MXview One 1.3.0 User Manual

Version 4.0, January 2024

www.moxa.com/products

MXview One 1.3.0 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

Trademarks

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

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	Quad-core CPU or better
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, Ubuntu 22.04 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

For Ubuntu 20.04 installation instructions, please refer to the Readme.txt included in the MXview One Linux software package, which can be downloaded from the Moxa website.

There are two ways to install MXview One on **Ubuntu 20.04**: offline and online installation. We recommend installing MXview One using the **offline method first** to avoid any compatibility issues.

If you are unable to activate MXview One using the online installation method, install the software using the offline method.

For Ubuntu 18.04 and 22.04

For Ubuntu 18.04 and 22.04 installation instructions, please refer to the Readme.txt included in the MXview One Linux software package, which can be downloaded from the Moxa website.

MXview One can only be installed on **Ubuntu 18.04 and 22.04** using the online installation method.

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
```

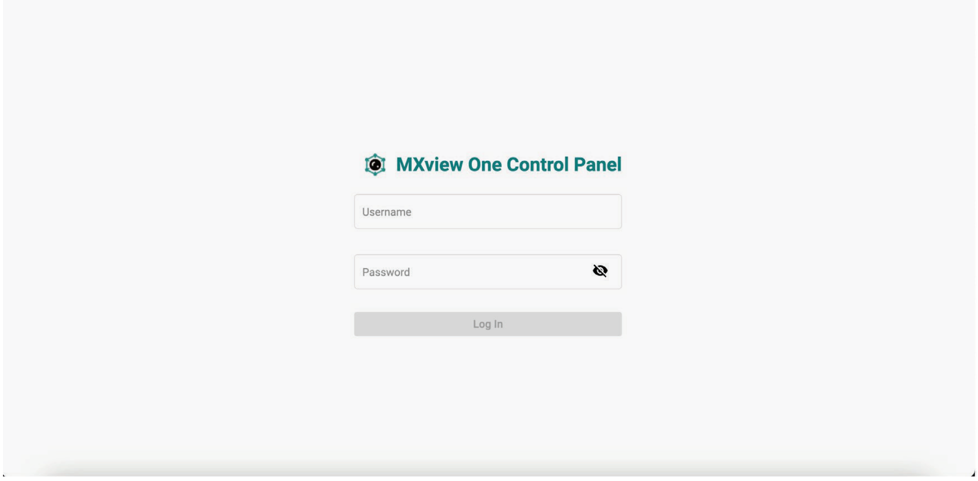
3. Getting Started

MXview One Control Panel

Server Control

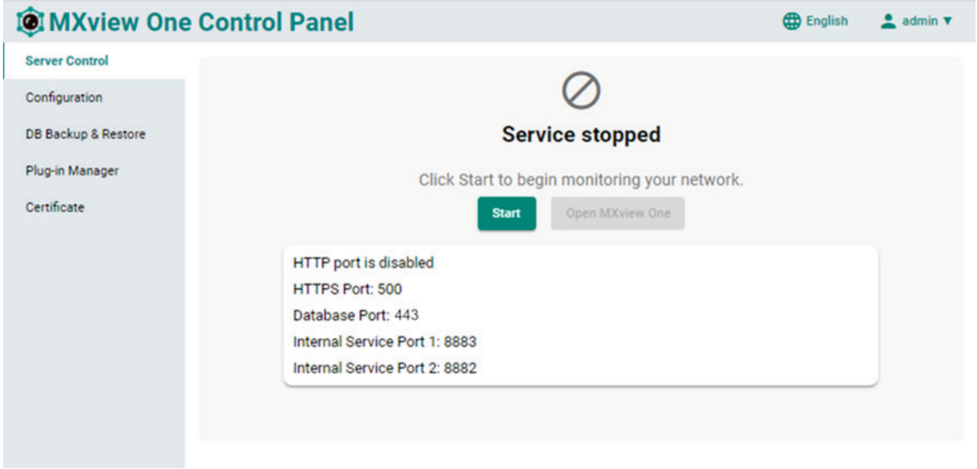
Start the MXview One server on the computer before launching the MXview One web console. On the server computer, double-click the MXview One desktop shortcut in the Windows operating system. For Ubuntu users, type in the local host IP address to open the page.

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**.

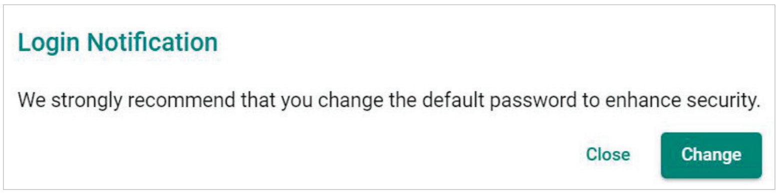


Service stopped

Click Start to begin monitoring your network.

HTTP port is disabled
HTTPS Port: 500
Database Port: 443
Internal Service Port 1: 8883
Internal Service Port 2: 8882

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

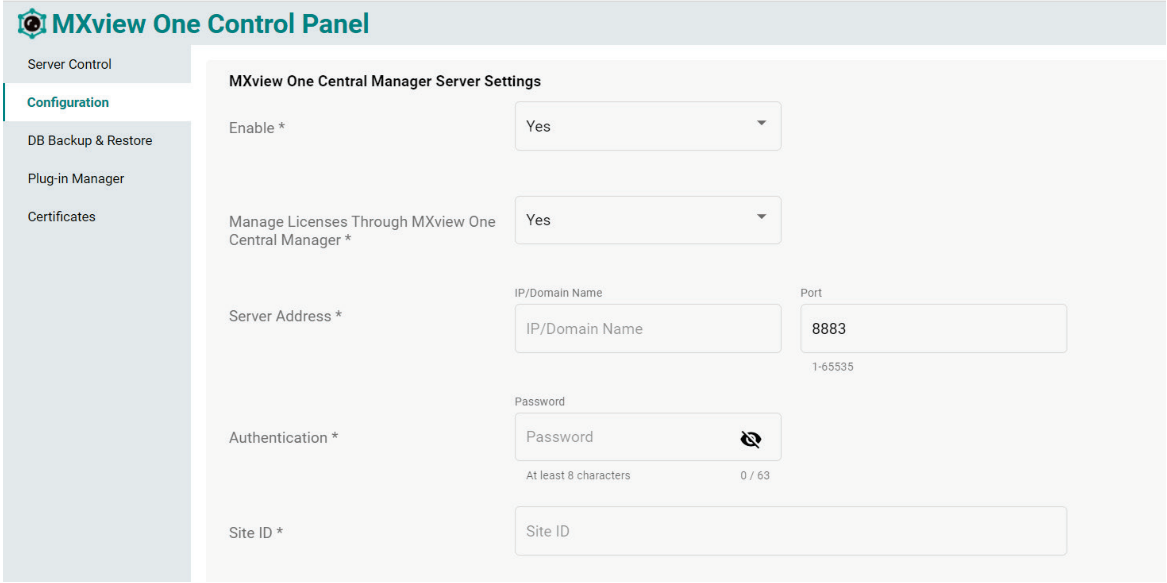


Login Notification

We strongly recommend that you change the default password to enhance security.

Configuration

Configure the following port numbers in the **Configuration** Page:



MXview One Control Panel

MXview One Central Manager Server Settings

Enable * : Yes

Manage Licenses Through MXview One Central Manager * : Yes

Server Address * : IP/Domain Name: IP/Domain Name; Port: 8883 (1-65535)

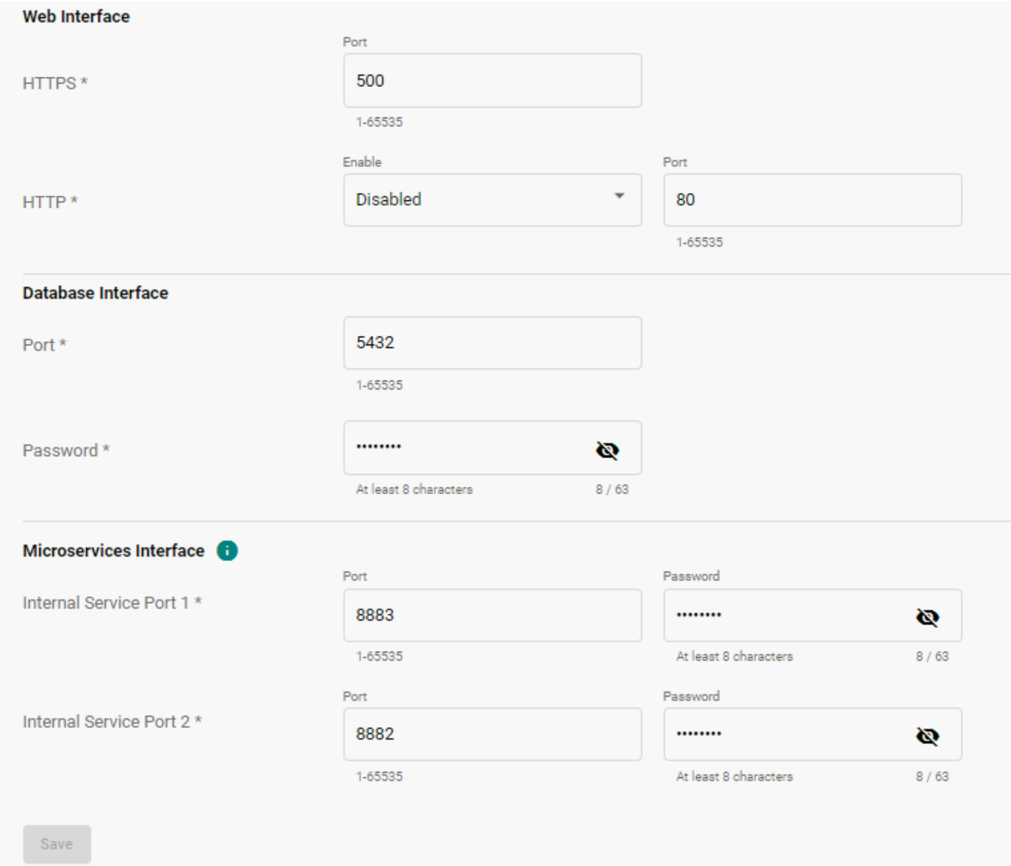
Authentication * : Password: Password (At least 8 characters, 0 / 63)

Site ID * : Site ID

MXview One Central Manager Server Settings

- **Enable**
  - **Yes:** This MXview One site will be managed through MXview One Central Manager. This requires the below MXview One Central Manager settings to be configured.
  - **No:** The MXview One site operates independently and cannot be managed through MXview One Central Manager.
- **Manage Licenses through MXview One Central Manager**
  - **Yes:** All the licenses of this MXview One site will be managed through MXview One Central Manager.
  - **No:** The licenses for this site are managed locally at the MXview One site.
- **Server Address**
  - **IP/Domain Name:** The IP address of MXview One Central Manager.
  - **Port:** The service port used to connect to MXview One Central Manager. The default port number is 8883.
- **Authentication**
  - **Password:** The password used to connect to MXview One Central Manager.
- **Site ID**
  - **Site ID:** This value represents the site ID as shown on the Site Management page in MXview One Central Manager.

Interface Settings



Web Interface

HTTPS * — Port: 500 (1-65535)

HTTP * — Enable: Disabled; Port: 80 (1-65535)

Database Interface

Port *: 5432 (1-65535)

Password *: •••••••• (At least 8 characters, 8 / 63)

Microservices Interface

Internal Service Port 1 * — Port: 8883 (1-65535); Password: •••••••• (At least 8 characters, 8 / 63)

Internal Service Port 2 * — Port: 8882 (1-65535); Password: •••••••• (At least 8 characters, 8 / 63)

Save

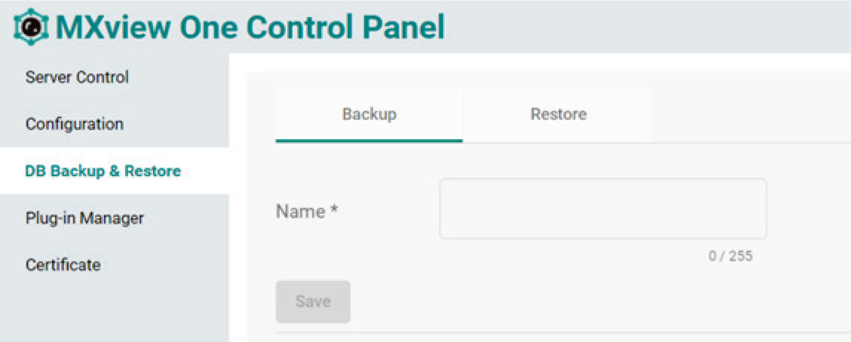
- **Web Interface**
  - **HTTPS:** Specify the HTTPS port of the MXview One Central Manager server. The default port is 443.
  - **HTTP:** Enable or disable HTTP. If enabled, specify the listening port of the server. The default port is 80.
- **Database Interface**
  - **Port:** Specify the service port of the MXview One Central Manager database server. The default port is 5432.
  - **Password:** The password used to connect to MXview One Central Manager.
- **Microservices Interface**
  - **Internal Service Port 1/2:**
    i. **Port:** Specify the communication ports between MXview One and its internal system. The default ports are 8883 and 8882.
    ii. **Password:** The password used for the microservices interface.

When finished, click **Save**.

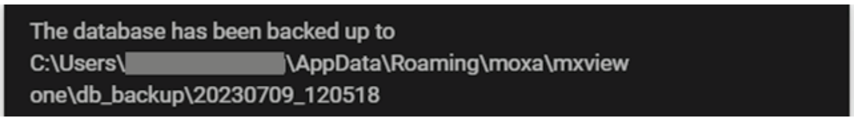
DB Backup & Restore

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.

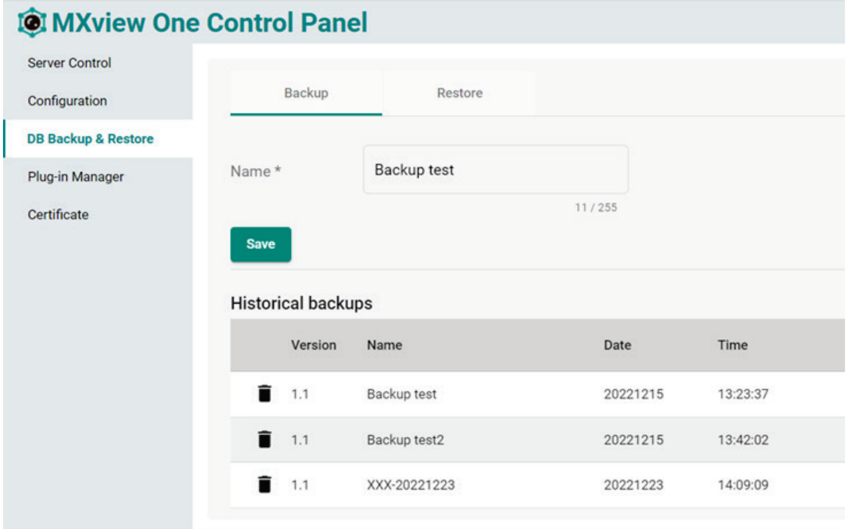


2. Choose the **Backup** tab to start the process of backing up the database.
3. In the **Name** field, specify the backup file name.
4. Click **Save**.
5. The message that the file of the backup database has been stored in the specified directory will be displayed.



The database has been backed up to C:\Users\[redacted]\AppData\Roaming\moxa\mxview one\db_backup\20230709_120518

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



Name * Backup test

11 / 255

Historical backups

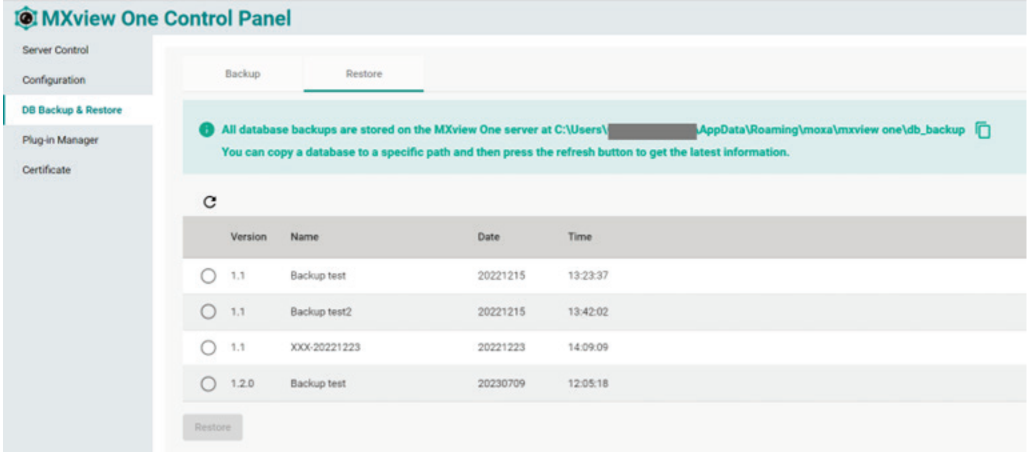
	Version	Name	Date	Time
🗑	1.1	Backup test	20221215	13:23:37
🗑	1.1	Backup test2	20221215	13:42:02
🗑	1.1	XXX-20221223	20221223	14:09:09

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.



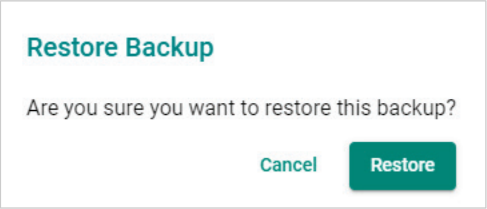
All database backups are stored on the MXview One server at C:\Users\[redacted]\AppData\Roaming\moxa\mxview one\db_backup
You can copy a database to a specific path and then press the refresh button to get the latest information.

	Version	Name	Date	Time
○	1.1	Backup test	20221215	13:23:37
○	1.1	Backup test2	20221215	13:42:02
○	1.1	XXX-20221223	20221223	14:09:09
○	1.2.0	Backup test	20230709	12:05:18

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

3. Click **Restore**.

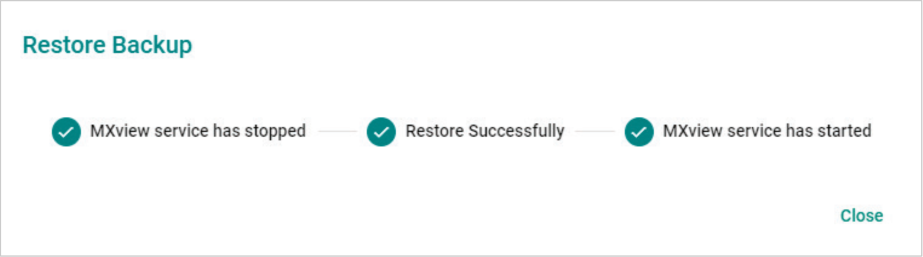
   A confirmation screen will appear.



Restore Backup

Are you sure you want to restore this backup?

4. Displaying the restoration process.



Restore Backup

✓ MXview service has stopped — ✓ Restore Successfully — ✓ MXview service has started

5. Click **Close**.

Plug-in Manager

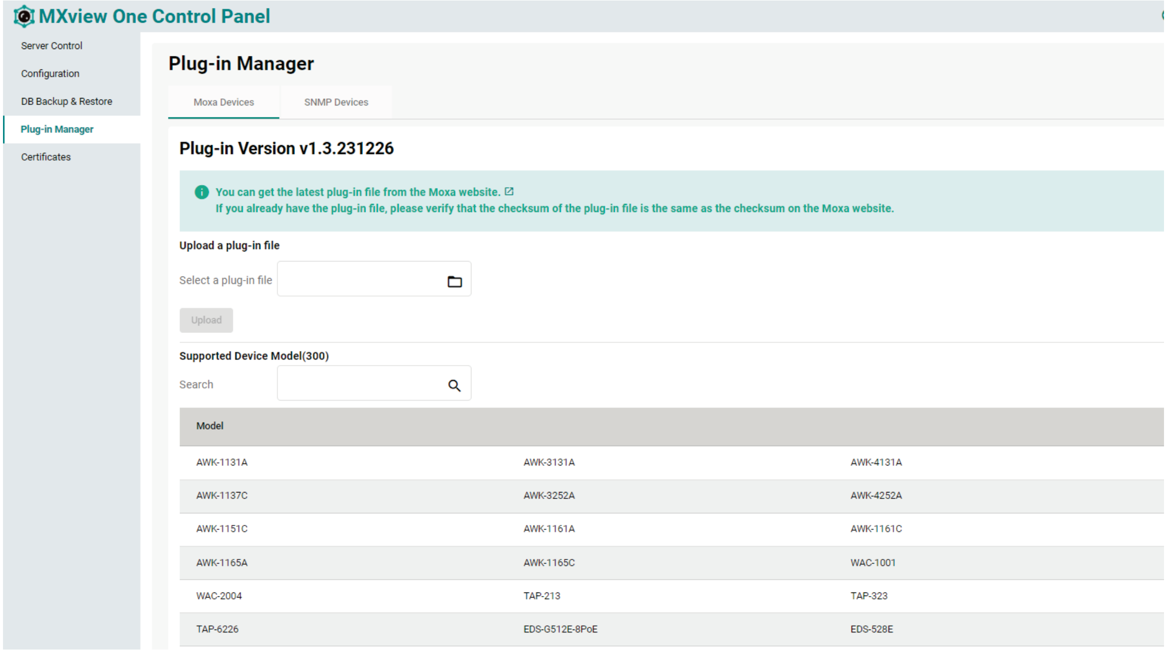
Navigate to **Plug-in Manager** on the **Control Panel**. The Plug-in Manager is a tool that can be used to manage the plug-in files. The **Plug-in Manager** screen features two tabs: **Moxa Devices** and **SNMP Devices**.

Moxa Devices

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 plug-in file from Moxa's website, and then upload the file in the Plug-in Manager. After uploading the plug-in files, these new models can be supported by MXview One.

The **Plug-in Manager** screen includes the following information:

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



Plug-in Manager

Plug-in Version v1.3.231226

You can get the latest plug-in file from the Moxa website.
If you already have the plug-in file, please verify that the checksum of the plug-in file is the same as the checksum on the Moxa website.

Upload a plug-in file

Select a plug-in file

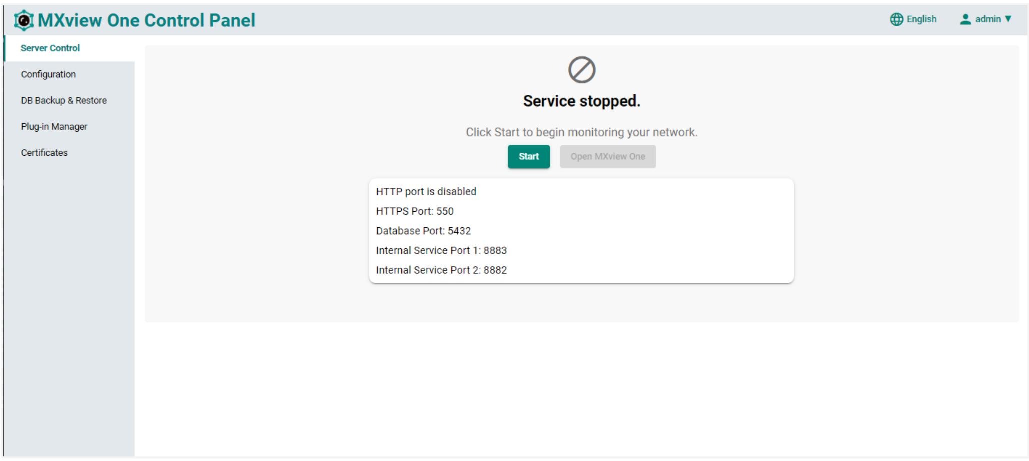
Supported Device Model(300)

Search

Model		
AWK-1131A	AWK-3131A	AWK-4131A
AWK-1137C	AWK-3252A	AWK-4252A
AWK-1151C	AWK-1161A	AWK-1161C
AWK-1165A	AWK-1165C	WAC-1001
WAC-2004	TAP-213	TAP-323
TAP-6226	EDS-G512E-8PoE	EDS-528E

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

1. Stop MXview One.



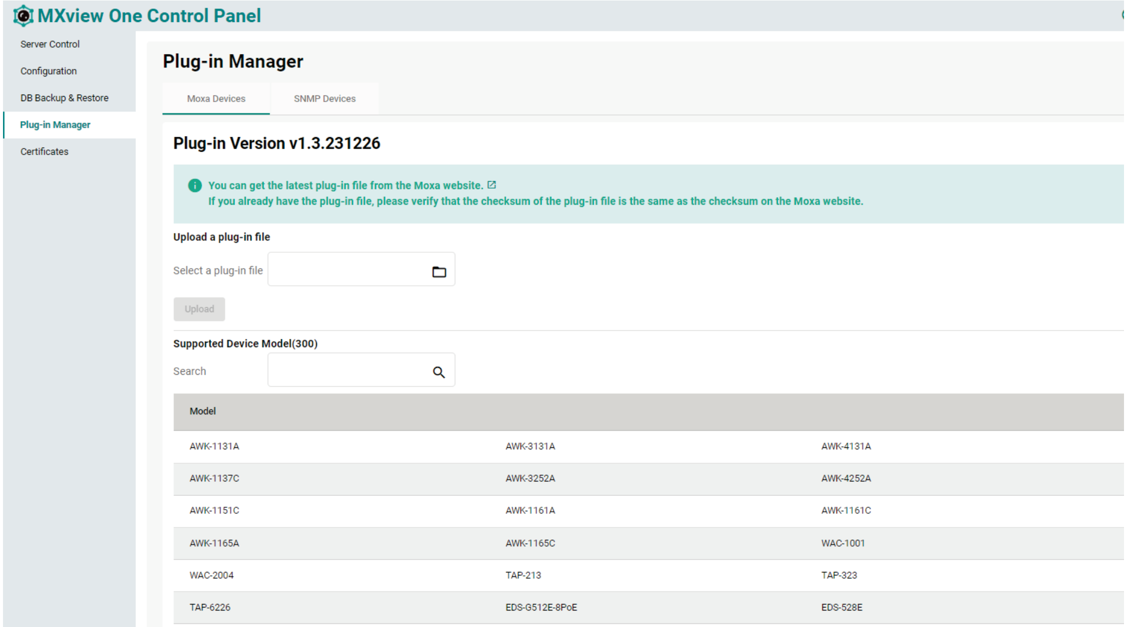
Service stopped.

Click Start to begin monitoring your network.

HTTP port is disabled
HTTPS Port: 550
Database Port: 5432
Internal Service Port 1: 8883
Internal Service Port 2: 8882

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 **Plug-in Manager** on the **Control Panel**.



Plug-in Manager

Plug-in Version v1.3.231226

You can get the latest plug-in file from the Moxa website.
If you already have the plug-in file, please verify that the checksum of the plug-in file is the same as the checksum on the Moxa website.

Upload a plug-in file

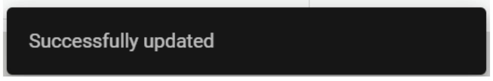
Supported Device Model(300)

Model		
AWK-1131A	AWK-3131A	AWK-4131A
AWK-1137C	AWK-3252A	AWK-4252A
AWK-1151C	AWK-1161A	AWK-1161C
AWK-1165A	AWK-1165C	WAC-1001
WAC-2004	TAP-213	TAP-323
TAP-6226	EDS-G512E-8PoE	EDS-528E

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.

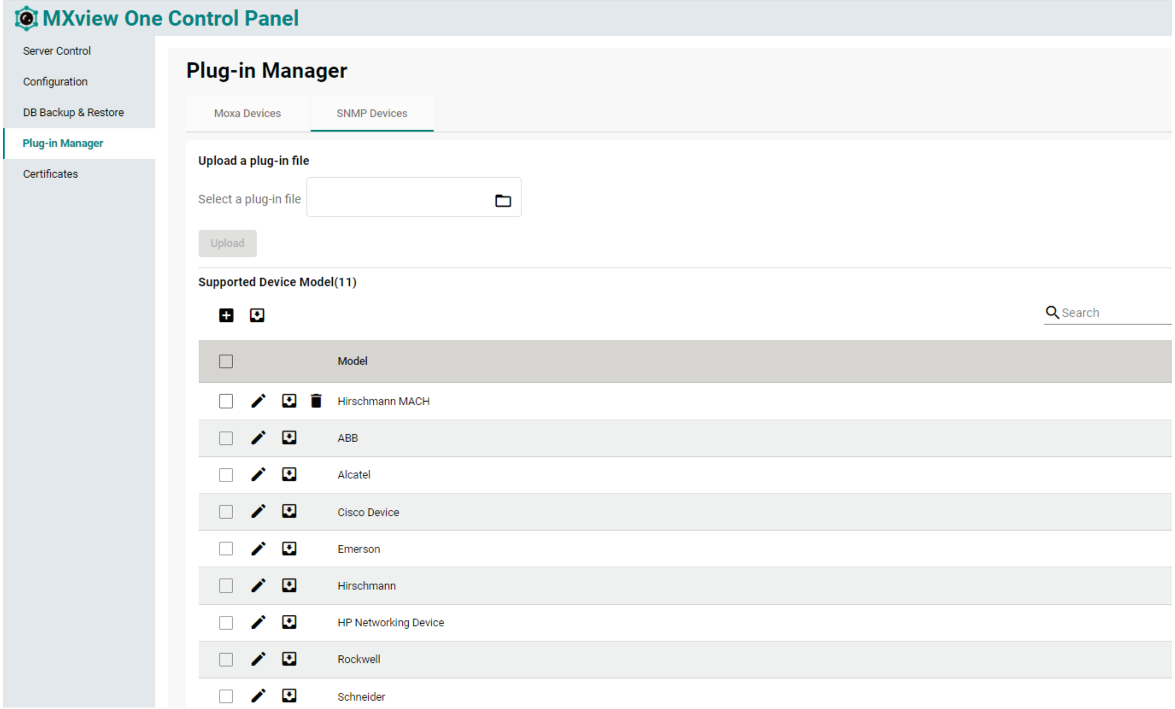
MXview One will upload the plug-in file and display the supported devices.



Successfully updated

SNMP Devices

MXview One supports third-party SNMP devices. Users can create an SNMP device plug-in by uploading MIB files and defining the OID and OID syntax mapping. When uploaded, the information of these devices can be viewed and monitored in MXview One.



Plug-in Manager

Upload a plug-in file

Supported Device Model(11)

□	Model
□	Hirschmann MACH
□	ABB
□	Alcatel
□	Cisco Device
□	Emerson
□	Hirschmann
□	HP Networking Device
□	Rockwell
□	Schneider

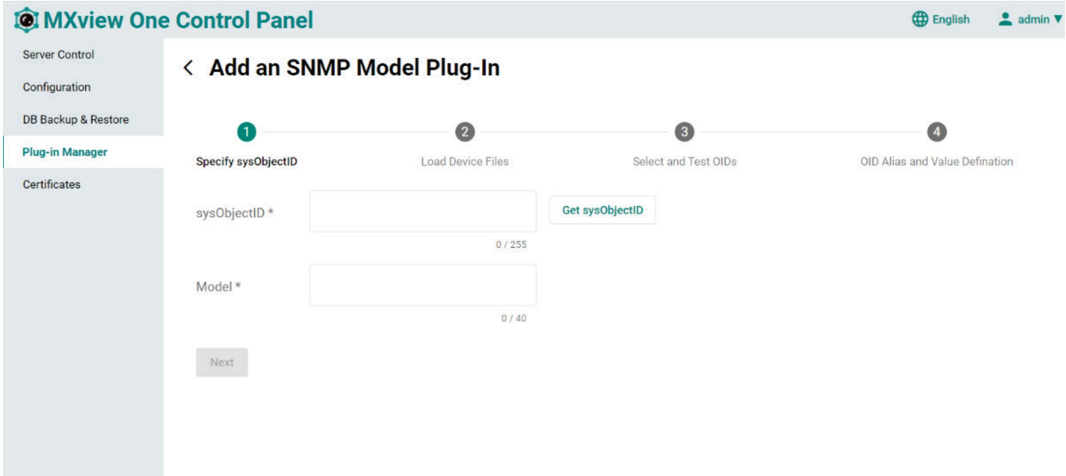
The tab SNMP Devices includes the following information:

- Upload a plug-in file.
- Supported Device Model: This is the third-party SNMP device plug-in list, including built-in and user-defined SNMP plug-in. You can edit, download but cannot delete the built-in plug-in. If your third-party device is not in the list, you can create a new SNMP plug-in, and please refer to the Create a Plug-in

Creating a Plug-in

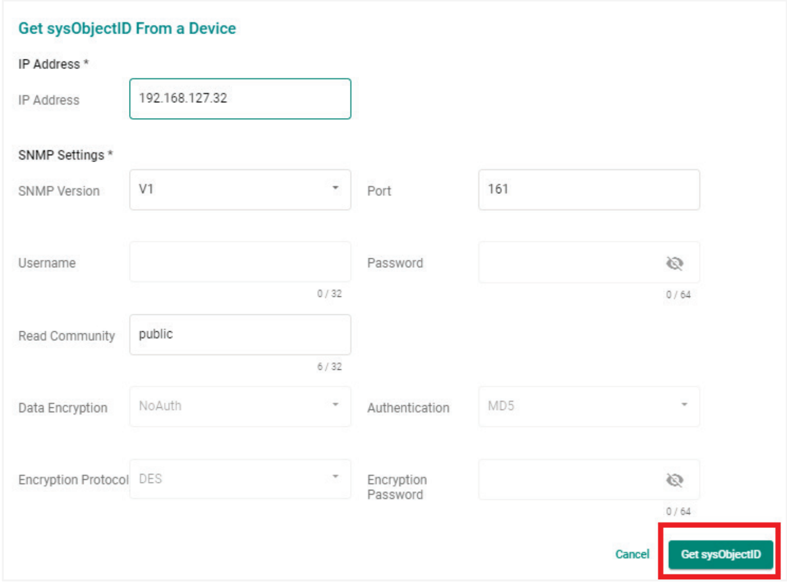
Steps to **Create an SNMP Plug-in**:

1. Navigate to **Control Panel > Plug-in Manager > SNMP Devices**.
2. Click the **Add** (+) icon.
   The **Add an SNMP Model Plug-in** screen will appear.



   There are four steps to creating a third-party SNMP device plug-in file:

3. Specify sysObjectID.
   a. **sysObjectID**: You can manually type in the sysObjectID or click the **Get sysObjectID** button to let MXview One retrieve the sysObjectID. When clicking the **Get sysObjectID** button, the **Get sysObjectID From a Device** window will appear.



Get sysObjectID From a Device

IP Address *

IP Address: 192.168.127.32

SNMP Settings *

SNMP Version: V1

Port: 161

Read Community: public

Data Encryption: NoAuth

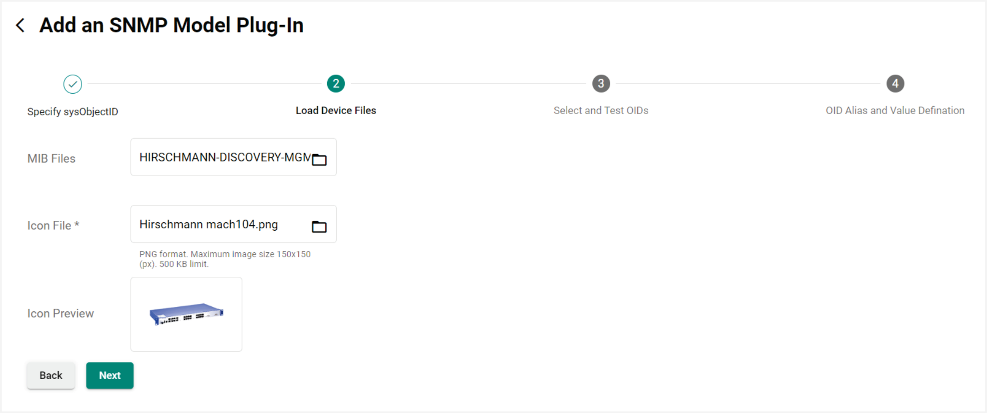
Authentication: MD5

Encryption Protocol: DES

   After specifying all the necessary information, click **Get sysObjectOID**. If successful, a confirmation message will appear.
   Model: Specify the model name. The model name only supports A-Z a-z 0-9 _ - , (comma) ( ) and space.

   b. When finished, click **Next**.

4. Load Device Files.
   a. **MIB Files**: Upload all the necessary MIB files. You can upload multiple MIB files at once.
   b. **Icon File**: Upload the device icon in PNG format. The maximum resolution is 150 x 150 px. The maximum file size is 500 KB limit.
      - **Icon Preview**: The icon preview will show the uploaded image as it will appear in the topology.



< Add an SNMP Model Plug-In

Specify sysObjectID — 2 Load Device Files — 3 Select and Test OIDs — 4 OID Alias and Value Defination

MIB Files: HIRSCHMANN-DISCOVERY-MGM

Icon File *: Hirschmann mach104.png

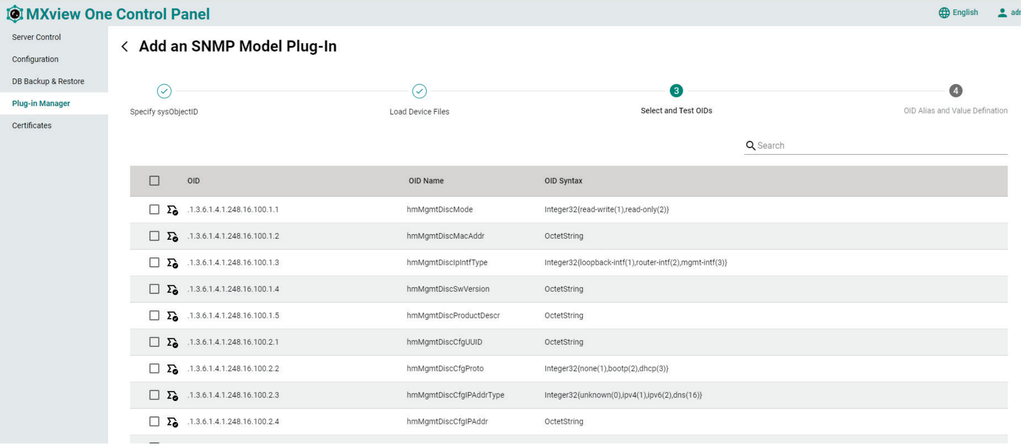
PNG format. Maximum image size 150x150 (px). 500 KB limit.

Icon Preview

Back Next

   c. When finished, click **Next**.

5. Select and Test OIDs.
   After uploading the MIB files, the OIDs from the MIB files will be shown. You can test the OIDs to check the value before selecting them and moving on to the next step.



MXview One Control Panel English adr

Server Control
Configuration
DB Backup & Restore
Plug-in Manager
Certificates

< Add an SNMP Model Plug-In

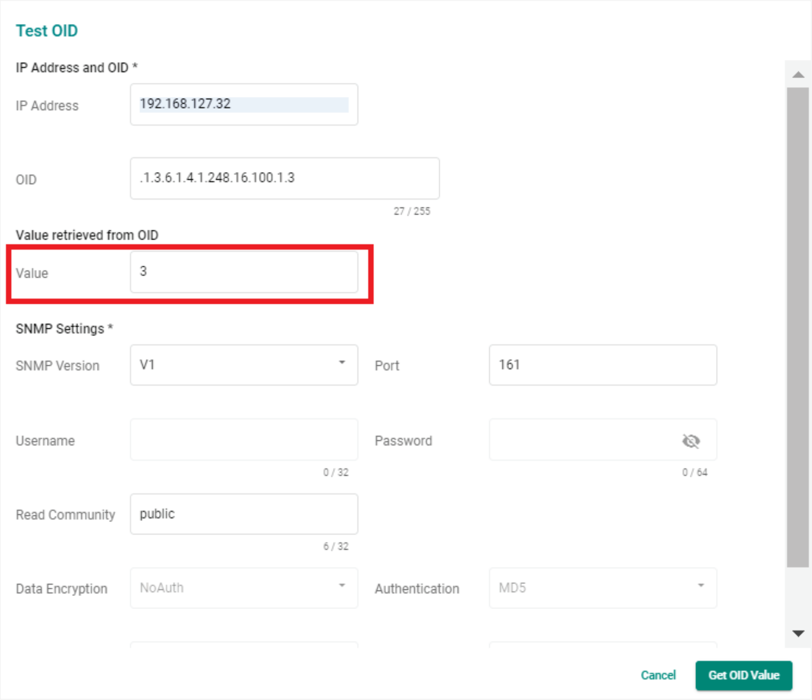
Specify sysObjectID — Load Device Files — 3 Select and Test OIDs — 4 OID Alias and Value Defination

Search

□		OID	OID Name	OID Syntax
□	Σ	.1.3.6.1.4.1.248.16.100.1.1	hmMgmtDiscMode	Integer32{read-write(1),read-only(2)}
□	Σ	.1.3.6.1.4.1.248.16.100.1.2	hmMgmtDiscMacAddr	OctetString
□	Σ	.1.3.6.1.4.1.248.16.100.1.3	hmMgmtDiscIpIntfType	Integer32{loopback-intf(1),router-intf(2),mgmt-intf(3)}
□	Σ	.1.3.6.1.4.1.248.16.100.1.4	hmMgmtDiscSwVersion	OctetString
□	Σ	.1.3.6.1.4.1.248.16.100.1.5	hmMgmtDiscProductDescr	OctetString
□	Σ	.1.3.6.1.4.1.248.16.100.2.1	hmMgmtDiscCfgUUID	OctetString
□	Σ	.1.3.6.1.4.1.248.16.100.2.2	hmMgmtDiscCfgProto	Integer32{none(1),bootp(2),dhcp(3)}
□	Σ	.1.3.6.1.4.1.248.16.100.2.3	hmMgmtDiscCfgIPAddrType	Integer32{unknown(0),ipv4(1),ipv6(2),dns(16)}
□	Σ	.1.3.6.1.4.1.248.16.100.2.4	hmMgmtDiscCfgIPAddr	OctetString

   a. Test OIDs.
      i. Click on the **Test OID** (Σ) icon of the OID you want to test.
         The **Test OID** window will appear.
      ii. Specify the IP address and SNMP settings.

iii. Click the **Get OID Value** button. The retrieved value will show in the **Value retrieved from OID** field.



Test OID

IP Address and OID *

IP Address: 192.168.127.32

OID: .1.3.6.1.4.1.248.16.100.1.3 (27 / 255)

Value retrieved from OID

Value: 3

SNMP Settings *

SNMP Version: V1

Port: 161

Username: (0 / 32)

Password: (0 / 64)

Read Community: public (6 / 32)

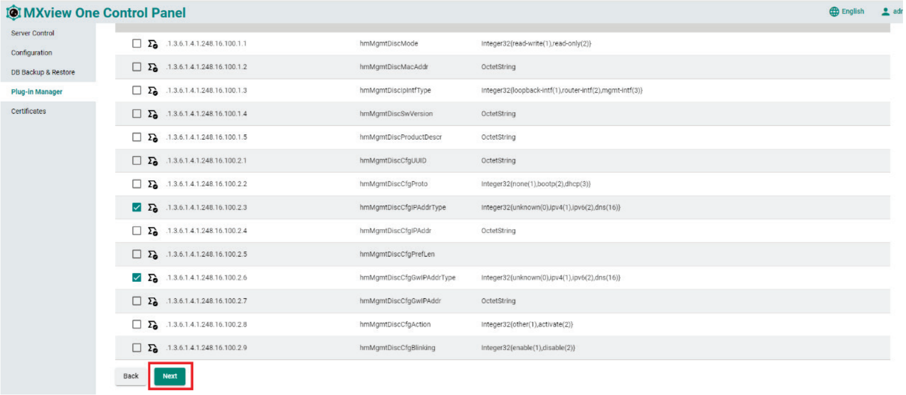
Data Encryption: NoAuth

Authentication: MD5

b. Select OIDs.

i. Select the OIDs you want to monitor in MXview One.

ii. When finished, click **Next**.

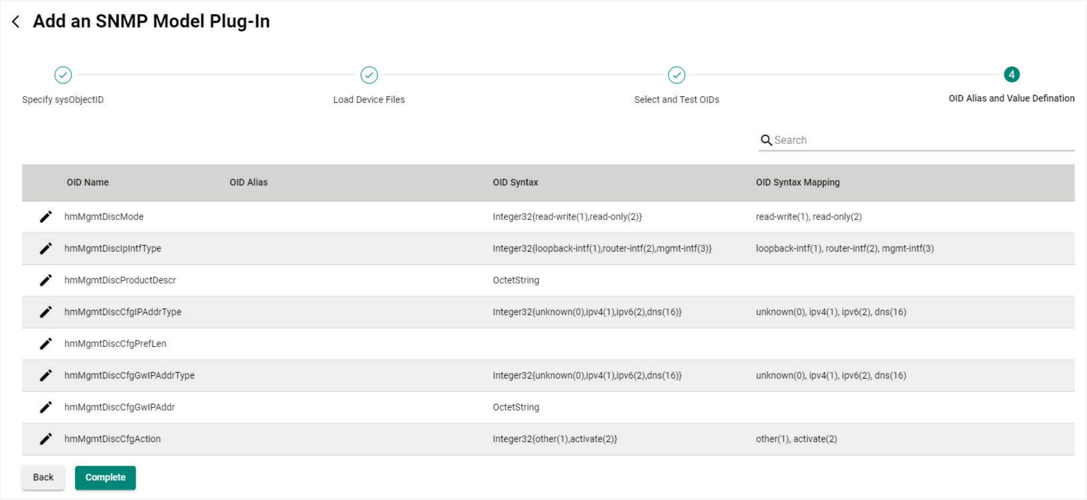


MXview One Control Panel

☐	.1.3.6.1.4.1.248.16.100.1.1	hmMgmtDiscMode	Integer32{read-write(1),read-only(2)}
☐	.1.3.6.1.4.1.248.16.100.1.2	hmMgmtDiscMacAddr	OctetString
☐	.1.3.6.1.4.1.248.16.100.1.3	hmMgmtDiscIpIntfType	Integer32{loopback-intf(1),router-intf(2),mgmt-intf(3)}
☐	.1.3.6.1.4.1.248.16.100.1.4	hmMgmtDiscSwVersion	OctetString
☐	.1.3.6.1.4.1.248.16.100.1.5	hmMgmtDiscProductDescr	OctetString
☐	.1.3.6.1.4.1.248.16.100.2.1	hmMgmtDiscCfgUUID	OctetString
☐	.1.3.6.1.4.1.248.16.100.2.2	hmMgmtDiscCfgProto	Integer32{none(1),bootp(2),dhcp(3)}
☑	.1.3.6.1.4.1.248.16.100.2.3	hmMgmtDiscCfgIPAddrType	Integer32{unknown(0),ipv4(1),ipv6(2),dns(16)}
☐	.1.3.6.1.4.1.248.16.100.2.4	hmMgmtDiscCfgIPAddr	OctetString
☐	.1.3.6.1.4.1.248.16.100.2.5	hmMgmtDiscCfgPrefLen	
☑	.1.3.6.1.4.1.248.16.100.2.6	hmMgmtDiscCfgGwIPAddrType	Integer32{unknown(0),ipv4(1),ipv6(2),dns(16)}
☐	.1.3.6.1.4.1.248.16.100.2.7	hmMgmtDiscCfgGwIPAddr	OctetString
☐	.1.3.6.1.4.1.248.16.100.2.8	hmMgmtDiscCfgAction	Integer32{other(1),activate(2)}
☐	.1.3.6.1.4.1.248.16.100.2.9	hmMgmtDiscCfgBlinking	Integer32{enable(1),disable(2)}

6. OID Alias and Value Definition

   An overview of all selected OIDs will be shown. The OID Alias, OID Syntax, and OID Syntax Mapping is listed for each entry.



Add an SNMP Model Plug-In

Specify sysObjectID — Load Device Files — Select and Test OIDs — 4 OID Alias and Value Defination

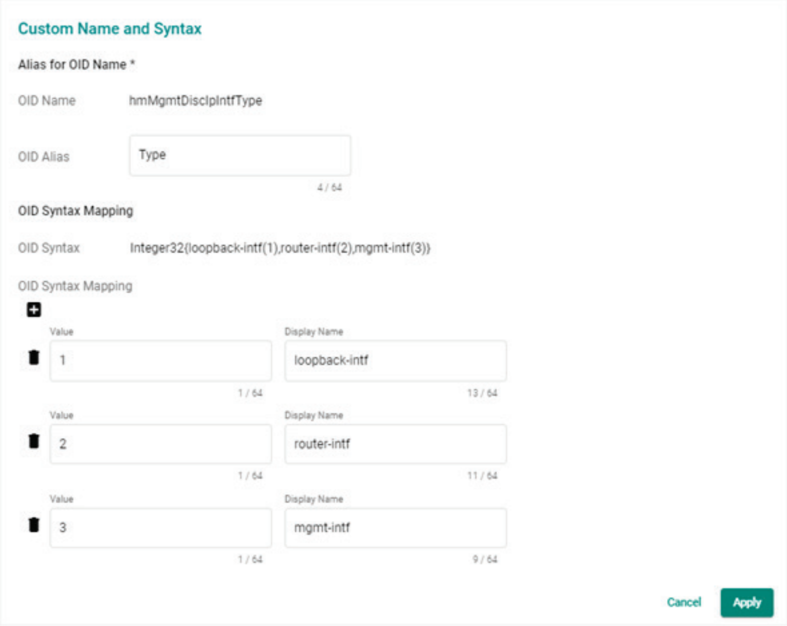
Search

	OID Name	OID Alias	OID Syntax	OID Syntax Mapping
✏	hmMgmtDiscMode		Integer32{read-write(1),read-only(2)}	read-write(1), read-only(2)
✏	hmMgmtDiscIpIntfType		Integer32{loopback-intf(1),router-intf(2),mgmt-intf(3)}	loopback-intf(1), router-intf(2), mgmt-intf(3)
✏	hmMgmtDiscProductDescr		OctetString	
✏	hmMgmtDiscCfgIPAddrType		Integer32{unknown(0),ipv4(1),ipv6(2),dns(16)}	unknown(0), ipv4(1), ipv6(2), dns(16)
✏	hmMgmtDiscCfgPrefLen			
✏	hmMgmtDiscCfgGwIPAddrType		Integer32{unknown(0),ipv4(1),ipv6(2),dns(16)}	unknown(0), ipv4(1), ipv6(2), dns(16)
✏	hmMgmtDiscCfgGwIPAddr		OctetString	
✏	hmMgmtDiscCfgAction		Integer32{other(1),activate(2)}	other(1), activate(2)

Back Complete

   If necessary, you can manually edit the OID information.

   a. Click the **Pencil** (✏) icon of the OID you want to edit.
      The **Custom Name and Syntax** window will appear.



Custom Name and Syntax

Alias for OID Name *

OID Name: hmMgmtDiscIpIntfType

OID Alias: Type (4 / 64)

OID Syntax Mapping

OID Syntax: Integer32{loopback-intf(1),router-intf(2),mgmt-intf(3)}

OID Syntax Mapping

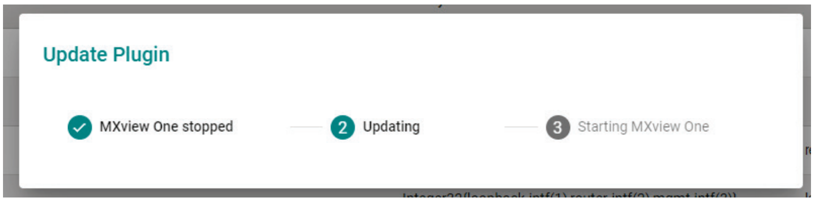
Value	Display Name
1 (1 / 64)	loopback-intf (13 / 64)
2 (1 / 64)	router-intf (11 / 64)
3 (1 / 64)	mgmt-intf (9 / 64)

Cancel Apply

   b. Edit the OID Alias and OID Syntax Mapping information as required.

   c. When finished, click **Apply**.

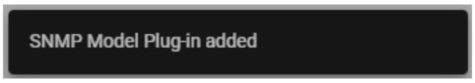
7. When finished with all four steps, click **Complete**.
   The **Update Plug-in** window will appear.



Update Plugin

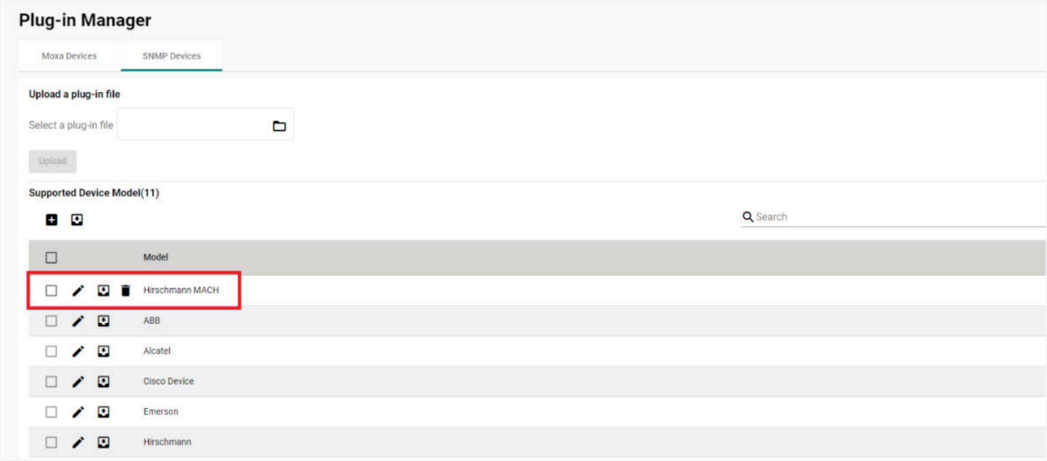
✓ MXview One stopped — 2 Updating — 3 Starting MXview One

8. If successful, a confirmation will appear indicating the plug-in was created.



SNMP Model Plug-in added

The plug-in will now show in the **Supported Device Model** list.



Plug-in Manager

Supported Device Model(11)

	Model
□	Hirschmann MACH
□	ABB
□	Alcatel
□	Cisco Device
□	Emerson
□	Hirschmann

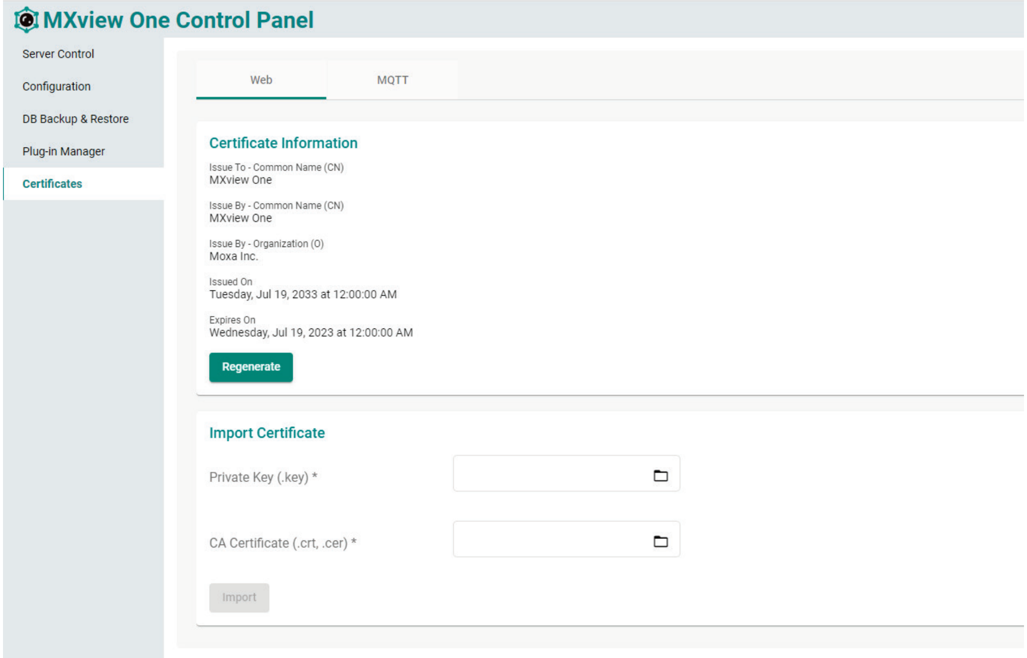
Certificates

From the **Certificate** page, you can view the certificates used by MXview One. By default, you can view information for **Web** certificates. If this MXview One instance is managed through MXview One Central Manager, an additional **MQTT** certificate tab will be available.

Web Certificates

On the **Web** tab, you can view the information for the current web certificates, including:

- Issue To – Common Name (CN)
- Issue By – Common Name (CN)
- Issue By – Organization (O)
- Issued On
- Expires On



Certificate Information

Issue To - Common Name (CN)
MXview One

Issue By - Common Name (CN)
MXview One

Issue By - Organization (O)
Moxa Inc.

Issued On
Tuesday, Jul 19, 2033 at 12:00:00 AM

Expires On
Wednesday, Jul 19, 2023 at 12:00:00 AM

Import Certificate

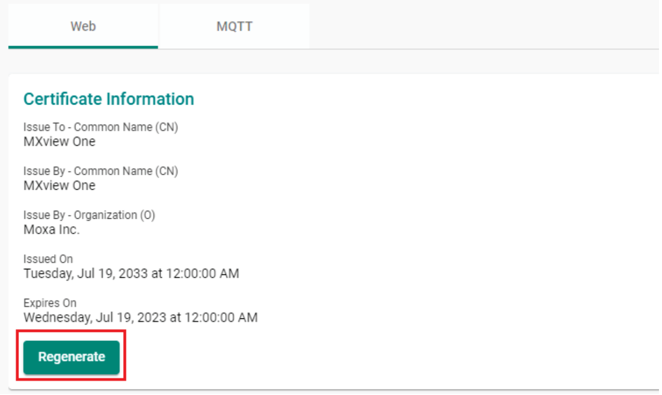
Private Key (.key) *

CA Certificate (.crt, .cer) *

Regenerating the Certificate

1. Click the **Regenerate** button.

   The **Regenerate Certificate** window will appear.



Certificate Information

Issue To - Common Name (CN)
MXview One

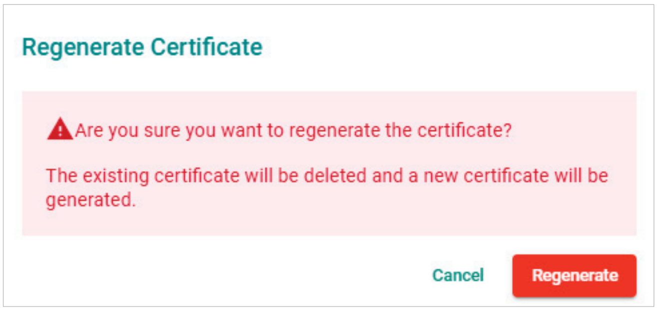
Issue By - Common Name (CN)
MXview One

Issue By - Organization (O)
Moxa Inc.

Issued On
Tuesday, Jul 19, 2033 at 12:00:00 AM

Expires On
Wednesday, Jul 19, 2023 at 12:00:00 AM

2. Click **Regenerate** to regenerate the certificate.

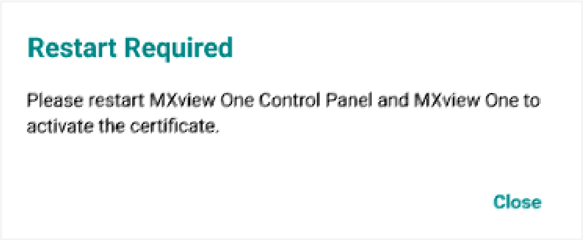


Regenerate Certificate

Are you sure you want to regenerate the certificate?

The existing certificate will be deleted and a new certificate will be generated.

3. After successfully regenerating the certificate, MXview One Central Manager Control Panel will need to be restarted for the certificate to take effect. Click Close and restart the instance.



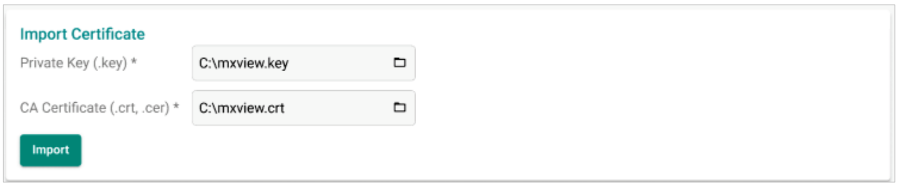
Restart Required

Please restart MXview One Control Panel and MXview One to activate the certificate.

Importing a Certificate

You can manually important a certificate file and key file.

1. Click the folder icon for the Private Key and CA Certificate fields and navigate to the certificate (.crt, .cer) and key (.key) file on the local host.

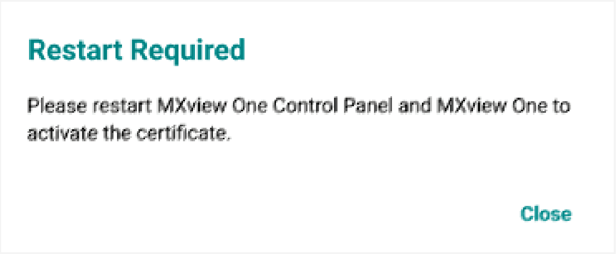


Import Certificate

Private Key (.key) * C:\mxview.key

CA Certificate (.crt, .cer) * C:\mxview.crt

2. Click **Import**.
3. After successfully importing the certificate, MXview One Control Panel will need to be restarted for the certificate to take effect. Click **Close** and restart the instance.



Restart Required

Please restart MXview One Control Panel and MXview One to activate the certificate.

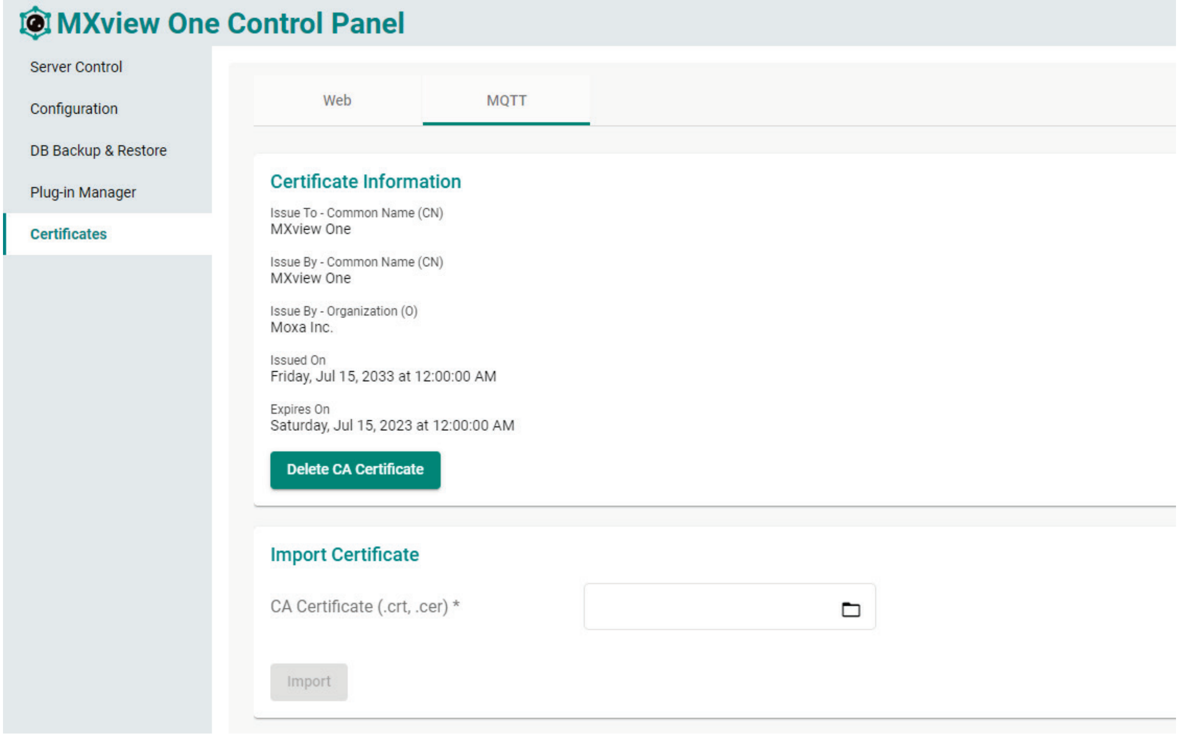
MQTT Certificates

NOTE

By default, no MQTT certificate will be available. To view MQTT certificate information, import the CA Certificate generated through MXview One Central Manager. Refer to Importing the MXview One Central Manager CA Certificate.

If this MXview One instance is managed through MXview One Central Manager, the MQTT tab will be available. On the **MQTT** tab, you can view the information for the current MQTT certificates, including:

- Issue To – Common Name (CN)
- Issue By – Common Name (CN)
- Issue By – Organization (O)
- Issued On
- Expires On



Certificate Information

Issue To - Common Name (CN)
MXview One

Issue By - Common Name (CN)
MXview One

Issue By - Organization (O)
Moxa Inc.

Issued On
Friday, Jul 15, 2033 at 12:00:00 AM

Expires On
Saturday, Jul 15, 2023 at 12:00:00 AM

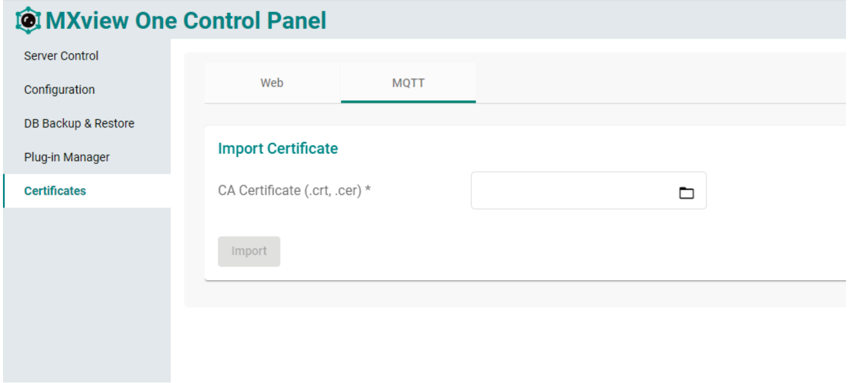
Import Certificate

CA Certificate (.crt, .cer) *

Importing the MXview One Central Manager CA Certificate

If this MXview One instance is managed through MXview One Central Manager, upload the CA certificate generated through MXview One Central Manager Control Panel here.

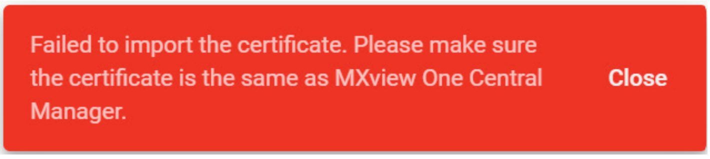
1. Click the folder icon for the CA Certificate field and navigate to the certificate file generated through MXview One Central Manager Control Panel on the local host.


MXview One Control Panel

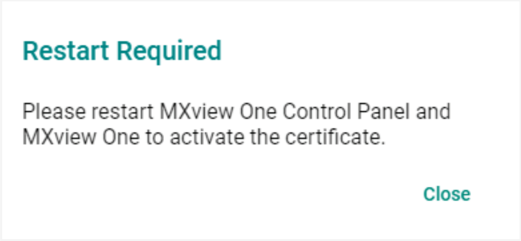
Import Certificate

CA Certificate (.crt, .cer) *

If the uploaded certificate is not from Central Manager, an error message will appear.


Failed to import the certificate. Please make sure the certificate is the same as MXview One Central Manager.

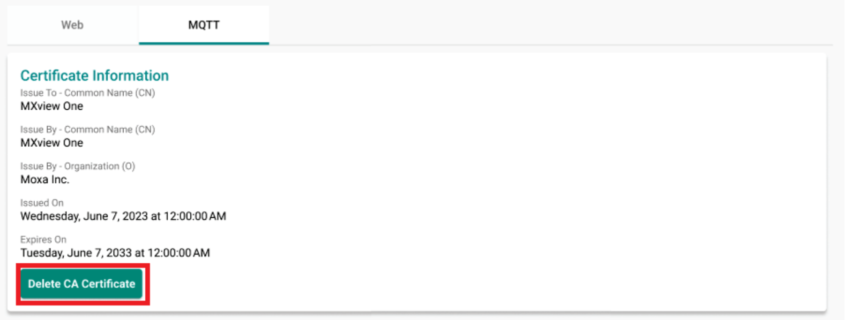
2. Click **Import**.
3. After successfully importing the certificate, MXview One Control Panel will need to be restarted for the certificate to take effect. Click **Close** and restart the instance.


Restart Required

Please restart MXview One Control Panel and MXview One to activate the certificate.

Deleting the CA Certificate

1. Click **Delete CA Certificate** to delete the current CA certificate file.
   The **Delete CA Certificate** window will appear.



Certificate Information

Issue To - Common Name (CN)
MXview One

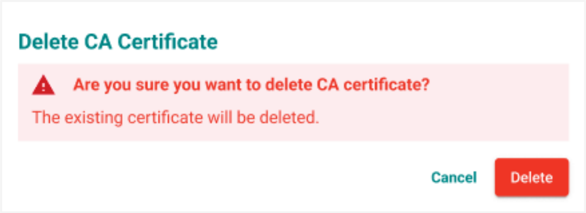
Issue By - Common Name (CN)
MXview One

Issue By - Organization (O)
Moxa Inc.

Issued On
Wednesday, June 7, 2023 at 12:00:00 AM

Expires On
Tuesday, June 7, 2033 at 12:00:00 AM

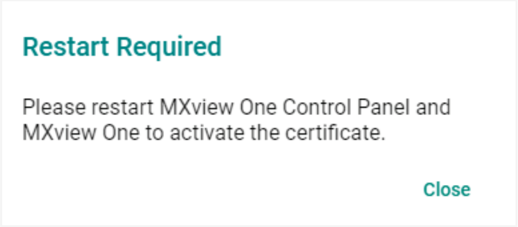
2. When prompted, click **Delete**.


Delete CA Certificate

Are you sure you want to delete CA certificate?

The existing certificate will be deleted.

3. After successfully deleting the certificate, MXview One Control Panel will need to be restarted for the certificate to take effect. Click **Close** and restart the instance.

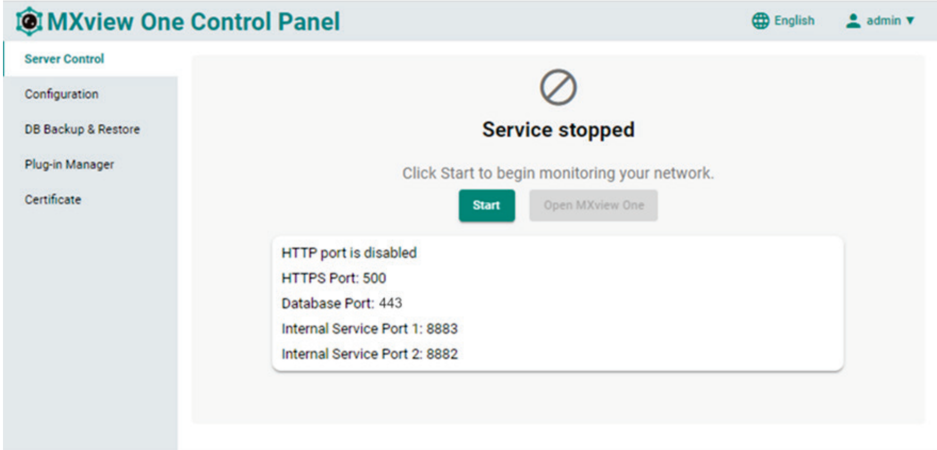


Restart Required

Please restart MXview One Control Panel and MXview One to activate the certificate.

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.

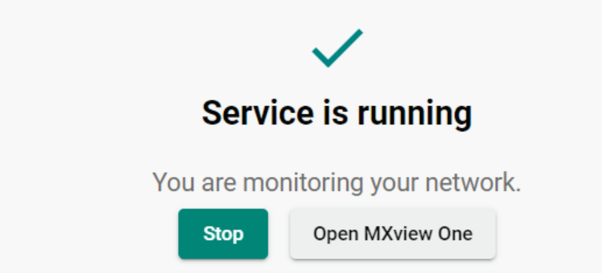


Service stopped

Click Start to begin monitoring your network.

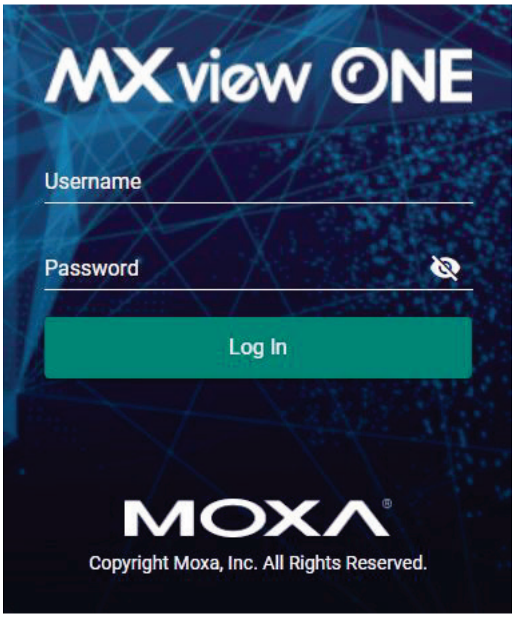
HTTP port is disabled
HTTPS Port: 500
Database Port: 443
Internal Service Port 1: 8883
Internal Service Port 2: 8882

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



Service is running

You are monitoring your network.



Provide the following login credentials

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

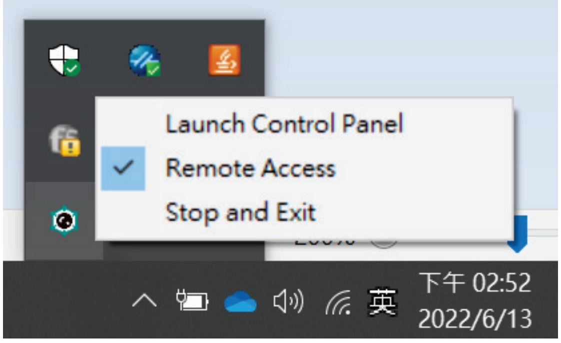
NOTE

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**.

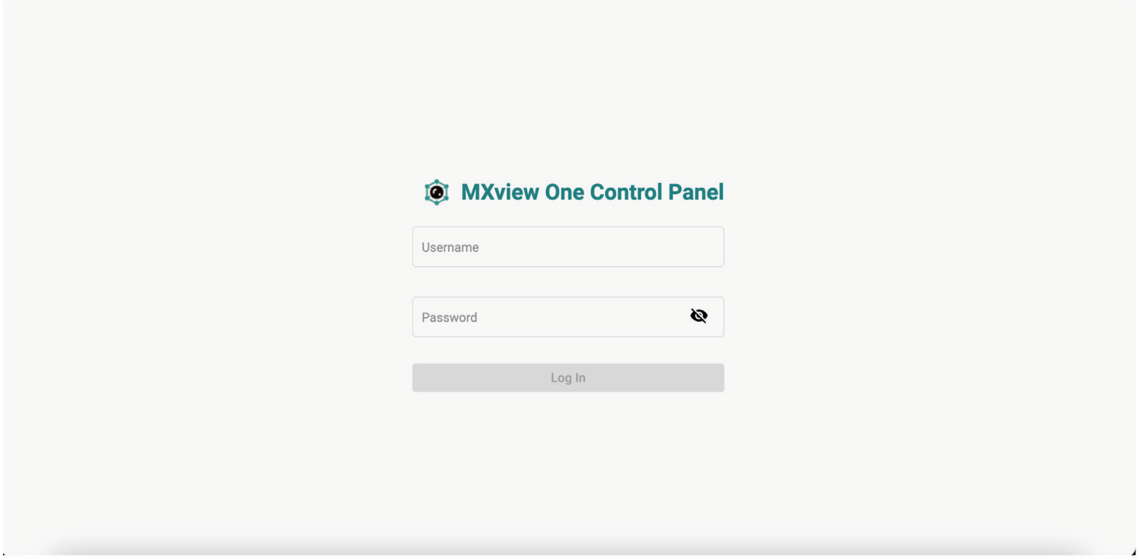


NOTE

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

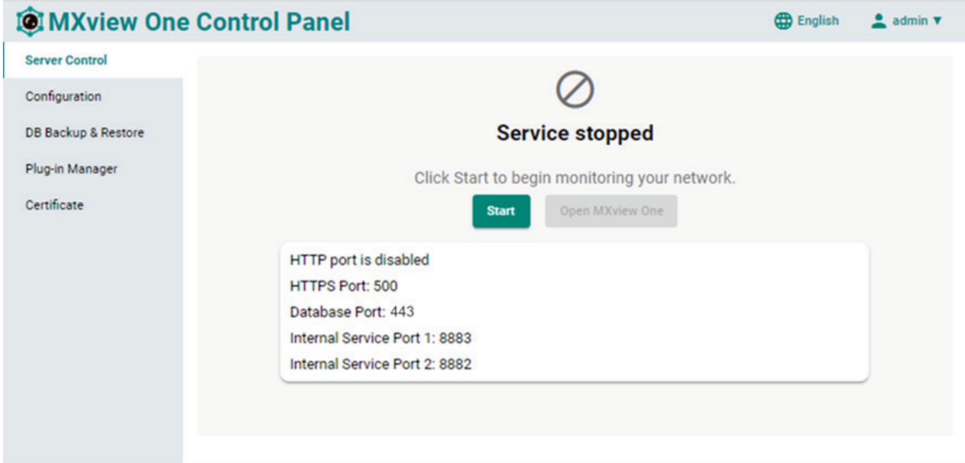
2. Open a web browser on the computer located at the remote site.
3. In the address bar, input the IP address or domain name of the computer that you want to log in to MXview One from.
   - Format: **https://[IP address]:[Port]**
   - Example: https://192.168.1.250:7100

   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



Service stopped

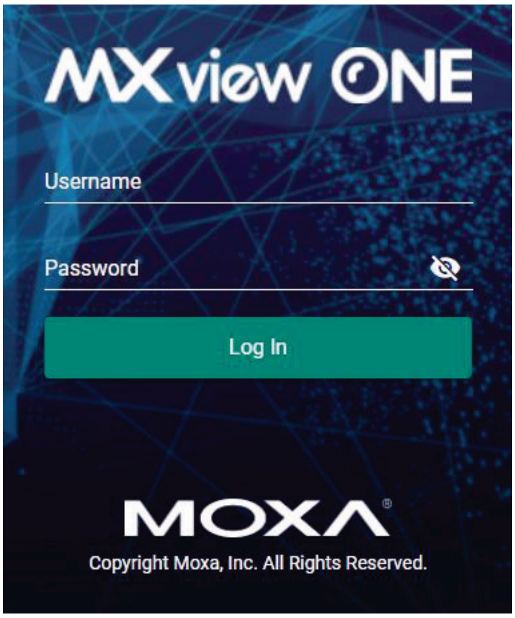
Click Start to begin monitoring your network.

HTTP port is disabled
HTTPS Port: 500
Database Port: 443
Internal Service Port 1: 8883
Internal Service Port 2: 8882

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.

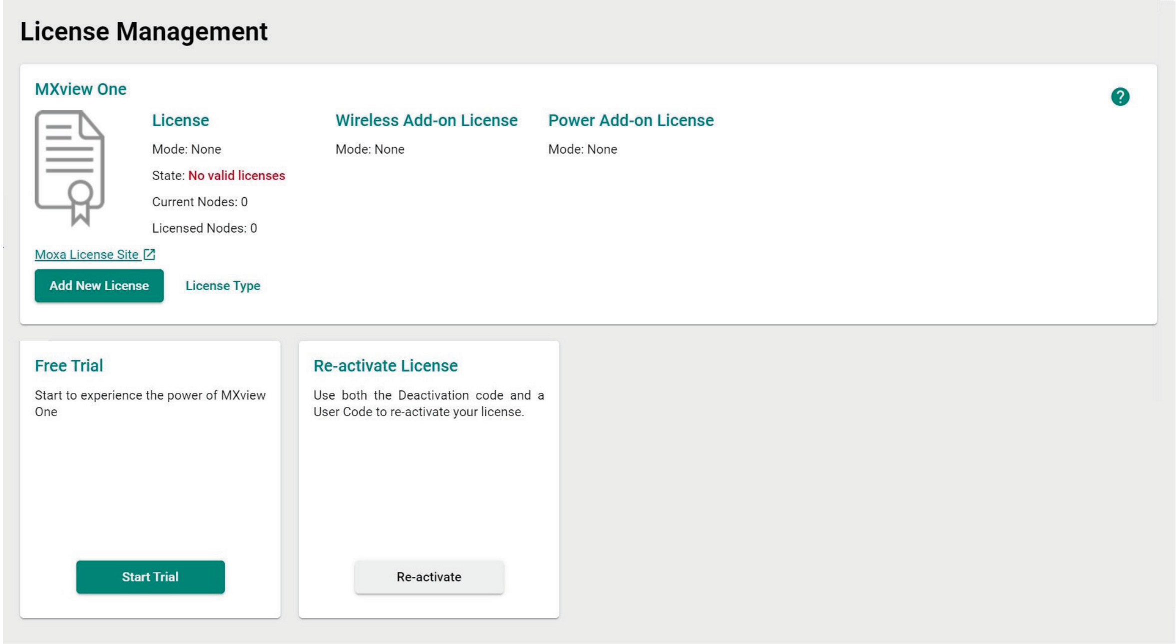
NOTE

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.**



License Management

MXview One

License

Mode: None

State: No valid licenses

Current Nodes: 0

Licensed Nodes: 0

Wireless Add-on License

Mode: None

Power Add-on License

Mode: None

Free Trial

Start to experience the power of MXview One

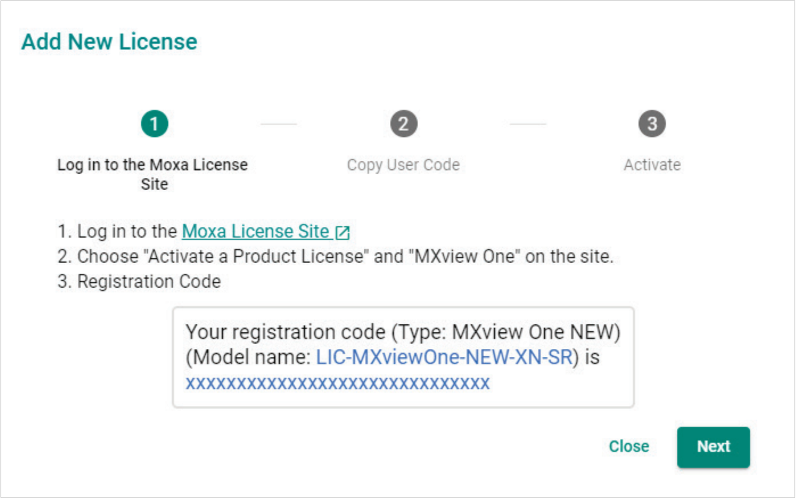
Re-activate License

Use both the Deactivation code and a User Code to re-activate your license.

Adding a New License

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

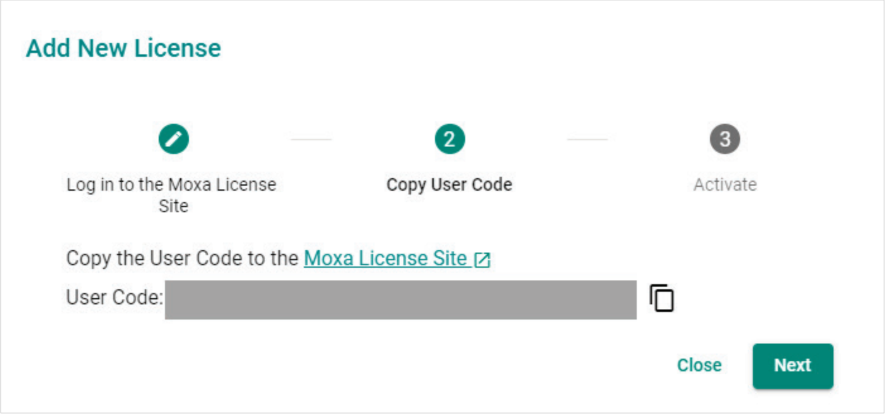
1. Navigate to **Menu** (☰) **> Administration > License Management**.
   The **License Management** screen appears.
   In the **Add New License** section, click **Add New License**.
2. Login to the Moxa License Site to activate the MXview One license. Click **Next** to get the User Code.



1. Log in to the Moxa License Site
2. Choose "Activate a Product License" and "MXview One" on the site.
3. Registration Code

Your registration code (Type: MXview One NEW) (Model name: LIC-MXviewOne-NEW-XN-SR) is xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

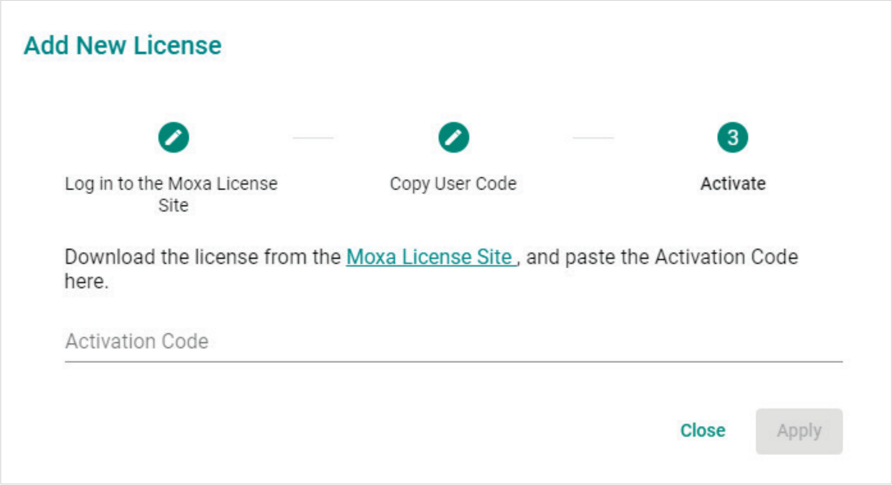
3. Copy the User Code.



Copy the User Code to the Moxa License Site

User Code:

4. Input a valid activation code.



Download the license from the Moxa License Site , and paste the Activation Code here.

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.

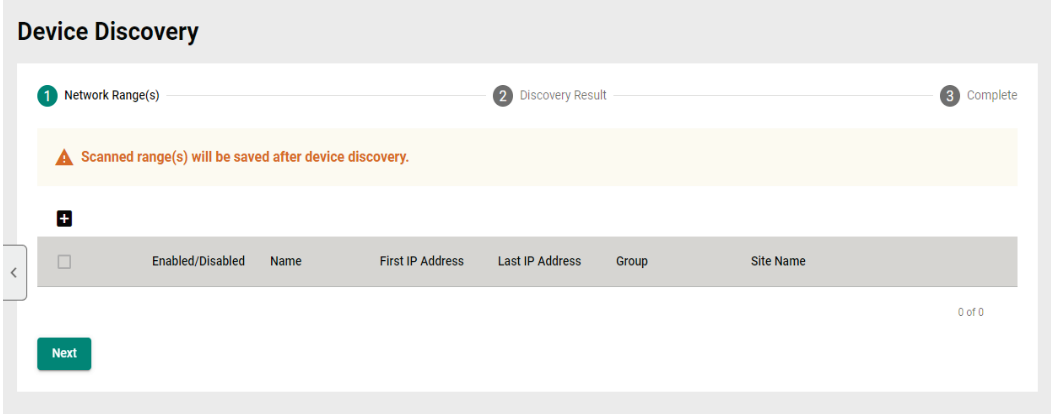
Using Device Discovery

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.



Device Discovery

1 Network Range(s) — 2 Discovery Result — 3 Complete

Scanned range(s) will be saved after device discovery.

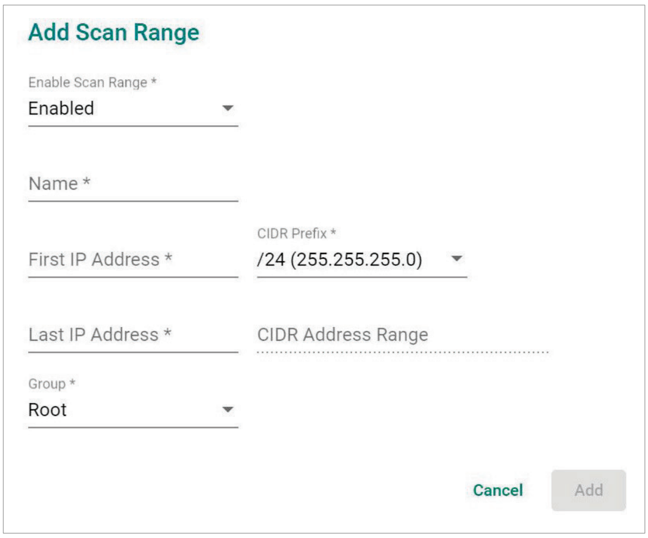
□	Enabled/Disabled	Name	First IP Address	Last IP Address	Group	Site Name

0 of 0

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.



Add Scan Range

Enable Scan Range *: Enabled

Name *

First IP Address *

CIDR Prefix *: /24 (255.255.255.0)

Last IP Address *

CIDR Address Range

Group *: Root

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**.

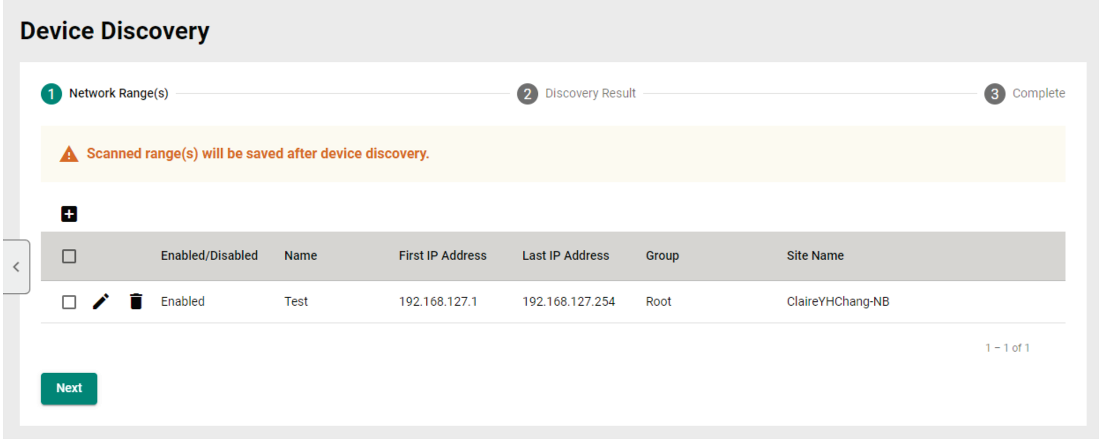
e. (Optional) Add additional network scan ranges, repeat the previous steps.

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.



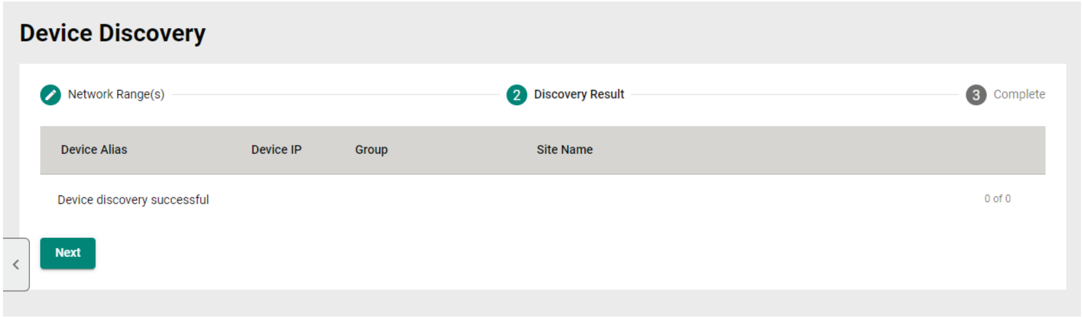
Device Discovery

⚠ Scanned range(s) will be saved after device discovery.

□			Enabled/Disabled	Name	First IP Address	Last IP Address	Group	Site Name
□	✎	🗑	Enabled	Test	192.168.127.1	192.168.127.254	Root	ClaireYHChang-NB

1 – 1 of 1

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.



Device Discovery

✓ Network Range(s) — 2 Discovery Result — 3 Complete

Device Alias	Device IP	Group	Site Name

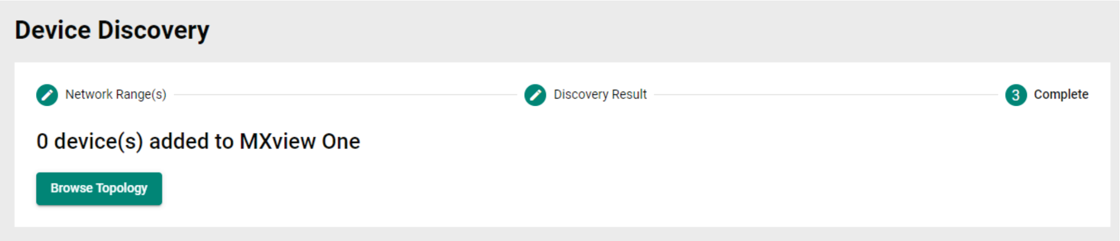
Device discovery successful

0 of 0

   b. Click **Next**.

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

   The **Topology** screen appears.



Device Discovery

✓ Network Range(s) — ✓ Discovery Result — 3 Complete

0 device(s) added to MXview One

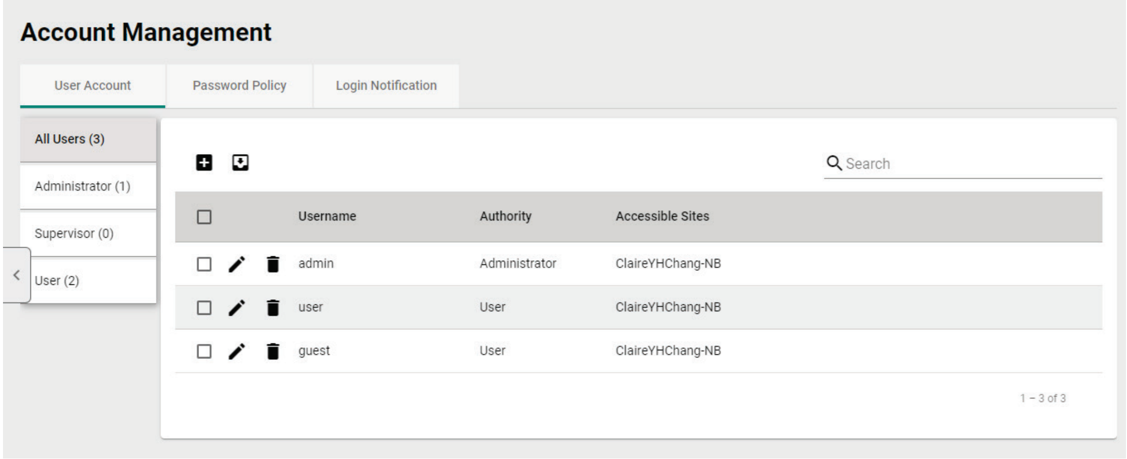
NOTE

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.



Account Management

□	Username	Authority	Accessible Sites
□	admin	Administrator	ClaireYHChang-NB
□	user	User	ClaireYHChang-NB
□	guest	User	ClaireYHChang-NB

1 – 3 of 3

MXview One provides three default accounts:

- admin
- user
- guest

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

