MXview User's Manual

Edition 11.1, March 2017

www.moxa.com/product



MXview User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

© 2017 Moxa Inc. All rights reserved.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc. All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

<u>Moxa China (Shanghai office)</u>
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505
<u>Moxa Asia-Pacific</u>
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Tel:

Fax:

+91-80-4172-9088

+91-80-4132-1045

Table of Contents

1.	Key Features	1-1
	Web-based Operation	1-2
	Auto Discovery and Topology Visualization	1-2
	Event Management	1-2
	Configuration and Firmware Management	2-1۱
_		1-2
2.	System Requirements and Supported Devices	2-1
	System Requirements	2-2
	Supported Devices	2-2
3.	Installation and System Backup	3-1
	Installation Procedure	3-2
	Uninstallation	3-2
	System Backup	3-2 2 2
	System Restore	
4.	Getting Started	4-1
	MXview Server Startup	4-2
	Login	
	Login Messages	4-44 4-5
	Password Policy	4-6
	Auto Installation of Runtime Environment (Java Runtime Environment)	
Б	Quick Start Using the Setup Wizard	E_1
5.	Using the Sotup Wizard	
	Step 1' Create Group	
	Step 2: Configure the SNMP Community String	
	Step 3: Add the networks you want to scan	5-3
	Step 4: Draw the topology	5-6
	Step 5: Set the SNMP Trap Server to get events in real time	5-7
	Virtual Demo Network	5-8
6.	Dashboard Overview	6-1
	Menu Bar	6-2
	Topology Map	6-3
	Device List	6-3
	Device Properties List	6-4
_		
7.	Device Discovery and Polling	
	Changing the Read Community String	1-/ د ح
	Stall Range	7-2 7-3
	Import Device List	
	Export Device List	
	Device Discovery	7-4
	Plug-in Manager for MXview	7-6
8.	Topology Management	8-1
	Multi-laver Tree Structure	8-1
	Auto Topology and Auto Layout	8-2
	Redundant Topologies	8-4
	PoE Power Consumption Visualization	8-5
	VPN Tunnel Visualization	8-5
	PRP/HSR Visualization	8-6
	Port Trunking	0-7 8-7
	Add Link	
	Delete Link	8-8
	Delete Device	8-9
	Navigation	8-9
	Background	8-10
	Export Topology	8-10
	OPC Tag Generation	8-10
9.	Event and Notification	9-1
	Monitoring Methods	9-2
	Monitoring via SNMP Trap Messages	9-2
	Monitoring via Periodic Polling	9-3
	Culor Coding Indicates Problems	9-3
	L VEH (NEUVELY	9-3

	Severity Level	9-4
	Custom Events	9-4
	Recent Events	9-7
	Event History	9-8
	Notification	9-9
	Add an SMS Action	
	Add an Email Action	
	Add an SNMP Trap	
	Add a Mobile Notification	
	Add a Sound	
	Add an External Program.	
	Add a Message Box	9-17
	System Event	9-18
	Network Event Playback	9-18
	Enable Playback Mode	9-19
	Enter Dayback Mode	0_10
	Time Made and Event Mede	
	Overview of Disvback User Interface	
10.	Traffic Reporting	10-1
	Checking the Trend	
	Threshold & Event Notification	
11	Device Management	11_1
11.		11-11
	Device Properties	
	Device virtual Panel	11-3
	Changing Device Properties	
	Assign Icon	
	Web Console Login	
	Management Interface	
	Configuration Backup and Restoration (Moxa devices only)	
	Firmware upgrade	
	Refresh Status	
	Mass Operation Configuration Export/Import and Firmware Upgrade	
	Export Configurations from Multiple Devices	11-7
	Import a Configuration to Multiple Devices	11-8
	Upgrade Firmware on Multiple Devices	11-8
	Scheduled Configuration Export/Import	11-8
	Configuration Change History and Comparison	11-9
	Device and Inventory Report	11-10
12.	Visualization Mode	12-1
	VI AN Visualization	12-2
	IGMP Snooning Visualization	12-2
	Traffic Load Visualization	12-3
	Security View	12-4
	Wireless Dashboard	12-10
13.	MIB	13-1
	MIB Browser	13-2
	OID Import Manager	13-3
	Trap Import Manager	13-5
14.	MXview License	
	Checking the License	1 <i>1</i> .1
	Liconce Ilnarade	14 ⁻ 1 1/1
_		
Α.	FAQ	A-1
в.	License	B-1

Moxa MXview network management software gives you a convenient graphical representation of your Ethernet network, and allows you to configure, monitor, and diagnose Moxa networking devices. MXview provides an integrated management platform that can manage Moxa networking devices, such as Ethernet switches and wireless APs, and SNMP-enabled and ICMP-enabled devices installed on subnets. MXview includes an integrated MIB complier that supports any third-party MIB. It also allows you to monitor third-party OIDs and Traps. Network and Trap components that have been located by MXview can be managed via web browsers from both local and remote sites—anytime, anywhere.

The following topics are covered in this chapter:

- Web-based Operation
- Auto Discovery and Topology Visualization
- Event Management
- Configuration and Firmware Management
- **Traffic Monitoring**

Web-based Operation

MXview uses the client-server model. You will need to install the MXview server on a Windows computer connected to the network(s) that are to be managed. After installing MXview, the network can be managed with Internet Explorer or Firefox, without installing additional software.

Auto Discovery and Topology Visualization

Within the scan range, MXview locates networking devices with SNMP or ICMP services enabled. MXview can collect topology information from devices with LLDP capability and draw the topology of the network, which shows physical connections. For ICMP devices without LLDP, MXview's advanced auto-topology function can verify the connection relationship through ARP algorithms, and help you create an accurate drawing of the network topology. If any managed PoE switches are in your network, the PoE power output information will also be visualized automatically (for more details on PoE visualization, refer to the PoE **Power Consumption Visualization section** in Chapter 8.)

Event Management

For troubleshooting purposes, MXview logs events that match preset conditions, such as link up/down, device unreachable, or traffic overloading. The most recent events will show up on the dashboard. Devices and links that generate events will be highlighted with different colors. When an event occurs, users can be notified in a number of different ways, including SMS, email, popup window, sound, or external program.

Configuration and Firmware Management

MXview provides an interface for managing Moxa networking devices from a central location. Users can remotely backup or update configuration files, and upgrade firmware.

Traffic Monitoring

MXview can log the network traffic of network devices that have been discovered.

System Requirements and Supported Devices

The following topics are covered in this chapter:

- **G** System Requirements
- Supported Devices

System Requirements

The computer that MXview is installed on must satisfy the following system requirements:

	System Requirements		
CPU	2 GHz or faster dual core CPU		
RAM	2 GB or higher		
Hard Disk Space	10 GB or higher		
OS	Windows XP Professional,		
	Windows 7 (32/64-bit),		
	Windows 8 (32/64-bit),		
	Windows Server 2008 (32/64-bit),		
	Windows Server 2012 (32/64-bit),		
	Windows Server 2012 R2		

Supported Devices

- MXview supports a full range of functions, such as network status, traffic log, and configuration/firmware file management.
- For other SNMP-enabled devices, MXview supports standard management functions, such as link up, link down, and SNMP MIBII information.
- MXview can only monitor the connectivity of devices that support ICMP.

Installation and System Backup

The following topics are covered in this chapter:

- □ Installation Procedure
- Uninstallation
- □ System Backup
- □ System Restore

Installation Procedure

- 1. Execute the installation program or insert the auto-run CD.
- 2. During the installation, you can choose the directory in which MXview will be installed and the default language, or leave the settings at the default values.
- 3. For the commercial version, you will be asked to enter a license key; the license key can be found on a label attached to the protective sleeve of the CD-ROM.
- 4. After the installation is complete, shortcuts for launching the MXview server will be created on the desktop and in the start menu.

Uninstallation

- 1. Select Start → Control Panel, and then select Add or Remove Programs.
- 2. Select MXview
- 3. Select Remove

You can also uninstall the software by selecting

Start \rightarrow All Programs \rightarrow Moxa \rightarrow MXview \rightarrow Uninstall MXview.

System Backup

To back up the system database and configuration, use **Project** → **Database Backup** to save the backup files. The **Backup startup** window will pop up.

The system exports the backup database to a directory. Use the following link to open the directory:

%MXviewPro_Data%\db_backup

Eventually, the **Database backup completed** event will appear on the **Recent Events** list. Right-click on the event to show the details, which includes the file path of the backup files.

Recen	Recent Events Ack All Unacked Last Fifty Events -							
Ack	ID 1	Source	Source IP	Device Alias	Severity	Description Time Issued		
	1	MXview Server	0.0.0.0		System Information	Database backup completed, store in %MXviewPRO Data%/db backup/ 2012-11-02 15:28:33		
Recen	t Events	Ack All Unack	ed Last Fifty Events	•		0 0 All Events		
Ack	ID 1	Source	Source IP	Device Alias	Severity	Description Time Issued		
	1	MXview Server	0.0.0.0	Dotoile	System Information	Database backup completed, store in %MXviewPRO Data%db backup\ 2012-11-02 15:28:33		
				Details				

	3			
Γ	Event ID: 1			
	Source:	MXview Server		
	Source IP:	0.0.0.0		
	Severity:	System Information		
L	Time Issued:	2012-11-02 15:28:33		
	AckTime:	None		
	Event Description:			
	Database backup com 21102 152833	pleted, store in <u>%MXviewPRO Data%db backup\201</u>		
	21102 192099			
	Detail Information			
		Close		

The backup folder uses the following naming convention: YYYYMMDD HHMMSS

The items included in the system backup are listed below:

- Topology
- Traffic
- Availability
- Event
- Threshold settings
- Job scheduler settings
- OID items
- Trap items
- System settings

System Restore

MXview versions 2.2 and higher supports configuration backup files, which use the file extension *db3. To restore a system configuration from a backup file, first shut down MXview. Then, select the **DB Restore tool** in **Start** \rightarrow **All Programs** \rightarrow **Moxa** \rightarrow **MXview** \rightarrow **DB Restore tool**. Log in using your username and password. Next, identify where the backup files are located: (1) MXview's archive repository, or (2) A custom specific directory. Identify the folder where your backup files are located, and then click **Restore**. The MXview system will restore the backup files.

This process is illustrated step-by-step below:

1. Select Start → All Programs → Moxa → MXview → DB Restore tool



2. Login with your username and password

Login	
UserName: Password:	
	Login Cancel

3. Choose the folder where the backup files are located

Database Restore Tool		×
Restore from MXview's archive repository	Restore from a specific folder	
Historical backups		
Date	Time	
2012/09/26 2012/10/01	15:04:17 16:24:59	
2012/11/02	15:28:33	
	Restore Close	e

4. Click Restore

Database Restore Tool
Restore from MXview's archive repository Restore from a specific folder
Backup Folder:
Close
Information
Database has been restored.

MXview versions 2.1 and earlier use *.dat backup files. To restore the system database and configuration from a .dat file, use **Project** \rightarrow **Import MXview Configuration file**, and then select the backup file to restore.

4

Getting Started

The following topics are covered in this chapter:

- MXview Server Startup
- Login
- Login Messages
- □ Account
- Password Policy
- **D** Auto Installation of Runtime Environment (Java Runtime Environment)



MXview is implemented as a web server to realize remote management through a single portal. The following figure illustrates the operational model.

The MXview server runs in the background on a Windows PC and communicates with network devices using Simple Network Management Protocol (SNMP) and a Moxa proprietary protocol that periodically polls specific MIB data and stores data in a local database.

The MXview client uses web browsers to provide a uniform web interface that enables network operators to access and operate over an intranet or the Internet.

MXview Server Startup

To start the MXview server, first double-click the MXview desktop shortcut. When the MXview window (shown below) pops up, configure the listening port of the server (or leave it at the default value of 80) and examine the runtime information. The server will launch when you click **Start**.

Clicking **Launch Client** will start the MXview client on the local computer. To learn how to use the MXview client remotely, refer to the **Login** section below.

MXview ver 2.7				
MX	VIOW Industrial N Managemen	etwork nt Software		
ver 2.7	Moxa Inc. All rights reserved 201	16.		
Service Info]			
HTTP Port	80 Disable HTTP port	Start		
HTTPS Port	443	Stop		
System Status:	Stop			
Connect to MXview with Built-in Browser				
ОК	Launch Client	Stop & Quit		

NOTE Selecting "Connect to MXview with Built-in Browser" is recommended.

Login

To launch the MXview client, open a web browser and input the MXview server's IP address or domain name in the address field. Note that if the server's listening port changes, you will need to input the IP address as follows: http://[IP address]:[Port] (e.g. http://192.168.1.250:8080). If you are using the server computer as the client, you may also click **Launch Client** on the control panel. The default account is **admin**. For MXview version 2.6 and earlier, no password is required. For MXview version 2.7 and later, the default password is **moxa**.



NOTE A maximum of 10 users can log in to the system at the same time.

NOTE For remote users, downloading "MXviewClient" from the MXview server, and using "MXviewClient" to login are recommended.

Login Messages

- 1. Navigate to **Project** \rightarrow **Preferences** \rightarrow **Login Notification**.
- 2. Users can set their Login Message and Login Authentication Failure Message.

MX Preferences	
Vser User	Login Messages
Account Management	
Password Policy	Login Message
Topology	
Appearance	
Security View	Login Authentication Failure Message
Advanced	
System Configuration	
SNMP Configuration	
Events	
Management Interface	
	OK Close

Account

There are 3 default accounts (admin, user and guest) with 2 different authorities (Administrator and User), as shown below.

Preferences					×
Ner User	Account Management				
Account Management					
Policy	Account List				
Login Notification	Active	User Nar	ne A	uthority	
Display		admin	Ac	dministrator	
		guest	U	ser	
Appearance					
Device Appearance					
Advanced					
System Configuration					
{03 SNMP Configuration			Create	Modify Remove	1
Events			Create	Remove	J
"Here"					
L L					
			ОК	Close	

Default User Name	Default Password	Authority
admin	moxa	Administrator
user	-	User
guest	-	User

The "Administrator" can change configurations in MXview, such as topology and scan range. The "User" authority has read-only permission. For MXview version 2.7 and later, accounts can be created, modified and removed and given different authority permissions.

NOTE Up to 100 accounts can be created.

Password Policy

- 1. Navigate to **Project** → **Preferences** → **Password Policy**.
- 2. For the Account Password Policy, users can set a minimum length for the password and enable the password complexity strength check.
- 3. For the Account Login Failure Lockout, users can set the retry failure threshold and lockout time.

MAX Preferences				×
User	Pas	sword Policy and Lockou	it Setting	
Account Management				
Password Policy	Account Password Policy —			
Login Notification	Minimum length	4	(4-16)	
Display	Enable password comple	exity strength check		
Topology	At least one digit (0~9))		
Appearance	Mixed upper and lowe	er case letters (A~Z, a~z)		
Device Appearance	At least one special c	haracter (~!@#\$%^&* ;:	.,.<>[[{}())	
Security View				
Advanced	Account Login Failure Lockou	t		
System Configuration	Enable Data failure thread ald		(4.40)	
Device	Retry failure threshold	3	(1-10)	
	Lockout time (min)	3	(1-60)	
SNMP Configuration				
Events				
Management Interface				
				Class
		OK	· [Close

Auto Installation of Runtime Environment (Java Runtime Environment)

The MXview client must run in a JRE environment. For users who do not have the appropriate version of JRE, MXview will guide users to install the appropriate version of JRE automatically.

Quick Start Using the Setup Wizard

MXview provides a Setup Wizard that can be used to quickly determine the network topology and handle basic configuration tasks.

The following topics are covered in this chapter:

- Using the Setup Wizard
 - Step 1: Create Group
 - > Step 2: Configure the SNMP Community String
 - > Step 3: Add the networks you want to scan
 - Step 4: Draw the topology
 - > Step 5: Set the SNMP Trap Server to get events in real time
- Virtual Demo Network

Using the Setup Wizard

The wizard will launch automatically when the software does not contain any nodes. To launch the Setup Wizard manually, select **Project** → **Wizard**. You should see the following window:

🔤 Setup Wizard		—
Welcome to MXview Industrial Network Management Software Setup Wiza	ard	
Welcome to the setup wizard.		
 This wizard will help you: 1. Add scan range 2. Draw Topology (with devices that support LLDP) 3. Set SNMP trap server 4. Use N-Snap to take an network snapshot. 		
	Next	Cancel

The wizard will guide you through five basic steps, described below.

Step 1: Create Group

Devices scanned by MXview can be organized into a multi-layer tree structure. Before finding devices, groups need to be created. Root is the only default group. All other created groups are placed under the next level of Root.

Create Gr	oup	,
	Root Test	
	Create	

Step 2: Configure the SNMP Community String

MXview uses SNMP to collect device information. The default SNMP configurations are:

- Version: v1
- Read community string: public
- Write community string: private

If necessary, update this information at this time:

🏧 Setup Wizard				
SNMP Settings Select SNMP version ar	d required parameter	s for acquiring device info	rmation	
	SNMP Version Read Community Write Community	V1 v public private]	
			Next	Cancel

Step 3: Add the networks you want to scan

MXview's operation is based on IP (Internet Protocol). Other devices in the scan range that use IP to operate will be located and monitored.

🔤 Setup Wizard					X	
Scan Range Add IP ranges to scan for devices						
Scan Range Active	ge First IP Addre 192.168.127.1	Last IP Address 192.168.127.254	Name SITE	Group Root	Add Network Modify Network Delete Network	
					Next Cancel	

Click **Add Network** to add a network range to scan. A window will pop up, with two tabs: **Single Range** and **Multiple Ranges**.

Single Range: Enter the first and last IP address in the desired range. Name this range in the Name field.

Single Range Multiple Ran	ages			
Active				
First IP Address		•		
Last IP Address				
Name				
Group	Root			•
			OK	Cancel

Multiple Ranges: The Multiple Ranges tab allows you to set up a complicated subnet for scanning. Select **enable** for the subnet range, similar to using a subnet mask. You can also name the scan range, as in the Single Range tab.

