MXview 3.1 User's Manual

Version 1.3, November 2019

www.moxa.com/product

MXview 3.1 User's Manual

Copyright Notice

Trademarks

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

Moxa Americas
Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa China (Shanghai office)
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Europe
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa Asia-Pacific
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Moxa India
Tel: +91-80-4172-9088
Fax: +91-80-4132-1045

Table of Contents

1

Introduction

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. MXview includes an integrated MIB complier that supports any third-party MIB. It also allows you to monitor third-party OIDs and Traps. Network and Trap components that have been located by MXview can be managed via web browsers from both local and remote sites—anytime, anywhere.

The following topics are covered in this chapter:

- **Key Features**
  - Web-based Operation
  - Auto Discovery and Topology Visualization
  - Event Management
  - Configuration and Firmware Management
  - Traffic Monitoring
- **MXview Operation Model**
- **System Requirements**
- **Supported Devices**

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 with Chrome or Firefox, without installing additional software.

Auto Discovery and Topology Visualization

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

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 SMS, email, popup window, sound, or external program.

Configuration and Firmware Management

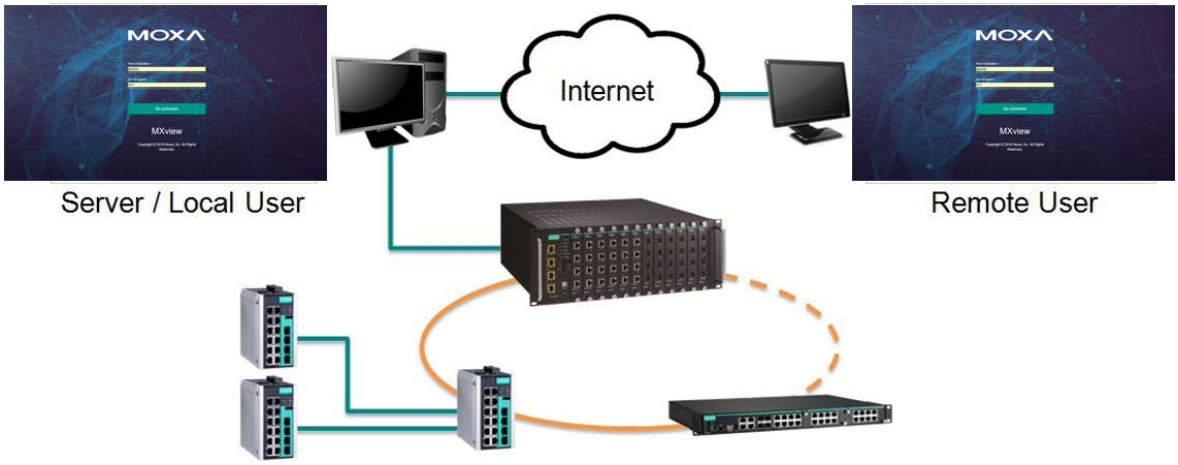
MXview provides an interface for managing Moxa networking devices from a central location. Users can remotely backup or update configuration files, and upgrade firmware.

Traffic Monitoring

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

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
OS	Windows 7 Service Pack 1 (64-bit) Windows 10 (64-bit) Windows Server 2012 R2 (64-bit) Windows Server 2016 (64-bit)
Client Browser Requirements	Browser: Chrome: Version 76 or later Firefox: Version 69 or later

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 and System Backup

The following topics are covered in this chapter:

- **Installation Procedure**
- **Uninstallation**
- **System Backup**
- **System Restore**

Installation Procedure

1. Execute the installation program.
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**
2. 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

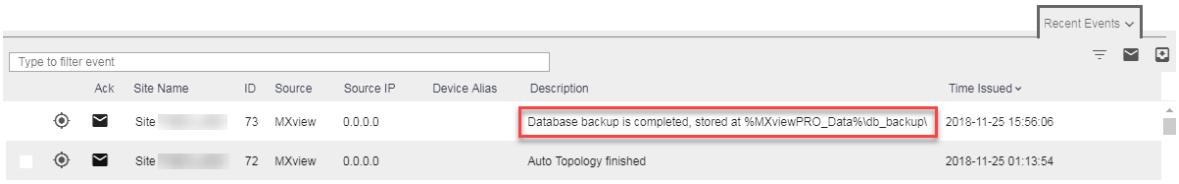
You can also uninstall the software by selecting
Start → All Programs → Moxa → MXview → Uninstall MXview

System Backup

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

1. Navigate to **Menu** ( ) → **Migrations** → **Database Backup**.
   The **Database Backup** screen appears.
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.



The backup folder uses the following naming convention: **YYYYMMDD HHMMSS**

The system backup includes the following items:

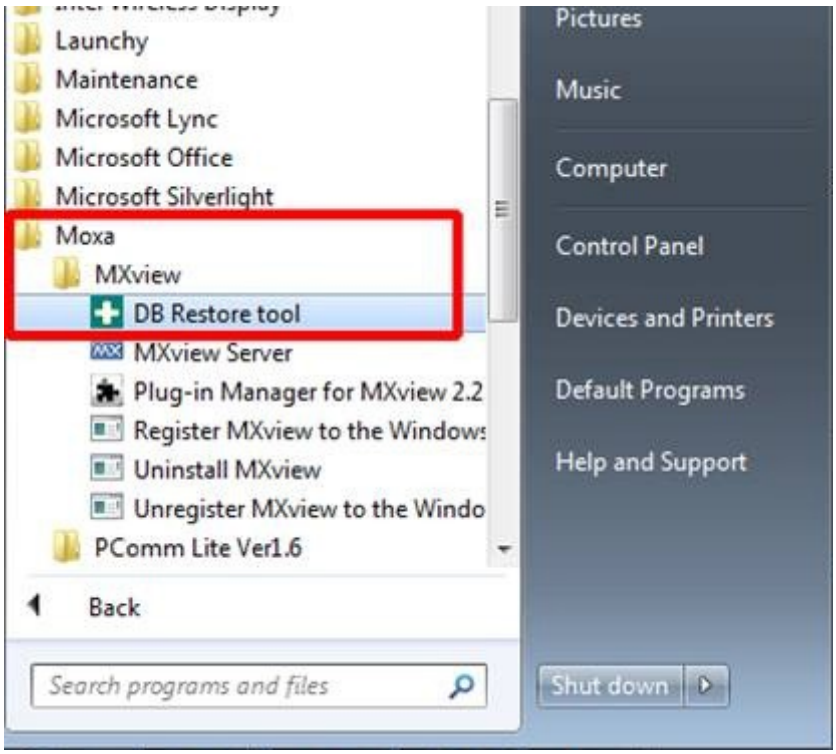
- Topology
- Traffic
- Availability
- Event
- Threshold settings
- Job scheduler settings
- OID items
- Trap items
- System settings

System Restore

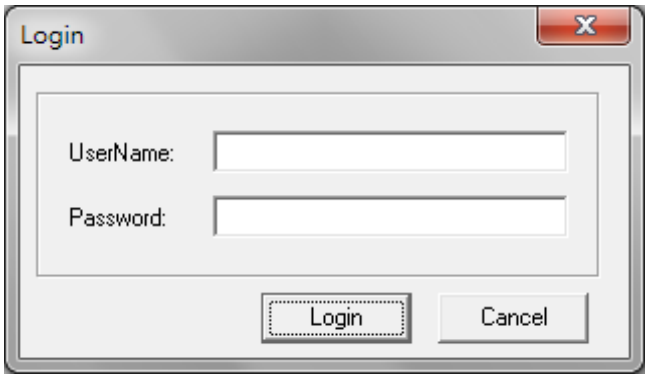
MXview versions 2.2 and higher supports configuration backup files, which use the file extension *db3. To restore a system configuration from a backup file, first shut down MXview. Then, select the **DB Restore tool** in **Start → All Programs → Moxa → MXview → DB Restore tool**. Log in using your username 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:

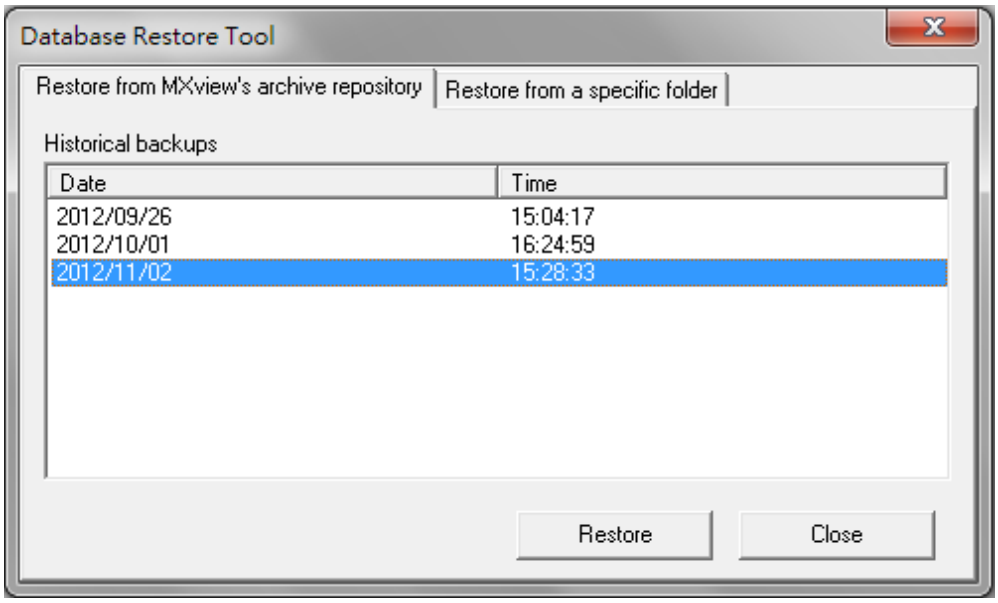
1. Select **Start → All Programs → Moxa → MXview → DB Restore tool**



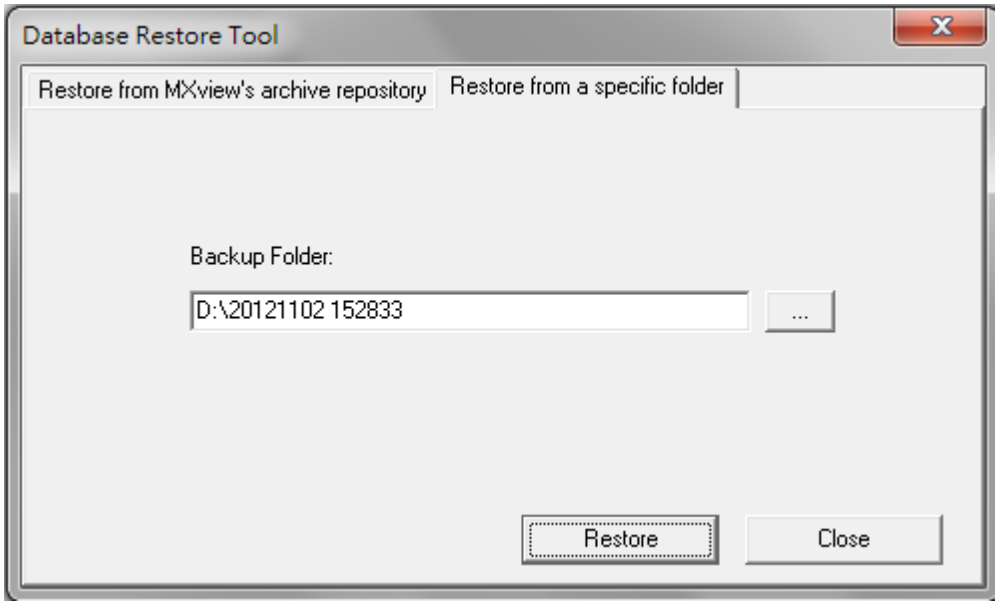
2. Login with your username and password



3. Choose the folder where the backup files are located



4. Click **Restore**.



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.

3

Getting Started

The following topics are covered in this chapter:

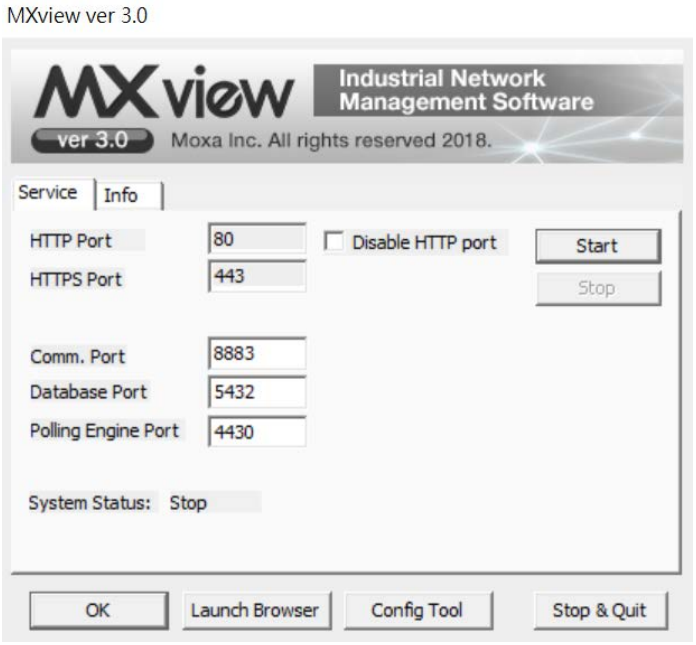
- **Starting the MXview Server and Logging Into MXview Locally**
- **Logging Into MXview Remotely**
- **Multiple MXview Sites**
- **Configuration of Multiple Sites**
- **Using the Setup Wizard**
- **License Management**
  - Checking the License
  - Adding a New License
  - Deactivating a License
- **Account Management**
  - Adding User Accounts
  - Modifying User Accounts
  - Deleting User Accounts
  - Exporting User Accounts
  - Configuring Account Passwords
  - Configuring Login Notifications
  - Changing the Display Language

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.

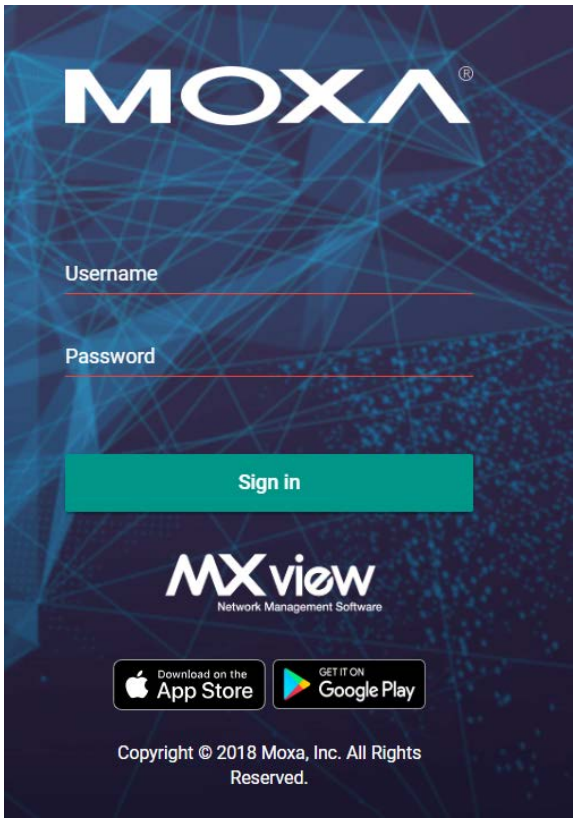
   The MXview server screen appears.



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.

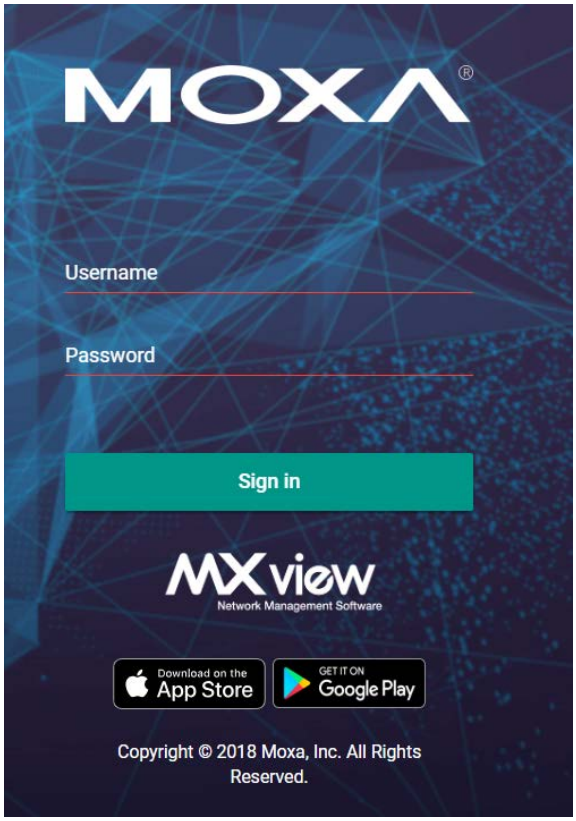
NOTE Alternatively, you can log in to MXview from a remote computer after starting the MXview service. For more information, see **Logging Into MXview Client**.

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**.

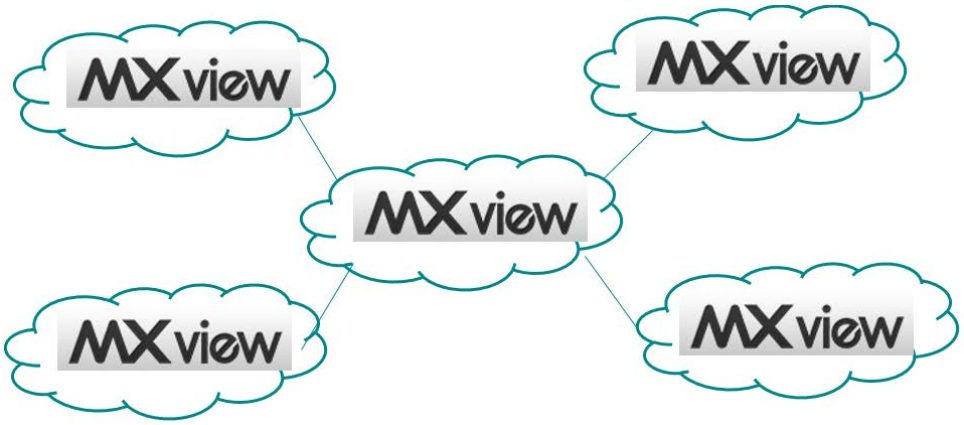
   The user account logs in to the MXview web console.

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

NOTE For remote users, Moxa recommends downloading **MXviewClient** from the MXview server and using **MXviewClient** to log in.

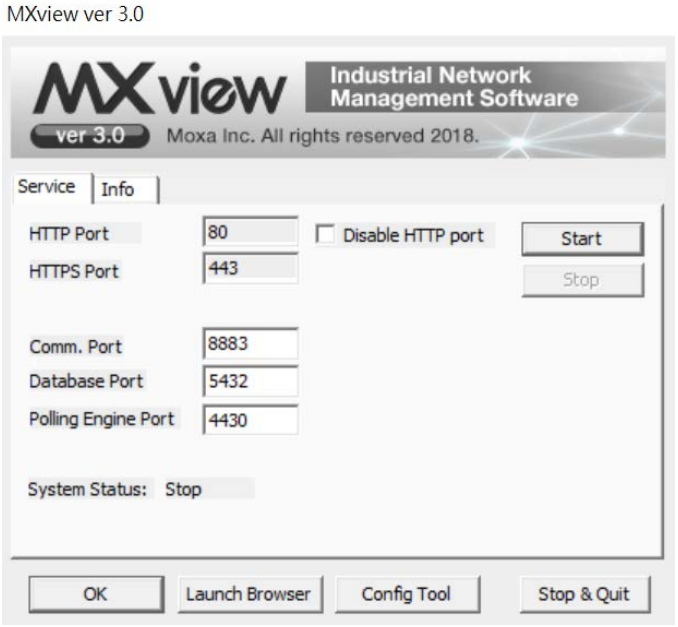
Multiple MXview Sites

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.

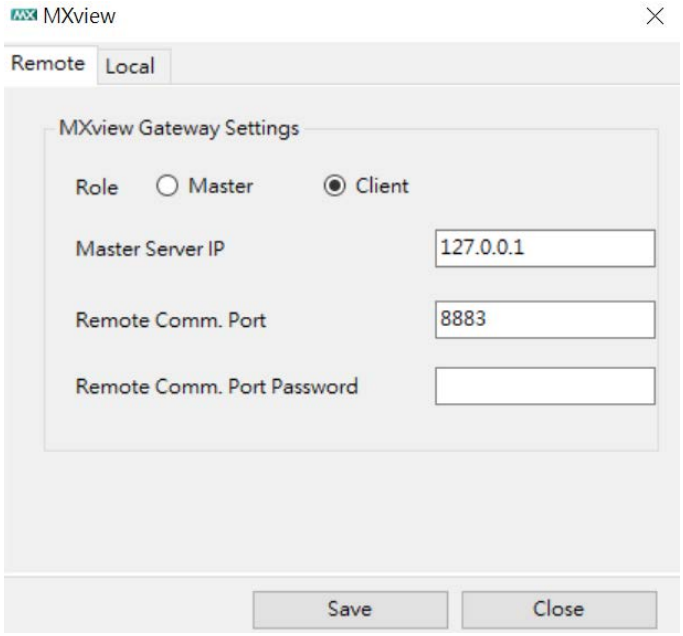


Configuration of Multiple Sites

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

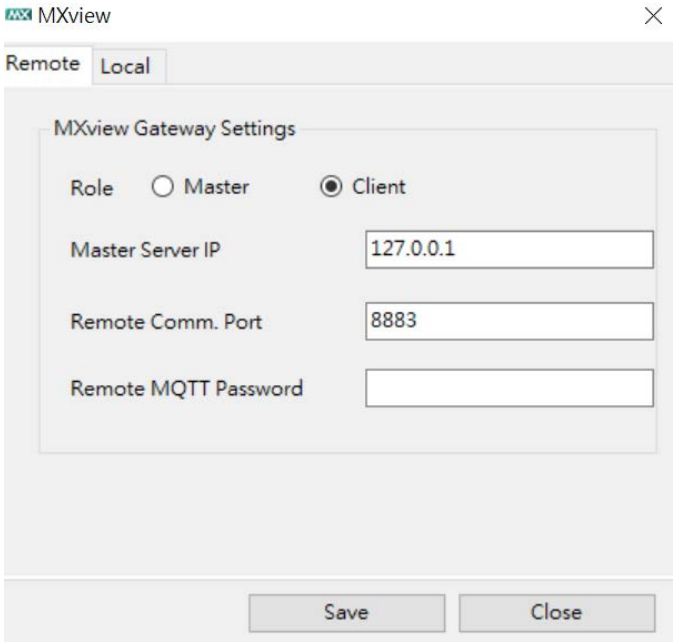


2. The control panel will pop up, choose the master if this MXview is configured to be the master to monitor multiple instances of MXview.

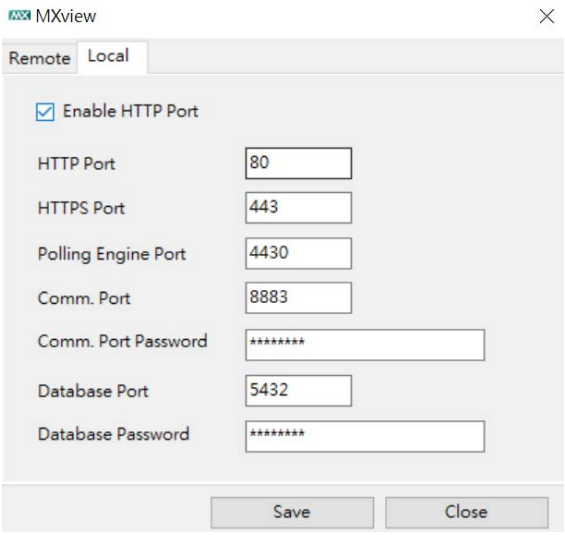


3. Choose Client if the MXview is the one to be monitored:

   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.



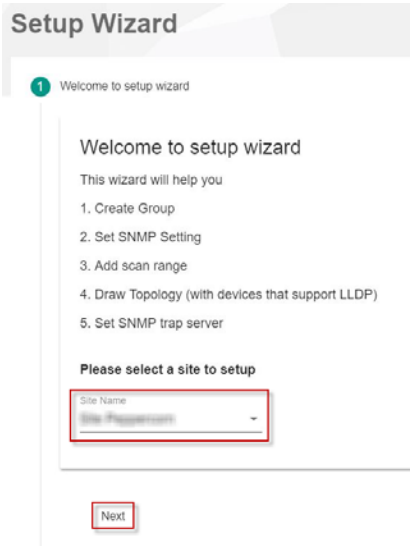
The Local tab shows the port setting and password of MXview. The default password of the remote communication port is 89191230, and the default database password is 89181230.



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** ( ) → **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**.



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

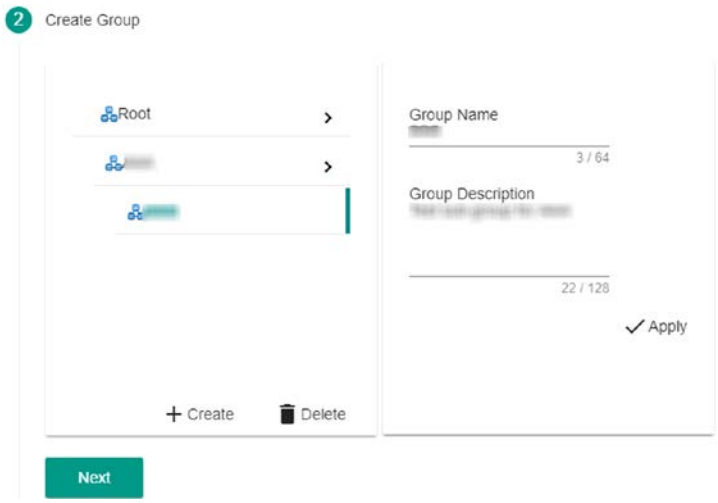
NOTE Before finding devices, groups need to be created. Root is the default group and the top-most layer in the tree structure. All other created groups are placed below the level of Root.

   a. Select the parent group.
   b. Click **Create** to create a new group under the parent group.

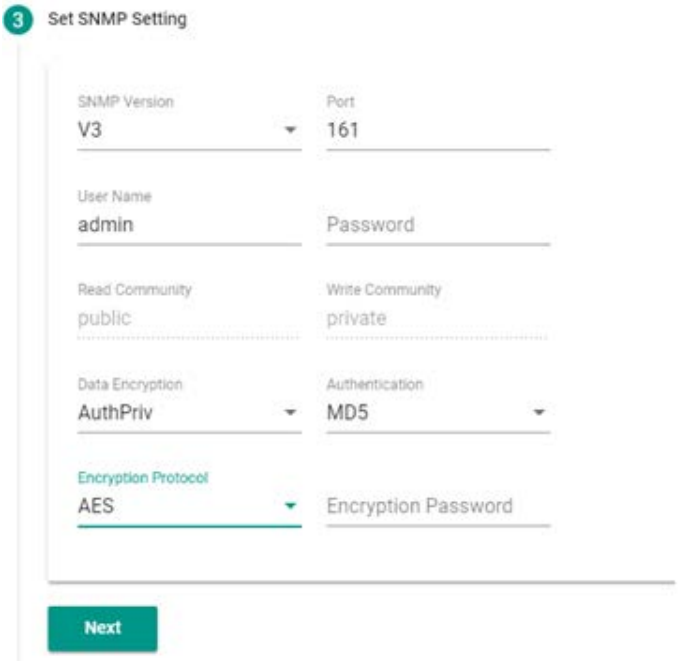
c. Specify the following:
   - **Group Name:** Type a name for the group.
   - **Group Description:** Type a description for the group.

d. Click **Apply**.
   MXview creates the new group below the selected parent group.

e. Click Next.



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**.



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** (+) 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:

- 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 **Apply**.

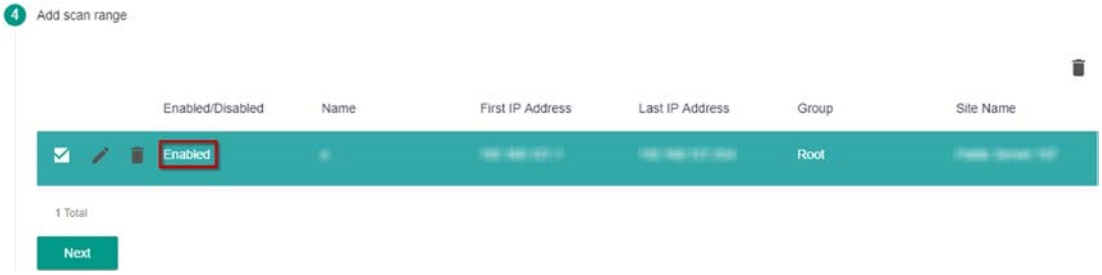
e. (Optional) To add additional network scan ranges, repeat the previous steps.

f. (Optional) To modify scan range settings, click the **Edit** (✎) icon next to an added scan range.

g. (Optional) To remove a scan range, click the **Delete** (🗑) 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.

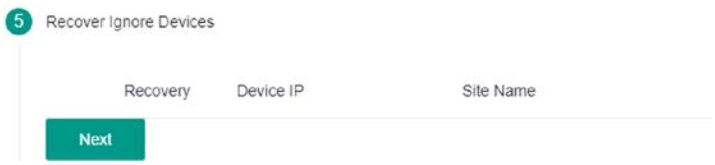


5. (Optional) Recover devices ignored (deleted) from a previous scan:

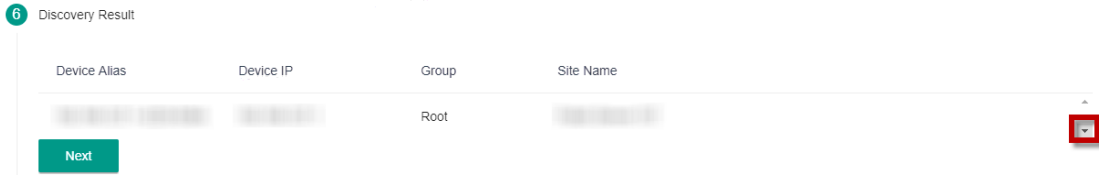
NOTE If an IP address scan range is removed (deleted) from a previous network scan, MXview excludes devices within the deleted range from the network topology. Use the Recovery feature to restore the devices from deleted scan ranges to the network topology.

a. Select a device from the list of ignored devices.

b. Click **Next**.
MXview scans for network devices.



