MXview One 1.1.0 User Manual

Version 2.0, January 2023

www.moxa.com/products

© 2023 Moxa Inc. All rights reserved.

MXview One 1.1.0 User Manual

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

Copyright Notice

© 2023 Moxa Inc. All rights reserved.

Trademarks

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

Disclaimer

- Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.
- Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.
- Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.
- This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction 6
- Key Features 6
  - Web-based Operation 6
  - Auto Discovery and Topology Visualization 6
  - Event Management 6
  - Configuration and Firmware Management 6
  - Traffic Monitoring 6
- System Requirements 7
- Supported Devices 7

2. Installation and Uninstallation 8
- Installation Procedure 8
  - For Windows 8
  - For Ubuntu 20.04 8
  - For Ubuntu 18.04 10
- Uninstallation 11
  - For Windows 11
  - For Ubuntu 11

3. Getting Started 12
- MXview One Control Panel 12
  - Server Control 12
  - Configuration 13
  - DB Backup & Restore 14
  - Plugin Manager 16
- Starting the MXview One Server and Logging Into MXview One 17
- Logging Into MXview One Remotely 18
- License Management 20
  - Checking the License 21
  - Adding a New License 21
- Using Device Discovery 23
- Account Management 25
  - Adding User Accounts 26
  - Modifying User Accounts 26
  - Deleting User Accounts 27
  - Exporting User Accounts 27
  - Configuring the Password Policy 27
  - Configuring Login Notifications 28
  - Changing the Display Language 29

4. License Management 30
- License Management Overview 30
- License Type 31
- Adding a New License 32
- Adding an Add-on License 34
- Deactivating a License 37
- Reactivating a Deactivated License 38
- Transferring a License to a Different Instance of MXview One 40
- Quantity of Monitored Devices Exceeds the Number of Node-based Licenses 42

5. Dashboard Widgets 44
- Dashboard Overview 44
- Device Summary 44
- Event Highlights 45

6. Device Discovery and Polling 46
- Device Discovery Overview 46
- Configuring IP Address Scan Ranges 47
- Configuring Device Polling Settings 49
- Changing Default SNMP Configuration 50

7. Topology Management 51
- Topology Overview 51
- Viewing Topology Map 52

Viewing Recent Events 54
Organizing the Topology Structure By Group Function 56
Redundant Topologies 59
PoE Power Consumption Visualization 59
VPN Tunnel Visualization 60
Port Trunking 60
Adding Devices and Links 61
Deleting Devices and Links 63
Updating the Topology Map 63
Refreshing the Topology Layout 64
Creating a New Topology Map 65
Setting/Editing the Background Image 66
Editing the Topology Appearance 67
Editing the Device Appearance 71
Exporting the Topology Map 73
8. Network and Traffic Monitoring 74
Viewing Link Properties 74
Viewing Port Traffic 75
Viewing Packet Error Rates 76
Monitoring Traffic Loads 77
Monitoring Network Security 77
Configuring Severity Thresholds for Traffic and Fiber Status Monitoring Events 82
Configuring Custom Port Labels 85
9. SFP Fiber Status 86
Viewing the SFP Fiber Status in Table View 86
Synchronize the SFP Threshold From the Device 87
10. Device Management 88
Viewing the Device List 88
Importing Device Configurations 91
Exporting Device Configurations 92
Upgrading Firmware 93
Configuring SNMP Trap Server 94
Configuring Port Settings 95
Configuring SNMP Configuration 96
Configuring Polling Settings 97
Configuring Advanced Settings 98
Changing the Device Icon 99
Signing on to Device Web Consoles 100
Changing Device Groups 101
Refreshing the Device Status 102
Deleting Devices 102
11. Events and Notifications 103
Event Monitoring 103
Viewing Event History 103
Viewing Syslog Events 105
Configuring Event Thresholds and Severity Levels 107
Notification Methods 111
Configuring Email Server Settings 111
Notification Management 111
Configuring New Event Notifications 112
Editing or Exporting Registered Actions 113
Editing or Exporting Notification Configurations 114
Custom Event Management 115
Configuring Custom Events 115
Viewing or Exporting Custom Event Settings 117
Enabling/Disabling or Editing Custom Events 118
12. Reports 119
Viewing Inventory Reports 119
13. Backups, Restores, and Compares 120
Backing Up the MXview One Database 120

Backing Up Device Configurations 121
Restoring Device Configurations 123
Comparing Archived Configuration Files 125
Creating Maintenance Scheduler for Database/Configuration Backups 127
14. Custom Integrations 129
Managing RESTful API Keys 129
Embedding Web Widgets 130
15. Wireless Add-on Module 132
Introduction 132
System Requirements 132
Supported Devices 132
Getting Started With the Wireless Add-on Module 133
Wireless Module Features 134
Main Dashboard 134
Dynamic Wireless Client Roaming 135
AP/Client Device Dashboard 137
AP Device Dashboard 137
Client Device Dashboard 138
Wireless Device Summary 139
Wireless Roaming Playback 140
16. Power Add-on Module 142
Introduction 142
System Requirements 142
Supported Devices With PRP/HSR Features 142
Getting Started With the Power Add-on Module 143
Power Module Features 144
Topology 144
Import SCD 146
GOOSE Message 147

1. Introduction

The Moxa MXview One network management software consists of three parts: The Main Module, Power Add-on Module, and the Wireless Add-on Module. The Moxa MXview One 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 One provides an integrated management platform that can manage Moxa networking devices, such as Ethernet switches, wireless APs, SNMP-enabled, and ICMP-enabled devices installed on subnets. The MXview Power Add-on Module provides additional advanced functions for power substation applications and the MXview One Wireless Add-on Module provides additional advanced functions for wireless applications to monitor and troubleshoot your network, and help you minimize downtime.

Key Features

Web-based Operation

You will need to install the MXview One on a Windows computer connected to the network(s) that are to be managed. After installing MXview One, the network can be managed using Chrome, Firefox, or Microsoft Edge (version 79+), without installing additional software.

Auto Discovery and Topology Visualization

Within the Device Discovery, MXview One locates networking devices with SNMP or ICMP services enabled. MXview One can collect topology information from devices with LLDP capability and draw the topology of the network, which shows wired and wireless connections. For ICMP devices without LLDP, MXview One 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 One logs events that match predefined conditions, such as link up/down, device unreachable, or traffic overloading. The most recent events will be displayed to inform users of the networking status. Devices and links that generate events will be highlighted with different colors. When an event occurs, users can be notified by email.

Configuration and Firmware Management

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

Traffic Monitoring

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

System Requirements

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

	System Requirements
CPU	3 GHz or faster dual core CPU
RAM	16 GB or higher
Hard Disk Space	SSD 1 TB or higher
OS	• Windows 10, Windows 11 (64-bit) Windows Server 2016, Window Server 2019, Windows Server 2022 (64- bit) • Linux - Ubuntu 18.04, Ubuntu 20.04 For the latest supported OS versions, please visit the MXview One website: https://www.moxa.com/en/products/industrial-network-infrastructure/network-management-software/mxview-one-series#resources
Client Browser Requirements	Browser: Chrome: Version 76 or later Firefox: Version 69 or later Microsoft Edge: Version 79 or later

Supported Devices

MXview One supports a full range of functions, such as network status, traffic log, and configuration/firmware file management.

- For other SNMP-enabled devices, MXview One supports standard management functions, such as link up, link down, and SNMP MIBII information.
- MXview One can only monitor the connectivity of devices that support ICMP.

Please check the MXview One datasheet on moxa.com for a list of Moxa devices that are supported.

2. Installation and Uninstallation

Installation Procedure

For Windows

1. Execute the installation program.
2. During the installation, you can check the EULA (End-User License Agreement) and choose the directory in which MXview One will be installed and the default language, or leave the settings as the default values.
3. After the installation is complete, shortcuts for launching the MXview One server will be created on the desktop and in the start menu.

NOTE

If your computer already has MXview installed, please uninstall it and then start the MXview One program installation process.

For Ubuntu 20.04

There are two ways to install MXview One on **Ubuntu 20.04**, including offline and online installation. We suggest users to install **offline**.

[Offline installation]

Step 1: Put these three files into the "~" Directory.

- installDepPacks.sh
- MXviewOneDepPack.tar
- MXview_One_Vx.x_Build_xxxxxxxx.deb

Step 2: Install dependent software by executing command line sequentially

#cd ~

#./installDepPacks.sh

Step 3: Install MXview One Linux

#sudo apt install ./MXview_One_Vx.x_Build_xxxxxxxx.deb

Step 4: Configure MXview One as a system service and restart Linux

#sudo /usr/mxview/mxview-control-panel/MXControlPanel service --action activate

#sudo reboot now

Step 5: After restarting, open a web browser and enter https://127.0.0.1

(Change the default IP address to the IP address of the computer where MXview One is running)

Provide the following login credentials

- Username: The default username is admin.
- Password: The default password is moxa.

[Online installation]

Step 1: Put the file into the "~" Directory.

- MXview_One_Vx.x_Build_xxxxxxxx.deb

Step 2: Install the database package.

#sudo apt install curl ca-certificates gnupg

#curl https://www.postgresql.org/media/keys/ACCC4CF8.asc | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/apt.postgresql.org.gpg >/dev/null

#sudo sh -c 'echo "deb http://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg main" > /etc/apt/sources.list.d/pgdg.list'

#sudo apt update

#sudo apt install postgresql-10

Step 3: Install the environment that runs Node.js.

#sudo apt install curl

#cd ~

#curl -sL https://deb.nodesource.com/setup_16.x | sudo bash -

#sudo apt -y install nodejs

Step 4: Install the MQTT communication software package.

#wget http://repo.mosquitto.org/debian/mosquitto-repo.gpg.key

#sudo apt-key add mosquitto-repo.gpg.key

#cd /etc/apt/sources.list.d/

#sudo wget http://repo.mosquitto.org/debian/mosquitto-buster.list

#sudo apt-get update

#sudo apt-get install mosquitto=1.6.10-0mosquitto1~buster1

Step 5: Install MXview One Linux

#cd ~

#sudo systemctl stop postgresql

#sudo apt install ./MXview_One_Vx.x_Build_xxxxxxxx.deb

Step 6: Configure MXview One as a system service and restart Linux

#sudo /usr/mxview/mxview-control-panel/MXControlPanel service --action activate

#sudo reboot now

Step 7: After restarting, open a web browser and enter https://127.0.0.1

(Change the default IP address to the IP address of the computer where MXview One is running)

Provide the following login credentials

- Username: The default username is admin.
- Password: The default password is moxa.

NOTE

We recommend you first try to perform **offline installation** to prevent any compatibility issues with online installation. If you fail to activate MXview One by online installation, please install it offline.

For Ubuntu 18.04

Install MXview One on **Ubuntu 18.04** using the online installation method.

[Online installation]

Step 1: Install the database package.

#sudo apt install curl ca-certificates gnupg

#curl https://www.postgresql.org/media/keys/ACCC4CF8.asc | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/apt.postgresql.org.gpg >/dev/null

#sudo sh -c 'echo "deb http://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg main" > /etc/apt/sources.list.d/pgdg.list'

#sudo apt update

#sudo apt install postgresql-10

Step 2: Install the environment that runs Node.js.

#sudo apt install curl

#cd ~

#curl -sL https://deb.nodesource.com/setup_16.x | sudo bash -

#sudo apt -y install nodejs

Step 3: Install the MQTT communication software package.

#wget http://repo.mosquitto.org/debian/mosquitto-repo.gpg.key

#sudo apt-key add mosquitto-repo.gpg.key

#cd /etc/apt/sources.list.d/

#sudo wget http://repo.mosquitto.org/debian/mosquitto-jessie.list

#sudo wget http://repo.mosquitto.org/debian/mosquitto-stretch.list

#sudo wget http://repo.mosquitto.org/debian/mosquitto-buster.list

#sudo apt-get update

#udo apt-get install mosquitto=1.6.10-0mosquitto1~buster1

Step 4: Install MXview One Linux

#sudo systemctl stop postgresql

#sudo apt install ./MXview_One_Vx.x_Build_xxxxxxxx.deb

Step 5: Configure MXview One as a system service and restart Linux

#sudo /usr/mxview/mxview-control-panel/MXControlPanel service --action activate

#sudo reboot now

Step 6: After restarting, open a web browser and enter https://127.0.0.1

(Change the default IP address to the IP address of the computer where MXview One is running)

Enter the following login credentials:

- Username: The default username is admin.
- Password: The default password is moxa.

Uninstallation

For Windows

1. Locate the **Control Panel** in Windows.
2. Under **Programs**, click **Uninstall a program**
   The **Uninstall or change a program** screen appears
3. Select **MXview One**
4. Click **Uninstall** or **Uninstall/Change** at the top of the program list

For Ubuntu

Execute the command line.

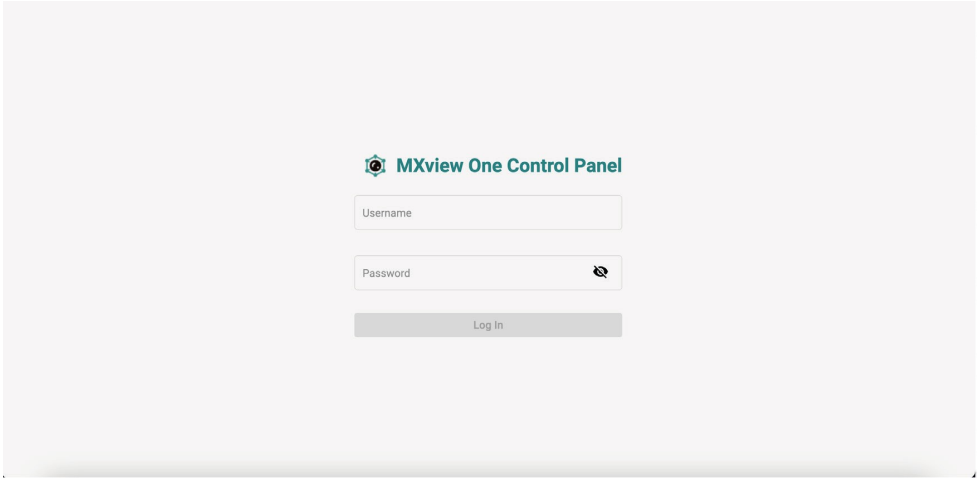
#sudo apt remove mxview

MXview One Control Panel

Server Control

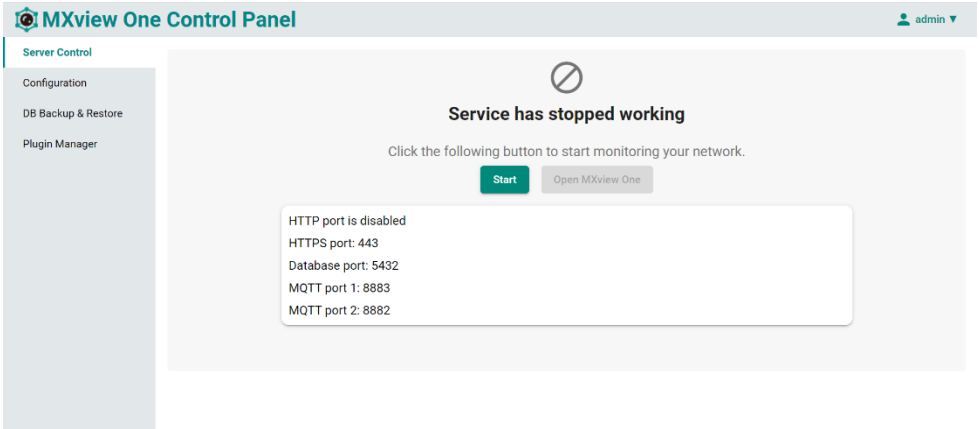
Start the MXview One server on the computer before launching the MXview One web console. On the server computer, double-click the MXview One desktop shortcut in the Windows operating system. For Ubuntu users, type in the local host IP address to open the page.

The MXview One Control Panel log in screen appears first and after logging in will direct to the Control Panel.

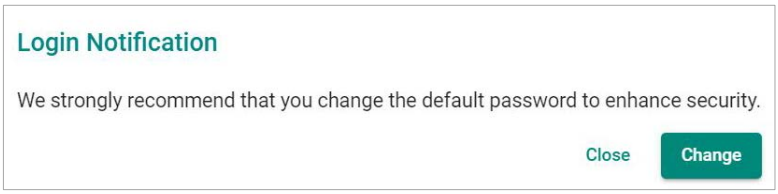


Provide the following login credentials

- **Username:** The default username is **admin**.
- **Password:** The default password is **moxa**.



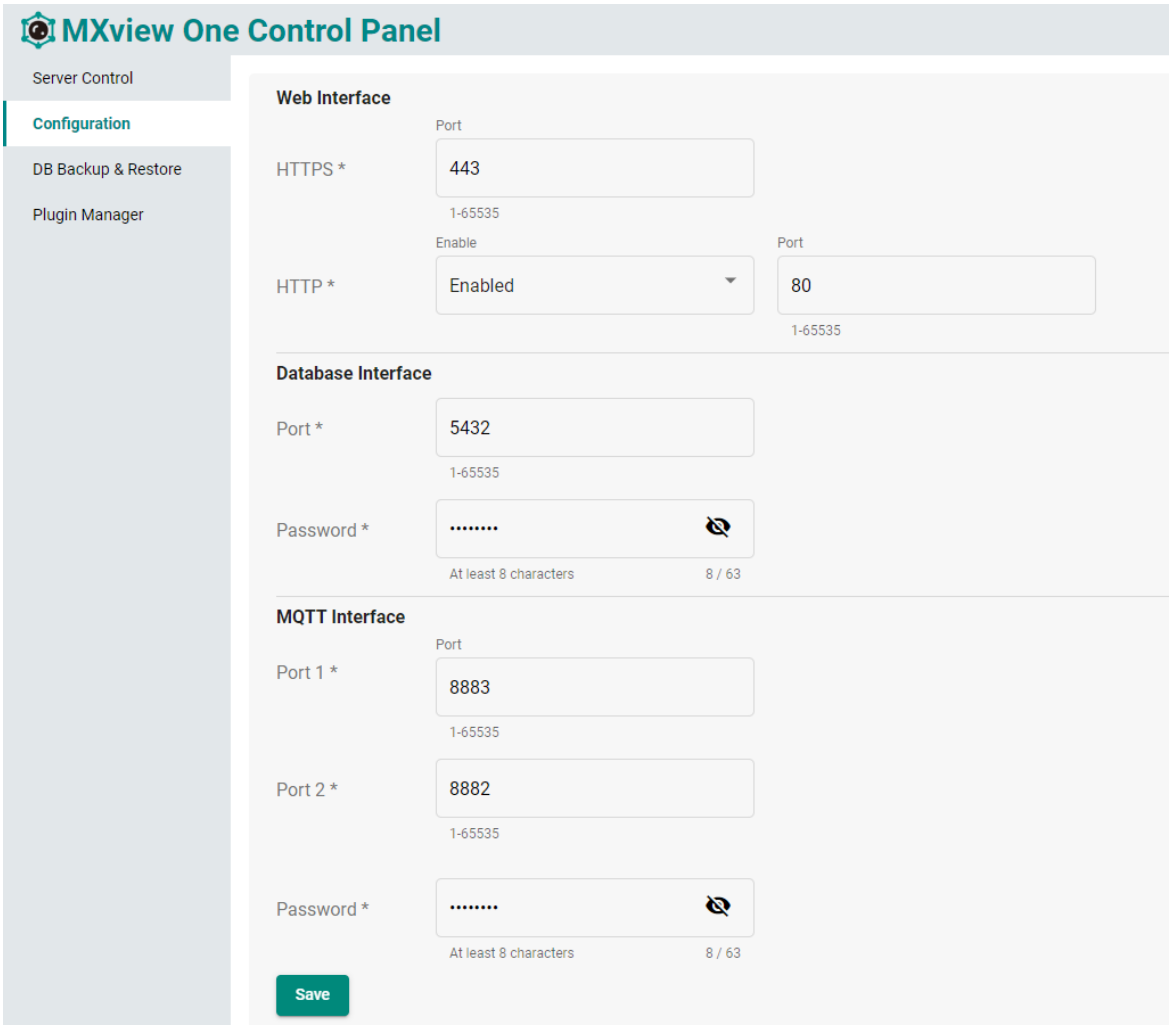
If it is the first time you log in to the MXview One Control Panel, please change the default password to enhance security.



Configuration

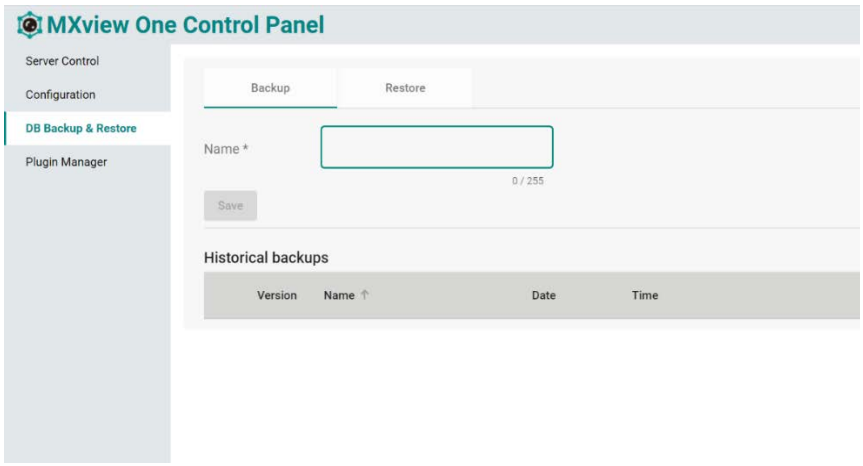
Configure the following port numbers in the **Configuration** Page and click **Save** once the setting is completed:

- **Web Interface**
  - **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 Interface**
  - **Database Port:** Specify the database port of the server or use the default value of **5432**.
- **MQTT Interface**
  - **MQTT Port:** Specify the communication port between MXview One and its internal system or use the default values of **8883** and **8882**.

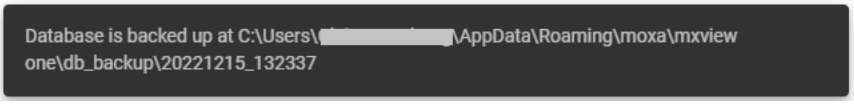


DB Backup & Restore

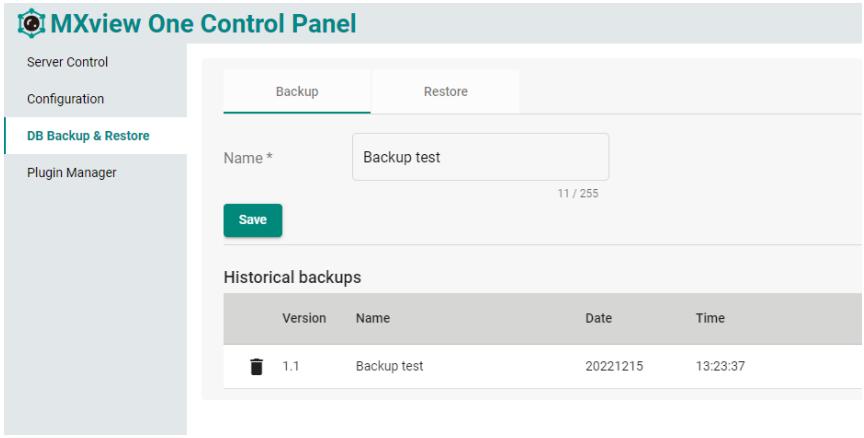
1. Navigate to **DB Backup & Restore** on the MXview One Control Panel.
   The Database Backup & Restore screen will appear and includes **Backup** and **Restore** functions.



2. Choose the **Backup** tab to start the process of backing up the database.
3. In the **Name** field, specify the backup file name.
4. Click **Save**.
5. The message that the file of the backup database has been stored in the specified directory will be displayed.



6. When the database has been backed up successfully it will appear in the **Historical backups** list.

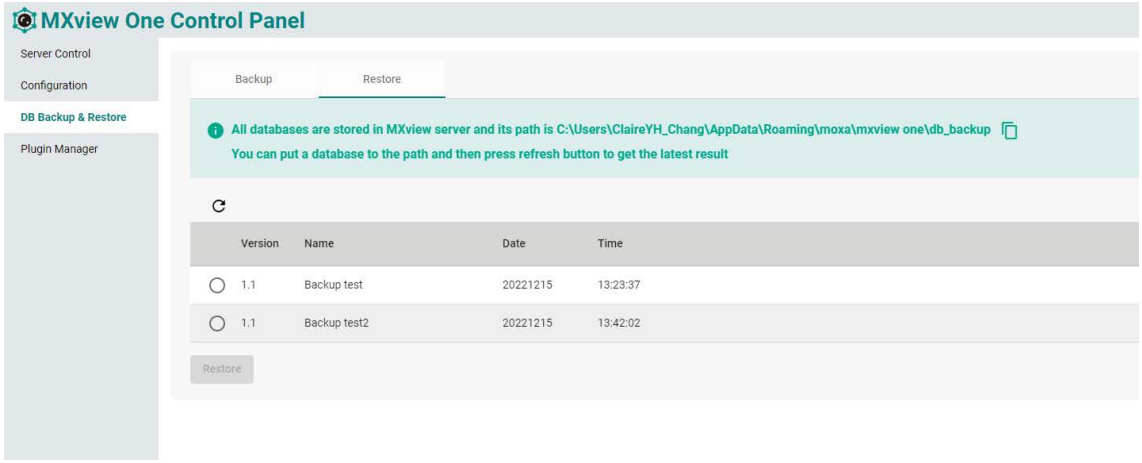


The system backup file includes the following items:

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

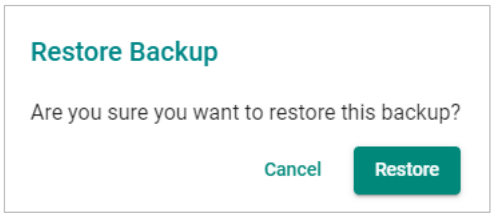
The MXview One system will restore the system configurations from a backup file.

1. Click the **Restore** Tab.

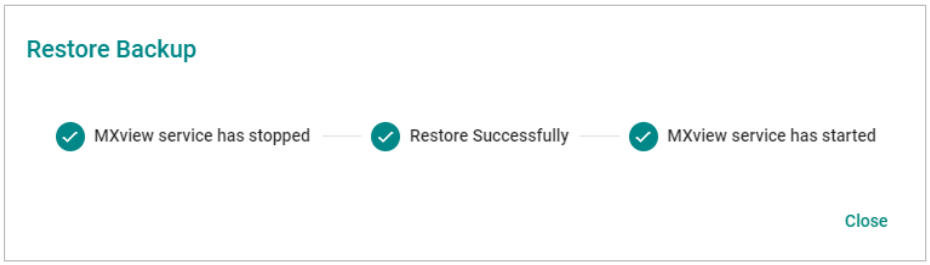


2. Choose the backups you want to restore in the table. You can also copy a a database to a specific path and then press refresh button to get the latest result.
3. Click **Restore**.

   A confirmation screen will appear.



4. Displaying the restoration process.



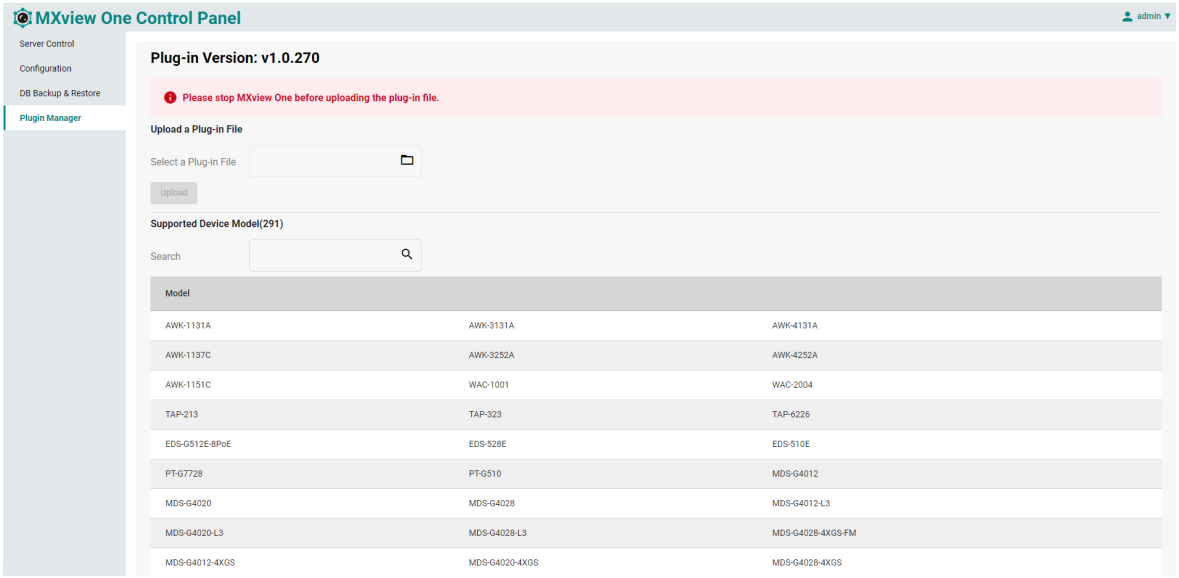
5. Click **Close**.

Plugin Manager

Navigate to **Plugin Manager** on the **Control Panel**. The Plugin Manager is a tool that can be used to manage the plugin files. When you discover a new Moxa product that has not been integrated in to the latest MXview One version, you may not be able to retrieve the product information from MXview One. To solve this, you can download the plugin file from Moxa's website, and then upload the file in the Plugin Manager. After uploading the plugin files, these new models can be supported by MXview One.

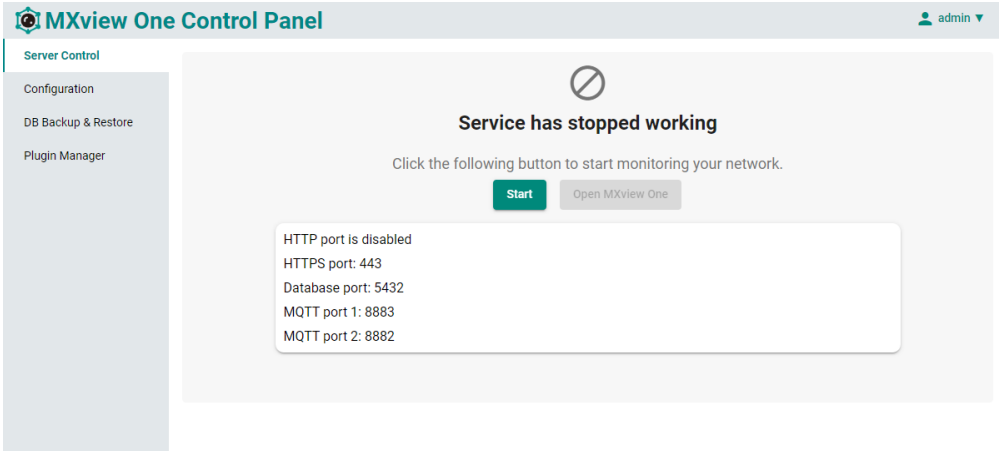
The **Plugin Manager** screen includes the following information:

- Plug-in file version
- Upload a Plug-in file
- Supported device model



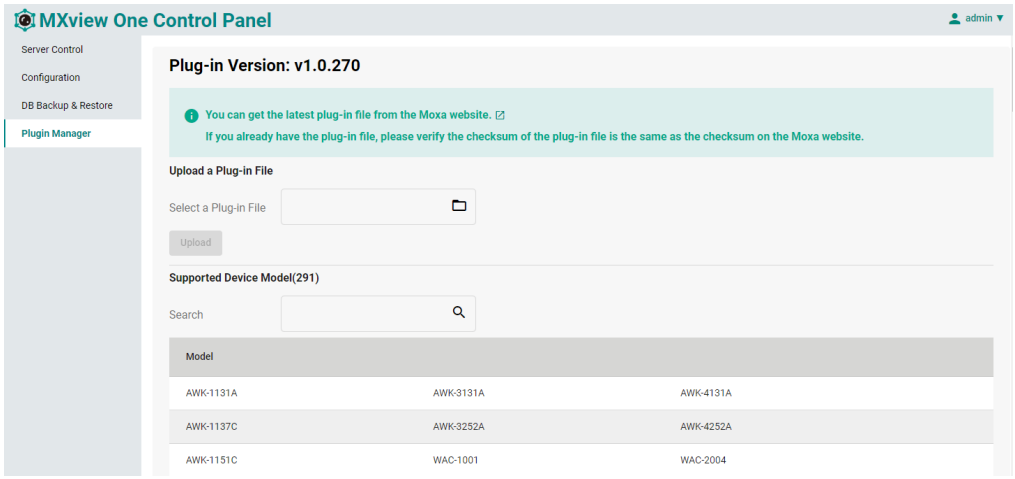
Steps to **Upload a Plug-in File**:

1. Stop MXview One.

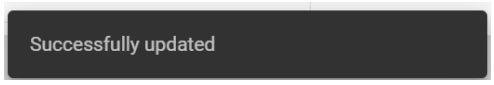


2. Download the latest plug-in file from the Moxa website. https://www.moxa.com/en/products/industrial-network-infrastructure/network-management-software/mxview-one-series#resources

3. Navigate to the **Plugin Manager** on the **Control Panel**.

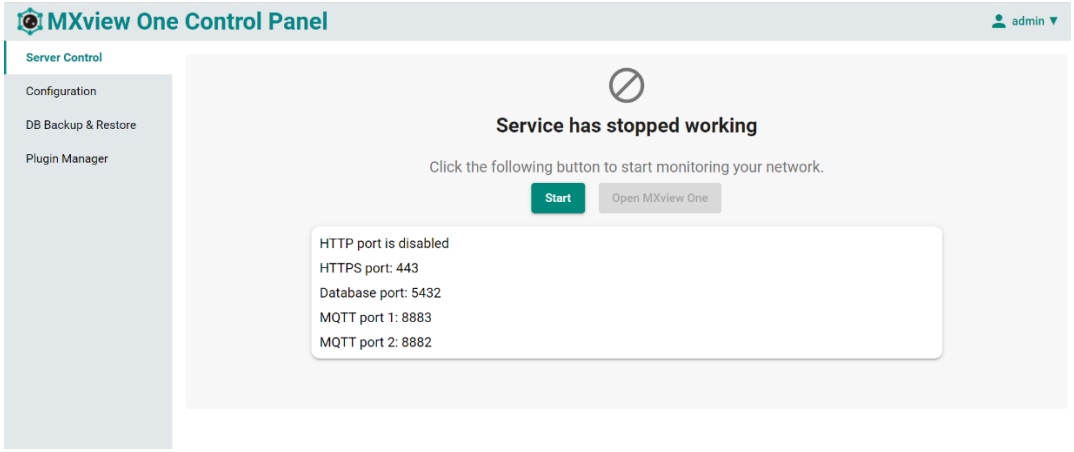


4. Click the folder (🗀) icon in **Select a Plug-in File** to upload the file (.zip) from your local machine.
5. Click **Upload** and if successful, the message below will be displayed.
   MXview One will upload the plug-in file and display the supported devices.

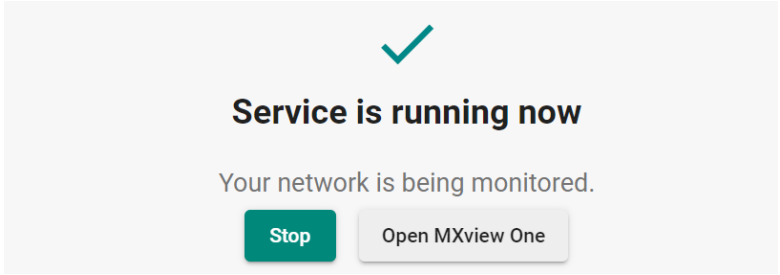


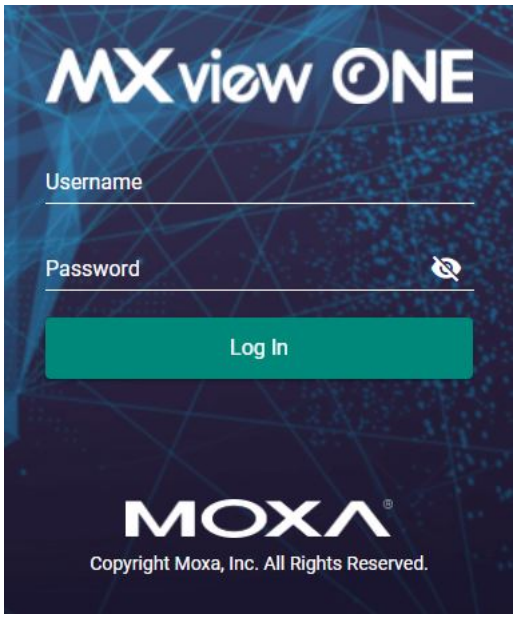
Starting the MXview One Server and Logging Into MXview One

1. Click **Start** on the Server Control page. The MXview One server will start running.



2. Wait for the status to display **Service is running now**, then click **Open MXview One** and log in to MXview One:





Provide the following login credentials

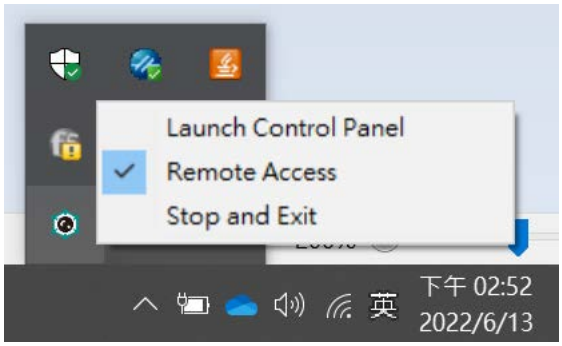
- **Username:** The default username is **admin**.
- **Password:** The default password is **moxa**.

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

Logging Into MXview One Remotely

You can log in remotely to MXview One that is installed on your local site computer from another computer.

1. Launch the MXview One server at the local site computer. Go to the tool bar and click the MXview One icon. Select **Remote Access**.

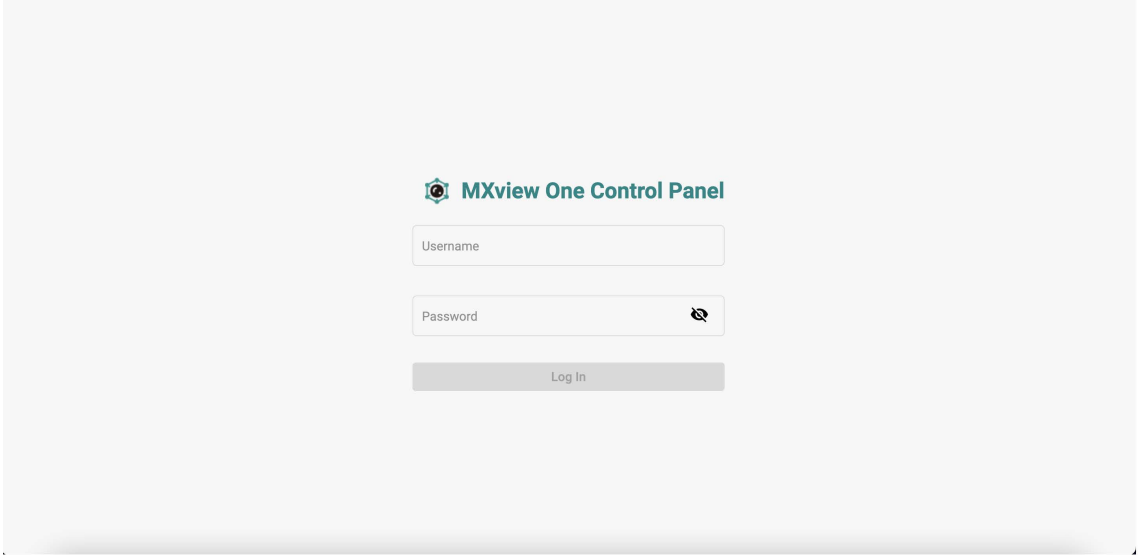


> **NOTE**
>
> If you want to close the remote function, just click the Remote Access again, then the function will be closed.

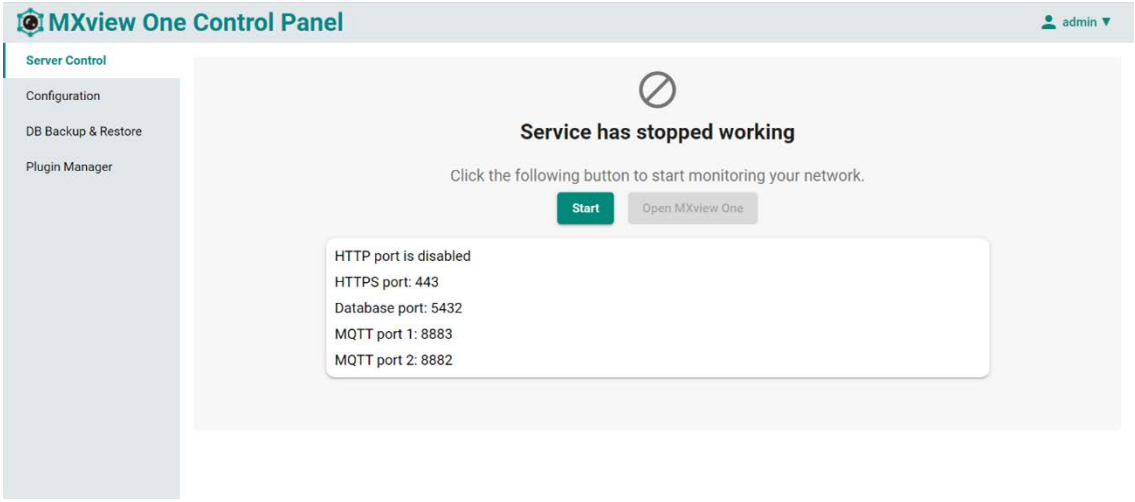
2. Open a web browser on the computer located at the remote site.

3. In the address bar, input the IP address or domain name of the computer that you want to log in to MXview One from.
   - Format: **https://[IP address]:[Port]**
   - Example: https://192.168.1.250:7100

   The MXview One Control Panel appears.



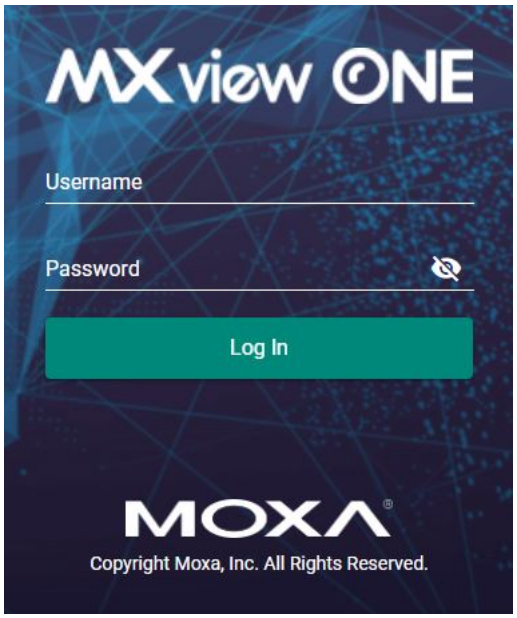
4. Provide the following login credentials
   - **Username:** The default username is **admin**.
   - **Password:** The default password is **moxa**.
5. You can choose one of the actions listed below:
   - Click the Start button
   - Click the Stop button
   - Change the configurations on the Configuration page



6. To open the MXview One web console, you can type the IP address of the computer at the local site into another web browser once the MXview One Control Panel displays 'Service is running now'.
   - Format: **https://[IP address]**
   - Example: https://192.168.1.250

   The MXview One web console appears.

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



NOTE

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

License Management

You can monitor your devices inside the networking status via MXview One. Please note, in order to monitor the devices, you need to activate the Node-based license. For example, if you activate 123 nodes in MXview One, then during the device discovery MXview One will only recognize up to 123 nodes. MXview One will stop the device discovery process once it reaches the 123-node limit.

To increase the node limit, you can purchase additional licenses and import the license into MXview One.

