setting** (labeled with a red '3'). This screen shows two lists: 'Available Columns' (containing Device Type, Device Model, System Description, System Old, System Name, System Contact, System Location, System Uptime, System Service, and Firmware Version) and 'Selected Columns'. Navigation buttons '>>', '<<', 'Move Up', and 'Move Down' are between the lists. Buttons for 'Cancel', 'Previous', and 'Ok' are at the bottom.

Figure 131 Report > Reports > Add (Inventory Summary Report)

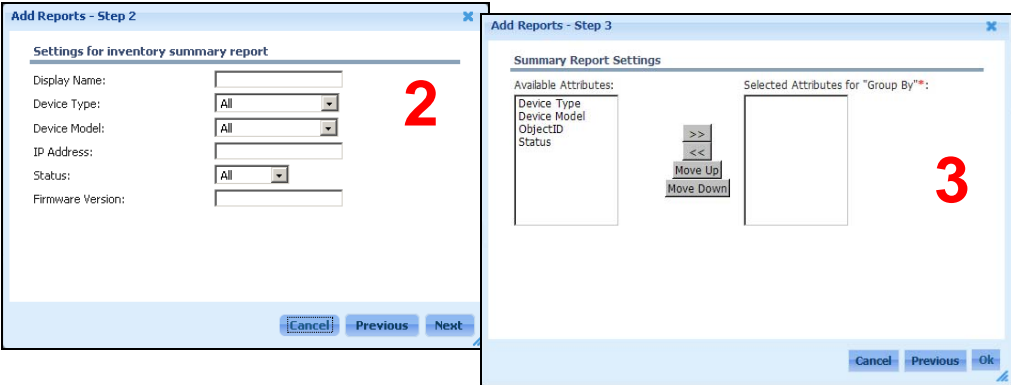


Figure 132 Report > Reports > Add (Events List Report)

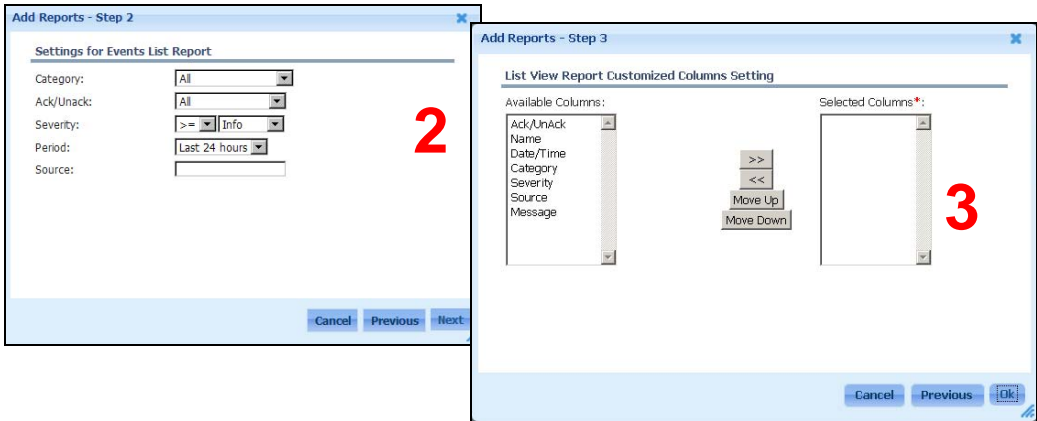


Figure 133 Report > Reports > Add (Events Summary Report)

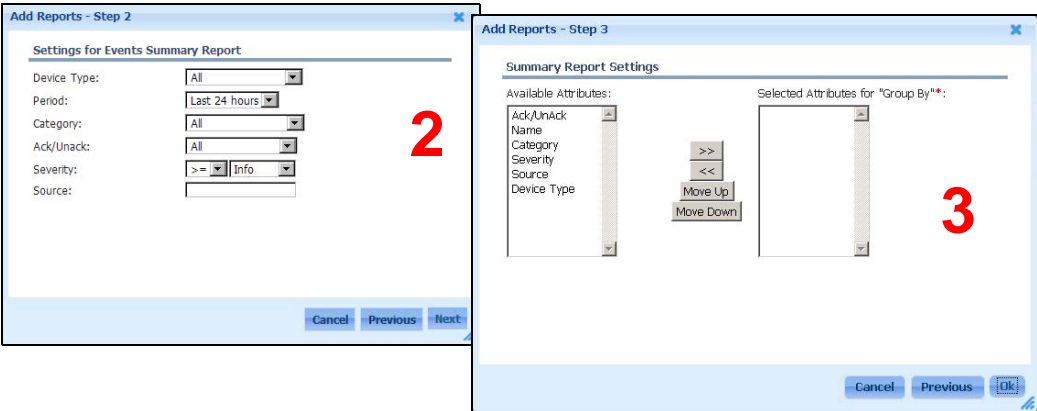


Figure 134 Report > Reports > Add (Top N Report)

The figure consists of two side-by-side screenshots of a software interface for adding reports.

The left screenshot is titled "Add Reports - Step 2" and shows a "Settings for Top N Report" dialog. It has a "Performance Monitor Library:" section with a list of metrics: Interface Unicast Traffic, Device CPU Utilization (highlighted with a red '2'), Memory Utilization, Interface Bandwidth Utilization, Interface Traffic, Interface Unicast Traffic, Interface Non-unicast Traffic, Interface Errors, monitorTest-template-1, and monitorTest2-template-2. At the bottom are "Cancel", "Previous", and "Next" buttons.

The right screenshot is titled "Add Reports - Step 3" and shows a "Top N Report Setting" dialog. It contains several dropdown menus: "Variable" (set to CPU), "Period" (set to Last 1 hour), "Device Type" (set to All), "Device Group" (set to All), and "Top N:" (set to 5). A red '3' is placed to the right of this dialog. At the bottom are "Cancel", "Previous", and "Ok" buttons.

Each field is described in the following table.

Table 78 Report > Reports > Add

LABEL	DESCRIPTION
Step 1 - General Properties	
Report Name	Enter a name to identify the report. Numbers (0-9), letters (a-z, A-Z), hyphen (-) and the underscore (_) are allowed. Spaces are not allowed.
Report Type	Select the type of the report.
Descriptions	Enter the further information for the report.
Cancel	Click this to discard the changes and exit this screen.
Next	Click this to proceed to the next step.
Step 2	
Display Name	Enter a name of the report, which you want to display on the top of the report. It is recommended to specify the related device names in this field. Numbers (0-9), letters (a-z, A-Z), hyphen (-) and the underscore (_) are allowed. Spaces are not allowed. This field is optional.
Device Type	Select which type of devices that you want to display the related information in the report. The options include Host , Switch , Firewall , Wireless AP , Router/Gateway , Wireless Controller , IP PBX , IP Phone , Peripheral , All (means all types mentioned), Others (means all types not mentioned).
Device Model	Select a specific model if you want to display the related information only in the report. Otherwise, leave it as the default (All). The available options vary depending on the device type you selected.
IP Address	Enter a valid IP address if you want to display the related device's information only in the report. Otherwise, leave it as blank.
Status	Select a specific status of devices that you want to display the related information only in the report. Otherwise, leave it as the default (All). unknown means a device is unreachable before the ENC determines it is offline.
Firmware Version	This field is available if you selected an Inventory related report. Enter the major firmware version of the device(s) that you are looking for to display the related device's information only in the report. Otherwise, leave it as blank.

Table 78 Report > Reports > Add



LABEL	DESCRIPTION
Discovered Date	<p>This field is available if you selected the Inventory List Report.</p> <p>Select how long ago the device(s) that you are looking for were added to the ENC. Select Custom to display the additional fields in this screen as shown.</p> <p>Figure 135 Specify a Discover Date</p>  <p>Click the text box next to Start Date or End Date and choose a date (or click Today) from the displayed calendar. Then click Done. The devices added during this period will be shown in the report.</p>
Category	<p>This field is available if you selected an Events related report. Select the category of events that you want to display in the report.</p> <ul style="list-style-type: none"> • Threshold Crossing: This is about a parameter's value is higher or lower than a set threshold. • Configuration: This is about a configuration change on the ENC. • Topology: This is about a network topology change detected by the ENC. • SNMP Traps: This is about SNMP traps sent from Devices. • All: This means all categories above.
Ack/Unack	<p>This field is available if you selected an Events related report.</p> <p>Select whether the events that you want to display have been Acknowledged or not (Unacknowledged). All means both.</p>
Severity	<p>Select the severity of events should be equal to (=), greater or equal to (>=), less or equal to (<=) a severity level selected on the second drop-down list box. See Table 73 on page 171 for more information about severity.</p>
Period	<p>Select how long ago the events that you are looking for were added to the ENC. Select Custom to display the additional fields in this screen as shown.</p> <p>Figure 136 Specify a Period</p>  <p>Click the text box next to Start Date or End Date and choose a date (or click Today) from the displayed calendar. The events added to the ENC during this period will be shown in the report.</p>
Source	<p>Select which person has acknowledged the events that you are looking for.</p>

Table 78 Report > Reports > Add

LABEL	DESCRIPTION
Performance Monitor Library	<p>This field is available if you selected Top N Report.</p> <p>Select which performance monitor report that you want to see. By default, the available options are:</p> <ul style="list-style-type: none"> • Device CPU Utilization • Memory Utilization • Interface Bandwidth Utilization • Interface Traffic • Interface Unicast Traffic • Interface Non-unicast Traffic • Interface Errors <p>You can define more performance monitor report in Configuration > Performance Monitor Library > Customized Monitor Library.</p>
Cancel	Click this to discard the changes and go back to the Report > Reports > Customized Reports screen.
Previous	Click this to discard the changes in this screen and go back to the last screen.
Next	Click this to proceed to the next screen.
Step 3	
Available Columns or Available Attributes	<p>This field is available if you selected Inventory or Events related report.</p> <p>Select the columns or attributes to include in this report and use the >> arrow to move them to the Selected Columns or Selected Attributes for "Group By" list.</p>
Selected Columns or Selected Attributes for "Group By"	<p>This field is available if you selected Inventory or Events related report.</p> <p>This section lists the columns or attributes included in this report. Select an item and click the << arrow if you want to remove it from the report. Select one or multiple items and then use Move Up or Move Down to adjust the displaying order in the report.</p>
Variable	<p>This field is available if you selected Top N Report.</p> <p>Select the variables to include in this report. The available options vary depending on what you selected in the Performance Monitoring field at the last step. This field is mandatory if a variable is available in this field.</p>
Top N	<p>This field is available if you selected Top N Report.</p> <p>Select the number of devices that have the most heavy performance loading to display in the report.</p>
Cancel	Click this to discard the changes and go back to the Report > Reports > Customized Reports screen.
Previous	Click this to discard the changes in this screen and go back to the last screen.
Ok	Click this to save the changes and close this screen.

7.2.2 Report Edit

Use this screen to change a report's name and description. To open the screen, select a report and click **Edit** in the **Report > Reports > Customized Reports** screen.

Figure 137 Report > Reports > Edit

Edit Reports

General Properties

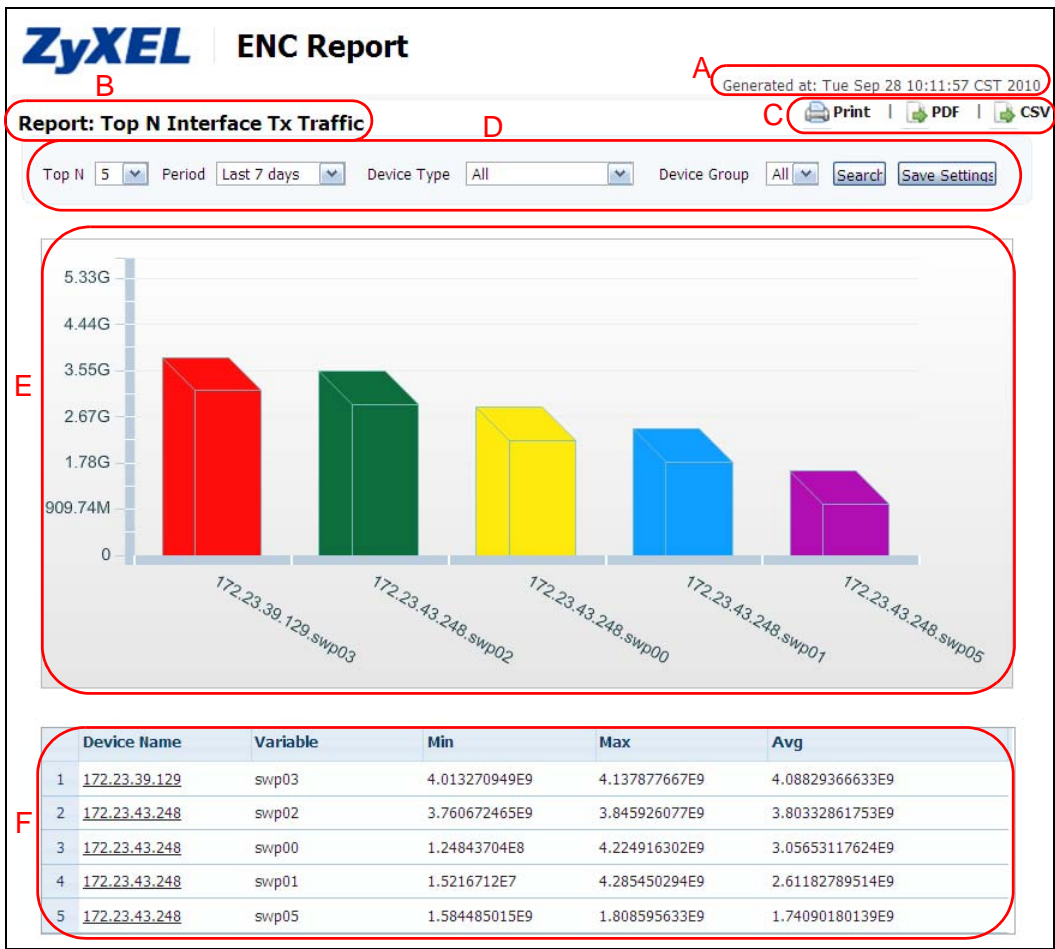
Report Name:

Descriptions:

7.2.3 A Report Example

You can view a report by clicking the report name in the **Report > Reports** screen. This section shows you an example about top 5 CPU utilization report.

Figure 138 A Report Example



- **A** - This shows when this report was generated.
- **B** - This shows the name of this report.
- **C** - Click **Print** to print this report. Click **PDF** or **CSV** to export the report to a PDF or CSV file.
- **D** - Use this section to modify the report settings. Click **Search** to generate the report based on the set criteria. Click **Save Settings** to save the changes and update the report in this screen.
- **E** - This section may show a line or bar chart depending on the selected report. The X-axis of the graph is the devices' parameters depending on the report type you selected. The Y-axis is the statistics of the parameters.
- **F** - This shows the statistics in a table. The columns vary depending on the report types you selected.

7.3 Scheduled Report Summary Screen

Click **Report > Schedule Report** to view the list of existing scheduled reports. Use the **Add** button to create new reports.

Figure 139 Report > Schedule Report

The screenshot shows a web interface titled 'Schedule Report'. At the top, there are three buttons: 'Add' (with a green plus icon), 'Edit' (with a yellow pencil icon), and 'Remove' (with a red trash icon). Below these is a table with four columns: 'Name', 'Type', 'Subject', and 'Export File Formats'. The first row of the table contains the following data: a checkbox, 'Daily-Report-Ex', 'daily', 'ENC Daily Report', and '[csv]'. At the bottom of the table, there is a pagination bar showing 'Page 1 of 1' and a 'View 1 - 1 of 1' link.

	Name	Type	Subject	Export File Formats
1	<input type="checkbox"/> Daily-Report-Ex	daily	ENC Daily Report	[csv]

Each field is described in the following table.

Table 79 Report > Schedule Report

LABEL	DESCRIPTION
Add	Click this to create a daily, weekly or monthly report in a time interval.
Edit	Click this to modify an existing scheduled report in a time interval.
Remove	Click this to delete the selected scheduled report.
check box	Select the check box, and click Edit to modify the settings or Remove to delete the scheduled report. Select or clear the check box at the table heading line to select or clear all check boxes in this column. Clear it to have all the check boxes being cleared.
Name	This field displays the name of the scheduled report. Click it and Edit to edit the scheduled report next to it. The Customize Scheduled Report screen appears. Otherwise, this field is a sequential value, and it is not associated with a specific scheduled report. For example, if you delete a scheduled report, the remaining scheduled reports are re-numbered.
Type	This field displays whether this is a daily, weekly or monthly report.
Subject	This field displays the subject line in the e-mail message the ENC sends.
Export File Formats	This field displays the format(s) of files that the ENC will send through e-mail when the scheduled report is generated.

7.4 Schedule Report Add/Edit Screen

Click **Add or Edit in the Report > Schedule Report** screen to configure a scheduled report. You can check whether the schedule report is successfully generated or not later in the **Maintenance > Log** screen.

Figure 140 Report > Schedule Report > Summary > Add

Each field is described in the following table.

Table 80 Report > Schedule Report > Add

LABEL	DESCRIPTION
Name	Enter the name of the schedule report. Only numbers (0-9), letters (a-z, A-Z), hyphen (-) and the underscore (_) are allowed. Spaces are not allowed.
Type	Select how often (daily , weekly or monthly) to generate the schedule report.

Table 80 Report > Schedule Report > Add

LABEL	DESCRIPTION
Send Time	<p>Select when to start generating the report. The ENC sends the report after it finishes generating it. The report generation time depends on the amount of information in the report. Having the ENC generate too many reports at the same time can affect performance. It is recommended that you vary the times for your reports.</p> <p>For a daily report, select the time (hour:minute) to generate the report.</p> <p>For a weekly report, select which week day (Sunday~Saturday) and time (hour:minute) to generate the report.</p> <p>For a weekly report, select which date (1~31) and time (hour:minute) per month to generate the report.</p>
Receiver Email Address List	<p>Enter a valid e-mail address to which the ENC sends the report and click Add to add it in the list below. You can enter as many valid e-mail addresses as you want. Select one or multiple entries and click Remove to delete them from the list. The ENC provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.</p>
Subject	<p>Enter the subject line in the e-mail message the ENC sends. Only numbers (0-9), letters (a-z, A-Z), characters ('+', '/', '=', '?', '!', '*', '#', '@', '\$', '_', '%', '-'), carriage returns (\n), line breaks (\r) and spaces are allowed.</p> <p>The ENC provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.</p>
Export File Formats	<p>Select the format(s) of the report(s) that you see. The available options are CSV, PDF and HTML. The ENC will send you an e-mail with a URL (Uniform Resource Locator). Click the URL to see the report(s).</p>
Available Items	<p>Select the reports to include in this schedule report and use the >> arrow to move them to the Selected Reports list. You can configure more reports in Report > Reports > Customized Reports.</p>
Selected Items	<p>This section lists the reports included in this schedule report. Select a report and click the << arrow if you want to remove it from the schedule report.</p>
Cancel	<p>Click this to discard the changes and exit this screen.</p>
Ok	<p>Click this to save your settings and close the screen.</p>

Application

8.1 Overview

Use the sub-menus under **Application** to look at and configure specific functions such as RMON (Remote Network Monitor), VLAN, port management and Wireless Access Point settings for ZyXEL Ethernet Switches.

8.1.1 What You Can Do in This Chapter

- Use the **Application > RMON** screens (see [Section 8.3 on page 190](#)) to configure RMON statistics, history, event and alarm settings.
- Use the **Application > VLAN Management** screens (see [Section 8.6 on page 207](#)) to configure VLAN settings for specific devices.
- Use the **Application > Port Management** screens (see [Section 8.7 on page 218](#)) to configure port management basic, bandwidth control, broadcast storm control, security, authentication settings for specific devices.
- Use the **Application > AP Manager** screen (see [Section 8.12 on page 234](#)) to configure wireless settings for specific devices which supports wireless access point function.

8.2 RMON Introduction

Similar to SNMP, RMON (Remote Network Monitor) allows you to gather and monitor network traffic.

Both SNMP and RMON use an agent, known as a probe, which are software processes running on network devices to collect information about network traffic and store it in a local MIB (Management Information Base). With SNMP, a network manager has to constantly poll the agent to obtain MIB information. With RMON, the probe is located on a remote device (ZyXEL Ethernet Switches), so a network manager (the ENC) does not need to constantly poll the probe for information. The probe communicates with the network manager via SNMP.

RMON groups contain detailed information about specific activities. The following table describes the RMON groups that the ZyXEL Ethernet Switches support.

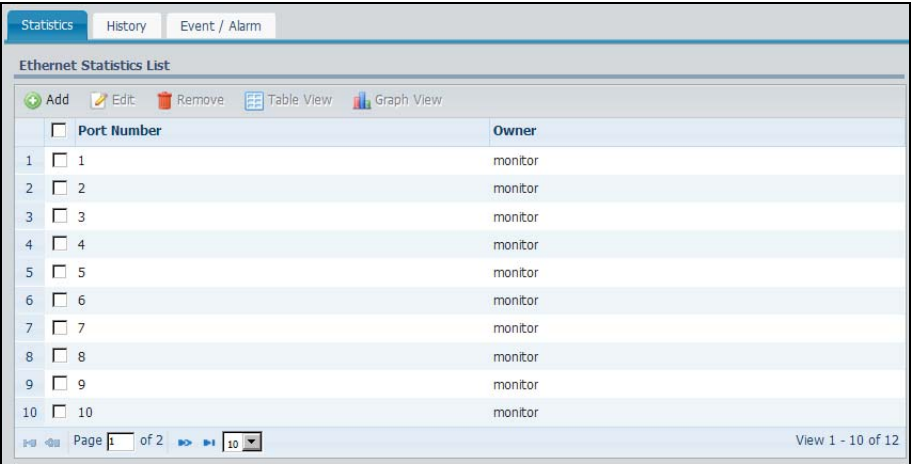
Table 81 Supported RMON Groups

GROUP	DESCRIPTION
Statistics	Defines event generation and resulting actions to be taken based on an alarm.
History	Records network traffic information on a specified Ethernet port.
Event/Alarm	Provides alerts when configured alarm conditions are met.

8.3 Statistics

Use this screen to look at network statistics on a selected device's ports. To open this screen, click a device that supports this feature in the OTV, Device View or Group View panel and click **Application > RMON > Statistics**. Then, select one or more ports or interfaces for which you want to view network statistics.

Figure 140 RMON > Statistics



The screenshot shows the 'RMON > Statistics' screen. At the top, there are tabs for 'Statistics', 'History', and 'Event / Alarm'. Below the tabs is the title 'Ethernet Statistics List'. Under the title, there are icons for 'Add', 'Edit', 'Remove', 'Table View', and 'Graph View'. The main area contains a table with two columns: 'Port Number' and 'Owner'. The table lists 10 ports, all owned by 'monitor'. At the bottom, there is a pagination bar showing 'Page 1 of 2' and 'View 1 - 10 of 12'.