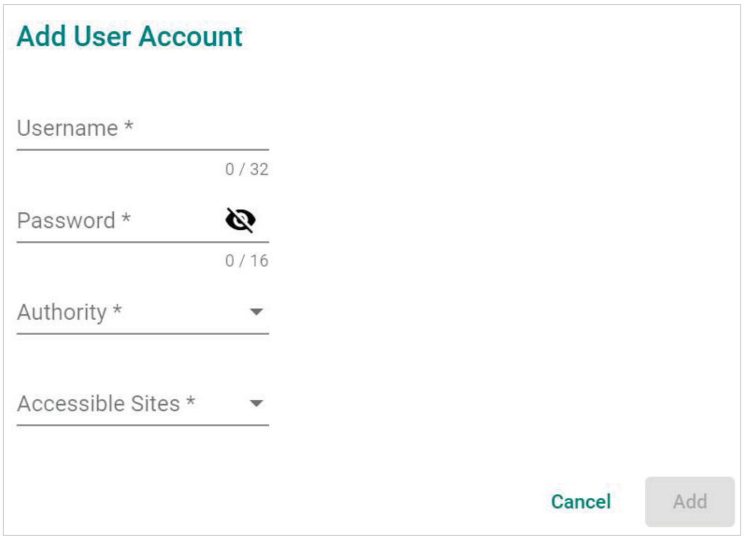
Each account can be assigned one of the following **Authority** permissions:

- **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**.

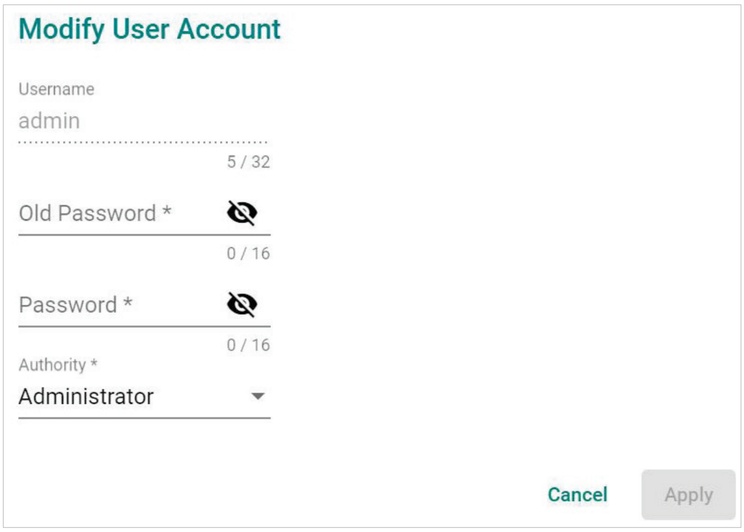
Modifying User Accounts

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.



Modify User Account

Username
admin
5 / 32

Old Password *
0 / 16

Password *
0 / 16

Authority *
Administrator

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).

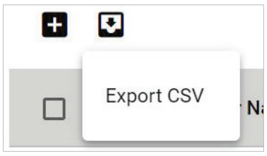
Exporting User Accounts

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.

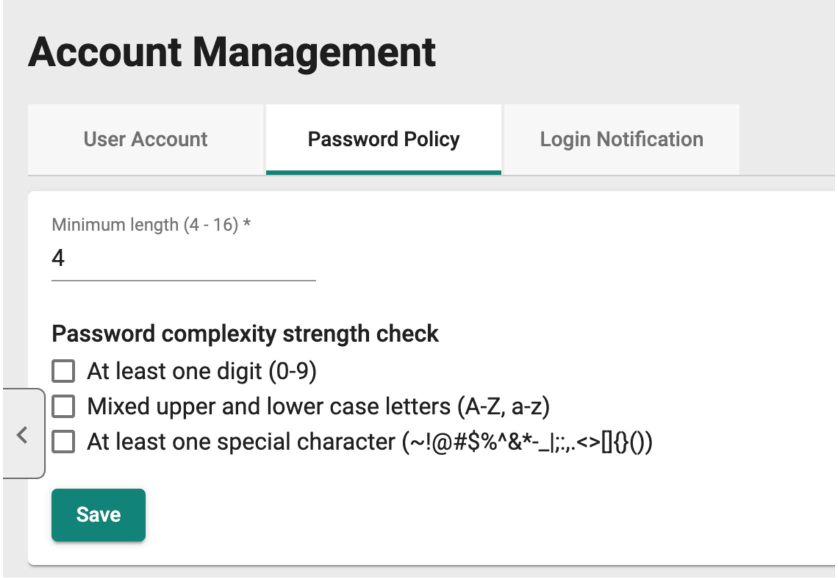


3. Select **Export CSV**.

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.



Minimum length (4 - 16) *
4

Password complexity strength check

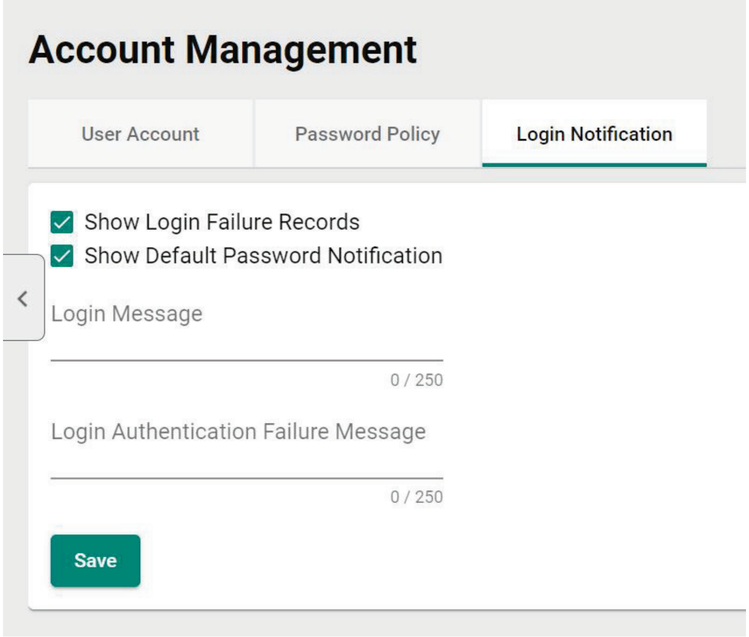
☐ At least one digit (0-9)
☐ Mixed upper and lower case letters (A-Z, a-z)
☐ At least one special character (~!@#$%^&*-_|;:,.<>[]{}())

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.



Account Management

☑ Show Login Failure Records

☑ Show Default Password Notification

Login Message

0 / 250

Login Authentication Failure Message

0 / 250

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.

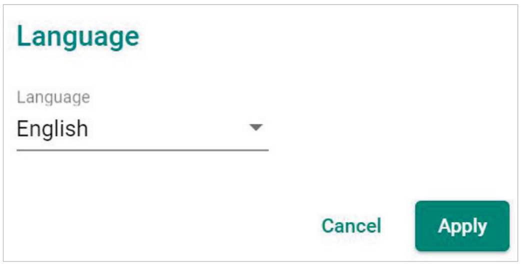
Changing the Display Language

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.



Language

Language
English

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**.

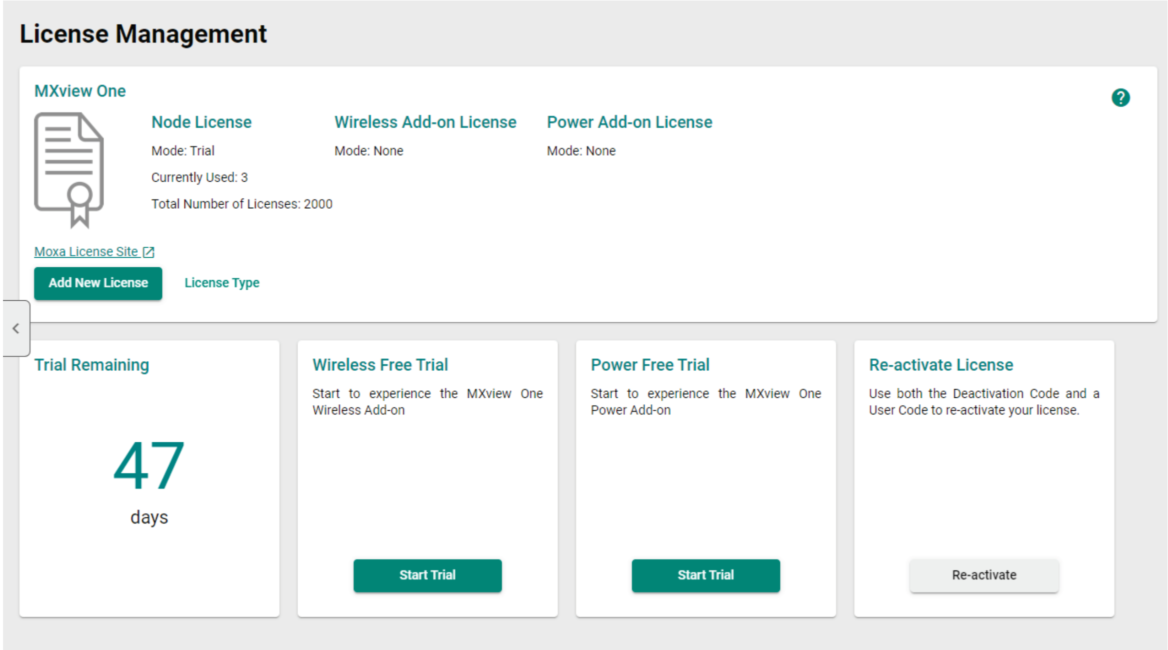
   MXview One updates the display language.

4. License Management

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 Management

MXview One

Node License
Mode: Trial
Currently Used: 3
Total Number of Licenses: 2000

Wireless Add-on License
Mode: None

Power Add-on License
Mode: None

Trial Remaining
47
days

Wireless Free Trial
Start to experience the MXview One Wireless Add-on

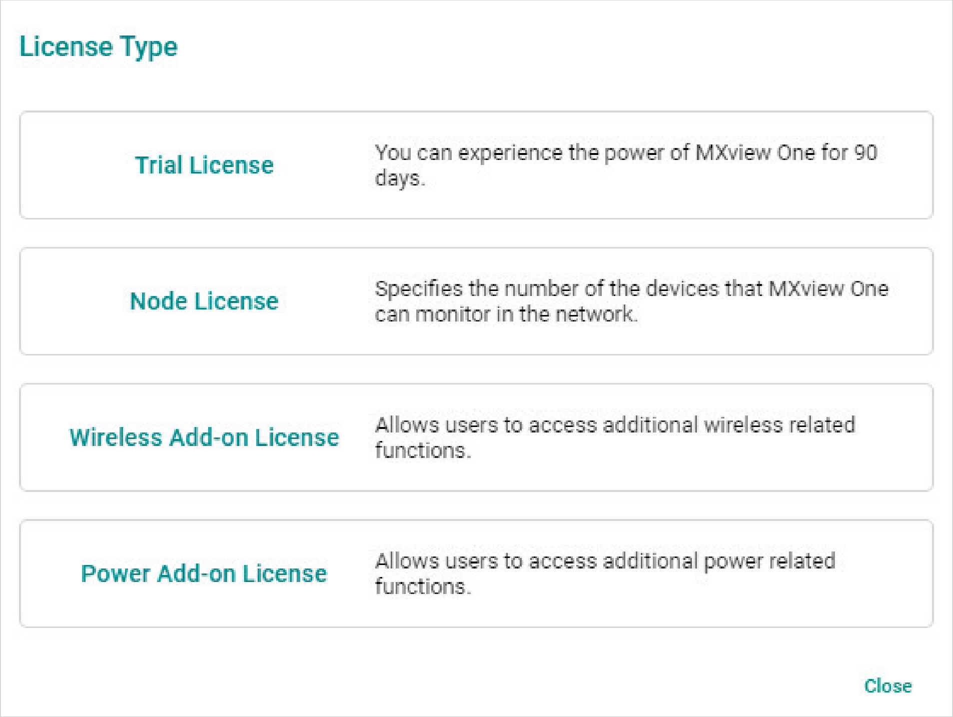
Power Free Trial
Start to experience the MXview One Power Add-on

Re-activate License
Use both the Deactivation Code and a User Code to re-activate your license.

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 90 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.



License Type

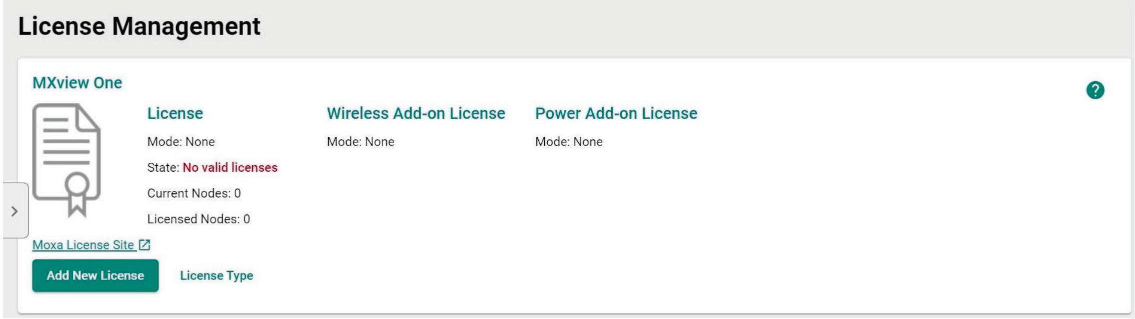
Trial License	You can experience the power of MXview One for 90 days.
Node License	Specifies the number of the devices that MXview One can monitor in the network.
Wireless Add-on License	Allows users to access additional wireless related functions.
Power Add-on License	Allows users to access additional 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**.



License Management

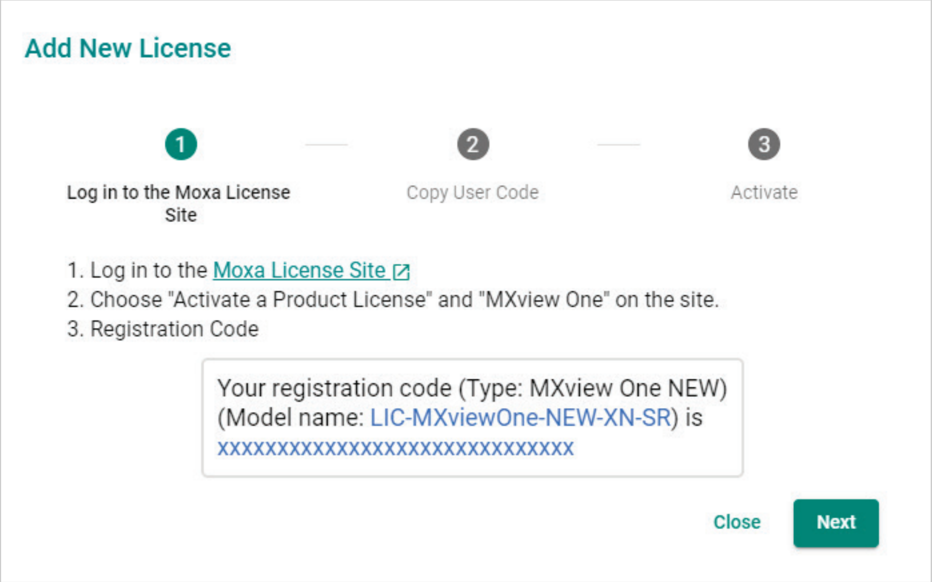
MXview One

License
Mode: None
State: No valid licenses
Current Nodes: 0
Licensed Nodes: 0

Wireless Add-on License
Mode: None

Power Add-on License
Mode: None

   The **Add New License** screen appears.

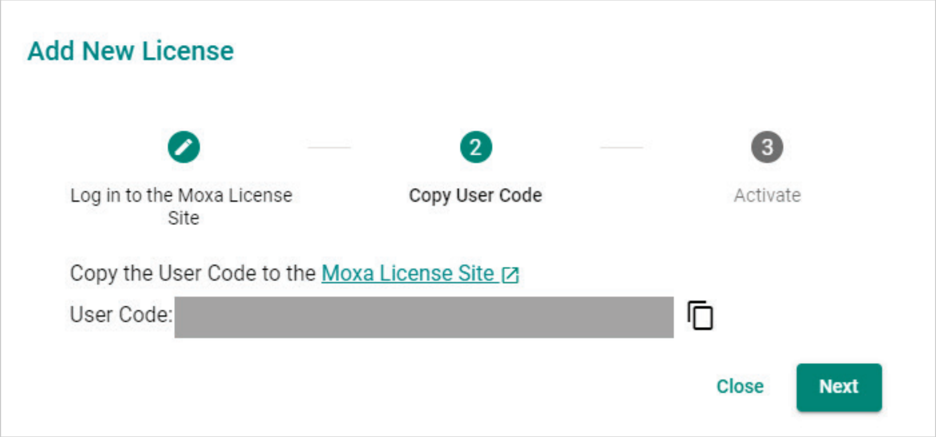


Add New License

1. Log in to the Moxa License Site
2. Choose "Activate a Product License" and "MXview One" on the site.
3. Registration Code

Your registration code (Type: MXview One NEW) (Model name: LIC-MXviewOne-NEW-XN-SR) is xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

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



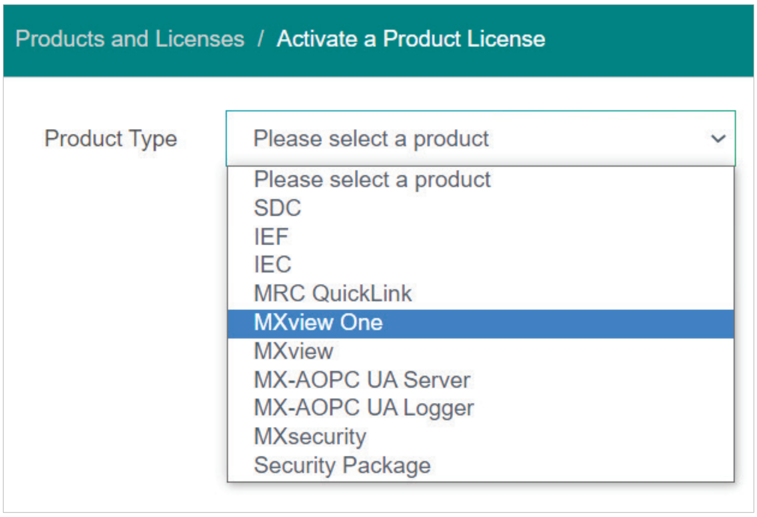
Add New License

Copy the User Code to the Moxa License Site

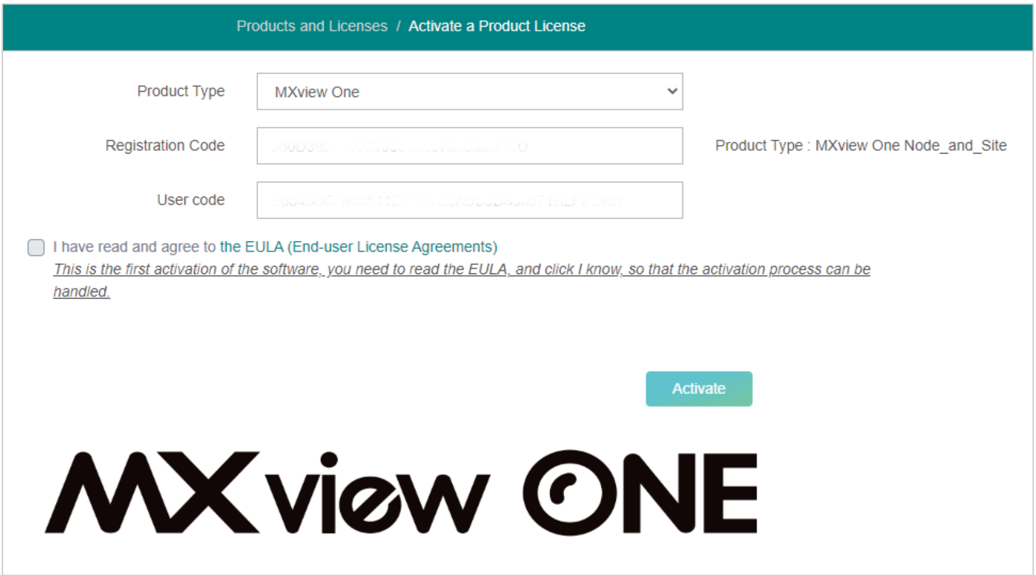
User Code: [redacted]

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.



Product Type: MXview One

Registration Code

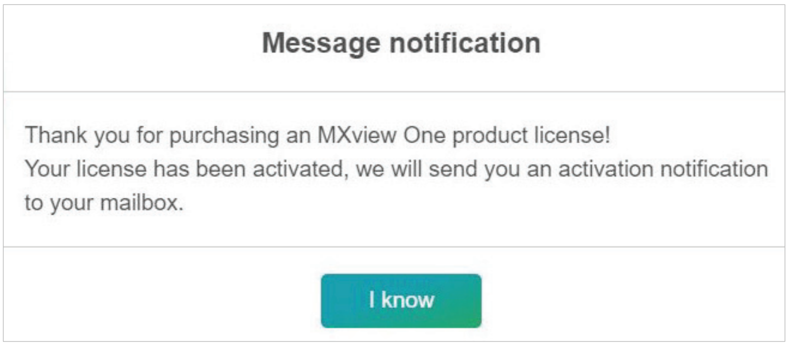
Product Type : MXview One Node_and_Site

User code

□ I have read and agree to the EULA (End-user License Agreements)

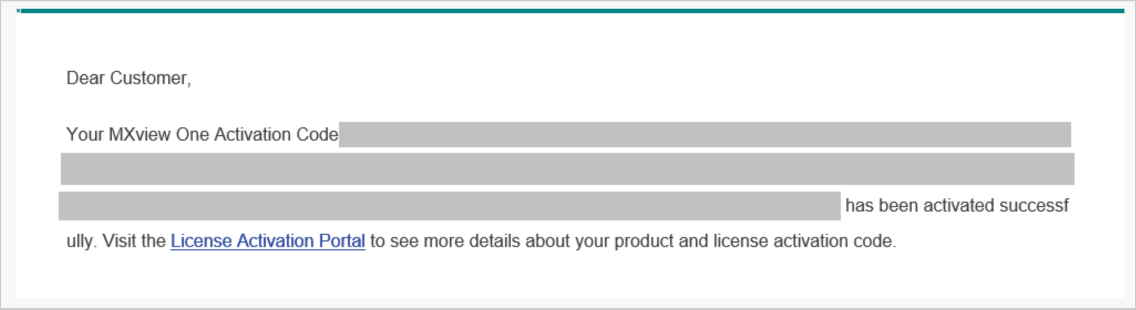
This is the first activation of the software, you need to read the EULA, and click I know, so that the activation process can be handled.

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.



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

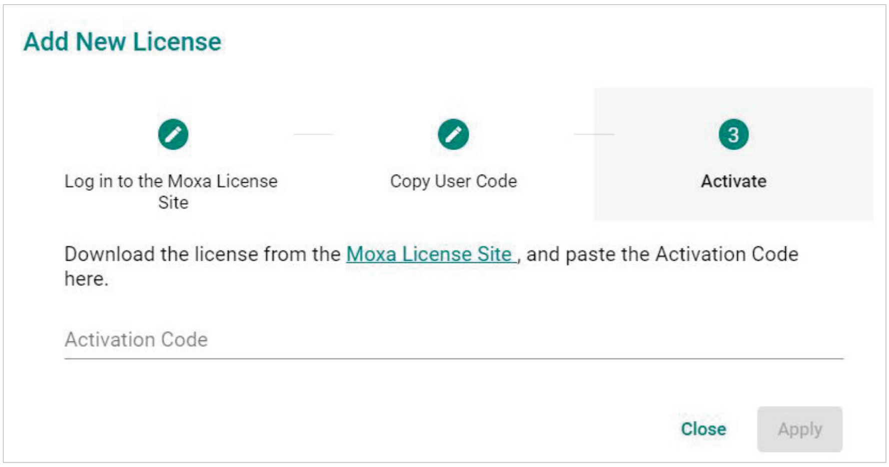
10. Check your email account you used to apply for your moxa account. The activation code will be sent to this email address.



Dear Customer,

Your MXview One Activation Code [redacted] has been activated successfully. Visit the License Activation Portal to see more details about your product and license activation code.

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



Add New License

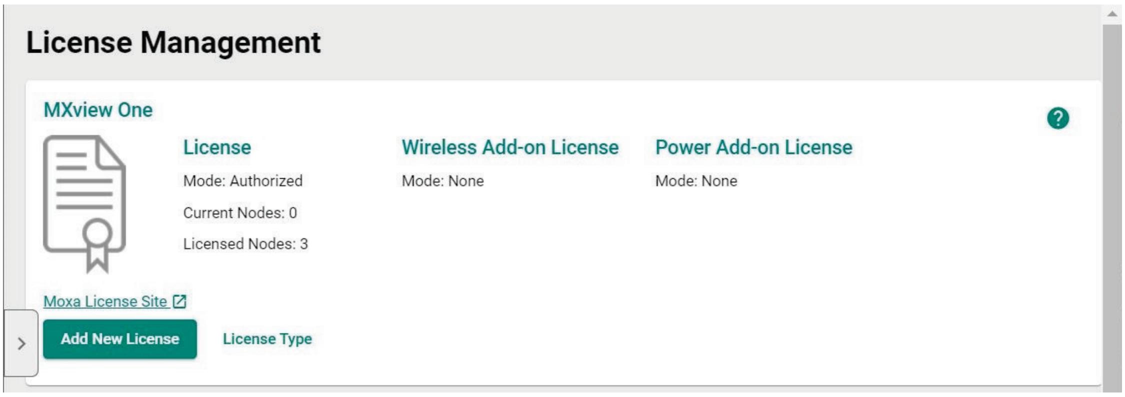
Download the license from the Moxa License Site , and paste the Activation Code here.

Activation Code

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.



License Management

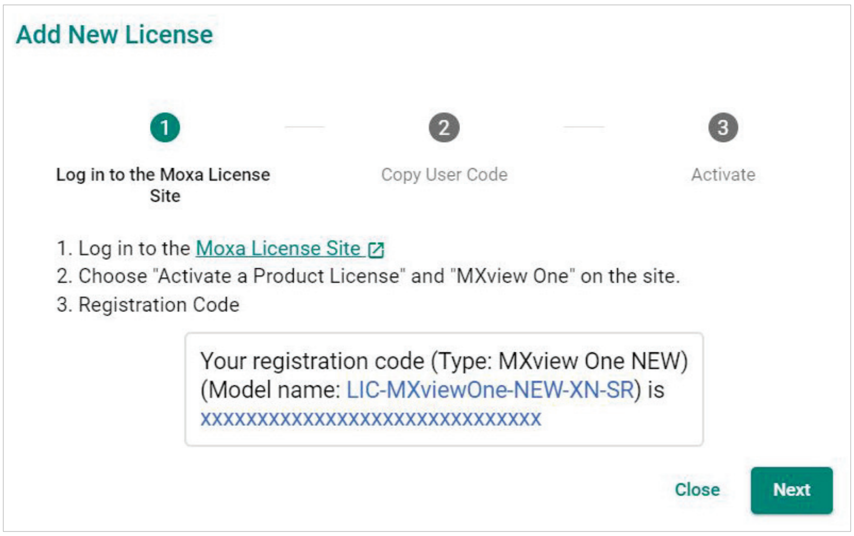
MXview One

License
Mode: Authorized
Current Nodes: 0
Licensed Nodes: 3

Wireless Add-on License
Mode: None

Power Add-on License
Mode: None

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



Add New License

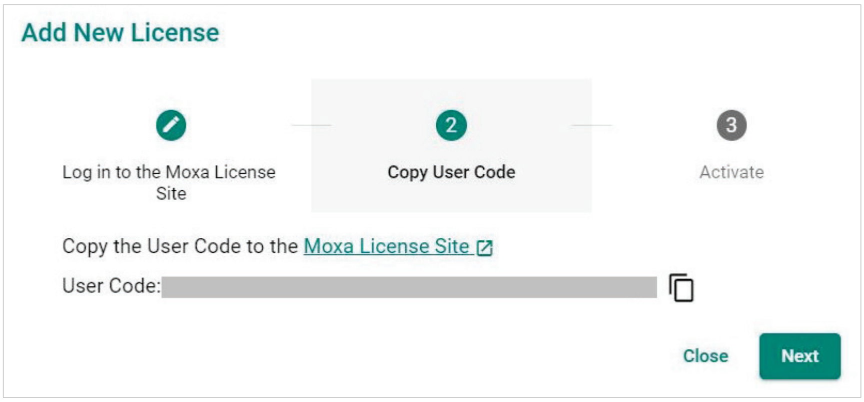
1. Log in to the Moxa License Site
2. Choose "Activate a Product License" and "MXview One" on the site.
3. Registration Code

Your registration code (Type: MXview One NEW) (Model name: LIC-MXviewOne-NEW-XN-SR) is XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

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

NOTE

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

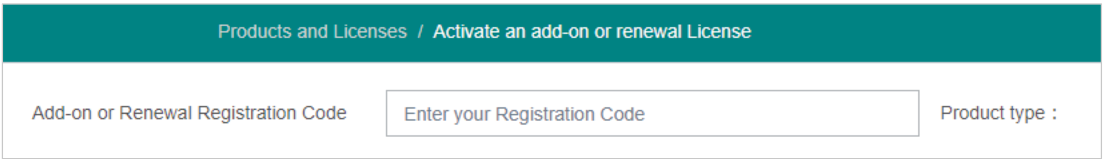


Add New License

Copy the User Code to the Moxa License Site

User Code: [redacted]

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.

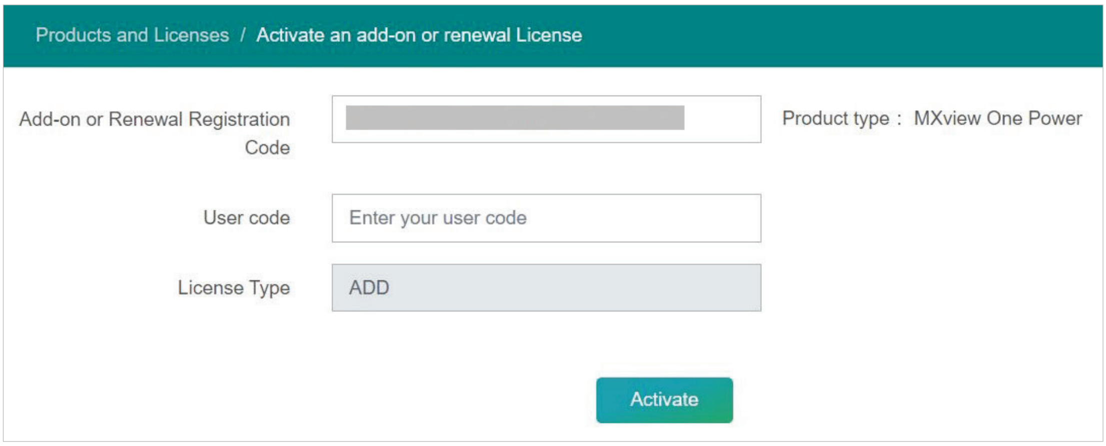


Products and Licenses / Activate an add-on or renewal License

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

Product type :

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



Products and Licenses / Activate an add-on or renewal License

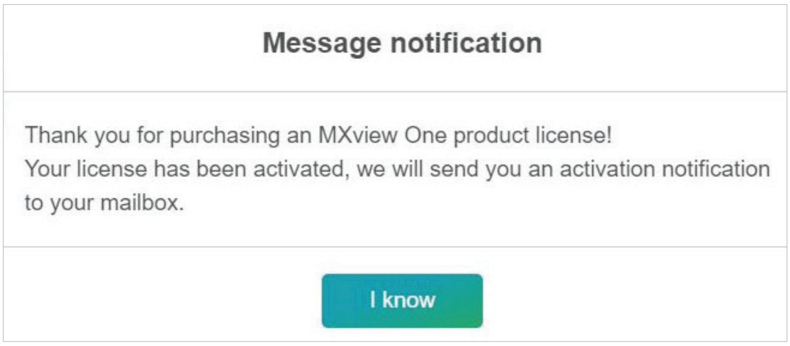
Add-on or Renewal Registration Code: [redacted]

Product type : MXview One Power

User code: Enter your user code

License Type: ADD

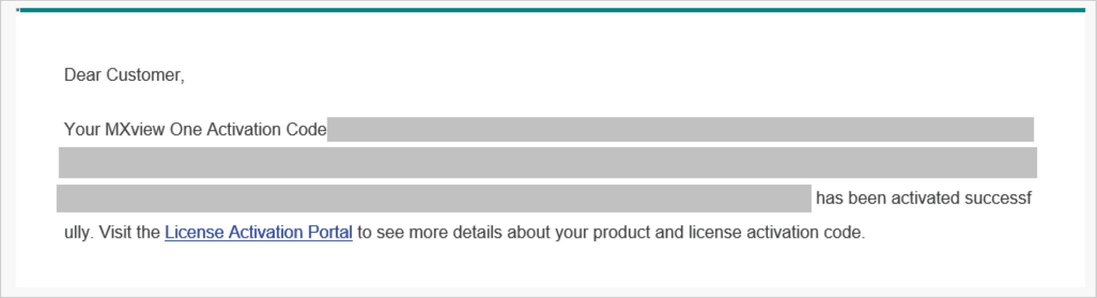
8. Once the process has been successfully completed, a pop-up window will appear to inform you that your license code has been activated. Click **I know** to close the window. If the license failed to activate, enter the correct Registration Code and User code again. If you are still experiencing problems,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



Message notification

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

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

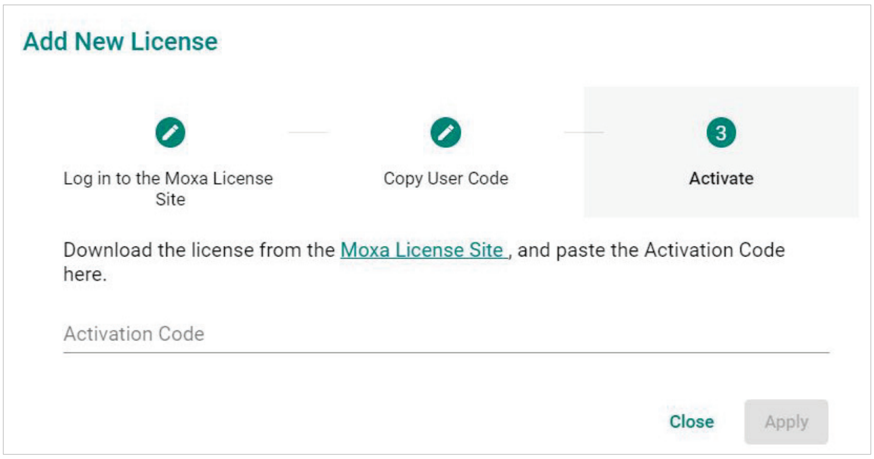


Dear Customer,

Your MXview One Activation Code [redacted] has been activated successfully. Visit the License Activation Portal to see more details about your product and license activation code.

10. Copy the activation code from the email.

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



Add New License

Log in to the Moxa License Site

Copy User Code

3 Activate

Download the license from the Moxa License Site , and paste the Activation Code here.

Activation Code

Close Apply

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.

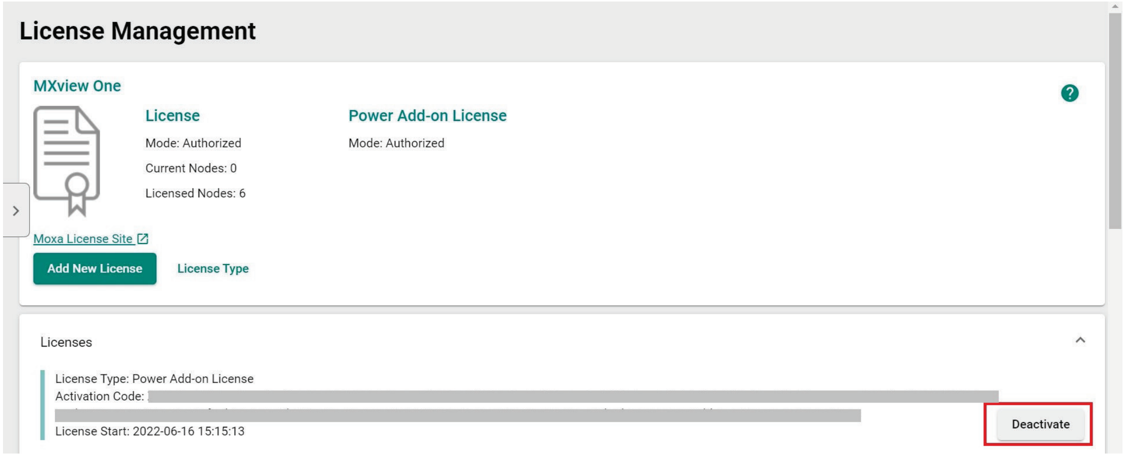
1. Navigate to **Menu** (☰) **> Administration > License Management**.

   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.



License Management

MXview One

License

Mode: Authorized

Current Nodes: 0

Licensed Nodes: 6

Power Add-on License

Mode: Authorized

Moxa License Site

Add New License License Type

Licenses

License Type: Power Add-on License

Activation Code: [redacted]

License Start: 2022-06-16 15:15:13

Deactivate

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

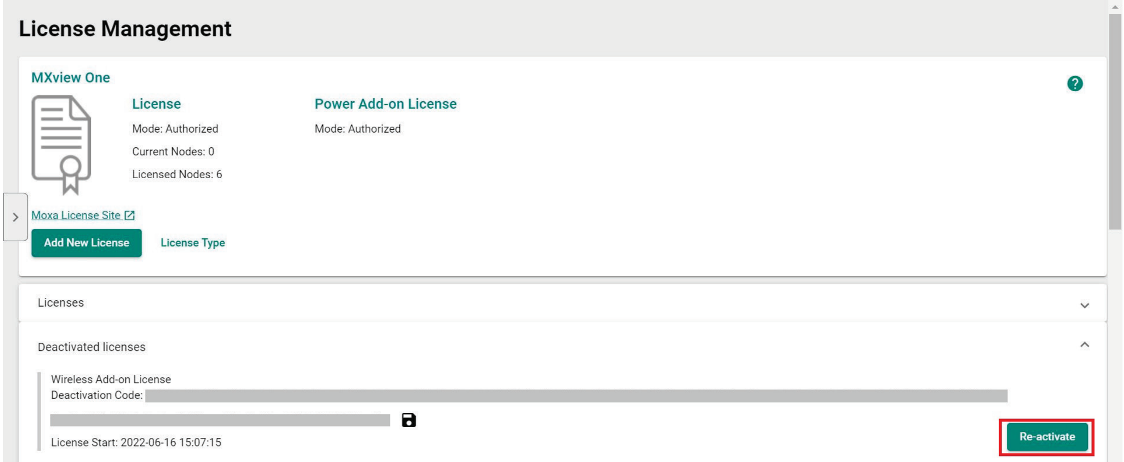
A deactivated license can be reactivated on the current instance of MXview One.

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.



License Management

MXview One

License

Mode: Authorized

Current Nodes: 0

Licensed Nodes: 6

Power Add-on License

Mode: Authorized

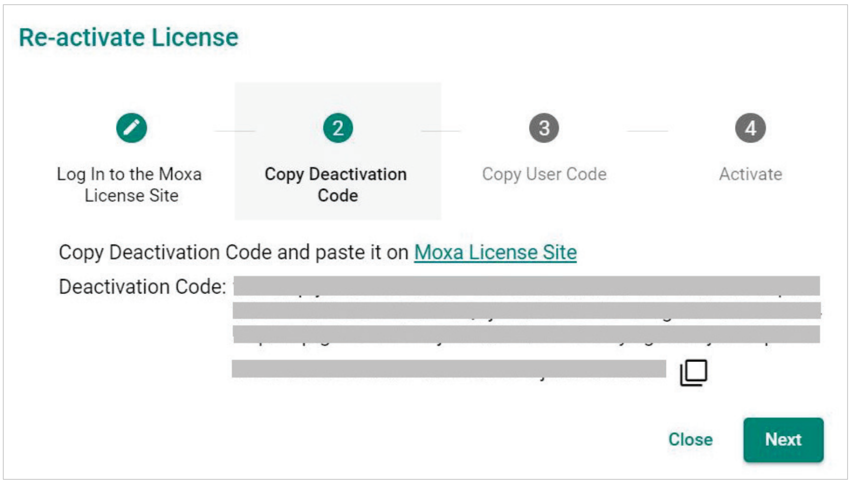
Deactivated licenses

Wireless Add-on License

Deactivation Code: [redacted]

License Start: 2022-06-16 15:07:15

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



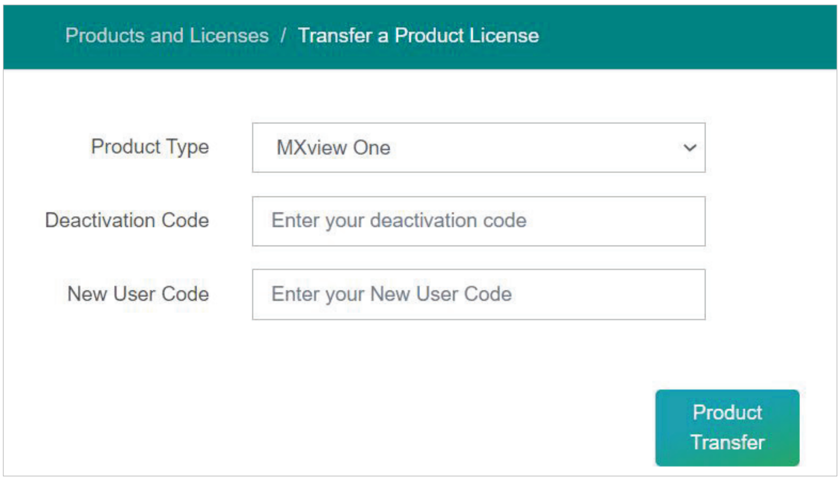
Re-activate License

Copy Deactivation Code and paste it on Moxa License Site

Deactivation Code: [redacted]

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**.



Products and Licenses / Transfer a Product License

Product Type: MXview One

Deactivation Code: Enter your deactivation code

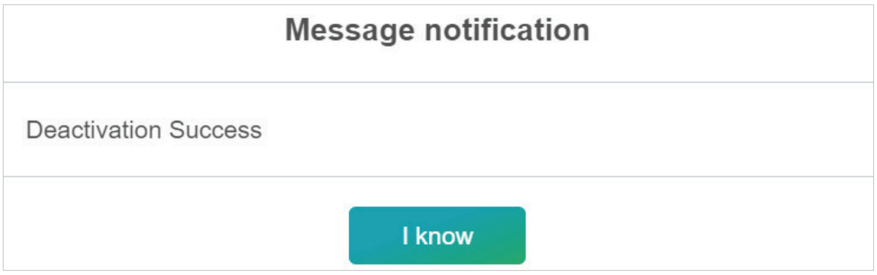
New User Code: Enter your New User Code

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.

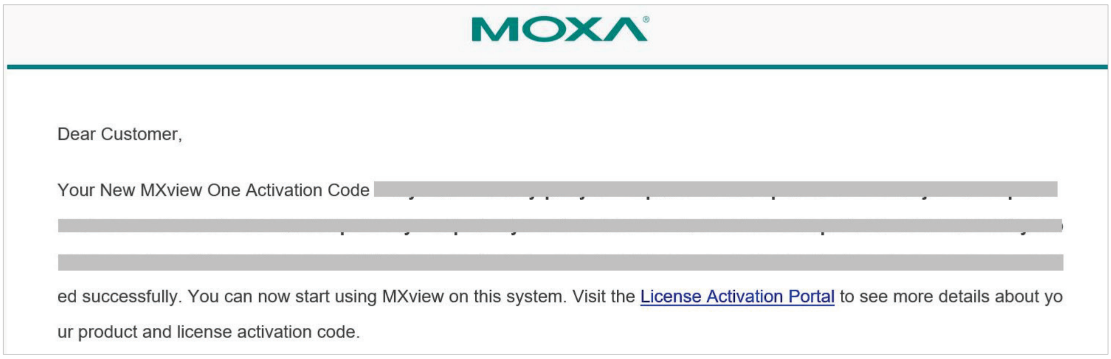
8. Once the process has been successfully completed, a pop-up window will appear to inform you that your license code has been deactivated. Click **I know** to close the window. If the license failed to deactivate, enter the license key again. If you are still experiencing problems, please contact Moxa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



Message notification

Deactivation Success

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



Dear Customer,

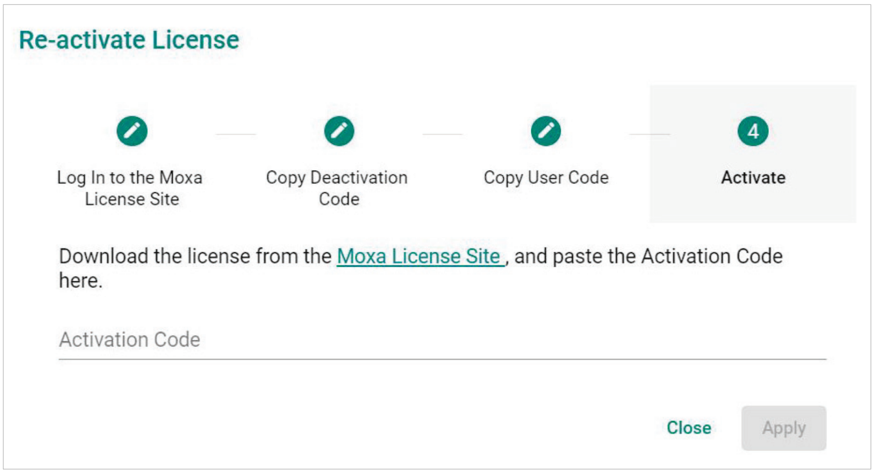
Your New MXview One Activation Code [redacted]

ed successfully. You can now start using MXview on this system. Visit the License Activation Portal to see more details about yo

ur product and license activation code.

10. Copy the activation code from the email.

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



Download the license from the Moxa License Site , and paste the Activation Code here.

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

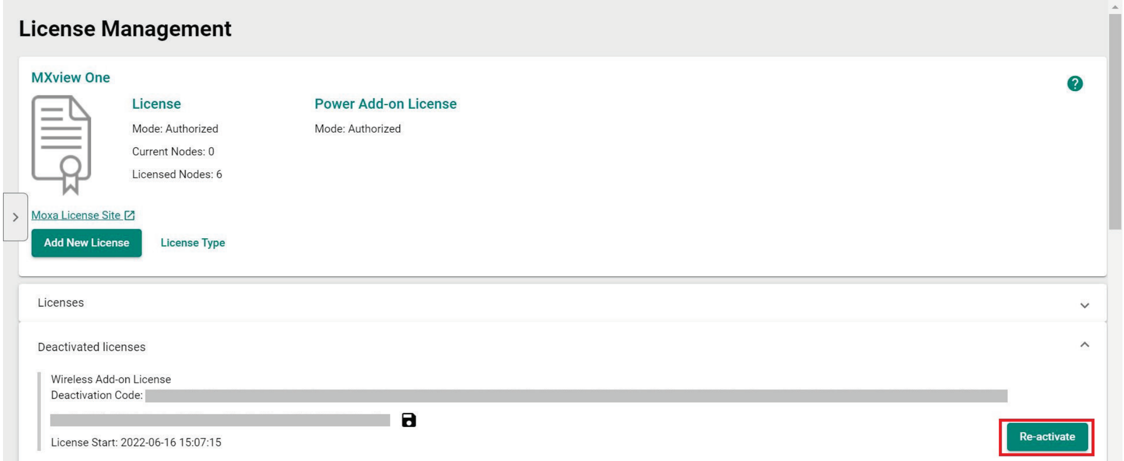
Transferring a License to a Different Instance of MXview One

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.



License: Mode: Authorized
Current Nodes: 0
Licensed Nodes: 6

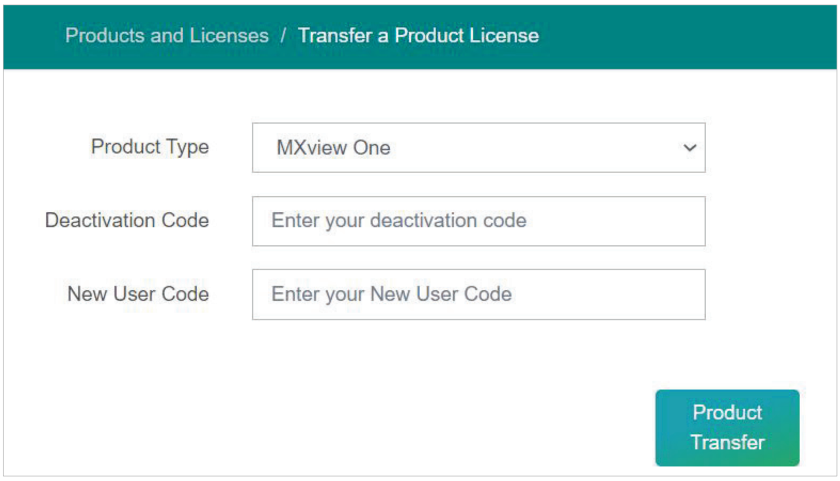
Power Add-on License: Mode: Authorized

Wireless Add-on License
Deactivation Code: [redacted]
License Start: 2022-06-16 15:07:15

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**.



Products and Licenses / Transfer a Product License

Product Type: MXview One

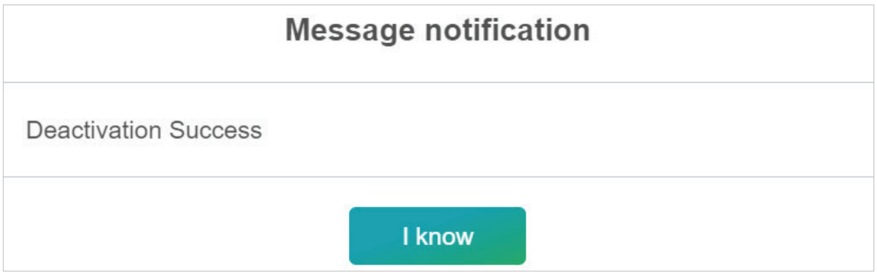
Deactivation Code: Enter your deactivation code

New User Code: Enter your New User Code

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.

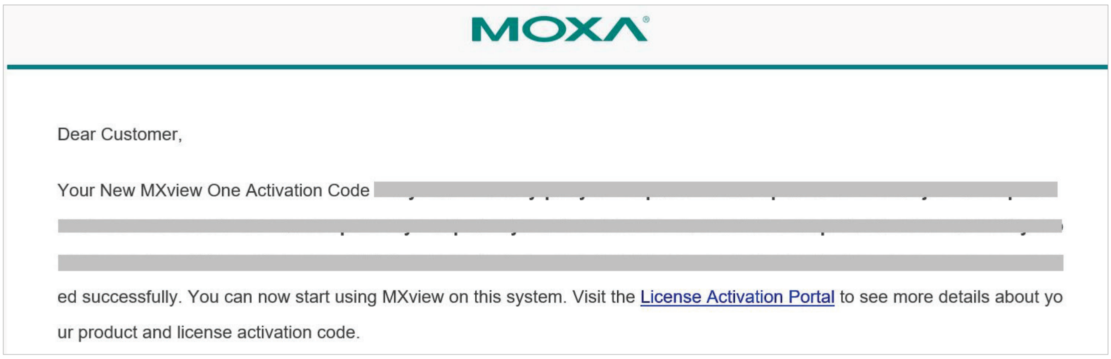
6. Once the process has been successfully completed, a pop-up window will appear to inform you that your license code has been deactivated. Click **I know** to close the window. If the license failed to deactivate, enter the license key again. If you are still experiencing problems, please contact Moxa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



Message notification

Deactivation Success

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



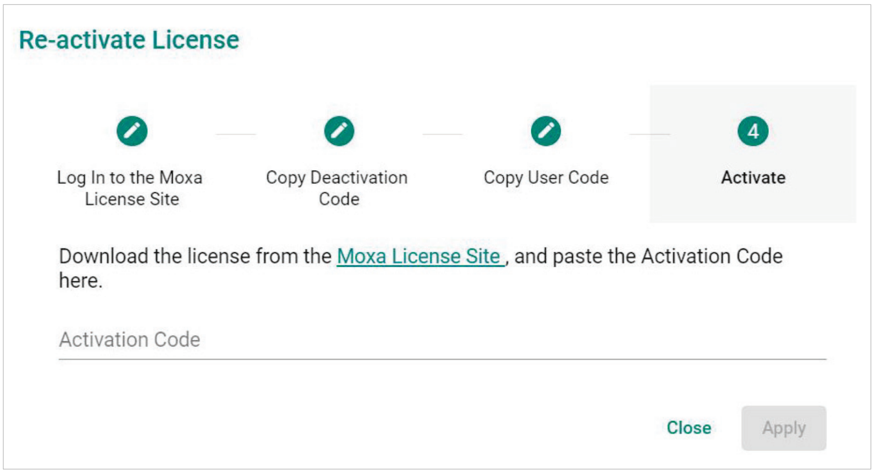
Dear Customer,

Your New MXview One Activation Code [redacted]

ed successfully. You can now start using MXview on this system. Visit the License Activation Portal to see more details about yo ur product and license activation code.

8. Copy the activation code from the email.

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



Re-activate License

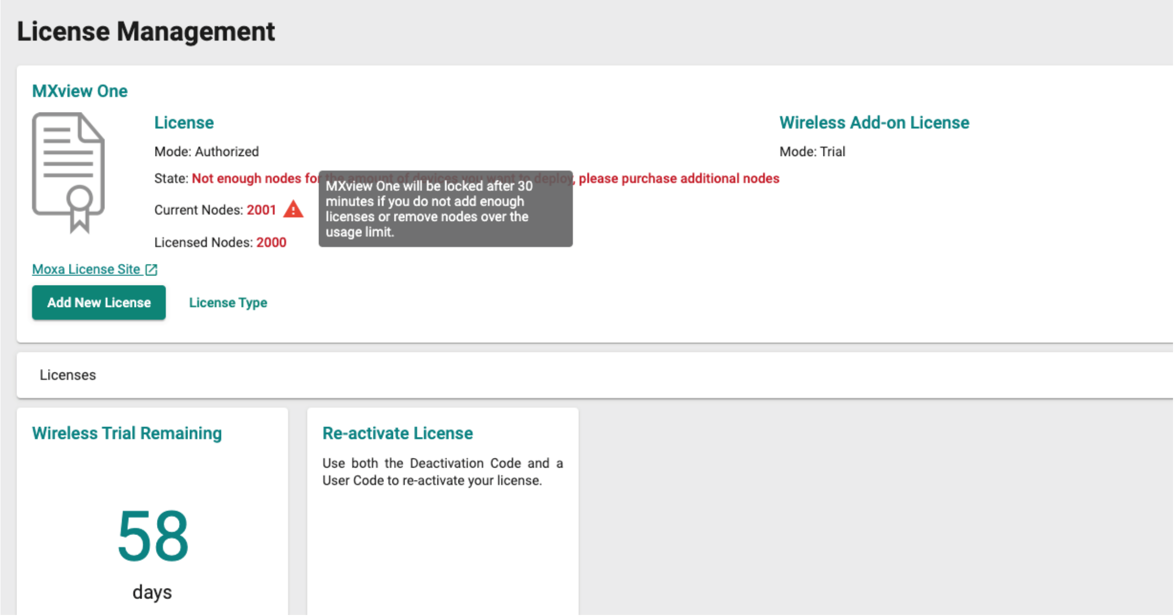
Download the license from the Moxa License Site , and paste the Activation Code here.

Activation Code

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.



License Management

MXview One

License

Mode: Authorized

State: Not enough nodes for the amount of devices you want to deploy, please purchase additional nodes

Current Nodes: 2001 ⚠

Licensed Nodes: 2000

MXview One will be locked after 30 minutes if you do not add enough licenses or remove nodes over the usage limit.

Wireless Add-on License

Mode: Trial

Wireless Trial Remaining

58

days

Re-activate License

Use both the Deactivation Code and a User Code to re-activate your license.

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

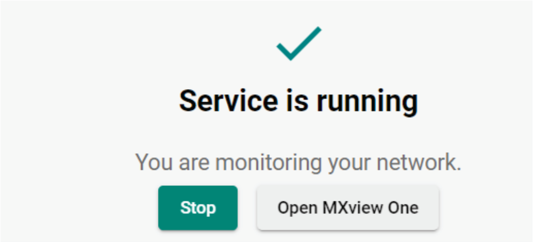
   Order the required quantity of Node-based Licenses from your channel or Moxa Sales Representative. Then, follow the instructions on **Adding a New License** to activate a new license.

2. **Delete Extra Devices**

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

b. Please follow the instructions below:

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



Service is running

You are monitoring your network.

- ❒ 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.

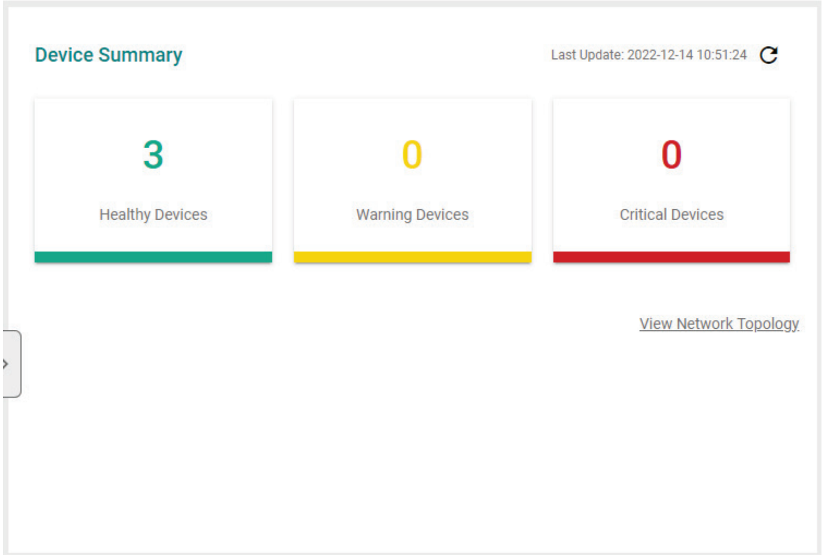
The **Dashboard** displays the following widgets:

- 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:



Device Summary

Last Update: 2022-12-14 10:51:24

3 Healthy Devices

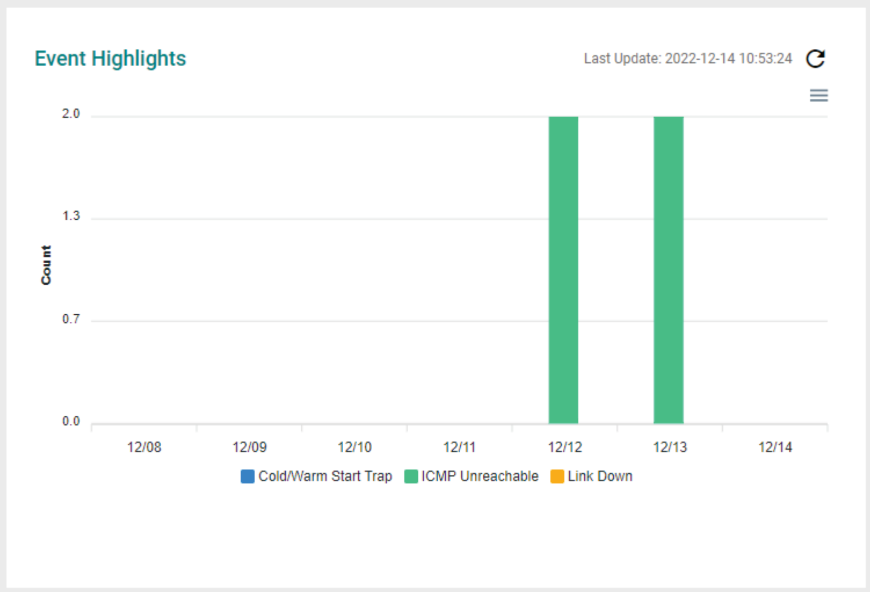
0 Warning Devices

0 Critical Devices

- **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

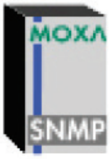
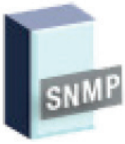
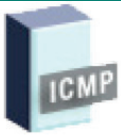
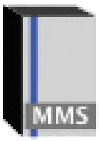
Device Discovery Overview

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

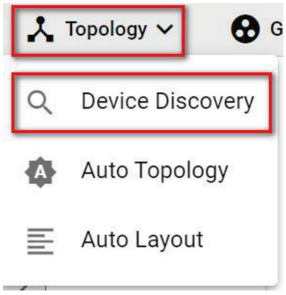
MXview One will display one of the following graphics to indicate devices:

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.	

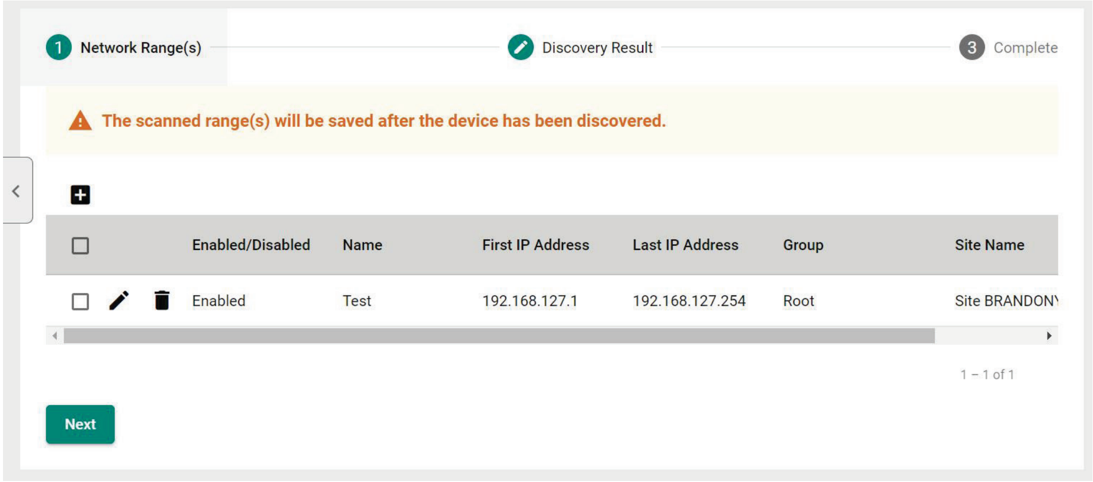
Configuring IP Address Scan Ranges

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.



1 Network Range(s) — Discovery Result — 3 Complete

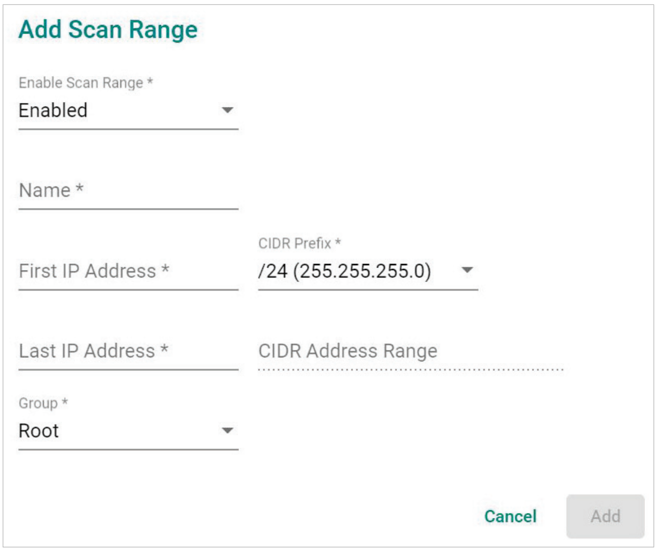
⚠ The scanned range(s) will be saved after the device has been discovered.

□		Enabled/Disabled	Name	First IP Address	Last IP Address	Group	Site Name
□	✎ 🗑	Enabled	Test	192.168.127.1	192.168.127.254	Root	Site BRANDON\

1 – 1 of 1

Next

2. To add a new scan range:
   a. Click the **Add** (⊞) button in the top left corner.
   The **Add Scan Range** screen will appear.



Add Scan Range

Enable Scan Range *
Enabled

Name *

First IP Address *

CIDR Prefix *
/24 (255.255.255.0)

Last IP Address *

CIDR Address Range

Group *
Root

Cancel Add

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.

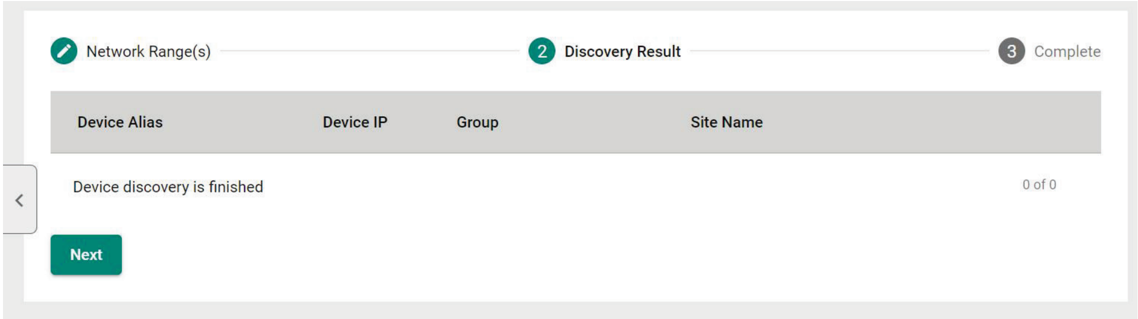
The **Edit Scan Range** screen appears.

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.



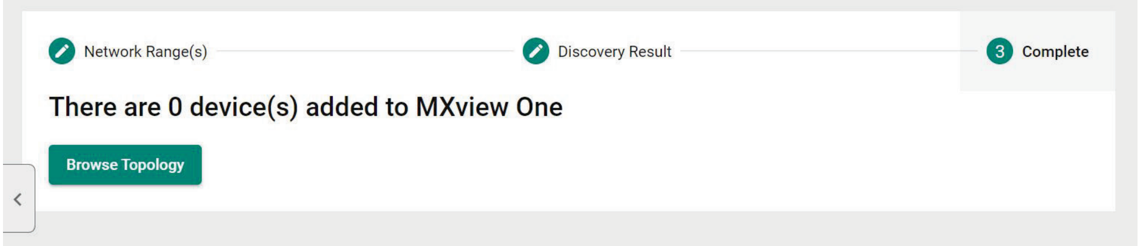
Device Alias	Device IP	Group	Site Name

Device discovery is finished

0 of 0

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

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



There are 0 device(s) 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

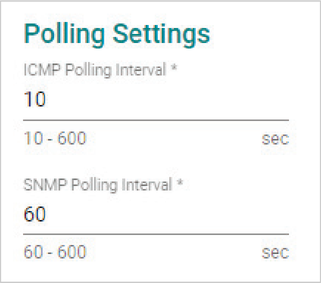
Devices in the assigned scan range can be discovered via SNMP and ICMP protocols. (The default polling interval of ICMP is 10 seconds, while SNMP is 60 seconds. Users can go to the **Default Device Template** page to change the polling intervals.) After a device is discovered, MXview One will use SNMP 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 > Default Device Template**.

   The **Default Device Template** screen appears.
2. Scroll down to the **Polling Settings** section.



Polling Settings

ICMP Polling Interval *

10

10 - 600 sec

SNMP Polling Interval *

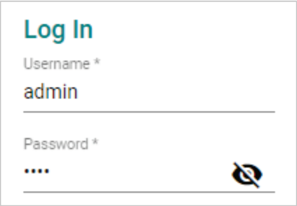
60

60 - 600 sec

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



Log In

Username *

admin

Password *

••••

6. Click **Save**.

   MXview One will update the modified settings.

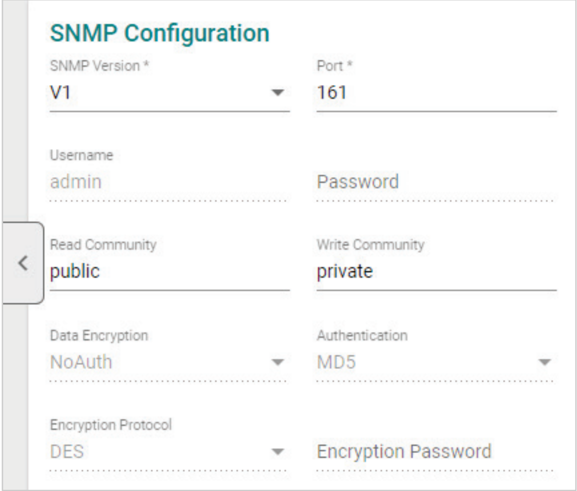
Changing Default SNMP Configuration

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

1. Navigate to **Menu** (☰) **> Administration > Default Device Template**.

   The **Default Device Template** screen will appear.

2. Scroll down to the **SNMP Configuration** section.



SNMP Configuration

SNMP Version * V1

Port * 161

Username admin

Password

Read Community public

Write Community private

Data Encryption NoAuth

Authentication MD5

Encryption Protocol DES

Encryption Password

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**.

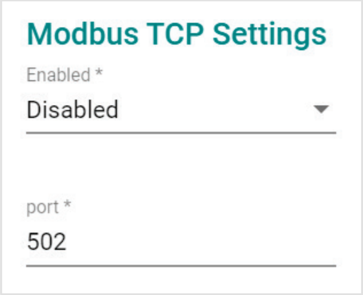
   MXview One updates the modified settings.

Changing Modbus TCP Settings

By configuring Modbus TCP Settings in the Default Device Template section, MXview One will be able to detect whether a device has Modbus attributes or not. If a device supports Modbus, a Modbus string will appear above the device icon in the topology to easily identify the device.

1. Navigate to **Menu** (☰) **> Administration > Default Device Template**.

   The **Default Device Template** screen will appear.
2. Scroll down to the **Modbus TCP Settings** section.



Modbus TCP Settings

Enabled *

Disabled

port *

502

3. Configure the following:

   a. **Enabled:** Enable or disabled Modbus TCP settings

      ❒ Enabled

      ❒ Disabled

   b. **Port:** Specify the Modbus TCP port
4. Click **Save**.

   MXview One updates the modified settings.

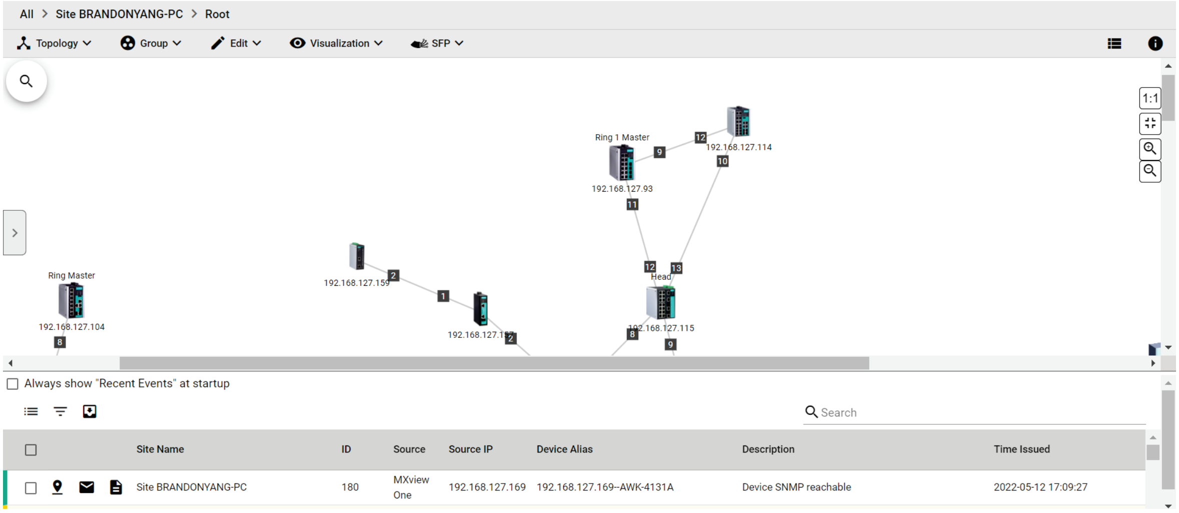
7. Topology Management

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.



□ Always show "Recent Events" at startup

Search

□	Site Name	ID	Source	Source IP	Device Alias	Description	Time Issued
□	Site BRANDONYANG-PC	180	MXview One	192.168.127.169	192.168.127.169--AWK-4131A	Device SNMP reachable	2022-05-12 17:09:27

Viewing the 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.

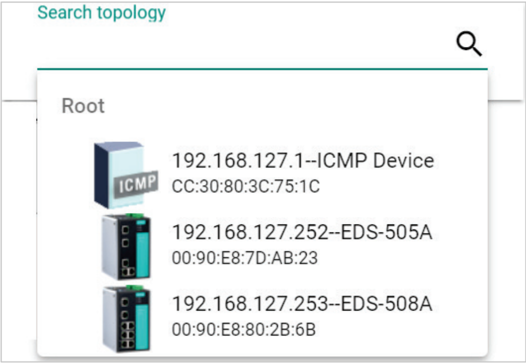
2. If the **List view** is displayed, click the **Topology view** ( ) icon in the top right corner.

   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.



Search topology

Root

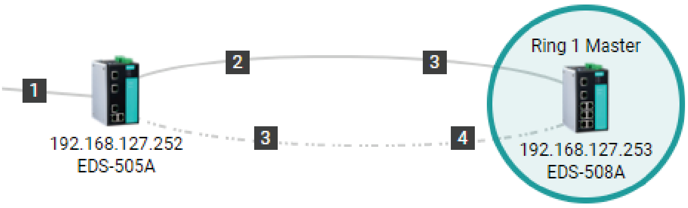
192.168.127.1--ICMP Device
CC:30:80:3C:75:1C

192.168.127.252--EDS-505A
00:90:E8:7D:AB:23

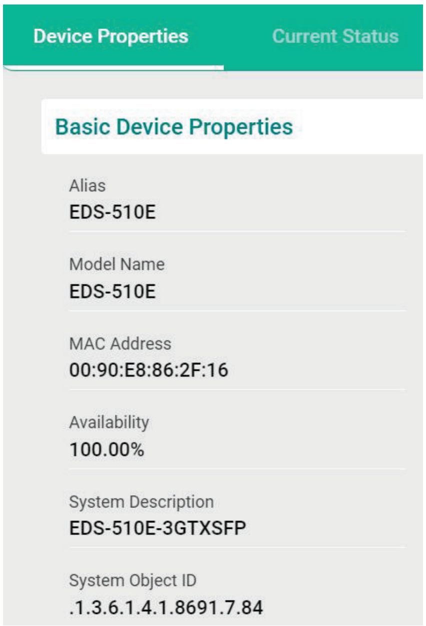
192.168.127.253--EDS-508A
00:90:E8:80:2B:6B

   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.



Device Properties | Current Status

Basic Device Properties

Alias
EDS-510E

Model Name
EDS-510E

MAC Address
00:90:E8:86:2F:16

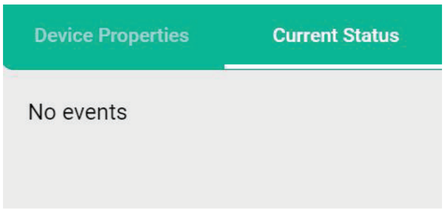
Availability
100.00%

System Description
EDS-510E-3GTXSFP

System Object ID
.1.3.6.1.4.1.8691.7.84

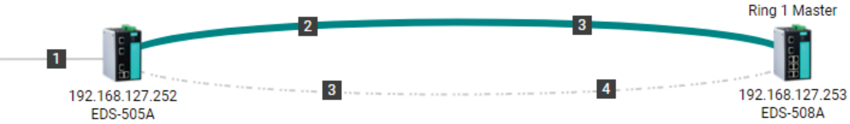
5. To view events associated with the device, click the **Current Status**.

   The **Current Status** pane displays events associated with the device.

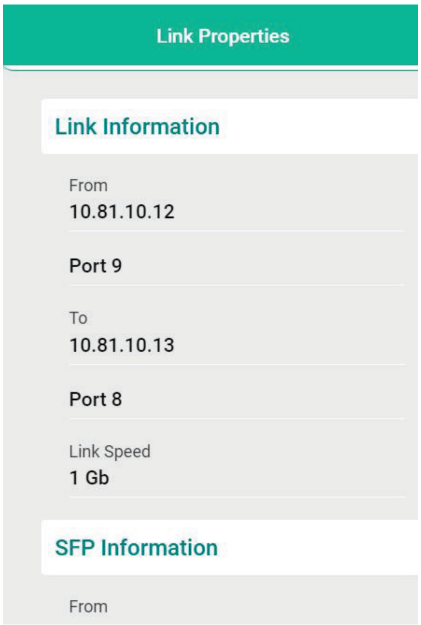


No events

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



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



Link Information

From
10.81.10.12

Port 9

To
10.81.10.13

Port 8

Link Speed
1 Gb

SFP Information

From

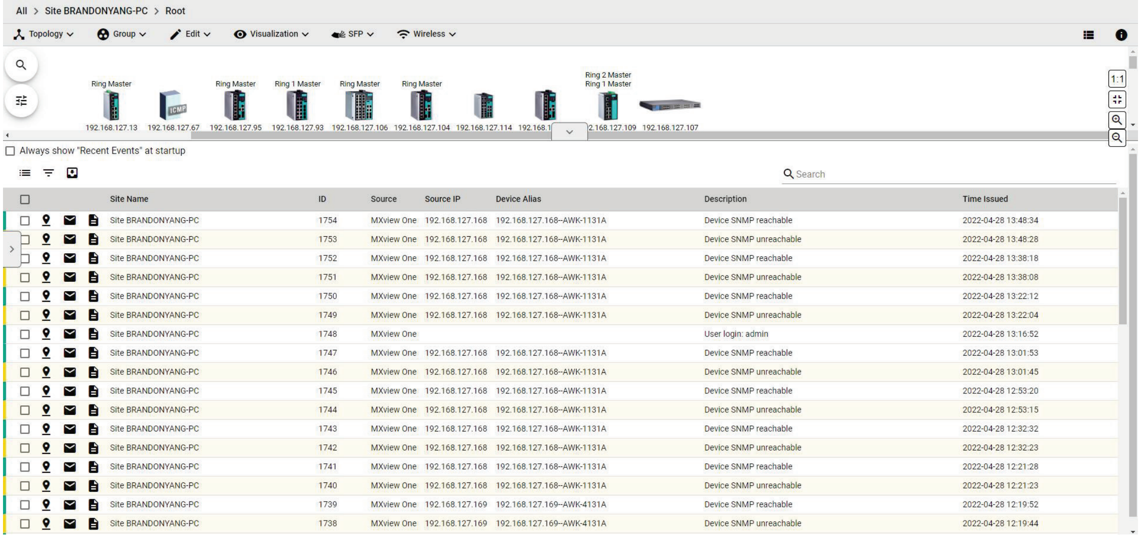
Viewing Recent Events

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 Event Monitoring.

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

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



□ Always show "Recent Events" at startup

□	Site Name	ID	Source	Source IP	Device Alias	Description	Time Issued
□	Site BRANDONYANG-PC	1754	MXview One	192.168.127.168	192.168.127.168--AWK-1131A	Device SNMP reachable	2022-04-28 13:48:34
□	Site BRANDONYANG-PC	1753	MXview One	192.168.127.168	192.168.127.168--AWK-1131A	Device SNMP unreachable	2022-04-28 13:48:28
□	Site BRANDONYANG-PC	1752	MXview One	192.168.127.168	192.168.127.168--AWK-1131A	Device SNMP reachable	2022-04-28 13:38:18
□	Site BRANDONYANG-PC	1751	MXview One	192.168.127.168	192.168.127.168--AWK-1131A	Device SNMP unreachable	2022-04-28 13:38:08
□	Site BRANDONYANG-PC	1750	MXview One	192.168.127.168	192.168.127.168--AWK-1131A	Device SNMP reachable	2022-04-28 13:22:12
□	Site BRANDONYANG-PC	1749	MXview One	192.168.127.168	192.168.127.168--AWK-1131A	Device SNMP unreachable	2022-04-28 13:22:04
□	Site BRANDONYANG-PC	1748	MXview One			User login: admin	2022-04-28 13:16:52
□	Site BRANDONYANG-PC	1747	MXview One	192.168.127.168	192.168.127.168--AWK-1131A	Device SNMP reachable	2022-04-28 13:01:53
□	Site BRANDONYANG-PC	1746	MXview One	192.168.127.168	192.168.127.168--AWK-1131A	Device SNMP unreachable	2022-04-28 13:01:45
□	Site BRANDONYANG-PC	1745	MXview One	192.168.127.168	192.168.127.168--AWK-1131A	Device SNMP reachable	2022-04-28 12:53:20
□	Site BRANDONYANG-PC	1744	MXview One	192.168.127.168	192.168.127.168--AWK-1131A	Device SNMP unreachable	2022-04-28 12:53:15
□	Site BRANDONYANG-PC	1743	MXview One	192.168.127.168	192.168.127.168--AWK-1131A	Device SNMP reachable	2022-04-28 12:32:32
□	Site BRANDONYANG-PC	1742	MXview One	192.168.127.168	192.168.127.168--AWK-1131A	Device SNMP unreachable	2022-04-28 12:32:23
□	Site BRANDONYANG-PC	1741	MXview One	192.168.127.168	192.168.127.168--AWK-1131A	Device SNMP reachable	2022-04-28 12:21:28
□	Site BRANDONYANG-PC	1740	MXview One	192.168.127.168	192.168.127.168--AWK-1131A	Device SNMP unreachable	2022-04-28 12:21:23
□	Site BRANDONYANG-PC	1739	MXview One	192.168.127.169	192.168.127.169--AWK-4131A	Device SNMP reachable	2022-04-28 12:19:52
□	Site BRANDONYANG-PC	1738	MXview One	192.168.127.169	192.168.127.169--AWK-4131A	Device SNMP unreachable	2022-04-28 12:19:44

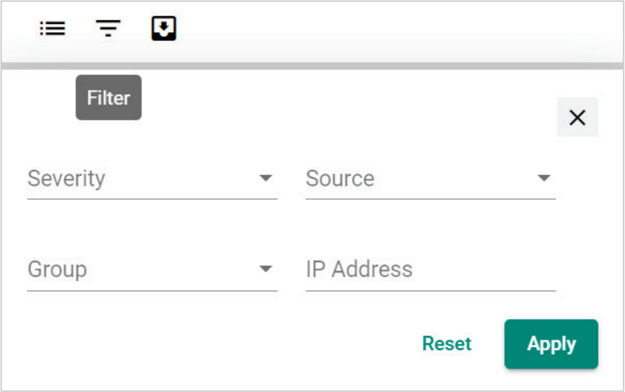
2. To filter the information in the table, type a full or partial string that matches the value in any of the table columns on the right of the search space.

   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
- ❒ **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.

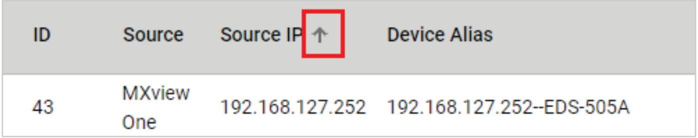
4. To acknowledge the events in the table:

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.

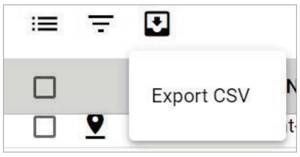
MXview One sorts the table by the column.



ID	Source	Source IP ↑	Device Alias
43	MXview One	192.168.127.252	192.168.127.252--EDS-505A

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.

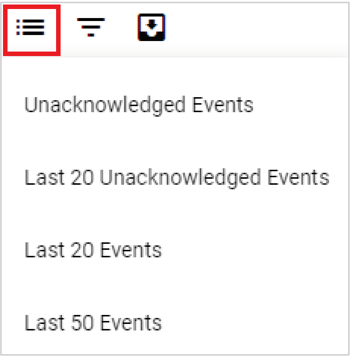
d. Click **Save**.

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

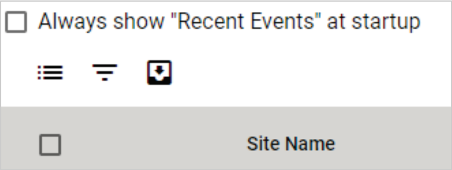
7. To quickly filter event, click the **Quick filter event** (☰) icon to find the events.

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.


☐ Always show "Recent Events" at startup

☐	Site Name

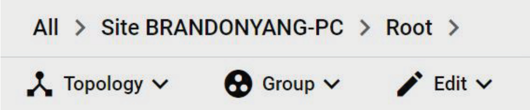
Organizing the Topology Structure By Group Function

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.

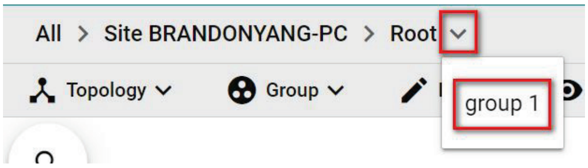
1. Navigate to **Menu** (☰) **> Topology**.

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

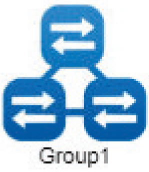
   - MXview One represents the Topology Map structure by a path at the top of the **Topology** screen:

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

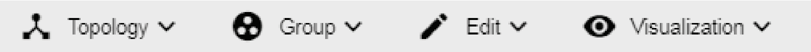
     

   - You can also click the following icon used to indicate user-defined groups within the Topology Map:

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

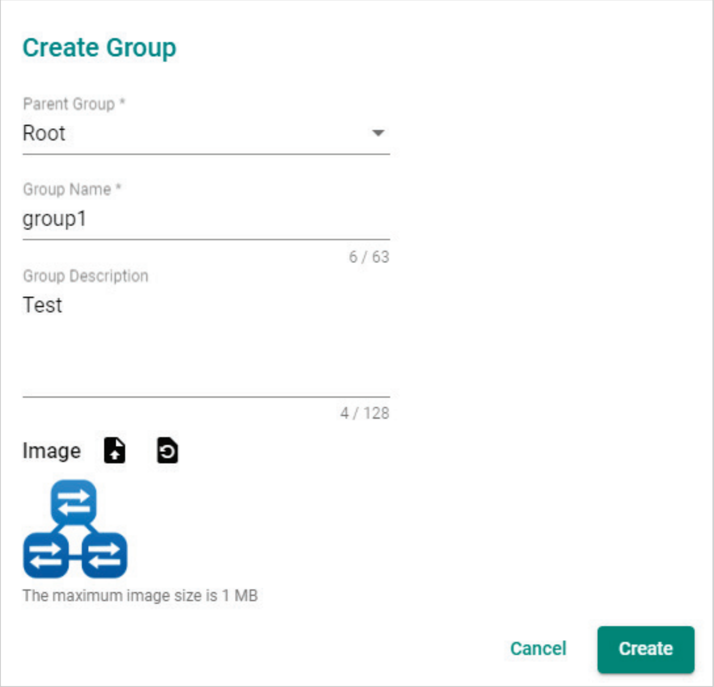
   The **Topology** screen displays the following toolbar above the Topology Map:

3. To create a group:

   a. Navigate to **Group > Create Group**.

      The **Create Group** screen appears.



Create Group

Parent Group *
Root

Group Name *
group1
6 / 63

Group Description
Test
4 / 128

   b. Configure the following:

      ❒ Parent Group

      ❒ Group Name

      ❒ Group Description

      ❒ Group Icon

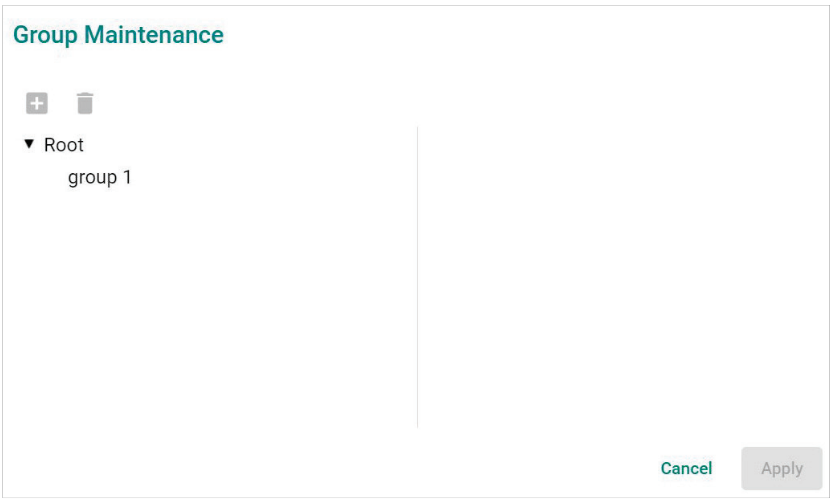
   c. Click **Create**.

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

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

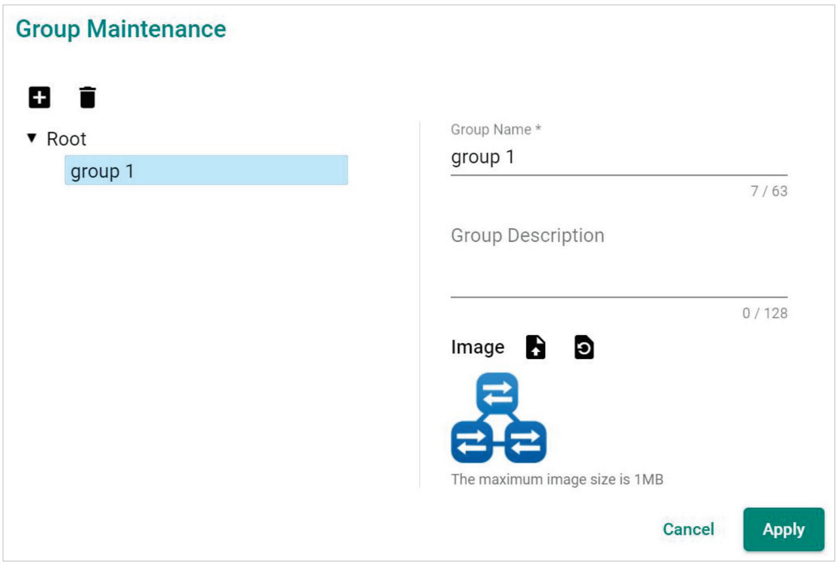
   a. Navigate to **Group > Group Maintenance**.

      The **Group Maintenance** screen appears.



Group Maintenance

b. Select a layer to modify.
   The group details appear to the right of the topology directory tree.



Group Maintenance

▼ Root
- group 1

Group Name *
group 1
7 / 63

Group Description
0 / 128

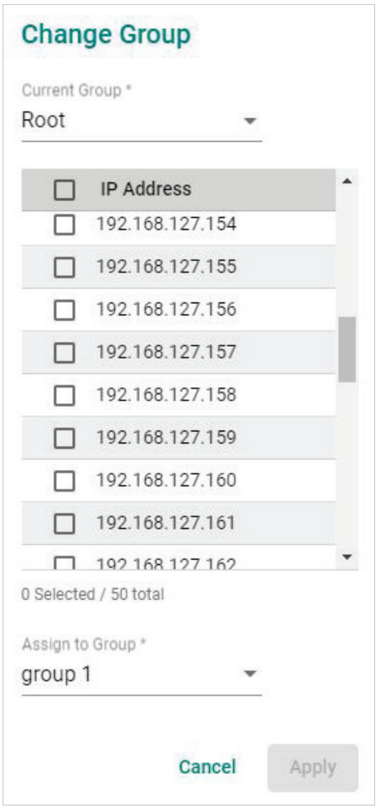
Image

The maximum image size is 1MB

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.



Change Group

Current Group *
Root

□	IP Address
□	192.168.127.154
□	192.168.127.155
□	192.168.127.156
□	192.168.127.157
□	192.168.127.158
□	192.168.127.159
□	192.168.127.160
□	192.168.127.161
□	192.168.127.162

0 Selected / 50 total

Assign to Group *
group 1

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.

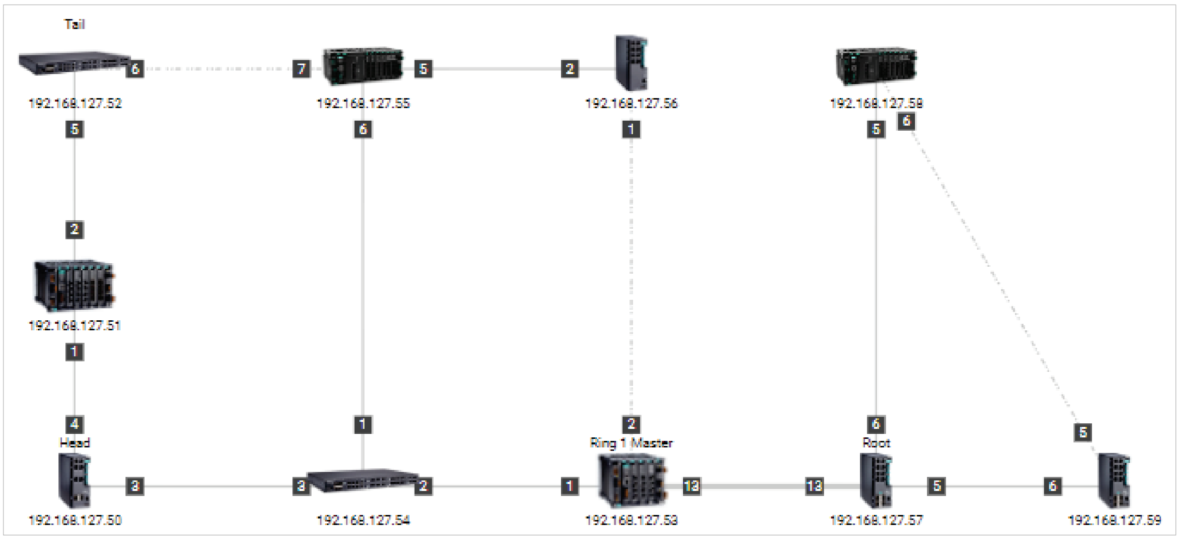
c. Select the IP address(es) of the device(s) that you want to reassign to a different group.

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.

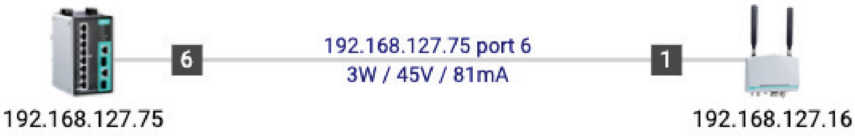
- RSTP has a **Root**
- Turbo Ring has a **Master**
- Turbo Chain has a **Head** and a **Tail**
- Dual Homing

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

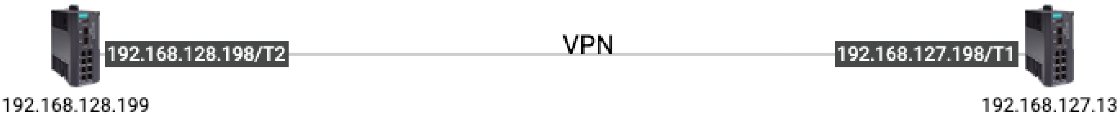
By periodic polling, a PoE link will display the port number, power (watts), voltage (V), and current (mA) directly on the topology map.



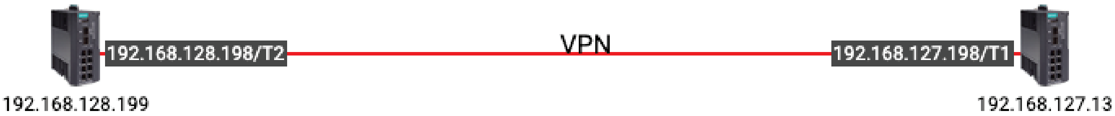
VPN Tunnel Visualization

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

1. The VPN tunnel is connected.



2. The VPN tunnel is disconnected.

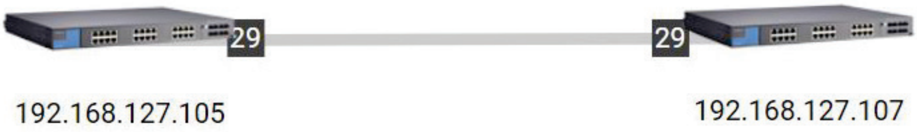


NOTE

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.

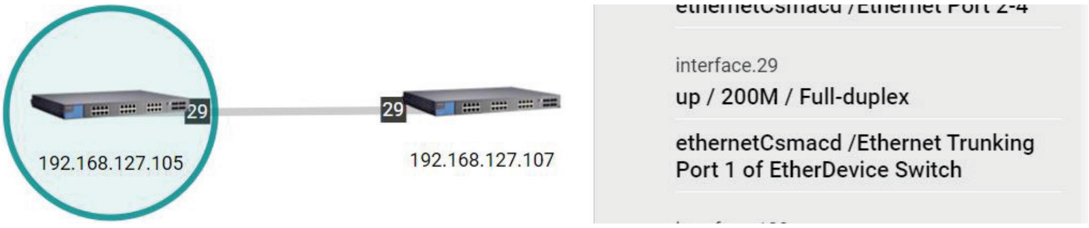


NOTE

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.



ethernetCsmacd /Ethernet Port 2-4

interface.29

up / 200M / Full-duplex

ethernetCsmacd /Ethernet Trunking Port 1 of EtherDevice Switch

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.

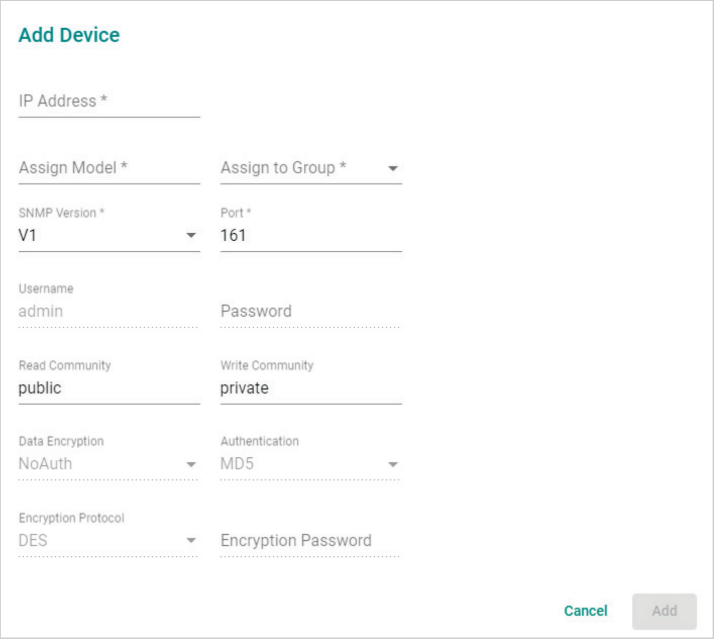
1. Navigate to **Menu** (☰) **> Topology**.

   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.



Add Device

IP Address *

Assign Model *

Assign to Group *

SNMP Version * V1

Port * 161

Username admin

Password

Read Community public

Write Community private

Data Encryption NoAuth

Authentication MD5

Encryption Protocol DES

Encryption Password

   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**

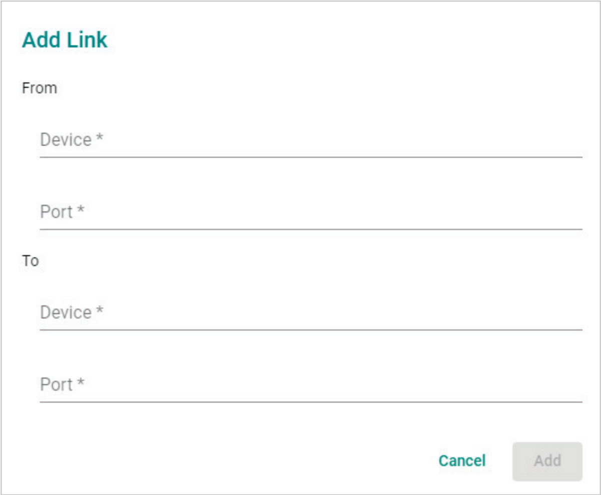
   c. Click **Add**.

   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.



Add Link

From

Device *

Port *

To

Device *

Port *

   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

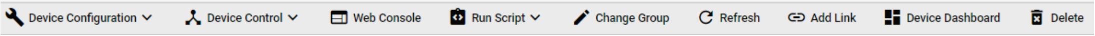
You can delete devices and links from the Topology Map. After a device is deleted, it will be removed from the topology map, and the device will not be polled or located when performing Device Discovery. Deleting a link will delete a link from the topology map, but it will not affect the actual network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

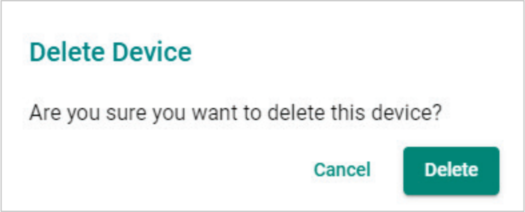
   a. Select the device.

   The following toolbar menu will appear.

   b. Click **Delete**.

   A confirmation screen will appear.

   Delete Device

   Are you sure you want to delete this device?

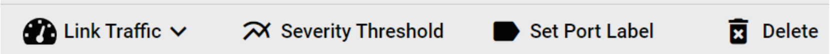
   c. Click **Delete**.

   MXview One deletes the device from the Topology Map.

3. To delete a link from the Topology Map:

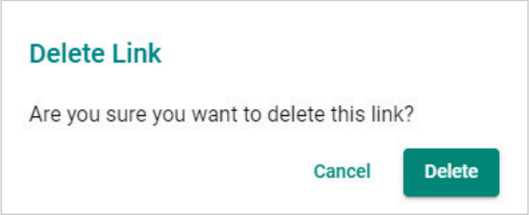
   a. Select the link.

   The following toolbar menu will appear.

   b. Click **Delete**.

   A confirmation screen will appear.

   Delete Link

   Are you sure you want to delete this link?

   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**.

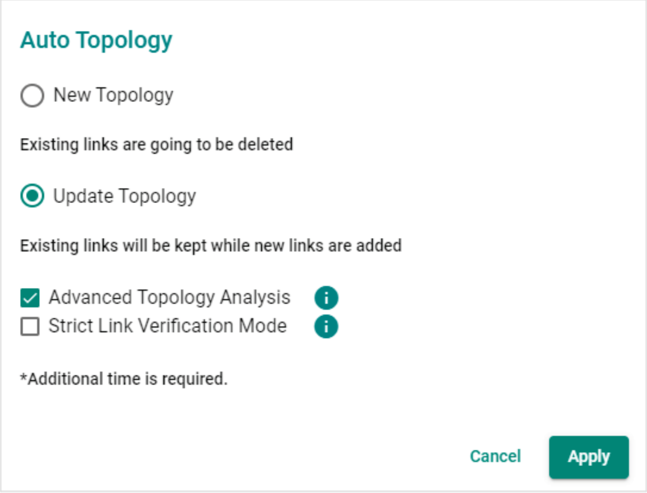
   The **Topology** screen appears and displays the Topology Map by default.

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.



Auto Topology

○ New Topology

Existing links are going to be deleted

● Update Topology

Existing links will be kept while new links are added

☑ Advanced Topology Analysis