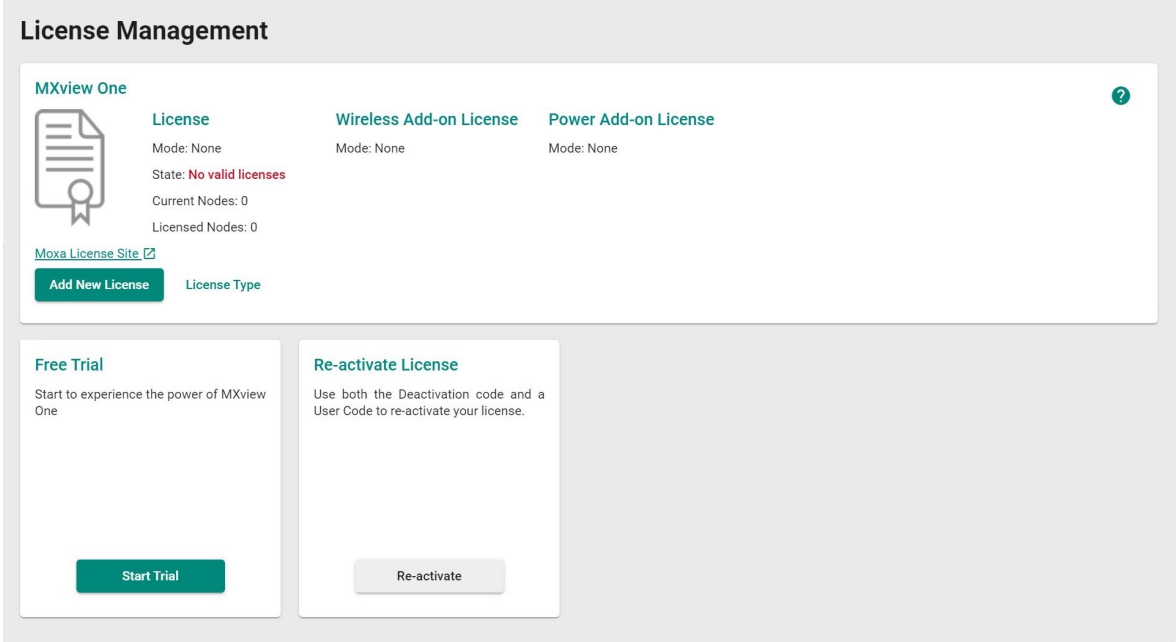
NOTE

Click "Start Trial" to start using MXview One.

Checking the License

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

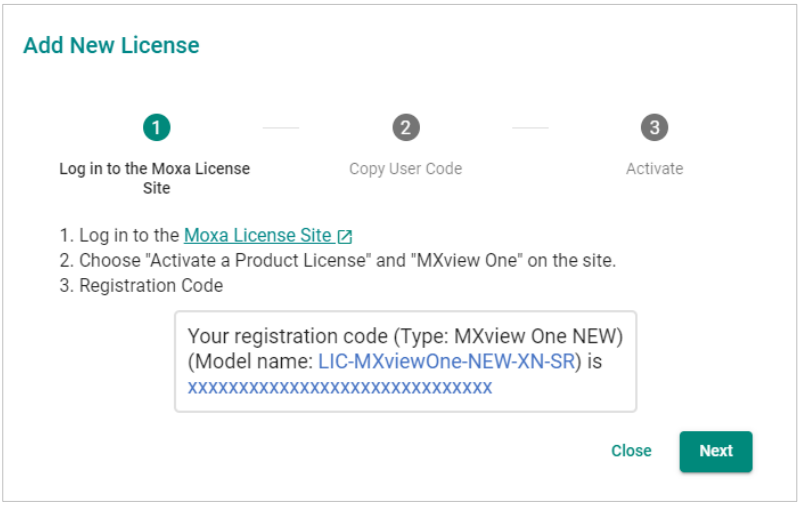
To access the **License Management** screen, navigate to **Menu** ( ) **> Administration > License Management.**



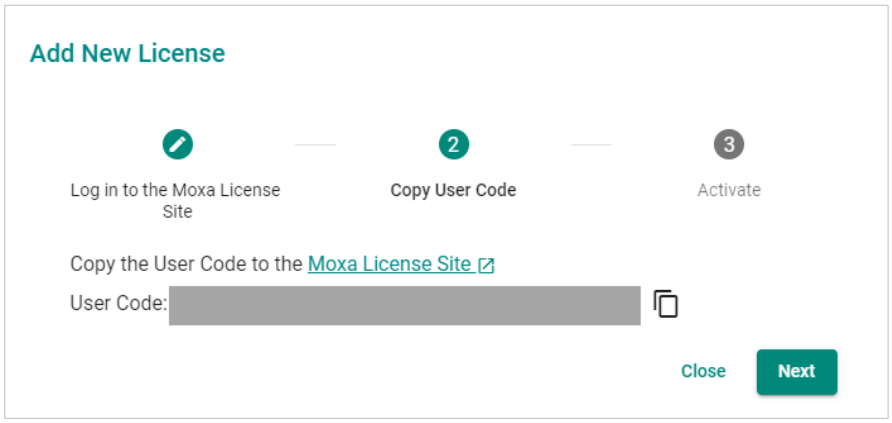
Adding a New License

To increase the node limit of your MXview One server, you need to add the node-based license.

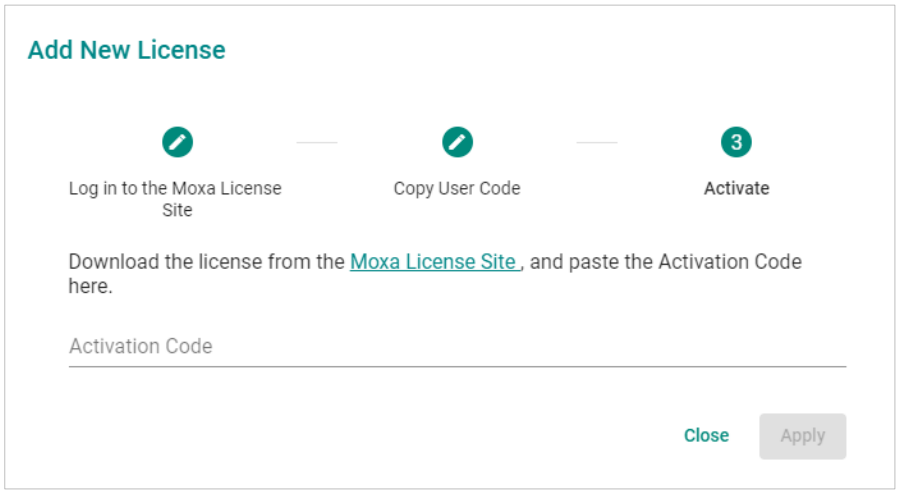
1. Navigate to **Menu** ( ) **> Administration > License Management**.
   The **License Management** screen appears.
   In the **Add New License** section, click **Add New License**.
2. Login to the Moxa License Site to activate the MXview One license. Click **Next** to get the User Code.



3. Copy the User Code.



4. Input a valid activation code.



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

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

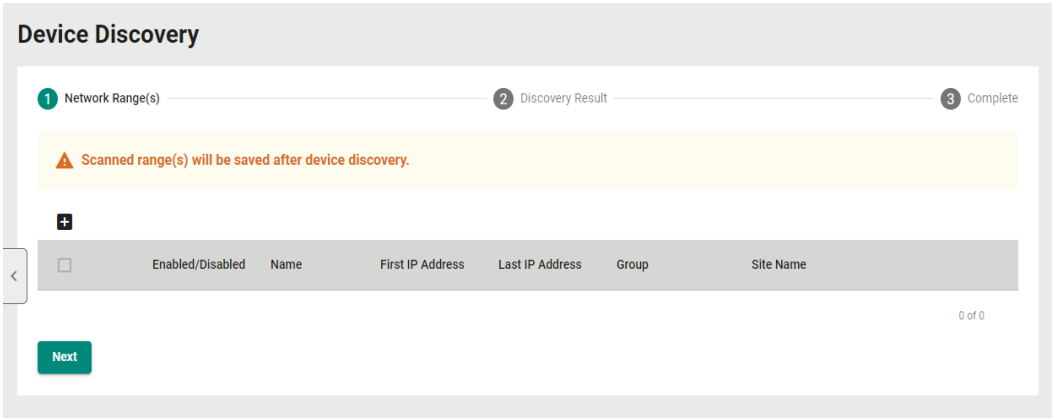
Using Device Discovery

MXview One provides Device Discovery to help users quickly determine the network topology and handle basic configuration tasks.

1. To launch Device Discovery manually please do the following:

   Navigate to **Menu** (☰) **> Device Discovery**.

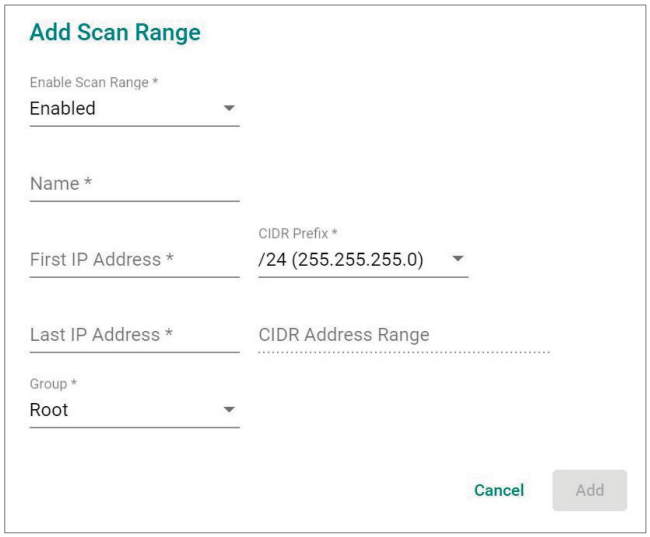
   Device Discovery appears to the right of the navigation panel.



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

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

> **NOTE**
>
> Moxa devices must have the SNMP function enabled for MXview One to scan the 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 One **Group** to assign the scan range to.

d. Click **Add**.

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

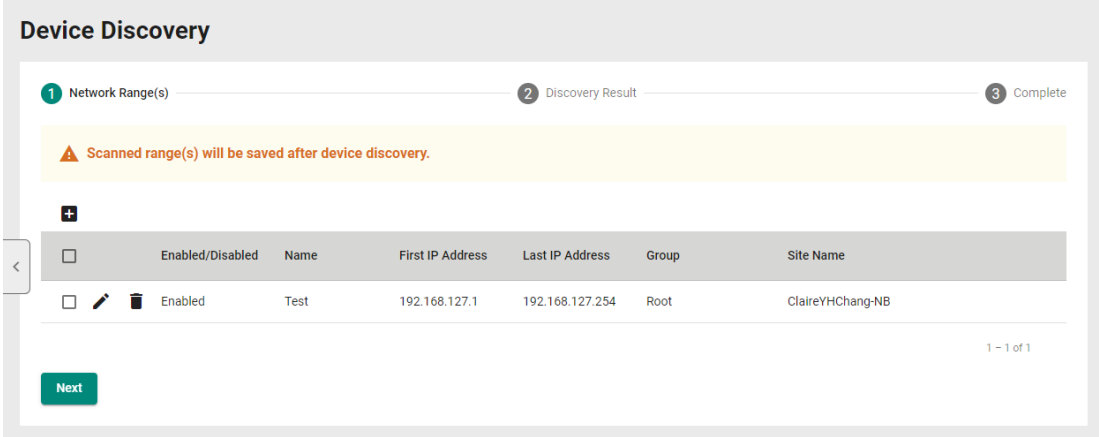
f. (Optional) Modify scan range settings, click the **Edit** (✎) icon next to an added scan range.

g. (Optional) Remove a scan range, click the **Delete** (🗑) icon next to the added scan range.

h. Select one or more scan ranges to scan.

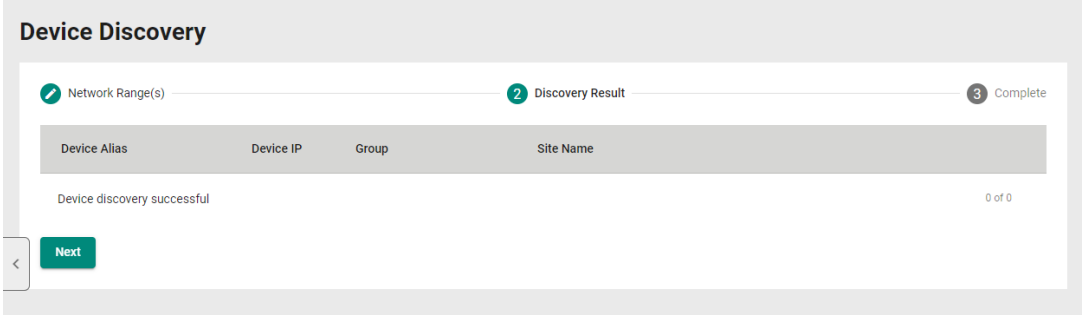
i. Click **Next**.

MXview One scans the specified IP address ranges for devices.



3. View devices discovered on the network.

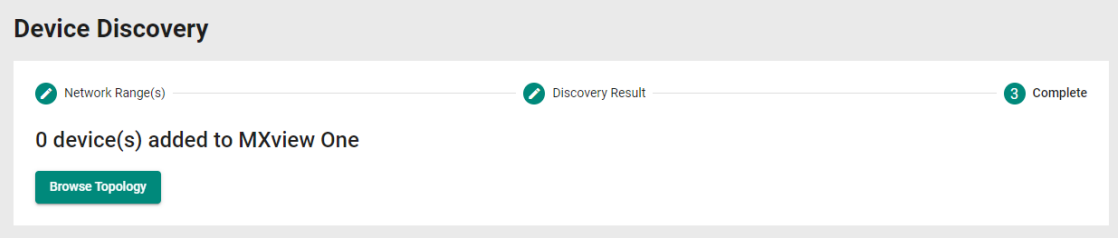
a. MXview One displays discovered devices on the **Discovery Result** list. Scroll down to view more devices on the list.



b. Click **Next**.

4. Click **Browse Topology** to view the detailed network topology.

The **Topology** screen appears.



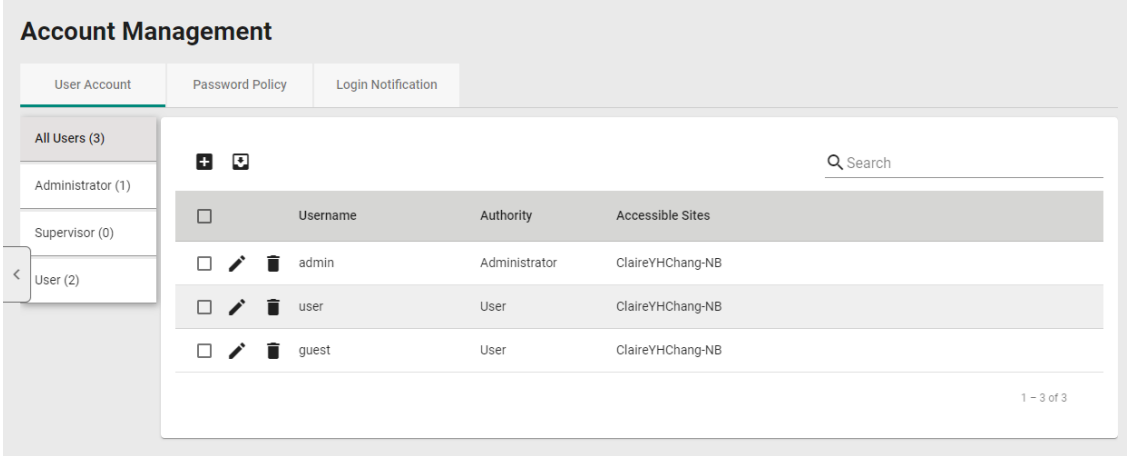
NOTE

MXview One cannot guarantee that it can draw the link of the topology for non LLDP devices. However, you can draw the link of the topology manually by clicking **Add Link**.

Account Management

To launch Account Management, please do the following: Navigate to **Menu** ( ) **> Account Management**.

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



MXview One provides three default accounts:

- admin
- user
- guest

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

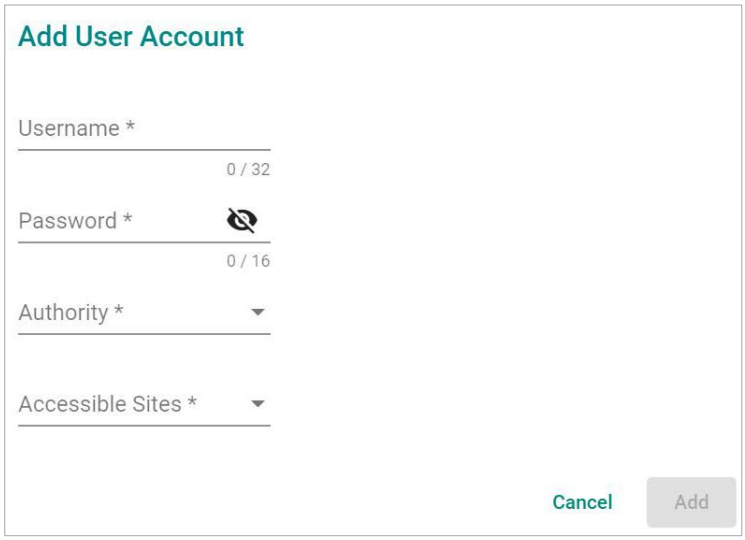
Each account can be assigned one of the following **Authority** permissions:

- **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 on all pages apart from the **Account Management** page.
- **User:** Has the permissions listed below.

Function	Description
Dashboard	Read-only
Topology	Read-only
Event History	Can do some actions: Export, Filter
Syslog Viewer	Can do some actions: Export, Filter
Inventory Report	Can do some actions: Export
About MXview One	Can check the version
User Manual	Can link to the document
API Documentation	Can link to the document

Adding User Accounts

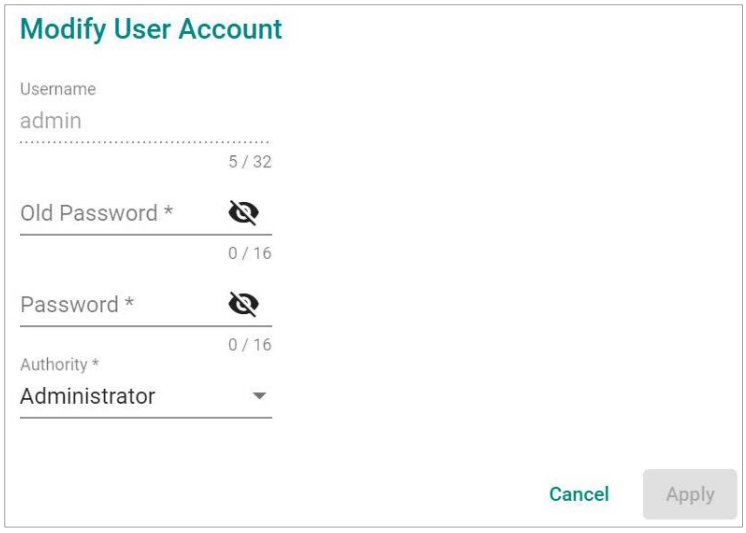
1. Navigate to **Menu** ( ) **> Administration > Account Management**.
   The **Account Management** screen appears.
2. Click the **Add** ( ) icon in the top right corner of the screen.
   The **Add user account** screen appears.



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

Modifying User Accounts

1. Navigate to **Menu** ( ) **> Administration > 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:
   - **Password:** Specify the login password (minimum length: 4 characters) for the account
   - **Authority:** Assign the authority permission (Administrator, Supervisor, or User) for the account
4. Click **Apply**.

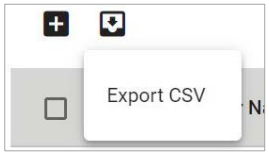
Deleting User Accounts

1. Navigate to **Menu** ( ) **> Administration > 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 left corner of the screen (if multiple accounts are selected).
   MXview One 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** ( ) **> Administration > Account Management**.
   The **Account Management** screen appears.
2. Click the **Export** ( ) icon.

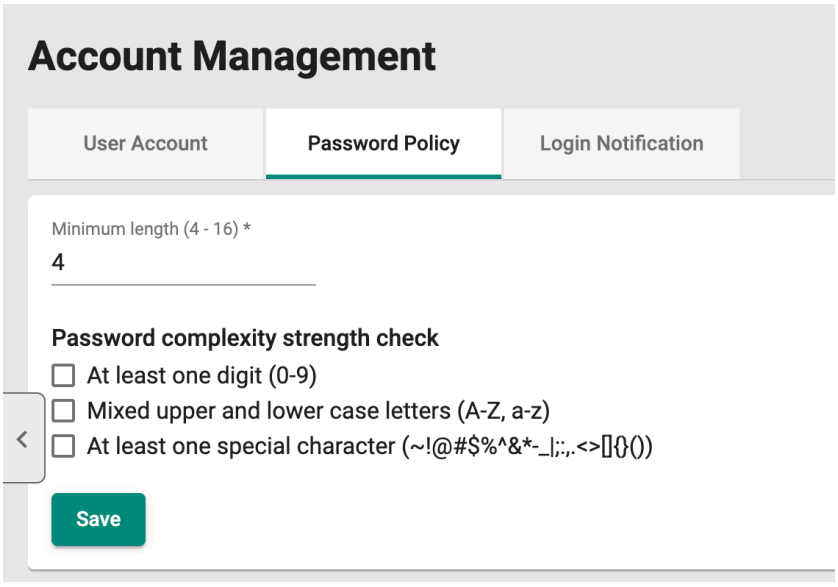


3. Select **Export CSV**.

Configuring the Password Policy

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

1. Navigate to **Menu** ( ) **> Administration > Account Management > Password Policy**.
   The **Password Policy** screen appears.



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

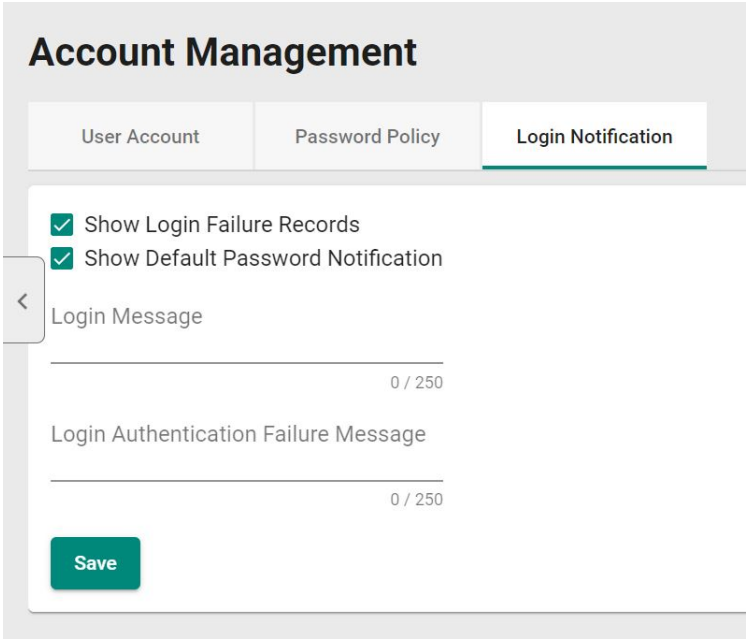
   MXview One requires all new account passwords to satisfy the modified password policy.

Configuring Login Notifications

Use the **Password Policy** screen to customize the notifications displayed when users log in to MXview One.

1. Navigate to **Menu** ( ) **> Administration > Account Management > Login Notification**.

   The **Login Notification** screen appears.



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

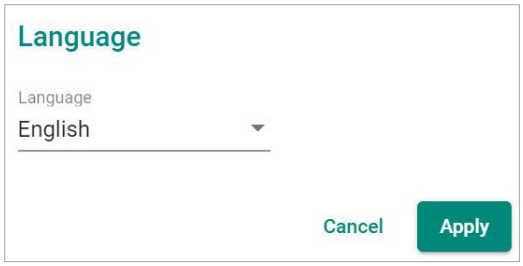
   MXview One displays the configured login notifications the next time a user logs in.

Changing the Display Language

Use the **Language** icon screen to customize the notifications displayed when users log in to MXview One.

1. Navigate to **Language** ( ).

   The **Language** screen appears.
2. Select language.



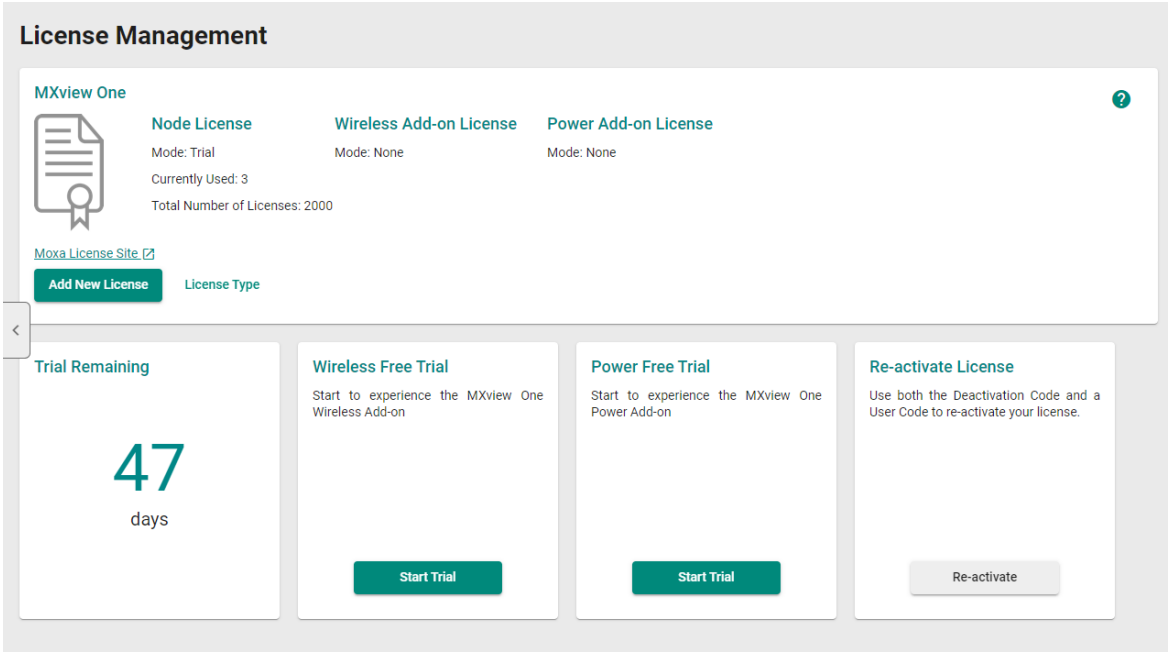
3. MXview One supports the following languages:
   - **German (Deutsch)**
   - **Japanese (日本語)**
   - **English**
   - **Spanish (Español)**
   - **French (Français)**
   - **Simplified Chinese (简体中文)**
   - **Traditional Chinese (繁體中文)**
4. Click **Save**.

   MXview One updates the display language.

License Management Overview

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

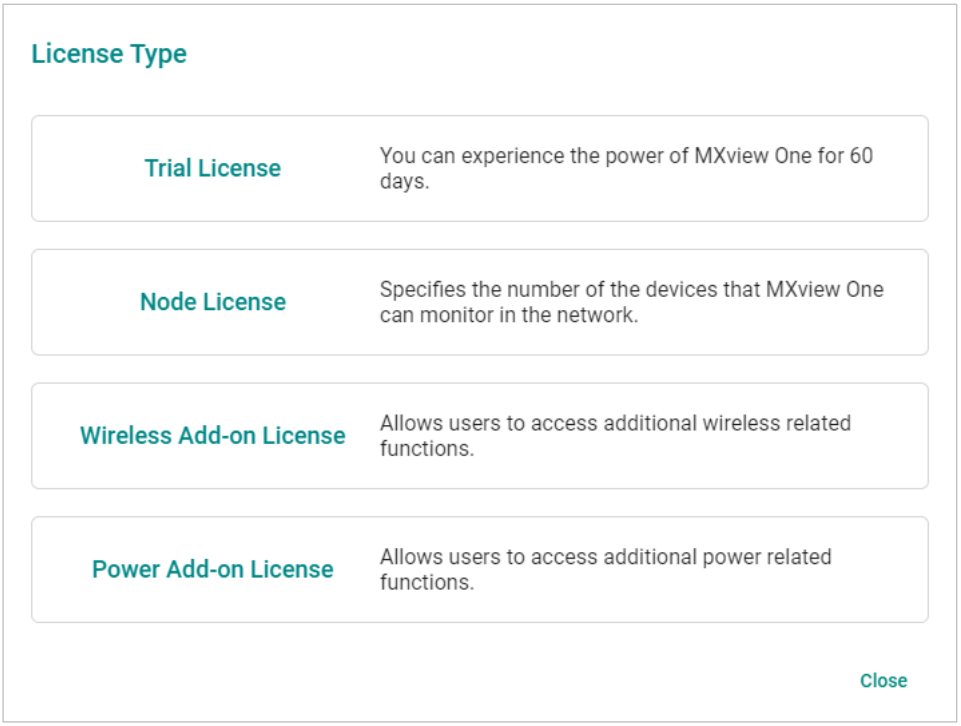
To access the **License Management** screen, navigate to **Menu** ( ) **> Administration > License Management**.



License Type

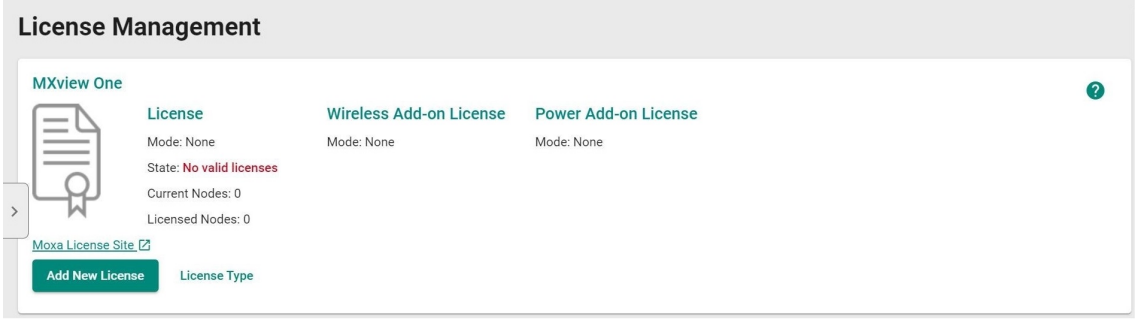
MXview One provides numerous types of licenses. Each license has a specific function.

Trial License	You can experience the power of MXview One for 60 days.
Node License	Specifies the number of devices that MXview One can monitor in the network.
Wireless Add-on License	Allows users to access additional wireless related functions.
Power Add-on License	Allows users to access additional power related functions.

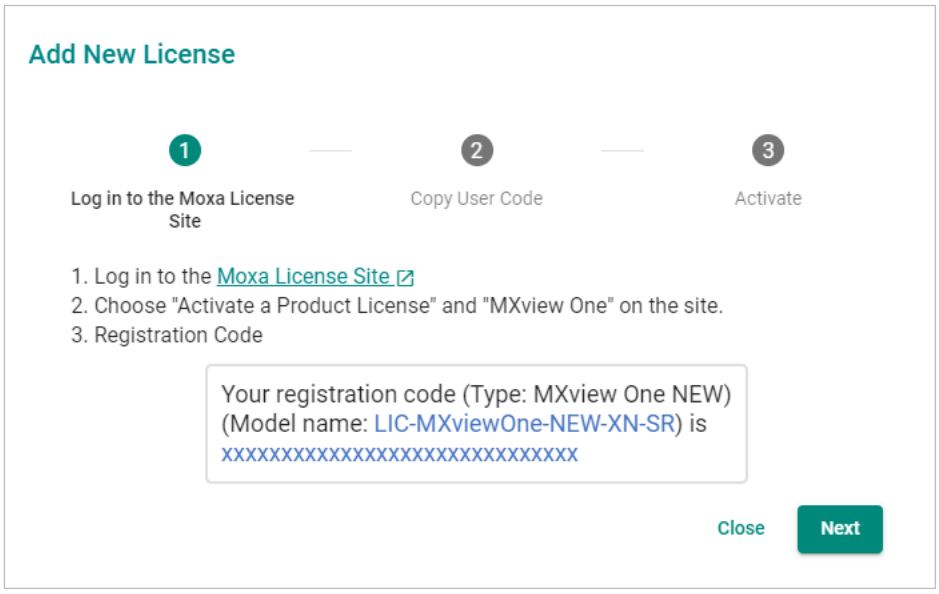


Adding a New License

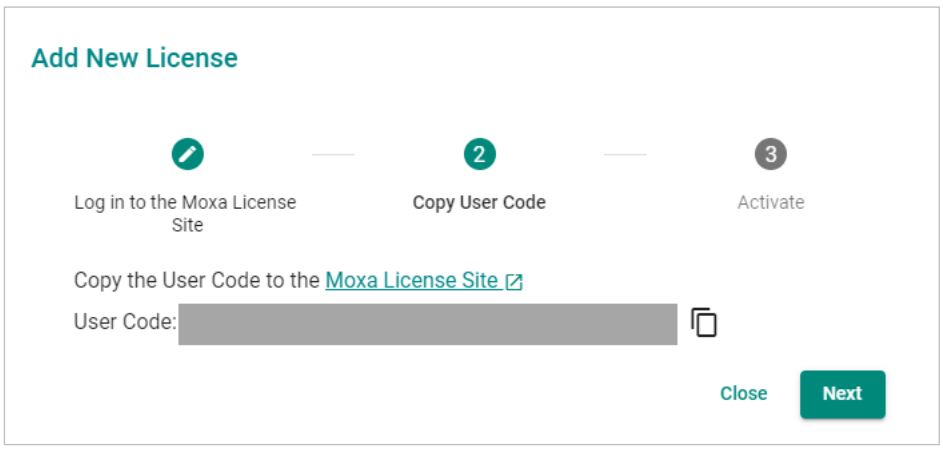
1. Navigate to **Menu** ( ) **> Administration > License Management**.
   The **License Management** screen appears.
2. In the **Add New License** section, click **Add New License**.



   The **Add New License** screen appears.

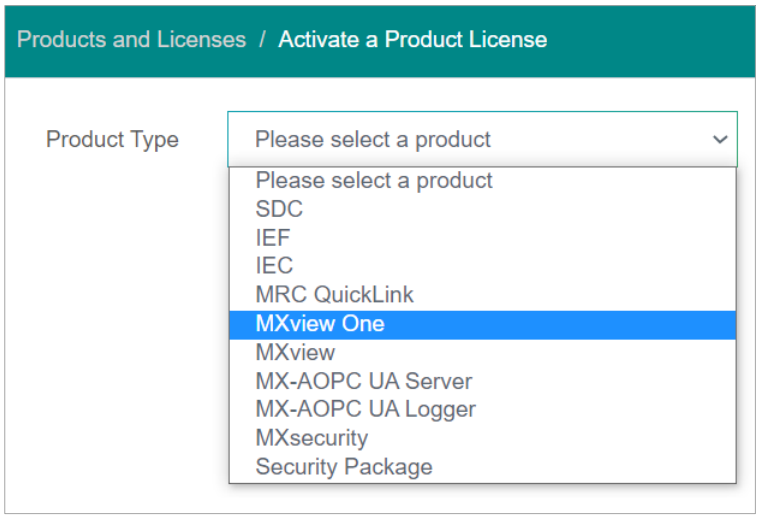


3. Click **Next**.
4. Copy the User Code and click **Next**.

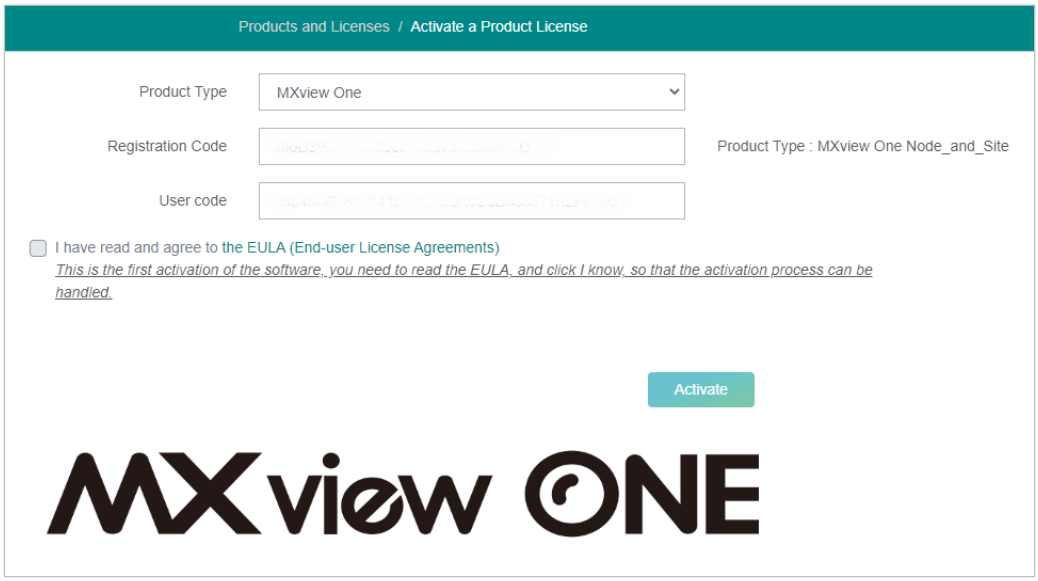


5. Open a web browser and go to https://license.moxa.com/. Select **MXview One** and Log in to your Moxa account.

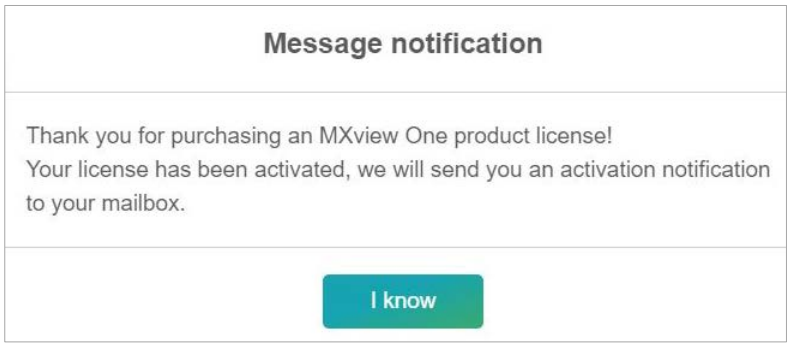
6. Click **Products and Licenses > Activate a Product License**. Then, select **MXview One** from the product type list.



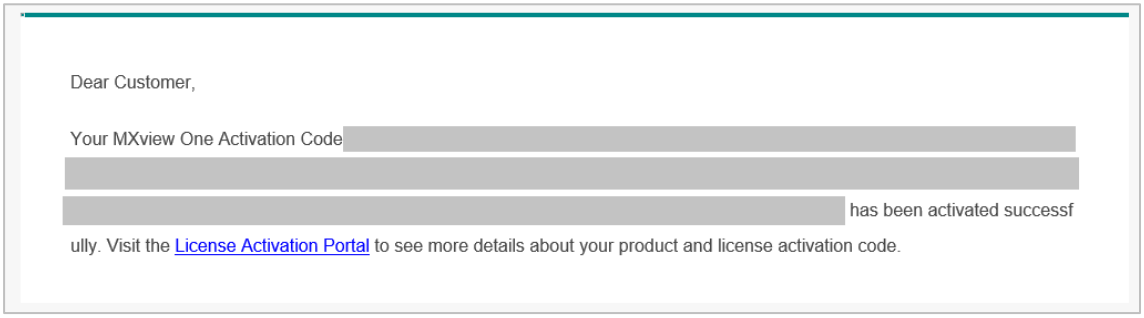
7. Input a valid **Registration Code** and see if the Product Type behind the Registration Code has displayed correctly of your license.
8. Paste a valid **User code** from MXview One. Click "I have read and agree to the EULA (End-user License Agreements)" checkbox. Then click **Activate** to get the activation code.



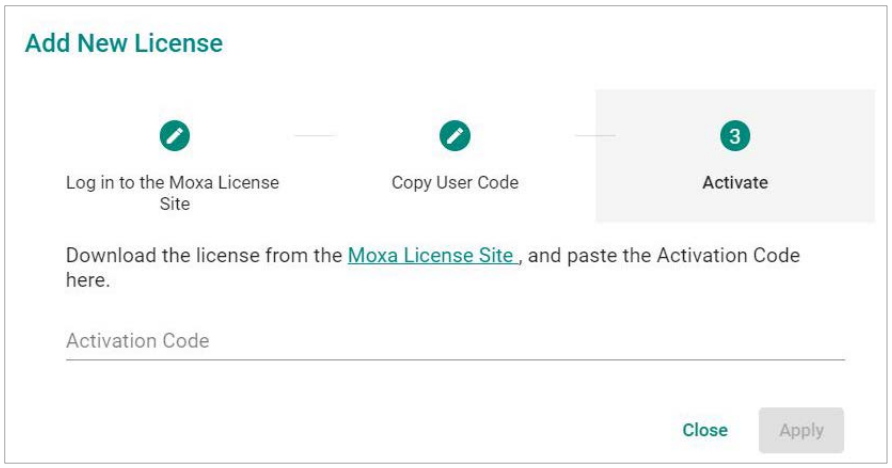
9. Once the process has been successfully completed, a pop-up window will appear to inform you that your license code has been activated. Click **I know** to close the window. If the license failed to activate, enter the correct Registration Code and User code again. If you are still experiencing problems,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



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



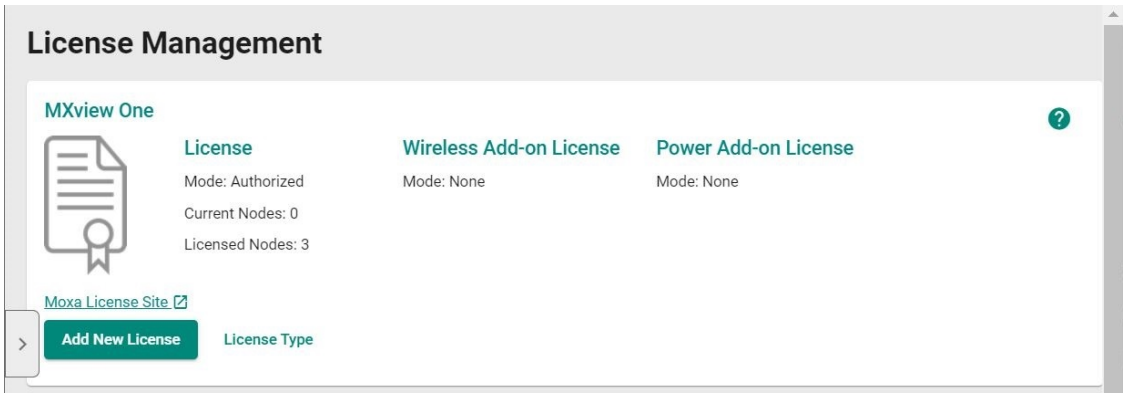
11. Copy the activation code from the email.
12. In MXview One, paste the activation code into the **Activation Code** field.



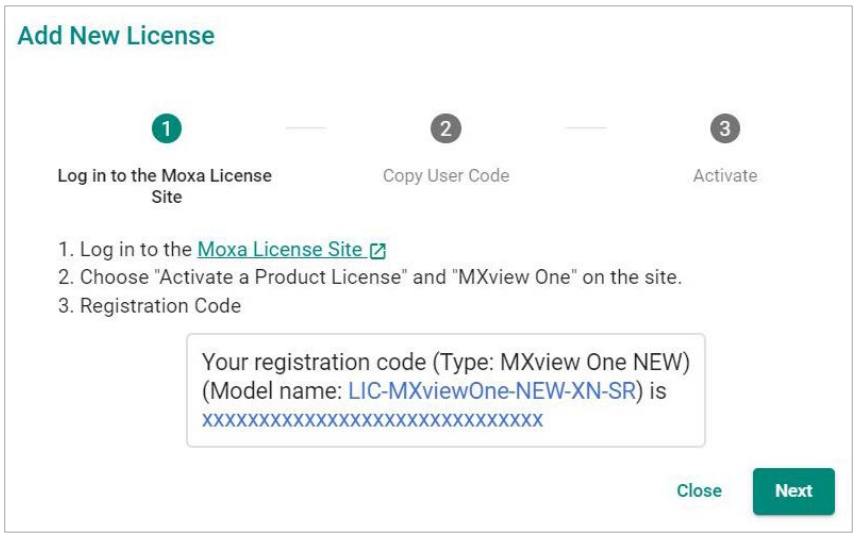
13. Click **Apply** and then MXview One will activate the new license.