	Port Number	Owner
1	<input type="checkbox"/> 1	monitor
2	<input type="checkbox"/> 2	monitor
3	<input type="checkbox"/> 3	monitor
4	<input type="checkbox"/> 4	monitor
5	<input type="checkbox"/> 5	monitor
6	<input type="checkbox"/> 6	monitor
7	<input type="checkbox"/> 7	monitor
8	<input type="checkbox"/> 8	monitor
9	<input type="checkbox"/> 9	monitor
10	<input type="checkbox"/> 10	monitor

The following table describes the labels in this screen.

Table 82 RMON > Statistics

LABEL	DESCRIPTION
Add	Click this to create an entry. Note: At the time of writing, this function is only available for ZyXEL Ethernet Switches using 3.90 firmware version.
Edit	Select an entry in the table and click this to modify it.
Remove	Select an entry in the table and click this to delete it.
Table View	Select one or more ports or interfaces in the table and click this to display the network statistics as a table.
Graph View	Select one port or interface in the table and click this to display the network statistics as a graph.
check box	Select the check box of an entry and click Edit , Remove , Table View or Graph View to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Port Number	This field displays the number of the port or interface on the selected device.
Owner	This field displays the application name that created this entry.

8.3.1 Add/Edit an RMON Port

If you want to view network statistics on one port or interface but the port is not in the **Ethernet Statistics List** in the **Application > RMON > Statistics** screen, click **Add** to add the port or interface. To do this, select a device that supports this feature in the OTV, Device View or Group View panel and click **Add** in the **Application > RMON > Statistics** screen.

You can also change the RMON owner setting for the port or interface by selecting it and then clicking **Edit** in the **Application > RMON > Statistics** screen.

Note: At the time of writing, this screen is only available for ZyXEL Ethernet Switches using 3.90 version firmware.

Figure 141 RMON > Statistics > Add/Edit

The following table describes the labels in this screen.

Table 83 RMON > Statistics > Add/Edit

LABEL	DESCRIPTION
Port Number	Enter the number of one port or interface to add to the ENC for viewing network statistics. This field displays the port's number and is read-only when you are editing a port statistic entry.
Owner	Enter a descriptive name of the application that creates this entry. You can use 1-31 printable ASCII characters. Spaces are allowed.
Cancel	Click this to discard all changes and close the screen.
Ok	Click this to save the settings and close this screen.

8.3.2 Viewing the Table

This screen displays network statistics for the selected port(s) or interface(s) as a table. After selecting the data source(s) you wish to display, click **Table View** on the **Application > RMON > Statistics** screen to open this screen.

Figure 142 RMON > Statistics > Table View

	Port Number	Octets	Total Packets	Broadcast Packets	Multicast Packets	Unicast Packets	U
1	6	645963257	6813328	2105017	4640592	67719	
2	8	0	0	0	0	0	
3	10	1609863972	21647380	2650594	6037526	12959260	

The following table describes the labels in this screen.

Table 84 RMON > Statistics > Table View

LABEL	DESCRIPTION
Device IP	This field displays the IP address of the selected device.
Port Number	This field displays the number of the selected port(s) or interface(s).
Polling Interval	Enter the number of seconds (5~3600) between data samplings the ENC retrieves from the selected device. Click Start Polling to have the ENC start to retrieve data from the device or Stop Polling to stop it. You have to stop pollings first if you want to change the settings for graphic display.
Delta Value	Select this to use Delta value as the method of obtaining the sample value. Clear this to use Absolute value as the method instead. Delta means the value is from the data sampled in each configured time interval. Absolute means the sampling value is accumulated since it started.
	The first column displays the index number of a data sampling. The number also indicates the order in which the port or interface (within all the selected ports or interfaces) is sampled.
Port Number	This is the number of the port or interface from which the ENC polled the data.
Octets	Select this to display the total number of octets received/transmitted on the port(s).
Total Packets	Select this to display the total number of all good packets received/transmitted on the port(s).
Broadcast Packets	This is the total number of good broadcast packets received/transmitted on the port(s).
Multicast Packets	This is the total number of good multicast packets received/transmitted on the port(s).
Unicast Packets	This is display the total number of good unicast packets received/transmitted on the port(s).
Undersize Packets	This is display the number of packets dropped by the port(s) because they were less than 64 octets long, and contained a valid FCS.
Fragments	This is display the number of packets received/transmitted on the port(s) because they were less than 64 octets long, and contained an invalid FCS, including non-integral and integral lengths.
Oversize Packets	This is display the number of packets dropped by the port(s) because they were longer than 1518 octets and contained an invalid FCS, including alignment errors in the graph of this section.
Jabbers	This is display the number of packets received/transmitted on the port(s) because they were longer than 1518 octets (non VLAN) or 1522 octets (VLAN) and contained an invalid FCS, including alignment errors.
64 Octets	This is the number of packets (including bad packets) received that were 64 octets in length in the graph of this section.
65~127 Octets	This is the number of packets (including bad packets) received that were between 65 and 127 octets in length in the graph of this section.
128~255 Octets	This is the number of packets (including bad packets) received that were between 128 and 255 octets in length in the graph of this section.
256~511 Octets	This is the number of packets (including bad packets) received that were between 256 and 511 octets in length in the graph of this section.
512~1023 Octets	This is the number of packets (including bad packets) received that were between 512 and 1023 octets in length in the graph of this section.
1024~1518 Octets	This is 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 in the graph of this section.

Table 84 RMON > Statistics > Table View

LABEL	DESCRIPTION
CRC Align Error	This is the number of frames received/transmitted on the port(s) because they were 64 to 1518 (non VLAN) or 1522 (VLAN) octets long but contained an invalid FCS and a non-integral number of octets.
Collisions	This is the number of packets for which transmission failed due to collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Drop Events	This is the total number of packets that were dropped by the port(s).
Close	Click Close to exit the screen.

8.3.3 Viewing the Graph

This screen displays a selected port or interface's network statistics as a graph. After selecting a port or an interface you wish to display, click **Graph View** on the **Application > RMON > Statistics** screen. Select the graph type and instances to display and click **Start Polling** to display the screen.

Note: The graph may take a few moments to display.

Figure 143 RMON > Statistics > Graph View



The following table describes the labels in this screen.

Table 85 RMON > Statistics > Graph View

LABEL	DESCRIPTION
Device IP	This field displays the IP address of the selected device.
Port Number	This field displays the number of the selected port or interface.

Table 85 RMON > Statistics > Graph View

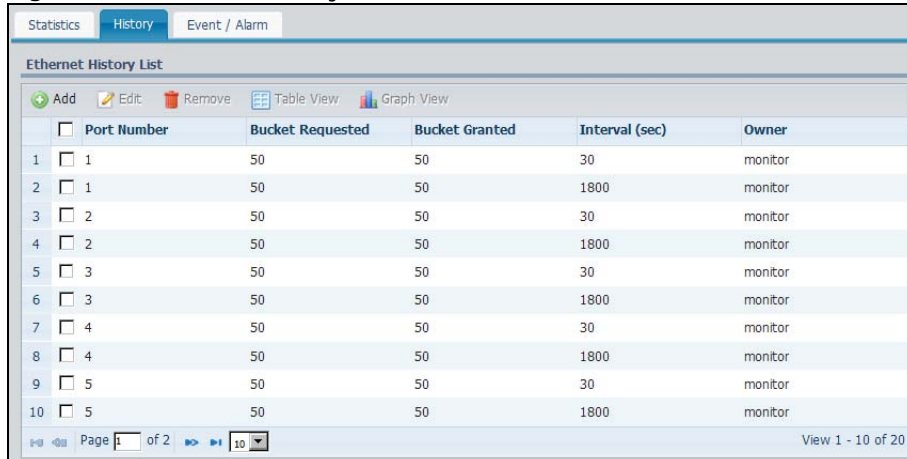
LABEL	DESCRIPTION
Polling Interval	Enter the number of seconds (5~3600) between data samplings the ENC retrieves from the selected device. Click Start Polling to have the ENC start to retrieve data from the device or Stop Polling to stop it. You have to stop pollings first if you want to change the settings for graphic display.
Graph Type	Select whether to display network statistics as a Line , Bar , or Pie graph.
Delta Value	Select this to use Delta value as the method of obtaining the sample value. Clear this to use Absolute value as the method instead. Delta means the value is from the data sampled in each configured time interval. Absolute means the sampling value is accumulated since it started.
View Octets	
Octets	Select this to display the total number of octets received/transmitted on the port(s).
View Packets Data	
Total Packets	Select this to display the total number of all good packets received/transmitted on the port(s).
Drop Event	Select this to display the total number of packets that were dropped by the port(s).
Broadcast Packets	Select this to display the total number of good broadcast packets received/transmitted on the port(s).
Multicast Packets	Select this to display the total number of good multicast packets received/transmitted on the port(s).
Unicast Packets	Select this to display the total number of good unicast packets received/transmitted on the port(s).
Undersize Packets	Select this to display the number of packets dropped by the port(s) because they were less than 64 octets long, and contained a valid FCS.
Fragments	Select this to display the number of packets received/transmitted on the port(s) because they were less than 64 octets long, and contained an invalid FCS, including non-integral and integral lengths.
Oversize Packets	Select this to display the number of packets dropped by the port(s) because they were longer than 1518 octets and contained an invalid FCS, including alignment errors in the graph of this section.
Jabbers	Select this to display the number of packets received/transmitted on the port(s) because they were longer than 1518 octets (non VLAN) or 1522 octets (VLAN) and contained an invalid FCS, including alignment errors.
Collisions	Select this to display the number of packets for which transmission failed due to collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
CRC Align Error	Select this to display the number of frames received/transmitted on the port(s) because they were 64 to 1518 (non VLAN) or 1522 (VLAN) octets long but contained an invalid FCS and a non-integral number of octets.
View Packet Size Data	
Packets of 64 Octets	Select this to display the number of packets (including bad packets) received that were 64 octets in length in the graph of this section.
Packets of 65 ~ 127 Octets	Select this to display the number of packets (including bad packets) received that were between 65 and 127 octets in length in the graph of this section.
Packets of 128 ~ 255 Octets	Select this to display the number of packets (including bad packets) received that were between 128 and 255 octets in length in the graph of this section.
Packets of 256 ~ 511 Octets	Select this to display the number of packets (including bad packets) received that were between 256 and 511 octets in length in the graph of this section.

Table 85 RMON > Statistics > Graph View

LABEL	DESCRIPTION
Packets of 512 ~ 1023 Octets	Select this to display the number of packets (including bad packets) received that were between 512 and 1023 octets in length in the graph of this section.
Packets of 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 in the graph of this section.
Close	Click Close to exit the screen.

8.4 History Config

Use this screen to view historical (accumulated) remote network monitoring (RMON) Ethernet statistics on a device's port. To open this screen, select a device in the OTV, Device View or Group View panel, and click **Application > RMON > History**.

Figure 144 RMON > History


The screenshot shows the 'Ethernet History List' screen. At the top, there are tabs for 'Statistics', 'History' (selected), and 'Event / Alarm'. Below the tabs are icons for 'Add', 'Edit', 'Remove', 'Table View', and 'Graph View'. The main area contains a table with the following data:

	<input type="checkbox"/>	Port Number	Bucket Requested	Bucket Granted	Interval (sec)	Owner
1	<input type="checkbox"/>	1	50	50	30	monitor
2	<input type="checkbox"/>	1	50	50	1800	monitor
3	<input type="checkbox"/>	2	50	50	30	monitor
4	<input type="checkbox"/>	2	50	50	1800	monitor
5	<input type="checkbox"/>	3	50	50	30	monitor
6	<input type="checkbox"/>	3	50	50	1800	monitor
7	<input type="checkbox"/>	4	50	50	30	monitor
8	<input type="checkbox"/>	4	50	50	1800	monitor
9	<input type="checkbox"/>	5	50	50	30	monitor
10	<input type="checkbox"/>	5	50	50	1800	monitor

At the bottom, there is a pagination bar showing 'Page 1 of 2' and a 'View 1 - 10 of 20' indicator.

The following table describes the labels in this screen.

Table 86 RMON > History

LABEL	DESCRIPTION
Add	Click this to add an entry.
Edit	Select an entry in the table and click this to modify it.
Remove	Select an entry in the table and click this to delete it.
Table View	Select one port or interface in the table and click this to display the accumulated network statistics as a table.
Graph View	Select one port or interface in the table and click this to display the accumulated network statistics as a graph.
check box	Select the check box of an entry and click Duplicate , Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Status	This field displays whether the port or interface is collecting data for statistics (Active) or not (Inactive).

Table 86 RMON > History (continued)

LABEL	DESCRIPTION
Port Number	This field displays the number of the port or interface on the selected device, which the ENC will poll for data.
Bucket Requested	This field displays the number of data samplings the network manager requests the probe to store.
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.
Owner	This field displays the application that created this entry.

8.4.1 Configuring an RMON History Entry

To configure a new RMON history entry, click **Add** in the **Application > RMON > History** screen.

To change the settings of a selected RMON history entry, click **Edit** in the screen.

Figure 145 RMON > History > Add/Edit

The following table describes the labels in this screen.

Table 87 RMON > History > Add/Edit

LABEL	DESCRIPTION
Port number	Select a port or an interface of the selected device that the ENC polls for data. The probe sends data from this port.
Bucket Requested	Specify the number of data samplings the ENC requests the probe to store.
Interval	Enter the time (in seconds) between data samplings.
owner	Enter a descriptive name of the application that creates this entry. You can use 1-31 printable characters. Spaces are allowed.
Cancel	Click this to discard all changes and close the screen.
OK	Click this to save the settings and close this screen.

8.4.2 Viewing the Table

Use this screen to display accumulated network statistics collected by the selected port or interface. After selecting the port or interface you wish to display, click **Table View** on the **Application >**

RMON > History screen. Click **Get/Refresh** to have the ENC retrieve statistics from the device and display.

Figure 146 RMON > History > Table View

	Control Index	Port Number	Table Index	Sampled Time	Dropped Events	Octets	Total Packets	Broadcast
1	3	2	481045	2010-09-15 15:37:17	0	83396352	402175	
2	3	2	481046	2010-09-15 15:37:47	0	83396352	402175	
3	3	2	481047	2010-09-15 15:38:18	0	83396352	402175	
4	3	2	481048	2010-09-15 15:38:48	0	83396352	402175	

The following table describes the labels in this screen.

Table 88 RMON > History > Table View

LABEL	DESCRIPTION
Device IP	This field displays the IP address of the selected device.
Port Number	This field displays the number of the selected port or interface.
Get/Refresh	Click this to update the statistics in this screen.
Control Index	This field displays the index number of a set of data samples. The Control Index and Table Index identifies a unique data sample. You may need to use them as a key to retrieve the data sample's statistics in a MIB browser.
Port Number	This is the number of a port or an interface from which the ENC polled the data.
Table Index	This field displays the index number of a data sample. The Control Index and Table Index identifies a unique data sample. You may need to use them as a key to retrieve the data sample's statistics in a MIB browser.
Sampled Time	This field displays the data sampling time.
Dropped Events	This is the total number of packets that were dropped by the port or interface since the last sample time.
Octets	This is the total number of octets received/transmitted on the port or interface since the last sample time.
Total Packets	This is the total number of all good packets received/transmitted on the port or interface since the last sample time.
Broadcast Packets	This is the total number of good broadcast packets received/transmitted on the port or interface since the last sample time.
Multicast Packets	This is the total number of good multicast packets received/transmitted on the port or interface since the last sample time.
Unicast Packets	This is the total number of good unicast packets received/transmitted on the port(s) since the last sample time.
CRC Align Errors	This is the number of frames received/transmitted on the port(s) because they were 64 to 1518 (non VLAN) or 1522 (VLAN) octets long but contained an invalid FCS and a non-integral number of octets since the last sample time.
Undersize Packets	This is the number of packets dropped by the port(s) because they were less than 64 octets long, and contained a valid FCS since the last sample time.
Oversize Packets	This is the number of packets dropped by the port(s) because they were longer than 1518 octets and contained an invalid FCS, including alignment errors in the graph of this section since the last sample time.

Table 88 RMON > History > Table View

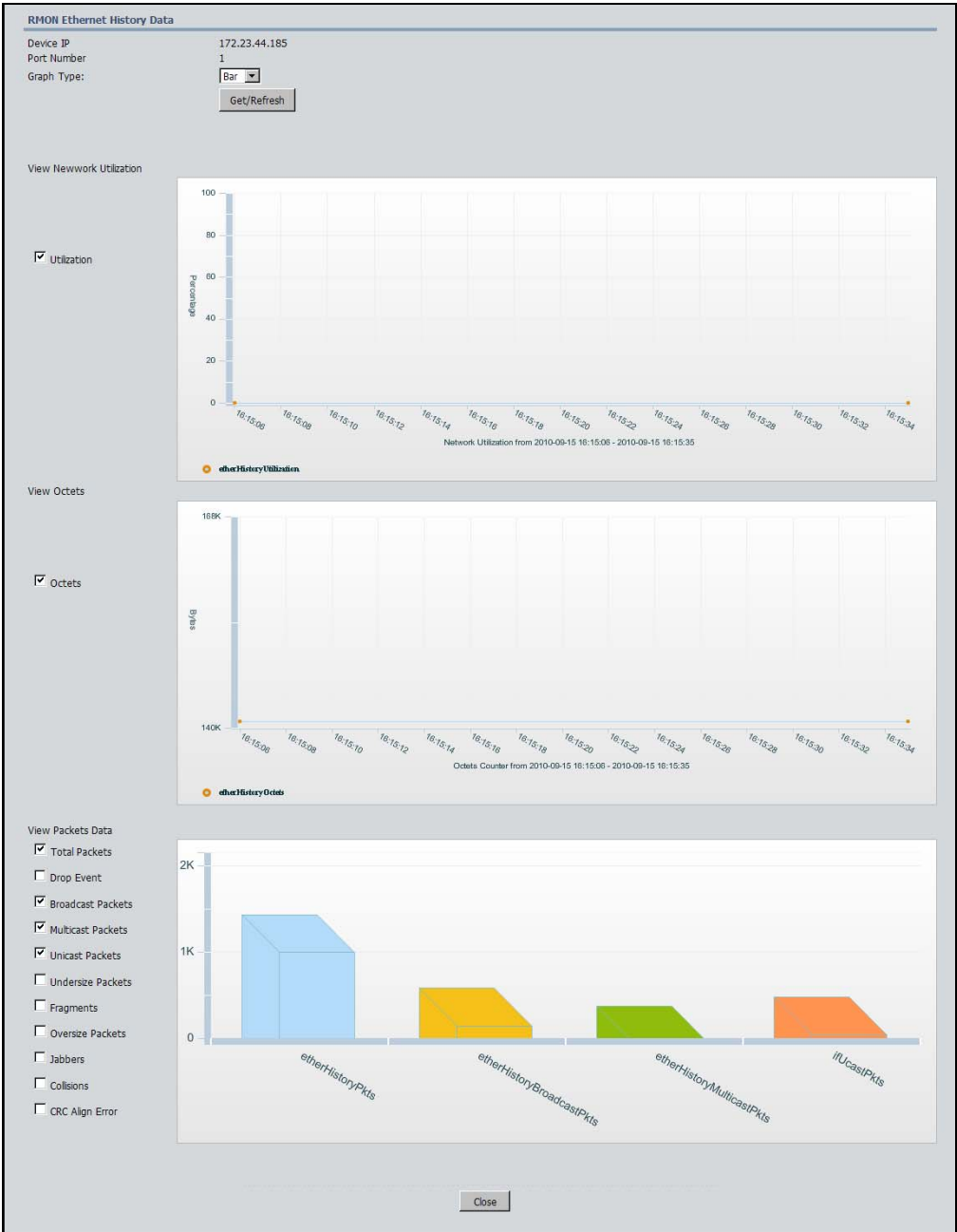
LABEL	DESCRIPTION
Fragments	This is the number of packets received/transmitted on the port or interface because they were less than 64 octets long, and contained an invalid FCS, including non-integral and integral lengths since the last sample time.
Jabbers	This is the number of packets received/transmitted on the port or interface because they were longer than 1518 octets (non VLAN) or 1522 octets (VLAN) and contained an invalid FCS, including alignment errors since the last sample time.
Collisions	This is the number of packets for which transmission failed due to collisions since the last sample time. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Utilization (%)	This field displays the mean physical layer network utilization (in hundredths of a percent) on this port or interface during this sampling interval.
Close	Click Close to exit the screen.

8.4.3 Viewing the Graph

This screen displays the accumulated network statistics on the selected port as a graph. After selecting a port or an interface you wish to display, click **Graph View** on the **Application > RMON > History** screen. Select the graph type and instances to display and click **Start Polling**. The screen appears as shown next.

Note: The graph may take a few moments to display.

Figure 147 RMON > History > Graph View



The following table describes the labels in this screen.

Table 89 RMON > History > Graph View

LABEL	DESCRIPTION
Device IP	This field displays the IP address of the device selected in the previous screen.
Port Number	This field displays the number of the selected port or interface.
Graph Type	Select whether to display the traffic statistics as a Line , Bar , or Pie graph.
Get/Refresh	Click this to update the statistics in this screen.

Table 89 RMON > History > Graph View

LABEL	DESCRIPTION
View Network Utilization	
Utilization	Select this to display the network utilization status in percentage (%) collected by the port.
View Octets	
Octets	Select this to display the total number of octets received/transmitted on the port.
View Packets Data	
Total Packets	Select this to display the total number of all good packets received/transmitted on the port.
Drop Event	Select this to display the total number of packets that were dropped by the port.
Broadcast Packets	Select this to display the total number of good broadcast packets received/transmitted on the port.
Multicast Packets	Select this to display the total number of good multicast packets received/transmitted on the port.
Unicast Packets	Select this to display the total number of good unicast packets received/transmitted on the port.
Undersize Packets	Select this to display the number of packets dropped by the port because they were less than 64 octets long, and contained a valid FCS.
Fragments	Select this to display the number of packets received/transmitted on the port because they were less than 64 octets long, and contained an invalid FCS, including non-integral and integral lengths.
Oversize Packets	Select this to display the number of packets dropped by the port because they were longer than 1518 octets and contained an invalid FCS, including alignment errors in the graph of this section.
Jabbers	Select this to display the number of packets received/transmitted on the port because they were longer than 1518 octets (non VLAN) or 1522 octets (VLAN) and contained an invalid FCS, including alignment errors.
Collisions	Select this to display the number of packets for which transmission failed due to collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
CRC Align Error	Select this to display the number of frames received/transmitted on the port because they were 64 to 1518 (non VLAN) or 1522 (VLAN) octets long but contained an invalid FCS and a non-integral number of octets.
Close	Click Close to exit the screen.