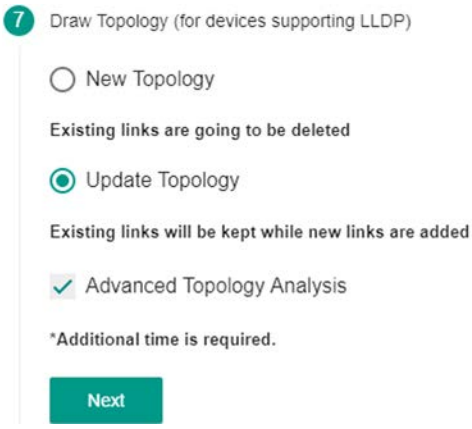
6. View devices discovered on the network.
   a. MXview displays discovered devices on the **Device Result** list. Scroll down to view more devices on the list.



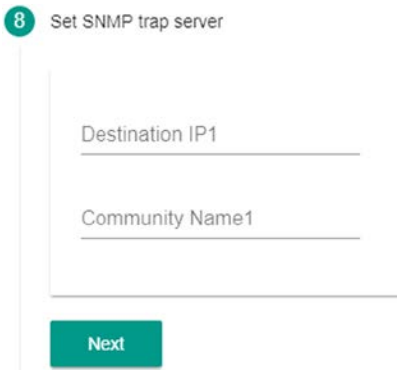
   b. Click **Next**.
7. Draw the network topology.

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) To 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.



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**.



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

License Management

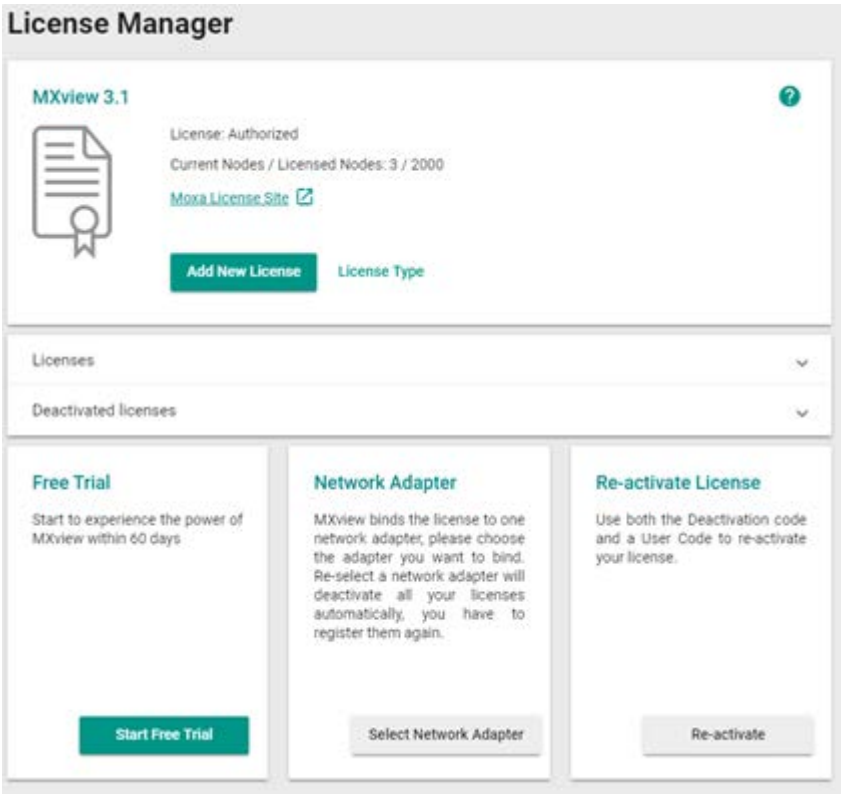
MXview is available in different versions, and each version supports a different number of nodes. For example, if your version of MXview supports 250 nodes, then during device discovery MXview will only recognize up to 250 nodes. MXview will stop the device discovery procedure once it reaches the 250-node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

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** ( ) → **License**.

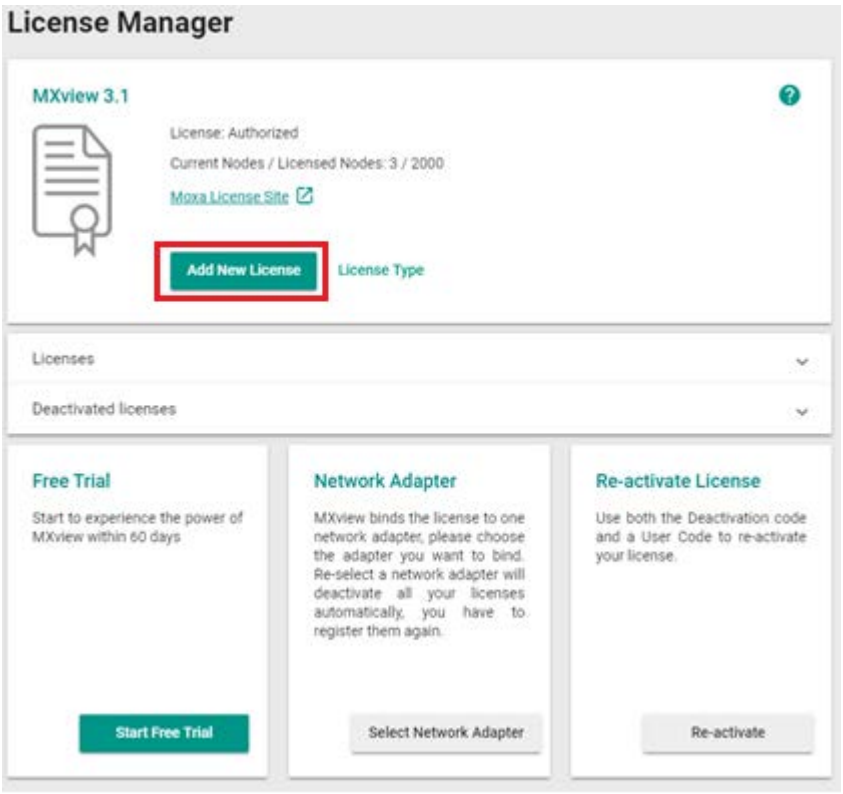


The **License Manager** screen displays the license type, the number of nodes in use, and the total number of nodes available under the current license.

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** ( ) → **License Manager**.
   The **License Manager** screen appears.
2. In the **Add New License** section, click **Add New License**.



3. Select the network adaptor to generate the user code which will be used for license registration later

   The **Activation** screen appears.

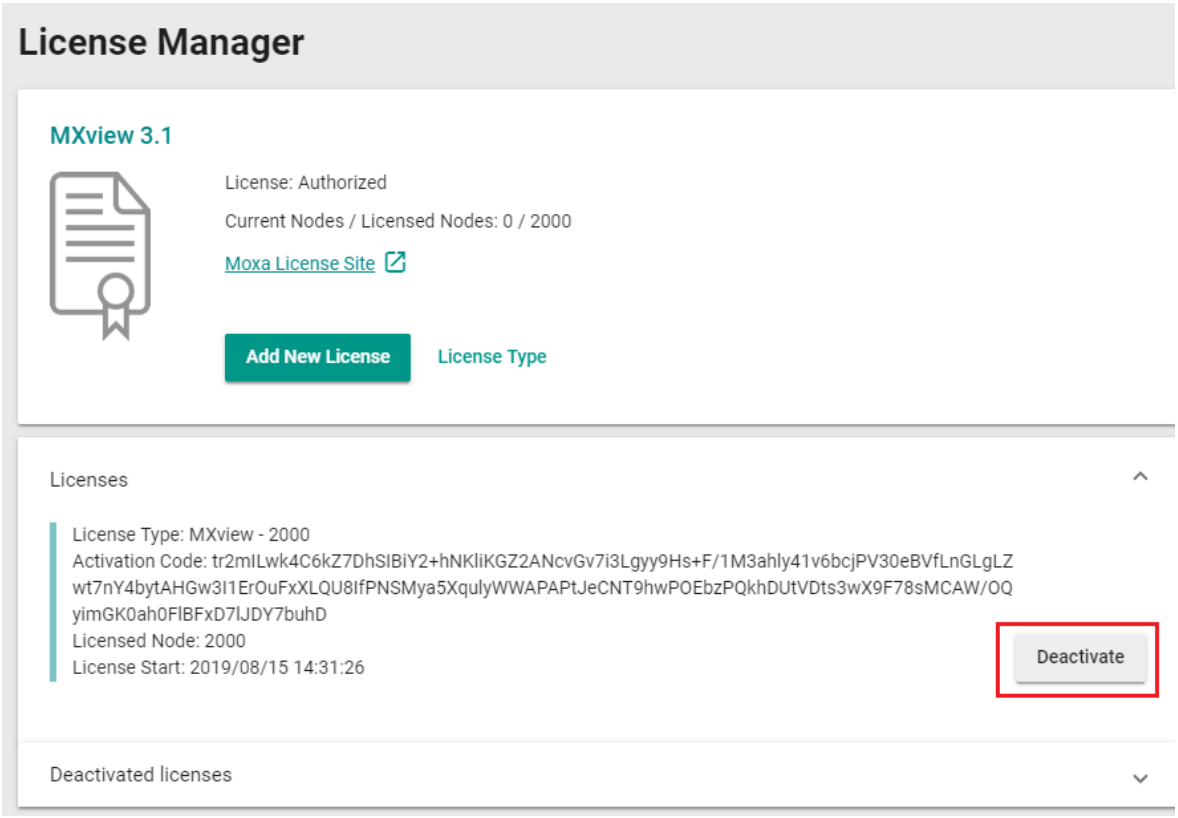
4. Input a valid activation code.

NOTE Please reference the license management page to get more details on how to get the activation code.

5. Click **Apply**.
   MXview activates the new license.

Deactivating a License

1. 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.
2. Navigate to **Menu** ( ) → **License Manager**.
   The **License Manager** screen appears.
3. Expand the **Licenses** section.
   A list of activated licenses and activation codes appears.
4. Click **Deactivate**.



MXview deactivates the license.

Account Management

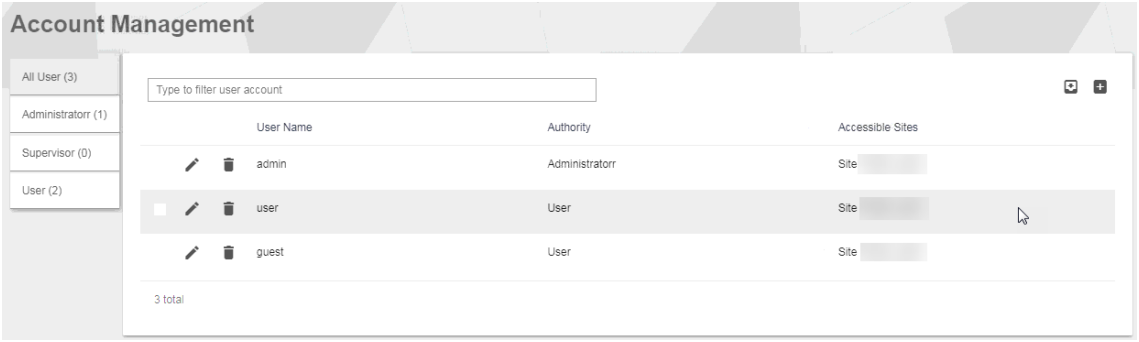
The Account Management screen allows you to view, add, modify, and delete user accounts from MXview. You can also export a list of user accounts and related information as a CSV file.

MXview provides three default accounts:

- **admin**
- **user**
- **guest**

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

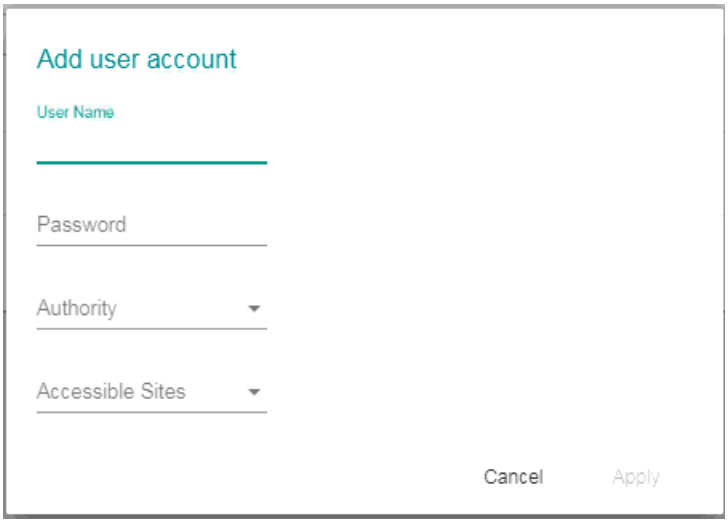
- **Administrator:** Has full access rights to modify any settings/configurations and can assign authorities to other accounts
- **Supervisor:** Has full access rights to modify any settings/configurations but cannot assign authorities to other accounts
- **User:** Has read-only permission



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

Adding User Accounts

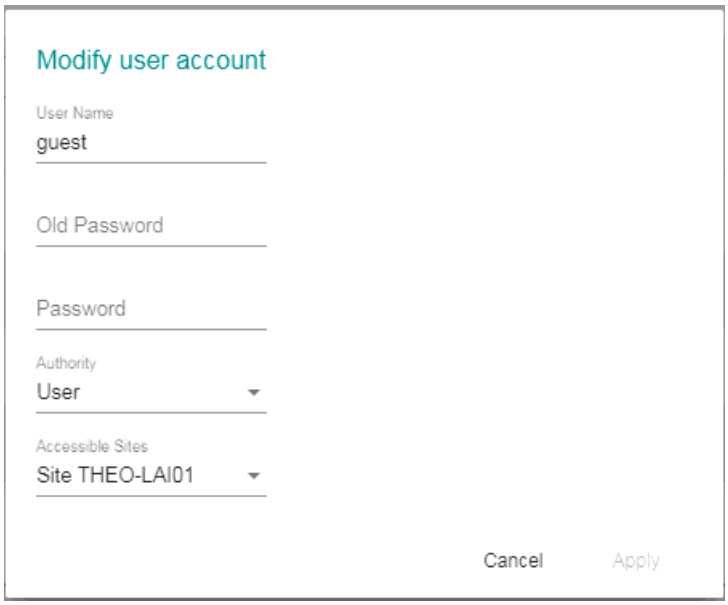
1. Navigate to **Menu** ( ) → **Account Management**.
   The **Account Management** screen appears.
2. Click the **Add** ( ) icon in the top right corner of the screen.
   The **Add user account** screen appears.



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 **Apply**.

Modifying User Accounts

1. Navigate to **Menu** ( ) → **Account Management**.
   The **Account Management** screen appears.
2. Click the **Edit** ( ) icon in front of the account you want to modify.
   The **Modify user account** screen appears.



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**.

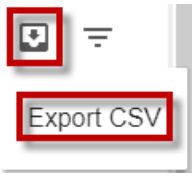
Deleting User Accounts

1. 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).
3. Click the **Delete** ( ) 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.

1. Navigate to **Menu** ( ) → **Account Management**.
   The **Account Management** screen appears.
2. Click the **Export** ( ) icon.

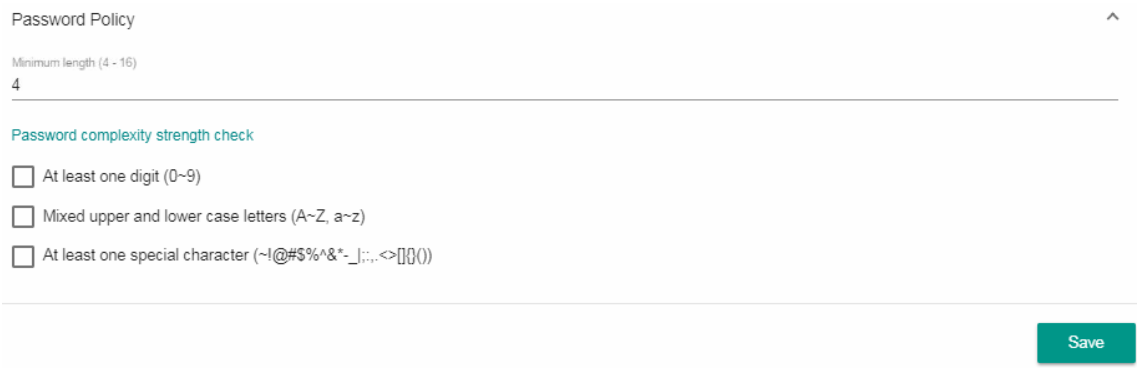


3. Select **Export CSV**.
4. Specify the location to save the configuration file.
5. Click **Save**.
   MXview exports the CSV file to the specified location.

Configuring Account Passwords

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

1. Navigate to **Menu** ( ) → **Preferences**.
   The **Preferences** screen appears.
2. In the **User** section, expand **Password Policy**.

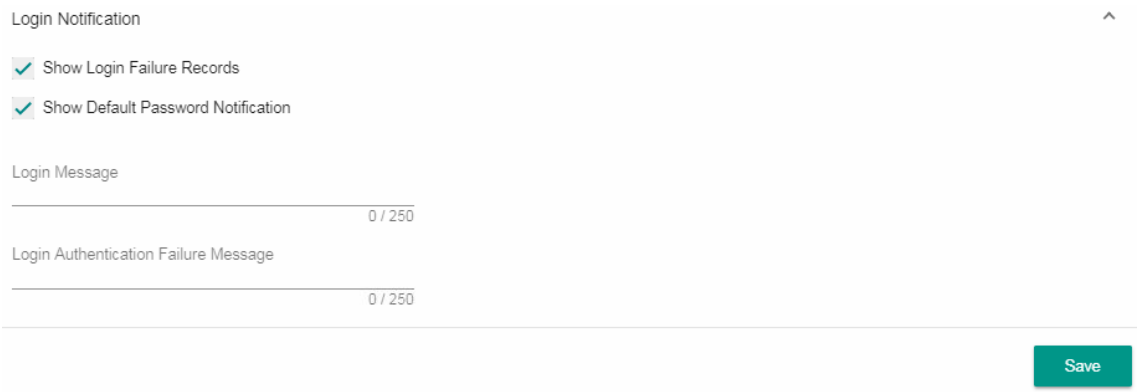


3. Specify the minimum password length (between 4 to 16 characters).
4. Select one or more of the following password complexity requirements:
   - **At least one digit (~9)**
   - **Mixed upper and lower case letters (A~Z, a~z)**
   - **At least one special character (~!@#$%^&*-_|;:,.<>[]{}())**
5. Click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

Configuring Login Notifications

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

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

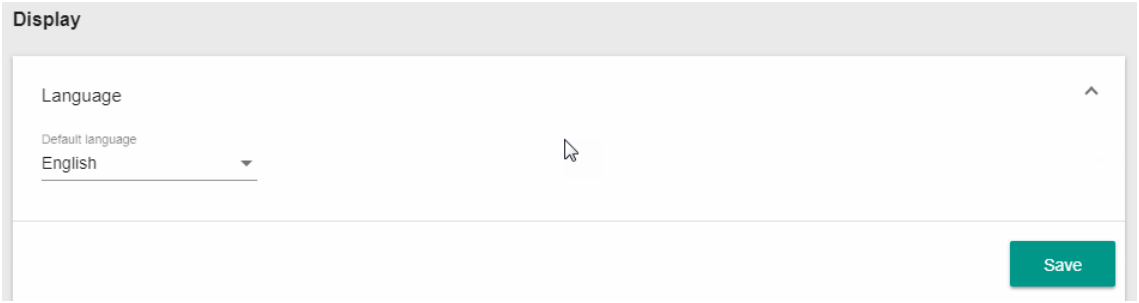


3. To enable the following notification(s), select the corresponding checkbox(es):
   - **Show Login Failure Records**
   - **Show Default Password Notification**
4. To disable the following notification(s), clear the corresponding checkbox(es):
   - **Show Login Failure Records**
   - **Show Default Password Notification**
5. To display a custom login message, type a string (up to 250 characters in length) in the **Login Message** field.
6. 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.

1. Navigate to **Menu** ( ) → **Preferences**.
   The **Preferences** screen appears.
2. In the **Display** section, expand **Language**.



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

4. Click **Save**.
   MXview updates the display language.

4

Dashboard Widgets

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

The following topics are covered in this chapter:

- **Dashboard Overview**
- **Device Summary**
- **Device Availability**
- **Event Highlights: Cold / Warm Start Trap**
- **Event Highlights: ICMP Unreachable**
- **Event Highlights: Link Down**
- **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** ( ) → **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**.

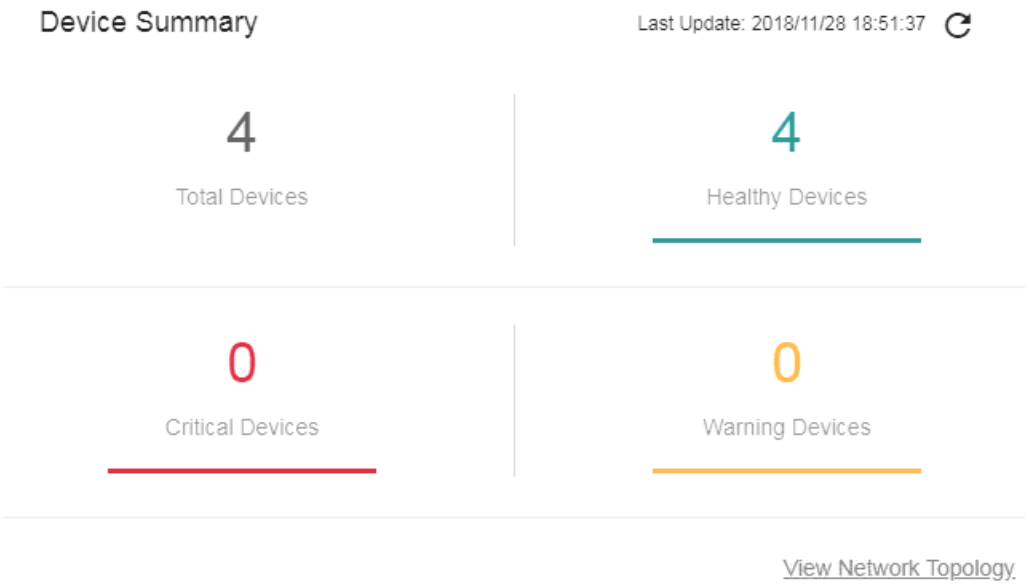
Device Summary

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 **Refresh** ( ) button following the **Last Update** timestamp.

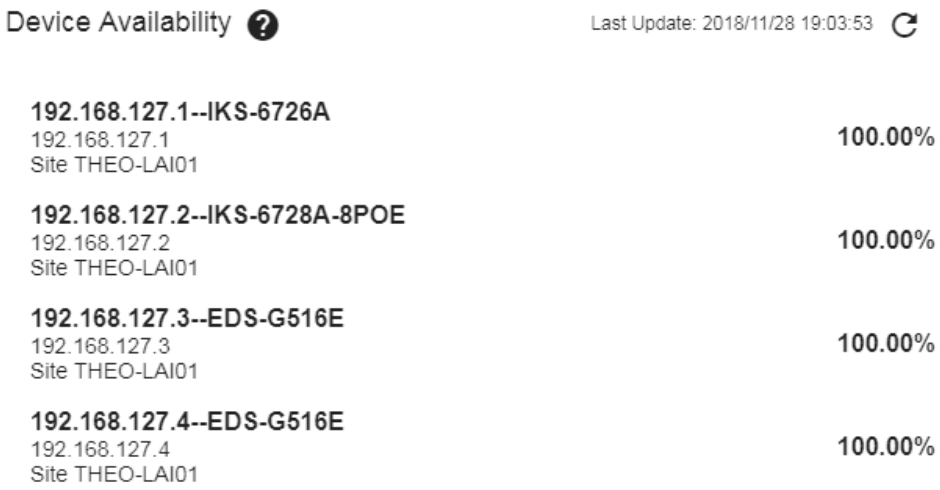


Device Availability

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** ( ) button following the **Last Update** timestamp.

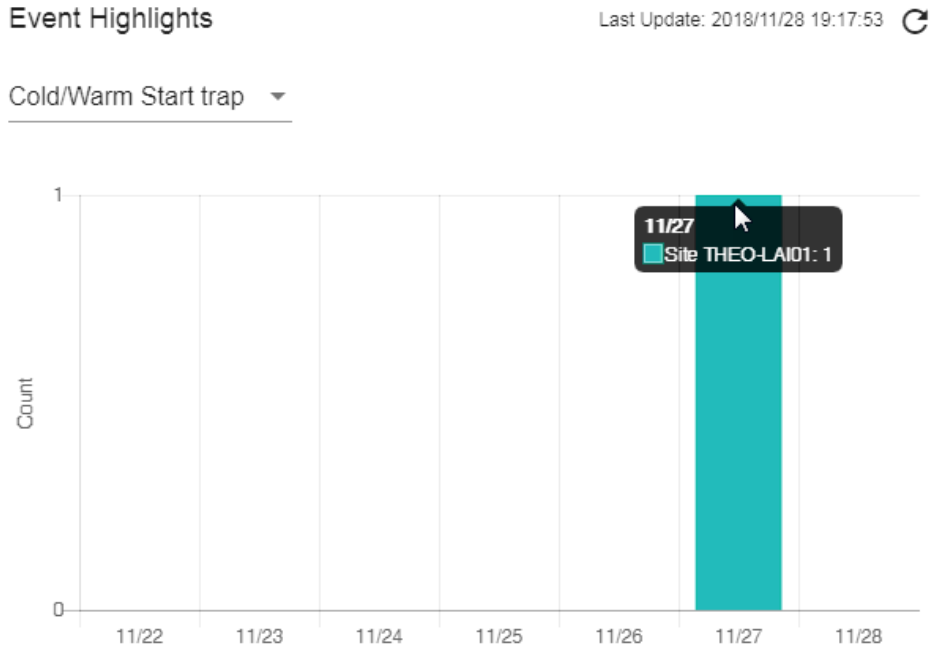


Event Highlights: Cold / Warm Start Trap

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** ( ) button following the **Last Update** timestamp.

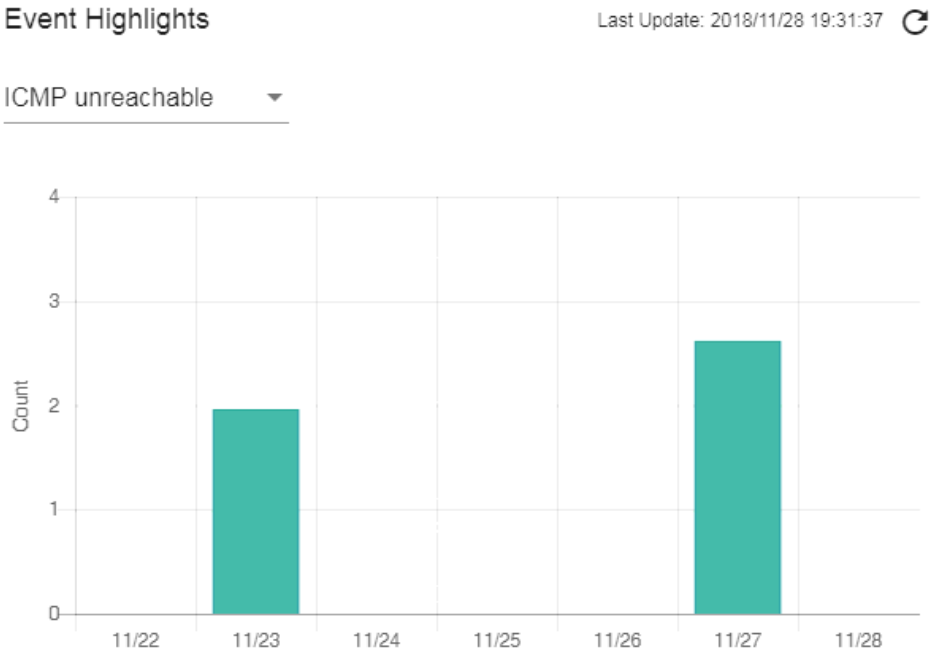


Event Highlights: ICMP Unreachable

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** (↻) button following the **Last Update** timestamp.