Adding an Add-on License

1. Navigate to **Menu** ( ) **> Administration > License Management**.
   The **License Management** screen will appear.

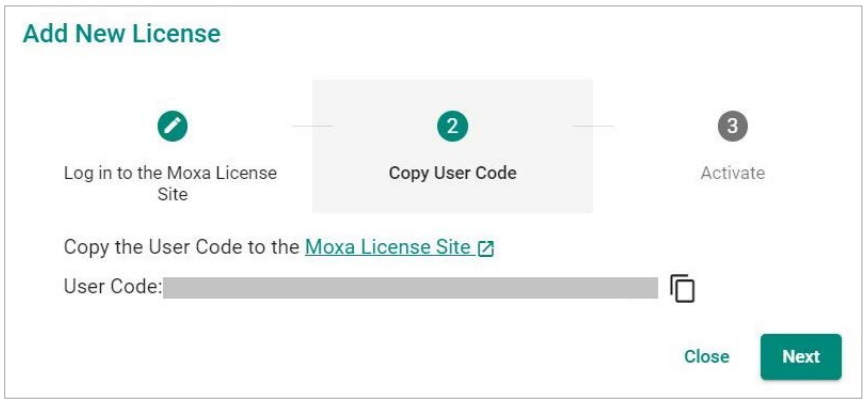


2. Click **Add New License**. The **Add New License** screen will appear.

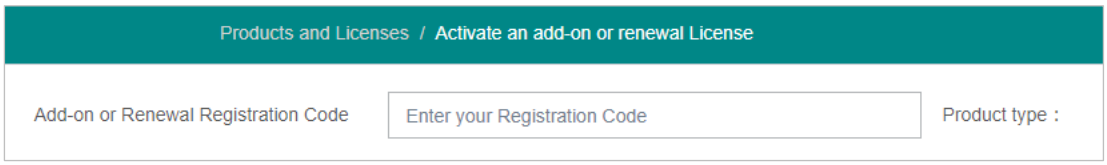


3. Click **Next**.
4. Copy the User Code and click **Next**.

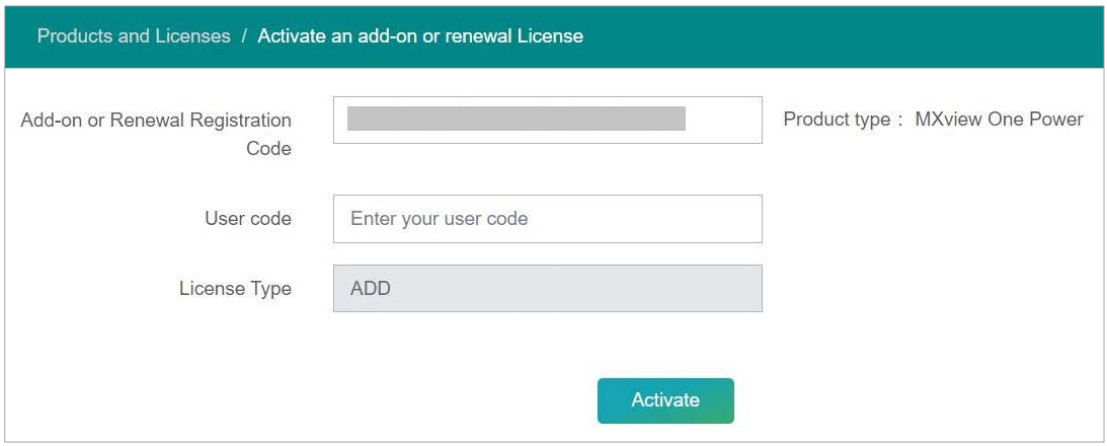
> **NOTE**
>
> Please activate the Node-based License before activating the Add-on License.



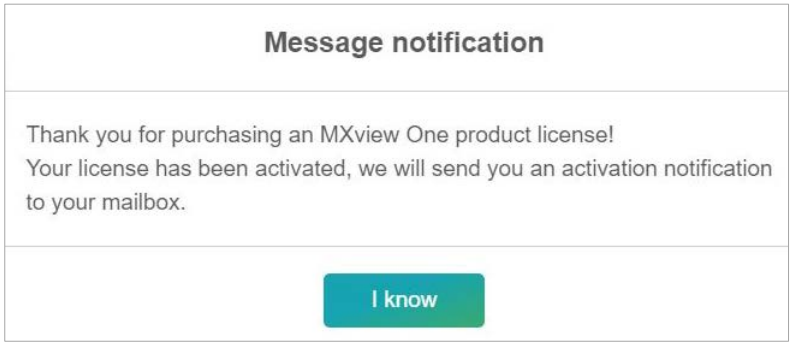
5. Open a web browser and go to https://license.moxa.com/. Select **MXview One** and log in to your Moxa account.
6. Click **Products and Licenses > Activate an add-on or renewal License**. Input a valid **Add-on Registration Code** and see if the Product Type behind the Registration Code has shown your license correctly.



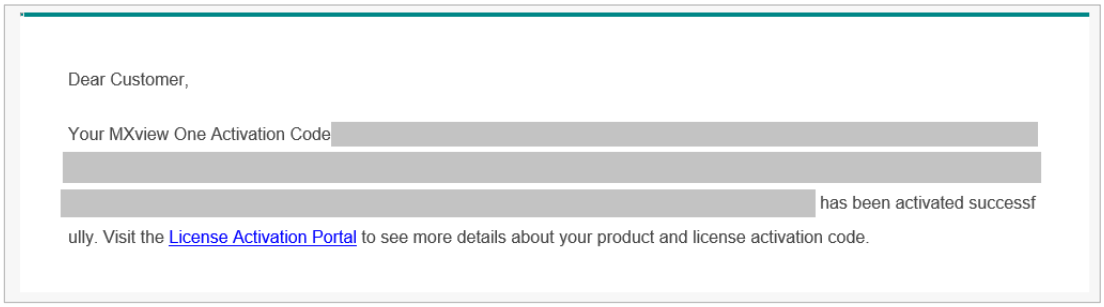
7. Paste a valid User code from MXview One. Then, click **Activate** to get the activation code.



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

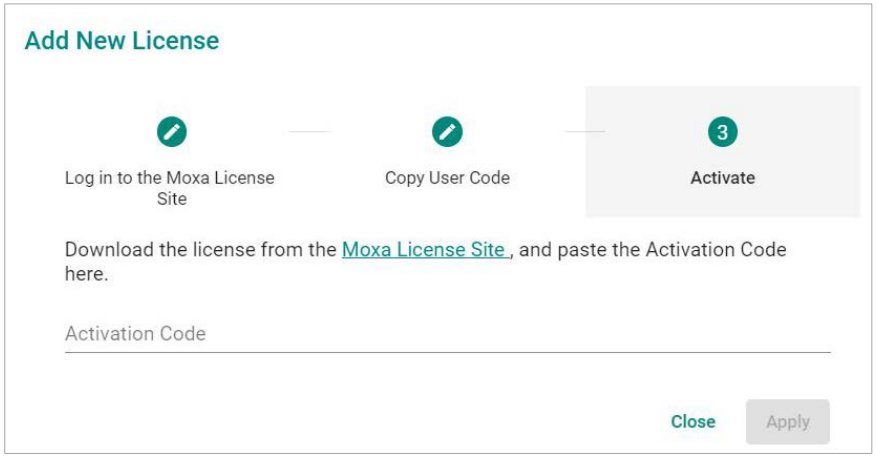


9. Check the email account you used to apply for your moxa account. The activation code will be sent to this email address.



10. Copy the activation code from the email.

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

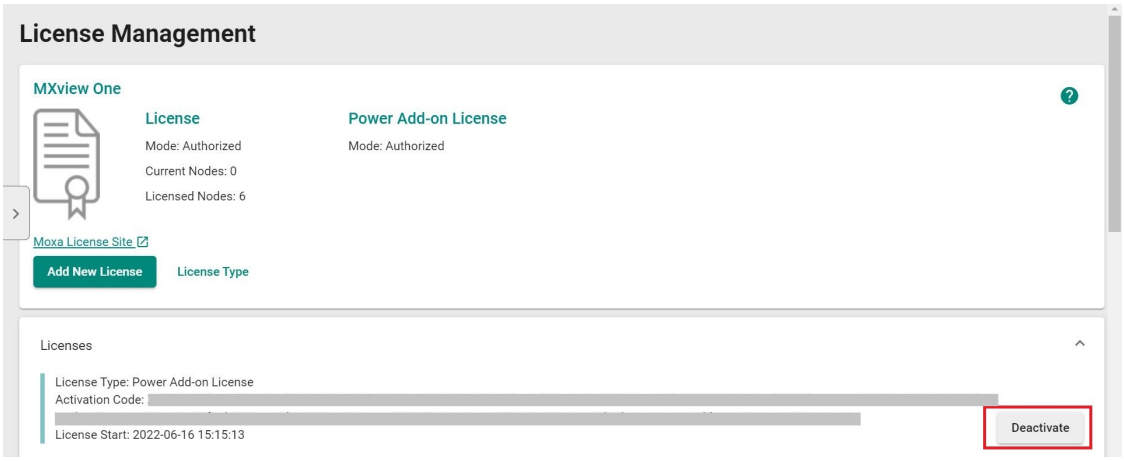


12. Click **Apply** and MXview One will activate the license.

Deactivating a License

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

1. Navigate to **Menu** ( ) **> Administration > License Management**.
   The **License Management** screen appears.
2. Expand the **Licenses** section.
   A list of activated licenses and activation codes appears.
3. Click **Deactivate** and MXview One will deactivate the license.



NOTE

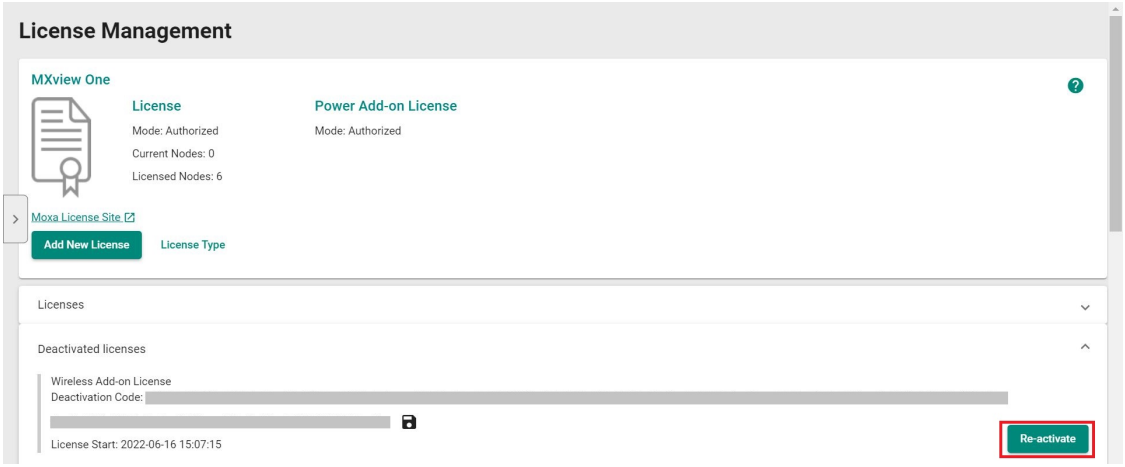
If you only have one Node-based License with one Add-on License, you will have to deactivate the Add-on License first, then deactivate the Node-based License next.

If you have more than one Node-based License, it is ok for you to deactivate the Node-based License or Add-on License without any order.

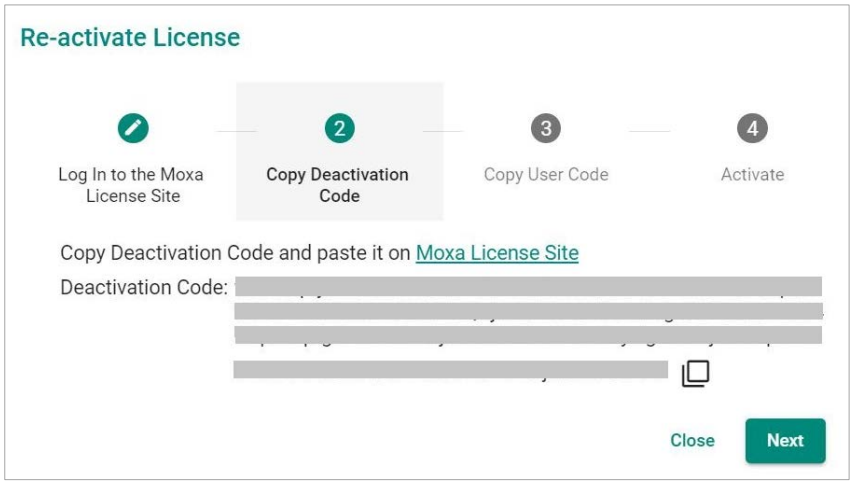
Reactivating a Deactivated License

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

1. Navigate to **Menu** ( ) **> Administration > License Management**.
   The **License Management** screen appears.
2. Expand the **Deactivated Licenses** section.
   A list of deactivated licenses and deactivation codes will appear.

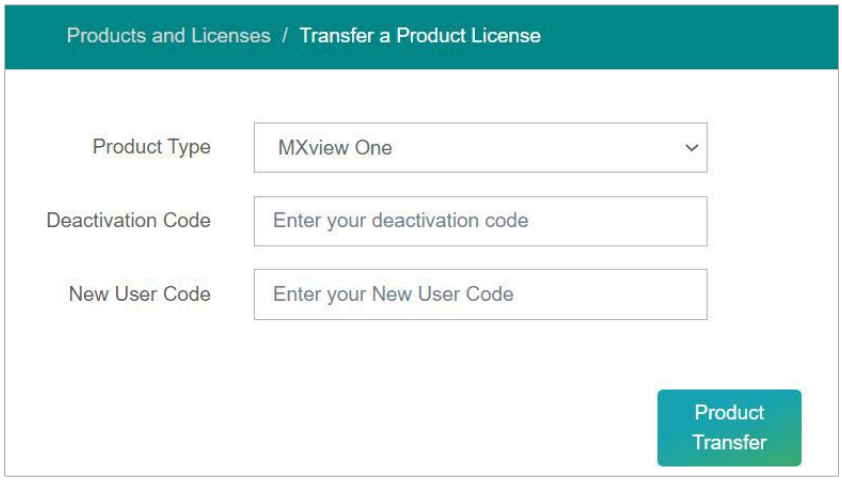


3. Click **Re-activate** and then click **Next**.
4. Copy the deactivation code and click **Next**.



5. Open a web browser and go to https://license.moxa.com. Select **MXview One** and log in using your Moxa account.
6. Select **Products and Licenses** and click **Transfer a Product License**. Then, select **MXview One** from the product type list.

7. Paste the **Deactivation Code** followed by the **New User Code** from MXview One. Then, click **Product Transfer**.

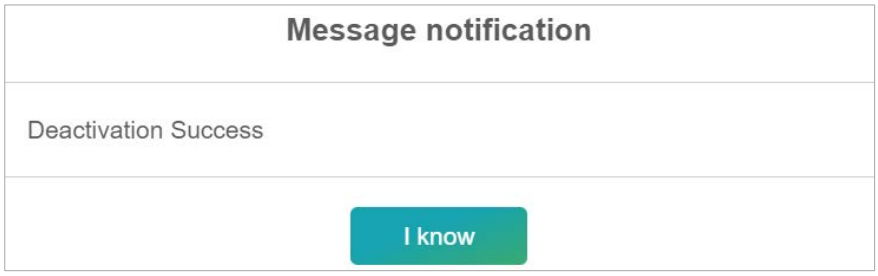


NOTE

'Reactivating a Deactivated License' and 'Transfer a Deactivated License to another MXview One instance' are using the same menu here.

If you are implementing 'Reactivating a Deactivated License' on the current instance of MXview One, please paste the current MXview One User code in the 'New User Code' section.

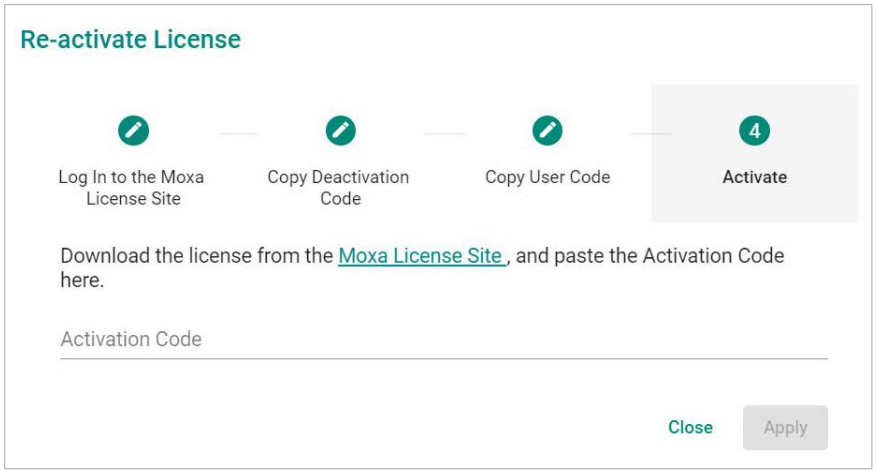
8. Once the process has been successfully completed, a pop-up window will appear to inform you that your license code has been deactivated. Click **I know** to close the window. If the license failed to deactivate, enter the license key again. If you are still experiencing problems, please contact Moxa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



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

10. Copy the activation code from the email.

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

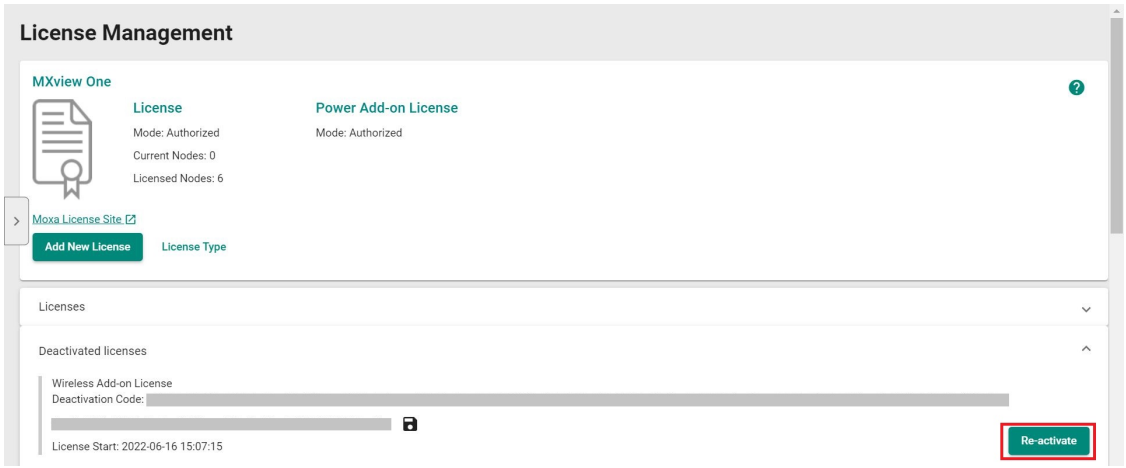


12. Click **Apply** and MXview One will reactivate the license.

Transferring a License to a Different Instance of MXview One

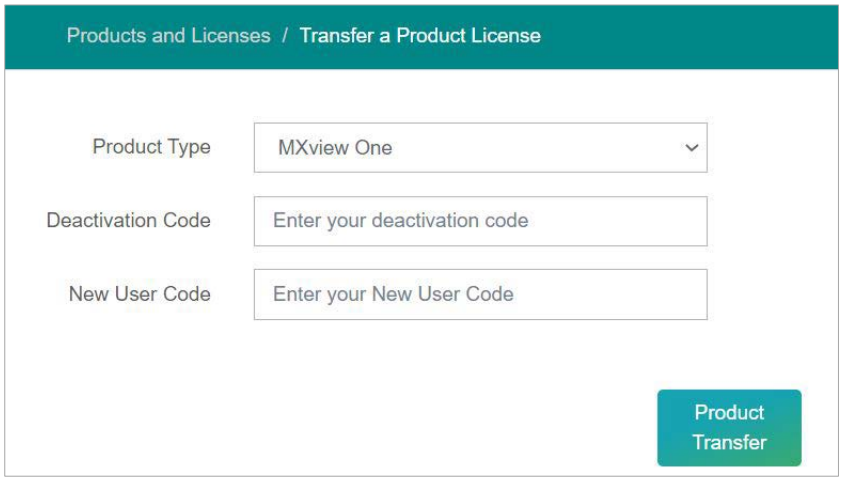
A deactivated license can be transferred to a new instance of MXview One.

1. Navigate to **Menu** ( ) **> Administration > License Management**.
   The **License Management** page will appear.
2. Expand the **Deactivated Licenses** section. A list of deactivated licenses and deactivation codes will appear. Copy the deactivation codes.



3. Open a web browser and go to https://license.moxa.com. Select **MXview One** and log in using your Moxa account.
4. Select **Products and Licenses** and click **Transfer a Product License**. Then, select **MXview One** from the product type list.

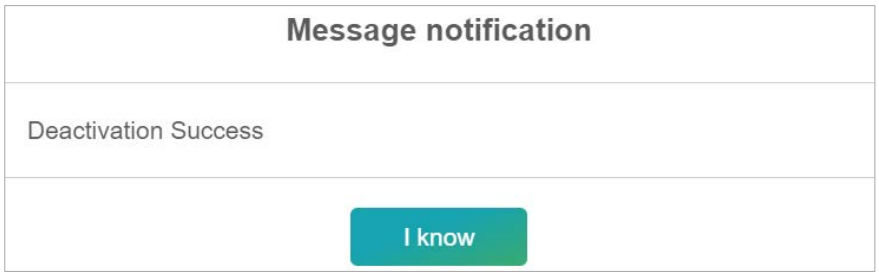
5. Paste the **Deactivation Code** and the **New User Code** from a new installation of MXview One. Then, click **Product Transfer**.



NOTE

To obtain a new User Code, please visit "**Adding a New License**", and follow steps 1 to 4 to obtain and copy the new User Code.

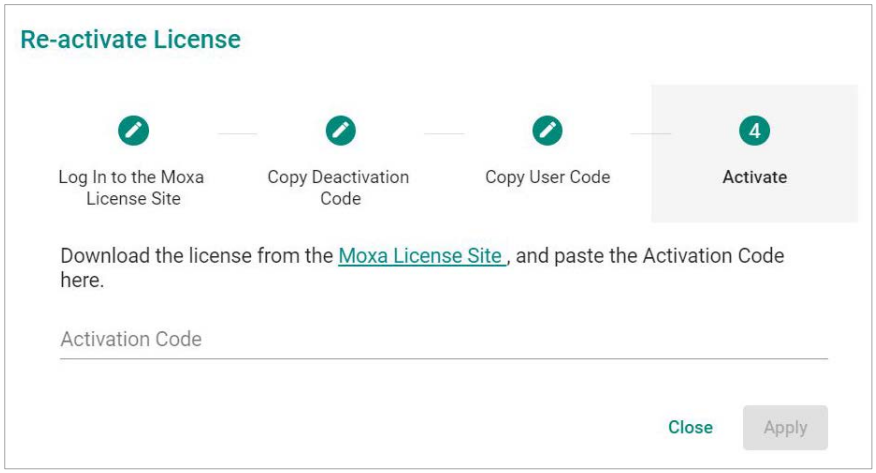
6. Once the process has been successfully completed, a pop-up window will appear to inform you that your license code has been deactivated. Click **I know** to close the window. If the license failed to deactivate, enter the license key again. If you are still experiencing problems, please contact Moxa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



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

8. Copy the activation code from the email.

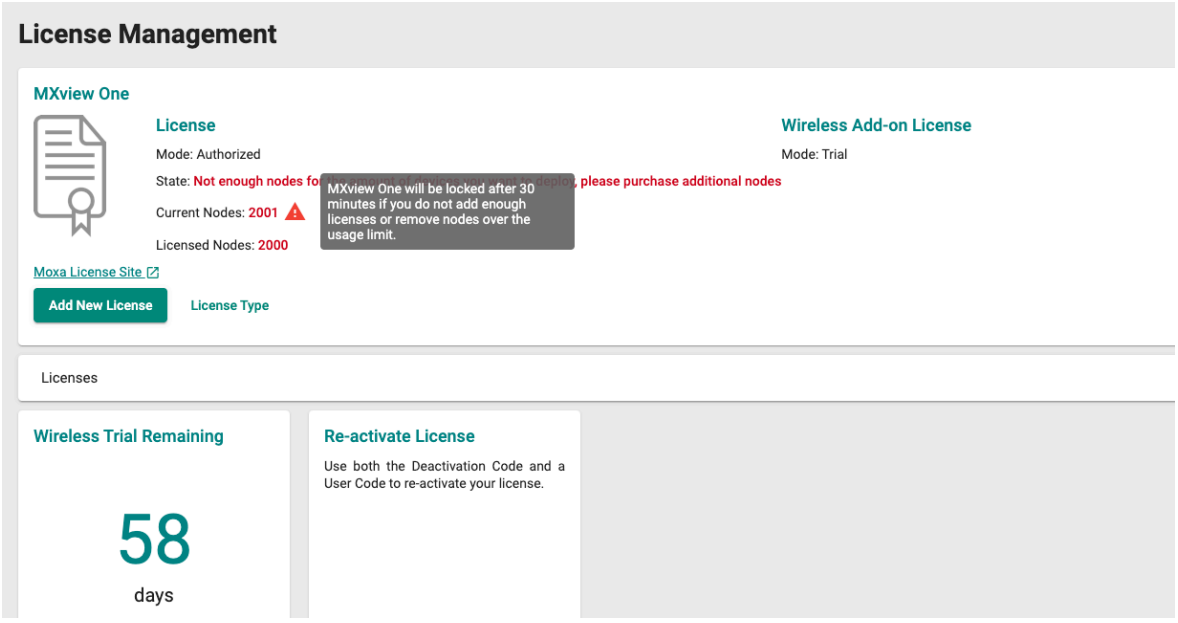
9. In MXview One, paste the activation code into the Activation Code field.



10. Click **Apply** and MXview One will reactivate the license.

Quantity of Monitored Devices Exceeds the Number of Node-based Licenses

When the quantity of monitored devices exceeds the activated number of license nodes, you can purchase additional Node-based Licenses and activate them as required. Or you can delete the extra devices that you don't have to monitor within 30 minutes.



1. **Buy Extra Node-based Licenses**

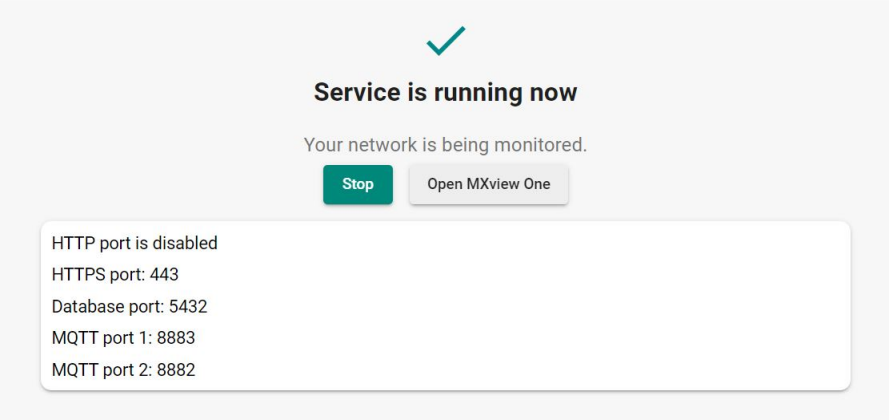
   Order the required quantity of Node-based Licenses from your channel or Moxa Sales Representative. Then, follow the instructions on **Adding a New License** to activate a new license.

2. **Delete Extra Devices**

   a. Within 30 minutes, you can delete the devices on the **Topology** page to meet the number of Node-based Licenses you available.

b. After 30 minutes, please follow the instructions below:

- ❒ Press the **Stop** button in the Control Panel.



- ❒ After 1 minute, Click **Start** and wait for the status to display 'Service is running now'. Then, click **Open MXview One** and Log in to MXview One.
- ❒ Navigate to **Menu** ( ) **> Topology**.

  The **Topology** screen will appear and displays the Topology Map by default.
- ❒ Click the devices you want to delete and then click **Delete**. From now on, MXview One will not count the delete devices.

5. Dashboard Widgets

The MXview One **Dashboard** contains several widgets that provide summary information about your network devices and event highlights.

Dashboard Overview

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

Use the **Dashboard** to gain a quick overview of your network devices, important system events.

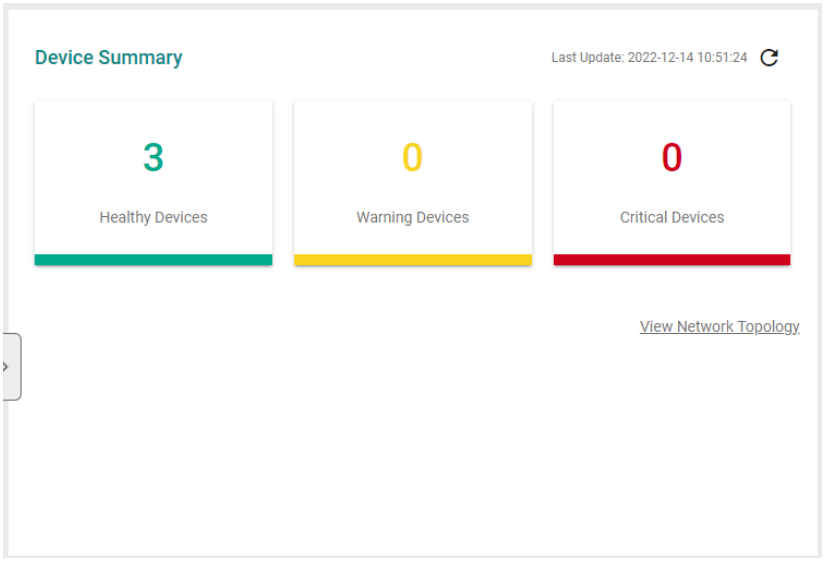
The **Dashboard** displays the following widgets:

- Device Summary
- Event Highlights: Cold/Warm Start Trap
- Event Highlights: ICMP Unreachable
- Event Highlights: Link Down

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

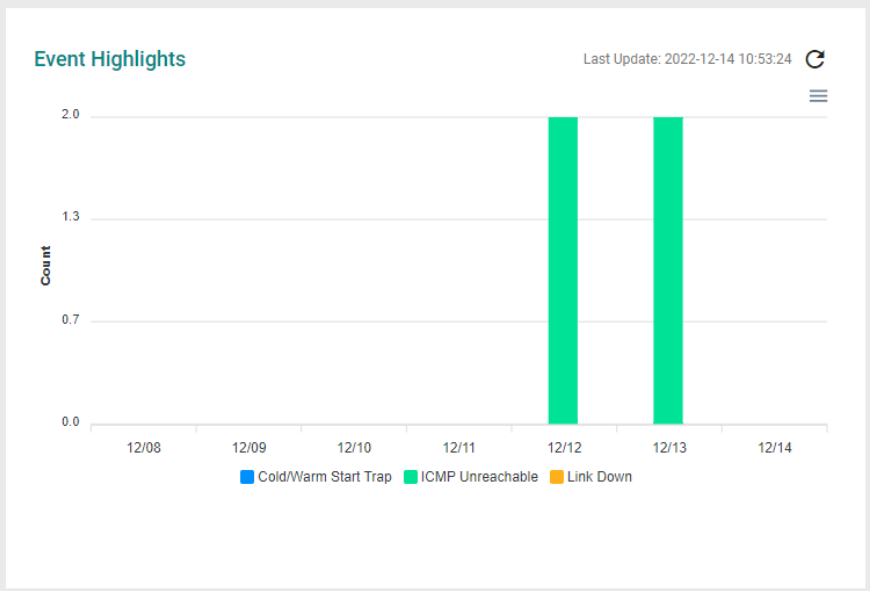
The **Device Summary** widget displays the following information about the devices on your network:



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

Event Highlights

The Event Highlights will display the following events during the past seven days: Cold/Warm Start Trap, ICMP Unreachable, and Link Down.



Event Highlights: The **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.

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

Event Highlights: The **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 event highlights 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 **Event History** screen, click a bar on the widget chart.
- To refresh the widget data, click the **Refresh** (↻) button following the **Last Update** timestamp.
- To download the Event Highlights data, click (≡) below the Refresh button.

6. Device Discovery and Polling

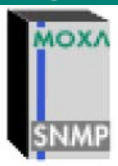
Device Discovery Overview

MXview One uses SNMP, ICMP, and MMS to discover devices within the scan ranges. When a Moxa device has been located, MXview One will generate an actual image of the device, demonstrated below, to indicate the device's location on the network.

MXview One 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

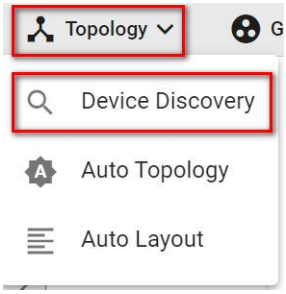
MXview One will display one of the following graphics to indicate devices:

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

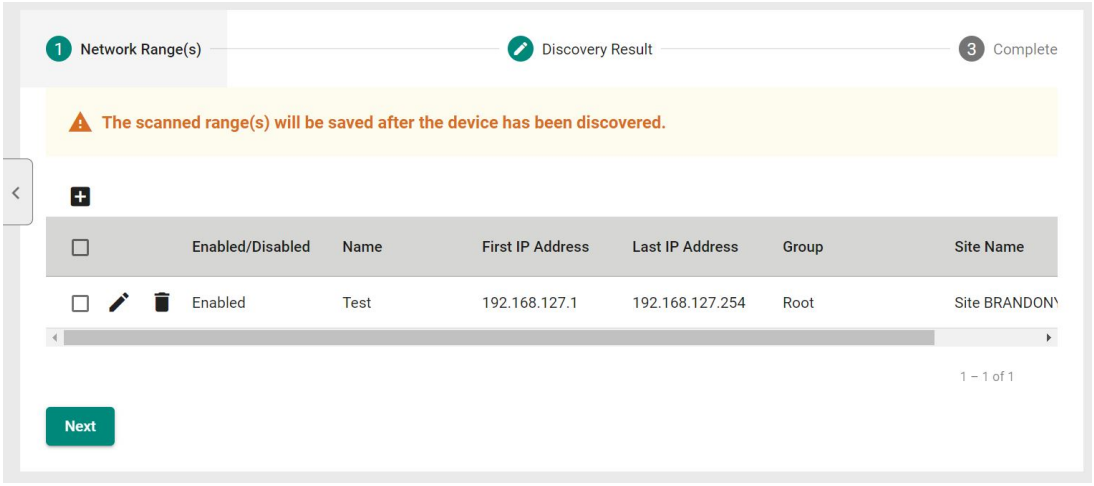
Configuring IP Address Scan Ranges

MXview One 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 **Device Discovery** to configure network scan ranges.

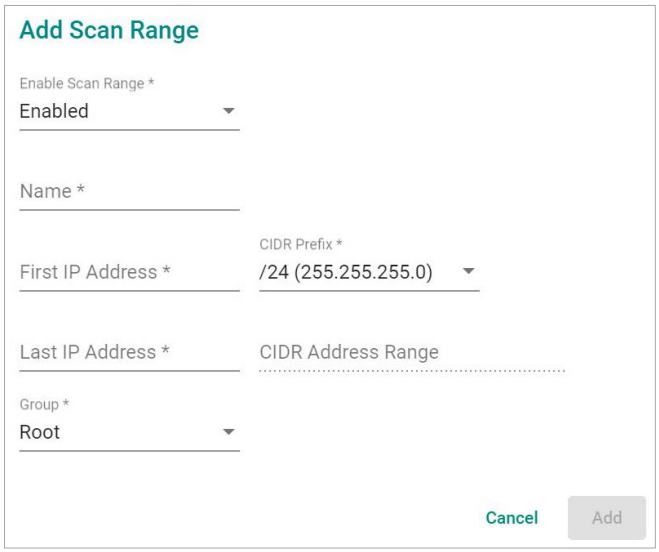
1. Access the **Device Discovery** screen by the following method:
   a. Navigate to **Menu** ( ) **> Device Discovery**.
   b. Navigate to **Menu** ( ) **> Topology**, and then navigate to **Topology > Device Discovery** from the Topology toolbar menu.



The **Device Discovery** screen will appear.



2. To add a new scan range:
   a. Click the **Add** ( ) button in the top left 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 applicable).

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

h. Click **Add**.

   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.

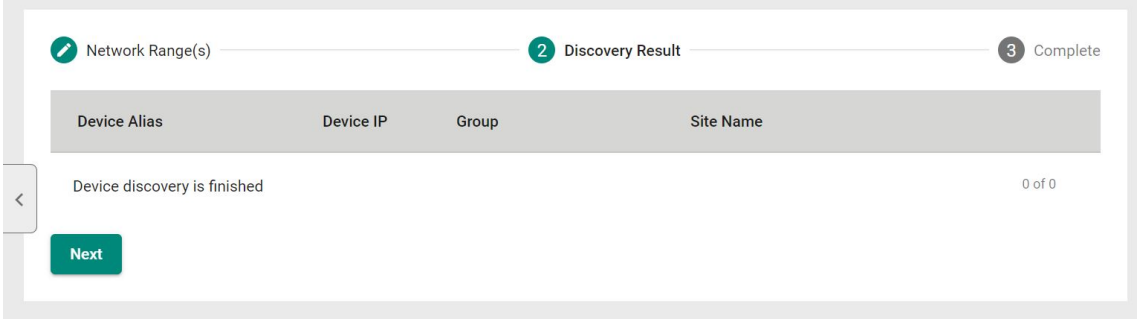
      The **Edit Scan Range** screen appears.

   c. Modify the scan range settings.

   d. Click **Apply**.

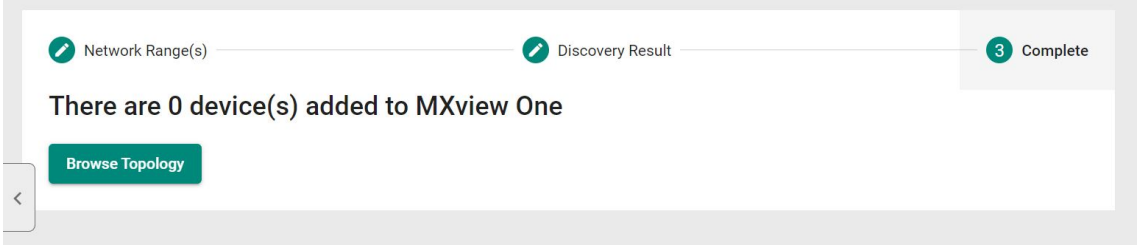
      The **Device Discovery** screen displays the **Network Range** table with the updated scan range information.

4. Click **Next** to discover the devices within the specific IP address ranges.



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

   The **Complete** tab and the number of devices added to MXview One.



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

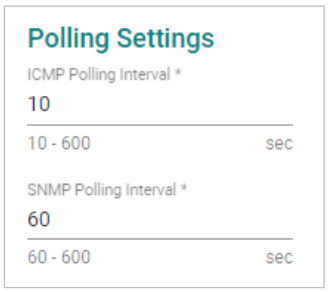
   The **Topology** screen will appear and display the updated Topology Map.

Configuring Device Polling Settings

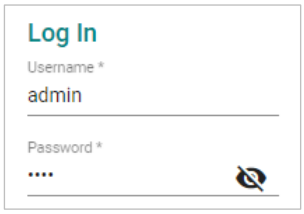
Devices in the assigned scan range can be discovered via SNMP and ICMP protocols. (The default polling interval of ICMP is 10 seconds, while SNMP is 60 seconds. Users can go to the **Device Settings Template** page to change the polling intervals.) After a device is discovered, MXview One will use SNMP and ICMP to poll the device periodically. To configure this function properly, you will need to know the following information:

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

1. Navigate to **Menu** ( ) **> Administration > Device Settings Template**.
   The **Device Settings Template** screen appears.
2. Scroll down to the **Polling Settings** section.



3. Configure the following ICMP polling settings:
   ICMP polling interval: Specify the time in seconds between polls. MXview One will use ICMP protocol to check if the device is alive.
4. Configure the following SNMP polling settings:
   SNMP polling interval: Specify the time in seconds between polls.
5. Scroll down to the **Log In** section to 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

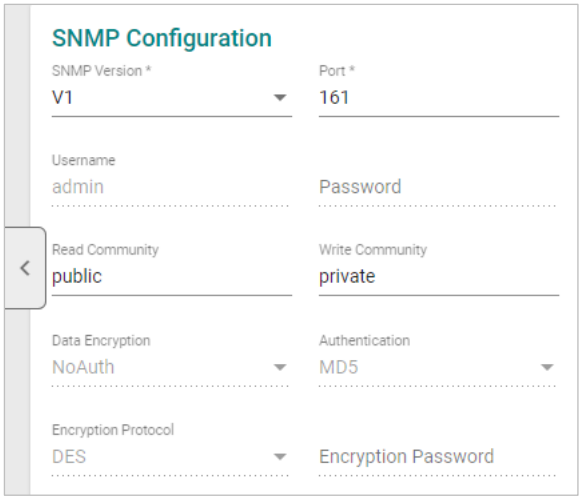


6. Click **Save**.
   MXview One will update the modified settings.

Changing Default SNMP Configuration

The default SNMP read community string that is used to discover devices is public. Use the Device Settings Template screen to change the default read community string or modify other default SNMP configuration.

1. Navigate to **Menu** ( ) **> Administration > Device Settings Template**.
   The **Device Settings Template** screen will appear.
2. Scroll down to the **SNMP Configuration** section.



3. Configure the following:
   a. **SNMP Version:** Select the SNMP protocol version
   b. **SNMP Port:** Specify the SNMP port
   c. **Username:** Specify the SNMP server username
   d. **Password:** Specify the SNMP server password
   e. **Read Community:** Specify the new community string
   f. **Write Community:** Specify the new community string
   g. **Data Encryption:** Select the data encryption method
      - ❒ NoAuth
      - ❒ AuthNoPriv
      - ❒ AuthPriv
   h. **Authentication:** Select the authentication method
      - ❒ MD5
      - ❒ SHA
      - ❒ SHA256
      - ❒ SHA512
   i. **Encryption Protocol:** Select the encryption protocol and input the Encryption Password.
      - ❒ DES
      - ❒ AES
4. Click **Save**.
   MXview One updates the modified settings.

7. Topology Management

MXview One 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.

Topology Overview

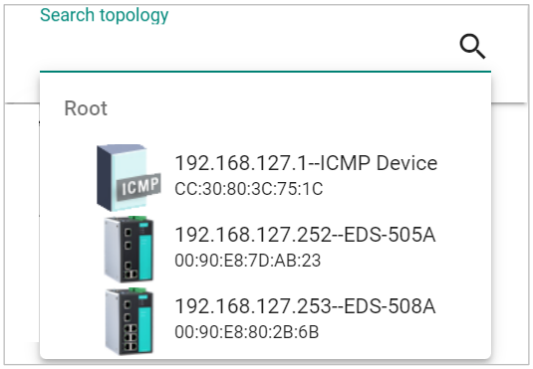
The Topology screen allows you to view the Topology Map, which is a graphical representation of the devices in your network, and perform most actions in MXview One. For example, you can use the Network Topology screen to do the following:

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

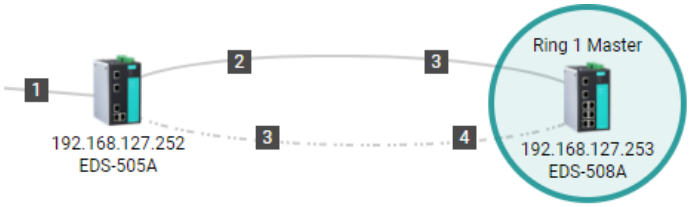
Viewing Topology Map

Use the Topology screen to view the Topology Map of your network.

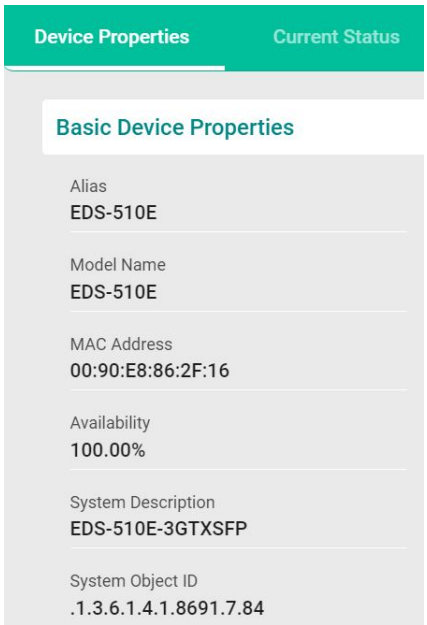
1. Navigate to **Menu** ( ) **> Topology**.
   The **Topology** screen will appear and displays the Topology Map by default.
2. If the **List view** is displayed, click the **Topology view** ( ) icon in the top right corner.
   The Topology screen will display a graphical representation of the devices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



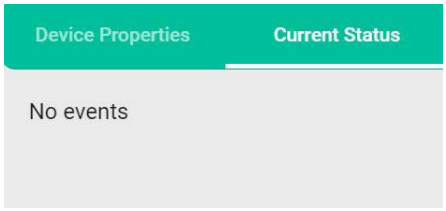
   b. Search the device in the drop-down directory tree or type a string in the search box. Click the specific device and MXview One will bring you to the device on the Topology Map.
4. To view the details of a specific device, select the device in the Topology Map.