8.5 Event/Alarm

Use this screen to configure events and alarms that occur when the sampled data exceeds the specified threshold. To open this screen, click a device in the OTV, Device View or Group View panel, and click **Application > RMON > Event /Alarm**.

To configure an alarm, you have to first configure at least one event in this screen. An event here defines:

- the action the device takes when an alarm is triggered,
- the SNMP Get/Set community to communicate with the device,
- and the application name that creates the event entry.

After you configure the event, you can then create an alarm and associate it with the event. An alarm here defines:

- which port or interface on the port will generate this alarm,
- a variable that you wish to monitor,
- which method to use for collecting data samplings,
- the falling and rising threshold values that determine when to trigger this alarm,
- and the application name that creates this alarm entry.

Figure 148 RMON > Event / Alarm

The screenshot displays the 'Event / Alarm' configuration page. It features two main sections: 'Event List' and 'Alarm List'. The 'Event List' section contains a table with columns: Type, Last Event Sent, Community, Description, and Owner. It lists two events: 'LOG & TRAP' and 'TRAP', both with a community of 'public' and owner of 'monitor'. The 'Alarm List' section contains a table with columns: Interval (sec), Sample Type, Startup Alarm, Port Number, Variable, and Owner. It lists one alarm: '30' seconds interval, 'Delta' sample type, 'Rising & Falling Alarm' startup, port '1', variable 'ifInOctets.1', and owner 'monitor'. Both sections include 'Add', 'Edit', and 'Remove' buttons. The 'Event List' also has a 'View Log' button. The 'Alarm List' has a 'Parameter' button. Both sections include pagination controls showing 'Page 1 of 1' and 'View 1 - 2 of 2' for the event list, and 'View 1 - 1 of 1' for the alarm list.

The following table describes the labels in this screen.

Table 90 RMON > Event / Alarm

LABEL	DESCRIPTION
Event List	
Add	Click this to create a new event.
Edit	Select an entry in the table and click this to modify it.
Remove	Select an entry in the table and click this to delete it.
check box	Select the check box of an entry and click Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Type	<p>This field displays the alarm type (NONE, LOG, TRAP or LOG & TRAP).</p> <p>LOG - The device generates a log when an associated alarm occurs.</p> <p>TRAP - The device sends a trap when an associated alarm occurs.</p> <p>NONE - The device does not generate any logs or traps when an associated alarm occurs.</p> <p>LOG & TRAP - The device generates a log and sends a trap when an associated alarm occurs.</p>
Last Event Send	This field displays the date and time the event was last generated and sent from the device to the ENC.
Community	This field displays the SNMP Get/Set community setting.
Description	This field displays further information about the event.
Owner	This field displays the name of the application that created this event.
Alarm List	
Add	Click this to create a new alarm.

Table 90 RMON > Event / Alarm (continued)

LABEL	DESCRIPTION
Edit	Select an entry in the Alarm List table and click this to modify it.
Remove	Select one or more entries in the Alarm List table and click this to delete them.
View Log	Select an entry in the Alarm List table and click this to display the falling and rising thresholds as a table.
Parameter	Click this to view a list of threshold parameters and their settings.
check box	Select the check box of an entry and click Edit , Remove , View Log or Parameter to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Interval (sec)	This field displays how often (in seconds) the ENC checks whether the parameter's value is within the set thresholds or not.
Sample Type	This field displays the method of obtaining the sample value (Absolute or Delta).
Startup Alarm	This field displays the alarm type (Rising , Falling , Rising & Falling Alarm) that can be sent when this alarm is first activated.
Port Number	This field displays the number of a port or an interface to which this alarm is sent.
Variable	This field displays the name of the MIB field whose data is to be sampled.
Owner	This field displays the name of the application that created this entry.

8.5.1 Configuring an Event

Use this screen to configure an event. To open this screen, click **Add** or select an entry and then click **Edit** in the **Event List** section of the **Application > RMON > Event / Alarm** screen.

Figure 149 RMON > Event / Alarm > Event List Add/Edit

The following table describes the labels in this screen.

Table 91 RMON > Event / Alarm > Event List Add/Edit

LABEL	DESCRIPTION
Type	<p>Select an event type.</p> <p>Select LOG to generate a log when an associated alarm is generated.</p> <p>Select TRAP to generate a trap when an associated alarm is generated.</p> <p>Select NONE to not generate a log or trap when an associated alarm is generated.</p> <p>Select LOG & TRAP to generate a log entry and trap when an associated alarm is generated.</p>
Community	This field displays the SNMP Get/Set community setting. You can use 1-31 printable ASCII characters. Spaces are allowed.

Table 91 RMON > Event / Alarm > Event List Add/Edit (continued)

LABEL	DESCRIPTION
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.
Cancel	Click this to save the settings and close this screen.
Ok	Click this to discard all changes and close the screen.

8.5.2 View Alarm Logs

Use this screen to configure events and alarms that occur when the sampled data exceeds the specified threshold. To open this screen, select an entry in the **Alarm List** and click **View Log** in the **Application > RMON > Event /Alarm** screen.

Figure 150 RMON > Event / Alarm > View Log

RMON Event Log					
<div>Statistics History Event / Alarm</div>					
View Log					
Event Index	Alarm Type	Log Index	Last Send Time	Variable	Description
1	FALLING	1765	2010-02-01 11:28:45	ifInOctets.12	1.3.6.1.2.1.2.2.1.10.12 [delta = 362, Falling Threshold = 500, interval = 30] [alarmIndex.1] [log-and-trap] ""
1	RISING	1766	2010-02-01 11:30:45	ifInOctets.12	1.3.6.1.2.1.2.2.1.10.12 [delta = 7631, Rising Threshold = 1000, interval = 30] [alarmIndex.1] [log-and-trap] ""
1	FALLING	1767	2010-02-01 11:31:15	ifInOctets.12	1.3.6.1.2.1.2.2.1.10.12 [delta = 0, Falling Threshold = 500, interval = 30] [alarmIndex.1] [log-and-trap] ""
1	FALLING	1861	2010-02-01 15:52:15	ifInOctets.12	1.3.6.1.2.1.2.2.1.10.12 [delta = 175, Falling Threshold = 500, interval = 30] [alarmIndex.1] [log-and-trap] ""
1	RISING	1862	2010-02-01 15:54:15	ifInOctets.12	1.3.6.1.2.1.2.2.1.10.12 [delta = 7597, Rising Threshold = 1000, interval = 30] [alarmIndex.1] [log-and-trap] ""
1	FALLING	1863	2010-02-01 15:56:45	ifInOctets.12	1.3.6.1.2.1.2.2.1.10.12 [delta = 175, Falling Threshold = 500, interval = 30] [alarmIndex.1] [log-and-trap] ""
1	RISING	1864	2010-02-01 15:57:45	ifInOctets.12	1.3.6.1.2.1.2.2.1.10.12 [delta = 7429, Rising Threshold = 1000, interval = 30] [alarmIndex.1] [log-and-trap] ""

The following table describes the labels in this screen.

Table 92 RMON > Event / Alarm > View Log

LABEL	DESCRIPTION
Event Index	This field displays the associated event's index number for this alarm log.
Alarm Type	This field displays whether this alarm log was generated because the value was higher than the RISING threshold or lower than the FALLING threshold.
Log Index	This field displays the index number of the alarm log.
Last Send Time	This field displays the date and time the alarm log was generated by the device.

Table 92 RMON > Event / Alarm > View Log (continued)

LABEL	DESCRIPTION
Variable	This field displays the name of the MIB field whose data was sampled.
Description	<p>This field displays:</p> <ul style="list-style-type: none"> the related object ID (for example, 1.3.6.1.2.1.2.2.1.10.12), the data collection method and the data sampling's index number (for example, delta=352), the name and the value of the threshold (for example, FALLING=50), the number of seconds between two data samplings (for example, interval=30), the index number of the alarm log (for example, alarmindex.1), the action(s) the device took when this alarm occurs (for example, log-and-trap).
Back	Click this to close this screen and go back to the previous screen.

8.5.3 Alarm Parameters

Use this screen to view the thresholds for the selected alarm and the associated event settings. To open this screen, select an alarm entry in the **Alarm List** and click **Parameter** in the **Application > RMON > Event / Alarm** screen.

Figure 151 RMON > Event / Alarm > Parameter

Condition	Threshold	Event Index	Event Status	Event Type	Event Commun	Event Owner	Event Description
1 Rising	1000000	1	💡	LOG & TRAP	public	monitor	
2 Falling	0	1	💡	LOG & TRAP	public	monitor	

The following table describes the labels in this screen.

Table 93 RMON > Event / Alarm > Parameter

LABEL	DESCRIPTION
Condition	This field displays whether this is about the Rising or Falling threshold.
Threshold	This field displays the threshold's value.
Event Index	This field displays the associated event's index number for this alarm log.
Event Status	This field displays whether the associated event is currently activated or not.
Event Type	This field displays the action(s) the device should take when the selected alarm is generated.
Event Community	This field displays the SNMP Get/Set community the ENC uses to communicate with the device.
Event Owner	This field displays the application name that created the associated event.
Event Description	This field displays the description about the associated event.
Back	Click this to close this screen and go back to the previous screen.

8.5.4 Configuring an Alarm

To create a new RMON alarm, click **Add** in the **Alarm List** of the **Application > RMON > Event / Alarm** screen.

To change the settings of a selected RMON alarm, click **Edit** instead in the **Event / alarm** screen.

Figure 152 RMON > Event / Alarm > Add

The following table describes the labels in this screen.

Table 94 RMON > Alarm Config > New

LABEL	DESCRIPTION
Port Number	Select which port or interface whose data will be sampled.
Variable	Select the type of data to be sampled.
Interval	Specify the time between data samplings.
Sample Type	Select the method of obtaining the sample value. Absolute: means the sampling value is accumulated since it started. Delta: means the value is from the data sampled in each configured time interval.
Startup Alarm	Select the startup alarm type. Rising Alarm: means the probe triggers an alarm when the value is greater or equal to the rising threshold. Falling Alarm: means the probe triggers an alarm when the value is less than or equal to the falling threshold. Rising & Falling Alarm: means Rising or Falling. That is, the probe triggers an alarm when either one of the above cases occurs.
Owner	Enter a descriptive name of the application that creates this entry. You can use 1-31 printable ASCII characters. Spaces are allowed.
Rising Condition	

Table 94 RMON > Alarm Config > New

LABEL	DESCRIPTION
Threshold	Specify a rising threshold (between 0 and 2147483647). When a value is greater or equal to this threshold, the probe triggers an alarm.
Event Index	Select an index number of a rising event.
Falling Condition	
Threshold	Specify the falling threshold (between 0 and 2147483647). When a value is less than or equal to this threshold, the probe triggers an alarm.
Event Index	Select an index number of a falling event.
Cancel	Click this to discard all changes and close the screen.
OK	Click this to save the settings and close the screen.

8.6 VLAN Management

Use this screen to view a list of configured IEEE 802.1Q VLANs and their group members. To open this screen, click **Application > VLAN Management**. The screen appears as [Figure 153](#). Select a device for which you wish to configure the VLAN settings from the **Device** or **VLAN Group** list on the left side of the screen.

Note: At the time of writing, this screen is only available for some ZyXEL Ethernet Switches. See [Appendix A on page 269](#) for the supported ZyXEL device list.

Note: This screen opens in another window. Check your open windows if you cannot see the screen after you click **Application > VLAN Management**.

Figure 153 VLAN Management > VLAN Management (Selecting a VLAN Group)

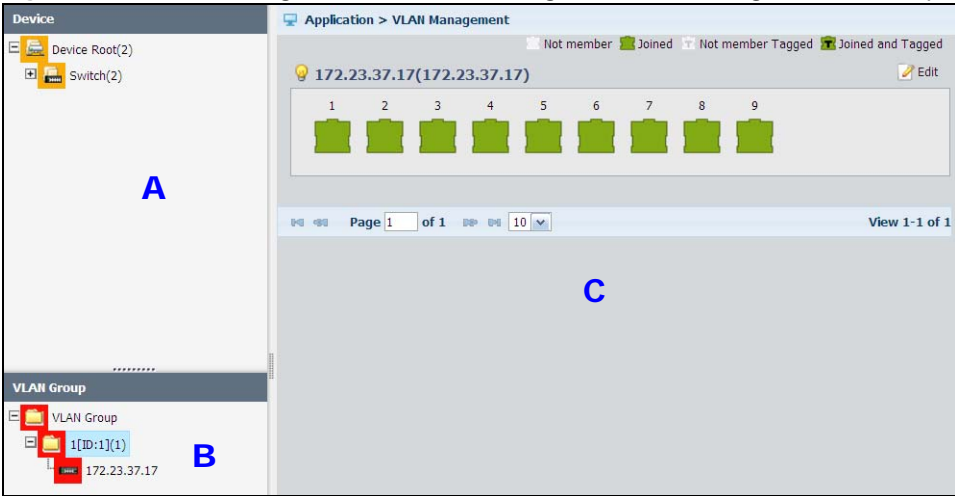
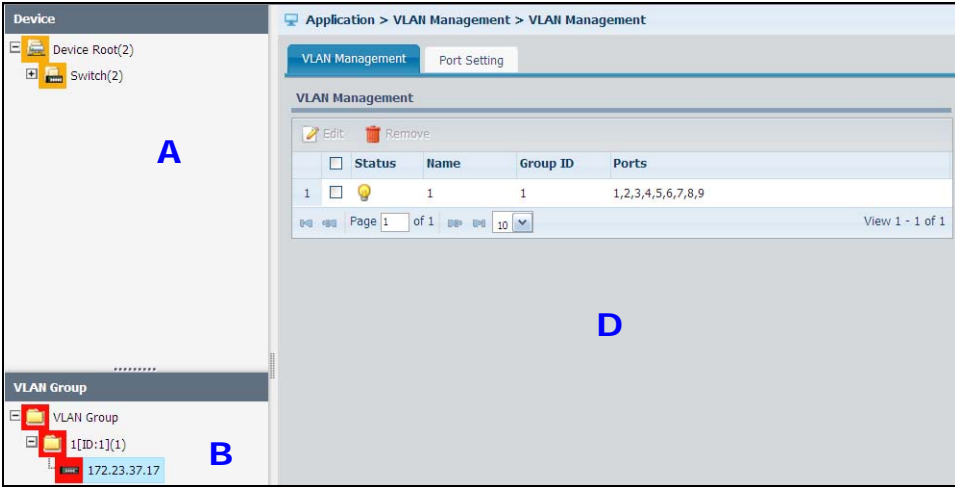


Figure 154 VLAN Management > VLAN Management (Selecting a Device)

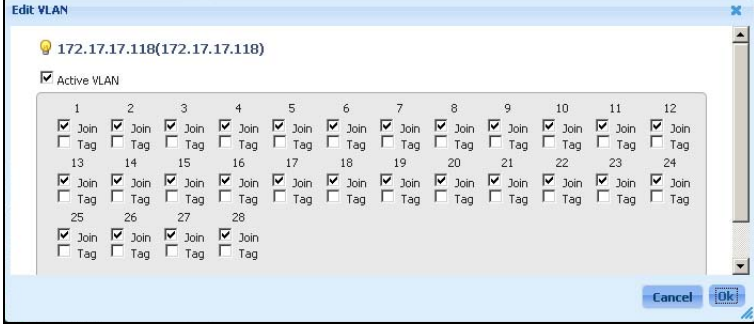


The following table describes the labels in this screen.

Table 95 VLAN Management > VLAN Management

LABEL	DESCRIPTION
Device panel (A)	This panel displays devices by groups. Each folder (group) also displays the number of devices that are included in the folder.
VLAN Group panel (B)	This panel displays devices by VLAN groups. You can see the VLAN name, ID group, and the number of devices that are included in each folder (VLAN group). For example, VLAN_100[ID:100](1).

Table 95 VLAN Management > VLAN Management (continued)

LABEL	DESCRIPTION
(C)	<p>If you select a folder in the VLAN Group panel, this screen displays all the devices in the folder and all the ports' VLAN settings.</p> <ul style="list-style-type: none"> • Not member: This port is not a member of the VLAN group. • Joined: This port is a member of the VLAN group. • Not member Tagged: This port is not a member of the VLAN group but outgoing traffic through this port is tagged with another VLAN ID. • Joined and Tagged: This port is a member of the VLAN group and outgoing traffic through this port is tagged with the VLAN ID. <p>Click Edit at the right top corner of each device's section to open the Edit VLAN screen.</p> <p>Figure 155 Edit VLAN</p>  <p>The following describes the fields in the Edit VLAN screen.</p> <ul style="list-style-type: none"> • Active VLAN: Select this to enable this VLAN on the device or clear this to disable it. • Join: Select this on a port to add the port to this VLAN group. Otherwise, clear this. • Tag: Select this on a port to add the VLAN ID to the port's outgoing traffic. Otherwise, clear this. • Cancel: Select this to discard the changes and exit this screen. • Ok: Click this to save the changes and exit this screen.
(D)	If you select a device in Device or VLAN Group panel, the following fields are available.
Edit	Click this to modify the selected VLAN group entry. See Section 8.6.2 on page 213 .
Remove	Click this to delete the selected VLAN group entry.
check box	Select the check box of an entry and click Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Status	This field displays whether the VLAN is enabled or not.
Name	This field displays the descriptive name for the VLAN.
Group ID	This field displays the identifier of the VLAN.
Ports	This field displays the port numbers that are members of this VLAN.

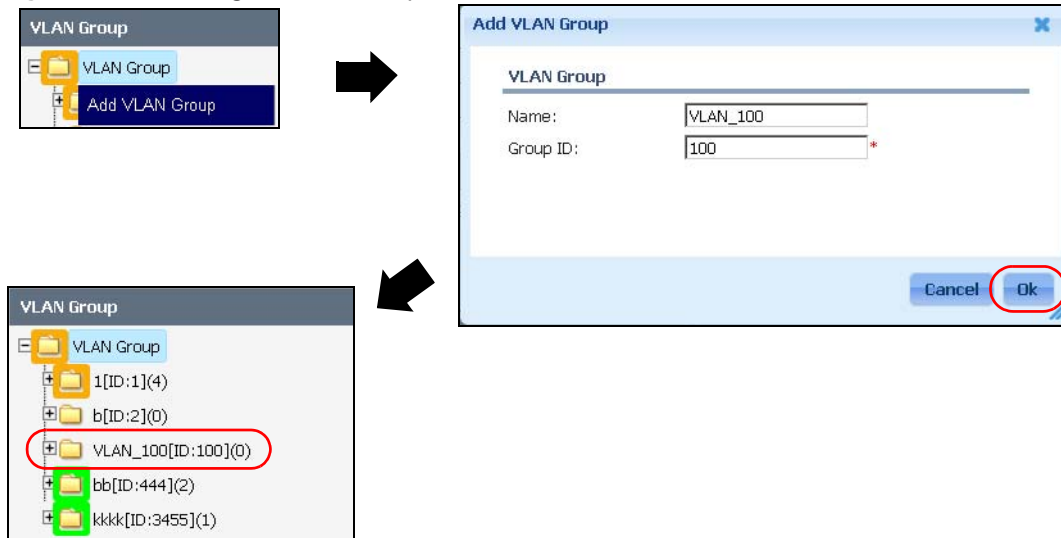
8.6.1 VLAN Management Configuration Examples

This section shows you how to create a VLAN group, and add/remove a device to a VLAN group easily by dragging and dropping.

To create a VLAN group:

- 1 Right-click the **VLAN Group** folder in the **VLAN Group** panel.
- 2 The **Add VLAN Group** screen appears.
- 3 Enter the VLAN group's name and ID. Click **Ok**.
- 4 The VLAN group is then created.

Figure 156 Creating a VLAN Group

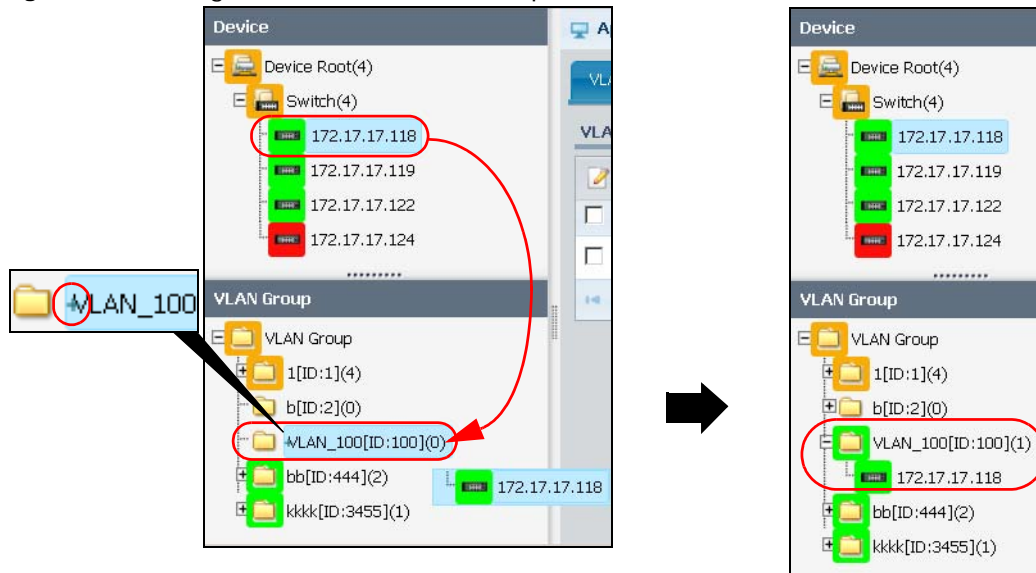


To add a device to a VLAN:

- 1 Select and hold a device from the **Device** panel (**172.17.17.118** in this example).
- 2 Drag it to a VLAN group in the **VLAN Group** panel until you see a plus mark (+) shown in the beginning of the VLAN group name.
- 3 Release your mouse.

- 4 The device is then added to the VLAN group (**VLAN_100** in this example).