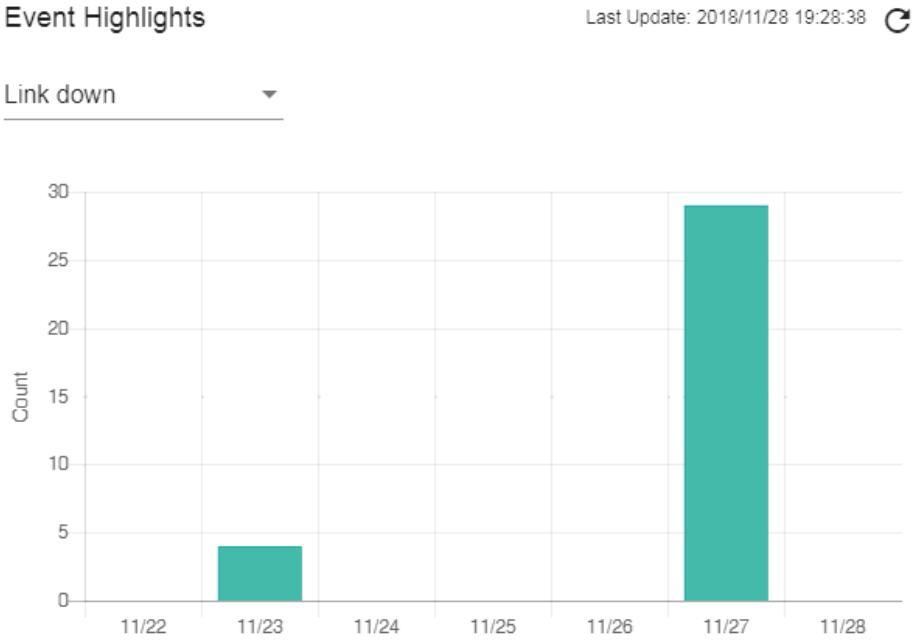


Event Highlights: Link Down

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:

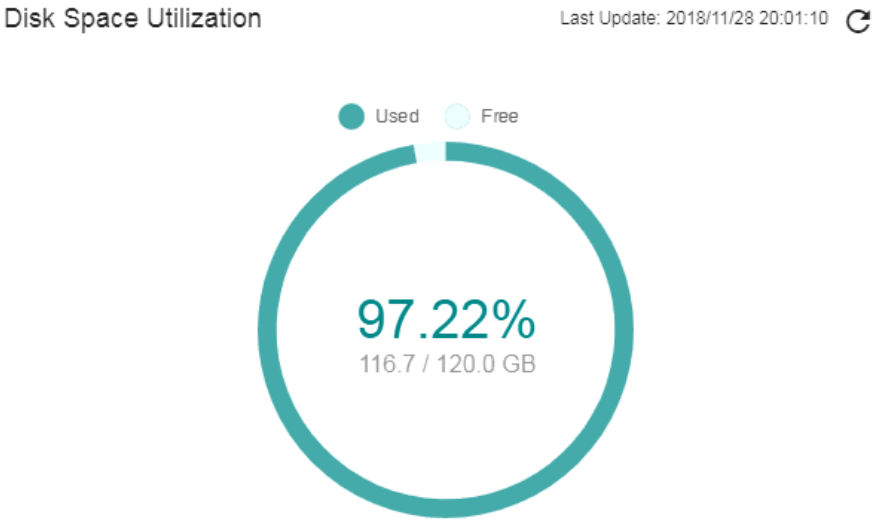
- To view the number of “link down” events issued at a site on a specific date, hover over a bar in the widget chart.
- To view additional details about the event on the **All Event** screen, click a bar on the widget chart.
- To change the type of event that the widget displays information for, select 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** (↻) button following the **Last Update** timestamp.



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** (↻) button following the Last Update timestamp.



5

License Management

NOTE Please refer to the License_Wizard.pdf on the MXview download page on Moxa's website to get details on MXview licenses.

6

Device Discovery and Polling

The following topics are covered in this chapter:

- **Device Discovery Overview**
- **Configuring IP Address Scan Ranges**
- **Configuring Background Discovery**
- **Configuring Device Polling Settings**
- **Changing Default SNMP Configurations**

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:

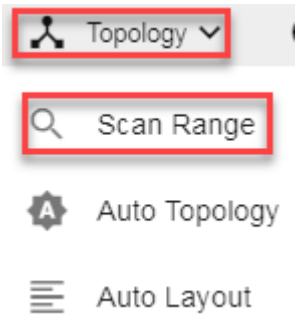
Device	Image
Moxa devices with SNMP enabled.	
Non-Moxa devices with SNMP enabled.	
Non-Moxa devices with ICMP enabled.	

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**.

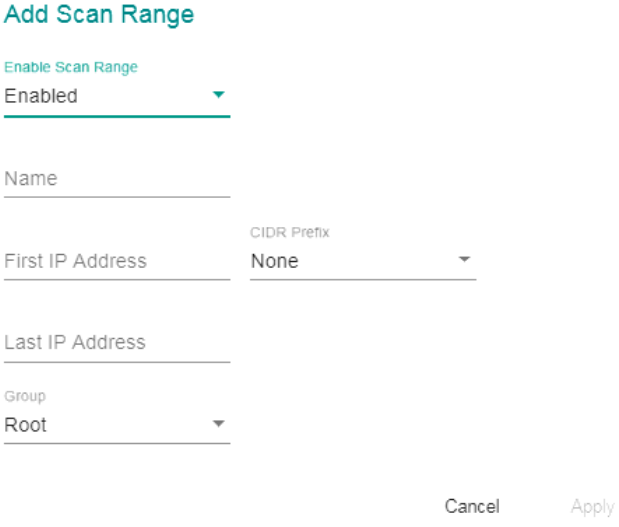
b. Navigate to **Menu** ( ) → **Network** → **Topology**, and then navigate to **Topology** → **Scan Range** from the Topology Map toolbar menu.



The **Scan Range Wizard** screen will appear.

2. To add a new scan range:

a. Click the **Add** ( ) button in the top right corner.
The **Add Scan Range** screen will appear.



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.

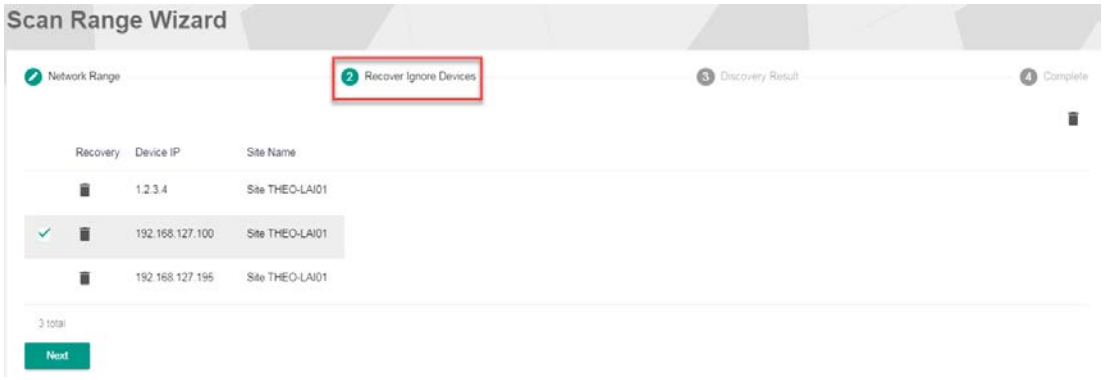
e. Provide the ending IP address for the scan range.

f. Select the **CIDR Prefix** (if any).

g. Assign the scan range to a **Group**.

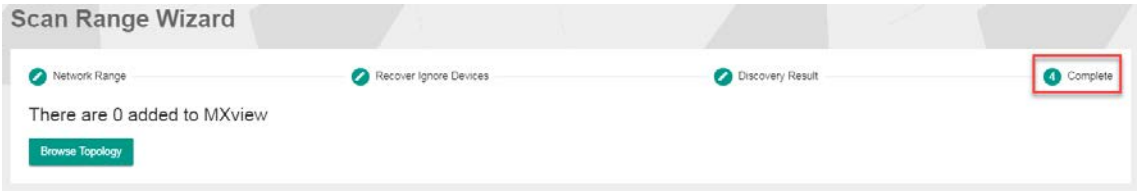
h. Click **Apply**.
The new scan range appears in the Network Range table.

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. o 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.



   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.

5. To complete scan range configuration, click **Next**.
   The **Scan Range Wizard** screen displays the **Complete** tab and the number of devices added to MXview.



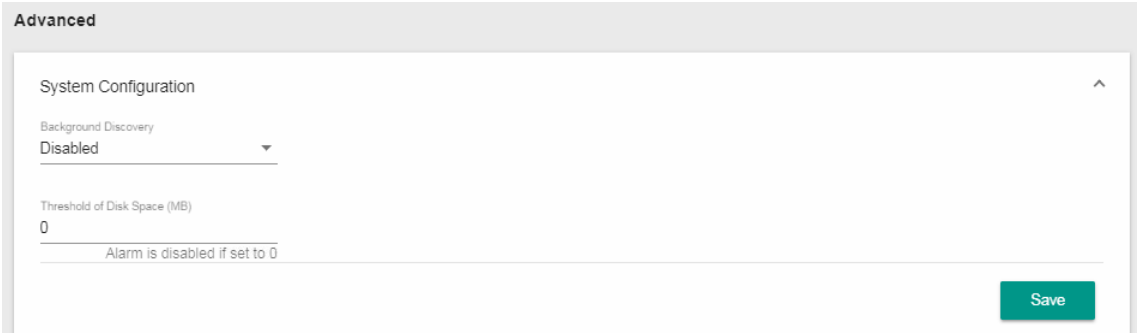
6. To view the updated topology, click **Browse Topology**.
   The **Network Topology** screen will appear and display the updated Topology Map.

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.



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.

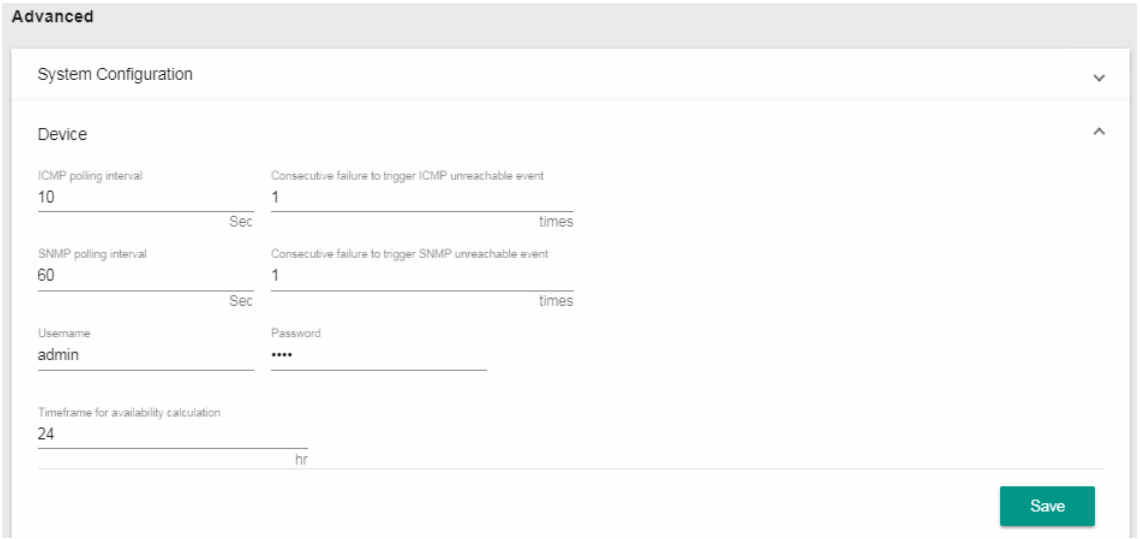
Configuring Device Polling Settings

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 **Chapter4: Dashboard Overview**.

1. Navigate to **Menu** ( ) → **Preferences**.
   The **Preferences** screen appears.
2. In the **Advanced** section, expand **Device**.
   The **Device** settings appear.

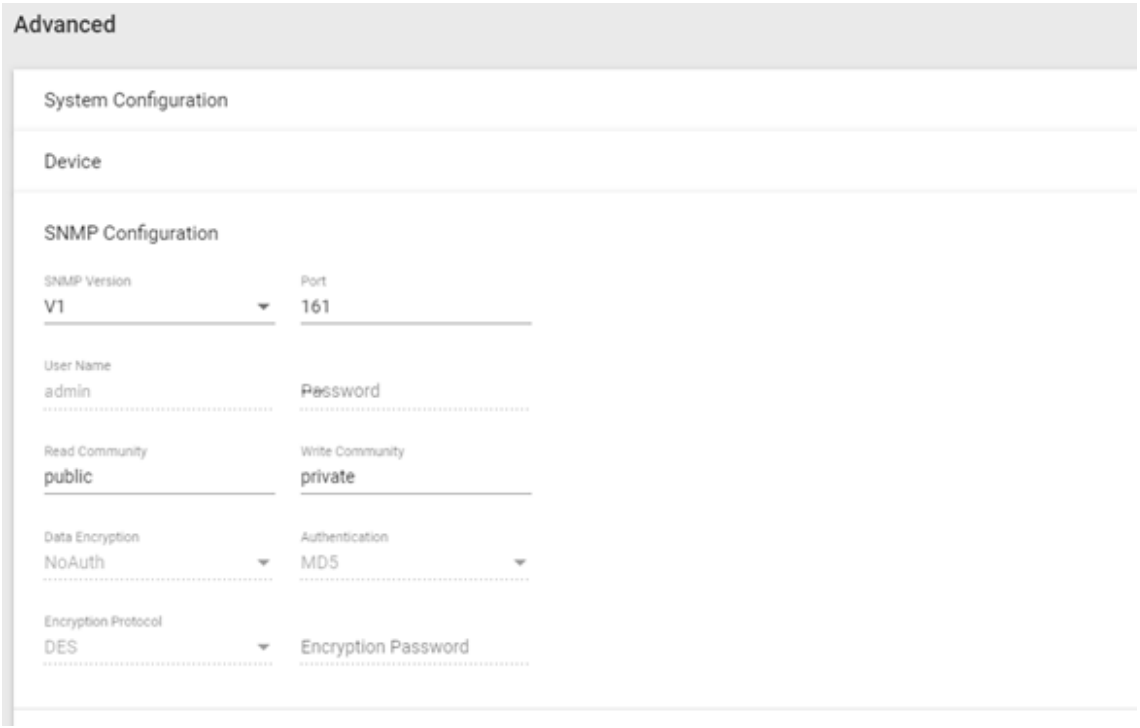


3. Configure the following ICMP polling settings:
   - **ICMP polling interval:** Specify the time in seconds between polls
   - **Consecutive failure to trigger ICMP unreachable event:** Specify the number of failed attempts before triggering the event
4. Configure the following SNMP polling settings:
   - **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.
2. In the **Advanced** section, expand **SNMP Configuration**.
   The **SNMP Configuration** settings will appear.



3. Configure the following:
   - **SNMP Version:** Select the SNMP protocol version
   - **User Name:** Specify the SNMP server username
   - **Password:** Specify the SNMP server password
   - **Read Community:** Specify the new community string
   - **Write Community:** Specify the new community string
   - **Data Encryption:** Select the data encryption method (NoAuth, AuthNoPriv, AuthPriv)
   - **Authentication:** Select the authentication method (MD5, SHA)
   - **Encryption Key:** Specify the encryption key
   - **Encryption Protocol:** Select the encryption protocol (DES, AES)
   - **SNMP Port:** Specify the SNMP port
4. Click **Save**.
   MXview updates the modified settings.

7

Topology Management

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.

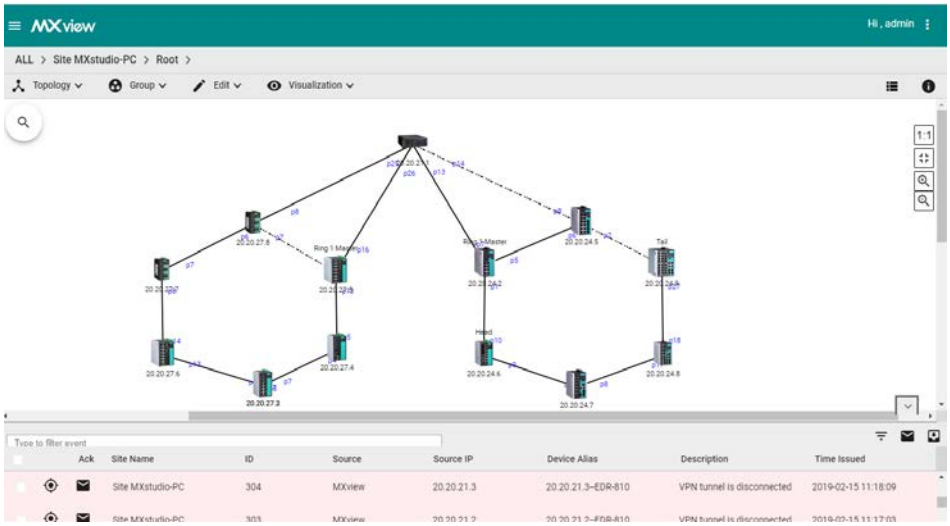
The following topics are covered in this chapter:

- **Network Topology Overview**
- **Viewing Topology Map**
- **Viewing Recent Events**
- **Organizing the Topology Structure**
- **Redundant Topologies**
- **PoE Power Consumption Visualization**
- **VPN Tunnel Visualization**
- **PRP/HSR Visualization**
- **Third-Party Icons**
- **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**

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:

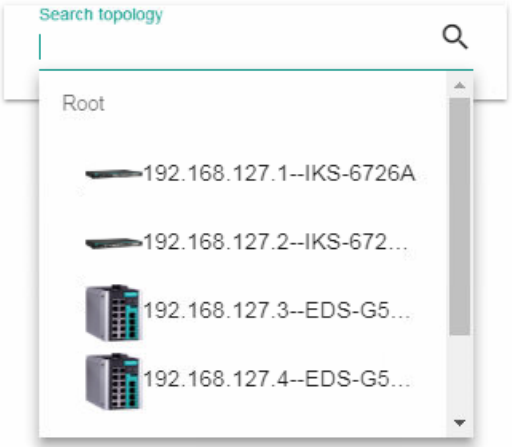
- Display a graphical representation of a real network.
- Show connecting relationships between devices.
- Indicate the status of devices and links.



Viewing Topology Map

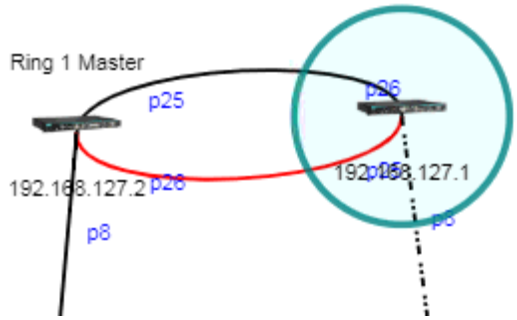
Use the **Network Topology** screen to view the Topology Map and export a PNG image of the Topology Map.

1. Navigate to **Menu** ( ) → **Network** → **Topology**.
   The **Network Topology** screen will appear and displays the Topology Map by default.
2. If **List view** is selected, click the **Topology view** ( ) 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 ( ) icon in the top left corner.
   The topology search box appears with a drop-down directory tree of the Topology Map structure.

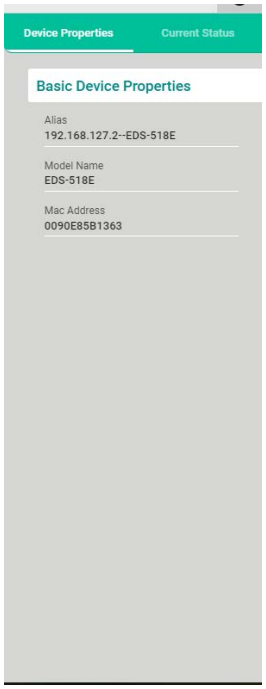


   b. Locate the device in the drop-down directory tree or type a string in the search box.

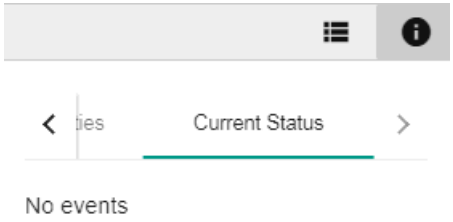
4. To view the details of a specific device, select the device in the Topology Map.



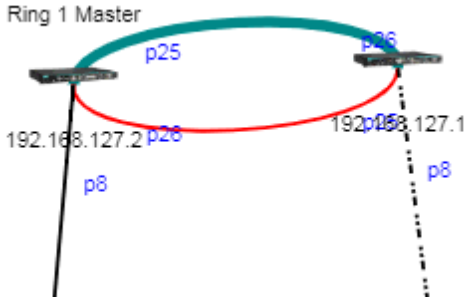
The **Device Properties** pane appears to the right of the Topology Map.



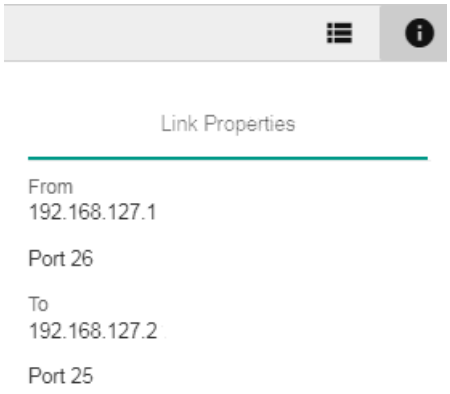
5. To view events associated with the device, click the right arrow (**>**) → **Current Status**.
The **Current Status** pane displays events associated with the device.



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.

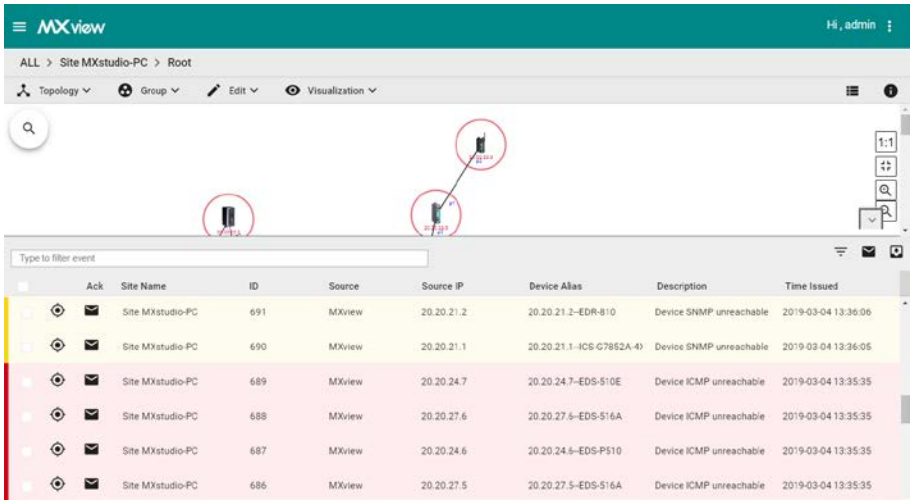


Viewing Recent Events

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.

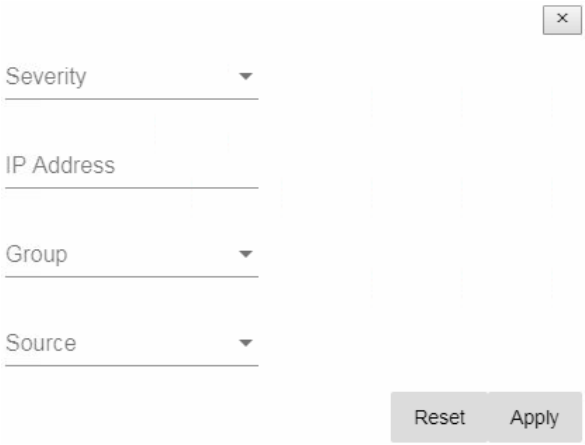
For more information on viewing all events, see **Chapter 10: Event Monitoring**.

1. Navigate to **Menu** ( ) → **Network** → **Topology**.
   The **Network Topology** screen will appear and displays the **Recent Events** panel on the bottom.

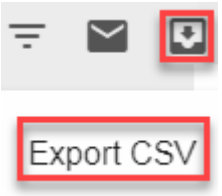


2. To filter the information in the table, type a full or partial string that matches the value in any of the table columns.
   MXview filters the table to only display events with values that fully or partially match the specified string.

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.



   b. Specify any of the following criteria:
      - **Severity:** Select the event severity level
      - **IP Address:** Select the device IP address
      - **Group:** Select the device group
      - **Source:** Select the source that detected the event (MXview, Trap, or Security Sensing)
   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 ( ) 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.
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 in the **Recent Events** tab:
   a. Click the Export ( ) icon.

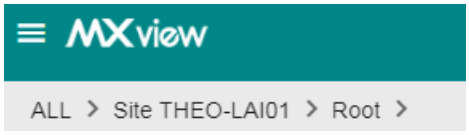


   b. Select **Export CSV**.
   c. Specify the location to save the exported file.
   d. Click **Save**.
      MXview exports the displayed event data as a CSV file.

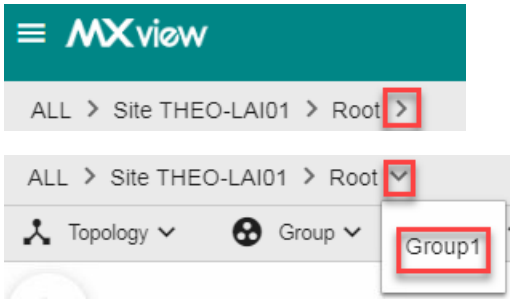
Organizing the Topology Structure

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:

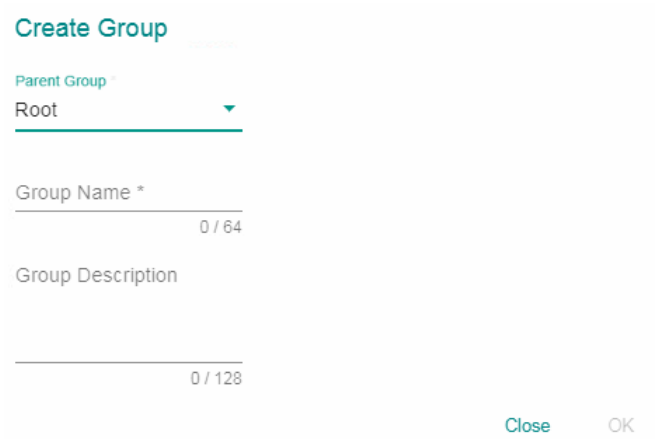
   - You can also click the following icon used to indicate user-defined groups within the Topology Map:

2. If **List view** is selected, click the **Topology view** ( ) 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.

b. Configure the following:

- **Parent Group**
- **Group Name**
- **Group Description**

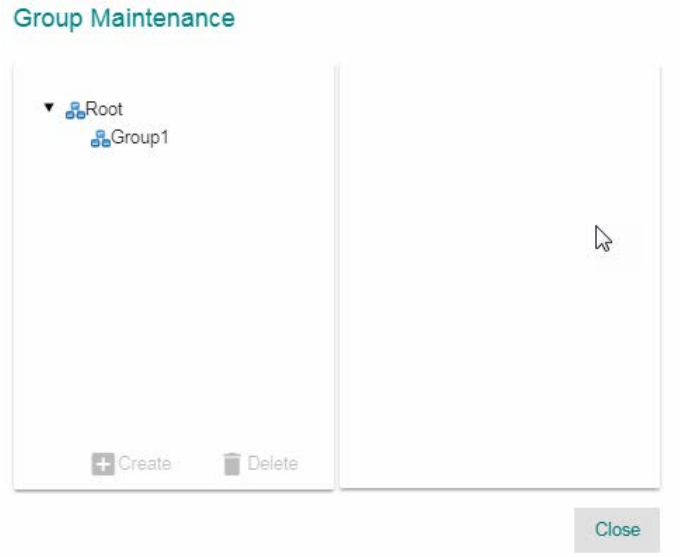
c. Click **OK**.

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

4. To reorganize the groups within the Topology Map structure:

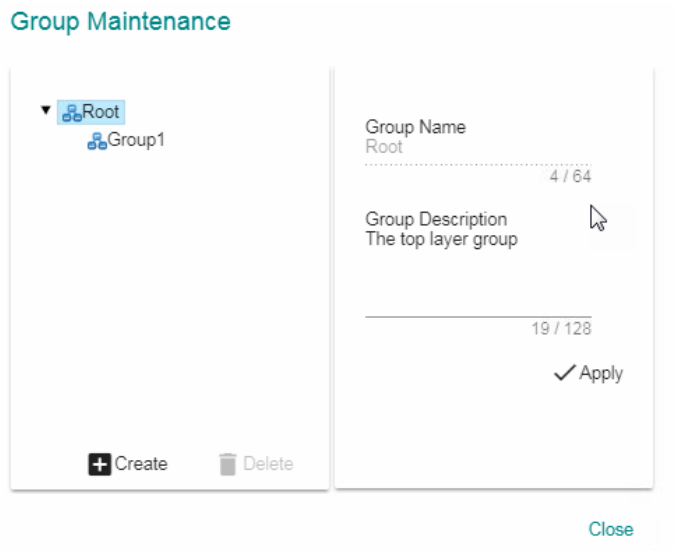
a. Navigate to **Group → Group Maintenance**.

The **Group Maintenance** screen appears.



b. Select a layer to modify.

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



c. Edit the group details or perform one of the following points:

d. (Optional) Click **Create** to add a new group below the selected layer.

e. (Optional) Click **Delete** to remove a group from the topology structure.

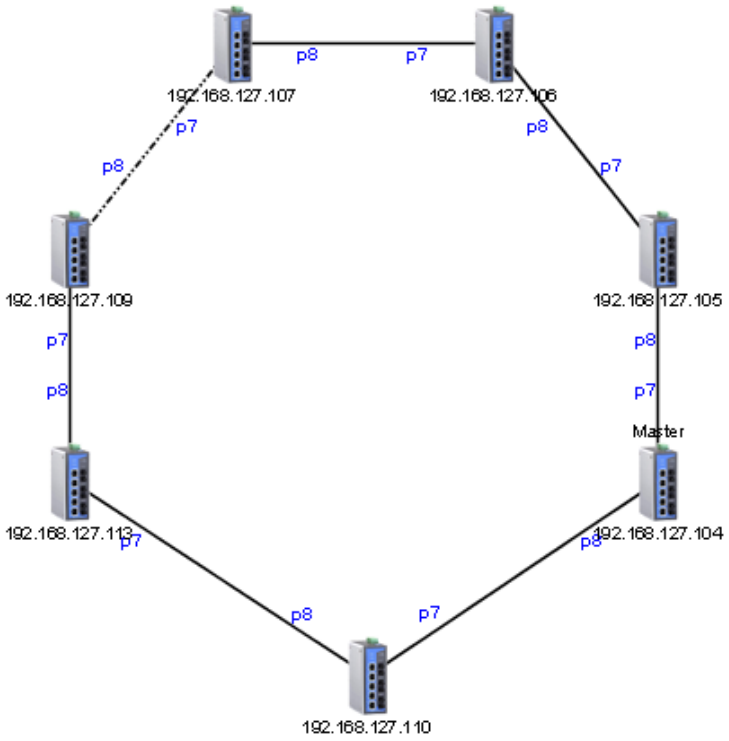
f. Click **Apply**.