□ Strict Link Verification Mode

*Additional time is required.

4. Select **Update Topology**.
5. (Optional) Select **Advanced Topology Analysis** to draw links for devices without an LLDP MIB.
6. (Optional) Select **Strict Link Verification Mode**. If enabled, links between devices will only be shown on the topology if the devices on both ends have the other device's information in their LLDP table.
7. 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

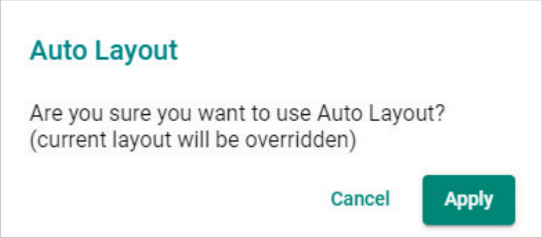
After changes have been made, use the **Auto Layout** feature to refresh the layout of the Topology Map. Auto Layout does not update any devices or links. It only redraws the topology to better fit the screen.

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.



Auto Layout

Are you sure you want to use Auto Layout?
(current layout will be overridden)

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**.

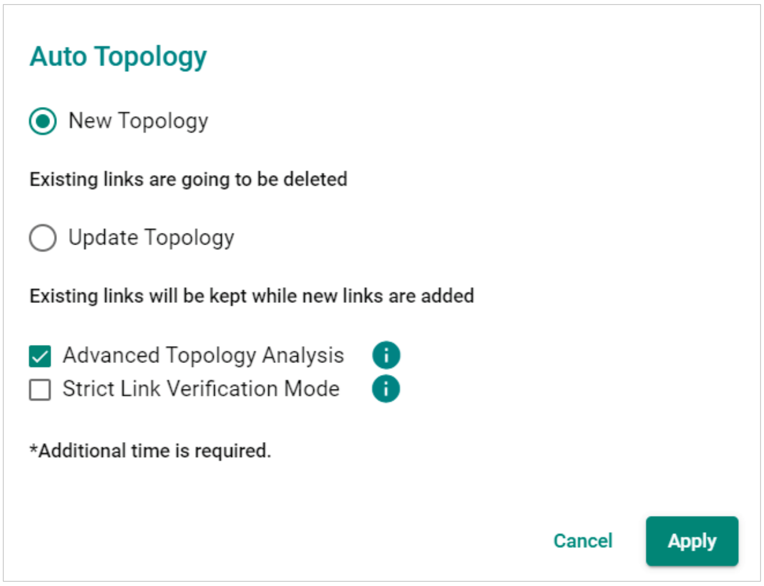
   The **Topology** screen appears and displays the Topology Map by default.

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.



Auto Topology

● New Topology

Existing links are going to be deleted

○ Update Topology

Existing links will be kept while new links are added

☑ Advanced Topology Analysis ⓘ
□ Strict Link Verification Mode ⓘ

*Additional time is required.

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**.

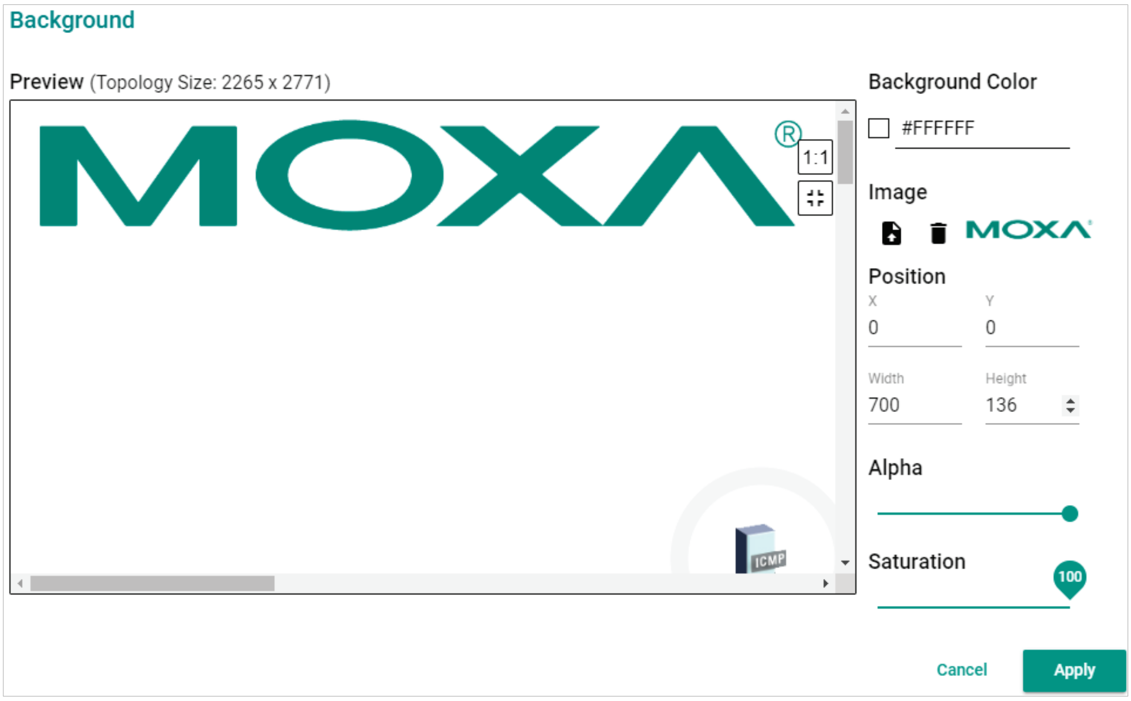
   The **Topology** screen appears and will display the Topology Map by default.

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.



Background

Preview (Topology Size: 2265 x 2771)

Background Color: □ #FFFFFF

Image

Position: X 0, Y 0

Width 700, Height 136

Alpha

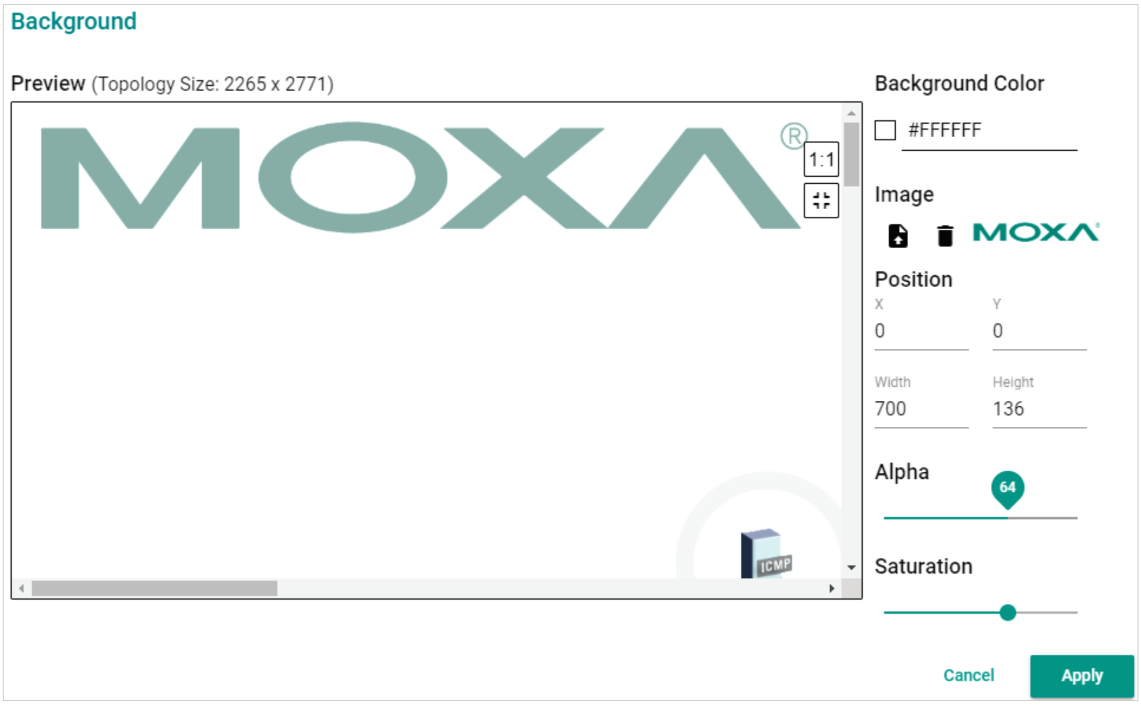
Saturation 100

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.



Background

Preview (Topology Size: 2265 x 2771)

Background Color

□ #FFFFFF

Image

Position

X: 0

Y: 0

Width: 700

Height: 136

Alpha: 64

Saturation

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

Editing the Topology Appearance

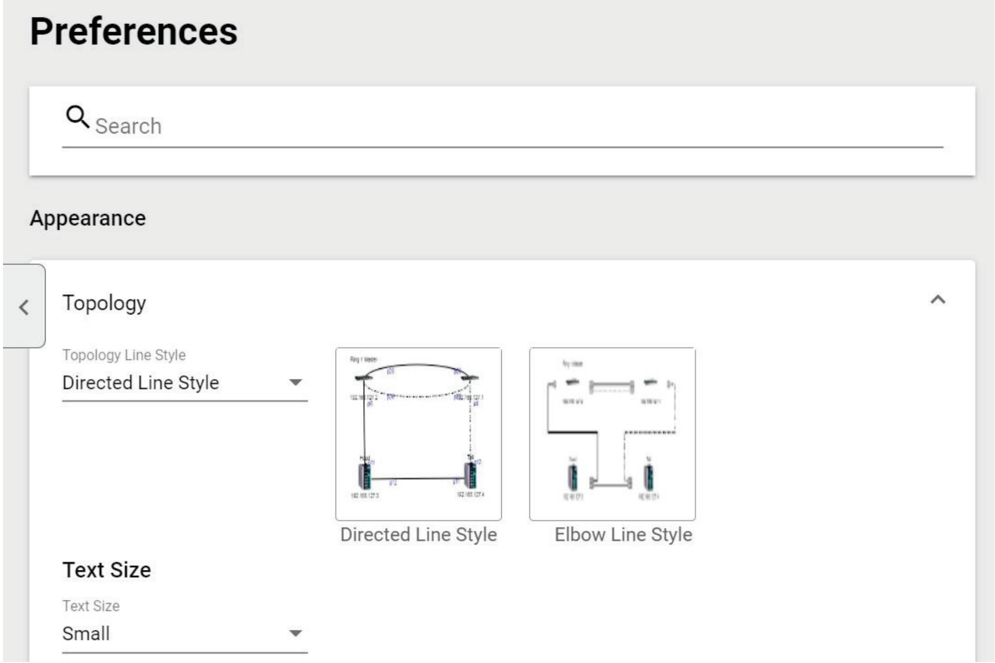
Use the **Preferences** screen to modify how the Topology Map displays the topology line style, PoE status, background color, link status, and traffic load.

1. Navigate to **Menu** (☰) **> Administration > Preferences.**.

   The **Preferences** screen appears.

2. In the **Appearance** section, expand **Topology**.

   The **Topology** settings appear.



Preferences

Appearance

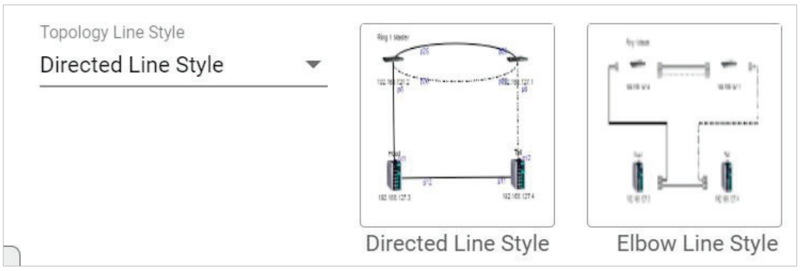
Topology

Topology Line Style: Directed Line Style

Text Size

Text Size: Small

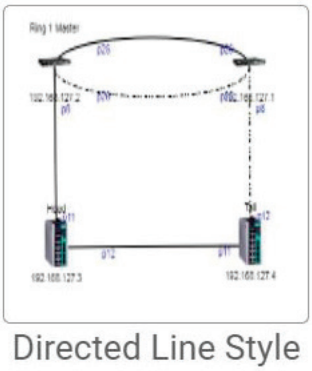
3. To modify the Topology Line Style, select one of the following from the drop-down list:



Topology Line Style: Directed Line Style

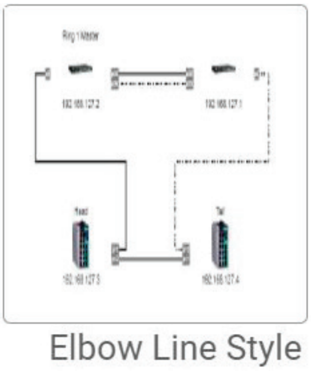
- **Directed Line Style**

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



- **Elbow Line Style**

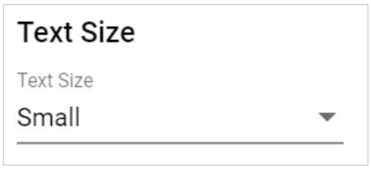
  MXview One applies the following style to the lines indicating the links between devices in the Topology Map:



4. To modify the text size in MXview One:

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

   - Large
   - Medium
   - Small

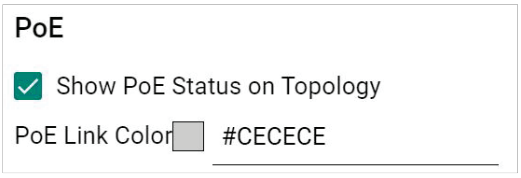


Text Size

Text Size: 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.

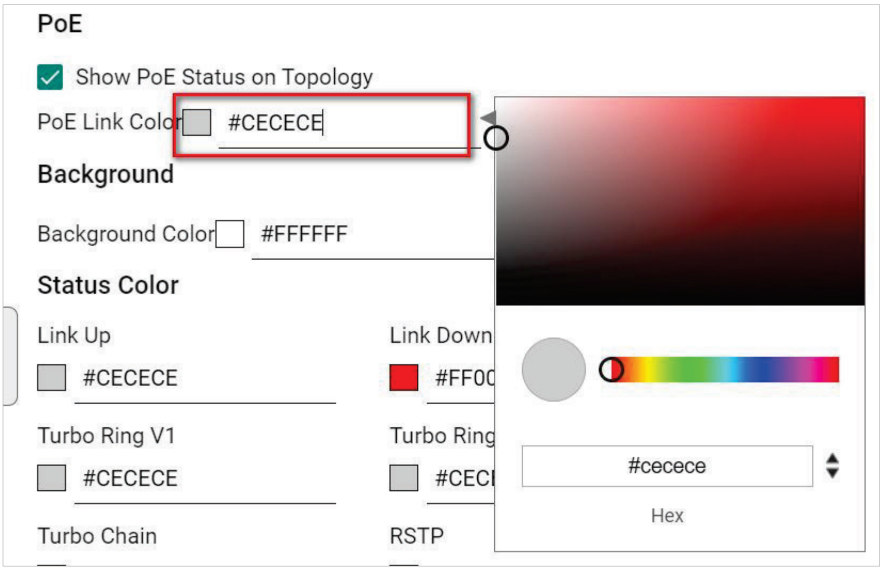


PoE

☑ Show PoE Status on Topology

PoE Link Color ▢ #CECECE

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



PoE

☑ Show PoE Status on Topology

PoE Link Color ▢ #CECECE

Background

Background Color ▢ #FFFFFF

Status Color

Link Up ▢ #CECECE

Link Down 🟥 #FF00

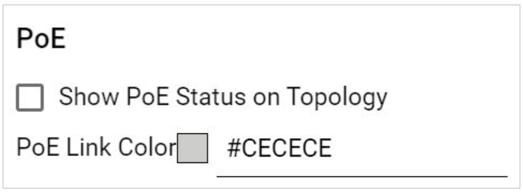
Turbo Ring V1 ▢ #CECECE

Turbo Ring ▢ #CECI

Turbo Chain

RSTP

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

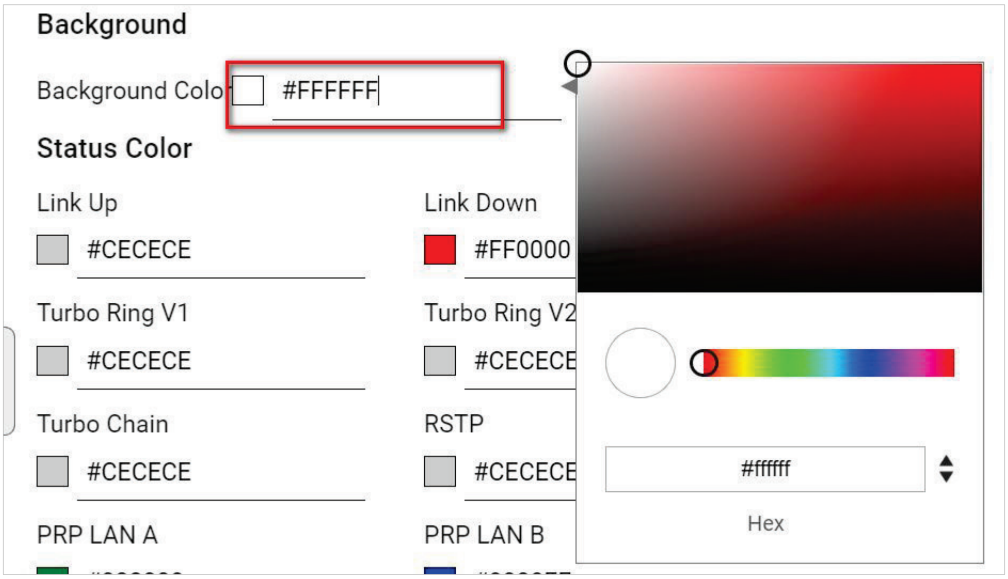


PoE

□ Show PoE Status on Topology

PoE Link Color ▢ #CECECE

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



Background

Background Color ▢ #FFFFFF

Status Color

Link Up ▢ #CECECE

Link Down 🟥 #FF0000

Turbo Ring V1 ▢ #CECECE

Turbo Ring V2 ▢ #CECECE

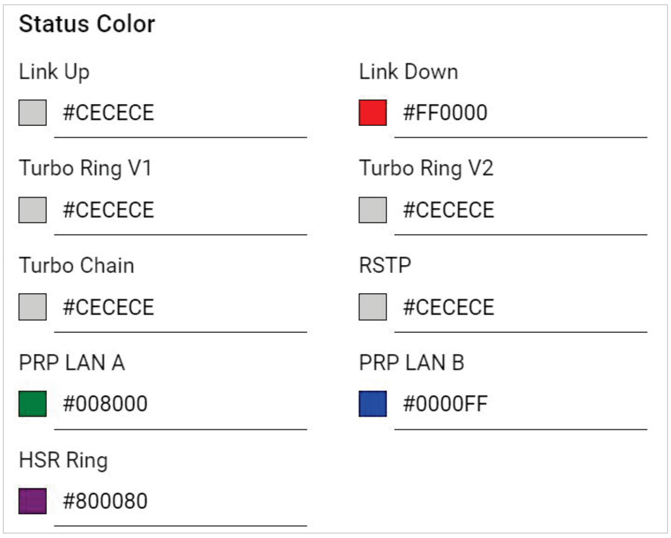
Turbo Chain ▢ #CECECE

RSTP ▢ #CECECE

PRP LAN A

PRP LAN B

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



Status Color

Link Up: #CECECE

Link Down: #FF0000

Turbo Ring V1: #CECECE

Turbo Ring V2: #CECECE

Turbo Chain: #CECECE

RSTP: #CECECE

PRP LAN A: #008000

PRP LAN B: #0000FF

HSR Ring: #800080

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

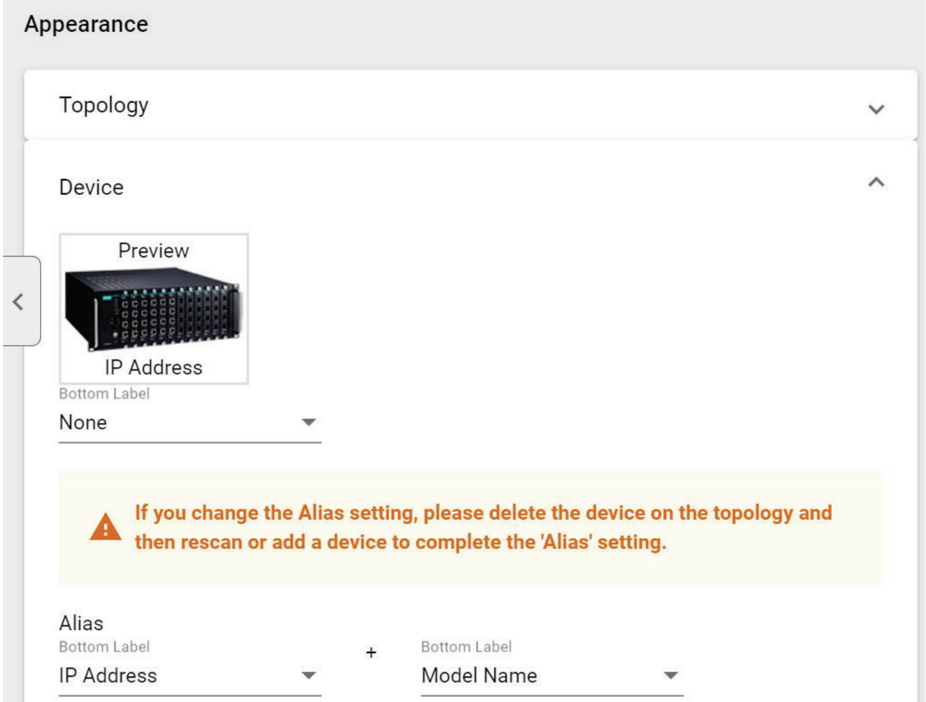
Use the **Preferences** screen to modify how devices appear in the Topology Map.

1. Navigate to **Menu** (☰) **> Administration > Preferences.**

   The **Preferences** screen will appear.

2. In the **Appearance** section, expand **Device**.

   The **Device** settings will appear.



Appearance

Topology

Device

Preview

IP Address

Bottom Label

None

⚠ 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.

Alias

Bottom Label

IP Address

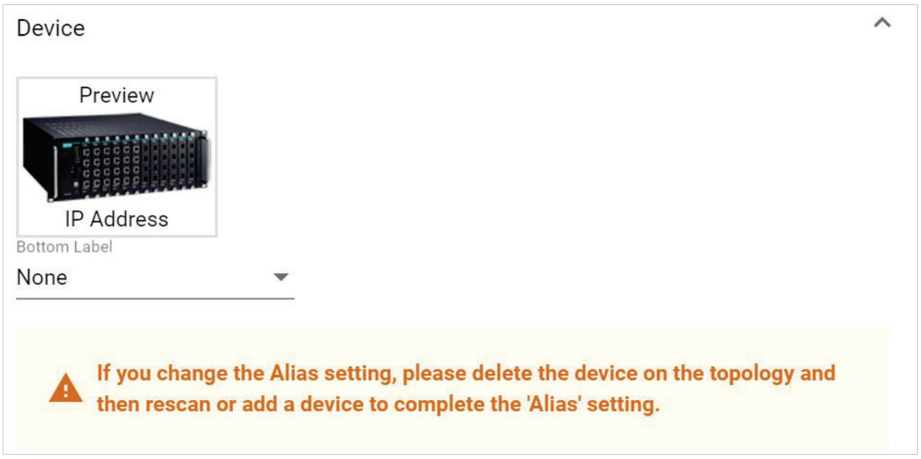
+

Bottom Label

Model Name

3. To modify the label that indicates the device in the Topology Map:

   a. Locate the **Bottom Label** drop-down list located below the Preview image:



Device

Preview

IP Address

Bottom Label

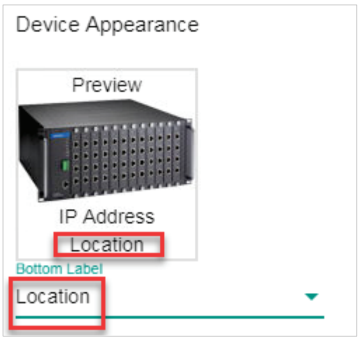
None

⚠ 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.

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

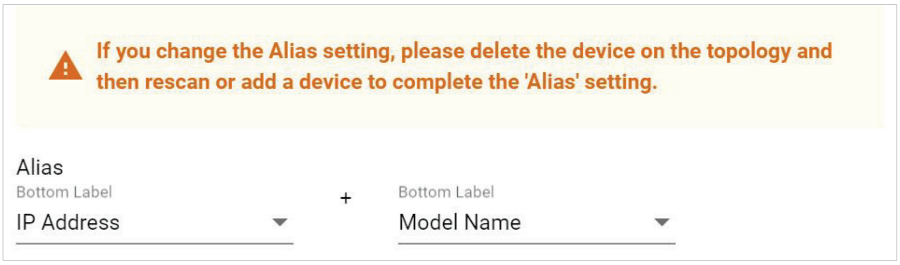
- ❒ Location
- ❒ Alias
- ❒ Model Name
- ❒ MAC

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



4. To modify the device alias:

a. Locate the **Alias** section.



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.

Alias

Bottom Label: IP Address + Bottom Label: Model Name

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 **Topolog**y 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

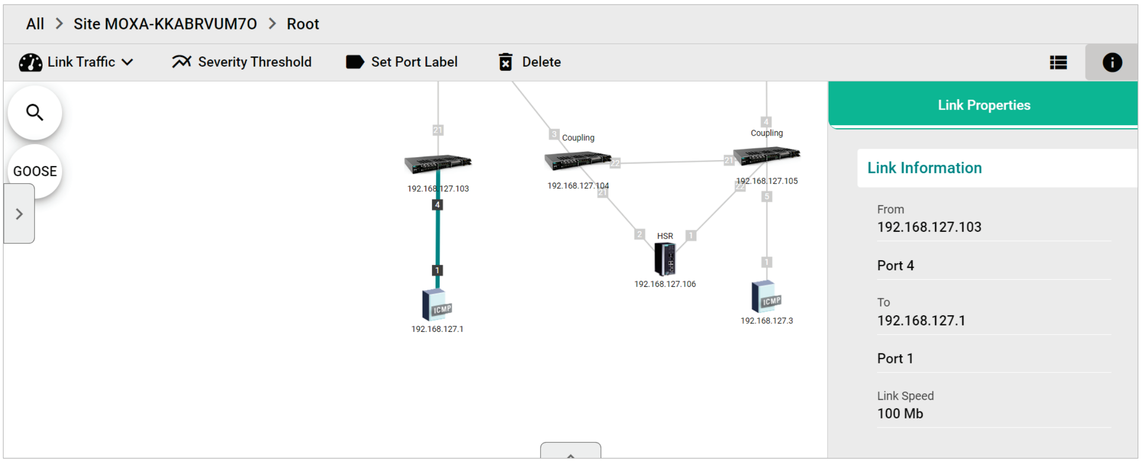
Click a link on the Topology Map to view link properties and perform the following:

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.



From
192.168.127.103

Port 4

To
192.168.127.1

Port 1

Link Speed
100 Mb

Viewing Port Traffic

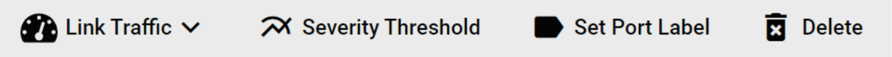
The **Port Traffic** screen displays a graph that shows the utilization percentage (Y-axis) over a specific time period (X-axis). You can also adjust the time period for the data that is displayed by changing the starting date and ending date. The minimum interval you can select is one day and the maximum interval you can select is 90 days.

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

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

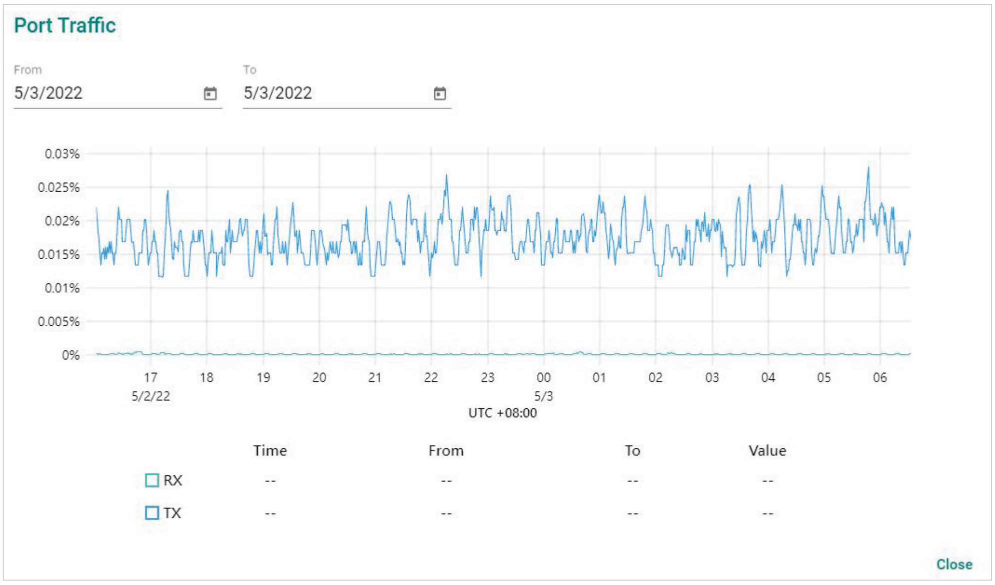
2. Click on a link between devices in the Topology Map.

   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.



Port Traffic

From 5/3/2022

To 5/3/2022

	Time	From	To	Value
□ RX	--	--	--	--
□ TX	--	--	--	--

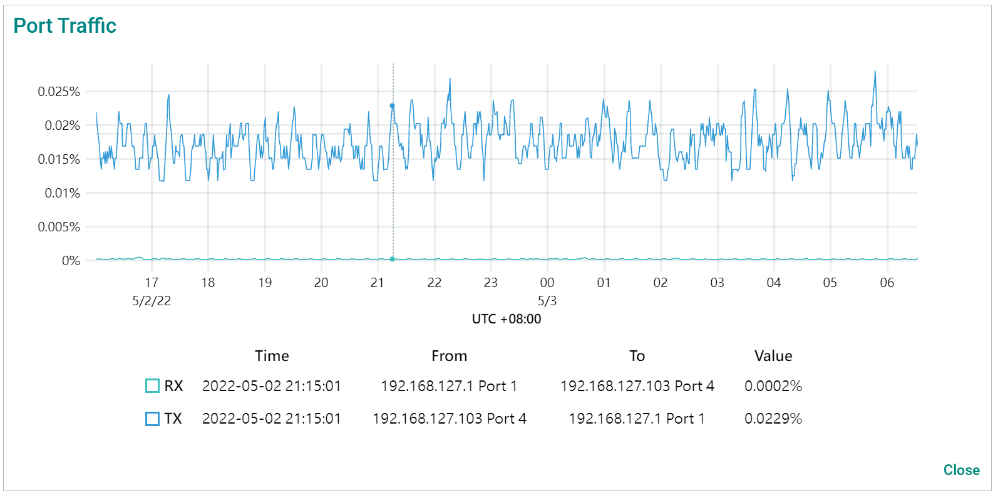
4. To adjust the time period for the graph data:

   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**.



Port Traffic

	Time	From	To	Value
□ RX	2022-05-02 21:15:01	192.168.127.1 Port 1	192.168.127.103 Port 4	0.0002%
□ TX	2022-05-02 21:15:01	192.168.127.103 Port 4	192.168.127.1 Port 1	0.0229%

Viewing Packet Error Rates

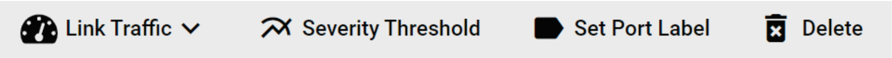
The **Packet Error Rate** screen displays a graph that shows the packet error rate (Y-axis) over a specific time period (X-axis). You can also adjust the time period for the data that is displayed by changing the start and end dates. The minimum interval is one day and the maximum interval you can select is 90 days.

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

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

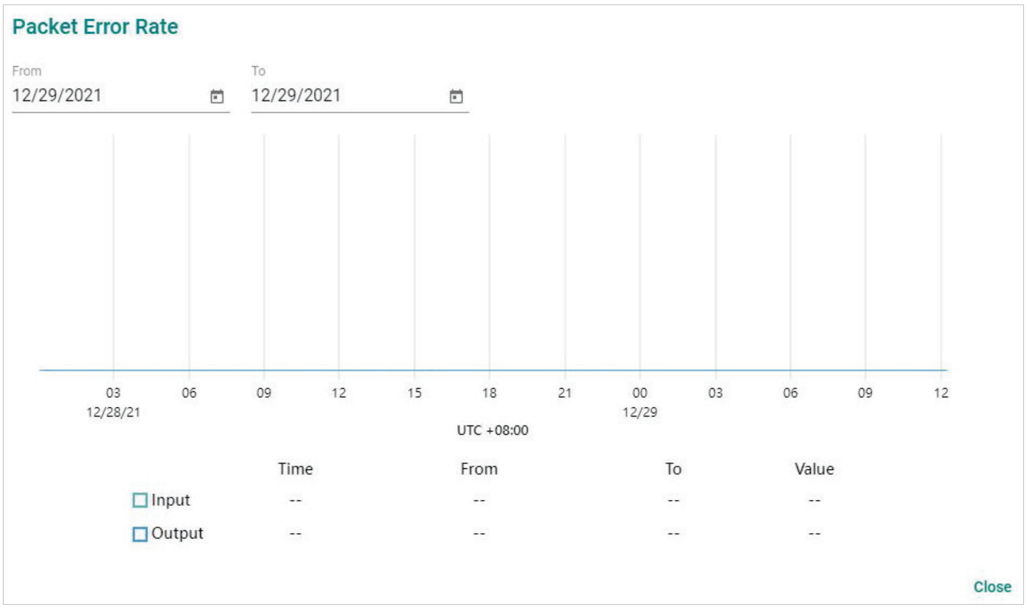
2. Click on a link between devices in the Topology Map.

   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.



Packet Error Rate

From
12/29/2021

To
12/29/2021

	Time	From	To	Value
□ Input	--	--	--	--
□ Output	--	--	--	--

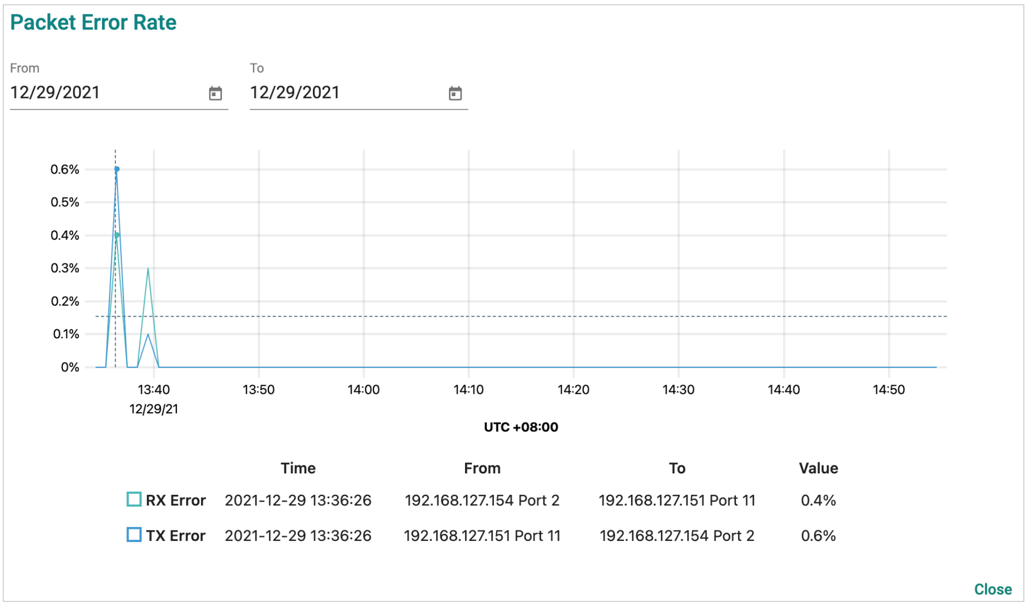
Close

4. To adjust the time period for the graph data:

   a. Click the **From** date and select a new starting date.

   b. Click the **To** date and select a new ending date.

5. Hover over a line to view the packet error rate.



Packet Error Rate

From
12/29/2021

To
12/29/2021

	Time	From	To	Value
□ RX Error	2021-12-29 13:36:26	192.168.127.154 Port 2	192.168.127.151 Port 11	0.4%
□ TX Error	2021-12-29 13:36:26	192.168.127.151 Port 11	192.168.127.154 Port 2	0.6%

Close

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.

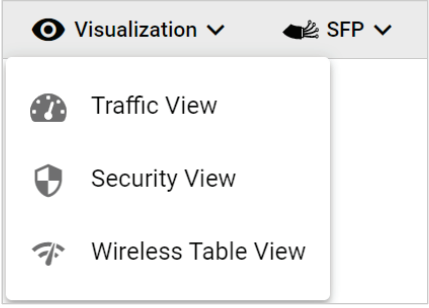
1. Navigate to **Menu** (☰) **> Topology**.

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

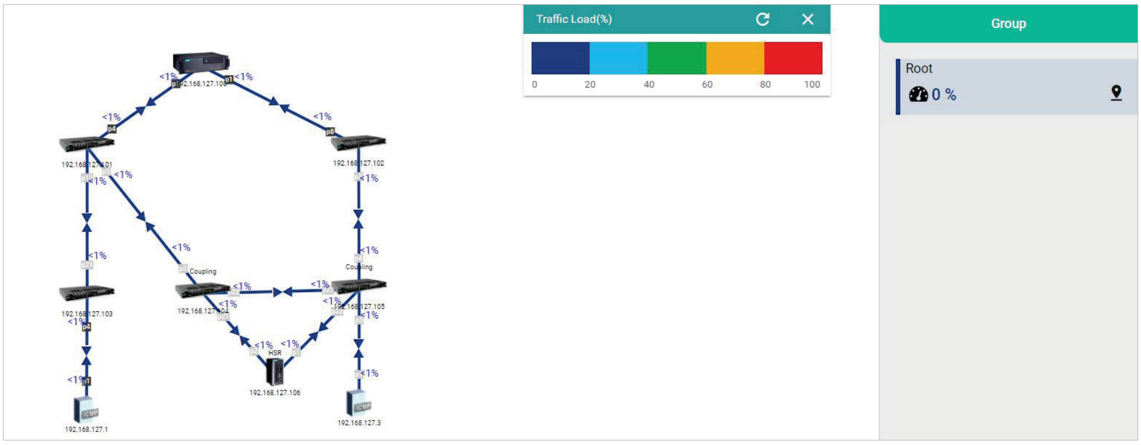
2. If **List view** is selected, click the **Topology view** (⛙) icon in the top right corner.

   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**.

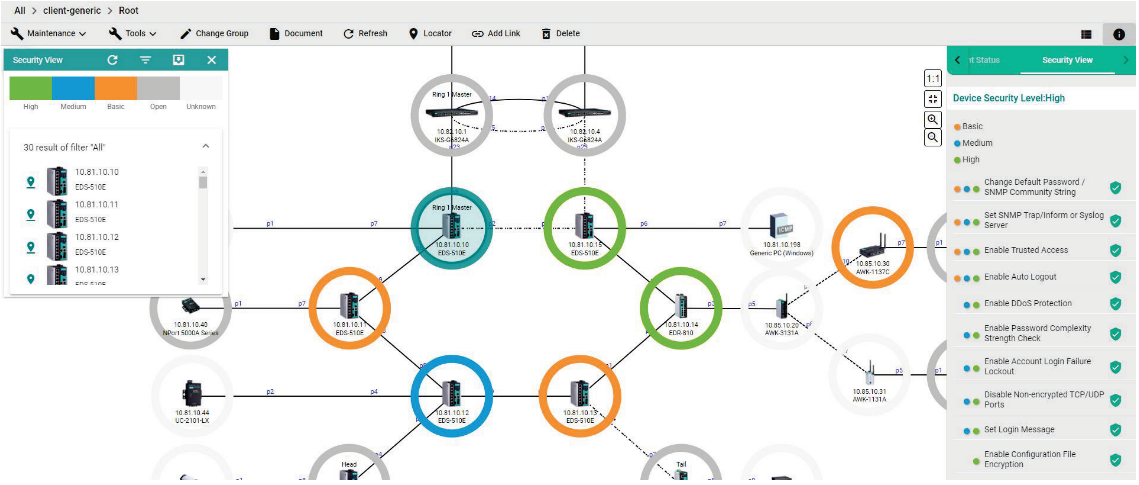
   The **Topology** screen will appear and display the Topology Map by default.

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.



30 result of filter "All"

- 10.81.10.10 EDS-510E
- 10.81.10.11 EDS-510E
- 10.81.10.12 EDS-510E
- 10.81.10.13 EDS-510E

Device Security Level:High

● Basic
● Medium
● High

● ● ●	Change Default Password / SNMP Community String	✓
● ● ●	Set SNMP Trap/Inform or Syslog Server	✓
● ● ●	Enable Trusted Access	✓
● ● ●	Enable Auto Logout	✓
● ●	Enable DDoS Protection	✓
● ●	Enable Password Complexity Strength Check	✓
● ●	Enable Account Login Failure Lockout	✓
● ●	Disable Non-encrypted TCP/UDP Ports	✓
● ●	Set Login Message	✓
●	Enable Configuration File Encryption	✓

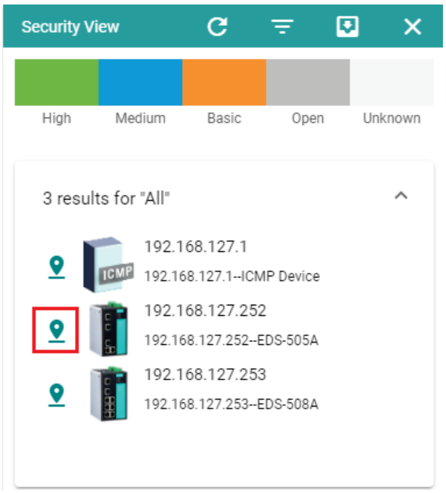
4. To filter the devices in the **Security View** window by security level:

   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.

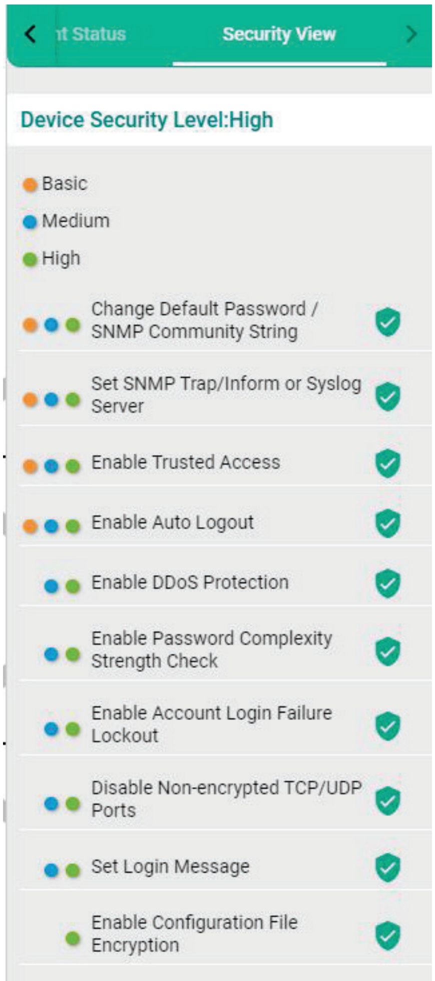
5. To locate a device in the Topology Map, click the device in the Security View window.



3 results for "All"

- 192.168.127.1 — 192.168.127.1--ICMP Device
- 192.168.127.252 — 192.168.127.252--EDS-505A
- 192.168.127.253 — 192.168.127.253--EDS-508A

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



Device Security Level:High

● Basic
● Medium
● High

●●● Change Default Password / SNMP Community String ✓

●●● Set SNMP Trap/Inform or Syslog Server ✓

●●● Enable Trusted Access ✓

●●● Enable Auto Logout ✓

●● Enable DDoS Protection ✓

●● Enable Password Complexity Strength Check ✓

●● Enable Account Login Failure Lockout ✓

●● Disable Non-encrypted TCP/UDP Ports ✓

●● Set Login Message ✓

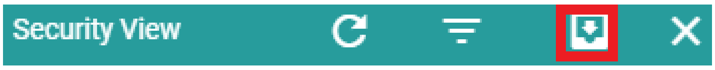
● Enable Configuration File Encryption ✓

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.



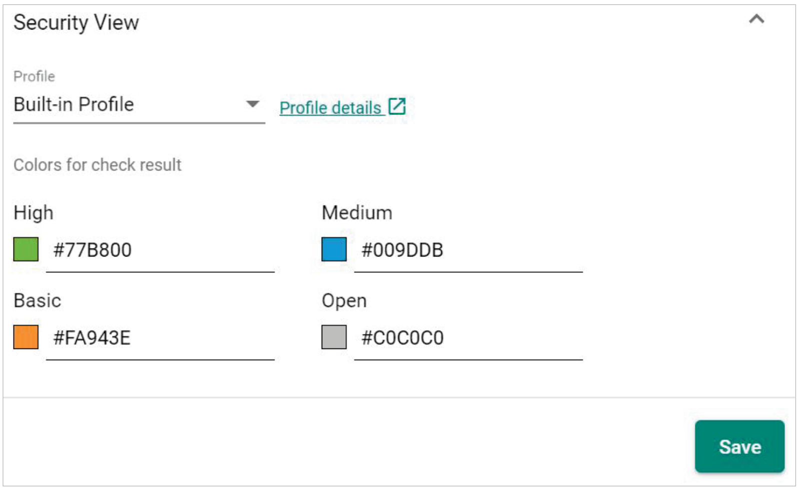
8. Review the following items in the Security View details pane:

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.



Security View

Profile
Built-in Profile

Profile details

Colors for check result

High
🟩 #77B800

Medium
🟦 #009DDB

Basic
🟧 #FA943E

Open
⬜ #C0C0C0

Save

   d. Click **Save**.

10. To define a custom security profile:

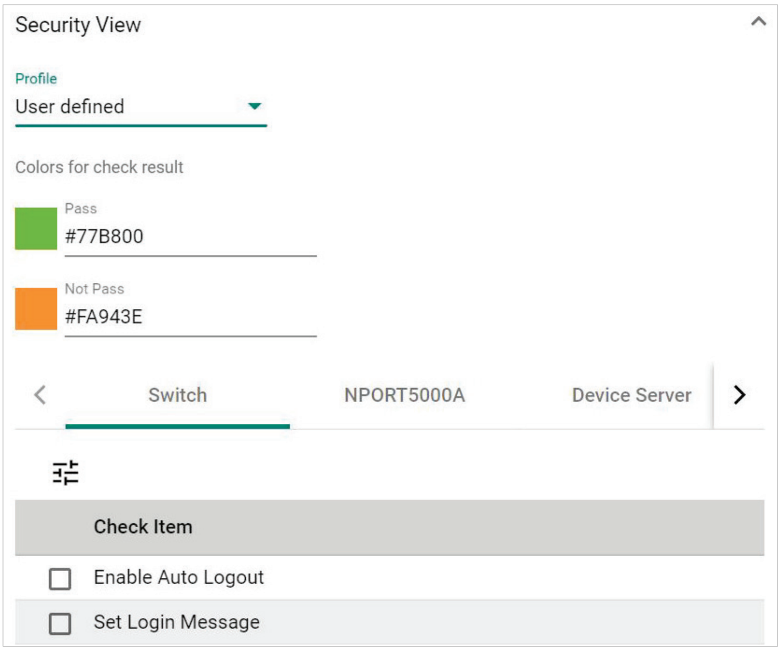
    a. Navigate to **Menu** (☰) **> Administration > Preferences**.

       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.



Security View

Profile: User defined

Colors for check result

🟩 Pass: #77B800

🟧 Not Pass: #FA943E

	Check Item
□	Enable Auto Logout
□	Set Login Message

    d. (Optional) Modify the colors for the check result.

    e. Click one of the following device tabs to configure the profile settings:

       - Switch
       - NPORT5000A
       - Device Server
       - Terminal Server
       - Gateway
       - Wireless
       - IO

    f. (Optional) Click the **Settings** (≢) 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.

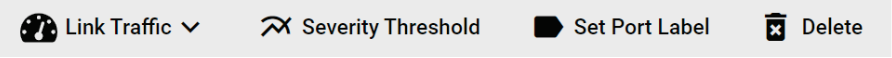
Since a link is bidirectional, the event will be triggered when the traffic condition in either direction satisfies the configured severity threshold.

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

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

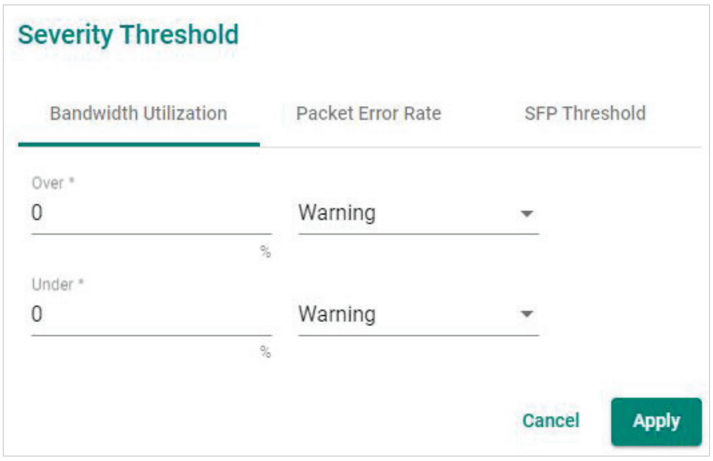
2. Click on a link between devices in the Topology Map.

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

3. Click **Severity Threshold**.

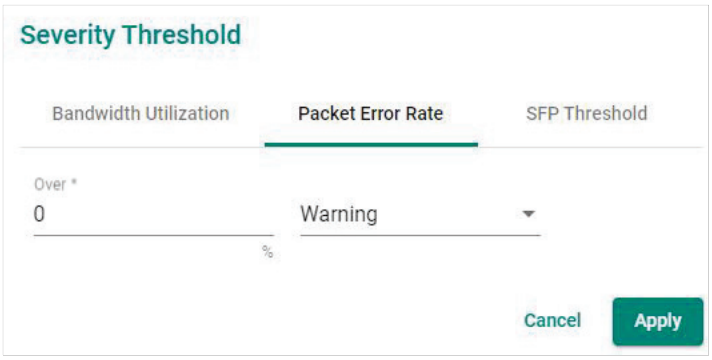
   The **Severity Threshold** screen will appear.

   Severity Threshold

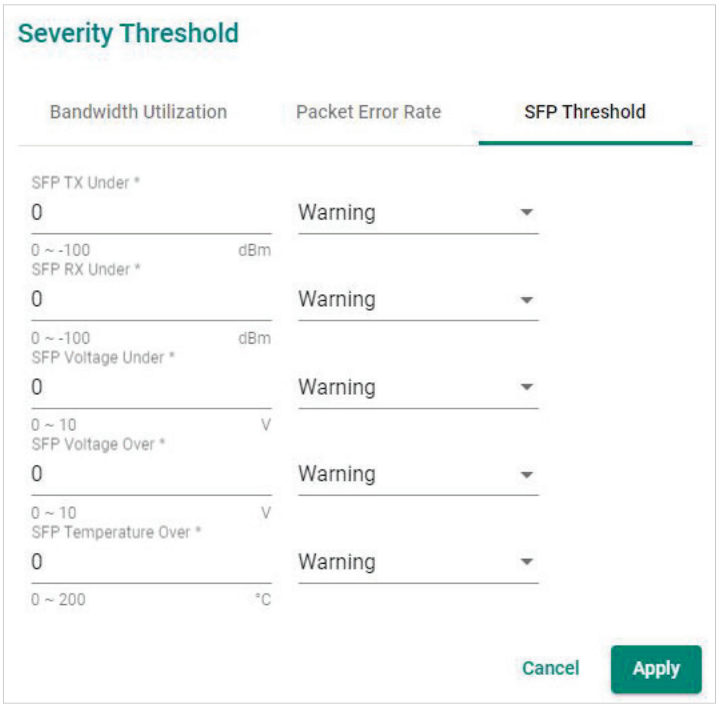
   Over * 0 % Warning

   Under * 0 % Warning

   Severity Threshold

   Over * 0 % Warning



SFP TX Under * 0 Warning 0 ~ -100 dBm

SFP RX Under * 0 Warning 0 ~ -100 dBm

SFP Voltage Under * 0 Warning 0 ~ 10 V

SFP Voltage Over * 0 Warning 0 ~ 10 V

SFP Temperature Over * 0 Warning 0 ~ 200 °C

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.

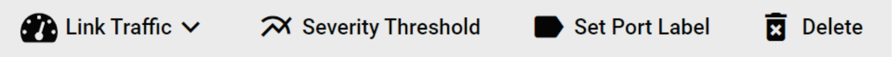
Configuring Custom Port Labels

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

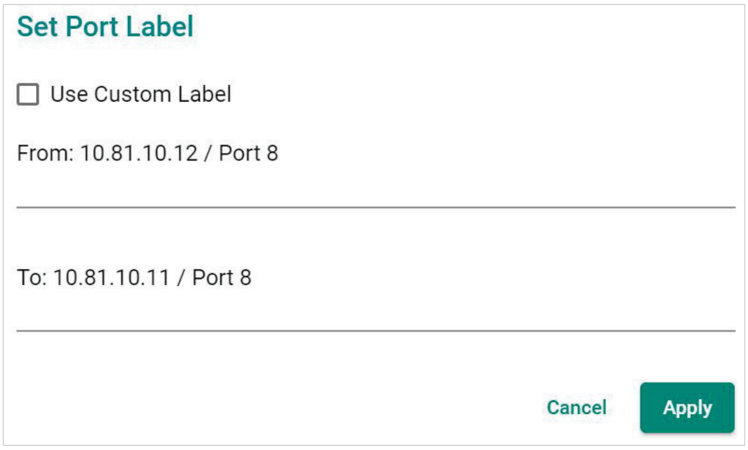
<Device IP Address> / <Port Number>

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.



Set Port Label

□ Use Custom Label

From: 10.81.10.12 / Port 8

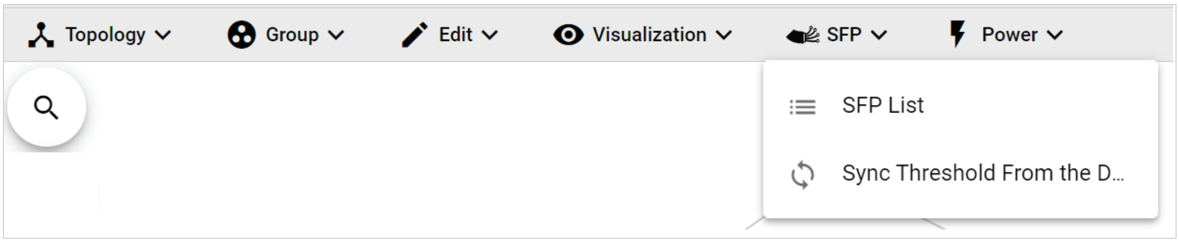
To: 10.81.10.11 / Port 8

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**.

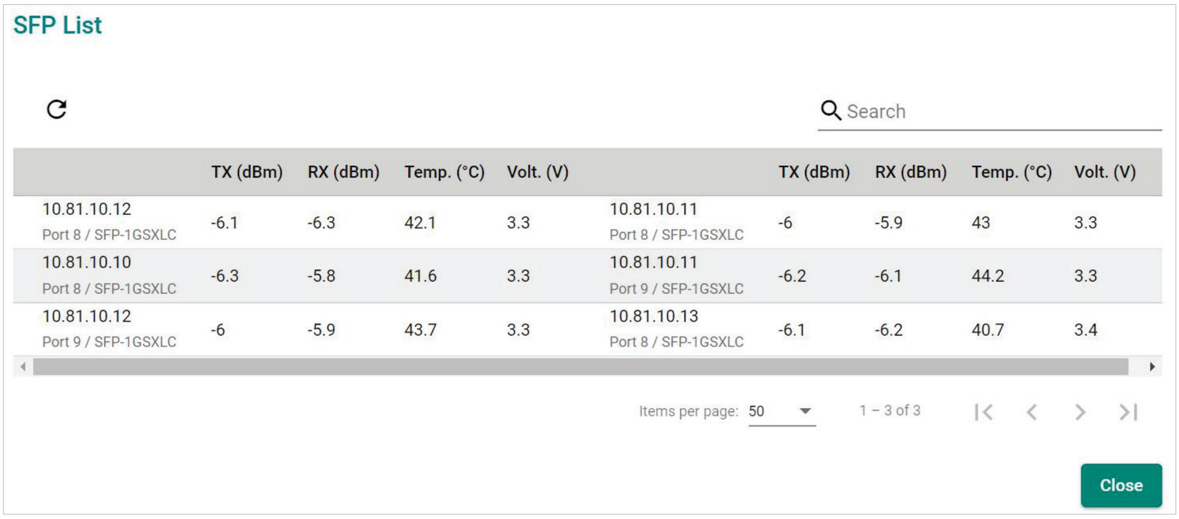
9. SFP Fiber Status

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.



SFP List

Search

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

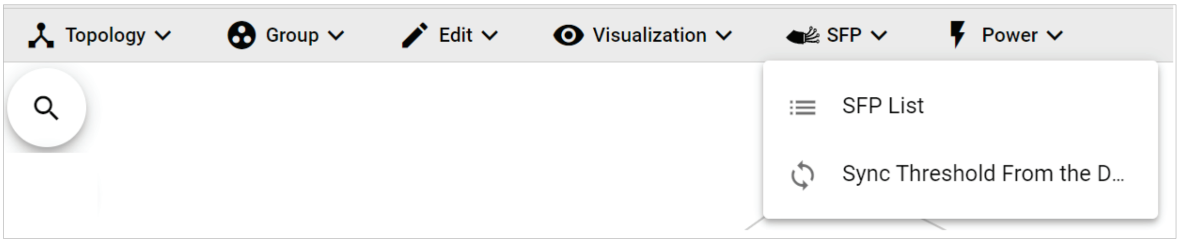
Items per page: 50   1 – 3 of 3

Close

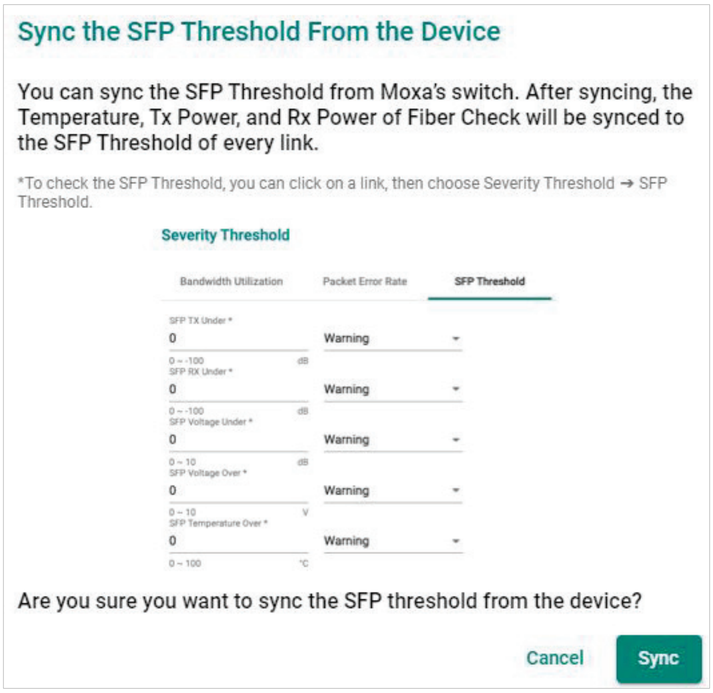
Synchronize the SFP Threshold From the Device

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.



Sync the SFP Threshold From the Device

You can sync the SFP Threshold from Moxa’s switch. After syncing, the Temperature, Tx Power, and Rx Power of Fiber Check will be synced to the SFP Threshold of every link.

*To check the SFP Threshold, you can click on a link, then choose Severity Threshold → SFP Threshold.

Severity Threshold

Bandwidth Utilization | Packet Error Rate | SFP Threshold

SFP TX Under *: 0 (0 ~ -100 dB) Warning
SFP RX Under *: 0 (0 ~ -100 dB) Warning
SFP Voltage Under *: 0 (0 ~ 10 dB) Warning
SFP Voltage Over *: 0 (0 ~ 10 V) Warning
SFP Temperature Over *: 0 (0 ~ 100 °C) Warning

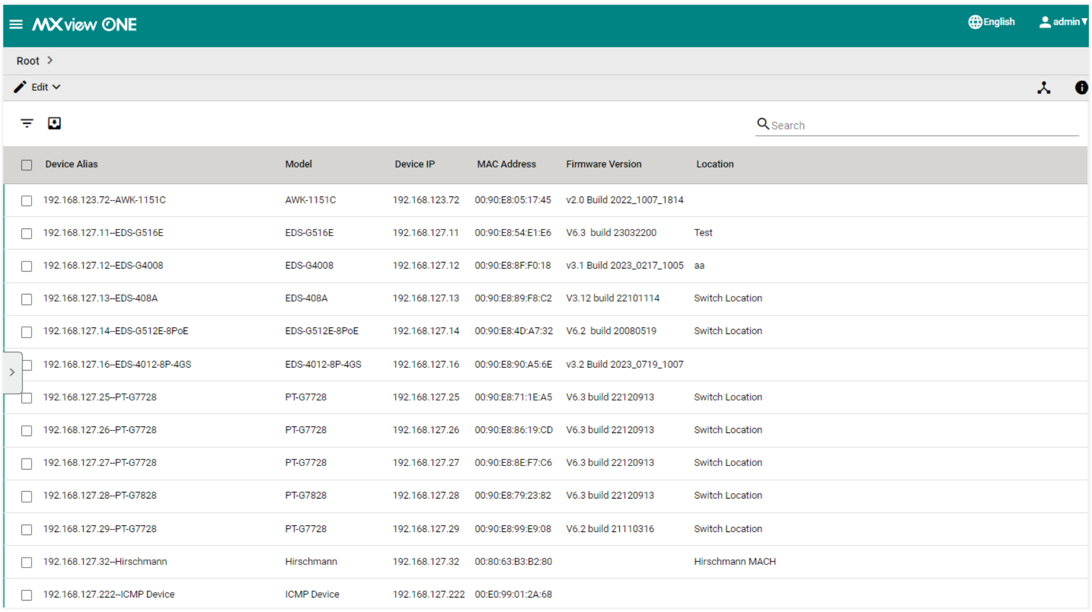
Are you sure you want to sync the SFP threshold from the device?

10. Device Operation in the Topology

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.



□ Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□ 192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2022_1007_1814	
□ 192.168.127.11--EDS-G516E	EDS-G516E	192.168.127.11	00:90:E8:54:E1:E6	V6.3 build 23032200	Test
□ 192.168.127.12--EDS-G4008	EDS-G4008	192.168.127.12	00:90:E8:8F:F0:18	v3.1 Build 2023_0217_1005	aa
□ 192.168.127.13--EDS-408A	EDS-408A	192.168.127.13	00:90:E8:89:F8:C2	V3.12 build 22101114	Switch Location
□ 192.168.127.14--EDS-G512E-8PoE	EDS-G512E-8PoE	192.168.127.14	00:90:E8:4D:A7:32	V6.2 build 20080519	Switch Location
□ 192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	192.168.127.16	00:90:E8:90:A5:6E	v3.2 Build 2023_0719_1007	
□ 192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location
□ 192.168.127.26--PT-G7728	PT-G7728	192.168.127.26	00:90:E8:86:19:CD	V6.3 build 22120913	Switch Location
□ 192.168.127.27--PT-G7728	PT-G7728	192.168.127.27	00:90:E8:8E:F7:C6	V6.3 build 22120913	Switch Location
□ 192.168.127.28--PT-G7828	PT-G7828	192.168.127.28	00:90:E8:79:23:82	V6.3 build 22120913	Switch Location
□ 192.168.127.29--PT-G7728	PT-G7728	192.168.127.29	00:90:E8:99:E9:08	V6.2 build 21110316	Switch Location
□ 192.168.127.32--Hirschmann	Hirschmann	192.168.127.32	00:80:63:B3:B2:80		Hirschmann MACH
□ 192.168.127.222--ICMP Device	ICMP Device	192.168.127.222	00:E0:99:01:2A:68		

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

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

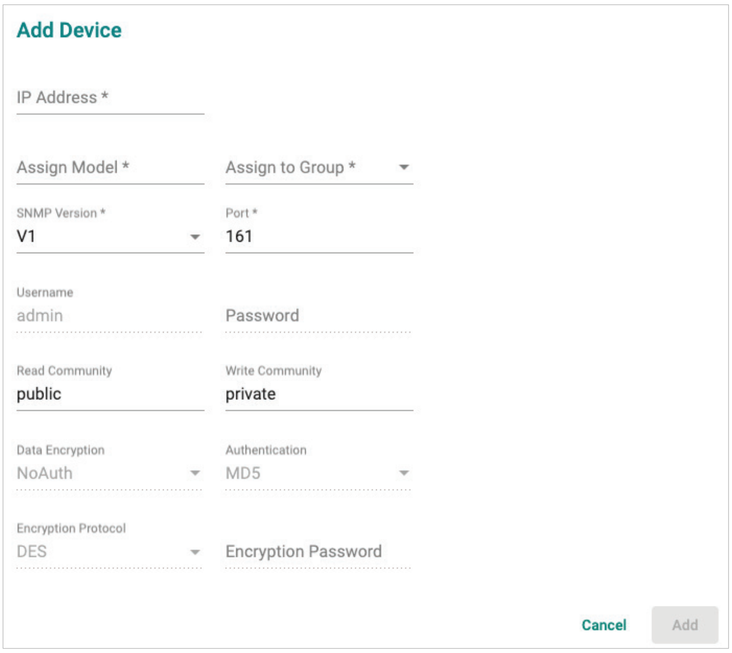
2. Click the **List view** (☰) icon in the top right corner.

   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.



Add Device

IP Address *

Assign Model *

Assign to Group *

SNMP Version *: V1

Port *: 161

Username: admin

Password

Read Community: public

Write Community: private

Data Encryption: NoAuth

Authentication: MD5

Encryption Protocol: DES

Encryption Password

   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**.

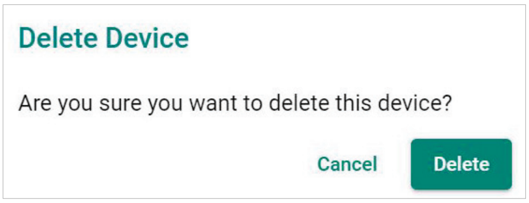
      MXview One adds the device to the topology.

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.

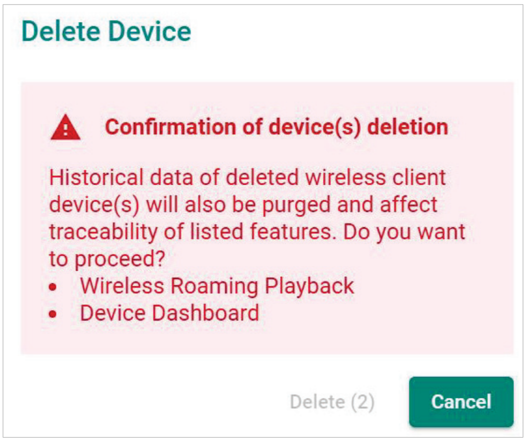
   c. For non AWK devices, read the message and then click **Delete** if you are sure you want to delete the device.



Delete Device

Are you sure you want to delete this 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.



Delete Device

Confirmation of device(s) deletion

Historical data of deleted wireless client device(s) will also be purged and affect traceability of listed features. Do you want to proceed?

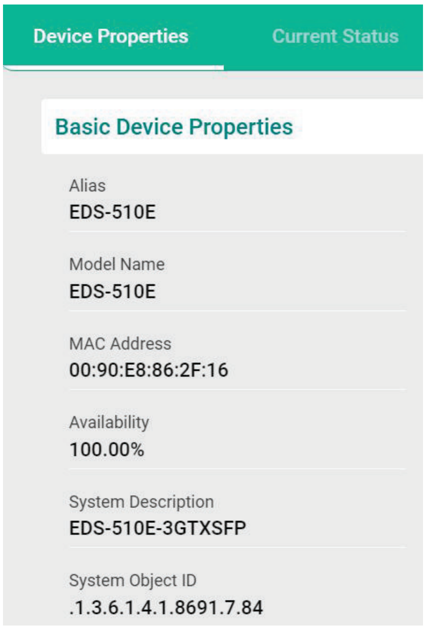
- Wireless Roaming Playback
- Device Dashboard

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 **Device Alias**.

   The **Device Properties** details pane will appear.



Basic Device Properties

Alias
EDS-510E

Model Name
EDS-510E

MAC Address
00:90:E8:86:2F:16

Availability
100.00%

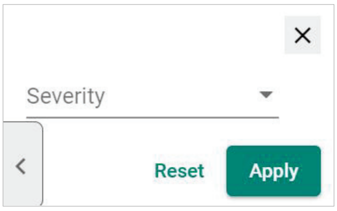
System Description
EDS-510E-3GTXSFP

System Object ID
.1.3.6.1.4.1.8691.7.84

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**

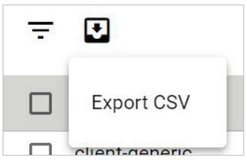
❒ **Information**

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**.

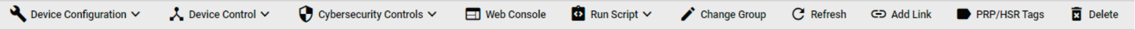
1. Navigate to **Menu** ( ) **> Topology**.

   The **Topology** screen will appear and display 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.

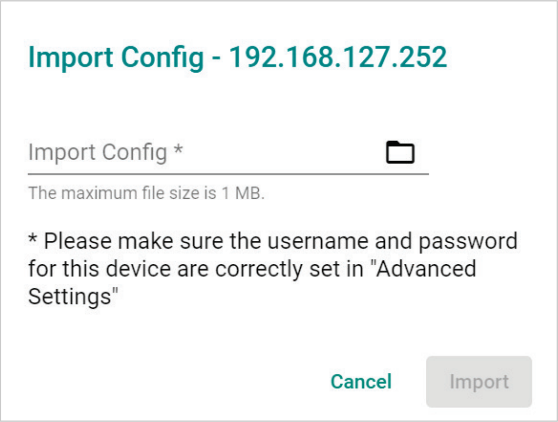
3. Select the device that you want to import configurations to:
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the site name in the Device List.

   The toolbar options change.



4. Navigate to **Device Control > Import Config**.

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



Import Config - 192.168.127.252

Import Config *

The maximum file size is 1 MB.

* Please make sure the username and password for this device are correctly set in "Advanced Settings"

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.

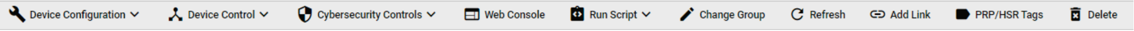
2. Select one of the following views:

   - **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.

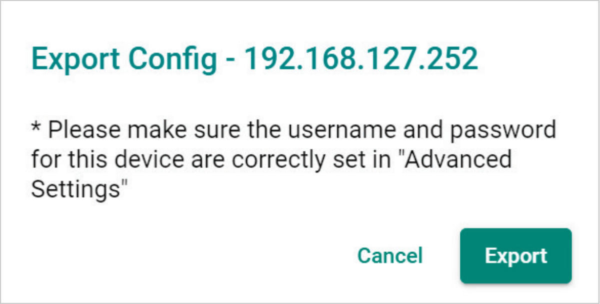
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the device in the Device List.

   The toolbar options change.



4. Navigate to **Device Control > Export Config**.

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



Export Config - 192.168.127.252

* Please make sure the username and password for this device are correctly set in "Advanced Settings"

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.

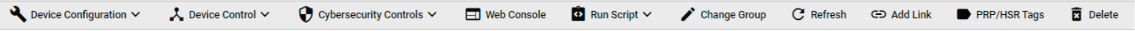
   b. **List view:** Displays a list of the devices in your network topology.

3. Select the device that you want to upgrade the firmware for:

   ➢ **Topology view:** Click the icon of the device in the Topology Map.

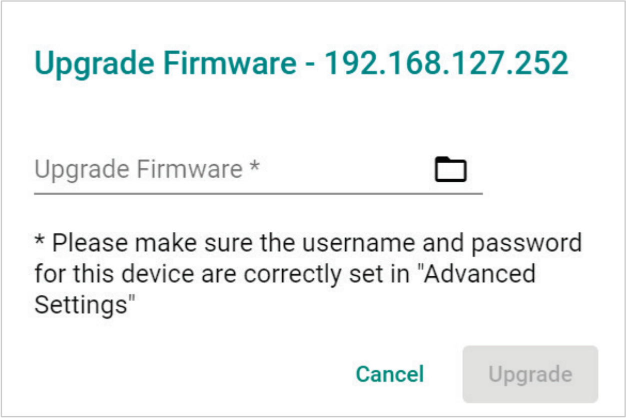
   ➢ **List view:** Select the check box next to the device in the Device List.

   The toolbar options change.



4. Navigate to **Device Control > Upgrade Firmware**.

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



Upgrade Firmware - 192.168.127.252

Upgrade Firmware *

* Please make sure the username and password for this device are correctly set in "Advanced Settings"

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.

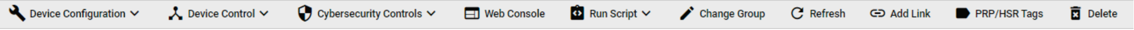
2. Select one of the following views:

   - **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.

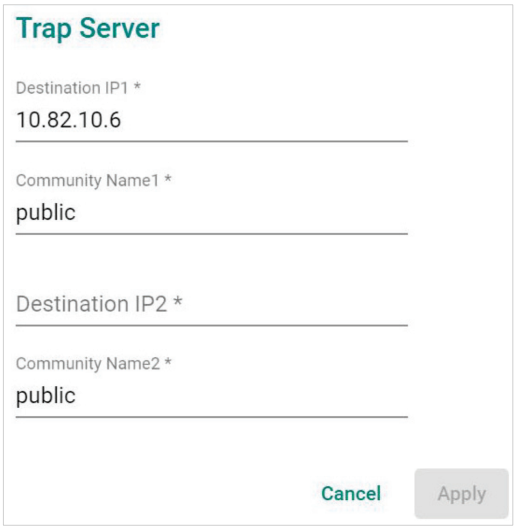
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the device in the Device List.

   The toolbar options change.



4. Navigate to **Device Configuration > Trap Server**.

   The **Trap Server** screen appears.



Trap Server

Destination IP1 *
10.82.10.6

Community Name1 *
public

Destination IP2 *

Community Name2 *
public

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**.

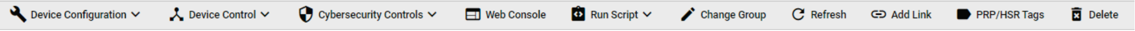
1. Navigate to **Menu** (☰) **> Topology**.

   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.

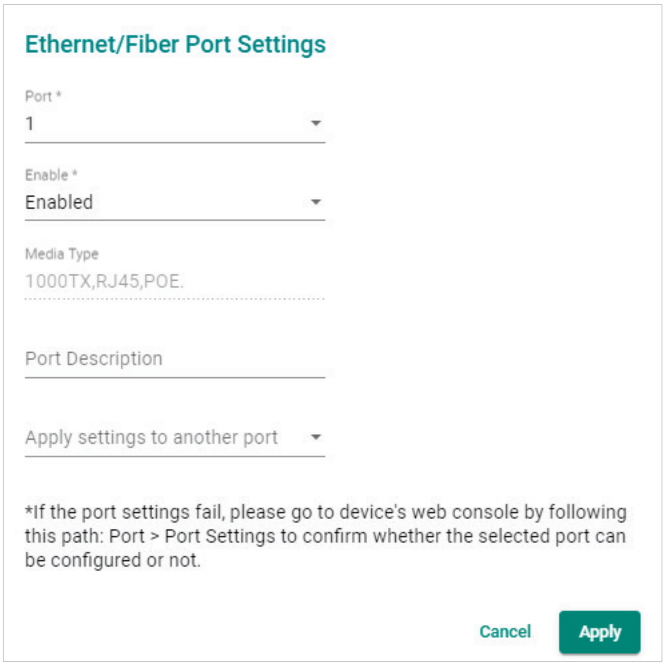
3. Select the device.
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the device in the Device List.

   The toolbar options will change.



4. Navigate to **Device Configuration > Ethernet/Fiber Port Settings**.

   The **Ethernet/Fiber Port Setting** screen appears.



Ethernet/Fiber Port Settings

Port * 1

Enable * Enabled

Media Type 1000TX,RJ45,POE.

Port Description

Apply settings to another port

*If the port settings fail, please go to device's web console by following this path: Port > Port Settings to confirm whether the selected port can be configured or not.

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 Communication Protocol

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**.

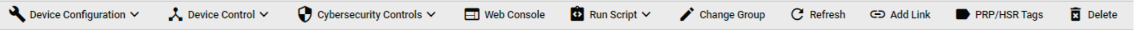
1. Navigate to **Menu** (☰) **> Topology**.

   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.

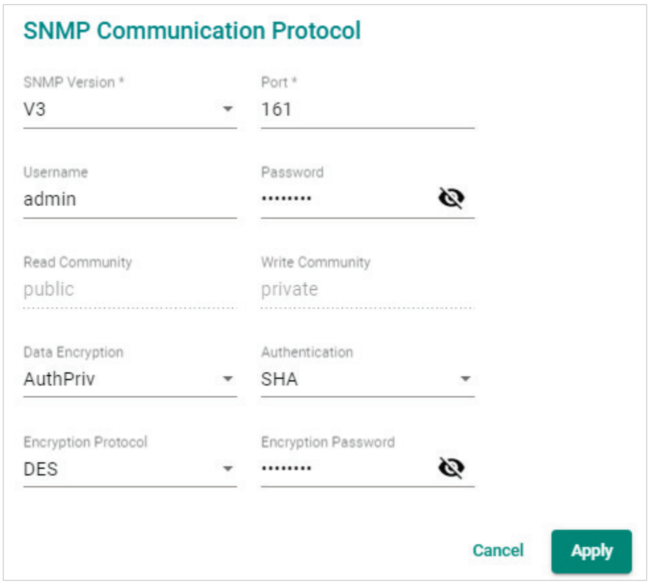
3. Select the device.
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the device in the Device List.

   The toolbar options will change.



4. Navigate to **Device Configuration > SNMP Communication Protocol**.

   The **SNMP Communication Protocol** screen will appear.



SNMP Communication Protocol

SNMP Version * V3

Port * 161

Username admin

Password ••••••••

Read Community public

Write Community private

Data Encryption AuthPriv

Authentication SHA

Encryption Protocol DES

Encryption Password ••••••••

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 communication protocol settings to the device.

NOTE

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

Configuring MXview One Polling Interval

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**.

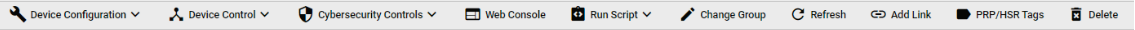
1. Navigate to **Menu** (☰) **> Topology**.

   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.

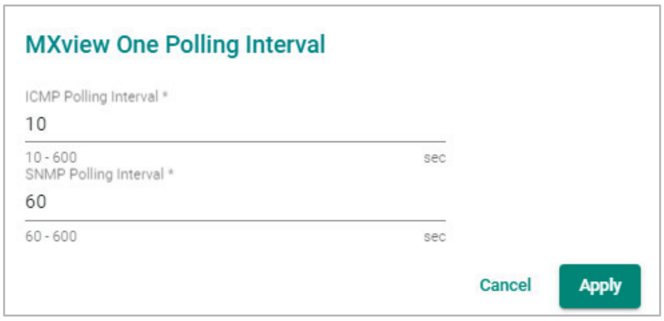
3. Select the device.
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the device in the Device List.

   The toolbar options change.



4. Navigate to **Device Configuration > MXview One Polling Interval**.

   The **MXview One Polling Interval** screen appears.



MXview One Polling Interval

ICMP Polling Interval *
10
10 - 600 sec

SNMP Polling Interval *
60
60 - 600 sec

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 Default Device Template function to set the function template. For more information, see **Default Device Template**.

Configuring Device Accounts

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.

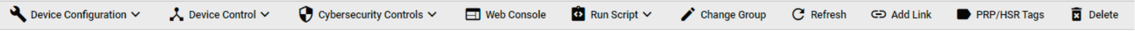
2. Select one of the following views:

   - **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.

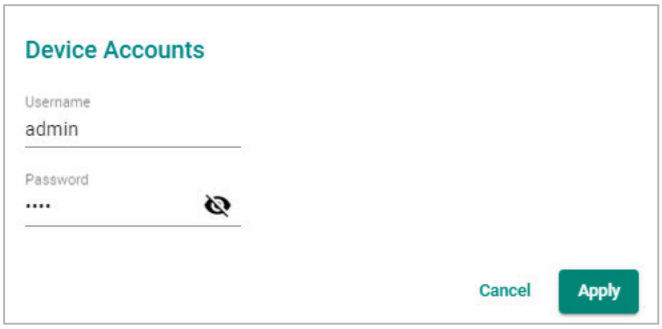
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the device in the Device List.

   The toolbar options change.



4. Navigate to **Device Configuration > Device Accounts**.

   The **Device Accounts** screen appears.



Device Accounts

Username
admin

Password
••••

5. Enter the **Username** and **Password** for the device web console.
6. Click **Apply**.

   MXview One updates the advanced settings.

Modifying the Device Alias

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.

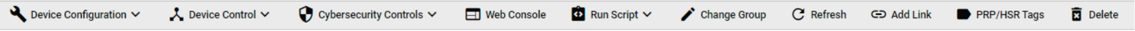
   ➢ **List view:** Displays a list of the devices in your network topology.

3. Select the device.

   ➢ **Topology view:** Click the icon of the device in the Topology Map.

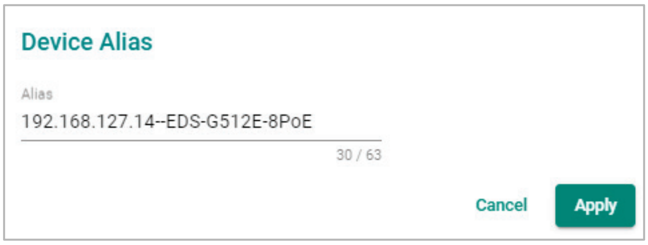
   ➢ **List view:** Select the check box next to the device in the Device List.

   The toolbar options change.



4. Navigate to **Device Configuration > Device Alias**.

   The **Device Alias** screen appears.



Device Alias

Alias
192.168.127.14--EDS-G512E-8PoE
30 / 63

5. Edit the **Alias** field.

6. 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.

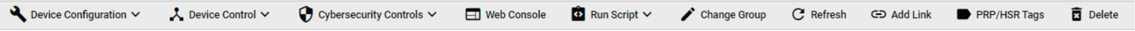
2. Select one of the following views:

   - **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.

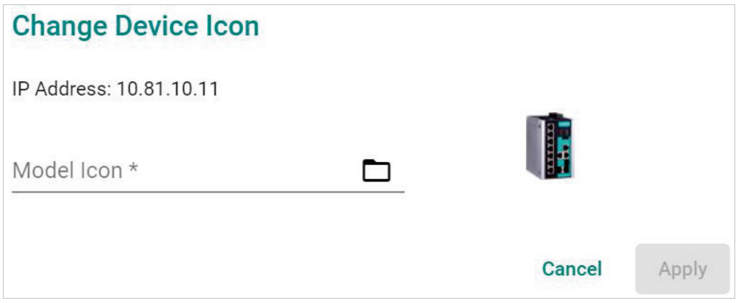
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the device in the Device List.

   The toolbar options will change.



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

   The **Change Device Icon** screen appears.



IP Address: 10.81.10.11

5. Click the folder (📁) icon to upload the device icon from your local machine. (The maximum image size is 100 KB.)

6. Click **Apply**.

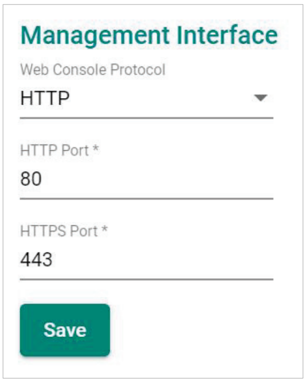
   MXview One will change the device icon to the uploaded JPG, GIF, or PNG image file.

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.



Web Console Protocol: HTTP

HTTP Port *: 80

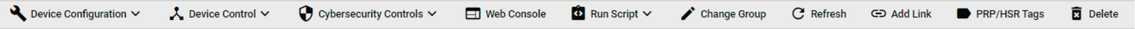
HTTPS Port *: 443

   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 **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**.

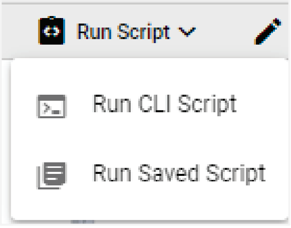
   The device web console will successfully log in.

Managing and Running Scripts

The **Run Script** function allows you to quickly perform a set of actions on one or multiple devices at once. You can run scripts on selected devices from the **Topology** or **Device Management** screen.

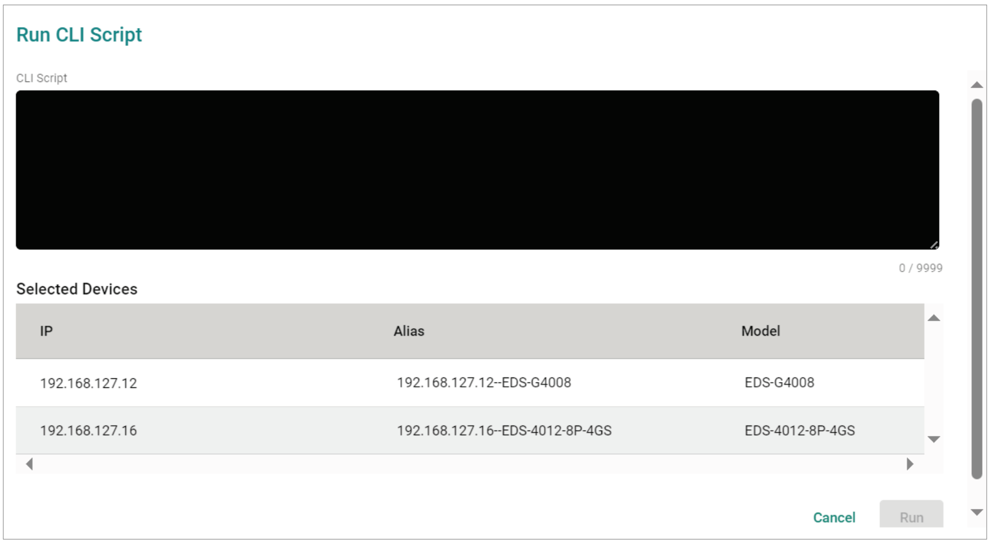
Click the **Run Script** ( ) icon in the menu bar to expand the script functions. There are two main functions:

- **Run CLI Script**: Write and run a CLI script and test if the script works correctly.
- **Run Saved Script**: Select and run a CLI Script from the Saved CLI Scripts database. Refer to the Saved CLI Scripts section.



Running a CLI Script

1. In the **Topology** or **Device Management** screen, select the device(s) to run the script on.
2. Click the **Run Script** ( ) icon in the menu bar and click **Run CLI Script**.
   The **Run CLI Script** window will appear.



Run CLI Script

CLI Script

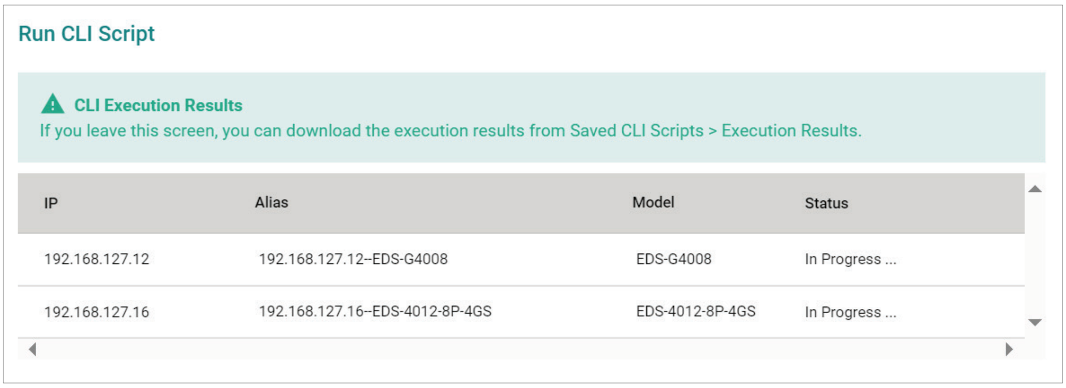
0 / 9999

Selected Devices

IP	Alias	Model
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008
192.168.127.16	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS

3. Enter the script:
   a. In the CLI Script field, enter the CLI command(s) to execute.
   b. Confirm the selected devices that the script will be executed on.
   c. Click **Run**.

4. The system will show the script execution status for each device.



Run CLI Script

CLI Execution Results

If you leave this screen, you can download the execution results from Saved CLI Scripts > Execution Results.

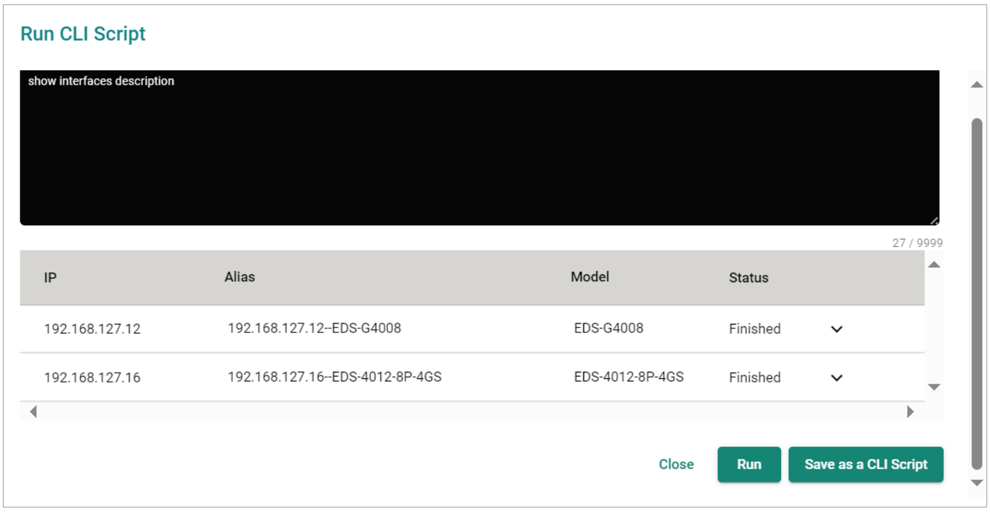
IP	Alias	Model	Status
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008	In Progress ...
192.168.127.16	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	In Progress ...

NOTE

You cannot perform any actions on the device while the script is running. If you close the MXview One web page, you can download the execution results from **Saved CLI Scripts > Execution Results** page.

5. Check the script results.

When all devices have finished running the script, click the **Expand** (⌄) icon next to the device to check the result.



Run CLI Script