Figure 157 Adding a Device to a VLAN Group



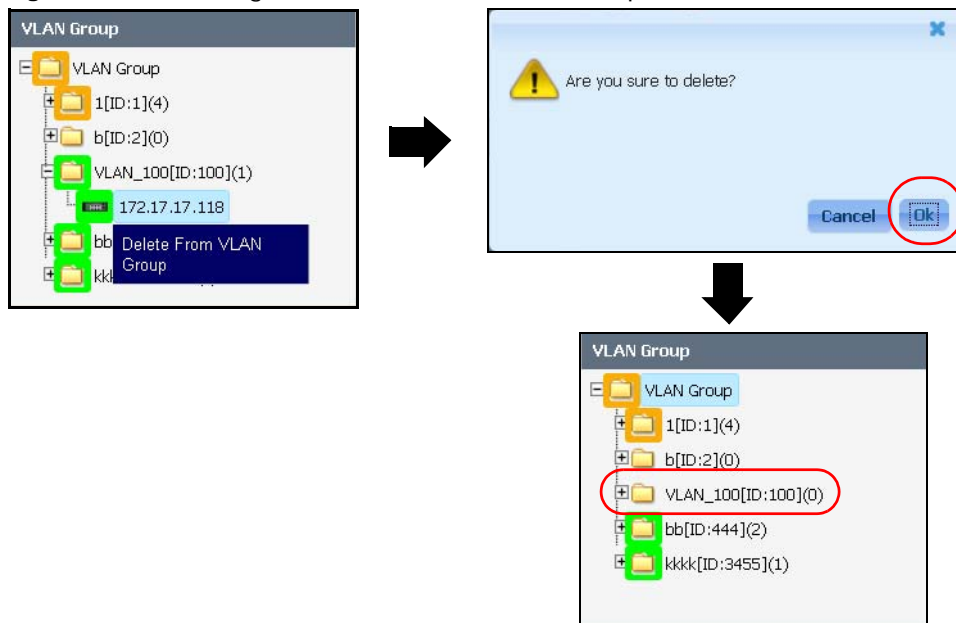
Note: After you drag and drop a device to a VLAN group, the ENC automatically creates the VLAN on the device.

To remove a device from a VLAN:

- 1 Right-click the device in the **VLAN Group** panel.
- 2 Select **Delete From VLAN Group**.
- 3 Confirm the action.

- The device is then removed from the VLAN group.

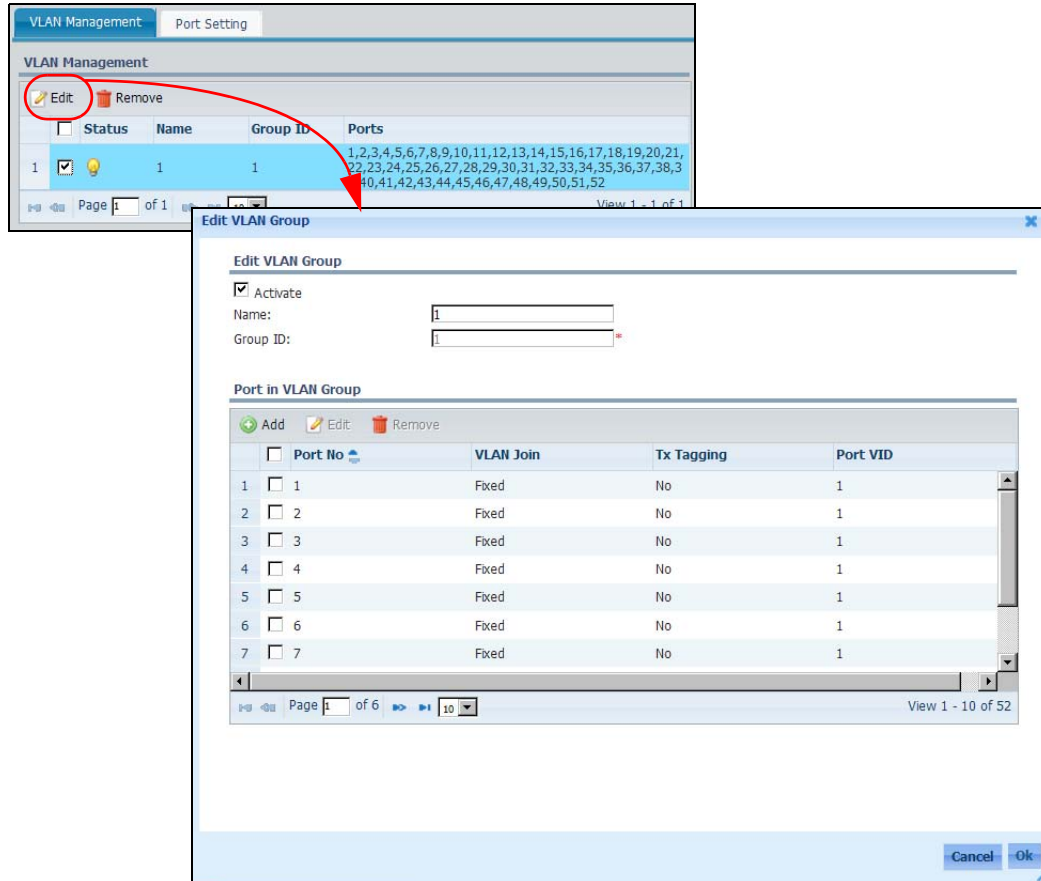
Figure 158 Removing a Device from the VLAN Group



8.6.2 Edit a VLAN Group

Use this screen to configure the selected VLAN's settings. To open this screen, select a device, a VLAN entry and then click **Edit** in the **Application > VLAN Management** screen.

Figure 159 VLAN Management > VLAN Management > Edit



The following table describes the labels in the **Edit VLAN Group** screen.

Table 96 VLAN Management > VLAN Management > Edit

LABEL	DESCRIPTION
Edit VLAN Group	
Activate	Select this to enable the VLAN or clear this to disable it.
Name	Enter a descriptive name for the VLAN for identification purposes.
Group ID	This field displays the VLAN identifier.
Port in VLAN Group	
Add	Click this to add a port and configure the VLAN settings.
Edit	Select a port in the table and click this to modify the port's VLAN settings.
Remove	Click this to delete the selected VLAN(s).
check box	Select the check box of an entry and click Duplicate , Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Port No	The port number identifies the port you are configuring.

Table 96 VLAN Management > VLAN Management > Edit (continued)

LABEL	DESCRIPTION
VLAN Join	This field displays Fixed if the port is a permanent member of this VLAN group. This field displays Normal if the port was dynamically joined to this VLAN group using GVRP.
Tx Tagging	Select this if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Port VID	This field displays the port VLAN ID. If an incoming frame received by the port is untagged, the device adds the port VLAN ID to the frame.
Isolation	This field is only available for some ZyXEL Ethernet Switches. Select the check box to block other ports from communicating with this port.
Cancel	Click this to discard all changes and close the screen.
OK	Click this to save the settings and close the screen. The ENC configures the port VLAN settings on the device automatically.

8.6.2.1 Add/Edit a Port

Use this screen to configure the selected port's VLAN settings. To open this screen, click **Add** or **Edit** in the **Application > VLAN Management > Edit** screen.

Figure 160 VLAN Management > VLAN Management > Edit > Add/Edit

The following table describes the labels in this screen.

Table 97 VLAN Management > VLAN Management > Edit > Add/Edit

LABEL	DESCRIPTION
Port Number	Select the number of a port to configure the port's VLAN settings.
VLAN Join	Select Fixed for the port to be a permanent member of this VLAN group. Select Normal for the port to dynamically join this VLAN group using GVRP.
Tx Tagging	Select this if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Port Setting	Click this if you want to configure additional VLAN settings for the port.
Cancel	Click this to discard all changes and close the screen.
OK	Click this to save the settings and close the screen.

8.6.2.1.1 Additional Port VLAN Settings

Use this screen to configure the selected port's additional VLAN settings. To open this screen, click **Port Setting** in the **Application > VLAN Management > Edit > Add or Edit** screen.

Figure 161 VLAN Management > VLAN Management > Edit > Add/Edit > Port Setting

The screenshot shows a 'Port Setting' dialog box with the following fields and controls:

- Port Number:** A text input field containing the value '1'.
- Port VID:** A text input field containing the value '1'.
- Ingress Check:** An unchecked checkbox.
- GVRP:** An unchecked checkbox.
- Acceptable Frame Type:** A dropdown menu currently set to 'All'.
- VLAN Trunking:** An unchecked checkbox.
- Buttons:** 'Cancel' and 'OK' buttons located at the bottom right of the dialog.

The following table describes the labels in this screen.

Table 98 VLAN Management > VLAN Management > Edit > Add/Edit > Port Setting

LABEL	DESCRIPTION
Port Number	This field displays the number of the selected port.
Port VID	This field displays the VLAN ID assigned to untagged frames that this port receives. Enter another VLAN ID if you want to change the setting.
Ingress Check	Select this to have the device discard incoming frames for VLANs that do not have this port as a member.
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on the port. Select All from the drop-down list box to accept all untagged or tagged frames on this port. Select Tag Only to accept only tagged frames on this port. All untagged frames will be dropped.
VLAN Trunking	Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the device.
Cancel	Click this to discard all changes and close the screen.
OK	Click this to save the settings and close the screen.

8.6.3 Port Setting

Use this screen to configure IEEE 802.1Q VLAN settings on a per-port basis. To open this screen, select a ZyXEL Ethernet Switch that supports this feature and then click **Application > VLAN Management**. Then select the Switch again and select the **Port Setting** tab.

Figure 162 VLAN Management > Port Setting

VLAN Management Port Setting

Port in VLAN Group

☐ Port Isolation

Copy

	Port VID *	Ingress Check	GVRP	Acceptable Frame Type	VLAN Trunking
1	1	<input type="checkbox"/>	<input type="checkbox"/>	All	<input type="checkbox"/>
2	1	<input type="checkbox"/>	<input type="checkbox"/>	All	<input type="checkbox"/>
3	1	<input type="checkbox"/>	<input type="checkbox"/>	All	<input type="checkbox"/>
4	1	<input type="checkbox"/>	<input type="checkbox"/>	All	<input type="checkbox"/>
5	1	<input type="checkbox"/>	<input type="checkbox"/>	All	<input type="checkbox"/>
6	1	<input type="checkbox"/>	<input type="checkbox"/>	All	<input type="checkbox"/>
7	1	<input type="checkbox"/>	<input type="checkbox"/>	All	<input type="checkbox"/>
8	1	<input type="checkbox"/>	<input type="checkbox"/>	All	<input type="checkbox"/>
9	1	<input type="checkbox"/>	<input type="checkbox"/>	All	<input type="checkbox"/>
10	1	<input type="checkbox"/>	<input type="checkbox"/>	All	<input type="checkbox"/>
11	1	<input type="checkbox"/>	<input type="checkbox"/>	All	<input type="checkbox"/>
12	1	<input type="checkbox"/>	<input type="checkbox"/>	All	<input type="checkbox"/>

Apply Reset

The following table describes the labels in this screen.

Table 99 VLAN Management > Port Setting

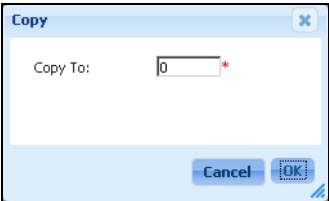
LABEL	DESCRIPTION
Port Isolation	<p>Port isolation means that each port can only communicate with the CPU management port and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected. This option is the most limiting but also the most secure.</p> <p>Select this to allows this port to communicate only with the CPU management port and the ports on which the isolation feature is not enabled.</p>
Copy	<p>Click this to copy the selected port's settings to other port(s). The screen appears as shown next.</p> <p>Figure 163 Copy</p>  <p>Specify one or multiple port numbers to which you want to copy the selected port's settings. You can use a comma (,) or hyphen (-) to specify multiple ports, for example, "2,7-8" means ports 2, 7, and 8. Click OK to apply the changes to the VLAN Management > Port Setting screen. Otherwise, click Cancel to discard the change and close this screen.</p> <p>The first column displays the number of a port on the selected device.</p>

Table 99 VLAN Management > Port Setting (continued)

LABEL	DESCRIPTION
Port VID	Enter a number between 1 and 4094 as the port VLAN ID. If an incoming frame received by the port is untagged, the device adds the port VLAN ID (PVID) to the frame.
Ingress Check	Select this to have the device discard incoming frames for VLANs that do not include this port in its member set. Clear this check box to disable ingress filtering on the port.
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on a port. The available options vary depending on device models. Select All from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select Tag Only to accept only tagged frames on this port. All untagged frames will be dropped.
VLAN Trunking	Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the device.
Apply	Click Apply to save your changes.
Reset	Click Reset to discard your changes and reset the fields to their last saved settings.

8.7 Port Basic Settings

Use this screen to configure and manage basic port settings. To open this screen, select a device that supports this feature in the OTV, Device View or Group View panel and click **Application > Port Management > Basic Setting**.

Figure 164 Port Management > Basic Setting

Port	Active	Speed/Duplex	Flow Control	802.1p Priority	BPDU Control	Loop Guard Ac	PD Power Stat	Class	PD Priority
1	<input checked="" type="checkbox"/>	Auto	<input type="checkbox"/>	0	Peer	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	Critical
2	<input checked="" type="checkbox"/>	Auto	<input type="checkbox"/>	0	Peer	<input type="checkbox"/>	<input type="checkbox"/>	1	Critical
28	<input checked="" type="checkbox"/>	Auto	<input type="checkbox"/>	0	Peer	<input type="checkbox"/>	<input type="checkbox"/>	0	Critical

The following table describes the labels in this screen.

Table 100 Port Management > Basic Setting

LABEL	DESCRIPTION
Port Status	Click View Status to view the port's status and statistics for traffic flowing through the port.
Power Management	
This section is only available for devices that support Power-over-Ethernet (PoE).	
Total Power(W)	This is the total power in Watts the PWR model can provide over the Ethernet.
Consuming Power(W)	This field displays the amount of power the device is currently supplying to the connected PoE-enabled devices.
Remaining Power(W)	This field displays the amount of power the device can still provide for PoE. The device must have at least 16 W of remaining power in order to supply power to a PoE device; even if the PoE device requested for a lower power supply than 16W.
Loop Guard	
Active Loop Guard	Select this option to enable loop guard on the device. The device generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop guard feature.
Basic Setting	

Table 100 Port Management > Basic Setting (continued)

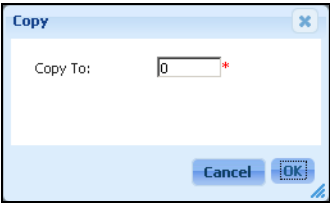
LABEL	DESCRIPTION
Copy	<p>Click this to copy the selected port's settings to another port. The screen appears as shown next.</p> <p>Figure 165 Copy</p>  <p>Specify the port number to which you want to copy the selected port's settings. You can use a hyphen and/or comma (,) to specify multiple ports. For example, 1,3-5,7 means ports 1, 3, 4, 5 and 7. Click OK to apply the changes to the Port Management > Basic Setting screen.. Otherwise, click Cancel to discard the change and close this screen.</p>
Port	This is the port index number.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Speed/Duplex	<p>Select the speed and the duplex mode of the Ethernet connection on this port. The choices are Auto, 10M/Half Duplex, 10M/Full Duplex, 100M/Half Duplex and 100M/Full Duplex for a 1000Base-T connection. 1000M/Full Duplex is supported by both 1000Base-T and 1000Base-X connections. 10G/Full Duplex is supported by the 10 Gigabit Ethernet connections.</p> <p>Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the device negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the device determines the connection speed by detecting the signal on the cable and using half duplex mode. When the device's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.</p>
Flow Control	<p>A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port.</p> <p>The device uses IEEE 802.3x flow control in full duplex mode and Back Pressure flow control in half duplex mode.</p> <p>IEEE 802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.</p> <p>Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select Flow Control to enable it.</p>
802.1p Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag.

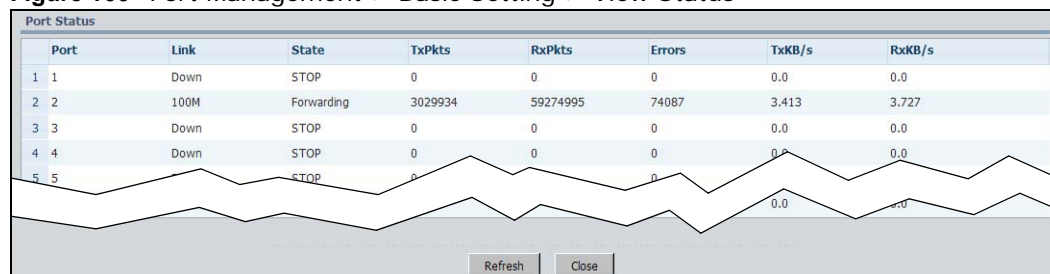
Table 100 Port Management > Basic Setting (continued)

LABEL	DESCRIPTION
BPDU Control	<p>Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency in the Switch Setup screen first.</p> <p>Select Peer to process any BPDU (Bridge Protocol Data Units) received on this port.</p> <p>Select Tunnel to forward BPDUs received on this port.</p> <p>Select Discard to drop any BPDU received on this port.</p> <p>Select Network to process a BPDU with no VLAN tag and forward a tagged BPDU.</p>
Loop Guard Active	Select Loop Guard Active to enable loop guard on the port. You have to globally enable loop guard by selecting the Active Loop Guard field before you enable it on the port.
PD Power Status	This field is only available for ZyXEL's Ethernet Switch PWR models. Select the check box to enable PoE (Power over Ethernet) on this port. Clear the check box to disable it on the port.
Class	This field is only available for ZyXEL's Ethernet Switch PWR models. This field displays the DSCP (DiffServ Code Point) number (between 0 and 63) for the port.
PD Priority	<p>This field is only available for ZyXEL's Ethernet Switch PWR models.</p> <p>When the total power requested exceeds the total PoE power budget the PoE device can provide, you can set the priority level to have the PoE device supplies power according to different priority levels. The priority from high to low is Critical > High > Low.</p> <p>Select Critical if the traffic flow through the port is very sensitive to jitter (for example, voice traffic).</p> <p>Select High if the traffic flow through the port is important but non-critical. The PoE device supplies power to the ports only after all critical-priority ports are served.</p> <p>Select Low if the traffic flow through this port is non-critical and can tolerate some delay. The PoE device supplies power to the ports only after all high-priority ports are served.</p>
Apply	Click Apply to save your changes.
Reset	Click Reset to discard your changes and reset the fields to their last saved settings.

8.7.1 View Port Status

Use this screen to view the port statistics.

To open this screen, select an entry and click **View Status** in the **Application > Port Management > Basic Setting** screen.

Figure 166 Port Management > Basic Setting > View Status

The following table describes the labels in this screen.

Table 101 Port Management > Basic Setting > View Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port.
Link	This field displays the speed (either 10M for 10Mbps, 100M for 100Mbps or another value depending on the uplink module being used). Down displays if the port is disconnected.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 8.7.1.1 on page 221 for more information). If STP is disabled, this field displays Forwarding if the link is up, otherwise, it displays STOP .
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
TxKB/s	This field shows the number of kilobytes per second transmitted on this port.
RxKB/s	This field shows the number of kilobytes per second received on this port.
Refresh	Click this to update this screen.
Close	Click this to exit this screen.

8.7.1.1 STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 102 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed. The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

8.8 Bandwidth Control Overview

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.

8.8.1 CIR and PIR

The Committed Information Rate (CIR) is the guaranteed bandwidth for the incoming traffic flow on a port. The Peak Information Rate (PIR) is the maximum bandwidth allowed for the incoming traffic flow on a port when there is no network congestion.

The CIR and PIR should be set for all ports that use the same uplink bandwidth. If the CIR is reached, packets are sent at the rate up to the PIR. When network congestion occurs, packets through the ingress port exceeding the CIR will be marked for drop.

Note: The CIR should be less than the PIR.

Note: The sum of CIRs cannot be greater than or equal to the uplink bandwidth.

8.8.2 Bandwidth Control Setup

To open this screen, select a device which supports this feature from the OTV, Device View or Group View panel and click **Application > Port Management > Bandwidth Control**.

Note: The table columns may vary depending on different device models.

Figure 167 Port Management > Bandwidth Control

The following table describes the labels in this screen.

Table 103 Port Management > Bandwidth Control

LABEL	DESCRIPTION
Activate Bandwidth Control	Select this check box to enable bandwidth control on the device.
Copy	<p>Click this to copy the selected port's settings to another port. The screen appears as shown next.</p> <p>Figure 168 Copy</p> <p>Specify the port number to which you want to copy the selected port's settings. Click OK to apply the changes to the Port Management > Bandwidth Control screen. Otherwise, click Cancel to discard the change and close this screen.</p>

Table 103 Port Management > Bandwidth Control (continued)

LABEL	DESCRIPTION
Port	This field displays the port number.
Commit Rate Active	Select this check box to activate commit rate limits on this port.
Ingress Commit Rate	Specify the guaranteed bandwidth in kilobits per second (Kbps) for the incoming traffic flow on a port. The commit rate should be less than the peak rate. The sum of commit rates cannot be greater than or equal to the uplink bandwidth.
Peak Rate Active	Select this check box to activate peak rate limits on this port.
Ingress Peak Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.
Egress Rate Active	Select this check box to activate egress rate limits on this port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the outgoing traffic flow on a port.
Apply	Click Apply to save your changes.
Reset	Click Reset to discard your changes and reset the fields to their settings last time saved.

8.9 Broadcast Storm Control

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the device receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for each packet type on each port.

To open this screen, select a device which supports this feature from the OTV, Device View or Group View panel in the **Application > Port Management > Broadcast Storm Control** screen.

Note: The table columns may vary depending on device models.

Figure 169 Port Management > Broadcast Storm Control

Port	Broadcast Active	Broadcast(pkt/s)	Multicast Active	Multicast(pkt/s)	DLF Active	DLF(pkt/s)
1	<input type="checkbox"/>	0	<input type="checkbox"/>	0	<input type="checkbox"/>	0
2	<input type="checkbox"/>	0	<input type="checkbox"/>	0	<input type="checkbox"/>	0
3	<input type="checkbox"/>	0	<input type="checkbox"/>	0	<input type="checkbox"/>	0
...						
28	<input type="checkbox"/>	0	<input type="checkbox"/>	0	<input type="checkbox"/>	0

The following table describes the labels in this screen.

Table 104 Port Management > Broadcast Storm Control

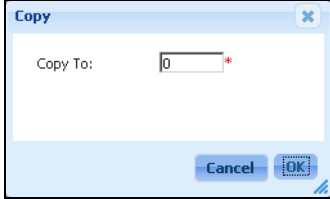
LABEL	DESCRIPTION
Activate Broadcast Storm Control	Select this check box to enable traffic storm control on the device. Clear this check box to disable this feature.
Copy	<p>Click this to copy the selected port's settings to another port. The screen appears as shown next.</p> <p>Figure 170 Copy</p>  <p>Specify the port number to which you want to copy the selected port's settings. Click OK to apply the changes to the Port Management > Broadcast Storm Control screen. Otherwise, click Cancel to discard the change and close this screen.</p>
Port	This field displays a port number.
Broadcast Active	Select this option to enable the limit for the number of broadcast packets the device receives per second on the port.
Broadcast(pkt/s)	Specify how many broadcast packets the port can receive per second.
Multicast Active	Select this option to enable the limit for the number of multicast packets the device receives per second on the port.
Multicast(pkt/s)	Specify how many multicast packets the port can receive per second.
DLF Active	Select this option to enable the limit for the number of destination lookup failure (DLF) packets the device receives per second on the port.
DLF(pkt/s)	Specify how many DLF packets the port can receive per second.