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

   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:



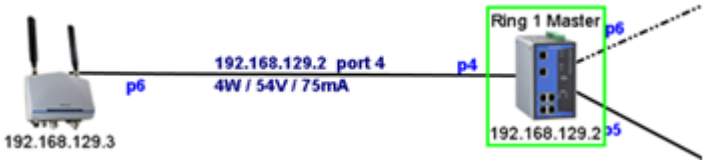
For devices that play a particular role in the topology, MXview will label the devices by displaying the roles above the images of the devices. Backup links will be indicated with dashed lines.

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

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

PoE Power Consumption Visualization

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



VPN Tunnel Visualization

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

- **Blue:** All VPN tunnels are connected

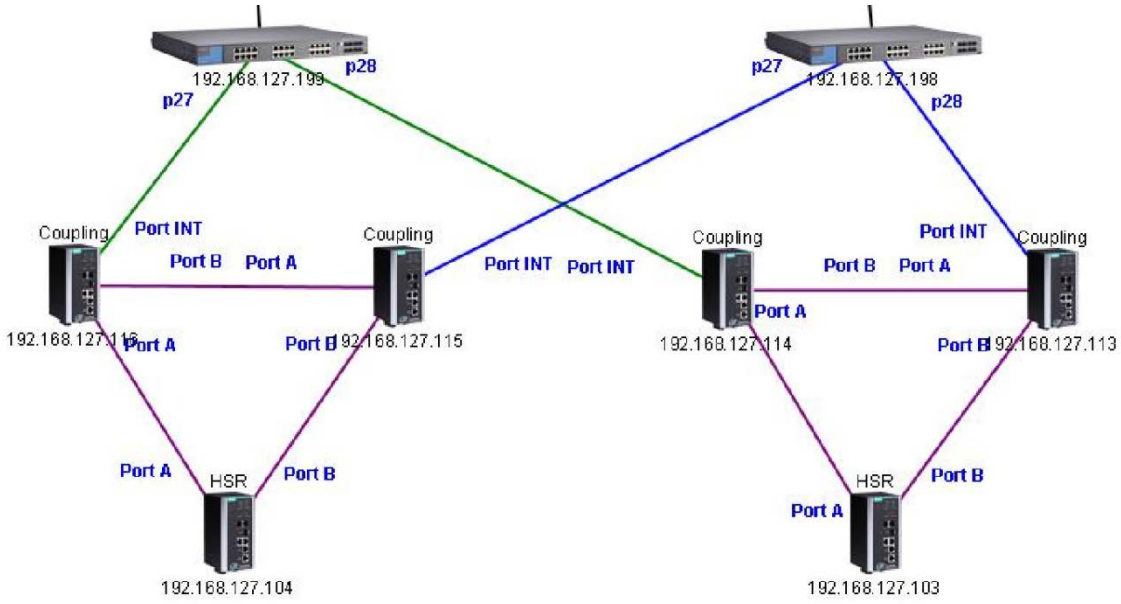
- **Yellow:** At least one VPN tunnel is disconnected

- **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 and PT-7728-PTP Series. (PT-7728-PTP support starts at version 2.9)

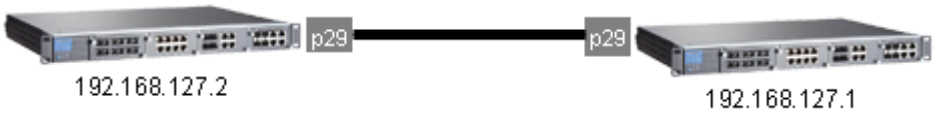
Third-Party Icons

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.

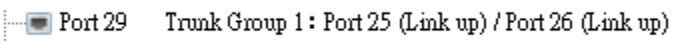
Port Trunking

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.

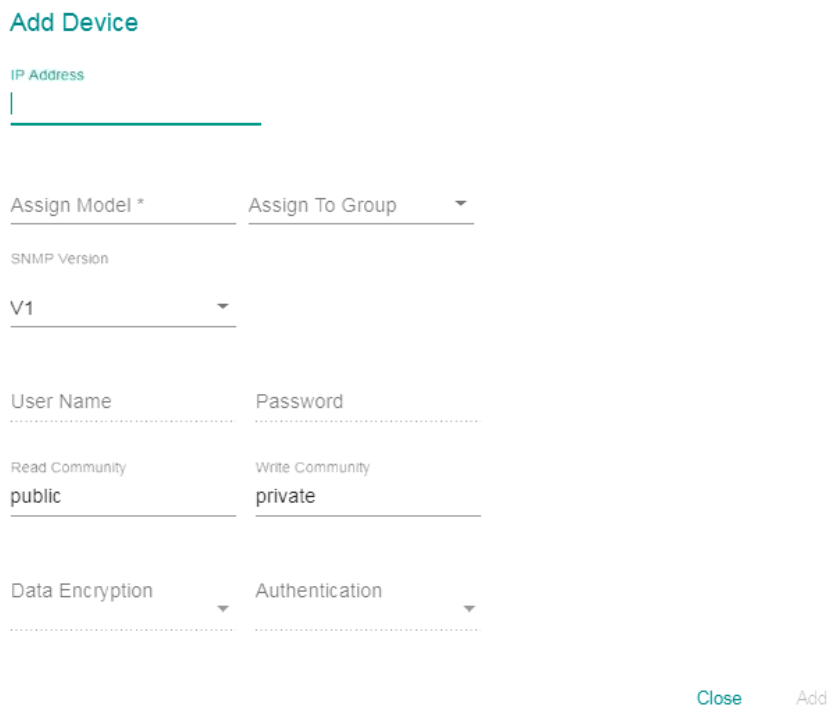


Adding Devices and Links

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.

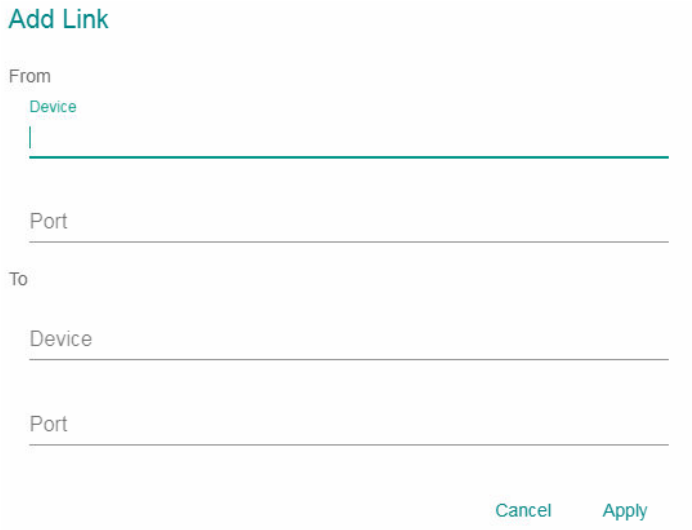
For information about List View, see **Chapter 9: Device Management > Viewing the Device List**.

1. Navigate to **Menu** ( ) → **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.



   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 **Apply**.
      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.

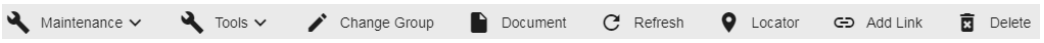
NOTE	Port numbers must be numeric and entered correctly to obtain the correct traffic information.

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

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.

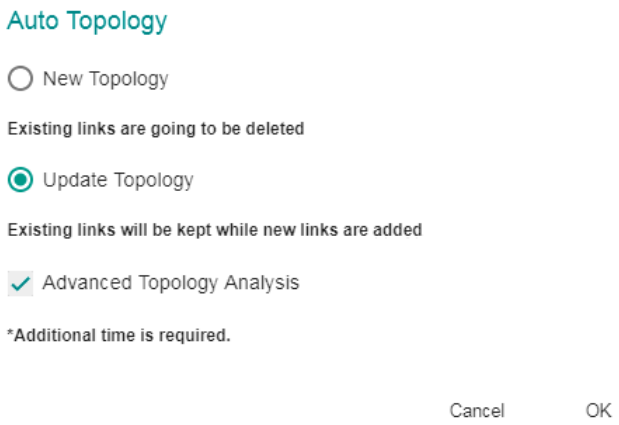
   b. Click **Delete**.
      A confirmation screen will appear.
   c. Click **OK**.
      MXview deletes the link from the Topology Map.

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** ( ) 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.

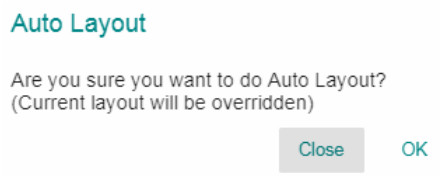


4. Select **Update Topology**.
5. (Optional) Select **Advanced Topology Analysis** to draw links for devices without an LLDP MIB.
6. Click **OK**.
   MXview will update the Topology Map.

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.

1. Navigate to **Menu** ( ) → **Network** → **Topology**.
   The **Network Topology** screen will appear and displays the Topology Map by default.
2. If **List view** is selected, click the **Topology view** ( ) 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.



4. Click **OK**.
   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.

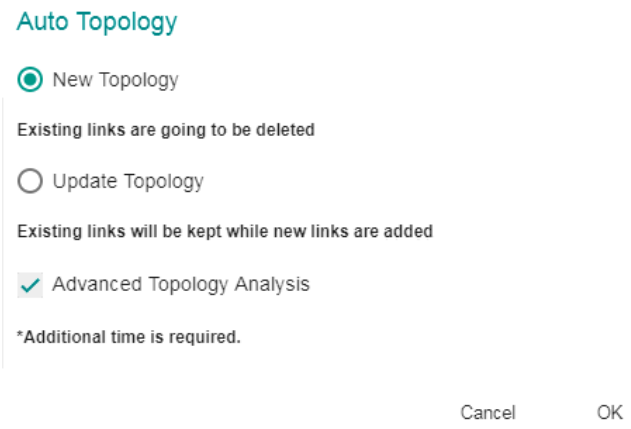
For devices with LLDP functionality, MXview can draw the physical topology map, down to the port level of the devices. For devices without an LLDP MIB, MXview is able to draw links by using ARP. To activate this function, select the **Advanced Topology Analysis** checkbox from the **Auto Topology** screen.

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.

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** ( ) 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.

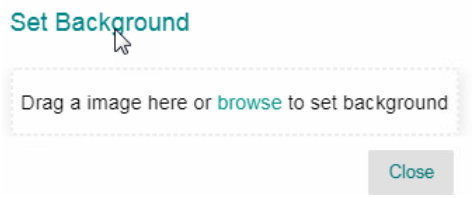


4. Select **New Topology**.
5. (Optional) Select **Advanced Topology Analysis** to draw links for devices without an LLDP MIB.
6. Click **OK**.
   MXview will create a new Topology Map.

Setting / Deleting the Background Image

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

1. Navigate to **Menu** ( ) → **Network** → **Topology**.
   The **Network Topology** screen appears and will display the Topology Map by default.
2. If **List view** is selected, click the **Topology view** ( ) 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** → **Set Background**.
   The **Set Background** screen appears.



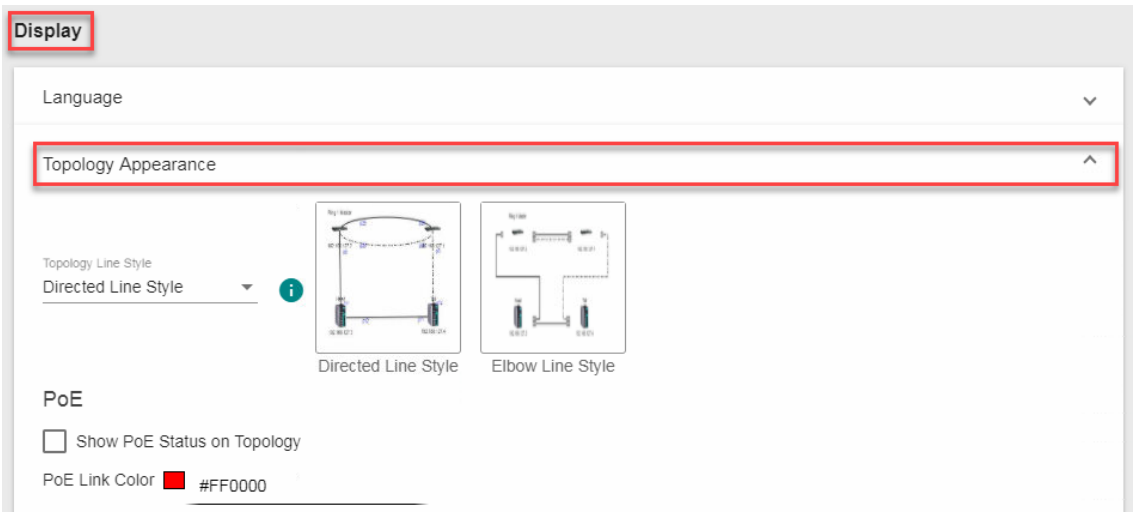
4. Upload the background image by using one of the following methods:
   - Drag and drop an image file into designated area on the **Set Background** screen.
   - Click browse on the **Set Background** screen to locate the file on your local machine.

   MXview will set the uploaded image as the Topology Map background.
5. To delete a background image, navigate to **Edit** → **Delete Background** and click **OK**.
   MXview will remove the background image from the Topology Map.

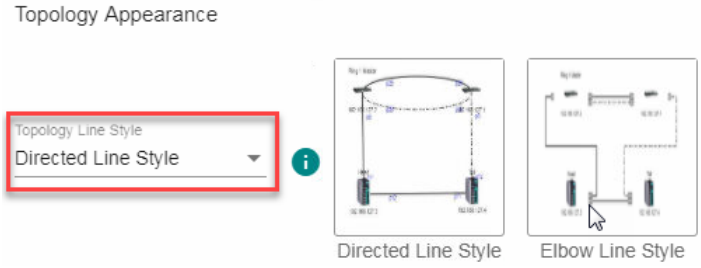
Editing the Topology Appearance

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



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

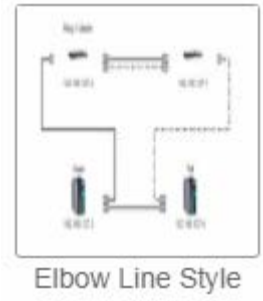


- **Directed Line Style**

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

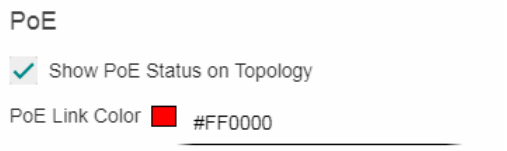
- **Elbow Line Style**

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

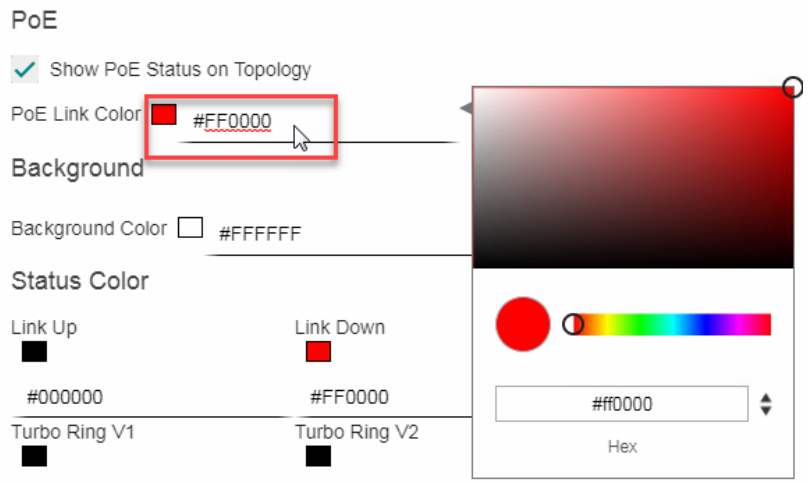


4. To modify how MXview displays Power-over-Ethernet (PoE) links:

   a. Select the **Show PoE Status on Topology** check box to indicate the PoE link status on the Topology Map.

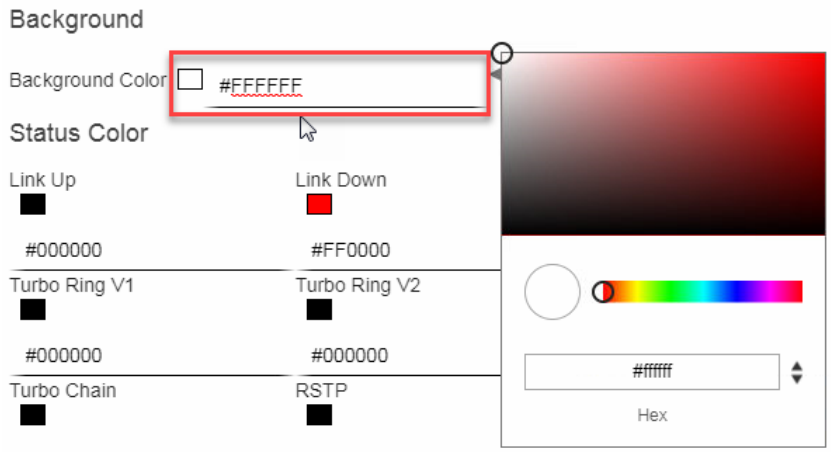


   b. Click the **PoE Link Color** field and specify a new color.



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

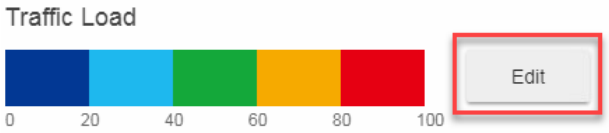
5. To modify the Topology Map background, click the **Background Color** field and specify a new color.



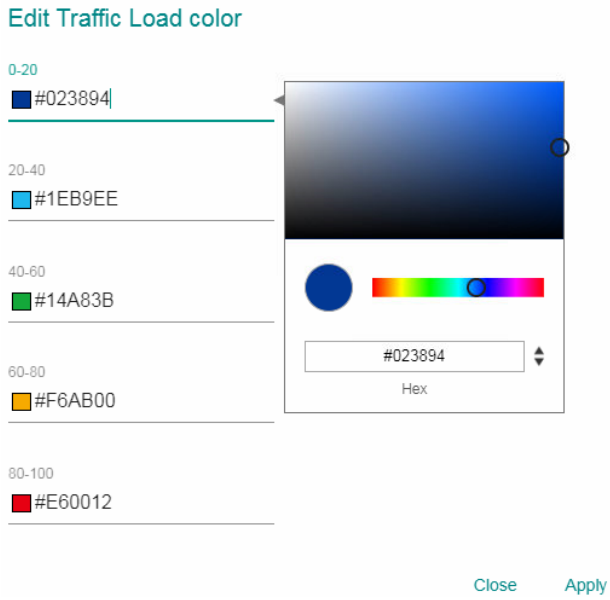
6. To modify the color used to indicate the status of specific links in the Topology Map, click to modify the **Status Color** hex code for any of the following links:

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

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



   The **Edit Traffic Load Color** screen will appear.

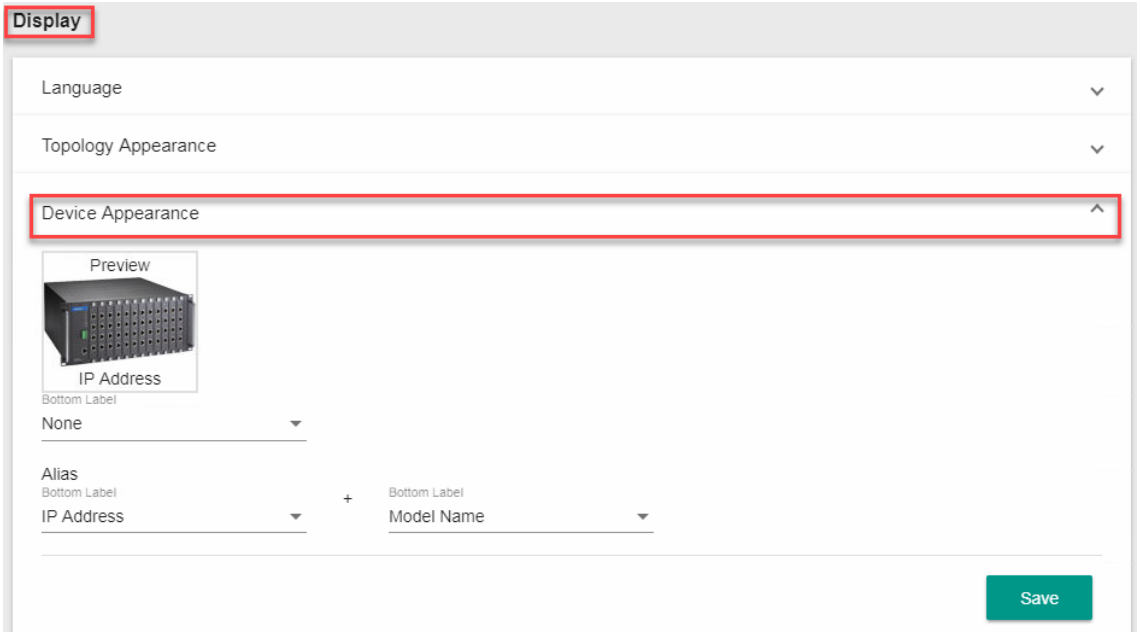


   b. Modify the color used to indicate a traffic load (%) range.
   c. Click **Apply**.
8. Click **Save**.
   MXview will update the modified settings.

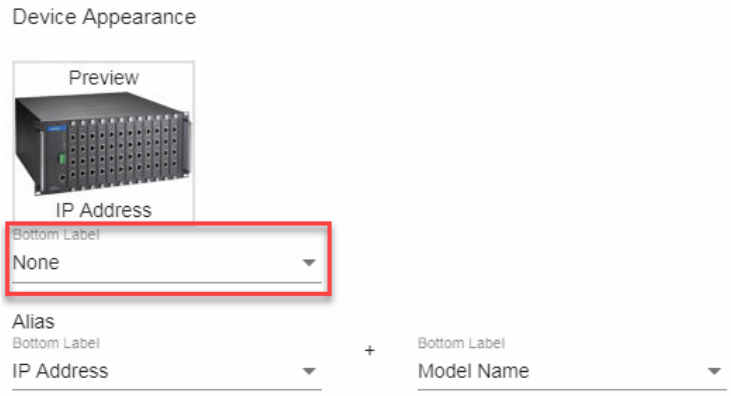
Editing the Device Appearance

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

1. Navigate to **Menu** ( ) → **Preferences**.
   The **Preferences** screen will appear.
2. In the **Display** section, expand **Device Appearance**.
   The **Device Appearance** settings will appear.



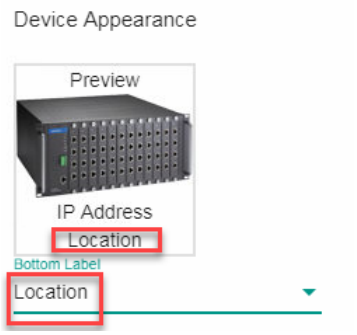
3. To modify the label that indicates the device in the Topology Map:
   a. Locate the **Bottom Label** drop-down list located below the **Preview** image:



b. Select one of the following properties from the **Bottom Label** drop-down:

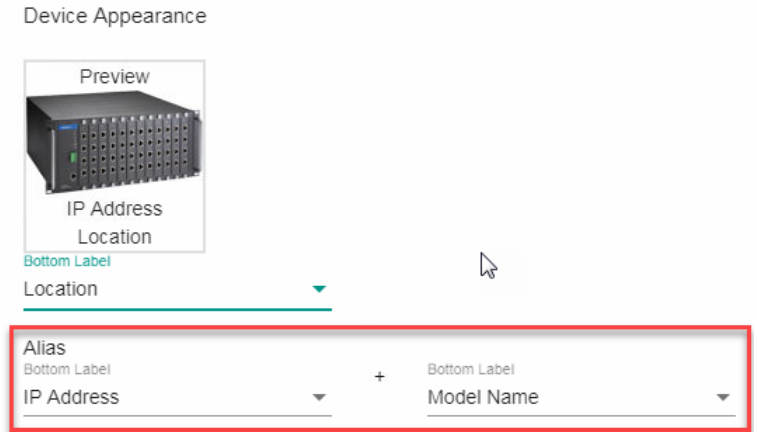
- **Location**
- **Alias**
- **Model Name**
- **MAC**

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



4. To modify the device alias:

a. Locate the **Alias** section.



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

- **IP Address**
- **MAC**
- **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** ( ) → **Network** → **Topology**.
   The **Network Topology** screen appears and displays the Topology Map by default.
2. If **List view** is selected, click the **Topology view** ( ) 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**.
4. Specify the location to save the exported file.
5. Click **Save**.
   MXview exports the PNG image of the Topology Map to the specified location.

8

Network and Traffic Monitoring

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.

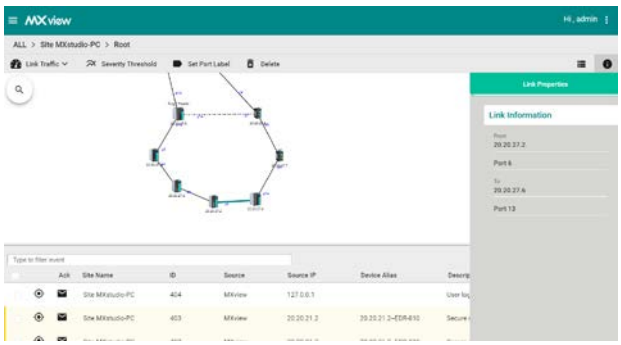
The following topics are covered in this chapter:

- **Viewing Link Properties**
- **Viewing Port Traffic**
- **Viewing Packet Error Rates**
- **Monitoring Traffic Loads**
- **Monitoring Network Security**
- **Visualizing VLAN Connections**
- **Monitoring Wireless Access Points and Clients**
- **Configuring Severity Thresholds for Traffic Monitoring Events**
- **Configuring Custom Port Labels**

Viewing Link Properties

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

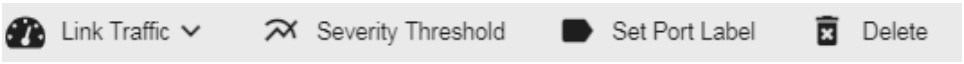
1. Navigate to **Menu** ( ) → **Network** → **Topology**.
   The **Network Topology** screen will appear and display the Topology Map by default.
2. Click on a link between devices in the Topology Map.
   The **Link Properties** pane appears to the right of the Topology Map.



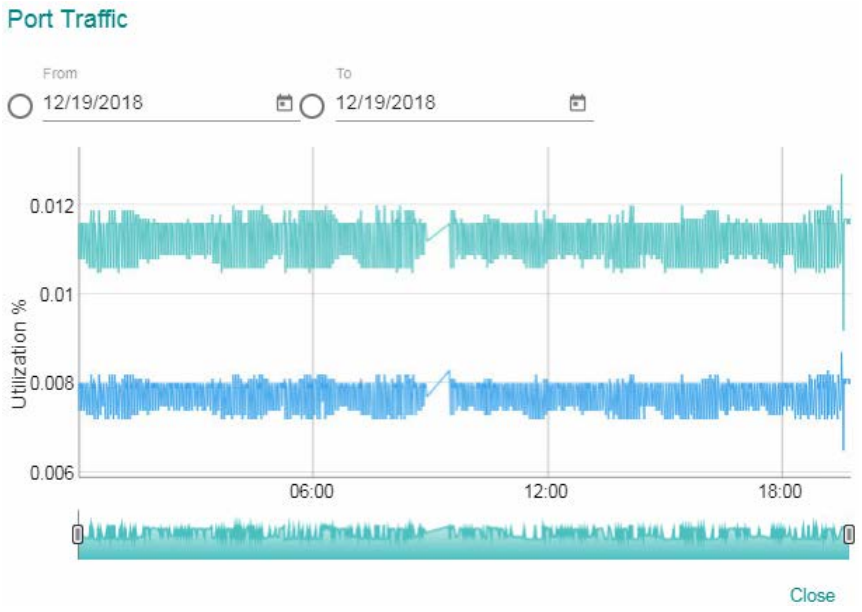
Viewing Port Traffic

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** ( ) → **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.

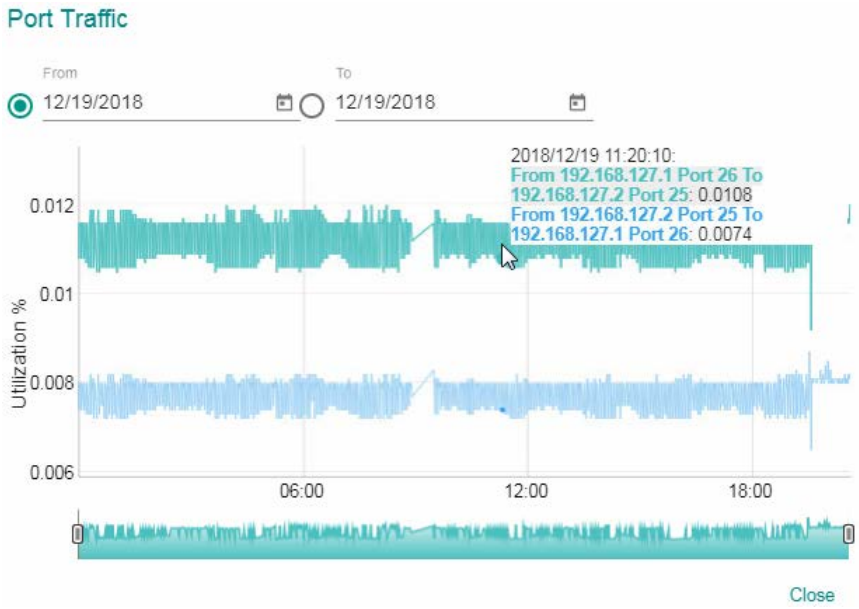


3. Navigate to **Link Traffic** → **Port Traffic**.
   The **Port Traffic** screen will appear.



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.