Single Range Mul	tiple Ranges				
Active enable	 enable . 	•	enable ~	• []	~
Name Group	Root		-		
			ок		Cancel

an Ran	ge				Add Network
Active	First IP Addre	Last IP Address	Name	Group	Modify Notwork
1	192.168.127.1	192.168.127.254	SITE	Root	
					Delete Network
					-
nport D	evice List				
nport D t a device I	evice List ist to import to MXvi	ew			
nport D t a device I ers\Deskto	evice List ist to import to MXvi ip\Device_List	ew			
oort D	evice List				

Another way to scan the network is to **Import Device List**. Click **Import Device List** and select a list file to load the devices into MXview.

NOTE A device's IP address must be configured properly before it can be managed by MXview.

At this point, MXview will enter the discovery stage. The time needed to complete this stage depends on the size of the scan range. Click **Cancel** at this point to exit the wizard; however, the configurations entered previously will be saved and the discovery process will continue running in the background.

🔤 Setup Wizard
Scanning Discovering devices and topology
16%
Clicking the Cancel button will exit the wizard. But the discovering process will keep working in background.
Next Cancel

Step 4: Draw the topology

After all devices have been located, MXview will be able to draw the topology for LLDP devices.

Informa	tion 🔀
2	Draw topology(with devices having LLDP)
	OK Cancel
Informa	tion 🛛
Informa	tion 🔀 Do You Want to Auto Layout Topology?

For devices without LLDP functionality, the topology can be drawn manually after the wizard is finished.

After all devices have been discovered and the topology has been created, click **Next** to continue to the next step.



Step 5: Set the SNMP Trap Server to get events in real time

To enable real-time event generation, the MXview server's IP address needs to be configured as a trap server. To do this, enter the IP address of the MXview Server and then click **Set** to activate the change.

If this step is skipped, devices can still be monitored by polling periodically, although a time latency will be introduced.

🟧 Setup Wizard	\mathbf{X}
SNMP Trap Server Set the SNMP trap server to capture events in rea	I time
IP Address Community String	· · ·
Enter the address and the community string, or *The process may take from a few seconds to a few minut *This action will overwrite the original settings of discove	leave them empty to skip tes depending on the number of discovered devices. red devices
	Next Cancel

After this point, MXview initialization is complete.

Setup Wizard Welcome to MXview Industrial Network Management Software Setup Wizard
Congratulations!
You have completed the basic configuration. MXview has already begun to monitor your network.
✓ Launch N-Snap to take an network snapshot.
Complete



Virtual Demo Network

MXview provides a virtual demo network that can be used to evaluate many features of MXview. To activate the virtual demo network, run Setup Wizard and select the **Start Demo Network** option at the bottom of the window.



Next

Cancel



By following the MXview Setup Wizard, you can easily build up the network environment.

	Setup Wizard						8
	Scan Range						
	Add IP rang	ges to scan for d	evices				
l r	Scan Rang	ge				Add Network	
[Active	First IP Addre	Last IP Addre	Name	Group		
		10.20.30.1	10.20.30.4	Virtual Network	Virtual Demo n	Modify Network	
						Delete Network	
Г	Import De	evice List					
s	elect a device li	st to import to MXvie	ew				
						Next	el
						Cance	

After the Setup Wizard is done, you can experience MXview with the virtual demo network.



6

Dashboard Overview

The Dashboard should appear when you log in to MXview. When using MXview, you will spend most of your time working from the Dashboard, which is divided into the following sections:

- 1. Menu Bar
- 2. Topology Map
- 3. Device List
- 4. Device Properties List
- 5. Small Scale Topology Map
- 6. Recent Event List
- 7. Status Bar



The following topics are covered in this chapter:

- Menu Bar
- Topology Map
- Device List
- Device Properties List
- Recent Events List

Menu Bar

All operations can be accessed from the following menu bar items:

Project

Use the **Project** menu to scan devices with multiple IP ranges, add devices with a specific IP address, maintain network groups, set up MXview preferences, or start the Setup Wizard. Also, you can back up data and configurations of the monitored networks, event history, job schedules, or network topology to a local file, or import a project file to create monitored networks on the fly.

View

Use the **View** menu to change the appearance of the Topology Map. For example, you can adjust the resolution or create a topology map.

Device

Use the **Device** menu to configure or examine the properties of objects.

Link

Use the **Link** menu to delete a link or get traffic reports.

Information

Use the **Information** menu to examine network-wide properties.

Event

Use the **Event** menu to examine events and set up notifications.

Tools

Use the **Tools** menu to launch additional services or programs, such as Moxa IP Configurator.

MIB

Use the **MIB** menu to compile or browse for a third party MIB. Import third party OIDs and Traps through the OID import manager and the Trap import manager.

Help

Use the **Help** menu to view license information or information about MXview.

Topology Map

The **Topology Map** displays connection relationships of monitored devices. For devices with LLDP capability, the connections can be drawn automatically.



Device List

The **Device List** shows the Topology Map structure in tree format. Note that link information is not shown. Type all or part of a device name in the "Search Devices" input box to only show devices whose names contain that keyword (for example, type "EDS" to show all EDS devices, or type "EDS-G509" to show all EDS-G509 switches in the network.

Q Search Devices	
Device List	
⊡ <mark>7</mark> 4 Root	~
192.168.127.5 SNMP Device	
	*

Device Properties List

The **Device Properties** list shows the properties of the device that is currently selected. If a device's interface is a PoE port, the icon will change to include a yellow electric charge.

- 🚺 Alias	192.168.129.2 EDS-P506A
- 🚺 ModelName	EDS-P506A
- 1 MAC Address	0090E8040404
- 🚺 Availability	100.00%
- 🕕 sysDescr	MOXA EDS-P506A-4P0E
- i sys0bjectId - i sysContact	1.3.6.1.4.1.8691.7.41
- 🚺 sysName	Managed Redundant Switch 00000
- sysLocation	Switch Location
- 1 ifNumber	8
interface.1	down / 100M / Full-duplex
Interface.2	up / 10M / Full-duplex
interface.3	down / 10M / Full-duplex
Sinterface.4	up / AWK-3121 / 10M / Full-du
🖲 🔳 interface.5	up / 10M / Full-duplex 👻

Recent Events List

This list shows the events that have occurred most recently.

Event Count lists the total number of events of different types, with different event types identified by different colored rectangles (e.g., red, yellow, and green, as shown in the following screen shot).

All Events is the shortcut of the menu item **Event** → **All**. When you click **All Events**, a window will pop up showing all events.

Recent Events Ack All Unacked Last Fifty Events 31 2 31 All Events						
Ack	ID	T ■ 1 Source Sou	Source IP	Severity	Description	Time Issued
	40	MXview Server	192.168.127.182	Information	Device ICMP reachable	2011-12-26 15:26:16 🔺
	39	MXview Server	192.168.127.236	Information	Device ICMP reachable	2011-12-26 15:26:16
	38	MXview Server	192.168.127.254	Information	Device ICMP reachable	2011-12-26 15:26:16
	37	MXview Server	192.168.127.252	Warning	Device SNMP unreachable	2011-12-26 15:26:16 📥
	36	MXview Server	192.168.127.253	Critical	Device ICMP unreachable	2011-12-26 15:26:15
	35	MXview Server	192.168.127.250	Critical	Device ICMP unreachable	2011-12-26 15:26:15 🧫
	24	MVview Cower	100 160 107 005	Critical	Dovice ICMP upreachable	2011 12 26 46 26 21 1100

Device Discovery and Polling

Devices in the assigned scan range can be discovered via SNMP and ICMP protocols. After a device is discovered, MXview will use SNMP and ICMP to poll the device periodically. To configure this function properly, you will need to know the following information:

- 1. The IP addresses of the devices on the network.
- 2. The Read community name assigned to the devices on the network.

Changing the Read Community String

The default Read community string that is used to discover devices is **public**. Take the following steps to change the value:

- 1. Select **Project** → **Preferences** → **SNMP Configuration**.
- 2. Enter the new Read community string.

WX Preferences	
Preferences	SNMP Configuration
User Display Advanced System Configuration Simple Configuration Events	SNMP Version VI v Read Community public Write Community private
	OK

Scan Range

You can assign multiple scan networks, with each network defined by a starting IP address and an ending IP address. MXview will discover all active devices that belong to the scan networks.

Take the following steps to add a scan network:

1. Select **Project → Scan Range**.

🚥 Network S	an Range			X
Scan Rang	e First IP Add 192.168.127	ess Last IP Address 1 192.168.127.50	s Name A	Add Network Modify Network Delete Network
Deleted De	vices Mod	al L	ocation	Recover
			OK and Run Discovery	Cancel

2. Click Add Network.

🗮 Add Network				
C Active				
First IP Address	1	25		
Last IP Address		8		
Name				
Group	Root	~		
	(ок	Cancel	

- 3. Input the starting and ending IP addresses of the range, and then click **OK**.
- 4. Click **OK & Discovery** to start discovery.
- **NOTE** Device discovery will require more time for larger networks. For this reason, if possible you should avoid defining large scan ranges.

Deleting a scan network will remove the monitored devices that belong to the network. Take the following steps to delete a scan network:

- 1. Select **Project → Scan Range**
- 2. Select a row in the table Scan Range
- 3. Click Delete Network
- 4. Click **OK** to activate the change

Modifying a scan network will remove devices that do not belong to the new network, and discover new devices within the new network. Take the following steps to modify a scan network:

- 1. Select Project → Scan Range
- 2. Select a row in the table Scan Range
- 3. Click Modify Network
- 4. Modify the starting and ending IP address of the range, and then click **OK**
- 5. Click **OK** to activate the change.

Deselecting the **Active** checkbox of a scanned network will stop device discovery for that network. Previously discovered devices will continue to be monitored, with the current status shown on the topology map.

Import/Export Device List

By using this function, users can easily export any device into a device list, and also can import any device list into MXview.

Import Device List

- 1. Select **Project → Import Device List**
- 2. Select a list and click **Open**
- 3. All the devices in the list are imported into MXview

Proj	<mark>ect</mark> View Device Link Information	n Event Tools MIB Help
	Scan Range Add Device	Neiwork Management Software
	Paste Device List	Root
	Group	
	Preferences	
	Wizard	
	Import MXview Configuration File	
	Database Backup	
_	Import Device List	
	Export Device List	
	Log Out	


Export Device List

- 1. On the Topology Map, Select the devices which will be exported into the list
- 2. Select Project → Export Device List
- 3. Enter a file name and click **Save**
- 4. The device list is saved



NOTE The **Device List** can be utilized in all the software of MXstudio, including MXconfig, MXview, and N-Snap.

Device Discovery

MXview will use SNMP and ICMP to discover devices within the scan ranges. When a Moxa device has been located, MXview will use an actual image of the device, such as the one shown here, to indicate the device's location on the network.



MXview will also list detailed properties and configuration parameters, including the following:

- MAC address
- Model name
- IP address
- Netmask
- Gateway
- Trap server address
- Auto IP configuration
- Type of redundancy protocol
- Role in redundancy protocol
- Status and properties of the port
- Status of the power
- Status and version of the SNMP protocol

MXview will use one of the following graphics to indicate devices:

Moxa devices with SNMP enabled.	SNMP
Third party devices with SNMP enabled.	SNMP
Third party devices with ICMP enabled.	ICMP

The IP address and location name of the discovered device will be shown under the image of the device. Take the following steps to change the location name:

- 1. Select the device
- 2. Select Device→ Maintenance→ Configure IP & SNMP
- 3. Select the **Basic** tab and then enter the new location name.

MXview will run conduct device discovery periodically to find new devices in the scan ranges. You may also use the following steps to conduct device discovery manually:

- 1. Select project → Scan Range
- 2. Click OK & Run Discovery

Discovered devices will be polled periodically by ICMP and SNMP. This is done for the following reasons:

- 1. To monitor the availability of devices.
- 2. To update properties and configuration parameters of devices.
- 3. To update traffic information, such as utilization.

Plug-in Manager for MXview

For Moxa devices without default support by MXview, add the Plug-in Kits of these devices into MXview through the **Plug-in Manager**, and the devices' icons will be shown on the MXview **Topology Map**.

- 1. Select MXview → Plug-in Manager for MXview in Start menu
- 2. Enter the username and password which are the same as MXview
- 3. In Plug-Ins page, click Add and select a Plug-in Kit folder
- 4. The Plug-in models are shown in the list and successfully added into MXview
- 5. Exit Plug-in Manager and login MXview, and these models' icons can be shown on Topology Map

Login			
UserName:			
	Login	Cancel	
Plug-in Manager fo	r MXview 2.4		
Plug-Ins Built-in Lis	t]		1
	rently installed	plug inc	
_• 🕞 Cur	rentry instaned	piug-ins	
_• Ser Cur	Version	Description	
Model	Version	Description Plug-In for ICS-G7748A	
Model ICS-G7748A ICS-G7750A-2×G	Version 1.0 1.0	Description Plug-In for ICS-G7748A Plug-In for ICS-G7750A-2×G	
Model ICS-G7748A ICS-G7750A-2XG ICS-G7752A-4XG	Version 1.0 1.0 1.0 1.0	Plug-Ins Plug-In for ICS-G7748A Plug-In for ICS-G7750A-2×G Plug-In for ICS-G7750A-4×G Plug-In for ICS-G7752A-4×G	
Model ICS-G7748A ICS-G7750A-2×G ICS-G7752A-4×G ICS-G7848A ICS-G7848A	Version 1.0 1.0 1.0 1.0 1.0 1.0 1.0	Plug-Ins Plug-In for ICS-G7748A Plug-In for ICS-G7750A-2×G Plug-In for ICS-G7752A-4×G Plug-In for ICS-G7848A Plug-In for ICS-G7850A-2×G	
Model ICS-G7748A ICS-G7750A-2×G ICS-G7752A-4×G ICS-G7850A-2×G ICS-G7850A-2×G ICS-G7850A-2×G	Version 1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0	Description Plug-In for ICS-G7748A Plug-In for ICS-G7750A-2×G Plug-In for ICS-G7752A-4×G Plug-In for ICS-G7848A Plug-In for ICS-G7850A-2×G Plug-In for ICS-7852A	
Model ICS-G7748A ICS-G7750A-2×G ICS-G7752A-4×G ICS-G7850A-2×G ICS-G7850A-2×G ICS-G7850A-2×G ICS-G7852A-4×G	Version 1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0	Description Plug-In for ICS-G7748A Plug-In for ICS-G7750A-2×G Plug-In for ICS-G7752A-4×G Plug-In for ICS-G7848A Plug-In for ICS-G7850A-2×G Plug-In for ICS-7852A	
Model ICS-G7748A ICS-G7750A-2×G ICS-G7752A-4×G ICS-G7850A-2×G ICS-G7850A-2×G ICS-G7852A-4×G	Version 1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0	Description Plug-In for ICS-G7748A Plug-In for ICS-G7750A-2XG Plug-In for ICS-G7752A-4XG Plug-In for ICS-G7848A Plug-In for ICS-G7850A-2XG Plug-In for ICS-7852A	
Model ICS-G7750A-2×G ICS-G7750A-2×G ICS-G7752A-4×G ICS-G7850A-2×G ICS-G7850A-2×G	Version 1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0	Description Plug-In for ICS-G7748A Plug-In for ICS-G7750A-2×G Plug-In for ICS-G7752A-4×G Plug-In for ICS-G7848A Plug-In for ICS-G7850A-2×G Plug-In for ICS-7852A	
Model ICS-G7748A ICS-G7750A-2×G ICS-G7752A-4×G ICS-G7850A-2×G ICS-G7850A-2×G ICS-G7852A-4×G	Version 1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0	Description Plug-In for ICS-G7748A Plug-In for ICS-G7750A-2×G Plug-In for ICS-G7752A-4×G Plug-In for ICS-G7848A Plug-In for ICS-G7850A-2×G Plug-In for ICS-7852A	Add Remove

Topology Management

The **Topology Map** is the core of MXview, and can be used to complete most actions. The Topology Map shows a graphical representation of the devices in your networks, and can be used to do the following:

- Display a graphical representation of a real network.
- Show connecting relationships between devices.
- Indicate the status of devices and links.

Multi-layer Tree Structure

The Topology Map can be organized into a multi-layer tree structure of up to 5 layers. It helps users manage a large number of nodes on the computer screen. For example, users can move nodes of the same subnet or location into the same group. Root, which is the only one group at the first layer, exists by default and cannot be deleted. Groups created by users are in the layer under Root. Devices can be moved between groups. MXview uses an icon to indicate user-defined groups:



The first layer will be shown as:



192.168.127.236

The second layer will be shown as:



192.168.127.237

Auto Topology and Auto Layout

For devices with LLDP functionality, MXview can draw the physical topology map, down to the port level of the devices. For devices without an LLDP MIB, MXview is able to draw links by using ARP. To activate this function, select the **Advanced Topology Analysis** checkbox.

MXview can do the following two tasks automatically: (1) Create a new topology, and (2) Update the existing topology.

Creating a new topology deletes all links, requests LLDP information from devices, and draws topology maps based on the gathered information.

- 1. Select View → Auto Topology
- 2. Select **New Topology**
- 3. Click OK

NOTE Links drawn manually will be also deleted by this action.

NOTE Your devices must have firmware version 3.1 or higher to use **Advanced Topology Analysis**.

NOTE If the AutoTopology function does not create an accurate representation of the actual network, deselect the **Advanced Topology Analysis** check box and try again.

Updating the existing topology adds new links and updates existing links, but does not change the status of links that are indicated as having been disconnected or links that were drawn manually.

- 1. Select View → Auto Topology
- 2. Select **Update Topology**
- 3. Click OK

🔤 Auto Topology
New Tapelegy
Existing links will be deleted first
Update Topology
Existing links will be kept while new links are added
Advanced Topology Analysis
Auduonai une is requireu.
OK Cancel

The following figure shows an example of a topology map:



Auto topology supports third-party devices which are compatible with LLDP MIB.

