### **MXview 3.2.11 User Manual**

Version 2.5, March 2024

www.moxa.com/products



#### MXview 3.2.11 User 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**

© 2024 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

### **Table of Contents**

1.	Introduction	6
	Key Features	6
	Web-based Operation	6
	Auto Discovery and Topology Visualization	6
	Event Management	6
	Configuration and Firmware Management	6
	Traffic Monitoring	6
	MXview Operation Model	7
	System Requirements	7
	Supported Devices	7
2.	Installation, System Backup, and Certificates	
	Installation Procedure	8
	Uninstallation	8
	System Backup	8
	Certificates	
3.	Getting Started	13
	Starting the MXview Server and Logging Into MXview Locally	
	Logging Into MXview Remotely	15
	Multiple MXview Sites	16
	Configuration of Multiple Sites	
	License Management	20
	Checking the License	20
	Using the Setup Wizard	21
	Adding a New License	
	Deactivating a License	
	Account Management	
	Adding User Accounts	
	Modifying User Accounts	
	Deleting User Accounts	
	Exporting User Accounts	
	Configuring Account Passwords	
	Configuring Login Notifications	
	Changing the Display Language	
4.	License Management	33
	License Management Overview	
	Adding a New License	34
	Adding an Upgrade and Add-on License	38
	Deactivating a License	40
	Reactivating a Deactivated License	40
	Transferring a License to a Different Installation of MXview	42
5.	Dashboard Widgets	44
	Dashboard Overview	44
	Device Summary	44
	Device Availability	45
	Event Highlights: Cold/Warm Start Trap	
	Event Highlights: ICMP Unreachable	
	Event Highlights: Link Down	48
	Disk Space Utilization	48
6.	Device Discovery and Polling	49
	Device Discovery Overview	
	Configuring IP Address Scan Ranges	50
	Configuring Background Discovery	52
	Configuring Device Polling Settings	
	Changing Default SNMP Configurations	
7.	Topology Management	
	Network Topology Overview	
	Viewing Topology Map	
	Viewing Recent Events	58

	Organizing the Topology Structure	60
	Redundant Topologies	63
	PoE Power Consumption Visualization	63
	VPN Tunnel Visualization	64
	PRP/HSR Visualization	64
	Third-party Icons	65
	Port Trunking	
	Adding Devices and Links	
	Deleting Devices and Links	
	Updating the Topology Map	
	Refreshing the Topology Layout	
	Creating a New Topology Map	
	Setting/Deleting the Background Image	
	Editing the Topology Appearance	
	Editing the Device Appearance	
_	Exporting the Topology Map	
8.	Network and Traffic Monitoring	
	Viewing Link Properties	
	Viewing Port Traffic	
	Viewing Packet Error Rates	
	Monitoring Traffic Loads	81
	Monitoring Network Security	82
	Visualizing VLAN Connections	87
	Monitoring Wireless Access Points and Clients	87
	Configuring Severity Thresholds for Traffic and Fiber Status Monitoring Events	
	Configuring Custom Port Labels	
9.	SFP Fiber Status	
-	Viewing the SFP Fiber Status in Table View	
10.	Device Management	
	Viewing the Device List	
	Importing Device Configurations	
	Exporting Device Configurations	
	Upgrading Firmware	
	Generating a QR Code for the Device	
	Assigning a Device Model	
	Configuring Basic Device Information	
	Configuring Device IP Settings	
	Configuring SNMP Trap Servers	
	Configuring Port Settings	
	Configuring SNMP Settings	102
	Configuring Polling Settings	103
	Configuring Advanced Settings	104
	Configuring Polling IP Settings	105
	Changing the Device Icon	106
	Signing on to Device Web Consoles	
	Pinging Devices	108
	Changing Device Groups	
	Uploading Device Documents	
	Refreshing the Device Status	
	Locating Device Status	
	-	
11.	Deleting Devices Events and Notifications	
11.		
	Event Monitoring	
	Viewing All Events	
	Viewing Syslog Events	
	Configuring the Server Disk Space Threshold	
	Configuring Event Thresholds and Severity Levels	
	Notification Methods	
	Configuring Email Server Settings	
	Configuring SNMP Trap Destinations for the MXview Server	101

	Configuring the SNMP Trap Destination for Devices	. 121
	Notification Management	
	Configuring New Event Notifications	. 122
	Add a Slack/Teams Notification	. 123
	Editing or Exporting Registered Actions	. 126
	Editing or Exporting Notification Configurations	. 127
	Custom Event Management	. 128
	Configuring Custom Events	. 128
	Viewing or Exporting Custom Event Settings	. 129
	Enabling/Disabling or Editing Custom Events	. 131
12.	Reports	.132
	Viewing VLAN Reports	. 132
	Viewing Inventory Reports	. 133
	Viewing Availability Reports	. 133
13.	Backups and Migrations	.135
	Backing Up the MXview Database	
	Backing Up Device Configurations	. 135
	Restoring Device Configurations	. 136
	Comparing Archived Configuration Files	
	Creating Scheduled Jobs for Database/Configuration Backups	. 141
14.	Custom Integrations	
	Managing API Keys	
	Embedding Web Widgets	
	Generating OPC Tags	
15.	Wireless Add-on Module	-
	Introduction	
	System Requirements	
	Supported Devices	
	Getting Started With the Wireless Add-on Module	
	Wireless Module Features	
	Main Dashboard	
	Dynamic Wireless Client Roaming	
	AP/Client Device Dashboard	
	AP Device Dashboard	
	Client Device Dashboard	
	Wireless Device Summary	
	Wireless Roaming Playback	
Α.		
	License (Net-SNMP)	
	The MIT License (Libxml2)	
	License Agreement (GoAhead)	
	License (OpenSSL)	
	License (zlib)	
	License (node-tacacs-plus)	. 170

The Moxa MXview network management software consists of two parts: The Main Module and the Wireless Add-on Module. The 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, wireless APs, SNMP-enabled, and ICMP-enabled devices installed on subnets. The MXview Wireless Add-on Module provides additional advanced functions for wireless applications to monitor and troubleshoot your network, and help you minimize downtime.

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.

### **Key Features**

### 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 using Chrome, Firefox, Microsoft Edge (version 79+), or Internet Explorer 11, 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.

### **Event Management**

For troubleshooting purposes, MXview logs events that match predefined 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 email, popup window, sound, or external program.

### **Configuration and Firmware Management**

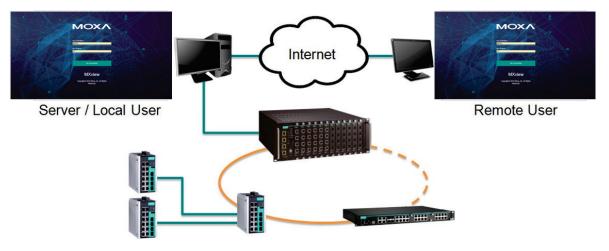
MXview provides an interface for managing Moxa networking devices from a central location. Users can remotely backup or update configuration files, and upgrade firmware.

### **Traffic Monitoring**

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

### **MXview Operation Model**

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.

### **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	8 GB or higher
Hard Disk Space	20 GB or higher
	Windows 7 Service Pack 1 (64-bit)
os	Windows 10 (64-bit)
03	Windows Server 2012 R2 (64-bit)
	Windows Server 2016 (64-bit)
	Browser:
	Chrome: Version 76 or later
Client Browser Requirements	Firefox: Version 69 or later
	Microsoft Edge: Version 79 or later
	Internet Explorer 11

### **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.

## 2. Installation, System Backup, and Certificates

### **Installation Procedure**

- 1. Execute the installation program.
- 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. You require a license to operate MXview, please check the License Chapter for more detail.
- 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
- Under Programs, click Uninstall a program
   The Uninstall or change a program screen appears
- 3. Select MXview
- 4. Click Uninstall or Uninstall/Change at the top of the program list

You can also uninstall the software by selecting

Start > All Programs > Moxa > MXview > Uninstall MXview

### System Backup

Use the Database Backup screen on the MXview web console to back up the MXview database and configuration files.

- 2. In the **Name** field, specify the backup directory.
  - Default directory: %MXviewPro\_Data%\db\_backup
- 3. Click **Apply**.

MXview exports the backup database to the specified directory.

The **Database backup completed** event will appear on the **Recent Events** list. Hover over the **Description** to view the file path of the backup files.

							Rec	ent Events 🗸	
Type to filter even	1							Ŧ.	
Ack	Site Name	ID	Source	Source IP	Device Alias	Description	Time Issued ~		
۲	Site	73	MXview	0.0.0.0		Database backup is completed, stored at %MXviewPRO_Data%\db_backup\	2018-11-25 15:56:06		Í
۱	Site	72	MXview	0.0.0.0		Auto Topology finished	2018-11-25 01:13:54		

The backup folder uses the following naming convention: YYYYMMDD HHMMSS

The system backup includes the following items:

- 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 > All Programs > Moxa > MXview > 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 > DB Restore tool

	Moxa ^ .
	DB Backup Folder
<b>H</b>	DB Restore tool
R	edscfgui
3	Library Programming Guide
2	Library Reference

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	15:04:17	
2012/10/01	16:24:59	
2012/11/02	15:28:33	
	Restore	Close

4. Click **Restore**.

Database Restore Tool	×
Restore from MXview's archive repository Restore from a specific folder	
Backup Folder:	
D:\20121102 152833	
Restore	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 > Import MXview Configuration file**, and then select the backup file to restore.

### Certificates

MXview uses an authentication certificate for HTTPS. By default, the web console certificate is generated and signed by MXview itself.

To change the certificates, follow the steps below:

- 1. Change the **server.pem** file.
  - a. Navigate to the directory with the server certificate (default: %mxviewpro\_data%).
  - b. Replace the server certificate file with the new file. The filename must be identical: **server.pem**

🔜   🕑 🔜 🖛   mxv						
	share > MOXA	View > AppData > Roaming > moxa > 1	mxview >			<b>∨</b> © S
<ul> <li>← → · ↑</li> <li>✓ Quick access</li> <li>Desktop</li> <li>✓ Downloads</li> <li>🔄 Documents</li> <li>🖃 Pictures</li> <li>Report</li> <li>SCD</li> <li>System32</li> <li>✓ Windows (C:)</li> <li>This PC</li> </ul>		<ul> <li>AppData &gt; Roaming &gt; moxa &gt; r</li> <li>Iame</li> <li>certs</li> <li>certs</li> <li>data</li> <li>db_backup</li> <li>device_config</li> <li>jobs</li> <li>log</li> <li>mxview-gateway</li> <li>nms-platform</li> <li>playback</li> <li>web</li> </ul>	moview → Date modified 2/5/2024 3:15 PM 2/5/2024 3:20 PM 2/7/2024 3:13 PM 2/5/2024 3:13 PM 2/5/2024 3:13 PM 2/1/2024 10:32 AM 2/5/2024 10:32 AM 2/5/2024 3:15 PM 2/5/2024 3:14 PM 2/5/2024 3:14 PM	Type File folder File folder File folder File folder File folder File folder File folder File folder File folder File folder	Size	V O Si
<ul> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Windows (C:)</li> <li>Network</li> </ul>	Ţ	atewaylock server.pem	2/14/2024 10:32 AM 2/5/2024 3:15 PM	File PEM File	0 KB 3 KB	

- 2. Change the **mxview.crt** and **mxview.key** files.
  - a. Navigate to the directory with the MXview certificate and key file (default: %mxviewpro\_data%\mxview-gateway).
  - b. Replace the MXview certificate file and key file with the new files. The filenames must be identical: **mxview.crt**, **mxview.key**

i 🛃 📑 🖛 i mxv	iew-	gateway				
File Home	Share	e View				
← → • ↑ 📙	> M	10XA > AppData > Roaming > r	noxa > mxview > mxview-gateway	>		ڻ ~
		Name	Date modified	Туре	Size	
📌 Quick access		apidoc	2/5/2024 3:14 PM	File folder		
Desktop	*	bin	2/5/2024 3:14 PM	File folder		
👆 Downloads	*		2/5/2024 3:15 PM	File folder		
Documents	*		2/5/2024 3:13 PM	File folder		
Pictures	*		2/5/2024 3:13 PM	File folder		
Report	~	logs	2/7/2024 12:01 AM	File folder		
-		node modules	2/5/2024 12:01 AM	File folder		
SCD		tacacs	2/5/2024 3:14 PM	File folder		
System32		ui_profiles	2/5/2024 3:14 PM	File folder		
🏪 Windows (C:)		utils	2/5/2024 3:15 PM	File folder		
💷 This PC		aclfile.conf	2/5/2024 3:13 PM	CONF File	1 KB	
_		gateway-version.json	2/5/2024 2:12 PM	JSON File	1 KB	
🧊 3D Objects		mg_mgtt.conf	2/5/2024 2:12 PM	CONF File	1 KB	
Desktop		mosquitto.conf	2/5/2024 3:22 PM	CONF File	37 KB	
🔮 Documents		mosquitto.com	2/5/2024 2:12 PM	Security Certificate	2 KB	
👆 Downloads		mxview.key	2/5/2024 2:12 PM	KEY File	2 KB	
h Music		package.json	2/5/2024 2:12 PM	JSON File	2 KB	
Pictures			2/5/2024 2:12 PM	JSON File	563 KB	
Videos		package-lock.json	2/5/2024 2:12 PM 2/5/2024 2:12 PM	PEM File	203 KB 4 KB	
		server.pem	2/5/2024 2:12 PM 2/7/2024 7:07 PM	JSON File	4 KB 1 KB	
🏪 Windows (C:)		sessions.json		JSON File	1 KB	
💣 Network		version.json	2/5/2024 2:12 PM	J2014 File	I KB	

3. After replacing all three files, stop and restart the MXview service. MXview will now use the new certificates.

Moxa Inc. All right	s reserved.	$\rightarrow$	$\ll$
ITTP Port	80 443	Disable HTTP port	Start Stop
Comm. Port Database Port	8883 5432		
Polling Engine Port	4430		
system Status: Sto	p		

# Starting the MXview Server and Logging Into MXview Locally

Start MXview server on the computer before launching the MXview web console locally.

1. On the server computer, double-click the MXview desktop shortcut.

The MXview server screen appears.

MXview ver 3.2.4

Service Info			
HTTP Port HTTPS Port	80 443	Disable HTTP port	Start Stop
Comm. Port	8883		
Database Port	5432		
Polling Engine Port	4430		

- 2. Configure the following port numbers:
  - > HTTP Port: Specify the listening port of the server or use the default value of 80.
  - > **HTTPS Port:** Specify the HTTPS port of the server or use the default value of **443**.
  - Comm. Port: Specify the Remote Communication port of the server or use the default value of 8883.
  - > Database Port: Specify the database port of the server or use the default value of 5432.
  - > Polling Engine Port: Specify the polling engine port of the server or use the default value of 4430.
- 3. Click Start.

The MXview server starts running.

- 4. To log in to the MXview web console from the server computer:
  - a. Click Launch Client.

The MXview web console appears.



- b. Provide the following login credentials
  - **Username:** The default account is **admin**.
  - **Password:** The default password is **moxa**.

The user account logs in to the MXview web console.

### NOTE

Alternatively, you can log in to MXview from a remote computer after starting the MXview service. For more information, see **Logging Into MXview Remotely**.

### **Logging Into MXview Remotely**

Use the MXview Client to launch the MXview web console from a remote computer.

- 1. Open a web browser.
- 2. In the address bar, input the IP address or domain name of the MXview server.
  - Format: http://[IP address]:[Port]
  - Example: http://192.168.1.250:8080)

The MXview web console appears.



- 3. Provide the following login credentials
  - > **Username:** The default account is **admin**.
  - > **Password:** The default password is **moxa**.

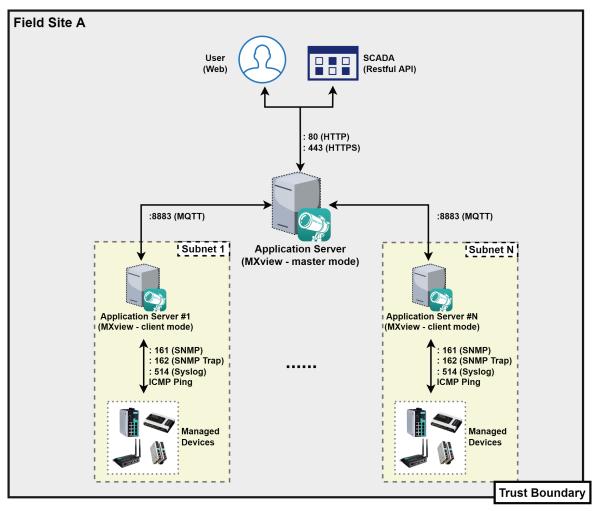
The user account logs in to the MXview web console.

### NOTE

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

### **Multiple MXview Sites**

MXview can be configured to the distributed structure as the following figure shows. Users can monitor and manage all of the MXview site at the master site at the same time. One MXview server can be configured to connect to 10 MXview servers with 1 layer and MXview cannot be configured to be the master and client at the same time.



### **Configuration of Multiple Sites**

1. Click the **Config Tool** when MXview server stops running.

MXview ver 3.2.4

ervice Info			
HTTP Port	80	Disable HTTP port	Start
HTTPS Port	443		Stop
Comm. Port	8883		
Database Port	5432		
Polling Engine Port	4430	-	

2. The control panel will pop up, choose the master if this MXview is configured to be the master to monitor multiple instances of MXview.

	ole <ul> <li>Master</li> <li>Master</li> </ul>		127.0.0.1		
Re	emote Comm. Port		8883		
Re	emote Comm. Port Passwo	ord			
Re	e-type the password for co	onfirmation			
		Add		Modify	
Ma	ster IP/Domain Name	Master Po	rt		

3. Choose Client if the MXview is the one to be monitored:

From V3.1.4, MXview supports pushing one client's data to two master MXview.

Enter the IP of the Master MXview on the Master Server IP, then, enter the remote communication port of Remote Comm. port which showed at the master side at the Remote Comm. Port and the Remote Comm. Password at the field, Remote Comm. Password, which also can be found at the local tab of MXview server. Click 'Add' to add the master to the list.

R	ole 🔿 Master 🤅	Client		
M	aster Server IP	[	127.0.0.1	
Re	emote Comm. Port	[	8883	
Re	emote Comm. Port Passwo	ord [	*****	
Re	e-type the password for co	onfirmation Add	i M	odify
Ma	ster IP/Domain Name	Master Po	rt	
127.	0.0.1	8883		Delete

To modify the master settings, select a row and the master data will be displayed in the upper textbox. Click 'Modify' to update the settings to the table.

	ole 🔿 Master 🤅 laster Server IP	y chem	127.0.0.1	
Re	emote Comm. Port		8883	
Remote Comm. Port Passw		ord	******	
		Ad	d N	lodify
-	ster IP/Domain Name 0.0.1	Master Po 8883	ort	Delete

The Local tab shows the port setting and password of MXview. The default password of the remote communication port is 89191230, and the default database password is 89191230.

Local				
able HTTP Port				
Port		80		
S Port		443		
g Engine Port		4430		
n. Addr		disable remote connectivity $\sim$		
n. Port		8883		
n. Port Password		****		
pe the password	for confirmation	*****		
ase Port		5432		
ase Password		*****		
pe the password	for confirmation	*****		
ation. Port		8884		
al. Port		8882		
	Port S Port g Engine Port n. Addr n. Port n. Port Port Password pe the password pase Port pase Password pe the password pe the password ation. Port	Port S Port g Engine Port n. Addr n. Port n. Port n. Port Password be the password for confirmation wase Port wase Password be the password for confirmation ation. Port		

### License Management

MXview is available in different versions, and each version supports a different number 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.

|--|

### NOTE

Click "Start Free Trial" to start using MXview.

### **Checking the License**

The **License Manager** screen displays information about your MXview license, including the number of licensed nodes currently in use. You can also use the **License Manager** screen to add a new license or deactivate an existing license.

To access the License Manager screen, navigate to Menu ( $\equiv$ ) > License.

MXview			0
	License Mode: None State: No valid licenses Current Nodes: 0	Wireless Add-on Mode: None	
Moxa License Site			
Add New License	License Type		
Add New License	License Type	Network Adapter	Re-activate License
		Network Adapter MXview binds the license to one network adapter, please choose the adapter you want to bind. Re-select a network adapter will deactivate all your licenses automatically, you have to register them again.	Re-activate License Use both the Deactivation code and User Code to re-activate your license.

The **License Manager** screen displays the license type, the number of nodes in use, and the total number of nodes available under the current license.

### **Using the Setup Wizard**

MXview provides a Setup Wizard to help administrators quickly determine the network topology and handle basic configuration tasks. The wizard launches automatically when no network nodes have been configured.

- 1. To launch the Setup Wizard manually:
  - a. Navigate to **Menu** (트) **> Wizard**.

The **Setup Wizard** appears to the right of the navigation panel.

- b. Select a site to set up from the Site Name drop-down list.
- c. Click Next.

Welcome to setup wizard
Welcome to setup wizard
This wizard will help you
1. Create Group
2. Set SNMP Settings
3. Add scan range
4. Draw Topology (for devices supporting LLDP)
5. Set SNMP trap server
Please select a site to setup
Site Name
Site

2. Create groups to organize scanned devices into a multi-layer tree structure.

### NOTE

Before finding devices, groups need to be created. Root is the default group and the top-most layer in the tree structure. All other created groups are placed below the level of Root.

- a. Select the parent group.
- b. Click **Create** to create a new group under the parent group.
- c. Specify the following:
  - **Group Name:** Type a name for the group.
  - **Group Description:** Type a description for the group.
- d. Click Apply.

MXview creates the new group below the selected parent group.

e. Click Next.

Parent Group *	
Root	
Group Name *	
group 1	
Group Description test	7/6
Image 🔒 🧿	4 / 12

- 3. Configure the SNMP settings.
  - a. Specify the following (update default settings if necessary):
    - □ SNMP Version: Default is "V1"
    - **User Name:** Provide the user name for the SNMP community string (if required)
    - **Password:** Provide the password for the SNMP community string (if required)
    - □ Read Community: Default is "public"
    - □ Write Community: Default is "private"
    - Data Encryption: Default is "NoAuth"
    - □ Authentication: Default is "MD5"
    - **Encryption Key:** Provide the encryption key (if required)
    - **Encryption Protocol:** Default is DES (if required)
    - **SNMP Port:** Default is 161

b. Click Next.

SNMP Version * V3	-	Port * 161	
User Name admin		Password 🔌	
Read Community		Write Community	
public		private	
Data Encryption		Authentication	
AuthPriv	•	MD5	8
Encryption Protocol			
AES		Encryption Password	3

4. Add the IP address ranges to scan for devices.

#### NOTE

MXview supports scanning multiple IP address ranges. The selected IP address scan ranges must be enabled in order for MXview to scan for devices.

a. Click the Add (1) icon.

The Add Scan Range screen appears.

- b. Select one of the following options:
  - **Enabled:** Select to enable scanning of the specified IP address range.
  - **Disabled:** Select to disable scanning of the specified IP address range.
- c. Configure the following:
  - **D** Provide a custom display Name for the scan range.
  - □ Specify the **First IP Address** of the scan range.
  - □ Specify the **Last IP Address** of the scan range.
  - □ Select the **CIDR Prefix** for the scan range (if applicable).
  - □ Select the MXview **Group** to assign the scan range to.
- d. Click Add.
- e. (Optional) Add additional network scan ranges, repeat the previous steps.
- f. (Optional) Modify scan range settings, click the **Edit** ( $\checkmark$ ) icon next to an added scan range.
- g. (Optional) Remove a scan range, click the **Delete** ( $\hat{I}$ ) icon next to the added scan range.
- h. Select one or more scan ranges to scan.

#### i. Click Next.

MXview scans the specified IP address ranges for devices.

F	Add scan range							
	Ð							
		Enabled/Disabled	Name	First IP Address	Last IP Address	Group	Site Name	
	□ ⁄ ∎	Enabled	Test	192.168.127.1	192.168.127.254		Site LyraCCLi-NB	
								1 – 1 of 1

5. (Optional) Recover devices ignored (deleted) from a previous scan:

#### NOTE

If an IP address scan range is removed (deleted) from a previous network scan, MXview excludes devices within the deleted range from the network topology. Use the Recovery feature to restore the devices from deleted scan ranges to the network topology.

- a. Select a device from the list of ignored devices.
- b. Click Next.
- c. MXview scans for network devices.
- 6. View devices discovered on the network.
  - MXview displays discovered devices on the **Device Result** list. Scroll down to view more devices on the list.

Device Alias	Device IP	Group	Site Name	
Device discovery is finished				

- b. Click Next.
- 7. Draw the network topology.

### NOTE

MXview is only able to automatically draw the topology for LLDP devices. For devices without LLDP functionality, the topology can be drawn manually after the wizard completes.

- a. Select one of the following options:
  - **New Topology:** Choose to draw a new topology and delete existing links.
  - **Update Topology:** Choose to add new links to an existing topology.
- b. (Optional) Perform an advanced topology analysis, which will analyze the connection on the ICMP device. Then, select the **Advanced Topology Analysis** check box.