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

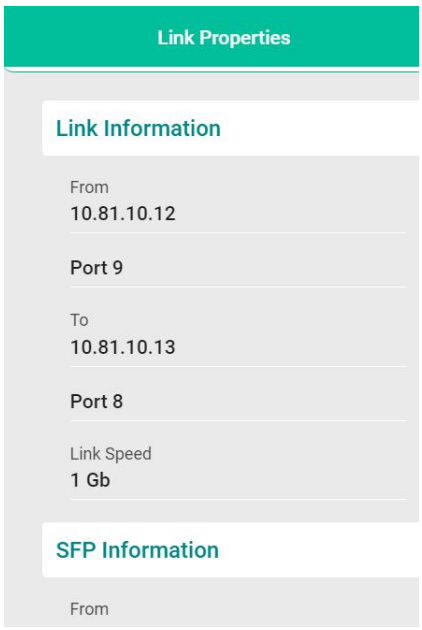


5. To view events associated with the device, click the **Current Status**.
   The **Current Status** pane displays events associated with the device.



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.



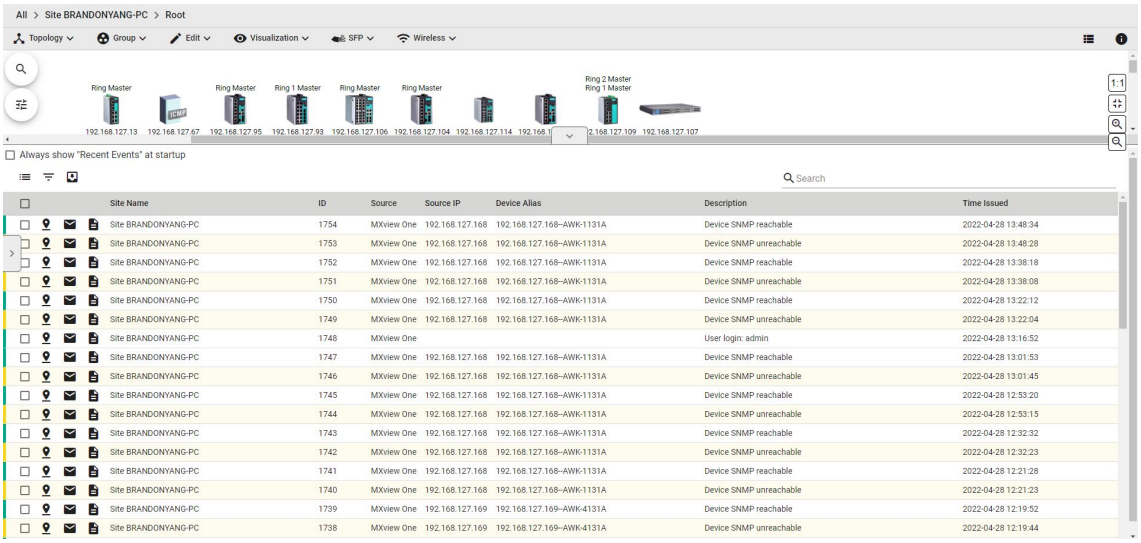
Viewing Recent Events

Use the **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** ( ) **> Topology**.

   The **Topology** screen will appear and displays the **Recent Events** panel on the bottom.



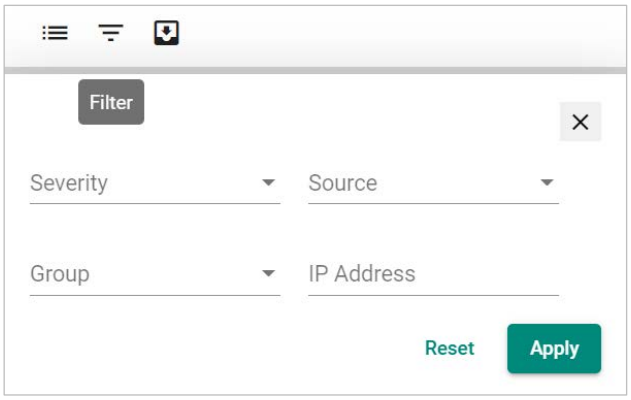
2. To filter the information in the table, type a full or partial string that matches the value in any of the table columns on the right of the search space.

   MXview One 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
        - Any
        - Information
        - Warning
        - Critical
        - System Information

- **Source:** Select the source that detected the event
  - Any
  - MXview One
  - Trap
  - Security Sensing
- **Group:** Select the device group
- **IP Address:** Select the device IP address

c. Click **Apply**.

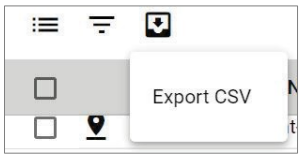
MXview One filters the table to only display events that match the specified criteria.

4. To acknowledge the events in the table:
   a. Click the Acknowledge ( ) icon before the specific event, then the event will be confirmed.
   b. If you want to acknowledge more events, click the checkbox before the events or click the checkbox on the tool bar to select all the events. Then, click the Acknowledge icon.
5. To sort the data in the table by a specific column, click the column heading.

   MXview One sorts the table by the column.

6. To export data displayed in the **Recent Events** tab:

   a. Click the **Export** ( ) icon.

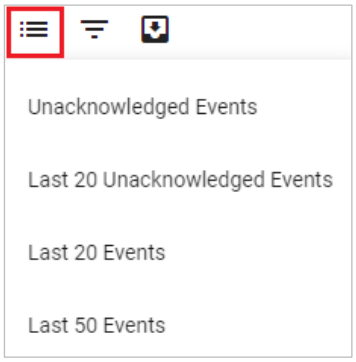


   b. Select **Export CSV**.
   c. Specify the location to save the exported file.
   d. Click **Save**.

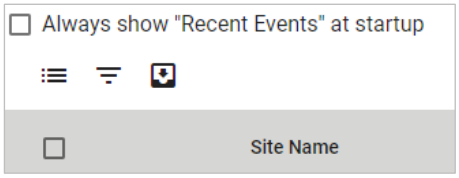
   MXview One exports the displayed event data as a CSV file.

7. To quickly filter event, click the **Quick filter event** ( ) icon to find the events.

   The events include the following:
   - Unacknowledged Events
   - Last 20 Unacknowledged Events
   - Last 20 Events
   - Last 50 Events.



8. MXview One allows users to display the Recent Events panel all the time by clicking the **Always show "Recent Events" at the startup** checkbox.



Organizing the Topology Structure By Group Function

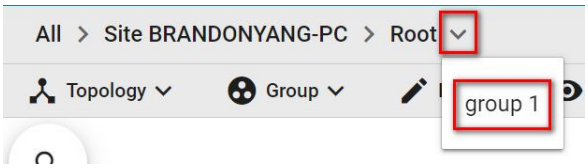
The Topology Map can be organized into a multi-layer tree structure of up to 5 layers. Organizing the topology structure into groups helps manage a large number of nodes on the computer screen. For example, users can move nodes of the same subnet or location into the same group. Root, which is the only 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** ( ) **> Topology**.

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

   - MXview One represents the Topology Map structure by a path at the top of the **Topology** screen:

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

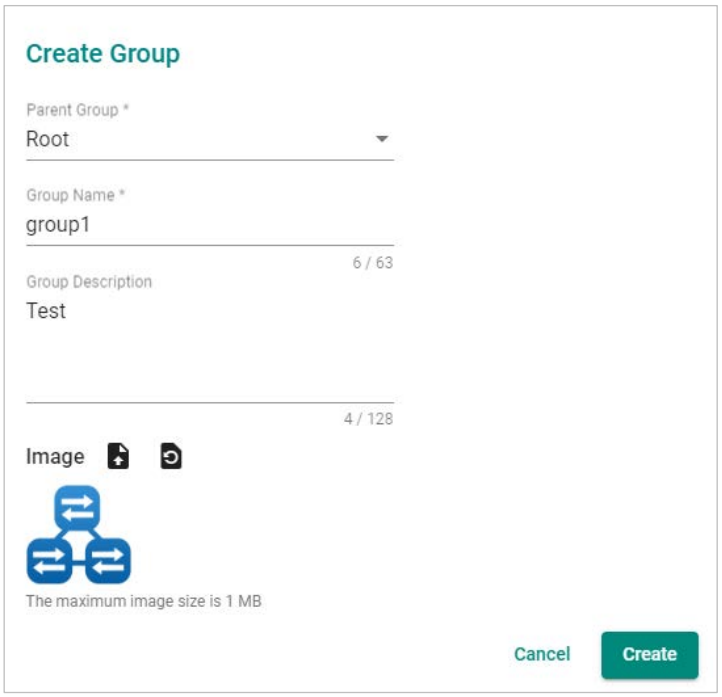


   - You can also click the following icon used to indicate user-defined groups within the Topology Map:

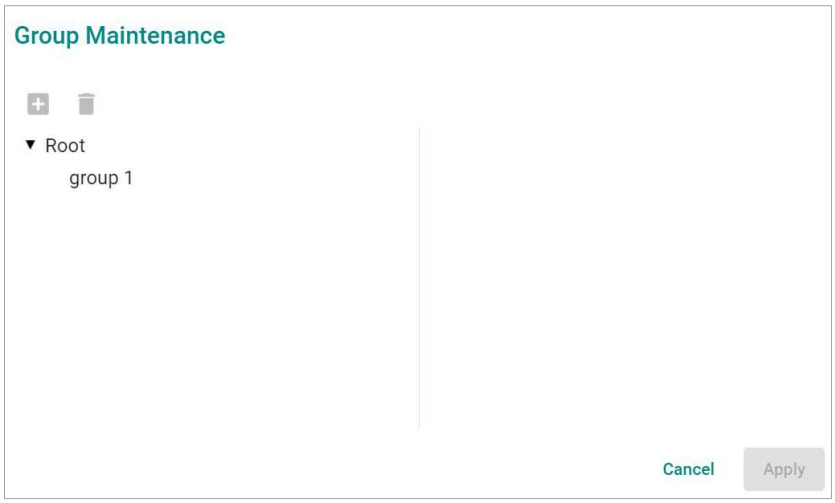
2. If **List view** is displayed, click the **Topology view** ( ) icon in the top right corner.

   The **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.

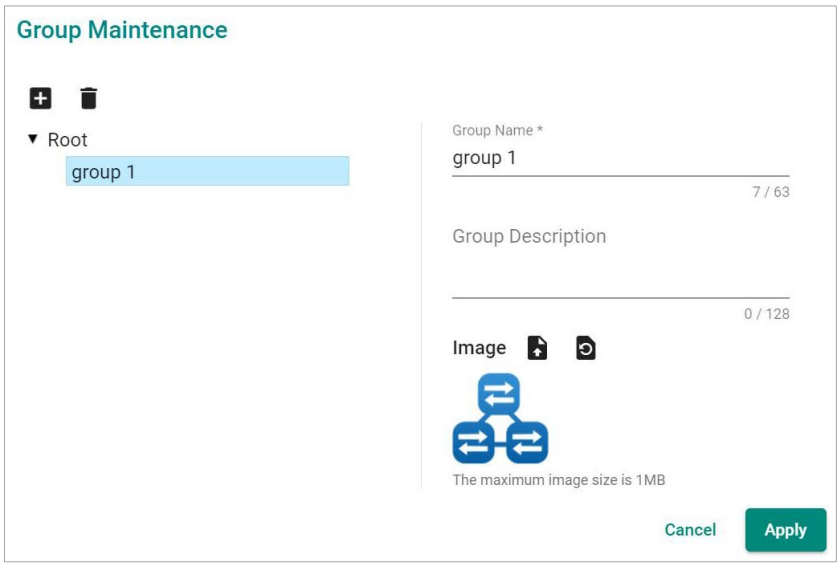


   b. Configure the following:
      - ❒ Parent Group
      - ❒ Group Name
      - ❒ Group Description
      - ❒ Group Icon
   c. Click **Create**.
      MXview One will add the group below to the specified parent group.
4. To reorganize the groups within the Topology Map structure:
   a. Navigate to **Group > 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. (Optional) Edit the group details or perform one of the following points:

i. (Optional) Click **Add** to add a new group below the selected layer.

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

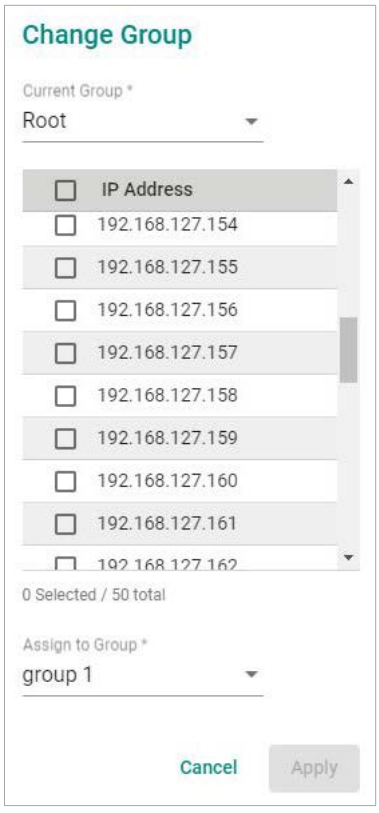
d. Click **Apply**.

5. To reassign the device(s) in a group:

a. There are two ways to reassign the device(s) in a group:

i. Navigate to Group > **Change Group**. The Change Group screen appears.

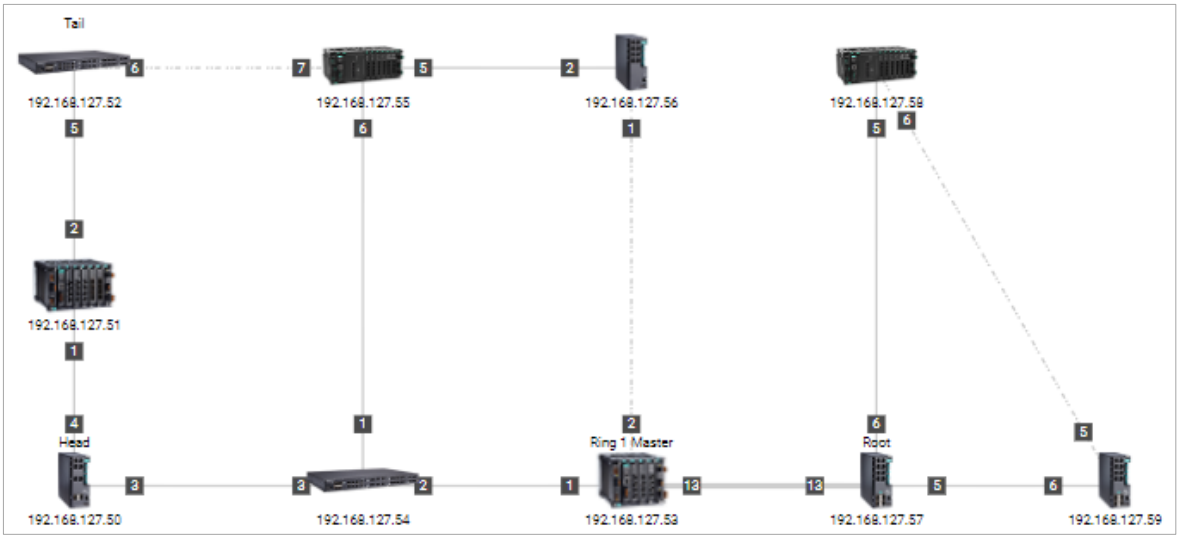
ii. Select the device(s) you want to reassign on the topology and click the Change Group icon on the toolbar.



b. If the **IP Address** list does not display the IP address(es) of the device(s) you want to reassign, select 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 One 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**
- Dual Homing

> **NOTE**
>
> Only the **Auto Topology** function can draw dashed lines for redundancy links. Redundant links that are added manually will appear as solid lines.

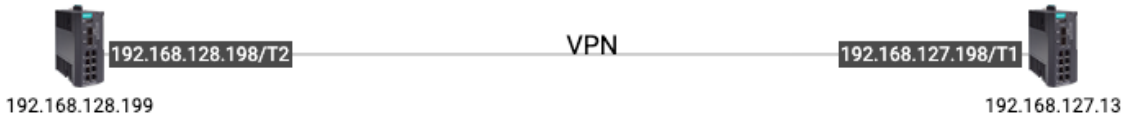
PoE Power Consumption Visualization

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

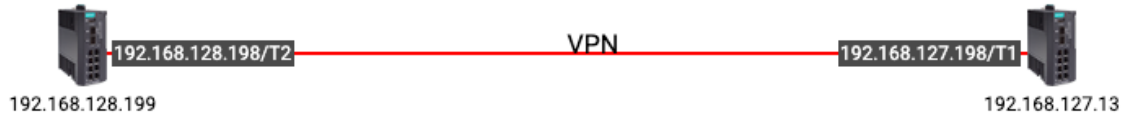
VPN Tunnel Visualization

The VPN tunnel link will display 'VPN' on the link.

1. The VPN tunnel is connected.



2. The VPN tunnel is disconnected.



NOTE

VPN Tunnel Visualization is only available on Moxa's EDR-810 and EDR-G9010 series of secure routers.

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. Trunking links that are added manually will appear as solid lines.

NOTE

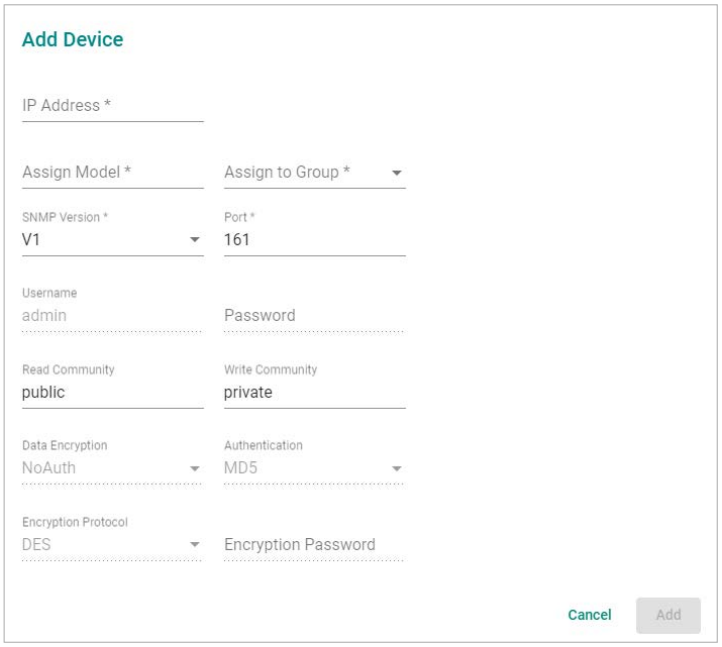
For trunked link, check **Device Properties** to get the port number corresponding to the trunking information.

Adding Devices and Links

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

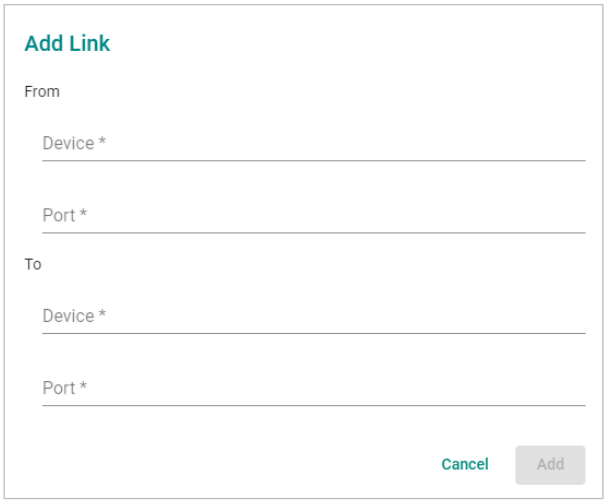
For information about List View, see Chapter 10: **Device Management** > **Viewing the Device List**.

1. Navigate to **Menu** ( ) **> Topology**.
   The **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
      - ❒ **Port:** Specify the port number
      - ❒ **Username:** Specify the device login Username
      - ❒ **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 Protocol:** Select the encryption protocol and input the **Encryption Password**
   c. Click **Add**.
      MXview One adds the device to the topology.

3. To add a link to the Topology Map:
   a. Navigate to **Edit > Add Link**.
      The **Add Link** screen will appear.



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

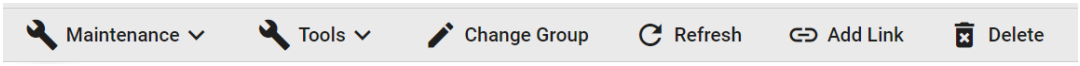
> **NOTE**
>
> Port numbers must be numeric and entered correctly to obtain the correct traffic information.

> **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.

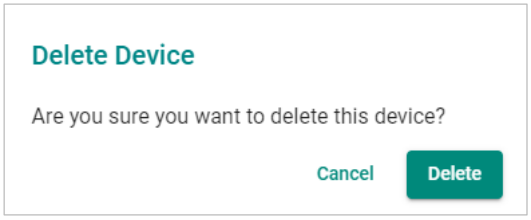
Deleting Devices and Links

You can delete devices and links from the Topology Map. After a device is deleted, it will be removed from the topology map, and 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.

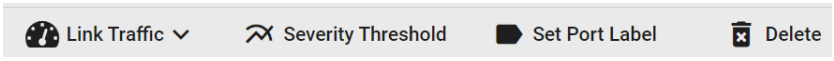
1. Navigate to **Menu** ( ) **> Topology**.
   The **Topology** screen will appear and display the Topology Map by default.
2. To delete a device from the Topology Map:
   a. Select the device.
      The following toolbar menu will appear.



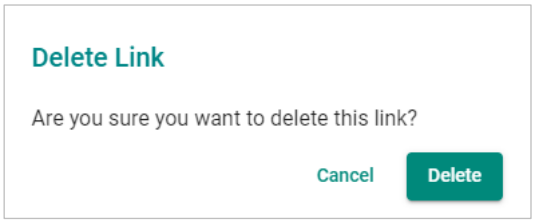
   b. Click **Delete**.
      A confirmation screen will appear.



   c. Click **Delete**.
      MXview One 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 **Delete**.
      MXview One deletes the link from the Topology Map.

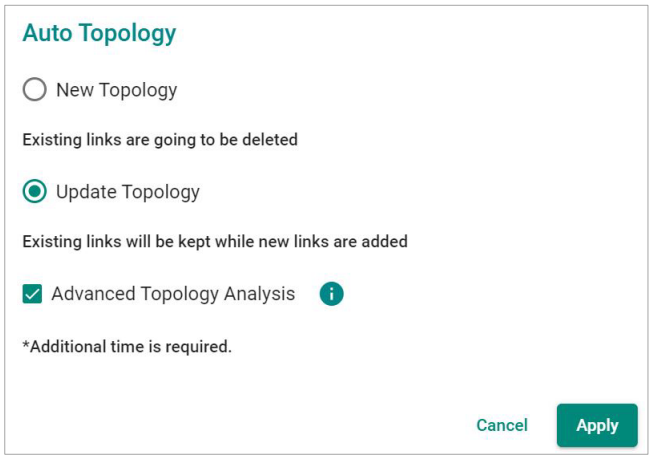
Updating the Topology Map

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 One can draw the physical topology map, down to the port level of the devices. For devices without an LLDP MIB, MXview One 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** ( ) **> Topology**.
   The **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 **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.



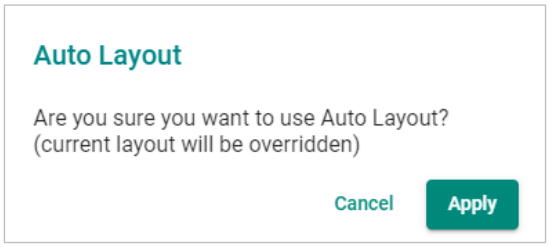
4. Select **Update Topology**.
5. (Optional) Select **Advanced Topology Analysis** to draw links for devices without an LLDP MIB.
6. Click **Apply**.
   MXview One will update the Topology Map.

> **NOTE**
>
> MXview One cannot guarantee that it can draw the link of the topology for non LLDP devices. However, you can draw the link of the topology manually by clicking **Add Link**.

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** ( ) **> Topology**.
   The **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 **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 **Apply**.
   MXview One 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.

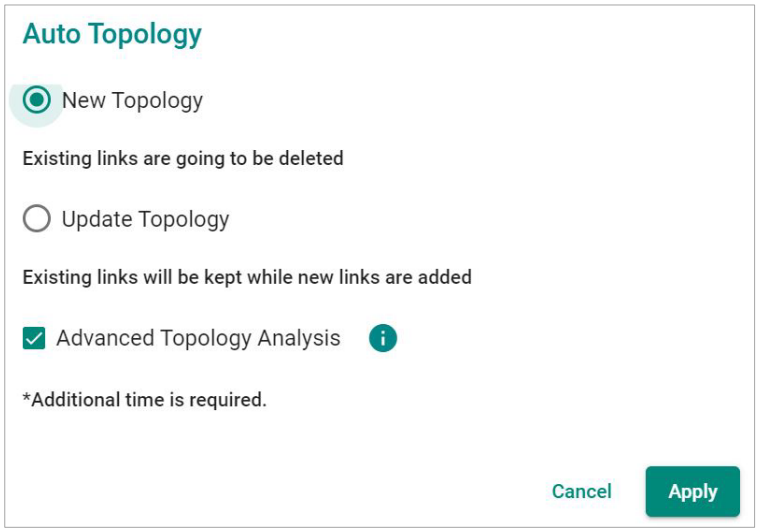
For devices with LLDP functionality, MXview One can draw the physical topology map, down to the port level of the devices. For devices without an LLDP MIB, MXview One is able to draw links by using ARP. To activate this function, select the **Advanced Topology Analysis** checkbox from the **Auto Topology**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



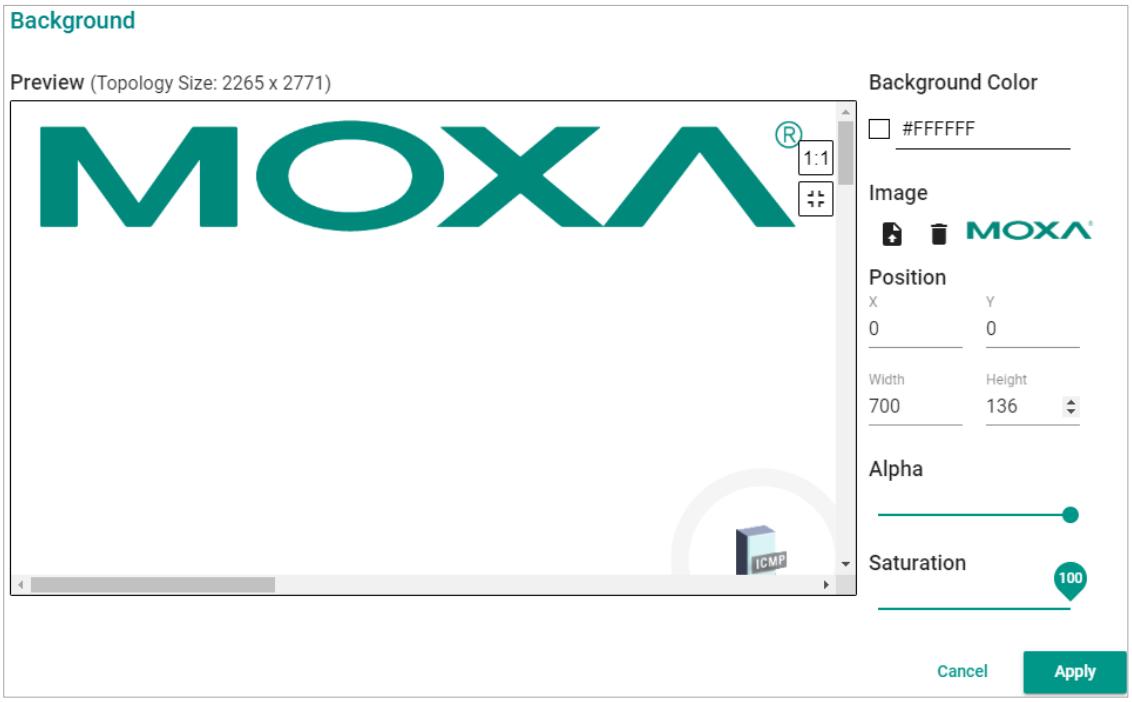
4. Select **New Topology**.
5. (Optional) Select **Advanced Topology Analysis** to draw links for devices without an LLDP MIB.
6. Click **Apply**.
   MXview One will create a new Topology Map.

> **NOTE**
>
> MXview One cannot guarantee that it can draw the link of the topology for non LLDP devices. However, you can draw the link of the topology manually by clicking **Add Link**.

Setting/Editing the Background Image

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

1. Navigate to **Menu** ( ) **> Topology**.
   The **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 **Topology** screen will display a graphical representation of the devices and links on your network.
3. Navigate to **Edit > Background**.
   The **Background** screen appears.



4. Upload the background image by using one of the following methods:
   - The image size must be less than 20 MB.
   - Click **Set Background** ( ) icon to upload the image file.

   MXview One will set the uploaded image as the Topology Map background.
5. Use the sliders to modify the **Alpha** and **Saturation** value of a background image.

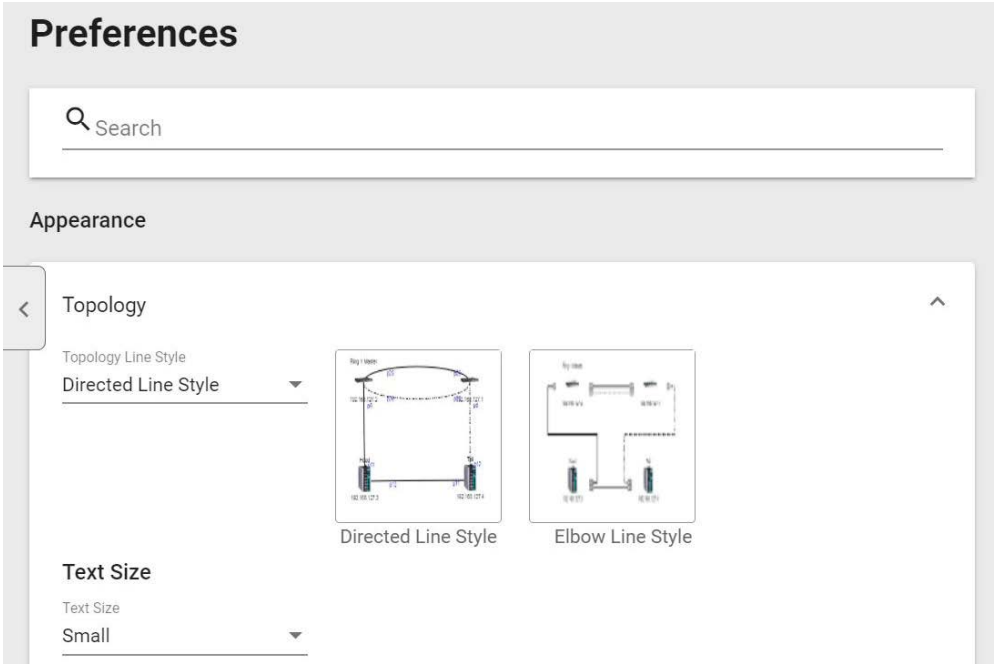
6. Under the **Position** section, modify the value of X and Y to move the origin of the image to a suitable location. Modify the 'Width' and 'Height' to change the size of the image.

7. To delete a background image, click ( ) to remove the background image from the Topology Map.

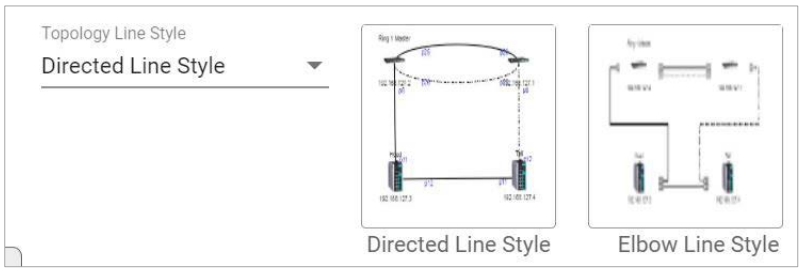
Editing the Topology Appearance

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

1. Navigate to **Menu** ( ) **> Administration > Preferences.**.
   The **Preferences** screen appears.
2. In the **Appearance** section, expand **Topology**.
   The **Topology** settings appear.

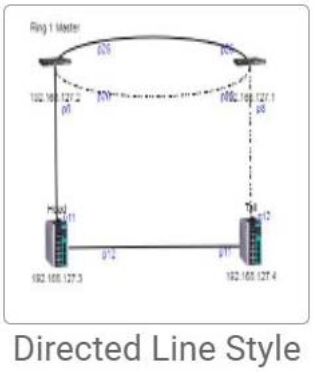


3. To modify the Topology Line Style, select one of the following from the drop-down list:



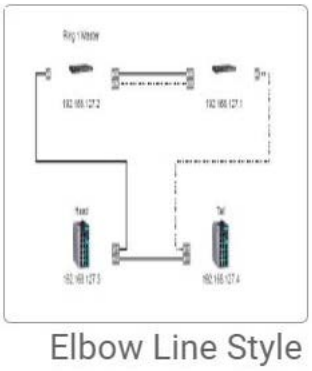
- **Directed Line Style**

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



- **Elbow Line Style**

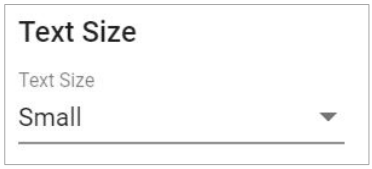
  MXview One applies the following style to the lines indicating the links between devices in the Topology Map:



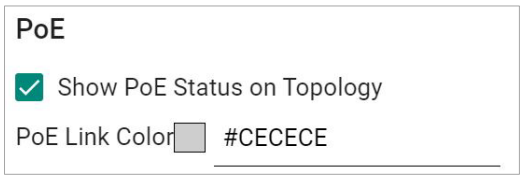
4. To modify the text size in MXview One:

   Select one of the following from the drop-down list:

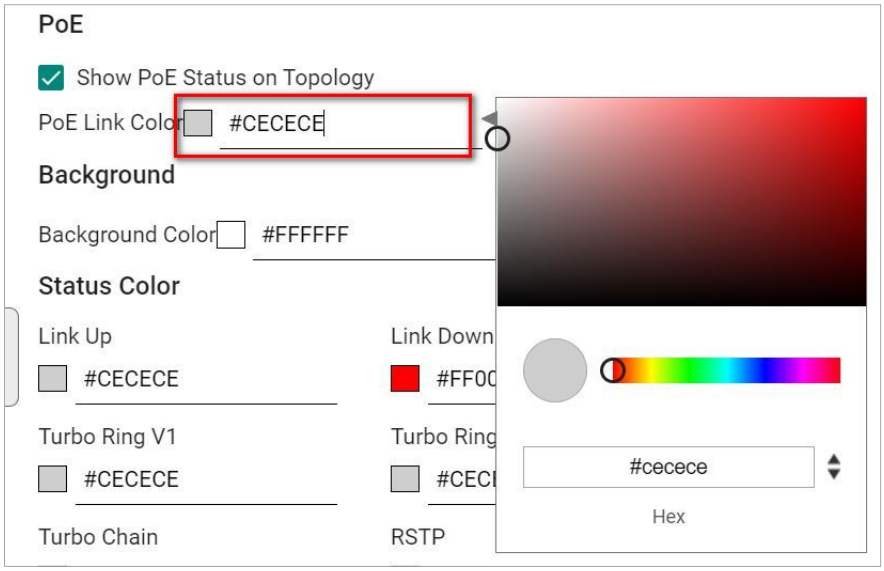
   - Large
   - Medium
   - Small



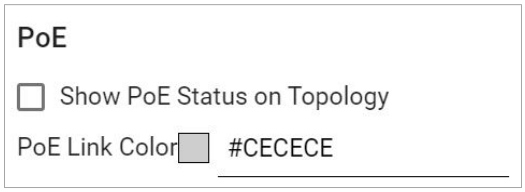
5. To modify how MXview One displays Power-over-Ethernet (PoE) links:
   a. Select the **Show PoE Status on Topology** check box to indicate the PoE link status on the Topology Map.



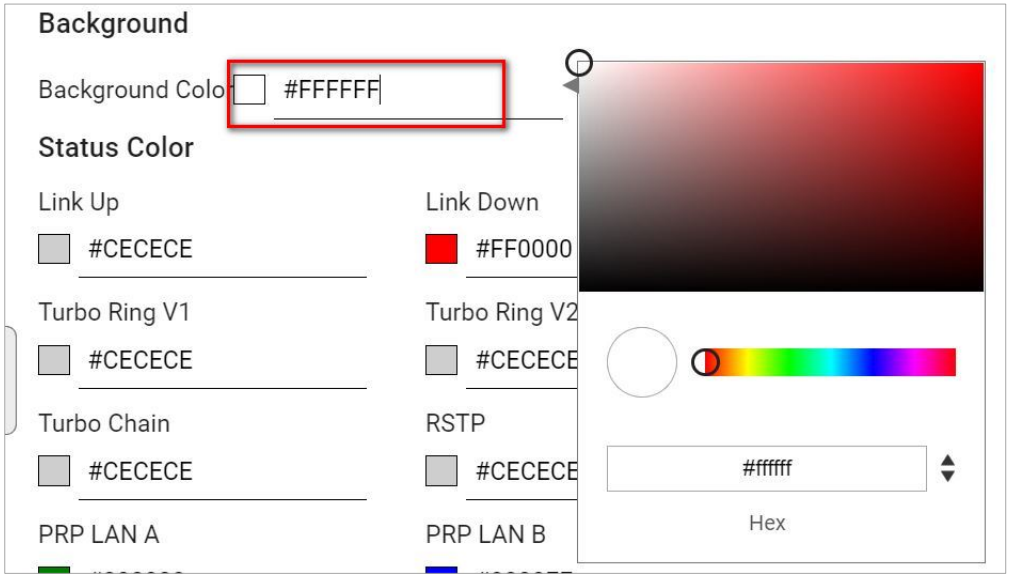
   b. Click the **PoE Link Color** field and specify a new color.



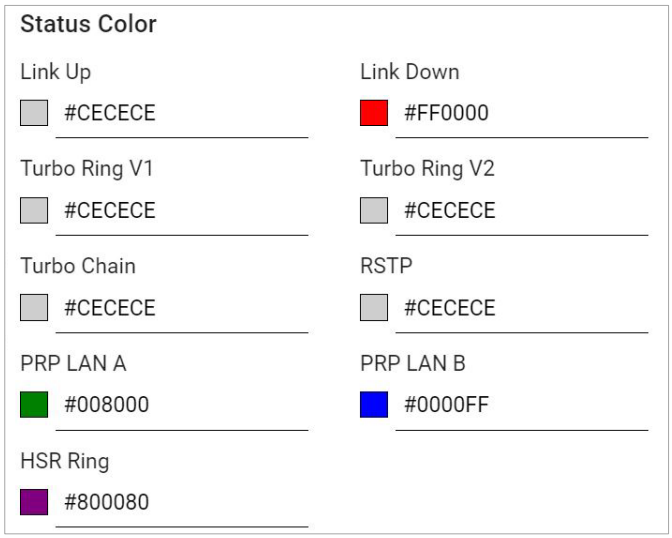
   c. (Optional) Clear the **Show PoE Status on Topology** check box to hide the PoE link status on the Topology Map.



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



7. 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



NOTE

The three status colors (**PRP LAN A, PRP LAN B, HSR Ring**) will appear when you activate the MXview Power license.

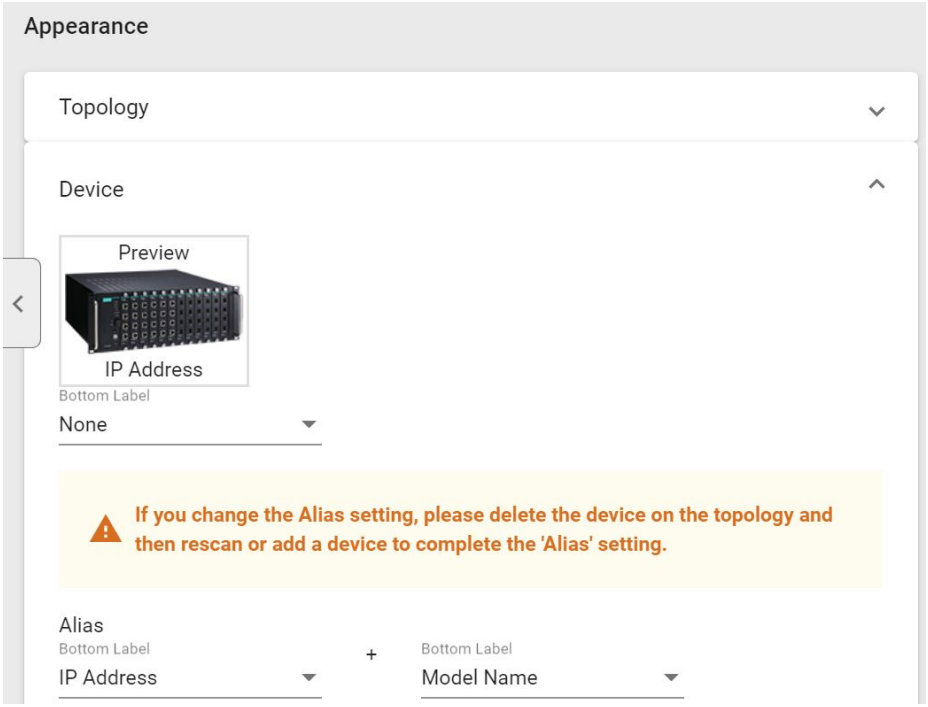
8. Click **Save**.

   MXview One will update the modified settings.

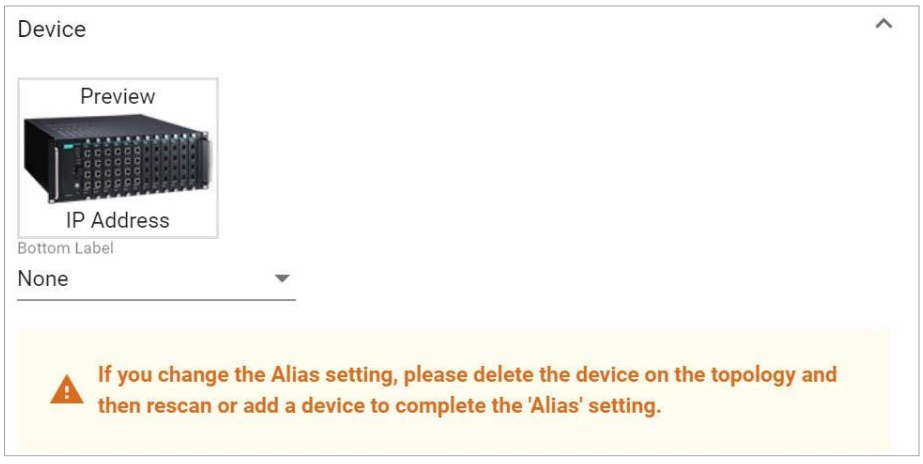
Editing the Device Appearance

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

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



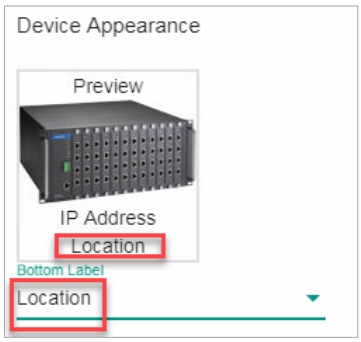
3. To modify the label that indicates the device in the Topology Map:
   a. Locate the **Bottom Label** drop-down list located below the Preview image:



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

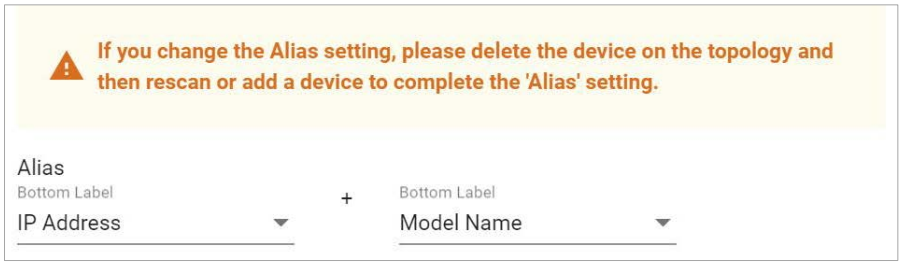
- ❒ Location
- ❒ Alias
- ❒ Model Name
- ❒ MAC

MXview One 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

NOTE

If you change the Alias setting, please delete the device on the topology and then rescan or add a device to complete the 'Alias' setting.

5. Click **Save**.

MXview One updates the modified settings.

Exporting the Topology Map

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

1. Navigate to **Menu** ( ) **> Topology**.
   The **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 **Topology** screen will display a graphical representation of the devices and links on your network.
3. Navigate to **Edit > Export Topology**.
   MXview One exports the PNG image of the Topology Map.