	Moxa Device*	Third-party SNMP Device	IP Device
Auto Topology LLDP MIB		LLDP MIB	Supported if
	ARP-based auto topology		connected to a
	(Moxa switch w/firmware 3.1)		Moxa switch.

NOTE LLDP is enable	d by default on Moxa devices.	Please keep LLDP enabled	to use the Auto Topology fu	unction.
---------------------	-------------------------------	--------------------------	-----------------------------	----------

Redundant Topologies

Redundant topologies have at least one backup link, which will be indicated with a dashed line:



For devices that play a particular role in the topology, MXview will label the devices by displaying the roles above the images of the devices. Backup links will be indicated with dotted lines.

- RSTP has a Root
- Turbo Ring has a Master
- Turbo Chain has a Head and a Tail

NOTE Only auto topology can draw dashed lines for redundancy links. Manually drawn redundant links will appear as solid lines.

PoE Power Consumption Visualization

By periodic polling, a PoE link will display the port number, power (watts), voltage (V), and current (mA) directly on the topology map.



VPN Tunnel Visualization

The VPN tunnel link will be indicated using different colored lines, as shown below. An icon in one of three different colors indicates VPN statuses:

• Blue: All VPN tunnels are connected

VPN 192. 683. 122. 254 / Ste ToSke1 192. 683. 122. 254 / Ste doste 192. 103. 128 122. 254 / Ste ToSke1 192. 103. 122. 254 / Ste doste 192. 103. 128 122. 254 / Ste ToSke1 192. 103. 122. 254 / Ste doste 192. 103. 128 122. 254 / Ste ToSke1 192. 103. 122. 123. 123. 123. 123. 123. 123. 12	Firewall VPN
Yellow: At least one VPN tunnel is disconnected	

VPN 192.168.122.254 / SiteTo Site1	192.168.122.254 / sitetosite	Firewall VPN
ĥ. <u>C</u>		_10
	03	
192.168.128.188 192.168.122.2547 Stefe See 2	192.408.122.254 / sitetosite2 1	92.168.127.245

• Red: All VPN tunnels are disconnected

VPN 192.168.122.254 / SiteTo Site1	192.168.122.254 / sitetosite	Firewall VPN
192.168.128.188 p3 192.168.122.2547.31e7e52e2	p3 192,408,122,254 / sitetosite2 19	12.168.127 245

NOTE VPN Tunnel Visualization is only available on Moxa's EDR-810 series of secure routers.

PRP/HSR Visualization

MXview is able to indicate different roles of PRP/HSR technology, including PRP, HSR, Coupling, and Quadbox. The links of PRP/Coupling LAN A, LAN B, and HSR Ring are indicated with different colored lines.





Third-Party Icons

MXview is able to support most network devices, even those made by many different vendors. Below is an example of a network which includes Moxa devices and a Cisco device. MXview will change the device icon to indicate that the device is a Cisco device.



Vendors with MXview support includes: ABB, CISCO, Emerson, Hirschmann, Rockwell, Schneider, and Siemens.



Port Trunking

Port trunking, also called link aggregation, involves grouping links into a link aggregation group. Trunking links will be indicated with thick, solid lines.



NOTE For trunked link, check "Device Properties" to get the port number corresponding to the trunking group.

Port 29 Trunk Group 1: Port 25 (Link up) / Port 26 (Link up)

Add Link

Use one of the following two options to connect two devices with a link in a topology map:

- 1. Right click on a device and then select **Add Link**.
- 2. Click on a device to select it and then click Link → Add Link on the menu bar.
- 3. Enter the ports and IP addresses corresponding to the link. Use the plus sign at the left bottom corner to add multiple entries at one time.

Source IP 192 . 168 . 127 . 105	From Port	Destination IP 0 . 0 . 0 . 0	Destination Port
		· · ·	
+		ОК	Cancel

NOTE Trunking and redundancy links added manually will appear as solid lines.

NOTE Port numbers must be numeric and entered correctly to obtain the correct traffic information.

NOTE For modular switches, a port number depends on the chassis to which the port belongs, but not on how many modules are inserted. For switches such as the PT-7828, the first module's port numbers are from 1 to 8, the second module's port numbers are from 9 to 16, and so on. The port number depends only on which slot the module is in; in other words, the port number is the same regardless of whether other slots are empty or occupied.

Delete Link

Use the following steps to remove a link in the topology map:

- 1. Select the link.
- 2. Right-click the link and select **Delete Link**, or select **Link → Delete Link**.



NOTE Deleting a link will delete a link from the topology map, but it will not affect the actual network configuration.

Delete Device

You can delete devices from the topology map. After a device is deleted, it will be removed from the topology map and scan range, and the device would not be polled or located when conduction device discovery. Take the following steps to delete a device:

- 1. Select the device
- 2. Right-click the device
- 3. Select **Delete Device**

Deleted devices will be recorded in **Project → Scan Range**.

MX	Network Scan Range	a			X
c	Scan Range				
1	Active	First IP Address	Last IP Address	Name	Add Network
		192.168.127.1	192.168.127.250	CBD	Modify Network
					Delete Network
ſ	Deleted Devices	Ma dal		4i	Recover
	192 168 127 100	Deleted Devi	ce 183	allon	
			0	<and discovery<="" run="" td=""><td>Cancel</td></and>	Cancel

You may recover devices that have been deleted. Once recovered, the devices will be polled and located when conducting device discovery Take the following steps to recover deleted devices:

- 1. Select Project → Scan Range
- 2. Select a row in table **Deleted Devices**
- 3. Click **Recover** and then click **OK**

Navigation

Mini map is a frame with a slider for adjusting the resolution. This function helps users zoom in to enlarge devices or zoom out to view more devices on the screen.



Background

You may insert a background image into the topology map to provide additional references, such as geographical information or deployment layout.

Take the following steps to insert or change a background image:

- 1. Select View → Set Background
- 2. Choose an image from the local file system.

Take the following steps to delete the background image from the topology map:

Project View Device	Link Netw	rork Event Tools Preferen	ces Help				
MXview	V Indus	trial Network Manag	Jement Software			MO	XV
Q - Search Device	ll Devices					[Q Navigation
Device list					10 10 2 2 2 0 2 2 2 0	- 2014038 - 51	- 310 - 10 - 10 - 10 - 10 - 10 - 10 - 10
	5. 1	W.LoLo.	*//	74X :	9° 4°	7' 8'	
Recent Event					Event Count 📕 0	0 🗖 0	All Events
ID .	▲ 1 Source	Severity	Descr	iption I	Issued Time	User	
Configur	ing Discovery	Range Failed	上午 09:35:01	Number of Managed D	evices / Max : 0 / 500		

Export Topology

The topology map can be exported as a JPEG image. Take the following steps to export the topology map:

- 1. Select View → Export Topology
- 2. Choose the location to which the image is saved.

OPC Tag Generation

MXview can generate OPC 2.0-compliant tags of device and link properties. OPC clients such as SCADA Systems can access and use these tags.

- 1. Select Tools → OPC Server
- 2. Click Start

Contract Con	×
Status	
Stopped	
Start	ОК

Currently, the default information that MXview can prepare as tags includes:

- 1. A **Health** tag, which represents the health status of whole network.
- 2. Device IP address, MAC address, and status, which are labeled beginning with D_.
- 3. A link's corresponding IP address and ports, which are labeled beginning with L_.

MXview can also transfer all the SNMP properties in Device Properties List to OPC tags.

- 1. Select Tools \rightarrow Custom OPC Tags
- 2. Click to manually add properties into list
- 3. Select properties in the list and click Register to implement them on devices
- 4. It shows Tag count and Registered device count
- 5. Click OK and finish transferring

www Custom OPC Tags		23
1 Click '+'/-' to add/remove one or more	Select Device Properties	to them
2. If you can't find a property of a device, c	Find	
Activate Property Name	Availability DslLed1 DslLed2 DslLed3 DslLed4 DslLed5 IpAddr IpMask activeProtocolOfRedundancy cpuLoading300s.0 cpuLoading30s cpuLoading30s.0 cpuLoading5s.0 defaultCotenueu OK Cancel	
- Tag count: 0/512	Registered device count: 0 / 1024	gister
	ОК	Close

NOTE The **Health** tag represents the health status of the entire network. There are three levels: Normal, Warning, and Critical, with the values 0, 1, and 2 respectively. MXview allows users to use only one tag to monitor the status of the whole network

🔤 Custom (OPC Tags	Select Devices	×
1. Click '+ 2. If you ci v v v v v v v v	7-' to add/remove one or more custom opt an't find a property of a device, close this dia Property Name cpuL.oading300s cpuL.oading30s cpuL.oading5s devTxRange memoryUsage powerConsumption stpRxPower.16 stpTemperature.16 stpTxPower.16 stpTxPower.16	All devices 192.168.127.1-ICS-G7852A-4XG 192.168.127.2-IKS-6728-8PoE 192.168.127.3-VPort 36-1MP 192.168.127.9-VPort 36-00 192.168.127.10-IEX-402-SHDSL 192.168.127.11-IEX-402-SHDSL 192.168.127.12-EDR-810 192.168.127.13-MGate MB3170 192.168.127.20-ICMP Device	Selected devices
		Sort by Model	OK Cancel
+	- Tag count: 10/512 Registe	red device count: 118/1024	Register
		ОК	Close

v cpuLoading300s v cpuLoading5s v devTxRange v memoryUsage v powerConsumption v sfpRxPower.16 v sfpTxPower.16 v sfpTxPower.16 v sfpVoltage.16	Activate	Property Name
Image Image Im	1	cpuLoading300s
Image Image Im	1	cpuLoading30s
Image	V	cpuLoading5s
Image memoryUsage Image: powerConsumption stpRxPower.16 Image: stpTemperature.16 stpTxPower.16 Image: stpVoltage.16 stpVoltage.16	1	devTxRange
v powerConsumption v sfpRxPower.16 v sfpTmperature.16 v sfpTxPower.16 v sfpVoltage.16	V	memoryUsage
Image: sfpRxPower.16 Image: sfpTxPower.16 Image: sfpVoltage.16	v	powerConsumption
Image: sfpTemperature.16 Image: sfpTxPower.16 Image: sfpVoltage.16	v	sfpRxPower.16
Image: sfpTxPower.16 Image: sfpVoltage.16	1	sfpTemperature.16
Image: SfpVoltage.16	v	sfpTxPower.16
	~	sfpVoltage.16

If the properties that you want to transfer are not shown in the properties list, you can use the MXview **MIB Browser** to manually import the MIB files. Then, the **OID Import Manager** can help import the OIDs into Devices Properties List and they will be easily transferred to OPC tags. In the same way, any third-party proprietary MIB can generate its OPC tag.

Example: Retrieving transmission distance though MXview OPC Server

To retrieve transmission distance through MXview OPC Server, the first step is load the relative MIB, and import the transmission distance SNMP OID "devTxRange" into Device Properties List. Then, users can easily find the property in the properties list and transfer it to an OPC tag.

- 1. Select **MIB → MIB Browser**
- 2. Select **File → Load MIB**
- 3. Select the SNMP MIB and add it into the MIB list

MIB Browser		- • •
File Unload MIB MIB Language -MIB Exit POE-MIB MIB MIB	Agent IP 127.0.0.1 SNMP v1 OID Get Get Next Get Subtree Walk Mame/OID Value	Set
		Close

- 4. Select MIB → OID Import Manager
- 5. Click **Add** and select the specific OID
- 6. Assign this OID to selected devices
- 7. The new OID appears in the **Devices Properties List**
- 8. The property "devTxRange" is shown in the properties list and can be transferred to an OPC tag



🛃 Assign Po	lled Devices				•
Name	devTxRange		OID	.1.3.6.1.4.1.8691.3	15.1.1.5.1.1.19.1
All List of Devi 192.168.127 192.168.127 192.168.127 192.168.127 192.168.127 192.168.127 192.168.127 192.168.127 192.168.127 192.168.127 192.168.127	ces 7.1 (192.168.127.1IC: 7.2 (192.168.127.2IK: 7.3 (192.168.127.3ED 7.4 (192.168.127.4ED 7.5 (192.168.127.5ED 7.6 (192.168.127.6ED 7.8 (192.168.127.9NP 7.10 (192.168.127.9NP 7.10 (192.168.127.10) 7.11 (192.168.127.10) 7.11 (192.168.127.12) 7.12 (192.168.127.12) 7.20 (192.168.127.20)	- -G7852A-4XG) S-G728-8PoE) S-G516E) S-G516E) S-G516E) ort 36-1MP) ort S8000) (EX-402-SHDSL) (EX-402-SHDSL) EDR-810) MGate MB3170) (CMP Device)		Add All Add All Remove Remove All	List of Selected Devices 192.168.127.7 (192.168.127.7AWK-3121)
evice Proj	perties				Assign Cancel
i mode seri fir mac/ mac/ ope: i enal i phe i phe i fir fir mac/ i seri i seri seri seri seri seri seri seri seri	elName ialNumber nwareVersion Address rationMode bleAutoIpConfig ddr ask aultGateway pServerAddr pTrapCommunity pZServerAddr pTrap2Community ServerIpAddr.1	AWK-3121-US 8288 1.9 Build 11 00:90:E8:40: ap disable 192.168.127. 255.255.255. 0.0.0.0 alert alert 0.0.0.0	101410 A9:44 7 0	5	192.168.127.7

9

Event and Notification

The following topics are covered in this chapter:

Monitoring Methods

- > Monitoring via SNMP Trap Messages
- > Monitoring via Periodic Polling
- > Color Coding Indicates Problems
- Event Recovery
- Severity Level
- Custom Events
- Recent Events
- Event History
- Notification
 - Add an SMS Action
 - Add an Email Action
 - > Add an SNMP Trap
 - Add a Mobile Notification
 - > Add a Sound
 - > Add an External Program
 - Add a Message Box

Syslog Event

Network Event Playback

- Enable Playback Mode
- Enter Playback Mode
- Time Mode and Event Mode
- > Overview of Playback User Interface

Monitoring Methods

Monitoring can be conducted using SNMP trap messages, periodic SNMP polling, periodic ICMP polling, or color coding, as described in the following subsections.

Monitoring via SNMP Trap Messages

By using the MXview server as a trap destination of a device, events associated with the device will be sent to the server in real time, and can be seen by remote clients.

Take the following steps to set the trap destination of all devices:

- 1. Select Tools → Set Trap Server to All
- 2. Enter the IP address of the MXview server and the community string.

🚥 Set Trap to All	\mathbf{X}
Server Number	1 🗸
IP Address	192 - 168 - 127 - 100
Community String	public
	OK Cancel

Take the following steps to set the trap destination of one device:

- 1. Select Device→ Maintenance→ Configure IP & Trap
- 2. Choose tab Trap Server
- 3. Enter the IP address of the MXview server and community string

🏧 192.168.127.122 Config IP and Trap	
Basic IP Configuration Trap Server	
Destination IP1 Community Name1 Destination IP2 Community Name2	
ОК	Cancel

The event types include port link up/down, power on/off, topology change, and configuration change.

Each discovered device will be monitored automatically by trap once its trap destination is configured correctly.

Monitoring via Periodic Polling

After a device has been discovered, MXview polls the status of the device's active port periodically. Keep in mind that since trap messages are transmitted by UDP protocol, there is no absolute guarantee that the messages will be received. What periodic polling does is provide a higher level of reliability for monitoring devices.

With periodic polling, MXview can passively monitor the device's SNMP service, bandwidth utilization, error packet rate, and collision rate. MXview can also actively monitor device availability through ICMP polling. MXview pings devices every 10 seconds, and calculates average availability in 24 hours.

Separate thresholds can be used for bandwidth utilization, error packet rate, collision rate, and device availability, respectively. When any of these thresholds are surpassed, the device will indicate that an event has occurred.

Color Coding Indicates Problems

When a link causes a warning to be issued or a critical event occurs (link down, for example), the color of the corresponding link line will change:



When a device causes a warning or a critical event occurs (device failure, for example), the errant device will be indicated with a box with red borders.



In addition, the events will be added to the recent events list.

ID	1 Source	Severity	Description	Issued Time	User
225	192.168.127.36	Critical	Port 1 Link Down	2009-11-24 21:36:51	
226	192.168.127.34	Critical	Port 2 Link Down	2009-11-24 21:36:52	

Event Recovery

Events will be recovered automatically when condition that caused the event is resolved.

ID	▲ 1 Source	Severity	Description	Issued Time	User
225	192.168.127.36	Critical	Port 1 Link Down	2009-11-24 21:36:51	
226	192.168.127.34	Critical	Port 2 Link Down	2009-11-24 21:36:52	
227	192.168.127.36	Information	Port 1 Link Down Recovery	2009-11-24 21:38:14	

Severity Level

Events can be set to one of three severity levels: critical, warning, or information. The conditions that give rise to a particular severity level can be configured by the user. To configure the severity levels, select **Project** \rightarrow **Preferences** \rightarrow **Events**, and then modify the settings.

wa Preferences	_			
No Basic	S	everity Threshold	%.	
- 22 User				
Display				
- Kanala Topology	Link Up		Information -	
- Kappearance	Link Down		Critical -	
Device Appearance	Pondwidth Kirolion (war /%)	0	Warning	
Advanced	Bandwidth Ounzaron Over (%)	U	wannig	
	Bandwidth Utilization Under (%)	0	Warning 👻	
O Device	Packet Error Rate Over (%)	0	Warning -	
- SNMP Configuration				
Events	Availability Under(%)	95.00	Warning -	
1				
		0	K Close	

Custom Events

By using the MXview Custom Events, users can define their own events with flexible thresholds, severity, description, and duration.