#### c. Click Next.

MXview draws the network topology.

7	Draw Topology (for devices supporting LLDP)				
	O New Topology				
	Existing links are going to be deleted				
	Update Topology				
	Existing links will be kept while new links are added				
	<ul> <li>Advanced Topology Analysis</li> <li>Strict Link Verification Mode</li> </ul>				
	*Additional time is required.				
	Next				

- 8. (Optional) Configure the SNMP trap server to capture real-time events.
  - a. Specify the following:
    - **Destination IP:** Provide the IP address of the SNMP trap server.
    - **Community Name:** Provide the community name of the SNMP trap server.
  - b. Click Next.

Destination IP1	
Community Name1	

 Click Browse Topology to view the detailed network topology. The Topology screen appears.

9	Complete		
	Browse Topology		

### Adding a New License

To increase the node limit of your MXview server, you need upgrade the license. To upgrade your license, obtain a valid activation code from your Moxa sales representative to add a new license.

- 1. Navigate to Menu ( $\equiv$ ) > License Manager.
- The License Manager screen appears.
- 2. In the Add New License section, click Add New License.

License Manager		0
License Mode: None State: No valid license Current Nodes: 0 Licensed Nodes: 0 Moxa License Site Add New License	Wireless Add-on Mode: None	
Free Trial Start to experience the power of MXview	Network Adapter MXview binds the license to one network adapter, please choose the adapter you want to bind. Re-select a network adapter will deactivate all your licenses automatically, you have to register them again.	Re-activate License Use both the Deactivation code and a User Code to re-activate your license.
Start Free Trial	Select Network Adapter	Re-activate

- Select the network adapter to generate the user code which will be used for license registration later. The Activation screen appears.
- 4. Input a valid activation code.

Activation		
User Code: 55DFBD8DA2C0D1E6241E Activation Code		
	Cancel	Apply

#### NOTE

Please reference Chapter 4: License Management to get more details on how to get the activation code.

5. Click Apply.

MXview activates the new license.

### **Deactivating a License**

By using this process to Transfer the MXview license from the legacy device to the new device allows users to deactivate the license to the new device.

- Navigate to Menu (<sup>□</sup>) > License Manager. The License Manager screen appears.
- Expand the Licenses section.

A list of activated licenses and activation codes appears.

3. Click **Deactivate**.

IXview	Manager		
	License Mode: Authorized Current Nodes: 0	Wireless Add-on Mode: None	
oxa License :	Licensed Nodes: 1		
Add New Lic	License Type		
	Code: IMcTgzeqSqgH2sebQBV j78ht5QvrHZ2EeTFtj4tP8oSiTQ	uClfMnpUqGMbmGe121jBkd+3uF3rjlwmWrNhJS4PIOKnFMXnGkdOOrsXva2EvIDL6KZ41c4Qdl3oMqZvvl7Pk75TVGWA7eNrYj7JQ5JYDknsnn2Y3tr50f4SP ur3V16nd4C7OGe11k	
	lode: 1		

MXview deactivates the license.

#### NOTE

Please reference Chapter 4: License Management to get more details on how to get the activation code.

### **Account Management**

The Account Management screen allows you to view, add, modify, and delete user accounts from MXview. You can also export a list of user accounts and related information as a CSV file.

MXview provides three default accounts:

- admin
- user
- guest

Each account can be assigned one of the following **Authority** permissions:

- Administrator: Has full access rights to modify any settings/configurations and can assign authorities to other accounts
- **Supervisor:** Has full access rights to modify any settings/configurations but cannot assign authorities to other accounts
- User: Has read-only permission

Account Ma	anagemer	t				
All User (3)	<b>+</b> •				Q Search	
Administrator (1)					Search	
(1) Supervisor (0)		User Name	Authority	Accessible Sites		
User (2)	- / 1	admin	Administrator	Site		
	- / 1	guest	User	Site		
	- / i	user	User	Site		
						1 – 3 of 3

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

### **Adding User Accounts**

- Navigate to Menu ( =) > Account Management. The Account Management screen appears.
- Click the Add (1) icon in the top right corner of the screen.
   The Add user account screen appears.

Add User Acco	unt		
User Name *			
	0/32		
Password *	Ø		
5-	0/16		
Authority *	•		
Accessible Sites *	•		
		Cancel	Ad

- 3. Configure the following account details:
  - > User Name: Specify the user name for the account
  - > Password: Specify the login password (minimum length: 4 characters) for the account
  - > Authority: Assign the authority permission (Administrator, Supervisor, or User) for the account
  - > Accessible Sites: Select which site(s) the account can access
- 4. Click Add.

### **Modifying User Accounts**

- Navigate to Menu (≡) > Account Management. The Account Management screen appears.
- Click the Edit (
   icon in front of the account you want to modify. The Modify user account screen appears.

Modify User A	ccount
User Name *	
guest	
	5/32
Old Password *	Ø
	0/16
Password *	Ø
Authority *	0 / 16
User	•
Accessible Sites *	
Site	-

- 3. Modify the following account details:
  - > User Name: Specify the user name for the account
  - > Password: Specify the login password (minimum length: 4 characters) for the account
  - > Authority: Assign the authority permission (Administrator, Supervisor, or User) for the account
  - > Accessible Sites: Select which site(s) the account can access
- 4. Click Apply.

### **Deleting User Accounts**

- Navigate to Menu (=) > Account Management. The Account Management screen appears.
- 2. (Optional) Select the check box(es) in front of one or more account(s).
- Click the **Delete** (1) icon in front of the account you want to delete, or in the top right corner of the screen (if multiple accounts are selected).

MXview deletes the account(s).

### **Exporting User Accounts**

The Account Management screen allows you to export a CSV file containing all user accounts with corresponding authority permissions and accessible sites.

- Navigate to Menu (<sup>□</sup>) > Account Management. The Account Management screen appears.
- 2. Click the **Export** ( ) icon.



- 3. Select **Export CSV**.
- 4. Specify the location to save the configuration file.
- Click Save.
   MXview exports the CSV file to the specified location.

### **Configuring Account Passwords**

Use the **Preferences** screen to modify the password requirements for user accounts.

- Navigate to Menu (=) > Preferences.
   The Preferences screen appears.
- 2. In the User section, expand Password Policy.

Password Policy	~
Minimum length (4 - 16) 4	
Password complexity strength check	
At least one digit (0~9)	
Mixed upper and lower case letters (A~Z, a~z)	
☐ At least one special character (~!@#\$%^&*l;;,.<>]]{}())	

- 3. Specify the minimum password length (between 4 to 16 characters).
- 4. Select one or more of the following password complexity requirements:
  - At least one digit (0~9)
  - > Mixed upper and lower case letters (A~Z, a~z)
  - > At least one special character (~!@#\$%^&\*-\_|;:,.<>[]{}())
- 5. Click Save.

MXview requires all new account passwords to satisfy the modified password policy.

Save

### **Configuring Login Notifications**

Use the Preferences screen to customize the notifications displayed when users log in to MXview.

- Navigate to Menu (=) > Preferences.
   The Preferences screen appears.
- 2. In the **User** section, expand **Login Notification**.

Login Notification		
<ul> <li>Show Login Failure Records</li> <li>Show Default Password Notification</li> </ul>		
Login Message		
	0/250	
Login Authentication Failure Message		
	0 / 250	

Save

- 3. To enable the following notification(s), select the corresponding checkbox(es):
  - > Show Login Failure Records
  - > Show Default Password Notification
- 4. To disable the following notification(s), clear the corresponding checkbox(es):
  - > Show Login Failure Records
  - > Show Default Password Notification
- 5. To display a custom login message, type a string (up to 250 characters in length) in the **Login Message** field.
- To display a custom login authentication failure message, type a string (up to 250 characters in length) in the Login Authentication Failure Message field.
- 7. Click Save.

MXview displays the configured login notifications the next time a user logs in.

### **Changing the Display Language**

Use the **Preferences** screen to customize the notifications displayed when users log in to MXview.

- Navigate to Menu (=) > Preferences.
  - The **Preferences** screen appears.
- 2. In the **Display** section, expand **Language**.

_anguage			
Default language		$\sim$	
English	*	~	

3. From the **Default Language** drop-down list, select the new display language.

- 4. MXview supports the following languages:
  - > German (Deutsch)
  - ➤ Japanese (日本語)
  - > English
  - > French (Français)
  - > Simplified Chinese (简体中文)
  - > Traditional Chinese (繁體中文)
- 5. Click Save.

MXview updates the display language.

### **License Management Overview**

The **License Manager** screen displays information about your MXview license, including the number of licensed nodes currently in use. You can also use the **License Manager** screen to add a new license or deactivate an existing license.

To access the **License Manager** screen, navigate to **Menu** ( $\equiv$ ) > **License**.

$\equiv$ <b>MX</b> view	*		Hi , admin 🚦
License Ma	anager		
MXview		Wireless Add-on Mode: None	Ø
Licenses			~
Deactivated licen	ses		~
Wireless Free Start to experienc in MXview	Trial e the Wireless Add-on	Network Adapter MXview binds the license to one network adapter, please choose the adapter you want to bind. Re-select a network adapter will deactivate all your licenses automatically, you have to register them again.	Re-activate License Use both the Deactivation code and a User Code to re-activate your license.
Start	Free Trial	Select Network Adapter	Re-activate

The **License Manager** screen displays the license type, the number of nodes in use, and the total number of nodes available under the current license.

### **Adding a New License**

- Navigate to Menu (=) > License Manager. The License Manager screen appears.
- 2. In the Add New License section, click Add New License.

$\equiv$ <b>MX</b> view	x		Hi , admin 🚦
License Ma	anager		
MXview			0
	License	Wireless Add-on	
	Mode: Authorized	Mode: None	
	Current Nodes: 0		
L CO	Licensed Nodes: 350		
Moxa License Site			
Add New Licens	se License Type		

The Add New License screen appears.

- 3. Click Next.
- 4. Select the network adapter to generate the user code which will be used for license registration later and click **Next**.

#### NOTE

If you have previously selected a network adapter, this step will not appear.

d New License			
Ø –	2	3	4
Login Moxa License Site	Select Network Adapter	Copy User Code	Activate
Please select a Netv	vork Adapter', MXview	uses it to generate your u	iser code.
Please select a Netv	work Adapter', MXview	uses it to generate your u	iser code.

5. Copy the generated user code and click **Next**.

d New License				
Ø –	- 0 -	3		4
Login Moxa License Site	Select Network Adapter	Copy User Code		Activate
Copy the User Code	to Moxa License Site			
			Close	Next

Open a web browser and go to <u>https://license.moxa.com</u>. Select **MXview** and log in using your Moxa account.

 Click Products and License > Activate a Product License. Then, select MXview from the product type list.

	Products and Licenses / Activate a Product License	
Product Type	Please select a product	~
	Please select a product SDC IEF IEC MRC QuickLink MXview	

8. Select a Sub-product type.

	Products and Licenses / Activate a Product License	
Product Type	MXview	~
Sub Product Type	Select your Sub-Product Type Select your Sub-Product Type Paid License (e.g. MXview-50, LIC-MXview-NEW-XN-SR) Free License Promotion License (e.g. Wireless 1-year special program) Conversion License (e.g. 2.x to 3.x)	✓
Network Management So		

#### Free License

If you want to activate a Free License, please perform the following steps:

- a. Select **Free License** as your sub product type.
- b. Paste a valid **User Code** from MXview.
- c. Then click **Activate** to get the activation code.

Product Type	MXview	~
Sub Product Type	Free License	~
User code	Enter your user code	

<b>MX</b> view
Network Management Software

#### Paid License

If you want to activate a Paid License, please perform the following steps:

- a. Select **Paid License** as your sub product type.
- b. Input a valid Registration Code.
- c. Paste a valid **User Code** from MXview.
- d. Then click **Activate** to get the activation code.

Product Type	MXview	~	
Sub Product Type	Paid License (e.g. MXview-50, LIC-I	~	
Registration Code	Enter your registration code		Product Type :
User code	Enter your user code		
		20 - 20 - 20 - 20 - 20 - 20 - 20 - 20 -	
		Activa	ite



#### **Conversion License**

This will convert the legacy v2.x license into a v3.x license of the same type. A full v2.x license will upgrade to a v3.x full license while a v2.x upgrade license will convert to a v3.x upgrade license. Legacy trial licenses cannot be converted.

~	

#### NOTE

NOTE

If you want to execute the Conversion License process, you don't have to deactivate the license from MXview v2.x.

Select **Conversion License** as your sub product type.

- a. Input a valid **Current License**.
- b. Paste a valid **User code** from MXview 3.x version.
- c. Then click **Activate** to get the activation code.

MXview		
		Activate
User code	Enter your user code	
Current license	Enter your current license	
Sub Product Type	Conversion License (e.g. 2.x to 3.x)	~
Product Type	MXview	~

Network Management Software

#### Promotion License

If you want to activate a Promotion License, please perform the following steps:

- a. Select **Promotion License** as your sub product type.
- b. Paste a valid **User Code** from MXview v3.2.x or later version.
- c. Then click **Activate** to get the activation code.

Product Type	MXview	~
Sub Product Type	Promotion License (e.g. Wireless 1-y	~
User code	Enter your user code	
		Activate
MX	view	

Network Management Software

9. Check your email account you used to apply for your moxa account. The activation code will be sent to this email address.



11. In MXview, paste the activation code into the Activation Code field.

	- 0	- 0 -	- 4
ogin Moxa License Site	Select Network Adapter	Copy User Code	Activate
ownload the licens	e from Moxa License S	Site, and paste the Activa	tion Code here

12. Click **Apply** and then MXview will activate the new license.

## Adding an Upgrade and Add-on License

- Navigate to Menu (=) > License Manager. The License Manager screen will appear.
- 2. Click Add New License. The Add New License screen will appear.

$\equiv$ MX view	*		Hi , admin 🚦
License Ma	anager		
MXview	License Mode: Authorized Current Nodes: 0 Licensed Nodes: 350	Wireless Add-on Mode: None	0
Moxa License Site			

- 3. Click Next.
- 4. Select the network adapter to generate the user code that will be used for license registration later. Then, click **Next**.

#### NOTE

If you have previously selected a network adapter, you do not need to perform this step.

Ø –	2	3	4
Login Moxa License Site	Select Network Adapter	Copy User Code	Activat
Please select a Net			

- 5. Copy the generated user code and click **Next**.
- Open a web browser and go to <u>https://license.moxa.com</u>. Select **MXview** and use your Moxa account to log in.
- 7. Click Products and Licenses > Activate an Add-on or Renewal License. Enter your Upgrade Registration Code.

Add-on or Renewal Registration	Enter your Registration Code	Product type :
Code		

8. Paste a valid **User code** from MXview. Then, click **Activate** to get the activation code.

Add-on or Renewal Registration Code		Product type : MXview
User code	Enter your user code	
License Type	ADD	
	Activate	

9. Once the process has been successfully completed, a pop-up window will appear to inform you that your license code has been deactivated. Click **I know** to close the window. If the license failed to activate, enter the license key again. If you are still experiencing problems, please contact Moxa Support.

Thank you for purchasing	an MXview product license!
Your license has been acti	ivated, we will send you an activation notification
to your mailbox.	
	Lknow

- 10. The software or service registration code is now activated, and you can use your new activation code to transfer the software or service.
- 11. Check the email account you used to apply for your moxa account. The activation code will be sent to this email address.

ΜΟΧΛ
Dear Customer, your New MXView Activation Code
has been artistated survessfully. You can now start usion MYGaw on this evolution. Weit that increas Artistion Portal In sea more datate about your modulate about your modulate and license artistion rode.
has been activated successfully. You can now start using MXview on this system. Visit the <u>License Activation Portal</u> to see more details about your product and license activation code.

- 12. Copy the activation code from the email.
- 13. In MXview, paste the activation code into the Activation Code field.

	- 0 -	- 0 -	4
ogin Moxa License Site	Select Network Adapter	Copy User Code	Activate
Download the licens	se from Moxa License S	Site, and paste the Activat	tion Code here.

14. Click **Apply** and MXview will activate the license.

# **Deactivating a License**

If you want to transfer a license to a different instance of MXview, the license has to be deactivated first.

- 2. Expand the **Licenses** section.

A list of activated licenses and activation codes appears.

3. Click **Deactivate** and MXview will deactivate the license.

$\equiv$ <b>MX</b> view	χ Sie see also and γ	Hi , admin 🚦
License Ma	nager	
MXview 3.1	LUrense Free Konses Durens Nodes / Ucrane Nodes / / 20 Mid New Liberne Tayle	
Licensed Node: 1	why full deployed and the order of the order	Deactivate

#### **Reactivating a Deactivated License**

A deactivated license can be reactivated on the current instance of MXview.

1. Navigate to **Menu** (≡) > License Manager.

The License Manager screen appears.

2. Expand the **Deactivated Licenses** section.

A list of deactivated licenses and deactivation codes will appear.

cense Ma	anager			
MXview				0
	License	Wireless Add-on		
	Mode: Authorized	Mode: None		
	Current Nodes: 0			
L L L L	Licensed Nodes: 300			
Moxa License Site				
Add New Licens	License Type			
icenses				
	ses			
Licenses Deactivated licen Deactivation Co			8	
Deactivated licen Deactivation Co License Start: 2	de: 021-04-19 22:42:12		8	
Deactivated licen	de: 021-04-19 22:42:12		8	
Deactivated licen Deactivation Co License Start: 2	de: 021-04-19 22:42:12 50		8	
Deactivated licen Deactivation Co License Start: 2 Licensed Node:	de: 021-04-19 22:42:12 50	8	8	
Deactivated licen Deactivation Co License Start: 2 Licensed Node: Deactivation Co	de: 021-04-19 22:42:12 50 de: 021-04-26 10:13:09	8	8	Re-activate Re-activate

3. Click **Re-activate** and then click **Next**.

4. Copy the deactivation code and click **Next**.

activate License	Wizard		
<b>o</b> -	2	3	4
Link to License Server	Copy Deactivate Code	Copy User Code	Generate License
Copy your Deactive	ite Code and paste on Li	icense Server	
Deactivaten Code	udaulio fariha yalioada co-ovie ostalia de contra glaca dualita de contra de cantalita de contra de	entre Colonia de Balan Integração de Colonia Al Deservição de Colonia Al Deservição de Colonia de Colonia Referi	nd Haan Likke scholl CashajiCe NCX1680-66-43
		Сору	Next

- 5. Open a web browser and go to <a href="https://license.moxa.com">https://license.moxa.com</a>. Select **MXview** and log in using your Moxa account.
- 6. Select **Products and Licenses** and click **Transfer a Product License**.
- 7. Paste the **Deactivation Code** followed by the **New User Code** from MXview. Then, click **Product Transfer**.

Product Type	MXview ~
Deactivation Code	Enter your deactivation code
New User Code	Enter your New User Code
	Dead

8. Once the process has been successfully completed, a pop-up window will appear to inform you that your license code has been deactivated. Click **I know** to close the window. If the license failed to deactivate, enter the license key again. If you are still experiencing problems, please contact Moxa Support.

Message notification		
Deactivation Success		
	I know	

- 9. The software or service registration code is now deactivated, and you can use your new activation code to reactivate the software or service.
- 10. Check the email account you used to apply for your moxa account. The activation code will be sent to this email address.

ΜΟΧΛ	
Dear Customer, your New MXview Activation Code has been activated successfully. You can now start using MXview on this system. Visit the <u>License Activation Portal</u> to see more details about your product and license activation code.	

11. Copy the activation code from the email.

12. In MXview, paste the activation code into the Activation Code field.

e-activate License			
<b>Ø</b>	- 0 -		4
Login Moxa License Site	Copy Deactivate Code	Copy User Code	Activate
Download the licens	e from <u>Moxa License S</u>	<u>Bite</u> , and paste the Activ	vation Code here.
Activation Code			

13. Click **Apply** and MXview will activate the license.

### Transferring a License to a Different Installation of MXview

A deactivated license can be transferred to a new installation of MXview.

- Navigate to Menu (<sup>□</sup>) > License Manager. The License Manager page will appear.
- Expand the Deactivated Licenses section. A list of deactivated licenses and deactivation codes will appear.

icense Manager		
MXview	Wireless Add-on	0
License		
Mode: Authorized	Mode: None	
Current Nodes: 0		
Licensed Nodes: 300		
Moxa License Site		
Add New License License Type		
Licenses		~
Deactivated licenses		^
Deactivation Code:		
table of the second sec		
License Start: 2021-04-19 22:42:12	5	
Licensed Node: 50		Re-activate
Deactivation Code:	Control (Review, National Concerning Manager Street, Manager Street, Street, Street, Street, Street, Street, St	
spectra a plan series i tals real		
License Start: 2021-04-26 10:13:09		Do particular
Licensed Node: 50		Re-activate

Open a web browser and go to <u>https://license.moxa.com</u>. Select **MXview** and log in using your Moxa account.

- 4. Select Products and Licenses and click Transfer a Product License.
- 5. Paste the **Deactivation Code** and the **New User Code** from a new installation of MXview. Then, click **Product Transfer**.

Product Type	MXview	$\sim$
Deactivation Code	Enter your deactivation code	
New User Code	Enter your New User Code	
		Product Transfer

#### \*

#### NOTE

To obtain a new User Code, please visit "**Adding a New License**", and follow steps 2 to 5 to obtain and copy the new user code.

6. Once the process has been successfully completed, a pop-up window will appear to inform you that your license code has been deactivated. Click **I know** to close the window. If the license failed to deactivate, enter the license key again. If you are still experiencing problems, please contact Moxa Support.

Message notification	
Deactivation Success	
	I know

- 7. The software or service registration code is now deactivated, and you can use your new activation code to transfer the software or service.
- 8. Check the email account you used to apply for your moxa account. The activation code will be sent to this email address.

ΜΟΧΛ
Dear Customer, your New MXview Activation Code
w8p52m824p85.w8p26m_e2rof.ex.p1m87w847w2x45ep88w8488CX2x44z4p8re322223788840342x42x42x42x42x42x42x42x42x42x42x42x42x4
has been activated successfully. You can now start using MXview on this system. Visit the License Activation Portal to see more details about your product and license activation code.

- 9. Copy the activation code from the email.
- 10. In MXview, paste the activation code into the Activation Code field.

<ul> <li>Image: A start of the start of</li></ul>	- 🖉 -	- 0 -	- 4
ogin Moxa License Site	Select Network Adapter	Copy User Code	Activate
	se from Moya License S	Site, and paste the Activat	tion Code here
		site, and paste the Actival	tion Code her

11. Click **Apply** and MXview will activate the license.

The MXview **Dashboard** contains several widgets that provide summary information about your network devices, event highlights, and server disk space utilization.

### **Dashboard Overview**

Use the **Dashboard** to gain a quick overview of your network devices, important system events, and server disk space utilization.

The **Dashboard** displays the following widgets:

- Device Summary
- Device Availability
- Event Highlights: Cold/Warm Start Trap
- Event Highlights: ICMP Unreachable
- Event Highlights: Link Down
- Disk Space Utilization

To access the Dashboard, navigate to **Menu** ( $\equiv$ ) > **Dashboard**.

To refresh the data displayed in all the widgets, click the **Settings** (:) icon in the top right corner of the screen and select **Refresh All**.

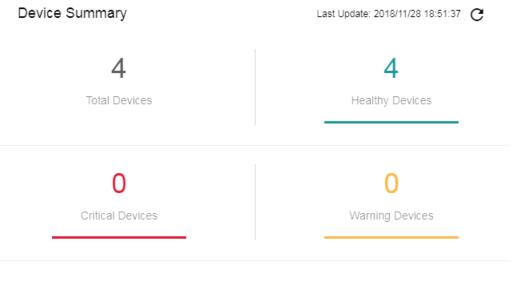
#### **Device Summary**

The Device Summary widget displays the following information about the devices on your network:

- **Total Devices:** The total number of devices detected on your network. Click to view additional details about the devices on the **Network Topology** screen.
- **Healthy Devices:** The number of devices with no critical events or warnings. Click to view additional details about the devices on the **Network Topology** screen.
- Critical Devices: The number of devices with critical events.
   Click to view additional details about the devices on the Network Topology screen.
- **Warning Devices:** The number of devices with warnings. Click to view additional details about the devices on the **Network Topology** screen.

You can perform the following actions on this widget:

- To view a visualization of the devices in your network topology, click **View Network Topology**. For more information, see **Topology Management**.
- To refresh the widget data, click the  ${\it Refresh}\ ({}^{\it C}{\it O}$  ) button following the  ${\it Last}\ {\it Update}\ {\it timestamp}.$



View Network Topology

### **Device Availability**

The **Device Availability** widget displays the availability of each device in your network topology. MXview calculates device availability by using the following formula:

Availability = (Uptime / (Uptime + Downtime)) x 100

To refresh the widget data, click the **Refresh** ( $^{\mathbb{C}}$ ) button following the **Last Update** timestamp.