```
show interfaces description
```

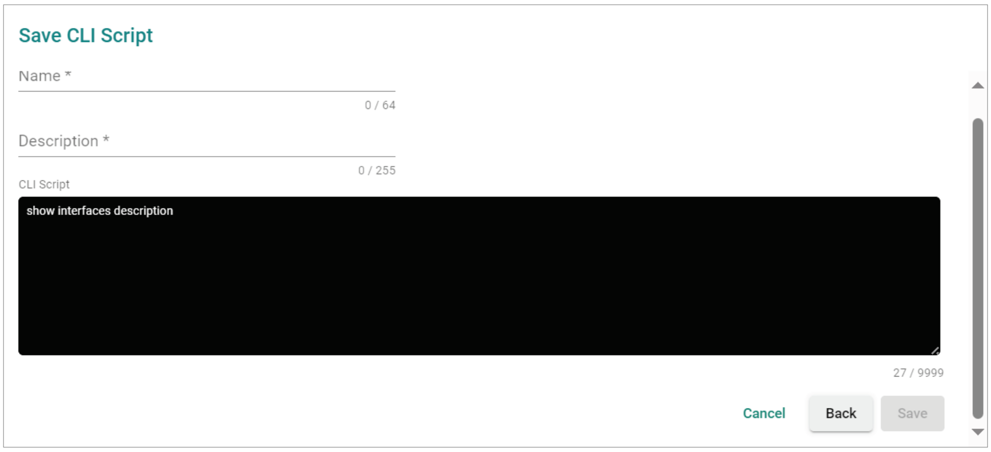
27 / 9999

IP	Alias	Model	Status	
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008	Finished	⌄
192.168.127.16	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	Finished	⌄

6. You can either run or save the script:

   a. **Run script**: Modify the CLI script (if necessary) and click **Run**. The system will execute the CLI script on the selected devices.

   b. **Save script**: Click **Save as a CLI Script** to save the CLI script for future use.
   The **Save CLI Script** window will appear.



Save CLI Script

Name *

0 / 64

Description *

0 / 255

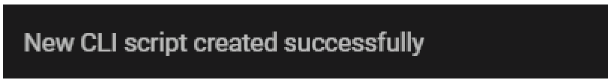
CLI Script