- 1. Select Event → Custom Events
- 2. Click to manually add properties into list
- 3. Set the Threshold Type, Threshold number, Severity, Description, and Duration
- 4. Select the properties in the list and click Register to implement them on devices
- 5. It shows Tag count and Registered device count
- 6. Click **OK** and finish setting

Activate	Event Name	Threshold 1	Гуре	Threshold	Severity	Description	Duratio	n
		(🔤 Se	lect Device Proper	ties	(×	
				F	ind			
			DslL	.ed1				
			DslL	.ed2				
			DSIL	.ed3 .ed4				
			DslL	.ed5				
			lpAd	dr				
			IpMa	ask				
			activ	eProtocolOfRedun	dancy			
			cpul	_oading300s.0				
			cpul	_oading30s				
			cpul	_oading30s.0				
			cpul	_oading5s.0				
			defa	ultGateway			-	
				Bobbola				
	Too.	count: 0/512		ſ	ОК	Cancel		

Clivate	Event Name	Threshold Type	Threshold	Severity		Description	Duration		
V	cpuLoading300s	Over 🗸	50	Warning	•	CPU Loading High!			
V	cpuLoading30s	Not Equal 🚽		Critical	•				
1	cpuLoading5s	Not Equal 🚽		Critical	•				
1	devTxRange	Not Equal 🚽		Critical	•				
1	memoryUsage	Not Equal 🚽		Critical	-				
1	powerConsumption	Not Equal 🚽		Critical	-				
1	sfpRxPower.16	Not Equal 🚽		Critical	-				
V	sfpTemperature.16	Not Equal 🚽		Critical	-				
V	sfpTxPower.16	Not Equal 🚽		Critical	-				
~	sfpVoltage.16	Not Equal 🚽 🚽		Critical	•				

			All devices		Selected devices	
ctivate	Event Name	Threshold	192.168.127.1ICS-G7852A-4XG		192.168.127.3EDS-G516E	
V	cpuLoading300s	Over	192.168.127.2IKS-6728-8PoE		192.168.127.4EDS-G516E	
1	cpuLoading30s	Over	192.168.127.7AWK-3121		192.168.127.5EDS-G516E	
1	cpuLoading5s	Over	192.168.127.8VPort 36-1MP		192.168.127.6EDS-G516E	
1	devTxRange	Below	192.168.127.9NPort S8000			
V	memoryUsage	Over	192.168.127.10IEX-402-SHDSL			
~	powerConsumption	Over	192.168.127.11IEX-402-SHDSL			
V	sfpRxPower.16	Below	192.168.127.12EDR-810			
V	sfpTemperature.16	Over	192.108.127.13MGale MB3170	<		
V	sfpTxPower.16	Over	192.108.127.201CMF Device			
	sfpVoltage.16	Over				
			Sort by Model		ОК	Cancel
+	- Tag cou	int: 10/512	Registered device count: 0 / 4096		Register	

While the events are triggered, they will be shown in the **Recent Events List** and the related devices will be marked in color.

Roc	đ						Y = 1 = = = 1. Man 🚟
				Part Hat 12 (2017) 2	1 Ring 1 klaster		*
			192.	192.192.193.1273	192.1687	p1 192.198.127.0 277	ш
•		19	2.169.127.7	192.168.127.13 192.1	69.127.12	p2 192.168.127.11 192.168.127.10	
Rece	ent Even	ts Ack All	Unacked Last Fifty E	vents 🗸		107 99	224 All Events
Ack	ID ID	Source	Source IP	Device Alias	Severity	Description	Time Issued
	435	MXview Server	192.168.127.6	192.168.127.6EDS-G516E	Warning	cpuLoading5s: Threshold = 10 , value = 19 CPU Loading High in 5s!	2014-06-19 14:35:51
	434	MXview Server	192.168.127.5	192.168.127.5EDS-G516E	Information	Port 8 Link Up	2014-06-19 14:35:29
	433	MXview Server	192.168.127.6	192.168.127.6EDS-G516E	Information	Port 7 Link Up	2014-06-19 14:35:27
	432	Тгар	192.168.127.5	192.168.127.5EDS-G516E	Warning	LLDP table has changed	2014-06-19 14:35:26
	431	Тгар	192.168.127.3	192.168.127.3EDS-G516E	Information	Turbo Ring Topology has changed	2014-06-19 14:35:26
	430	Тгар	192.168.127.6	192.168.127.6EDS-G516E	Information	Turbo Ring Topology has changed	2014-06-19 14:35:26
	429	Тгар	192.168.127.6	192.168.127.6EDS-G516E	Warning	LLDP table has changed	2014-06-19 14:35:26
	428	Тгар	192.168.127.5	192.168.127.5EDS-G516E	Information	Port 8 Link Up	2014-06-19 14:35:25 🖕

Once the triggered properties are back to normal status, MXview will show recovery events in the **Recent Events List**.

Rece	Recent Events Ack All Unacked Last Fifty Events -						
Ack	ID 1	Source	Source IP	Device Alias	Severity	Description	Time Issued
	436	MXview Server	192.168.127.6	192.168.127.6EDS-G516E	Information	cpuLoading5s is recovered: Threshold = 10 , value = CPU Loading Recovery!	2014-06-19 14:36:48
	435	MXview Server	192.168.127.6	192.168.127.6EDS-G516E	Warning	cpuLoading5s: Threshold = 10 , value = 19 CPU Loading High in 5s!	2014-06-19 14:35:51
	434	MXview Server	192.168.127.5	192.168.127.5EDS-G516E	Information	Port 8 Link Up	2014-06-19 14:35:29
	433	MXview Server	192.168.127.6	192.168.127.6EDS-G516E	Information	Port 7 Link Up	2014-06-19 14:35:27 =
	432	Trap	192.168.127.5	192.168.127.5EDS-G516E	Warning	LLDP table has changed	2014-06-19 14:35:26
	431	Trap	192.168.127.3	192.168.127.3EDS-G516E	Information	Turbo Ring Topology has changed	2014-06-19 14:35:26
	430	Trap	192.168.127.6	192.168.127.6EDS-G516E	Information	Turbo Ring Topology has changed	2014-06-19 14:35:26

NOTE The unit of duration is minutes, and only integer values can be set.

Recent Events

MXview shows recent events at the bottom of the Dashboard.

Rece	ent Even	ts Ack All	Unacked Last Fifty H	events 👻			28 32	31 All Events	
Ack	ID 1	Source	Source IP	Device Alias	Severity	Description		Time Issued	
	66	Trap	192.168.127.6	192.168.127.6	Information	Turbo Ring Topology has changed		2014-06-19 09:26:21	•
	65	Trap	192.168.127.5	192.168.127.5	Warning	LLDP table has changed		2014-06-19 09:26:21	
	64	Trap	192.168.127.5	192.168.127.5	Information	Port 8 Link Up		2014-06-19 09:26:20	
	63	Trap	192.168.127.6	192.168.127.6	Information	Port 7 Link Up		2014-06-19 09:26:20	
	62	Trap	192.168.127.6	192.168.127.6	Critical	Port 7 Link Down		2014-06-19 09:26:19	
	61	Trap	192.168.127.5	192.168.127.5	Critical	Port 8 Link Down		2014-06-19 09:26:19	
	60	Trap	192.168.127.5	192.168.127.5	Information	Port 8 Link Up		2014-06-19 09:26:19	=
	59	Trap	192.168.127.6	192.168.127.6	Information	Port 7 Link Up		2014-06-19 09:26:19	
	58	Trap	192.168.127.3	192.168.127.3	Information	Turbo Ring Topology has changed		2014-06-19 09:26:18	Ŧ

Event History

To show the event history of all devices, select $\textbf{Event} \rightarrow \textbf{All}$ from the menu bar.

To show the event history of a single device, right click the device and select **Events**.

🗮 All Events						×
Filter Cond	itions					
A				0 (
Group	Any			. 0 . (J . U Seventy Any	Reset
Source	Any	✓ A	ck Any	Y From	▼ 00 ▼ : 00 ▼ To	✓ 23 ♥ : 59 ♥
Ack A	AII D					Query
Ack	ID	Source	Source IP	Severity	Description	Time Issued
	19	MXview Server	192.168.127.106	Critical	Device ICMP unreachable	2011-12-26 15:26:11
i ii	20	MXview Server	192.168.127.113	Critical	Device ICMP unreachable	2011-12-26 15:26:11
	21	MXview Server	192.168.127.111	Critical	Device ICMP unreachable	2011-12-26 15:26:11
	22	MXview Server	192.168.127.109	Critical	Device ICMP unreachable	2011-12-26 15:26:11
	23	MXview Server	192.168.127.110	Critical	Device ICMP unreachable	2011-12-26 15:26:11
	24	MXview Server	192.168.127.236	Warning	Device SNMP unreachable	2011-12-26 15:26:13
	25	MXview Server	192.168.127.112	Critical	Device ICMP unreachable	2011-12-26 15:26:13
	26	MXview Server	192.168.127.150	Critical	Device ICMP unreachable	2011-12-26 15:26:13
	27	MXview Server	192.168.127.67	Critical	Device ICMP unreachable	2011-12-26 15:26:13
	28	MXview Server	192.168.127.91	Critical	Device ICMP unreachable	2011-12-26 15:26:13
	29	MXview Server	192.168.127.162	Critical	Device ICMP unreachable	2011-12-26 15:26:13
	30	MXview Server	192.168.127.200	Critical	Device ICMP unreachable	2011-12-26 15:26:13
	31	MXview Server	192.168.127.103	Critical	Device ICMP unreachable	2011-12-26 15:26:15
	32	MXview Server	192.168.127.102	Critical	Device ICMP unreachable	2011-12-26 15:26:15
	33	MXview Server	192.168.127.237	Critical	Device ICMP unreachable	2011-12-26 15:26:15
	34	MXview Server	192.168.127.235	Critical	Device ICMP unreachable	2011-12-26 15:26:15
	35	MXview Server	192.168.127.250	Critical	Device ICMP unreachable	2011-12-26 15:26:15
	36	MXview Server	192.168.127.253	Critical	Device ICMP unreachable	2011-12-26 15:26:15
	37	MXview Server	192.168.127.252	Warning	Device SNMP unreachable	2011-12-26 15:26:16
	38	MXview Server	192.168.127.254	Information	Device ICMP reachable	2011-12-26 15:26:16
	39	MXview Server	192.168.127.236	Information	Device ICMP reachable	2011-12-26 15:26:16
	40	MXview Server	192.168.127.182	Information	Device ICMP reachable	2011-12-26 15:26:16
	41	MXview Server	192.168.127.183	Information	Device ICMP reachable	2011-12-26 15:26:16
	42	MXview Server	192.168.127.181	Information	Device ICMP reachable	2011-12-26 15:26:16
	43	MXview Server	192.168.127.252	Information	Device ICMP reachable	2011-12-26 15:26:16
	44	MXview Server	192.168.127.1	Information	Device ICMP reachable	2011-12-26 15:26:17
	45	MXview Server	192.168.127.12	Information	Device ICMP reachable	2011-12-26 15:26:17 🔍
					- · ···- · · ·	
First Pag	je 🗌 🗌	Previous Page	Next Page	Last Page	1/1 Export to CSV	Clear All Close

The table contains 40 entries on a page. Use the page controls at the bottom to navigate between pages.

First Page	Previous Page	Next Page	Last Page	1/1
------------	---------------	-----------	-----------	-----

You can sort the table by clicking the header cells.

Time issued 🗠 🕆	~	l
-----------------	---	---

To filter the table, use the selection box of the header cell and select a value.

Filter Cond	itions		
Group	Any IP	0.0.0.0 Severity Any	Reset
Source	Any Ack Any	▼ From ▼ 00 ¥:00 ▼ To	✓ 23 ✓: 59 ✓

NOTE The sorting and filtering functions only affect table entries currently showing on the screen. They do not regenerate the entire table. This remains true even if there are currently fewer than 40 entries showing.

You can export all events to a CSV file, or delete all events from the database.

Export to CSV	Clear All

Notification

You can associate an action, such as send a text message, send an email, make a sound, or run an external program, with a combination of a type of event, a source IP address, and a severity level.

There are 7 actions:

- SMS send a SMS text message
- Email send an email
- Program run an external program
- Sound make a sound
- Message Box show a message box
- SNMP Trap send a SNMP trap to other SNMP trap server
- Mobile Client send a push notification to mobile devices

Name SMS Type SMS Phone Number EMail Program Sound Message Box SNMP Trap Mobile Client Mobile Client

There are 19 event types:

- ICMP unreachable
- SNMP unreachable
- Power off
- Power on
- Link down
- Power change to DC
- Power change to AC
- Input Bandwidth Utilization over Threshold
- Input Bandwidth Utilization under Threshold
- Output Bandwidth Utilization over Threshold
- Output Bandwidth Utilization under Threshold
- Input Packet Error Rate over Threshold
- Output Packet Error Rate over Threshold
- Device availability under Threshold
- A custom event is triggered
- A custom event is recovered
- Secure router under DDoS attack
- Secure router firewall under attack
- Secure router trust access under attack

Motification		-X
	Notification	
Notification Name		
Event Type	Secure router trust access under attack	-
Source	ICMP unreachable SNMP unreachable Power off	
Action	Power on Link down Power change to DC Power change to AC	
	OK Cancel	•

Add an SMS Action

To send an SMS notification, first connect an SMS modem, such as the Moxa Oncell, to an MXview Server COM port. Take the following steps to configure SMS notification:

1. Select Event → Notification.

🔤 Notification					×
Action List					
Name		Туре	Contact /	Program / File	New
					Modify
					Delete
Notification List					
Name	Туре	Source	Component	Actions	New
					Modify
					Delete
					Delete
Notification	n Settings				ОК

2. Click Notification Settings.

🔤 Notification Settings	×
EMail SMS SNMP Trap Mobile Client	
SMS COM Port Setup	
COM Port	СОМЗ
Baud Rate	115200 👻
Mode	TEXT Mode 🔹
	OK Cancel

- 3. Turn to SMS page. Select the COM port, Baud Rate, and Mode to which the modem is connected, and then click **OK**.
- 4. Click **New** in the Action List.
- 5. Select SMS as the type, type the phone number, give the action a name, and then click $\ensuremath{\text{OK.}}$

Actions		—
Name	Admin SMS	
Туре	SMS •	
Phone Number	0920123456	
	OK Cancel	

6. Click **New** in the Notification List.

7. Select the action just added and the corresponding event type, source IP.

www.Notification	—		
Notification			
Notification Name			
Event Type	ICMP unreachable		
Source	💿 IP 💿 Group		
Action	Admin SMS		
	OK Cancel		

8. Click **OK**.

Add an Email Action

Take the following steps to configure the Email (SMTP) server to send an Email notification:

- 1. Select **Event** → **Notification**.
- 2. Click Notification Settings.

🔤 Notification Settings 🧮			
EMail SMS SNMP Trap Mobi	le Client		
EMail Server Setup			
Domain Name / IP			
Port Number	25		
Encryption	None		
User Name			
Password			
Sender Address			
	OK Cancel		

- 3. Turn to Email page. Input the SMTP server that can send an e-mail and the user name and password needed to log in to the server, and then click **OK**.
- 4. Click **New** in the Action List.
- 5. Select Email as the type, type the email address, give the action a name, and then click OK.

actions	
Name	Admin Email
Туре	SMS -
Phone Number	admin@your.com
	OK Cancel

- 6. Click **New** in the Notification List.
- 7. Select the action just added and the corresponding event type, source IP.
- 8. Click **OK**.

Add an SNMP Trap

MXview can collaborate with other network management software, and send SNMP Traps to third-party NMSes. MXview supports up to two trap servers. Take the following steps to add an SNMP Trap:

- 1. Select Event → Notification.
- 2. Click Notification Settings.

WW Notification Settings	•••
EMail SMS SNMP Trap Mobile Clien	at
SNMP Trap	
SNMP Version	SNMP Version 1 -
Community Name 1	
Trap Server 1	
Community Name 2	
Tran Sonier 2	
Trap Server 2	
	OK Cancel

- 3. Click the **SNMP Trap** tab. Enter the SNMP version and trap server information, and then click **OK**.
- 4. Click **New** in the Action List.
- 5. Select SNMP Trap as the Type, give the action a name, and then click **OK**.

Actions	
Name	MXview Trap
Туре	SNMP Trap 🔹
	OK Cancel

- 6. Click **New** in the Notification List.
- 7. Select the action just added and the corresponding event type, source IP.
- 8. Click **OK**.

Add a Mobile Notification

MXview can send mobile notifications through Apple APNS or Google C2DM with Moxa's mobile APP *MXview ToGo*.

- 1. Select Event → Notification.
- 2. Click **New** in Action List.
- 3. When the Actions window opens, type in a Name and select Mobile Client as the type.
- 4. Click **Receiver** to select an Email as identification.
- 5. Click **OK.**

Actions		×
Name	Admin Mobile	
Туре	Mobile Client 👻]
Email	admin@your.com	Receiver
	OK Cancel	
Active Mobile Us	sers	×
admin@your.cor	n	
	ОК	Cancel

- 6. Click **New** in Notification List.
- 7. Type in a Notification Name, select Event Type, enter Source IP, and click the Actions.
- 8. Click **OK**.

NOTE This function should be used with Moxa's mobile APP *MXview ToGo*. After setting an Email as identification in *MXview ToGo* and connecting to MXview Server, you will be able to find the Email in the **Receiver** list.

- **NOTE** Using Mobile Notification should give MXview server the capability to connect to Apple APNS or Google C2DM. Please allow the following outgoing ports in your firewall policies:
 - Google: 5228, 5229, and 5230
 - Apple: 443, 2194, 2195, and 5223
- **NOTE** Use the following commands to review communication between MXview server and Apple APNS or Google C2DM:
 - telnet gcm.googleapis.com 5228
 - telnet gateway.sandbox.push.apple.com 443

NOTE The Apple APNS certificate should be renewed annually. Please check Moxa's website for latest APNS certificate.

Add a Sound

When a sound notification is triggered, the MXview server will play the associated sound file. The sound will play repeatedly until some stops it manually. Take the following steps to add a sound:

- 1. Select Event → Notification.
- 2. Click **New** in Action List.
- Select Sound as the type, select a file from the local computer, give the action a name, and then click OK. The file will be uploaded to the MXview server.