Device Availability 🕐

Last Update: 2018/11/28 19:03:53 C

<b>192.168.127.1IKS-6726A</b> 192.168.127.1 Site THEO-LAI01	100.00%
<b>192.168.127.2IKS-6728A-8POE</b> 192.168.127.2 Site THEO-LAI01	100.00%
<b>192.168.127.3EDS-G516E</b> 192.168.127.3 Site THEO-LAI01	100.00%
<b>192.168.127.4EDS-G516E</b> 192.168.127.4 Site THEO-LAI01	100.00%

# **Event Highlights: Cold/Warm Start Trap**

The **Event Highlights: Cold/Warm Start Trap** widget displays the number of cold start traps and warm start traps issued by devices at a site, and the day on which the events occurred.

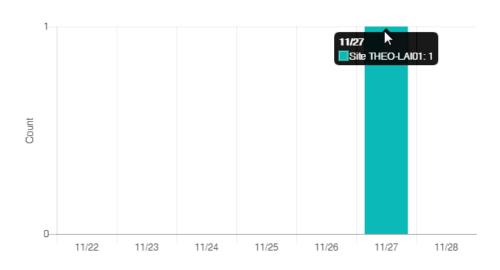
You can perform the following actions on this widget:

- To view the number of cold/warm start traps issued at a site on a specific date, hover over a bar in the widget chart.
- To view additional details about the event on the All Event screen, click a bar on the widget chart.
- To change the type of event that the widget displays information for, select a different event type from the drop-down list in the top left corner of the widget.
- To refresh the widget data, click the **Refresh** ( $^{\mathbb{C}}$ ) button following the **Last Update** timestamp.

Event Highlights

Last Update: 2018/11/28 19:17:53 C

Cold/Warm Start trap 📼



# **Event Highlights: ICMP Unreachable**

The **Event Highlights: ICMP Unreachable** widget displays the number times an ICMP-enabled device on your network was unreachable, and the day on which the events occurred.

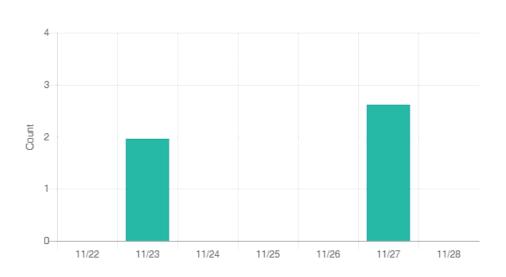
You can perform the following actions on this widget:

- To view the number of "ICMP unreachable" events issued at a site on a specific date, hover over a bar in the widget chart.
- To view additional details about the event on the All Event screen, click a bar on the widget chart.
- To change the type of event that the widget displays information for, select a different event type from the drop-down list in the top left corner of the widget.
- To refresh the widget data, click the **Refresh** ( $^{\mathbb{C}}$ ) button following the **Last Update** timestamp.

Event Highlights

Last Update: 2018/11/28 19:31:37 C

ICMP unreachable



# **Event Highlights: Link Down**

The **Event Highlights: Link Down** widget displays the number of times a port link was down on a device on a specific date.

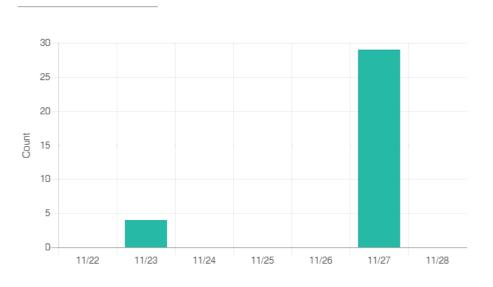
You can perform the following actions on this widget:

- To view the number of "link down" events issued at a site on a specific date, hover over a bar in the widget chart.
- To view additional details about the event on the All Event screen, click a bar on the widget chart.
- To change the type of event that the widget displays information for, select a different event type from the drop-down list in the top left corner of the widget.
- To refresh the widget data, click the **Refresh** ( $^{\circ}$ ) button following the **Last Update** timestamp.

Event Highlights

Link down

Last Update: 2018/11/28 19:28:38 C



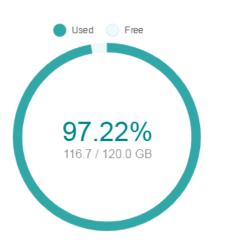
### **Disk Space Utilization**

The **Disk Space Utilization** widget displays information about how much storage capacity is still available on the MXview server computer.

To refresh the widget data, click the **Refresh** ( $^{\mathbb{C}}$ ) button following the Last Update timestamp.

Disk Space Utilization

Last Update: 2018/11/28 20:01:10 C



# 6. Device Discovery and Polling

### **Device Discovery Overview**

MXview uses SNMP and ICMP to discover devices within the scan ranges. When a Moxa device has been located, MXview will generate an actual image of the device, demonstrated below, 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
- Power Status
- Status and Version of the SNMP Protocol

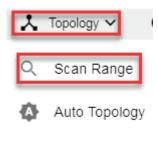
MXview will display one of the following graphics to indicate devices:

Device	Image
Moxa devices with SNMP enabled.	NMP
Non-Moxa devices with SNMP enabled.	SNMP
Non-Moxa devices with ICMP enabled.	ICMP

# **Configuring IP Address Scan Ranges**

MXview allows you to scan multiple ranges of IP addresses within your network. Each network range is defined by a starting IP address and an ending IP address. Use the **Scan Range Wizard** to configure network scan ranges.

- 1. Access the Scan Range Wizard screen by the following method:
  - a. Navigate to Menu (=) > Network > Scan Range.
  - b. Navigate to **Menu** (=) > **Network** > **Topology**, and then navigate to **Topology** > **Scan Range** from the Topology Map toolbar menu.



Auto Layout

The Scan Range Wizard screen will appear.

can Range Wizard					
1 Network Range	2 Re	ecover Ignore Devices	<b>3</b> D	scovery Result	(d) Comple
Enabled/Disabled	Name	First IP Address	Last IP Address	Group	+ Site Name
<ul> <li>Enabled</li> </ul>	2	1.2.3.4	1.2.3.4	Root	Site THEO-LAI01
🖍 🔋 Enabled	demo	192.168.127.1	192.168.127.220	Root	Site THEO-LAI01

- 2. To add a new scan range:
  - a. Click the Add (<sup>1</sup>) button in the top right corner.
     The Add Scan Range screen will appear.

Enable Scan Range Enabled	*	
Name test		
First IP Address		CIDR Prefix
192.168.127.1		/24 (255.255.255.0) 🔻
Last IP Address		CIDR Address Range
192.168.127.254		192.168.127.1 - 192.168.127.254
Group		
Root	*	

- b. Select the scan range status:
  - Enabled
  - Disabled
- c. Provide a Name for the scan range.

- d. Provide the starting IP address for the scan range.
- e. Provide the ending IP address for the scan range.
- f. Select the CIDR Prefix (if any).
- g. Assign the scan range to a **Group**.
- h. Click Apply.

The new scan range appears in the Network Range table.

- 3. To edit a scan range:
  - a. Select the check box next to the scan range in the **Network Range** table.
  - b. Click the Edit ( ) icon.
     The Add Scan Range screen appears.
  - c. Modify the scan range settings.
  - d. Click Apply.

The **Scan Range Wizard** screen displays the **Network Range** table with the updated scan range information.

- 4. Recover previously deleted devices and discover new devices in the scan range:
  - a. Click Next.

The Scan Range Wizard screen displays the Recover Ignore Devices tab.

Sc	an F	Rang	e Wizard				
0	Netwo	rk Range			2 Recover Ignore Devices	- 3 Discovery Result	(1) Complete
	F	Recovery	Device IP	Site Name			
		Î	1.2.3.4	Site THEO-LAI01			
	~	Î	192.168.127.100	Site THEO-LAI01			
		Î	192.168.127.195	Site THEO-LAI01			
	3 total						
	Next						

- b. Select the device(s) you want to recover.
- c. Click Next.
  - The Scan Range Wizard screen displays the Discovery Result tab.
- d. Wait for device discovery to finish.

The **Discovery Result** tab displays newly discovered devices (if any) from the scan range.

Scan Range V	lizard				
Network Range		🖉 Recover l	nore Devices	3 Discovery Result	Complete
Device Alias	Device IP	Group	Site Name		
Device discovery is finis	hed	r			

5. To complete scan range configuration, click **Next**.

The  $\mbox{Scan}\xspace$  Range  $\mbox{Wizard}\xspace$  screen displays the  $\mbox{Complete}\xspace$  tab and the number of devices added to MXview.

Scan Range Wizard			
Network Range	Recover Ignore Devices	Discovery Result	Complete
There are 0 added to MXviev	V		
Browse Topology			

6. To view the updated topology, click **Browse Topology**.

The **Network Topology** screen will appear and display the updated Topology Map.

# **Configuring Background Discovery**

Background Discovery automatically scans configured IP address scan ranges every 30 minutes to detect if any new devices have been added.



#### NOTE

Background Discovery requires configuring IP address scan ranges. For more information, see **Configuring IP Address Scan Ranges**.

- 1. Navigate to Menu (≡) > Preferences.
- The **Preferences** screen will appear.
- 2. In the Advanced section, expand System Configuration.

The System Configuration settings will appear.

anced	
System Configuration	
Background Discovery	
Disabled	
	n
'hreshold of Disk Space (MB)	
)	
Alarm is disabled if set to	

- 3. To enable Background Discovery:
  - a. Select Enabled from the Background Discovery drop-down list.
  - b. Click Save.

MXview scans the configured IP address scan ranges every 30 minutes for new devices.

- 4. To disable Background Discovery:
  - a. Select **Disabled** from the Background Discovery drop-down list.
  - b. Click Save.

MXview stops scanning the configured IP address scan ranges every 30 minutes for new devices.

# **Configuring Device Polling Settings**

Devices in the assigned scan range can be discovered via SNMP and ICMP protocols. (The default polling interval of ICMP is 10 seconds, while SNMP is 60 seconds. Users can go to the preferences page to change the polling intervals.) 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:

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

#### **NOTE**

MXview **Dashboard** widgets also use the device polling settings. For more information about the MXview **Dashboard** widgets, see Chapter 5: **Dashboard Overview**.

- Navigate to Menu (=) > Preferences.
   The Preferences screen appears.
- 2. In the **Advanced** section, expand **Device**.

The **Device** settings appear.

ممعدما

vanced			
System Configuration			
Device			
ICMP polling interval		Consecutive failure to trigger ICMP unreachable event	
10		1	
	Sec	times	
SNMP polling interval		Consecutive failure to trigger SNMP unreachable event	
60		1	
	Sec	times	
Username		Password	
admin		••••	
Timeframe for availability calculati	on		
24			
		hr	

- 3. Configure the following ICMP polling settings:
  - > ICMP polling interval: Specify the time in seconds between polls
  - Consecutive failure to trigger ICMP unreachable event: Specify the number of failed attempts before triggering the event
- 4. Configure the following SNMP polling settings:
  - > SNMP polling interval: Specify the time in seconds between polls
  - Consecutive failure to trigger SNMP unreachable event: Specify the number of failed attempts before triggering the event
- 5. Configure the device web console login credentials:
  - > **Username:** The login username for the device web console
  - > Password: The login password for the device web console
- 6. Configure the timeframe (in hours) for calculating device availability.
- 7. Click Save.

MXview will update the device polling settings.

# **Changing Default SNMP Configurations**

The default SNMP read community string that is used to discover devices is public. Use the Preferences screen to change the default read community string or modify other default SNMP configurations.

1. Navigate to **Menu** (≡) > **Preferences**.

The **Preferences** screen will appear.

In the Advanced section, expand SNMP Configuration.
 The SNMP Configuration settings will appear.

System Configurati	on		
Device			
SNMP Configuratio	n		
SNMP Version *		Port *	
V3		161	
Read Community		Password Q	
Read Community			
public		private	
Data Encryption		Authentication	
AuthPriv	*	MD5	
Encryption Protocol			
AES	-	Encryption Password	6

- 3. Configure the following:
  - a. SNMP Version: Select the SNMP protocol version
  - b. User Name: Specify the SNMP server username
  - c. Password: Specify the SNMP server password
  - d. Read Community: Specify the new community string
  - e. Write Community: Specify the new community string
  - f. Data Encryption: Select the data encryption method (NoAuth, AuthNoPriv, AuthPriv)
  - g. Authentication: Select the authentication method (MD5, SHA)
  - h. Encryption Key: Specify the encryption key
  - i. Encryption Protocol: Select the encryption protocol (DES, AES)
  - j. SNMP Port: Specify the SNMP port
- 4. Click Save.

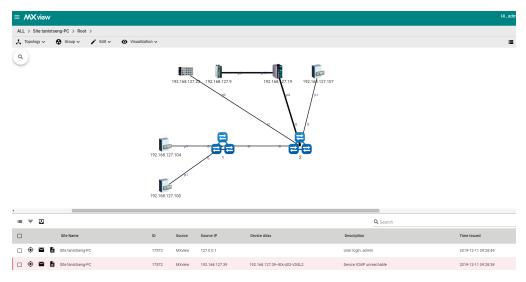
MXview updates the modified settings.

MXview allows you to view a graphical representation of your network topology, add/delete devices and links to the Topology Map, organize the topology structure, and export the Topology Map as a PNG image. You can also scan specific IP address ranges to discover devices on your network.

### **Network Topology Overview**

The Network Topology screen allows you to view the Topology Map, which is a graphical representation of the devices in your network, and perform most actions in MXview. For example, you can use the Network Topology screen to do the following:

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



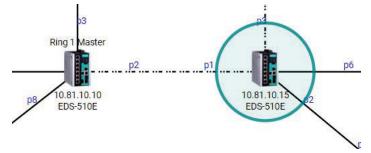
# **Viewing Topology Map**

Use the Network Topology screen to view the Topology Map and export a PNG image of the Topology Map.

- 1. Navigate to Menu (=) > Network > Topology.
- The **Network Topology** screen will appear and displays the Topology Map by default.
- If List view is selected, click the Topology view (<sup>\*</sup>) icon in the top right corner. The Network Topology screen will display a graphical representation of the devices and links on your network.
- 3. To search the Topology Map for a specific device:
  - a. Click the magnifying glass (<sup>Q</sup>) icon in the top left corner.
     The topology search box appears with a drop-down directory tree of the Topology Map structure.

Q
-
4
-

- b. Locate the device in the drop-down directory tree or type a string in the search box.
- 4. To view the details of a specific device, select the device in the Topology Map.



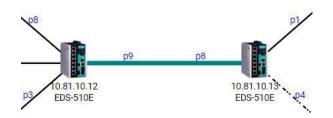
The **Device Properties** pane appears to the right of the Topology Map.

Device Properties	Current Status
Basic Device Prope	rties
Alias	
EDS-510E	
Model Name	
EDS-510E	
MAC Address	
00:90:E8:86:2F:16	
Availability	
100.00%	
System Description	
EDS-510E-3GTXSFP	
System Object ID	
.1.3.6.1.4.1.8691.7.8	34

To view events associated with the device, click the Current Status.
 The Current Status pane displays events associated with the device.

5	Current Status	Device Properties
		No events
		No events

6. To view details about a link between devices, select a link in your Topology Map.



The Link Properties pane appears to the right of the Topology Map.

Link Properties
Link Information
From
10.81.10.12
Port 9
То
10.81.10.13
Port 8
Link Speed
1 Gb
SFP Information
From

#### **Viewing Recent Events**

Use the **Network Topology** screen to view recent events from devices in your topology. You can filter the events in the list or export the data as a CSV file.

For more information on viewing all events, see Chapter 10: **Event Monitoring**.

ungut	e to <b>menu</b> (🖿	) > N	etwo	ork > To	opology.		
The <b>Net</b>	twork Topolo	<b>gy</b> sci	reen	will app	ear and display	s the <b>Recent Ev</b>	ents panel on the
= MXview							Hi, adn
ALL > Site tanists	eng-PC > Root >						
🙏 Topology 🗸	😧 Group 🗸 🖌 Edit 🗸 💿 Visa	ualization $\checkmark$			-		=
٩	192.168.127.52			192.1	66.127.247		
= - •						Q Search	
						<ul> <li>→ assiren</li> </ul>	
	Site Name	ID	Source	Source IP	Device Alias	Description	Time Issued
• • • • •		ID 17573	Source MXview	Source IP 127.0.0.1	Device Alias		Time Issued 2019-12-11 09:28:49
	Site tanistseng-PC				Device Allas 192.168.127.39-IEX-402-VDSL2	Description	
. • • •	Site tanistseng-PC Site tanistseng-PC	17573	MXview	127.0.0.1		Description User login: admin	2019-12-11 09:28:49
	Site tanistseng-PC Site tanistseng-PC Site tanistseng-PC	17573	MXview MXview	127.0.0.1 192.168.127.39	192.168.127.39-IEX-402-VDSL2	Description User login: admin Device ICMP unreachable	2019-12-11 09-28-49 2019-12-11 09-28-38
	Site tanisteeng-PC Site tanisteeng-PC Site tanisteeng-PC Site tanisteeng-PC	17573 17572 17571	MXview MXview MXview	127.0.0.1 192.168.127.39 192.168.127.253	192.168.127.39-4EX-402-VD5L2 192.168.127.259-MD6-64028	Description User login: admin Device ICMP unreschable Device SNMP unreschable	2019-12-11 09:28:49 2019-12-11 09:28:38 2019-12-11 09:28:35
	Site tanistiseng-PC Site tanistieng-PC Site tanisteng-PC Site tanisteng-PC Site tanisteng-PC	17573 17572 17571 17570	MXview MXview MXview MXview	127.0.0.1 192.168.127.39 192.168.127.253 192.168.127.247	192.168.127.39-IEX-402-VDSL2 192.168.127.253-MD5-G4028 192.168.127.247-ED5-0512E-8PoE	Device SNAP unreschable	2019-12-11 09:28:40 2019-12-11 09:28:38 2019-12-11 09:28:35 2019-12-11 09:28:34
	Site taristiseng PC Site taristiseng PC Site taristiseng PC Site taristiseng PC Site taristiseng PC Site taristiseng PC	17573 17572 17571 17570 17569	MXview MXview MXview MXview MXview	127.0.0.1 192.168.127.29 192.168.127.253 192.168.127.247 192.168.127.245	192.168.127.39-IEX.402.VD6L2 192.168.127.253-MD6-04028 192.168.127.2453-MD6-04028 192.168.127.245-ED9-0512E-8PoE 192.168.127.245-AWK-1131A	Description User logis admin Device ISMP usreschable Device SMMP usreschable Device SMMP usreschable	2019-12-11 09-28-49 2019-12-11 09-28-38 2019-12-11 09-28-38 2019-12-11 09-28-34 2019-12-11 09-28-34 2019-12-11 09-28-33
	Site taristiseng PC Site taristiseng PC Site taristiseng PC Site taristiseng PC Site taristiseng PC Site taristiseng PC Site taristiseng PC	17573 17572 17571 17570 17569 17568	MXview MXview MXview MXview MXview	127.0.0.1 192.168.127.283 192.168.127.283 192.168.127.247 192.168.127.245 192.168.127.249	192.168.127.39-IEX-402.405.12 192.168.127.29-4405-64028 192.168.127.247-605-6512E-874E 192.168.127.245-409X(1131A 192.168.127.249-409X(1131A		2019-12-11 09-28-49 2019-12-11 09-28-39 2019-12-11 09-28-39 2019-12-11 09-28-39 2019-12-11 09-28-39 2019-12-11 09-28-39 2019-12-11 09-28-39

2. To filter the information in the table, type a full or partial string that matches the value in any of the table columns.

MXview filters the table to only display events with values that fully or partially match the specified string.

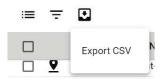
- 3. To filter the information in the table by specific criteria:
  - a. Click the Filter (=) icon below the Recent Events tab.
     The criteria selection screen appears.

:=	≂ 🖸			
				×
	Severity		Source	•
	Group	•	IP Address	
			Reset	Apply

- b. Specify any of the following criteria:
  - **Severity:** Select the event severity level
  - **Source:** Select the source that detected the event (MXview, Trap, or Security Sensing)
  - **Group:** Select the device group
  - □ IP Address: Select the device IP address
- c. Click Apply.

MXview filters the table to only display events that match the specified criteria.

- 4. To filter the information in the table by event acknowledgement (Ack) status:
  - a. Click the envelope ( $\bowtie$ ) icon below the **Recent Events** tab.
  - b. Select the event acknowledgement status from the list that appears.
     MXview filters the table to only display events that match the selected acknowledgement status.
- To sort the data in the table by a specific column, click the column heading.
   MXview sorts the table by the column.
- 6. To export data displayed in the **Recent Events** tab:
  - a. Click the **Export** ( ) icon.



- b. Select **Export CSV**.
- c. Specify the location to save the exported file.
- d. Click Save.

MXview exports the displayed event data as a CSV file.

## **Organizing the Topology Structure**

The Topology Map can be organized into a multi-layer tree structure of up to 5 layers. Organizing the topology structure into groups helps 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 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.

1. Navigate to **Menu** (≡) > **Network** > **Topology**.

The Network Topology screen appears and displays the Topology Map by default.

MXview represents the Topology Map structure by a path at the top of the Network Topology screen:



If the Topology Map contains groups under the Root layer, you can click the right arrow (>) and select the group:

ALL > Site THE	D-LAI01 > Root	$\sim$
📩 Topology 🗸	🔂 Group 🗸	Group1

> You can also click the following icon used to indicate user-defined groups within the Topology Map:



If List view is selected, click the Topology view (<sup>\*</sup>) icon in the top right corner.
 The Network Topology screen displays the following toolbar above the Topology Map:



- 3. To create a group:
  - a. Navigate to Group > Create Group.
     The Create Group screen appears.

Create Group			
Parent Group *			
Root	*		
Group Name *			
Test			
Group Description	4 / 64		
Test			
	4/100		
Image 🔒 🦻	4 / 128		
88			
		Cancel	Create

- b. Configure the following:
  - Parent Group
  - □ Group Name
  - □ Group Description
  - □ Group Icon
- c. Click **OK**.

MXview will add the group below to the specified parent group.

- 4. To reorganize the groups within the Topology Map structure:
  - a. Navigate to Group > Group Maintenance.

The Group Maintenance screen appears.

Group Maintenance

▼	Root SGroup1		
			ß
	+ Create	Telete	
			Close

b. Select a layer to modify.

The group details appear to the right of the topology directory tree.

#### Group Maintenance

Root	Group Name *
а	a
	1/6
	Group Description
	0 / 12
	Image 🗈 🖸

- c. Edit the group details or perform one of the following points:
- d. (Optional) Click  $\ensuremath{\textbf{Create}}$  to add a new group below the selected layer.
- e. (Optional) Click  $\ensuremath{\textbf{Delete}}$  to remove a group from the topology structure.
- f. Click Apply.

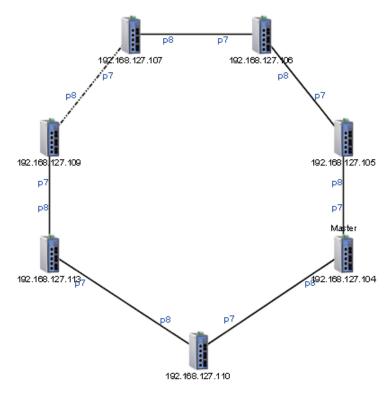
- 5. To reassign the device(s) in a group:
  - a. Navigate to Group > Change Group. The Change Group screen appears.

Current Root	Gioup	•	
	IP Address		
	192.168.127.1		-
	192.168.127.2		l
	192.168.127.3		l
	192.168.127.4		+
0 Se	elected / 4 total		
Assign t	o Group *		
Group	1	Ŧ	

- b. If the **IP Address** list does not display the IP address(es) of the device(s) you want to reassign, select the source group from the **Current Group** drop-down list.
- c. Select the IP address(es) of the device(s) that you want to reassign to a different group.
- d. From the **Assign to Group** drop-down list, select the new group for the selected device(s).
- e. Click Apply.

# **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 dashed lines.

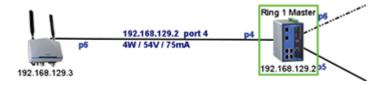
- RSTP has a Root
- Turbo Ring has a Master
- Turbo Chain has a Head and a Tail

#### ΝΟΤΕ

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

192. 168. 122.254 / SiteToSite1 192. 168. 122.254 / SiteToSite1	
192.168.122.188 132.168.122.254 / Stret-Ste2 392.468.122.254 / Stret-Ste2 392.554 / Ste2 392.554 /	68 127 246

• Yellow: At least one VPN tunnel is disconnected

VPN 192.168.122.254 / SiteTo Site1	192.168.122.254 / sitetosite	Firewall VPN
192.168.128.188 192.168.122.2547.3teToSite2	ps 192 496 122 254 / sitetosite2 1	92.168.127.245

• Red: All VPN tunnels are disconnected

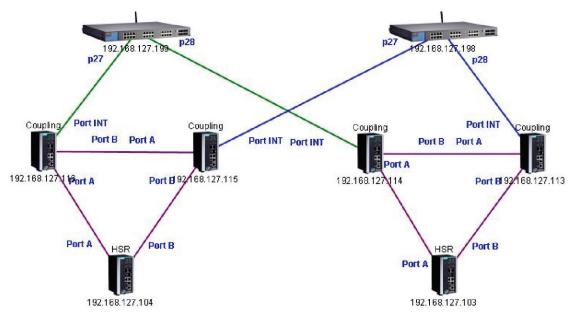


#### NOTE

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.