```
show interfaces description
```

27 / 9999

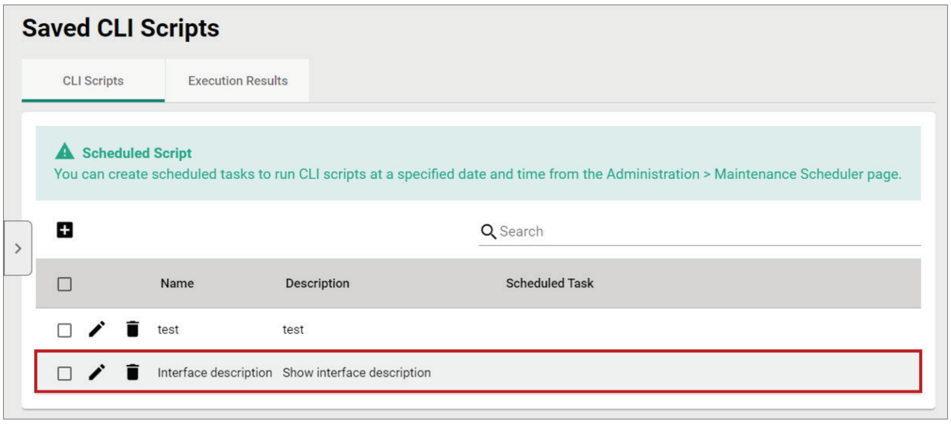
   i. Enter a name and description for the script.
   The CLI Script field is read-only and cannot be modified here.

   ii. Click **Save**. A confirmation message will appear.



New CLI script created successfully

   iii. The CLI script will be stored and shown in the **Saved CLI Scripts** section.



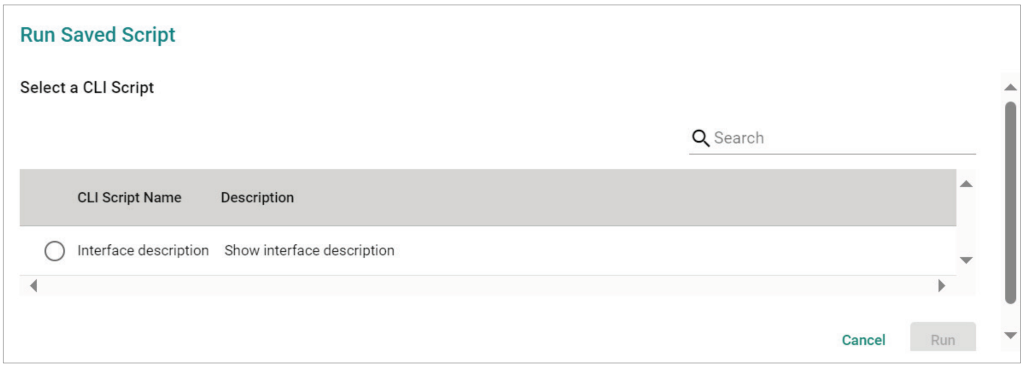
Saved CLI Scripts

Scheduled Script
You can create scheduled tasks to run CLI scripts at a specified date and time from the Administration > Maintenance Scheduler page.

□	Name	Description	Scheduled Task
□	test	test	
□	Interface description	Show interface description	

Running a Saved CLI Script

1. In the **Topology** or **Device Management** screen, select the device(s) to run the script on.
2. Click the **Run Script** () icon in the menu bar and click **Run Saved Script**.
   The **Run Saved Script** window will appear.

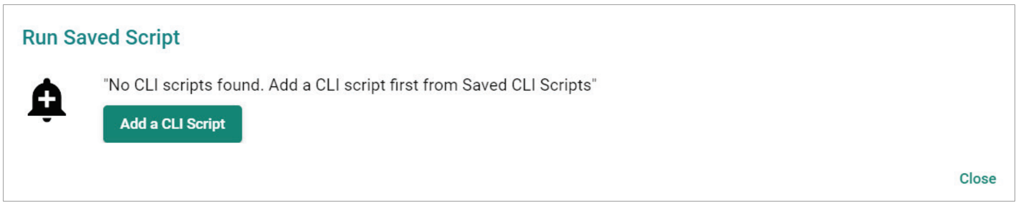


Run Saved Script

Select a CLI Script

	CLI Script Name	Description
○	Interface description	Show interface description

If no saved scripts can be found, the following message will appear.

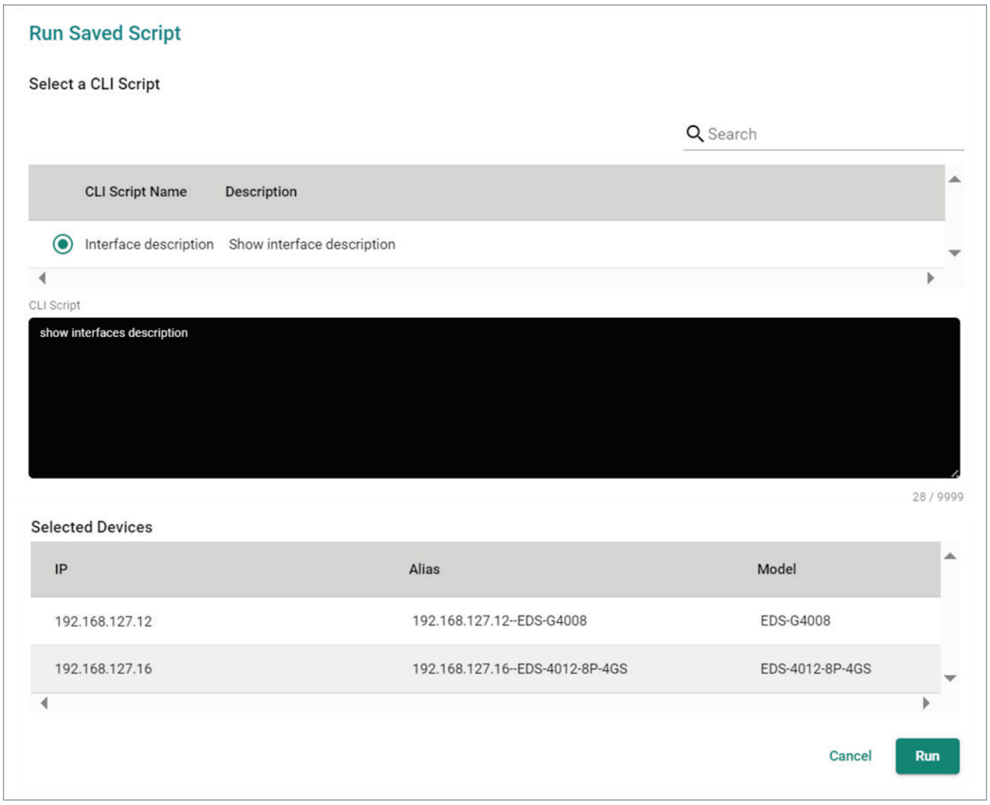


Run Saved Script

"No CLI scripts found. Add a CLI script first from Saved CLI Scripts"

Click the **Add a CLI Script** to create a script. Refer to Adding a CLI Script.

3. Select the script you want to execute and confirm the selected devices that the script will be executed on.
   You can modify the script if necessary.



Run Saved Script

Select a CLI Script

	CLI Script Name	Description
●	Interface description	Show interface description

CLI Script