Actions		×
Name	Admin Sound	
Туре	Sound	•
Sound	beep.wav	Directory
	OK Cancel	

- 4. Click **New** in the Notification List.
- 5. Select the action just added and the corresponding event type, source IP.
- 6. Click **OK**.

When an associated event occurs, the sound file will be played and a window will pop up:



The sound will not stop until someone clicks OK.

NOTE When more than one event occurs, the sound file corresponding to the first event will be played first, and the sounds corresponding to subsequent events will be queued. After first sound is stopped, the next sound in the queue will be played.

NOTE Only the wav format is supported.

Add an External Program

When a program notification is triggered, the MXview server will execute the associated program. Take the following steps to add a program:

- 1. Select **Event** → **Notification**.
- 2. Click **New** in the Action List.
- 3. Select Program as the type, select a file from the local computer, give the action a name, and then click **OK**. The file will be uploaded to the MXview server.
- 4. Click **New** in the Notification List.
- 5. Select the action just added, the corresponding event type, and the source IP.
- 6. Click **OK**.

When an associated event occurs, the program file will be executed.

Add a Message Box

When a message box notification is triggered, the MXview server will display the message box. You can create a new message box by following the steps below:

- 1. Select **Event** → **Notification**.
- 2. Click **New** in the Action List.
- 3. Select Message Box as the type, give the action a name, and then click OK.
- 4. Click **New** in the Notification List.
- 5. Select the action just added, the corresponding event type, and the source IP.
- 6. Click **OK**.

When an associated event occurs, the system will show the message box.
Syslog Event

MXview can act as a Syslog Event Server with Syslog Event Viewer. Take the following steps to use the viewer to check all syslog events:

- 1. Select Event → Syslog Event Viewer
- 2. Enter Filter Conditions
- 3. Click Query

	Any		•	From	▼ 00 ▼ 00 ▼	То	✓ 23 ▼ 59 ▼
Priority	Higher th	an or equals to 👻 [Debug 🗸	IP 19	2 . 168 . 127 . 3]	Reset
Message]	Query
Time Stamp		IP	Priority	Facility	Message		
015-01-08 1	14-12-21	102 168 127 3	Warning	local5	- Ian 01 00:47:00 102 168 127 3	INFO:Co	nfiguration change activated
015-01-08 1	14:12:36	192 168 127 3	Warning	local5	Jan 01 00:47:14 192 168 127 3	INFO:Pot	wer 1 transition (Off -> On)
015-01-08 1	14:12:41	192.168.127.3	Warning	local5	Jan 01 00:47:19 192.168 127 3	INFO:Po	wer 1 transition (On -> Off)
015-01-08 1	14:12:45	192,168,127,3	Warning	local5	Jan 01 00:47:23 192.168.127.3	INFO:Po	wer 1 transition (Off -> On)
015-01-08 1	14:12:58	192.168.127.3	Warning	local5	Jan 01 00:47:37 192.168.127.3	INFO:Co	nfiguration change activated
015-01-08 1	14:13:13	192.168.127.3	Warning	local5	Jan 01 00:47:51 192.168.127.3	INFO:Po	wer 1 transition (On -> Off)
015-01-08 1	14:13:30	192,168,127,3	Informational	local5	Jan 01 00:00:03 192.168.127.3	INFO:Co	ld start
015-01-08 1	14:13:30	192.168.127.3	Informational	local5	Jan 01 00:00:08 192.168.127.3	INFO:Por	rt 3 link on
015-01-08 1	14:13:30	192.168.127.3	Informational	local5	Jan 01 00:00:08 192.168.127.3	INFO:Por	rt 3 link off
015-01-08 1	14:13:30	192.168.127.3	Informational	local5	Jan 01 00:00:08 192.168.127.3	INFO:Por	rt 3 link on
015-01-08 1	14:13:30	192.168.127.3	Warning	local5	Jan 01 00:00:08 192.168.127.3	INFO:Po	wer 1 transition (Off -> On)
015-01-08 1	14:14:04	192.168.127.3	Warning	local5	Jan 01 00:00:41 192.168.127.3	INFO:Po	wer 2 transition (On -> Off)
015-01-08 1	14:14:05	192.168.127.3	Warning	local5	Jan 01 00:00:42 192.168.127.3	INFO:Po	wer 2 transition (Off -> On)
015-01-08 1	14:14:15	192.168.127.3	Warning	local5	Jan 01 00:00:52 192.168.127.3	INFO:Po	wer 1 transition (On -> Off)
015-01-08 1	14:14:16	192.168.127.3	Warning	local5	Jan 01 00:00:53 192.168.127.3	INFO:Po	wer 1 transition (Off -> On)
015-01-08 1	14:14:17	192.168.127.3	Warning	local5	Jan 01 00:00:54 192.168.127.3	INFO:Po	wer 1 transition (On -> Off)
015-01-08 1	14:14:18	192.168.127.3	Warning	local5	Jan 01 00:00:55 192.168.127.3	INFO:Po	wer 1 transition (Off -> On)
015-01-08 1	14:14:19	192.168.127.3	Warning	local5	Jan 01 00:00:56 192.168.127.3	INFO:Po	wer 1 transition (On -> Off)
015-01-08 1	14:14:20	192.168.127.3	Warning	local5	Jan 01 00:00:57 192.168.127.3	INFO:Po	wer 1 transition (Off -> On)

Network Event Playback

Whenever MXview detects that a device under its management is experiencing an event, such as link down, MXview will update the device status in the topology map. Moreover, MXview will keep records of status changes in a database for up to 30 days, and provides an interface that allows users to go back and check network status from any time within 30 days in a visualized way.

Enable Playback Mode

The playback mode is disabled by default. To enable it:

- 1. Select **Project** → **Preferences**
- 2. Click System Configuration, choose Enable for Playback

MX Preferences	
Preferences Basic User Display Topology Period Device Panel Advanced System Configuration	System Configuration Background Discovery Disable Threshold of Disk Space 0 MB (Alarm is disabled if set to 0) Playback Threshold of devices and links while an e
Device SNMP Configuration Events	* When "Playback" function is enable vent happened, and you can enter plenable o watch detail process. * Additional disk space is required when "Playback" function is enabled.
	OK Close

Enter Playback Mode

To enter the playback mode, choose Playback as operation mode at the index page.



Time Mode and Event Mode

There are two event playback modes. In time mode, MXview will replay the event on the topology map on a second-to-second basis. In event mode, MXview will replay event by event. Users can select playback speeds from 1X to 16X.

Overview of Playback User Interface



• Topology map

The topology map displays the network status at the time indicated in the time indicator.

Event List and All Event button

The events surrounding the current displayed event are displayed in this window. The most recent event is highlighted. Click **All Events** to access an all events search box, with filters. In the filtered results, you can click on a filtered event to jump straight to that event in the playback.

• Control pane

The control pane includes a time indicator, time slider, and calendar, which correspond to the network currently displayed on the topology map.

Users can slide to the time point they would like to check. The slider covers 24 hours in the selected date. To change the date, users can click on the calendar and choose a different date.

MXview compiles traffic statistics for devices running on the network. The statistics are used to create reports that show trend utilization and performance of the device interfaces. Statistics are complied for the following items:

- Traffic utilization (%)
- Error packet rate (%)

Events will be generated when one of these items is above or below the corresponding thresholds.

Checking the Trend

Before MXview can collect traffic statistics between two devices, a link must be created (see the section "Adding a Link" in chapter 8 to see how to add a link).

Right-click on a link, then choose **Link Traffic**, and choose either **Port Traffic** or **Packet Error Rate** monitoring mode.



In Port Traffic mode, the graph shows the utilization percentage by a specific time period. You can define your time period at the window's top right corner. The minimum interval is one day.



The Y-axis scale (percentage) is adjustable, and is accurate to 4 decimal points. To change the Y-axis scale, you just need to roll your mouse wheel down or up. No matter what scale you change it to, you can press the **Default Size** to restore graph scale back to the original setting.

The data shown here can be exported. At the bottom of the window, you can export the graph as a PNG file or export the data as a CSV file.

The interface for **Packet Error Rate** and **Port traffic** monitoring is identical.

Threshold & Event Notification

The traffic conditions below can trigger events:

- 1. Bandwidth utilization is over a threshold.
- 2. Bandwidth utilization is under a threshold.
- 3. Packet error rate is over a threshold.

Since a link is bidirectional, the event will be triggered when one of the directions satisfies any event's trigger condition.

To learn how to change the threshold, refer to **Monitoring Methods** \rightarrow **Color Coding Indicates Problems** \rightarrow **Severity Level** in Chapter 9.

To learn how to configure notification, refer to **Monitoring Methods** \rightarrow **Color Coding Indicates Problems** \rightarrow **Notification** in Chapter 9.

11

Device Management

The following topics are covered in this chapter.

- Device Properties
- Device Virtual Panel
- Changing Device Properties
- Assign Icon
- Web Console Login
- Management Interface
- **Configuration Backup and Restoration (Moxa devices only)**
- Firmware upgrade
- Refresh Status
- □ Mass Operation Configuration Export/Import and Firmware Upgrade
 - Export Configurations from Multiple Devices
 - > Import a Configuration to Multiple Devices
 - > Upgrade Firmware on Multiple Devices
 - Scheduled Configuration Export/Import
 - > Configuration Change History and Comparison
- Device and Inventory Report

Device Properties

MXview provides three ways to view device properties.

- Device Property box in main window (see the Device Property List section in chapter 4)
- 2. Fast Device Property

Right click on a device in the main screen and click **property**.

You may select a device and right click on it. Properties that are listed include model name, MAC address, IP address, Netmask, gateway, port type and status, power status, redundancy protocol, SNMP, and ICMP availability.

3. Customizable Device Property

In the menu bar, select $\textbf{Information} \! \rightarrow \! \textbf{Device Property}$

Device property provides a highly customizable table to view the device properties in your network. On the top of the window, editable optional items include **IP**, **Alias**, **Property** and **Value**.

By selecting the drop-down menu on each option item, you can filter specific items which you wish to display.

The p**roperty** item has the same property as an **inventory report** (Refer to the section **Inventory Report** in Chapter 11). As a result, you can use device property to filter out the specific property you want to see.

MX Device Properties			×
IP -	Alias 👻	Property	🔹 🛛 Value 🔍 👻
192.168.127.12	Matt's Switch #2	power1InputStatus	on
192.168.127.27	Matt's Switch #1	power1InputStatus	on
192.168.127.61	192.168.127.61 EDS-4	power1InputStatus	on
192.168.127.62	192.168.127.62 EDS-4	power1InputStatus	on
192.168.127.155	192.168.127.155 EDS	power1InputStatus	on
192.168.127.156	192.168.127.156 EDS	power1InputStatus	on
192.168.127.250	192.168.127.250 EDS	power1InputStatus	off
192.168.127.251	192.168.127.251 EDS	power1InputStatus	off
192.168.129.2	192.168.129.2 EDS-P5	. power1InputStatus	on
192.168.129.4	192.168.129.4 EDS-G5	. power1InputStatus	off
192.168.129.5	192.168.129.5 EDS-G5	. power1InputStatus	off
192.168.129.8	192.168.129.8 EDS-40	power1InputStatus	off
		Export to CSV	Close

The **Device Property** window is able to export to a CSV file. To do this, simply click the **Export to CSV** button.

Device Virtual Panel

MXview can show the front panel of Moxa switches, and indicate the active status of ports and LED indicators:

Right click on a device and select Panel

2 192.168.127.105	×
	^
Ethernet Port 8 100TX,RJ45.	
•	
3	
1 EDS-408A	*

Changing Device Properties

Take the following steps to change a device's location, name, contact, IP, netmask, gateway, trap server, and SNMP configuration:

- 1. Select a device.
- 2. Select Device → Maintenance → Configure IP & Trap.

Click the **Basic** tab to change the name, location, and contact information for a device. The new values will be written to the device's firmware.

Click the **IP Configuration** tab to change a device's IP address, netmask, gateway, DNS server, and method of obtaining the IP.

Click the **Trap Server** tab to change IP addresses and community strings of trap servers. Moxa switches can send trap messages to at most 2 trap servers.

🏧 192.168.127.122 Config IP and Trap 🛛 🛛 🔀								
Basic IP	Configura	tion	Tra	рS	erver			
IP Address	192	•	168		127	4	122	
Netmask	255	:	255	<u>.</u> 2	255	3	0	
Gateway	0		0	12	0	4	0	
DNS1 IP	0	:	0	1.	0	3	0	
DNS2 IP	0	8	0	30	0	.	0	
Auto IP	Disabled	~						
							ок	Cancel

Assign Icon

MXview allows users to change the device icon manually. Follow the steps below to select a device icon from within MXview's icon database.

- 1. Select a device.
- 2. Select Device →Maintenance → Assign model.

You will see the **Assign Model** window pop up. Select a switch model from the drop-down list, and click the **Assign** button to confirm your selection.

Assign N	Model	×
IP	192.168.127.4	
Model	EDS-408A	
	CISCO	Assign to model Cisco ICMP Device SNMP Device ABB Cisco Emerson Hirschmann MOXA Device Rockwell

Web Console Login

To log in to the device's web console, select **Device** \rightarrow **console**.

NOTE For IE6, MXview will open the console in the window of the MXview Client.

Management Interface

- 1. Navigate to **Project** → **Preferences** → **Management Interface**.
- 2. The Web console protocol can be set to HTTP or HTTPS, and then the port numbers of the HTTP and HTTPS can be set by users. In addition, the Telnet port can be set as well.

IIII Preferences		X			
🙀 User	Management Interface				
Password Policy					
Login Notification	Web console protocol	HTTP •			
Display	HTTP Port	80			
	HTTPS Port	443			
Appearance					
	Telnet Port	23			
Security View					
Advanced					
- SNMP Configuration					
Events					
Management Interface					
		OK Close			

Configuration Backup and Restoration (Moxa devices only)

Take the following steps to back up a device's configuration file to a local computer:

- 1. Select **Device** → **Maintenance** → **Configuration** → **Load from Device**.
- 2. Choose the location where you would like to save the file.

Take the following steps to restore a device's configuration file:

1. Select **Device** → **Configuration** → **Load to Device**.

^{###} Load to Device 192.168.127.237						
From File		Browse				
	ок	Cancel				

2. Choose the file and click **OK**.

Firmware upgrade

To up upgrade a device's firmware, select **Device** \rightarrow **Firmware Upgrade**. The firmware will be uploaded to and installed on the device.



Refresh Status

Since some device data is collected by polling, there may be a time delay for some data. To refresh a device to get its updated status, select **Device** \rightarrow **Refresh**.

Mass Operation Configuration Export/Import and Firmware Upgrade

MXview lets users export/import configuration and upgrade firmware in a mass deployment to a group of devices.

Export Configurations from Multiple Devices

1. Select Tools → Configuration Center

M Configuration Center		X
	~	MAC
- List of Douloop		
List of Devices		Location
192.168.127.1 PT-7828	<u>^</u>	
192.168.127.5 SNMP Device		List of Configurations
192.168.127.12 EDS-408A		Filename Creating Time Last Checking Time
192.168.127.27 EDS-408A		
192.168.127.34 EDS-408A		
192.168.127.67 ICMP Device		
192.168.127.88 EDS-518A		
192.168.127.91 ICMP Device		
192.168.127.102 ICMP Device		
192.168.127.103 ICMP Device		
192.168.127.104 EDS-408A		
192.168.127.105 EDS-408A		
192.168.127.106 EDS-408A		
192.168.127.107 EDS-408A		
192.168.127.109 EDS-408A		
192.168.127.110 EDS-408A		
192.168.127.111 EDS-408A		
192.168.127.112 EDS-408A		
192.168.127.113 EDS-408A		
192.168.127.150 AWK-4121		
192.168.127.162 EDS-408A		
192.168.127.181 ICMP Device		
192.168.127.182 ICMP Device		
192.168.127.183 ICMP Device		Compare Download Delete
192.168.127.200 SNMP Device		Download Delete
192.168.127.235 EDS-G509		
192.168.127.236 EDS-G509	~	
100 160 107 027 800 600 4		
Export from Device	Import to Device	Close

2. Click Export from Device

- 3. Select a folder in which to store configuration files
- 4. Select devices to export configuration files from and add them to the list. Click Export

Export Configuration		Þ
IP Address	Status	
192.168.127.34	Success	~
192.168.127.67	Exporting	
192.168.127.88	Waiting	
192.168.127.91	Waiting	
192.168.127.102	Waiting	
192.168.127.103	Waiting	
192.168.127.104	Waiting	
192.168.127.105	Waiting	
192.168.127.106	Waiting	
192.168.127.107	Waiting	
192.168.127.109	Waiting	
192.168.127.110	Waiting	
192.168.127.111	Waiting	
192.168.127.112	Waiting	
192.168.127.113	Waiting	
192.168.127.150	Waiting	
192.168.127.162	Waiting	~
	Cancel	:0

After a few seconds, the configuration files will be exported to the designated folder, with IP addresses and timestamps in the filenames.

Import a Configuration to Multiple Devices

Moxa switches can import a segment of a configuration file and change device configurations based on the parameters the segment describes. MXview helps users import a segment of a configuration file to multiple devices.

- 1. Select Tools → Configuration Center
- 2. Click Import to Device
- 3. Select a configuration file segment
- 4. Select devices to import configuration files to and add them to the list. Click Import

After a few seconds, the configuration file segment will be imported to devices and activated.

Upgrade Firmware on Multiple Devices

- 1. Select Information → Firmware Version
- 2. Click Upgrade
- 3. Select a firmware file
- 4. Select devices that upgrade firmware and add to the list. Click Upgrade

The firmware will be upgraded to devices one by one. MXview will wait for 30 seconds before upgrading the next device on the list, in order to give the upgrading devices sufficient time to finish the process.