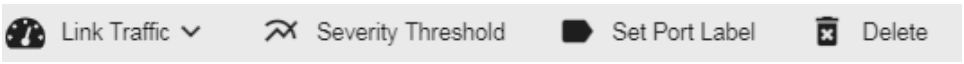
5. Hover over a line to view the direction of traffic.
   For example, the green line at the top of the following graph represents traffic from 1**92.168.127.1 (device IP address) Port 26 to 192.168.127.2 (device IP address) Port 25**.



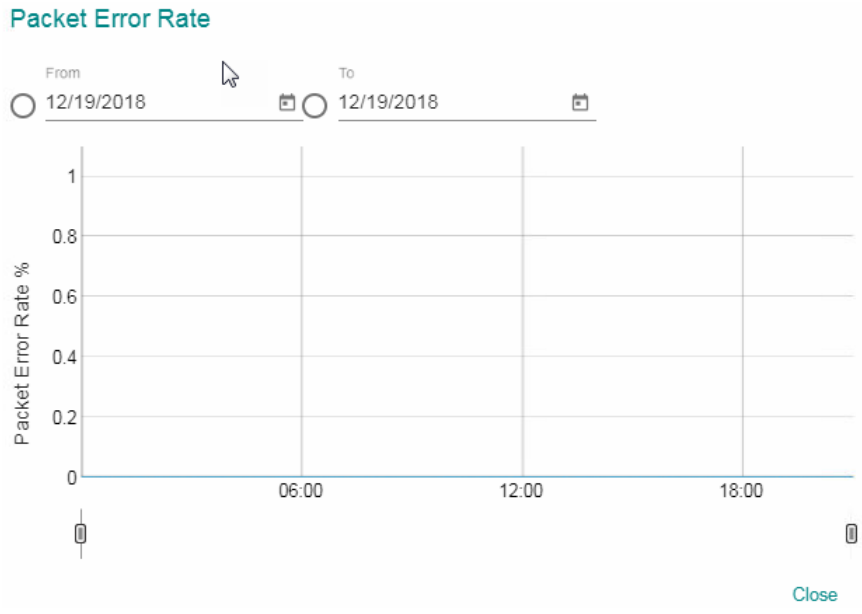
Viewing Packet Error Rates

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.

1. Navigate to **Menu** ( ) → **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 toolbar appear when a link is selected.



3. Navigate to **Link Traffic** → **Packet Error Rate**.
4. The **Packet Error Rate** screen appears.

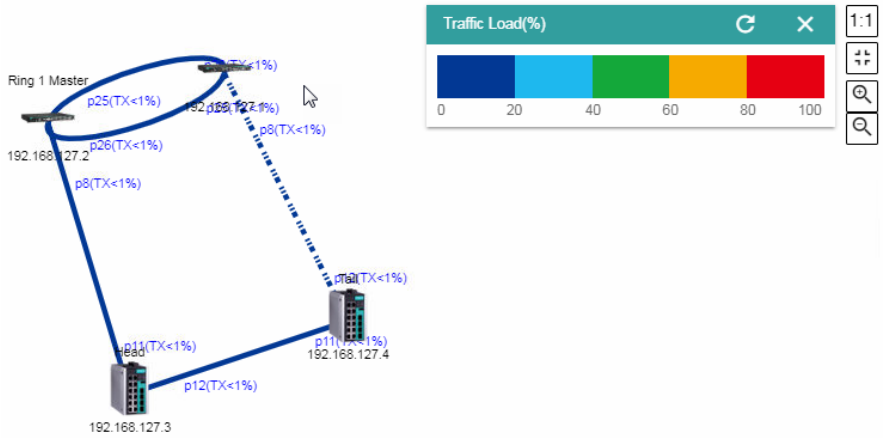


5. To adjust the time period for the graph data:
   a. Click the **From** date and select a new starting date.
   b. Click the **To** date and select a new ending date.

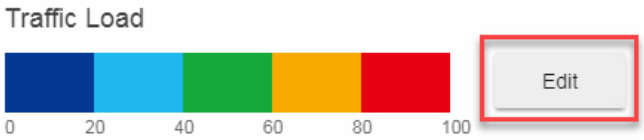
Monitoring Traffic Loads

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

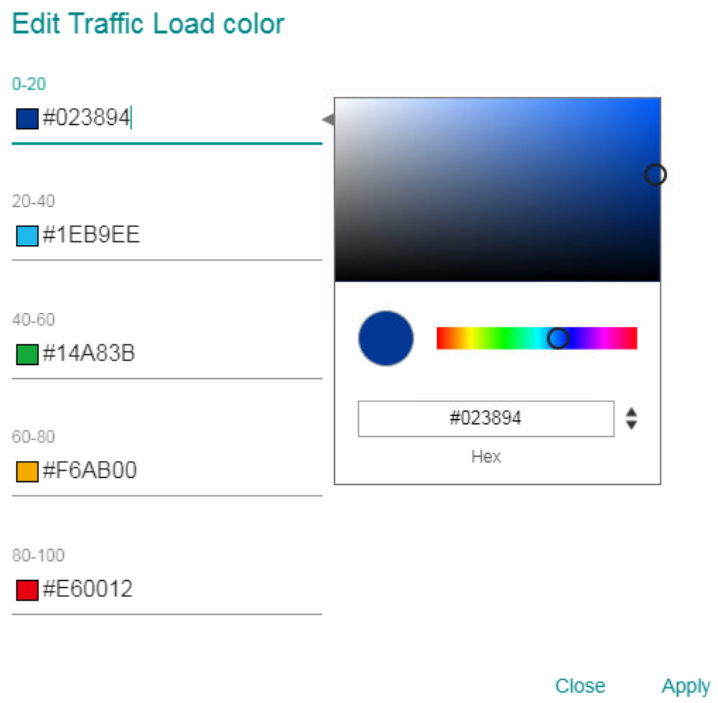
1. Navigate to **Menu** ( ) → **Network** → **Topology**.
   The **Network Topology** screen will appear and displays the Topology Map by default.
2. If **List view** is selected, click the **Topology view** ( ) icon in the top right corner.
   The **Network Topology** screen will display a graphical 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**.



The E**dit Traffic Load Color** screen appears.



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 component-level requirements.

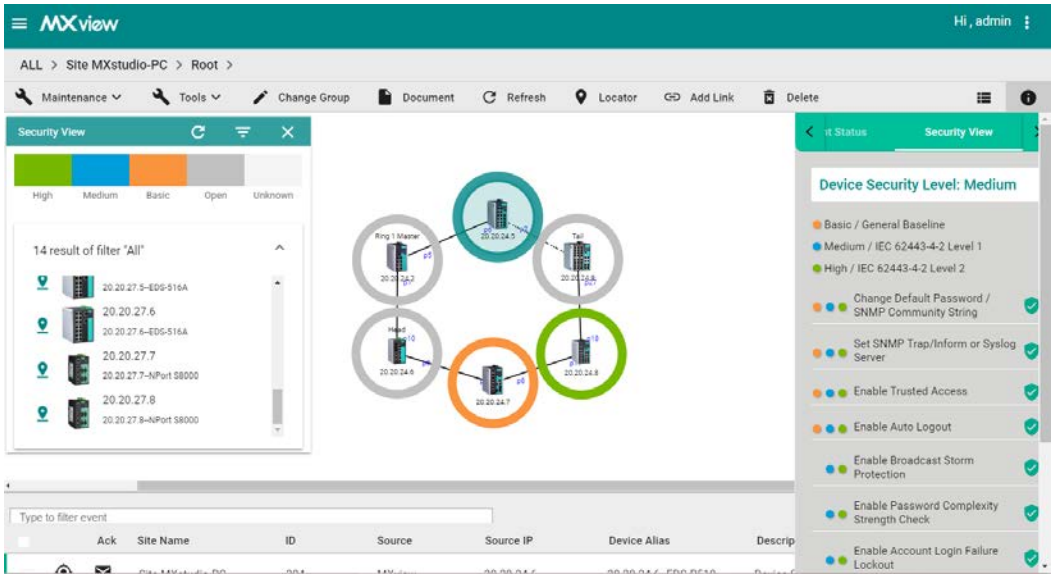
Moxa's MXview follows Moxa's security guidelines, which are based on the current IEC 62443-4-2 component-level recommendations. Security View checks the security level of Moxa's network devices. There are five levels for checking the results in Security View:

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

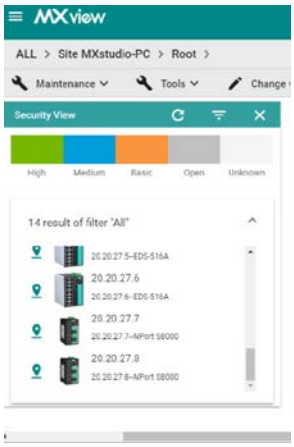
NOTE The definition of general baseline is based on several industrial cybersecurity policies and requirements.

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

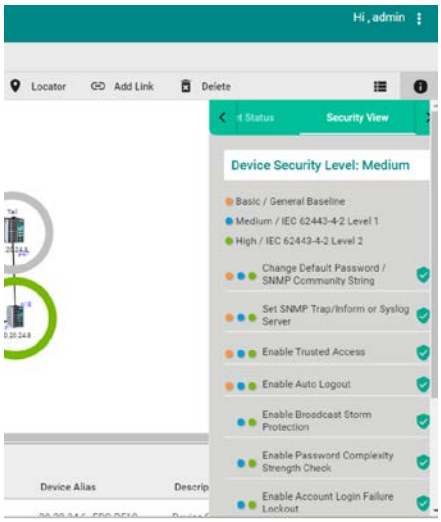
3. From the toolbar menu, navigate to **Visualization → Security View**.
   The **Security View** window will appear and the Topology Map indicates the security level of each device with a color-coded circle.



4. To filter the devices in the **Security View** window by security level:
   a. Click the **Filter** ( ) 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.



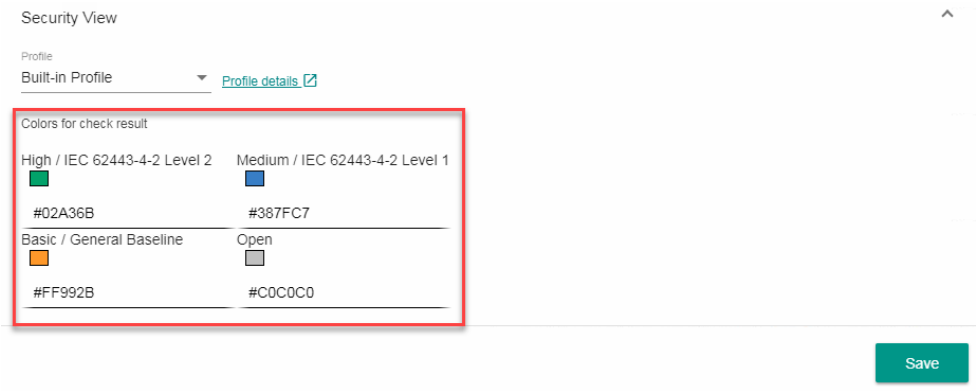
6. View security details for a specific device by using one of the following methods:
   - Select a device from the Topology Map.
   - Select a device from the **Security View** window.

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

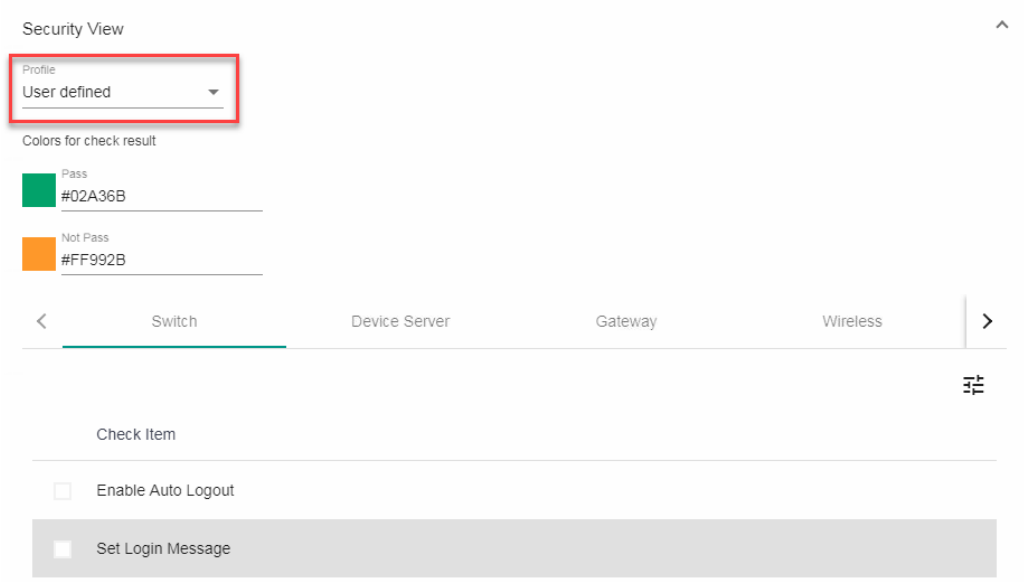
7. Review the following items in the **Security View** details pane:

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

8. To modify the colors used to indicate the security levels:
   a. Navigate to **Menu** ( ) → **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.



   d. Click **Save**.
9. 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.

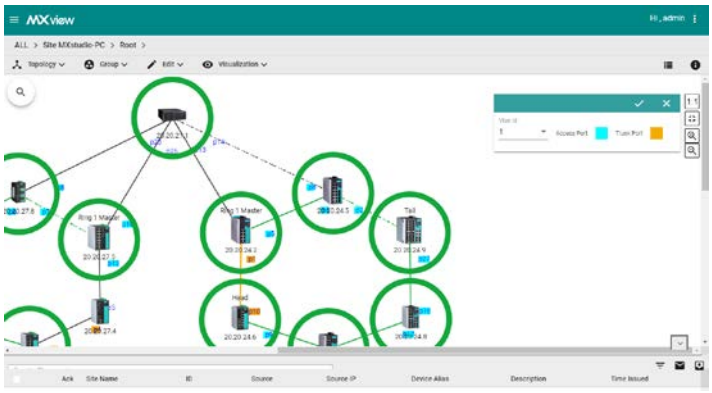


   d. (Optional) Modify the colors for the check result.
   e. Click one of the following device tabs to configure the profile settings:
      - **Switch**
      - **Device Server**
      - **Gateway**
      - **Wireless**
   f. (Optional) Click the **Settings** ( ) icon to select a baseline.
   g. Select 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.

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** ( ) 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.



4. Selecting a specific VLAN ID.
   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

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.

1. Navigate to **Menu** ( ) → **Network** → **Topology**.
   The **Network Topology** screen will appear and displays the Topology Map by default.
2. If **List view** is selected, click the **Topology view** ( ) 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** → **Wireless Table View**.
   The **Wireless Table View** screen appears.

4. To view details for a specific device, select the device from the table.
   The wireless device details pane appears.

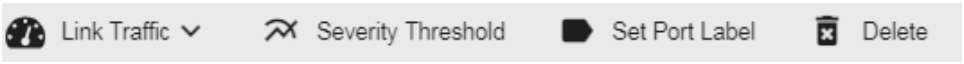
Configuring Severity Thresholds for Traffic Monitoring Events

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

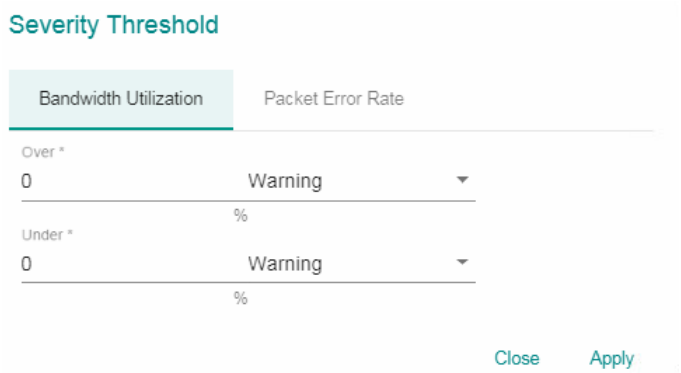
- Bandwidth utilization is over a threshold.
- Bandwidth utilization is under a threshold.
- Packet error rate is over a threshold.

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** ( ) → **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.



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**
      - **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. Click **Apply**.

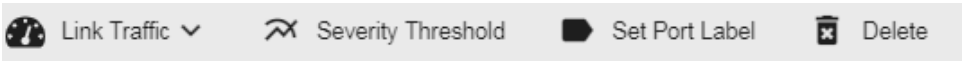
Configuring Custom Port Labels

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

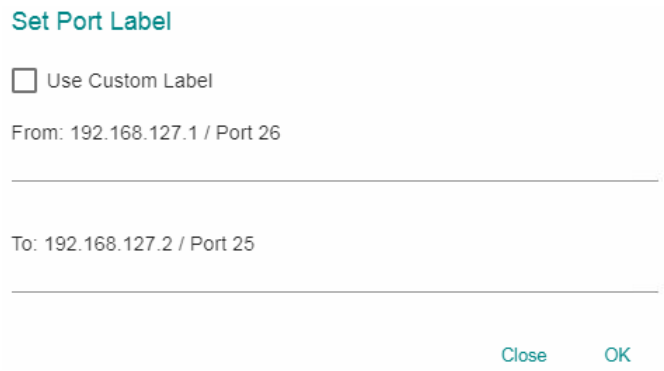
<Device IP Address> / <Port Number>

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

1. Navigate to **Menu** ( ) → **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 Set Port Label.
   The **Set Port Label** screen appears.



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 **OK**.

9

Device Management

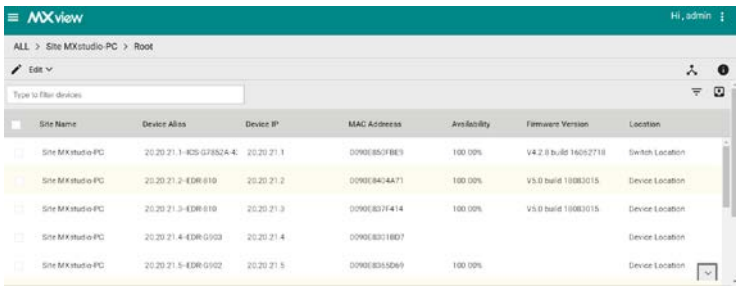
The MXview **Network Topology** screen provides several features and tools for managing and maintaining devices in your network topology.

The following topics are covered in this chapter:

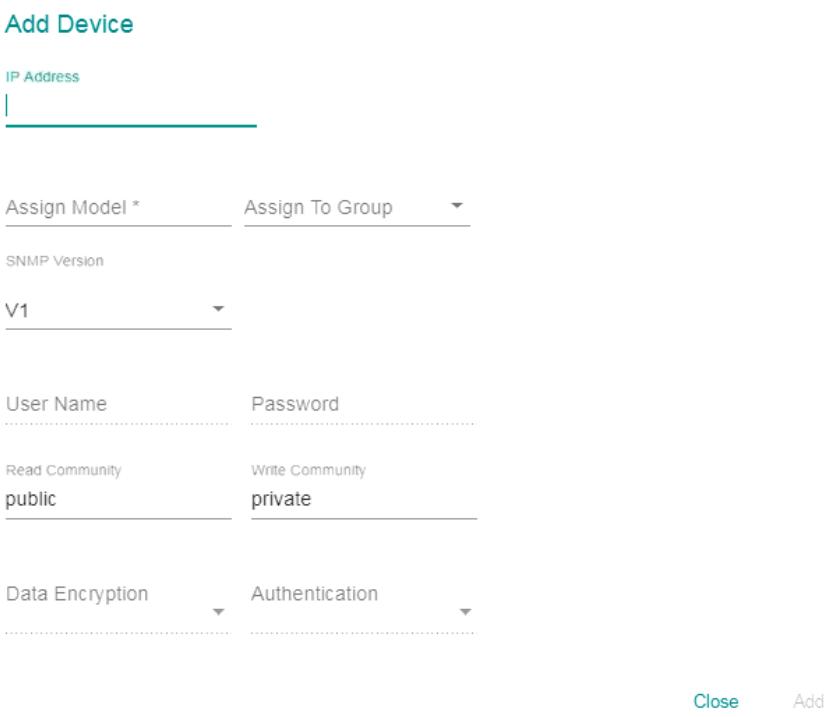
- **Viewing the Device List**
- **Importing Device Configurations**
- **Exporting Device Configurations**
- **Upgrading Firmware**
- **Generating a QR Code for the Device**
- **Assigning a Device Model**
- **Configuring Basic Device Information**
- **Configuring Device IP Settings**
- **Configuring SNMP Trap Servers**
- **Configuring Port Settings**
- **Configuring SNMP Settings**
- **Configuring Polling Settings**
- **Configuring Advanced Settings**
- **Configuring Polling IP Settings**
- **Changing the Device Icon**
- **Signing on to Device Web Consoles**
- **Pinging Devices**
- **Changing Device Groups**
- **Uploading Device Documents**
- **Refreshing the Device Status**
- **Locating Devices**
- **Deleting Devices**

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.



1. Navigate to **Menu** ( ) → **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.

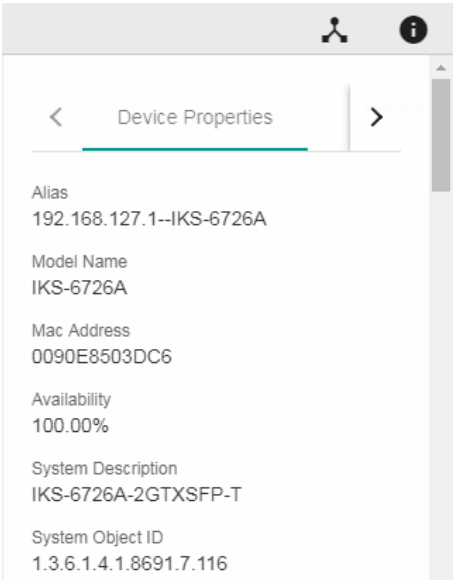


   b. Configure the following:
      - **IP Address:** Specify the IP address of the device
      - **Assign Model:** Select the model of the device
      - **Assign To Group:** Select the group to assign the device to
      - **SNMP Version:** Select the SNMP version
      - **User Name:** Specify the 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.



5. To filter the device list by severity level:

a. a. Click the **Filter** ( ) icon in the top right corner.
The **Severity** drop-down list appears.

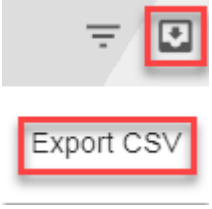
b. Select one of the following severity levels:

- **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.

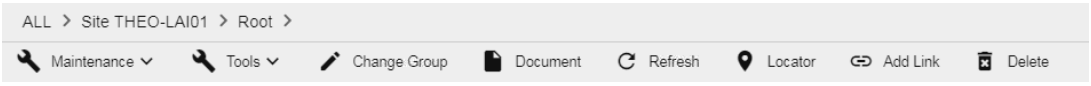
d. Click **Save**.
MXview will export the displayed data as a CSV file.

Importing Device Configurations

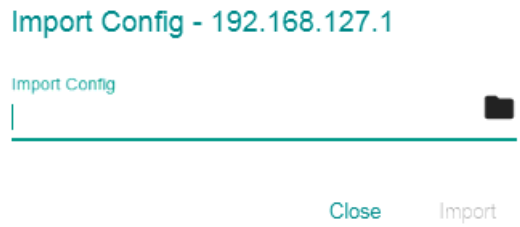
Use the **Network Topology** screen to import an INI-formatted configuration file to a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

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.



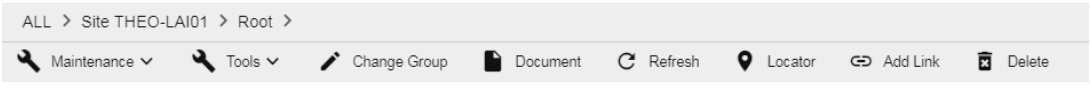
5. Click the folder ( ) icon to upload the configuration file from your local machine.
6. Click **Import**.
   MXview imports the configuration file to the specified device.

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**.

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 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.



4. Navigate to **Maintenance** → **Export Config**.
   The **Export Config** screen will appear and indicate the IP address of the selected device.

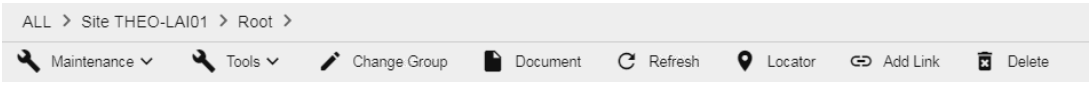
5. Click **Export**.
6. Specify the location to save the configuration file.
7. Click **Save**.
   MXview saves the device configurations as an INI file in the specified location.

Upgrading Firmware

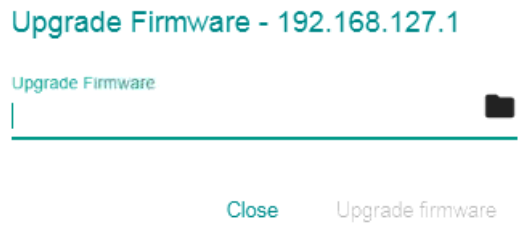
Use the **Network Topology** screen to upgrade the firmware (ROM-formatted file) on a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

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



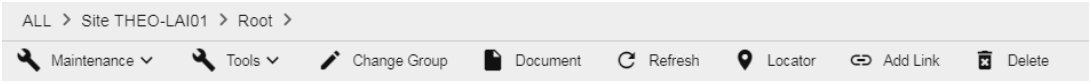
5. Click the folder ( ) icon to upload the ROM-formatted firmware file from your local machine.
6. Click **Upgrade firmware**.
   MXview will upgrade the firmware on the specified device.

Generating a QR Code for the Device

MXview allows you to generate a QR code that be can 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** ( ) → **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.



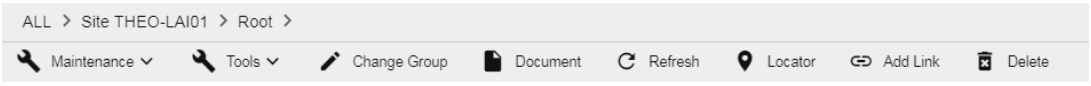
4. Navigate to **Maintenance** → **Generate QR Code**.
5. Specify the location to save the QR code.
6. Click **Save**.
   MXview will save a zipped PNG file of the QR code to the specified location.
7. Print the QR code and attach it to the device.
8. Scan the QR code by using the **MXview ToGo** mobile 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** ( ) → **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.



4. Navigate to **Maintenance** → **Assign Model**.
   The **Assign Model** screen appears.

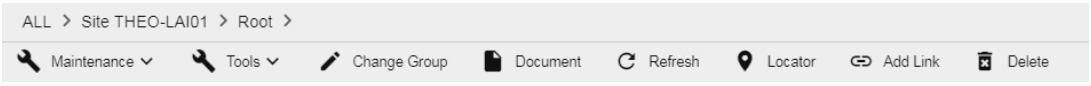
5. Select the device model from the drop-down list.
6. Click **Apply**.
   MXview assigns the selected model to the device.

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** ( ) → **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.

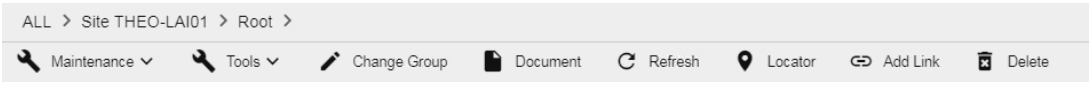
5. Specify the following device information:
   - **Model**
   - **Location**
   - **Contact**
6. Click **Apply**.
   MXview will update the device information.

Configuring Device IP Settings

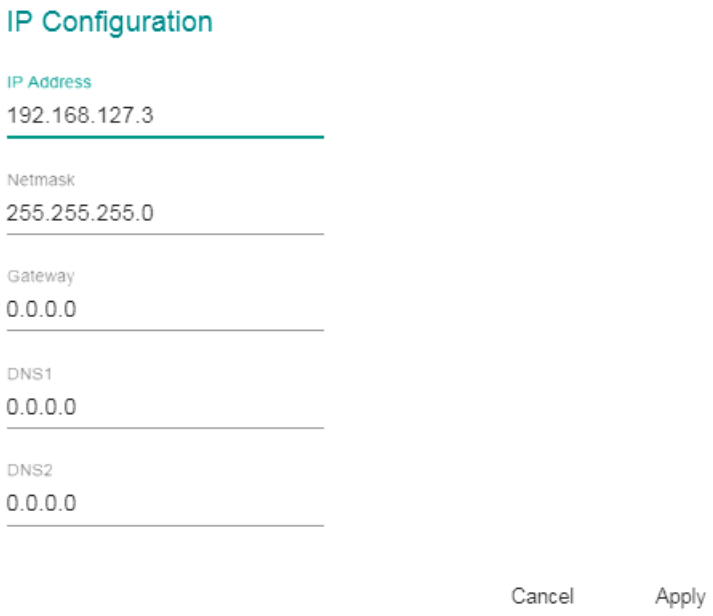
Use the **Network Topology** screen to configure IP settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to **Menu** ( )→ **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.



4. Navigate to **Maintenance** → **IP Configuration**.
   The **IP Configuration** screen will appear.



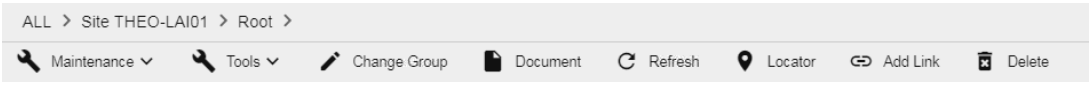
5. Specify the following IP configurations:
   - **IP Address**
   - **Netmask**
   - **Gateway**
   - **DNS1**
   - **DNS2**
6. Click **Apply**.
   MXview updates the device IP configurations.

Configuring SNMP Trap Servers

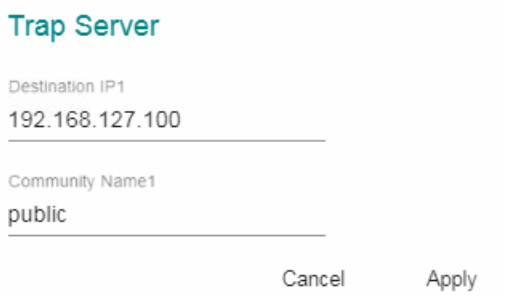
MXview can collaborate with other network management software and send SNMP Traps to non-Moxa NMS. MXview supports up to two trap servers depending on the device.