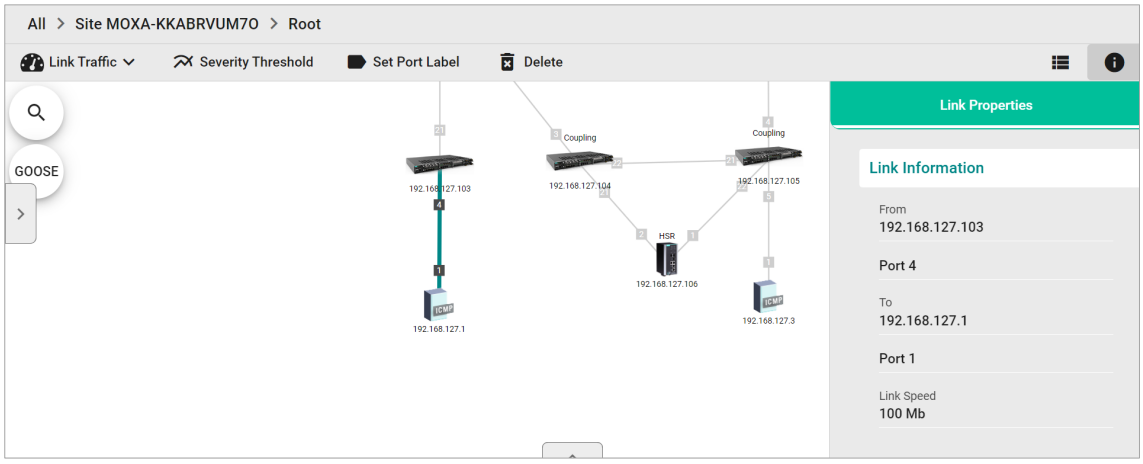
8. Network and Traffic Monitoring

MXview One 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, as well as wireless access points and clients.

Viewing Link Properties

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

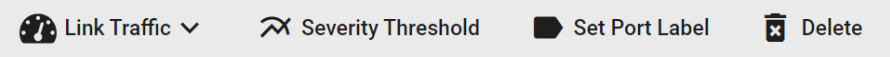
1. Navigate to **Menu** (☰) **> Topology**.
   The **Topology** screen will appear and display the Topology Map by default.
2. Click on a link between devices in the Topology Map.
   The **Link Properties** pane appears to the right of the Topology Map.



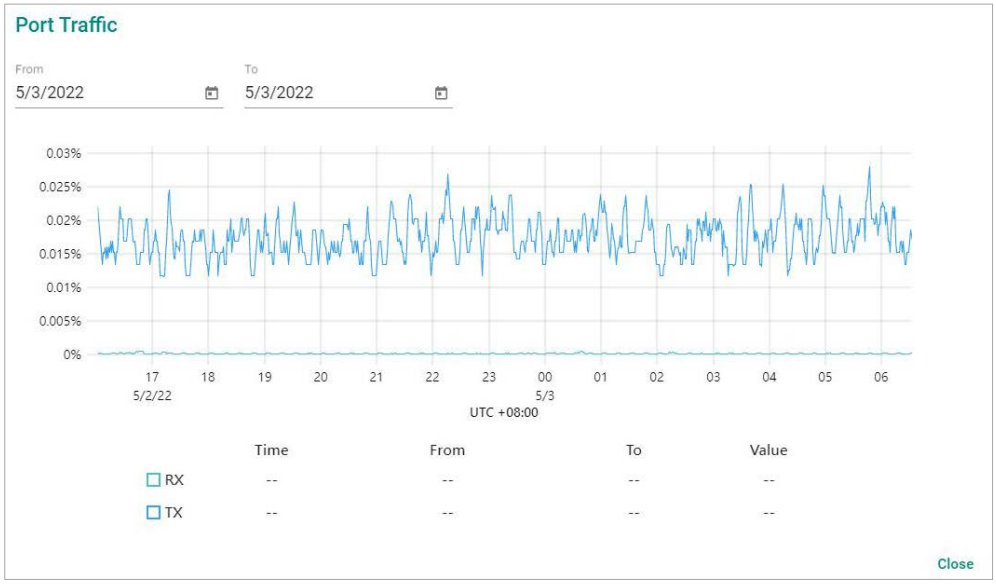
Viewing Port Traffic

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 and the maximum interval you can select is 90 days.

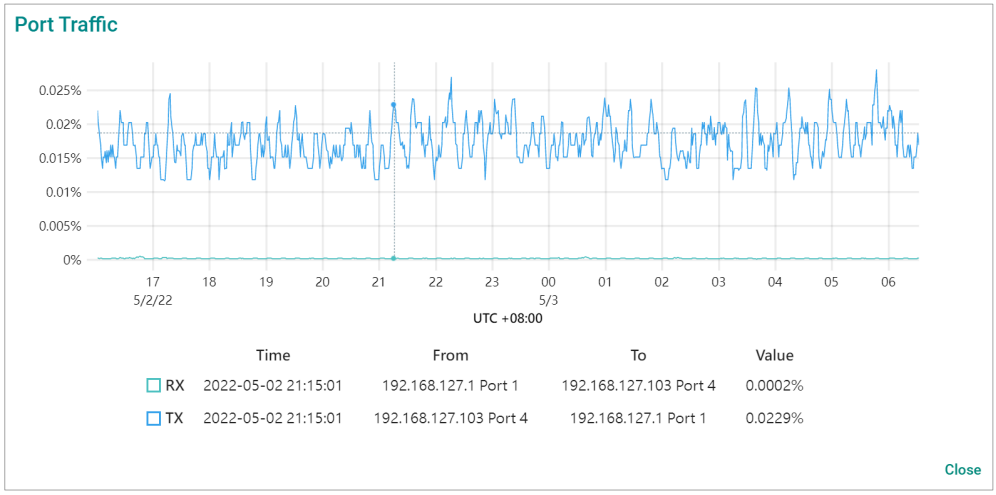
1. Navigate to **Menu** ( ) **> Topology**.
   The **Topology** screen appears and displays the Topology Map by default.
2. Click on a link between devices in the Topology Map.
   The **Link Properties** pane and the following toolbar appear when a link is selected.



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



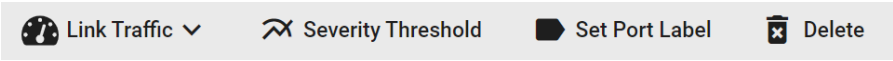
4. To adjust the time period for the graph data:
   a. Click the **From** date and select a new starting date.
   b. Click the **To** date and select a new ending date.
5. Hover over a line to view the direction of traffic.
   For example, the green line at the top of the following graph represents traffic from **192.168.127.1 (device IP address) Port 1 to 192.168.127.103 (device IP address) Port 4**.



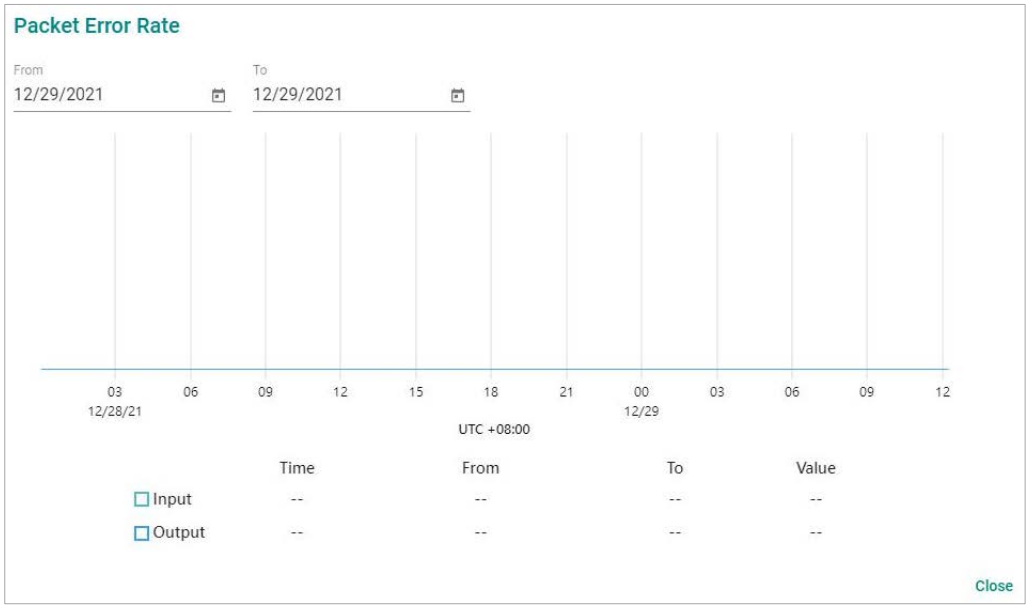
Viewing Packet Error Rates

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 and the maximum interval you can select is 90 days.

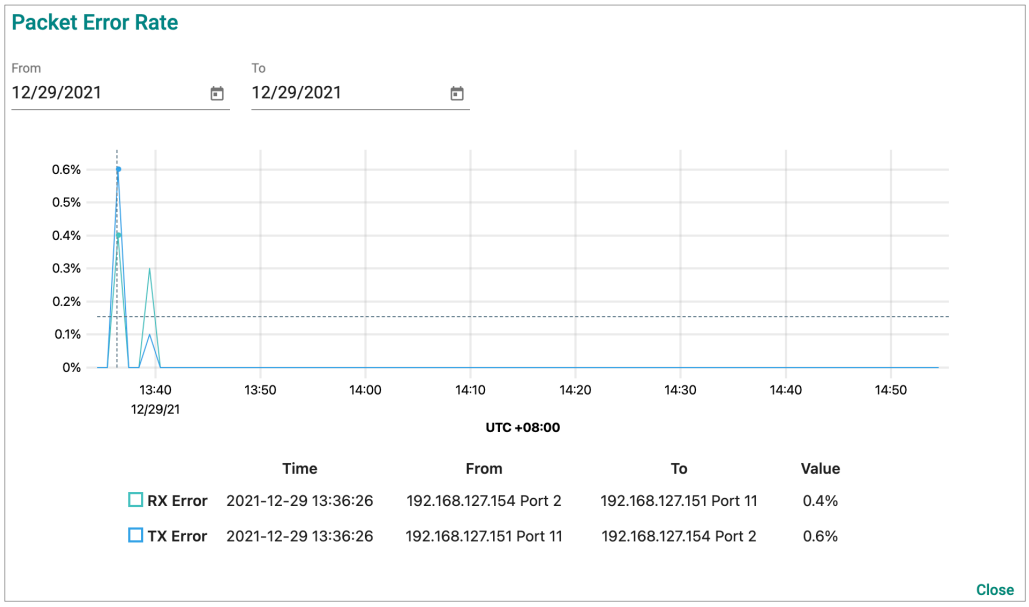
1. Navigate to **Menu** ( ) **> Topology**.
   The **Topology** screen appears and displays the Topology Map by default.
2. Click on a link between devices in the Topology Map.
   The **Link Properties** pane and toolbar appear when a link is selected.



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



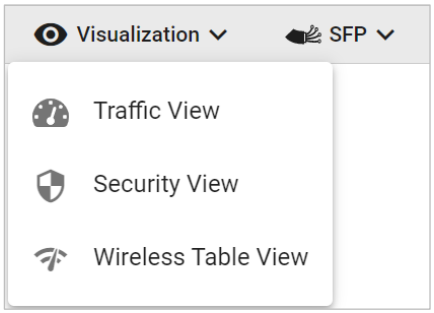
4. To adjust the time period for the graph data:
   a. Click the **From** date and select a new starting date.
   b. Click the **To** date and select a new ending date.
5. Hover over a line to view the packet error rate.



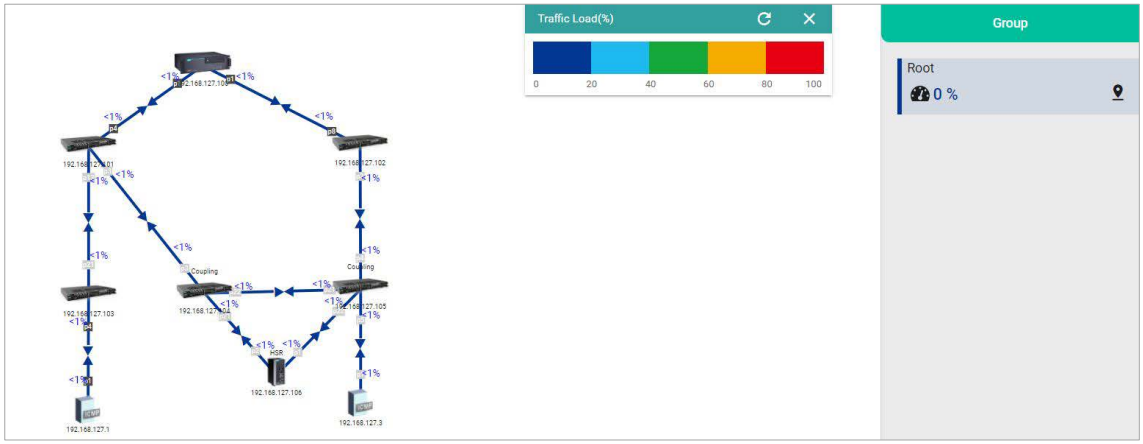
Monitoring Traffic Loads

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

1. Navigate to **Menu** ( ) **> Topology**.
   The **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 **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.



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

- High
- Medium
- Basic
- Open: Security Level below basic
- Unknown: Devices without security-related information for MXview One

NOTE

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

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

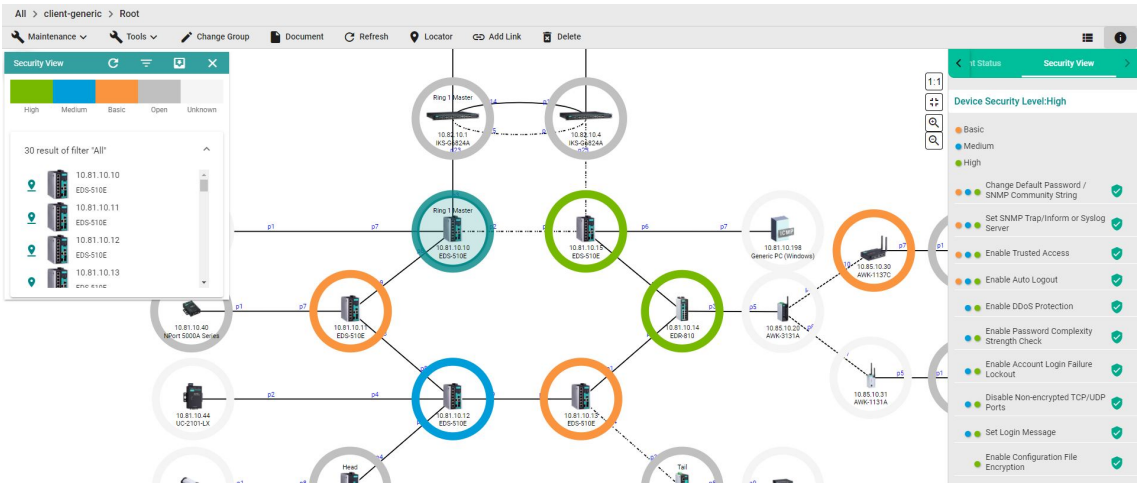
   The **Topology** screen will appear and display the Topology Map by default.

2. If **List view** is selected, click the **Topology view** ( ) icon in the top right corner.

   The **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.



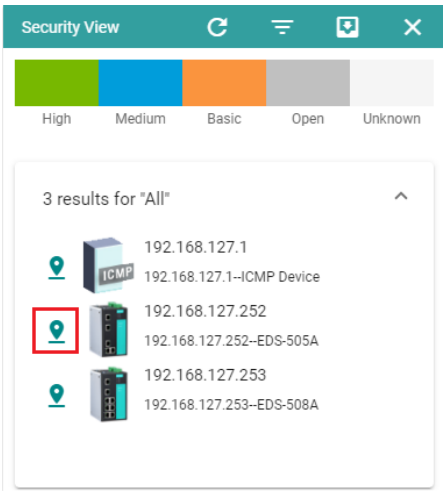
4. To filter the devices in the **Security View** window by security level:

   a. Click the **Filter** ( ) icon.

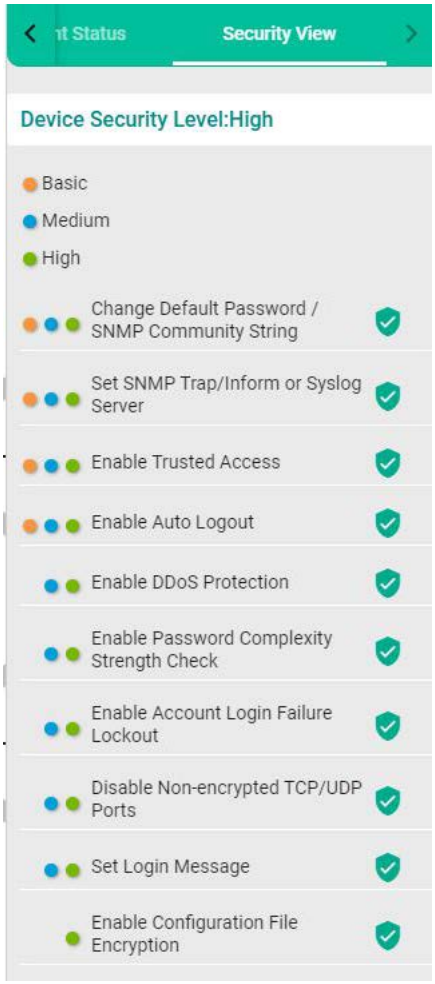
   b. Select the security level.

      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. View the Security View Report:

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

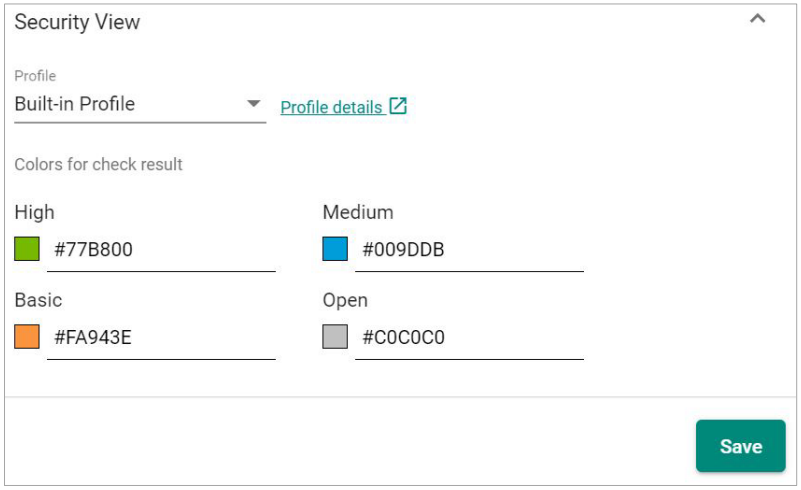
8. Review the following items in the Security View details pane:

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

NOTE

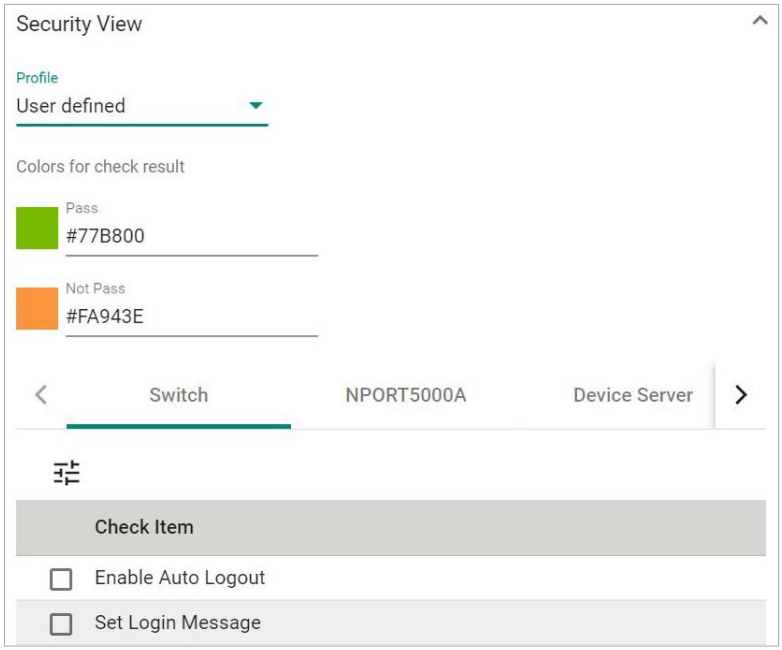
Users can use Security Wizard function in MXconfig to easily set the Security View status of devices.

9. To modify the colors used to indicate the security levels:
   a. Navigate to **Menu** ( ) **> Administration > Preferences**.
      The **Preferences** screen will appear.
   b. Under the **Appearance** section, expand **Security View**.
   c. In the **Colors for check result** section, modify the color used to indicate a security level.



   d. Click **Save**.

10. To define a custom security profile:
    a. Navigate to **Menu** ( ) **> Administration > Preferences**.
       The **Preferences** screen will appear.
    b. Under the **Appearance** 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
        - ❒ NPORT5000A
        - ❒ Device Server
        - ❒ Terminal Server
        - ❒ Gateway
        - ❒ Wireless
        - ❒ IO
    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**.

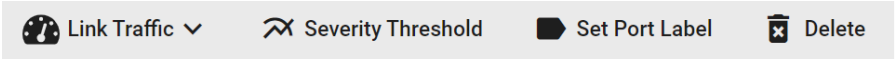
Configuring Severity Thresholds for Traffic and Fiber Status Monitoring Events

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

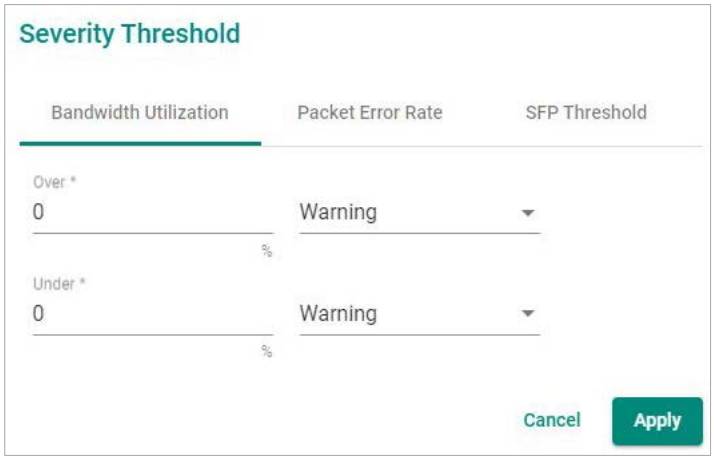
- Bandwidth utilization is over the threshold.
- Bandwidth utilization is under the threshold.
- Packet error rate is over the threshold.
- Fiber Rx is under the threshold.
- Fiber Tx is under the threshold.
- Fiber temperature is over the threshold.
- Fiber voltage is under the threshold.
- Fiber voltage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

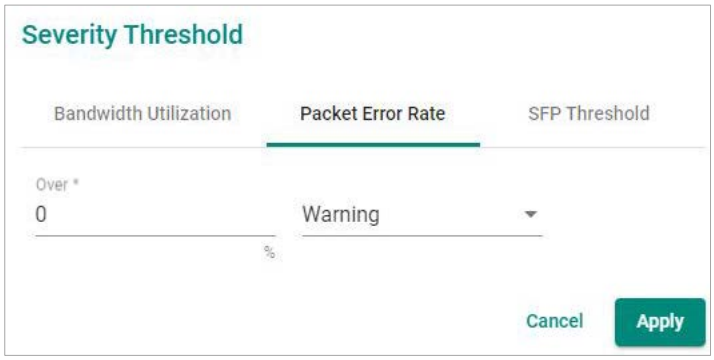
Since a link is bidirectional, the event will be triggered when the traffic condition in either direction satisfies the configured severity threshold.

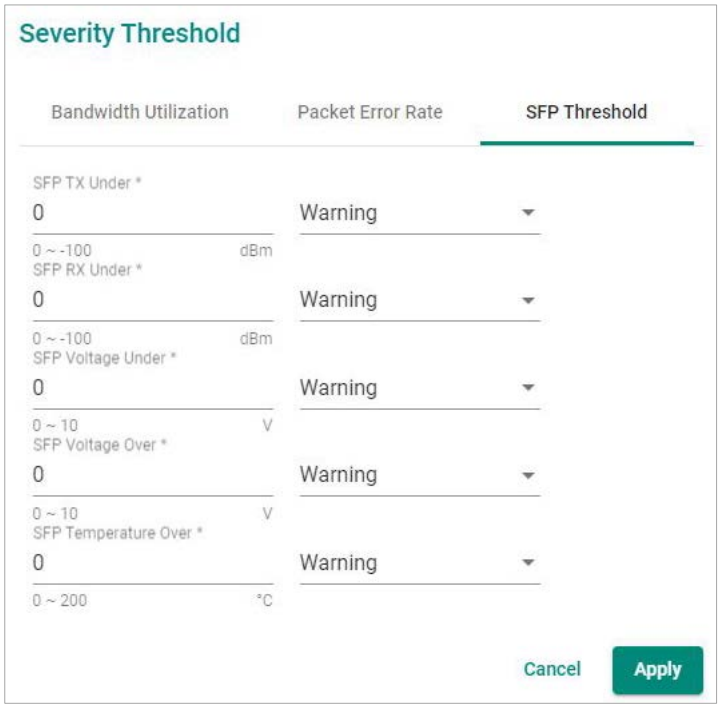
1. Navigate to **Menu** ( ) **> Topology**.
   The **Topology** screen will appear and display the Topology Map by default.
2. Click on a link between devices in the Topology Map.
   The **Link Properties** pane and toolbar appear when a link is selected.



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. To trigger an event when the SFP Tx falls below a specific range:
   a. Click the **SFP Threshold** tab.
   b. In the **SFP Tx Under** field, specify the maximum Tx threshold in dB (0~-100)
   c. From the adjacent drop-down list, select one of the following severity levels:
      - ❒ Information
      - ❒ Warning
      - ❒ Critical

8. To trigger an event when the SFP Rx falls below a specific range:
   a. Click the **SFP Threshold** tab.
   b. In the **SFP Rx Under** field, specify the maximum Rx threshold in dB (0~-100)
   c. From the adjacent drop-down list, select one of the following severity levels:
      - ❒ Information
      - ❒ Warning
      - ❒ Critical
9. To trigger an event when the SFP voltage falls below a specific range:
   a. Click the **SFP Threshold** tab.
   b. In the **SFP Voltage Under** field, specify the maximum voltage in V (0~10)
   c. From the adjacent drop-down list, select one of the following severity levels:
      - ❒ Information
      - ❒ Warning
      - ❒ Critical
10. To trigger an event when the SFP voltage exceeds a specific range:
    a. Click the **SFP Threshold** tab.
    b. In the **SFP Voltage Over** field, specify the minimum voltage in V (0~10)
    c. From the adjacent drop-down list, select one of the following severity levels:
       - ❒ Information
       - ❒ Warning
       - ❒ Critical
11. To trigger an event when the SFP temperature exceeds a specific range:
    a. Click the **SFP Threshold** tab.
    b. In the **SFP Temperature Over** field, specify the minimum temperature in Celsius (0~100)
    c. From the adjacent drop-down list, select one of the following severity levels:
       - ❒ Information
       - ❒ Warning
       - ❒ Critical
12. Click **Apply**.

    MXview One will update the modified settings.
13. (Optional) Configure the Severity Threshold and Fiber status:
    a. Navigate to **Menu** ( ) **> Administration > Global Device Settings**.

       The **Global Device Settings** screen appears.
    b. To set the threshold, you can go to the sections below to complete the settings.
       - ❒ Bandwidth Utilization
       - ❒ Packet Error Rate
       - ❒ SFP Threshold
    c. Click **Save**.

       MXview updates the web console protocol settings.

NOTE

If you complete the Bandwidth Utilization, Packet Error Rate, and SFP Threshold settings in the Global Device Settings section, the settings will be implemented to all the devices in your topology.

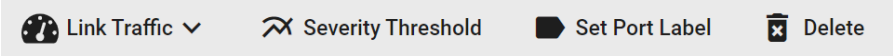
Configuring Custom Port Labels

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

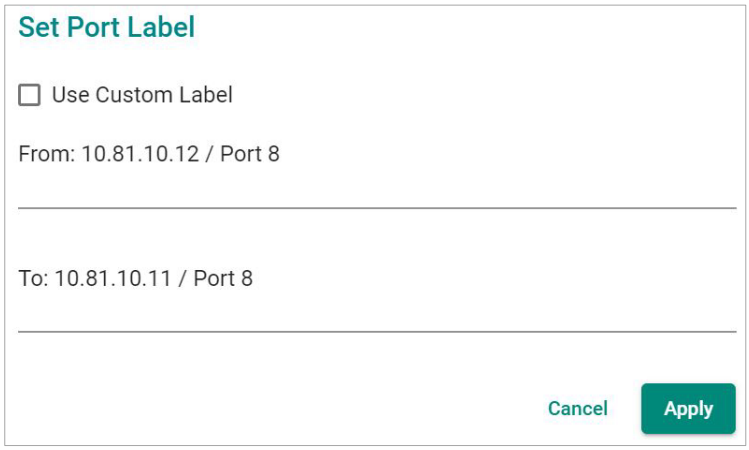
<Device IP Address> / <Port Number>

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

1. Navigate to **Menu** ( ) **> Topology**.
   The **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.



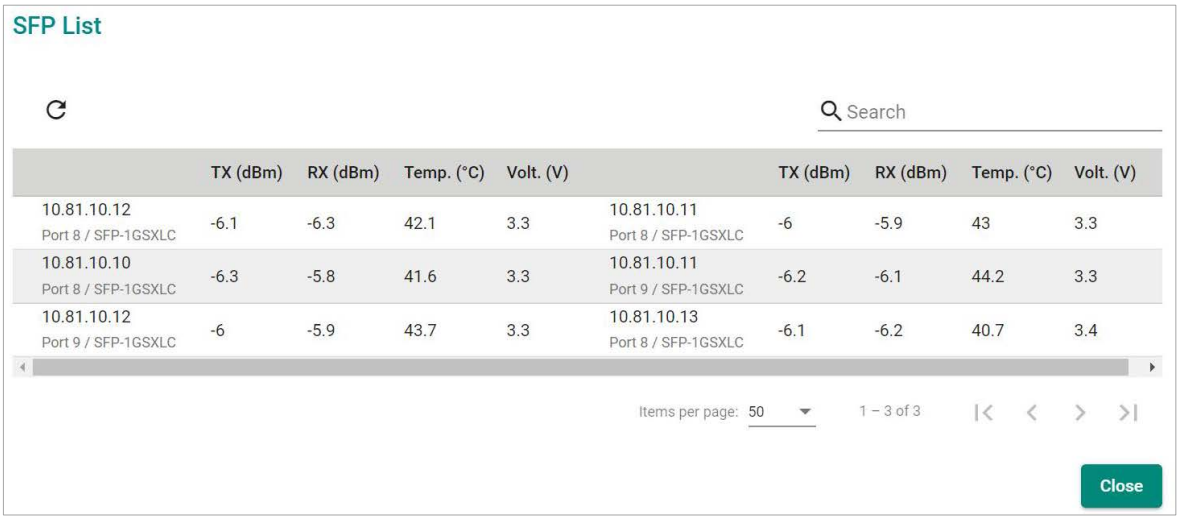
4. Select the **Use Custom Label** check box.
5. In the **From** field, provide a new label for the source port.
6. In the **To** field, provide a new label for the destination port.
7. Click **Apply**.

9. SFP Fiber Status

Viewing the SFP Fiber Status in Table View

MXview One collects and display fiber status in **SFP > SFP List**

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

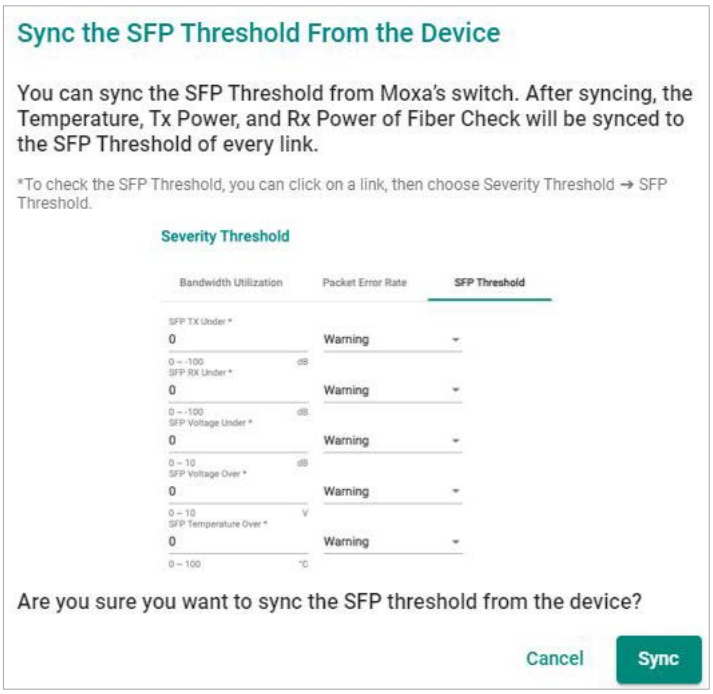


Synchronize the SFP Threshold From the Device

MXview One can synchronize the threshold from devices, which can detect Moxa's SFP connector to get the specific threshold.

Navigate to **SFP > Sync Threshold From the Device**

Click **Sync** and the threshold from the devices will sync to the SFP Threshold of every link.

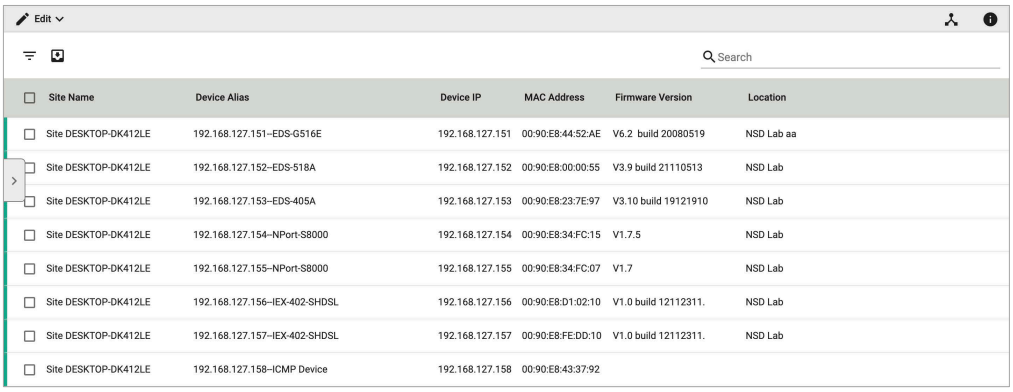


10. Device Management

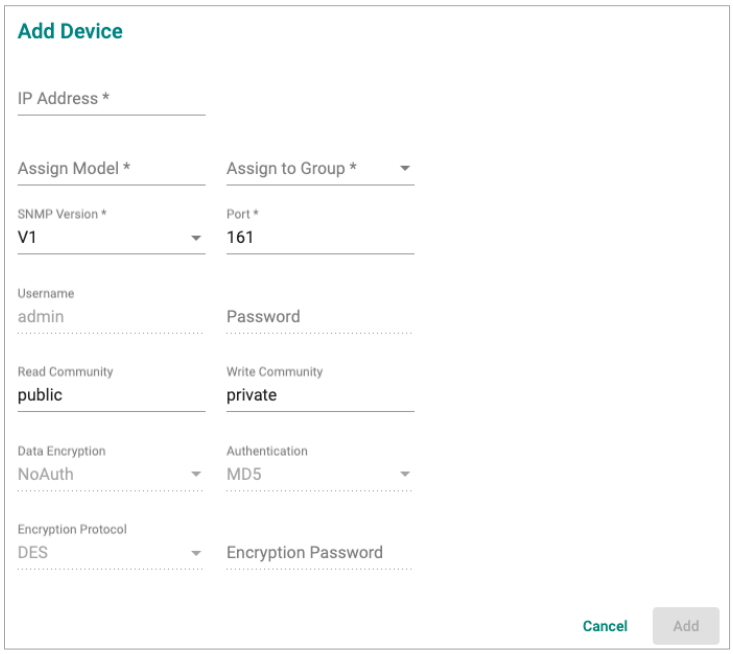
The MXview One **Topology** screen provides several features and tools for managing and maintaining devices in your network topology.

Viewing the Device List

The **List view** on the **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** ( ) **> Topology**.
   The **Topology** screen will appear and display the Topology Map in Topology view.
2. Click the **List view** ( ) icon in the top right corner.
   The **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
   - ❒ **Username:** Specify the device login Username
   - ❒ **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**.

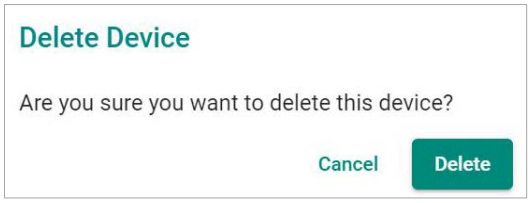
MXview One adds the device to the topology.

4. To delete devices in your network topology:

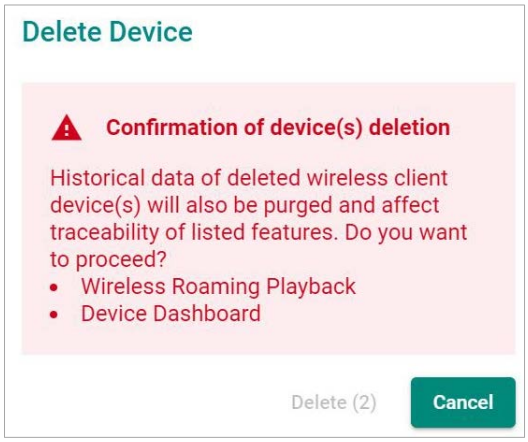
a. Check the box on the first column of devices.

b. Click the **Delete** ( ) icon on the menu bar. The **Delete Device** screen appears.

c. For non AWK devices, read the message and then click **Delete** if you are sure you want to delete the device.



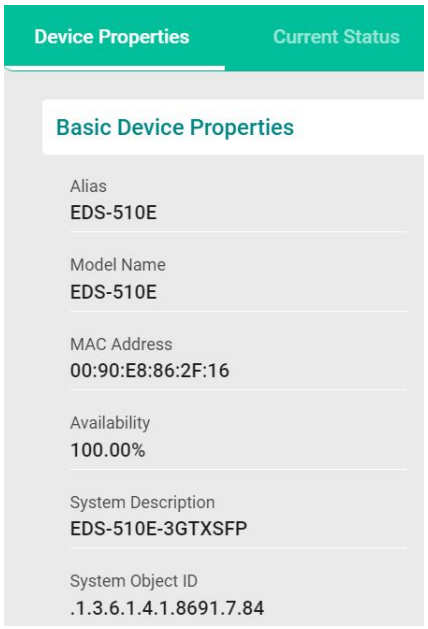
d. For AWK devices, read the message and wait for the countdown. Click **Delete** if you are sure you want to delete the device.



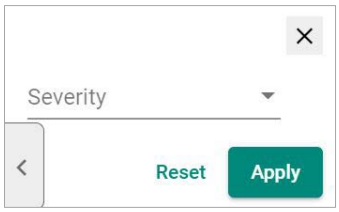
NOTE

If you click the check box for all the devices, when you click the Delete icon, you will delete all the devices in the topology.

5. To view device properties, select the check box next to the **Site Name**.
   The **Device Properties** details pane will appear.



6. To filter the device list by severity level:
   a. Click the **Filter** ( ) icon in the top left corner.
      The **Severity** drop-down list appears.



   b. Select one of the following severity levels:
      - ❒ **Critical**
      - ❒ **Warning**
      - ❒ **Information**
   c. Click **Apply**.
      MXview One filters the device list to only display devices with the selected severity level.
7. To export the device list:
   a. Click the **Export** ( ) icon.

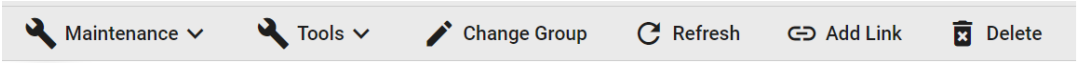
   b. Select **Export CSV**.
      MXview One will export the displayed data as a CSV file.

Importing Device Configurations

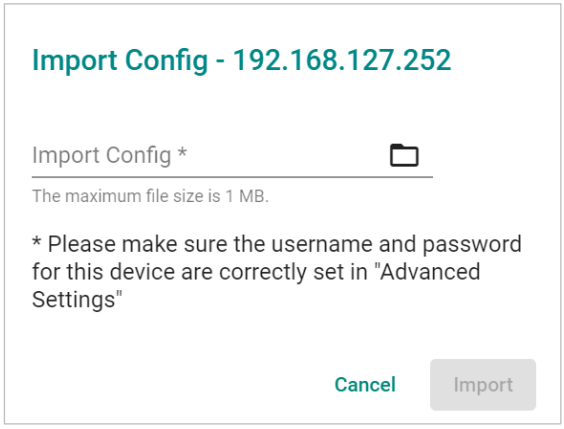
Use the **Topology** screen to import an INI-formatted configuration file to a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to **Menu** ( ) **> Topology**.
   The **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 site name 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.



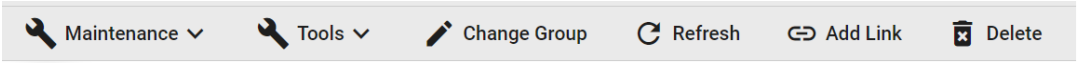
5. Click the folder ( ) icon to upload the configuration file from your local machine.
6. Click **Import**.
   MXview One imports the configuration file to the specified device.

Exporting Device Configurations

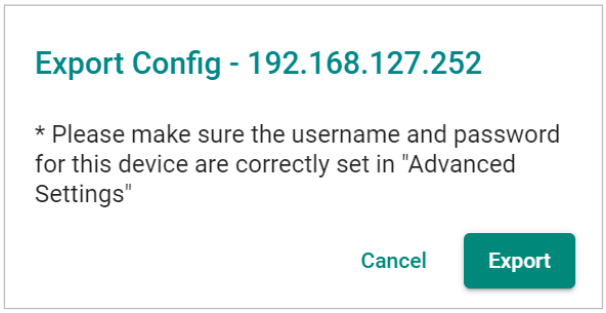
Use the **Topology** screen to export an INI-formatted configuration file from a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to **Menu** ( ) **> Topology**.
   The **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**.
   MXview One exports the device configurations as an INI file in the specified location.

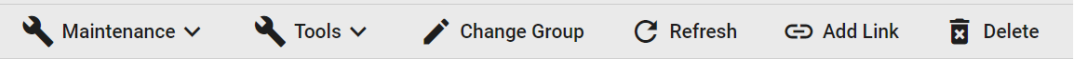
Upgrading Firmware

Use the **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**.

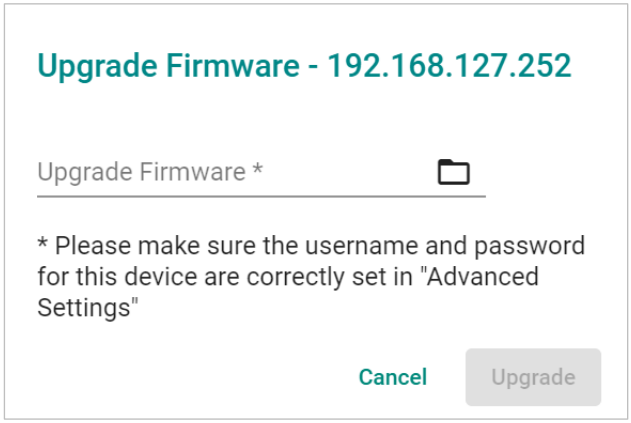
1. Navigate to **Menu** ( ) **> Topology**.
   The **Topology** screen appears and displays the Topology Map by default.
2. Select one of the following views:
   - **Topology view:** Displays a graphical representation of the devices in your network topology.

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

   The toolbar options change.



4. Navigate to **Maintenance > Upgrade Firmware**.
   The Upgrade Firmware screen appears and indicates the IP address of the selected device.



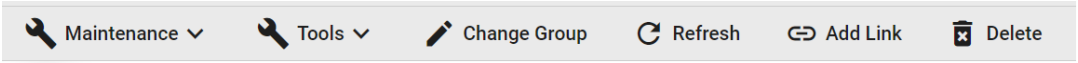
5. Click the folder ( ) icon to upload the ROM-formatted firmware file from your local machine.
6. Click **Upgrade**.
   MXview One will upgrade the firmware on the specified device.