#### NOTE

PRP/HSR Visualization is only available with Moxa's PT-G503 Series, PT-7728-PTP Series, and PT-G7728 Series with the LM-7000H-2GPHR module.

#### **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

Only auto topology can draw thick lines for trunking links. Manually drawn trunking links will appear as 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)

### **Adding Devices and Links**

MXview allows you to manually add devices and links to an automatically generated Topology Map. The **Network Topology** screen allows you to add devices from Topology View or List View.

For information about List View, see Chapter 10: Device Management > Viewing the Device List.

1. Navigate to **Menu** ( $\equiv$ ) > **Network** > **Topology**.

The Network Topology screen appears and displays the Topology Map by default.

- 2. To add a device to the Topology Map:
  - a. Click Edit > Add Device.

The Add Device screen will appear.

P Address *				
Assign Model *		Assign To Group *		
SNMP Version *		Port *		
V1	•	161		
User Name		Password 🔌		
Read Community		Write Community		
public		private		
Data Encryption	Ŧ	Authentication		
Encryption Protocol	Ŧ	Encryption Password	ø	

- b. Configure the following:
  - □ IP Address: Specify the IP address of the device
  - □ Assign Model: Select the model of the device
  - **Assign To Group:** Select the group to assign the device to
  - SNMP Version: Select the SNMP version
  - □ User Name: Specify the device login user name
  - **Password:** Specify the password
  - **Read Community:** Specify the SNMP read community string
  - □ Write Community: Specify the SNMP write community string
  - **Data Encryption:** Select the data encryption method
  - **Authentication:** Select the authentication method
  - Encryption Key: Specify the encryption key
- c. Click Add.

MXview adds the device to the topology.

- 3. To add a link to the Topology Map:
  - a. Navigate to Edit > Add Link.

The Add Link screen will appear.

- b. Configure the following information for the two devices joined by the link:
  - Device: Specify the IP address of the device
  - **Port:** Specify the device port number
- c. Click Add.

MXview adds the link between the specified devices.

#### **NOTE**

Links drawn between two devices in the Topology Map are bidirectional. You may specify either device as the **From** device or the **To** device.



#### NOTE

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

#### •

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

#### NOTE

NOTE

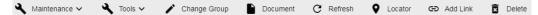
For modular switches, a port number depends on the chassis to which the port belongs, but not on how many modules are inserted. For switches such as the PT-7828, the first module's port numbers are from 1 to 8, the second module's port numbers are from 9 to 16, and so on. The port number depends only 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.

### **Deleting Devices and Links**

You can delete devices and links from the Topology Map. After a device is deleted, it will be removed from the topology map and scan range, and the device will not be polled or located when performing device discovery. Deleting a link will delete a link from the topology map, but it will not affect the actual network configuration.

- 1. Navigate to **Menu** (≡) > **Network** > **Topology**.
  - The **Network Topology** screen will appear and display the Topology Map by default.
- 2. To delete a device from the Topology Map:
  - a. Select the device.

The following toolbar menu will appear.



b. Click Delete.

A confirmation screen will appear.

c. Click OK.

MXview deletes the device from the Topology Map.

- 3. To delete a link from the Topology Map:
  - a. Select the link.

The following toolbar menu will appear.

👔 Link Traffic 🗸 🛪 Severity Threshold 🕒 Set Port Label 🕱	Label 🗙 Delete
--	----------------

b. Click Delete.

A confirmation screen will appear.

c. Click OK.

MXview deletes the link from the Topology Map.

### **Updating the Topology Map**

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.

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 from the **Auto Topology** screen.

1. Navigate to **Menu** (=) > **Network** > **Topology**.

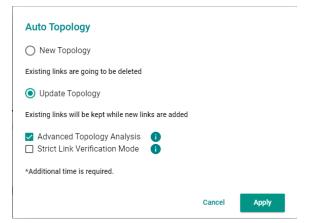
The Network Topology screen appears and displays the Topology Map by default.

2. If **List view** is selected, click the **Topology view**  $(\overset{\text{L}}{\rightarrow})$  icon in the top right corner.

The **Network Topology** screen displays a graphical representation of the devices and links on your network.

3. Navigate to **Topology > Auto Topology**.

The Auto Topology screen appears.



- 4. Select Update Topology.
- 5. (Optional) Select Advanced Topology Analysis to draw links for devices without an LLDP MIB.
- 6. Click **OK**.

MXview will update the Topology Map.

### **Refreshing the Topology Layout**

After changes have been made, use the Auto Layout feature to refresh the layout of the Topology Map. Auto Layout does not update any devices or links. It only redraws the topology to better fit the screen.

- Navigate to Menu (=) > Network > Topology. The Network Topology screen will appear and displays the Topology Map by default.
- If List view is selected, click the Topology view (<sup>A</sup>) icon in the top right corner.
   The Network Topology screen will display a graphical representation of the devices and links on your network.
- 3. Navigate to **Topology > Auto Layout**.

The Auto Layout screen appears.

Auto Layout	
Are you sure you want to do Auto Layou (Current layout will be overridden)	t?
Cancel	Apply

4. Click Apply.

MXview refreshes the Topology Map layout.

### **Creating a New Topology Map**

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

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 from the **Auto Topology** screen.

#### NOTE

Links drawn manually will also be deleted by this action.



#### NOTE

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



#### NOTE

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



#### NOTE

Strict Link Verification Mode" checks the LLDP table of both ends of the devices and draws a link if and only if the link data is included in both devices.

- Navigate to Menu (=) > Network > Topology. The Network Topology screen appears and displays the Topology Map by default.
- 2. If **List view** is selected, click the **Topology view** (<sup>1</sup>) icon in the top right corner.
  - The **Network Topology** screen displays a graphical representation of the devices and links on your network.

1

3. Navigate to **Topology > Auto Topology**.

The Auto Topology screen appears.

Auto Topology		
New Topology		
Existing links are going to be deleted		
O Update Topology		
Existing links will be kept while new links are added		
<ul> <li>Advanced Topology Analysis</li> <li>Strict Link Verification Mode</li> <li>Image: Strict Link Verification Mode</li> </ul>		
*Additional time is required.		
	Cancel	Apply

- 4. Select New Topology.
- 5. (Optional) Select Advanced Topology Analysis to draw links for devices without an LLDP MIB.
- 6. Click **OK**.

MXview will create a new Topology Map.

### Setting/Deleting the Background Image

MXview allows you to customize the Topology Map by uploading a background image in JPG, GIF, or PNG format.

Navigate to Menu (=) > Network > Topology.

The **Network Topology** screen appears and will display the Topology Map by default.

- If List view is selected, click the Topology view (<sup>\*</sup>) icon in the top right corner. The Network Topology screen will display a graphical representation of the devices and links on your network.
- 3. Navigate to **Edit > Background**.

The **Background** screen appears.

#### Background



- 4. Upload the background image by using one of the following methods:
  - > The image size must be less than 20 MB.
  - > Drag and drop an image file into designated area on the **Set Background** screen.
  - > Click browse on the **Set Background** screen to locate the file on your local machine.
  - MXview will set the uploaded image as the Topology Map background.
- 5. Use the sliders to modify the Alpha and Saturation value of a background image.
- 6. Modify the value of X and Y to move the origin of the image to a suitable location. Modify the 'Width' and 'Height' to change the size of the image.

#### Background



7. To delete a background image, click  $ar{f I}$  to remove the background image from the Topology Map.

## **Editing the Topology Appearance**

Use the **Preferences** screen to modify how the Topology Map displays the topology line style, PoE status, background color, link status, and traffic load.

1. Navigate to **Menu** (≡) > **Preferences**.

The **Preferences** screen appears.

In the Display section, expand Topology Appearance.
 The Topology Appearance settings appear.

anguage			
ppology Appearance			
rected Line Style	Directed Line Style	Elbow Line Style	
οE			
Show PoE Status on Topolog	ay.		
DE Link Color 📕 #FF0000	JY .		

3. To modify the Topology Line Style, select one of the following from the drop-down list:

Topology Appearance

	No Corp. Browner and Corp.	Nyrian I m ganarating an an
Topology Line Style Directed Line Style		
	Directed Line Style	Elbow Line Style

#### > Directed Line Style

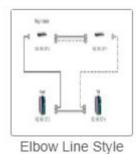
MXview applies the following style to the lines indicating the links between devices in the Topology Map:



Directed Line Style

#### > Elbow Line Style

 $\mathsf{MXview}$  applies the following style to the lines indicating the links between devices in the Topology Map:



- 4. To modify how MXview displays Power-over-Ethernet (PoE) links:
  - a. Select the **Show PoE Status on Topology** check box to indicate the PoE link status on the Topology Map.

PoE			
✓ Show PoE Status on Topology			
PoE Link Color #FF0000			

b. Click the **PoE Link Color** field and specify a new color.

PoE			
✓ Show PoE Status on Topole	ogy		`
PoE Link Color HFF0000			'
Background	6	100 C	
Background Color 🗌 #FFFFF	F		
Status Color			
Link Up	Link Down	0	
#00000	#FF0000	#ff0000	
Turbo Ring V1	Turbo Ring V2	Hex	

c. (Optional) Clear the **Show PoE Status on Topology** check box to hide the PoE link status on the Topology Map.

#### PoE

Show PoE Stat	us on Topology
PoE Link Color	#FF0000

5. To modify the Topology Map background, click the Background Color field and specify a new color.

Background		<b>^</b>
Background Color	# <u>EFFFF</u>	
Status Color	2	
Link Up	Link Down	
#000000	#FF0000	
Turbo Ring V1	Turbo Ring ∨2	0
#000000	#000000	######
Turbo Chain	RSTP	Hex

- 6. To modify the color used to indicate the status of specific links in the Topology Map, click to modify the **Status Color** hex code for any of the following links:
  - Link Up

\_ .

.

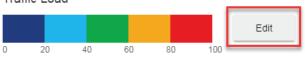
- Link Down
- > Turbo Ring V1
- > Turbo Ring V2
- > Turbo Chain
- > RSTP
- PRP/Coupling LAN A
- > PRP/Coupling LAN B
- HSR Ring

Status Color

Link Up	Link Down
#000000	#FF0000
Turbo Ring V1	Turbo Ring V2
200000	#000000
Turbo Chain	RSTP
#000000	#000000
PRP/Coupling LAN A	PRP/Coupling LAN B
#0000FF	#008000
HSR Ring	
#800080	

- 7. To modify the colors used to indicate the traffic load levels:
  - a. Check the Traffic Load legend and click Edit.

Traffic Load



The Edit Traffic Load Color screen will appear.

Edit Traffic Load color	
0-20 #023894	-
20-40 #1EB9EE	_
40-60 #14A83B	
60-80	#023894 Hex
80-100	
#E60012	_

Close Apply

- b. Modify the color used to indicate a traffic load (%) range.
- c. Click Apply.
- 8. Click Save.

MXview will update the modified settings.

### **Editing the Device Appearance**

Use the **Preferences** screen to modify how devices appear in the Topology Map.

- Navigate to Menu (=) > Preferences. The Preferences screen will appear.
- 2. In the **Display** section, expand **Device Appearance**.

The **Device Appearance** settings will appear.

Language					
Topology Appearance					
Device Appearance					
Preview					
IP Address					
Bottom Label					
None	•				
Alias					
Bottom Label IP Address		+	Bottom Label		
	-		Model Name	*	

- 3. To modify the label that indicates the device in the Topology Map:
  - a. Locate the **Bottom Label** drop-down list located below the Preview image:

Device Appearance

Alias Bottom Label IP Address		+ Bottom Label Model Name	<b>.</b>
Bottom Label None	•		
IP Address			
Preview			

- b. Select one of the following properties from the **Bottom Label** drop-down:
  - □ Location
  - Alias
  - Model Name
  - □ MAC

MXview displays the selected property below the IP address of the device.

Device Appearance

Pre	view	
IP Ad	ldress	
Loca	ation	
Bottom Label		
Location		

- 4. To modify the device alias:
  - a. Locate the **Alias** section.

Device Appearance

Preview		
IP Address		
Location Bottom Label	N	
	13	
Location	•	
Alias		
Bottom Label	+ Bottom Label	

•

b. From the first drop-down list in the Alias section, select one of the following:

Model Name

-

- □ IP Address
- □ MAC

IP Address

- Model Name
- Location
- □ SysName

- c. From the second drop-down list in the Alias section, select one of the following:
  - □ IP Address
  - □ MAC
  - Model Name
  - Location
  - □ SysName
- 5. Click Save.

MXview updates the modified settings.

# **Exporting the Topology Map**

MXview allows you to export the Topology Map as a PNG image.

1. Navigate to Menu ( $\equiv$ ) > Network > Topology.

The **Network Topolog**y screen appears and displays the Topology Map by default.

- If List view is selected, click the Topology view (<sup>\*</sup>) icon in the top right corner.
   The Network Topology screen will display a graphical representation of the devices and links on your network.
- 3. Navigate to **Edit > Export Topology**.

MXview exports the PNG image of the Topology Map to the specified location.

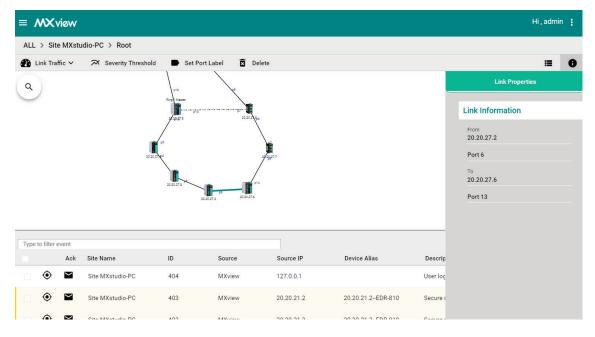
MXview allows you to monitor the traffic between devices on your network and trigger events for specific traffic conditions. You can apply topology views to monitor traffic load, network security, wireless access points and clients, and also visualize VLAN connections.

## **Viewing Link Properties**

Click a link on the Topology Map to view link properties and perform the following:

- Navigate to Menu (=) > Network > Topology. The Network Topology screen will appear and display the Topology Map by default.
- 2. Click on a link between devices in the Topology Map.

The **Link Properties** pane appears to the right of the Topology Map.



## **Viewing Port Traffic**

The **Port Traffic** screen displays a graph that shows the utilization percentage (Y-axis) over a specific time period (X-axis). You can also adjust the time period for the data that is displayed by changing the starting date and ending date. The minimum interval you can select is one day.

1. Navigate to Menu ( $\equiv$ ) > Network > Topology.

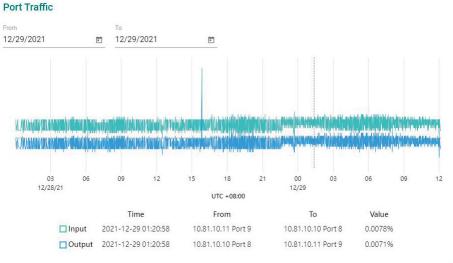
The Network Topology screen appears and displays the Topology Map by default.

2. Click on a link between devices in the Topology Map.

The Link Properties pane and the following toolbar appear when a link is selected.

- 🖚 Link Traffic 🗸 Set Port Label Delete 3. Navigate to Link Traffic > Port Traffic. The Port Traffic screen will appear. **Port Traffic** 12/29/2021 1 12/29/2021 Ē A MANIMUM iden pultainain direatainai V. MANHAMANA 18 12 03 06 no 12 15 21 00 03 nc 12/28/21 12/29 UTC +08:00 Time From То Value 🗖 Input Output Close
- 4. To adjust the time period for the graph data:
  - a. Click the **From** date and select a new starting date.
  - b. Click the **To** date and select a new ending date.
- 5. Hover over a line to view the direction of traffic.

For example, the green line at the top of the following graph represents traffic from **10.81.10.11** (device IP address) Port 9 to **10.81.10.10** (device IP address) Port 8.



Close

## **Viewing Packet Error Rates**

The **Packet Error Rate** screen displays a graph that shows the packet error rate (Y-axis) over a specific time period (X-axis). You can also adjust the time period for the data that is displayed by changing the start and end dates. The minimum interval is one day.

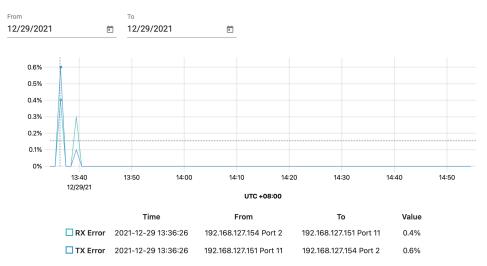
- Click on a link between devices in the Topology Map.
   The Link Properties pane and toolbar appear when a link is selected.



Close

- 4. To adjust the time period for the graph data:
  - a. Click the **From** date and select a new starting date.
  - b. Click the **To** date and select a new ending date.
- 5. Hover over a line to view the packet error rate.

#### **Packet Error Rate**



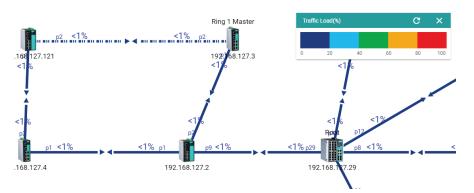
Close

# **Monitoring Traffic Loads**

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

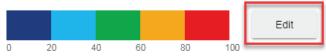
- Navigate to Menu (=) > Network > Topology. The Network Topology screen will appear and displays the Topology Map by default.
- If List view is selected, click the Topology view (<sup>\*</sup>) icon in the top right corner.
   The Network Topology screen will display a graphical representation of the devices and links on your network.
- 3. From the toolbar menu, navigate to **Visualization > Traffic View**.

The **Traffic Load** legend will appear and the Topology Map color-codes each link to indicate the traffic load.



- 4. To modify the colors used to indicate the traffic load levels:
  - a. Navigate to Menu (=) > Preferences.
     The Preferences screen will appear.
  - b. Under the Display section, expand Topology Appearance.
  - c. Locate the **Traffic Load** legend and click **Edit**.

Traffic Load



The Edit Traffic Load Color screen appears.

Edit Traffic Load color		
0-20		
#023894		
20-40		
#1EB9EE		
40-60		
#14A83B		
60-80		
#F6AB00		
80-100		
#E60012		
		-
	Cancel	Apply

- d. Modify the color used to indicate a traffic load (%) range.
- e. Click Apply.

### **Monitoring Network Security**

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 and procedure, system-level requirements, and componentlevel requirements.

Moxa's MXview follows Moxa's security guidelines, which are based on the 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: Based on IEC 62443-4-2 level 2
- Medium: Based on IEC 62443-4-2 level 1
- Basic: General baseline
- Open: Security Level below basic
- Unknown: Devices without security-related information for MXview

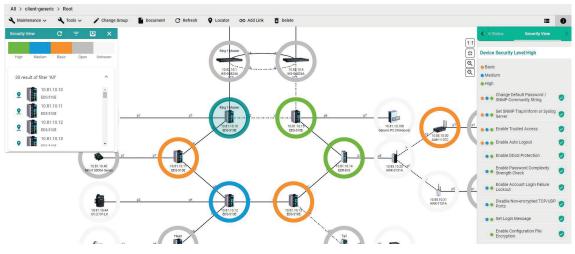
### NOTE

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

- Navigate to Menu (=) > Network > Topology. The Network Topology screen will appear and display the Topology Map by default.
- If List view is selected, click the Topology view (<sup>1</sup>) icon in the top right corner. The Network Topology screen will display a graphical representation of the devices and links on your network.

#### 3. From the toolbar menu, navigate to **Visualization > Security View**.

The **Security View** window will appear and the Topology Map indicates the security level of each device with a color-coded circle.



- 4. To filter the devices in the Security View window by security level:
  - a. Click the **Filter** ( $\overline{=}$ ) icon.
  - b. Select the security level.

The **Security View** window filters the list of devices to only show devices that match the selected security level.

5. To locate a device in the Topology Map, click the device in the Security View window.



The **Security View** details pane will appear on the right and the Topology Map highlights the circle around the device.

<b>&lt;</b> 11.5	Status Security View >
Device	e Security Level:High
e Basi Med High	ium
•••	Change Default Password /
•••	Set SNMP Trap/Inform or Syslog
	Enable Trusted Access
•••	Enable Auto Logout 🥥
••	Enable DDoS Protection
	Enable Password Complexity Strength Check
••	Enable Account Login Failure
	Disable Non-encrypted TCP/UDP 🥏
	Set Login Message 🛛 🥥
	Enable Configuration File

- 6. View security details for a specific device by using one of the following methods:
  - > Select a device from the Topology Map.
  - > Select a device from the **Security View** window.

The **Security View** details pane will appear and displays the device security level and security-related configuration statuses.

7. View the Security View Report:

Click **Export** to export the Security View Report in either CSV or PDF format.



8. Review the following items in the Security View details pane:

Item	Description
Enable Auto Logout	Check if the Auto Logout function is enabled or not
Set Login Message	Check if both the Web Login Message and Web Login Fail Message
Set Login Message	are configured or not.
Disable Non-encrypted TCP/UDP	Check if non-encrypted TCP/UDP Ports are disabled or not. HTTP,
Ports	Telnet, and Moxa Proprietary Protocol should be disabled. SNMP
	must be set to V3 only.
Enable Account Login Failure	Check if the Account Login Failure Lockout function is enabled or
Lockout	not
Enable Trusted Access	Check if the Trusted Access function is enabled or not. At least one
	rule must be set.
Enable Password Complexity	Check if the Password Complexity Strength Check function is
Strength Check	enabled or not
Enable Configuration File Encryption	Check if the Configuration File Encryption function is enabled or
	not. At least one rule must be enabled.
	Check if Broadcast Storm Protection is enabled or not. For eCos
	switches, MXview checks whether Broadcast Storm Protection is
Enable Broadcast Storm Protection	enabled. For EDR switches and routers, MXview checks whether at
	least one form of DoS protection is enabled. For MXnos switches,
	MXview checks whether at least one of the following is enabled or
	not: Broadcast, Multicast, or DLF protection.
Set SNMP Trap/Inform or Syslog	Check if the SNMP Trap/Inform or Syslog Server is set or not
Server	
Change Default Password/SNMP	Check if the Default Password or SNMP Community String is set or
Community String	not

- 9. To modify the colors used to indicate the security levels:
  - a. Navigate to **Menu** ( $\blacksquare$ ) > **Preferences**.

The **Preferences** screen will appear.

- b. Under the **Display** section, expand **Security View**.
- c. In the **Colors for check result** section, modify the color used to indicate a security level.

Security View		^
Profile Built-in Profile	Profile details	
Colors for check result		
High	Medium	
#77B800	#009DDB	
Basic	Open	
#FA943E	#C0C0C0	
		Save

d. Click Save.

- 10. To define a custom security profile:
  - a. Navigate to Menu (=) > Preferences.
     The Preferences screen will appear.
  - b. Under the **Display** section, expand **Security View**.
  - c. From the **Profile** drop-down list, select **User-defined**. The user-defined profile settings will appear.

Security	y View			^
Profile User det	fined 🔹			
Colors fo	r check result			
Pas #7	ss 77B800			
	t Pass FA943E	_		
<	Switch	NPORT5000A	Device Server	>
荘				
	Check Item			
	Enable Auto Logout			
	Set Login Message			

- d. (Optional) Modify the colors for the check result.
- e. Click one of the following device tabs to configure the profile settings:
  - Switch
  - □ NPORT5000A
  - Device Server
  - □ Terminal Server
  - □ Gateway
  - □ Wireless
  - □ **IO**
- f. (Optional) Click the **Settings**  $(\stackrel{\exists \pm}{=})$  icon to select a baseline.
- g. Select the check box for each item you want to add to security profile.
- h. Click Save.

# **Visualizing VLAN Connections**

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.

- Navigate to Menu (=) > Network > Topology. The Network Topology screen appears and displays the Topology Map by default.
- If List view is selected, click the Topology view (<sup>\*</sup>) icon in the top right corner.
   The Network Topology screen displays a graphical representation of the devices and links on your network.
- 3. From the toolbar menu, navigate to **Visualization > VLAN View**.

The **VLAN View** window appears.