Table 104 Port Management > Broadcast Storm Control (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes.
Reset	Click Reset to discard your changes and reset the fields to their settings last time saved.

8.10 Port Security

Port security allows to configure the Static MAC Forwarding and MAC Address Learning features.

8.10.1 Static MAC Forwarding

A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

Static MAC address forwarding together with port security allows only computers in the MAC address table on a port to access the device.

8.10.2 MAC Address Learning

This feature allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on ZyXEL Ethernet Switches.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable port security together with MAC address learning as this will result in many broadcasts. By default, MAC address learning is still enabled even though the port security is not activated.

8.10.3 Port Security Configuration

Select a device which supports this feature from the OTV, Device View or Group View panel and click **Application > Port Management > Security** to open the screen as shown next.

Figure 171 Port Management > Security

Basic Setting Bandwidth Control Broadcast Storm Control **Security** Authentication

Device Security Setup

☐ Activate Security

Static MAC Forwarding

+ Add Edit Remove

	Status	MAC Address	VID	Port
1	<input type="checkbox"/>	00:13:49:00:00:0a	10	2

MAC Address Learning

Copy

Port	Security Activate	Address Learning Activate	Limited Number of Learned MAC Address
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0

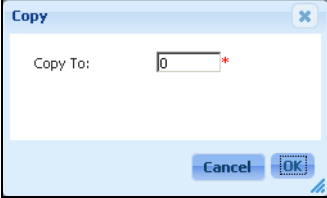
Apply Reset

The following table describes the labels in this screen.

Table 105 Port Management > Security

LABEL	DESCRIPTION
Device Security Setup	
Activate Security	Select this option to enable port security on the device.
Static MAC Forwarding	
Add	Click this to create a static MAC address rule for a port.
Edit	Click this to modify a selected static MAC address rule.
Remove	Click this to delete the selected static MAC address rule(s) from the table.
check box	Select the check box of an entry and click Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Status	This field displays whether this static MAC address forwarding rule is active or not. You may temporarily deactivate a rule without deleting it.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the ID number of the VLAN group.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
MAC Address Learning	

Table 105 Port Management > Security (continued)

LABEL	DESCRIPTION
Copy	<p>Click this to copy the selected port's settings to another port. The screen appears as shown next.</p> <p>Figure 172 Copy</p>  <p>Specify the port number to which you want to copy the selected port's settings. Click OK to apply the changes to the Port Management > Security screen. Otherwise, click Cancel to discard the change and close this screen.</p>
Port	This field displays a port number.
Security Activate	<p>Select this check box to enable the port security feature on this port. The device forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped.</p> <p>Clear this check box to disable the port security feature. The device forwards all packets on this port.</p>
Address Learning Activate	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Addresses	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only five devices' MAC addresses learned on port 2 may access port 2 at any one time. A sixth device must wait until one of the five learned MAC addresses ages out. MAC address aging out time can be set in the Switch Setup screen. The valid range is from "0" to "16384". "0" means this feature is disabled.
Apply	Click Apply to save your changes.
Reset	Click Reset to discard your changes and reset the fields to their settings last time saved.

8.10.4 Add Static MAC Forwarding

Use this screen to configure a static MAC forwarding rule. Click **Add** in the **Static MAC Forwarding** section of the **Application > Port Management > Security** screen to open the screen.

Figure 173 Port Management > Security > Static MAC Forwarding - Add

The following table describes the labels in this screen.

Table 106 Port Management > Security > Static MAC Forwarding - Add

LABEL	DESCRIPTION
Rule Activate	Select this to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port	Enter the port where traffic from the MAC address entered in the previous field will be automatically forwarded.
Cancel	Click this to discard the changes and close the screen.
OK	Click this to save the changes and close the screen.

8.11 Authentication Overview

Authentication is the process of determining who a user is and validating access to the device. The device can authenticate users who try to log in based on user accounts configured on the device itself. The device can also use an external authentication server to authenticate a large number of users.

The device supports RADIUS (Remote Authentication Dial-In User Service, see [Section 8.11.2 on page 229](#)) and TACACS+ (Terminal Access Controller Access-Control System Plus, see [Section 8.11.2 on page 229](#)) as external authentication, authorization and accounting servers.

Figure 174 Authentication Server



8.11.1 Local User Accounts

By storing user profiles locally on the device, your device is able to authenticate and authorize users without interacting with a network authentication server.

8.11.2 RADIUS and TACACS+

RADIUS and TACACS+ are security protocols used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS and TACACS+ authentication both allow you to validate an unlimited number of users from a central location.

The following table describes some key differences between RADIUS and TACACS+.

Table 107 RADIUS vs TACACS+

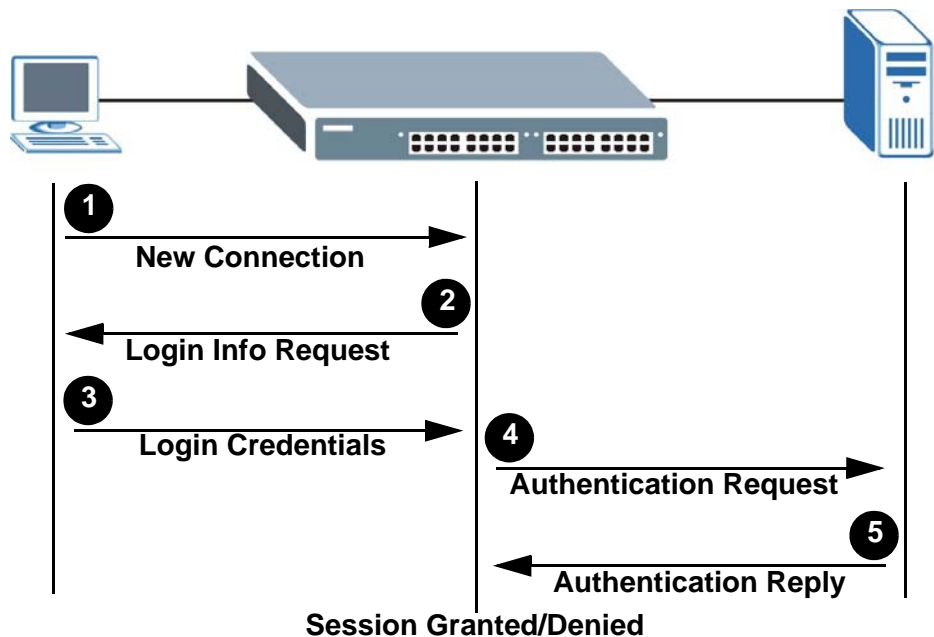
	RADIUS	TACACS+
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the client (the device) and the TACACS server is encrypted.

8.11.3 802.1x Authentication Overview

The following figure illustrates how a client connecting to a IEEE 802.1x authentication enabled port goes through a validation process. The device prompts the client for login information in the form of a user name and password. When the client provides the login credentials, the device sends an

authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

Figure 175 IEEE 802.1x Authentication Process



8.11.4 RADIUS Authentication Setup

Use this screen to configure your RADIUS server settings. To open this screen, select a device which supports this feature from the OTV, Device View or Group View panel and click **Application > Port Management > Authentication > Radius Authentication**.

Figure 176 Port Management > Authentication > Radius Authentication

Port Management

Basic Setting | Bandwidth Control | Broadcast Storm Control | Security | **Authentication**

Radius Authentication | TACACS+ Authentication | 802.1x Authentication

Radius Authentication Server Setup

Mode:

Timeout: secs

	IP Address	UDP Port	Shared Secret
1	<input type="text" value="0.0.0.0"/>	<input type="text" value="1812"/>	<input type="text"/>
2	<input type="text" value="0.0.0.0"/>	<input type="text" value="1812"/>	<input type="text"/>

The following table describes the labels in this screen.

Table 108 Port Management > Authentication > Radius Authentication

LABEL	DESCRIPTION
Mode	<p>This field only applies if you configure multiple RADIUS servers.</p> <p>Select index-priority and the device tries to authenticate with the first configured RADIUS server, if the RADIUS server does not respond then the device tries to authenticate with the second RADIUS server.</p> <p>Select round-robin to alternate between the RADIUS servers that it sends authentication requests to.</p>
Timeout	<p>Specify the amount of time in seconds that the device waits for an authentication request response from the RADIUS server.</p> <p>If you are using index-priority for your authentication and you are using two RADIUS servers then the timeout value is divided between the two RADIUS servers. For example, if you set the timeout value to 30 seconds, then the device waits for a response from the first RADIUS server for 15 seconds and then tries the second RADIUS server.</p>
	The first column displays a read-only number representing a RADIUS server entry.
IP Address	Enter the IP address of an external RADIUS server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for authentication is 1812 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the device. This key is not sent over the network. This key must be the same on the external RADIUS server and the device.
Apply	Click Apply to save your changes.
Reset	Click Reset to discard your changes and reset the fields to their settings last time saved.

8.11.5 TACACS+ Authentication Setup

Use this screen to configure your TACACS+ server settings. See [Section 8.11.2 on page 229](#) for more information on TACACS+ servers. To open this screen, select a device which supports this

feature from the OTV or Device View or Group View panel and click **Application > Port Management > Authentication > TACACS+ Authentication**.

Figure 177 Port Management > Authentication > TACACS+ Authentication

Port Management

Basic Setting | Bandwidth Control | Broadcast Storm Control | Security | **Authentication**

Radius Authentication | **TACACS+ Authentication** | 802.1x Authentication

TACACS+ Authentication Server Setup

Mode:

Timeout: * secs

	IP Address	TCP Port	Shared Secret
1	<input type="text" value="0.0.0.0"/>	<input type="text" value="49"/>	<input type="text"/>
2	<input type="text" value="0.0.0.0"/>	<input type="text" value="49"/>	<input type="text"/>

Apply Reset

The following table describes the labels in this screen.

Table 109 Port Management > Authentication > TACACS+ Authentication

LABEL	DESCRIPTION
Mode	<p>This field is only valid if you configure multiple TACACS+ servers.</p> <p>Select index-priority and the device tries to authenticate with the first configured TACACS+ server, if the TACACS+ server does not respond then the device tries to authenticate with the second TACACS+ server.</p> <p>Select round-robin to alternate between the TACACS+ servers that it sends authentication requests to.</p>
Timeout	<p>Specify the amount of time in seconds that the device waits for an authentication request response from the TACACS+ server.</p> <p>If you are using index-priority for your authentication and you are using two TACACS+ servers then the timeout value is divided between the two TACACS+ servers. For example, if you set the timeout value to 30 seconds, then the device waits for a response from the first TACACS+ server for 15 seconds and then tries the second TACACS+ server.</p>
	The first column displays a read-only number representing a TACACS+ server entry.
IP Address	Enter the IP address of an external TACACS+ server in dotted decimal notation.
TCP Port	The default port of a TACACS+ server for authentication is 49 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ server and the device. This key is not sent over the network. This key must be the same on the external TACACS+ server and the device.
Apply	Click Apply to save your changes.
Reset	Click Reset to discard your changes and reset the fields to their settings last time saved.

8.11.6 802.1x Authentication Setup

Use this screen to activate IEEE 802.1x security. To open this screen, select a device which supports this feature from the OTV or Device View or Group View panel and click **Application > Port Management > Authentication > 802.1x Authentication**.

Note: The available fields in the **MAC Authentication** section may vary depending on device models.

Figure 178 Port Management > Authentication > 802.1x Authentication

Port	802.1x	Reauthentication	Reauthentication Timer
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600

The following table describes the labels in this screen.

Table 110 Port Management > Authentication > 802.1x Authentication

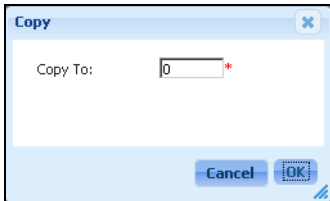
LABEL	DESCRIPTION
Activate 802.1x Authentication	Select this check box to permit 802.1x authentication on the device. Note: You must first enable 802.1x authentication on the device before configuring it on each port.
Copy	Click this to copy the selected port's settings to another port. The screen appears as shown next. Figure 179 Copy  Specify the port number to which you want to copy the selected port's settings. Click OK to apply the changes to the Port Management > Authentication > 802.1x Authentication screen. Otherwise, click Cancel to discard the change and close this screen.
Port	This field displays a port number.
802.1x	Select this checkbox to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the device before configuring it on each port.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.

Table 110 Port Management > Authentication > 802.1x Authentication (continued)

LABEL	DESCRIPTION
Reauthentication Timer	Specify the length of time required to pass before a client has to re-enter his or her username and password to stay connected to the port.
Apply	Click Apply to save your changes.
Reset	Click Reset to discard your changes and reset the fields to their settings last time saved.

8.12 AP Manager

This function is available for devices which supports wireless AP.

8.12.1 The AP Profile Screen

Use this screen to configure and look at wireless access point (AP) profiles which help configure wireless settings for multiple wireless APs. To open this screen, click **Application > AP Manager > AP Profile**.

Figure 180 AP Manger > AP Profile

The following table describes the labels in this screen.

Table 111 AP Manger > AP Profile

LABEL	DESCRIPTION
Add	Click this to create an entry.
Edit	Select an entry in the table and click this to modify it.
Remove	Select an entry in the table and click this to delete it.
check box	Select the check box of an entry and click Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Profile Name	This field displays the name of a wireless AP profile.
SSID	<p>This field displays the SSID this wireless AP profile uses.</p> <p>The SSID (Service Set IDentity) identifies the Service Set with which a wireless station is associated. Wireless clients associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.</p> <p>When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.</p>
Channel	This field displays the operating frequency/channel this wireless AP profile uses.

Table 111 AP Manger > AP Profile (continued)

LABEL	DESCRIPTION
Transmit Power	This field displays the transmitting power in percentage this wireless AP profile uses.
Last Update	This field displays the date and time (yyyy-mm-dd hh:mm:ss) this wireless AP profile was last time updated.

8.12.2 Add/Edit an AP Profile

Use this screen to configure a new or an existing wireless AP profile which helps configure multiple wireless APs at one time. To open this screen, click **Add** in the **Application > AP Manager > AP Profile** screen or select an entry and click **Edit** in the **AP Profile** screen.

Note: If you are editing a profile, the ENC will apply the changes to the associated wireless APs right after you click **Ok** in this screen.

Figure 181 AP Manager > AP Profile > Add/Edit

The following table describes the labels in this screen.

Table 112 AP Manager > AP Profile > Add/Edit

LABEL	DESCRIPTION
Profile Name	Enter up to 32 characters for the name of wireless AP profile. You can use alphanumeric (0-9, a-z, A-Z), underscores (_) and hyphens (-). Spaces are not allowed.
SSID	Enter a descriptive name (up to 32 printable SCII characters) which identifies the wireless LAN. Wireless clients associating to the access point (AP) must have the same SSID. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Channel	Select Auto and a channel set (1, 6, 11 or 1, 4, 7, 11 or 1, 5, 9, 13) if you want the AP automatically switches a channel within the channel set when the original channel has problems with wireless interference. Alternatively, select Manual and a specific channel if you want to fix the channel.

Table 110 Port Management > Authentication > 802.1x Authentication (continued)

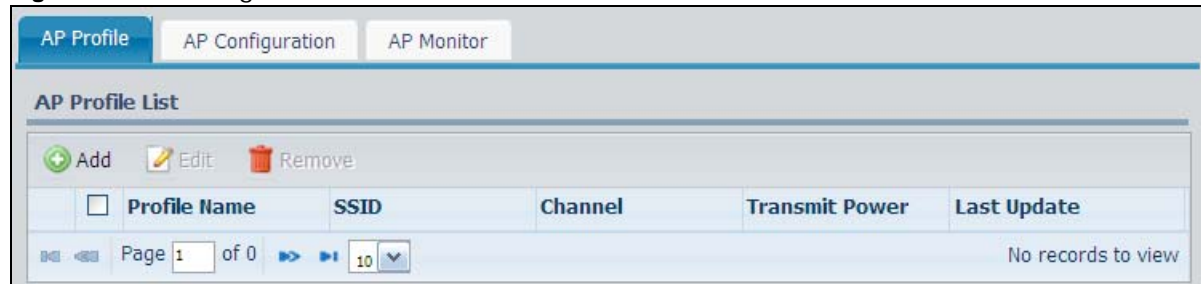
LABEL	DESCRIPTION
Reauthentication Timer	Specify the length of time required to pass before a client has to re-enter his or her username and password to stay connected to the port.
Apply	Click Apply to save your changes.
Reset	Click Reset to discard your changes and reset the fields to their settings last time saved.

8.12 AP Manager

This function is available for devices which supports wireless AP.

8.12.1 The AP Profile Screen

Use this screen to configure and look at wireless access point (AP) profiles which help configure wireless settings for multiple wireless APs. To open this screen, click **Application > AP Manager > AP Profile**.

Figure 180 AP Manger > AP Profile

The following table describes the labels in this screen.

Table 111 AP Manger > AP Profile

LABEL	DESCRIPTION
Add	Click this to create an entry.
Edit	Select an entry in the table and click this to modify it.
Remove	Select an entry in the table and click this to delete it.
check box	Select the check box of an entry and click Edit or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Profile Name	This field displays the name of a wireless AP profile.
SSID	<p>This field displays the SSID this wireless AP profile uses.</p> <p>The SSID (Service Set IDentity) identifies the Service Set with which a wireless station is associated. Wireless clients associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.</p> <p>When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.</p>
Channel	This field displays the operating frequency/channel this wireless AP profile uses.

Table 111 AP Manger > AP Profile (continued)

LABEL	DESCRIPTION
Transmit Power	This field displays the transmitting power in percentage this wireless AP profile uses.
Last Update	This field displays the date and time (yyyy-mm-dd hh:mm:ss) this wireless AP profile was last time updated.

8.12.2 Add/Edit an AP Profile

Use this screen to configure a new or an existing wireless AP profile which helps configure multiple wireless APs at one time. To open this screen, click **Add** in the **Application > AP Manager > AP Profile** screen or select an entry and click **Edit** in the **AP Profile** screen.

Note: If you are editing a profile, the ENC will apply the changes to the associated wireless APs right after you click **Ok** in this screen.

Figure 181 AP Manager > AP Profile > Add/Edit

The following table describes the labels in this screen.

Table 112 AP Manager > AP Profile > Add/Edit

LABEL	DESCRIPTION
Profile Name	Enter up to 32 characters for the name of wireless AP profile. You can use alphanumeric (0-9, a-z, A-Z), underscores (_) and hyphens (-). Spaces are not allowed.
SSID	<p>Enter a descriptive name (up to 32 printable SCII characters) which identifies the wireless LAN. Wireless clients associating to the access point (AP) must have the same SSID.</p> <p>When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.</p> <p>You can select Room No. from the drop-down list to postfix the configured room number of the AP to the SSID.</p>

Table 112 AP Manager > AP Profile > Add/Edit (continued)

LABEL	DESCRIPTION
Channel	Select Auto and a channel set (1, 6, 11 or 1, 4, 7, 11 or 1, 5, 9, 13) if you want the AP automatically switches a channel within the channel set when the original channel has problems with wireless interference. Alternatively, select Manual and a specific channel if you want to fix the channel.
Transmit Power	Set the output power this wireless AP profile uses. If there is a high density of APs in an area, decrease the output power of the ENC to reduce interference with other APs. Select one of the following 100%, 50% or 25%.
System Name	Select Use device's display name as system name to configure an wireless AP's system name as its display name in the ENC when you apply this profile to the device. Alternatively, select Customized and enter a name to configure the device's system name as the specified name.
Security	<p>Select None to allow wireless stations to communicate with the access points without any data encryption or authentication.</p> <p>Select WPA to configure and enable WPA or WPA-PSK authentication and encryption.</p> <p>Select WPA2 to configure and enable WPA2 or WPA2-PSK authentication and encryption.</p> <p>Select WPA/WPA2 to have both WPA2 and WPA wireless clients be able to communicate with the ENC even when the ENC is using WPA2 or WPA2-PSK.</p> <p>Select WEP to configure and enable WEP encryption.</p>
The following fields are available if you select WPA , WPA2 , or WPA/WPA2 in the Security field.	
Group Key Update Timer	Enter the rate at which the wireless AP or the RADIUS server sends a new group key out to all clients.
Use WPA with Pre-shared Key	Select this option if you do not have a RADIUS server in your network and want to use a pre-shared key WPA or WPA2.
Pre-shared Key	<p>The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials.</p> <p>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).</p>
Use WPA with RADIUS Server	Select this option if you have a RADIUS server in your network and want to use it for user authentication and encryption.
Server IP	Enter the IP address of the external authentication server in dotted decimal notation.
Authentication Port	<p>Enter the port number of the external authentication server. The default port number is 1812.</p> <p>You need not change this value unless your network administrator instructs you to do so with additional information.</p>
Shared Secret Key	<p>Enter a password (from 8 to 63 case-sensitive ASCII characters) as the key to be shared between the external authentication server and the ENC.</p> <p>The key must be the same on the external authentication server and your wireless AP. The key is not sent over the network.</p>
The following fields are available if you select WEP in the Security field.	
Encryption	Select to use 64 Bit or 128 Bit WEP key(s) for excrypting wireless packets.
Mode	<p>Select HEX to enter hexadecimal characters as a WEP key.</p> <p>Select ASCII to enter ASCII characters as WEP key.</p>

Table 112 AP Manager > AP Profile > Add/Edit (continued)

LABEL	DESCRIPTION
WEP Key	<p>The WEP keys are used to secure your data from eavesdropping by unauthorized wireless users. Both the wireless AP and wireless clients must use the same WEP key for data transmission.</p> <p>If you chose 64 Bit in the Encryption field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each key.</p> <p>If you chose 128 Bit in the Encryption field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each key.</p> <p>You must configure all four keys. Only one key can be activated at any one time. Select a default key to use for data encryption.</p>
Authentication Method	<p>Select Open System, Shared Key or Both.</p> <p>This field specifies whether the wireless clients have to provide the WEP key to login to the wireless network. Keep this setting at Both or Open System unless you want to force a key verification before communication between the wireless client and the wireless AP occurs. Select Shared Key to force the clients to provide the WEP key prior to communication.</p>
Cancel	Click this to discard all changes and close the screen.
Ok	Click this to save the settings and close this screen.

8.12.3 The AP Configuration Screen

Use this screen to search and check the basic settings such as IP address, MAC address and AP profile for wireless APs. To open this screen, click **Application > AP Manager > AP Configuration**.