1. Navigate to **Menu** ( ) → **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 **Maintenance** → **Trap Server**.
   The **Trap Server** screen appears.



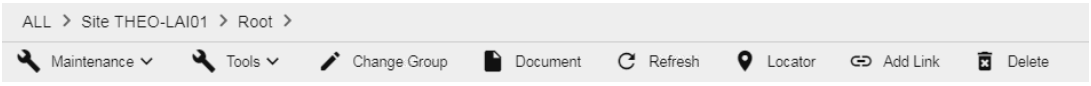
5. Configure the following SNMP trap server settings for the device:
   - **Destination IP1**
   - **Community Name1**
   - (Optional) **Destination IP2**
   - (Optional) **Community Name2**
6. Click **Apply**.
   MXview sends SNMP traps to the configured trap server(s) when events are detected on the device.

Configuring Port Settings

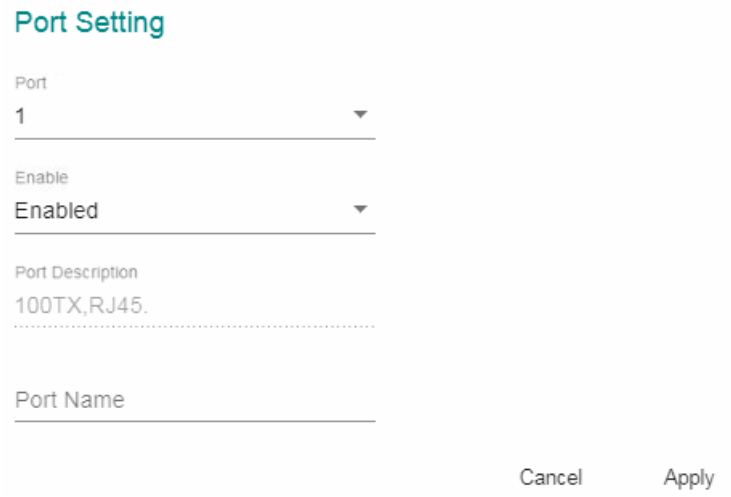
Use the **Network Topology** screen to configure port settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to **Menu** ( ) → **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. Navigate to **Maintenance** → **Port Settings**.
   The **Port Setting** screen appears.



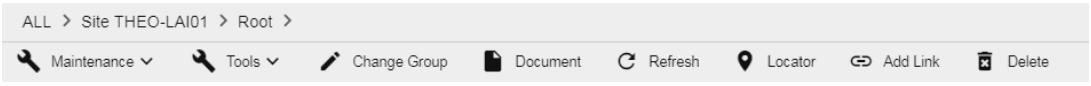
5. Configure the following port settings for the device:
   - **Port:** Select the port number.
   - **Enable:** Enable or disable the port.
   - **Port Description:** Provide a description of the port.
   - **Port Name:** Provide a custom name for the port.
   - **Apply settings to another port:** Select 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

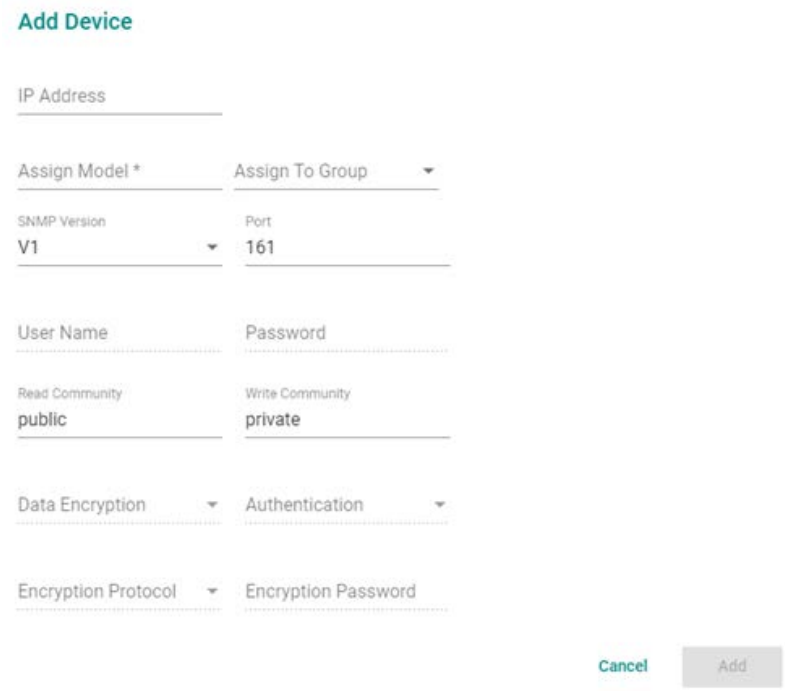
Use the **Network Topology** screen to configure SNMP settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to **Menu** ( ) → **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. Navigate to **Maintenance** → **SNMP Settings**.
   The **SNMP Configuration** screen will appear.



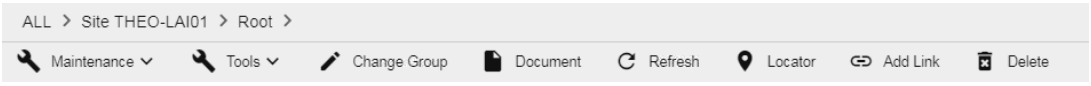
5. Configure the following SNMP settings for the device:
   - **SNMP Version**
   - **User Name**
   - **Password**
   - **Read Community**
   - **Write Community**
   - **Data Encryption**
   - **Authentication**
   - **Encryption Key**
   - **Encryption Protocol**
   - **SNMP Port**
6. Click **Apply**.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

Configuring Polling Settings

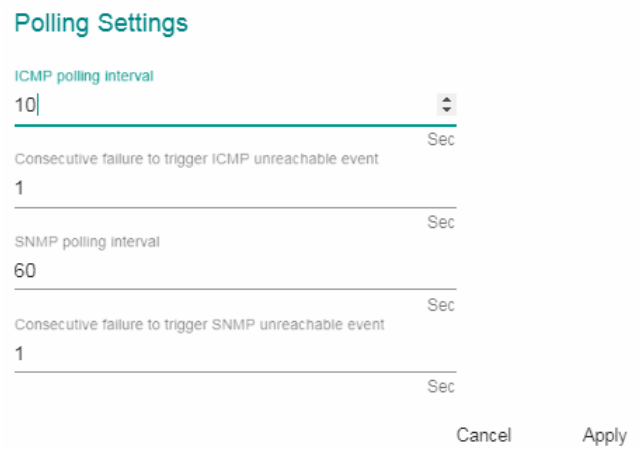
Use the **Network Topology** screen to configure ICMP or SNMP polling settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

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.



4. Navigate to **Maintenance** → **Polling Settings**.
   The **Polling Settings** screen appears.

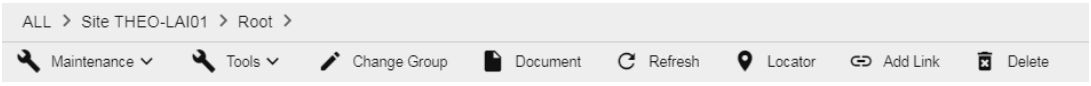


5. Configure the following polling settings for the device:
   - **ICMP polling interval**
   - **Consecutive failure to trigger ICMP unreachable event**
   - **SNMP polling interval**
   - **Consecutive failure to trigger SNMP unreachable event**
6. Click **Apply**.
   MXview will update the polling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

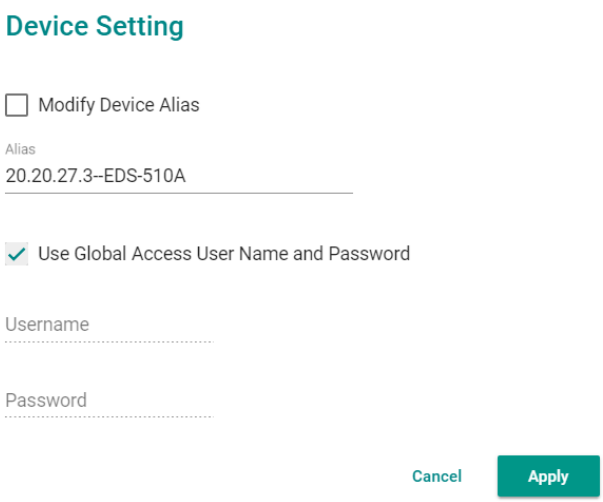
Configuring Advanced Settings

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** ( ) → **Network** → **Topology**.
   The **Network Topology** screen will appear and display the Topology Map by default.
2. Select one of the following views:
   a. **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.
   a. **Topology view:** Click the icon of the device in the Topology Map.
   b. **List view:** Select the check box next to the device in the Device List.
   The toolbar options change.



4. Navigate to **Maintenance** → **Advanced Settings**.
   The **Device Settings** screen appears.



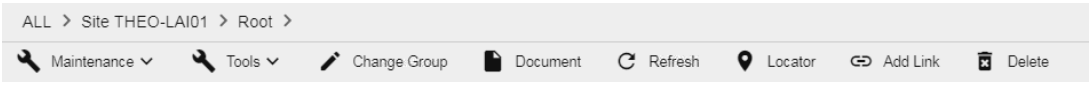
5. To modify device alias:
   a. Select the **Modify Device Alias** check box.
   b. Edit the **Alias** field.
6. To specify login credentials for the device web console (if different from the global MXview credentials):
   a. Clear the **Use Global Access User Name and Password** check box.
   b. Enter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

Configuring Polling IP Settings

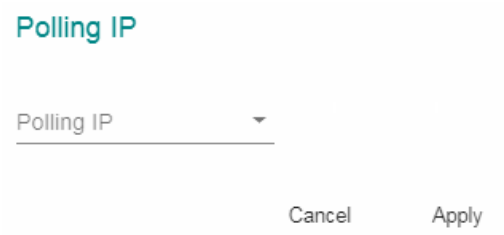
Use the **Network Typology** screen to configure the IP address used to poll a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to **Menu** ( ) → **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.



4. Navigate to **Maintenance** → **Polling IP**.
   The **Polling IP** screen will appear.



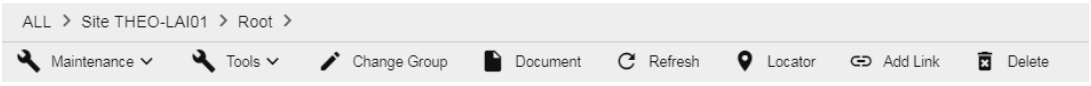
5. Select the IP address used to poll the device.
6. Click **Apply**.
   MXview will update the polling IP address for the device.

Changing the Device Icon

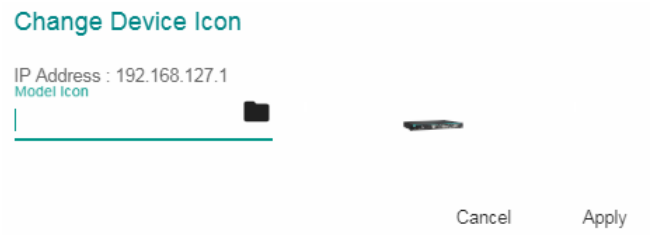
Use the **Network Topology** screen to change the device icon by selecting the device from the **Topology Map** or **Device List**, and then upload a JPG, GIF, or PNG image file.

1. Navigate to **Menu** ( ) → **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.



4. Navigate to **Maintenance** → **Change Device Icon**.
   The **Change Device Icon** screen appears.



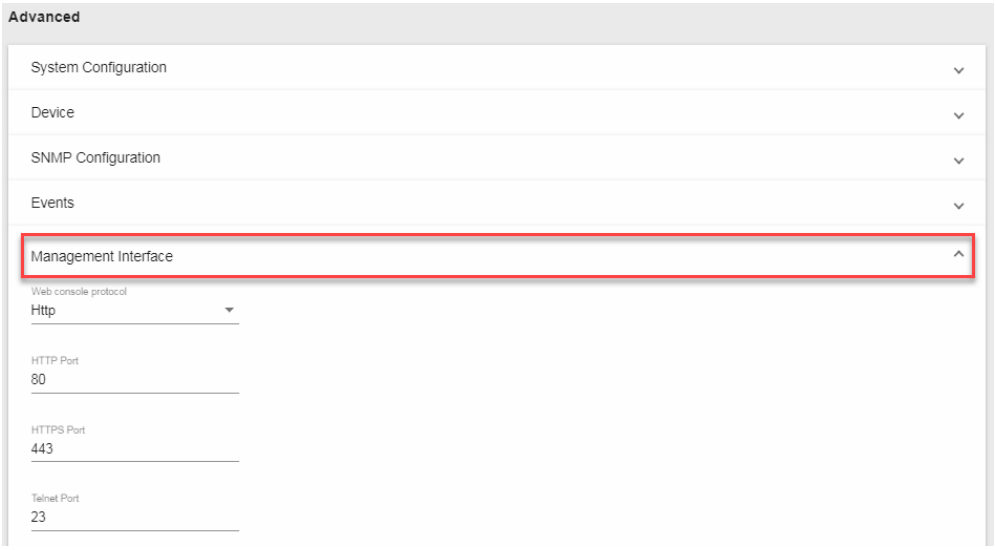
5. Click the folder ( ) icon to upload the device icon from your local machine.
6. Click **Apply**.
   MXview will change the device icon to the uploaded JPG, GIF, or PNG image file.

Signing on to Device Web Consoles

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

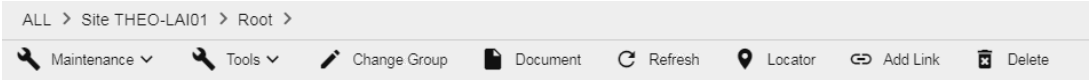
NOTE You can use the **Preferences** screen to configure the web console protocol. The web console protocol can be set to HTTP or HTTPS, and then the port numbers of the HTTP and HTTPS can be set by users. In addition, the Telnet port can be set as well.

1. (Optional) Configure the web console protocol:
   a. Navigate to **Menu** ( ) → **Preferences**.
   The **Preferences** screen appears.
   b. In the **Advanced** section, expand **Management Interface**.
   The **Management Interface** settings appear.



   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** ( ) → **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.



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.

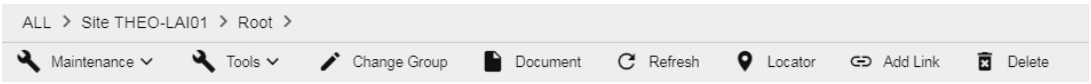
6. Enter the **Username** and **Password** for the device web console.
7. Click **Login**.
   The device web console will successfully log in.

Pinging Devices

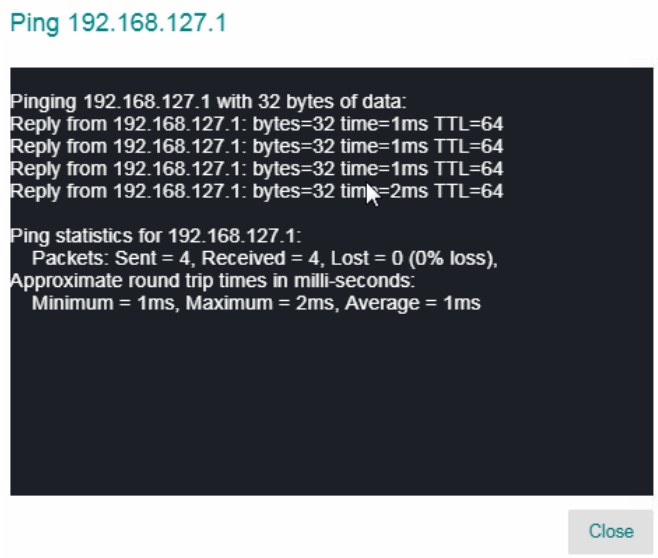
Use the **Network Topology** screen to ping devices in your network topology from the **Topology Map** or **Device List**.

1. Navigate to **Menu** ( ) → **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.



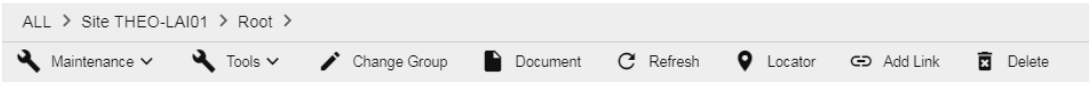
5. Wait for the ping test to finish and view the results.

Changing Device Groups

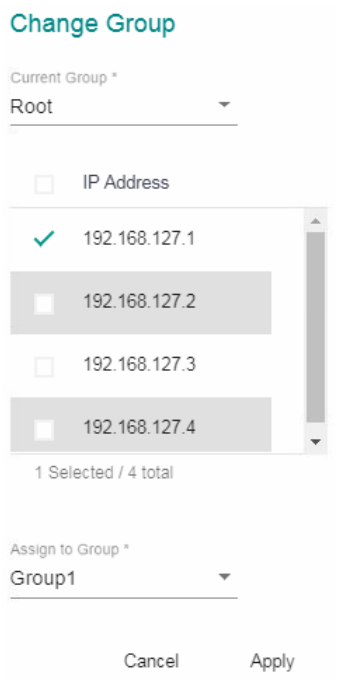
Use the **Network Topology** screen to change the assigned group for a device by selecting the device from the **Topology Map** or **Device List**.

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.



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



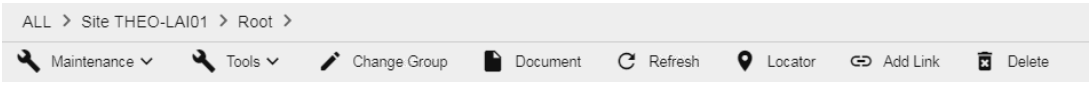
5. (Optional) Select additional IP addresses to assign other devices from the current group to the new group.
6. From the **Assign to Group** drop-down list, select the new group that you want to assign the selected device(s) to.
7. Click **Apply**.
   MXview will assign the selected device(s) to the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

Uploading Device Documents

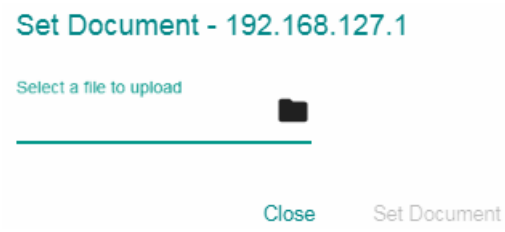
Use the **Network Topology** screen to upload PDF documentation (e.g., user's manual, quick installation guide) for a device. Uploaded documents can be downloaded for future reference.

1. Navigate to **Menu** ( ) → **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 **Document**.
   The **Set Document** screen will appears.



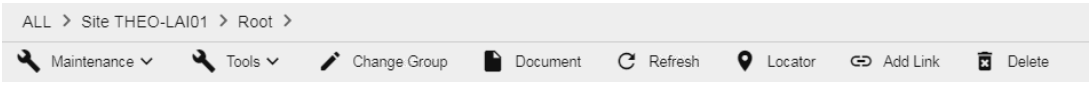
5. Click the folder ( ) icon to upload a PDF document from your local machine.
6. Click **Set Document**.
   MXview uploads the PDF document for the device.

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** ( ) → **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.



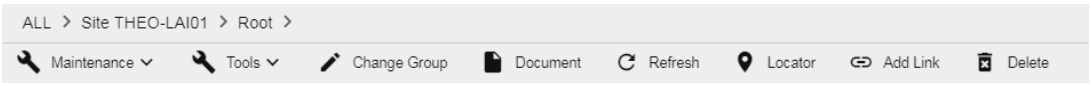
4. Click **Refresh**.
   MXview polls the device for updated data.

Locating Devices

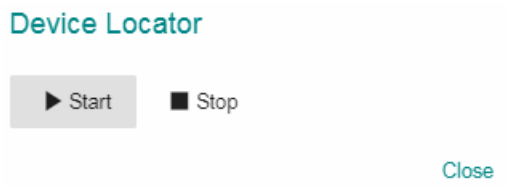
Use the **Device Locator** to locate a device in the field. When the **Device Locator** is activated, all the LEDs on the device start blinking to help you locate the device.

1. Navigate to **Menu** ( ) → **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.



4. Click **Locator**.
   The **Device Locator** screen appears.



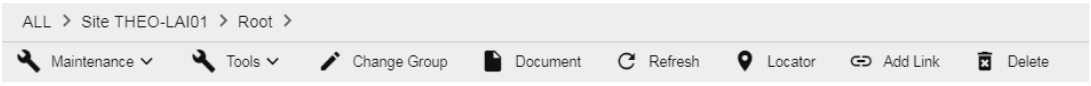
5. Click **Start**.
   All the LEDs on the device start blinking.
6. After you have located the device, click **Stop**.
   All the LEDs on the device stop blinking.

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.

10

Events and Notifications

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

The following topics are covered in this chapter:

- **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 SMS Notification Settings
  - Configuring SNMP Trap Destinations for the MXview Server
  - Configuring the SNMP Trap Destination for Devices
- **Notification Management**
  - Configuring New Event Notifications
  - Editing or Exporting Registered Actions
  - Editing or Exporting Notification Configurations
- **Custom Event Management**
  - Configuring Custom Events
  - Viewing or Exporting Custom Event Settings
  - Enabling/Disabling or Editing Custom Events

Event Monitoring

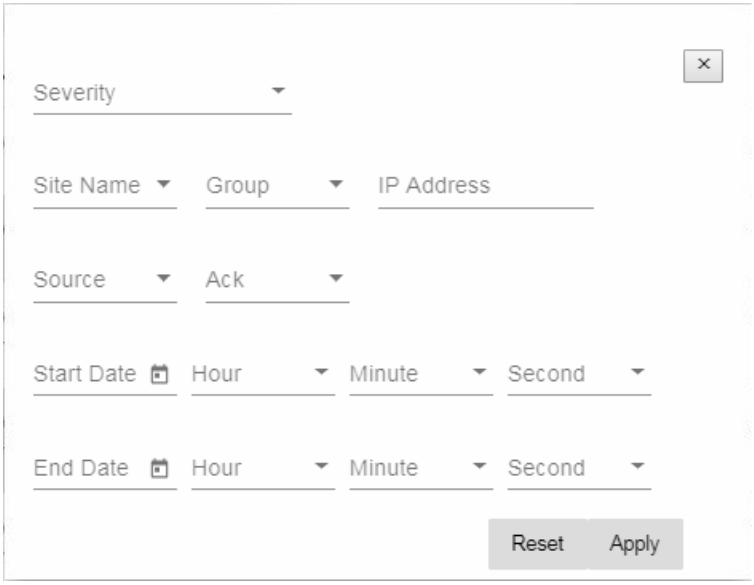
Viewing All Events

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.

1. Navigate to **Menu** ( ) → **Event** → **All Events**.
   The **All Events** screen will display the following information in a table format:

Column	Description
Ack	Acknowledge 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
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** ( ) icon in the top right corner.
      The following screen will appear.



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

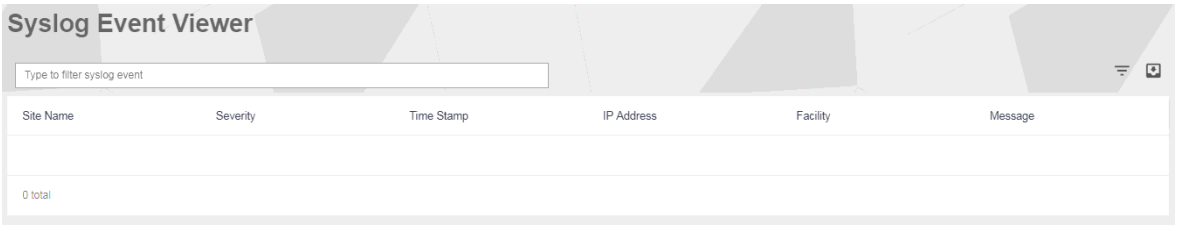
c. Click **Apply**.
MXview filters the table to only display events that match the specified criteria.

4. 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.

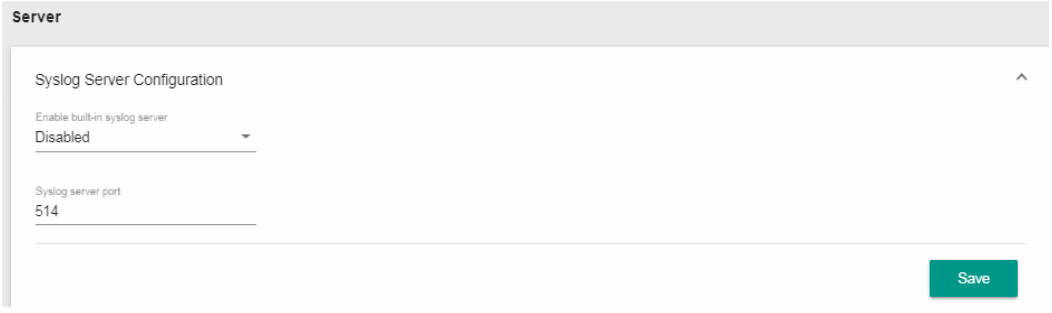
b. Select **Export CSV**.
c. Specify the location to save the exported file.
d. Click **Save**.
MXview exports the displayed event data as a CSV file.

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.



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.



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** ( ) → **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** ( ) icon in the top right corner.
The following screen will appear.

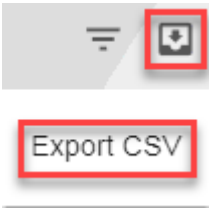
b. Specify any of the following criteria:

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
Priority	Select the criteria operator for matching the event severity level: • **Higher than or equal to** • **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.

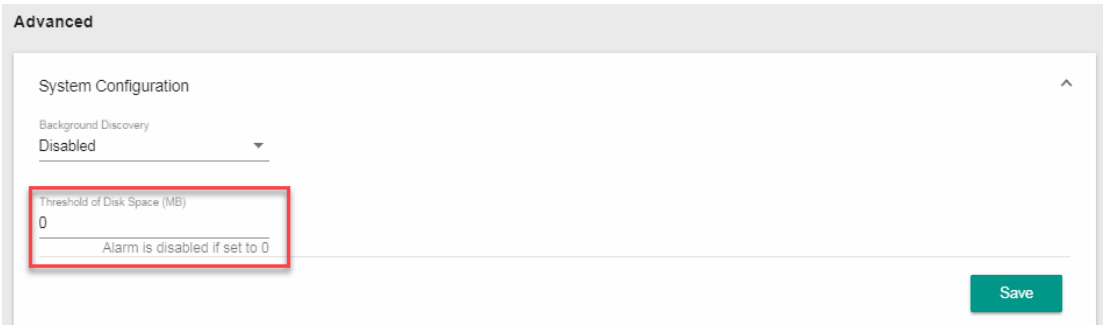


   b. Select **Export CSV**.
   c. Specify the location to save the exported file.
   d. Click **Save**.
   MXview exports the displayed event data as a CSV file.

Configuring the Server Disk Space Threshold

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

1. Navigate to **Menu** ( ) → **Preferences**.
   The **Preferences** screen appears.
2. 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.



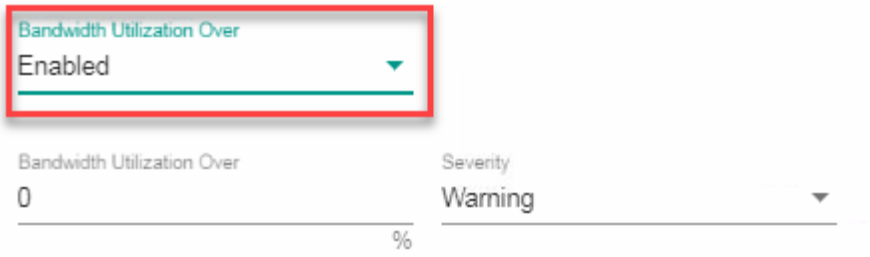
4. Click **Save**.
   MXview will trigger an event when the threshold for the available disk space remaining is reached.

Configuring Event Thresholds and Severity Levels

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

1. Navigate to **Menu** ( ) → **Preferences**.
   The **Preferences** screen will appear.
2. In the **Advanced** section, expand **Events**.
   The **Events** settings will appear.
3. Select one of the following severity levels for **Link Up** events:
   - **Information**
   - **Warning**
   - **Critical**
4. Select one of the following severity levels for **Link Down** events:
   - **Information**
   - **Warning**
   - **Critical**

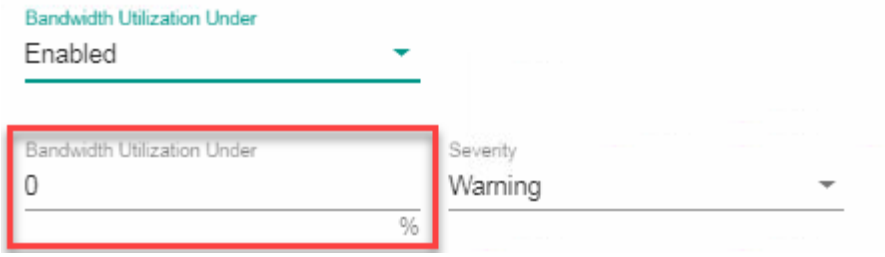
5. To trigger events when network bandwidth utilization exceeds a threshold:
   a. Select **Enabled** from the first **Bandwidth Utilization Over** drop-down list.



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

   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.

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

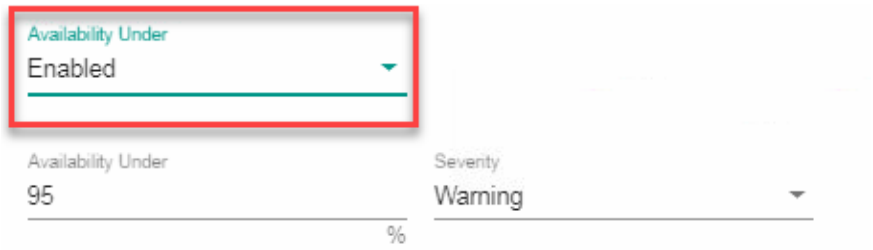


   c. Select the **Severity** level for the event.
7. To trigger events when the packet error rate exceeds a threshold:
   a. Select **Enabled** from the first **Packet Error Rate Over** drop-down list.