= MX view						Hi , admi	in E
ALL > Site MXstudio-PC > Root >							
🙏 Topology 🗸 😁 Group 🗸 🧨	Edit 🗸 🕢 Visualization 🗸					:=	0
Q 10 10 10 10 10 10 10 10 10 10			20.22 24.9	Varid <u> </u>	t Trunk Port	×	1:1 1:1 0 0
2000 27.4	Hed 2020.24.6		20/20/24.8			_	<u>,</u>
Ack Site Name	ID Source	Source IP	Device Alias	Description	Time Issued		

4. Selecting a specific VLAN ID.

 ${\sf MXview}$  indicates devices, ports, and links that are associated with the VLAN ID using color-coded circles.

# **Monitoring Wireless Access Points and Clients**

MXview collects the wireless information from all the Moxa AWK series devices, and displays the information on the **Wireless Table View** screen.

Use the Wireless Table View screen to view the following information:

The number of wireless access points in your topology

Column	Description
Device Name	The device name of the access point
IP Address	The IP address of the access point
MAC Address	The MAC address of the access point
Modulation	The modulation of the access point

• The number of wireless clients in your topology

	- 37
Column	Description
Online	The connection status of the client
Device Name	The device name of the client
IP Address	The IP address of the client
MAC Address	The MAC address of the client
Signal Strength (dBM)	The signal strength of the client in dBM
SNR (db)	The signal-to-noise ratio of the client in db



### NOTE

The Wireless Table View screen only supports the AWK-1131A Series, AWK-3131A Series, and AWK-4131A Series devices.

### NOTE

The dashboard can only show AWK devices as APs and clients. It does not support third-party clients.

.

### NOTE

The Wireless Table View screen refreshes automatically every 15 seconds.

- Navigate to Menu (=) > Network > Topology. The Network Topology screen will appear and displays the Topology Map by default.
- If List view is selected, click the Topology view (<sup>1</sup>) icon in the top right corner. The Network Topology screen will display a graphical representation of the devices and links on your network.
- From the toolbar menu, navigate to Visualization > Wireless Table View. The Wireless Table View screen appears.
- To view details for a specific device, select the device from the table. The wireless device details pane appears.

## **Configuring Severity Thresholds for Traffic and Fiber Status Monitoring Events**

MXview allows you to configure the following traffic conditions on a link to trigger events:

- Bandwidth utilization is over the threshold.
- Bandwidth utilization is under the threshold.
- Packet error rate is over the threshold.
- Fiber Rx is under the threshold.
- Fiber Tx is under the threshold.
- Fiber temperature is over the threshold.
- Fiber voltage is under the threshold.
- Fiber voltage is over the threshold.

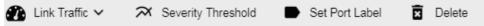
Since a link is bidirectional, the event will be triggered when the traffic condition in either direction satisfies the configured severity threshold.

1. Navigate to Menu ( $\equiv$ ) > Network > Topology.

The Network Topology screen will appear and display the Topology Map by default.

2. Click on a link between devices in the Topology Map.

The Link Properties pane and toolbar appear when a link is selected.



#### 3. Click Severity Threshold.

The Severity Threshold screen will appear.

Bandwidth Utilization	Packet Error Rate	SFP Threshold
Over *		
0	Warning	•
	96	
Under *	Warning	
0	Warning	
	70	
		Cancel App
Bandwidth Utilization		SFP Threshold
Bandwidth Utilization	Packet Error Rate	SFP Threshold
Bandwidth Utilization SFP TX Under * 0		SFP Threshold
Bandwidth Utilization SFP TX Under * 0	Packet Error Rate	SFP Threshold
Bandwidth Utilization SFP TX Under * 0 0 ~ -100	Packet Error Rate Warning	SFP Threshold
Bandwidth Utilization SFP TX Under * 0 0~-100 SFP RX Under * -12 0~-100	Packet Error Rate Warning	SFP Threshold
Bandwidth Utilization SFP TX Under * 0 0 ~ -100 SFP RX Under * -12 0 ~ -100 SFP Voltage Under *	Warning Warning	SFP Threshold
Bandwidth Utilization SFP TX Under * 0 0 ~ -100 SFP RX Under * -12 0 ~ -100 SFP Voltage Under * 0 0 ~ 10	Packet Error Rate Warning Warning dBm	SFP Threshold
Bandwidth Utilization SFP TX Under * 0 0 ~ -100 SFP RX Under * -12 0 ~ -100 SFP Voltage Under * 0 0 ~ 10 SFP Voltage Over *	Packet Error Rate Warning Warning Warning Warning Warning	SFP Threshold
Bandwidth Utilization SFP TX Under * 0 0 ~ -100 SFP RX Under * -12 0 ~ -100 SFP Voltage Under * 0 0 ~ 10 SFP Voltage Over * 0 0 ~ 10 0 ~ 10 SFP Voltage Over * 0 0 ~ 10 0 ~ 1	Packet Error Rate       dBm     Warning       dBm     Warning       dBm     Warning       v     Warning	SFP Threshold
Bandwidth Utilization SFP TX Under * 0 0 ~-100 SFP RX Under * -12 0 ~-100 SFP Voltage Under * 0 0 ~ 10 SFP Voltage Over * 0	Packet Error Rate          Warning         dBm         Warning         dBm         Warning         Warning         Warning         Warning         Warning	SFP Threshold

- 4. To trigger an event when the bandwidth utilization on a link exceeds a specified percentage:
  - a. Click the **Bandwidth Utilization** tab.
  - b. In the **Over** field, specify the maximum bandwidth utilization percentage.
  - c. From the adjacent drop-down list, select one of the following severity levels:
    - Information
    - □ Warning
    - □ Critical
- 5. To trigger an event when the bandwidth utilization on a link falls below a specified percentage:
  - a. Click the **Bandwidth Utilization** tab.
  - b. In the **Under** field, specify the minimum bandwidth utilization percentage.
  - c. From the adjacent drop-down list, select one of the following severity levels:
    - □ Information
    - O Warning
    - Critical

- 6. To trigger an event when the packet error rate exceeds a specified percentage:
  - a. Click the Packet Error Rate tab.
  - b. In the **Over** field, specify the maximum bandwidth utilization percentage.
  - c. From the adjacent drop-down list, select one of the following severity levels:
    - □ Information
    - Warning
    - □ Critical
- 7. To trigger an event when the SFP Tx falls below a specific range:
  - a. Click the **SFP Threshold** tab.
  - b. In the SFP Tx Under field, specify the maximum Tx threshold in dB (0~-100)
  - c. From the adjacent drop-down list, select one of the following severity levels:
    - □ Information
    - □ Warning
    - □ Critical
- 8. To trigger an event when the SFP Rx falls below a specific range:
  - a. Click the SFP Threshold tab.
  - b. In the SFP Rx Under field, specify the maximum Rx threshold in dB (0~-100)
  - c. From the adjacent drop-down list, select one of the following severity levels:
    - □ Information
    - Warning
    - Critical
- 9. To trigger an event when the SFP voltage falls below a specific range:
  - a. Click the  $\ensuremath{\textbf{SFP}}$   $\ensuremath{\textbf{Threshold}}$  tab.
  - b. In the SFP Voltage Under field, specify the maximum voltage in V (0~10)
  - c. From the adjacent drop-down list, select one of the following severity levels:
    - Information
    - O Warning
    - Critical
- 10. To trigger an event when the SFP voltage exceeds a specific range:
  - a. Click the SFP Threshold tab.
  - b. In the SFP Voltage Over field, specify the minimum voltage in V  $(0 \sim 10)$
  - c. From the adjacent drop-down list, select one of the following severity levels:
    - □ Information
    - □ Warning
    - □ Critical
- 11. To trigger an event when the SFP temperature exceeds a specific range:
  - a. Click the **SFP Threshold** tab.
  - b. In the SFP Temperature Over field, specify the minimum temperature in Celsius (0~100)
  - c. From the adjacent drop-down list, select one of the following severity levels:
    - □ Information
    - Warning
    - Critical

# **Configuring Custom Port Labels**

MXview uses the following port labelling convention to identify directions of traffic on a link.

<Device IP Address> / <Port Number>

You can use the Set Port Label screen to customize the port labels.

- 1. Navigate to Menu ( $\blacksquare$ ) > Network > Topology.
  - The **Network Topology** screen will appear and display the Topology Map by default.
- 2. Click on a link between devices in the Topology Map.

The Link Properties pane and toolbar appear when a link is selected.

👔 Link Traffic 🗸	lpha Severity Threshold	🕒 Se	t Port Label	X	Delete
Click Set Port Label.					
The Set Port Label sc	reen appears.				
Set Port Label					
Use Custom Label					
From: 10.81.10.12 / Po	rt 8				
To: 10.81.10.11 / Port 8	3				
		Cancel	Apply		

- 4. Select the **Use Custom Label** check box.
- 5. In the **From** field, provide a new label for the source port.
- 6. In the **To** field, provide a new label for the destination port.
- 7. Click Apply.

3.

# Viewing the SFP Fiber Status in Table View

MXview collects and display fiber status in SFP > SFP List

👗 Topology 🗸	🔂 Group 🗸	🖍 Edit 🗸 💿 Visualization 🗸	SFP ∨
٩			:≡ SFP List

The list shows Fiber TX, RX, temperature, and voltage of the cables that are connected.

T									
	X (dBm)	RX (dBm)	Temp. (°C)	Volt. (V)		TX (dBm)	RX (dBm)	Temp. (°C)	Volt. (V)
10.81.10.12 -6	5.1	-6.3	42.1	3.3	10.81.10.11 Port 8 / SFP-1GSXLC	-6	-5.9	43	3.3
10.81.10.10 -6 Port 8 / SFP-1GSXLC	6.3	-5.8	41.6	3.3	10.81.10.11 Port 9 / SFP-1GSXLC	-6.2	-6.1	44.2	3.3
10.81.10.12 Port 9 / SFP-1GSXLC -6	6	-5.9	43.7	3.3	10.81.10.13 Port 8 / SFP-1GSXLC	-6.1	-6.2	40.7	3.4

The MXview **Network Topology** screen provides several features and tools for managing and maintaining devices in your network topology.

### **Viewing the Device List**

The **List view** on the **Network Topology** screen will display a list of discovered devices in your network topology. You can also use this view to manually add devices to your network topology or export filtered data as a CSV file.

/ Ed	lit 🗸						× 0
Ŧ					<b>Q</b> Search		
	Site Name	Device Alias	Device IP	MAC Address	Availability	Firmware Version	Location
	client-generic	EDS-510E	10.81.10.10	00:90:E8:86:2F:12	100.00%	V5.4 build 21042021	Switch Location
	client-generic	EDS-510E	10.81.10.11	00:90:E8:86:2F:15	100.00%	V5.4 build 21042021	Switch Location
	client-generic	EDS-510E	10.81.10.12	00:90:E8:86:2E:F3	100.00%	V5.4 build 21042021	Switch Location
	client-generic	EDS-510E	10.81.10.13	00:90:E8:86:2F:17	100.00%	V5.4 build 21042021	Switch Location
	client-generic	EDR-810	10.81.10.14	00:90:E8:72:20:01	100.00%	V5.10 build 21100708.	Device Locatior
	client-generic	EDS-510E	10.81.10.15	00:90:E8:86:2F:16	100.00%	V5.4 build 21042021	Switch Location
	client-generic	EDS-G512E-8PoE	10.81.10.16	00:90:E8:85:8B:54	100.00%	V6.0 build 18022316	Switch Location
	client-generic	EDS-408A	10.81.10.17	00:90:E8:86:B1:A0	100.00%	V3.10 build 19121910	Switch Location

1. Navigate to Menu ( $\equiv$ ) > Network > Topology.

The Network Topology screen will appear and display the Topology Map in Topology view.

2. Click the **List view** (■) icon in the top right corner.

The **Network Topology** screen displays a list of devices on your network.

- 3. To add a device to your network topology:
  - a. Click **Edit > Add Device**.
    - The Add Device screen will appear.

#### Add Device

	Assign To Group 👻	
	Port	
*	161	-
	Password	
	Write Community private	
Ŧ	Authentication	
*	Encryption Password	
	•	Port     161     Password     Write Community     private     Authentication

Cancel /

- b. Configure the following:
  - **IP Address:** Specify the IP address of the device
  - □ Assign Model: Select the model of the device
  - □ Assign To Group: Select the group to assign the device to
  - □ SNMP Version: Select the SNMP version
  - **User Name:** Specify the device login user name
  - **Password:** Create a password
  - **Read Community:** Specify the SNMP read community string
  - □ Write Community: Specify the SNMP write community string
  - **Data Encryption:** Select the data encryption method
  - **Authentication:** Select the authentication method
  - **Encryption Key:** Specify the encryption key
- c. Click Add.

MXview adds the device to the topology.

4. To view device properties, select the check box next to the device.

The Device Properties details pane will appear.

Device Properties	Current Status
Basic Device Prop	erties
Alias	
EDS-510E	
Model Name	
EDS-510E	
MAC Address	
00:90:E8:86:2F:16	
Availability	
100.00%	
System Description	
EDS-510E-3GTXSF	P
System Object ID	
.1.3.6.1.4.1.8691.7	.84

- 5. To filter the device list by severity level:
  - a. Click the Filter (<sup>™</sup>) icon in the top right corner.
     The Severity drop-down list appears.

	×
Severity	~
Reset	t Apply

- b. Select one of the following severity levels:
  - Critical
  - □ Warning
  - Information
- c. Click Apply.

MXview filters the device list to only display devices with the selected severity level.

- 6. To export the device list:
  - a. Click the **Export** ( ) icon.



- b. Select Export CSV.
- c. Specify the location to save the exported file.
- d. Click Save.

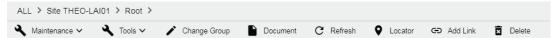
MXview will export the displayed data as a CSV file.

### **Importing Device Configurations**

Use the **Network Topology** screen to import an INI-formatted configuration file to a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

- 1. Navigate to **Menu** (≡) > **Network** > **Topology**.
  - The Network Topology screen will appear and displays the Topology Map by default.
- 2. Select one of the following views:
  - > Topology view: Displays a graphical representation of devices in your network topology.
  - List view: Displays a list of the devices in your network topology.
- 3. Select the device that you want to import configurations to:
  - > Topology view: Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options change.



4. Navigate to Maintenance > Import Config.

The Import Config screen appears and indicates the IP address of the selected device.

```
Import Config - 192.168.127.1
```

Import Config		
	Close	Import

- 5. Click the folder (▶) icon to upload the configuration file from your local machine.
- 6. Click Import.

MXview imports the configuration file to the specified device.

### **Exporting Device Configurations**

Use the **Network Topology** screen to export an INI-formatted configuration file from a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

The **Network Topology** screen will appear and display the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.

- 3. Select the device that you want to export configurations from.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options change.

ALL > Site THEO-L	AI01 > Root >						
🔧 Maintenance 🗸	🔧 Tools 🗸	/ Change Group	Document	C Refresh	Locator	GD Add Link	Delete

4. Navigate to Maintenance > Export Config.

The Export Config screen will appear and indicate the IP address of the selected device.

Export Config - 192.168.127.1

Close Export

- 5. Click Export.
- 6. Specify the location to save the configuration file.
- 7. Click Save.

MXview saves the device configurations as an INI file in the specified location.

## **Upgrading Firmware**

Use the **Network Topology** screen to upgrade the firmware (ROM-formatted file) on a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

- - The **Network Topology** screen appears and displays the Topology Map by default.
- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - b. **List view:** Displays a list of the devices in your network topology.
- 3. Select the device that you want to upgrade the firmware for:
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options change.

ALL > Site THEO-L	AI01 > Root >						
🔧 Maintenance 🗸	🔧 Tools 🗸	🖍 Change Group	Document	C Refresh	Locator	G Add Link	🖬 Delete

4. Navigate to Maintenance > Upgrade Firmware.

The Upgrade Firmware screen appears and indicates the IP address of the selected device.

Upgrade Firmware - 192.168	127.103
Upgrade Firmware *	ב
Cancel	Upgrade

5. Click the folder (**b**) icon to upload the ROM-formatted firmware file from your local machine.

#### 6. Click Upgrade.

MXview will upgrade the firmware on the specified device.

# Generating a QR Code for the Device

MXview allows you to generate a QR code that can be printed and attached to a field device. Use the **MXview ToGo** mobile app to scan the QR code on a field device to allow field engineers to check the device status from the mobile app.

1. Navigate to Menu ( $\equiv$ ) > Network > Topology.

The Network Topology screen appears and displays the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device that you want to upgrade the firmware for.
  - > Topology view: Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options will change.

ALL > Site THEO-LAI01 > Root > ▲ Maintenance ~ ▲ Tools ~ / Change Group Document C Refresh Locator Add Link Delete

- 4. Navigate to **Maintenance > Generate QR Code**.
- 5. Specify the location to save the QR code.
- 6. Click Save.

MXview will save a zipped PNG file of the QR code to the specified location.

- 7. Print the QR code and attach it to the device.
- 8. Scan the QR code by using the **MXview ToGo** mobile app.

**MXview ToGo** will display the device status, event list, device properties, port status, and other device information from the MXview server.

## **Assigning a Device Model**

Use the **Network Topology** screen to assign a device model to a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to Menu ( $\equiv$ ) > Network > Topology.

The Network Topology screen appears and displays the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device that you want to upgrade the firmware for.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options change.

ALL > Site THEO-L	AI01 > Root >					
🔧 Maintenance 🗸	🔧 Tools 🗸	Document	C Refresh	Locator	GD Add Link	Delete

#### 4. Navigate to Maintenance > Assign Model.

The Assign Model screen appears.

Assign Model		
IP Address : 192.168.127.1		
Model : IKS-6726A		
Select Model		H - HHE (HHE) (HHE)
IKS-6726A	-	

Close Apply

- 5. Select the device model from the drop-down list.
- 6. Click Apply.

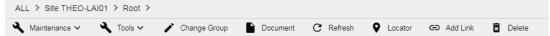
MXview assigns the selected model to the device.

# **Configuring Basic Device Information**

Use the **Network Topology** screen to configure basic information for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

- 1. Navigate to Menu ( $\equiv$ ) > Network > Topology.
- The Network Topology screen will appear and display the Topology Map by default.
- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device that you want to upgrade the firmware for.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options change.



4. Navigate to Maintenance > Basic Information.

The Basic Information screen appears.

Model		
Name		
Location		
Switch	Location	

**Basic Information** 

Contact

Close Apply

- 5. Specify the following device information:
  - > Model
  - > Location
  - > Contact
- 6. Click **Apply**.

MXview will update the device information.

# **Configuring Device IP Settings**

Use the **Network Topology** screen to configure IP settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to Menu ( $\blacksquare$ ) > Network > Topology.

The **Network Topology** screen appears and displays the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options change.

ALL > Site THEO-LAI01 > Root >

4. Navigate to Maintenance > IP Configuration.

The IP Configuration screen will appear.

IP Configuration			
This feature is not available for	Layer 3 devices.		
IP Address *			
10.81.10.10			
Netmask *			
255.255.255.0			
Gateway			
0.0.0.0			
DNS1			
0.0.0.0			
DNS2			
0.0.0.0			
		Cancel	Apply

- 5. Specify the following IP configurations:
  - > IP Address
  - > Netmask
  - > Gateway
  - > DNS1
  - > DNS2
- 6. Click Apply.

MXview updates the device IP configurations.

# **Configuring SNMP Trap Servers**

MXview can collaborate with other network management software and send SNMP Traps to non-Moxa NMS. MXview supports up to two trap servers depending on the device.

1. Navigate to Menu ( $\blacksquare$ ) > Network > Topology.

The Network Topology screen will appear and display the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options change.

ALL > Site THEO-L	AI01 > Root >						
🔾 Maintenance 🗸	🔦 Tools 🗸	🖍 Change Group	Document	c Refresh	Q Locator	GD Add Link	Delete

4. Navigate to Maintenance > Trap Server.

#### The Trap Server screen appears.

Trap Server	
Destination IP1 *	
10.82.10.6	-
Community Name1 *	
public	
	-
Destination IP2 *	-
Destination IP2 *	-
	-
Community Name2 *	-

- 5. Configure the following SNMP trap server settings for the device:
  - > Destination IP1
  - Community Name1
  - > (Optional) **Destination IP2**
  - > (Optional) Community Name2
- 6. Click Apply.

MXview sends SNMP traps to the configured trap server(s) when events are detected on the device.

# **Configuring Port Settings**

Use the **Network Topology** screen to configure port settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to Menu ( $\equiv$ ) > Network > Topology.

The Network Topology screen appears and displays the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options will change.

ALL > Site THEO-LAI01 > Root >

4. Navigate to Maintenance > Port Settings.

Port Settings	
Port *	
1	•
Enable *	
Enabled	•
Media Type	
100TX,RJ45.	
Port Description	
Apply settings to another port	
Apply settings to another port	

The Port Setting screen appears.

- 5. Configure the following port settings for the device:
  - > **Port:** Select the port number.
  - > **Enable:** Enable or disable the port.
  - > **Port Description:** Provide a description of the port.
  - > Port Name: Provide a custom name for the port.
  - Apply settings to another port: Select to apply the configured settings to other ports on the device.
- 6. Click **Apply**.

MXview will update the port settings to the device.

# **Configuring SNMP Settings**

Use the **Network Topology** screen to configure SNMP settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to Menu ( $\blacksquare$ ) > Network > Topology.

The Network Topology screen appears and displays the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options will change.

ALL > Site THEO-LAI01 > Root > Maintenance > Tools > Change Group Document C Refresh O Locator G Add Link Delete

4. Navigate to **Maintenance > SNMP Settings**.

The SNMP Configuration screen will appear.

SNMP Configurati	on		
SNMP Version *		Port *	
V3	•	161	
User Name		Password	
admin		Ø	
Read Community		Write Community	
public		private	
Data Encryption		Authentication	
AuthPriv	•	SHA	•
Encryption Protocol		Encryption Password	
DES	•	······	Ø
		Cancel	Apply

- 5. Configure the following SNMP settings for the device:
  - > User Name
  - > Password
  - > Read Community
  - > Write Community
  - > Data Encryption
  - > Authentication
  - Encryption Key
  - > Encryption Protocol
  - > SNMP Port
  - > SNMP Version
- 6. Click **Apply**.

MXview updates the port settings to the device.

# **Configuring Polling Settings**

Use the **Network Topology** screen to configure ICMP or SNMP polling settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to Menu (≡) > Network > Topology.

The Network Topology screen will appear and display the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options change.

ALL > Site THEO-LAID1 > Root >

4. Navigate to Maintenance > Polling Settings.

The Polling Settings screen appears.

Polling Settings			
ICMP polling interval *			
10			
10 - 600 Consecutive failure to trigger ICMP unreachable event *	Sec		
1			
1 - 9999 SNMP polling interval *	times		
60			
60 - 600 Consecutive failure to trigger SNMP unreachable event *	Sec		
1			
1 - 9999	times		
		Cancel	Apply

- 5. Configure the following polling settings for the device:
  - > ICMP polling interval
  - > Consecutive failure to trigger ICMP unreachable event
  - > SNMP polling interval
  - > Consecutive failure to trigger SNMP unreachable event
- 6. Click **Apply**.

MXview will update the polling settings for the device.

# **Configuring Advanced Settings**

Use the **Network Topology** screen to configure advanced settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to Menu ( $\blacksquare$ ) > Network > Topology.

The Network Topology screen will appear and display the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options change.

ALL > Site THEO-LAID1 > Root >

4. Navigate to Maintenance > Advanced Settings.

The Device Settings screen appears.

Device Settings		
Modify Device Alias Alias EDS-510E		
Use Global Access User Name and Password		
Username		
Password		
	Cancel	Apply

- 5. To modify device alias:
  - a. Select the **Modify Device Alias** check box.
  - b. Edit the **Alias** field.
- 6. To specify login credentials for the device web console (if different from the global MXview credentials):
  - a. Clear the Use Global Access User Name and Password check box.
  - b. Enter the User Name and Password for the device web console.
- 7. Click **Apply**.

MXview updates the device settings.

# **Configuring Polling IP Settings**

Use the **Network Typology** screen to configure the IP address used to poll a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to Menu ( $\blacksquare$ ) > Network > Topology.

The **Network Topology** screen will appear and display the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options will change.

ALL > Site THEO-L	AI01 > Root >						
🔾 Maintenance 🗸	🔦 Tools 🗸	🖍 Change Group	Document	C Refresh	Locator	🕒 Add Link	Delete

4. Navigate to Maintenance > Polling IP.

The **Polling IP** screen will appear.

Polling IP			
Polling IP			
10.82.10.2	•		
			_
		Cancel	Apply

- 5. Select the IP address used to poll the device.
- 6. Click **Apply**.

MXview will update the polling IP address for the device.

# **Changing the Device Icon**

Use the **Network Topology** screen to change the device icon by selecting the device from the **Topology Map** or **Device List**, and then upload a JPG, GIF, or PNG image file.

1. Navigate to Menu ( $\equiv$ ) > Network > Topology.

The Network Topology screen will appear and display the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options will change.

ALL > Site THEO-LAI01 > Root >

4. Navigate to **Maintenance > Change Device** Icon.

The Change Device Icon screen appears.