```
show interfaces description
```

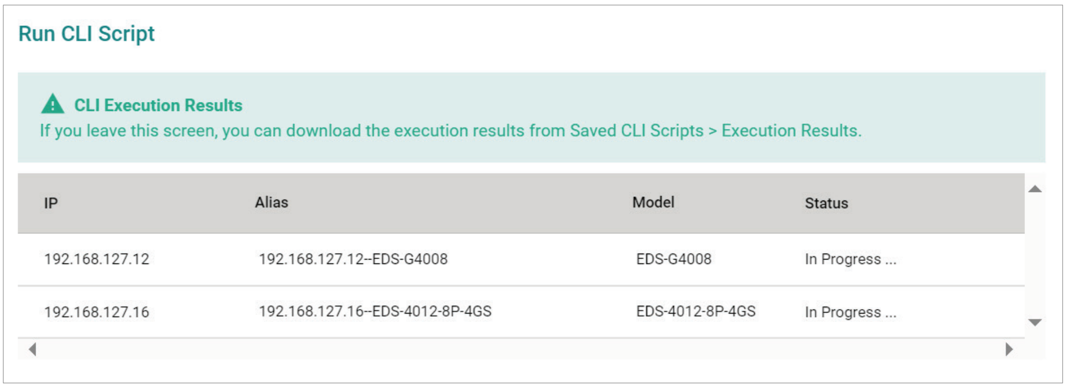
28 / 9999

Selected Devices

IP	Alias	Model
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008
192.168.127.16	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS

4. Click **Run**.

5. The system will show the script execution status for each device.



Run CLI Script

⚠ CLI Execution Results

If you leave this screen, you can download the execution results from Saved CLI Scripts > Execution Results.

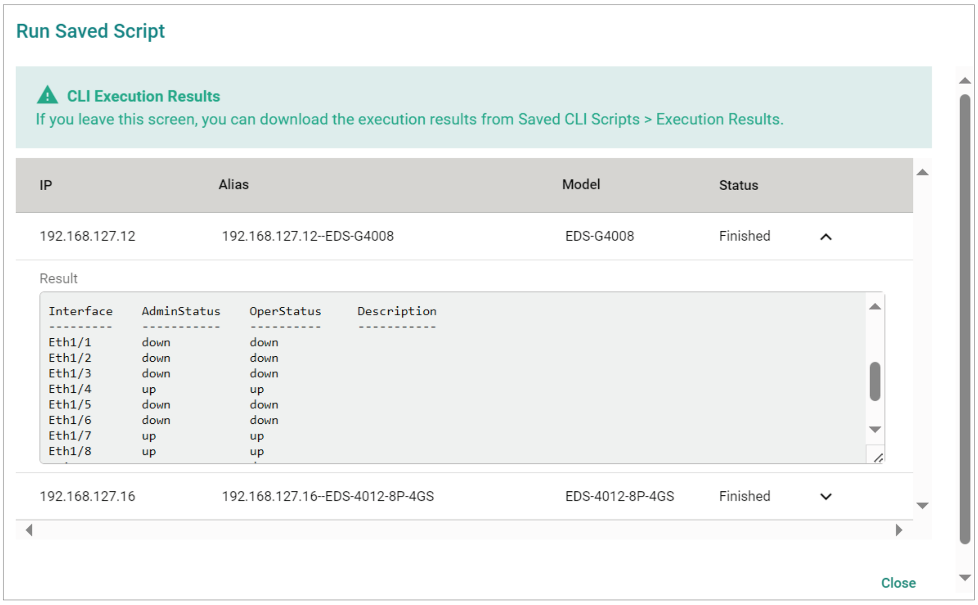
IP	Alias	Model	Status
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008	In Progress ...
192.168.127.16	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	In Progress ...

NOTE

You cannot perform any actions on the device while the script is running. If you close the MXview One web page, you can download the execution results from **Saved CLI Scripts > Execution Results** page.

6. Check the script results

   When all devices have finished running the script, click the **Expand** (﹀) icon next to the device to check the result.



Run Saved Script

⚠ **CLI Execution Results**
If you leave this screen, you can download the execution results from Saved CLI Scripts > Execution Results.

IP	Alias	Model	Status	
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008	Finished	^

Result