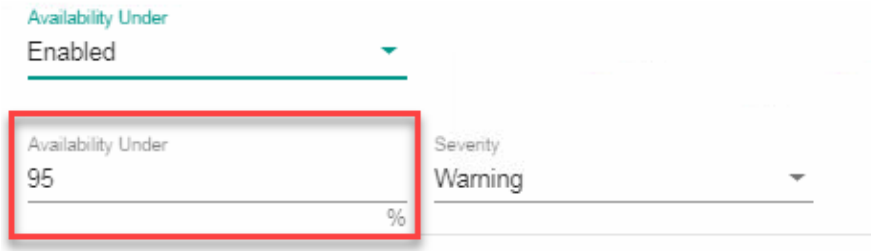
b. Specify the packet error rate (in percent) for the threshold.

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.



   b. Specify the device availability level (in percent) for the threshold.



   c. Select the **Severity** level for the event.
9. Click **Save**.
   MXview will update the event settings.

Notification Methods

MXview supports email, SMS, 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.

1. Navigate to **Menu** ( ) → **Preferences**.
   The **Preferences** screen will appear.
2. 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 SMS Notification Settings

Use the **Preferences** screen to configure SMS settings for event notifications.

1. Navigate to **Menu** ( ) → **Preferences**.
   The **Preferences** screen will appear.
2. In the **Server** section, expand **SMS Setting**.
   The **SMS Setting** configurations will appear.
3. Configure the following:
   - **COM Port**
   - **Baud Rate**
   - **Mode**
4. Click **Save**.
   MXview can send SMS 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.

1. Navigate to **Menu** ( ) → **Preferences**.
   The **Preferences** screen appears.
2. In the **Server** section, expand **SNMP Server of MXview**.
   The **SNMP 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**.

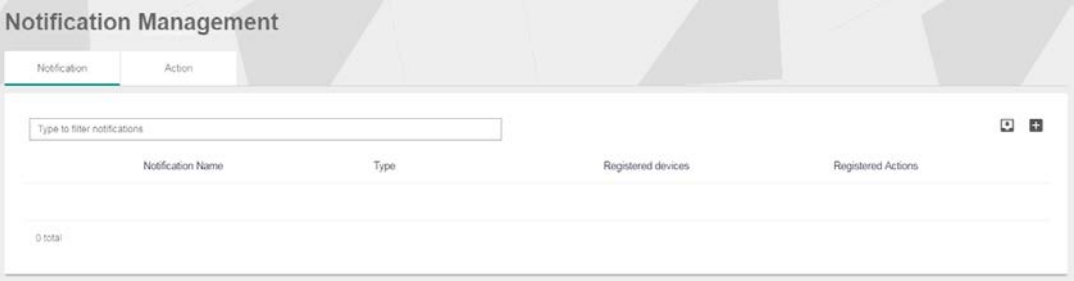
Configuring the SNMP Trap Destination for Devices

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.

1. Navigate to **Menu** ( ) → **Preferences**.
   The **Preferences** screen will appear.
2. In the **Server** section, expand **SNMP Server of Device**.
   The **SNMP 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

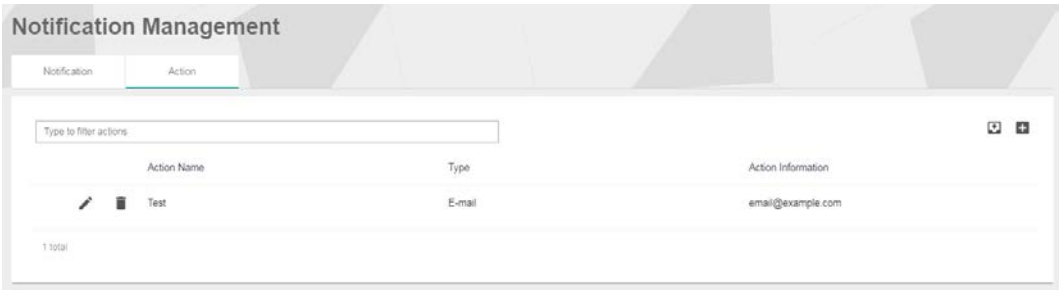
The **Notification Management** screen allows you to configure event notifications by issuing a registered action (e.g., sending an email message to a specified recipient) when configured events are detected on your network.



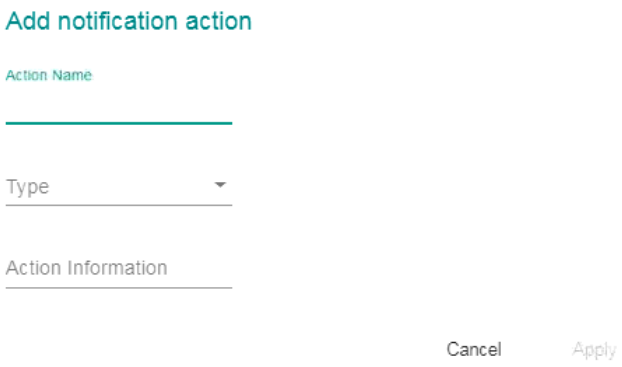
Configuring New Event Notifications

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).



   b. Click the **Add** ( ) icon in the top right corner.
      The **Add notification action** screen will appear.



   c. In the **Action Name** field, type a name to describe the action.
   d. From the **Type** drop-down list, select one of the following actions:
      - **SMS:** Sends an SMS message to the specified mobile phone number
      - **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

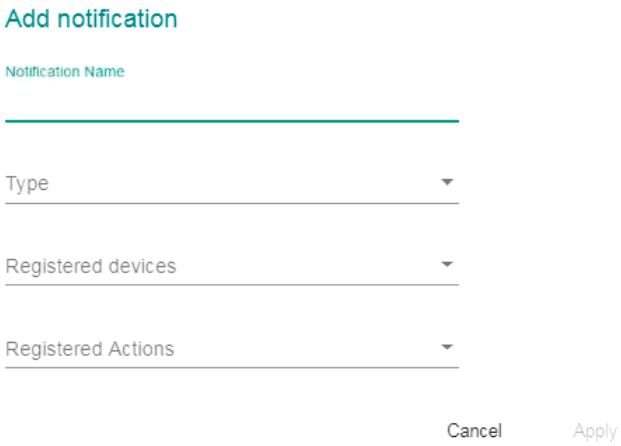
e. Provide additional information required for the action (if any).

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).

b. Click the **Add** ( ) icon in the top right corner.
The **Add** notification screen appears.



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.

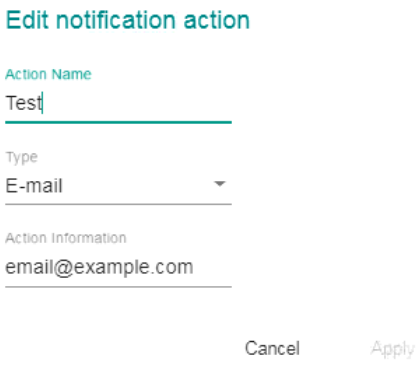
f. From the **Registered Actions** drop-down list, select the action that MXview performs when the specified event is detected on the previously selected device(s).

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

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.

1. 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.



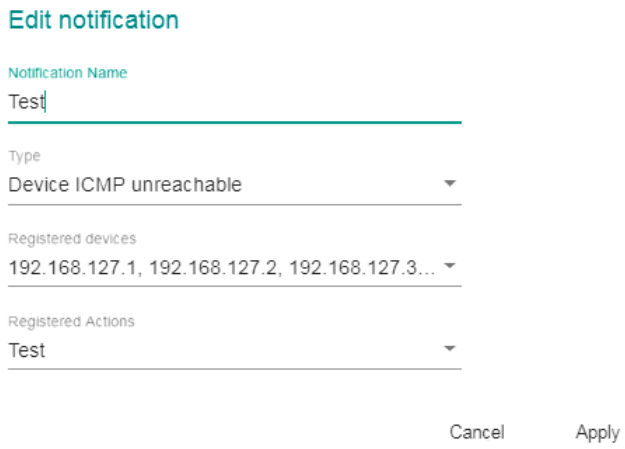
   b. Modify the following settings:
      - **Action Name**
      - **Type**
      - **Action information**
   c. Click **Apply**.
      The **Action** tab appears and displays the updated action information.
4. To export data displayed on the **Action** tab:
   a. Click the **Export** ( ) icon.

   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.

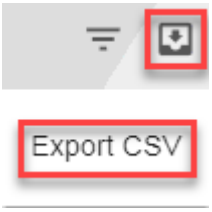
Editing or Exporting Notification Configurations

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

1. 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.



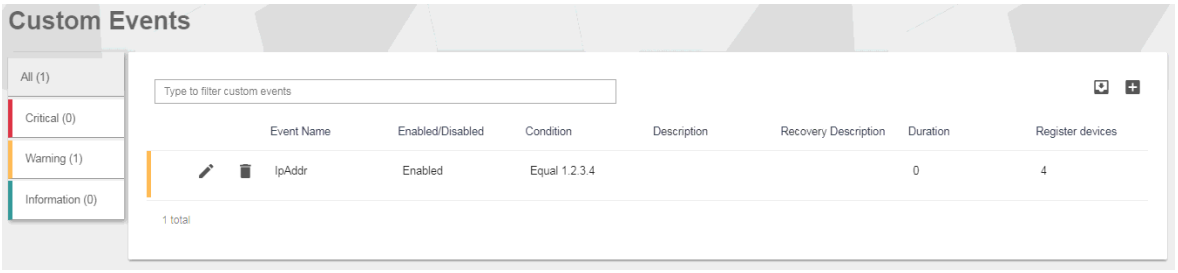
   b. Modify the following settings:
      - **Notification Name**
      - **Type**
      - **Registered devices**
      - **Registered Actions**
   c. Click **Apply**.
      The **Notification** tab appears and displays the updated notification information.
4. To export data displayed on the **Action** tab:
   a. Click the **Export** ( ) icon.



   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.

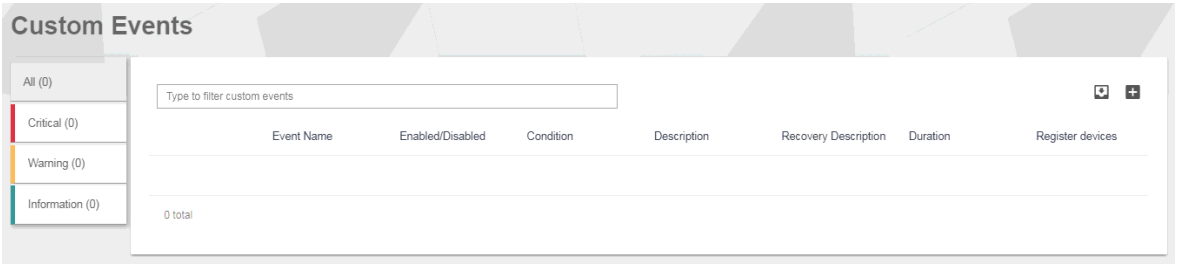
Custom Event Management

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.

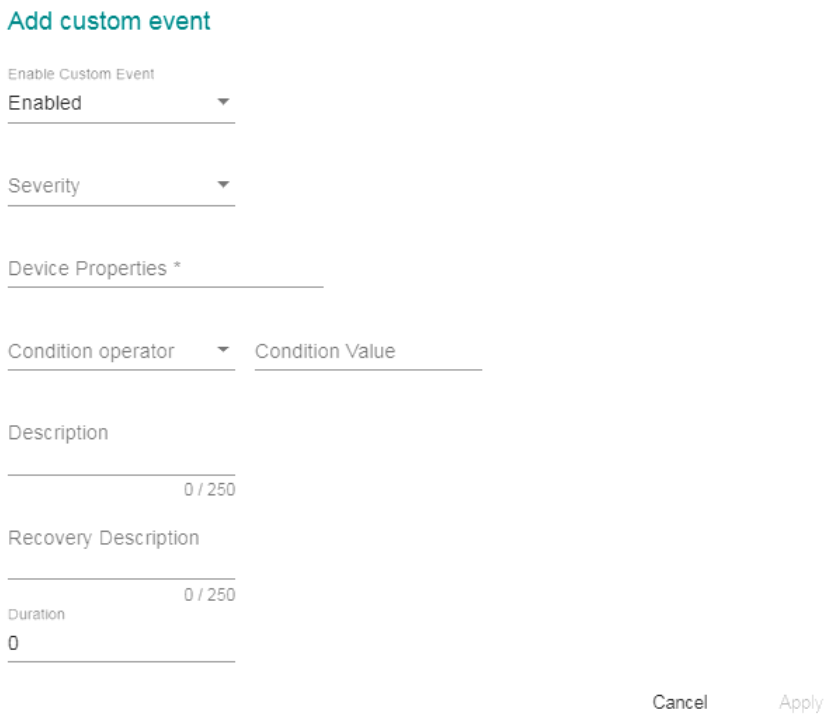


Configuring Custom Events

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.



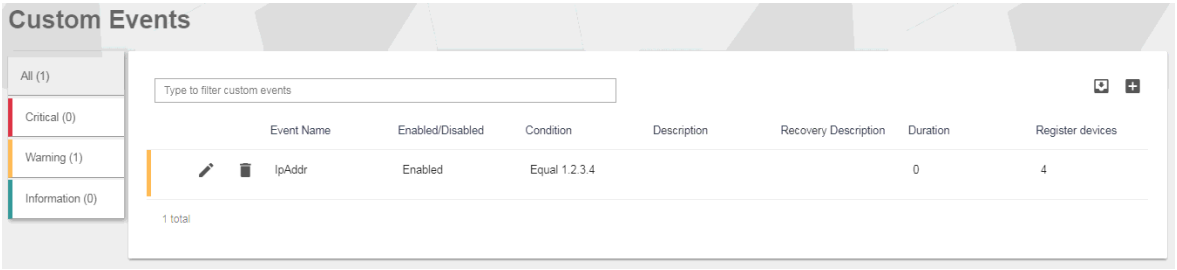
1. Navigate to **Menu** ( ) → **Event** → **Custom Events Management**.
   The **Custom Events** screen appears.
2. Click the **Add** ( ) button in the upper-right corner of the screen.
   The **Add custom event** screen will appear.



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.

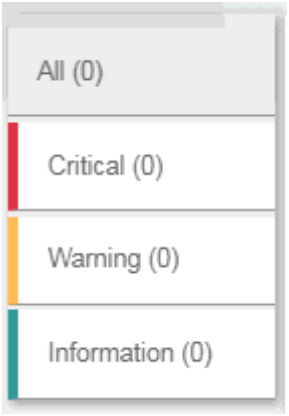


1. Navigate to **Menu** ( ) → **Event** → **Custom Events Management**.
   The **Custom Events** screen will appear and displays the following information in a table format:

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.

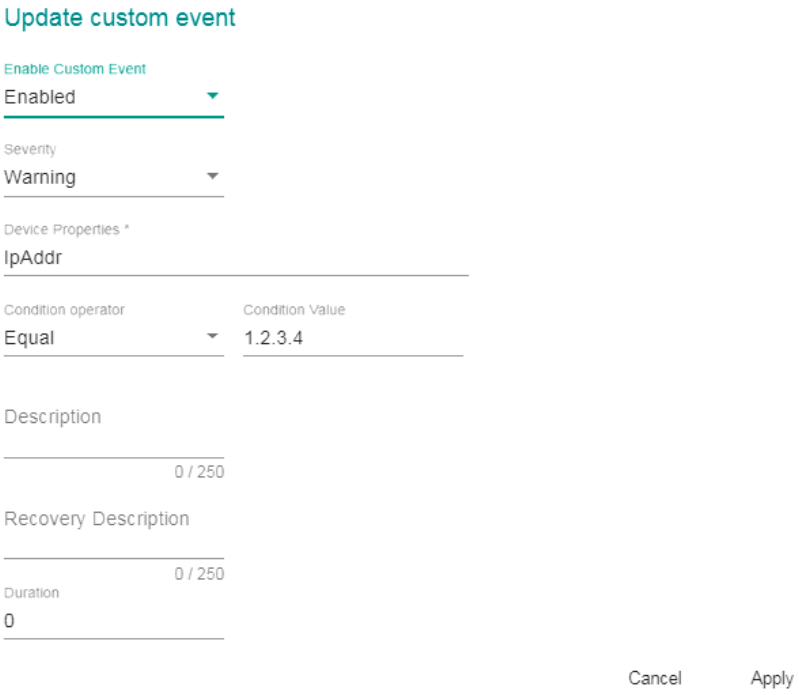
4. To sort the data in the table by a specific column, click the column heading.
MXview sorts the table by the column.
5. To export data displayed on the **All Events** screen:
   a. Click the **Export** ( ) icon.

   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.

1. Navigate to **Menu** ( ) → **Event** → **Custom Events Management**.
   The **Custom Events** screen appears.
2. Click the **Edit** ( ) icon next to the event you want to enable/disable.
   The **Update custom event** screen appears.



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.
5. Click **Apply**.
   The **Custom Events** screen will appear and displays the updated event information.

11

Reports

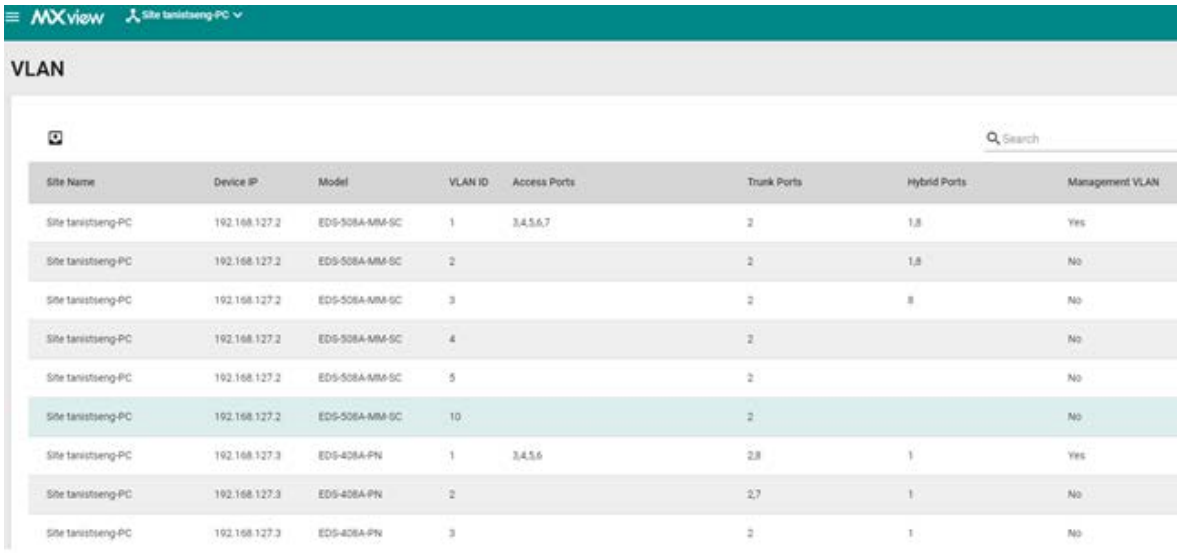
MXview provides reports that summarize key information about your VLAN configuration, network devices, and device availability.

The following topics are covered in this chapter:

- **Viewing VLAN Reports**
- **Viewing Inventory Reports**
- **Viewing Availability Reports**

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.



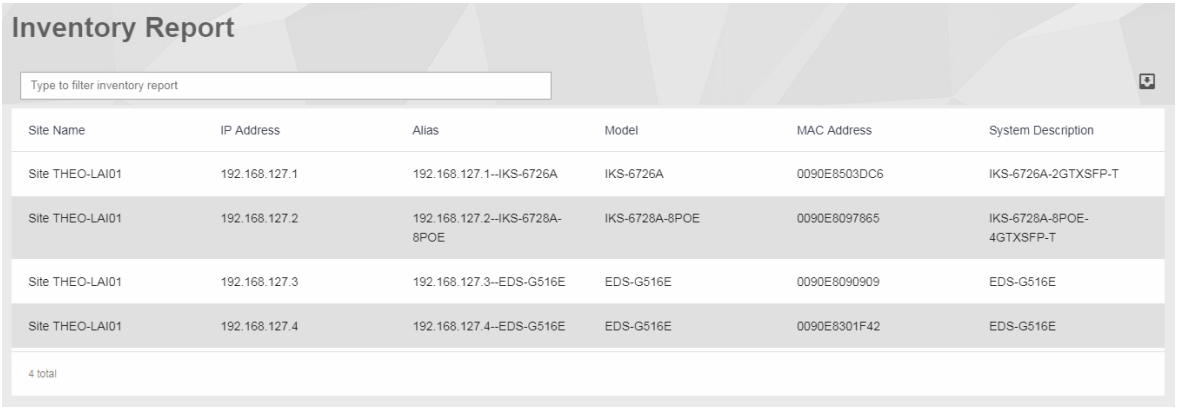
1. Navigate to **Menu** ( ) → **Reports** → **VLAN Report**.
   The **VLAN report** screen will appear and display the following information in a table format:

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.



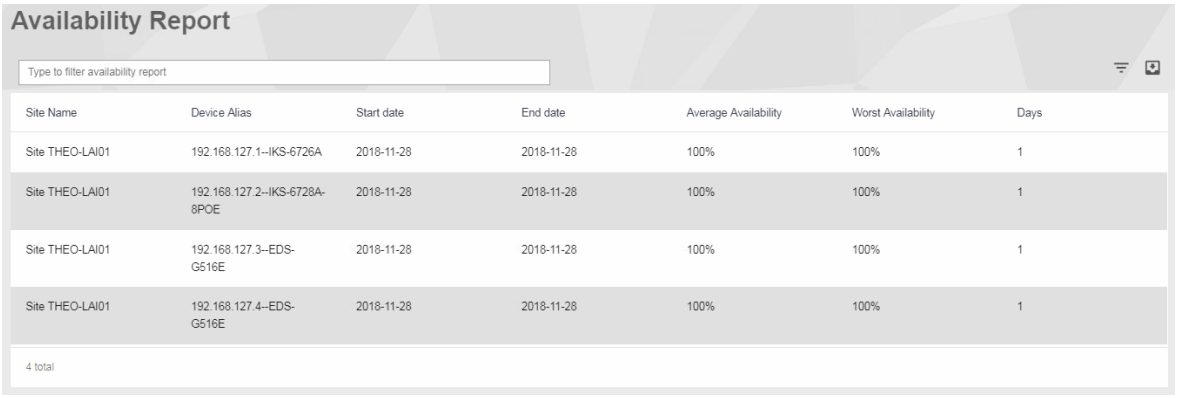
1. Navigate to **Menu** ( ) → **Reports** → **Inventory Report**.
   The **Inventory Report** screen appears and displays the following information in a table format:

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

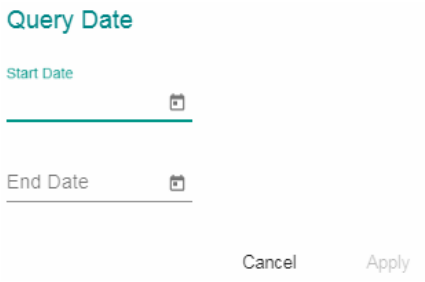
Use the **Availability Report** screen to view information about the device availability on your network. You can also export the report as a CSV file or a PDF file.



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** ( ) icon in the top right corner.
      The **Query Date** screen appears.



   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.

12

Backups and Migrations

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.

The following topics are covered in this chapter:

- **Backing Up the MXview Database**
- **Backing Up Device Configurations**
- **Restoring Device Configurations**
- **Archiving Device Configurations to the MXview Server**
- **Comparing Archived Configuration Files**
- **Creating Scheduled Jobs for Database/Configuration Backups**

Backing Up the MXview Database

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

1. Navigate to **Menu** ( ) → **Migrations** → **Database Backup**.
   The **Database Backup** screen appears.
2. 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.

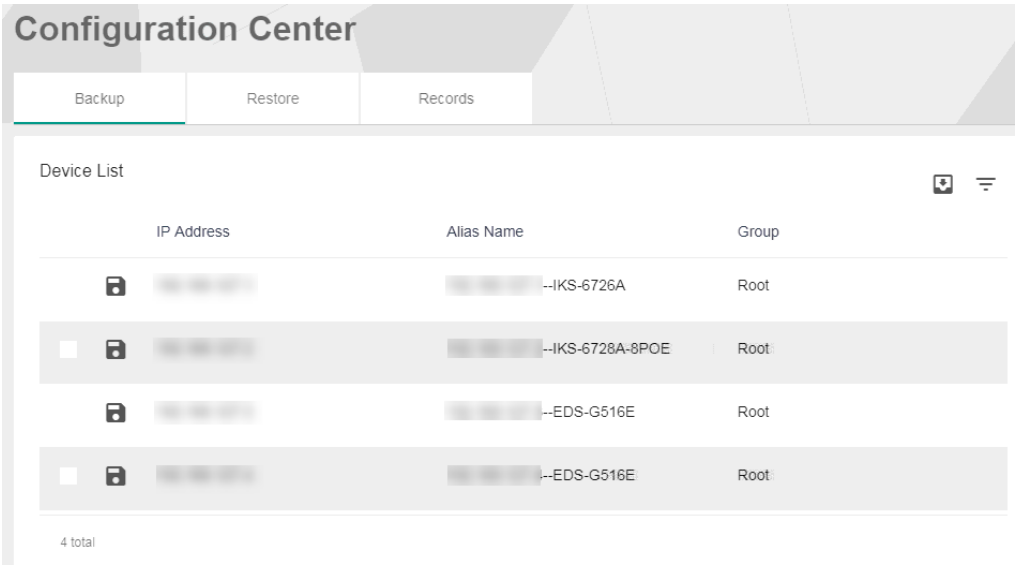
Backing Up Device Configurations

Use the **Configuration Center** screen to export configuration backup files from one or more devices.

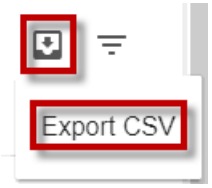
1. Navigate to **Menu** ( ) → **Migrations** → **Configuration Center**.

The **Configuration Center** screen appears.

2. Click the **Backup** tab.
   Available devices will appear in the **Device List**.



3. (Optional) To 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 back up configurations from all available devices:
   a. Click the **Export** ( ) icon.



   b. Select **Export CSV**.

c. Specify the location to save the configuration file.

d. Click **Save**.
MXview exports configurations from all available devices as a CSV file.

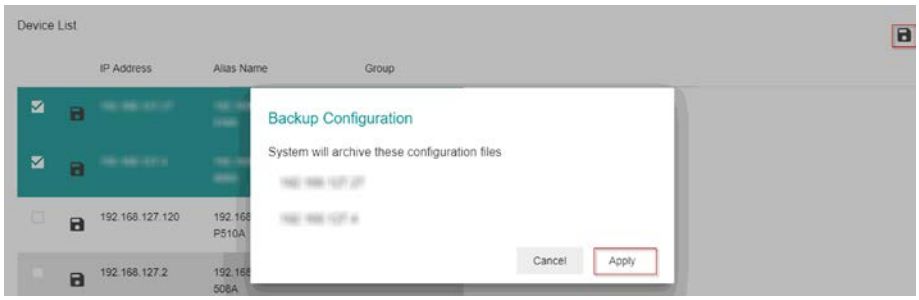
5. To back up configurations from specific devices:

a. Select the check box next to the device(s) you want to back up.

b. Click the **Save** ( ) icon in either of the following locations:

- For a single device, click the **Save** ( ) next to the selected device.
- For multiple devices, click the **Save** ( ) icon in the upper right corner of the screen.

The **Backup Configuration** screen appears.



c. Click **Apply**.
MXview archives configuration files from selected device(s) to the MXview server.

For more information, see the following topics:

- **Archiving Device Configurations to the MXview Server**
- **Comparing Archived Configuration Files**

d. Specify the location to save the exported configuration backup file.

e. Click **Save**.
MXview will export configurations from the selected device(s) as a ZIP file.

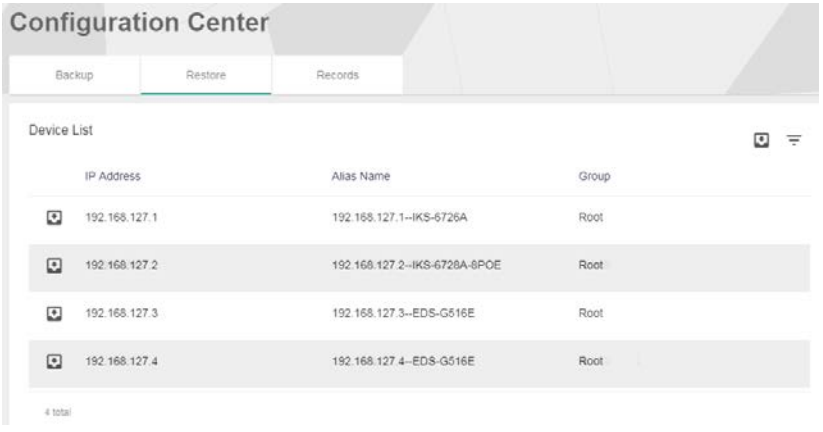
Restoring Device Configurations

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).

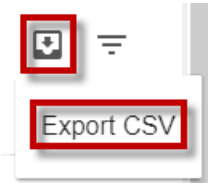
NOTE Restoring archived device configurations requires archiving device configurations to the MXview server. For more information, see **Archiving Device Configurations to the MXview Server**.

1. Navigate to **Menu** ( ) → **Migrations** → **Configuration Center**.
The **Configuration Center** screen will appear.