Configuring SNMP Trap Server

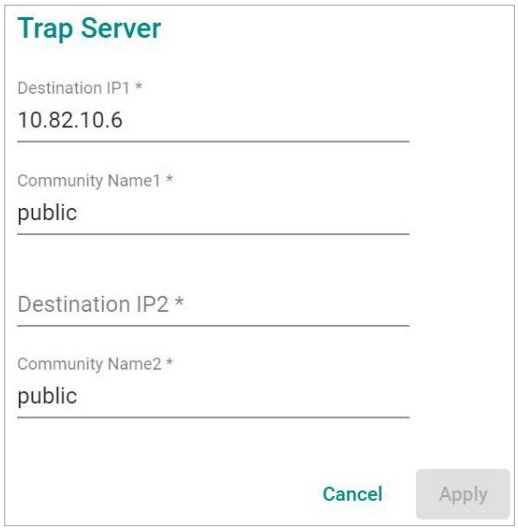
MXview One can collaborate with other network management software and send SNMP Traps to non-Moxa NMS. MXview One supports up to two trap servers depending on the device.

1. Navigate to **Menu** (☰) **> Topology**.
   The **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 One sends SNMP traps to the configured trap server(s) when events are detected on the device.

NOTE

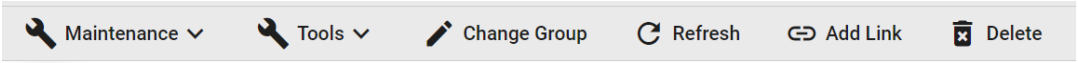
When a device fails to reply within seven seconds, MXview One will display the message "Failed to update device Trap server settings." Please confirm the execution results via the same settings page or go to the web page of the devices.

Configuring Port Settings

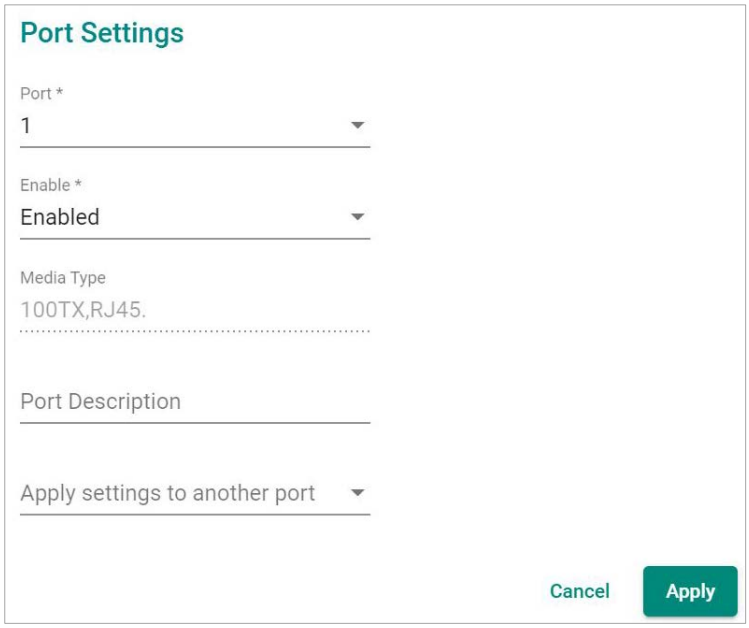
Use the **Topology** screen to configure port settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to **Menu** ( ) **> Topology**.
   The **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.



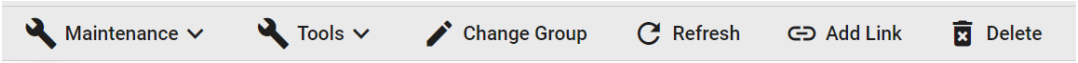
5. Configure the following port settings for the device:
   - **Port:** Select the port number.
   - **Enable:** Enable or disable the port.
   - **Port Description:** Provide a description of the port.
   - **Apply settings to another port:** Select to apply the configured settings to other ports on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

Configuring SNMP Configuration

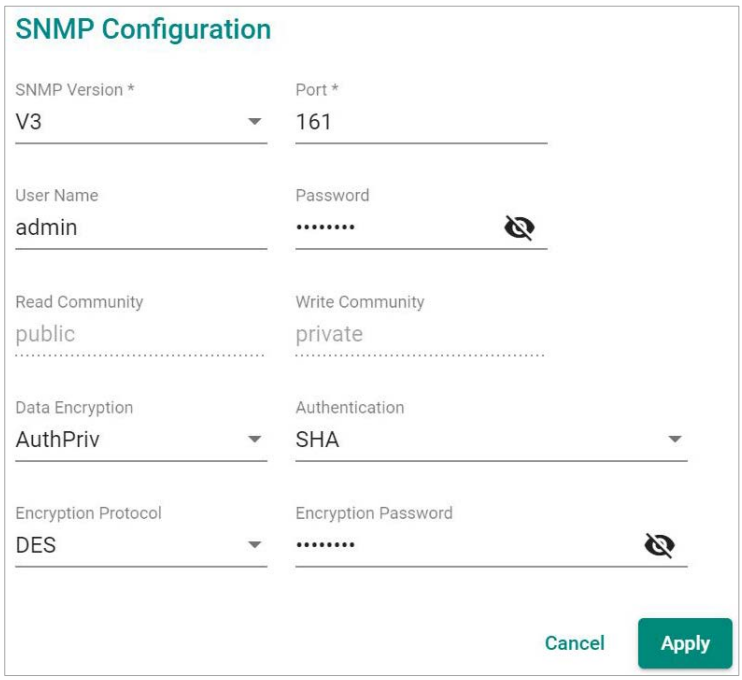
Use the **Topology** screen to configure SNMP settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to **Menu** ( ) **> Topology**.
   The **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 Configuration**.
   The **SNMP Configuration** screen will appear.



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

NOTE

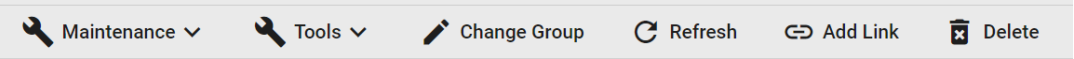
For the first time, users can use the Device Settings Template function to set the function template. For more information, see **Changing Default SNMP Configuration**.

Configuring Polling Settings

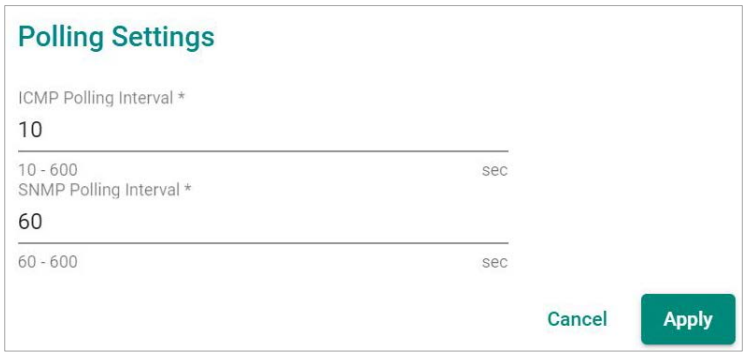
Use the **Topology** screen to configure ICMP or SNMP polling settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to **Menu** ( ) **> Topology**.
   The **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**
   - **SNMP polling interval**
6. Click **Apply**.
   MXview One will update the polling settings for the device.

NOTE

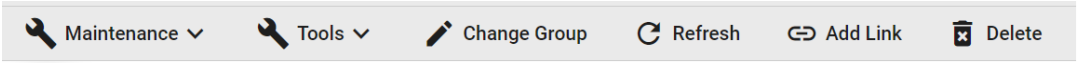
For the first time, users can use the Device Settings Template function to set the function template. For more information, see **Configuring Device Polling Settings**.

Configuring Advanced Settings

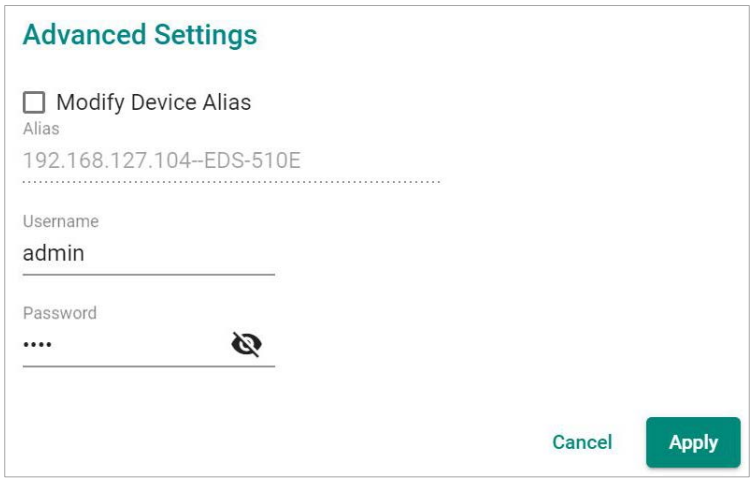
Use the **Topology** screen to configure advanced settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to **Menu** ( ) **> Topology**.
   The **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 > Advanced Settings**.
   The **Advanced Settings** screen appears.



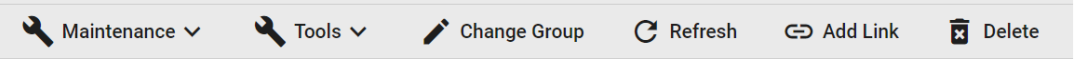
5. To modify device alias:
   a. Select the **Modify Device Alias** check box.
   b. Edit the **Alias** field.
6. To specify login credentials for the device web console
   Enter the **Username** and **Password** for the device web console.
7. Click **Apply**.
   MXview One updates the advanced settings.

Changing the Device Icon

Use the **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** ( ) **> Topology**.
   The **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. (The maximum image size is 100 kB.)
6. Click **Apply**.
   MXview One will change the device icon to the uploaded JPG, GIF, or PNG image file.

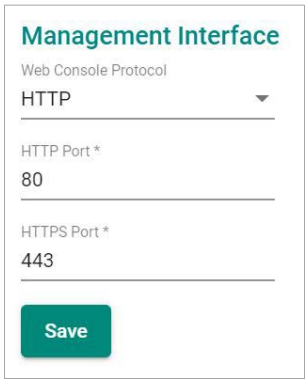
Signing on to Device Web Consoles

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

NOTE

You can use the **Global Device Settings** 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.

1. (Optional) Configure the web console protocol:
   a. Navigate to **Menu** ( ) **> Administration > Global Device Settings**.
      The **Global Device Settings** screen appears.
   b. Find the **Management Interface** to complete the settings.



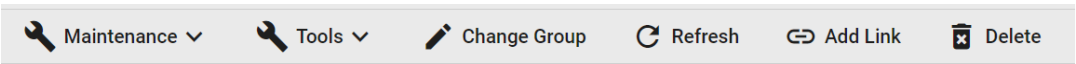
   c. Configure the following:
      - ❒ **Web Console Protocol**
      - ❒ **HTTP Port**
      - ❒ **HTTPS Port**
   d. Click **Save**.
      MXview One updates the web console protocol settings.

NOTE

If you complete the Management Interface settings in the Global Device Settings section, the settings will be applied to all the devices in your topology.

2. Navigate to **Menu** ( ) **> Topology**.
   The **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.

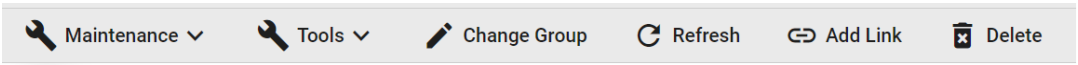
6. Enter the **Username** and **Password** for the device web console.
7. Click **Login**.
   The device web console will successfully log in.

Changing Device Groups

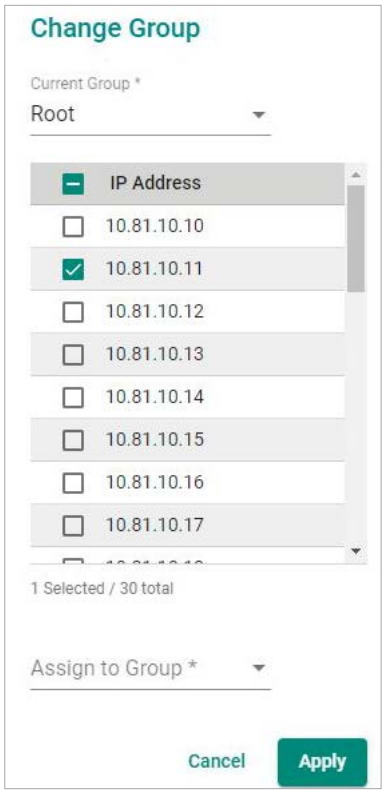
Use the **Topology** screen to change the assigned group for a device by selecting the device from the **Topology Map** or **Device List**.

1. Navigate to **Menu** ( ) **> Topology**.
   The **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 One will assign the selected device(s) to the new group.

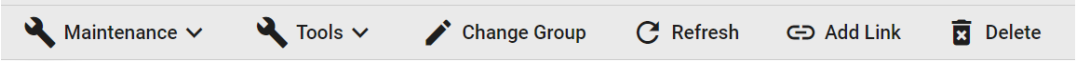
Refreshing the Device Status

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

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

   The **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 One polls the device for updated data.

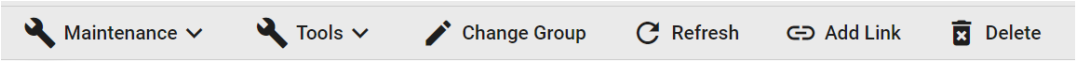
Deleting Devices

Use the **Topology** screen to delete devices from the Topology Map. After a device is deleted, it will be removed from the topology map and the device will not be polled.

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

   The **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 One removes the device from your network topology.

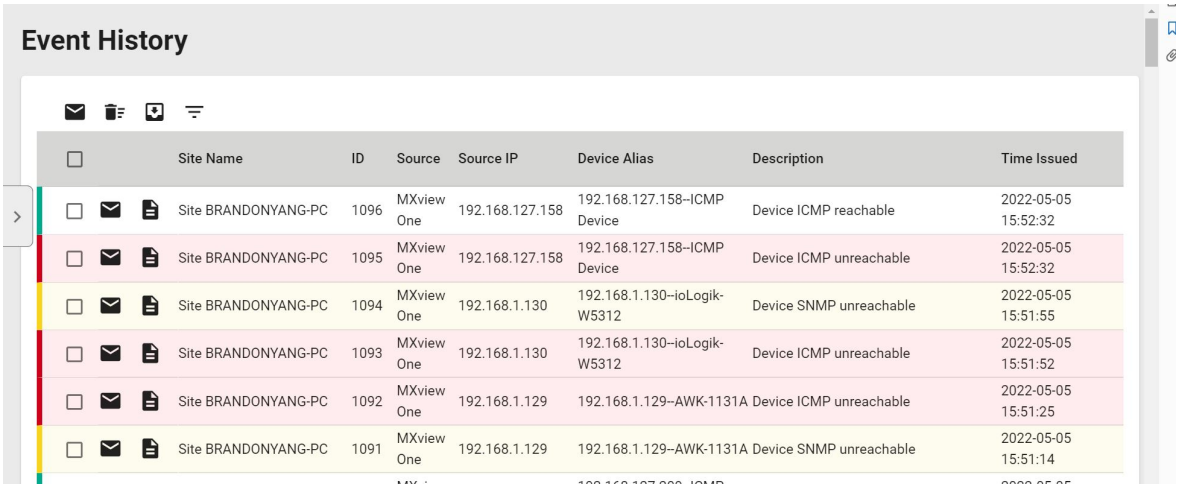
11. Events and Notifications

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

Event Monitoring

Viewing Event History

The **Event History** 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.

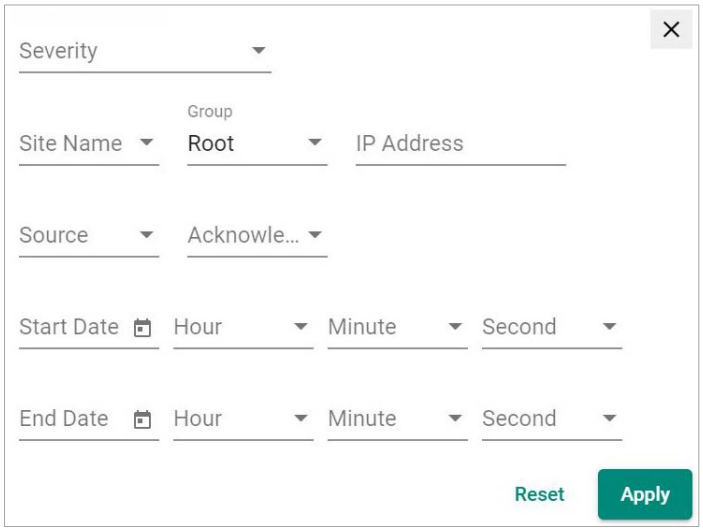


1. Navigate to **Menu** ( ) **> Event Management > Event History**.

   The **Event History** screen will display the following information in a table format:

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

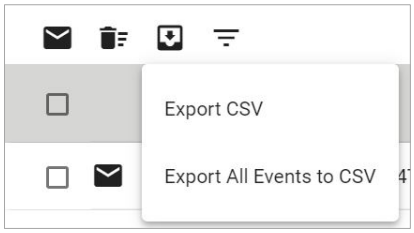
2. To filter the information in the table by specific criteria:
   a. Click the **Filter** ( ) icon in the top left corner.
      The following screen will appear.



   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
Acknowledge	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

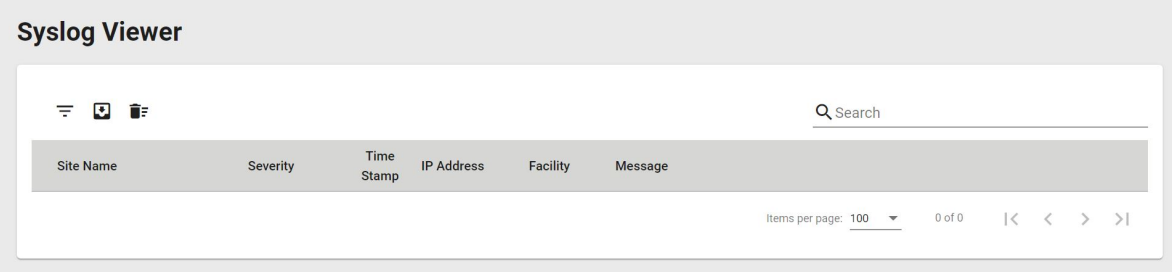
   c. Click **Apply**.
      MXview One filters the table to only display events that match the specified criteria.
3. To sort the data in the table by a specific column, click the column heading.
   MXview One sorts the table by the column.
4. To export data displayed on the **Event History** screen:
   a. Click the **Export** ( ) icon.



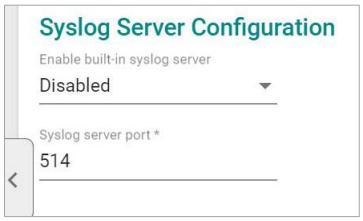
   b. Select **Export CSV** for just the events on the first page or **Export All Events to CSV** for all event pages.
      MXview One exports the displayed event data as a CSV file.

Viewing Syslog Events

The **Syslog 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** ( ) **> Administration > System Settings**.
      The **System Settings** screen appears.
   b. Find the **Syslog Server Configuration** section.
      The **Syslog Server Configuration** settings will appear.

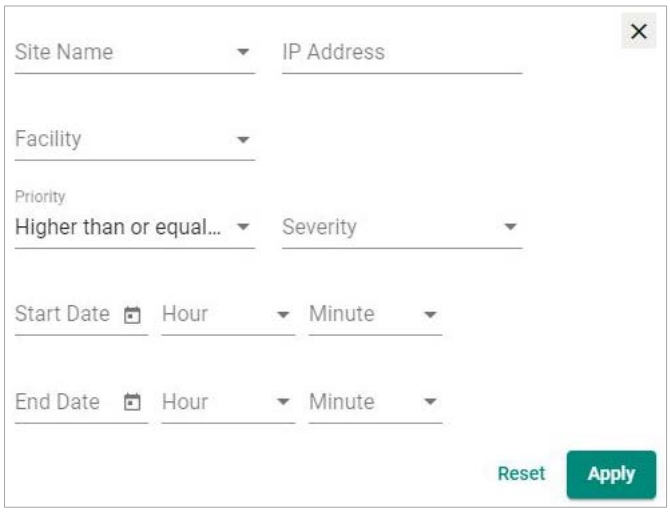


   c. Select **Enabled** from the Enable built-in syslog server drop-down list.
   d. Specify the syslog server communication port.
   e. Click **Save**.
      MXview One enables the built-in syslog server and starts logging syslog events.
2. Navigate to **Menu** ( ) **> Event Management > Syslog Viewer**.
   The **Syslog Viewer** screen displays the following information in a table format:

Column	Description
Site Name	The site to which the device that issued the event belongs
Severity	The severity of the event
Time Stamp	The time the event was issued
IP Address	The IP address of the device that issued the event
Facility	The group the device is assigned to
Message	The description of the event

3. To search the information in the table, type a full or partial string that matches the value in any of the table columns.
   MXview One searches the table to only display results that fully or partially match the specified string.

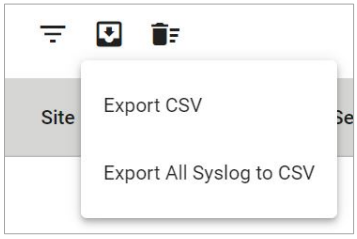
4. To filter the information in the table by specific criteria:
   a. Click the **Filter** ( ) icon in the top left corner.
      The following screen will appear.



   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 One 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 One sorts the table by the column.
6. To export data displayed on the **Syslog Viewer** screen:
   a. Click the **Export** ( ) icon.

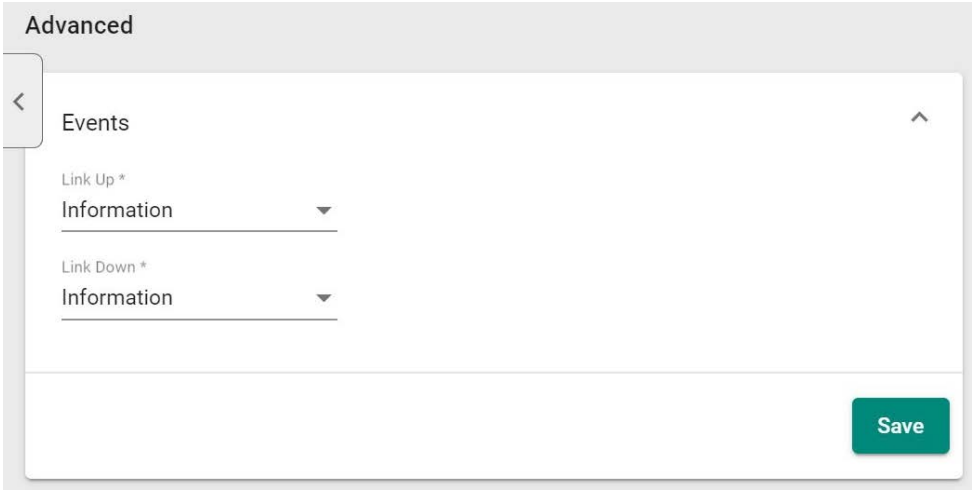


   b. Select **Export CSV** for just the first syslog page or **Export All Syslog to CSV** for all syslog pages.
      MXview One exports the displayed syslog data as a CSV file.

Configuring Event Thresholds and Severity Levels

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

1. Navigate to **Menu** ( ) **> Administration > 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**
   - **Waning**
   - **Critical**
4. Select one of the following severity levels for **Link Down** events:
   - **Information**
   - **Warning**
   - **Critical**
5. Navigate to **Menu** ( ) **> Administration > Global Device Settings**.
   The **Global Device Settings** screen will appear.

> **NOTE**
>
> Once you save the settings in the Global Device Settings section, the settings will synchronize to each device in the topology.

6. 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.

7. 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.

8. 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 for the threshold.

   c. Select the **Severity** level for the event.

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

   b. Specify the SFP TX threshold level.

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

   b. Specify the SFP RX threshold level.

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

b. Specify the SFP Voltage threshold level.

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

    b. Specify the SFP Voltage threshold level.

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

    b. Specify the SFP Temperature threshold level.

> **NOTE**
>
> If the threshold is set as '0', the threshold function will be disabled.

14. Click **Save**.
    MXview One will update the event threshold settings.

Notification Methods

MXview One supports email notifications for events. The notification method requires specific server configurations.

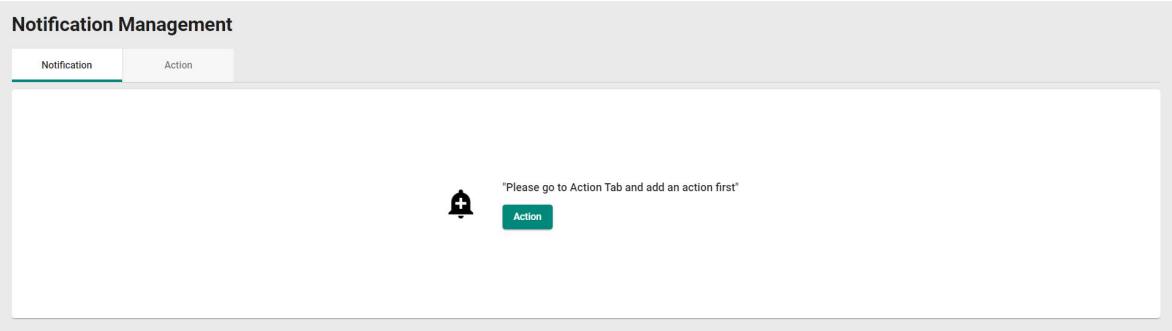
Configuring Email Server Settings

Use the **System Settings** screen to configure an email server to send email notifications for event notifications.

1. Navigate to **Menu** (☰) **> Administration > System Settings**.
   The **System Settings** screen will appear.
2. Find the **Email Server Configuration** section.
3. Configure the following:
   - **Server Domain Name/IP**
   - **Port number**
   - **Encryption**
   - **Username**
   - **Password**
   - **Sender Address**
4. Click **Save**.
   MXview One can send email messages for configured event notifications.

Notification Management

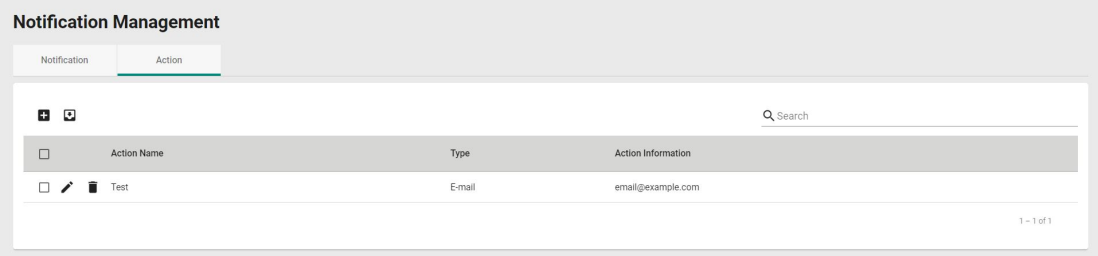
The **Notification Management** screen allows you to configure event notifications by issuing a registered action (e.g., sending an email message to a specified recipient) when configured events are detected on your network.



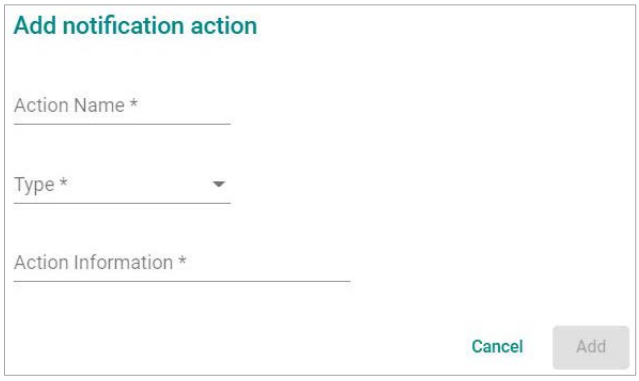
Configuring New Event Notifications

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

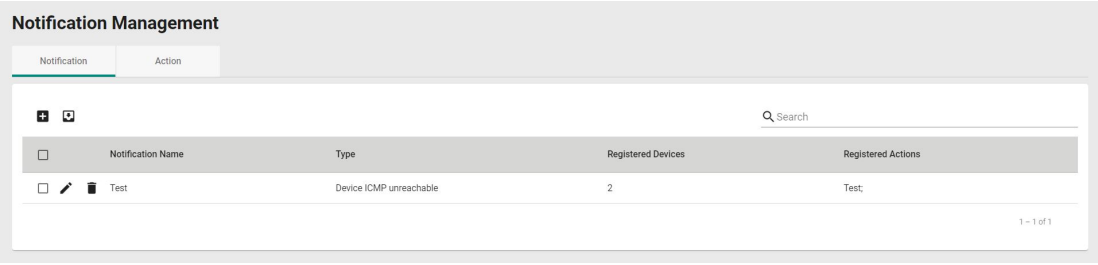
1. Navigate to **Menu** ( ) **> Notification Management**.
   The **Notification Management** screen appears.
2. To register an action:
   a. Click the **Action** tab.
      The **Action** tab displays a list of registered actions (if any).



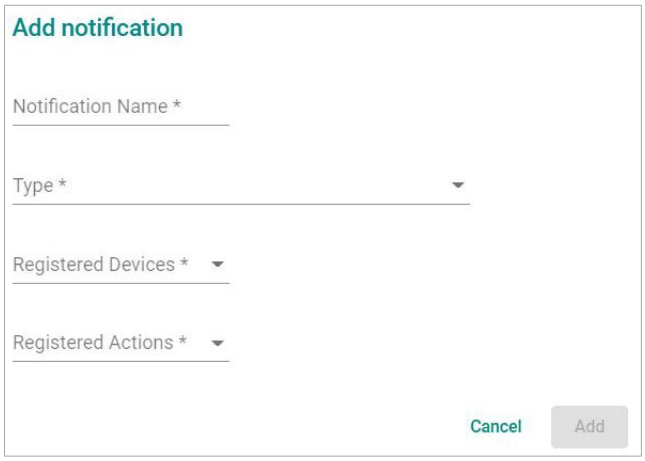
   b. Click the **Add** ( ) icon in the top right corner.
      The **Add notification action** screen will appear.



   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:
      - **E-mail:** Sends an email to the specified email address.
   e. Provide additional information required for the action (if any).
   f. Click **Add**.
      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.

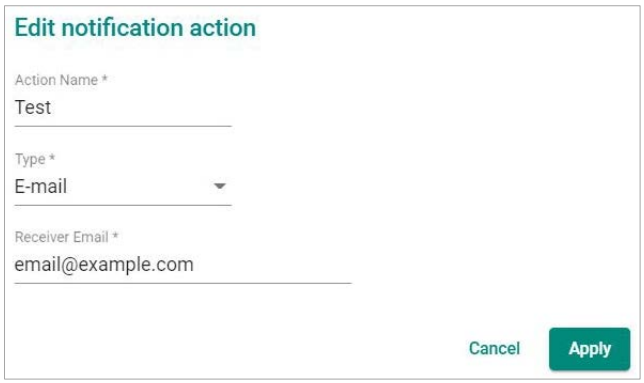


c. In the **Notification Name** field, type a name to describe the event notification.
d. From the **Type** drop-down list, select the event type.
e. From the **Registered Devices** drop-down list, select the network device(s) you want to monitor.
f. From the **Registered Actions** drop-down list, select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

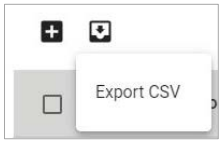


b. Modify the following settings:
- ❒ Action Name
- ❒ Type
- ❒ Action information

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.



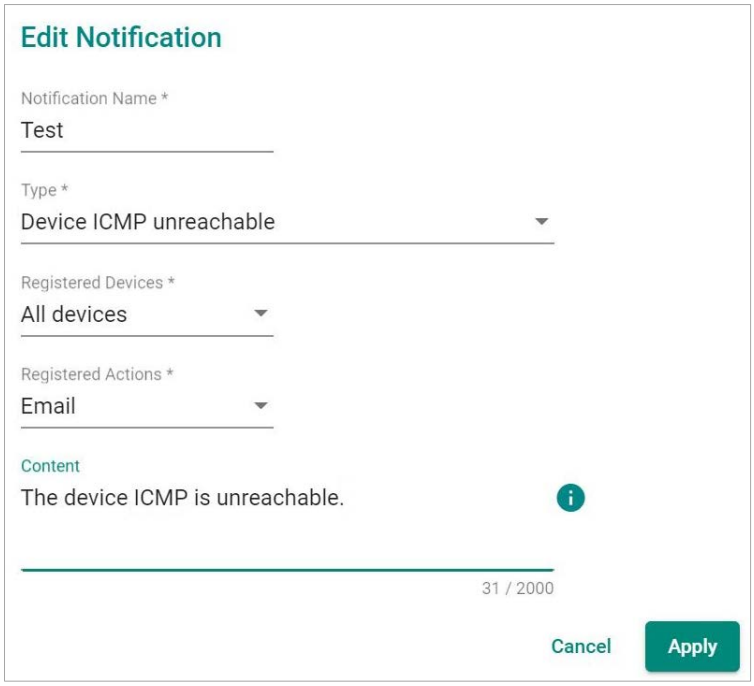
   b. MXview One exports the displayed action data as a CSV file.

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** ( ) **> 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.

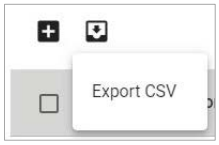


   b. Modify the following settings:
      - ❒ Notification Name
      - ❒ Type
      - ❒ Registered devices
      - ❒ Registered Actions

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

4. To export data displayed on the **Notification** tab:

   a. Click the **Export** ( ) icon.

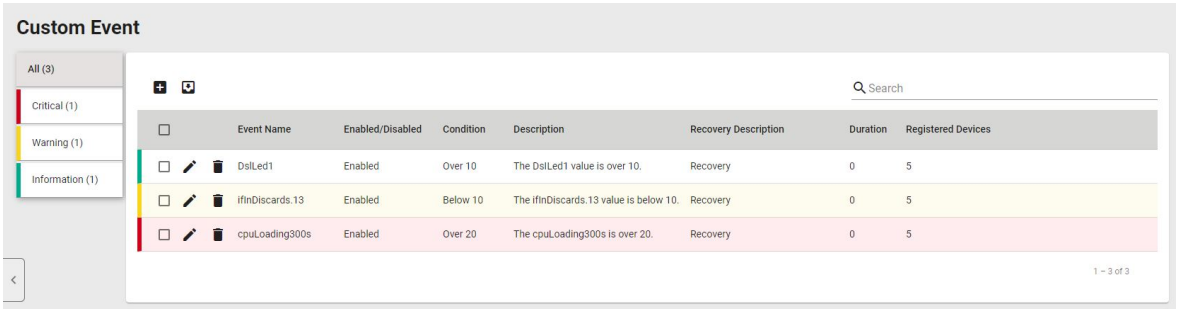


   b. Select **Export CSV**.

      MXview One exports the displayed notification data as a CSV file.

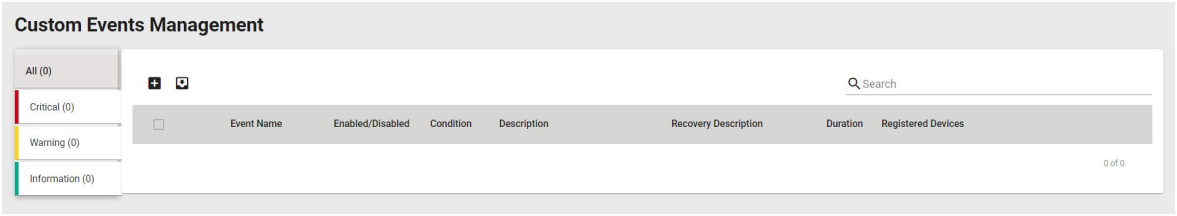
Custom Event Management

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

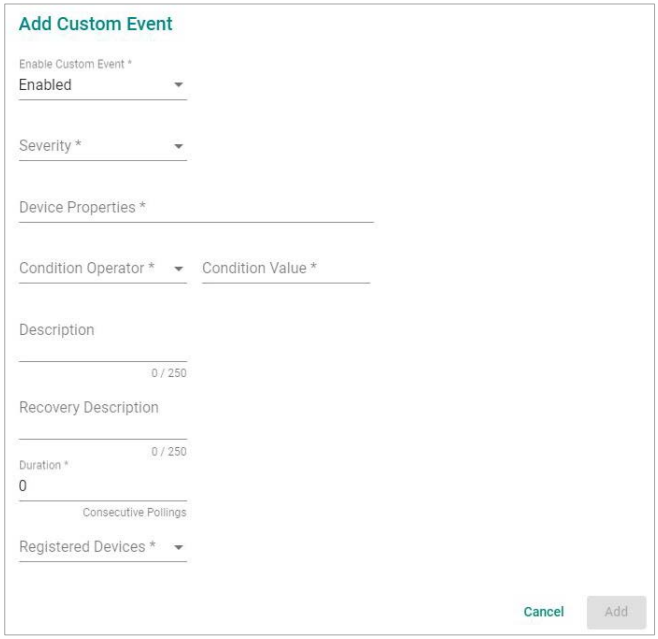


Configuring Custom Events

The Custom Event 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 Management > Custom Event**.
   The **Custom Event** screen appears.
2. Click the **Add** ( ) button in the top left corner of the screen.
   The **Add custom event** screen will appear.

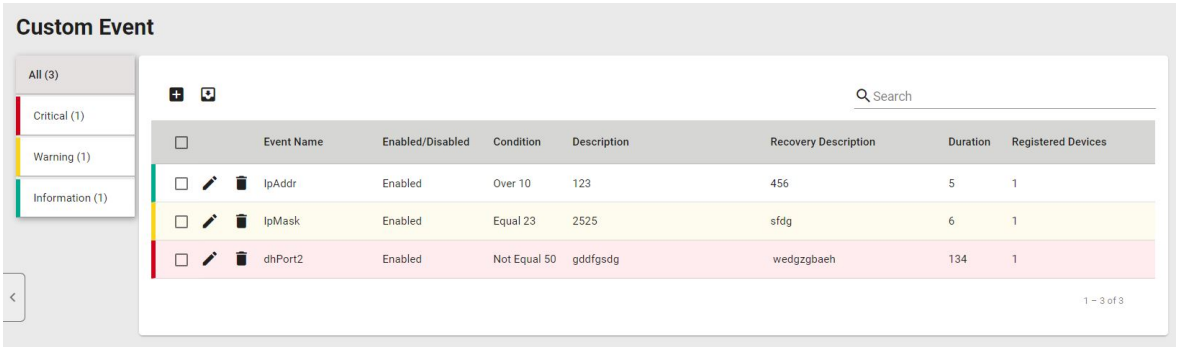


3. Select the default event status:
   - **Enabled:** MXview One monitors the event
   - **Disabled:** MXview One does not monitor the event
4. Select one of the following severity levels for the event:
   - Information
   - Warning
   - Critical
5. Click the **Device Properties** and select the device 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, users can specify how many times an event can happen without any action being taken. If the number of times the event happens exceeds the **Duration**, then MXview One will send an alert.
10. From the **Register Devices** drop-down list, select the devices to monitor for the custom event.
11. Click **Add**.
    The custom event appears in the **Custom Event** table.

> **NOTE**
>
> If the threshold is set as '0', the threshold function will be disabled.

Viewing or Exporting Custom Event Settings

The **Custom Event** screen provides information about all the custom events configured on MXview One. You can use the **Custom Event** 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 Management > Custom Event**.

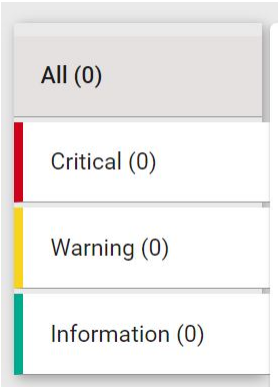
   The **Custom Event** screen will appear and displays the following information in a table format:

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 times of consecutive pollings for the event
Registered Devices	The number or registered devices that the event applies to

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

   MXview One 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.



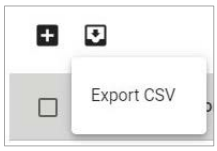
   MXview One filters the table to only display events that match the selected severity level.

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

   MXview One sorts the table by the column.

5. To export data displayed on the **Custom Event** screen:

   a. Click the **Export** ( ) icon.

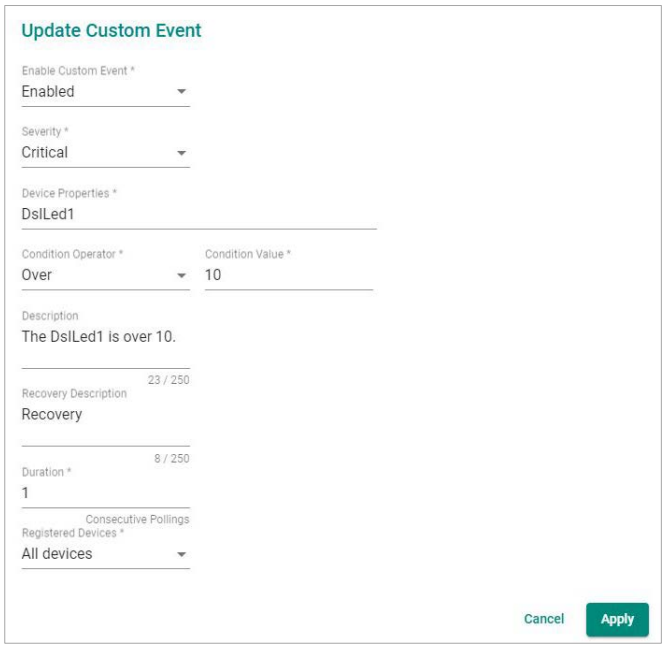


   b. Select **Export CSV.**
   MXview One exports the displayed event data as a CSV file.

Enabling/Disabling or Editing Custom Events

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

1. Navigate to **Menu** ( ) **> Event Management > Custom Event**.
   The **Custom Event** 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 Event** screen will appear and displays the updated event information.

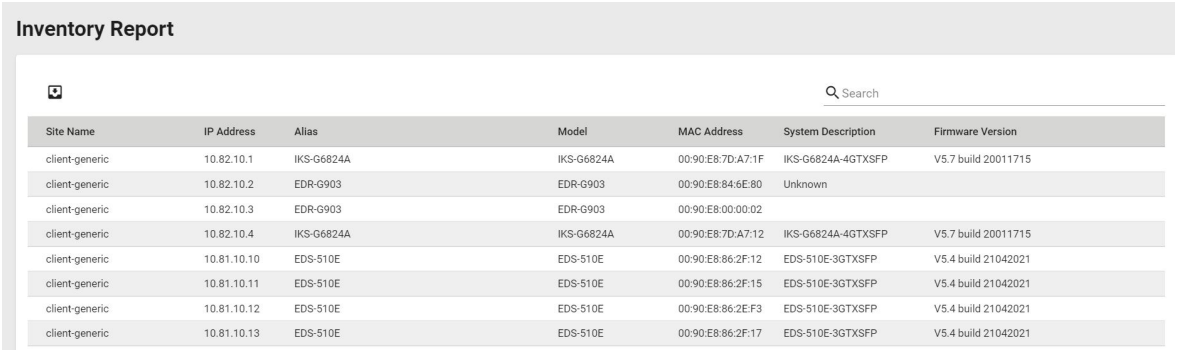
> **NOTE**
>
> If the threshold is set as '0', the threshold function will be disabled.

12. Reports

MXview One provides reports that summarize key information about your network devices.

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
Firmware Version	The firmware version of the device

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

   MXview One 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 One 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

      MXview One exports the report data in the selected format.

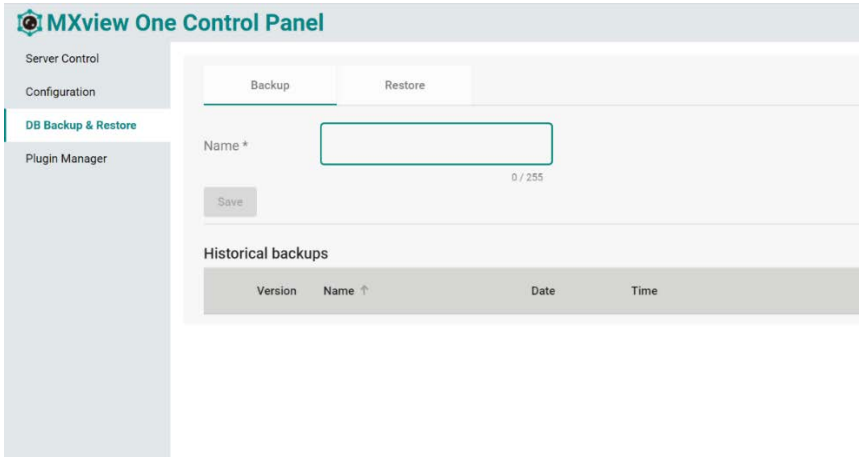
13. Backups, Restores, and Compares

The MXview One web console provides several features to assist database backups and device configuration migrations. MXview One 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 One database.