```
Interface    AdminStatus    OperStatus    Description
---------    -----------    ----------    -----------
Eth1/1       down           down
Eth1/2       down           down
Eth1/3       down           down
Eth1/4       up             up
Eth1/5       down           down
Eth1/6       down           down
Eth1/7       up             up
Eth1/8       up             up
```

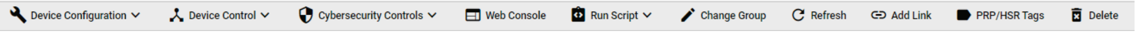
IP	Alias	Model	Status	
192.168.127.16	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	Finished	﹀

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**.

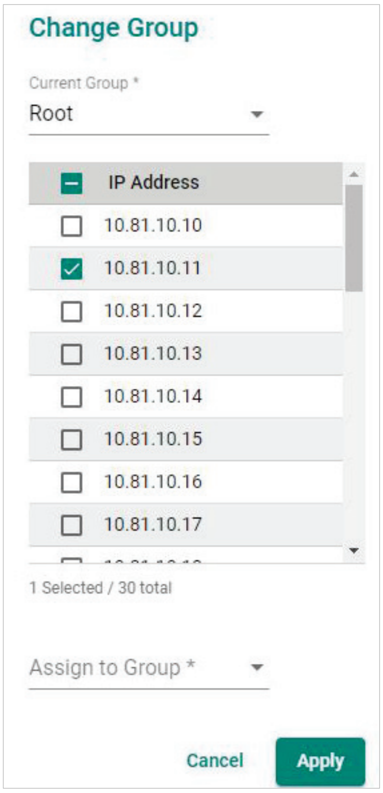
1. Navigate to **Menu** (☰) **> Topology**.
   The **Topology** screen will appear and display the Topology Map by default.
2. Select one of the following views:
   - **Topology view:** Displays a graphical representation of the devices in your network topology.
   - **List view:** Displays a list of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



Change Group

Current Group *
Root

▬	IP Address
□	10.81.10.10
☑	10.81.10.11
□	10.81.10.12
□	10.81.10.13
□	10.81.10.14
□	10.81.10.15
□	10.81.10.16
□	10.81.10.17

1 Selected / 30 total

Assign to Group *

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

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

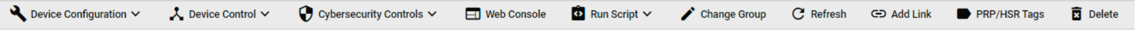
Refreshing the Device Status

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.

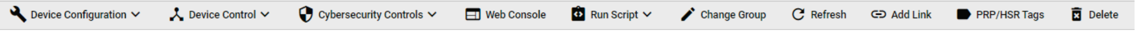
2. Select one of the following views:

   - **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. Device Management

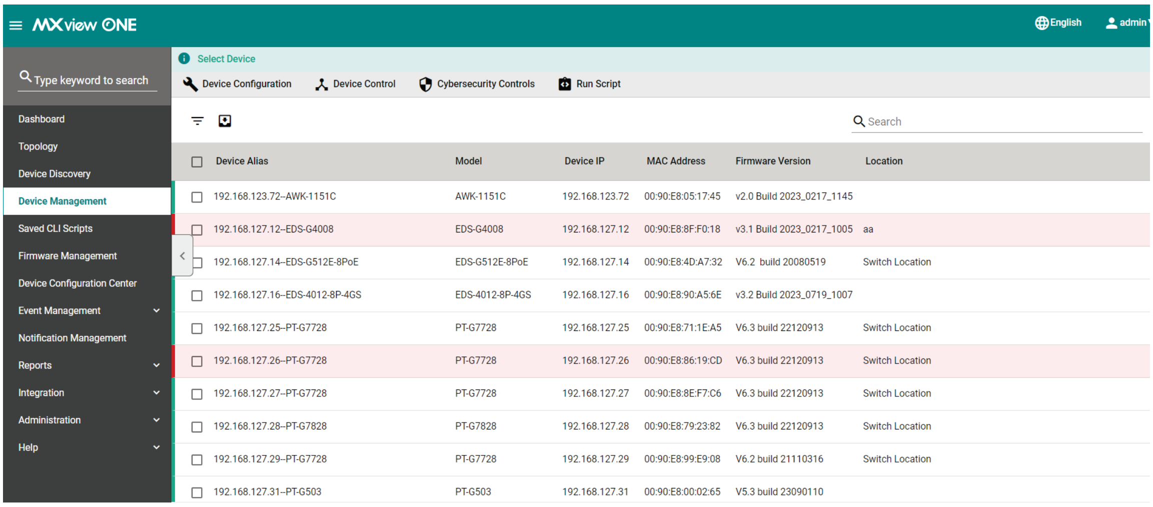
The **Device Management** section provides quick access buttons to commonly used device management functions. Users can perform these functions either from the Topology Menu Bar, or directly from the Device Management page. This features also enables users to perform certain functions directly from within MXview One, without having to go to the device’s web console.

Device Management Overview

At the top of this screen is the menu bar which provides quick access buttons for device management functions. At the bottom part of the page is the device list which allows users to select the devices to perform the quick function on.

The quick access functions are organized into four main types:

- Device Configuration
- Device Control
- Cybersecurity Controls
- Run Script



□	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
□	192.168.127.12--EDS-G4008	EDS-G4008	192.168.127.12	00:90:E8:8F:F0:18	v3.1 Build 2023_0217_1005	aa
□	192.168.127.14--EDS-G512E-8PoE	EDS-G512E-8PoE	192.168.127.14	00:90:E8:4D:A7:32	V6.2 build 20080519	Switch Location
□	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	192.168.127.16	00:90:E8:90:A5:6E	v3.2 Build 2023_0719_1007	
□	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location
□	192.168.127.26--PT-G7728	PT-G7728	192.168.127.26	00:90:E8:86:19:CD	V6.3 build 22120913	Switch Location
□	192.168.127.27--PT-G7728	PT-G7728	192.168.127.27	00:90:E8:8E:F7:C6	V6.3 build 22120913	Switch Location
□	192.168.127.28--PT-G7828	PT-G7828	192.168.127.28	00:90:E8:79:23:82	V6.3 build 22120913	Switch Location
□	192.168.127.29--PT-G7728	PT-G7728	192.168.127.29	00:90:E8:99:E9:08	V6.2 build 21110316	Switch Location
□	192.168.127.31--PT-G503	PT-G503	192.168.127.31	00:90:E8:00:02:65	V5.3 build 23090110	

Refer to the following section for an overview of all functions in each category.

Device Configuration

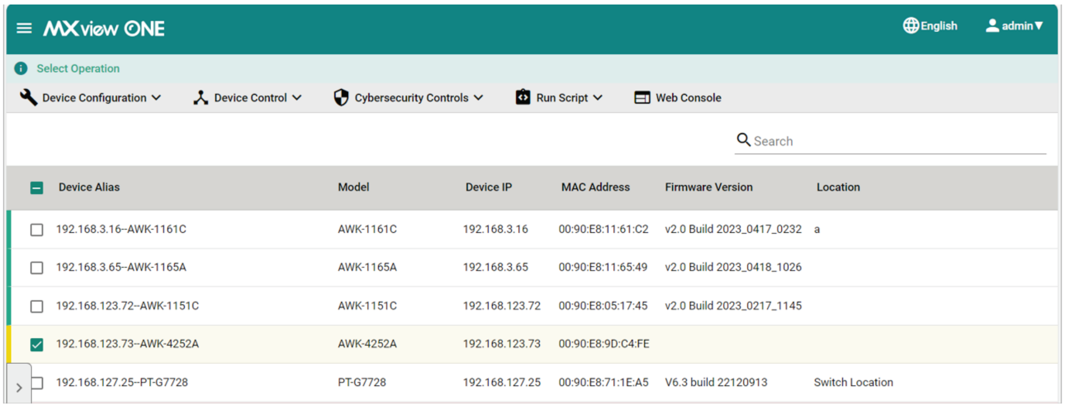
Change Wi-Fi Channel

If the performance of your wireless devices is affected by interruptions in the current Wi-Fi channel, you can use the Change Wi-Fi Channel function to switch to another channel to improve performance.

1. Navigate to **Menu** (☰) **> Device Management**.

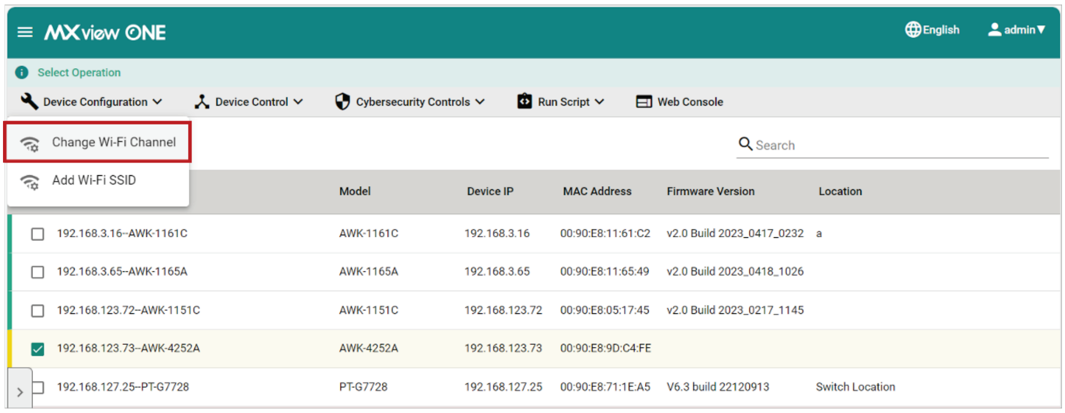
   The **Device Management** screen will appear.

2. Selected the device(s) to configure from the device list.



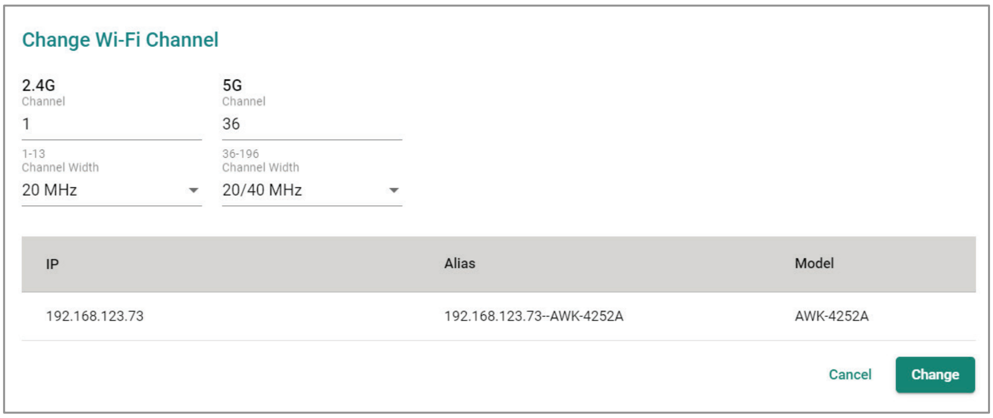
	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.3.16--AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
□	192.168.3.65--AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
□	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
☑	192.168.123.73--AWK-4252A	AWK-4252A	192.168.123.73	00:90:E8:9D:C4:FE		
□	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location

3. From the **Device Configuration** drop-down list, select **Change Wi-Fi Channel**.
   The **Change Wi-Fi Channel** screen will appear.



	Model	Device IP	MAC Address	Firmware Version	Location
□ 192.168.3.16--AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
□ 192.168.3.65--AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
□ 192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
☑ 192.168.123.73--AWK-4252A	AWK-4252A	192.168.123.73	00:90:E8:9D:C4:FE		
□ 192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location

4. Modify the Wi-Fi channel settings.



Change Wi-Fi Channel

2.4G
Channel: 1
1-13
Channel Width: 20 MHz

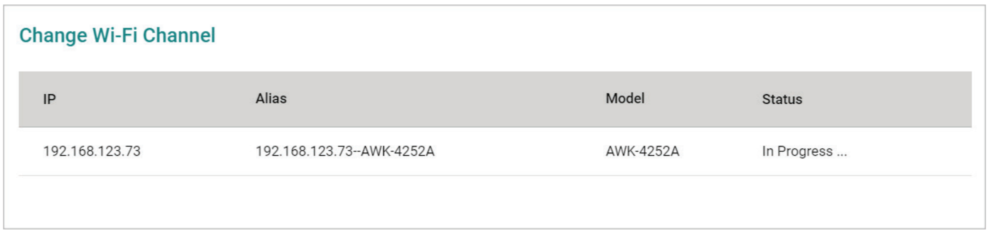
5G
Channel: 36
36-196
Channel Width: 20/40 MHz

IP	Alias	Model
192.168.123.73	192.168.123.73--AWK-4252A	AWK-4252A

Setting	Description	Limit
Channel	Enter the channel for the 2.4 GHz and 5 GHz band.	2.4 GHz: 1 to 13 5 GHz: 36 to 196

Setting	Description	Limit
Channel Width	Select the width of the channel.	2.4 GHz: 20 MHz, 20/40 MHz 5 GHz: 20 MHz, 20/40 MHz, 20/40/80 MHz

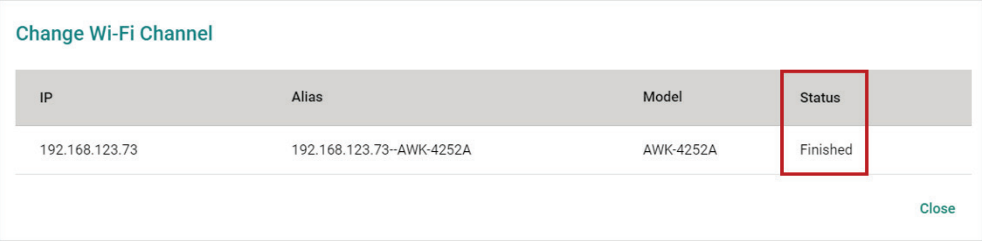
5. When finished, click **Change**. The system will execute the action.



Change Wi-Fi Channel

IP	Alias	Model	Status
192.168.123.73	192.168.123.73--AWK-4252A	AWK-4252A	In Progress ...

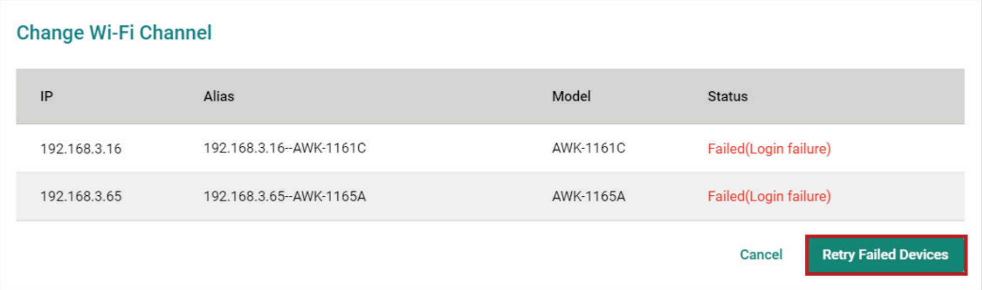
6. If successful, a confirmation will be shown in the Status column.



Change Wi-Fi Channel

IP	Alias	Model	Status
192.168.123.73	192.168.123.73--AWK-4252A	AWK-4252A	Finished

If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.



Change Wi-Fi Channel

IP	Alias	Model	Status
192.168.3.16	192.168.3.16--AWK-1161C	AWK-1161C	Failed(Login failure)
192.168.3.65	192.168.3.65--AWK-1165A	AWK-1165A	Failed(Login failure)

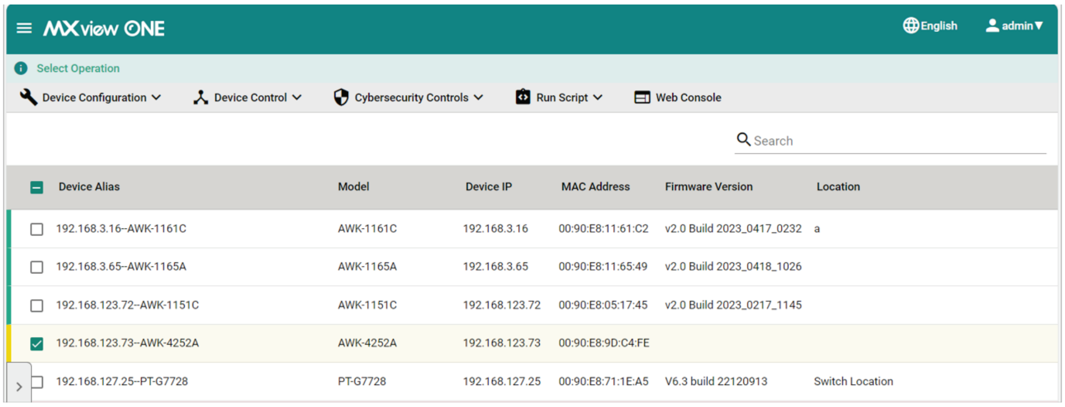
Add Wi-Fi SSID

Use the **Add Wi-Fi SSID** function to create additional Wi-Fi SSIDs for your wireless environment.

1. Navigate to **Menu** (☰) **> Device Management**.

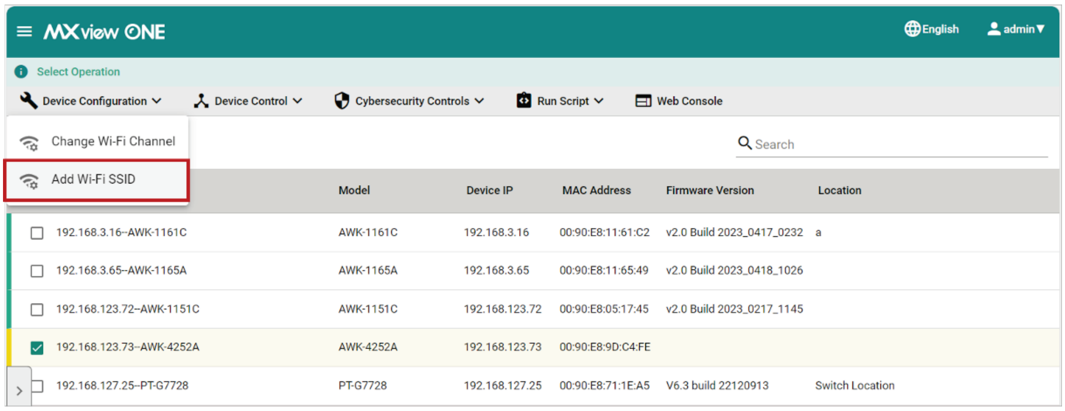
   The **Device Management** screen will appear.

2. Selected the device(s) to configure from the device list.



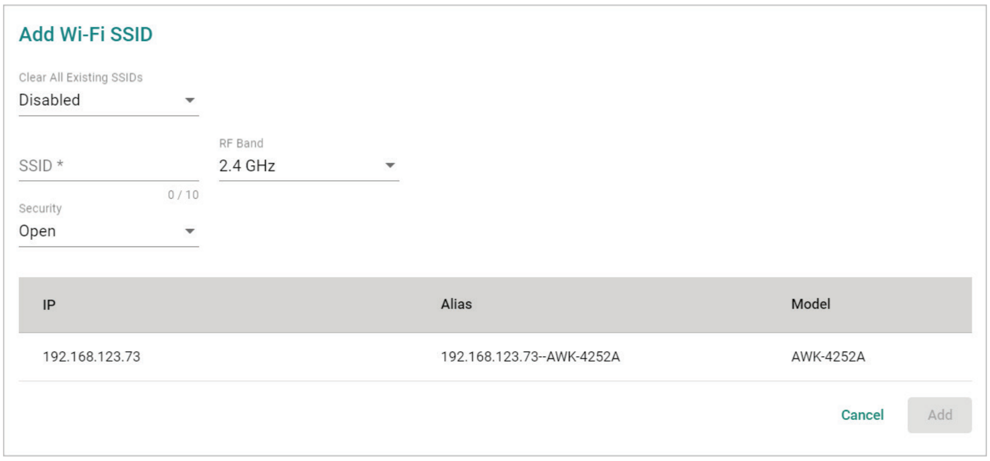
	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.3.16--AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
□	192.168.3.65--AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
□	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
☑	192.168.123.73--AWK-4252A	AWK-4252A	192.168.123.73	00:90:E8:9D:C4:FE		
□	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location

3. From the **Device Configuration** drop-down list, select **Add Wi-Fi SSID**.
   The **Add Wi-Fi SSID** screen will appear.



	Model	Device IP	MAC Address	Firmware Version	Location
□ 192.168.3.16--AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
□ 192.168.3.65--AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
□ 192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
☑ 192.168.123.73--AWK-4252A	AWK-4252A	192.168.123.73	00:90:E8:9D:C4:FE		
□ 192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location

4. Modify the Wi-Fi SSID settings.



Add Wi-Fi SSID

Clear All Existing SSIDs: Disabled

SSID *: 0 / 10

RF Band: 2.4 GHz

Security: Open

IP	Alias	Model
192.168.123.73	192.168.123.73--AWK-4252A	AWK-4252A

Clear All Existing SSIDs

Setting	Description
Enabled or Disabled	Choose to keep or delete all existing SSIDs on the selected device(s).

SSID

Setting	Description
SSID Name	Enter a name for the SSID.

RF Band

Setting	Description
2.4 GHz, 5 GHz	Select the RF band for this SSID.

Security

Setting	Description
Open WPA WPA2 WPA3 WPA/WPA2 Mixed WPA2/WPA3 Mixed	Select the security mode for the SSID.

When using any security mode other than **Open**, configure the following settings:

WPA Mode

Setting	Description
Personal	Authenticate WPA, WPA2, or WPA3 with a Pre-shared key (PSK).

Protected Management Frame

Setting	Description

Disabled	Disable the protected management frame. This option is not available when using WPA3.
802.11w	Use the 802.11w protocol as the protected management frame.

Encryption

Setting	Description
AES	Use Advance Encryption System (AES) encryption.
TKIP/AES Mixed	Use TKIP/AES Mixed encryption. This option provides a TKIP broadcast key and TKIP+AES unicast key to support legacy AP clients. This option is rarely used and is not available when using WPA3.

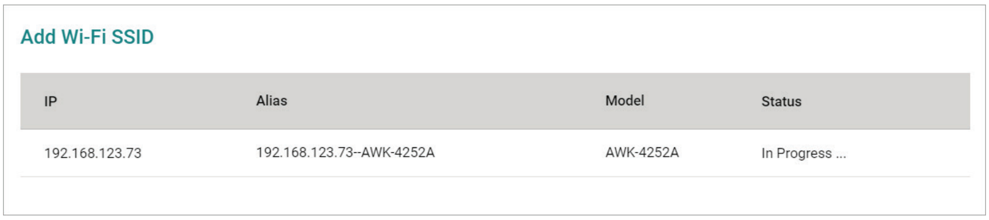
EAPOL Version

Setting	Description
1	Use EAPOL Version 1 as the security authentication method.
2	Use EAPOL Version 2 as the security authentication method.

Passphrase

Setting	Description
8 to 63 characters	Enter the passphrase. This is the master key to generate keys for encryption and decryption.

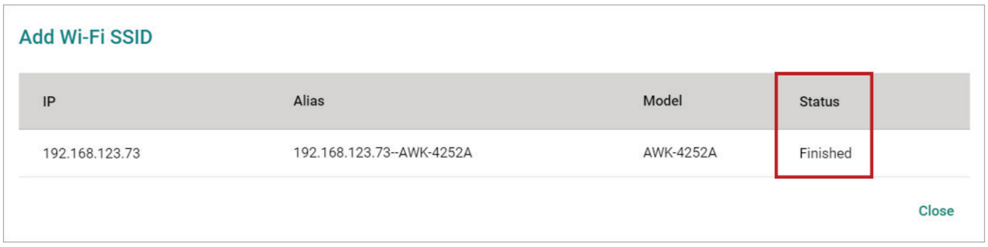
5. When finished, click **Add**. The system will execute the action.



Add Wi-Fi SSID

IP	Alias	Model	Status
192.168.123.73	192.168.123.73--AWK-4252A	AWK-4252A	In Progress ...

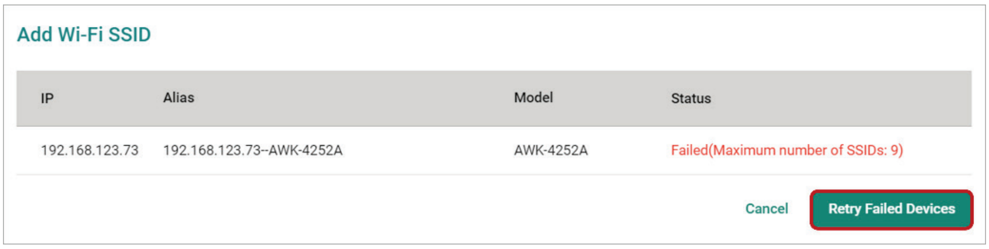
6. If successful, a confirmation will be shown in the Status column.



Add Wi-Fi SSID

IP	Alias	Model	Status
192.168.123.73	192.168.123.73--AWK-4252A	AWK-4252A	Finished

If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.



Add Wi-Fi SSID

IP	Alias	Model	Status
192.168.123.73	192.168.123.73--AWK-4252A	AWK-4252A	Failed(Maximum number of SSIDs: 9)

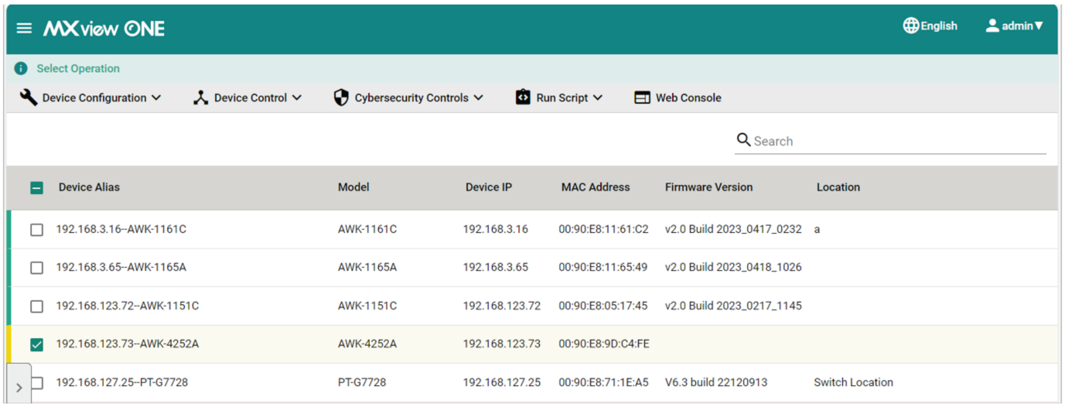
Dynamic Sticky MAC

Use the **Dynamic Sticky MAC** function to configure Dynamic Sticky MAC settings for one or multiple selected devices at once.

1. Navigate to **Menu** (☰) **> Device Management**.

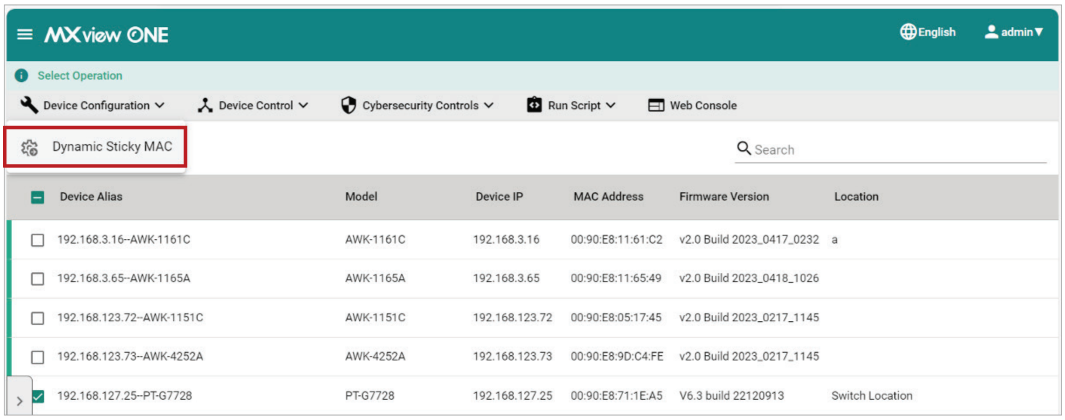
   The **Device Management** screen will appear.

2. Selected the device(s) to configure from the device list.



	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.3.16--AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
□	192.168.3.65--AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
□	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
☑	192.168.123.73--AWK-4252A	AWK-4252A	192.168.123.73	00:90:E8:9D:C4:FE		
□	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location

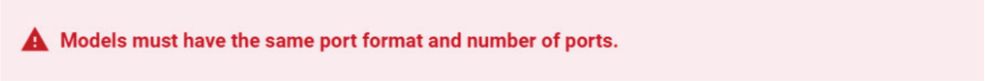
3. From the **Device Configuration** drop-down list, select **Dynamic Sticky MAC**.
The **Dynamic Sticky MAC** screen will appear.



	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.3.16--AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
□	192.168.3.65--AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
□	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
□	192.168.123.73--AWK-4252A	AWK-4252A	192.168.123.73	00:90:E8:9D:C4:FE	v2.0 Build 2023_0217_1145	
☑	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location

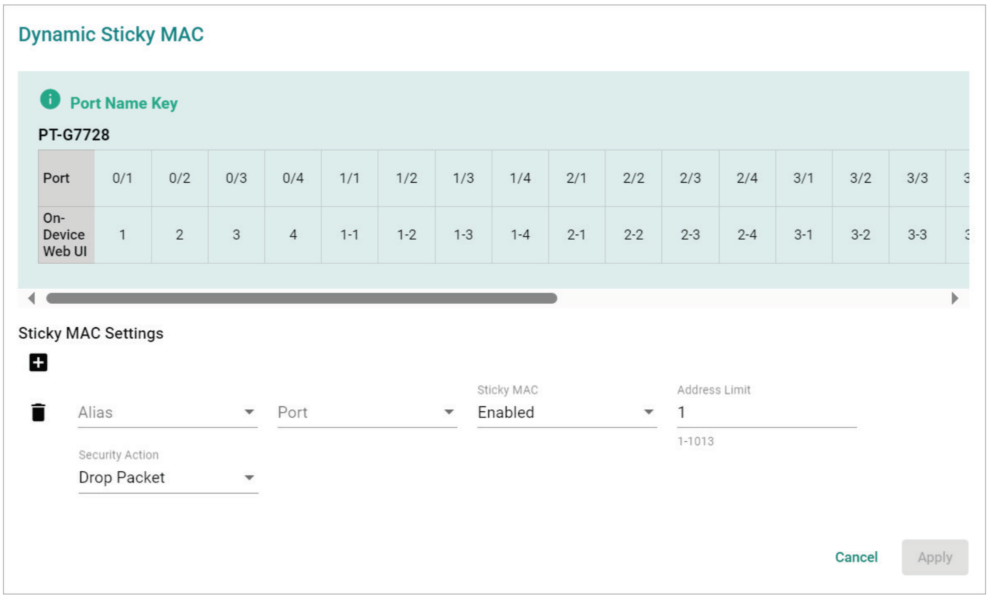
NOTE

You can only select devices with the same port format (either non-modular or modular device) and the same number of ports to execute the Dynamic Sticky MAC function. For example, you can set multiple non-modular switches at the same time, but not non-modular and modular switches. Because non-modular switch and modular switches have different port formats. An error message will appear if the selection is incompatible.



⚠ Models must have the same port format and number of ports.

4. Click the Add (⊞) icon and configure the following settings:



Dynamic Sticky MAC

Port Name Key

PT-G7728

Port	0/1	0/2	0/3	0/4	1/1	1/2	1/3	1/4	2/1	2/2	2/3	2/4	3/1	3/2	3/3	3
On-Device Web UI	1	2	3	4	1-1	1-2	1-3	1-4	2-1	2-2	2-3	2-4	3-1	3-2	3-3	3

Sticky MAC Settings

Alias:

Port:

Sticky MAC: Enabled

Address Limit: 1 (1-1013)

Security Action: Drop Packet

Alias

Setting	Description
Device Alias	Select the device(s) to configure Sticky MAC settings for.

Port

Setting	Description
Port	Select the port(s) associated with the device for which to configure the Sticky MAC settings for. You can refer to the Port Name Key section at the top of the page to understand the correlation between the ports listed in the Port drop-down menu and the on-device web UI.

Sticky MAC

Setting	Description
Enabled or Disabled	Enable or disable the Sticky MAC function for the selected port(s).

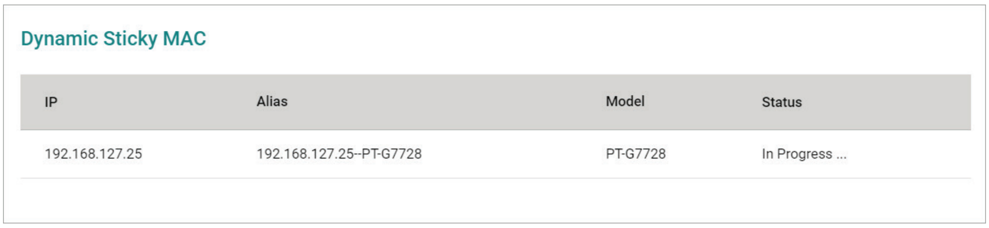
Address Limit

Setting	Description
1 to 1013	Specify the maximum numbers of the learned MAC addresses.

Security Action

Setting	Description
Shutdown Port	Shut down the port if a violation occurs.
Drop Packet	Drop the packet if a violation occurs.

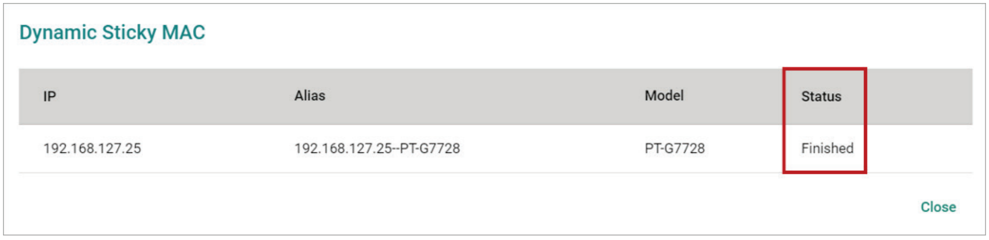
5. When finished, click **Apply**. The system will execute the action.



Dynamic Sticky MAC

IP	Alias	Model	Status
192.168.127.25	192.168.127.25--PT-G7728	PT-G7728	In Progress ...

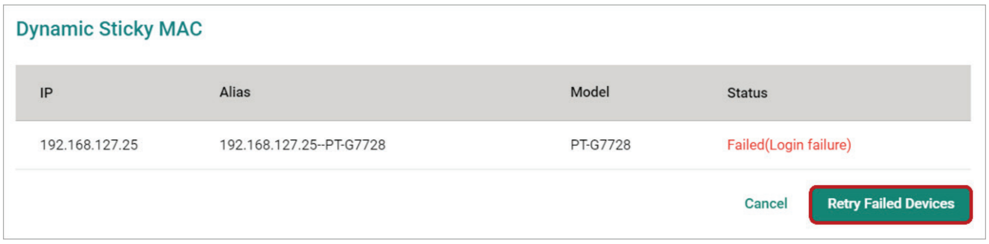
6. If successful, a confirmation will be shown in the Status column.



Dynamic Sticky MAC

IP	Alias	Model	Status
192.168.127.25	192.168.127.25--PT-G7728	PT-G7728	Finished

If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.



Dynamic Sticky MAC

IP	Alias	Model	Status
192.168.127.25	192.168.127.25--PT-G7728	PT-G7728	Failed(Login failure)

Device Control

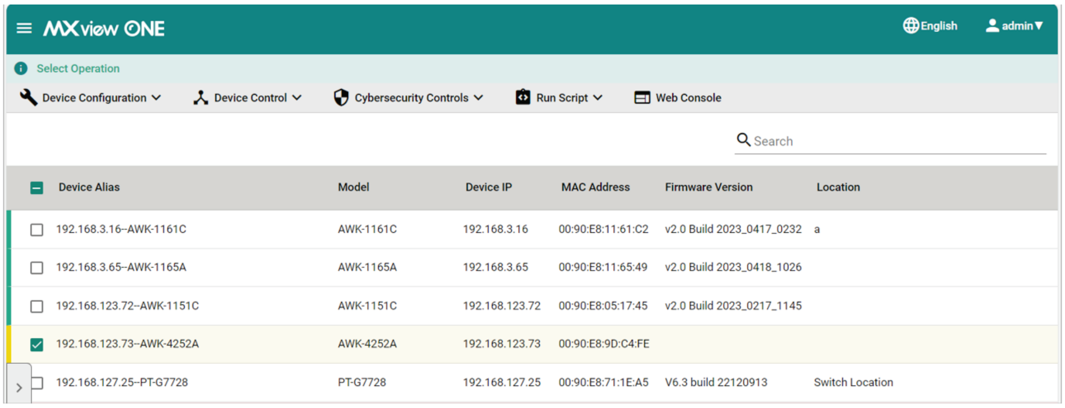
Reboot

Use the **Reboot** function to manually reboot devices or configure a reboot schedule.

1. Navigate to **Menu** (☰) **> Device Management**.

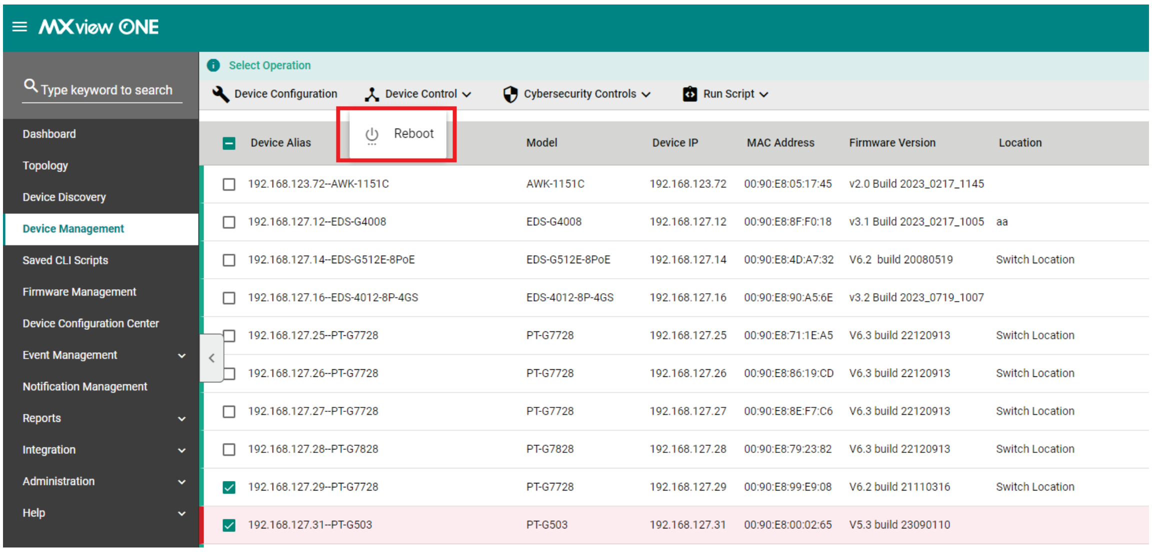
   The **Device Management** screen will appear.

2. Selected the device(s) to configure from the device list.



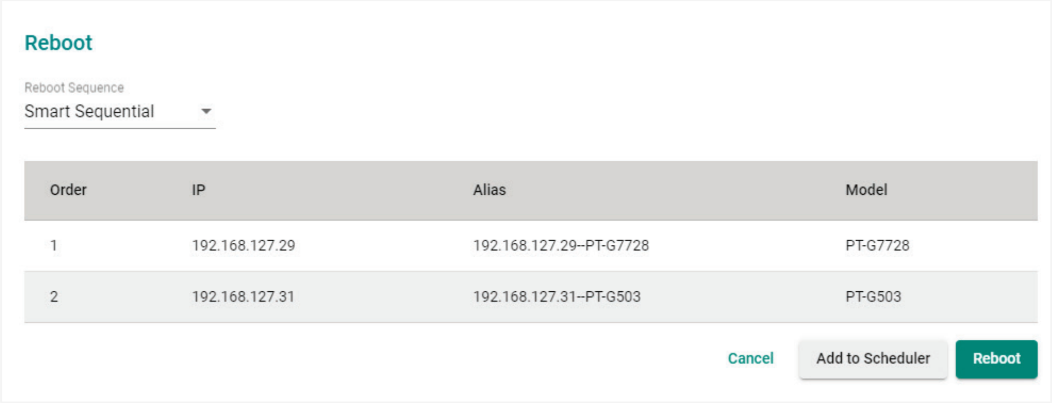
	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.3.16--AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
□	192.168.3.65--AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
□	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
☑	192.168.123.73--AWK-4252A	AWK-4252A	192.168.123.73	00:90:E8:9D:C4:FE		
□	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location

3. From the **Device Control** drop-down list, select **Reboot**.
   The **Reboot** screen will appear.



	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
□	192.168.127.12--EDS-G4008	EDS-G4008	192.168.127.12	00:90:E8:8F:F0:18	v3.1 Build 2023_0217_1005	aa
□	192.168.127.14--EDS-G512E-8PoE	EDS-G512E-8PoE	192.168.127.14	00:90:E8:4D:A7:32	V6.2 build 20080519	Switch Location
□	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	192.168.127.16	00:90:E8:90:A5:6E	v3.2 Build 2023_0719_1007	
□	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location
□	192.168.127.26--PT-G7728	PT-G7728	192.168.127.26	00:90:E8:86:19:CD	V6.3 build 22120913	Switch Location
□	192.168.127.27--PT-G7728	PT-G7728	192.168.127.27	00:90:E8:8E:F7:C6	V6.3 build 22120913	Switch Location
□	192.168.127.28--PT-G7828	PT-G7828	192.168.127.28	00:90:E8:79:23:82	V6.3 build 22120913	Switch Location
☑	192.168.127.29--PT-G7728	PT-G7728	192.168.127.29	00:90:E8:99:E9:08	V6.2 build 21110316	Switch Location
☑	192.168.127.31--PT-G503	PT-G503	192.168.127.31	00:90:E8:00:02:65	V5.3 build 23090110	

4. Configure the reboot sequence and execution time.



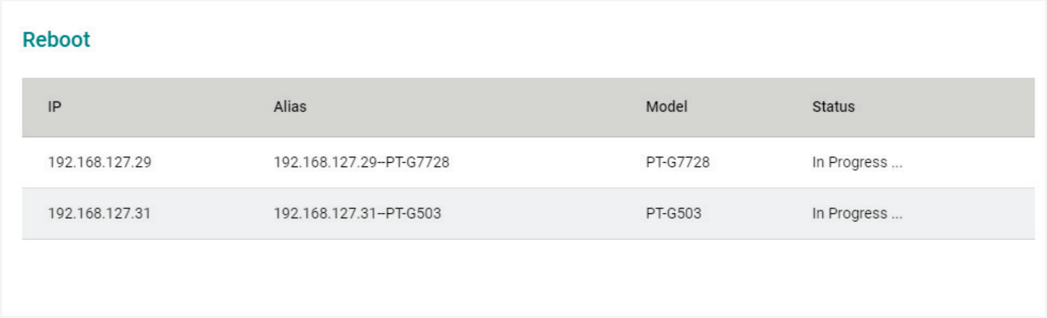
Reboot Sequence: Smart Sequential

Order	IP	Alias	Model
1	192.168.127.29	192.168.127.29--PT-G7728	PT-G7728
2	192.168.127.31	192.168.127.31--PT-G503	PT-G503

   a. Select the reboot sequence:
      - **Strict Sequential**: Reboot the devices based on the device sequence in the topology starting from the device furthest away from the computer running MXview One, proceeding to the nearest one.
      - **Smart Sequential:** Reboot the devices based on the device sequence in the topology but simultaneously reboot all devices in the same topology layer.

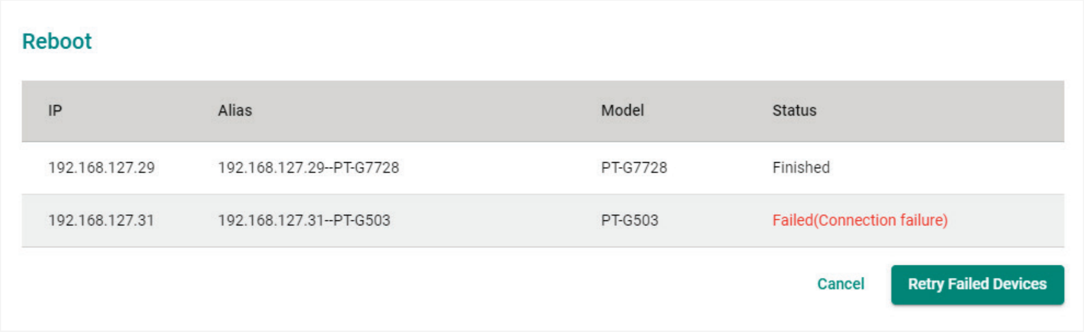
   b. Select an execution time:
      - **Reboot**: Click **Reboot** to restart the devices instantly.
      - **Add to Scheduler:** Click **Add to Schedular** to create a new scheduled task. MXview One will reboot the devices based on the specified time and date in the schedule.

5. To reboot devices instantly, click **Reboot**. The system will execute the action.



IP	Alias	Model	Status
192.168.127.29	192.168.127.29--PT-G7728	PT-G7728	In Progress ...
192.168.127.31	192.168.127.31--PT-G503	PT-G503	In Progress ...

6. If successful, a confirmation will be shown in the Status column.
   If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.



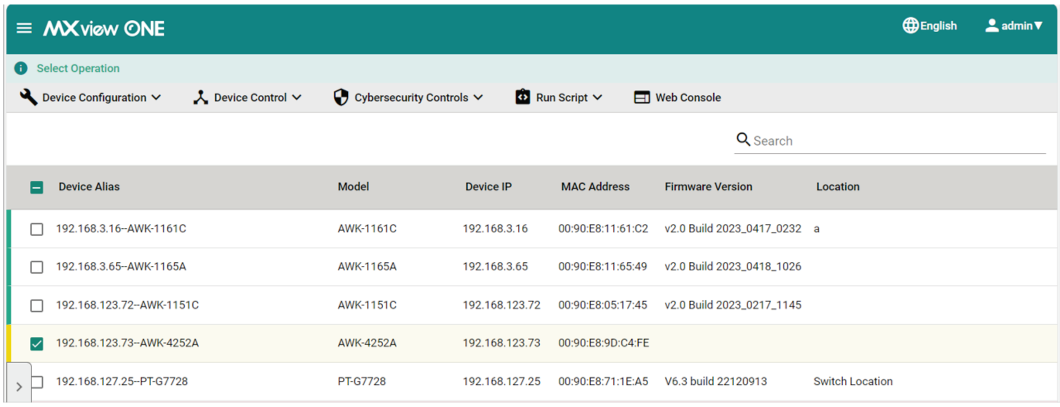
Reboot

IP	Alias	Model	Status
192.168.127.29	192.168.127.29--PT-G7728	PT-G7728	Finished
192.168.127.31	192.168.127.31--PT-G503	PT-G503	Failed(Connection failure)

Create Snapshot

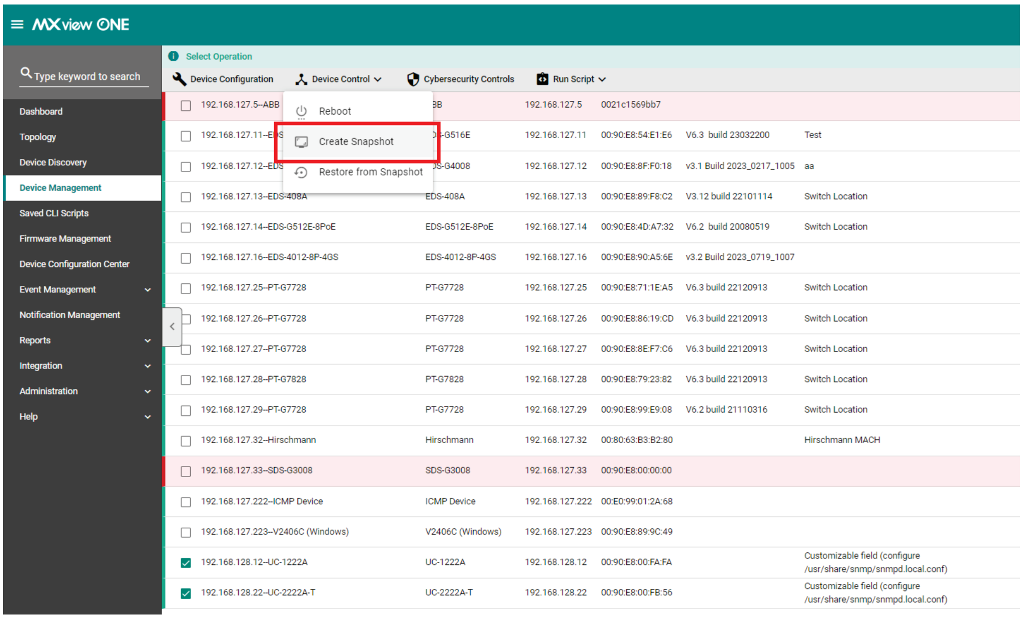
Use the **Snapshot** function to create a snapshot of the current configuration. The snapshot can be used to restore the configuration later.

1. Navigate to **Menu** (☰) **> Device Management**.
   The **Device Management** screen will appear.
2. Selected the device(s) to configure from the device list.



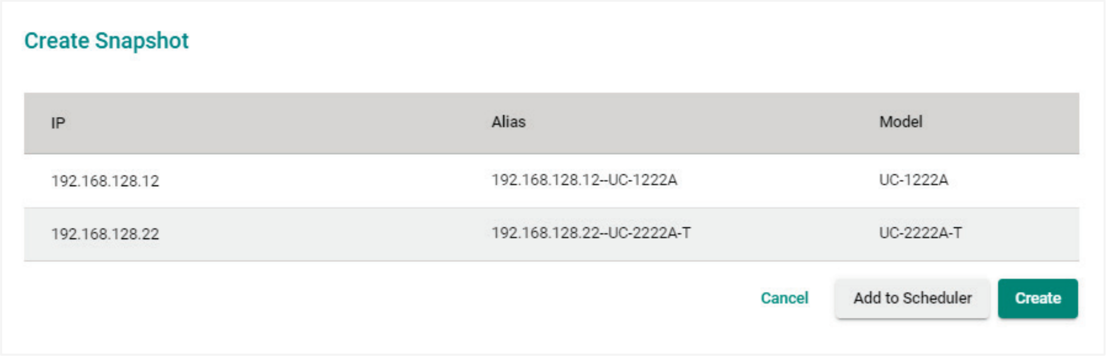
	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.3.16--AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
□	192.168.3.65--AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
□	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
☑	192.168.123.73--AWK-4252A	AWK-4252A	192.168.123.73	00:90:E8:9D:C4:FE		
□	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location

3. From the **Device Control** drop-down list, select **Create Snapshot**.
   The **Create Snapshot** screen will appear.



□	192.168.127.5--ABB	BB	192.168.127.5	0021c1569bb7		
□	192.168.127.11--E S	-G516E	192.168.127.11	00:90:E8:54:E1:E6	V6.3 build 23032200	Test
□	192.168.127.12--EDS	S-G4008	192.168.127.12	00:90:E8:8F:F0:18	v3.1 Build 2023_0217_1005	aa
□	192.168.127.13--EDS-408A	EDS-408A	192.168.127.13	00:90:E8:89:F8:C2	V3.12 build 22101114	Switch Location
□	192.168.127.14--EDS-G512E-8PoE	EDS-G512E-8PoE	192.168.127.14	00:90:E8:4D:A7:32	V6.2 build 20080519	Switch Location
□	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	192.168.127.16	00:90:E8:90:A5:6E	v3.2 Build 2023_0719_1007	
□	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location
□	192.168.127.26--PT-G7728	PT-G7728	192.168.127.26	00:90:E8:86:19:CD	V6.3 build 22120913	Switch Location
□	192.168.127.27--PT-G7728	PT-G7728	192.168.127.27	00:90:E8:8E:F7:C6	V6.3 build 22120913	Switch Location
□	192.168.127.28--PT-G7828	PT-G7828	192.168.127.28	00:90:E8:79:23:82	V6.3 build 22120913	Switch Location
□	192.168.127.29--PT-G7728	PT-G7728	192.168.127.29	00:90:E8:99:E9:08	V6.2 build 21110316	Switch Location
□	192.168.127.32--Hirschmann	Hirschmann	192.168.127.32	00:80:63:B3:B2:80		Hirschmann MACH
□	192.168.127.33--SDS-G3008	SDS-G3008	192.168.127.33	00:90:E8:00:00:00		
□	192.168.127.222--ICMP Device	ICMP Device	192.168.127.222	00:E0:99:01:2A:68		
□	192.168.127.223--V2406C (Windows)	V2406C (Windows)	192.168.127.223	00:90:E8:89:9C:49		
☑	192.168.128.12--UC-1222A	UC-1222A	192.168.128.12	00:90:E8:00:FA:FA		Customizable field (configure /usr/share/snmp/snmpd.local.conf)
☑	192.168.128.22--UC-2222A-T	UC-2222A-T	192.168.128.22	00:90:E8:00:FB:56		Customizable field (configure /usr/share/snmp/snmpd.local.conf)

4. Configure the execution time.

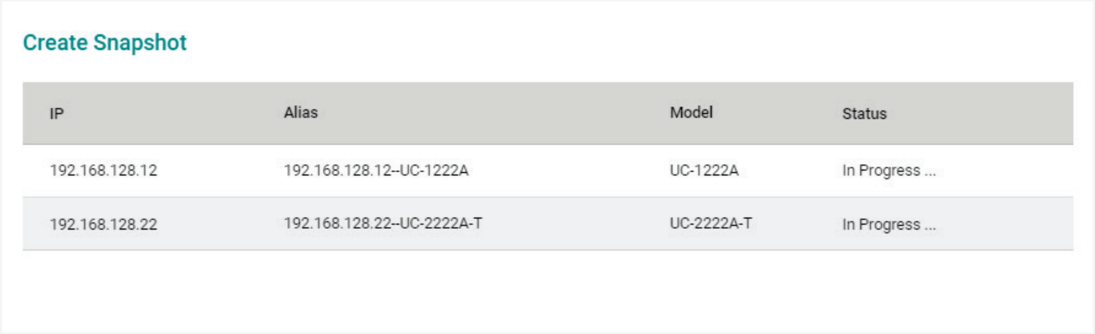


Create Snapshot

IP	Alias	Model
192.168.128.12	192.168.128.12--UC-1222A	UC-1222A
192.168.128.22	192.168.128.22--UC-2222A-T	UC-2222A-T

- **Create**: Click **Create** to create a snapshot instantly.
- **Add to Scheduler:** Click **Add to Schedular** to create a new scheduled task. MXview One will create a snapshot based on the specified time and date in the schedule.

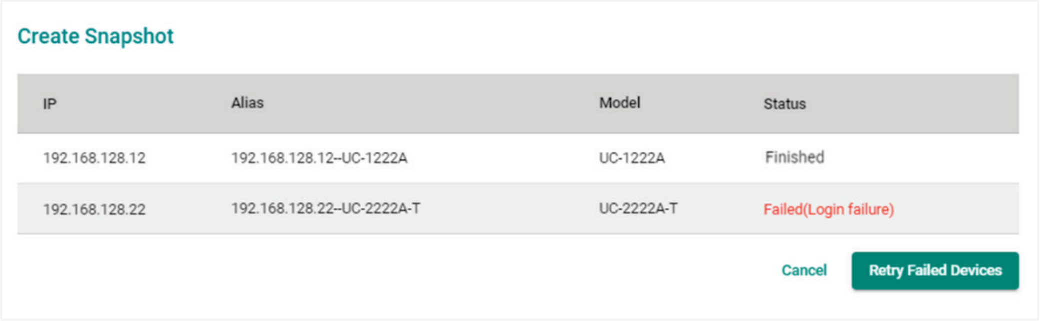
5. To create a snapshot instantly, click **Create**. The system will execute the action.



Create Snapshot

IP	Alias	Model	Status
192.168.128.12	192.168.128.12--UC-1222A	UC-1222A	In Progress ...
192.168.128.22	192.168.128.22--UC-2222A-T	UC-2222A-T	In Progress ...

6. If successful, a confirmation will be shown in the Status column.
If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.



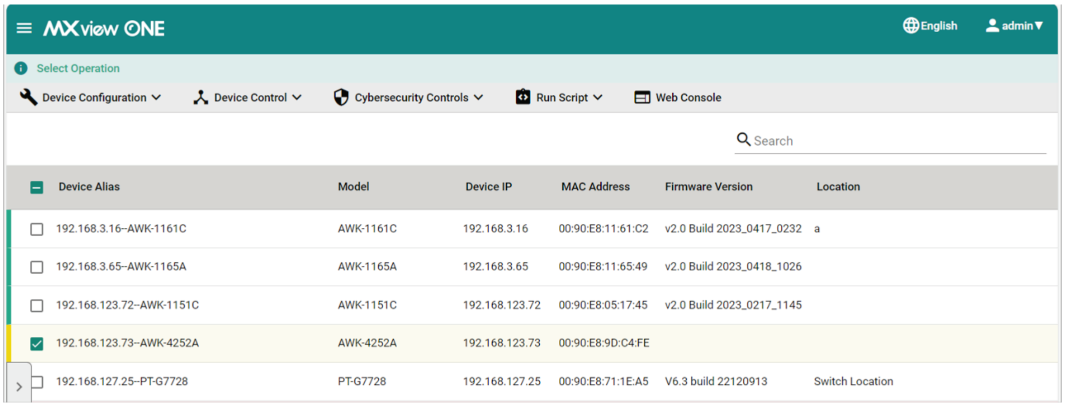
Create Snapshot

IP	Alias	Model	Status
192.168.128.12	192.168.128.12--UC-1222A	UC-1222A	Finished
192.168.128.22	192.168.128.22--UC-2222A-T	UC-2222A-T	Failed(Login failure)

Restore From Snapshot

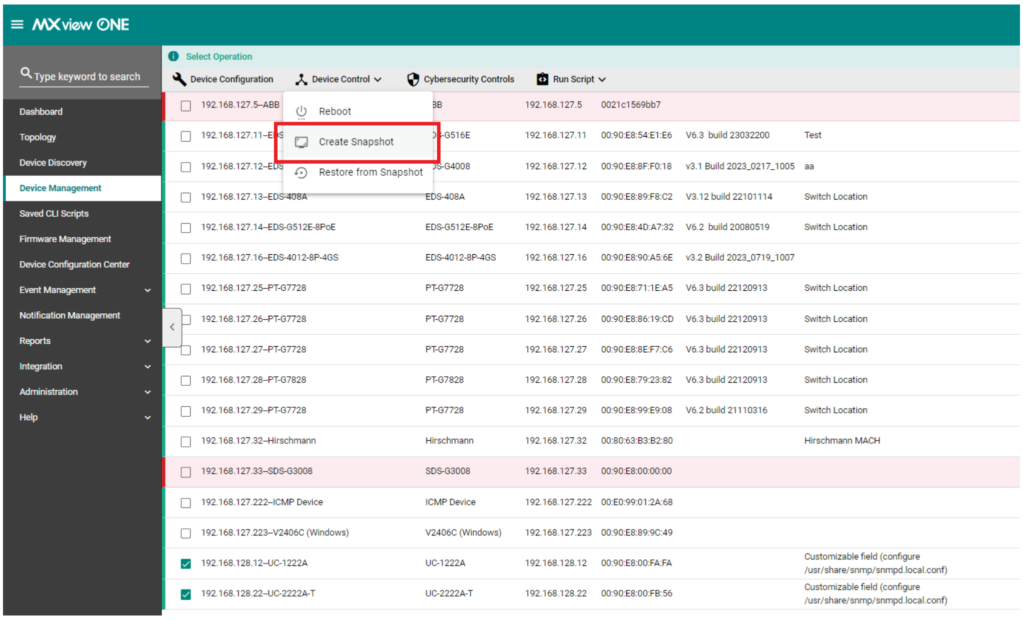
Use the **Restore from Snapshot** to restore the configuration from a previously created snapshot.

1. Navigate to **Menu** (☰) **> Device Management**.
   The **Device Management** screen will appear.
2. Selected the device(s) to configure from the device list.



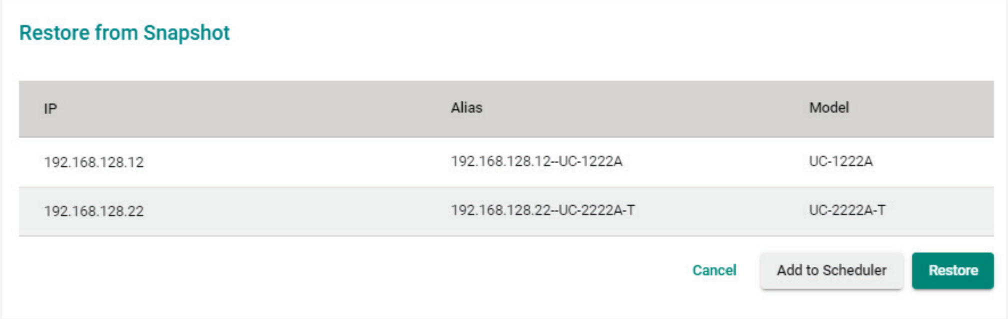
	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
☐	192.168.3.16--AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
☐	192.168.3.65--AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
☐	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
☑	192.168.123.73--AWK-4252A	AWK-4252A	192.168.123.73	00:90:E8:9D:C4:FE		
☐	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location

3. From the **Device Control** drop-down list, select **Restore from Snapshot**.
   The **Restore from Snapshot** screen will appear.



☐	192.168.127.5--ABB	3B	192.168.127.5	0021c1569bb7		
☐	192.168.127.11--E	-G516E	192.168.127.11	00:90:E8:54:E1:E6	V6.3 build 23032200	Test
☐	192.168.127.12--EDS	S-G4008	192.168.127.12	00:90:E8:8F:F0:18	v3.1 Build 2023_0217_1005	aa
☐	192.168.127.13--EDS-408A	EDS-408A	192.168.127.13	00:90:E8:89:F8:C2	V3.12 build 22101114	Switch Location
☐	192.168.127.14--EDS-G512E-8PoE	EDS-G512E-8PoE	192.168.127.14	00:90:E8:4D:A7:32	V6.2 build 20080519	Switch Location
☐	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	192.168.127.16	00:90:E8:90:A5:6E	v3.2 Build 2023_0719_1007	
☐	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location
☐	192.168.127.26--PT-G7728	PT-G7728	192.168.127.26	00:90:E8:86:19:CD	V6.3 build 22120913	Switch Location
☐	192.168.127.27--PT-G7728	PT-G7728	192.168.127.27	00:90:E8:8E:F7:C6	V6.3 build 22120913	Switch Location
☐	192.168.127.28--PT-G7828	PT-G7828	192.168.127.28	00:90:E8:79:23:82	V6.3 build 22120913	Switch Location
☐	192.168.127.29--PT-G7728	PT-G7728	192.168.127.29	00:90:E8:99:E9:08	V6.2 build 21110316	Switch Location
☐	192.168.127.32--Hirschmann	Hirschmann	192.168.127.32	00:80:63:B3:B2:80		Hirschmann MACH
☐	192.168.127.33--SDS-G3008	SDS-G3008	192.168.127.33	00:90:E8:00:00:00		
☐	192.168.127.222--ICMP Device	ICMP Device	192.168.127.222	00:E0:99:01:2A:68		
☐	192.168.127.223--V2406C (Windows)	V2406C (Windows)	192.168.127.223	00:90:E8:89:9C:49		
☑	192.168.128.12--UC-1222A	UC-1222A	192.168.128.12	00:90:E8:00:FA:FA		Customizable field (configure /usr/share/snmp/snmpd.local.conf)
☑	192.168.128.22--UC-2222A-T	UC-2222A-T	192.168.128.22	00:90:E8:00:FB:56		Customizable field (configure /usr/share/snmp/snmpd.local.conf)

4. Configure the execution time.

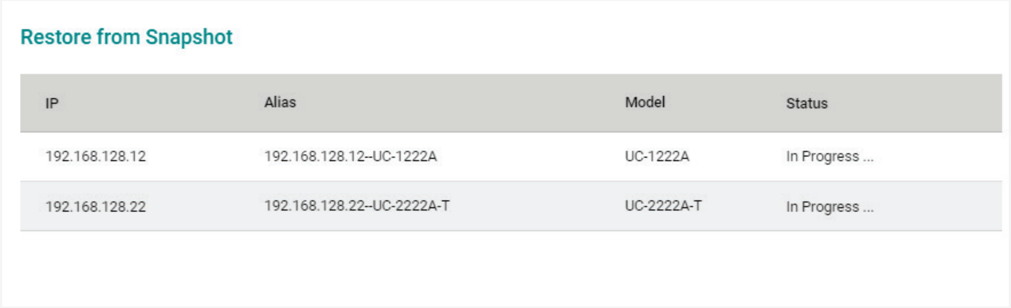


Restore from Snapshot

IP	Alias	Model
192.168.128.12	192.168.128.12--UC-1222A	UC-1222A
192.168.128.22	192.168.128.22--UC-2222A-T	UC-2222A-T

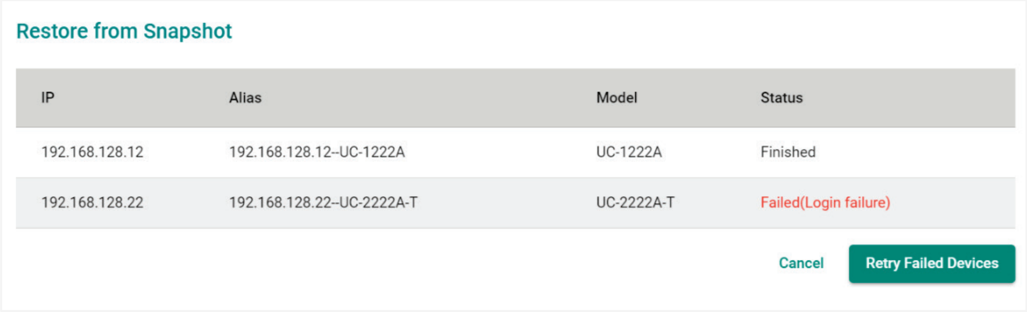
- **Restore**: Click **Restore** to restore the snapshot instantly.
- **Add to Scheduler:** Click **Add to Schedular** to create a new scheduled task. MXview One will restore the snapshot based on the specified time and date in the schedule.

5. To restore the snapshot instantly, click **Restore**. The system will execute the action.



IP	Alias	Model	Status
192.168.128.12	192.168.128.12--UC-1222A	UC-1222A	In Progress ...
192.168.128.22	192.168.128.22--UC-2222A-T	UC-2222A-T	In Progress ...

6. If successful, a confirmation will be shown in the Status column.
If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.



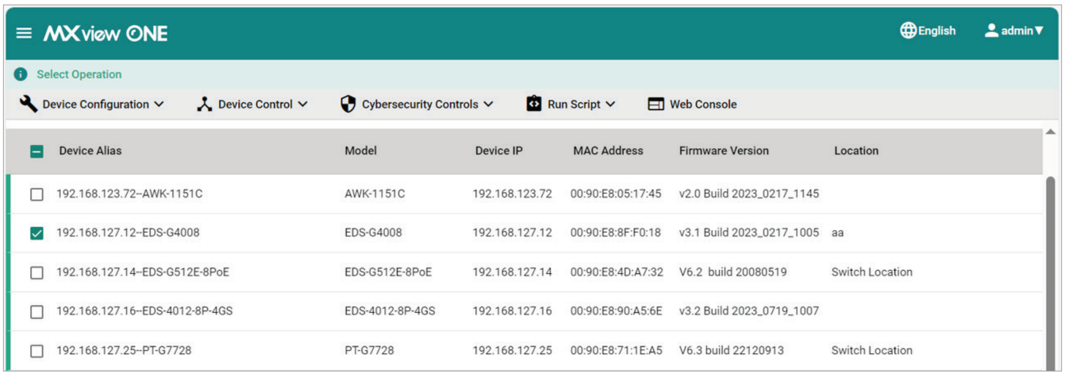
IP	Alias	Model	Status
192.168.128.12	192.168.128.12--UC-1222A	UC-1222A	Finished
192.168.128.22	192.168.128.22--UC-2222A-T	UC-2222A-T	Failed(Login failure)

Cybersecurity Controls

Sticky MAC On/Off

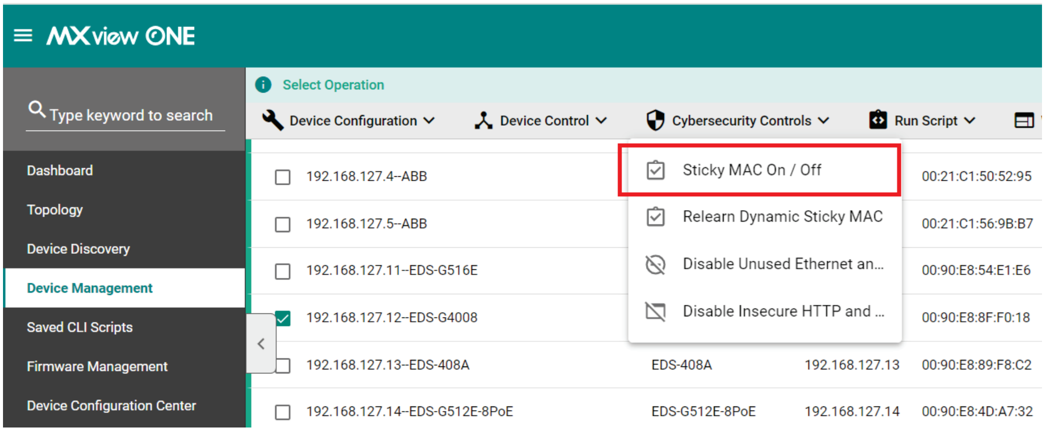
Use the **Sticky MAC On/Off** function to enable or disable Sticky MAC for the selected device(s).

1. Navigate to **Menu** (☰) **> Device Management**.
The **Device Management** screen will appear.
2. Selected the device(s) to configure from the device list.



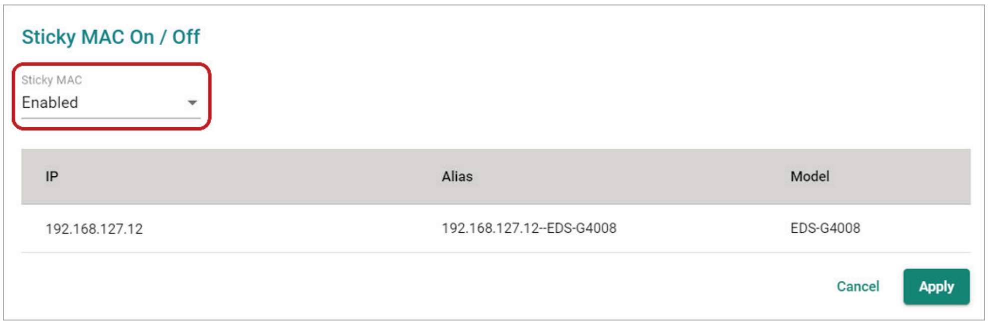
☐	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
☐	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
☑	192.168.127.12--EDS-G4008	EDS-G4008	192.168.127.12	00:90:E8:8F:F0:18	v3.1 Build 2023_0217_1005	aa
☐	192.168.127.14--EDS-G512E-8PoE	EDS-G512E-8PoE	192.168.127.14	00:90:E8:4D:A7:32	V6.2 build 20080519	Switch Location
☐	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	192.168.127.16	00:90:E8:90:A5:6E	v3.2 Build 2023_0719_1007	
☐	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location

3. From the **Cybersecurity Controls** drop-down list, select **Sticky MAC On/Off**.
   The **Sticky MAC On/Off** screen will appear.



☐	192.168.127.4--ABB			00:21:C1:50:52:95
☐	192.168.127.5--ABB			00:21:C1:56:9B:B7
☐	192.168.127.11--EDS-G516E			00:90:E8:54:E1:E6
☑	192.168.127.12--EDS-G4008			00:90:E8:8F:F0:18
☐	192.168.127.13--EDS-408A	EDS-408A	192.168.127.13	00:90:E8:89:F8:C2
☐	192.168.127.14--EDS-G512E-8PoE	EDS-G512E-8PoE	192.168.127.14	00:90:E8:4D:A7:32

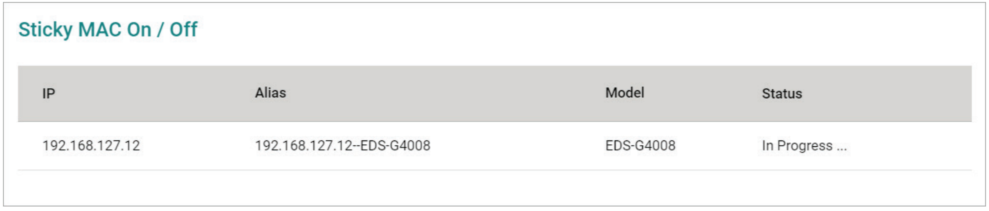
4. Choose to enable or disable Sticky MAC.


Sticky MAC On / Off

Sticky MAC: Enabled

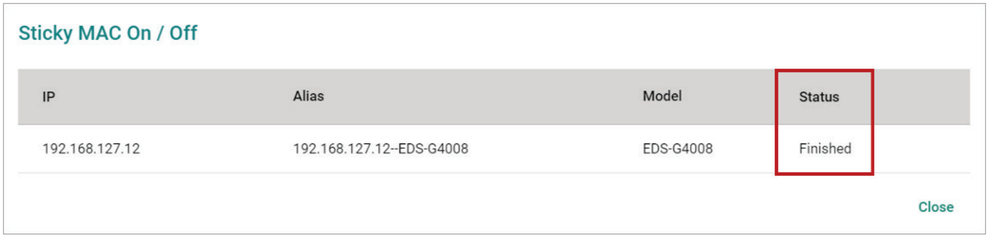
IP	Alias	Model
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008

5. Click **Apply**. The system will execute the action.


Sticky MAC On / Off

IP	Alias	Model	Status
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008	In Progress ...

6. If successful, a confirmation will be shown in the Status column.


Sticky MAC On / Off

IP	Alias	Model	Status
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008	Finished

   If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.

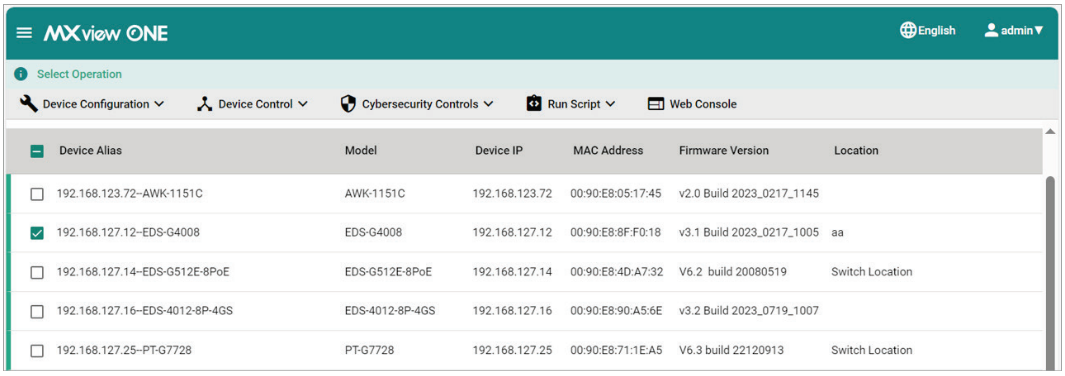
Relearning Dynamic Sticky MAC

Use the **Relearn Dynamic Sticky MAC** function to reset all previously learned MAC addresses and relearn them again for the selected device(s).

1. Navigate to **Menu** (☰) **> Device Management**.

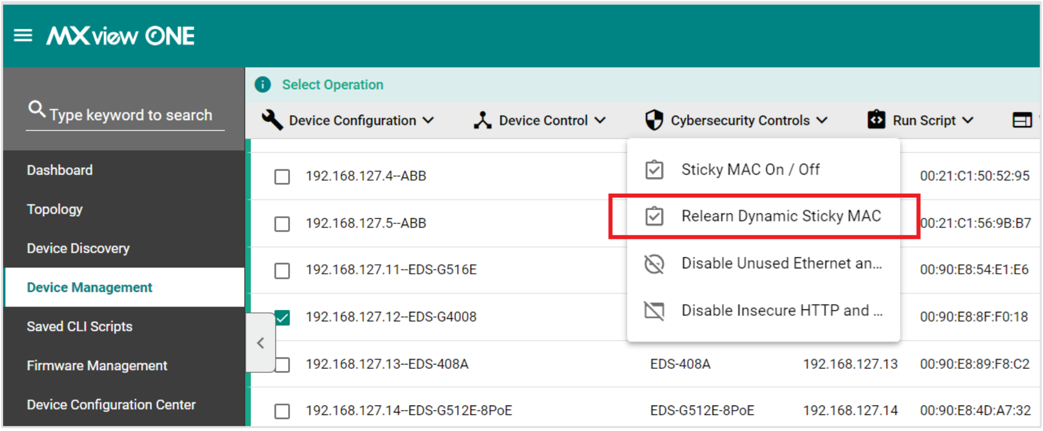
   The **Device Management** screen will appear.

2. Selected the device(s) to configure from the device list.



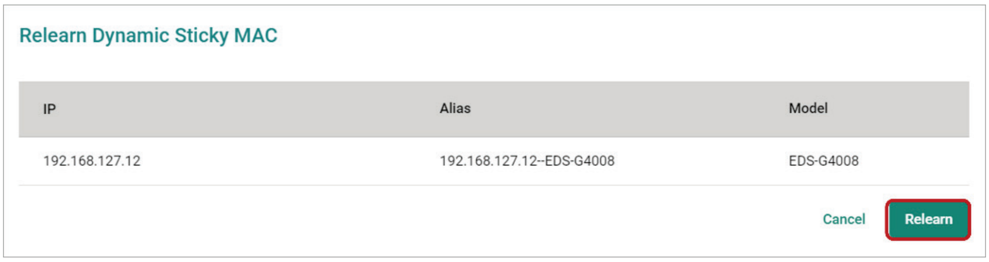
	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
☐	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
☑	192.168.127.12--EDS-G4008	EDS-G4008	192.168.127.12	00:90:E8:8F:F0:18	v3.1 Build 2023_0217_1005	aa
☐	192.168.127.14--EDS-G512E-8PoE	EDS-G512E-8PoE	192.168.127.14	00:90:E8:4D:A7:32	V6.2 build 20080519	Switch Location
☐	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	192.168.127.16	00:90:E8:90:A5:6E	v3.2 Build 2023_0719_1007	
☐	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location

3. From the **Cybersecurity Controls** drop-down list, select **Relearn Dynamic Sticky MAC**. The **Relearn Dynamic Sticky MAC** screen will appear.



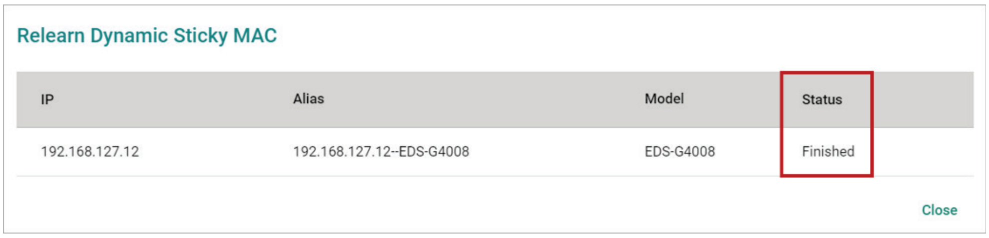
☐	192.168.127.4--ABB			00:21:C1:50:52:95
☐	192.168.127.5--ABB			00:21:C1:56:9B:B7
☐	192.168.127.11--EDS-G516E			00:90:E8:54:E1:E6
☑	192.168.127.12--EDS-G4008			00:90:E8:8F:F0:18
☐	192.168.127.13--EDS-408A	EDS-408A	192.168.127.13	00:90:E8:89:F8:C2
☐	192.168.127.14--EDS-G512E-8PoE	EDS-G512E-8PoE	192.168.127.14	00:90:E8:4D:A7:32

4. Click **Relearn**. The system will execute the action.


Relearn Dynamic Sticky MAC

IP	Alias	Model
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008

5. If successful, a confirmation will be shown in the Status column.


Relearn Dynamic Sticky MAC

IP	Alias	Model	Status
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008	Finished

   If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.

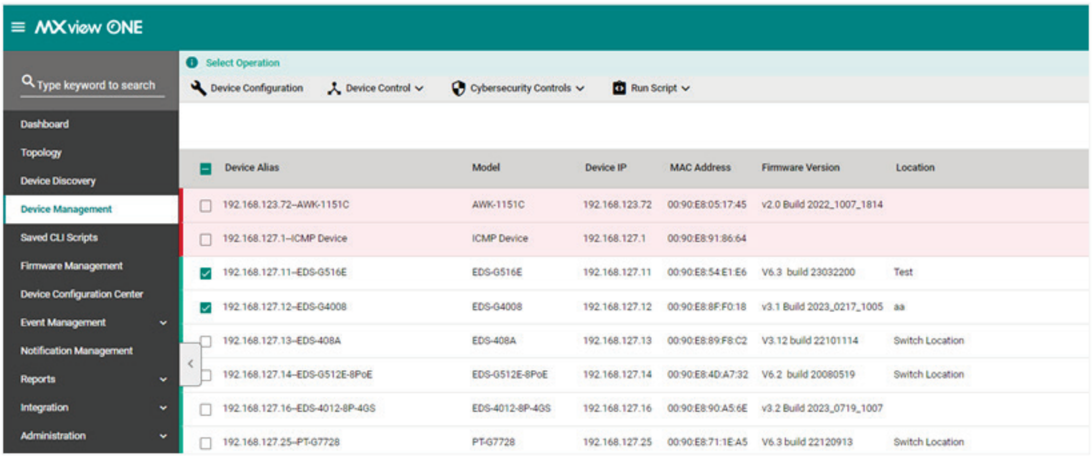
Disable Unused Ethernet and Fiber Ports

Use the **Disable Unused Ethernet and Fiber Ports** function to disable any unused Ethernet or fiber ports to make sure these ports cannot be exploited to gain unauthorized access to the device.

1. Navigate to **Menu** (☰) **> Device Management**.

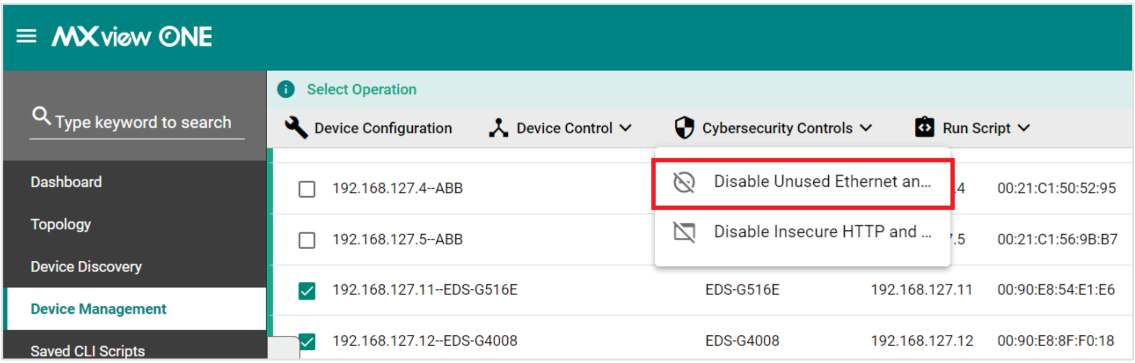
   The **Device Management** screen will appear.

2. Selected the device(s) to configure from the device list.



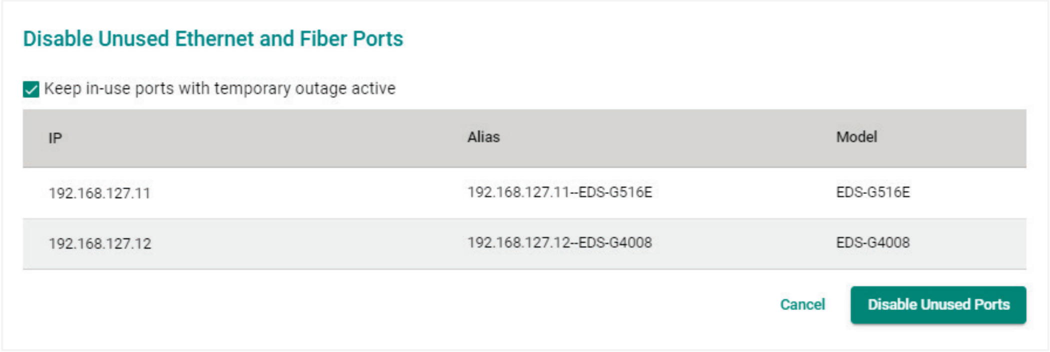
	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2022_1007_1814	
□	192.168.127.1--ICMP Device	ICMP Device	192.168.127.1	00:90:E8:91:86:64		
☑	192.168.127.11--EDS-G516E	EDS-G516E	192.168.127.11	00:90:E8:54:E1:E6	V6.3 build 23032200	Test
☑	192.168.127.12--EDS-G4008	EDS-G4008	192.168.127.12	00:90:E8:8F:F0:18	v3.1 Build 2023_0217_1005	aa
□	192.168.127.13--EDS-408A	EDS-408A	192.168.127.13	00:90:E8:89:F8:C2	V3.12 build 22101114	Switch Location
□	192.168.127.14--EDS-G512E-8PoE	EDS-G512E-8PoE	192.168.127.14	00:90:E8:4D:A7:32	V6.2 build 20080519	Switch Location
□	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	192.168.127.16	00:90:E8:90:A5:6E	v3.2 Build 2023_0719_1007	
□	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location

3. From the **Cybersecurity Controls** drop-down list, select **Disable Unused Ethernet and Fiber Ports**. The **Disable Unused Ethernet and Fiber Ports** screen will appear.



□	192.168.127.4--ABB		.4	00:21:C1:50:52:95
□	192.168.127.5--ABB		.5	00:21:C1:56:9B:B7
☑	192.168.127.11--EDS-G516E	EDS-G516E	192.168.127.11	00:90:E8:54:E1:E6
☑	192.168.127.12--EDS-G4008	EDS-G4008	192.168.127.12	00:90:E8:8F:F0:18

4. Choose to keep ports with temporary inactivity active.

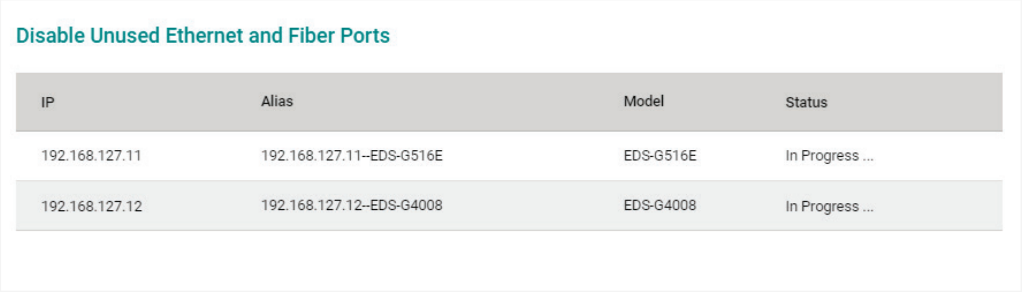


Disable Unused Ethernet and Fiber Ports

☑ Keep in-use ports with temporary outage active

IP	Alias	Model
192.168.127.11	192.168.127.11--EDS-G516E	EDS-G516E
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008

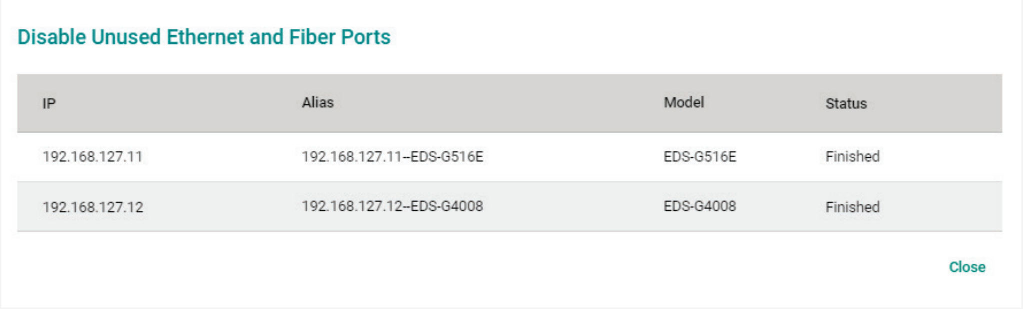
5. Click **Disable Unused Ports**. The system will execute the action.



Disable Unused Ethernet and Fiber Ports

IP	Alias	Model	Status
192.168.127.11	192.168.127.11--EDS-G516E	EDS-G516E	In Progress ...
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008	In Progress ...

If successful, a confirmation will be shown in the Status column.



Disable Unused Ethernet and Fiber Ports

IP	Alias	Model	Status
192.168.127.11	192.168.127.11--EDS-G516E	EDS-G516E	Finished
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008	Finished

If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.

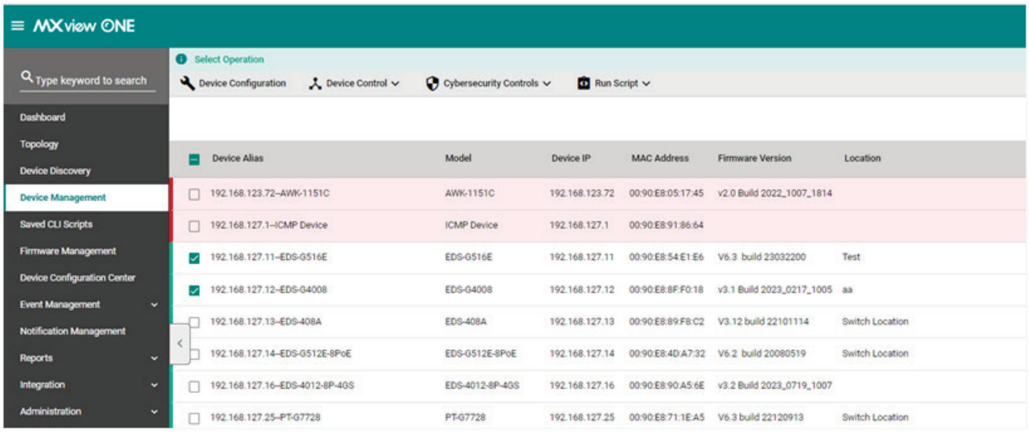
Disable Insecure HTTP and Telnet Console

Use the **Disable Insecure HTTP and Telnet Console** function to disable the non-secure HTTP and Telnet connection interfaces.

1. Navigate to **Menu** (☰) **> Device Management**.

   The **Device Management** screen will appear.

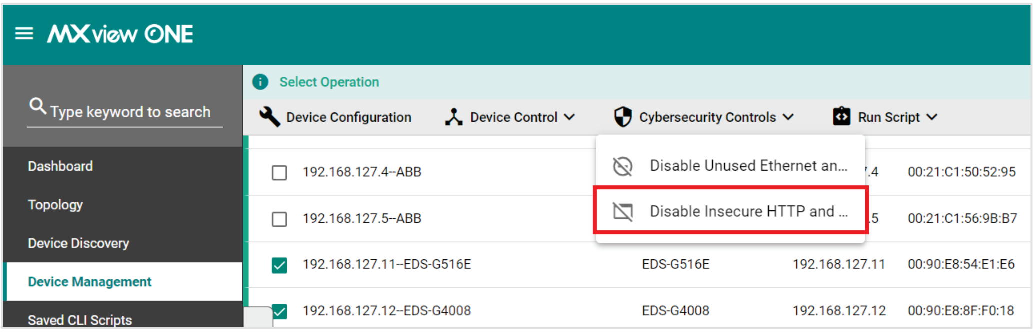
2. Selected the device(s) to configure from the device list.



☐	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
☐	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2022_1007_1814	
☐	192.168.127.1--ICMP Device	ICMP Device	192.168.127.1	00:90:E8:91:86:64		
☑	192.168.127.11--EDS-G516E	EDS-G516E	192.168.127.11	00:90:E8:54:E1:E6	V6.3 build 23032200	Test
☑	192.168.127.12--EDS-G4008	EDS-G4008	192.168.127.12	00:90:E8:8F:F0:18	v3.1 Build 2023_0217_1005	aa
☐	192.168.127.13--EDS-408A	EDS-408A	192.168.127.13	00:90:E8:89:F8:C2	V3.12 build 22101114	Switch Location
☐	192.168.127.14--EDS-G512E-8PoE	EDS-G512E-8PoE	192.168.127.14	00:90:E8:4D:A7:32	V6.2 build 20080519	Switch Location
☐	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	192.168.127.16	00:90:E8:90:A5:6E	v3.2 Build 2023_0719_1007	
☐	192.168.127.25--PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913	Switch Location

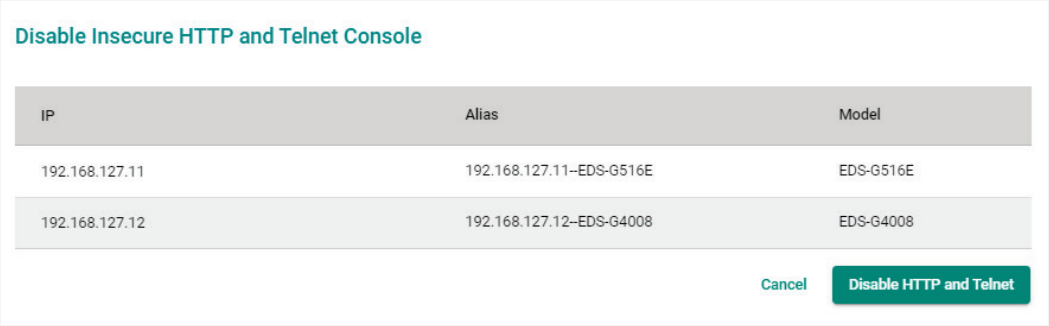
3. From the **Cybersecurity Controls** drop-down list, select **Disable Insecure HTTP and Telnet Console**.

The **Disable Insecure HTTP and Telnet Console** screen will appear.



☐	192.168.127.4--ABB		.4	00:21:C1:50:52:95
☐	192.168.127.5--ABB		5	00:21:C1:56:9B:B7
☑	192.168.127.11--EDS-G516E	EDS-G516E	192.168.127.11	00:90:E8:54:E1:E6
☑	192.168.127.12--EDS-G4008	EDS-G4008	192.168.127.12	00:90:E8:8F:F0:18

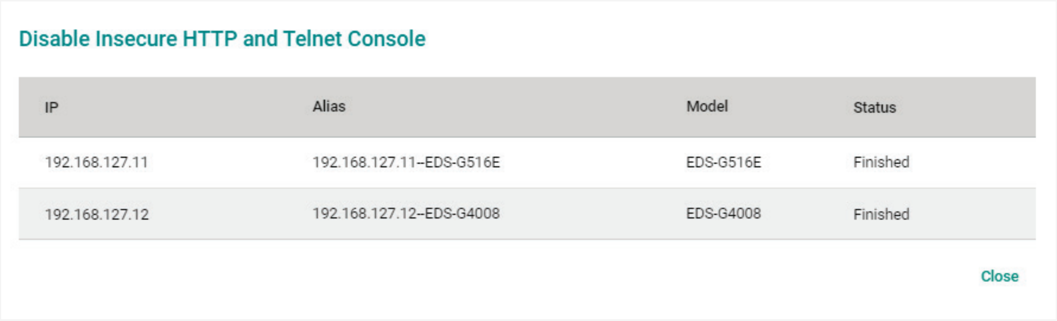
4. Click **Disable HTTP and Telnet**. The system will execute the action.



Disable Insecure HTTP and Telnet Console

IP	Alias	Model
192.168.127.11	192.168.127.11--EDS-G516E	EDS-G516E
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008

If successful, a confirmation will be shown in the Status column.



Disable Insecure HTTP and Telnet Console

IP	Alias	Model	Status
192.168.127.11	192.168.127.11--EDS-G516E	EDS-G516E	Finished
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008	Finished

If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.

Run Script

Refer to the Managing and Running Scripts section.

12. Saved CLI Scripts

The CLI Scripts function allows users to generate and execute CLI scripts from within MXview One. This function allows users to quickly execute batch configurations on multiple devices at once.

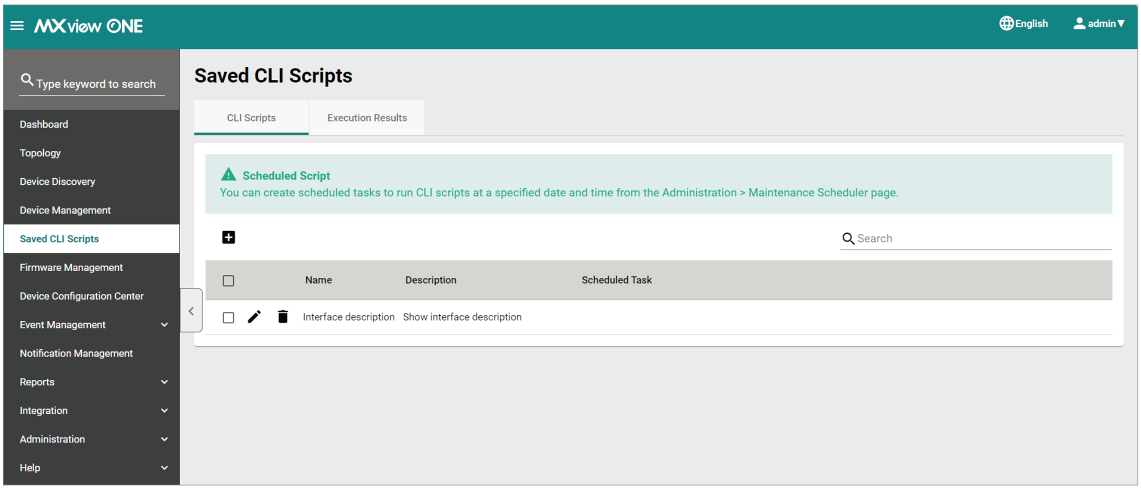
Saved CLI Scripts Overview

To access the **Saved CLI Scripts**, in the function tree, navigate to **Saved CLI Scripts**.

If there are no saved CLI scripts, a script will need to be created by clicking the Add (⊞) icon. Refer to **Adding a CLI Script** for information on how to create a script.

If there are saved CLI scripts, the following tabs will be available:

- **CLI Scripts**: This list shows all saved CLI scripts. From this table, you can create, edit, or delete CLI scripts.
- **Execution Results**: From this tab, you can download or delete the execution results of previously executed scripts.



Saved CLI Scripts

Scheduled Script
You can create scheduled tasks to run CLI scripts at a specified date and time from the Administration > Maintenance Scheduler page.

□		Name	Description	Scheduled Task
□		Interface description	Show interface description	

CLI Scripts

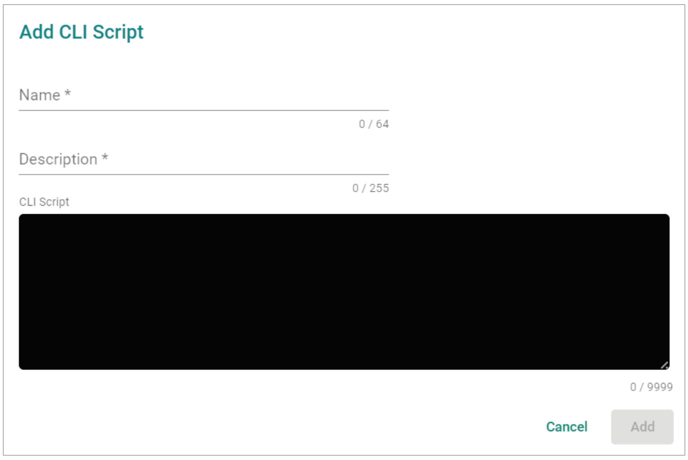
Adding a CLI Script

1. Navigate to **Menu** (☰) **> Saved CLI Scripts > CLI Scripts**.

   The **Saved CLI Scripts** screen will appear. A list of configured CLI scripts will show in the **CLI Scripts** list (if any).

2. Click the **Add** (⊞) icon.

   The **Add CLI Script** screen will appear.



Add CLI Script

Name *

0 / 64

Description *

0 / 255

CLI Script

0 / 9999

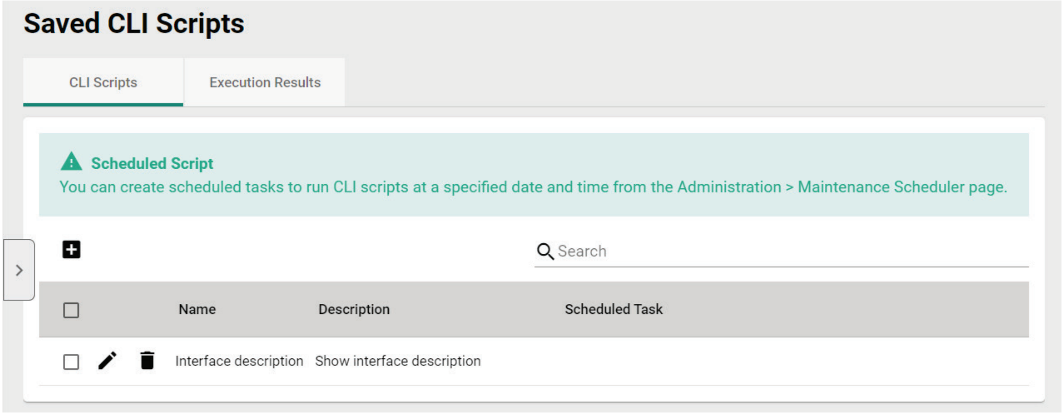
3. Configure the following settings:

   a. **Name**: Enter a name for the CLI script.

   b. **Description**: Enter a description for the CLI script.

   c. **CLI Script**: Enter the CLI command(s) to execute.

4. Click **Add**.
   The CLI script will be added to the table.



Saved CLI Scripts

Scheduled Script
You can create scheduled tasks to run CLI scripts at a specified date and time from the Administration > Maintenance Scheduler page.

□	Name	Description	Scheduled Task
□ ✎ 🗑	Interface description	Show interface description	

Searching for a CLI Script

1. Navigate to **Menu** (☰) **> Saved CLI Scripts > CLI Scripts**.

   The **Saved CLI Scripts** screen will appear. A list of configured CLI scripts will show in the **CLI Scripts** list (if any).

2. In the **Search** (🔍) field, type the full or partial information of the CLI script.
   All CLI scripts matching the entered string will be shown in the table.

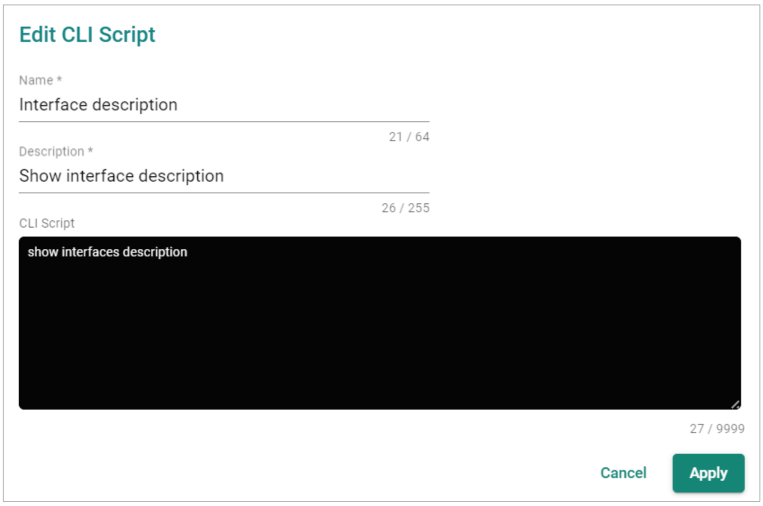
Editing a CLI Script

1. Navigate to **Menu** (☰) **> Saved CLI Scripts > CLI Scripts**.

   The **Saved CLI Scripts** screen will appear. A list of configured CLI scripts will show in the **CLI Scripts** list (if any).

2. Click the **Edit** (✎) icon next to the script you want to edit.

   The **Edit CLI Script** screen will appear.



Edit CLI Script

Name *
Interface description
21 / 64

Description *
Show interface description
26 / 255

CLI Script
```
show interfaces description
```
27 / 9999

3. Configure the following settings:
   a. **Name**: Enter a name for the CLI script.
   b. **Description**: Enter a description for the CLI script.
   c. **CLI Script**: Enter the CLI command(s) to execute.
4. Click **Apply**.
   A confirmation will appear to verify the CLI script was updated.

CLI script updated successfully

Deleting a CLI Script

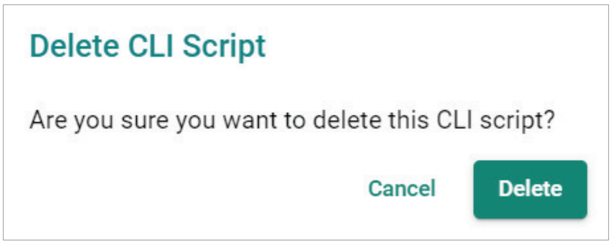
NOTE

A CLI script cannot be deleted if it is linked to a scheduled task. To delete the script, modify or delete the scheduled task first on the **Administration> Maintenance Scheduler** page.

1. Navigate to **Menu** (≡) **> Saved CLI Scripts > CLI Scripts**.

   The **Saved CLI Scripts** screen will appear. A list of configured CLI scripts will show in the **CLI Scripts** list (if any).

2. Click the **Delete** (🗑) icon next to the CLI script you want to delete.
   A confirmation window will appear.



Delete CLI Script

Are you sure you want to delete this CLI script?

3. Click **Delete**.
   A confirmation will appear to verify the CLI script was deleted.

CLI script deleted successfully

Deleting Multiple CLI Scripts

NOTE

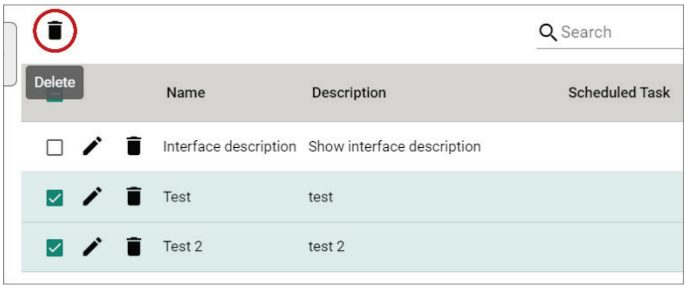
A CLI script cannot be deleted if it is linked to a scheduled task. To delete the script, modify or delete the scheduled task first on the **Administration> Maintenance Scheduler** page.

1. Navigate to **Menu** (≡) **> Saved CLI Scripts > CLI Scripts**.

   The **Saved CLI Scripts** screen will appear. A list of configured CLI scripts will show in the **CLI Scripts** list (if any).

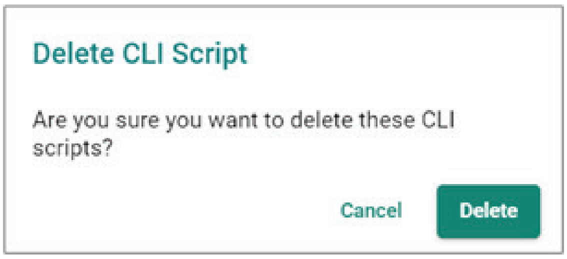
2. Select the checkbox of the scripts you want to delete in the list.

3. Click the **Delete** (🗑) icon at the top of the page.



	Name	Description	Scheduled Task
☐ ✎ 🗑	Interface description	Show interface description	
☑ ✎ 🗑	Test	test	
☑ ✎ 🗑	Test 2	test 2	

4. A confirmation window will appear.



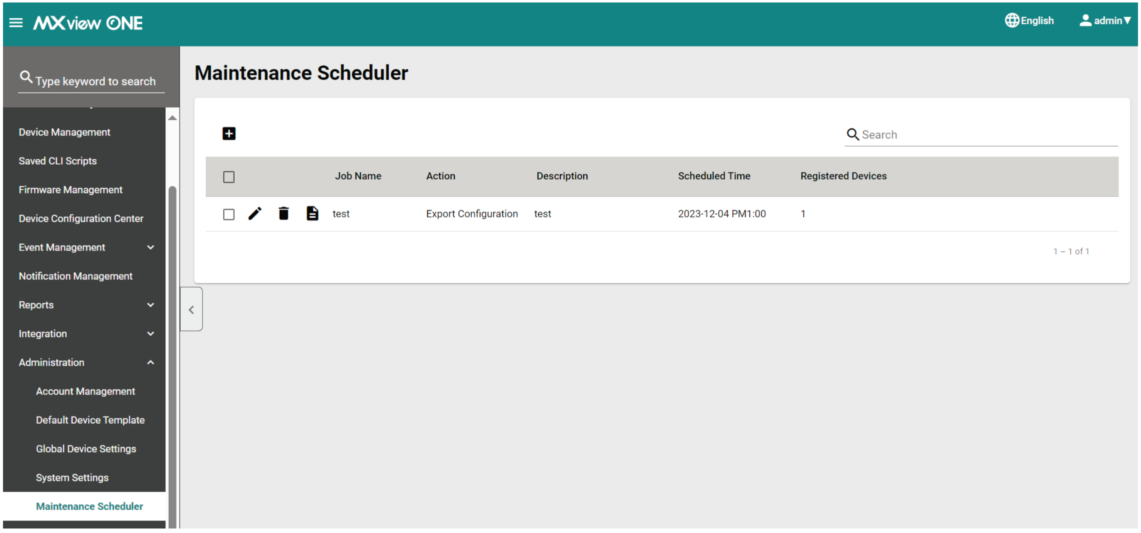
Delete CLI Script

Are you sure you want to delete these CLI scripts?

5. Click **Delete**.
   A confirmation will appear to verify the CLI script was deleted.

Creating a CLI Script Scheduled Task

1. Navigate to **Menu** (☰) **> Administration > Maintenance Scheduler**.
   The **Maintenance Scheduler** screen will appear.

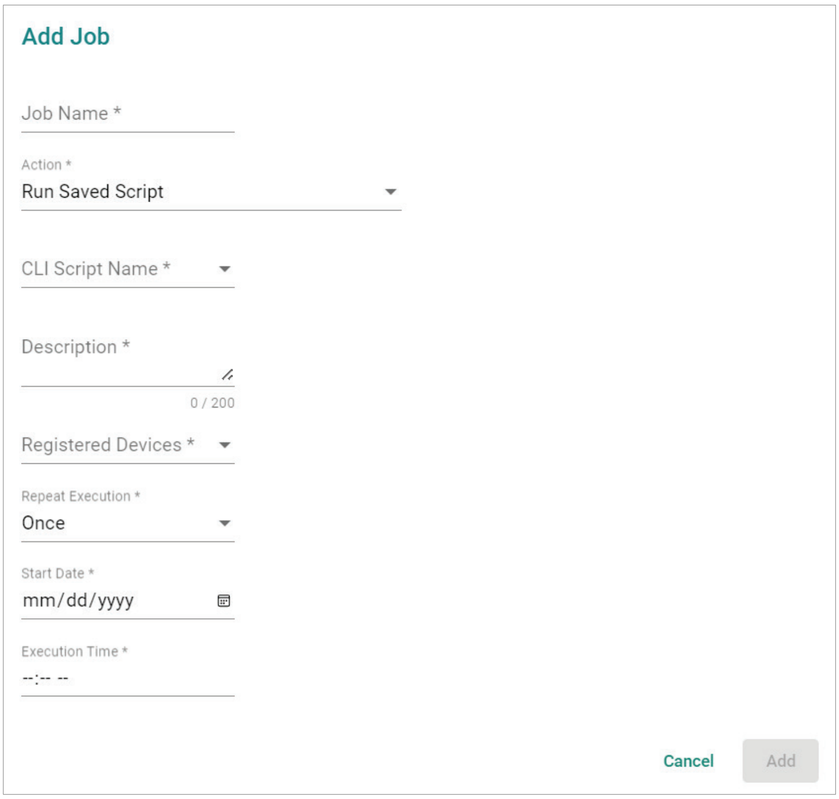


Maintenance Scheduler

□	Job Name	Action	Description	Scheduled Time	Registered Devices
□	test	Export Configuration	test	2023-12-04 PM1:00	1

1 – 1 of 1

2. Click the **Add** (⊞) icon.
   The **Add Job** screen will appear.



Add Job

Job Name *

Action *
Run Saved Script

CLI Script Name *

Description *

0 / 200

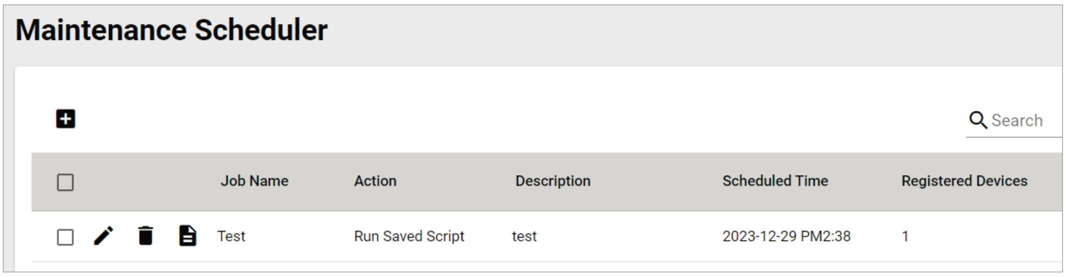
Registered Devices *

Repeat Execution *
Once

Start Date *
mm/dd/yyyy

Execution Time *
--:-- --

3. Configure the following settings:
   a. **Job Name**: Enter a name for the job.
   b. **Action**: Select **Run Saved Script** from the Action drop-down list.
   c. **CLI Script Name**: Select the CLI script that you want to execute.
   d. **Description**: Enter a description for the job.
   e. **Registered Devices**: Select the devices that you want to run the selected CLI script on.
   f. **Repeat Execution**: Select the job execution frequency: Once, Daily, Weekly, Monthly.
   g. **Start Date**: If you select **Once** in the Repeat Execution field, specify the start date to begin executing the scheduled job.
   h. **On**: If you select **Weekly** or **Monthly** in the Repeat Execution field, specify when to begin executing the scheduled job.
   i. **Execution Time**: Specify the time of day to run the scheduled job.
4. Click **Add**.
   MXview One will display the scheduled job in the Maintenance Scheduler table and will run the CLI script for the selected devices according to the defined schedule.



Maintenance Scheduler

□	Job Name	Action	Description	Scheduled Time	Registered Devices
□	Test	Run Saved Script	test	2023-12-29 PM2:38	1

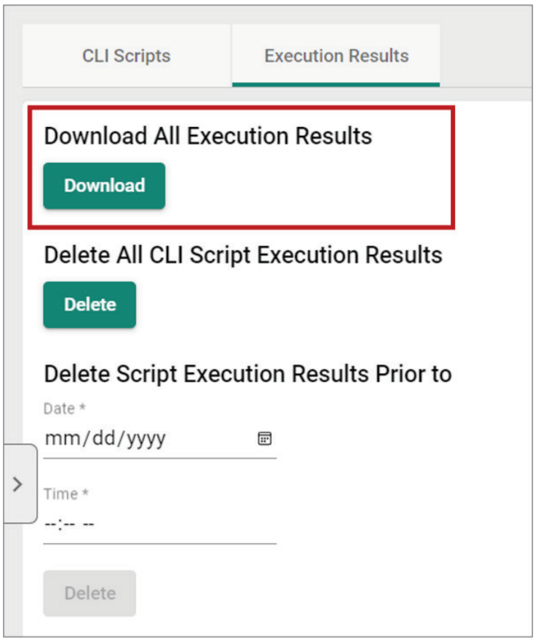
Execution Results

Download All Execution Results

1. Navigate to **Menu** (☰) **> Saved CLI Scripts**.

   The **Saved CLI Scripts** screen will appear.

2. Go to the **Execution Results** tab.


CLI Scripts
Execution Results
Download All Execution Results
Download
Delete All CLI Script Execution Results
Delete
Delete Script Execution Results Prior to
Date *
mm/dd/yyyy
Time *
--:-- --
Delete

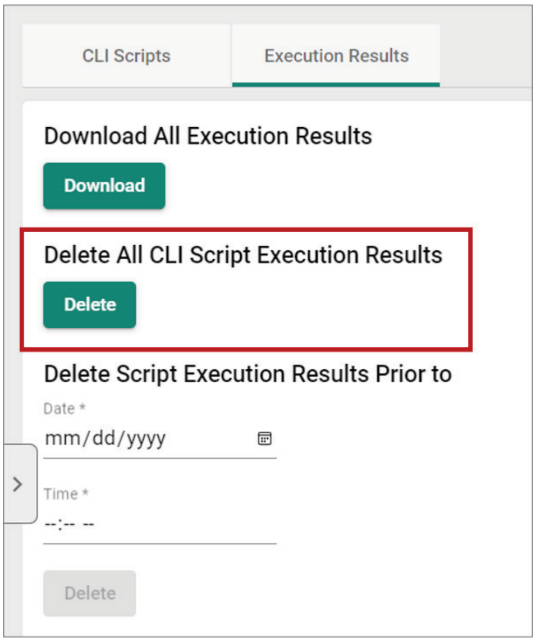
3. Click **Download**.
   MXview One will download all the CLI script execution results as a ZIP file.

Delete All Execution Results

1. Navigate to **Menu** (☰) **> Saved CLI Scripts**.

   The **Saved CLI Scripts** screen will appear.

2. Go to the **Execution Results** tab.



Download All Execution Results

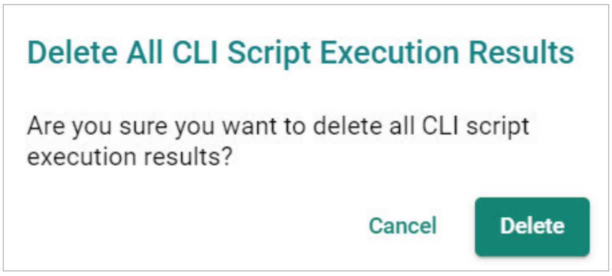
Delete All CLI Script Execution Results

Delete Script Execution Results Prior to

Date * mm/dd/yyyy

Time * --:-- --

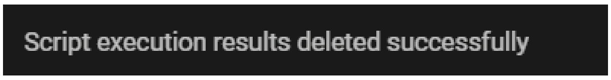
3. Click **Delete**.
   A confirmation window will appear.



Delete All CLI Script Execution Results

Are you sure you want to delete all CLI script execution results?

4. Click **Delete**.
   A confirmation will appear to verify all execution results have been deleted.



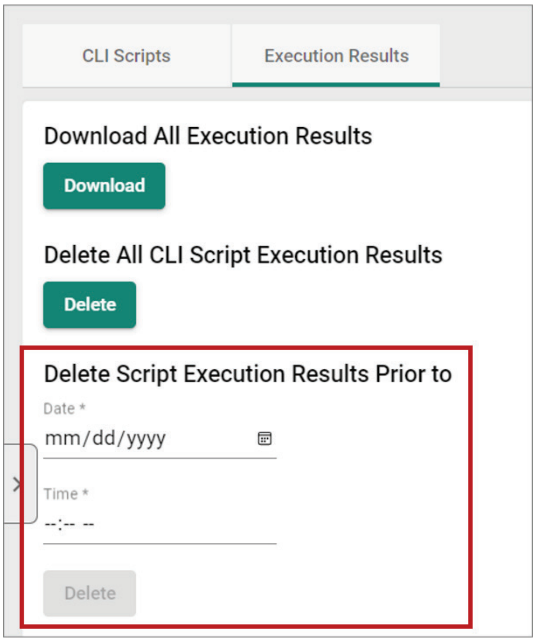
Script execution results deleted successfully

Delete Execution Results Prior to a Specified Time

1. Navigate to **Menu** (☰) **> Saved CLI Scripts**.

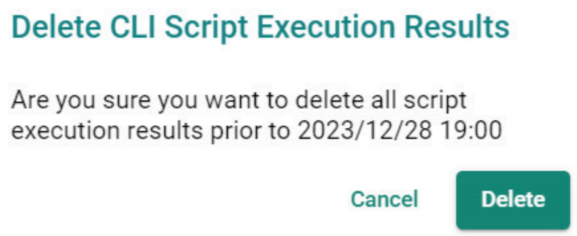
   The **Saved CLI Scripts** screen will appear.

2. Go to the **Execution Results** tab.


CLI Scripts
Execution Results
Download All Execution Results
Download
Delete All CLI Script Execution Results
Delete
Delete Script Execution Results Prior to
Date *
mm/dd/yyyy
Time *
--:-- --
Delete

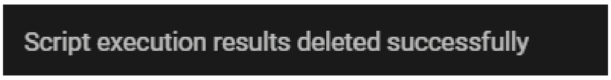
3. Specify the **Date** and **Time**. All execution results prior to this time will be deleted.

4. Click **Delete**.
   A confirmation window will appear.



Are you sure you want to delete all script execution results prior to 2023/12/28 19:00

5. Click **Delete**.
   A confirmation will appear to verify all execution results have been deleted.



Script execution results deleted successfully

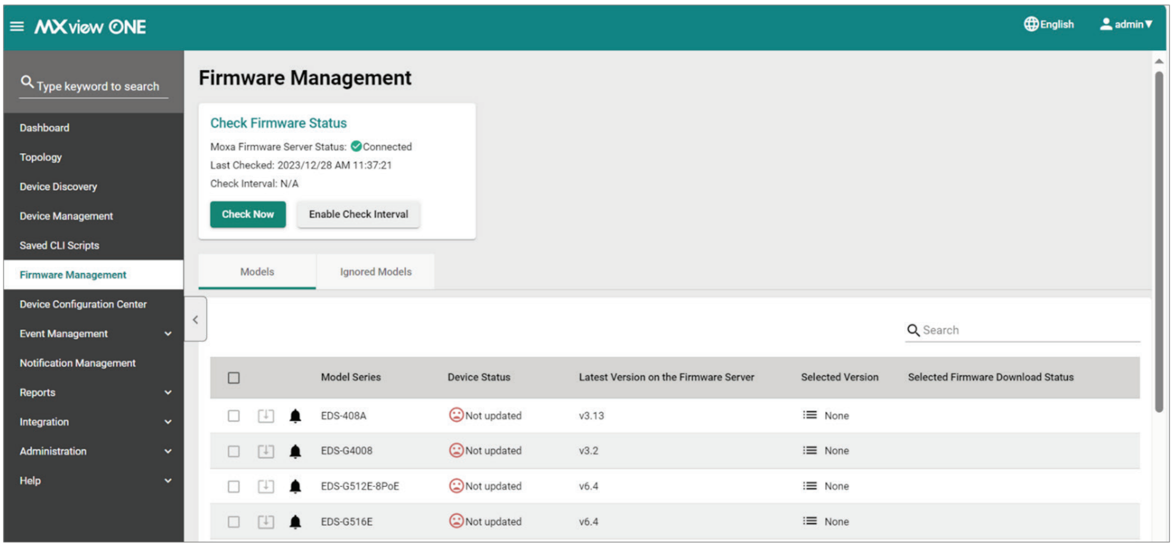
13. Firmware Management

MXview One features Moxa Firmware Server integration to check for the availability of the latest firmware for devices. From the Firmware Management section, users can review the release notes, download the firmware file, and perform firmware updates for multiple devices at once.

Firmware Management Overview

To access the Firmware Management page, in the function tree, navigate to **Menu** (☰) **> Firmware Management**.

On this page, users can find the **Check Firmware Status** function and a table of with the firmware information of all model series in the topology.



Firmware Management

Check Firmware Status

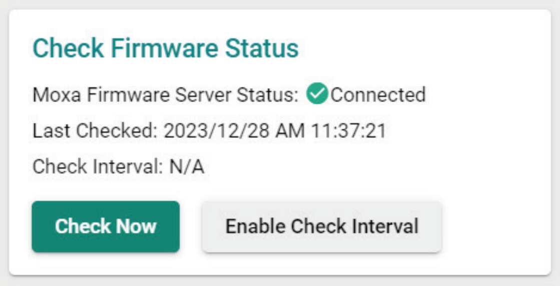
Moxa Firmware Server Status: ✓Connected

Last Checked: 2023/12/28 AM 11:37:21

Check Interval: N/A

□	Model Series	Device Status	Latest Version on the Firmware Server	Selected Version	Selected Firmware Download Status
□	EDS-408A	Not updated	v3.13	None	
□	EDS-G4008	Not updated	v3.2	None	
□	EDS-G512E-8PoE	Not updated	v6.4	None	
□	EDS-G516E	Not updated	v6.4	None	

Check Firmware Status



Check Firmware Status

Moxa Firmware Server Status: ✓Connected

Last Checked: 2023/12/28 AM 11:37:21

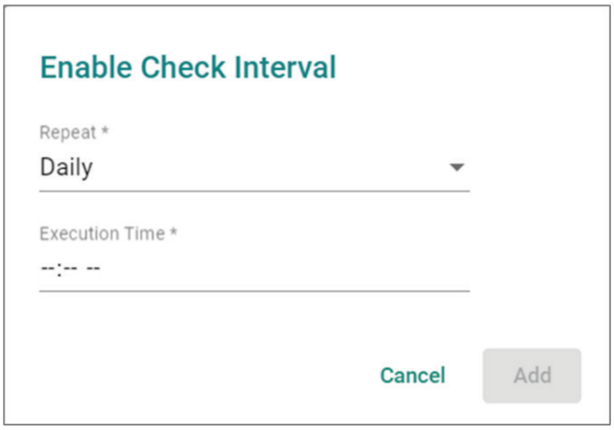
Check Interval: N/A

The **Check Firmware Status** section includes the following the information:

- **Moxa Firmware Server Status**: This indicates the status of the MXview One connection to the Moxa Firmware Server.
- **Last Checked**: This is the date and time MXview One last checked the firmware information on the Moxa Firmware Server.
- **Check Interval**: If Check Interval is enabled, this shows the interval at which MXview One will check for firmware information. If no interval is configured, this will show "N/A".

There are two ways for MXview One to check for the firmware information on the Moxa Firmware Server:

- **Check Now**: Click **Check Now** to immediately check for updated firmware information.
- **Enable Check Interval**: Specify a time and date interval at which MXview One will check for new firmware information.



Enable Check Interval

Repeat *
Daily

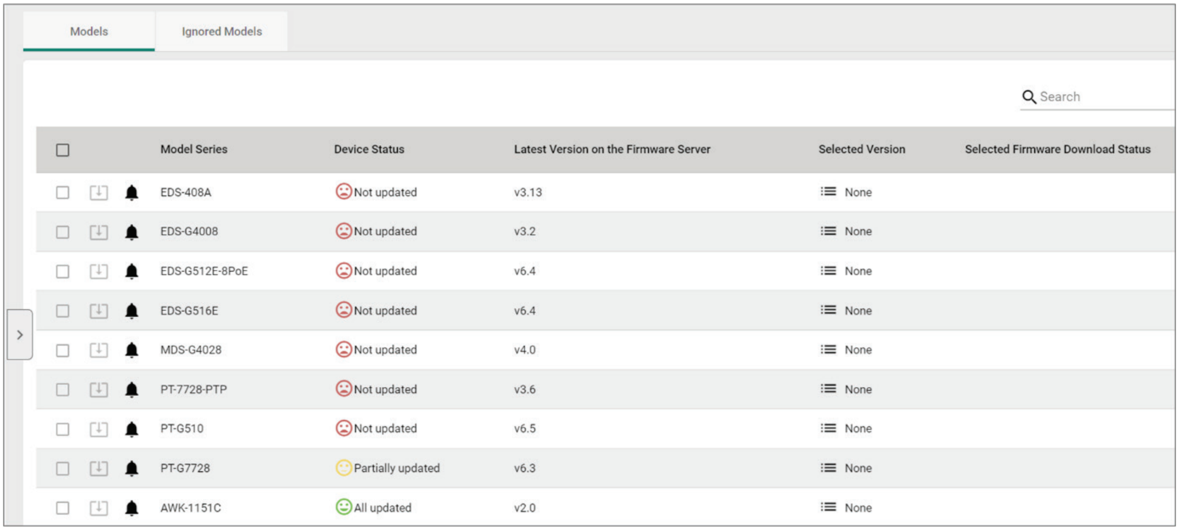
Execution Time *
--:-- --

Model Series Table Overview

The models table is divided into two separate tabs: **Models** and **Ignored Models**.

Models

The **Models** tab shows an overview of all the model series and their respective firmware information. All identical models will be shown by a single representative entry in this table.



□			Model Series	Device Status	Latest Version on the Firmware Server	Selected Version	Selected Firmware Download Status
□			EDS-408A	Not updated	v3.13	None	
□			EDS-G4008	Not updated	v3.2	None	
□			EDS-G512E-8PoE	Not updated	v6.4	None	
□			EDS-G516E	Not updated	v6.4	None	
□			MDS-G4028	Not updated	v4.0	None	
□			PT-7728-PTP	Not updated	v3.6	None	
□			PT-G510	Not updated	v6.5	None	
□			PT-G7728	Partially updated	v6.3	None	
□			AWK-1151C	All updated	v2.0	None	

This screen includes the following information:

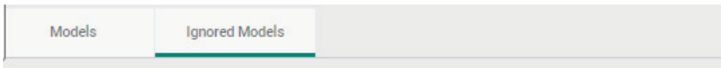
Itom	Description
Model Series	The model name. All identical models will be represented by a single entry. For example, if there are multiple EDS-408A devices, only one EDS-408A entry will appear in the table.
Device Status	The current firmware version status of the model series. The following statuses can be shown: • **All updated**: The firmware version of all models of this type is up to date. • **Partially updated**: The firmware version of some of the models of this type is not up to date. • **Not updated**: The firmware version of all models of this type is not up to date. • **No information available**: There is no firmware version information available on the firmware server for this model.
Latest Version on the Firmware Server	The latest firmware version of this model series on the Moxa firmware server.
Selected Version	Shows the currently selected firmware version and its release notes. Users can select a different firmware version. Refer to Selecting a Firmware Version.
Selected Firmware Download Status	After selecting a firmware version to download, this shows the firmware file download progress as a percentage.

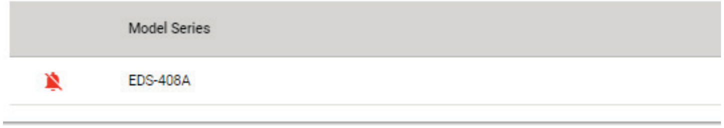
The following actions are available from this screen:

Icon	Name	Description
🔔	Disable new version notifications	Click this icon to prevent MXview One from checking for and sending notifications for new firmware versions for that model series. This will add the model series to the Ignored Models list. Refer to Ignored Models for more information.
⤓	Upgrade firmware	Click this icon to initiate a firmware upgrade. Refer to Upgrading Firmware.
☰	Select firmware version	Click this icon to select a different firmware version. Refer to Selecting a Firmware Version.
🛡	Security patch available	This icon indicates a new security patch is available for that model series.
🔕	Enable new version notifications	Click this icon to enable MXview One to check for and send notifications for new firmware versions for that model series.

Ignored Models

The Ignored Models lists all models for which MXview One is not checking for new firmware and is not sending notifications. To add a model series to the Ignored Models list, click the **bell** (🔔) icon on the Models tab next to the model series.



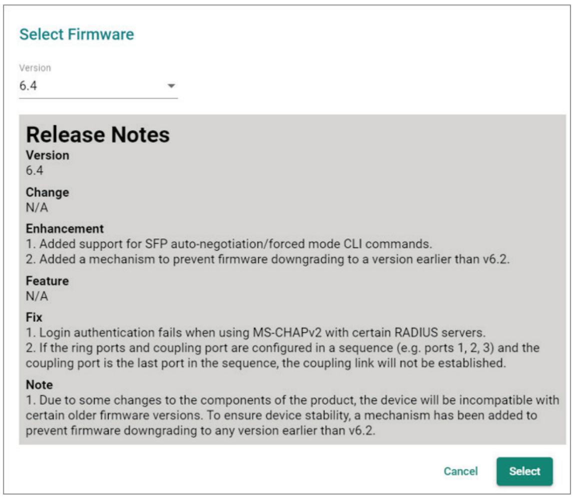


	Model Series
🔕	EDS-408A

Selecting a Firmware Version

Users can manually select a firmware version to upgrade to. When upgrading firmware, MXview One will apply the selected firmware to all similar models.

1. Navigate to **Menu** (☰) **> Firmware Management**.
2. Go to **Models** tab.
3. In the device list, click the **Select Firmware** (☰) icon of the corresponding model series in the Selected Version column.
   The **Select Firmware** window will appear.
4. Select a different firmware version from the Version drop-down menu. The release notes for the selected firmware version will appear in the section below.



Select Firmware

Version
6.4

Release Notes

Version
6.4

Change
N/A

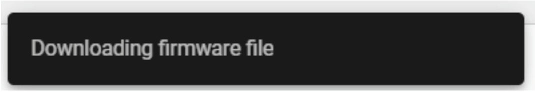
Enhancement
1. Added support for SFP auto-negotiation/forced mode CLI commands.
2. Added a mechanism to prevent firmware downgrading to a version earlier than v6.2.

Feature
N/A

Fix
1. Login authentication fails when using MS-CHAPv2 with certain RADIUS servers.
2. If the ring ports and coupling port are configured in a sequence (e.g. ports 1, 2, 3) and the coupling port is the last port in the sequence, the coupling link will not be established.

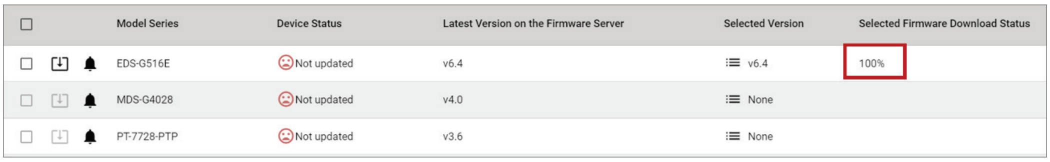
Note
1. Due to some changes to the components of the product, the device will be incompatible with certain older firmware versions. To ensure device stability, a mechanism has been added to prevent firmware downgrading to any version earlier than v6.2.

5. Click **Select**.
6. MXview One will begin download the selected firmware.



Downloading firmware file

7. The download progress will be shown in the Selected Firmware Download Status.

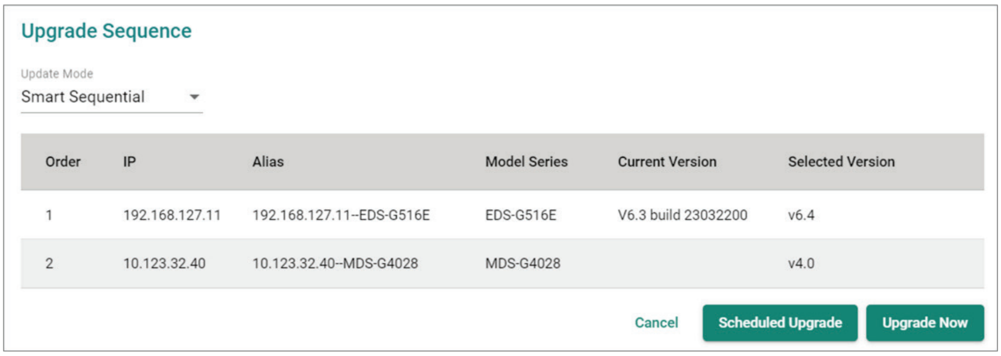


☐		Model Series	Device Status	Latest Version on the Firmware Server	Selected Version	Selected Firmware Download Status
☐		EDS-G516E	☹ Not updated	v6.4	☰ v6.4	100%
☐		MDS-G4028	☹ Not updated	v4.0	☰ None	
☐		PT-7728-PTP	☹ Not updated	v3.6	☰ None	

Upgrading Firmware

Once you have selected a firmware version and MXview One has finished downloading the firmware file, you can upgrade the firmware of the selected model series. To select and download a firmware version, refer to Selecting a Firmware Version.

1. Navigate to **Menu** (☰) **> Firmware Management**.
2. Go to the **Models** tab.
3. In the device list, select the model series to upgrade firmware for.
   You can select multiple model series.
4. Click the **Upgrade Firmware** (⇩) icon.
5. Configure the reboot sequence and execution time.



Upgrade Sequence

Update Mode: Smart Sequential

Order	IP	Alias	Model Series	Current Version	Selected Version
1	192.168.127.11	192.168.127.11--EDS-G516E	EDS-G516E	V6.3 build 23032200	v6.4
2	10.123.32.40	10.123.32.40--MDS-G4028	MDS-G4028		v4.0

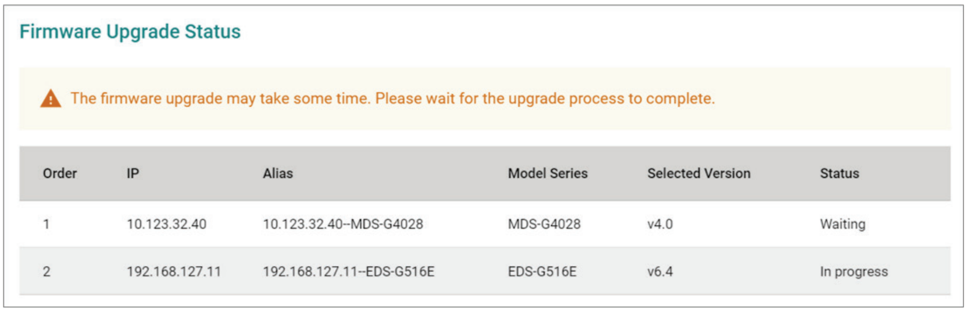
   a. Select the reboot sequence:
      - **Strict Sequential**: Upgrade the devices based on the device sequence in the topology starting from the device furthest away from the computer running MXview One, proceeding to the nearest one.
      - **Smart Sequential:** Upgrade the devices based on the device sequence in the topology but simultaneously upgrade all devices in the same topology layer.

NOTE

The computer running MXview One must be added to the topology in order for MXview One to determine the upgrade sequence. If the computer running MXview One is not added to the topology, you cannot select an update mode and MXview One will update the device firmware concurrently.

   b. Select an execution time:
      - **Upgrade Now**: Click **Upgrade Now** to upgrade the devices instantly.
      - **Scheduled Upgrade:** Click **Scheduled Upgrade** to create a new scheduled task. MXview One will upgrade the devices based on the specified time and date in the schedule.

6. To upgrade the devices instantly, click **Upgrade Now**. The system will execute the action.



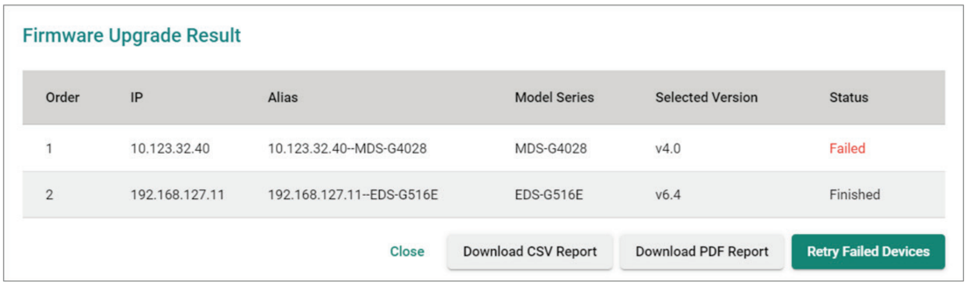
Firmware Upgrade Status

⚠ The firmware upgrade may take some time. Please wait for the upgrade process to complete.

Order	IP	Alias	Model Series	Selected Version	Status
1	10.123.32.40	10.123.32.40--MDS-G4028	MDS-G4028	v4.0	Waiting
2	192.168.127.11	192.168.127.11--EDS-G516E	EDS-G516E	v6.4	In progress

7. Click **Download CSV Report** or **Download PDF Report** to download a summary report of the firmware upgrade.

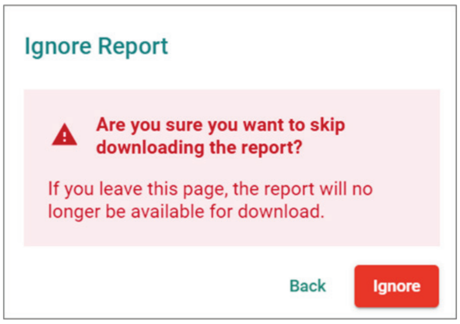
8. If the firmware upgrade was unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.



Firmware Upgrade Result

Order	IP	Alias	Model Series	Selected Version	Status
1	10.123.32.40	10.123.32.40--MDS-G4028	MDS-G4028	v4.0	Failed
2	192.168.127.11	192.168.127.11--EDS-G516E	EDS-G516E	v6.4	Finished

9. If you close this page without downloading the results report, a confirmation will appear. Clicking **Ignore** will delete the results report permanently.



Ignore Report

⚠ Are you sure you want to skip downloading the report?

If you leave this page, the report will no longer be available for download.

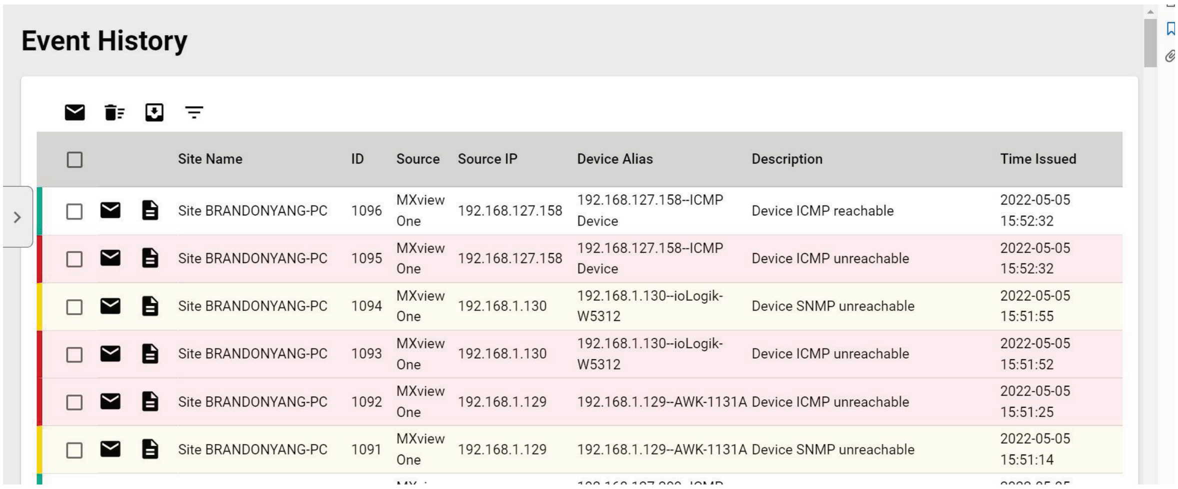
14. Events and Notifications

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.



Event History

□			Site Name	ID	Source	Source IP	Device Alias	Description	Time Issued
□	✉	🗎	Site BRANDONYANG-PC	1096	MXview One	192.168.127.158	192.168.127.158--ICMP Device	Device ICMP reachable	2022-05-05 15:52:32
□	✉	🗎	Site BRANDONYANG-PC	1095	MXview One	192.168.127.158	192.168.127.158--ICMP Device	Device ICMP unreachable	2022-05-05 15:52:32
□	✉	🗎	Site BRANDONYANG-PC	1094	MXview One	192.168.1.130	192.168.1.130--ioLogik-W5312	Device SNMP unreachable	2022-05-05 15:51:55
□	✉	🗎	Site BRANDONYANG-PC	1093	MXview One	192.168.1.130	192.168.1.130--ioLogik-W5312	Device ICMP unreachable	2022-05-05 15:51:52
□	✉	🗎	Site BRANDONYANG-PC	1092	MXview One	192.168.1.129	192.168.1.129--AWK-1131A	Device ICMP unreachable	2022-05-05 15:51:25
□	✉	🗎	Site BRANDONYANG-PC	1091	MXview One	192.168.1.129	192.168.1.129--AWK-1131A	Device SNMP unreachable	2022-05-05 15:51:14

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

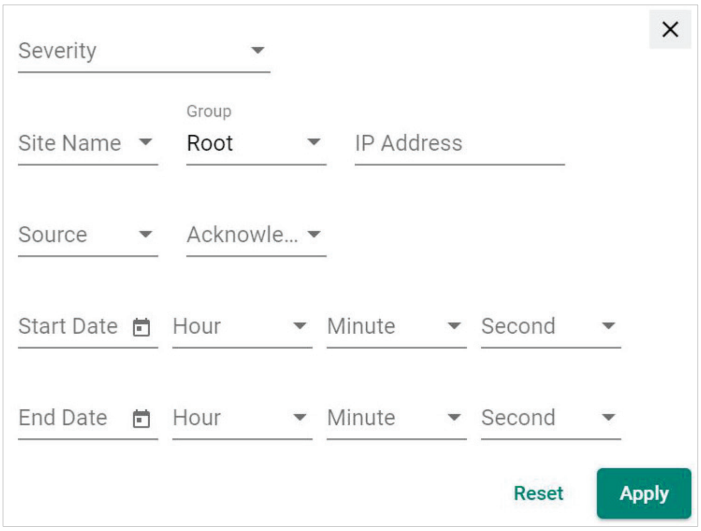
   The **Event History** screen will display the following information in a table format:

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**.

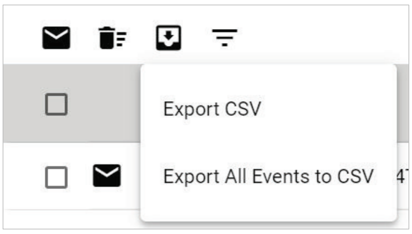
   MXview One filters the table to only display events that match the specified criteria.

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.

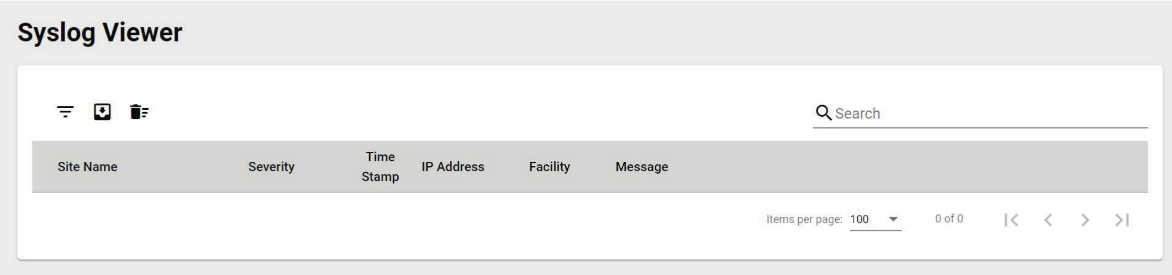


   b. Select **Export CSV** for just the events on the first page or **Export All Events to CSV** for all event pages.

   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.



Syslog Viewer

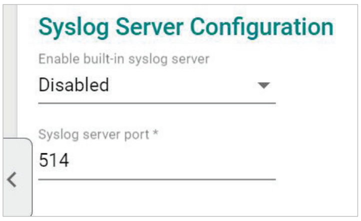
Site Name	Severity	Time Stamp	IP Address	Facility	Message

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.



Syslog Server Configuration

Enable built-in syslog server: Disabled

Syslog server port *: 514

   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**.

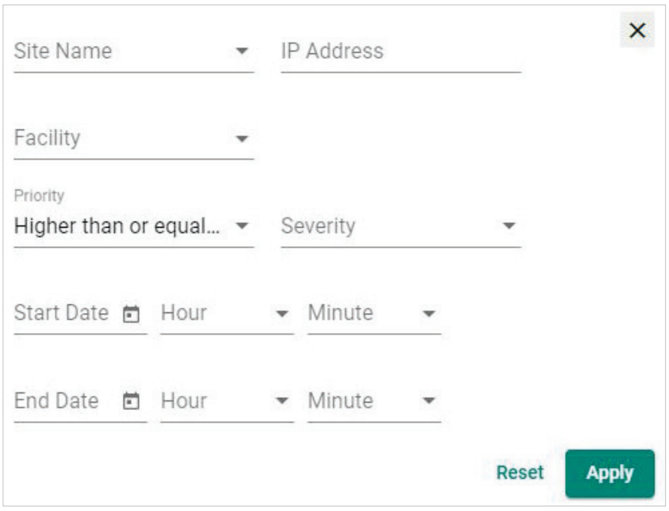
   The **Syslog Viewer** screen displays the following information in a table format:

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.



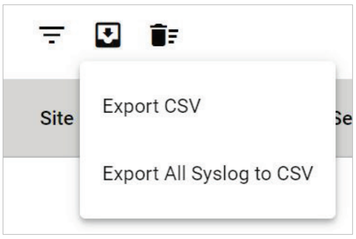
   b. Specify any of the following criteria:

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

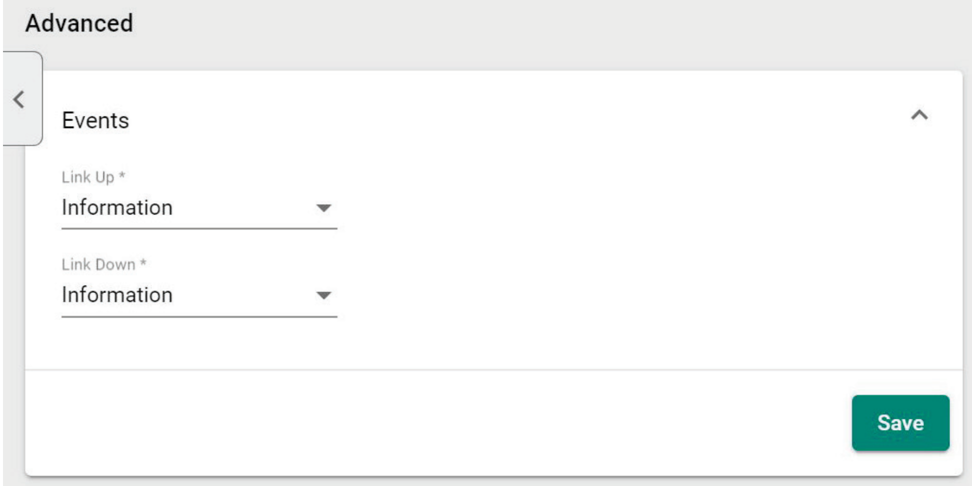
Use the **Preferences** and **Global Device Settings** screen to configure default event thresholds and severity levels.

1. Navigate to **Menu** (☰) **> Administration > Preferences**.

   The **Preferences** screen will appear.

2. In the **Advanced** section, expand **Events**.

   The **Events** settings will appear.



Advanced

Events

Link Up *: Information

Link Down *: Information

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**.

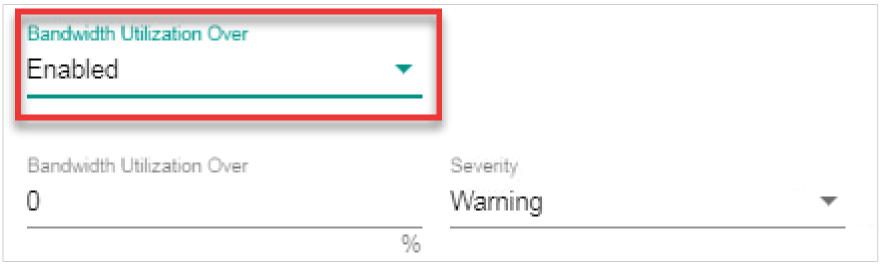
   The **Global Device Settings** screen will appear.

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.

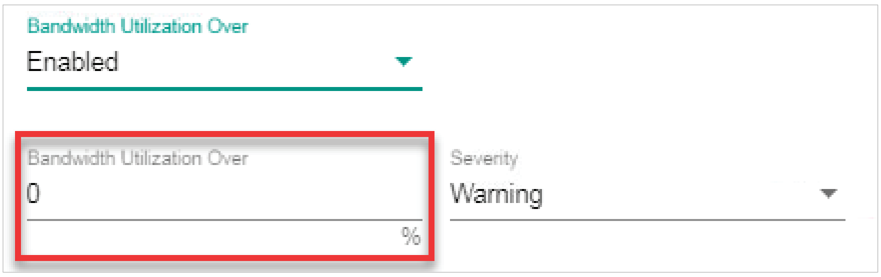


Bandwidth Utilization Over: Enabled

Bandwidth Utilization Over: 0 %

Severity: Warning

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



Bandwidth Utilization Over
Enabled

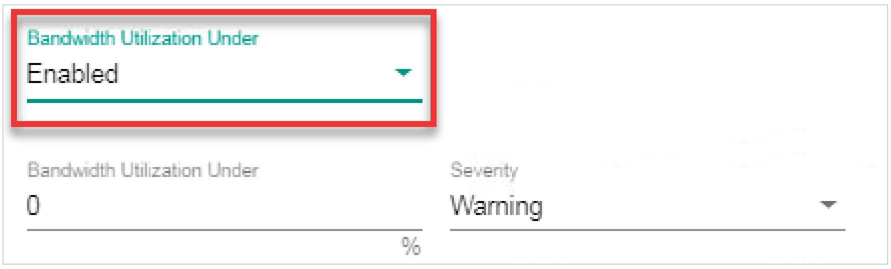
Bandwidth Utilization Over
0 %

Severity
Warning

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.

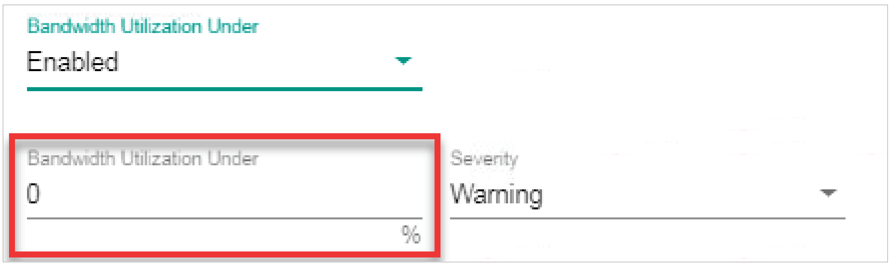


Bandwidth Utilization Under
Enabled

Bandwidth Utilization Under
0 %

Severity
Warning

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



Bandwidth Utilization Under
Enabled

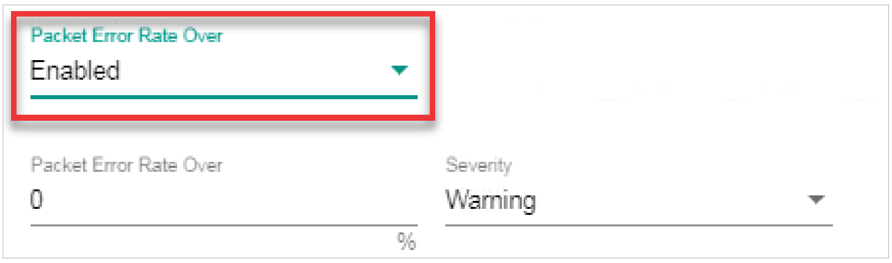
Bandwidth Utilization Under
0 %

Severity
Warning

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.

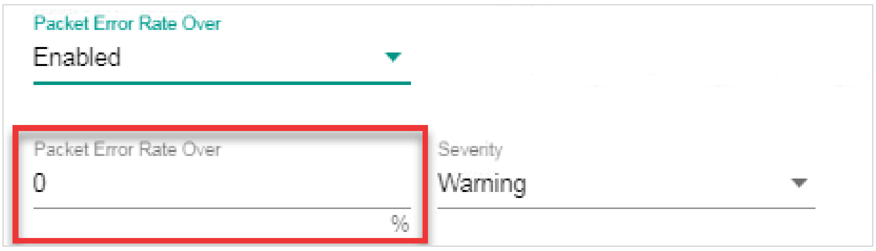


Packet Error Rate Over
Enabled

Packet Error Rate Over
0 %

Severity
Warning

b. Specify the packet error rate for the threshold.



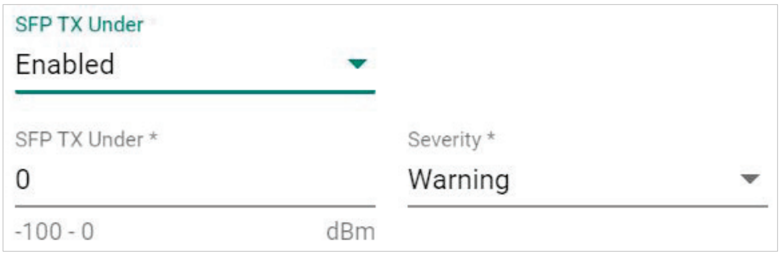
Packet Error Rate Over
Enabled

Packet Error Rate Over
0 %

Severity
Warning

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

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

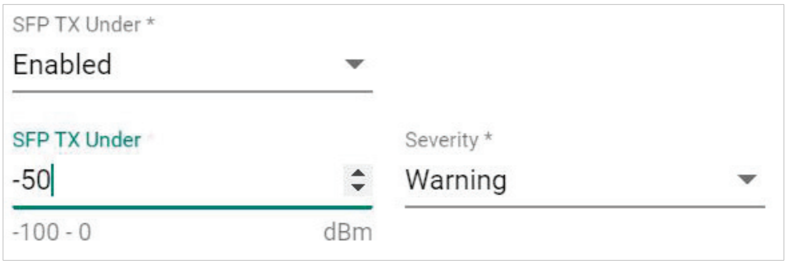


SFP TX Under
Enabled

SFP TX Under *
0
-100 - 0 dBm

Severity *
Warning

   b. Specify the SFP TX threshold level.

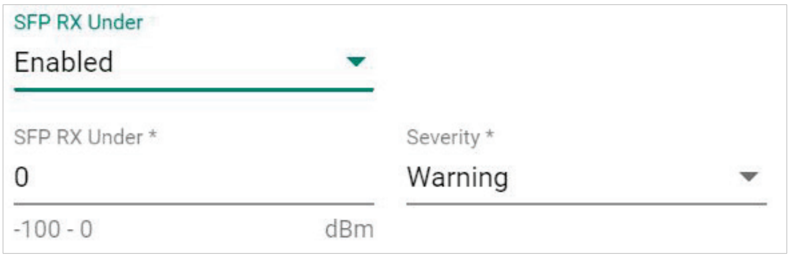


SFP TX Under *
Enabled

SFP TX Under
-50
-100 - 0 dBm

Severity *
Warning

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

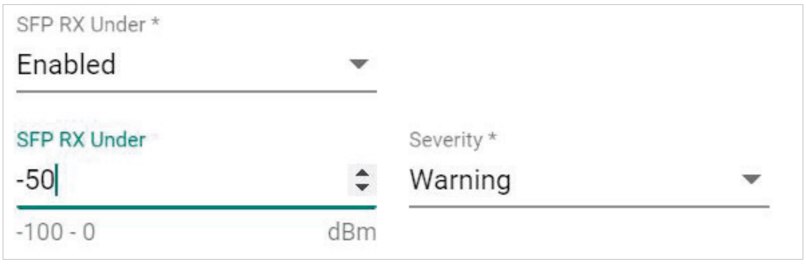


SFP RX Under
Enabled

SFP RX Under *
0
-100 - 0 dBm

Severity *
Warning

    b. Specify the SFP RX threshold level.

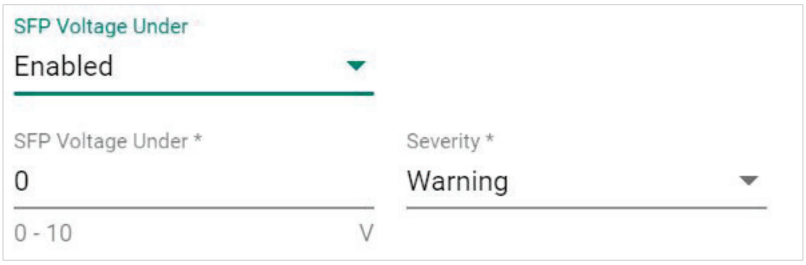


SFP RX Under *
Enabled

SFP RX Under
-50
-100 - 0 dBm

Severity *
Warning

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

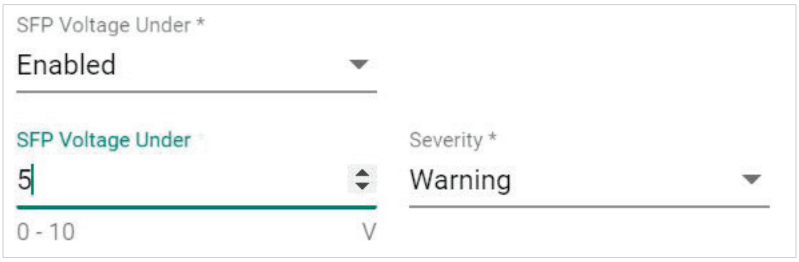


SFP Voltage Under
Enabled

SFP Voltage Under *
0
0 - 10 V

Severity *
Warning

b. Specify the SFP Voltage threshold level.

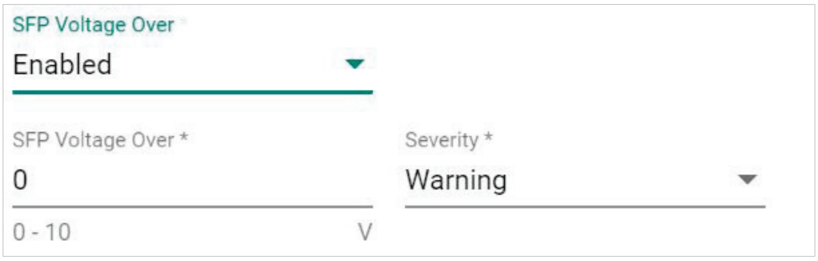

SFP Voltage Under *
Enabled

SFP Voltage Under
5
0 - 10 V

Severity *
Warning

12. To trigger events when the SFP voltage is over a certain threshold:

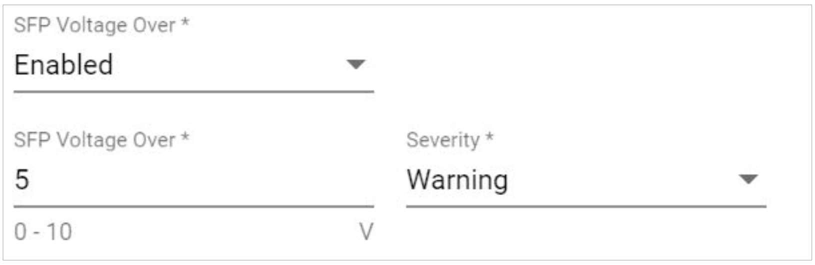
    a. Select **Enabled** from the first **SFP Voltage Over** drop-down list.


SFP Voltage Over
Enabled

SFP Voltage Over *
0
0 - 10 V

Severity *
Warning

    b. Specify the SFP Voltage threshold level.

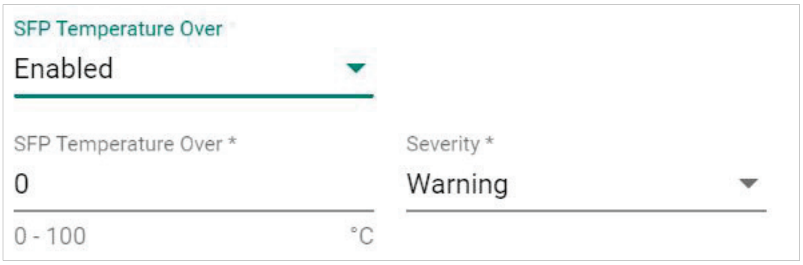

SFP Voltage Over *
Enabled

SFP Voltage Over *
5
0 - 10 V

Severity *
Warning

13. To trigger events when the SFP temperature is over a certain threshold:

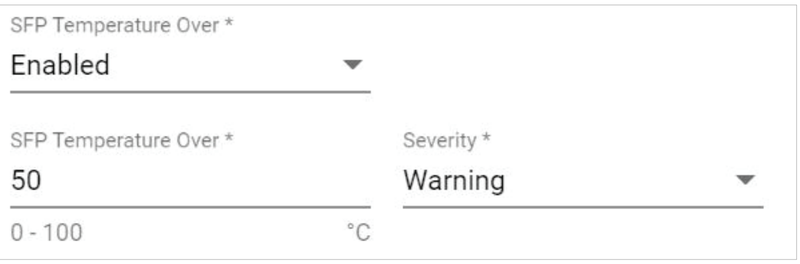
    a. Select **Enabled** from the first **SFP Temperature Over** drop-down list.


SFP Temperature Over
Enabled

SFP Temperature Over *
0
0 - 100 °C

Severity *
Warning

    b. Specify the SFP Temperature threshold level.


SFP Temperature Over *
Enabled

SFP Temperature Over *
50
0 - 100 °C

Severity *
Warning

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.

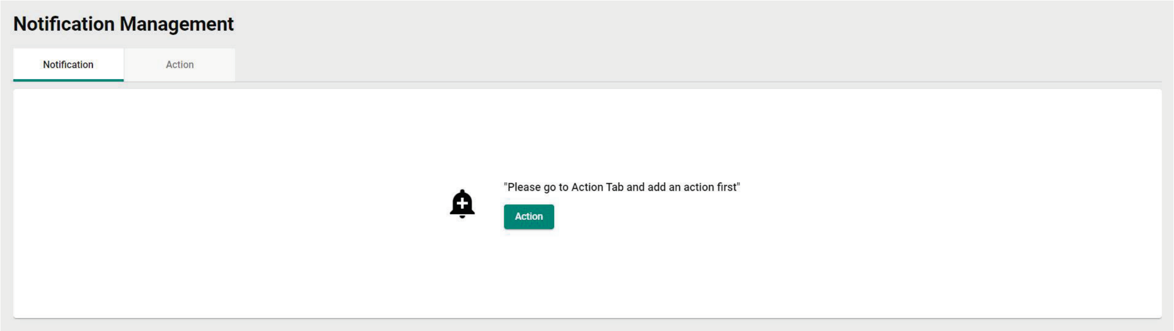
1. Navigate to **Menu** (☰) **> Administration > System Settings**.

   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.



Notification Management

"Please go to Action Tab and add an action first"

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.

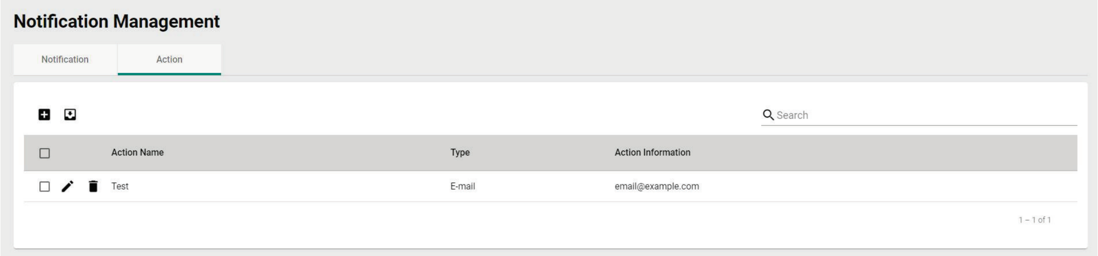
1. Navigate to **Menu** (☰) **> Notification Management**.

   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).



Notification Management

Notification | Action

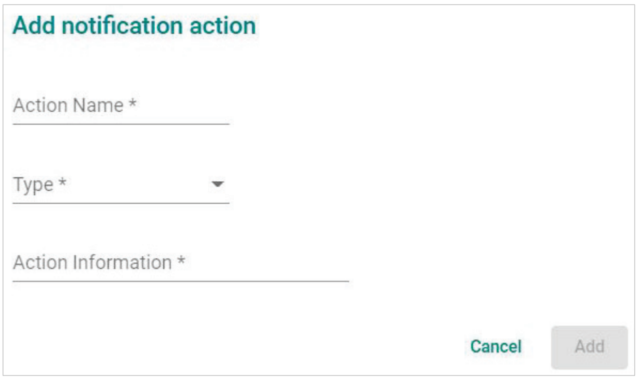
Search

□	Action Name	Type	Action Information
□	Test	E-mail	email@example.com

1 – 1 of 1

   b. Click the **Add** (⊞) icon in the top right corner.

   The **Add notification action** screen will appear.



Add notification action

Action Name *

Type *

Action Information *

   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).

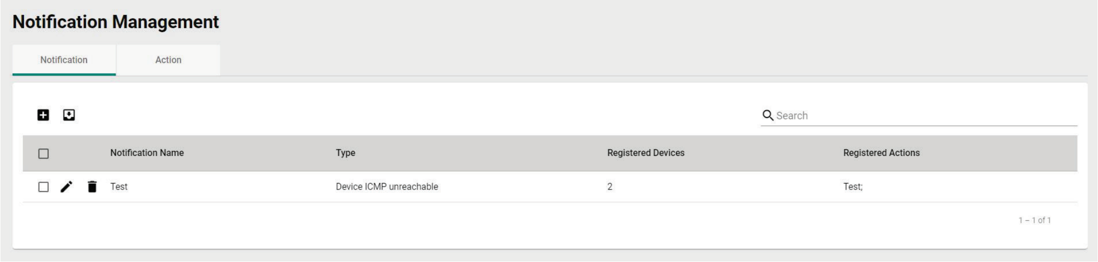
   f. Click **Add**.

   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).



Notification Management

Notification | Action

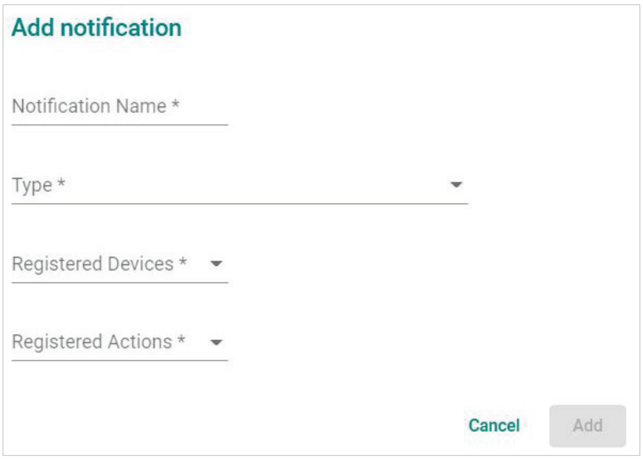
Search

□	Notification Name	Type	Registered Devices	Registered Actions
□	Test	Device ICMP unreachable	2	Test;

1 – 1 of 1

b. Click the **Add** (⊞) icon in the top right corner.

The **Add** notification screen appears.



Add notification

Notification Name *

Type *

Registered Devices *

Registered Actions *

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.

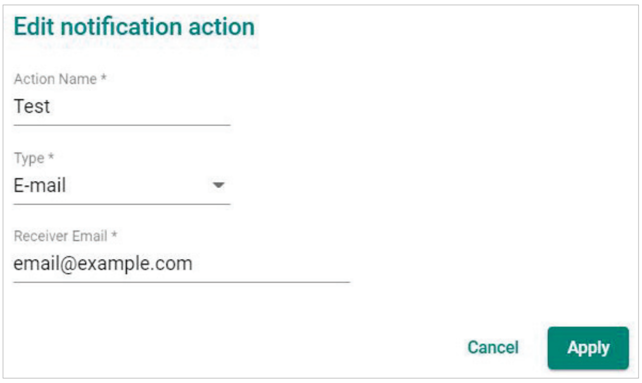
2. Click the **Action** tab.

   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.



Edit notification action

Action Name *
Test

Type *
E-mail

Receiver Email *
email@example.com

   b. Modify the following settings:

   ❒ Action Name

   ❒ Type

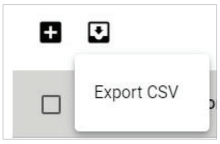
   ❒ Action information

   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.

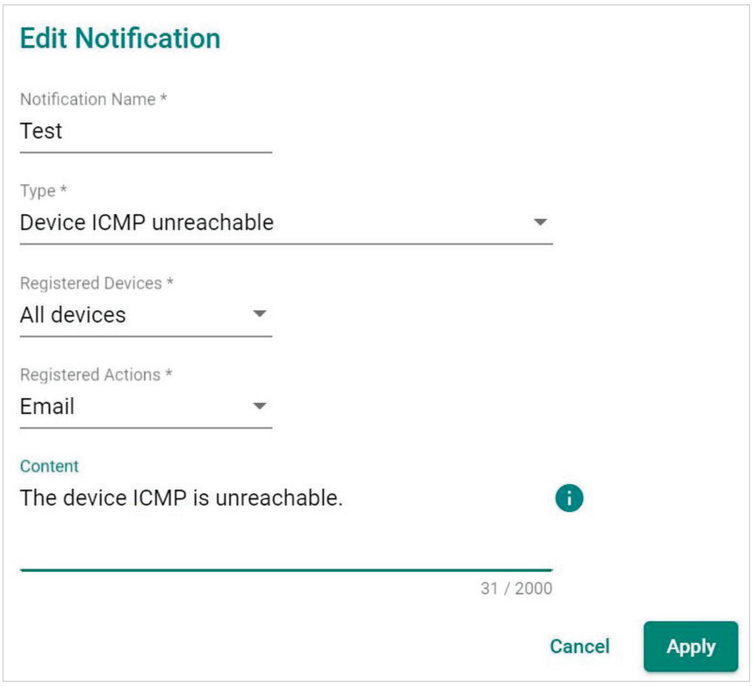
2. Click the **Notification** tab.

   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.



Edit Notification

Notification Name *
Test

Type *
Device ICMP unreachable

Registered Devices *
All devices

Registered Actions *
Email

Content
The device ICMP is unreachable.

31 / 2000

   b. Modify the following settings:

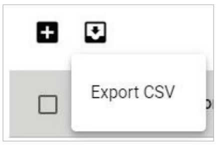
      - ❒ Notification Name
      - ❒ Type
      - ❒ Registered devices
      - ❒ Registered Actions

   c. Click **Apply**.

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

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

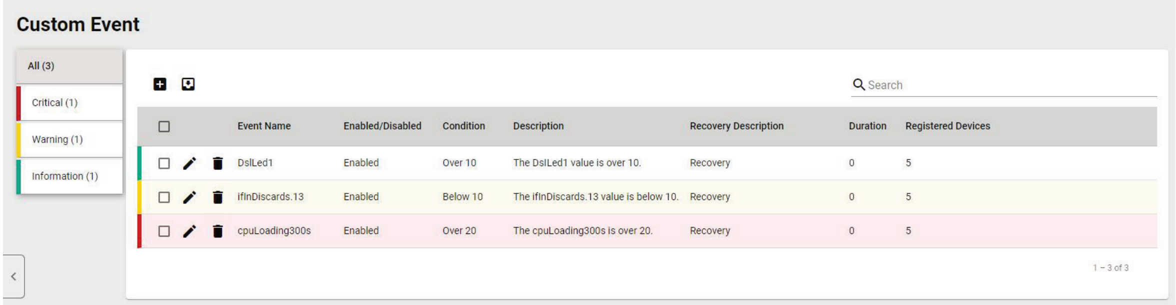
   a. Click the **Export** (⬇) icon.



   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.



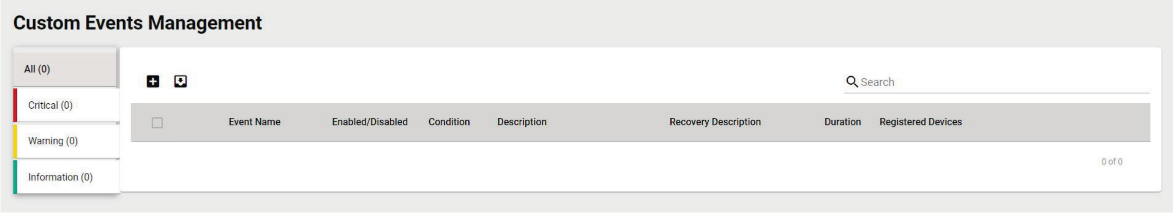
Custom Event

□	Event Name	Enabled/Disabled	Condition	Description	Recovery Description	Duration	Registered Devices
□	DslLed1	Enabled	Over 10	The DslLed1 value is over 10.	Recovery	0	5
□	ifInDiscards.13	Enabled	Below 10	The ifInDiscards.13 value is below 10.	Recovery	0	5
□	cpuLoading300s	Enabled	Over 20	The cpuLoading300s is over 20.	Recovery	0	5

1 – 3 of 3

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.



Custom Events Management

□	Event Name	Enabled/Disabled	Condition	Description	Recovery Description	Duration	Registered Devices

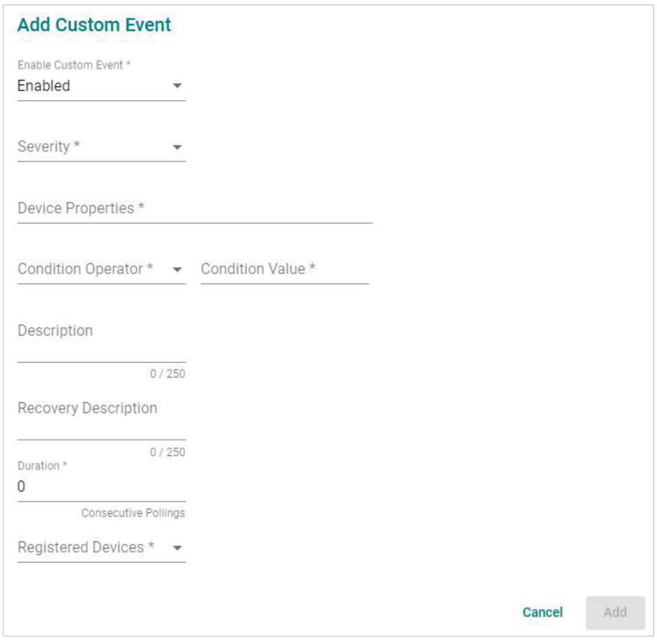
0 of 0

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.



Add Custom Event

Enable Custom Event *
Enabled

Duration *
0
Consecutive Pollings

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**.

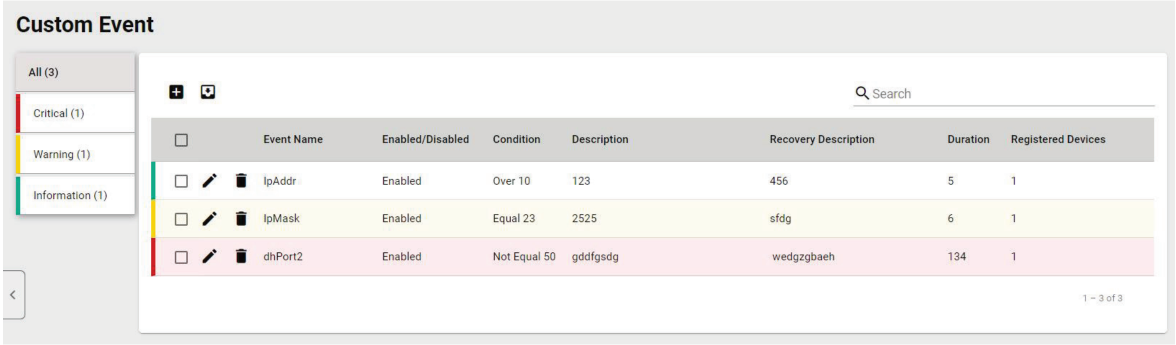
    The custom event appears in the **Custom Event** table.

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.



□	Event Name	Enabled/Disabled	Condition	Description	Recovery Description	Duration	Registered Devices
□	IpAddr	Enabled	Over 10	123	456	5	1
□	IpMask	Enabled	Equal 23	2525	sfdg	6	1
□	dhPort2	Enabled	Not Equal 50	gddfgsdg	wedgzgbaeh	134	1

1. Navigate to **Menu** (☰) **> Event Management > Custom Event**.

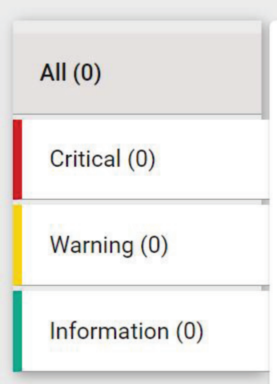
   The **Custom Event** screen will appear and displays the following information in a table format:

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.



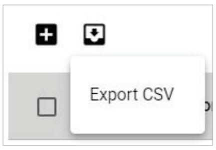
   MXview One filters the table to only display events that match the selected severity level.

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.

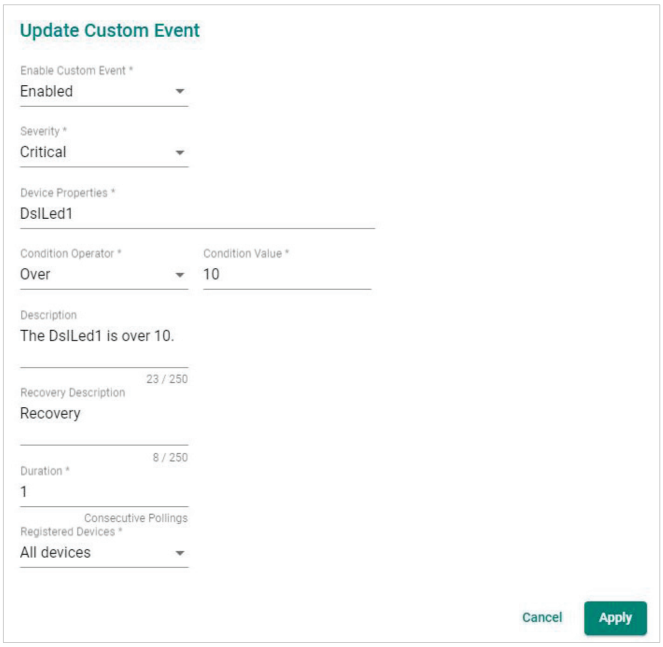


   b. Select **Export CSV.**
   MXview One exports the displayed event data as a CSV file.

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.



Update Custom Event

Enable Custom Event * Enabled

Severity * Critical

Device Properties * DslLed1

Condition Operator * Over

Condition Value * 10

Description The DslLed1 is over 10.

23 / 250

Recovery Description Recovery

8 / 250

Duration * 1

Consecutive Pollings

Registered Devices * All devices

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

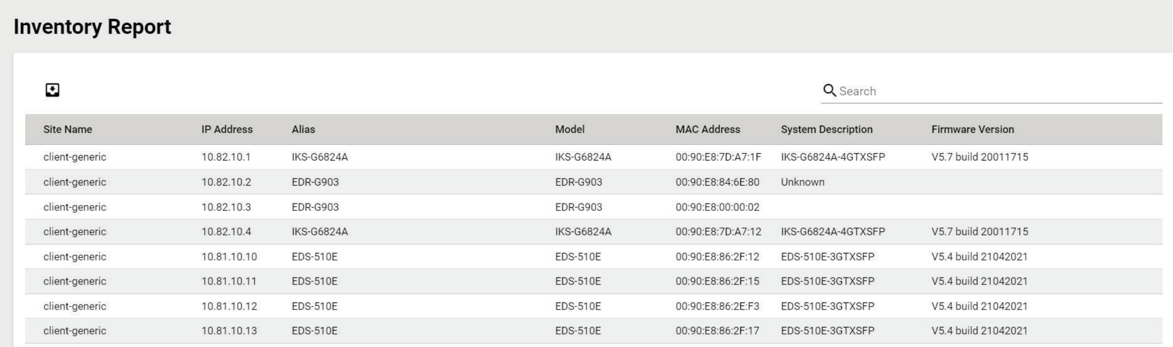
If the threshold is set as '0', the threshold function will be disabled.

15. 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.



Inventory Report

Search

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

1. Navigate to **Menu** (☰) **> Reports > Inventory Report**.

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

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

16. Backups, Restores, and Compares

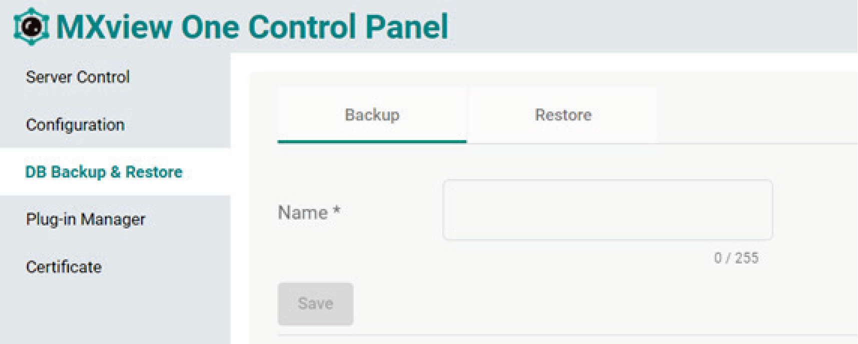
The MXview One web console provides several features to assist database backups and device configuration migrations. MXview One allows you to back up or restore configurations for multiple devices, and also compare changes between different versions of archived configuration files. You can also create scheduled jobs to automatically export/import device configurations or back up the MXview One database.

Backing Up the MXview One Database

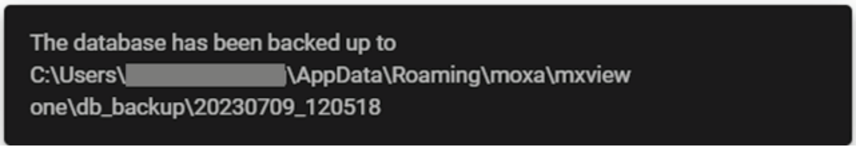
Use the **DB Backup & Restore** screen on the **Control Panel** to back up the MXview One database.

1. Navigate to **DB Backup & Restore** on the MXview One Control Panel.

   The Database Backup & Restore screen appears.

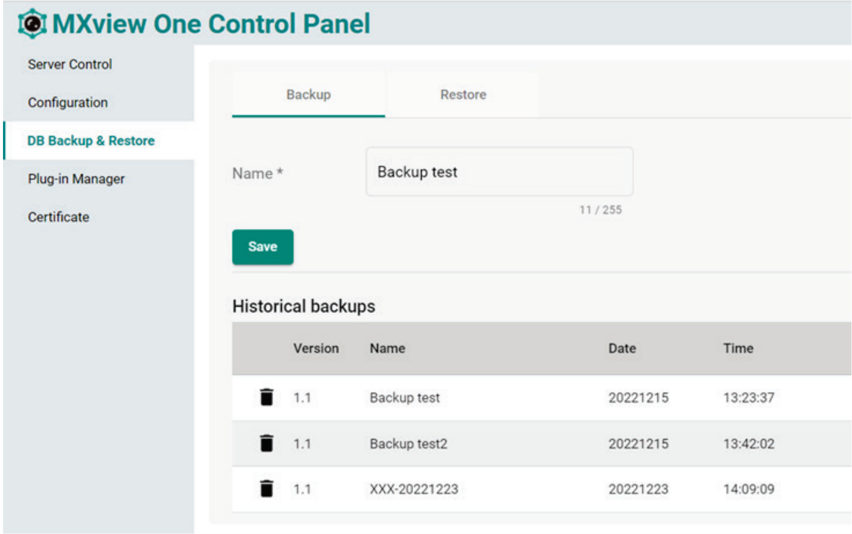


2. Choose the **Backup** tab to start the process of backing up the database.
3. In the **Name** field, specify the backup file name.
4. Click **Save**.
5. The message that the file of the backup database has been stored in the specified directory will be displayed.



The database has been backed up to C:\Users\[redacted]\AppData\Roaming\moxa\mxview one\db_backup\20230709_120518

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



Name * Backup test

Historical backups

	Version	Name	Date	Time
🗑	1.1	Backup test	20221215	13:23:37
🗑	1.1	Backup test2	20221215	13:42:02
🗑	1.1	XXX-20221223	20221223	14:09:09

Backing Up Device Configurations

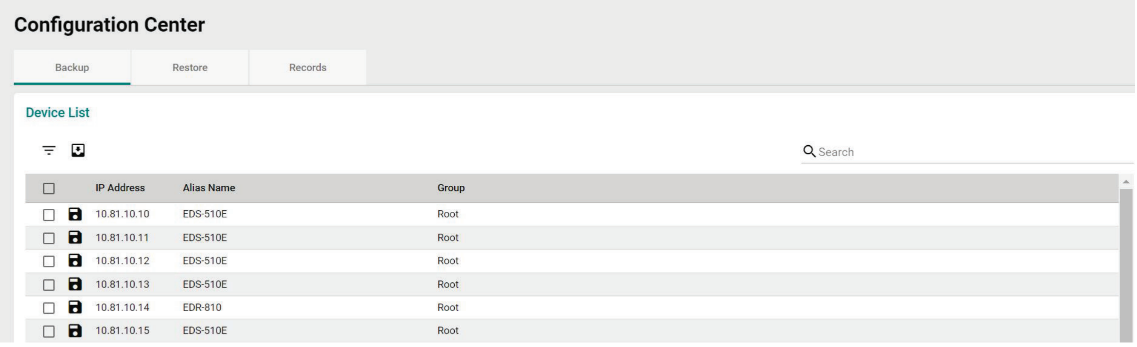
Use the **Device Configuration Center** screen to export configuration backup files from one or more devices.

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**.



Configuration Center

Device List

□	IP Address	Alias Name	Group
□	10.81.10.10	EDS-510E	Root
□	10.81.10.11	EDS-510E	Root
□	10.81.10.12	EDS-510E	Root
□	10.81.10.13	EDS-510E	Root
□	10.81.10.14	EDR-810	Root
□	10.81.10.15	EDS-510E	Root

3. (Optional) Filter the devices in the **Device List**:

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

   b. Specify any of the following criteria:

      ❒ **Group:** The group in the MXview One tree structure that the device is assigned to

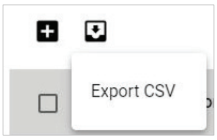
      ❒ **IP Address:** The IP address of the device

   c. Click **Apply**.

      MXview One filters the **Device List** according to the specified criteria.

4. To export the device list from all available devices:

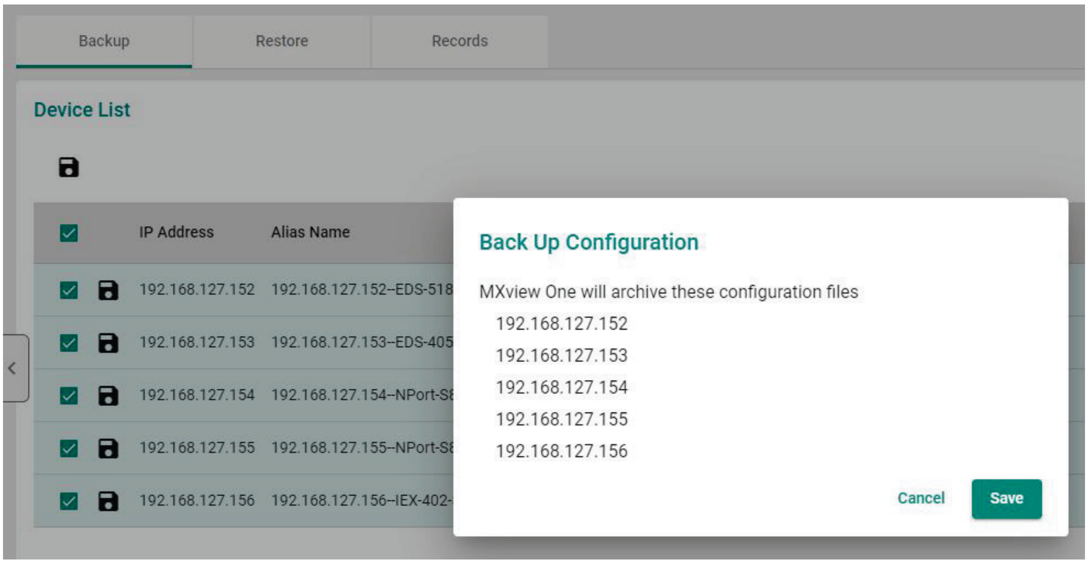
   a. Click the **Export** ( ) icon.



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.



Device List

☑		IP Address	Alias Name
☑	💾	192.168.127.152	192.168.127.152--EDS-518
☑	💾	192.168.127.153	192.168.127.153--EDS-405
☑	💾	192.168.127.154	192.168.127.154--NPort-S8
☑	💾	192.168.127.155	192.168.127.155--NPort-S8
☑	💾	192.168.127.156	192.168.127.156--IEX-402-

Back Up Configuration

MXview One will archive these configuration files
192.168.127.152
192.168.127.153
192.168.127.154
192.168.127.155
192.168.127.156

   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

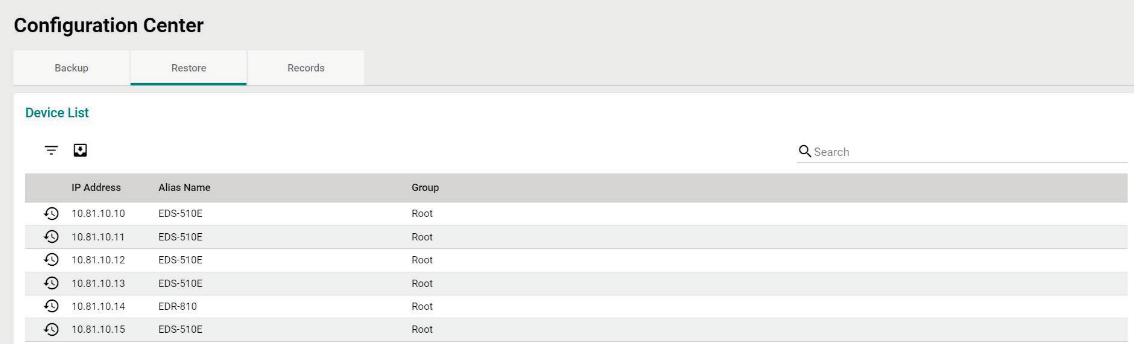
Use the **Configuration Center** screen to restore configurations to one or more devices by restoring an archived configuration from the MXview One server or importing a local configuration backup file (in INI format).

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**.



Configuration Center

	IP Address	Alias Name	Group
↺	10.81.10.10	EDS-510E	Root
↺	10.81.10.11	EDS-510E	Root
↺	10.81.10.12	EDS-510E	Root
↺	10.81.10.13	EDS-510E	Root
↺	10.81.10.14	EDR-810	Root
↺	10.81.10.15	EDS-510E	Root

3. (Optional) Filter the devices in the **Device List**:

   a. Click the **Filter** (≡) icon.

   b. Specify any of the following criteria:

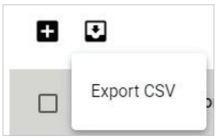
   - **Group:** The group that the device is assigned to
   - **IP Address:** The IP address of the device

   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.



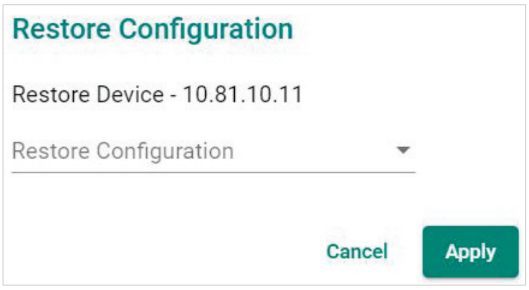
   b. Select **Export CSV**.

   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**.

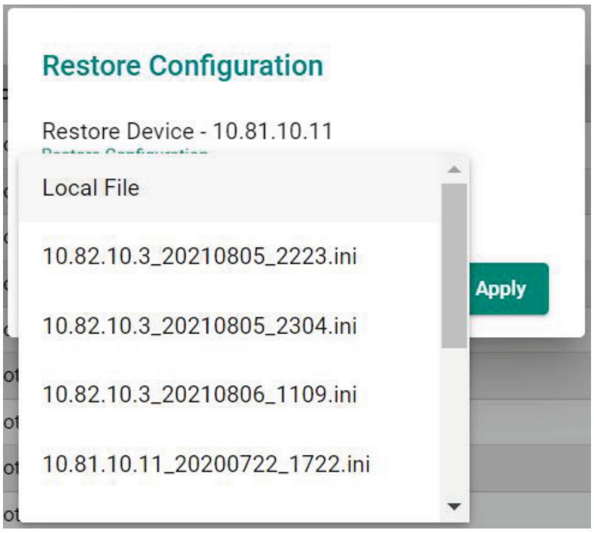
   The **Restore Configuration** screen will appear.



Restore Configuration

Restore Device - 10.81.10.11

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

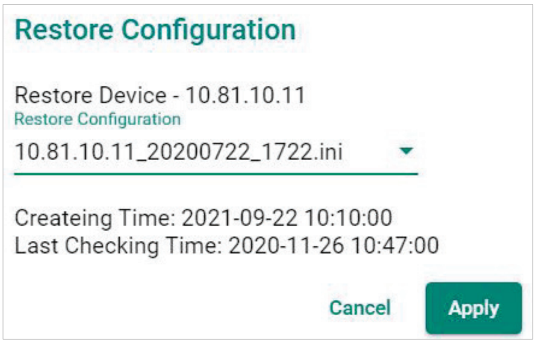


Restore Configuration

Restore Device - 10.81.10.11

Local File
10.82.10.3_20210805_2223.ini
10.82.10.3_20210805_2304.ini
10.82.10.3_20210806_1109.ini
10.81.10.11_20200722_1722.ini
Apply

c. Click **Apply**.



Restore Configuration

Restore Device - 10.81.10.11

Restore Configuration: 10.81.10.11_20200722_1722.ini

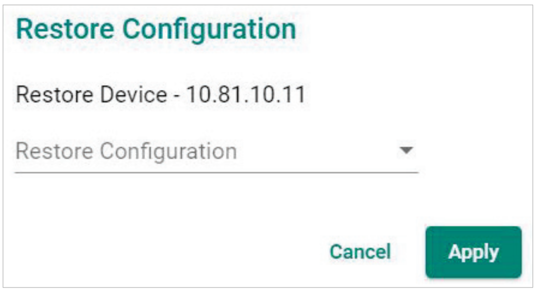
Createing Time: 2021-09-22 10:10:00
Last Checking Time: 2020-11-26 10:47:00

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.

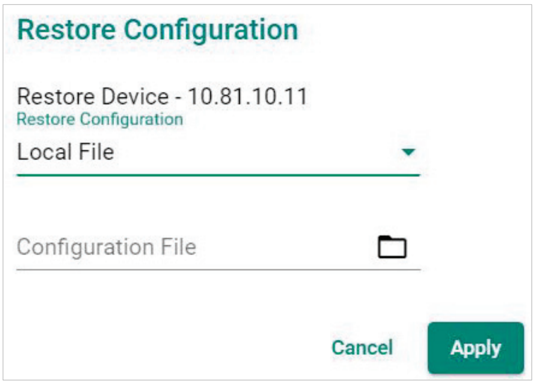


Restore Configuration

Restore Device - 10.81.10.11

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

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



Restore Configuration

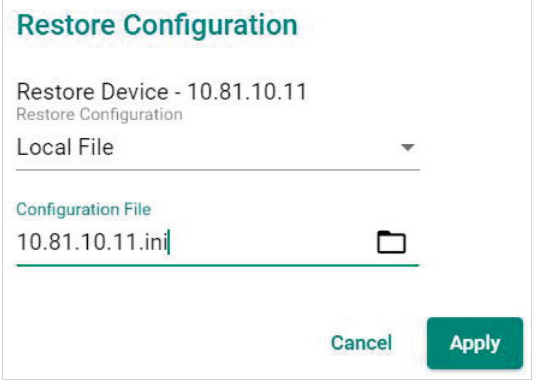
Restore Device - 10.81.10.11

Restore Configuration: Local File

Configuration File

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

e. Click **Apply**.



Restore Configuration

Restore Device - 10.81.10.11

Restore Configuration: Local File

Configuration File: 10.81.10.11.ini

MXview One imports the configuration file to the selected device.

Comparing Archived Configuration Files

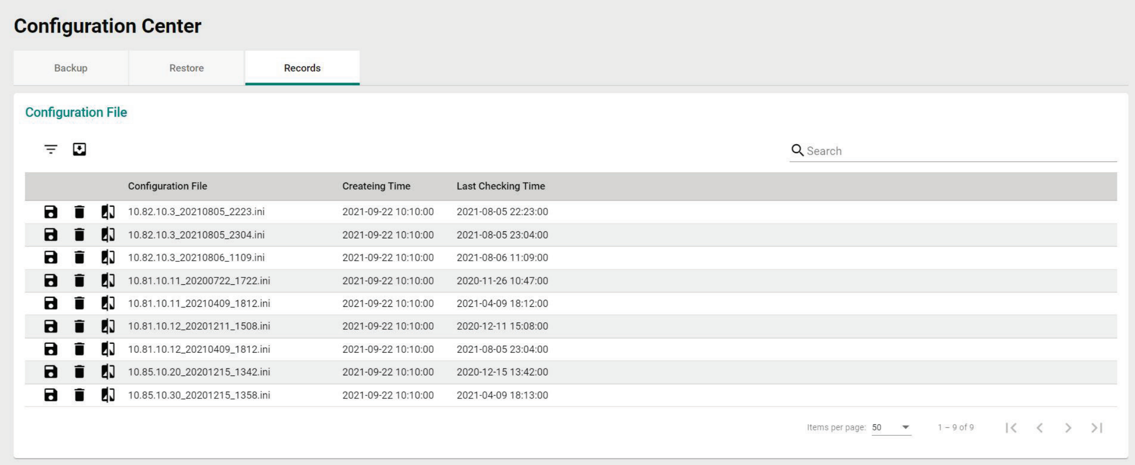
Use the **Device Configuration Center** to compare changes in the history of saved configuration files.

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.



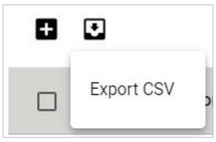
Configuration Center

Configuration File

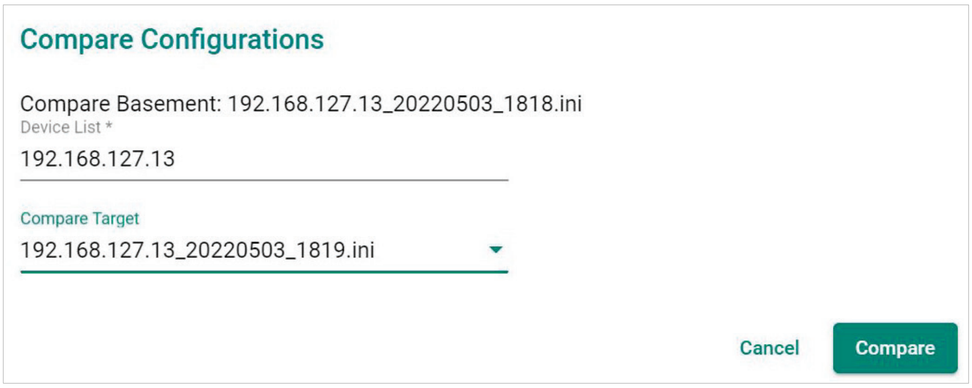
Configuration File	Createing Time	Last Checking Time
10.82.10.3_20210805_2223.ini	2021-09-22 10:10:00	2021-08-05 22:23:00
10.82.10.3_20210805_2304.ini	2021-09-22 10:10:00	2021-08-05 23:04:00
10.82.10.3_20210806_1109.ini	2021-09-22 10:10:00	2021-08-06 11:09:00
10.81.10.11_20200722_1722.ini	2021-09-22 10:10:00	2020-11-26 10:47:00
10.81.10.11_20210409_1812.ini	2021-09-22 10:10:00	2021-04-09 18:12:00
10.81.10.12_20201211_1508.ini	2021-09-22 10:10:00	2020-12-11 15:08:00
10.81.10.12_20210409_1812.ini	2021-09-22 10:10:00	2021-08-05 23:04:00
10.85.10.20_20201215_1342.ini	2021-09-22 10:10:00	2020-12-15 13:42:00
10.85.10.30_20201215_1358.ini	2021-09-22 10:10:00	2021-04-09 18:13:00

Items per page: 50   1 – 9 of 9

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.



Compare Configurations

Compare Basement: 192.168.127.13_20220503_1818.ini

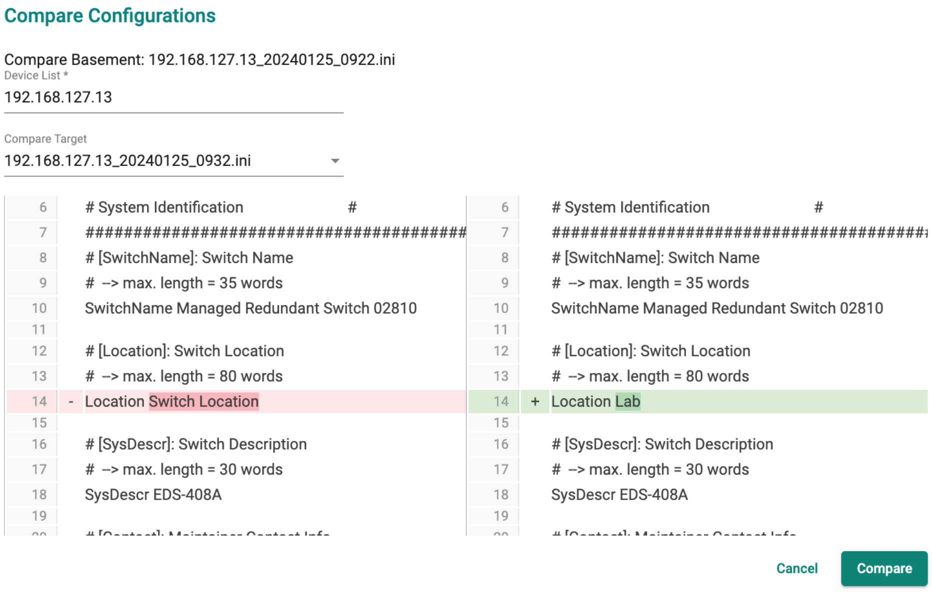
Device List *
192.168.127.13

Compare Target
192.168.127.13_20220503_1819.ini

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.



Compare Configurations

Compare Basement: 192.168.127.13_20240125_0922.ini

Device List *: 192.168.127.13

Compare Target: 192.168.127.13_20240125_0932.ini