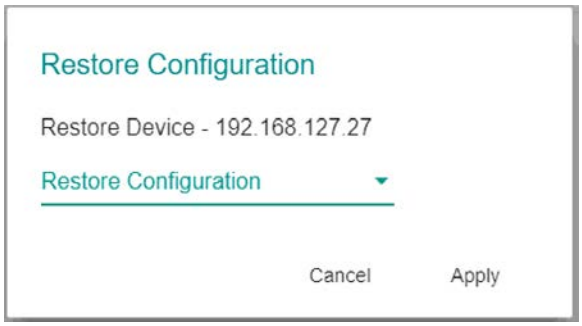
2. Click the **Restore** tab.
Available devices will appear in the **Device List**.



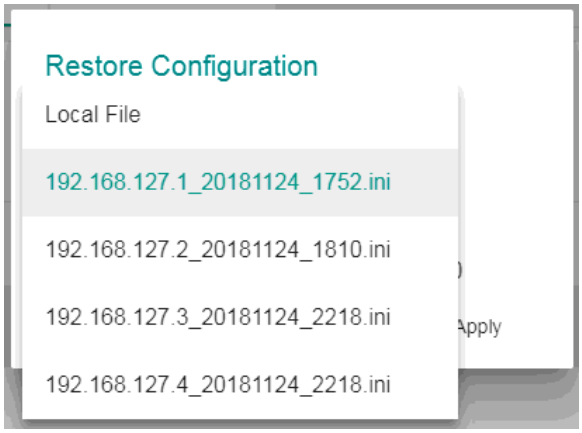
3. (Optional) To filter the devices in the **Device List**:
   a. Click the **Filter** ( ) icon.
   b. Specify any of the following criteria:
      - **Group:** The group that the device is assigned to
      - **IP Address:** The IP address of the device
   c. Click **Apply**.
      MXview filters the **Device List** according to the specified criteria.
4. (Optional) To export configurations from all available devices:
   a. Click the **Export** ( ) icon.



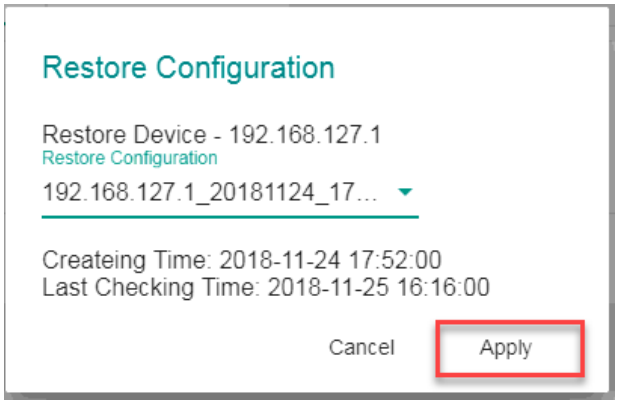
   b. Select **Export CSV**.
      MXview exports configurations from all devices as a CSV file.
5. To restore an archived configuration file to a device:
   a. Click the **Import** ( ) icon next to the **IP Address** of a device in the **Device List**.
      The **Restore Configuration** screen will appear.



   b. From the **Restore Configuration** drop-down list, select the archived device configuration to restore.



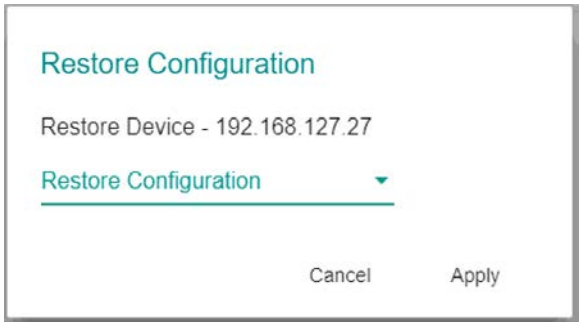
c. Click **Apply**.



MXview imports the configuration file to the selected device.

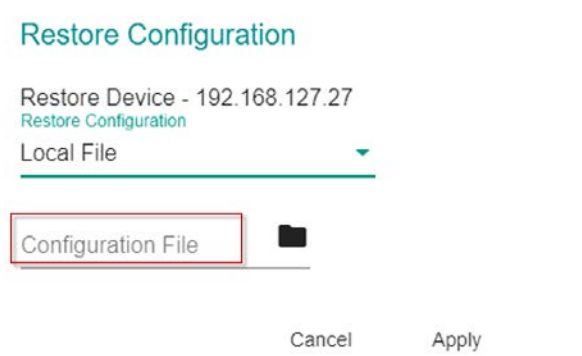
6. To import a local configuration file to a device:

a. Click the **Import** ( ) icon next to the **IP Address** of a device in the **Device List**. The **Restore Configuration** screen appears.



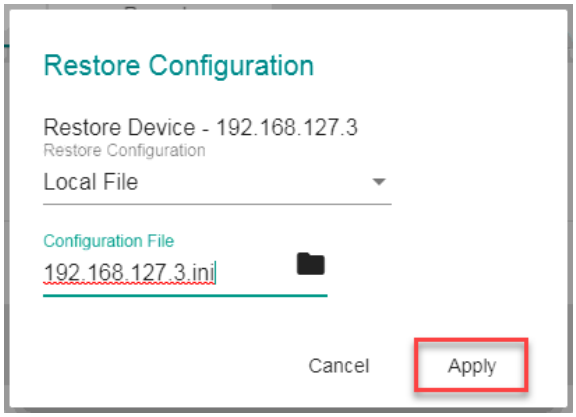
b. From the **Restore Configuration** drop-down list, select Local File.

c. Click Configuration File field to a select the configuration file.



d. Select the configuration file to import and click Open.

e. Click **Apply**.

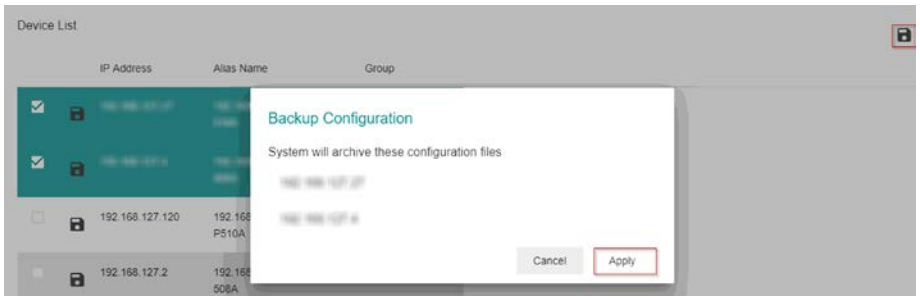


MXview imports the configuration file to the selected device.

Archiving Device Configurations to the MXview Server

Archiving configuration backup files to the MXview server allows you to restore the archived device configurations from the MXview server without manually importing a local configuration file. You can also compare changes between different versions of the archived configuration backup file.

1. Navigate to **Menu** ( ) → **Migrations** → **Configuration Center**.
   The **Configuration Center** screen will appear.
2. Click the **Backup** tab.
   Available devices appear in the **Device List**.
3. Select the check box next to the device(s) you want to archive.
4. Click the **Save** ( ) icon in the upper right corner of the screen.
   The **Backup Configuration** screen appears.

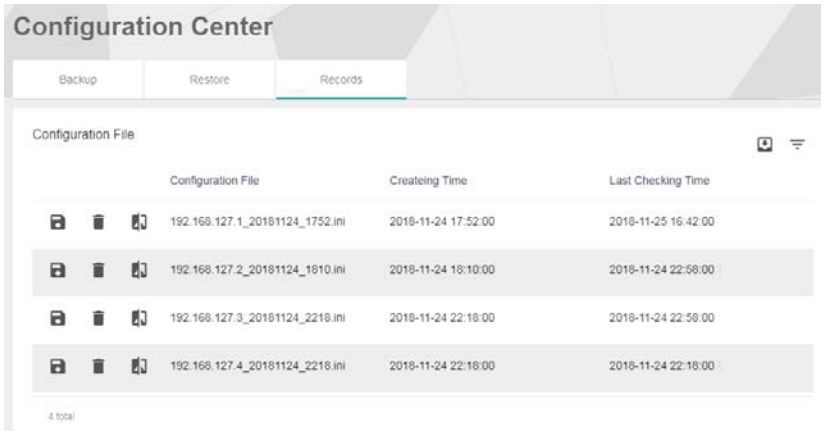


5. Click **Apply**.
   MXview archives configuration files from the selected device(s) to the MXview server.
   For more information, see **Comparing Archived Configuration Files**.
6. Specify the location to save the exported configuration backup file.
7. Click **Save**.
   MXview exports configurations from the selected device(s).

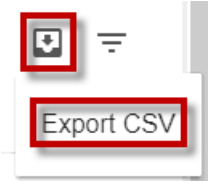
Comparing Archived Configuration Files

Use the MXview Configuration Center to compare changes in the history of saved configuration files.

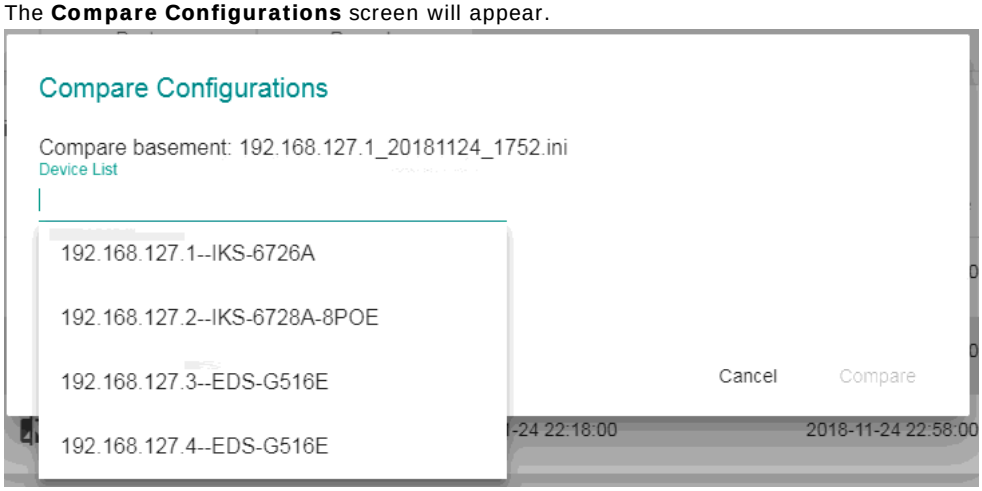
1. Navigate to **Menu** ( ) → **Migrations** → **Configuration Center**.
   The **Configuration Center** screen appears.
2. Click the **Records** tab.
   A list of archived configuration files appears.



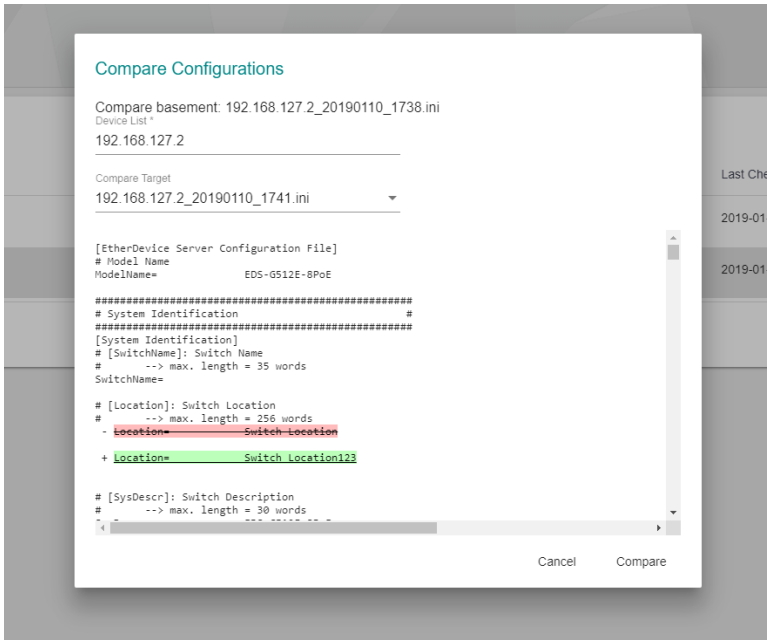
3. (Optional) To filter the list of configuration files:
   a. Click the **Filter** ( ) icon.
   b. Specify any of the following criteria:
      - **Group:** The group that the device is assigned to
      - **Start Date:** The earliest file creation date
      - **Start Time:** The earliest file creation 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) To 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** ( ) icon next to the configuration file you want to compare.
   The **Compare Configurations** screen will appear.



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.

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.

1. Navigate to **Menu** ( ) → **Migrations** → **Job Scheduler**.
   The **Job Scheduler** screen appears.
2. (Optional) To 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.

13

Custom Integrations

MXview supports several features that enable integration with third-party applications or external systems.

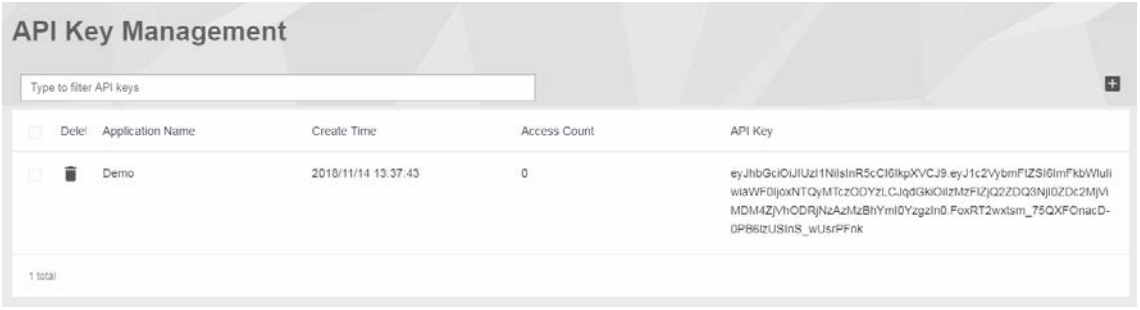
The following topics are covered in this chapter:

- **Managing API Keys**
- **Embedding Web Widgets**
- **Generating OPC Tags**

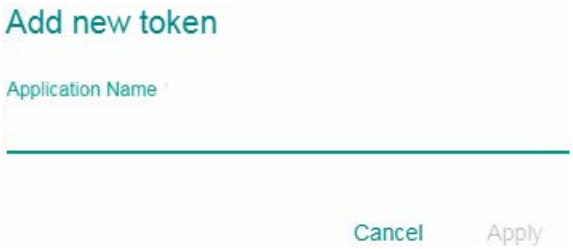
Managing API Keys

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.

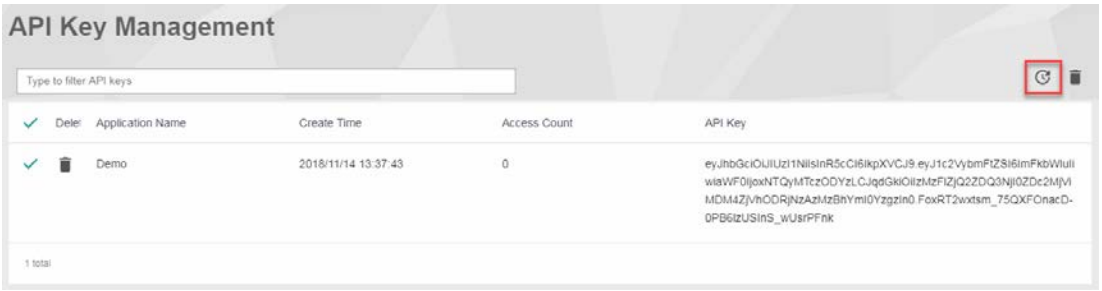
1. Navigate to **Menu** ( ) → **Integration** → **RESTful API Management**.
   The **API Key Management** screen will appear.



2. (Optional) To 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** ( ) icon in the top right corner of the screen.
      The **Add new token** screen will appear.



   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** ( ) icon will appear in the top right corner of the screen.



   b. Click the **Regenerate** ( ) icon.
      MXview will regenerate the API key for the selected application.

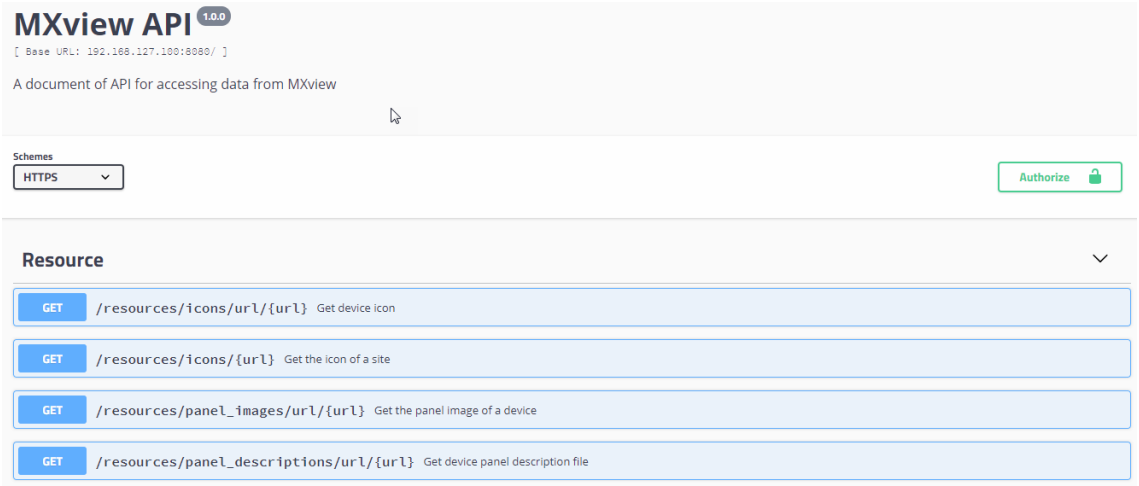
NOTE Regenerating the API key will prevent any APIs that use the old API key from working properly.

5. To delete an application:
   a. Select the check box next to the **Application Name**.
   b. Click the **Delete** ( ) icon in either one of the following locations:
      - Next to the **Application Name**.
      - In the top right 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.

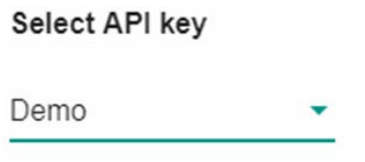
6. To view API reference documentation, navigate to **Menu** ( ) → **Integration** → **API Reference**.
   The **MXview API** screen will appear and display the reference document for supported MXview APIs.



Embedding Web Widgets

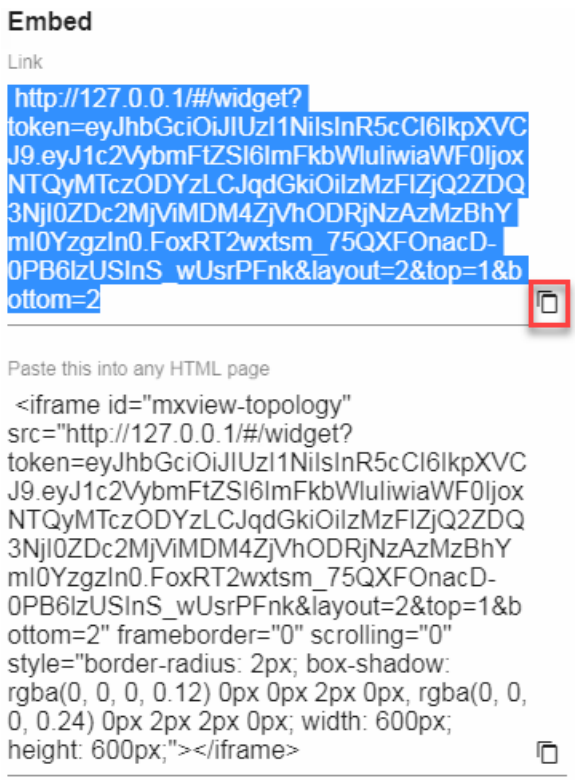
MXview allows you embed the Topology Map and Recent Events widgets from the MXview **Network Topology** screen in third-party applications.

1. 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.

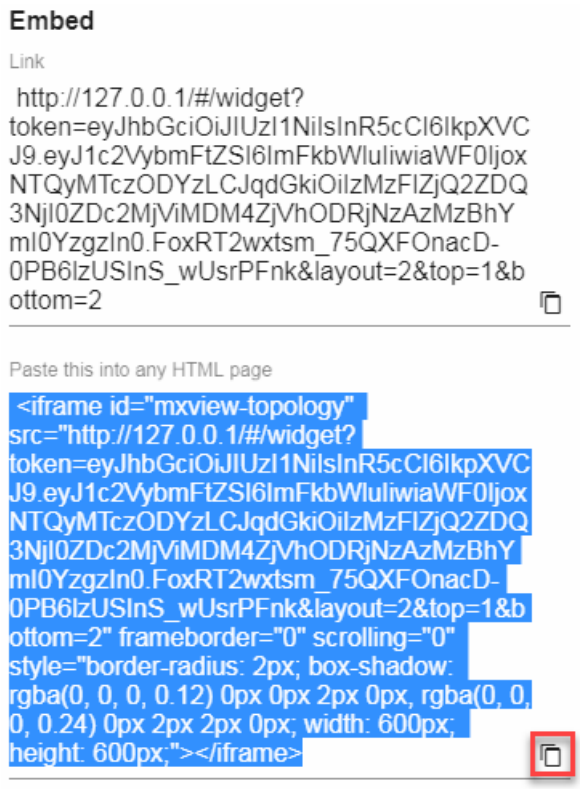


3. From the **Select Layout** drop-down list, select the widget(s) you want to embed:
   - **Topology and recent events:** Embeds both the Topology Map and Recent Events widgets in the target application
   - **Topology:** Embeds only the Topology Map in the target application
   - **Recent event:** 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** (⧉) icon in the **Link** section.



   - To embed the link in a static HTML page, click the **Copy link** (⧉) icon in the **Paste this into any HTML page** section.



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.

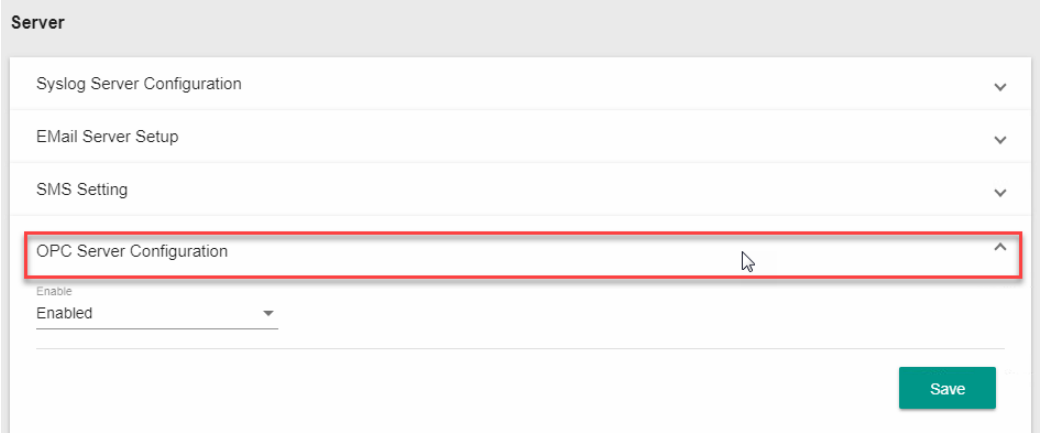
Currently, the default information that MXview can prepare as tags includes:

- 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_**.

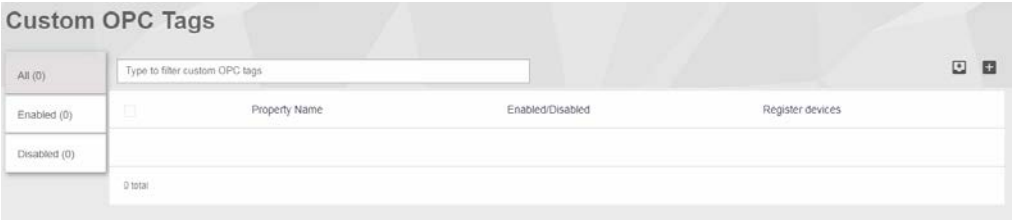
NOTE The **Health** tag represents the health status of the entire network. There are three levels: Normal, Warning, and Critical, with the values 0, 1, and 2 respectively. MXview allows users to use only one tag to monitor the status of the whole network.

In addition to the default OPC tags, MXview allows you to add custom OPC tags for supported SNMP device properties.

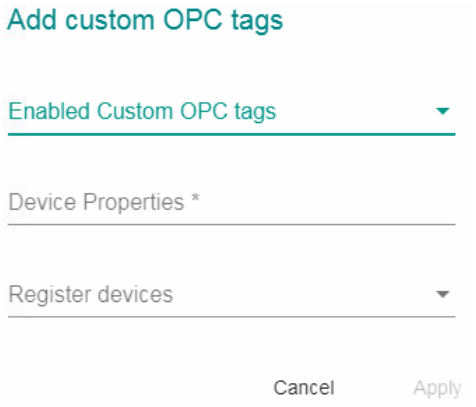
1. To enable the OPC server and start generating default OPC tags:
   a. Navigate to **Menu** ( ) → **Preferences**.
   The **Preferences** screen will appear.
   b. In the **Server** section, expand **OPC Server Configuration**.
   The **OPC Server Configuration** settings will appear.



   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.



b. Click the **Add** ( ) icon in the top right corner.
The Add custom OPC tags screen will appear.



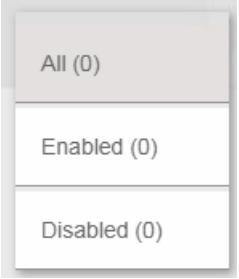
c. Configure the following:
   - **Enabled Custom OPC tags:** Select to enable to disable the custom OPC tags
   - **Device Properties:** Select the SNMP properties to generate custom OPC tags
   - **Registered Devices:** Select the devices to implement the custom OPC tags

d. Click **Apply**.
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.

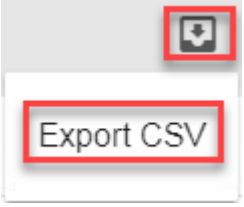
MXview filters the table to only display OPC tags with values that fully or partially match the specified string.

   - Click one of the following OPC tag statuses on the left side of the screen.



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.

A

License

License (Net-SNMP)

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

Please carefully review all sections of the license information.

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

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

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

All Rights Reserved

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

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

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

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

All rights reserved.

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

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

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

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

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

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

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

All rights reserved.

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

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

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

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

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

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

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

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

Use is subject to license terms below.

This distribution may include materials developed by third parties.

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

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

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

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

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

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

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

Copyright (c) 2003-2009, Sparta, Inc

All rights reserved.

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

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

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

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

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

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

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

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

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

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

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

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

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

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

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

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

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

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

oss@fabasoft.com

Author: Bernhard Penz

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

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

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

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

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

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

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

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

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

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

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

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

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

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

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

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

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

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

The MIT License (Libxml2)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

License Agreement (GoAhead)

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

1. Definitions.

“Documentation” means any documentation GoAhead provides with the Original Code.

“GoAhead” means GoAhead Software, Inc.

“Agreement” means this document.

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

“Original Code” means the source code to GoAhead’s proprietary computer software entitled GoAhead WebServer that is provided to You by GoAhead.

“You” means an individual or a legal entity exercising rights under, and complying with all of the terms of, this license or a future version of this license. For legal entities, “You” includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, “control” means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of fifty percent (50%) or more of the outstanding shares or beneficial ownership of such entity.

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

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

2. License.

Limited Original Code Grant.

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

Binary Code.

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

Restrictions on Use.

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

Documentation.

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

Copyright Notice.

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

License Back to GoAhead.

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

3. Terms, Trademards and Brand.

License and Use.

GoAhead hereby grants to You a limited world-wide, royalty-free, non-exclusive license to use the GoAhead trade names, trademarks, logos, service marks and product designations posted in Exhibit A (collectively, the

"GoAhead Marks") in connection with the activities by You under this Agreement. Additionally, GoAhead grants You a license under the terms above to such GoAhead trademarks as shall be identified at a URL (the "URL") provided by GoAhead. The use by You of GoAhead Marks shall be in accordance with GoAhead's trademark policies regarding trademark usage as established at the Web site designated by the URL, or as otherwise communicated to You by GoAhead at its sole discretion. You understand and agree that any use of GoAhead Marks in connection with this Agreement shall not create any right, title or interest in or to such GoAhead Marks and that all such use and goodwill associated with GoAhead Marks will inure to the benefit of GoAhead.

Promotion by You of GoAhead WebServer Mark.

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

No Modifications to Server Identification Field.

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

4. Term.

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

5. Warranty Disclaimers.

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

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

GOAHEAD DOES NOT WARRANT THE ORIGINAL CODE AGAINST INFRINGEMENT OR THE LIKE WITH RESPECT TO ANY COPYRIGHT, PATENT, TRADE SECRET, TRADEMARK OR OTHER PROPRIETARY OR INTELLECTUAL PROPERTY RIGHT OF ANY THIRD PARTY AND DOES NOT WARRANT THAT THE ORIGINAL CODE DOES NOT INCLUDE ANY VIRUS, SOFTWARE ROUTINE OR OTHER SOFTWARE DESIGNED TO PERMIT UNAUTHORIZED ACCESS, TO DISABLE, ERASE OR OTHERWISE HARM SOFTWARE, HARDWARE OR DATA, OR TO PERFORM ANY OTHER SUCH ACTIONS.

Any warranties that by law survive the foregoing disclaimers shall terminate 90 days from the date You received the Original Code.

6. Limitation of Liability.

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

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

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

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

7. Indemnification by You.

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

8. High-Risk Activities.

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

9. Government Restricted Rights.

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

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

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

10. Governing Law and Interpretation.

This Agreement shall be interpreted under and governed by the laws of the State of Washington, without regard to its rules governing the conflict of laws. You hereby consent to the exclusive jurisdiction of the state and federal courts located in King County, Washington over any disputes arising out of related to this Agreement. If any provision of this Agreement is held illegal or unenforceable by a court or tribunal of competent jurisdiction, the remaining provisions of this Agreement shall remain in effect and the invalid provision deemed modified to the least degree necessary to remedy such invalidity.

11. Entire Agreement.

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

License (OpenSSL)

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

LICENSE ISSUES

==========

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

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

OpenSSL License

/*===

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

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. 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/)”
4. 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.
6. 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

/