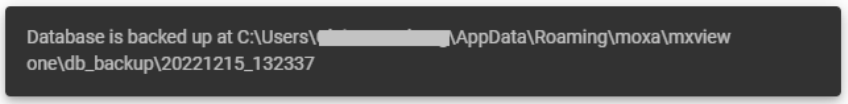
Backing Up the MXview One Database

Use the **DB Backup & Restore** screen on the **Control Panel** to back up the MXview One database.

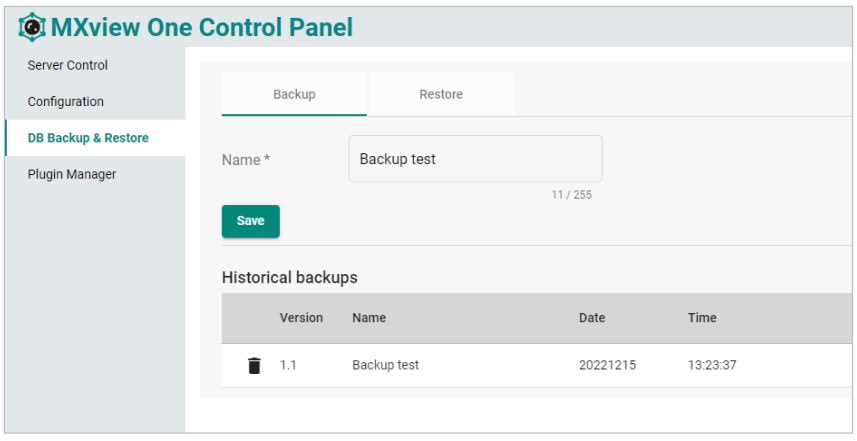
1. Navigate to **DB Backup & Restore** on the MXview One Control Panel.
   The Database Backup & Restore screen appears.



2. Choose the **Backup** tab to start the process of backing up the database.
3. In the **Name** field, specify the backup file name.
4. Click **Save**.
5. The message that the file of the backup database has been stored in the specified directory will be displayed.



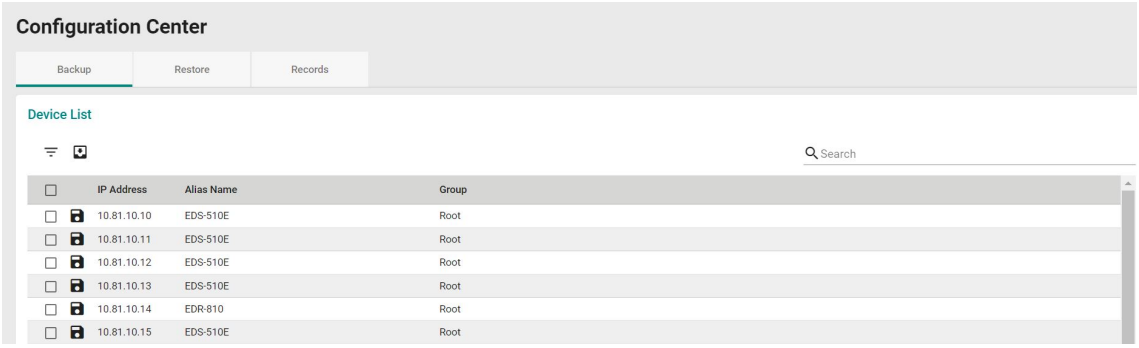
6. The **Database backup completed** will appear on the **Historical backups** list.



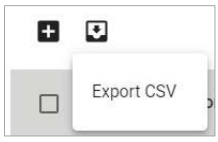
Backing Up Device Configurations

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

1. Navigate to **Menu** ( ) **> Device Configuration Center**.
   The **Device Configuration Center** screen appears.
2. Click the **Backup** tab.
   Available devices will appear in the **Device List**.



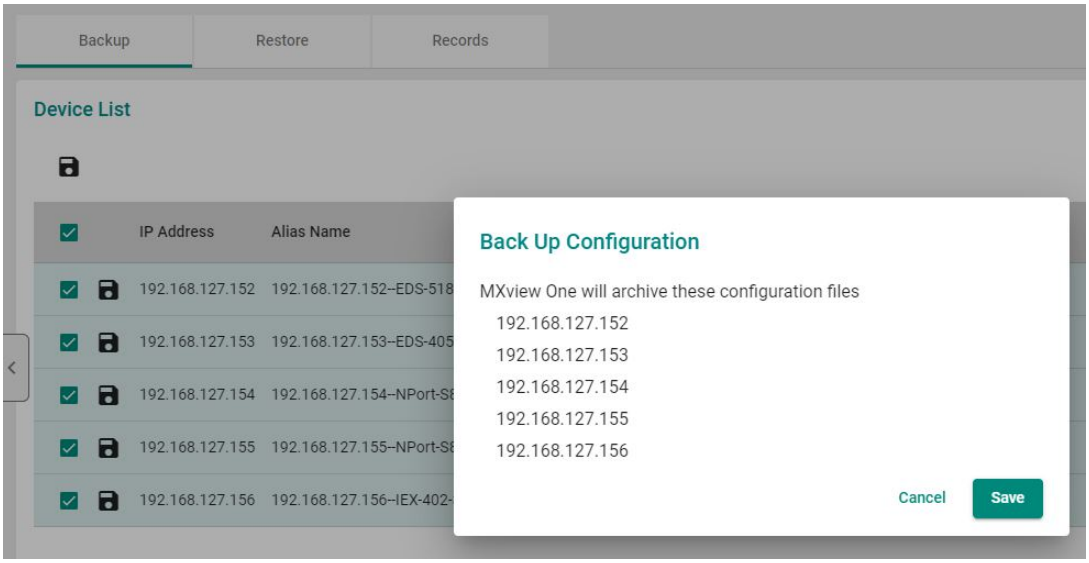
3. (Optional) Filter the devices in the **Device List**:
   a. Click the **Filter** ( ) icon.
   b. Specify any of the following criteria:
      - ❒ **Group:** The group in the MXview One tree structure that the device is assigned to
      - ❒ **IP Address:** The IP address of the device
   c. Click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



   MXview One exports the 'All available devices' list as a CSV file.

5. To back up configurations from specific devices:
   a. Select the check box next to the device(s) you want to back up.
   b. Click the **Backup** (💾) icon in either of the following locations:
      - ❒ For a single device, click the **Backup** (💾) next to the selected device.
      - ❒ For multiple devices, click the **Backup** (💾) icon in the upper left corner of the screen.

      The **Backup Configuration** screen appears.



   c. Click **Save**.

      MXview One archives configuration files from selected device(s) to the MXview One server and displays them in the **Records** tab. Also, MXview One will export configurations from the selected device(s) as a ZIP file.

      For more information, please see the following topics:

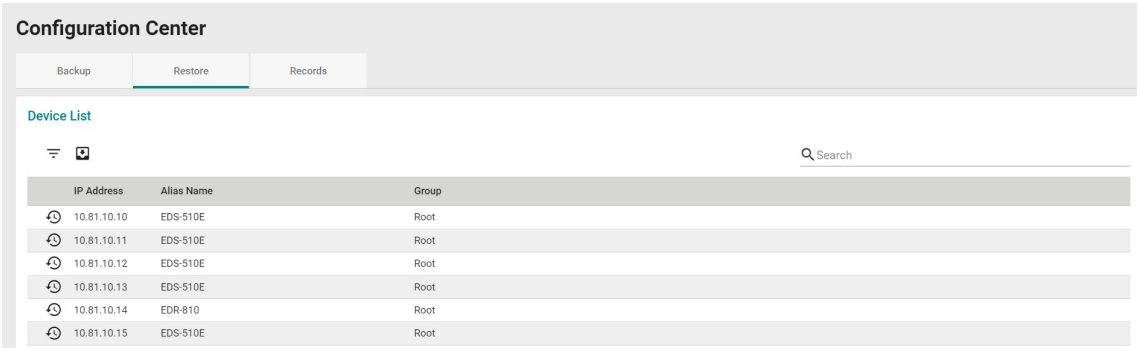
      Comparing Archived Configuration Files

> **NOTE**
>
> If MXview One compares two configuration files and they are the same, it will only leave the latest one. If the two configuration files are different, MXview One will keep both in the **Records** tab.

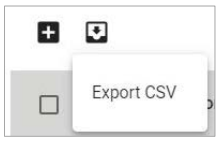
Restoring Device Configurations

Use the **Configuration Center** screen to restore configurations to one or more devices by restoring an archived configuration from the MXview One server or importing a local configuration backup file (in INI format).

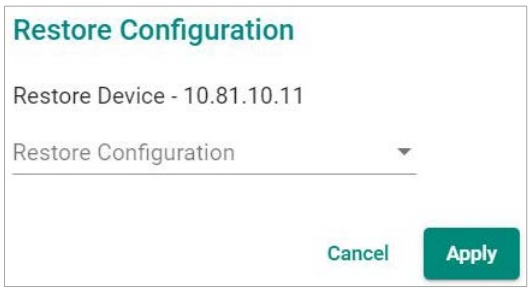
1. Navigate to **Menu** ( ) **> Device Configuration Center**.
   The **Device Configuration Center** screen will appear.
2. Click the **Restore** tab.
   Available devices will appear in the **Device List**.



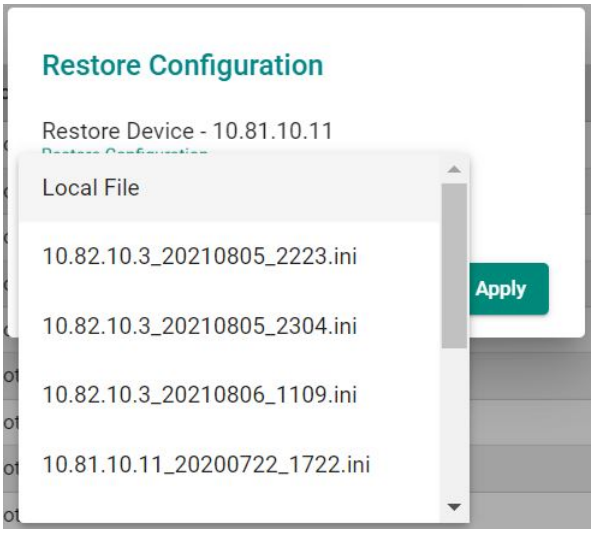
3. (Optional) Filter the devices in the **Device List**:
   a. Click the **Filter** ( ) icon.
   b. Specify any of the following criteria:
      - **Group:** The group that the device is assigned to
      - **IP Address:** The IP address of the device
   c. Click **Apply**.
      MXview One filters the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



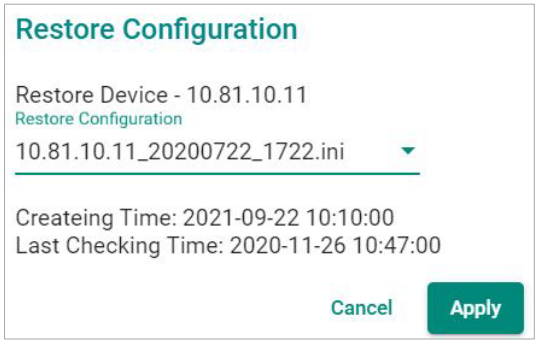
   b. Select **Export CSV**.
      MXview One exports the 'All available devices' list as a CSV file.
5. To restore an archived configuration file to a device:
   a. Click the **Restore** ( ) icon next to the **IP Address** of a device in the **Device List**.
      The **Restore Configuration** screen will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



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



c. Click **Apply**.

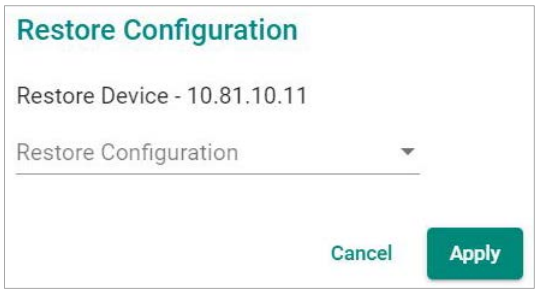


MXview One imports the configuration file to the selected device.

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

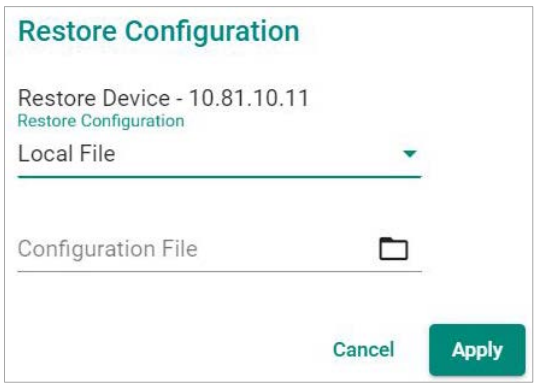
a. Click the **Restore** (⟲) icon next to the **IP Address** of a device in the **Device List**.

The **Restore Configuration** screen appears.



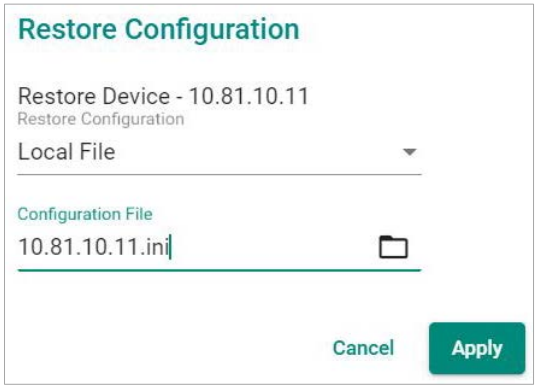
b. From the **Restore Configuration** drop-down list, select **Local File**.

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



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

e. Click **Apply**.

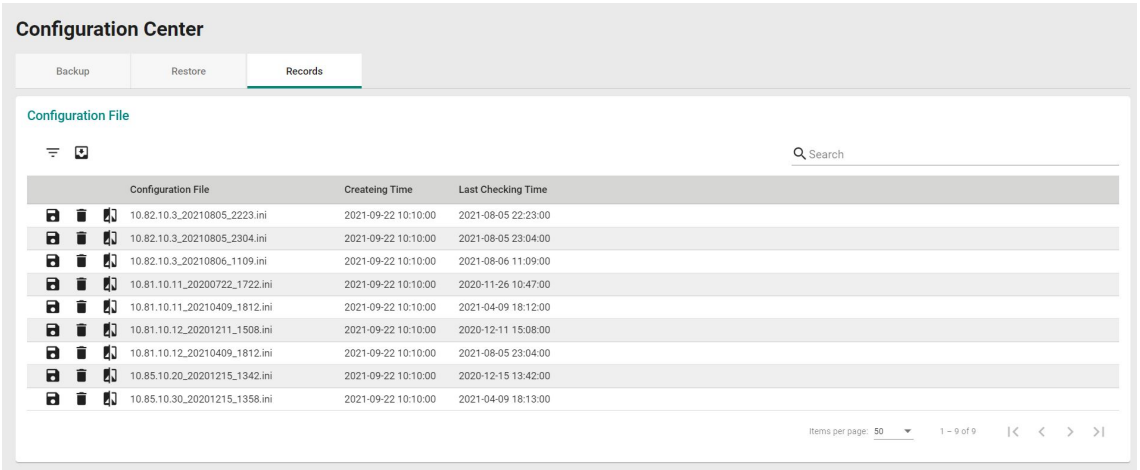


MXview One imports the configuration file to the selected device.

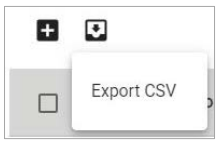
Comparing Archived Configuration Files

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

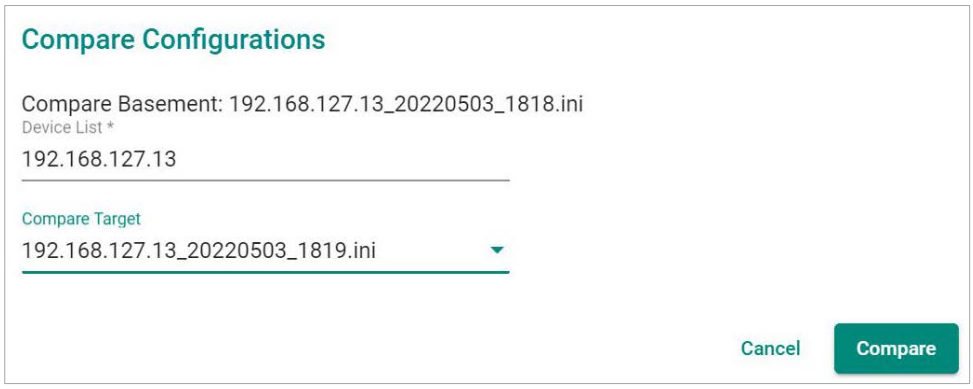
1. Navigate to **Menu** ( ) **> Device Configuration Center**.
   The **Device Configuration Center** screen appears.
2. Click the **Records** tab.
   A list of archived backup configuration files appears.



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



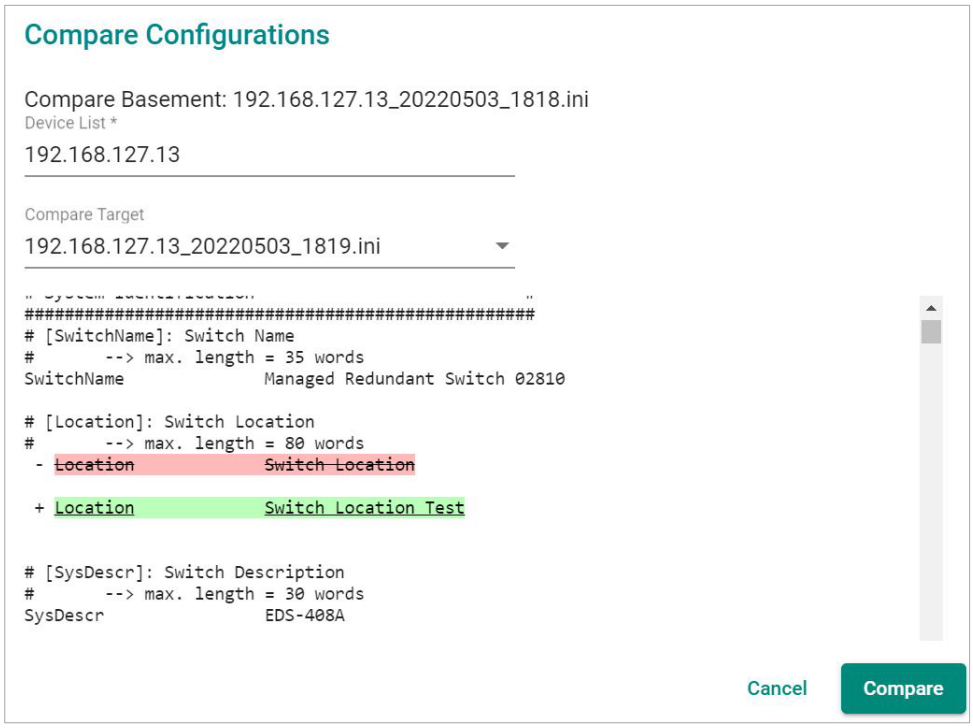
   b. Select **Export CSV**.
      MXview One exports all the devices information as a CSV file.
5. Click the **Compare** ( ) icon next to the configuration file you want to compare.
   The **Compare Configurations** screen will appear.



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 One will display a comparison of the selected configuration files.



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

> **NOTE**
>
> The green lines are the configurations of Compare Target. The red lines are the configurations of Compare basement.

Creating Maintenance Scheduler for Database/Configuration Backups

Use the **Maintenance Scheduler** to automatically export/import device configurations or back up the MXview One database on a predefined schedule.

1. Navigate to **Menu** ( ) **> Administration > Maintenance Scheduler**.

   The **Maintenance Scheduler** screen appears.
2. (Optional) Search a previously saved scheduled job, type a job name in the search box.

   The **Maintenance Scheduler** table displays a list of matching scheduled jobs.
3. Click the **Add** ( ) button.

   The **Add 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 **Add**.

    MXview One will display the scheduled job on the **Maintenance Scheduler** table and will execute the job according to the defined schedule.

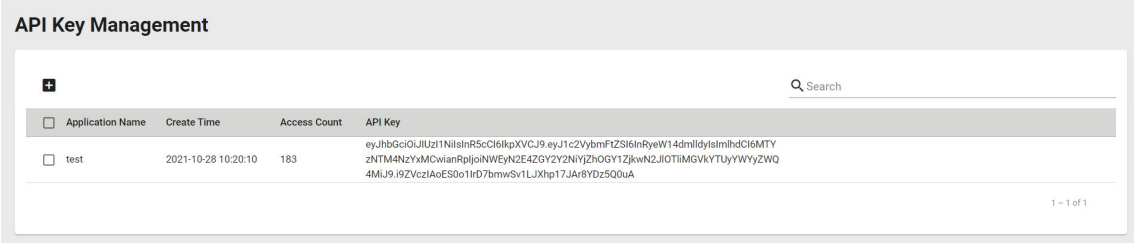
14. Custom Integrations

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

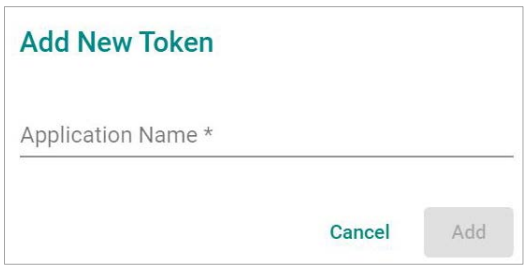
Managing RESTful API Keys

MXview One supports 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 > API Key Management**.
   The **API Key Management** screen will appear.



2. (Optional) Search the list of applications, type a string in the search box.
   MXview One filters the list of applications to display only the applications that contain full or partial matching strings.
3. To add a new API key for an application:
   a. Click the **Add** ( ) icon in the top left corner of the screen.
      The **Add New Token** screen will appear.



   b. Specify an **Application Name**.
   c. Click **Add**.
      MXview One will add the new application to the **API Key Management** screen and display the generated API key.
4. To regenerate an API key for an existing application:
   a. Select the check box next to the **Application Name**.
      The **Regenerate the API Key** ( ) icon will appear in the top left corner of the screen.

b. Click the **Regenerate the API Key** ( ) icon.

MXview One will regenerate the API key for the selected application.

NOTE

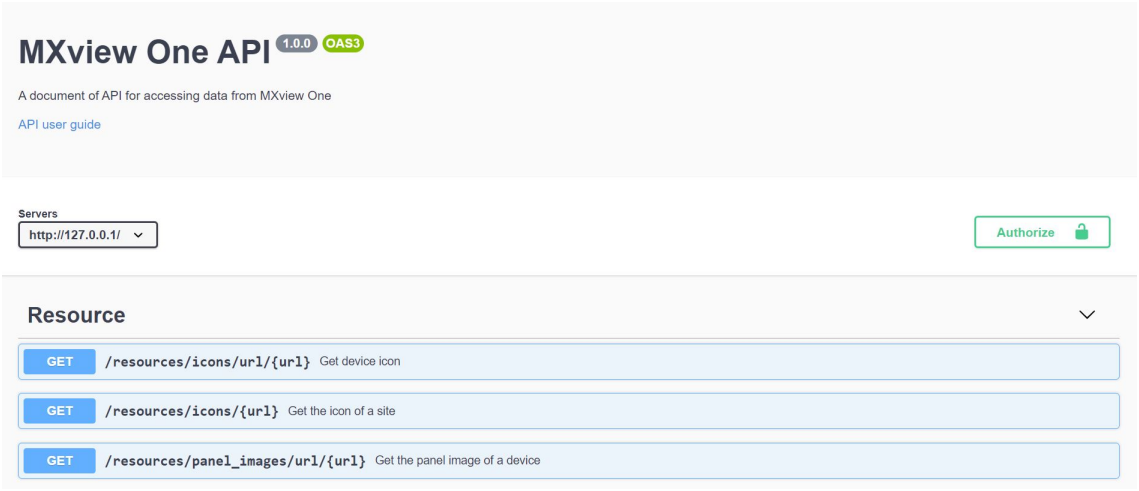
Regenerating the API key will prevent any APIs that use the old API key from working properly.

5. To delete an application:
   a. Select the check box next to the **Application Name**.
   b. Click the **Delete** ( ) icon in the top left corner of the screen.
   MXview One 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** ( ) **> Help > API Documentation**.
   The **MXview One API** screen will appear and display the reference document for supported MXview One APIs. Click **API user guide** below the MXview One API title, where you can find the guidelines for using the RESTful API functions.

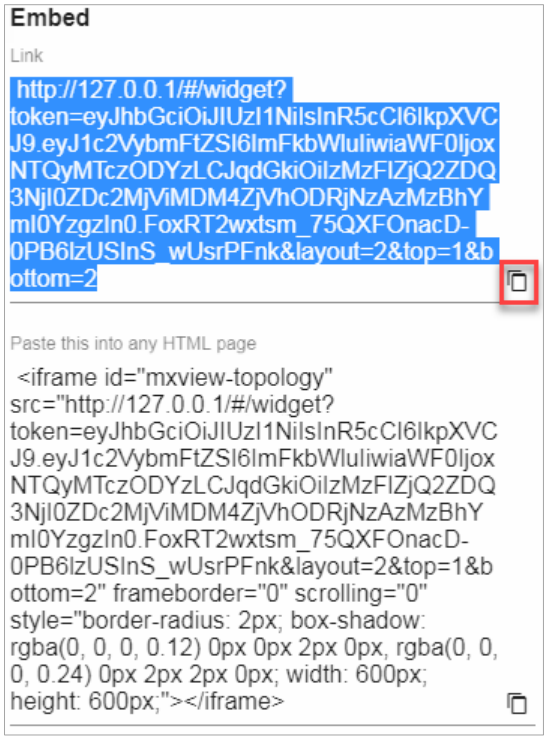


Embedding Web Widgets

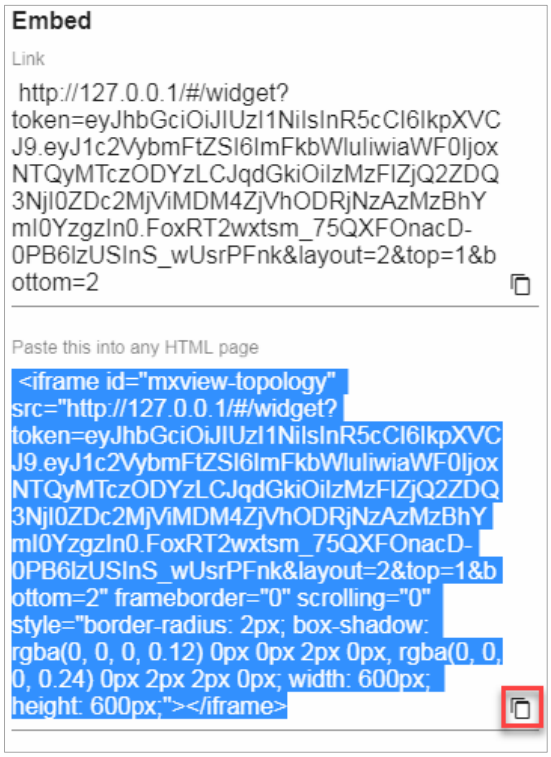
MXview One allows you to embed the Topology Map and Recent Events widgets from the MXview One **Topology** screen in third-party applications.

1. Navigate to **Menu** ( ) **> Integration > Embedded Web Widget**.
   The **Embedded Web 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.



15. Wireless Add-on Module

MXview One supports several optional modules that extend the functionality of the main module. These modules require a separate license to use.

Introduction

The MXview One Wireless Add-on Module provides a set of tools to help you monitor and troubleshoot your wireless network through MXview One and supports up to a total of 200 wireless APs and clients. The add-on gives you clear, real-time information about the status of your wireless network including the client roaming status and key wireless performance indicators such as SNR and noise level. The wireless module also instantly notifies you of any problems with your wireless devices and helps you narrow down the root cause of the problem, allowing for quick and easy troubleshooting.

System Requirements

The computer that the MXview One Wireless Add-on Module is installed on must satisfy the following system requirements based on the maximum capacity of 200 wireless APs and clients:

	System Requirements
CPU	2 GHz or faster dual core CPU
RAM	8 GB or higher
Hard Disk Space	20 to 30 GB for 1 month of performance and event history recording
OS	Windows 10 (64-bit) Windows 11 (64-bit) Windows Server 2016 (64-bit) Windows Server 2019 (64-bit)
Browser Requirements	Chrome: Version 76 or later Firefox: Version 69 or later Microsoft Edge: Version 79 or later

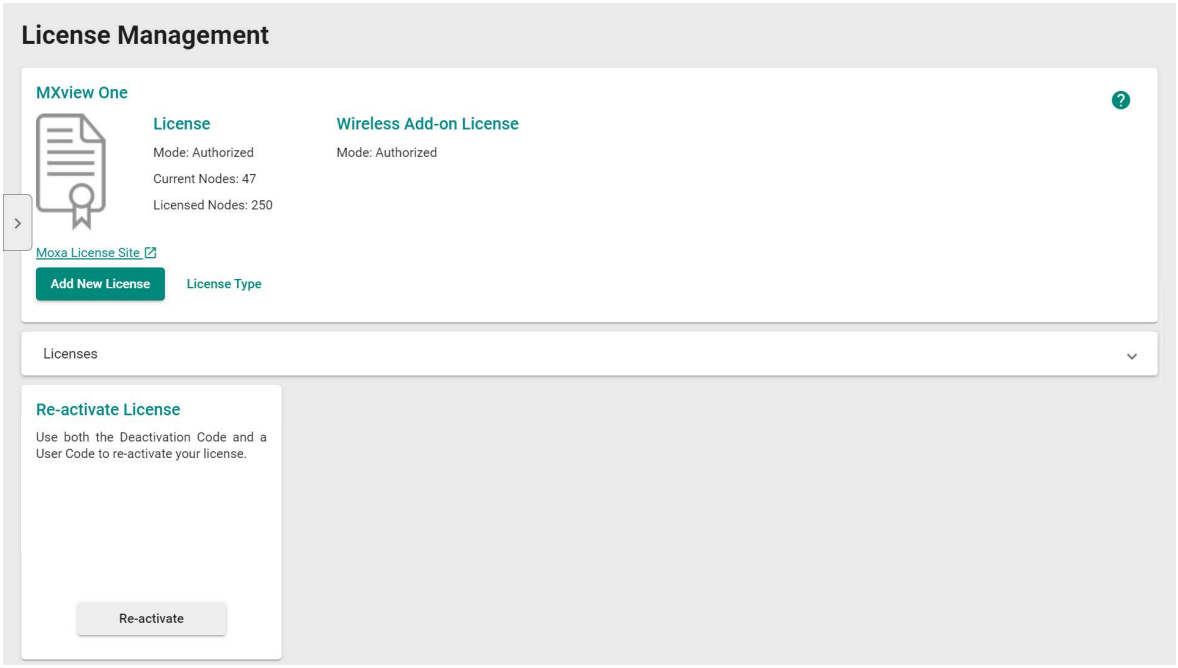
Supported Devices

The MXview One Wireless Add-on Module supports the following wireless devices:

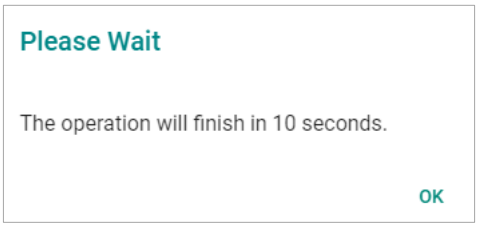
- AWK-3131A Series (firmware v1.16 or above)
- AWK-4131A Series (firmware v1.16 or above)
- AWK-1131A Series (firmware v1.22 or above)
- AWK-1137C Series (firmware v1.6 or above)

Getting Started With the Wireless Add-on Module

In order to use the MXview One Wireless Add-on module, you will need to activate it first. You can choose to activate a new license, or enable the wireless 60-Day free trial through the license management page.



The system will automatically restart after you activate the module. A message will appear telling you to wait 10 seconds while the module activates. Once done, click **OK** to refresh your browser and enable the Wireless Add-on features.



- For detailed information on how to activate the MXview One Wireless Add-on Module, refer to **License Management**.
- To add wireless devices to your MXview One network, refer to **Using Device Discovery**.

NOTE

Please activate the Node-based License first and then the Wireless Add-on License.

Wireless Module Features

The MXview One Wireless Add-on Module offers a set of features specifically designed to help you monitor and troubleshoot your wireless network more easily.

Main Dashboard

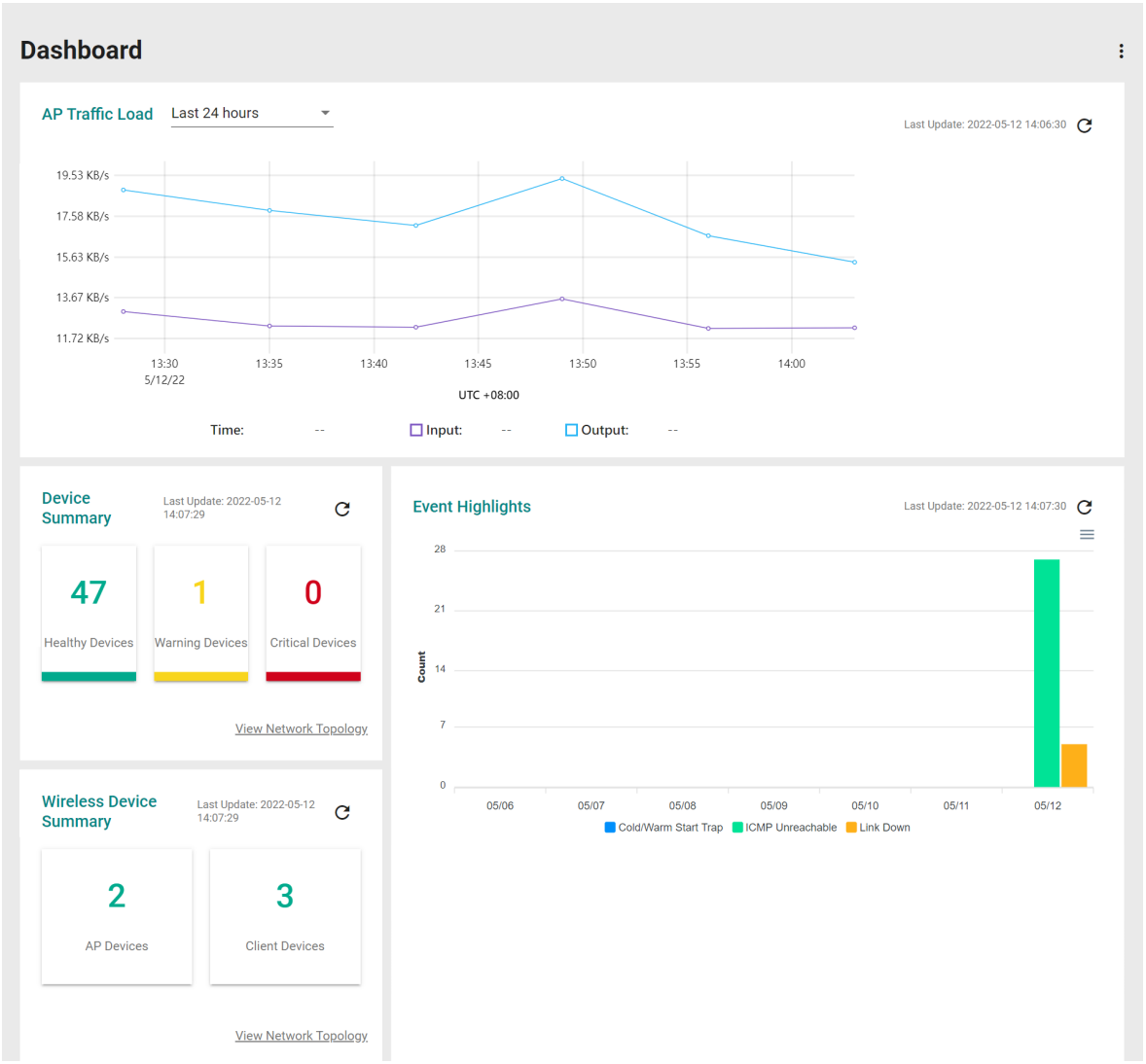
If the wireless module is activated, the MXview One Dashboard will show two additional types of information: AP Traffic load and the Wireless Device Summary.

The AP Traffic Load graph shows the aggregated traffic of all the AP devices monitored by MXview One. You can select a specific time to check the wireless network status at that time. MXview One provides three time sections: **Last 24 hours, Last week,** and **Last 2 weeks**.

The Wireless Device Summary shows the number of deployed wireless devices. Clicking one of the cards will direct you to the Wireless Device Summary screen where you can find more detailed information about the wireless devices. Refer to Chapter 5: **Dashboard Widgets** for more information about the other cards on the dashboard.

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

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



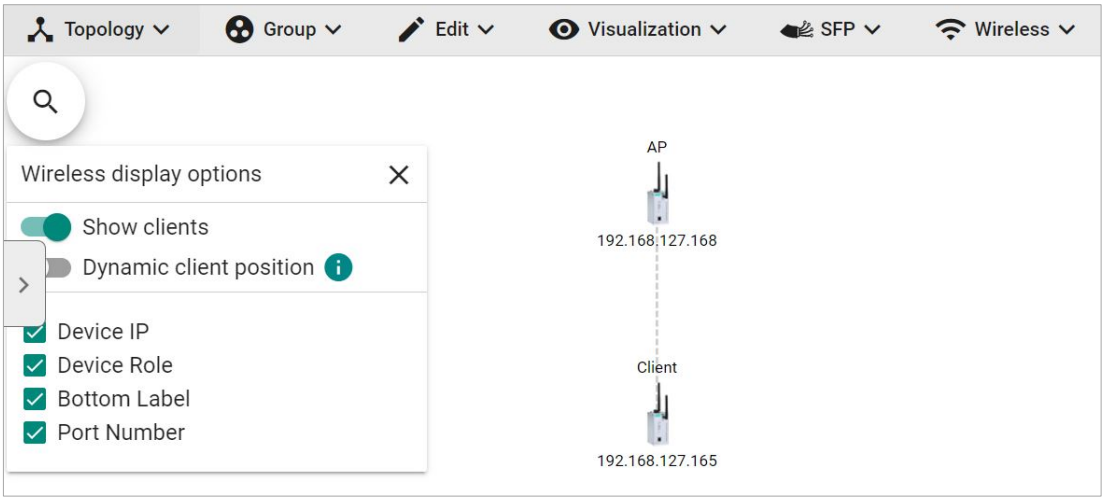
Dynamic Wireless Client Roaming

The MXview One Wireless Add-on Module features dynamic wireless roaming display, which updates roaming connections of wireless clients in real-time. Instead of using LLDP data to draw links between devices, MXview One uses both the client list data from the wireless AP and AP data from the wireless client to detect wireless roaming changes.

To enable the dynamic wireless client roaming function, toggle the **Dynamic client position** option. In this mode, wireless clients will automatically move below the AP they connect to when roaming. The link between the client and AP on the topology will also change dynamically if the client connects to another AP.

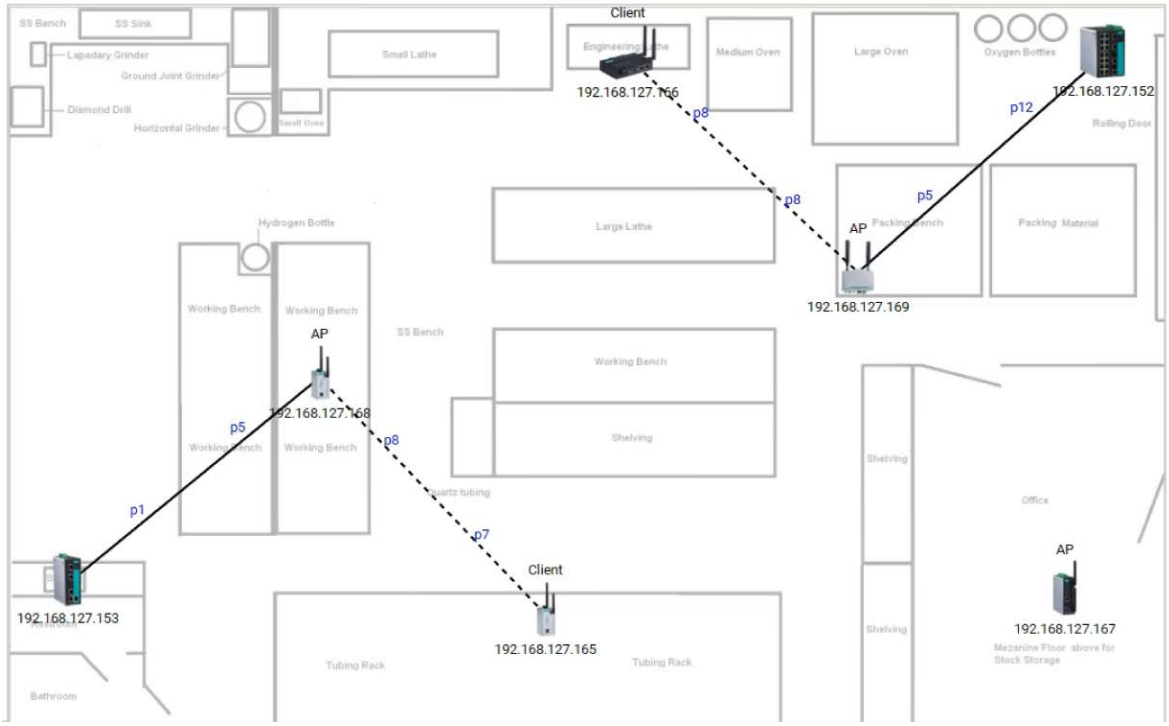
Refer to the table below for a description of each display option.

Option	Description
Show clients	Toggle this option on or off to show or hide wireless clients on the topology
Dynamic client position	Enable this option to have wireless clients move to a position close to the AP they are associated with Disabling this option will return the clients to their original position

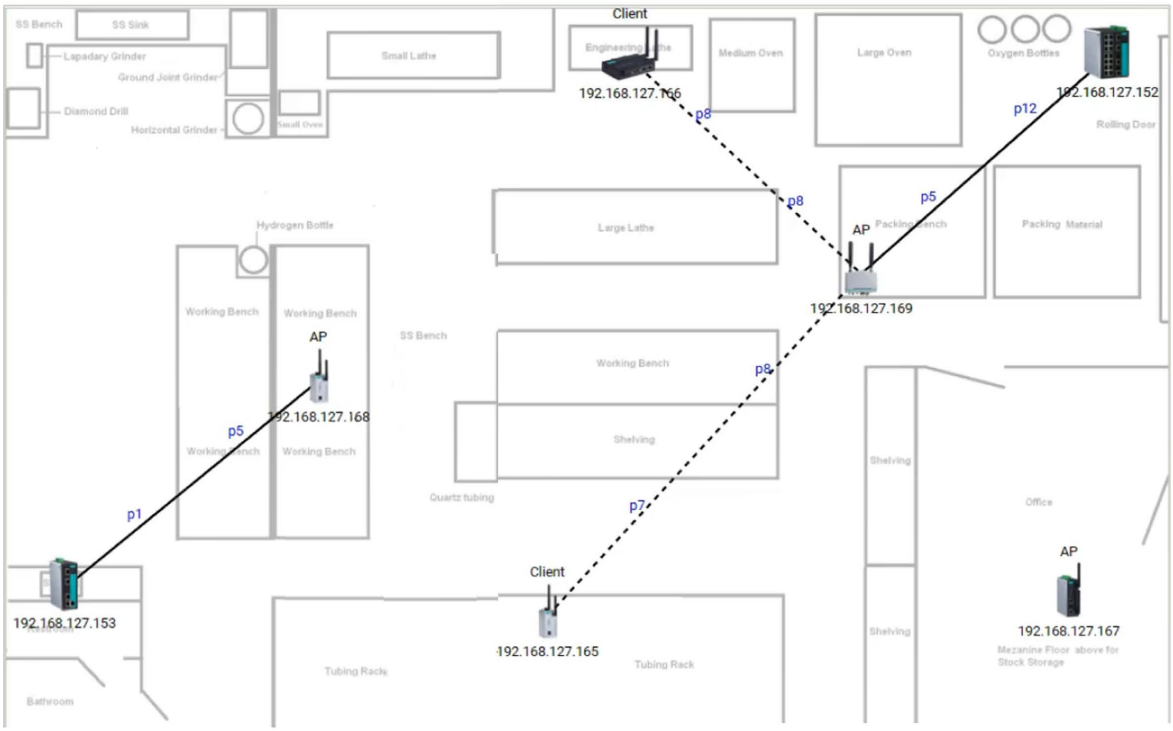


The following diagrams are an example of the dynamic roaming display showing dynamic client-AP link changes.