Figure 182 AP Manager > AP Configuration

The following table describes the labels in this screen.

Table 113 AP Manager > AP Configuration

LABEL	DESCRIPTION
Name	Enter the full or partial name of the device you are looking for.
Device Model	Select the device model name for the search criteria.
IP Address	Enter an IP address for the search criteria.

Table 113 AP Manger > AP Configuration (continued)

LABEL	DESCRIPTION
Status	Select the device's status (Online , Offline , Un-Monitorer , or Un-Registered) for the search criteria.
Device Group	Select the group to which the device belongs.
Enable Status Polling	Select whether the device's status polling is enabled (true) or not (false) for the search criteria.
AP Profile	Select an AP profile with which the device is applied.
Search	Click this to search the matched device(s) according to your input criteria.
Access Web GUI	Select a device from the table and click this to access the Web Configurator.
Edit AP Profile	Select a device from the table and click this to edit the applied AP profile.
check box	Select the check box of an entry and click Access Web GUI or Edit AP Profile to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Status	This field displays the status of a matched wireless AP.
Name	This field displays the AP's display name.
IP Address	This field displays the AP's IP address.
MAC Address	This field displays the AP's MAC address.
AP Profile	This field displays the AP profile name the AP is using. N/A displays if you have not applied any wireless AP profile to the AP.
Configuration Status	<p>This field displays the status of the applied AP profile to the AP. The possible values are:</p> <ul style="list-style-type: none"> • N/A - There is no AP profile being applied to the AP. • Waiting - The AP profile has not yet been applied to the AP because the AP is unavailable. If you selected Apply it when AP is available in the AP Manger > AP Configuration > Edit AP Profile screen (see Figure 183), you see this status before the AP is available. • Running - The ENC is applying the AP profile to the AP. • Success - The AP profile has been successfully applied to the AP. • Fail - The AP profile is failed to be applied to the AP because the AP is unavailable. If you selected Apply Now in the AP Manger > AP Configuration > Edit AP Profile screen (see Figure 183) but the AP was unavailable at that time, you see this status.
Device Model	This field displays the AP's model name.

Maintenance

The `root` account and any other Administrator accounts can use the Maintenance screens to:

- View, add, remove, or edit users who can access the ENC
- Change the ENC's IP address
- Configure login lockout settings
- Configure mail server settings
- Maintain global reporting settings, such as how many days of logs to keep
- Upload and customize device icons and Map images (see [Section 1.3.3 on page 24](#) for more information about Map)
- Backup the current configuration and restore a different configuration
- Export the current database tables to a CSV file
- Register the ENC (you have to register ENC if you want to upgrade to standard version, or increase the number of devices the ENC supports.)
- Monitor the number of logs received by time or by device
- Manage system logs
- Get basic information about the ENC

The Operator and User accounts can use the Maintenance screens to:

- View a list of users who can access the ENC
- Get basic information about the ENC

9.1 User Account Overview

An account is a user with permissions inherited from the associated account type. "root" is the predefined administrator belonging to the Administrator account type. Only administrator accounts including the "root" and other Administrator accounts can do everything as well as manage the ENC system.

9.2 Types of Accounts

ENC provides three account types with different privilege levels. The Web Configurator screens vary depending on which account you use to log in. Only one user from the same IP address can log into

the ENC at one time. Multiple users from different IP address can log in at the same time. The following table describes and shows the default user name and password for the different accounts.


Table 116 Types of Accounts

TYPE	PRIVILEGE	DEFAULT SETTINGS
Administrator	<p>Create non-root Administrator, Operator and User accounts.</p> <p>Log out other users.</p> <p>The root account cannot be deleted and logged out by anyone from the system. Only one root administrator can exist. The other Administrator accounts can be deleted and logged out by the root and other Administrators.</p> <p>Device management (For example, manage devices and their configurations, firmware upgrade, backup and restore configuration files, events and alarms management, log file management and so on.)</p> <p>ENC system management and setup (For example, configuration backup and restore, database table export, server, Map, log settings and so on).</p>	<p>User name: root</p> <p>Password: root</p>
Operator	<p>Basic device management (For example, view and configure devices, device firmware upgrade, device configuration backup and restore, view and acknowledge device events, perform simple configuration tasks, generate reports.)</p> <p>Basic ENC system management (For example, view a list of users who can access the ENC.)</p>	No default account.
User	<p>View information of devices.</p> <p>Basic ENC system management (For example, view a list of users who can access the ENC.)</p>	No default account.

9.3 User Account

Use this screen to display a list of root and all the other user accounts. To open this screen, click **Maintenance > User Account**.

Figure 185 User Account



The screenshot shows a web interface titled "Account" with a table of user accounts. At the top, there are buttons for "Add", "Edit", "Remove", and "Revoke". The table has columns for "Status", "Name", "Account Type", "Map Access", and "Description". There are 6 rows of accounts listed. At the bottom, there is a pagination bar showing "Page 1 of 1" and "View 1 - 6 of 6".

	Status	Name	Account Type	Map Access	Description
1	<input type="checkbox"/>	scott	Administrator	DefaultMap	sadasd
2	<input type="checkbox"/>	yvonne	Administrator	DefaultMap	
3	<input type="checkbox"/>	nate	Administrator	DefaultMap	
4	<input type="checkbox"/>	brad	Administrator	DefaultMap	dasdas
5	<input type="checkbox"/>	roger	Administrator	DefaultMap	dsadas
6	<input type="checkbox"/>	root	Administrator	DefaultMap	DEFAULT_USER

The following table describes the fields in this screen.

Table 117 User Account

LABEL	DESCRIPTION
Add	Click Add to create a new user account if you have this permission. Only the "root" and Administrators can create and manage user accounts.
Edit	Click this to modify an existing user account.
Remove	Click this to erase the selected user accounts from the ENC. You can delete a user only when the user has logged out.
Revoke	Click this to disconnect the selected on-line user(s) after you confirm the action.
check box	Select the check box of an entry and click Edit , Remove or Revoke to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Status	This field displays if this user is currently logged in or not.
Name	This field displays the name of the user.
Account Type	This field displays the type of the user account.
Map Access	This field displays the Map(s) the user is allowed to access. Only Administrators can change the Map access settings for Operators and Users. Administrators can access to all available Maps.
Description	This field displays additional information for the user.

9.3.1 User Account Add

Use this screen to create or edit a user. o open this screen, click **Add** or **Edit** in the **Maintenance > User Account** screen.

Figure 186 User Account > Add/Edit (Administrator)

The screenshot shows the 'Add Account' dialog box with the 'Administrator' radio button selected. The 'General Settings' section includes fields for Name, Password, Verify Password, and Email Address, each with a red asterisk indicating a required field. There is also a Description text area. The 'Map Access' section contains the text 'All maps will be bound with Administrator.' At the bottom right are 'Cancel' and 'Ok' buttons.

Figure 187 User Account > Add/Edit (Operator and User)

The screenshot shows two overlapping 'Add Account' dialog boxes. The background box has the 'Operator' radio button selected, and the foreground box has the 'User' radio button selected. Both boxes show the 'General Settings' section with required fields (Name, Password, Verify Password, Email Address) marked with red asterisks and a Description text area. The 'Map Access' section in the foreground box shows two list boxes: 'Available Maps' containing 'JapanBg' and 'DefaultMap', and 'Allowed Map Access' which is empty. Double arrow buttons (>> and <<) are positioned between the two list boxes. At the bottom right of the foreground box are 'Cancel' and 'Ok' buttons.

The following table describes the fields in this screen.

Table 118 User Account > Add/Edit

LABEL	DESCRIPTION
General Settings	
Account Type	Select the type of the new user account.
Name	Type up to 32 alphanumeric characters (0-9, a-z, A-Z), underscores (_) and/or hyphens (-) for the name of this account. Spaces are not allowed.
Password	Type up to 32 characters for the corresponding password of the user account.
Verify Password	Type the same password again here to make sure that the one you typed above was typed as intended.
Email Address	Type a valid e-mail address for this user.
Description	Type extra information about this user.
Map Access	This section configures the Map(s) that are allowed the user to access. Select Map(s) from the Available Maps field and click >> to move them to the Allowed Map Access field. You can select Map(s) in the Allowed Map Access field and click << to remove them from the list.
Cancel	Click this to go back to the previous screen without saving any changes.
Ok	Click this to save your settings and close this screen.

9.4 Server

Use this screen to configure the ENC's IP address or domain name, client login lockout, and mail server settings. To open this screen, click **Maintenance > Server**.

Figure 188 Server

The screenshot shows the 'Server Configuration' screen with the following sections and fields:

- Server Configuration**
 - Server IP/Domain: 172.17.17.127 *
- Client Login Lockout**
 - Maximum Retry Count: 100 * 1~99
 - Lock Period: 1 * 1~65535 minutes
 - User Change Password Period: 90 * 0~65535 days, 0:unlimited
- Mail Relay**
 - SMTP Server IP/Domain: *
 - Sender Mail: *
 - ☐ Authentication
 - User Name: *
 - Password: *

At the bottom right, there are 'Apply' and 'Reset' buttons.

The following table describes the fields in this screen.

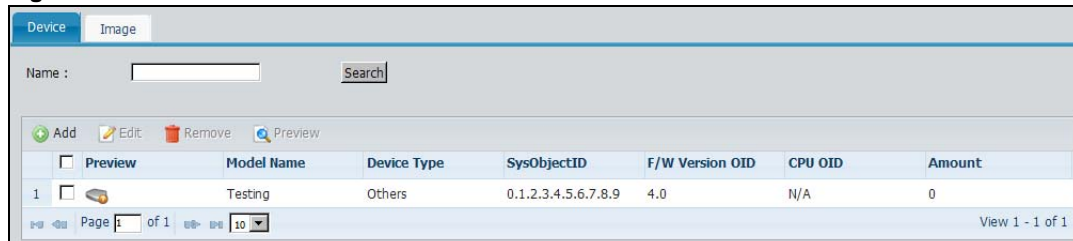
Table 119 Server

LABEL	DESCRIPTION
Server Configuration	
Server IP/Domain	Type a new IP address or domain name if you want to change the current setting.
Client Login Lockout	
Maximum Retry Count	The ENC can lock a user out if you use a wrong user name or password to log in the ENC. Enter up to how many times a user can re-enter his/her account information before the ENC locks the user out.
Lock Period	Enter the number of minutes for the lockout period. A user cannot log into the ENC during the lockout period, even if he/she enters correct account information.
User Change Password Period	Enter the maximum number of days within which a user must change his password for the ENC login. If the user does not change his/her password within the configured time, the ENC will show a reminder when the user logs in next time. 0 means unlimited.
Mail Relay	
SMTP Server IP/Domain	Enter the IP address or domain name of a mail server. The ENC will send notifications to users through this mail.
Sender Mail	Enter a valid e-mail address. This is the sender's e-mail address that you want to show to mail receivers.
Authentication	Select this if authentication is required for the mail server login.
User Name	Enter the user name for the mail server login.
Password	Enter the corresponding password for the mail server login.
Apply	Click this to save the changes.
Reset	Click this to discard the changes and exit the screen.

9.5 Customize Device Models


The ENC provides some default device models (such as **Switch**, **Router/Gateway**, **Firewall**, **Wireless AP**, and so on). The device types are applied to device settings on the ENC when devices are discovered or manually added to the ENC. Use this screen if you want to customize a device type (for example, for a new ZyXEL device or non-ZyXEL device). To open this screen, click **Maintenance > Customize**.

Figure 189 Customize > Device



The following table describes the fields in this screen.

Table 120 Customize > Device

LABEL	DESCRIPTION
Name	Enter a part or full name of a device model for which to search.
Search	Click this to perform the search.
Add	Click this to create a device model in the ENC.
Edit	Click this to modify a selected device model.
Remove	Click this to delete selected device model(s).
Preview	Click this to view the full-size device icon for a selected device model. Figure 190 Icon Preview 
check box	Select the check box of an entry and click Edit , Remove or Preview to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Preview	This field displays the thumbnail-size icon for a device model in the ENC.
Model Name	This field displays the name of the device model.
Category	This field displays the model of the device.
SysObjectID	This field displays the MIB object ID of the device model.
F/W Version OID	This field displays the firmware version object ID of the device model so that the ENC can retrieve the firmware version through SNMP.
CPU OID	This field displays the CPU object ID of this device model so that the ENC can get the CPU usage through SNMP.
Amount	This field displays the number of managed devices that belong to this device model.

9.5.1 Device Model Add/Edit

Use this screen to configure a device model. Before you configure a device model in this screen, you must know its MIB object ID and firmware version object ID. Each device model should associate with an existing or a new device icon (uploaded through the **Maintenance > Customize**

> **Image** screen). To open this screen, click **Add** or **Edit** in the **Maintenance > Customize > Device** screen.

Figure 191 Customize > Device > Add/Edit

The following table describes the fields in this screen.

Table 121 Customize > Device > Add/Edit

LABEL	DESCRIPTION
Name	Type up to 32 alphanumeric characters (0-9, a-z, A-Z), underscores (_) and/or hyphens (-) for the name of a device model.
SysObjectID	Enter the MIB object ID of the device model.
F/W Version OID	Enter the MIB object ID of the firmware version for which this device model's settings will apply.
CPU OID	Enter the MIB object ID of the device model's CPU. This field is optional.
Device Type	Select the type of the device model.

The following table describes the fields in this screen.

Table 122 Customize > Image

LABEL	DESCRIPTION
Add	Click this to upload a new device icon or Map image to the ENC.
Edit	Click this to modify a selected entry.
Remove	Click this to delete selected entr(ies).
Preview	Click this to view the full-size image of a selected entry.
check box	Select the check box of an entry and click Edit , Remove or Preview to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Preview	This field displays the thumbnail-size image of the device icon or Map image.
Image Name	This field displays the name of the device icon or Map image.
Image Type	This field displays whether this image is a Device Icon or Map image (Background Image).
Size	This field displays the size (in pixels) of this image. The higher the number of pixels, the more granulated information you can see in the image.
Device Type	This field displays the device type to which this image belongs if this is a device icon. N/A displays for a Map image.

9.6.1 Images Add/Edit

Use this screen to upload a device icon or Map image to the ENC. To open this screen, click **Add** or **Edit** in the **Maintenance > Customize > Image** screen.

Figure 194 Customize > Image > Add (Image Type: Object)

The 'Add Custom Image' dialog box has a title bar with a close button. Under the 'General Settings' tab, the 'Image Type' is set to 'Object' (selected with a radio button). The 'Image Name' field is empty. The 'Device Type' dropdown is set to 'Others'. The 'Image' field is empty, with a 'Browse...' button to its right. A note below the field states '(48X48 is the perfect size for uploading.)'. At the bottom right are 'Cancel' and 'Ok' buttons.

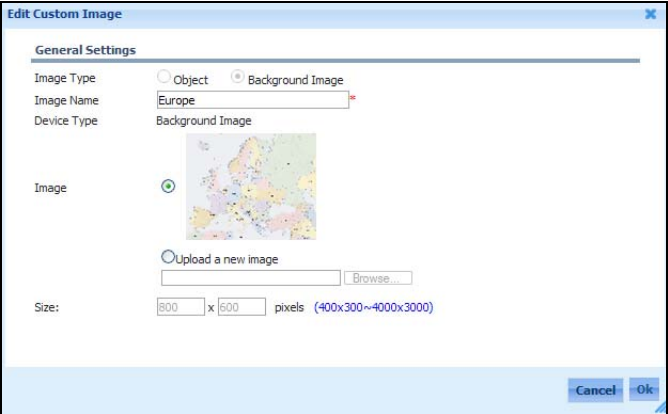
Figure 195 Customize > Image > Add (Image Type: Background Image)

The 'Add Custom Image' dialog box has a title bar with a close button. Under the 'General Settings' tab, the 'Image Type' is set to 'Background Image' (selected with a radio button). The 'Image Name' field is empty. The 'Device Type' dropdown is set to 'Background Image'. The 'Size' field shows '800 x 600 pixels' with a note '(400x300~4000x3000)'. The 'Image' field is empty, with a 'Browse...' button to its right. At the bottom right are 'Cancel' and 'Ok' buttons.

Figure 196 Customize > Image > Edit (Image Type: Object)

The 'Edit Custom Image' dialog box has a title bar with a close button. Under the 'General Settings' tab, the 'Image Type' is set to 'Object' (selected with a radio button). The 'Image Name' field contains 'Test'. The 'Device Type' dropdown is set to 'Others'. The 'Image' field shows a selected icon (a blue circle with a white cross). Below it, there is an option to 'Upload a new image' with a 'Browse...' button. A note below the field states '(48X48 is the perfect size for uploading.)'. At the bottom right are 'Cancel' and 'Ok' buttons.

Figure 197 Customize > Image > Edit (Image Type: Background Image)



The following table describes the fields in this screen.

Table 123 Customize > Image > Add/Edit

LABEL	DESCRIPTION
Image Type	Select Object to upload a device icon image or Background Image to upload a Map image. This field is grayed out if you are editing an existing image file.
Image Name	Type up to 32 alphanumeric characters (0-9, a-z, A-Z), underscores (_) and/or hyphens (-) for the name of this image file. Spaces are not allowed.
Device Type	Select the category of the device icon you want to upload if you selected Object as the image type. This field displays Background Image if you selected Background Image as the image type.
Size	Enter the size of the background image in pixels that you want to display in the MAP.
Image	<p>Click the text box or Browse to select the image file you want to upload to the ENC. It is recommended to upload an image of 48 by 48 pixels for a device icon and an image of 800 by 600 pixels for a Map image.</p> <p>If you are editing for an existing image, this field displays the image preview. You can select Upload a new image and click the text box or Browse to choose another image file to upload.</p>

9.7 Backup/Restore

Use this screen to back up and restore the ENC's system settings. To open this screen, click **Maintenance > Backup/Restore**.

Figure 198 Backup/Restore - Backup Location (Local Host)

Figure 199 Backup/Restore - Backup Location (FTP Site)

Figure 200 Backup/Restore - Backup Location (Storage Server)

The following table describes the fields in this screen.

Table 124 Backup/Restore

LABEL	DESCRIPTION
Backup Location	
Fields in this section are different depending on the option you select in the Location field.	
Location	Select whether to back up the ENC's system settings to a local folder in the computer where the ENC is installed (Local Host), an FTP Site , or a Storage Server (such as a Network Attached Storage (NAS) server).
Archive Location	This field is available if you select Local Host as the backup location. Type the full path of a folder on the computer where the ENC is installed, to which you want to back up or restore the configuration.
The following fields are available if you select FTP Site as the backup location.	
FTP Host/IP	Enter the IP address of an FTP server.

Table 124 Backup/Restore

LABEL	DESCRIPTION
Port	Enter a new port if your FTP server does not use port 21 for the service.
User Name	Enter the user name for your FTP account.
Password	Enter the password for your FTP account.
FTP path	Specify in which folder you want to store the backup file.
The following fields are available if you select Storage Server as the backup location.	
Network Folder	Type the full path of a folder on a storage server, to which you want to back up or restore the configuration.
Authentication	Select this if your server prompts for identification before allowing access.
User Name	Enter the user name for server login if authentication is required.
Password	Enter the corresponding password for server login.
Apply	Click this to save the changes in this section.
Database Backup/Restore	
BackUp	Click this to add a backup file (a ZIP file containing a SQL file and other files such as device firmware and configuration files) to the list. The file can be generated by performing backup immediately or by uploading a backup file.
Restore	Select a backup file in the list and click this to restore the file to the ENC after you double confirm the action. If you want to restore a file that does not exist on the ENC, you have to upload the file to the ENC first. You can upload a file through the Maintenance > Backup/Restore > Backup screen (by selecting Upload BackUp File).
Remove	Select one or more backup files in the list and click this to remove the file from the list.
Name	This displays the name of an existing configuration file of the ENC. Click this name to download the file to the computer where you are using to access the ENC.
Time	This field displays the date and time of backup of the configuration file.
Version	This displays the software version of the ENC when the configuration file was backed up.
Note	This displays additional information about the backup file.
Schedule BackUp	
Enable Schedule BackUp	Select this to have the ENC automatically perform system backup periodically.
Schedule Type	Select Daily to perform backup once per day or Weekly to perform backup once per week.
Time	Select at which hour you want to perform daily backup. Select on which week day and at which hour you want to perform weekly backup. Note: This is based on the time zone setting of the ENC server, not your computer.
Apply	Click this to save the changes in this section.

9.7.1 Backup

Use this screen to create a backup file (a SQL file) by performing backup immediately or add a backup file by uploading it from the computer you are using to the ENC. To open this screen, click the **Backup** icon in the **Maintenance > Backup/Restore** screen.

Figure 201 Backup/Restore > Backup

The following table describes the fields in this screen.

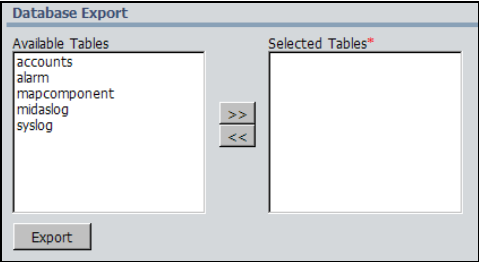
Table 125 Backup/Restore > Backup

LABEL	DESCRIPTION
BackUp Type	Select BackUp Database if you want to perform backup immediately. Select UploadBackUp File if you want to upload a backup file from the computer you are using to access the ENC and then you can restore.
File Name	This field is available if you selected BackUp Database in the BackUp Type field. Enter the file name to which you want to back up the ENC configuration.
File Path	This field is available if you selected UploadBackUp File in the BackUp Type field. Enter the full path of a SQL file you want to upload from the computer you are using to access the ENC.
Description	Enter additional information about the specified file.
Cancel	Click this to discard the changes and exit this screen.
Ok	Click this to perform backup if you selected BackUp Database in the BackUp Type field. Otherwise, click this to upload the specified file to the ENC.

9.8 Data Export

Use this screen to export data of specific database table(s) from the ENC to CSV files (in a ZIP file) on the computer you are using to access the ENC. To open this screen, click **Maintenance > Data Export**.

Figure 202 Data Export



The following table describes the fields in this screen.

Table 126 Data Export

LABEL	DESCRIPTION
Available Tables	Select the table(s) about which you want to export the data and use the >> arrow to move them to the Selected Tables list. See Table 127 on page 258 for more information about the available database tables.
Selected Tables	This section lists the tables about which you want to export the data. Select one or more table(s) and click the << arrow if you need to remove them from the Selected Tables list.
Export	Click this to begin data export.

The following table describes the database tables that you can export the table data in this screen.