Change Device Icon		
IP Address: 10.81.10.11	-	
Model Icon *		
	Cancel	Apply

5. Click the folder (<sup>**b**</sup>) icon to upload the device icon from your local machine.

#### 6. Click Apply.

MXview will change the device icon to the uploaded JPG, GIF, or PNG image file.

# **Signing on to Device Web Consoles**

MXview allows you to use the **Network Topology** screen to the web console for a device from the **Topology Map** or **Device List**.



### NOTE

You can use the **Preferences** screen to configure the web console protocol. 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.

- 1. (Optional) Configure the web console protocol:
  - a. Navigate to Menu ( $\equiv$ ) > Preferences.

The **Preferences** screen appears.

b. In the  $\ensuremath{\text{Advanced}}$  section, expand  $\ensuremath{\text{Management}}$  Interface.

The Management Interface settings appear.

Advanced	
System Configuration	~
Device	~
SNMP Configuration	~
Events	~
Management Interface	^
Web console protocol Http	
Http	

- c. Configure the following:
  - Web Console Protocol
  - □ HTTP Port
  - □ HTTPS Port
  - Telnet Port
- d. Click Save.

MXview updates the web console protocol settings.

2. Navigate to Menu ( $\equiv$ ) > Network > Topology.

The Network Topology screen will appear and display the Topology Map by default.

- 3. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 4. Select the device.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options change.

ALL > Site THEO-L	AI01 > Root >						
🔾 Maintenance 🗸	🔾 Tools 🗸	🖍 Change Group	Document	C Refresh	Locator	G Add Link	Delete

#### 5. Navigate to **Tools > Web Console**.

The login screen for device web console appears in a new browser tab.



#### NOTE

You may need to allow pop-ups on your web browser in order to view the device web console.

- 6. Enter the **Username** and **Password** for the device web console.
- 7. Click Login.

The device web console will successfully log in.

### **Pinging Devices**

Use the **Network Topology** screen to ping devices in your network topology from the **Topology Map** or **Device List**.

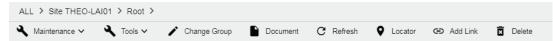
1. Navigate to Menu ( $\equiv$ ) > Network > Topology.

The Network Topology screen will appear and display the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device.
  - > Topology view: Click the icon of the device in the Topology Map.

> List view: Select the check box next to the device in the Device List.

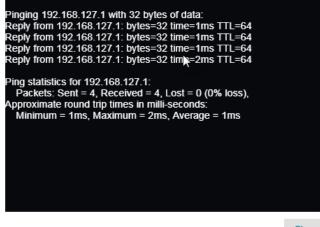
The toolbar options change.



4. Navigate to **Tools > Ping**.

The Ping screen will appear and will start the ping test.

```
Ping 192.168.127.1
```



Close

5. Wait for the ping test to finish and view the results.

## **Changing Device Groups**

Use the **Network Topology** screen to change the assigned group for a device by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to Menu (≡) > Network > Topology.

The Network Topology screen will appear and display the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options change.

ALL > Site THEO-L	AI01 > Root >						
🔾 Maintenance 🗸	🔦 Tools 🗸	🖍 Change Group	Document	c Refresh	Locator	GD Add Link	Delete

#### 4. Click Change Group.

The **Change Group** screen will appear and displays the following information:

Root		*	
	IP Address		
	10.81.10.10		
	10.81.10.11		
	10.81.10.12		
	10.81.10.13		
	10.81.10.14		
	10.81.10.15		
	10.81.10.16		
	10.81.10.17		
_	40.04.40.40		
	ed / 30 total I to Group *	-	

- 5. (Optional) Select additional IP addresses to assign other devices from the current group to the new group.
- 6. From the **Assign to Group** drop-down list, select the new group that you want to assign the selected device(s) to.

#### 7. Click Apply.

MXview will assign the selected device(s) to the new group.

# **Uploading Device Documents**

Use the **Network Topology** screen to upload PDF documentation (e.g., user's manual, quick installation guide) for a device. Uploaded documents can be downloaded for future reference.

1. Navigate to Menu ( $\equiv$ ) > Network > Topology.

The Network Topology screen appears and displays the Topology Map by default.

- 2. Select one of the following views:
  - > Topology view: Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options will change.

ALL > Site THEO-L	AI01 > Root >						
🔧 Maintenance 🗸	🔧 Tools 🗸	🖍 Change Group	Document	C Refresh	Locator	🕒 Add Link	X Delete

4. Click Document.

The Set Document screen will appears.

Set Document - 192.168.1	27.167
Select a file to upload *	
Maximum document size is 20MB.PDF only.	
Cancel	Set Document

- Click the folder (■) icon to upload a PDF document from your local machine. The maximum document size is 20 MB and has to be a PDF.
- 6. Click Set Document.

MXview uploads the PDF document for the device.

## **Refreshing the Device Status**

Since some device data is collected by polling, there may be a time delay for some data. Use the **Network Topology** screen to refresh the device status by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to Menu ( $\equiv$ ) > Network > Topology.

The Network Topology screen appears and displays the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device.
  - > **Topology view:** Click the icon of the device in the Topology Map.

> List view: Select the check box next to the device in the Device List.

The toolbar options change.

ALL > Site THEO-I	LAI01 > Root >						
🔧 Maintenance 🗸	🔧 Tools 🗸	🖍 Change Group	Document	C Refresh	Locator	👄 Add Link	Delete

#### 4. Click Refresh.

MXview polls the device for updated data.

# **Locating Devices**

Use the **Device Locator** to locate a device in the field. When the **Device Locator** is activated, all the LEDs on the device start blinking to help you locate the device.

1. Navigate to Menu ( $\equiv$ ) > Network > Topology.

The Network Topology screen appears and will display the Topology Map by default.

- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device.
  - > **Topology view:** Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options will change.

ALL > Site THEO-L	AI01 > Root >						
🔾 Maintenance 🗸	🔦 Tools 🗸	🖍 Change Group	Document	c Refresh	Locator	GD Add Link	Delete

4. Click Locator.

The **Device Locator** screen appears.

Device Lo	cator	
► Start	Stop	
		Close

5. Click Start.

All the LEDs on the device start blinking.

After you have located the device, click **Stop**.
 All the LEDs on the device stop blinking.

## **Deleting Devices**

Use the **Network Topology** screen to 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 will not be polled.

- 1. Navigate to Menu (≡) > Network > Topology.
  - The Network Topology screen appears and displays the Topology Map by default.
- 2. Select one of the following views:
  - > **Topology view:** Displays a graphical representation of the devices in your network topology.
  - > List view: Displays a list of the devices in your network topology.
- 3. Select the device.
  - > Topology view: Click the icon of the device in the Topology Map.
  - > List view: Select the check box next to the device in the Device List.

The toolbar options will change.



4. Click Delete.

MXview removes the device from your network topology.

MXview allows you to monitor system events, create custom monitoring events, and configure event notifications.

## **Event Monitoring**

### **Viewing All Events**

The **All Events** screen provides information about all the network events for devices in your topology. Use the filters to customize the information displayed in the table. You can also export the data as a CSV file.

#### All Events

M if U	Ŧ						
	Site Name	ID	Source	Source IP	Device Alias	Description	Time Issued
	Site DESKTOP-TUTNU4T	222	MXview	10.122.10.215		User login: admin	2021-12-29 16:33:10
	Site DESKTOP-TUTNU4T	221	MXview	10.122.10.215		User login failed: admin\	2021-12-29 16:33:08
	Site DESKTOP-TUTNU4T	220	MXview	192.168.127.166	192.168.127.166AWK-1137C	Device ICMP reachable	2021-12-29 16:00:30
- 🖬 🔒	Site DESKTOP-TUTNU4T	219	MXview	192.168.127.166	192.168.127.166AWK-1137C	Device ICMP unreachable	2021-12-29 16:00:20
	Site DESKTOP-TUTNU4T	218	MXview	192.168.127.166	192.168.127.166AWK-1137C	Device ICMP reachable	2021-12-29 15:56:00
- 🖬 🔒	Site DESKTOP-TUTNU4T	217	MXview	192.168.127.166	192.168.127.166AWK-1137C	Device ICMP unreachable	2021-12-29 15:55:50
	Site DESKTOP-TUTNU4T	216	MXview	10.123.35.32		User login: admin	2021-12-29 14:42:25

#### 1. Navigate to Menu ( $\equiv$ ) > Event > All Events.

The **All Events** screen will display the following information in a table format:

Column	Description
Ack	Acknowledge status of the event
Show Details	The detailed information of this event
Site Name	The site to which the device that issued the event belongs
ID	The unique identifier of the event
Source IP	The IP address of the device that issued the event
Source	The source of the event
Device Alias	The unique name of the device
Description	The description of the event
Time Issued	The time the event was issued

2. To filter the information in the table, type a full or partial string that matches the value in any of the table columns.

MXview filters the table to only display results that fully or partially match the specified string.

- 3. To filter the information in the table by specific criteria:
  - a. Click the Filter (<sup>-</sup>Ξ) icon in the top right corner.
     The following screen will appear.

Severity	•					×
Site Name 🔻	Group Root		IP Add	lress		
Source -	Acknowle	9 ۹				
Start Date 📋	Hour	•	Minute	•	Second	•
End Date 📋	Hour	*	Minute	*	Second	•
					Reset	Apply

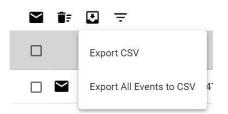
b. Specify any of the following criteria:

Criteria	Description
Severity	Select the severity level of the event
Site Name	Select the site to which the device that issued the event belongs
Group	Select the group to which the device is assigned
IP Address	Specify the IP address of the device
Source	Select the source of the event
Ack	Select the acknowledgement status of the event
Start Date	Specify the start date and time for the event data to display
End Date	Specify the end date and time for the event data to display

c. Click Apply.

MXview filters the table to only display events that match the specified criteria.

- To sort the data in the table by a specific column, click the column heading. MXview sorts the table by the column.
- 5. To export data displayed on the **All Events** screen:
  - a. Click the **Export** ( ) icon.



- b. Select **Export CSV** for just the events on the first page or **Export All Events to CSV** for all event pages.
- c. Specify the location to save the exported file.
- d. Click Save.

MXview exports the displayed event data as a CSV file.

### **Viewing Syslog Events**

The **Syslog Event Viewer** screen provides information about the syslog events on your network. Use the filters to customize the information displayed in the table. You can also export the data as a CSV file.

Syslog Viewer					
<b>₹ 2</b> ∎=					Q Search
Site Name	Severity	Time Stamp IP Address	Facility	Message	
					Items per page: $100 = 0 \text{ of } 0 \text{ of } 0 \neq 0$

- 1. Enable the built-in syslog server.
  - a. Navigate to Menu (≡) > Preferences.
     The Preferences screen appears.
  - b. In the Server section, expand Syslog Server Configuration.
     The Syslog Server Configuration settings will appear.

erver					
Syslog Server Configuration					^
Enable built-in syslog server					
Disabled -					
Quality and the second					
Syslog server port 514					
				Save	

- c. Select **Enabled** from the Enable built-in syslog server drop-down list.
- d. Specify the syslog server communication port.
- e. Click Save.
  - MXview enables the built-in syslog server and starts logging syslog events.
- 2. Navigate to Menu ( $\equiv$ ) > Event > Syslog Viewer.

The **Syslog Event Viewer** screen displays the following information in a table format:

Column	Description
Ack	The acknowledgement status of the event
Site Name	The site to which the device that issued the event belongs
ID	The unique identifier of the event
Source IP	The IP address of the device that issued the event
Device Alias	The unique name of the device that issued the event
Description	The description of the event
Time Issued	The time the event was issued

3. To filter the information in the table, type a full or partial string that matches the value in any of the table columns.

MXview filters the table to only display results that fully or partially match the specified string.

- 4. To filter the information in the table by specific criteria:
  - a. Click the Filter (<sup>™</sup>) icon in the top right corner.
     The following screen will appear.

Site Name	•	IF	o Address		<u> </u>	×
Facility	•					
Priority Higher than or	equal 👻	S	everity		•	
Start Date 🖻	Hour	•	Minute	•		
End Date 🖻	Hour	*	Minute	•		
					Reset	Apply

b. Specify any of the following criteria:

Criteria	Description		
Site Name	Select the site to which the device that issued the event belongs		
IP Address	Specify the IP address of the device that issued the event		
Facility	Select the group to which the device is assigned		
Select the criteria operator for matching the event severity level:			
Priority	Higher than or equal to		
i noney	• Equals		
	Lower than or equal to		
Severity	Select the severity level of the event		
Start Date	Specify the start date and time for the event data to display		
End Date	Specify the end date and time for the event data to display		

c. Click Apply.

MXview filters the table to only display events that match the specified criteria.

5. To sort the data in the table by a specific column, click the column heading.

- MXview sorts the table by the column.
- 6. To export data displayed on the **All Events** screen:
  - a. Click the **Export** ( ) icon.

Ŧ		
Site	Export CSV	Se
	Export All Syslog to CSV	

- b. Select Export CSV for just the first syslog page or Export All Events to CSV for all syslog pages.
- c. Specify the location to save the exported file.
- d. Click Save.

MXview exports the displayed event data as a CSV file.

## **Configuring the Server Disk Space Threshold**

MXview allows you to trigger an event notification when the MXview server reaches a configured disk space threshold.

- Navigate to Menu (=) > Preferences.
   The Preferences screen appears.
- In the Advanced section, expand System Configuration.
   The System Configuration settings will appear.
- 3. In the **Threshold of Disk Space (MB)** field, specify the threshold for available disk space remaining on the MXview server in MB.

System Configuration			
Background Discovery			
Disabled	<b>*</b>		
Disabled	<b>T</b>		
	<u>·</u>		
Disabled Threshold of Disk Space (MB)	<u> </u>		

4. Click Save.

MXview will trigger an event when the threshold for the available disk space remaining is reached.

### **Configuring Event Thresholds and Severity Levels**

Use the **Preferences** screen to configure default event thresholds and severity levels.

- Navigate to Menu (=) > Preferences. The Preferences screen will appear.
- In the Advanced section, expand Events. The Events settings will appear.
- 3. Select one of the following severity levels for **Link Up** events:
  - > Information
  - > Waning
  - > Critical
- 4. Select one of the following severity levels for **Link Down** events:
  - > Information
  - > Warning
  - > Critical
- 5. To trigger events when network bandwidth utilization exceeds a threshold:
  - a. Select Enabled from the first Bandwidth Utilization Over drop-down list.

Severity
Varning 🔹

b. Specify the percentage of bandwidth utilization for the threshold.

Bandwidth Utilization Over Enabled	•	
Bandwidth Utilization Over 0	Severity Warning	g 👻

- c. Select the **Severity** level for the event.
- 6. To trigger events when network bandwidth utilization falls below a threshold:
  - a. Select **Enabled** from the first **Bandwidth Utilization Under** drop-down list.

Bandwidth Utilization Under Enabled	•		
Bandwidth Utilization Under		Severity	
0		Warning	-
	%		

b. Specify the percentage of bandwidth utilization for the threshold.

Bandwidth Utilization Under Enabled	
Bandwidth Utilization Under	Seventy
0	Warning
9/	

- c. Select the **Severity** level for the event.
- 7. To trigger events when the packet error rate exceeds a threshold:
  - a. Select **Enabled** from the first **Packet Error Rate Over** drop-down list.

Packet Error Rate Over Enabled	•		
Packet Error Rate Over		Severity	
0		Warning	-
	%		 

b. Specify the packet error rate for the threshold.

Packet Error Rate Over Enabled	•	
Packet Error Rate Over	Severity	
0	Warning	g 🔻
	%	

c. Select the Severity level for the event.

- 8. To trigger events when device availability falls below a certain threshold:
  - a. Select **Enabled** from the first **Availability Under** drop-down list.

Availability Under Enabled	-		
Availability Under		Severity	
95		Warning	-
	0/4		

b. Specify the device availability level for the threshold.

Availability Under Enabled	
Availability Under	Seventy
95	Warning -
%	

- c. Select the **Severity** level for the event.
- 9. To trigger events when the SFP TX value is below a certain threshold:
  - a. Select **Enabled** from the first **SFP TX Under** drop-down list.

SFP TX Under Enabled	•		
SFP TX Under *		Severity *	
0		Warning	•
-100 - 0	dBm		

b. Specify the SFP TX threshold level.

SFP TX Under * Enabled	•		
SFP TX Under		Severity *	
-50	\$	Warning	•
-100 - 0	dBm		

- 10. To trigger events when the SFP RX value is below a certain threshold:
  - a. Select **Enabled** from the first **SFP RX Under** drop-down list.

SFP RX Under Enabled	•		
SFP RX Under *		Severity *	
0		Warning	•
-100 - 0	dBm		

b. Specify the SFP RX threshold level.

SFP RX Under *			
Enabled	•		
SFP RX Under		Severity *	
-50	\$	Warning	-
-100 - 0	dBm		

- 11. To trigger events when the SFP voltage is below a certain threshold:
  - a. Select **Enabled** from the first **SFP Voltage Under** drop-down list.

SFP Voltage Under Enabled	•		
SFP Voltage Under *		Severity *	
0		Warning	•
0 - 10	V		

b. Specify the SFP Voltage threshold level.

SFP Voltage Under *			
Enabled			
SFP Voltage Under		Severity *	
5	\$	Warning	-
0 - 10	V		

- 12. To trigger events when the SFP voltage is over a certain threshold:
  - a. Select **Enabled** from the first **SFP Voltage Over** drop-down list.

SFP Voltage Over Enabled	•		
SFP Voltage Over *		Severity *	
0		Warning	•
0 - 10	V		

b. Specify the SFP Voltage threshold level.

SFP Voltage Over *			
Enabled	•		
SFP Voltage Over *		Severity *	
5		Warning	*
0 - 10	V	·	

- 13. To trigger events when the SFP temperature is over a certain threshold:
  - a. Select Enabled from the first SFP Temperature Over drop-down list.

SFP Temperature Over Enabled	•		
SFP Temperature Over *		Severity *	
0		Warning	*
0 - 100	°C		

b. Specify the SFP Temperature threshold level.

SFP Temperature Over * Enabled	•		
SFP Temperature Over *	39 1	Severity *	
50		Warning	•
0 - 100	°C		

#### 14. Click Save.

MXview will update the event settings.

## **Notification Methods**

MXview supports email, and SNMP trap notifications for events. Each notification method requires specific server configurations.

### **Configuring Email Server Settings**

Use the Preferences screen to configure an email server to send email notifications for event notifications.

- In the Server section, expand Email Sever Setup.
   The Email Server Setup settings will appear.
- 3. Configure the following:
  - > Server Domain Name/IP
  - > Port number
  - > Encryption
  - > Username
  - > Password
  - > Sender Address
- 4. Click Save.

MXview can send email messages for configured event notifications.

## **Configuring SNMP Trap Destinations for the MXview Server**

Use the **Preferences** screen to configure the SNMP trap destination(s) for the MXview server.

- Navigate to Menu (=) > Preferences.
   The Preferences screen appears.
- In the Server section, expand SNMP Trap Server of MXview. The SNMP Trap Server of MXview settings will appear.
- 3. Configure the following:
  - > SNMP Version
  - > IP Address of Trap Server 1
  - Community of Trap Server 1
  - > IP Address of Trap Server 2
  - > Community of Trap Server 2
- 4. Click Save.

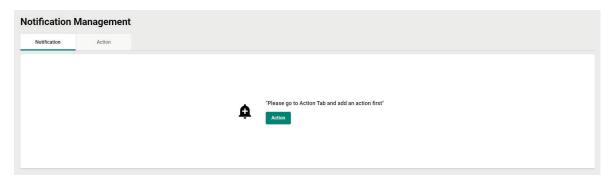
### **Configuring the SNMP Trap Destination for Devices**

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.

- Navigate to Menu (=) > Preferences.
   The Preferences screen will appear.
- In the Server section, expand SNMP Trap Server of Device. The SNMP Trap Server of Device settings will appear.
- 3. Configure the following:
  - > Destination IP1: Specify the IP address of the MXview server
  - > Community Name1: Specify the community string of the MXview server
- 4. Click Save.

## **Notification Management**

The **Notification Management** screen allows you to configure event notifications by issuing a registered action (e.g., sending an email message to a specified recipient) when configured events are detected on your network.



## **Configuring New Event Notifications**

MXview event notifications require at least one registered action (e.g., sending an email message to a specified recipient), which MXview performs when a specified event is detected on your network.

- 1. Navigate to Menu (=) > Event > Notification Management.
- The Notification Management screen appears.
- 2. To register an action:
  - a. Click the **Action** tab.

The Action tab displays a list of registered actions (if any).

Notification Management			
Notification Action			
		Q Search	
Action Name	Туре	Action Information	
🗆 🖍 📋 Test	E-mail	email@example.com	
			1 – 1 of 1

b. Click the **Add** ( $\blacksquare$ ) icon in the top right corner.

The <b>Add</b>	notification	action	screen	will	appear.

Add notifica	tion action		
Action Name *			
Type *	•		
Action Informa	tion *		
		Cancel	Add

- c. In the Action Name field, type a name to describe the action.
- d. From the  $\ensuremath{\textbf{Type}}$  drop-down list, select one of the following actions:
  - **E-mail:** Sends an email message to the specified email address
  - **Sound File:** Plays the uploaded sound file
  - Message Box: Displays a message box when the event occurs SNMP Trap: Sends an SNMP trap
  - □ Slack: Send a message to Slack
  - □ Microsoft Teams: Send a message to Microsoft Teams
- e. Provide additional information required for the action (if any).
- f. Click Apply.

The registered action appears in the table on the **Action** tab.

- 3. To add a new event notification:
  - a. Click the Notification tab.

The **Notification** tab displays a list of configured event notifications (if any).

Notification	n Management					
Notification	Action					
• •				Q Search		
	Notification Name	Туре	Registered Devices		Registered Actions	
	Test	Device ICMP unreachable	2		Test;	
						1 - 1 of 1

b. Click the Add (<sup>1</sup>/<sub>1</sub>) icon in the top right corner.
 The Add notification screen appears.

Add notification	
Notification Name *	
Type *	•
Registered Devices * 👻	
Registered Actions * 👻	
	Cancel Add

- c. In the Notification Name field, type a name to describe the event notification.
- d. From the Type drop-down list, select the event type.
- e. From the Registered devices drop-down list, select the network device(s) you want to monitor.
- f. From the **Registered Actions** drop-down list, select the action that MXview performs when the specified event is detected on the previously selected device(s).

#### g. Click Apply.

The event notification appears in the table on the **Notification** tab.

### Add a Slack/Teams Notification

Use the Action tab on the Notification Management screen to Add a Slack/Teams action

To Create a Slack Notification please perform the following steps:

Add notification action		
Action Name		
Slack		
Туре		
Slack		
Webhook	Test Connection	
	Cancel	Add

- 1. Create a Webhook on Slack
- 2. Install Incoming Webhook on Slack
- 3. Select the channel that you want to post to

4. Generate a Slack Webhook

### Integration Settings

#### Post to Channel

Messages that are sent to the incoming webhook will be posted here.

• Tanis Yukai Tseng

or create a new channel

~

#### Webhook URL

Send your JSON payloads to this URL. Show setup instructions

https://hooks.slack.com/services/T69C5LR5E/B0160KNTNAV/poHjaV48PXvd0z

Copy URL • Regenerate

#### 5. Copy the Webhook URL to MXview

Add notification action		
Action Name Slack		
Type Slack		
Webhook		
https://hooks.slack.com/services/T69C	Test Connection	
	Canaal	Add

You can click **Test Connection** to check whether the webhook works.



MXview connection test

To create a Microsoft Teams notification please perform the following steps:

 Create a Webhook on Microsoft Teams. <u>https://docs.microsoft.com/en-</u> us/microsoftteams/platform/webhooks-and-connectors/how-to/add-incoming-webhook

Apps		
inc	Q	Microsoft Corporation
All		The Incoming Webhook connector enables external services to notify you about activities
Personal apps		that you want to track.
Bots		

- 2. Select Connector

  - 公 Pin
  - 🚿 Hide
  - Manage channel
  - 🖂 Get email address
  - Cet link to channel
  - 🖉 Edit this channel
  - 싶다 Connectors
  - 前 Delete this channel
- 3. Configure the Incoming Webhook and click Create

### Connectors for "MXview Notification Testing" channel in "NSD Team" team



Send feedback

The Incoming Webhook connector enables external services to notify you about activities that you want to track. To use this connector, you'll need to create certain settings on the other service, which needs to support a webhook that's compatible with the Office 365 connector format.

#### Fields marked with \* are mandatory

To set up an Incoming Webhook, provide a name and select Create. \*

MXview Notification

Customize the image to associate with the data from this Incoming Webhook.



Copy the URL below to save it to the clipboard, then select Save. You'll need this URL when you go to the service that you want to send data to your group.



4. Copy the Webhook URL to MXview

You can click Test Connection to check whether the webhook works.