Scheduled Configuration Export/Import

1. Select **Tools** → **Job Scheduler**

**	
List of Job	Information of Job
	Name of Job: View Details
	Action of Job:
	Frequency of Job:
	Description of Job:
	Show Log Open Folder
Add Delete	Close

2. Click Add.

3. Enter a job name and select **Import Configuration**, **Export Configuration** or **Database Backup** in the drop-down box.

MXX				
Step 1 - Job Information	Step 2 - Select Devices	Step 3 - Schedule Time		
Name of Job	daily_export			
Action of Joh	Export Configuratio	n	~	
1000101000	Export comigatatio			
Description of Job				
		Next		Cancel

- 4. Select the devices that apply and add them to the list. Click **Next**
- 5. Select the execution routine.

Configuration Change History and Comparison

When MXview exports configurations from devices, whether manually or by schedule, MXview will compare the exported configuration with the last configuration exported and stored on the MXview server. If there is any difference MXview will save the configuration on the MXview server. Users can then check the change history of the configuration file:

- 1. Select Tools → Configuration Center
- 2. Check List of Configurations

And users can compare any 2 stored configurations at MXview server

- 1. Select Tools → Configuration Center
- 2. Click Compare
- 3. Select two IP addresses and their configurations

Change 465 Delete 1877 Insert 0	
6_192.168.127.88_20111226_1731.ini	5_192.168.127.34_20111226_1730.ini
1: [EtherDevice Server Configuration File]	1: [EtherDevice Server Configuration File]
2:	2:
3:#Model Name	3: # Model Name
4. 5: ModelName EDS-518A-SS-SC	5: ModelName EDS-408A
6:	6:
7:	7:
8:	8:
9. ####################################	9: ####################################
11:#System Identification #	11: # System Identification #
12:	12:
13: ####################################	13:####################################
14:	14:
15: # [SwitchName]: Switch Name	15: # [SwitchName]: Switch Name
16: 17:#> may length = 20 words	16: 17:#> max length = 20 words
18:	18:
19: SwitchName Managed Redundant Switch 00015	19: SwitchName Managed Redundant Switch 09611
20:	20:
21:	21:
22. 23: # Il ocation!: Switch Location	22: 22: # [Location]: Switch Location
24:	23. # [Eddalon]. dwith Eddalon
25: #> max. length = 80 words	25: #> max. length = 80 words
26:	26:
27: Location Switch Location	27: Location Switch Location
28:	28:
30:	30:
31: # [SysDescr]: Switch Description	31: # [SysDescr]: Switch Description
32:	32:
33:#> max. length = 30 words	33:#> max. length = 30 words
34: 35: SveDescr MOV& ED9-5198-59-90	34: 25: SveDeccr EDS-4094
10. 0yobosti III 0/// ED0-010//00-00	

The inserted, deleted and modified lines in the configuration will be highlighted.

Device and Inventory Report

MXview can summarize device information in a formal report. Both a Device Availability Report and Inventory Report are available.

Device Availability Report

The device availability report includes information about Device IP, Device Alias, Availability average, and Availability worst data. You can narrow the report by a specific time period by dates and groups.

vailability Report						
Availability Date Se	lection					
			r			
Group Any	✓ From 2012/7/5	*	~ То	2012/7/5	~	
						luery
Device IP	Device Alias	From date	End date	Availability Av	Availabilit	Days
192.168.127.1	192.168.127.1 PT-7828	2012-07-05	2012-07-05	100.000	100.000	1
192.168.127.12	192.168.127.12 EDS-408A	2012-07-05	2012-07-05	100.000	100.000	1
192.168.127.27	192.168.127.27 EDS-408A	2012-07-05	2012-07-05	100.000	100.000	1
192.168.127.41	192.168.127.41 EDS-408A	2012-07-05	2012-07-05	100.000	100.000	1
192.168.127.42	192.168.127.42 EDS-408A	2012-07-05	2012-07-05	100.000	100.000	1
192.168.127.44	192.168.127.44 EDS-408A	2012-07-05	2012-07-05	100.000	100.000	1
92.168.127.43	192.168.127.43 EDS-408A	2012-07-05	2012-07-05	100.000	100.000	1
92.168.127.46	192.168.127.46 EDS-408A	2012-07-05	2012-07-05	100.000	100.000	1
192.168.127.45	192.168.127.45 EDS-408A	2012-07-05	2012-07-05	100.000	100.000	1
92.168.127.61	192.168.127.61 EDS-408A	2012-07-05	2012-07-05	100.000	100.000	1
192.168.127.62	192.168.127.62 EDS-408A	2012-07-05	2012-07-05	100.000	100.000	1
192.168.127.65	192.168.127.65 PT-510	2012-07-05	2012-07-05	100.000	100.000	1
192.168.127.112	192.168.127.112 IKS-6726 Series	2012-07-05	2012-07-05	100.000	100.000	1
192.168.127.155	192.168.127.155 EDS-408A	2012-07-05	2012-07-05	100.000	100.000	1
92.168.127.156	192.168.127.156 EDS-508A	2012-07-05	2012-07-05	100.000	100.000	1
92.168.127.160	192.168.127.160 EDS-408A	2012-07-05	2012-07-05	100.000	100.000	1
192.168.127.164	192.168.127.164 EDS-408A	2012-07-05	2012-07-05	100.000	100.000	1
192.168.127.162	192.168.127.162 EDS-508A	2012-07-05	2012-07-05	100.000	100.000	1
92.168.127.115	192.168.127.115 ICMP Device	2012-07-05	2012-07-05	6.715	6.715	1
92.168.127.250	192.168.127.250 EDS-510A	2012-07-05	2012-07-05	100.000	100.000	1
92.168.127.153	192.168.127.153 ICMP Device	2012-07-05	2012-07-05	100.000	100.000	1
192.168.127.251	192.168.127.251 EDS-518A	2012-07-05	2012-07-05	100.000	100.000	1
92.168.127.181	192.168.127.181 ICMP Device	2012-07-05	2012-07-05	100.000	100.000	1
92.168.127.182	192.168.127.182 ICMP Device	2012-07-05	2012-07-05	100.000	100.000	1
92.168.127.183	192.168.127.183 ICMP Device	2012-07-05	2012-07-05	17.588	17.588	1
92.168.127.240	192.168.127.240 PT-7528	2012-07-05	2012-07-05	100.000	100.000	1
100 160 107 060	100 160 107 260 100 07000	2012 07 06	2012 07 06	6 716	6 716	4
	ſ	Export to CS	v	Export to PDF		Close

The availability report can be exported to a PDF or CSV file.

Report Generat	AV8 e date:2012-07-05	ulability Rep	ort	Fro Ei	m date:2012 1d date:2012	-07-05 -07-05
Device IP	Device Alias	Availability Average	Availability Worst	From date	End date	Days
192.168.127.1	192.168.127.1 PT-7828	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.12	192.168.127.12 EDS-408A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.27	192.168.127.27 EDS-408A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.41	192.168.127.41 EDS-408A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.42	192.168.127.42 EDS-408A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.44	192.168.127.44 EDS-408A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.43	192.168.127.43 EDS-408A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.46	192.168.127.46 EDS-408A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.45	192.168.127.45 EDS-408A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.61	192.168.127.61 EDS-408A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.62	192.168.127.62 EDS-408A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.65	192.168.127.65 PT-510	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.112	192.168.127.112 IKS-6726 Series	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.155	192.168.127.155 EDS-408A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.156	192.168.127.156 EDS-508A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.160	192.168.127.160 EDS-408A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.164	192.168.127.164 EDS-408A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.162	192.168.127.162 EDS-508A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.115	192.168.127.115 ICMP Device	6.715	6.715	2012-07-05	2012-07-05	1
192.168.127.250	192.168.127.250 EDS-510A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.153	192.168.127.153 ICMP Device	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.251	192.168.127.251 EDS-518A	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.181	192.168.127.181 ICMP Device	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.182	192.168.127.182 ICMP Device	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.183	192.168.127.183 ICMP Device	17.588	17.588	2012-07-05	2012-07-05	1
192.168.127.240	192.168.127.240 PT-7528	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.253	192.168.127.253 ICS-G7828	6.715	6.715	2012-07-05	2012-07-05	1
192.168.127.248	192.168.127.248 ICMP Device	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.249	192.168.127.249 ICMP Device	100.000	100.000	2012-07-05	2012-07-05	1
192.168.127.254	192.168.127.254 ICMP Device	100.000	100.000	2012-07-05	2012-07-05	1

	А	В	С	D	E	F	G
1	Device availability	1					
2	Device IP	Device Alias	Availability Average	Availability Worst	From date	End date	Days
3	192.168.127.1	192.168.127.1 PT-7828	100	100	2012/7/5	2012/7/5	1
4	192.168.127.12	192.168.127.12 EDS-408A	100	100	2012/7/5	2012/7/5	1
5	192.168.127.27	192.168.127.27 EDS-408A	100	100	2012/7/5	2012/7/5	1
6	192.168.127.41	192.168.127.41 EDS-408A	100	100	2012/7/5	2012/7/5	1
-7	192.168.127.42	192.168.127.42 EDS-408A	100	100	2012/7/5	2012/7/5	1
8	192.168.127.44	192.168.127.44 EDS-408A	100	100	2012/7/5	2012/7/5	1
9	192.168.127.43	192.168.127.43 EDS-408A	100	100	2012/7/5	2012/7/5	1
10	192.168.127.46	192.168.127.46 EDS-408A	100	100	2012/7/5	2012/7/5	1
11	192.168.127.45	192.168.127.45 EDS-408A	100	100	2012/7/5	2012/7/5	1
12	192.168.127.61	192.168.127.61 EDS-408A	100	100	2012/7/5	2012/7/5	1
13	192.168.127.62	192.168.127.62 EDS-408A	100	100	2012/7/5	2012/7/5	1
14	192.168.127.65	192.168.127.65 PT-510	100	100	2012/7/5	2012/7/5	1
15	192.168.127.112	192.168.127.112 IKS-6726 Series	100	100	2012/7/5	2012/7/5	1
16	192.168.127.155	192.168.127.155 EDS-408A	100	100	2012/7/5	2012/7/5	1
17	192.168.127.156	192.168.127.156 EDS-508A	100	100	2012/7/5	2012/7/5	1
18	192.168.127.160	192.168.127.160 EDS-408A	100	100	2012/7/5	2012/7/5	1
19	192.168.127.164	192.168.127.164 EDS-408A	100	100	2012/7/5	2012/7/5	1
20	192.168.127.162	192.168.127.162 EDS-508A	100	100	2012/7/5	2012/7/5	1
21	192.168.127.115	192.168.127.115 ICMP Device	6.715	6.715	2012/7/5	2012/7/5	1
22	192.168.127.250	192.168.127.250 EDS-510A	100	100	2012/7/5	2012/7/5	1
23	192.168.127.153	192.168.127.153 ICMP Device	100	100	2012/7/5	2012/7/5	1
24	192.168.127.251	192.168.127.251 EDS-518A	100	100	2012/7/5	2012/7/5	1
25	192.168.127.181	192.168.127.181 ICMP Device	100	100	2012/7/5	2012/7/5	1
26	192.168.127.182	192.168.127.182 ICMP Device	100	100	2012/7/5	2012/7/5	1
27	192.168.127.183	192.168.127.183 ICMP Device	17.588	17.588	2012/7/5	2012/7/5	1
28	192.168.127.240	192.168.127.240 PT-7528	100	100	2012/7/5	2012/7/5	1
29	192.168.127.253	192.168.127.253 ICS-G7828	6.715	6.715	2012/7/5	2012/7/5	1
30	192.168.127.248	192.168.127.248 ICMP Device	100	100	2012/7/5	2012/7/5	1
31	192.168.127.249	192.168.127.249 ICMP Device	100	100	2012/7/5	2012/7/5	1
32	192.168.127.254	192.168.127.254 ICMP Device	100	100	2012/7/5	2012/7/5	1

By default, the availability is calculated based on 24-hour intervals. To change this, in the menu select **Project** \rightarrow **Preferences** \rightarrow **Advanced** \rightarrow **Devices** \rightarrow **Timeframe for availability calculation**

Enter the calculation timeframe base in the box and click **OK**. Units are entered in hours..

Inventory Report

Select **Information** →**Inventory Report** to generate an inventory report.

Inventory report provides a summary of each device's properties. With **Inventory Report**, MXview will export reports separately for all the devices in your network. Each device has a single PDF Report. The PDF filename is determined by device IP. The title of the report is the device alias, which you can edit in MXview. If there is any third-party MIB compiled in, the proprietary information will be included into the report (refer to **Chapter 13- MIB**).

192.	168.127.12.pdf - Adobe Reader	
Eme H		
4		Tools Sign Comment
Ľ	Matt's S	witch #2
Ø	Report Generate date: 2012-06-06	
	Property	Value
	IP	192.168.127.12
	Device Alias	Matt's Switch #2
	MAC Address	0090E819290B
	sysDescr	MOXA EDS-408A
	sysObjectId	1.3.6.1.4.1.8691.7.7
	sysContact	89191230
	sysName	Managed Redundant Switch 07022
	sysLocation	Matt's Desk
	modelName	EDS-408A
	firmwareVersion	V3.0 build 11070113
	IpMask	255.255.255.0
	defaultGateway	0.0.0.0
	dnsServer1IpAddr	0.0.0.0
	snmpTrapCommunity	public 🔹

12 Visualization Mode

The following topics are covered in this chapter.

- VLAN Visualization
- IGMP Snooping Visualization
- **D** Traffic Load Visualization
- Security View
- Wireless Dashboard

VLAN Visualization

Moxa switches support 802.1Q tagged VLAN. MXview collects each device's VLAN configuration and integrates the information with color-coded visualization to provide a network-wide view.

1. Click the VLAN icon in the topology toolbox.



2. After selecting a specific VLAN ID, devices, ports and links that are associated with the ID will be color-coded.

To view the VLAN information in a table format, select Network \rightarrow VLAN

WX YLA	N							×
80	02.1Q Port	-based						
Devi	ce IP	Model	Location	VLAN ID	Joined Acces	Joined T	Manage	
192.1	68.127.103	Managed	factory	1	1,2,3,4,5,6,7,8,		N	~
192.1	68.127.102	Managed Red	Switch Locat	1	1,2,3,4,5,6,7,8,		N	
192.10	68.127.70	Moxa EDS-51	Switch Locat	1	1,2,3,4,5,6,7,8,		N	
192.10	68.127.69	Moxa EDS-51	Switch Locat	1	1,2,3,4,5,6,7,8,		N	
192.10	68.127.68	Moxa EDS-51	Switch Locat	1	1,2,3,4,5,6,7,8,		N	
192.1	68.127.67	Moxa EDS-51	Switch Locat	1	1,2,3,4,5,6,7,8,		N	
192.10	68.127.66	Moxa EDS-51	Switch Locat	1	1,2,3,4,5,6,7,8,		N	
192.10	68.127.65	Moxa EDS-51	Switch Locat	1	1,2,3,4,5,6,7,8,		N	
192.10	68.127.64	Moxa EDS-51	Switch Locat	1	1,2,3,4,5,6,7,8,		N	
192.10	68.127.63	Moxa EDS-51	Switch Locat	1	1,2,3,4,5,6,7,8,		N	
192.10	68.127.62	Moxa EDS-51	Switch Locat	1	1,2,3,4,5,6,7,8,		N	
192.10	68.127.61	Moxa EDS-51	Switch Locat	1	1,2,3,4,7,8,9,1		N	
192.10	68.127.14	Moxa EDS-51	factory	1	1,2,3,4,5,6,9,1		N	
192.10	68.127.13	Managed Red	factory	1	1,2,3,4,5,6,7,8,		N	
192.10	68.127.12	Moxa EDS-40	Switch Locat	1	1,2,3,4,5,6,7,8,		N	
192.10	68.127.11	Managed Red	Switch Locat	1	1,2,3,4,5,6,7,8,		N	
192.1	68.127.2	Moxa PT-7828	factory	1	27,28,TK1,		N	
192.1	68.127.1	Managed Red	factory	1	9,10,11,12,13,		N	~
							Close	

IGMP Snooping Visualization

Moxa switches support IGMP snooping. MXview collects each device's IGMP snooping configuration and visualizes the information to provide a network-wide view.

1. Click the IGMP icon in the topology toolbox.



2. After selecting a specific VLAN ID and multicast address, devices, ports and links that are associated with the stream will be color-coded.

Traffic Load Visualization

MXview collects the traffic load information of every link and displays the information to provide users with a network-wide view.

1. Click the Traffic Load icon in the topology toolbox.



2. The Traffic Load window pops up. It uses different colors to differentiate between different traffic load levels.



3. All of the links will be color-coded to indicate how much traffic they are carrying.



- 2 Preferences × 🌛 Basic Appearance 🧞 User a) Display Language Topology English • Background Color PoE link Color Device Appearance 255, 255, 255 👻 0,0,0 Ŧ advanced 🤌 System Configuration Status Color Turbo Ring V1 Color Turbo Ring V2 Color C Device 0,0,0 0,0,0 SNMP Configuration • • Turbo Chain Color RSTP Color Events 0, 0, 0 0,0,0 • • Link up Color Link down Color 0,0,0 0,0,0 • • Traffic Load(%) **V** V V V V 60 100 20 40 80 0 ок Close
- 4. Navigate to **Project** → **Preferences** → **Appearance** to redefine the traffic load levels.

Security View

ISA/IEC 62443 is a continuously evolving cybersecurity standard whose guidelines have already been adopted in many industrial automation applications. This standard, including its subsections, aims to cover points such as general requirements, policies & procedure, system-level requirements, and component-level requirements.

Moxa's MXview follows Moxa's security guidelines, which are based on the current IEC 62443-4-2 component-level recommendations. Security View checks the security level of Moxa's network devices. There are five levels for checking the results in Security View:

- High: IEC 62443-4-2 level 2
- Medium: IEC 62443-4-2 level 1
- Basic: General baseline
- Open: Security Level below basic
- Unknown: Devices without security-related information for MXview

NOTE The definition of general baseline is based on several industrial cybersecurity policies and requirements.