Table 127 Database Tables

TABLES	DESCRIPTION
accounts	This table contains all user account information.
alarm	This table contains all event alarm information.
mapcomponent	This table contains all device/network/interface information.
midaslog	This table contains all system log information of the ENC.
syslog	This table contains all devices' syslog information.

9.9 Registration

Use this screen to:

- Upgrade to the standard version of the ENC; or
- Increase the number of devices support in the ENC.

Note: The ENC uses myZyXEL.com for registration and activation. See the Quick Start Guide for the registration during the ENC installation. You have to use the registration screen to upgrade the ENC to the standard version or increase the number of devices support; you cannot log in to myZyXEL.com separately for these.

The following information may be required for registration.

Table 128 Information for Using an Existing MyZyXEL.com Account

If you want to use an existing myZyXEL.com account, you need your...
<ul style="list-style-type: none"> myZyXEL.com user name myZyXEL.com password

Table 129 Information for Upgrading the Version or Number of Devices

If you want to upgrade to the standard version or increase the number of devices support, you need your...
<ul style="list-style-type: none"> license key (iCard for the upgrade or increase)

9.9.1 Registration Screen

Use this screen to view your current license status. You can also upgrade your license by entering a license key in this screen. To open this screen, click **Maintenance > Registration**.

Figure 203 Registration

The screenshot shows a web interface for registration. It is divided into two main sections: 'License Status' and 'Service Upgrade'.
License Status: This section displays the current license information. It includes fields for 'License Version' (Standard), 'Expiration Date' (unlimited), 'Support Devices' (1000), and a 'Service Refresh' button.
Service Upgrade: This section allows for upgrading the license. It includes an 'Authentication Code (A/C)' field with the value '0284B797D773774CCEB224E58594BB56000C' and a 'License Key' field with a red asterisk indicating a required field. An 'Upgrade' button is located at the bottom of this section.

The following table describes the fields in this screen.

Table 130 Registration

LABEL	DESCRIPTION
License Status	
License Version	This field displays what version (Standard or Trial) of the ENC you have. You can upgrade your ENC from the trial version to standard version by entering a PIN number on an iCard that you bought.
Support Devices	This field displays the maximum number of devices the ENC can currently support.
Expiration Date	This field displays the date your ENC service expires. unlimited means no expiration.
Service Refresh	Click this button to renew the license information in this screen. You might do this if you re-install the ENC on a different computer.
Service Upgrade	

Table 130 Registration

LABEL	DESCRIPTION
Authentication Code (A/C)	This field displays the authentication code for the ENC. The A/C is a unique number that identifies this installation of the ENC. You have to enter this number in myZyXEL.com if you log in to myZyXEL.com directly.
License Key	Enter your iCard's PIN number and click Upgrade to activate the standard version from trial or extend the number of devices the ENC can support. If you reach the maximum number of devices the ENC can support and you want to extend the number, you need to buy a new iCard (specific to the ENC). Enter the new PIN number in this screen to increase the number.
Upgrade	Click Upgrade to apply a license to the ENC.

9.10 Log

Use this screen to view specific ENC system logs based on the time period, severity level, event category, and/or message content that you specified in this screen. To open this screen, click **Maintenance > Log**.

Figure 204 Log

The screenshot shows the 'System Log' interface. At the top, there are search filters: 'Time' (Last 24 hours), 'Severity' (>= Info), 'Category/Event' (All Category All Event), and a 'Keyword' field. Below these is a 'Search' button. Underneath the search filters are 'Export' and 'Remove' buttons. The main area is a table with columns: Time, Severity, Category, Event, and Message. The table contains 10 log entries, each with a checkbox in the 'Time' column. The messages include events like 'Custom Icon Test has been edited', 'Background Image Test2 has been added', 'Custom Icon Test has been added', 'Custom Device Testing has been added', 'TACACS+ Authentication Edit', 'Radius Authentication Edit', 'Static MAC Forwarding Setting', and 'Bandwidth Control Edit'. At the bottom, there is a pagination bar showing 'Page 1 of 5' and 'View 1 - 10 of 50'.

	Time	Severity	Category	Event	Message
1	<input type="checkbox"/> 2010-09-15 19:33:59	Info	Custom Icon	Icon Edit	Custom Icon Test has been edited by user root.
2	<input type="checkbox"/> 2010-09-15 19:29:42	Info	Custom Icon	Icon Add	Background Image Test2 has been added by user root.
3	<input type="checkbox"/> 2010-09-15 19:28:56	Info	Custom Icon	Icon Add	Custom Icon Test has been added by user root.
4	<input type="checkbox"/> 2010-09-15 19:24:17	Info	Custom Device	Custom Device Add	Custom Device Testing has been added by user root.
5	<input type="checkbox"/> 2010-09-15 19:10:48	Info	Port Management	TACACS+ Authentication Edit	User 172.23.33.133 failed to edit 172.23.33.133@root - Port TACACS+ Authentication.
6	<input type="checkbox"/> 2010-09-15 19:04:04	Info	Port Management	Radius Authentication Edit	User 172.23.33.133 failed to edit 172.23.33.133@root - Port Radius Authentication.
7	<input type="checkbox"/> 2010-09-15 19:03:47	Info	Port Management	Radius Authentication Edit	User 172.23.33.133 failed to edit 172.23.33.133@root - Port Radius Authentication.
8	<input type="checkbox"/> 2010-09-15 19:03:34	Info	Port Management	Radius Authentication Edit	User 172.23.33.133 failed to edit 172.23.33.133@root - Port Radius Authentication.
9	<input type="checkbox"/> 2010-09-15 18:52:03	Info	Port Management	Static MAC Forwarding Setting	172.23.33.133@172.23.33.133 - Port Static MAC Forwarding has been set by user root.
10	<input type="checkbox"/> 2010-09-15 18:50:26	Info	Port Management	Bandwidth Control Edit	172.23.33.133@172.23.33.133 - Port Bandwidth Control has been edited by user root.

The following table describes the fields in this screen.

Table 131 Log

LABEL	DESCRIPTION
Time	Select within the number of hours or days in the past during which the ENC's system logs were generated for the search criteria.
Severity	The log severity level from high to low are Fatal > Error > Warn > Info . Select the comparison expression for the logs you want to see. The options are greater than or equal to (>=), equal to (=), and less than or equal to (<=). For example, select ">= Error " if you want to see the fatal and error logs.

Table 131 Log

LABEL	DESCRIPTION
Category/Event	Select the category and event type of the logs you want to view.
Keyword	Type a keyword of the message you want to view the logs.
Search	Click this to have the ENC pull the logs according to the search criteria.
Export	Click this to export the log entries displayed in this screen to a MidasLog.csv file on the computer you are using to access the ENC.
Remove	Click this to delete the selected logs after you double confirm the action.
check box	Select the check box of an entry and click Export or Remove to take the action for the entry respectively. Select or clear the check box at the table heading line to select or clear all check boxes in this column.
Time	This field displays the date and time the log entry was generated.
Severity	This field displays the severity level of the log entry.
Category	This field displays the category name to which the log belongs.
Event	This field displays the event type to which the log belongs.
Message	This field states the reason for the log.

9.11 About

Use this screen to see the ENC's software version, release date and copyright. To open this screen, click **Maintenance > About**.

Figure 205 About


About	
SoftWare Version:	1.1.218.61.00
Release Date:	2010-09-30
Copyright:	Copyright(c) 2010 ZyXEL Communications Corp. (All rights reserved)

The following table describes the fields in this screen.

Table 132 About

LABEL	DESCRIPTION
SoftWare Version	This is the ENC's software version.
Release Date	This is the release date of the said software version.
Copyright	This shows copyright information such as the year when the software was released and the name of the company that released it.

Troubleshooting

This chapter covers potential problems and the corresponding remedies.

10.1 Installation Problem

The ENC or PostgreSQL cannot be installed properly

- 1 Make sure that the computer meets the minimum hardware and software requirements. See the quick start guide for more information.
- 2 Close all programs before the installation.
- 3 Remove any previous versions of the ENC software from your computer. See the Quick Start Guide for information on how to do this.
- 4 Stop PostgreSQL before the ENC installation if it has been installed in the same computer.
- 5 Re-install the ENC.
- 6 If the problem still persists, contact your vendor. You may need to provide the following information:
 - all LOG files under the “%ENC_install_path%\ENC\ENC\lib\configuration” directory, and “%install_path%\pgsql\installPG.log” and “%ENC_HOME%\bin\midas.log” files
 - the operating system name and version of the computer
 - the ENC version that you want to install
 - the PostgreSQL version if you have installed it before the ENC
 - a screenshot capture of the Command Prompt window that shows the ENC’s installation progress

10.2 Problem Accessing the ENC

I cannot access the ENC

- 1 Make sure that the computer you are using to access the ENC meets the minimum hardware and software requirements. See the Quick Start Guide for more information.
- 2 Make sure you are using the correct IP address.
- 3 Make sure the ENC is running by checking the Windows system tray. You can also click **Start > Run** and type "services.msc" to enter the **Services** screen, make sure the status of services "ENC_pgsql" and "ZyXEL Enterprise Network Center" are both **Started**.
- 4 Make sure the firewall on the ENC server and/or any firewall device between your computer and the ENC allows your access. Turn them off to have a quick test if you do not have security concerns.
- 5 Check for any error in the "%ENC_install_path%\ENC\ENC\bin\midas.log" file.
- 6 Restart the ENC.

I forget the **root** password.

The default password is **root**. If you have changed it, contact your local vendor.

I can see the Login screen, but I cannot log in to the ENC.

Make sure you have entered the user name and password correctly. The user name and password are case-sensitive, so make sure [Caps Lock] is not on. If this does not work, contact the network administrator or local vendor.

10.3 Problem Finding a Device

In the OTV panel, I cannot find my device.

- 1 By default, auto-discovery is disabled. You have to start it manually in the **Tool > Auto-Discovery** screen if you have not run the program yet.
- 2 The maximum number of devices the ENC can manage depends on the license the ENC is using. For example, a trial license supports up to 50 devices. The ENC stops an auto-discovery process if 50 devices have been added to the OTV. You can extend the number of devices by purchasing more licenses. Alternatively, you can remove some devices and then add the new devices.
- 3 You can manually add the device to the ENC. See the Quick Start Guide.
- 4 If you expect to find the device through auto-discovery but cannot find it in the OTV, check the following:

- 4a Check if the auto-discovery program is still active (you can see a **Stop** button in the **Auto-Discovery** screen if it is; otherwise, a **Discover** button displays instead). Wait for a while and check the OTV again if the program is running.
- 4b Make sure your auto-discovery filter rule(s) do not exclude the device.
- 4c If the device supports SNMP, make sure you configure the same SNMP version and community on the ENC. The device's SNMP (port 161) should also be enabled.
- 4d You may have a firewall between the ENC and the device that blocks auto-discovery packets. You may need to stop it or configure a firewall rule to allow traffic between them.
- 4e If the device does not support SNMP, you can use ping to find it by selecting **Enable Ping** in the **Auto-Discovery** screen. If the device does not respond to ping, disable any anti-probe related function on the device.
- 4f Click the **Refresh** icon to update the device list in the OTV.

10.4 Map Problems

I cannot see the Map image that I have uploaded.

Make sure your web browser and the version of it support the image display. See [Section 1.1 on page 17](#) for the browser requirements.

I received "Discover is only allowed on default map" when I perform Auto-Discovery.

Auto-Discovery only searches for and adds devices to the default Map. You have to switch the Map to the default one by clicking the **Map** icon on the left hand of the screen and then changing the Map in the **Map > Open** screen.

10.5 Script Problems

I see "Connection Error" when I execute a script.

- 1 Make sure the telnet service is enabled on the device(s) to which you want to apply the script.
- 2 Make sure there are not any firewall devices between the ENC and the device(s) or configure a firewall rule on them, which allows telnet access from the ENC to the device. Try to turn the firewall off first to see if it helps.

10.6 Event Action Problems

I see “connection fail” when I test an e-mail notification action.

- 1 Make sure you have entered a correct IP address or domain name for the mail server in the **Maintenance > Server** screen.
- 2 Make sure you have entered an existing e-mail address for the **Sender Mail** setting.
- 3 Make sure the **Authentication** settings are correct.

10.7 VLAN/Port Management Problems

I cannot see some switches in the VLAN/Port Management screen.

At the time of writing, VLAN Management and Port Management are not available for all switches. Check the supported switch models listed in the release note.

10.8 Lose Connection Problems

The ENC begins to respond extremely slowly.

You may have lost the connection with the ENC due to one of the following reasons:

- The network is busy. Try to do your operation again later.
- The ENC server is busy or disconnected. Try to do your operation again later.
- An administrator disconnected your session. Try to log in to the ENC again later. Contact the ENC administrator if this happens again.
- Another person used the same account to log in to the ENC. Two or more users may have the same account but only one account can log in at the same time. The first user will be logged out (without notification) when a second user logs in, in this case. Try to log in to the ENC again later. It is suggested that every user has an unique account.

10.9 Syslog Problems

I cannot see any device logs in the **Tool > Syslog View > Log Viewer** screen.

- 1 The ENC does not automatically collect system logs from devices. To see a device's syslog on the ENC, you have to configure the syslog settings on devices to forward syslogs to the ENC server.
- 2 If the syslog settings on the device is properly configured but you still cannot see any of them on the ENC, make sure no firewall or any devices between the device and the ENC blocks the traffic.

10.10 Configuration Backup Problems

I see "backup configuration failed, download the file from FTP failed".

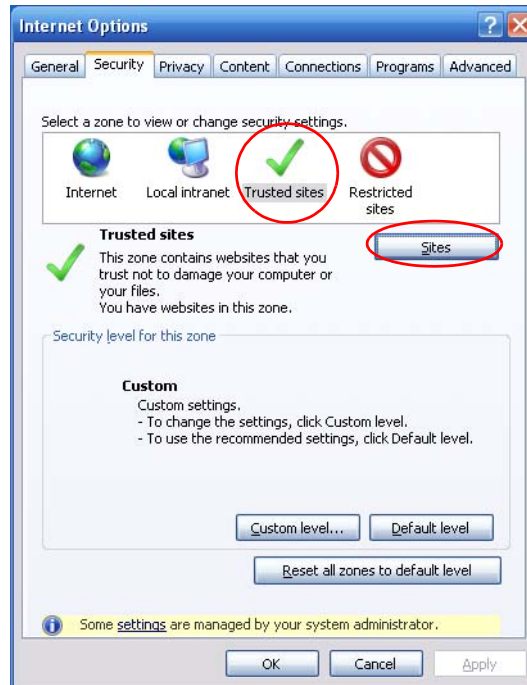
- 1 The ENC uses the device's login username and password settings configured in the **Tool > Inventory > Device** screen to connect to the device through FTP and then backs up the configuration file. Make sure you have configured the correct user name and password for the device on the ENC and the device allows FTP access.

10.11 Other Problem

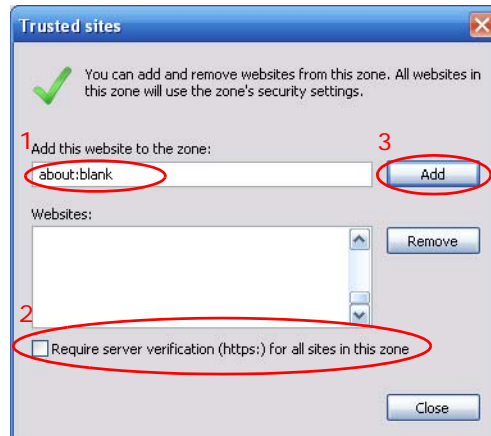
I suddenly cannot type-in any texts into screen fields.

- 1 If you are using Internet Explorer, you may encounter this problem. You can click **Tools > Internet Options > Security** from your browser.

- 2 Click **Trusted sites** and then the **Sites** button.



- 3 Type "about:blank" in the **Add this website to the zone** field. Do NOT **Require server verification (https:)** for all sites in this zone. Then click **Add**.



- 4 Click **Close** and then **OK**. Then your problem should be resolved.

Product Specifications

This appendix summarizes ENC's specifications.

ENC Specifications

This section summarizes ENC's specifications.

Table 134 Software Specifications

FEATURE	DESCRIPTION
Default Administrator's Name	root
Default Administrator's Password	root
Web Configurator Access	http://{ENC server's IP}
User Account Types	Administrator, Operator, User
Number of managed devices	Up to 1000
Number of HTTP connections	Up to 20 (up to 10 is recommended)
License Types	<ul style="list-style-type: none"> • Trial - up to 50 devices, all function supported within 45 days • Standard - the number of devices supported depending on iCard node license you bought
Environment Specification	<ul style="list-style-type: none"> • 2002/95/EC (RoHS) Restriction of Hazardous Substances Directive • 2002/96/EC (WEEE) (WEEE) Waste Electrical and Electronic Equipment Directive • European Parliament and Council Directive 94/62/EC of 20 December 1994 on packaging and packaging waste
Supported ZyXEL Devices	<ul style="list-style-type: none"> • Ethernet Switch - XGS-4528F, GS-4024, GS-2200-24, ES-3124PWR, ES-2024A, ES-4124, XGS-4526, ES-3124, ES-3148, ES-2024PWR, ES-2108, ES-2108PWR, ES-2108-G, GS-4012F, XGS-4028 • ZyWALL (ZLD-based) - ZyWALL USG 100/200/300/1000/2000 • Wireless AP - NWA1100, NWA3100, NWA3160, NWA3163, NWA3165, NWA3166, NWA3500, NWA3550, NWA1300-N Series • IP PBX - X6004, X2002 • IP Phone - V301-T1, V501-T1

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

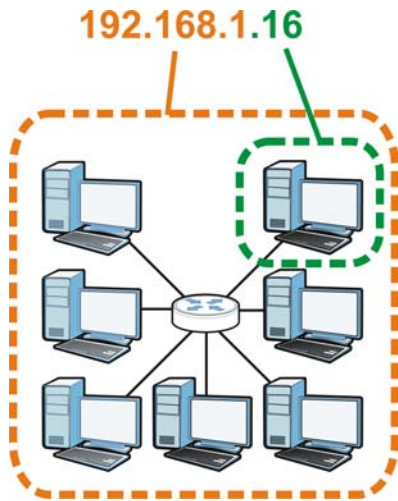
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 206 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 135 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	11111111	11111111	11111111	00000000
Network Number	11000000	10101000	00000001	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 136 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 137 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 138 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192

Table 138 Alternative Subnet Mask Notation (continued)

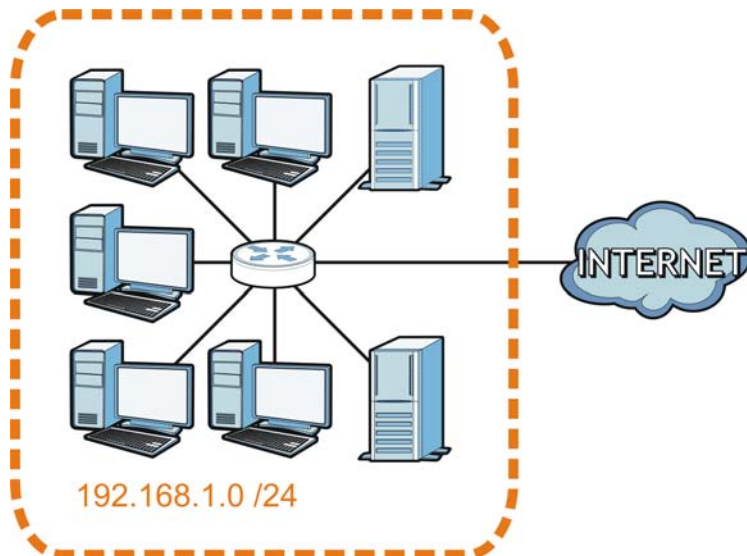
SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

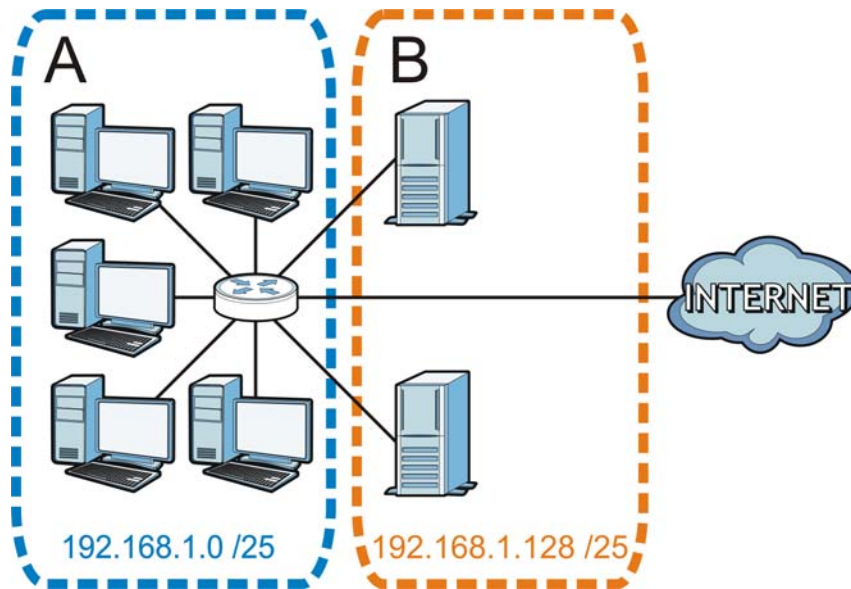
Figure 207 Subnetting Example: Before Subnetting

You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 208 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 139 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000

Table 139 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 140 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 141 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 142 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 143 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 144 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 145 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14

Table 145 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ENC.