2	MXview Notification 10:53 AM
96	MXview connection test
	← Reply

### **Editing or Exporting Registered Actions**

Use the **Action** tab on the **Notification Management** screen to edit registered actions or export a CSV file containing registered action information.

- Navigate to Menu (=) > Event > Notification Management. The Notification Management screen will appear.
- 2. Click the **Action** tab.

The **Action** tab displays a list of registered actions.

- 3. To edit a registered action:
  - a. Click the Edit ( ) icon next to the action you want to edit.
     The Edit notification action screen will appear.

Edit notificati	on action		
Action Name *			
Test			
Type *			
E-mail	•		
Receiver Email *			
email@example.	com		

- b. Modify the following settings:
  - Action Name
  - 🗆 Туре
  - □ Action information
- c. Click Apply.
  - The **Action** tab appears and displays the updated action information.
- 4. To export data displayed on the Action tab:
  - a. Click the **Export** ( ) icon.



- b. Select Export CSV.
- c. Specify the location to save the exported file.
- d. Click Save. MXview exports the displayed event data as a CSV file.

## **Editing or Exporting Notification Configurations**

Use the **Notification** tab on the **Notification Management** screen to edit configured notifications or export a CSV file containing notification configuration information.

- Navigate to Menu (=) > Event > Notification Management. The Notification Management screen will appear.
- 2. Click the **Notification** tab.

The Notification tab displays a list of configured notifications.

- 3. To edit a notification:
  - a. Click the Edit (
    ) icon next to the action you want to edit. The Edit notification screen will appear.

Edit notification

Notification Name	
Test	
Туре	
Device ICMP unreachable	-
Registered devices	
192.168.127.1, 192.168.127.2, 192.168.127.3	3 ▼
Desistered Advises	
Registered Actions	
Test	

el Apply

- b. Modify the following settings:
  - Notification Name
  - 🗆 Туре
  - □ Registered devices
  - Registered Actions
- c. Click Apply.

The **Notification** tab appears and displays the updated notification information.

- 4. To export data displayed on the **Action** tab:
  - a. Click the **Export** ( ) icon.

٠		
	Export CSV	2

- b. Select **Export CSV**.
- c. Specify the location to save the exported file.
- d. Click Save.

MXview exports the displayed event data as a CSV file.

## **Custom Event Management**

The **Custom Events** screen provides information about all the custom events configured on MXview. You can use the **Custom Events** screen to view whether a custom event is enabled or disabled, modify a custom event, or export custom event configurations as a CSV file.

II (2)	<b>H</b> .						Q Search		
Critical (2)		Event Name	Enabled/Disabled	Condition	Description	Recovery Description	Duration	Registered Devices	
Varning (0)		powerConsumption	Enabled	Over 10	Test 10.81.10.10		0	1	
nformation (0)		portEnable.11	Enabled	Over 10	Flapping	Flapping	10	2	

### **Configuring Custom Events**

The Custom Events screen allows you to define your own events to monitor with flexible detection thresholds, severity levels, and duration times. You can also export the custom event configurations as a CSV file.

Custom Even	ts Managen	nent									
All (0)	<b>=</b> 0							QS	earch		
Critical (0) Warning (0)		Event Name	Enabled/Disabled	Condition	Description	Recovery D	escription	Duration	Registered Devices		
Information (0)										0 of	fO

- Navigate to Menu (=) > Event > Custom Events Management. The Custom Events screen appears.
- Click the Add (1) button in the upper-right corner of the screen. The Add custom event screen will appear.

Enable Custom Event			
Enabled	•		
Severity	•		
Device Properties *			
Condition operator	*	Condition Value	-
Description			
07	250		
Recovery Description			
0 / . Duration	250		
0			

- 3. Select the default event status:
  - > **Enabled:** MXview monitors the event
  - > Disabled: MXview does not monitor the event
- 4. Select one of the following severity levels for the event:
  - > Information
  - > Critical
  - > Warning
  - > System Information
- 5. Click the Device Properties and select the device property to monitor.
- 6. Configure the following threshold criteria:
  - > Condition operator: Select the criteria operator for matching the condition value
  - > Condition value: Specify the value for the criteria operator to match
- 7. (Optional) In the **Description** field, type a string (up to 250 characters in length) to describe the custom monitoring.
- 8. (Optional) In the **Recovery Description** field, type a string (up to 250 characters in length) to describe how to recover from the event.
- 9. In the **Duration** field, specify the number of consecutive pollings for the event.
- 10. From the Register Devices drop-down list, select the devices to monitor for the custom event.
- 11. Click Apply.

The custom event appears in the table on the **Notification** tab.

### **Viewing or Exporting Custom Event Settings**

The **Custom Events** screen provides information about all the custom events configured on MXview. You can use the **Custom Events** screen to view whether a custom event is enabled or disabled, modify a custom event, or export custom event configurations as a CSV file.

(2)	+ •						Q Search		
ritical (2)		Event Name	Enabled/Disabled	Condition	Description	Recovery Description	Duration	Registered Devices	
arning (0)		powerConsumption	Enabled	Over 10	Test 10.81.10.10		0	1	
formation (0)		portEnable.11	Enabled	Over 10	Flapping	Flapping	10	2	

#### 1. Navigate to Menu (≡) > Event > Custom Events Management.

The **Custom Events** screen will appear and displays the following information in a table format:

Column	Description
Event Name	The name of the event
Enabled/Disabled	The monitoring status of the event
Condition	The threshold criteria configured for the event
Description	The description of the event
Recovery Description	The recovery description of the event
Duration	The number of consecutive pollings for the event
Registered Devices	The number or registered devices that the event applies to

2. To filter the information in the table, type a full or partial string that matches the value in any of the table columns.

MXview filters the table to only display events with values that fully or partially match the specified string.

3. To filter the information in the table by event severity, click one of the color-coded severity levels in the left-side panel.



MXview filters the table to only display events that match the selected severity level.

- To sort the data in the table by a specific column, click the column heading. MXview sorts the table by the column.
- 5. To export data displayed on the **All Events** screen:
  - a. Click the **Export** ( ) icon.



- b. Select Export CSV.
- c. Specify the location to save the exported file.
- d. Click Save.

MXview exports the displayed event data as a CSV file.

## **Enabling/Disabling or Editing Custom Events**

To enable or disable a custom event, edit the custom event settings.

- Navigate to Menu (=) > Event > Custom Events Management. The Custom Events screen appears.
- Click the Edit (
   ) icon next to the event you want to enable/disable.

   The Update custom event screen appears.

Condition Value 1.2.3.4	_	
	_	
	_	
	_	
	_	
1 2 2 /		
1.2.3.4	-	
		Cancel

- 3. From the Enable Custom Event drop-down list, select one of the following:
  - > Enabled
  - > Disabled
- 4. Modify any additional event settings you wish to change.
- Click Apply.
   The Custom Events screen will appear and displays the updated event information.

MXview provides reports that summarize key information about your VLAN configuration, network devices, and device availability.

## **Viewing VLAN Reports**

Use the **VLAN** report screen to view information about the VLAN configuration on your network. You can also export the report as a CSV file or a PDF file.

VI	

•						Q Search	
Site Name	Device IP	Model	VLAN ID	Access Ports	Trunk Ports	Hybrid Ports	Management VLAN
lient-generic	10.82.10.1	IKS-G6824A-4GTXSFP	1	2,3,4,5,6,7,9,10,11,12,13,16,17,18,19,20,21,22,2	4	14	Yes
client-generic	10.82.10.1	IKS-G6824A-4GTXSFP	8	8,23		14,15	No
client-generic	10.82.10.1	IKS-G6824A-4GTXSFP	10	1		14,15	No
client-generic	10.82.10.4	IKS-G6824A-4GTXSFP	1	2,3,4,5,6,7,8,9,10,11,12,13,16,17,18,19,20,21,22 4	2	14	Yes
client-generic	10.82.10.4	IKS-G6824A-4GTXSFP	8	23		14,15	No
client-generic	10.82.10.4	IKS-G6824A-4GTXSFP	10		1	14,15	No
client-generic	10.81.10.10	EDS-510E-3GTXSFP	1	1,2,3,4,5,6,7,8,9,10			Yes
client-generic	10.81.10.11	EDS-510E-3GTXSFP	1	1,2,3,4,5,6,7,8,9,10			Yes
client-generic	10.81.10.12	EDS-510E-3GTXSFP	1	1,2,3,4,5,6,7,8,9,10			Yes

### 1. Navigate to Menu (≡) > Reports > VLAN Report.

The VLAN report screen will appear and display the following information in a table format:

Column	Description
Site Name	The site that the VLAN device belongs to
Device IP	The IP address of the VLAN device
Model	The model number of the VLAN device
VLAN ID	The VLAN ID of the device
Access Ports	The access ports on the VLAN device
Trunk Ports	The trunk ports on the VLAN device
Management VLAN	The management status of the VLAN device
Hybrid Ports	The hybrid ports on the VLAN device

2. To filter the information in the table, type a full or partial string that matches the value in any of the table columns.

MXview filters the table to only display results that fully or partially match the specified string.

3. To sort the data in the table by a specific column, click the column heading.

MXview sorts the table by the column.

- 4. To export the report data:
  - a. Click the **Export** ( ) icon.
  - b. Select one of the following report formats:
    - □ Export CSV
    - Export PDF
  - c. Specify the location to save the exported file.
  - d. Click Save.

MXview exports the report data in the selected format.

# **Viewing Inventory Reports**

Use the **Inventory Report** screen to view information about the devices on your network. You can also export the report as a CSV file or a PDF file.

#### **Inventory Report**

					Q Search	
Site Name	IP Address	Alias	Model	MAC Address	System Description	Firmware Version
client-generic	10.82.10.1	IKS-G6824A	IKS-G6824A	00:90:E8:7D:A7:1F	IKS-G6824A-4GTXSFP	V5.7 build 20011715
client-generic	10.82.10.2	EDR-G903	EDR-G903	00:90:E8:84:6E:80	Unknown	
client-generic	10.82.10.3	EDR-G903	EDR-G903	00:90:E8:00:00:02		
client-generic	10.82.10.4	IKS-G6824A	IKS-G6824A	00:90:E8:7D:A7:12	IKS-G6824A-4GTXSFP	V5.7 build 20011715
client-generic	10.81.10.10	EDS-510E	EDS-510E	00:90:E8:86:2F:12	EDS-510E-3GTXSFP	V5.4 build 21042021
client-generic	10.81.10.11	EDS-510E	EDS-510E	00:90:E8:86:2F:15	EDS-510E-3GTXSFP	V5.4 build 21042021
client-generic	10.81.10.12	EDS-510E	EDS-510E	00:90:E8:86:2E:F3	EDS-510E-3GTXSFP	V5.4 build 21042021
client-generic	10.81.10.13	EDS-510E	EDS-510E	00:90:E8:86:2F:17	EDS-510E-3GTXSFP	V5.4 build 21042021

#### 1. Navigate to Menu (≡) > Reports > Inventory Report.

The Inventory Report screen appears and displays the following information in a table format:

Column	Description
Site Name	The site that the device belongs to
IP Address	The IP address of the device
Alias	The unique name of the device
Model	The model number of the device
MAC Address	The MAC address of the device
System Description	The description of the device

2. To filter the information in the table, type a full or partial string that matches the value in any of the table columns.

MXview filters the table to only display results that fully or partially match the specified string.

3. To sort the data in the table by a specific column, click the column heading.

MXview sorts the table by the column.

- 4. To export the report data:
  - a. Click the **Export** ( ) icon.
  - b. Select one of the following report formats:
    - Export CSV
    - Export PDF
  - c. Specify the location to save the exported file.
  - d. Click Save.

MXview exports the report data in the selected format.

## **Viewing Availability Reports**

Use the **Availability Report** screen to view information about the device availability on your network. You can also export the report as a CSV file or a PDF file.

ailability Rep	oort					
					C	<b>2</b> Search
Site Name	Device Alias	Start Date	End Date	Average Availability	Worst Availability	Days
client-generic	IKS-G6824A	2021-12-27	2021-12-27	100%	100%	1
client-generic	EDS-408A	2021-12-27	2021-12-27	100%	100%	1
client-generic	EDS-408A	2021-12-27	2021-12-27	100%	100%	1
client-generic	EDS-408A	2021-12-27	2021-12-27	100%	100%	1
client-generic	EDR-G903	2021-12-27	2021-12-27	100%	100%	1
client-generic	EDS-510E	2021-12-27	2021-12-27	100%	100%	1
client-generic	EDS-510E	2021-12-27	2021-12-27	100%	100%	1

#### 1. Navigate to **Menu** (≡) > **Reports** > **Availability Report**.

The **Availability Report** screen appears and displays the following information in a table format:

Column	Description
Site Name	The site that the device belongs to
Device Alias	The unique name of the device
Start Date	The start date for the device availability report
End Date	The end date for the device availability report
Average Availability	The average device availability from the start date to the end date
Worst Availability	The worst device availability from the start date to the end date
Days	The number of days used to calculate device availability

2. To filter the information in the table, type a full or partial string that matches the value in any of the table columns.

MXview filters the table to only display results that fully or partially match the specified string.

- 3. To change the date range for the report:
  - a. Click the **Filter**  $(\overline{-})$  icon in the top right corner.

The **Query Date** screen appears.

Cancel Apply

- b. Select the Start Date.
- c. Select the End Date.
- d. Click Apply.

MXview filters the table to only display device availability for the specified data range.

4. To sort the data in the table by a specific column, click the column heading.

- MXview will sort the table by the column.
- 5. To export the report data:
  - a. Click the **Export** (🗳) icon.
  - b. Select one of the following report formats:
    - □ Export CSV
    - □ Export PDF
  - c. Specify the location to save the exported file.
  - d. Click Save.

MXview will export the report data in the selected format.

The MXview web console provides several features to assist database backups and device configuration migrations. MXview allows you to back up or restore configurations for multiple devices, and also compare changes between different versions of archived configuration files. You can also create scheduled jobs to automatically export/import device configurations or back up the MXview database.

## **Backing Up the MXview Database**

Use the Database Backup screen to back up the MXview database and configuration files.

- Navigate to Menu (≡) > Migrations > Database Backup. The Database Backup screen appears.
- In the Name field, specify the directory to where MXview exports the database backup and configuration files.

Default directory: %MXviewPro\_Data%\db\_backup

3. Click Apply.

A popup message appears indicating that the database has been backed up.

## **Backing Up Device Configurations**

Use the **Configuration Center** screen to export configuration backup files from one or more devices.

- Navigate to Menu (≡) > Migrations > Configuration Center. The Configuration Center screen appears.
- 2. Click the **Backup** tab.

Available devices will appear in the **Device List**.

Configu	ration Ce	enter			
Backu	þ	Restore	Records		
Device Lis	t				
					Q Search
	IP Address	Alias Name		Group	·
	10.81.10.10	EDS-510E		Root	
	10.81.10.11	EDS-510E		Root	
	10.81.10.12	EDS-510E		Root	
	10.81.10.13	EDS-510E		Root	
	10.81.10.14	EDR-810		Root	
	10.81.10.15	EDS-510E		Root	

- 3. (Optional) Filter the devices in the Device List:
  - a. Click the **Filter** (=) icon.
  - b. Specify any of the following criteria:
    - **Group:** The group in the MXview tree structure that the device is assigned to
    - IP Address: The IP address of the device
  - c. Click Apply.

MXview filters the **Device List** according to the specified criteria.

- 4. To export the device list from all available devices:
  - a. Click the **Export** ( ) icon.



- b. Select Export CSV.
- c. Click Save.
  - MXview exports configurations from all available devices as a CSV file.
- 5. To back up configurations from specific devices:
  - a. Select the check box next to the device(s) you want to back up.
  - b. Click the **Backup** (**b**) icon in either of the following locations:
    - □ For a single device, click the **Backup** (**b**) next to the selected device.
    - $\Box$  For multiple devices, click the **Backup** ( $\Box$ ) icon in the upper left corner of the screen.

The **Backup Configuration** screen appears.

Bac	kup	Restore	Records			
Device L	ist					
	IP Address	Alias Name		Backup Configuration		
	10.81.10.10	EDS-510E		MXview will archive these configuration files		
	10.81.10.11	EDS-510E		10.81.10.10		
	10.81.10.12	EDS-510E		10.01.10.11		
	10.81.10.13	EDS-510E			Cancel	Save
	10.81.10.14	EDR-810		Koot		
	-					

c. Click Save.

MXview archives configuration files from selected device(s) to the MXview server and displays them in the **Records** tab. Also, MXview will export configurations from the selected device(s) as a ZIP file. For more information, please see the following topics:

for more mornation, piease see the following top

Comparing Archived Configuration Files

### NOTE

If MXview compares two configuration files and they are the same, it will only leave the latest one. If the two configuration files are different, MXview will keep both in the **Records** tab.

# **Restoring Device Configurations**

Use the **Configuration Center** screen to restore configurations to one or more devices by restoring an archived configuration from the MXview server or importing a local configuration backup file (in INI format).



### NOTE

Restoring archived device configurations requires archiving device configurations to the MXview server. For more information, see **Archiving Device Configurations to the MXview Server**.

- Navigate to Menu (=) > Migrations > Configuration Center. The Configuration Center screen will appear.
- 2. Click the **Restore** tab.

Available devices will appear in the **Device List**.

Confi	guration	Center			
В	ackup	Restore	Records		
Device					Q, Search
	8				Q Search
	IP Address	Alias Name		Group	
Ð	10.81.10.10	EDS-510E		Root	
Ð	10.81.10.11	EDS-510E		Root	
Ð	10.81.10.12	EDS-510E		Root	
Ð	10.81.10.13	EDS-510E		Root	
Ð	10.81.10.14	EDR-810		Root	
0	10.81.10.15	EDS-510E		Root	

- 3. (Optional) Filter the devices in the **Device List**:
  - a. Click the **Filter**  $(\overline{-})$  icon.
  - b. Specify any of the following criteria:
    - **Group:** The group that the device is assigned to
    - □ IP Address: The IP address of the device
  - c. Click Apply.

MXview filters the **Device List** according to the specified criteria.

- 4. (Optional) Export configurations from all available devices:
  - a. Click the **Export** ( ) icon.

Ð		
	Export CSV	þ

b. Select Export CSV.

MXview exports configurations from all devices as a CSV file.

- 5. To restore an archived configuration file to a device:
  - a. Click the **Restore**  $(\mathfrak{S})$  icon next to the **IP Address** of a device in the **Device List**.

The **Restore Configuration** screen will appear.

<b>Restore Configuration</b>		
Restore Device - 10.81.10.11		
Restore Configuration	•	
	Cancel	Apply

b. From the **Restore Configuration** drop-down list, select the archived device configuration to restore.

	Restore Configuration			
	Restore Device - 10.81.10.11 Device Conferencies Local File			
	10.82.10.3_20210805_2223.ini		-	
	10.82.10.3_20210805_2304.ini	Ap	oply	
nc tc	10.82.10.3_20210806_1109.ini			
ot_	10.81.10.11_20200722_1722.ini	•		

c. Click Apply.

Restore Configuration	
Restore Device - 10.81.10.11 Restore Configuration	
10.81.10.11_20200722_1722.ini	
Createing Time: 2021-09-22 10:10:00 Last Checking Time: 2020-11-26 10:47:	00
Cancel	Apply

MXview imports the configuration file to the selected device.

- 6. To import a local configuration file to a device:
  - a. Click the Restore  $(\mathfrak{G})$  icon next to the IP Address of a device in the Device List.

The **Restore Configuration** screen appears.

<b>Restore Configuration</b>		
Restore Device - 10.81.10.11		
Restore Configuration	•	
	Cancel	Apply

b. From the Restore Configuration drop-down list, select Local File.

c. Click Configuration File field to a select the configuration file.

Restore Configuration		
Restore Device - 10.81.10.11 Restore Configuration		
Local File	•	
Configuration File		
	Cancel	Apply

- d. Select the configuration file to import and click Open.
- e. Click Apply.

Restore Configuration		
Restore Device - 10.81.10.11 Restore Configuration		
Local File	•	
Configuration File		
10.81.10.11.ini		
	Cancel	Apply

MXview imports the configuration file to the selected device.

## **Comparing Archived Configuration Files**

Use the MXview Configuration Center to compare changes in the history of saved configuration files.

- Navigate to Menu (=) > Migrations > Configuration Center. The Configuration Center screen appears.
  - The configuration center screen appe
- 2. Click the **Records** tab.

A list of archived backup configuration files appears.

Backup	Restore	Records				
nfiguratio	on File					
<b>⊽ ⊡</b>				Q Search		
	Configuration File	Createing Time	Last Checking Time			
i 6	10.82.10.3_20210805_2223.ini	2021-09-22 10:1	0:00 2021-08-05 22:23:00			
16	10.82.10.3_20210805_2304.ini	2021-09-22 10:1	0:00 2021-08-05 23:04:00			
16	10.82.10.3_20210806_1109.ini	2021-09-22 10:1	0:00 2021-08-06 11:09:00			
16	10.81.10.11_20200722_1722.ini	2021-09-22 10:1	0:00 2020-11-26 10:47:00			
16	10.81.10.11_20210409_1812.ini	2021-09-22 10:1	0:00 2021-04-09 18:12:00			
16	10.81.10.12_20201211_1508.ini	2021-09-22 10:1	0:00 2020-12-11 15:08:00			
16	10.81.10.12_20210409_1812.ini	2021-09-22 10:1	0:00 2021-08-05 23:04:00			
16	10.85.10.20_20201215_1342.ini	2021-09-22 10:1	0:00 2020-12-15 13:42:00			
8 1	10.85.10.30_20201215_1358.ini	2021-09-22 10:1	0:00 2021-04-09 18:13:00			

- 3. (Optional) Filter the list of configuration files:
  - a. Click the **Filter** ( $\overline{-}$ ) icon.
  - b. Specify any of the following criteria:
    - **Group:** The group that the device is assigned to
    - **Start Date:** The earliest file creation date
    - **Start Time:** The earliest file creation time on the Start Date
    - **End Date:** The latest file creation or update date
    - **End Time:** The latest file creation or update time on the End Date

c. Click Apply.

- 4. (Optional) Export configurations from all available devices:
  - a. Click the **Export** ( ) icon.



b. Select Export CSV.

MXview exports configurations from all devices as a CSV file.

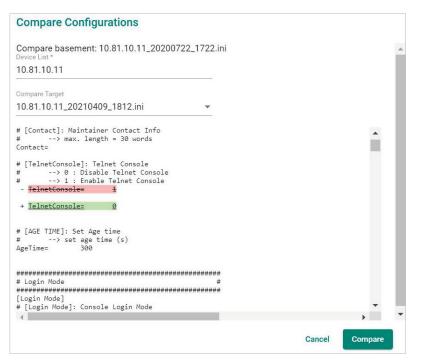
5. Click the **Compare** ( $\blacksquare$ ) icon next to the configuration file you want to compare.

### The Compare Configurations screen will appear.

Compare Configurations				
Compare basement: 192.168.127.1_20181124_ Device List	1752.ini			
192.168.127.1IKS-6726A				
192.168.127.2IKS-6728A-8POE				
192.168.127.3EDS-G516E		Cancel	Compare	0
192.168.127.4EDS-G516E	-24 22:18:00		2018-11-24 22:58	3:00

- 6. Select the device from the Device List drop-down list.
- 7. Select the target configuration file to compare from the **Compare Target** drop-down list.
- 8. Click Compare.

MXview will display a comparison of the selected configuration files.



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

### NOTE

The green lines are the configurations of Compare Target. The red lines are the configurations of Compare basement.

# Creating Scheduled Jobs for Database/Configuration Backups

Use the MXview Job Scheduler to automatically export/import device configurations or back up the MXview database on a predefined schedule.

- Navigate to Menu (≡) > Migrations > Job Scheduler. The Job Scheduler screen appears.
- (Optional) Locate a previously saved scheduled job, type a job name in the search box. The **Job Scheduler** table displays a list of matching scheduled jobs.
- 3. Click the **Add** (**±**) button.
  - The Add new job screen appears.
- 4. Specify the Job Name.
- 5. Select one of the following options from the Action drop-down box:
  - > Export Configuration
  - > Import Configuration
  - > Database Backup
- 6. Type a **Description** for the job.
- 7. Select the **Registered Devices** that apply.
- 8. Select a job frequency from the **Repeat Execution** drop-down box:
  - > Once
  - > Daily
  - > Weekly
  - > Monthly

- 9. Specify the **Start Date** to begin executing the scheduled job.
- 10. Specify the **Execution Time** on the Start Date to run the scheduled job.
- 11. Click Apply.

MXview will display the scheduled job on the **Job Scheduler** table and will execute the job according the defined schedule.

MXview supports several features that enable integration with third-party applications or external systems.

## **Managing API Keys**

MXview supports several RESTful APIs for custom integrations with third-party products. Use the **API Key Management** screen to add new applications and generate API keys.

1. Navigate to Menu (≡) > Integration > RESTful API Management.

The API Key Management screen will appear.