1. Click the Security View icon in the topology toolbox



2. The Security View window pops up. Different colors indicate different security levels, and all devices are color-coded with their respective security levels.

MXview								- 6	×
Project View Device Link	Information Event Tools MIB	Help							
MX view In	udustrial Network Mana	ugəməni Sofiwarə					MC)X/	Ľ
Q- Search Devices	Root					🗙 👋 =	1		0
Device List			(Security view				• ×	1 î
■ 🖧 Root ■ 192.168.127.2-EDS-51 ■ 192.168.127.1 EDS-40				Filter All VIP	Address: 192.168.127.3		Security Let	vel: High	
192.168.127.3-EDS-G	516E P	p2 p2 p1	p2 🕋	IP Address CI	heck Items	(Current Setting	H M B	
				192.168.127.1 En	able Auto Logout	E	nabled	000	
A V				192.168.127.3 Dis	sable Non-encrypted TCP	/UDP Ports E	nabled	000	
Device Tropenses	192.168.127.3	3 192.168.127.2	192.168.127.1	En	able Account Login Failur	e Lockout E	nabled	000	
				En	able Trusted Access	E Strongth Chack	nabled	000	
				En	able Configuration File El	ncryption E	nabled	ö ö ö	=
				En	able Broadcast Storm Pro	otection E	nabled	000	
				Se	t SNMP Trap/Inform or Sy	slog Server S	et banged	$\circ \circ \circ$	
				High Mediu	um Basic	Open U	nknown		-
					1009	%			
				Launch MXconfig	Export	Scan		ose	
					Export	ocum		000	
									*
									F
0-0-1	Recent Events A	ck All Unacked Last Fifty Events	•			12 97	155	All Ever	nts
[]	Ack	ID Source	Source IP	Device Alias	Severity	Description	Time Issu	ied	
		278 Trap	192.168.127.2	192.168.127.2EDS-51	Warning	Authentication failure	2016-09-1	9 13:22:20	^
Q De Fit	•	277 Trap	192.168.127.2	192.168.127.2EDS-51	Information	Account authentication	on fail 2016-09-1	9 13:22:20	
Т	opology has been saved successfu	ully 下	午 01:22:30	Managed Devices (Cur	rent/Max):3/20				

Users can see the Check Items and Current Settings in the window. H, M, B indicates High, Medium, and Basic levels. indicates the Check Item has been successfully setup, indicates the Check Item is unnecessary for that level, and BLANK indicates the Check Item has not been successfully setup yet.

Security view					23
Filter All 👻	IP Address: 192.168.127.2	Security Level:	Med	lium	
IP Address	Check Items	Current Setting	н	М	в
192.168.127.1	Enable Auto Logout	Enabled	0	0	0
192.168.127.2	Set Login Message	Set	0	0	•
192.168.127.3	Disable Non-encrypted TCP/UDP Ports	Enabled	0	0	•
	Enable Account Login Failure Lockout	Enabled	0	0	•
	Enable Trusted Access	Enabled	0	0	0
	Enable Password Complexity Strength Check	Enabled	0	0	•
	Enable Configuraiton File Encryption	Disabled		•	•
	Enable Broadcast Storm Protection	Enabled	0	Ø	0
	Set SNMP Trap/Inform or Syslog Server	Set	0	0	0
	Change Default Password / SNMP Communit	Changed	0	Ø	0
High	ledium Basic Open	Unknown			
	100%				
Launch MXconfig	Export Scan	CI	ose		

- Security view Filter Medium IP Address: 192.168.127.2 Security Level: Medium Ŧ Current Setting IP Address Check Items H M B 192.168.127.2 Enable Auto Logout Enabled Set Login Message Set Disable Non-encrypted TCP/UDP Ports Enabled Enable Account Login Failure Lockout Enabled Enable Trusted Access Enabled Enable Password Complexity Strength Check Enabled Enable Configuraiton File Encryption Disabled Enable Broadcast Storm Protection Enabled Set SNMP Trap/Inform or Syslog Server Set Change Default Password / SNMP Communit... Changed High Medium Basic Open Unknown Launch MXconfig Export Scan Close
- 4. By using Filter, users can select devices with a specific security level in the window.

 Click Export to export the details of the devices' IP addresses, Check Items, and Current Settings in a CSV file.

Security view				•	23
Filter All	P Address: 192.168.127.2	Security Level:	Мес	lium	
IP Address	Check Items	Current Setting	н	М	в
192.168.127.1	Enable Auto Logout	Enabled	0	0	0
192.168.127.2	Set Login Message	Set	0	0	0
192.168.127.3	Disable Non-encrypted TCP/UDP Ports	Enabled	Ø	Ø	0
	Enable Account Login Failure Lockout	Enabled	Ø	Ø	•
	Enable Trusted Access	Enabled	Ø	Ø	0
	Enable Password Complexity Strength Check	Enabled	Ø	Ø	•
	Enable Configuraiton File Encryption	Disabled		0	•
	Enable Broadcast Storm Protection	Enabled	Ø	Ø	•
	Set SNMP Trap/Inform or Syslog Server	Set	Ø	0	0
	Change Default Password / SNMP Communit	Changed	Ø	Ø	0
High	Medium Basic Open	Unknown			
	100%				
Launch MXconfig	Export Scan	CI	lose		

6. Click Launch MXconfig to activate MXconfig for mass configuration of security-related parameters. In the Security Wizard of MXconfig, all parameters relating to the different security levels can be listed, and users can easily enter their information for mass configuration.

Security view		
Filter All 🗸	IP Address: 192.168.127.2	Security Level: Medium
IP Address	Check Items	Current Setting H M B
192.168.127.1	Enable Auto Logout	Enabled 🛛 🕑 🕑
192.168.127.2	Set Login Message	Set 🛛 🛇 🗢
192.168.127.3	Disable Non-encrypted TCP/UDP Ports	Enabled 🛛 🛇 🗢
	Enable Account Login Failure Lockout	Enabled 🛛 🛇 🗢
	Enable Trusted Access	Enabled 🛛 🖉 🖉
	Enable Password Complexity Strength Check	Enabled 🛛 🖉 🗨 🖨
	Enable Configuraiton File Encryption	Disabled O
	Enable Broadcast Storm Protection	Enabled 🛛 🖉 🗢
	Set SNMP Trap/Inform or Syslog Server	Set 🛛 🛇 🗢 🥥
	Change Default Password / SNMP Communit	Changed 🛛 🛇 🛇
High N	ledium Basic Open	Unknown
	100%	
Launch MXconfig	Export Scan	Close

MXconfig						
	Q 🖻 🧰	🍳 😭 🔤 🎨 🗃	🚨 💁 💁 😡 🖷			
ALL	Model	IP Adddress	MAC Address Serial	Firmware Version	Name	Location
		Import Device Please select the types of dev	rices you want to search.	×		
		Active Device Type	al Server	Progress Status Preparing		
		Industrial Wireles	35	Preparing		
		Industrial Etherne	et Switches/Secure Routers/DSL Exte	Preparing		
		Industrial IP Cam	leras/Video Encoders/Video Decoder	Preparing		
		Industrial Etherne	at Gateway	Preparing T		
		Timeout 500	ms Retry	3		
		Device List				
		192.168.127.1				
		192.168.127.2				
		192.168.127.3				
				,	_	
			Search	Close		
						Informatio
						LLDP
						Forwardin
						Interface
						menace

NOTE

	9 👩 🍳	R 🔒 🖉 🕻	7 🔤 🍥 🗃	\mid 🙇 💁		2		
ALL		Model	IP Adddress	MAC Address	Serial	Firmware Version	Name	Location
	3.127.1 3.127.2	EDS-510E-3GTXSFP	92.168.127.2	0090E84BD034	01961	V5.2build16091412		
192.168	3.127.3	EDS-G516E-T 1	92.168.127.3	0090E854E1E6	08477	V5.0build16070518		Switch L
		EDS-405A	92.168.127.1	0090E82D049F	06217	V3.4.8build1412181	5Managed Redunda	Switch L
Security/Witzerd								
le View								
Display IP Address 🗸								
Selected devices	Profile	General Baseline	• •		Custom	Save	Load	
192.168.127.1								
192.168.127.2	Enable				Name			
192.100.127.3		Auto Logout						
		Accessible IP						
		Syslog Server						
		Tran Server						
		SNMP Sotting						
	V	Sinimi Setting						
		Password						
Load settings from this device								
							Next	Cancel
								Gancor
	Ne	tmask 255.2	55.255.0					
	Ga	teway U.U.U Madarose 00.00	.U .F8.2D.04.0F					
		, Autress 00-90	-E0-2D-04-9F					•
Total Count: 3								

7. Navigate to Project → Preferences → Security View to redefine the color of the different security levels. Users can also define their own security profile by selecting User-defined Profile. All of the check items can be set for Security View, and it shows Pass or Not Pass for checked results.

Preferences			—
Ner User		Security View	
Viser	Profile Colors for check m High / IE Medium Basic / 0 Open	Security View Built-in Profile Security EC 62443-4-2 Level 2 (/IEC 62443-4-2 Level 1 General Baseline	Profile details…
Management Interface			Close
		ОК	Close

MXX Preferences				
Vser User	Security View			
With Preferences User User Password Policy User Display Display Display Device Appearance Device Appearance Advanced Optice	Security View Profile User defined Custom Colors for check result Pass Vot Pass Vot Pass Switch Gateway Enabled Check Item Enable Auto Logout Set Login Message Disable Non-encrypted TCP/UDP Ports Enable Account Login Failure Lockout Enable Access Enable Password Complexity Strength Check			
SNMP Configuration	Enable Password Complexity Strength Check Enable Configuraiton File Encryption Enable Broadcast Storm Protection Set SNMP Trap/Inform or Syslog Server Change Default Password / SNMP Community String			
	OK Close			

Below is the detailed description for each item:

- Enable Auto Logout: Check if the Auto Logout function is enabled or not
- Set Login Message: Check if the Login Message is set or not
- Disable Non-encrypted TCP/UDP Ports: Check if the Non-encrypted TCP/UDP Ports are disabled or not
- Enable Account Login Failure Lockout: Check if the Account Login Failure Lockout function is enabled or not
- Enable Trusted Access: Check if the Trusted Access function is enabled or not
- Enable Password Complexity Strength Check: Check if the Password Complexity Strength Check function is enabled or not
- Enable Configuration File Encryption: Check if the Configuration File Encryption function is enabled or not
- Enable Broadcast Storm Protection: Check if the Broadcast Storm Protection function is enabled or not
- Set SNMP Trap/Inform or Syslog Server: Check if the SNMP Trap/Inform or Syslog Server is set or not
- Change Default Password/SNMP Community String: Check if the Default Password or SNMP
 Community String is set or not

Wireless Dashboard

MXview collects the wireless information from all the Moxa AWK series devices, and displays the information into a Wireless Dashboard for an overview.

- 1. Navigate to **Information** → **Wireless Dashboard** to activate the Wireless Dashboard.
- 2. All the Access Points (APs) and Clients are listed. Device Name, IP Address, MAC Address, Signal Strength, and SNR are shown on the dashboard. Furthermore, the connection between the APs and Clients can also be shown on the dashboard.

Wireless Dashbo	ard					- 0	×
Auto Refresh: 14					Search:		0
1	Number of APs:	3		Numbe	r of Clients: 3		. V
Device Name 💠	IP Address 🗘	MAC Address	Device Name	♦ IP Address ♦	MAC Address	 Signal Strength (dBm) 	SNR (dB)
AWK-4131A-US_2	20.20.88.2	00:90:E8:53:3C:B2	AWK-4131A-US_3	20.20.88.3	00:90:E8:53:3C:AB	-106	4
AWK-3131A_4697q	10.10.14.2	00:90:E8:58:8F:85	AWK-3131A_4761	10.10.14.3	00:90:E8:58:8F:C5	-75	23
AWK-1131A-EU_4	10.10.14.4	00:90:E8:59:A8:3E	AWK-1131A-EU_5	10.10.14.5	00:90:E8:59:A8:8E	-95	15
Device Name	IP Address	MAC Address	Device Name	IP Address	MAC Address	Signal Strength (dBm)	SNR (dB)
		F	Previous 1 Ne	xt			8
			Show All 👻 Entrie	S			

3. By clicking the icon, users can set the threshold for Signal Strength and SNR. In the meantime, different colors can be set for indication on the dashboard.

				×
Enable	Parameter Column	Condition	Value	Color
	Signal Strength (dBm) SNR (dB)	= •	0	▼
				ОК

NOTE Only the AWK-1131A series, AWK-3131A series, and AWK-4131A series support Wireless Dashboard.

NOTE Wireless Dashboard is refreshed automatically every 15 seconds.

MXview's embedded MIB compiler supports third-party MIB files. After compiling the MIB file, any device's parameter can be monitored in MXview.

This chapter covers the following application tools of the MIB compiler:

- MIB Browser
- OID Import Manager
- Trap Import Manager

MIB Browser

MIB browser provides an easy and comfortable browsing interface for reading proprietary MIB parameters. OID import manager makes all monitored parameters customizable, and they can be read in the device properties window list. With Trap Import Manager, the third-party traps can be displayed in the event history box.

MIB Browser is a simple and fast interface that lets you browse MIB files. It is able to load third-party MIB files. After loading the MIB, the OID tree will be listed in the left column. You can unfold these OIDs and get the parameter you need.

MIB Bro	wser			×
File Abo	out			
CID-CISCO-CPU-MIB		Agent IP: 192.168 OID: 1.3.6.1.4.	127.252 SNMP v1	
	Dusyrer (50) avgBusy1 (57) avgBusy5 (58)	Get	Get Next Get Subtree Walk Set	
	jdleCount (59)	Name/OID	Yalue	Г
	🃝 idle Wired (60)	busyPer	3	
		avgBusy1	4	
		avgBusy5	3	10
		idleCount	4836	
		id le Wired	0	
		1.3.6.1.4.1.9.2.1.61.0	cisco Systems, Inc.170 West Tasman Dr.San Jose, CA 95134-1706U.S.A.Ph +1-408-526-40	
		1.3.6.1.4.1.9.2.1.62.0	18024	
		1.3.6.1.4.1.9.2.1.63.0	0	
		1.3.6.1.4.1.9.2.1.64.0	0	
		1.3.6.1.4.1.9.2.1.65.0	2	
		1.3.6.1.4.1.9.2.1.66.0	0	
		1.3.6.1.4.1.9.2.1.67.0	0	
		1.3.6.1.4.1.9.2.1.68.0	0	
_		1.3.6.1.4.1.9.2.1.69.0	0	
name	lepu (1)	1.3.6.1.4.1.9.2.1.70.0	0	
OID	1.3.6.1.4.1.9.2.1	1.3.6.1.4.1.9.2.1.71.0	0	
	VALUE lopu OBJECT I	1.3.6.1.4.1.9.2.1.72.0	0.0.0	
description	DENTIFIER	1.3.6.1.4.1.9.2.1.73.0	flash:/c2950-i6q4i2-mz.121-11.EA1.bin	
	::= 1.3.6.1.4.1.9.2.1	1.3.6.1.4.1.9.2.1.74.0	3	
		1.3.5.1.4.1.9.2.2.1.1.1.1	Past Ethemet	1
		1.3.5.1.4.1.9.2.2.1.1.1.2	Past Ethemet	
		1.3.5.1.4.1.9.2.2.1.1.1.3	Past Ethernet	Ŧ
			Close	

To open the MIB Browser: Select $\textbf{MIB} \rightarrow \textbf{MIB}$ Browser

- Click File →Load MIB to load a MIB file.
- Select the item in the MIB tree:
- Click Get to get the parameter of selected item.
- Click Get Next to get the OID next to the item you selected.
- Click **Get Subtree** to get all the OIDs in the sub tree folder.
- Click **Walk** to get the OID's parameter in sequence.
- Click **Set** to set up parameters of the selected OID.

OID Import Manager

OID Import manager helps to add specific OID items for SNMP polling. It supports third-party MIB with polling. After compiling the MIB files, you can monitor third-party OIDs through SNMP polling.

To open the import manager: Select **MIB → OID Import Manager**

List of Polling OIDs		
Name	Value	Show Details
CPU.avgBusy5	1.3.6.1.4.1.9.2.1.58.0	
PU.avgBusy1	.1.3.6.1.4.1.9.2.1.57.0	Assian
PU.busyPer	.1.3.6.1.4.1.9.2.1.56.0	
PU.idle Wired	.1.3.6.1.4.1.9.2.1.60.0	
PU.idleCount	.1.3.6.1.4.1.9.2.1.59.0	
		Add
		Modify
		Dalata
		Delete

- List of Polling OIDs lists all specific polling items.
- Click Show Details to see the OID name, OID, and the devices which this OID is assigned to.
- Click Add to add an OID form the standard MIB or a third party MIB
- Click **Modify** to modify an imported OID's name.
- Click **Delete** to remove an imported OID

There are two steps to add a new OID and assign it to the specific device.

1. Add a specific OID

Click **Add** to add a new OID for polling. A window will pop up. You can import MIB files by selecting **File** \rightarrow **Load MIB.** In this window you can edit the **Name** for the OID you selected. This name will be displayed in the device properties window.

🚱 Add a New Polling OID			
File			
RFC1213-MIB where the system (1) where the	Name ip OID 1.3.6.1.2.1.4 Operation Get Test Name Value OID Description VALUE ip OBJECT IDENTIFIER ::= 1.3.6.1.2.1.4	Index	
		Add	Cancel

Click the **Test** button to try to get the OID parameter first. You can find the description for this OID in the **OID description** window. Click the **Add** button to add this OID into the import manager.