Once you have decided on the network number, pick an IP address for your ENC that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ENC will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ENC unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

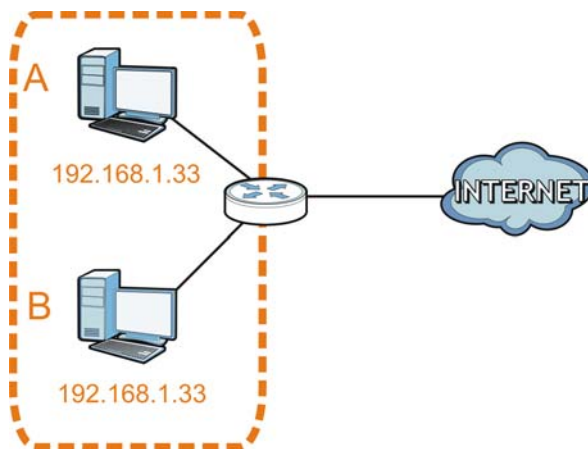
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

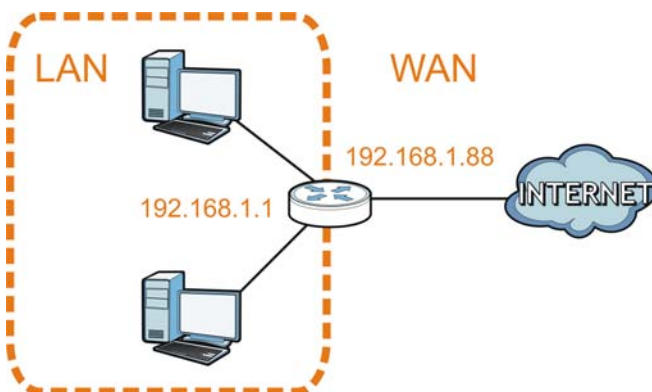
Figure 209 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

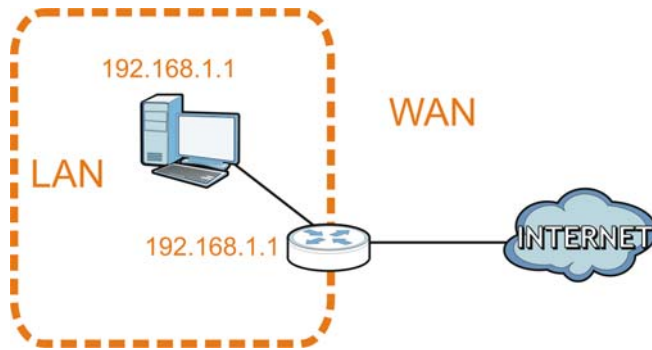
Figure 210 Conflicting Router IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 211 Conflicting Computer and Router IP Addresses Example



Pop-up Windows, JavaScript and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

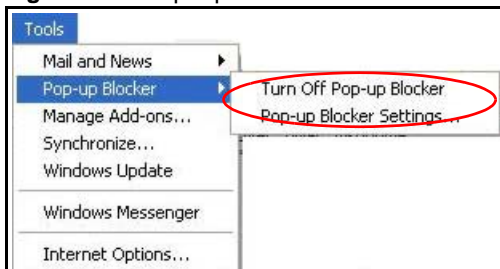
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 212 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.

- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 213 Internet Options: Privacy



- 3 Click **Apply** to save this setting.

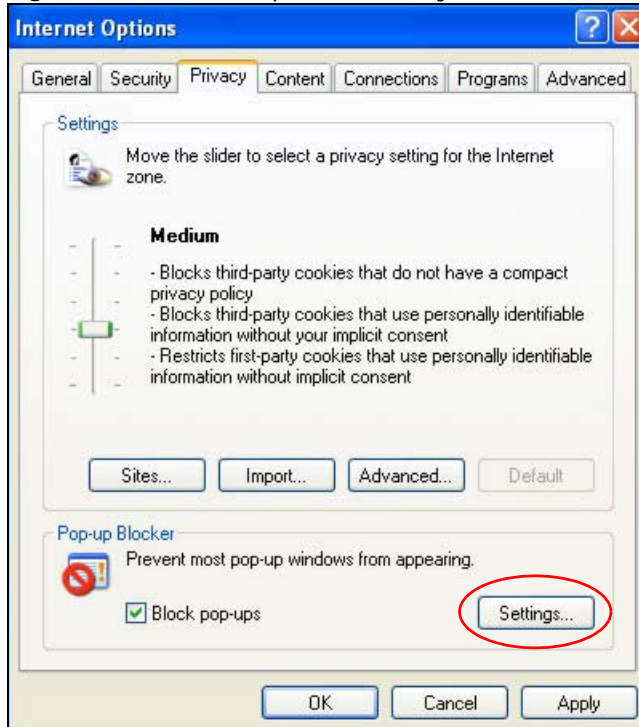
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

Figure 214 Internet Options: Privacy



- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

- Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 215 Pop-up Blocker Settings



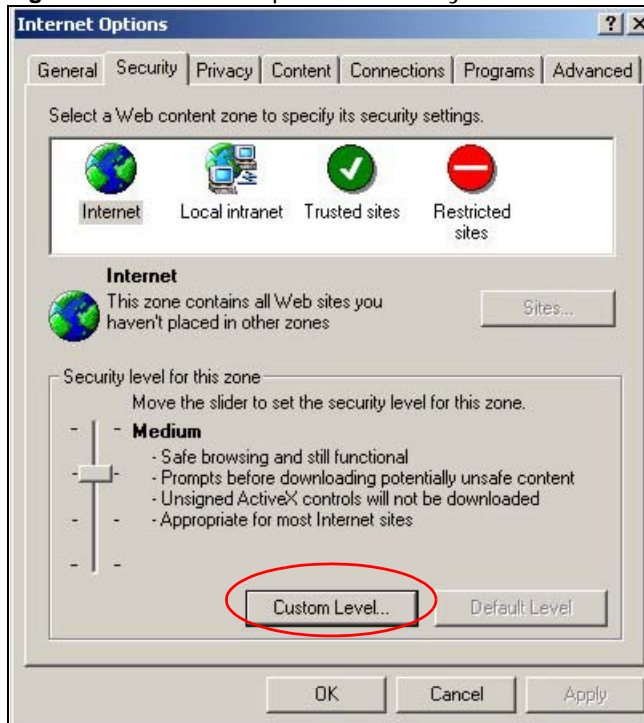
- Click **Close** to return to the **Privacy** screen.
- Click **Apply** to save this setting.

JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

- 1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

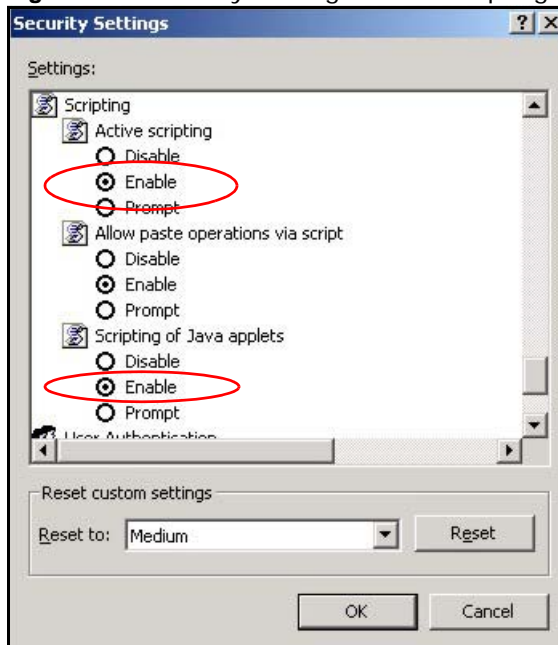
Figure 216 Internet Options: Security



- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

- 6 Click **OK** to close the window.

Figure 217 Security Settings - Java Scripting

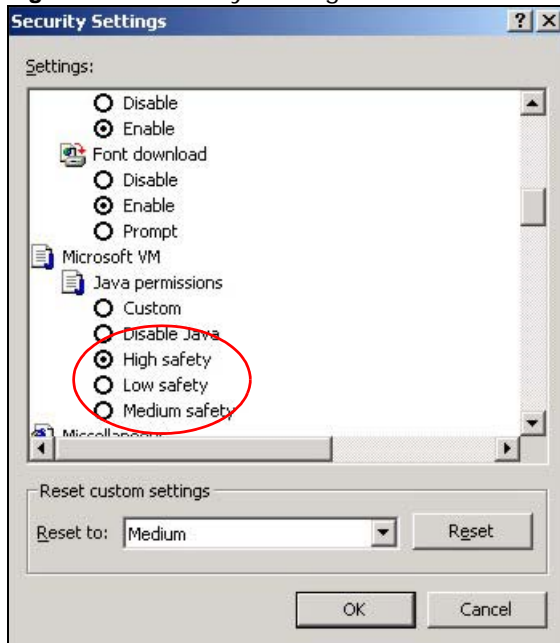


Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.

- 5 Click **OK** to close the window.

Figure 218 Security Settings - Java

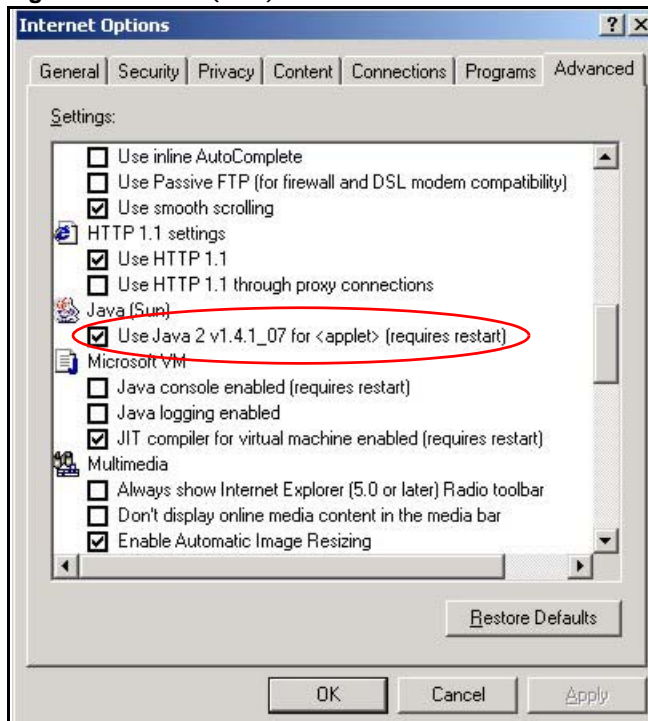


JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

- 3 Click **OK** to close the window.

Figure 219 Java (Sun)

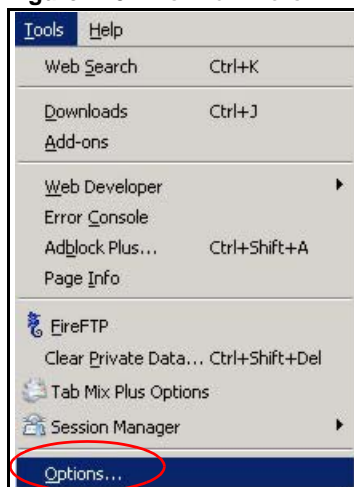


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

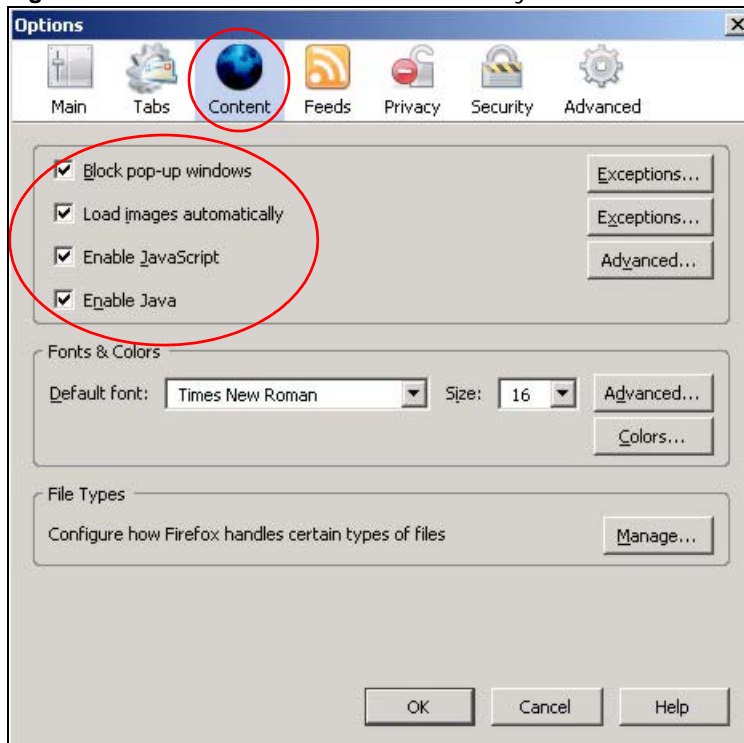
You can enable Java, Javascript and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

Figure 220 Mozilla Firefox: Tools > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 221 Mozilla Firefox Content Security



Open Software Announcements

End-User License Agreement for "ENC"

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED. HOWEVER CERTAIN COMPONENTS OF THE SOFTWARE, AND THIRD PARTY OPEN SOURCE PROGRAMS INCLUDED WITH THE SOFTWARE, HAVE BEEN OR MAY BE MADE AVAILABLE BY ZyXEL LISTED IN THE BELOW NOTICE (COLLECTIVELY THE iOPEN-SOURCED COMPONENTASi). FOR THESE OPEN-SOURCED COMPONENTS YOU SHOULD COMPLY WITH THE TERMS OF THIS LICENSE AND ANY APPLIABLE LICNESING TERMS GOVERNING USE OF THE OPEN-SOURCED COMPONENTS, WHICH HAVE BEEN PROVIDED ON THE LICENSE NOTICE AS BELOW FOR THE SOFTWARE.

1. Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2. Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3. Copyright

The Software and Documentation contain material that is protected by International Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4. Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or

otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL listed in the below Notice (collectively the iOpen-Sourced Componentsi) You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components, which have been provided on the License Notice as below for the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the Software, and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5. Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6. No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERRUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7. Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE,

OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyxEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyxEL's AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8. Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyxEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9. Audit Rights

ZyxEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10. Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyxEL all copies of the Software and Documentation in your possession or under your control. ZyxEL may terminate this License Agreement for any reason, including, but not limited to, if ZyxEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyxEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11. General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyxEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

NOTE: Some components of this product incorporate source code covered under the open source code licenses. Further, for at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the ZyxEL Technical Support

(support@zyxel.com.tw), for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the version of the Programs that we distributed to you if we are in possession of such.

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyxEL Communications Corporation.

This Product includes mibble software under GPL license.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no

warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works

in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program

subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

The product includes jQuery project software. You may use any jQuery project under the terms of either the MIT License or the GNU General Public License (GPL) Version2.

The MIT License is recommended for most projects. It is simple and easy to understand and it places almost no restrictions on what you can do with a jQuery project.

If the GPL suits your project better you are also free to use a jQuery project under that license.

You don't have to do anything special to choose one license or the other and you don't have to notify anyone which license you are using. You are free to use a jQuery project in commercial projects as long as the copyright header is left intact.

The GPL License is on the above.

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The product includes FusionCharts Free software. FusionCharts Free is dual licensed under the MIT (X11) and GNU GPL licenses. You can choose the license that best suits your project, and use it accordingly in both your commercial or personal projects.

The GPL License and the MIT License are both on the above.

In a nutshell, the above licenses allow you to:

- iUse the software for any purpose, commercial or personal
- iModify the software's source code to suit your needs
- iShare the software with your friends and neighbors
- iRe-distribute the software as part of your software or hardware applications

RE-DISTRIBUTION AS A PART OF A PRODUCT/SOFTWARE/APPLICATION

FusionCharts Free is completely free to OEM and distribute with your open or closed source applications. We would be thankful to receive the following information from you:

iYour company name & address

iName and description of your product with which you'll be re-distributing "FusionCharts Free"

Send us an email at support@fusioncharts.com with the above information. We would also appreciate a link back from your product website to our website www.fusioncharts.com/free

WARRANTY

InfoSoft Global expressly disclaims any warranty for the software. THE SOFTWARE AND ANY RELATED DOCUMENTATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH YOU.

INDEMNIFICATION

You hereby indemnify and hold harmless InfoSoft Global and its affiliates against any loss, liability, damages, costs or expenses suffered or incurred by the Indemnified Parties at any time as a result of any claim, action or proceeding arising out of or relating to your use, operation or damages, costs or expenses which may be suffered or incurred at any time by you as a result of your reliance upon or use of the Software. InfoSoft Global SHALL NOT BE LIABLE FOR DAMAGES OF ANY KIND, INCLUDING GENERAL, DIRECT, SPECIAL, INCIDENTAL AND CONSEQUENTIAL DAMAGES, RESULTING FROM OR ARISING OUT OF THIS AGREEMENT OR YOUR USE OF THE SOFTWARE.

Legal Information

Copyright

Copyright © 2011 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

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.

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 ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the

corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Index

Numbers

802.1Q VLAN [208](#)

A

absolute [207](#)
 account permissions
 Map [27](#)
 account types [243](#)
 add device
 read community [40](#)
 write community [40](#)
 administrator account type [244](#)
 administrator permissions [243](#)
 AES [40](#)
 alternative subnet mask notation [273](#)
 ARP [151](#)
 authentication
 and RADIUS [230](#)
 MD5 [40](#)
 SHA1 [40](#)
 auto-discovery
 tutorial [60](#)

B

background image of Map [31](#)
 bandwidth control [222](#)
 broadcast storm control [224](#)

C

CIR [222](#)
 color of device icons [24](#)
 color of network icons [24](#)

command scripts
 editing [107](#)
 managing [106](#)
 note of write commands [108](#)
 Committed Information Rate, see CIR [222](#)
 common tables fields [44](#)
 Compiling MIB databases [159](#)
 cookies [17](#)
 copy device
 Map [43](#)
 copyright [301](#)
 creating a VLAN group [210](#)

D

daily reports [169, 185](#)
 dashboard [19, 85](#)
 delta [207](#)
 DES [40](#)
 destination lookup failure, see DLF [224](#)
 Device Discovery
 automatic [135](#)
 manual [135](#)
 device icon
 color definitions [24](#)
 device list window
 right-click menus [33](#)
 device port
 network statistics [190, 235, 238, 240](#)
 device view [25](#)
 device window
 unassociate a device [42](#)
 disclaimer [4, 301](#)
 DLF [224](#)
 dragging a device to a VLAN [210](#)

E

encryption
 AES [40](#)
 DES [40](#)
examples (tutorials) [47](#)
external authentication server [230](#)

F

Firefox [17](#)
flow control
 back pressure [220](#)
 IEEE 802.3x [220](#)
functions of OTV [24](#)

G

Graph [199](#)
graph of RMON statistics [193](#)
group view [26](#)

H

help of Web Configurator [20](#)

I

IANA [278](#)
iCard [259](#)
icon
 Info event [43](#)
 Major event [43](#)
 Minor event [43](#)
 offline [43](#)
 online [43](#)
 partial online [43](#)
 un-monitored [43](#)
IEEE 802.1x
 reauthentication [234](#)

IEEE 802.3x flow control [220](#)
Info event icon [43](#)
Internet Assigned Numbers Authority
 See IANA [278](#)
Internet Explorer [17](#)

J

Java permissions [17](#)
JavaScript [17](#)

L

license key [259](#)
limit MAC address learning [228](#)
link of Map [27, 82](#)
login [18](#)
login account types [243](#)
 administrator [244](#)
 operator [244](#)
 user [244](#)
logout
 Web Configurator [20](#)
logs
 event [123, 126, 127, 128, 129, 131](#)
logs of Web Configurator operations [20](#)

M

MAC address [151](#)
 maximum number per port [228](#)
MAC address learning [226, 228, 229](#)
main menus [21](#)
main window [33](#)
Major event icon [43](#)
Map [24](#)
 account permissions [27](#)
 background image [31](#)
 link [27, 82](#)
 menu bar [27](#)
 menu bar location [28](#)
 zoom [28](#)

MD5 [40](#)
 menu bar location of Map [28](#)
 menu bar of Map [27](#)
 message center [20](#)
 severity [21](#)
 MIB (Management Information Base)
 compiling [159](#)
 Minor event icon [43](#)
 monthly reports [169](#), [185](#)

N

NAT [278](#)
 navigation panel [24](#)
 Netscape Navigator [17](#)
 network statistics for a device port [190](#), [235](#), [238](#),
 [240](#)
 number of broadcast, multicast and DLF packet
 limits [224](#)
 number of devices
 increase allowed [258](#)

O

on-line help [20](#)
 Operator account type [244](#)
 OTV [24](#)
 right-click menus [33](#)
 OTV functions [24](#)
 OTV network icon
 color definitions [24](#)

P

paste device
 Map [43](#)
 Peak Information Rate, see PIR [222](#)
 ping test [158](#)
 PIR [222](#)
 pop-up windows [17](#)
 port isolation [217](#)

port security [226](#)
 address learning [228](#)
 port-based VLAN
 port isolation [217](#)
 product registration [302](#)

R

RADIUS [230](#)
 advantages [230](#)
 and authentication [230](#)
 Network example [230](#)
 server [230](#)
 read community [40](#)
 registration
 iCard [259](#)
 license key [259](#)
 product [302](#)
 related documentation [3](#)
 Remote Network Monitor, see RMON [189](#)
 removing a device from a VLAN [210](#)
 resolution recommended [17](#)
 right-click menus
 OTV [33](#)
 RMON [189](#)
 alarm [189](#)
 device ports [190](#), [235](#), [238](#), [240](#)
 event [189](#)
 graph view [193](#)
 history [189](#)
 table view [191](#)
 RMON event [203](#)
 logs [205](#)
 parameters [206](#)
 thresholds [207](#)
 RMON groups [189](#)
 RMON history
 graph view [199](#)
 table view [197](#)
 RMON probe [189](#)
 root account [244](#)

S

- scheduled reports [169, 185](#)
 - requirements [177](#)
- screen resolution [17](#)
- Service Set [235](#)
- Service Set IDentification [235](#)
- severity setting of message center [21](#)
- SHA1 [40](#)
- SNMP
 - agents [93](#)
 - commands [94](#)
 - managed devices [93](#)
- SSID [235](#)
- static MAC address [226](#)
- static MAC forwarding [226, 229](#)
- STP
 - port state [222](#)
- subnet [271](#)
- subnet mask [272](#)
- subnetting [274](#)
- supported browsers [17](#)
- syntax conventions [5](#)
- system logs [123, 126, 127, 128, 129, 131](#)
- system uptime [87](#)

T

- TACACS+ [230](#)
 - setup [232](#)
- time-stamp of logs [123](#)
- title bar [20](#)
- trace route test [158](#)
- troubleshooting
 - access the ENC [263](#)
 - auto-discovery [264](#)
 - configuration backup [267](#)
 - connection lost [266](#)
 - event action [266](#)
 - installation [263](#)
 - Map [265](#)
 - script [265](#)
 - syslog [267](#)
 - VLAN/port management [266](#)

- tutorial
 - auto-discovery with filters [60](#)
- tutorials [47](#)

U

- unassociate a device [42](#)
- upgrade
 - license version [258](#)
- uploading
 - command scripts [107](#)
- user account type [244](#)
- user profiles [230](#)

V

- version
 - license
 - upgrade [258](#)
 - standard [258](#)
- VLAN
 - port-based, isolation [217](#)
- VLAN management
 - note [208, 209](#)

W

- warranty [301](#)
 - note [301](#)
- Web Configurator [17](#)
 - common table fields [44](#)
 - device view [25](#)
 - group view [26](#)
 - idle timeout [19](#)
 - logout [20](#)
 - message center [20](#)
 - recommended resolution [17](#)
 - requirements [17](#)
 - supported browsers [17](#)
- weekly reports [169, 185](#)
- write community [40](#)