In the first scenario there are two wireless APs that each have one client connected to it.



When the client roams to another AP, MXview One will automatically redraw the link to the new AP on the wireless topology diagram.

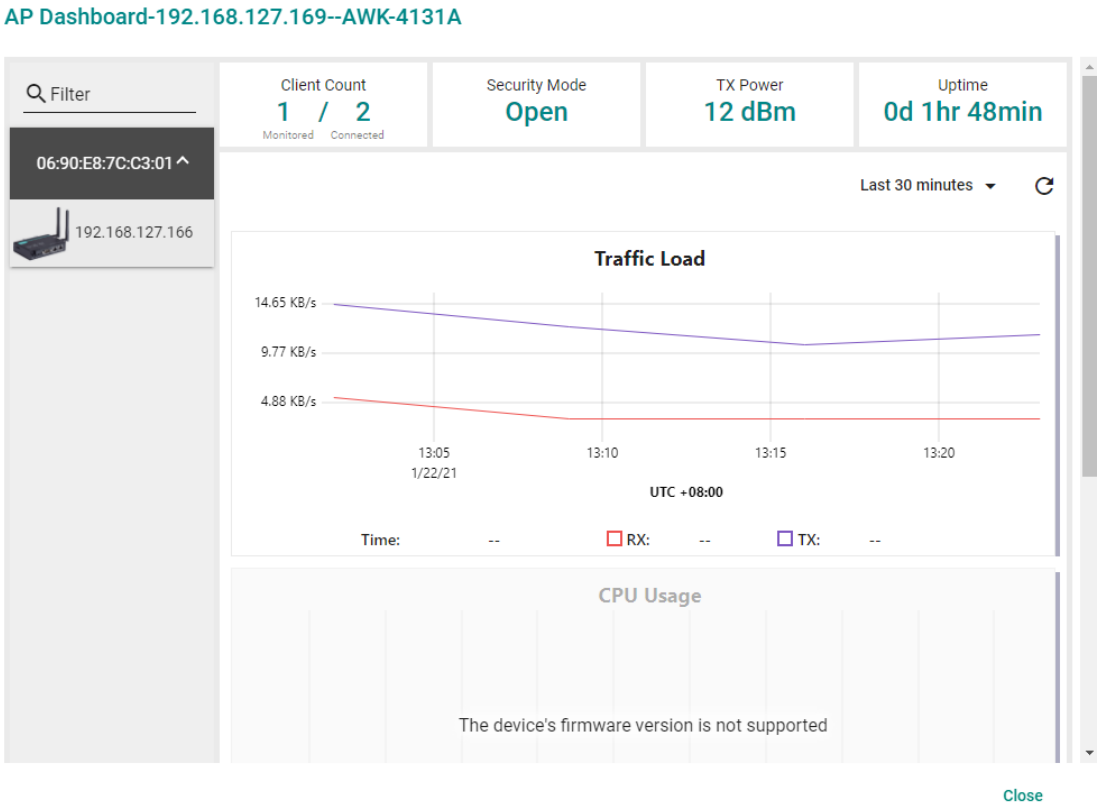


AP/Client Device Dashboard

Use the **AP/Client Device Dashboard** screens to see detailed information and performance statistics of the client or AP.

To access the AP/Client Device Dashboard, click on any wireless AP or client device's icon on the topology diagram and click **Device Dashboard** in the toolbar.

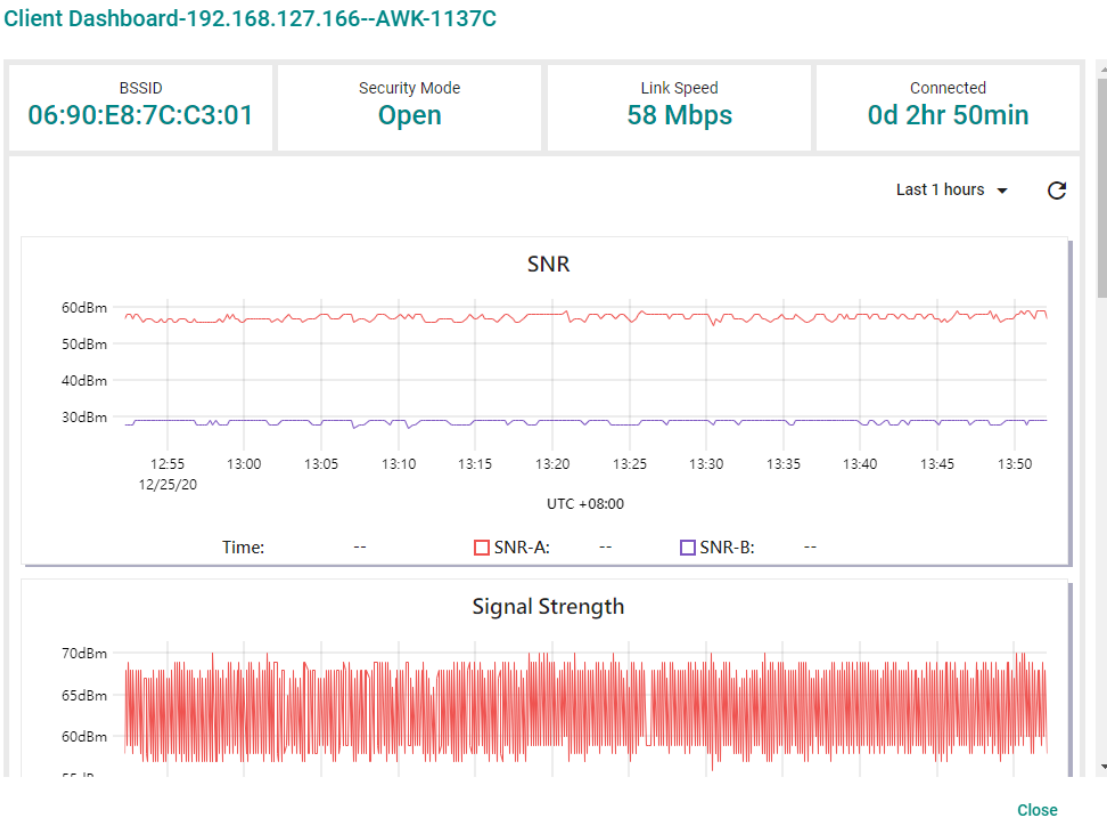
AP Device Dashboard



The AP Device Dashboard shows the following information:

Parameter	Description	
Client Count	Monitored	The total number of wireless clients connected to this AP that are monitored by MXview One
	Connected	The total number of wireless clients that are connected to this AP
Security Mode	The Security Mode of the AP: Open, WEP, WPA, or WPA2	
TX Power	The current transmission power of the AP	
Uptime	The total time the wireless AP has been online since the last restart	
Traffic Load	The current and historical traffic throughput of the wireless interface	
CPU Usage	The current and historical CPU usage of the AP (only supported by certain firmware versions)	
Memory Usage	The current and historical memory usage of the AP (only supported by certain firmware versions)	

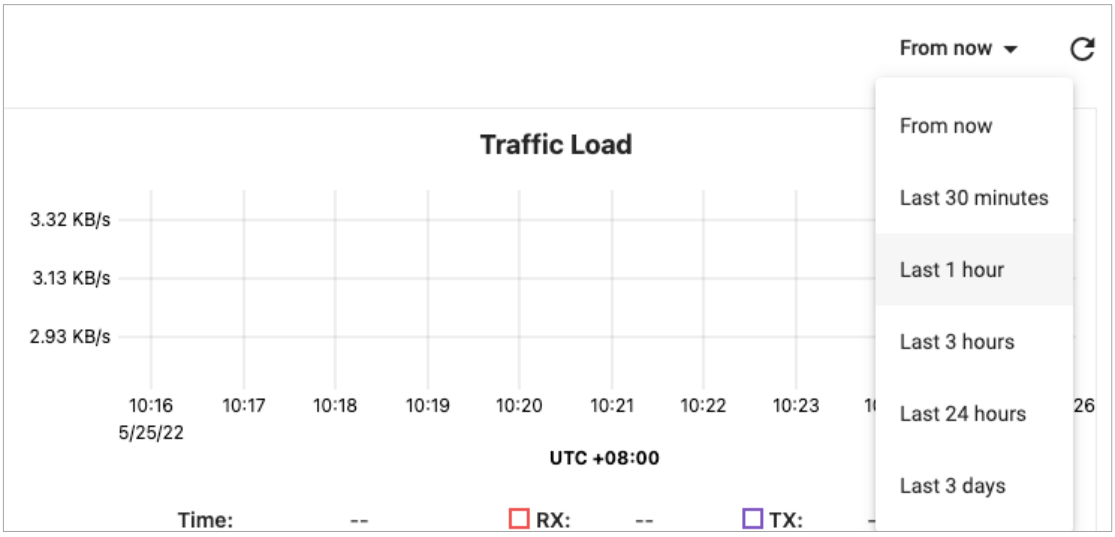
Client Device Dashboard



The Client Device Dashboard shows the following information:

Parameter	Description
BSSID	The BSSID of the wireless AP the client is connected to
Security Mode	The Security Mode of the client: Open, WEP, WPA, or WPA2
Link Speed	The real-time bandwidth of the connection to the AP
Connected	The total time the wireless client has been connected to the AP
SNR	The current and historical Signal-to-Noise ratio of the client If the wireless device has multiple antennas, the SNR of each antenna will be separately shown as SNR-A and SNR-B
Signal Strength	The current and historical signal strength of the client
Noise Floor	The current and historical noise floor of the client
Traffic Load	The current and historical traffic throughput of the wireless interface
CPU Usage	The current and historical CPU usage of the client (only supported by certain firmware versions)
Memory Usage	The current and historical memory usage of the client (only supported by certain firmware versions)

You can view the device diagnostics and usage parameters in real-time or recall the history for up to the last 3 days from the drop-down menu in the top-right. You can zoom in on the timeline to examine a narrower time period. Double-click the timeline to return to the original view.

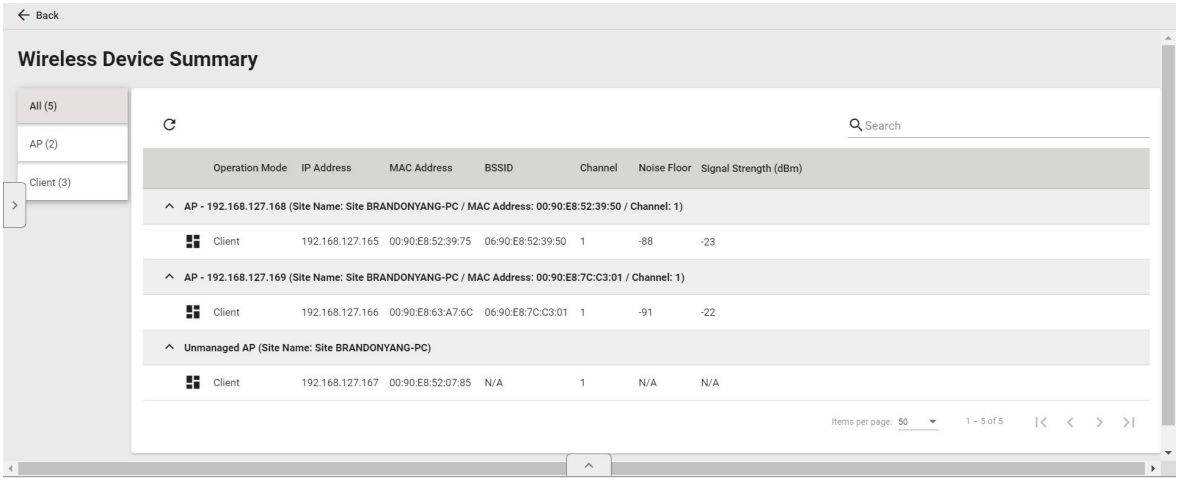


Wireless Device Summary

The Wireless Device Summary screen provides detailed information about all the AP and client devices including the device's IP and MAC address, operation mode, and current signal strength.

To access the Wireless Device Summary screen, expand the **Wireless** ( ) menu in the toolbar and click **Wireless Device Summary**.

Click **Back** in the top-left corner to return to the topology view.

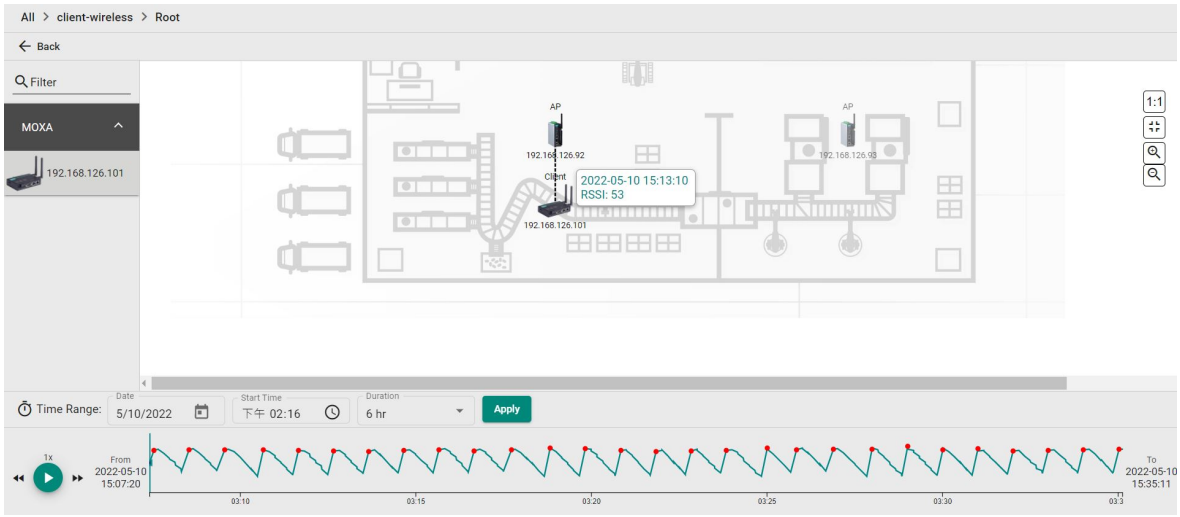


Wireless Roaming Playback

Through the Wireless Roaming Playback screen, you can recall the roaming history of a specific client. By default, MXview One will keep the roaming playback data for 30 days.

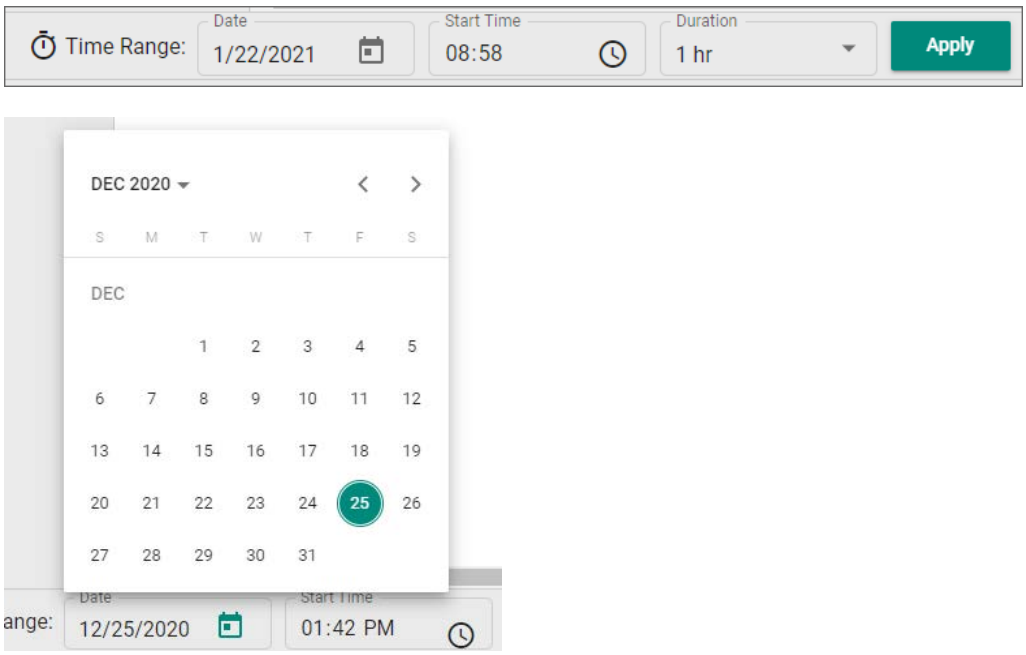
To access the Wireless Roaming Playback screen, expand the **Wireless** ( ) menu in the toolbar and click **Wireless Roaming Playback**.

Click **Back** in the top-left corner to return to the topology view.

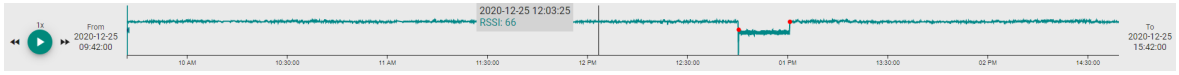


On the left-hand side is a list of wireless clients, in the center is the topology map, and located at the bottom is the playback progress bar. Select any client from the list and click **Play** ( ) to start playing the wireless roaming history for the selected time range. You can adjust the playback speed by clicking the **Decrease Speed** ( ) or **Increase Speed** ( ) button to increase or decrease the playback speed respectively.

To view the history for a specific time and date, click ( ) to choose the starting date, set the time in the Start Time field, select the duration of the playback history from the Duration drop-down menu, and click **Apply**.



The progress bar also displays the RSSI value at the time. In addition, the red dots indicate the time when the wireless client roamed to a different AP. You can zoom in on the timeline to examine a narrower time period. Click **Apply** to return to the original view.



16. Power Add-on Module

MXview One supports several optional modules that extend the functionality of the main module. These modules require a separate license to use.

Introduction

The MXview Power Add-on Module provides a set of features to help you monitor and troubleshoot your power substation network that follows the IEC 61850 standard and supports switches that have the PRP/HSR function with deep visualization. To monitor the IED (Intelligent Electronic Device), which is an important device that can receive data and issue commands on the network, MXview Power supports the MMS protocol to view and provide the status of the IED. Furthermore, there is a critical packet called GOOSE in power substation networks, and MXview Power can also help customers troubleshoot GOOSE events such as GOOSE Timeout and GOOSE Tampered. The power module instantly notifies you of any problems with your power devices and helps you narrow down the root cause of the problem, allowing for quick and easy troubleshooting.

System Requirements

The computer that the MXview Power Add-on Module is installed on must satisfy the same system requirements as those required for MXview One. See **System Requirements** in Chapter 1 for more information.

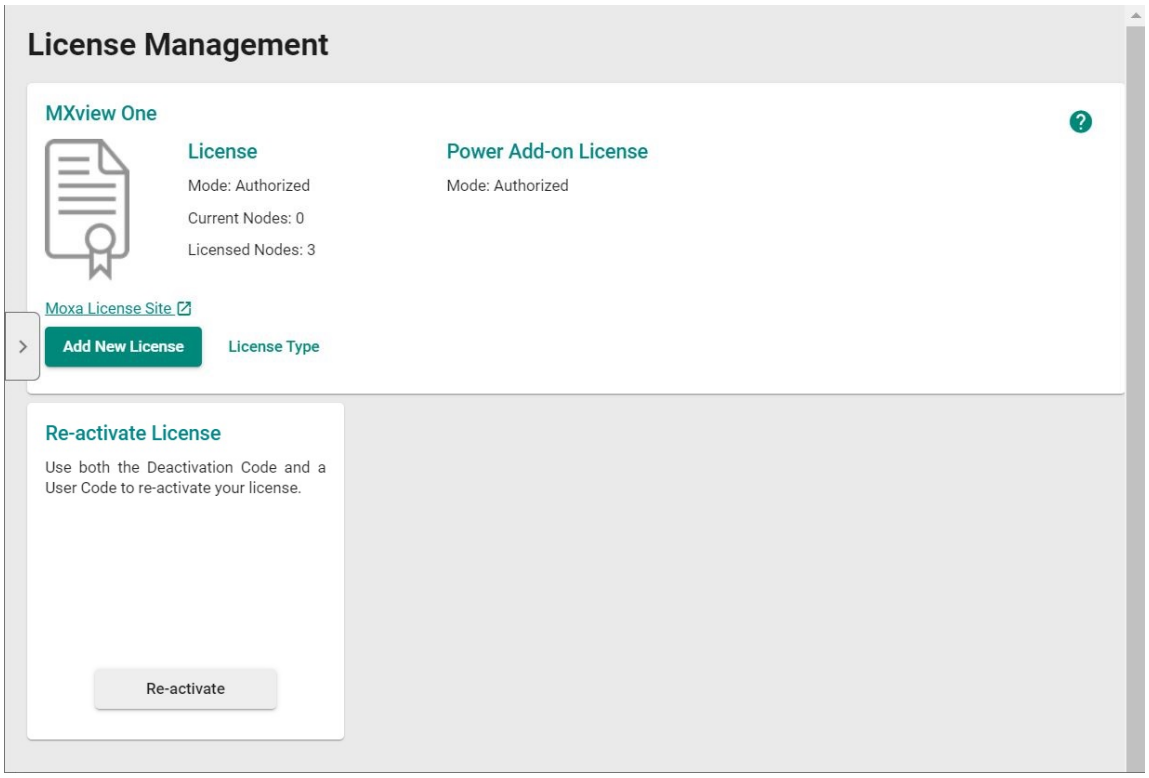
Supported Devices With PRP/HSR Features

PRP/HSR features can be visualized with the devices that support PRP/HSR functions or have a PRP/HSR module.

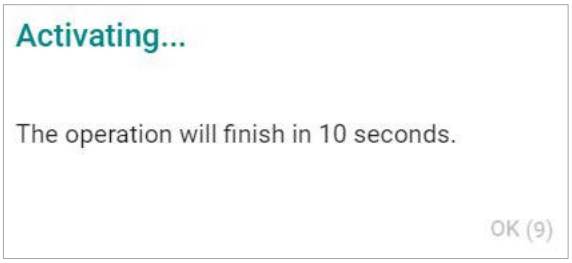
- PT-G503 Series (firmware v5.1 or above)
- PT-G7728 Series and LM-7000H-2GPHR module (firmware v6.2 or above)
- DA-820C Series and DN-PRP-HSR-I210 or DA-PRP-HSR-I210 (OS Win 10 or above)

Getting Started With the Power Add-on Module

In order to use the MXview Power Add-on module, you will need to activate it first. You can choose to activate a new license or enable the Power 60-day free version through the License Management page.



The system will automatically restart after you activate the module. A message will appear telling you to wait 10 seconds while the module activates. Once done, click **OK** to refresh your browser and enable the Power Add-on features.



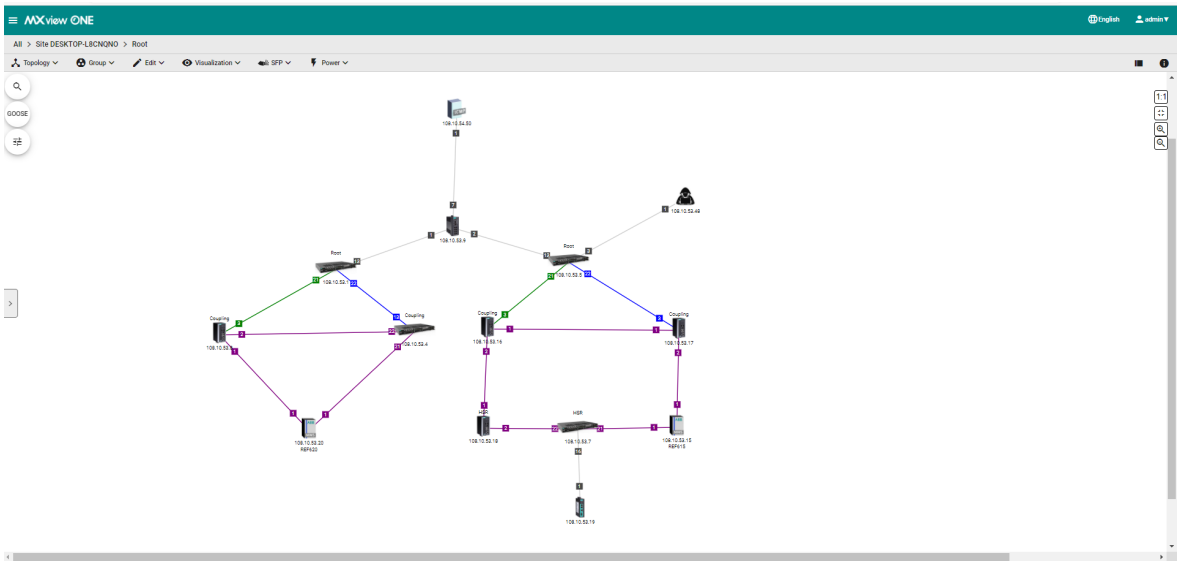
- For detailed information on how to activate the MXview Power Add-on Module, refer to **Chapter 4: License Management**.
- To add power devices to your MXview One network, refer to **Using Device Discovery**.

NOTE

Please activate the Node-based License and then the Power Add-on License.

Power Module Features

The MXview Power Add-on Module offers a set of features specifically designed to help you monitor and troubleshoot your power substation network more easily.



Topology

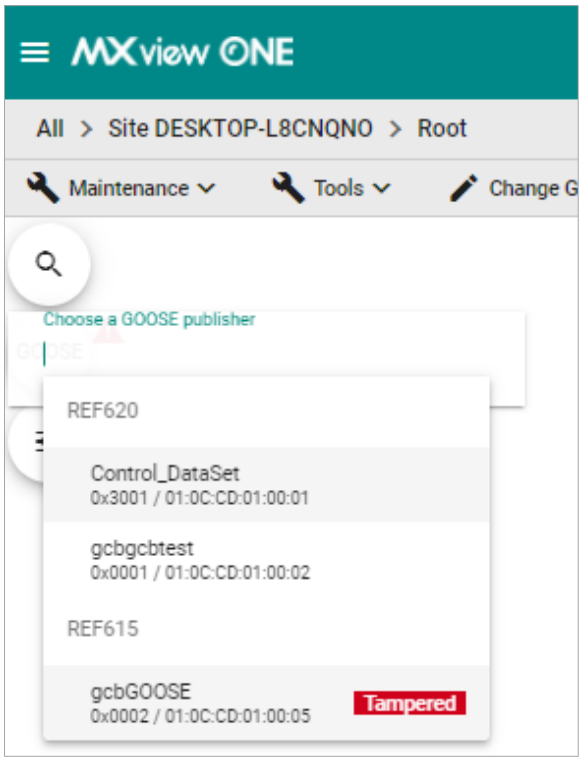
After you enable the MXview Power add-on module, you will see the panel has changed on the left hand-side.

GOOSE panel

1. Before you import the SCD file, the GOOSE panel will be displayed in light gray. At this point, it has limited functionality.

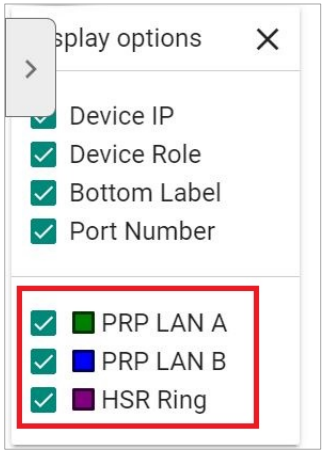
2. Once you have imported the SCD file via **Power > Import SCD**, you can find the IED as a GOOSE publisher identity via the GOOSE panel.
   a. Click **GOOSE panel**.

b. Scroll down or type the GOOSE-related information, such as IED name or GoCB name.



Display Options

1. Once you have activated the MXview Power add-on module, you can see the display options include extra functions such as PRP LAN A, PRP LAN B, and HSR Ring.
2. If the box is checked, you can see the color of the link for the PRP/HSR on the topology. If you uncheck the box, then the link will not display the color for the PRP/HSR function.



NOTE

PRP LAN A is represented by a green line, PRP LAN B by a blue line, and HSR Ring by a purple line.

NOTE

MXview One cannot guarantee that it can draw the link of the topology for non LLDP devices, such as an IED device. However, you can draw the link of the topology manually by clicking **Add Link**.

Import SCD

The SCD (Substation Configuration Description) file includes the information of the critical packet – GOOSE message in the network. To visualize the GOOSE message flow in MXview Power, the user has to import the SCD file.

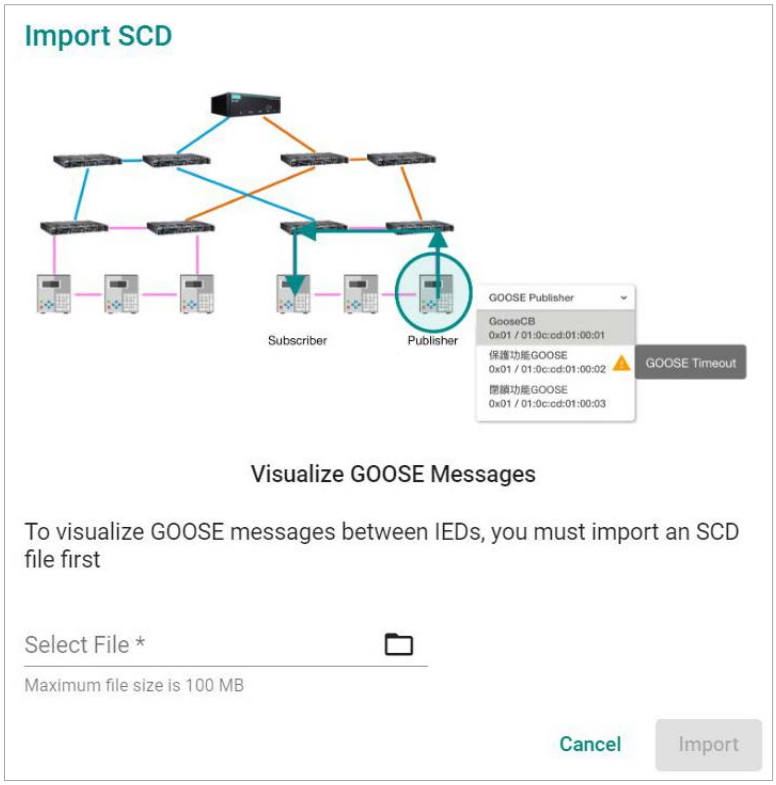
1. Navigate to **Menu** ( ) **> Topology**

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

2. To import the SCD file to the Topology Map:

   a. Click **Power > Import SCD**.

   The **Import SCD** screen will appear.

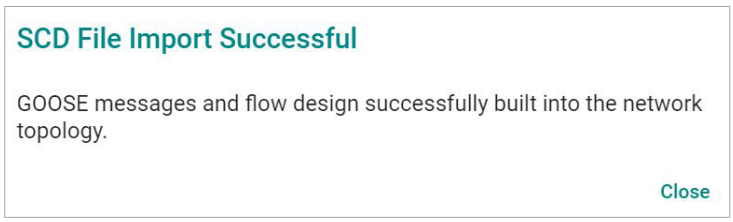


   b. Upload the SCD file by using one of the following methods:

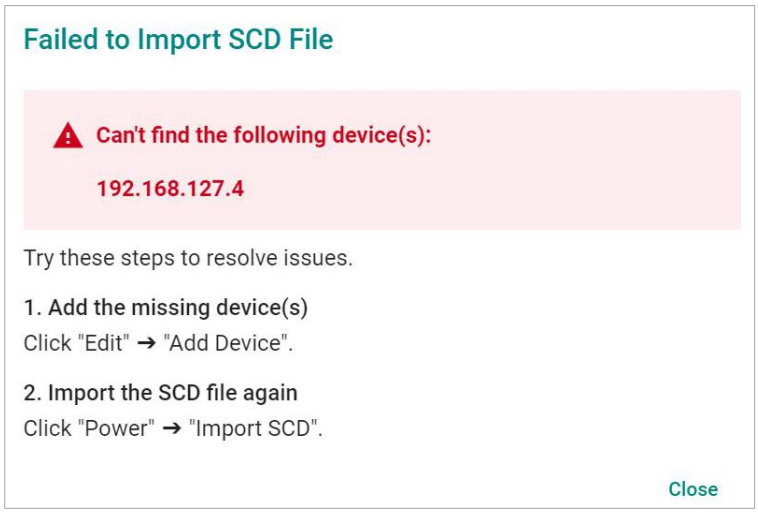
   - ❒ The file size must be less than 100 MB.
   - ❒ Click **File** ( ) icon to upload the SCD file.

3. Click **Import**.
4. MXview Power will import the uploaded SCD file into the Topology Map.

   If the SCD file is correct, the user will see the message below.



If the SCD file content cannot find the devices in the Topology, then MXview Power will display the missing devices and provide the steps for the user to resolve the problem.

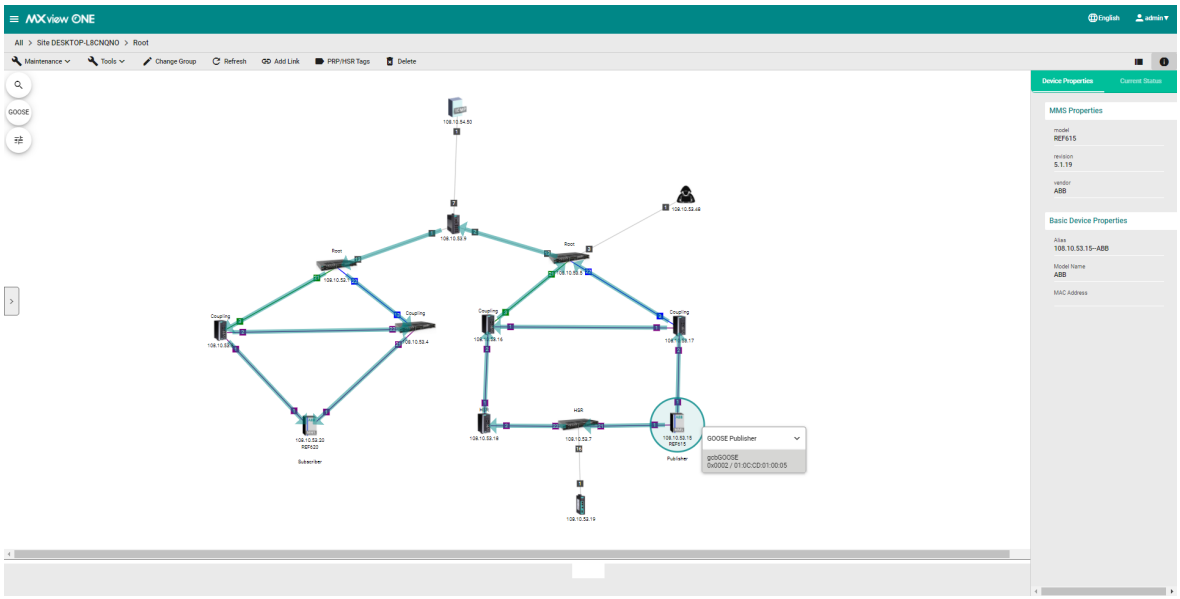


GOOSE Message

MXview Power can display the GOOSE Message information on the Topology or in the IED Device Property panel by importing the SCD file. Moxa's PT switch, which was specifically designed for use in power substation systems, can detect GOOSE events. MXview Power can collect the GOOSE events and alert users when there is something wrong. Users can follow the step-by-step guidelines to solve the GOOSE events.

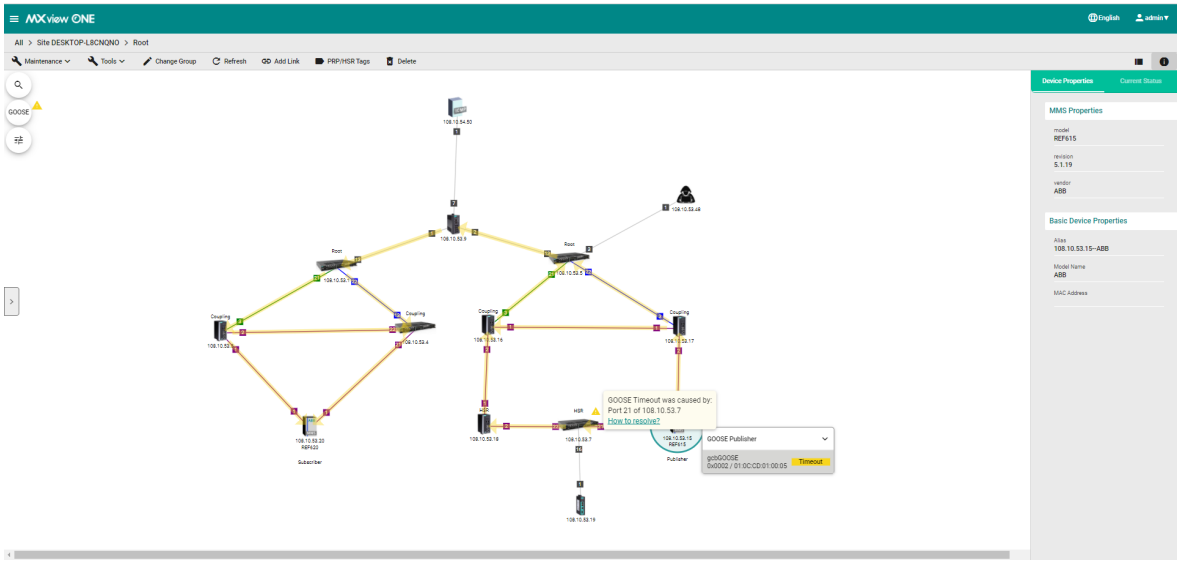
GOOSE Flow

There are two roles for IED device(s): Subscriber and Publisher. The topology displays the flow of the GOOSE packet, which starts from the Publisher and ends at the Subscriber. The route you see on the GOOSE flow is not the completed GOOSE packet publishing direction. The purpose of displaying the GOOSE flow is to troubleshoot the path of the GOOSE packet for certain cases such as a GOOSE event (e.g. GOOSE Timeout, GOOSE Tampered), a device malfunction, or a link going down. The GOOSE flow will show the path the packet took to enable faster troubleshooting and minimize substation network recovery times.

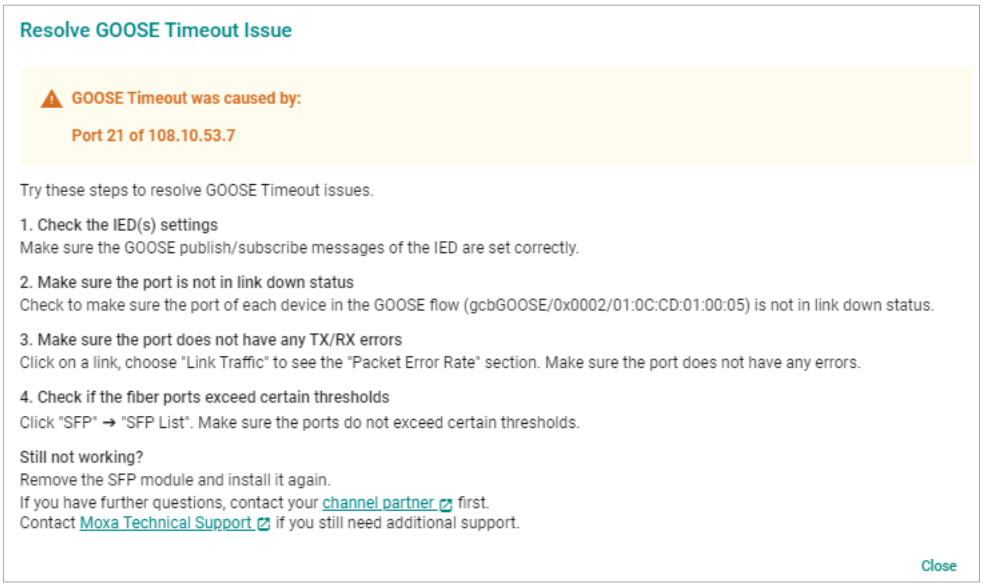


GOOSE Timeout

When a GOOSE Timeout event happens, MXview Power can display the event and indicate the possibly affected devices on the Topology by placing a yellow triangle next to them. When users click on the IED device, it will display the specific GOOSE message and will also include a Timeout status notification.



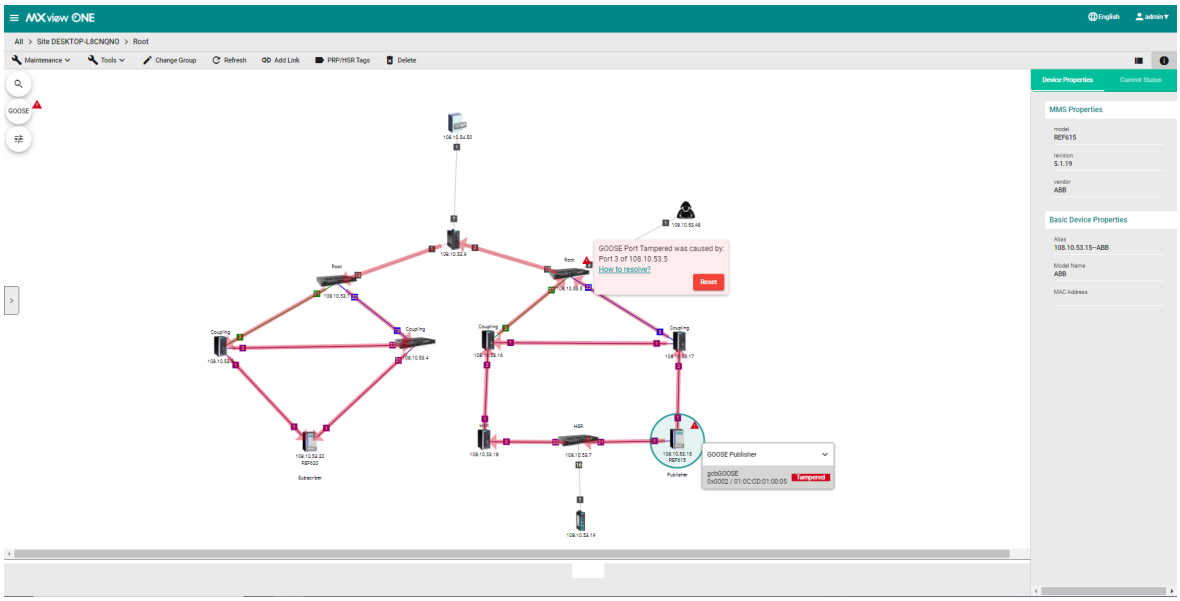
Click the **How to resolve** link and MXview Power will provide you with step-by-step instructions to solve the problem.



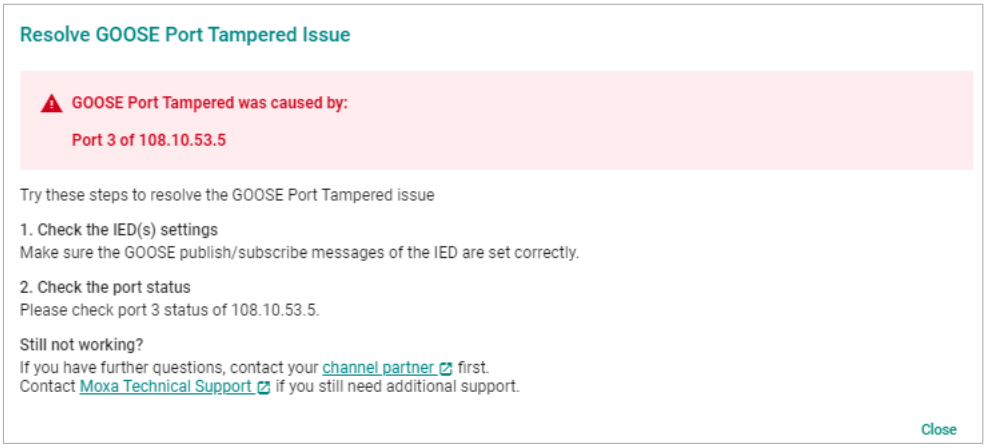
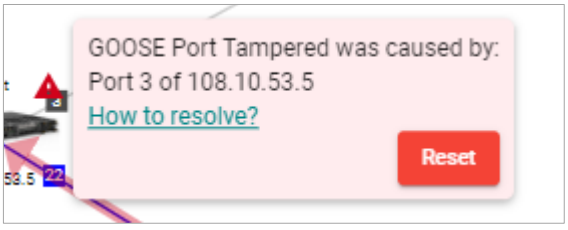
Once the problem is solved, MXview Power will provide the recovery status in the Recent Event panel and the yellow triangle will disappear.

GOOSE Tampered

When a GOOSE Tampered event happens, MXview Power can display the event and provide the possibly affected devices on the Topology by placing a red triangle next to them. When users click on the IED device, it will display the specific GOOSE message and will also include a Tampered status notification.



Click the **How to resolve** link and MXview Power will provide you with step-by-step instructions to solve the problem.



In order to enhance security, MXview Power allows users to click the **Reset** button to clear the events log for the devices. Once the event logs are cleared, MXview Power will provide the recovery status in the Recent Event panel and the red triangle will disappear.