2. Assign polling OID to the device

Click the Assign button in OID import manager. An Assign Polled Devices window will pop up

🚱 Assign Polled Devices		
Name ipInDelivers	OID .1.3.6.1.2.1.4.9.0	
All List of Devices 192.168.127.36 (192.168.127.36 ICMP Device) 192.168.127.38 (192.168.127.38 ICMP Device)	Add Add All Remove Remove All	List of Selected Devices 192.168.127.3 (192.168.127.3 EDS-408A) 192.168.127.4 (192.168.127.4 EDS-408A) 192.168.127.253 (192.168.127.253 IKS-G6824)
		Assign Cencel

This window will list all devices in the network. Select the device you wish to assign then click **Add**. The selected device will be moved to the right. After selecting the device, click **Assign** to finish.

After adding a device, click the device in the main screen. The third-party MIB OID can be read in the device property window.

Device Properties	
.20	down / 10M /
🗄 🔳 interface.21	down / 10M /
🕀 📼 interface.22	down / 10M /
🖻 🔳 interface.23	down / 10M /
🖻 🔳 interface.24	down / 100M /
🕀 📼 interface.25	down / 10M /
🕀 📼 interface.26	down / 10M /
🕀 📼 interface.27	up / -1 /
🗄 📼 interface.28	up / 1G /
📑 💇 ipAdEntAddr.192.16	58.127.252 192.1
🛛 💑 CPU.busyPer	1
🛛 📸 CPU. avgBusyl	4
🛛 🕂 🂑 CPU. avgBusy5	4
🛛 🥁 CPU.idleCount	4936
CPU.idleWired	0 🗾
•	Þ

Trap Import Manager

Trap Import Manager can read third-party MIB files, and compile the MIB into MXview. With this tool, MXview can understand traps from third-party MIBs.

To open the trap import manager, select **MIB** → **Trap Import Manager**

🚱 Trap Import Manager		- 0 🛛
List of Traps		
Name	Trap OID	Show Dataila
c2900RpsFailed	1.3.6.1.4.1.9.9.87.2.0.3	Show Details
c2900BroadcastStorm	1.3.6.1.4.1.9.9.87.2.0.2	
c2900AddressViolation	1.3.6.1.4.1.9.9.87.2.0.1	Import
		Modify Description
		Delete
		Close

- The list of traps column will list all the traps which are already imported.
- Click Show Details to read detailed information, including Trap Name, OID, and its descriptions.
- Click **Import** to load MIB files and select the trap to import.
- Click **Modify Description** to name the description for the Trap. The description here will be the trap event which shows in the event list.
- Click **Delete** to remove an imported Trap.

There are three steps to add a new Trap to MXview.

1. Load a MIB

Click the **Import** button. The **Import Dialog** window will pop up. Then click **Load MIB** and select a MIB file to load.

After the MIB is loaded, click **Parse**. The column on the right will list all the Traps.

🔂 Impor

CISCO-

t Dialog			X
.oad MIB Remove MIB	c2900AddressViolation	c2900AddressViolation	···· ^
C2900-MIB.my	c2900BroadcastStorm	c2900BroadcastStorm	
	c2900RpsFailed	c2900RpsFailed	···
	linkDown	linkDown	
	linkUp	linkUp	
	coldStart	coldStart	
	warmStart	warmStart	

authenticationFailure

Import

Cancel

2. Select Trap to import

Parse

Select the check box corresponding to the Trap you would like to import.

Click the button behind each Trap to show its OID and the original description of its MIB.

authenticationFailure

😼 c2900Address¥iolation 🛛 🔀					
OID	1.3.6.1.4.1.9.9.87.2.0.1				
Enterprise	1.3.6.1.4.1.9.9.87.2				
VALUE c2900Add	ressViolation NOTIFICATION-TYPE (
Objects: [1.3	3.6.1.4.1.9.9.87.1.4.1.1.25]				
Status: Curre	Status: Current				
Description:	The addressViolation notification is generated				
	when an address violation is detected	≡			
	on a secured port. The generation of the				
	addressViolation notification can be enabled				
	or suppressed using the object				
	c2900ConfigAddressViolationAction.				
	The particular secured port is indicated by				
	the value of c2900PortIfInder	×			
	Close				

3. Edit description

In the Trap list, the description field is editable. You are able to write a customized description here.



When finished, click the **Import** button. The dialog will be closed and returned to the **Trap Import Manager** window. You will find imported Traps in your List.



NOTE The system will notify you with a pop-up window if an OID has already been imported.



MXview is available in different versions, which the different versions supporting different numbers of nodes. For example, if your version of MXview supports 250 nodes, then during device discovery MXview will only recognize up to 250 nodes. MXview will stop the device discovery procedure once it reaches the 250-node limit.

The MXview license that you purchase specifies the node limit for that version of MXview. To increase the node limit, you can purchase license upgrade and import the upgrade into MXview.

Checking the License

The number of currently managed nodes and the node limit is shown in the Status Bar on the Dashboard.

```
The Number of Managed Devices / Max : 24 / 50
```

To check the details, select **Help** \rightarrow **License**.

MX License			
Number of Manage	ed Devices / Max		
Edition	Кеу	Activation Time	Add License
Commercial-500	DYFHLHAU77CRDP3N4MF5WI5YA6	2009-11-04 11:52:06	
			Close

License Upgrade

To increase the node limit of your MXview, you need upgrade the license.

- 1. Select **Help → License**.
- 2. Click Add License.

🔤 License			
Number of Manag	ged Devices / Max		
Edition	Key	Activation Time	Add License
Commercial-500	DYFHLHAU77CRDP3N4MF5WI5YA6	2009-11-04 11:52:06	
			Close
3. Find the license label in the software package, which is shown as:

MXview Upgrade-50 Key: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

4. Enter the key of the new license and click ${\bf OK}.$

<u></u>	
Input License Key	
	OK Cancel

5. Restart the MXview client.

Why do events show up late?

Make sure you have configured your switches' SNMP trap server to the MXview server's IP address, since doing so will provide real-time responses to events. Otherwise, MXview will collect information periodically.

Why can't I discover all of the devices on my network?

Please check the following:

- 1. Make sure your license supports a sufficient number of nodes.
- 2. Make sure your scan range includes all of the IP addresses of devices on your network.
- 3. Make sure your switches do not go into protection mode because they consider MXview packets to be part of a broadcast storm.

Why does one device have more than one icon?

MXview identifies devices by IP address. For this reason, if one device has more than one IP address within the scan range, the device will be viewed as multiple devices.

Will deleting a link in MXview cause the link to be disconnected in the real network?

No. The topology map shows the status of the real network, but cannot be used to configure the real network.

After a link in a ring is disconnected, why does it take a few seconds for the redundant link to become solid in the topology map?

MXview uses polling to determine if redundant links have become non-redundant. For this reason, the topology map will not be updated until all devices in the network have been polled. In addition, since it takes a finite amount of time to transmit the network status to the MXview server, it will take at least that amount of time for the topology map to be updated.

License

License (Net-SNMP)

Various copyrights apply to this package, listed in several separate sections below.

Please carefully review all sections of the license information.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000 Copyright 1996, 1998-2000. The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR

CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,

WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,

WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The MIT License (Libxml2)

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.

License Agreement (GoAhead)

THIS LICENSE AGREEMENT IS BETWEEN YOU AND GOAHEAD (BOTH AS DEFINED BELOW). THIS AGREEMENT GRANTS YOU ONLY A LIMITED LICENSE TO USE GOAHEAD PROPRIETARY COMPUTER SOFTWARE. BY EXECUTING THIS AGREEMENT OR USING THE SOFTWARE, YOU CERTIFY THAT YOU WILL USE THE SOFTWARE ONLY IN THE MANNER PERMITTED HEREIN.

1. Definitions.

"Documentation" means any documentation GoAhead provides with the Original Code.

"GoAhead" means GoAhead Software, Inc.

"Agreement" means this document.

"**Modifications**" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications.

"**Original Code**" means the source code to GoAhead's proprietary computer software entitled GoAhead WebServer that is provided to You by GoAhead.

"**You**" means an individual or a legal entity exercising rights under, and complying with all of the terms of, this license or a future version of this license. For legal entities, "You" includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct

or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of fifty percent (50%) or more of the outstanding shares or beneficial ownership of such entity.

"**Response Header**" means the first portion of the response message output by the GoAhead WebServer, containing but not limited to, header fields for date, content-type, server identification and cache control.

"Server Identification Field" means the field in the Response Header which contains the text "Server: GoAhead-Webs".

2. License.

Limited Original Code Grant.

Subject to the terms of this Agreement, GoAhead hereby grants You a worldwide, royalty-free, nonexclusive, nontransferable license, without right of sublicense, subject to third party intellectual property claims, (a) to use and reproduce the Original Code, (b) to create Modifications from the Original Code, and (c) to distribute source code copies of the Original Code form solely when embedded in other software (in a manner that does not allow the Original Code to be separated) that provides material functionality in addition to the functionality provided by the Original Code.

Binary Code.

Subject to the terms of this Agreement, GoAhead hereby grants You a worldwide, royalty-free, nonexclusive, nontransferable license, without right of sublicense, to copy and distribute binary code copies of the Original Code together with Your Modifications in binary code.

Restrictions on Use.

You may sublicense third parties to use Your Modifications if You enter into a license agreement with such third parties that bind such third parties to all the obligations under this Agreement applicable to You and that are otherwise substantially similar in scope and application to this Agreement (without limiting the protections afforded to GoAhead). You may not rent, lease, or loan the software.

Documentation.

Subject to the terms of this Agreement, GoAhead hereby grants You a worldwide, royalty-free, nonexclusive, nontransferable license, without right of sublicense, to copy and distribute the Documentation in connection with the authorized distribution of the Original Code and Modifications.

Copyright Notice.

You agree to include copies of the following notice (the "Notice") regarding proprietary rights in all copies of the Original Code and Modifications that You distribute, as follows: (a) embedded in the binary code; and (b) on the title pages of all documentation. Furthermore, You agree to use commercially reasonable efforts to cause any licensees of your products to embed the Notice in object code and on the title pages or relevant documentation. The Notice is as follows: Copyright (c) 20XX GoAhead Software, Inc. All Rights Reserved. Unless GoAhead otherwise instructs, the year 20xx is to be replaced with the year during which the release of the Original Code containing the notice is issued by GoAhead. If this year is not supplied with Documentation, GoAhead will supply it upon request.

License Back to GoAhead.

You hereby grant in both source code and binary code to GoAhead a world-wide, royalty-free, non-exclusive license to copy, modify, display, use and sublicense any Modifications You make that are distributed or planned for distribution. Within 30 days of either such event, You agree to ship to GoAhead a file containing the Modifications (in a media to be determined by the parties), including any programmers' notes and other programmers' materials. Additionally, You will provide to GoAhead a complete description of the product, the product code or model number, the date on which the product is initially shipped, and a contact name, phone number and e-mail address for future correspondence. GoAhead will keep confidential all data specifically marked as such.

3. Terms, Trademards and Brand.

License and Use.

GoAhead hereby grants to You a limited world-wide, royalty-free, non-exclusive license to use the GoAhead trade names, trademarks, logos, service marks and product designations posted in Exhibit A (collectively, the "GoAhead Marks") in connection with the activities by You under this Agreement. Additionally, GoAhead grants You a license under the terms above to such GoAhead trademarks as shall be identified at a URL (the "URL") provided by GoAhead. The use by You of GoAhead Marks shall be in accordance with GoAhead's trademark policies regarding trademark usage as established at the Web site designated by the URL, or as otherwise communicated to You by GoAhead at its sole discretion. You understand and agree that any use of GoAhead Marks in connection with this Agreement shall not create any right, title or interest in or to such GoAhead Marks and that all such use and goodwill associated with GoAhead Marks will inure to the benefit of GoAhead.

Promotion by You of GoAhead WebServer Mark.

In consideration for the licenses granted by GoAhead to You herein, You agree to notify GoAhead when You incorporate the GoAhead WebServer in Your product and to inform GoAhead when such product begins to ship. You agree to promote the Original Code by prominently and visibly displaying a graphic of the GoAhead WebServer mark on the initial Web page of Your product that is displayed each time a user connects to it. You also agree that GoAhead may identify your company as a user of the GoAhead WebServer by placing your company logo on its Web site. You may further promote the Original Code by displaying the GoAhead WebServer mark in marketing and promotional materials such as the home page of your Web site or Web pages promoting the product. You also agree to use the latest available logo and script code from GoAhead available from the official GoAhead download location.

No Modifications to Server Identification Field.

You agree not to remove or modify the Server identification Field contained in the Response Header as defined in Section 1.7 and 1.8.

4. Term.

This Agreement and license are effective from the time You execute this Agreement until this Agreement is terminated. You may terminate this Agreement at any time by uninstalling or destroying all copies of the Original Code including all binary versions and removing any Modifications to the Original Code existing in any products. This Agreement will terminate immediately and without further notice if You fail to comply with any provision of this Agreement. All restrictions on use, and all other provisions that may reasonably be interpreted to survive termination of this Agreement, will survive termination of this Agreement for any reason. Upon termination, You agree to uninstall or destroy all copies of the Original Code, Modifications, and Documentation.

5. Warranty Disclaimers.

THE ORIGINAL CODE, THE DOCUMENTATION, AND THE MEDIA UPON WHICH THE ORIGINAL CODE IS RECORDED (IF ANY) ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, EXPRESS, STATUTORY OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

The entire risk as to the quality and performance of the Original Code (including any Modifications You make) and the Documentation is with You. Should the Original Code or the Documentation prove defective, You (and not GoAhead or its distributors, licensors or dealers) assume the entire cost of all necessary servicing or repair. GoAhead does not warrant that the functions contained in the Original Code will meet your requirements or operate in the combination that You may select for use, that the operation of the Original Code will be uninterrupted or error free, or that defects in the Original Code will be corrected. No oral or written statement by GoAhead or by a representative of GoAhead shall create a warranty or increase the scope of this warranty.

GOAHEAD DOES NOT WARRANT THE ORIGINAL CODE AGAINST INFRINGEMENT OR THE LIKE WITH RESPECT TO ANY COPYRIGHT, PATENT, TRADE SECRET, TRADEMARK OR OTHER PROPRIETARY OR INTELLECTUAL PROPERTY RIGHT OF ANY THIRD PARTY AND DOES NOT WARRANT THAT THE ORIGINAL CODE DOES NOT INCLUDE ANY VIRUS, SOFTWARE ROUTINE OR OTHER SOFTWARE DESIGNED TO PERMIT UNAUTHORIZED ACCESS, TO DISABLE, ERASE OR OTHERWISE HARM SOFTWARE, HARDWARE OR DATA, OR TO PERFORM ANY OTHER SUCH ACTIONS. Any warranties that by law survive the foregoing disclaimers shall terminate 90 days from the date You received the Original Code.

6. Limitation of Liability.

YOUR SOLE REMEDIES AND GOAHEAD'S ENTIRE LIABILITY ARE SET FORTH ABOVE. IN NO EVENT WILL GOAHEAD OR ITS DISTRIBUTORS OR DEALERS BE LIABLE FOR DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE ORIGINAL CODE, THE INABILITY TO USE THE ORIGINAL CODE, OR ANY DEFECT IN THE ORIGINAL CODE, INCLUDING ANY LOST PROFITS, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

You agree that GoAhead and its distributors and dealers will not be LIABLE for defense or indemnity with respect to any claim against You by any third party arising from your possession or use of the Original Code or the Documentation.

In no event will GoAhead's total liability to You for all damages, losses, and causes of action (whether in contract, tort, including negligence, or otherwise) exceed the amount You paid for this product.

SOME STATES DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, AND SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY HAVE OTHER RIGHTS THAT VARY FROM STATE TO STATE.

7. Indemnification by You.

You agree to indemnify and hold GoAhead harmless against any and all claims, losses, damages and costs (including legal expenses and reasonable counsel fees) arising out of any claim of a third party with respect to the contents of the Your products, and any intellectual property rights or other rights or interests related thereto.

8. High-Risk Activities.

The Original Code is not fault-tolerant and is not designed, manufactured or intended for use or resale as online control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines or weapons systems, in which the failure of the Original Code could lead directly to death, personal injury, or severe physical or environmental damage. GoAhead and its suppliers specifically disclaim any express or implied warranty of fitness for any high-risk uses listed above.

9. Government Restricted Rights.

For units of the Department of Defense, use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013. Contractor/manufacturer is GoAhead Software, Inc., 10900 N.E. 8th Street, Suite 1200, Bellevue, Washington 98004.

If the Commercial Computer Software Restricted rights clause at FAR 52.227-19 or its successors apply, the Software and Documentation constitute restricted computer software as defined in that clause and the Government shall not have the license for published software set forth in subparagraph (c)(3) of that clause.

The Original Code (i) was developed at private expense, and no part of it was developed with governmental funds; (ii) is a trade secret of GoAhead (or its licensor(s)) for all purposes of the Freedom of Information Act; (iii) is "restricted computer software" subject to limited utilization as provided in the contract between the vendor and the governmental entity; and (iv) in all respects is proprietary data belonging solely to GoAhead (or its licensor(s)).

10. Governing Law and Interpretation.

This Agreement shall be interpreted under and governed by the laws of the State of Washington, without regard to its rules governing the conflict of laws. You hereby consent to the exclusive jurisdiction of the state and federal courts located in King County, Washington over any disputes arising out of related to this Agreement. If any provision of this Agreement is held illegal or unenforceable by a court or tribunal of

competent jurisdiction, the remaining provisions of this Agreement shall remain in effect and the invalid provision deemed modified to the least degree necessary to remedy such invalidity.

11. Entire Agreement.

This Agreement is the complete agreement between GoAhead and You and supersedes all prior agreements, oral or written, with respect to the subject matter hereof.

License (OpenSSL)

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/*______

* Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
- The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
- 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
- Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE

OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* _____

* This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

/

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

* Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
- 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"The word "cryptographic" can be left out if the rouines from the library being used are not cryptographic related :).
- 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A

PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

/

License (zlib)

/* zlib.h -- interface of the "zlib" general purpose compression library version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided "as-is", without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

- 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
- 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
- 3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

/