Ŧ				Q Search	
Application Name	Create Time	Access Count	API Key		
test	2021-10-28 10:20:10	183	eyJhbGciOiJIUz11NiIsInR5cCl6lkpXVCJ9.eyJ1c2VybmFtZSl6lnRyeW14dmlldylsImlhdCl6MTY zNTM4NzYxMCwianRpljoiNWEyN2E4ZGY2Y2NiYjZhOGY1ZjkwN2JIOTIiMGVkYTUyYWYyZWQ		
	2021-10-26 10.20.10	103	4MiJ9.i9ZVczIAoES0o1IrD7bmwSv1LJXhp17JAr8YDz5Q0uA		

- (Optional) Filter the list of applications, type a string in the search box.
   MXview filters the list of applications to display only the applications that contain full or partial matching strings.
- 3. To add a new application:
  - a. Click the Add (<sup>1</sup>/<sub>1</sub>) icon in the top right corner of the screen.
     The Add new token screen will appear.

Add new token		
Application Name *		
	Cancel	Add

- b. Specify an Application Name.
- c. Click Apply.

MXview will add the new application to the **API Key Management** screen and display the generated API key.

- 4. To regenerate an API key for an existing application:
  - a. Select the check box next to the **Application Name**.

The **Regenerate the API Key**  $( {}^{\textcircled{O}} )$  icon will appear in the top right corner of the screen.

Ĩ	C				Q Search	
	Application Name	Create Time	Access Count	API Key		
2	test	2021-10-28 10:20:10	183	eyJhbGciOiJIUz1NiIsInR5cCl6lkpXVCJ9.eyJ1c2VybmFtZSI6inRyeW14dmlldyIsImlhdCl6MTY zNTM4NzYxMCwianRpIjoiNWEyN2E4ZGY2Y2NiYjZhOGY1ZjkwN2JOTIMGVI:YTUyYWYyZWQ 4MiJ9.i9ZVczIAoES0o1HD7bmwSy1LJXhp17JAr8YDzSQ0uA		

b. Click the **Regenerate the API Key**  $(\mathfrak{G})$  icon.

MXview will regenerate the API key for the selected application.

## NOTE

Regenerating the API key will prevent any APIs that use the old API key from working properly.

- 5. To delete an application:
  - a. Select the check box next to the Application Name.
  - b. Click the **Delete** (<sup>1</sup>) icon in the top left corner of the screen.
     MXview will delete the application.

### NOTE

Deleting the application will prevent any APIs that use the old API key from working properly.

6. To view API reference documentation, navigate to **Menu** (≡) > **Integration** > **API Reference**. The **MXview API** screen will appear and display the reference document for supported MXview APIs.

MXview API 🚥 🚥	
A document of API for accessing data from MXview	
API user guide	
Servers https://127.0.0.1/ ~	Authorize 🔒
Resource	~
GET /resources/icons/url/{url} Get device icon	
GET /resources/icons/{url} Get the icon of a site	
GET /resources/panel_images/url/{url} Get the panel image of a device	
GET /resources/panel_descriptions/url/{url} Get device panel description file	

## **Embedding Web Widgets**

MXview allows you embed the Topology Map and Recent Events widgets from the MXview **Network Topology** screen in third-party applications.

- Navigate to Menu ( =) > Integration > Embedded Web Widget. The Embedded Widget screen will appear.
- 2. From the **Select API Key** drop-down list, select the **Application Name** for the API key you want to use.

### Select API key

Demo	•

- 3. From the **Select Layout** drop-down list, select the widget(s) you want to embed:
  - Topology and recent events: Embeds both the Topology Map and Recent Events widgets in the target application
  - > **Topology:** Embeds only the Topology Map in the target application
  - > **Recent event:** Embeds only the Recent Events widget in the target application
- 4. Copy and paste the widget link for the target application:
  - > To embed the widget in a web application, click the **Copy link** ( $\Box$ ) icon in the **Link** section.

Embed

Link http://127.0.0.1/#/widget? token=eyJhbGciOiJIUzI1NilsInR5cCl6lkpXVC J9.eyJ1c2VybmFtZSl6lmFkbWluliwiaWF0ljox NTQyMTczODYzLCJqdGkiOilzMzFIZjQ2ZDQ 3NjI0ZDc2MjViMDM4ZjVhODRjNzAzMzBhY mI0YzgzIn0.FoxRT2wxtsm\_75QXFOnacD-0PB6lzUSInS\_wUsrPFnk&layout=2&top=1&b ottom=2

Paste this into any HTML page

<iristication </tr>

<iframe id="mxview-topology"</td>

src="http://127.0.0.1/#/widget?

token=eyJhbGciOiJIUzI1NiIsInR5cCl6lkpXVC

J9.eyJ1c2VybmFtZSl6lmFkbWluliwiaWF0ljox

NTQyMTczODYzLCJqdGkiOilzMzFlZjQ2ZDQ

3NjI0ZDc2MjViMDM4ZjVhODRjNzAzMzBhY

ml0YzgzIn0.FoxRT2wxtsm\_75QXFOnacD

0PB6lzUSInS\_wUsrPFnk&layout=2&top=1&b

ottom=2" frameborder="0" scrolling="0"

style="border-radius: 2px; box-shadow:

rgba(0, 0, 0, 0.12) 0px 0px 2px 0px, rgba(0, 0, 0, 0.24) 0px 2px 2px 0px; width: 600px;

height: 600px;">

➤ To embed the link in a static HTML page, click the Copy link (<sup>1</sup>) icon in the Paste this into any HTML page section.

#### Embed

Link

http://127.0.0.1/#/widget? token=eyJhbGciOiJIUzI1NiIsInR5cCl6IkpXVC J9.eyJ1c2VybmFtZSl6ImFkbWluliwiaWF0Ijox NTQyMTczODYzLCJqdGkiOiIzMzFIZjQ2ZDQ 3NjI0ZDc2MjViMDM4ZjVhODRjNzAzMzBhY mI0YzgzIn0.FoxRT2wxtsm\_75QXFOnacD-0PB6IzUSInS\_wUsrPFnk&layout=2&top=1&b ottom=2

Paste this into any HTML page

<iframe <="" id="mxview-topology" th=""><th></th></iframe>	
src="http://127.0.0.1/#/widget?	
	10
token=eyJhbGciOiJIUzI1NiIsInR5cCl6lkpXV	
J9.eyJ1c2VybmFtZSl6ImFkbWluliwiaWF0ljc	x
NTQyMTczÓDYzLCJqdGkiOilzMzFlZjQ2ZĎ	Q
3Njl0ZDc2MjViMDM4ŻjVhODRjNzAzMzBh	
mlÓYzgzIn0.FoxRT2wxtsm 75QXFOnacD-	
0PB6lzUSInS wUsrPFnk&layout=2⊤=18	b
ottom=2" frameborder="0" scrolling="0"	
style="border-radius: 2px; box-shadow:	
rgba(0, 0, 0, 0.12) 0px 0px 2px 0px, rgba(0,	0.
0, 0.24) Opx 2px 2px 0px; width: 600px;	
height: 600px;">	Ē

# **Generating OPC Tags**

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.

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

- A **Health** tag, which represents the health status of whole network.
- Device IP address, MAC address, and status, which are labeled beginning with D\_.
- A link's corresponding IP address and ports, which are labeled beginning with L\_.

### ΝΟΤΕ

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.

In addition to the default OPC tags, MXview allows you to add custom OPC tags for supported SNMP device properties.

- 1. To enable the OPC server and start generating default OPC tags:
  - a. Navigate to **Menu** (<sup>□</sup>) > **Preferences**. The **Preferences** screen will appear.
  - b. In the Server section, expand OPC Server Configuration.

The **OPC Server Configuration** settings will appear.

erver		
Syslog Server Configuration		
EMail Server Setup		
SMS Setting		
OPC Server Configuration	<i>€</i>	
Enable		
Enabled -		

c. From the **Enable** drop-down list, select **Enabled**.

#### d. Click Save.

MXview will enable the OPC server and start generating default OPC tags.

- 2. To add custom OPC tags:
  - a. Navigate to Menu (=) > Integration > Custom OPC Tags.
     The Custom OPC Tags screen will appear.

Custom OPC Tags			
All (0)	+ •		Q Search
Enabled (0)	Property Name	Enabled/Disabled Registered Devices	
Disabled (0)			0 of 0 < >

 b. Click the Add (1) icon in the top right corner. The Add custom OPC tags screen will appear.

Add custom OPC tags		
Enabled Custom OPC Tags *		
Device Properties *		
Registered Devices *		
	Cancel	Add

- c. Configure the following:
  - **Enabled Custom OPC tags:** Select to enable to disable the custom OPC tags
  - **Device Properties:** Select the SNMP properties to generate custom OPC tags
  - **Registered Devices:** Select the devices to implement the custom OPC tags
- d. Click Add.

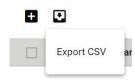
MXview creates custom OPC tags for the selected SNMP device properties.

- 3. (Optional) Filter the list of custom OPC tags displayed in the table:
  - Use the search box to type a full or partial string that matches the value in any of the table columns. MXview filters the table to only display OPC tags with values that fully or partially match the specified string.
  - > Click one of the following OPC tag statuses on the left side of the screen.

All (0)	
Enabled (0)	
Disabled (0)	
L	_

MXview filters the table to only display OPC tags that match the selected status.

- 4. To export the data displayed on the **Custom OPC Tags** screen:
  - a. Click the **Export** ( ) icon.



- b. Select Export CSV.
- c. Specify the location to save the exported file.
- d. Click Save.

MXview exports the displayed event data as a CSV file.

MXview supports several optional modules that extend the functionality of the main module. These modules require a separate license to use.

# Introduction

The MXview Wireless Add-on Module provides a set of tools to help you monitor and troubleshoot your wireless network through MXview and supports up to a total of 200 wireless APs and clients. The add-on gives you clear, real-time information about the status of your wireless network including the client roaming status and key wireless performance indicators such as SNR and noise level. The wireless module also instantly notifies you of any problems with your wireless devices and helps you narrow down the root cause of the problem, allowing for quick and easy troubleshooting.

### **System Requirements**

The computer that the MXview Wireless Add-on Module is installed on must satisfy the following system requirements based on the maximum capacity of 200 wireless APs and clients:

	System Requirements
CPU	2 GHz or faster dual core CPU
RAM	8 GB or higher
Hard Disk Space	20 to 30 GB for 1 month of performance and event history recording
	Windows 7 Service Pack 1 (64-bit)
	Windows 10 (64-bit)
OS	Windows Server 2012 R2 (64-bit)
	Windows Server 2016 (64-bit)
	Windows Server 2019 (64-bit)
	Chrome: Version 76 or later
Browser Requirements	Firefox: Version 69 or later
biowser Requirements	Microsoft Edge: Version 79 or later
	Internet Explorer 11

### **Supported Devices**

The MXview Wireless Add-on Module supports the following wireless devices:

- AWK-3131A Series (firmware v1.16 or above)
- AWK-4131A Series (firmware v1.16 or above)
- AWK-1131A Series (firmware v1.22 or above)
- AWK-1137C Series (firmware v1.6 or above)

# Getting Started With the Wireless Add-on Module

In order to use the MXview Wireless Add-on module, you will need to activate it first. You can choose to activate a new license, or enable the wireless free trial through the license manager.

≡ MXviøw	Site DESKTOP-NVV5C	/1 ~		
License Ma	nager			
MXview	_	Wireless Addon Mode: None		
Trial Remaining	g 9 <sub>Days</sub>	Wireless Trial Remaining Start to experience the Wireless Addon in MXview	Network Adapter MXview binds the license to one network adapter, please choose the adapter you want to bind. Re-select a network adapter will deactivate all your licenses automatically, you have to register them again.	Re-activate License Use both the Deactivation code and a User Code to re-activate your license.
Kee	p Trial	Start Free Trial	Select Network Adapter	Re-activate

The system will automatically restart after you activate the module. A message will appear telling you to wait 10 seconds while the module activates. Once done, click **OK** to refresh your browser and enable the Wireless Add-on features.

		1
Ту	Please Wait	
	The operation will finish in 10 seconds.	
	ок	
8	Wireless Addon in MXview license to one network	(

- For detailed information on how to activate the MXview Wireless Add-on Module, refer to License Management.
- To add wireless devices to your MXview network, refer to Using the Setup Wizard.



#### NOTE

Please activate the Full Version License first, then activate the Wireless Add-on License.

# **Wireless Module Features**

The MXview Wireless Add-on Module offers a set of features specifically designed to help you monitor and troubleshoot your wireless network more easily.

### Main Dashboard

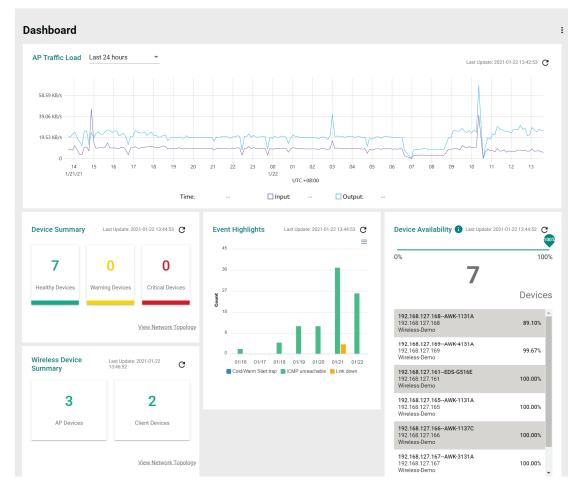
If the wireless module is activated, the MXview Dashboard will show two additional types of information: AP Traffic load and the Wireless Device Summary.

The AP Traffic Load graph shows the aggregated traffic of all the AP devices monitored by MXview. You can select a specific time to check the wireless network status at that time.

The Wireless Device Summary shows the number of deployed wireless devices. Clicking one of the cards will direct you to the Wireless Device Summary screen where you can find more detailed information about the wireless devices. Refer to Chapter 5: **Dashboard Widgets** for more information about the other cards on the dashboard.

To access the Dashboard, navigate to **Menu** ( $\equiv$ ) > **Dashboard**.

To refresh the data displayed in all the widgets, click the **Settings** (:) icon in the top-right corner of the screen and select **Refresh All**.



## **Dynamic Wireless Client Roaming**

The MXview Wireless Add-on Module features dynamic wireless roaming display, which updates roaming connections of wireless clients in real-time. Instead of using LLDP data to draw links between devices, MXview uses both the client list data from the wireless AP and AP data from the wireless client to detect wireless roaming changes.

To enable Dynamic Wireless Client Roaming, toggle the **Dynamic wireless topology** option in the in Display Options window. You can also enable the **Dynamic wireless client position** option. In this mode, wireless clients will automatically move to the AP they connect to when roaming. The link between the client and AP on the topology will also change dynamically if the client connects to another AP.

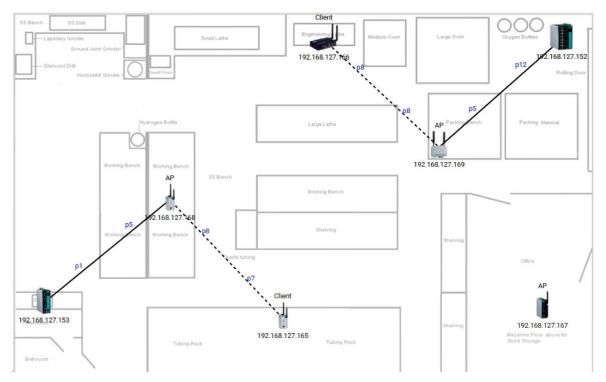
Refer to the table below for a description of each display option.

Option	Description
Show all wireless clients	Toggle this option on or off to show or hide wireless clients on the
Show all wheless chefts	topology
Dynamic wireless topology	Enable this option to display dynamic links of the wireless devices
	Enable this option to have wireless clients move to a position close to
Dynamic wireless client position	the AP they are associated with
	Disabling this option will return the clients to their original position

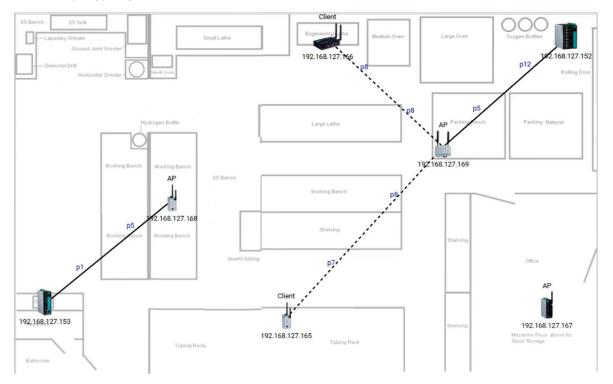
$\equiv$ MX view	
All > Wireless-Demo > Root	
🙏 Topology 🗸 🚷 Group 🗸 🧪 Edit 🗸	O Visualization ∨ ♦ SFP ∨ ♀ Wireless ∨
Q	Working Bench 192.168.127.168 SS Bench
Display Options X Show all wireless clients Dynamic wireless topology Dynamic wireless client position	Client

The following diagrams are an example of the dynamic roaming display showing dynamic client-AP link changes.





When the client roams to another AP, MXview will automatically redraw the link to the new AP on the wireless topology diagram.



## **AP/Client Device Dashboard**

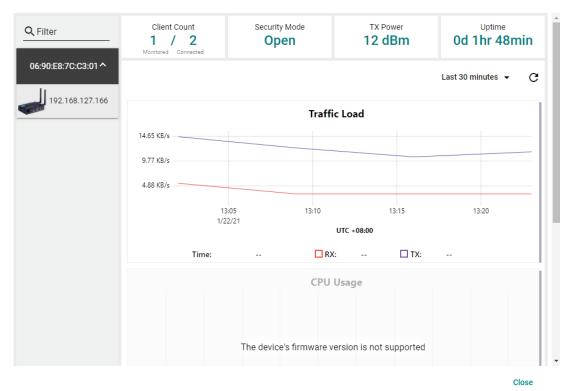
Use the **AP/Client Device Dashboard** screens to see detailed information and performance statistics of the client or AP.

To access the AP/Client Device Dashboard, click on any wireless AP or client device's icon on the topology diagram and click **Device Dashboard** in the toolbar.



### **AP Device Dashboard**

#### AP Dashboard-192.168.127.169--AWK-4131A

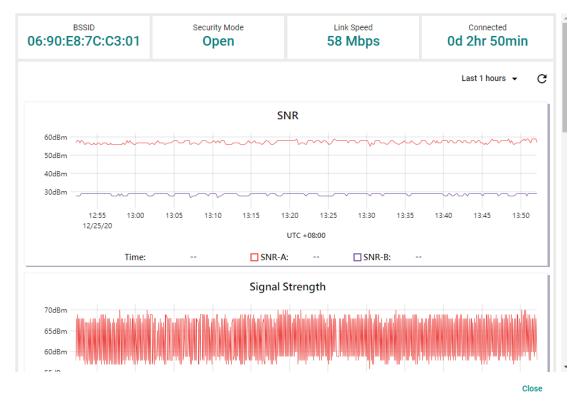


The AP Device Dashboard shows the following information:

Parameter	Description	
Client Count	Monitored	The total number of wireless clients connected to this AP that are monitored by MXview
	Connected	The total number of wireless clients that are connected to this AP
Security Mode	The Security	Mode of the AP: Open, WEP, WPA, or WPA2
TX Power	The current transmission power of the AP	
Uptime	The total time the wireless AP has been online since the last restart	
Traffic Load	The current and historical traffic throughput of the wireless interface	
CPU Usage	The current and historical CPU usage of the AP (only supported by certain firmware versions)	
Memory Usage	The current and historical memory usage of the AP (only supported by certain firmware versions)	

### **Client Device Dashboard**

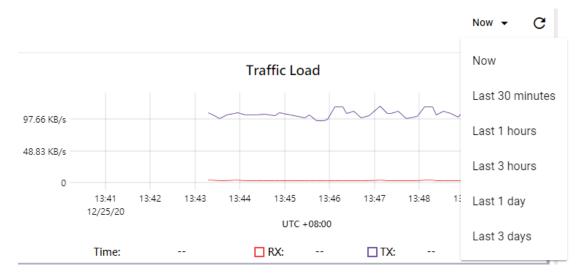
#### Client Dashboard-192.168.127.166--AWK-1137C



The Client Device Dashboard shows the following information:

Parameter	Description
BSSID	The BSSID of the wireless AP the client is connected to
Security Mode	The Security Mode of the client: Open, WEP, WPA, or WPA2
Link Speed	The real-time bandwidth of the connection to the AP
Connected	The total time the wireless client has been connected to the AP
	The current and historical Signal-to-Noise ratio of the client
SNR	If the wireless device has multiple antennas, the SNR of each antenna will be
	separately shown as SNR-A and SNR-B
Signal Strength	The current and historical signal strength of the client
Noise Floor	The current and historical noise floor of the client
Traffic Load	The current and historical traffic throughput of the wireless interface
	The current and historical CPU usage of the client (only supported by certain
CPU Usage	firmware versions)
Momory Hoago	The current and historical memory usage of the client (only supported by certain
Memory Usage	firmware versions)

You can view the device diagnostics and usage parameters in real-time or recall the history for up to the last 3 days from the drop-down menu in the top-right. You can zoom in on the timeline to examine a narrower time period. Double-click the timeline to return to the original view.



### **Wireless Device Summary**

The Wireless Device Summary screen provides detailed information about all the AP and client devices including the device's IP and MAC address, operation mode, and current signal strength.

To access the Wireless Device Summary screen, expand the **Wireless** menu in the toolbar and click **Wireless Device Summary**.

Click **Back** in the top-left corner to return to the topology view.

ss-Demo	> Root								
s Dev	vice Summary								
	Operation Mode	IP Address	MAC Address	BSSID	Channel	Noise Floor	Signal Strength (dBm)		
	AP - 192.168.127.168	(Wireless-Demo)							
	AP	192.168.127.168	00:90:E8:52:39:50	06:90:E8:52:39:50	1	N/A	N/A		
	Client	192.168.127.165	00:90:E8:52:39:75	06:90:E8:52:39:50	1	-87	-21		
	Client	192.168.127.164	00:90:E8:00:04:48	06:90:E8:52:39:50	1	-96	-62		
	∧ AP - 192.168.127.169	(Wireless-Demo)							
	AP	192.168.127.169	00:90:E8:7C:C3:01	06:90:E8:7C:C3:01	1	N/A	N/A		
	Client	192.168.127.166	00:90:E8:63:A7:6C	06:90:E8:7C:C3:01	1	-85	-32		
	Client	192.168.127.167	00:90:E8:52:07:85	06:90:E8:7C:C3:01	1	-87	-49		
								ltems per page: 50 ▼ 1-8 of 8   <	

### **Wireless Roaming Playback**

Through the Wireless Roaming Playback screen, you can recall the roaming history of a specific client. By default, MXview will keep the roaming playback data for 30 days.

To access the Wireless Roaming Playback screen, expand the **Wireless** menu in the toolbar and click **Wireless Roaming Playback**.

≡ MX view	Hi , admin 🚦
All > Wireless-Demo > Root	
← Back	
Q, Filter	1:1
MOXA	1:1 # @ @
192.168.127.165 Party later	<u>র</u> ব
192.188.127.166	
102 104/2721 00         1130-00           Column         2021-01-22 11/26:04           FRSS 166         FRSS 166	
12 142 142 142 142 142 142 142 142 142 1	
instance instanc	
bitters	
O Time Range:         1/22/2021         Start Time         Ourston         Apply	
	To 2021-01-22 11:27:00
	11:27:00

Click **Back** in the top-left corner to return to the topology view.

On the left-hand side is a list of wireless clients, in the center is the topology map, and located at the bottom is the playback progress bar. Select any client from the list and click **Play** () to start playing the wireless roaming history for the selected time range. You can adjust the playback speed by clicking the **Decrease Speed** () or **Increase Speed** () button to increase or decrease the playback speed respectively.

To view the history for a specific time and date, click ( i) to choose the starting date, set the time in the Start Time field, select the duration of the playback history from the Duration drop-down menu, and click **Apply**.

Ō	Time I	Range		ate /22/2	021	Ē		Start T 08:5				
	DEC	2020	Ŧ			<	>	L				
	S	М	Т	W	Т	F	S					
	DEC							L				
			1	2	3	4	5	L				
	6	7	8	9	10	11	12	Ŀ				
	13	14	15	16	17	18	19	L				
	20	21	22	23	24	25	26					
	27	28	29	30	31			1				
ao.	- Date -					t lime -						
nge:	12/2	5/202	0		01:	42 PN	1	0				

The progress bar also displays the RSSI value at the time. In addition, the red dots indicate the time when the wireless client roamed to a different AP. You can zoom in on the timeline to examine a narrower time period. Click **Apply** to return to the original view.



# 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.

3. 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

/

# License (node-tacacs-plus)

https://github.com/santsys/node-tacacs-plus/blob/master/LICENSE

MXview uses the above nodejs package to implement its own TACACS client. The open source location is

https://github.com/moxa-nsd/mxview-gateway-tacacs-client