```
# System Identification                 #
##########################################
# [SwitchName]: Switch Name
# --> max. length = 35 words
SwitchName Managed Redundant Switch 02810

# [Location]: Switch Location
# --> max. length = 80 words
- Location Switch Location

# [SysDescr]: Switch Description
# --> max. length = 30 words
SysDescr EDS-408A

# [Contact]: Maintainer Contact Info
```

```
# System Identification                 #
##########################################
# [SwitchName]: Switch Name
# --> max. length = 35 words
SwitchName Managed Redundant Switch 02810

# [Location]: Switch Location
# --> max. length = 80 words
+ Location Lab

# [SysDescr]: Switch Description
# --> max. length = 30 words
SysDescr EDS-408A

# [Contact]: Maintainer Contact Info
```

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.

17. Custom Integrations

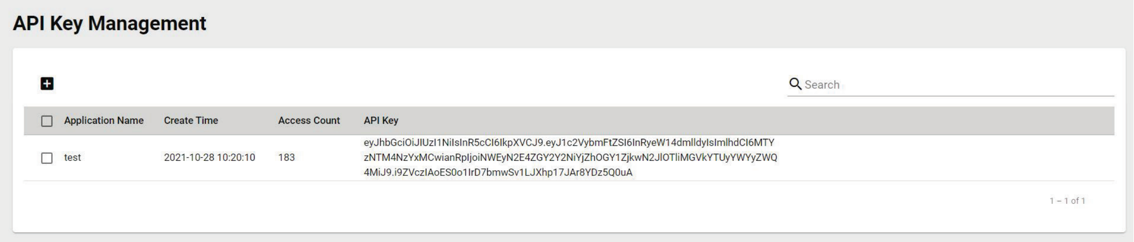
MXview One supports several features that enable integration with third-party applications or external systems.

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.



API Key Management

☐ Application Name	Create Time	Access Count	API Key
☐ test	2021-10-28 10:20:10	183	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6InRyeW14dmlldyIsImlhdCI6MTY zNTM4NzYxMCwianRpIjoiNWEyN2E4ZGY2Y2NiYjZhOGY1ZjkwN2JlOTliMGVkYTUyYWYyZWQ 4MiJ9.i9ZVczIAoES0o1IrD7bmwSv1LJXhp17JAr8YDz5Q0uA

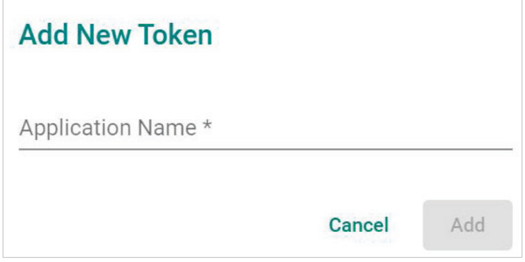
2. (Optional) Search the list of applications, type a string in the search box.

   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.



Add New Token

Application Name *

   b. Specify an **Application Name**.

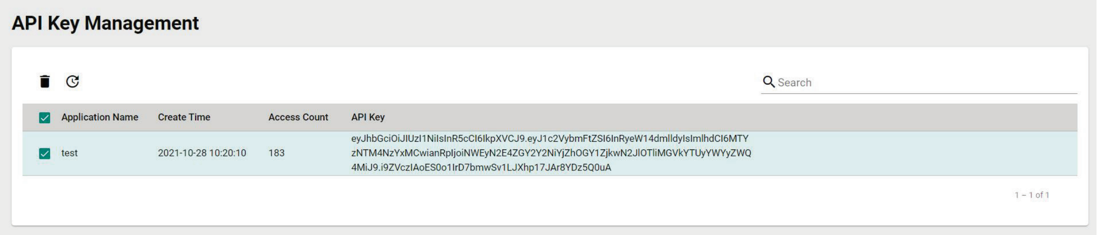
   c. Click **Add**.

   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.



API Key Management

☑ Application Name	Create Time	Access Count	API Key
☑ test	2021-10-28 10:20:10	183	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6InRyeW14dmlldyIsImlhdCI6MTY zNTM4NzYxMCwianRpIjoiNWEyN2E4ZGY2Y2NiYjZhOGY1ZjkwN2JlOTliMGVkYTUyYWYyZWQ 4MiJ9.i9ZVczIAoES0o1IrD7bmwSv1LJXhp17JAr8YDz5Q0uA

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

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

NOTE

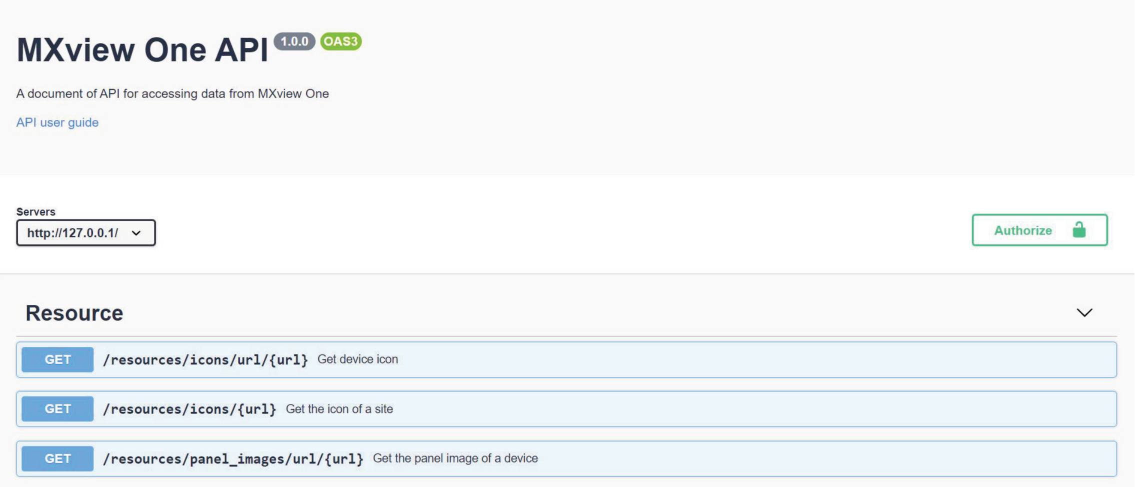
Regenerating the API key will prevent any APIs that use the old API key from working properly.

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.



MXview One API 1.0.0 OAS3

A document of API for accessing data from MXview One

API user guide

Servers
http://127.0.0.1/

Authorize

Resource

GET /resources/icons/url/{url} Get device icon

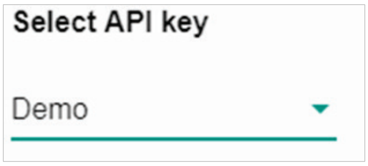
GET /resources/icons/{url} Get the icon of a site

GET /resources/panel_images/url/{url} Get the panel image of a device

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.

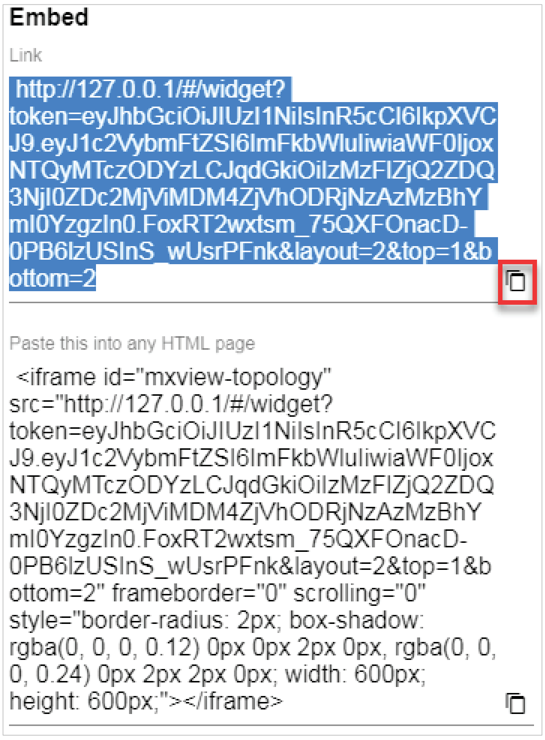
1. Navigate to **Menu** (☰) **> Integration > Embedded Web Widget**.
   The **Embedded Web Widget** screen will appear.
2. From the **Select API Key** drop-down list, select the **Application Name** for the API key you want to use.



Select API key

Demo

3. From the **Select Layout** drop-down list, select the widget(s) you want to embed:
   - **Topology and Recent Events:** Embeds both the Topology Map and Recent Events widgets in the target application
   - **Topology:** Embeds only the Topology Map in the target application
   - **Recent event:** Embeds only the Recent Events widget in the target application
4. Copy and paste the widget link for the target application:
   - To embed the widget in a web application, click the **Copy link** (⧉) icon in the **Link** section.



Embed

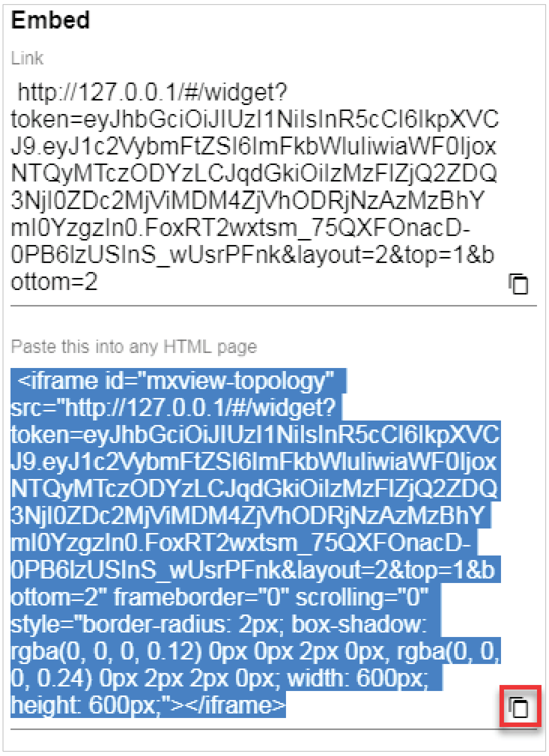
Link

```
http://127.0.0.1/#/widget?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTQyMTczODYzLCJqdGkiOiIzMzFlZjQ2ZDQ3NjI0ZDc2MjViMDM4ZjVhODRjNzAzMzBhYmI0YzgzIn0.FoxRT2wxtsm_75QXFOnacD-0PB6IzUSInS_wUsrPFnk&layout=2&top=1&bottom=2
```

Paste this into any HTML page

```
<iframe id="mxview-topology" src="http://127.0.0.1/#/widget?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTQyMTczODYzLCJqdGkiOiIzMzFlZjQ2ZDQ3NjI0ZDc2MjViMDM4ZjVhODRjNzAzMzBhYmI0YzgzIn0.FoxRT2wxtsm_75QXFOnacD-0PB6IzUSInS_wUsrPFnk&layout=2&top=1&bottom=2" frameborder="0" scrolling="0" style="border-radius: 2px; box-shadow: rgba(0, 0, 0, 0.12) 0px 0px 2px 0px, rgba(0, 0, 0, 0.24) 0px 2px 2px 0px; width: 600px; height: 600px;"></iframe>
```

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



Embed

Link

```
http://127.0.0.1/#/widget?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTQyMTczODYzLCJqdGkiOiIzMzFlZjQ2ZDQ3NjI0ZDc2MjViMDM4ZjVhODRjNzAzMzBhYmI0YzgzIn0.FoxRT2wxtsm_75QXFOnacD-0PB6IzUSInS_wUsrPFnk&layout=2&top=1&bottom=2
```

Paste this into any HTML page

```
<iframe id="mxview-topology" src="http://127.0.0.1/#/widget?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTQyMTczODYzLCJqdGkiOiIzMzFlZjQ2ZDQ3NjI0ZDc2MjViMDM4ZjVhODRjNzAzMzBhYmI0YzgzIn0.FoxRT2wxtsm_75QXFOnacD-0PB6IzUSInS_wUsrPFnk&layout=2&top=1&bottom=2" frameborder="0" scrolling="0" style="border-radius: 2px; box-shadow: rgba(0, 0, 0, 0.12) 0px 0px 2px 0px, rgba(0, 0, 0, 0.24) 0px 2px 2px 0px; width: 600px; height: 600px;"></iframe>
```

18. 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

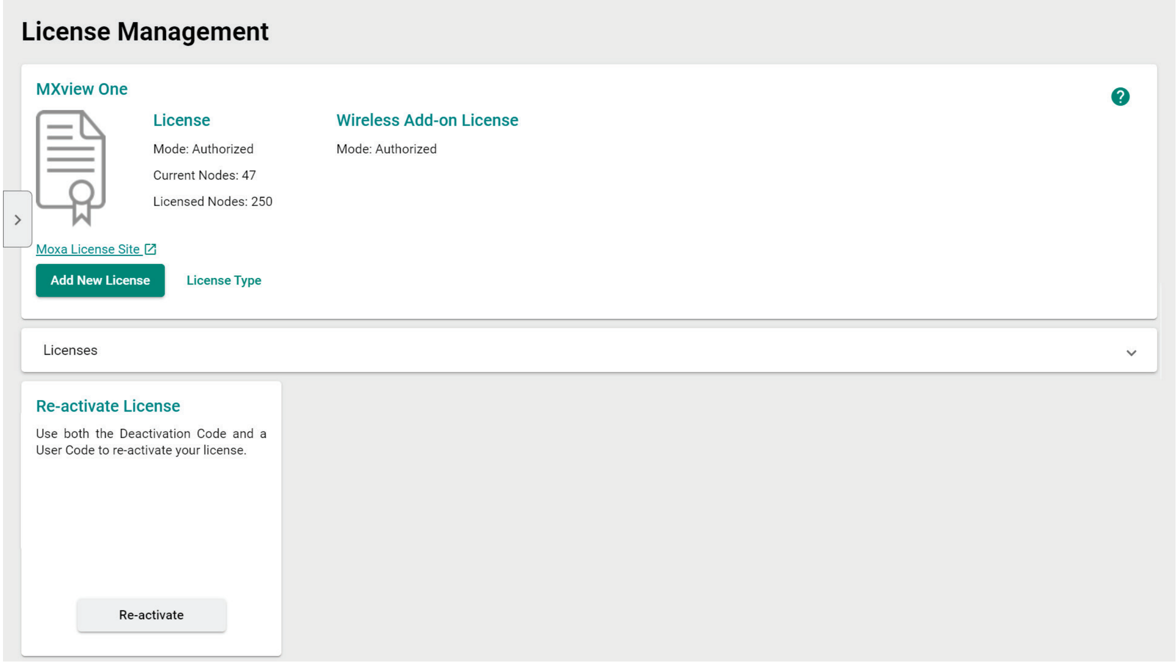
Supported Devices

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

- AWK-3131A Series (firmware v1.16 or higher)
- AWK-4131A Series (firmware v1.16 or higher)
- AWK-1131A Series (firmware v1.22 or higher)
- AWK-1137C Series (firmware v1.6 or higher)
- AWK-1151C Series (firmware v2.0 or higher)
- AWK-3252A Series (firmware v2.0 or higher)
- AWK-4252A Series (firmware v2.0 or higher)

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 90-Day free trial through the license management page.



License Management

MXview One

License

Mode: Authorized

Current Nodes: 47

Licensed Nodes: 250

Wireless Add-on License

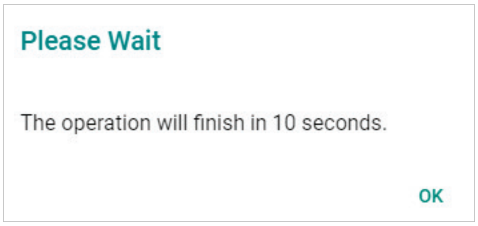
Mode: Authorized

Moxa License Site

Re-activate License

Use both the Deactivation Code and a User Code to re-activate your license.

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.



Please Wait

The operation will finish in 10 seconds.

- 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

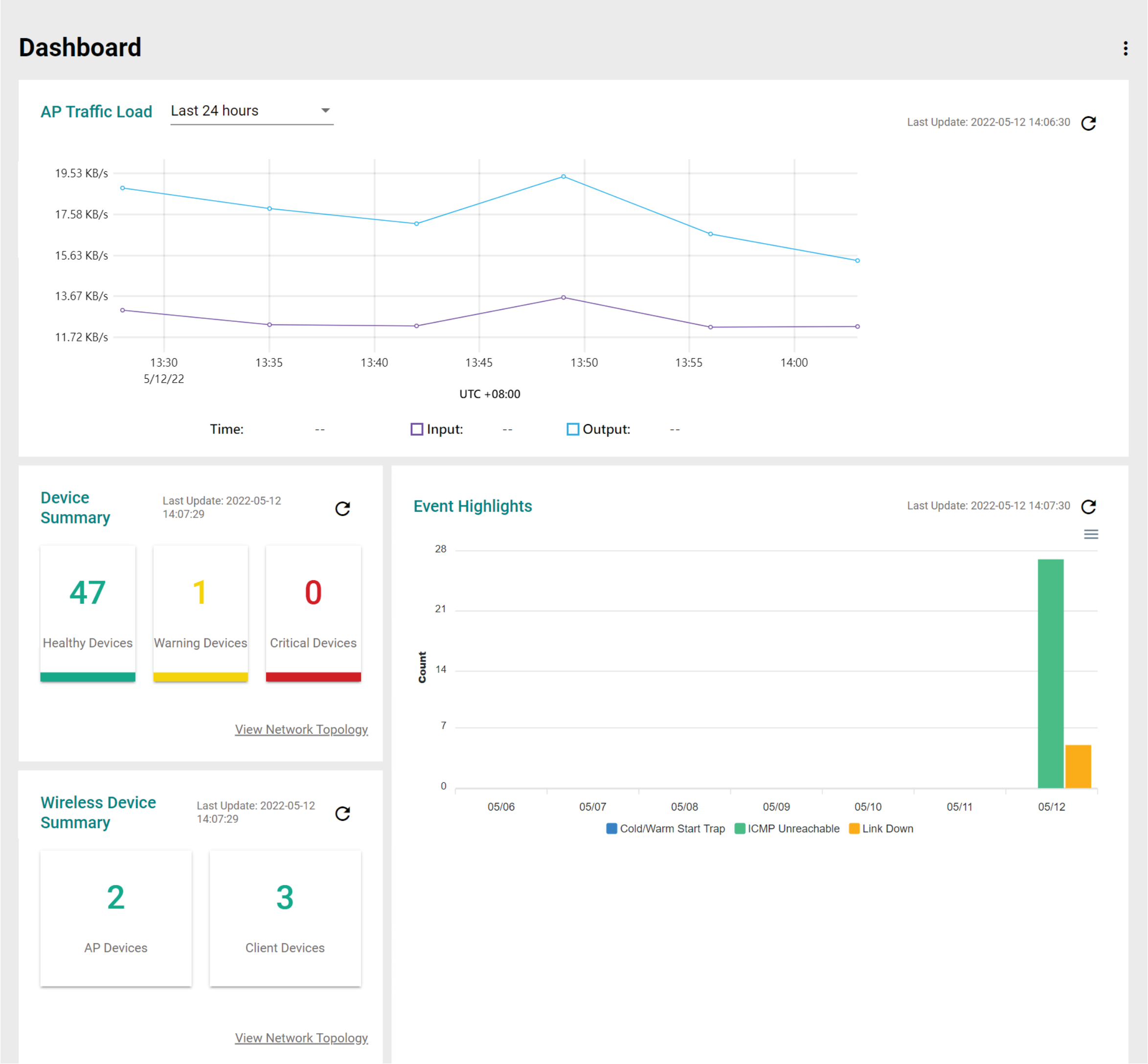
If the wireless module is activated, the MXview One Dashboard will show two additional types of information: AP Traffic load and the Wireless Device Summary.

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**.



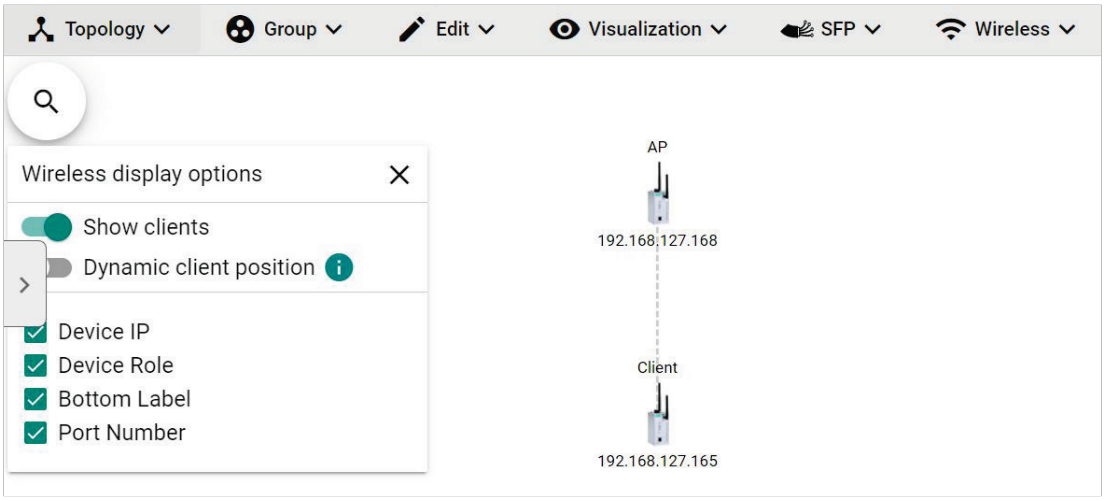
Dynamic Wireless Client Roaming

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



Wireless display options

● Show clients

○ Dynamic client position

☑ Device IP

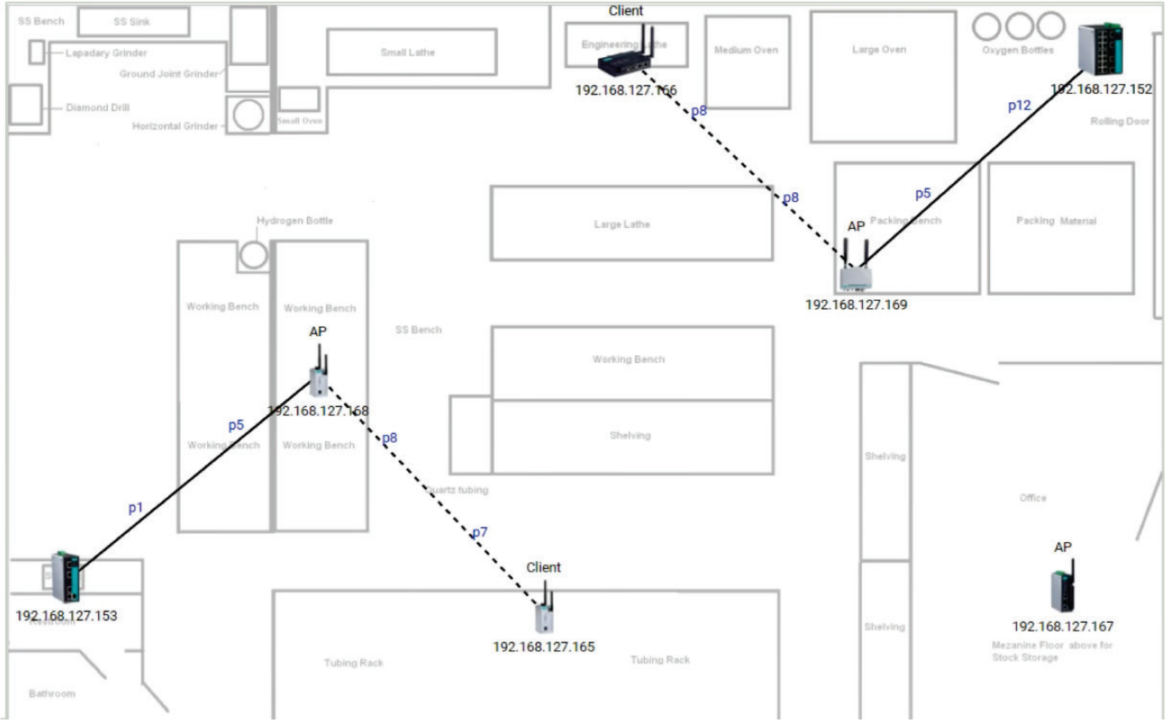
☑ Device Role

☑ Bottom Label

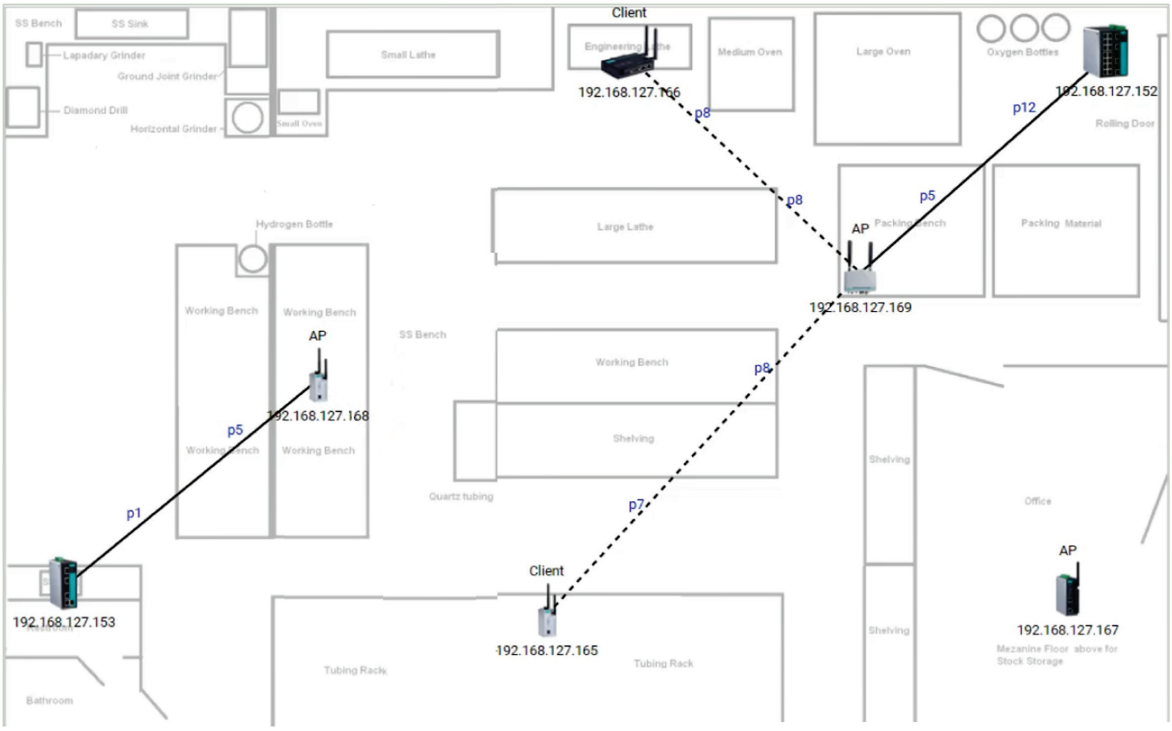
☑ Port Number

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.



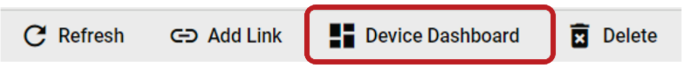
When the client roams to another AP, MXview One will automatically redraw the link to the new AP on the wireless topology diagram.



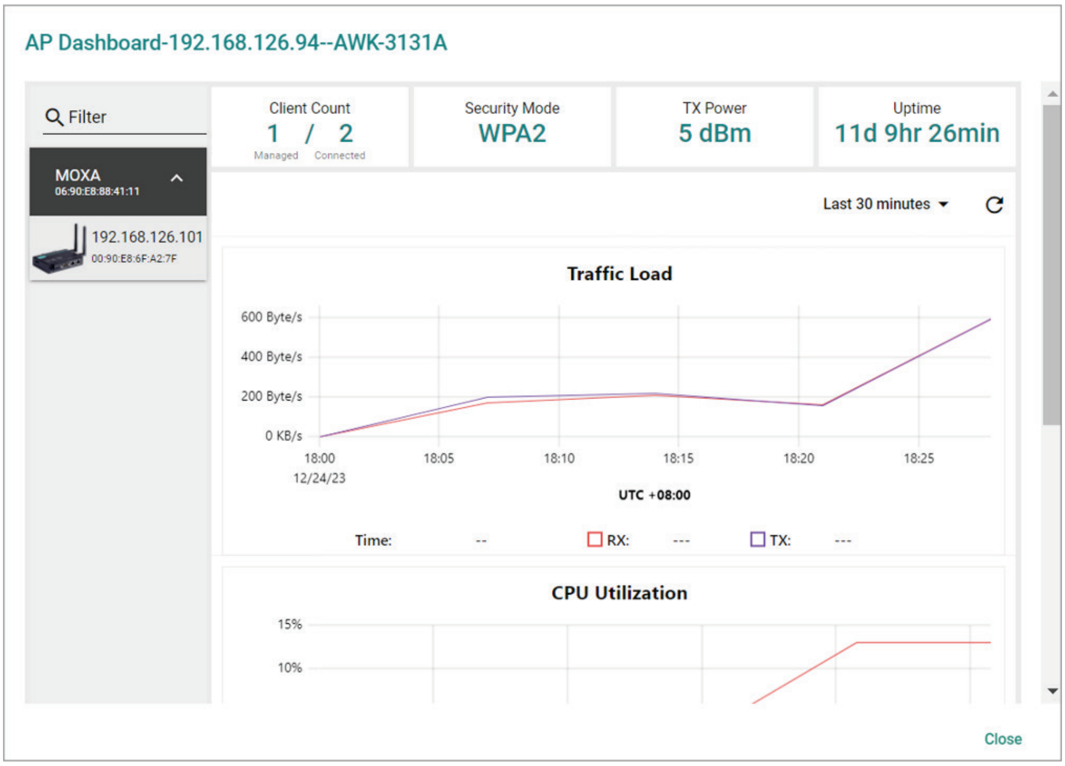
AP/Client Device Dashboard

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



AP Dashboard-192.168.126.94--AWK-3131A

Client Count: 1 / 2 (Managed / Connected)

Security Mode: WPA2

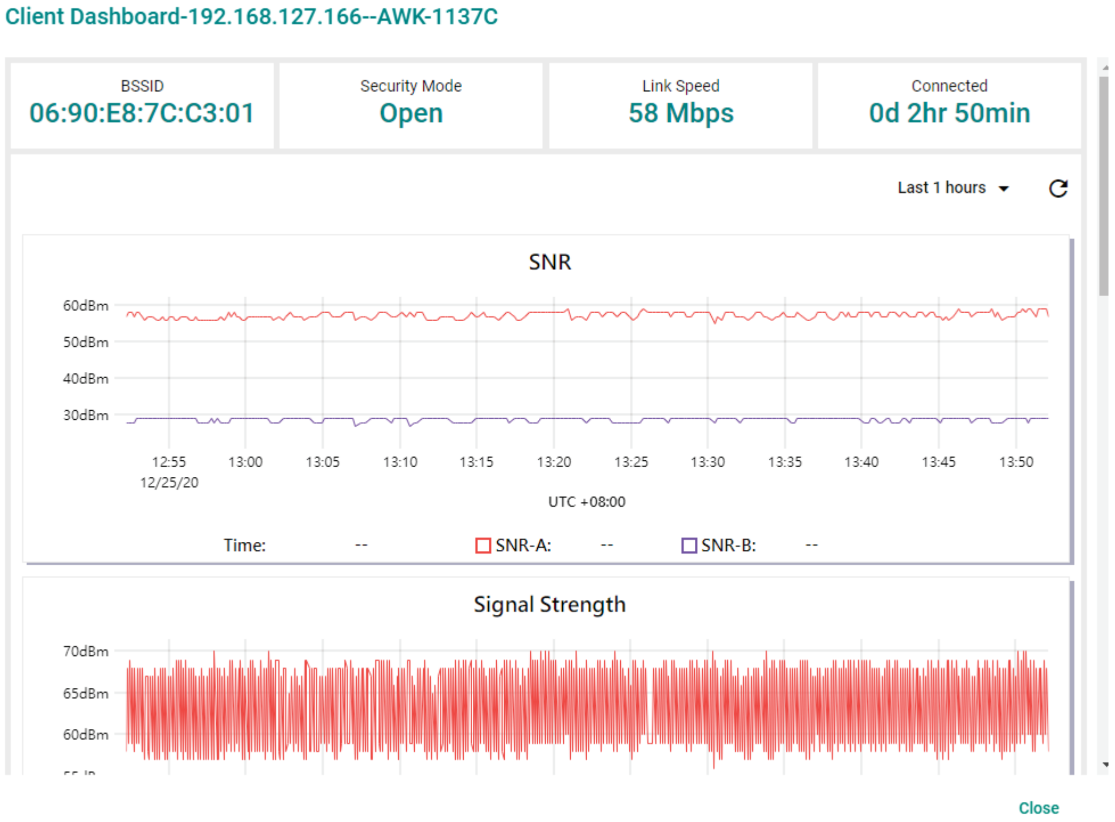
TX Power: 5 dBm

Uptime: 11d 9hr 26min

The AP Device Dashboard shows the following information:

Parameter	Description	
Client Count	Managed	The total number of wireless clients connected to this AP that are managed 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 Utilization	The current and historical CPU utilization of the AP (only supported by certain firmware versions)	
Memory Utilization	The current and historical memory utilization of the AP (only supported by certain firmware versions)	

Client Device Dashboard



Client Dashboard-192.168.127.166--AWK-1137C

BSSID: 06:90:E8:7C:C3:01

Security Mode: Open

Link Speed: 58 Mbps

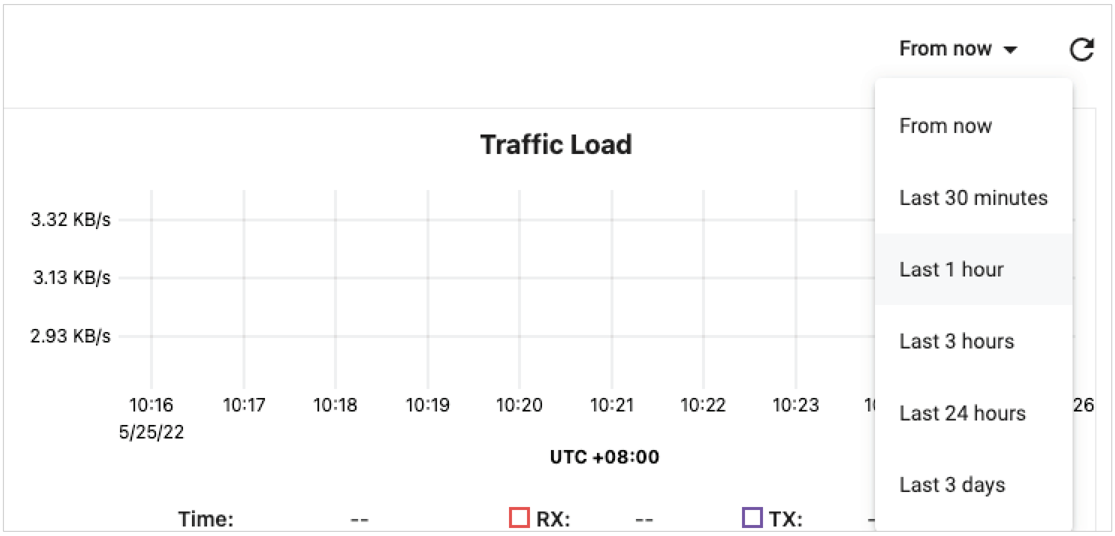
Connected: 0d 2hr 50min

Last 1 hours

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 Utilization	The current and historical CPU utilization of the client (only supported by certain firmware versions)
Memory Utilization	The current and historical memory utilization 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.

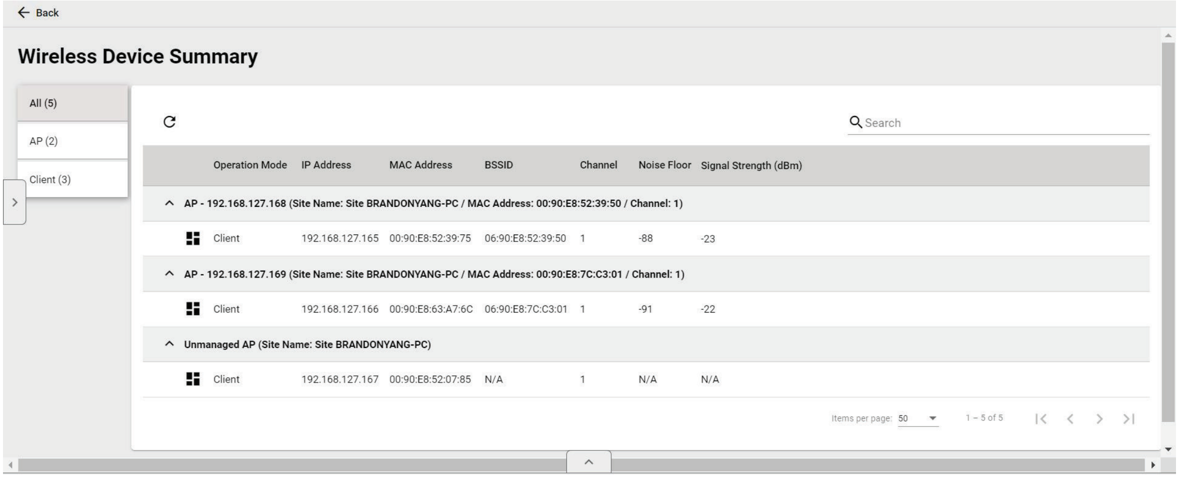


Wireless Device Summary

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.



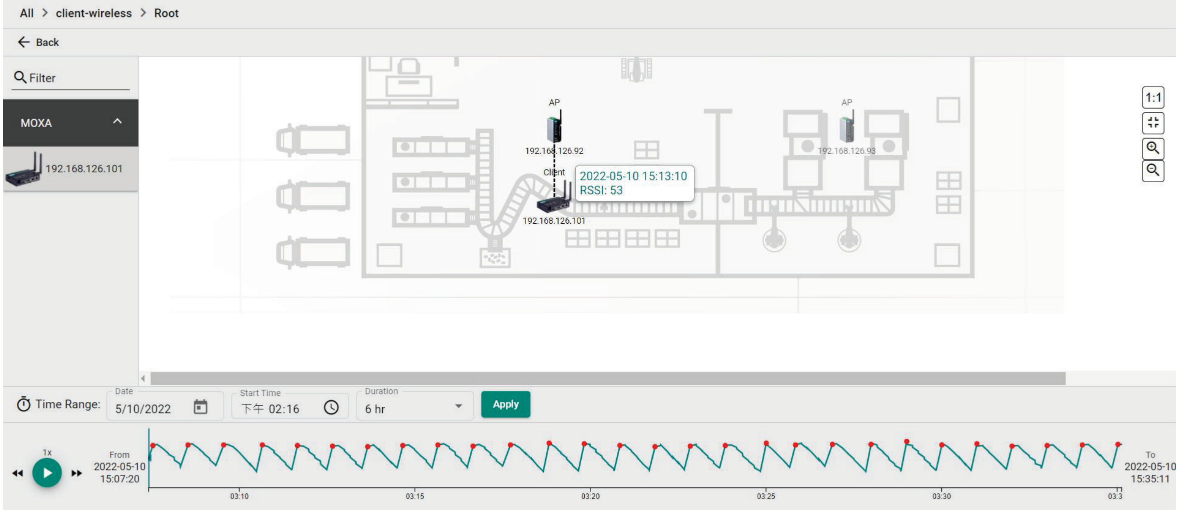
Operation Mode	IP Address	MAC Address	BSSID	Channel	Noise Floor	Signal Strength (dBm)
AP - 192.168.127.168 (Site Name: Site BRANDONYANG-PC / MAC Address: 00:90:E8:52:39:50 / Channel: 1)						
Client	192.168.127.165	00:90:E8:52:39:75	06:90:E8:52:39:50	1	-88	-23
AP - 192.168.127.169 (Site Name: Site BRANDONYANG-PC / MAC Address: 00:90:E8:7C:C3:01 / Channel: 1)						
Client	192.168.127.166	00:90:E8:63:A7:6C	06:90:E8:7C:C3:01	1	-91	-22
Unmanaged AP (Site Name: Site BRANDONYANG-PC)						
Client	192.168.127.167	00:90:E8:52:07:85	N/A	1	N/A	N/A

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.



All > client-wireless > Root

← Back

Filter

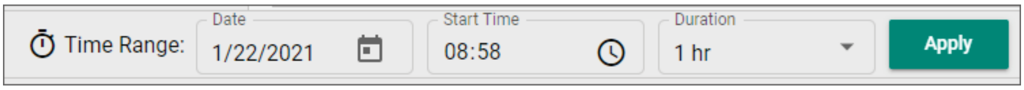
MOXA

192.168.126.101

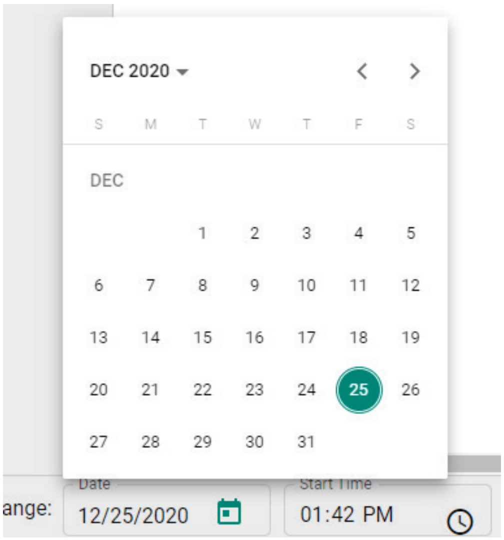
Time Range: Date 5/10/2022 Start Time 下午 02:16 Duration 6 hr Apply

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**.



Time Range: Date 1/22/2021 Start Time 08:58 Duration 1 hr

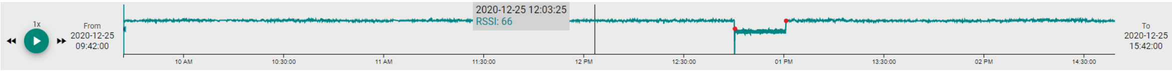


DEC 2020

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

ange: Date 12/25/2020 Start Time 01:42 PM

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.



19. 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.

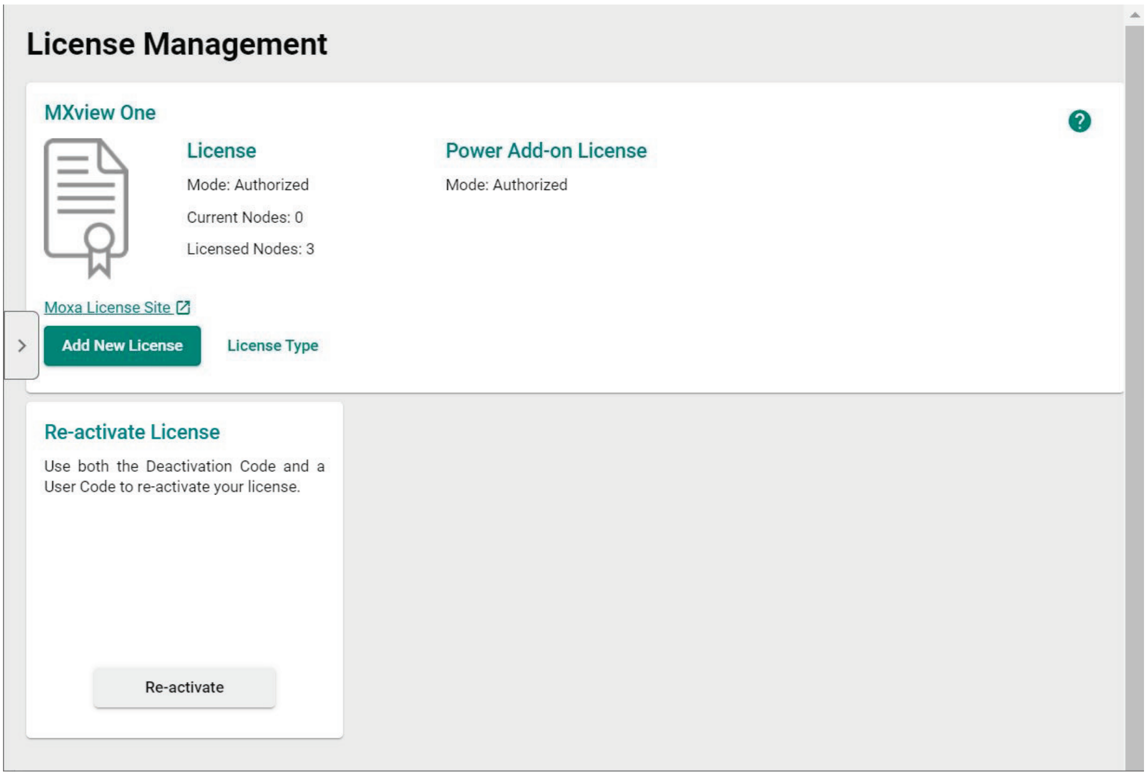
Supported Devices With PRP/HSR Features

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 higher)
- PT-G510 Series (firmware v6.4 or higher)
- PT-G7728/G7828 Series and LM-7000H-2GPHR module (firmware v6.2 or higher)
- DA-820C Series and DN-PRP-HSR-I210 or DA-PRP-HSR-I210 (OS Win 10 or higher)

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 90-day free version through the License Management page.



License Management

MXview One

License

Mode: Authorized

Current Nodes: 0

Licensed Nodes: 3

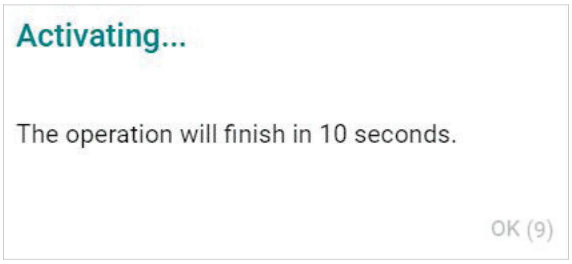
Power Add-on License

Mode: Authorized

Re-activate License

Use both the Deactivation Code and a User Code to re-activate your license.

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.



Activating...

The operation will finish in 10 seconds.

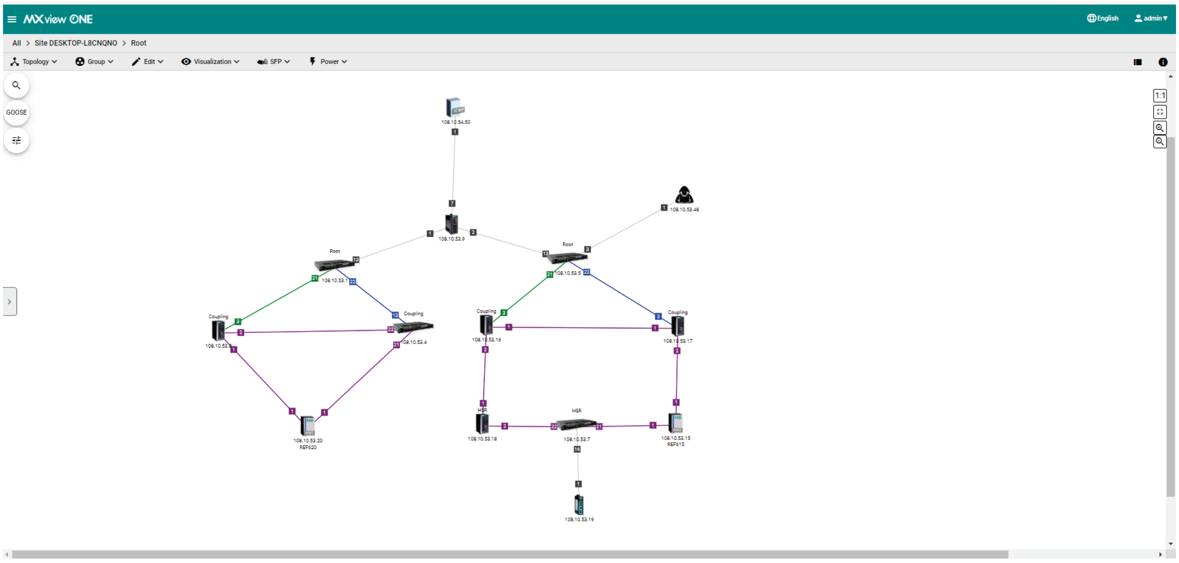
- For detailed information on how to activate the MXview Power Add-on Module, refer to **Chapter 4: License Management**.
- To add power devices to your MXview One network, refer to **Using Device Discovery**.

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.

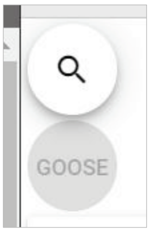


Topology

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

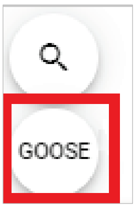
GOOSE panel

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

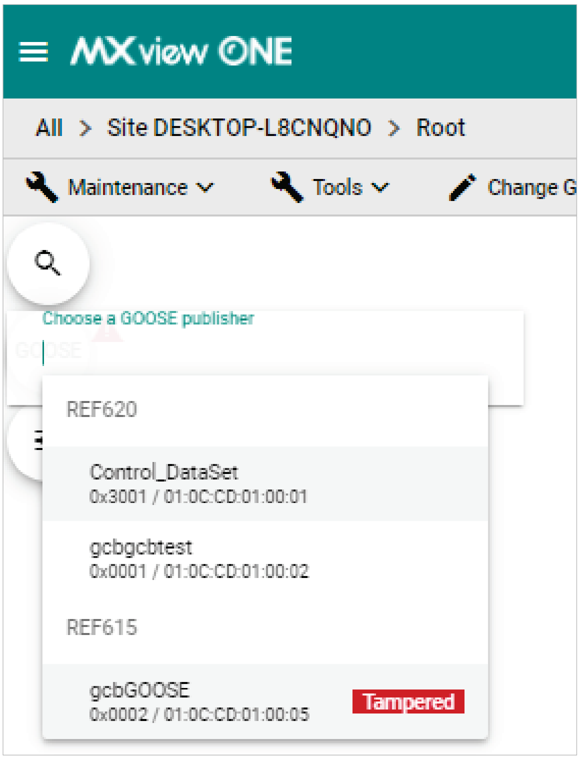


2. Once you have imported the SCD file via **Power > Import SCD**, you can find the IED as a GOOSE publisher identity via the GOOSE panel.

   a. Click **GOOSE panel**.

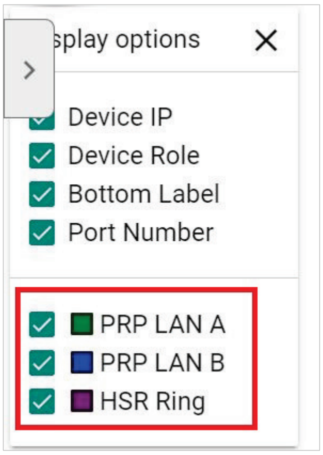


b. Scroll down or type the GOOSE-related information, such as IED name or GoCB name.


MXview ONE
All > Site DESKTOP-L8CNQNO > Root
Maintenance
Tools
Change G
Choose a GOOSE publisher
REF620
Control_DataSet
0x3001 / 01:0C:CD:01:00:01
gcbgcbtest
0x0001 / 01:0C:CD:01:00:02
REF615
gcbGOOSE
0x0002 / 01:0C:CD:01:00:05
Tampered

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

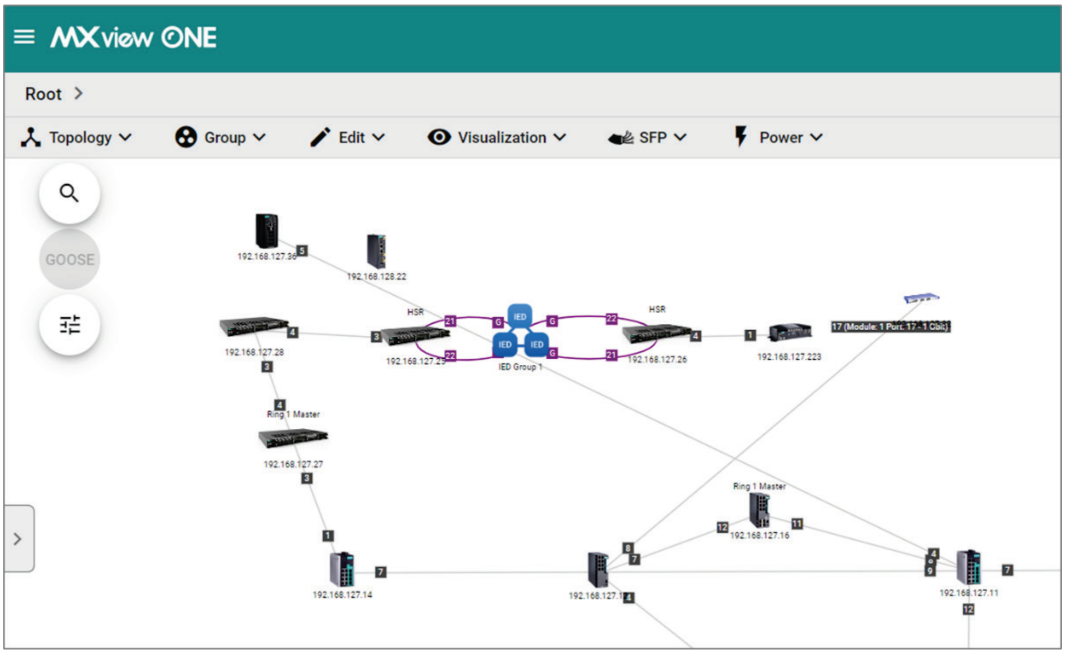
PRP LAN A is represented by a green line, PRP LAN B by a blue line, and HSR Ring by a purple line.

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**.

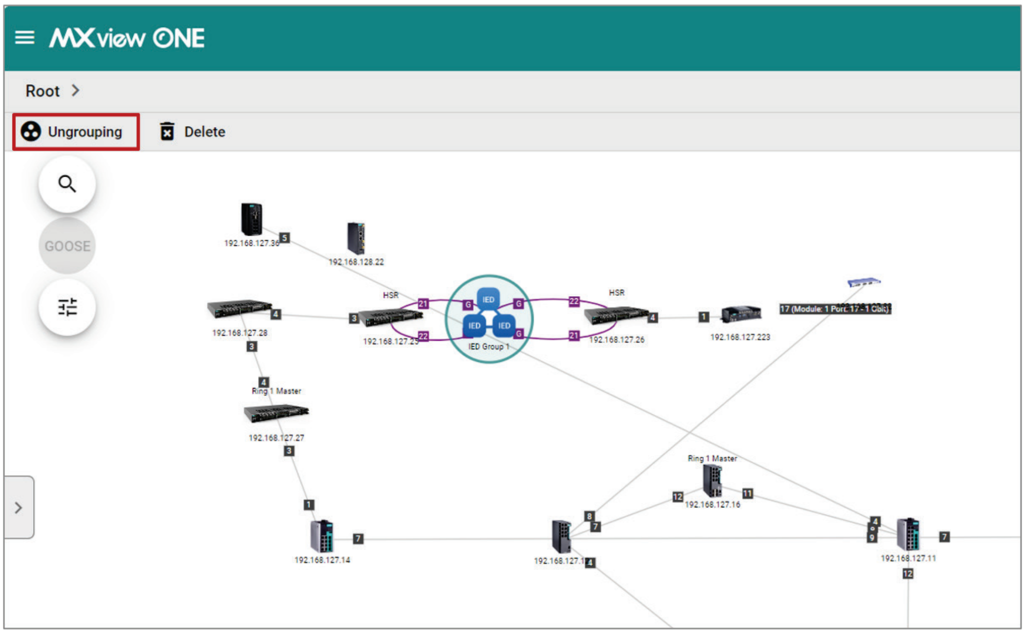
Ungrouping an IED Group

After executing the **Auto Topology** function, MXview One will automatically group the IEDs within the same HSR ring into an IED Group and represent the HSR link with a purple line. If you want to display the IEDs within the Root group or display GOOSE Message information in the topology, you can use the **Ungrouping** function.

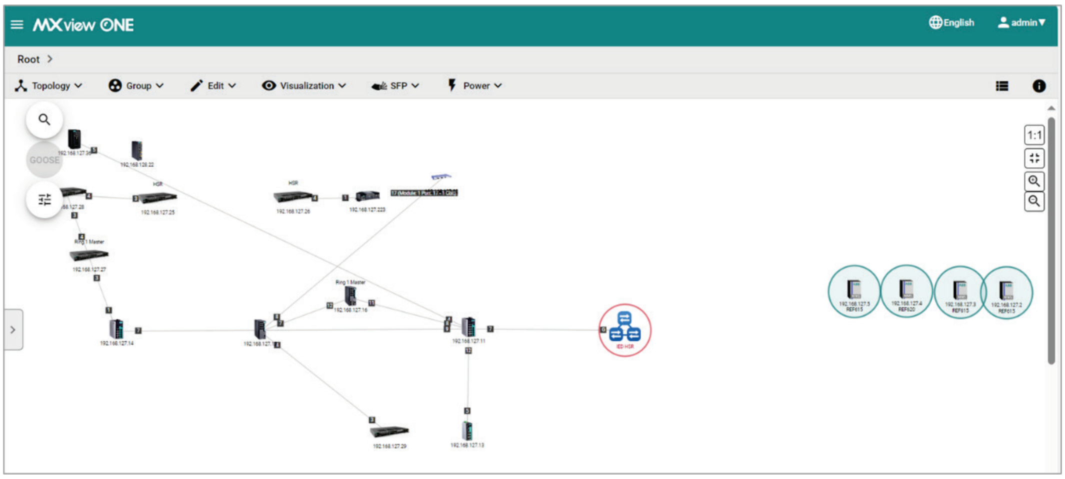


1. Navigate to **Menu** (☰) **> Topology**

   The **Topology** screen will appear and display the Topology Map by default.
2. Click on the IED group in the topology that you want to ungroup.
3. Click **Ungrouping**.



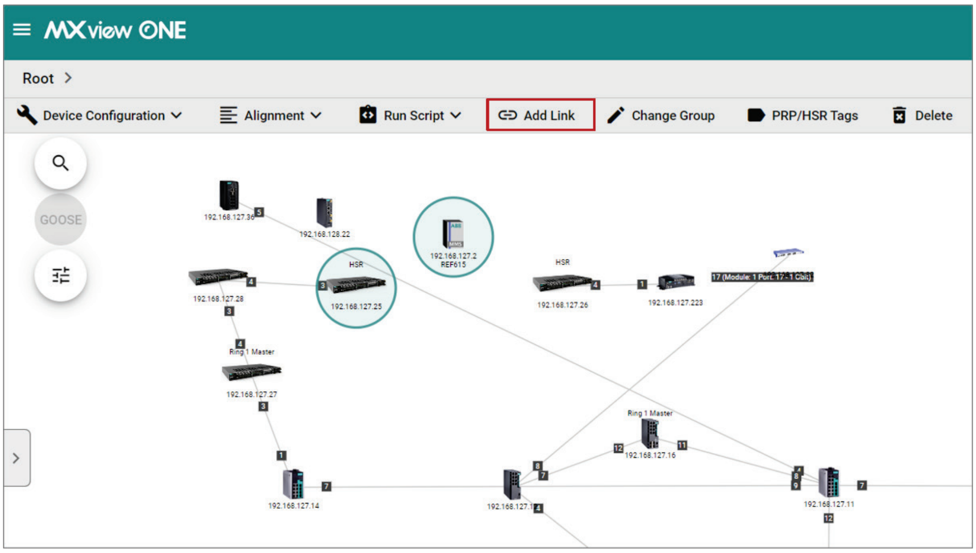
4. After ungrouping an IED group, the individual IEDs will be shown on the right-hand side of the topology.



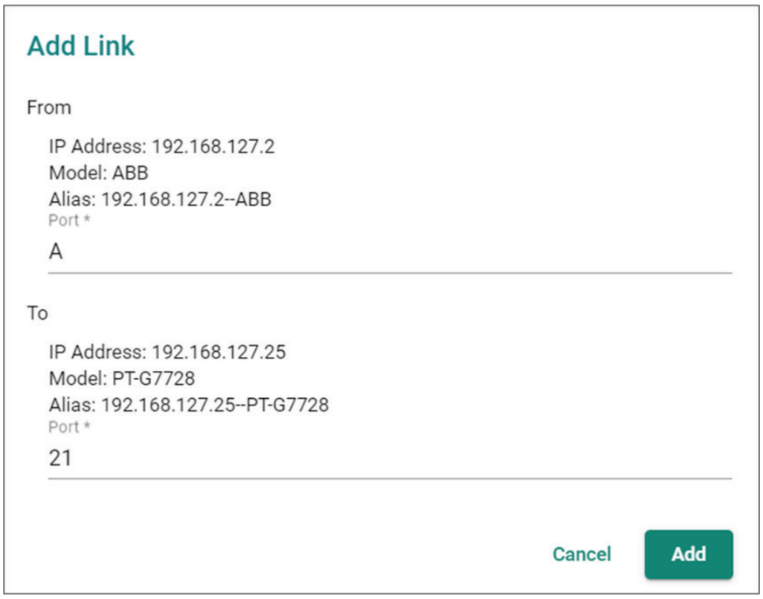
5. Align the network connections for each IED.

   a. Drag and move the IEDs to their appropriate position in the topology.

   b. Select the devices to draw a connection between and click **Add Link**.
   The **Add Link** screen will appear.



c. Specify the device port number. You can set the port number to non-numerical mode (e.g., A, B) on the IED side.



Add Link

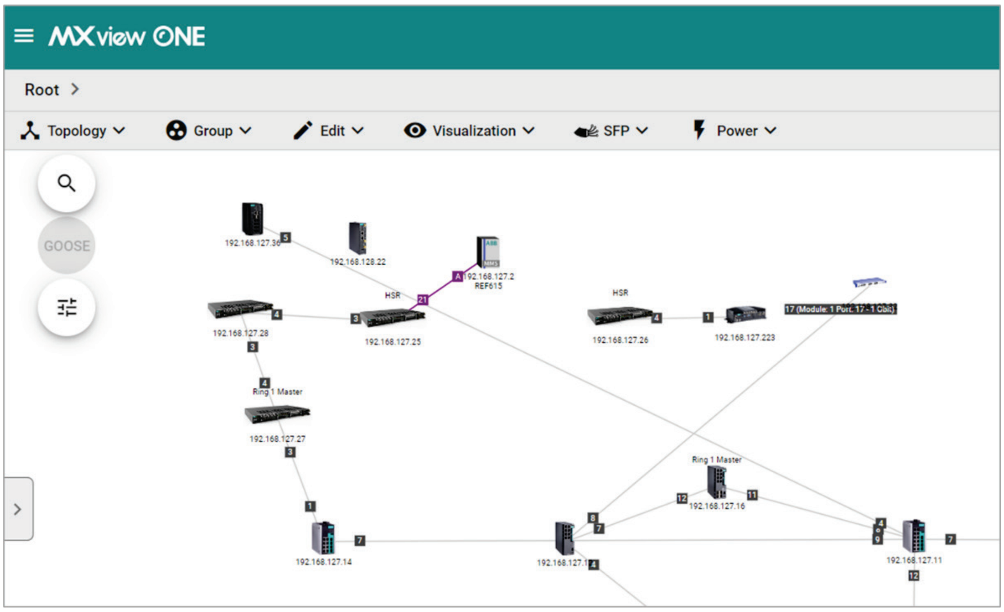
From

IP Address: 192.168.127.2
Model: ABB
Alias: 192.168.127.2--ABB
Port *
A

To

IP Address: 192.168.127.25
Model: PT-G7728
Alias: 192.168.127.25--PT-G7728
Port *
21

d. Click **Add**. MXview One will draw the connection on the topology.

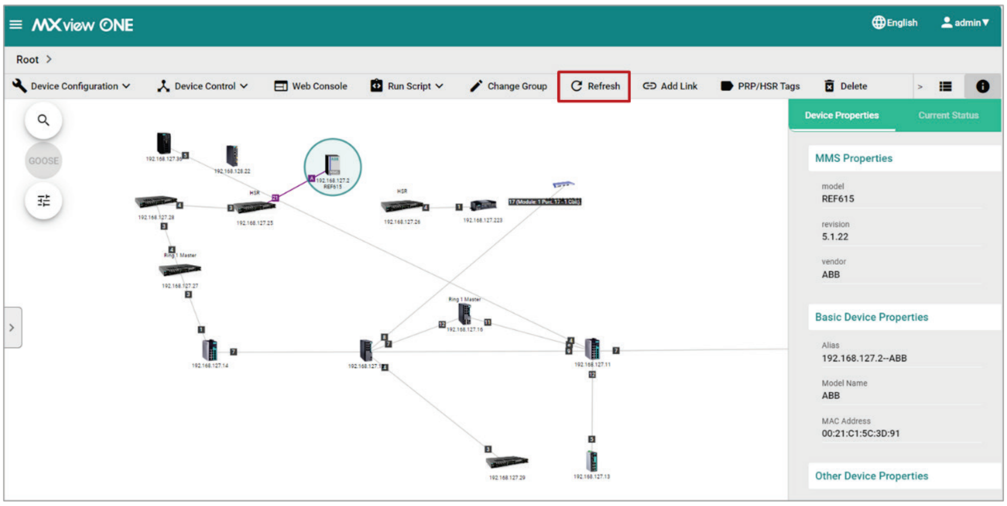


e. Repeat this process for any other remaining IED connections.

6. (**Optional**) Refresh the IED information.

a. Select one or multiple IEDs.

b. Click **Refresh**. MXview One will retrieve the latest information from the IED.



MMS Properties

model
REF615

revision
5.1.22

vendor
ABB

Basic Device Properties

Alias
192.168.127.2--ABB

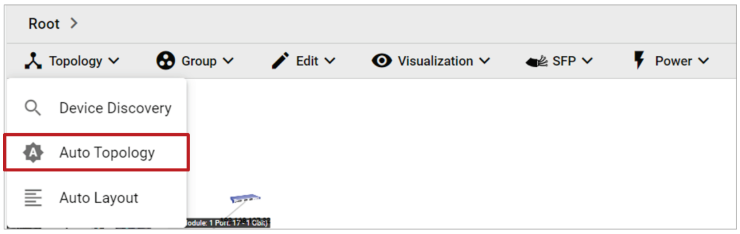
Model Name
ABB

MAC Address
00:21:C1:5C:3D:91

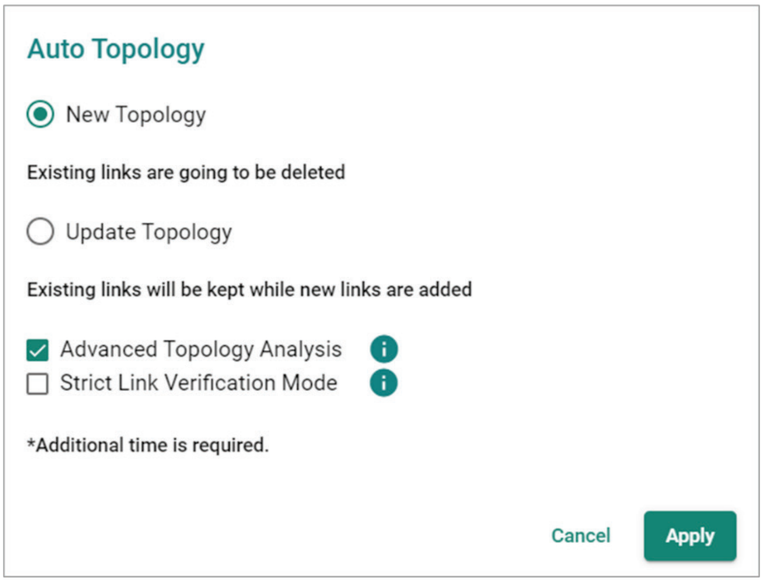
Other Device Properties

7. (**Optional**) Restore the original IED group.

a. Go to **Topology > Auto Topology**.
The **Auto Topology** screen will appear.



b. Select **New Topology** or **Update Topology**.



Auto Topology

● New Topology

Existing links are going to be deleted

○ Update Topology

Existing links will be kept while new links are added

☑ Advanced Topology Analysis
□ Strict Link Verification Mode

*Additional time is required.

c. Click **Apply**.
MXview One will restore the topology and IED group to their original state.

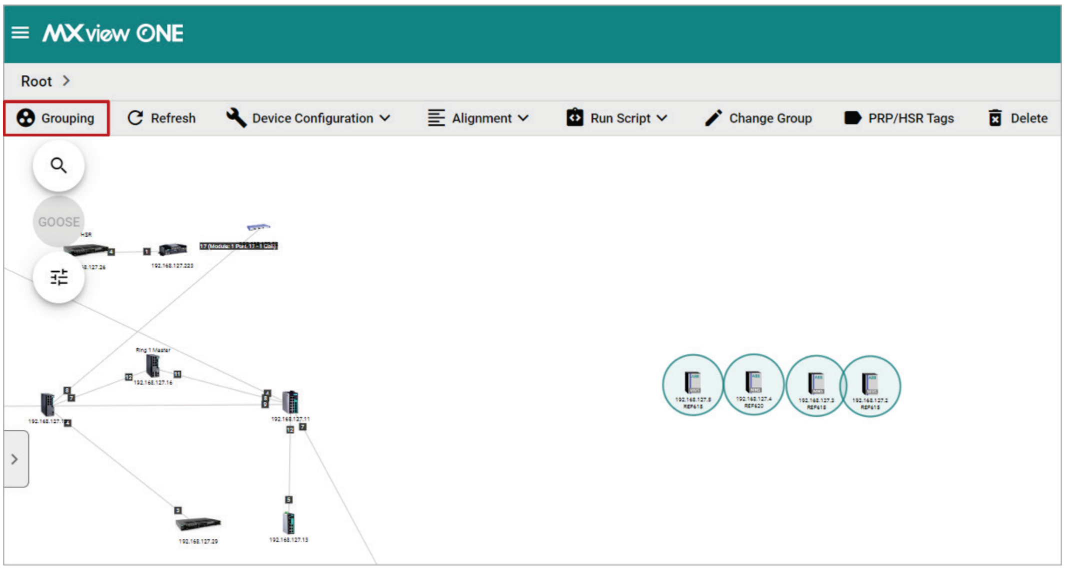
NOTE

To display GOOSE Message information on the topology, you must first ungroup the IED group, manually draw the links between the IEDs, and import the SCD file.

Creating an IED Group

Using the **Grouping** function, you can assign multiple IEDs on the topology to a single IED group.

1. Navigate to **Menu** (≡) **> Topology**
   The **Topology** screen will appear and display the Topology Map by default.
2. Select the IEDs in the topology that you want to group together.
3. Click **Grouping**.



4. MXview One will combine the selected IEDs together and show them as a single group on the topology.
   To ungroup an IED group, refer to Ungrouping an IED Group.

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.

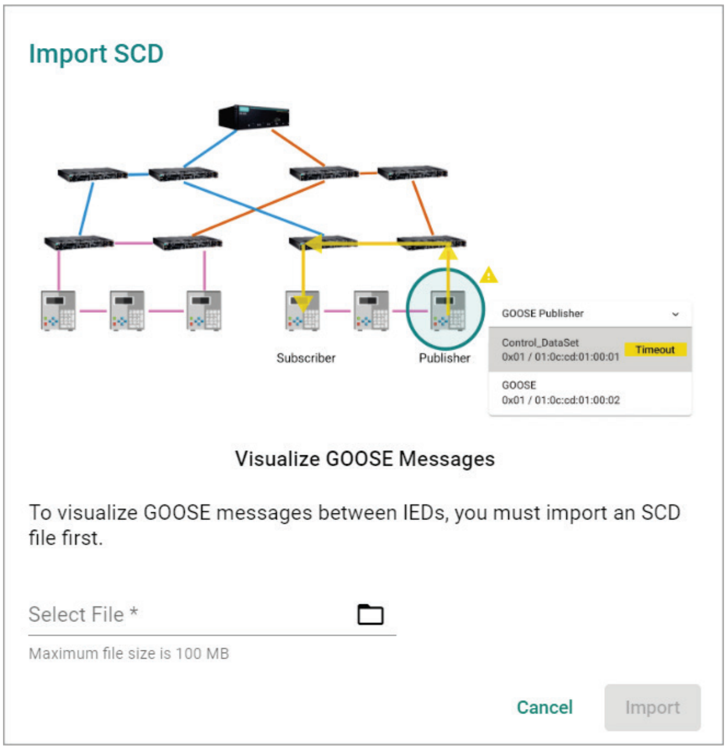
1. Navigate to **Menu** (☰) **> Topology**

   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.



Import SCD

Visualize GOOSE Messages

To visualize GOOSE messages between IEDs, you must import an SCD file first.

Select File *

Maximum file size is 100 MB

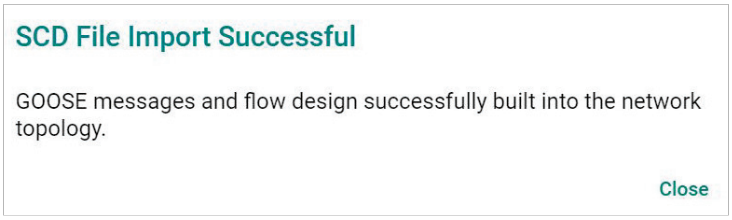
Cancel Import

   b. Upload the SCD file by clicking the **File** (🗀) icon. The file size must be less than 100 MB.

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.

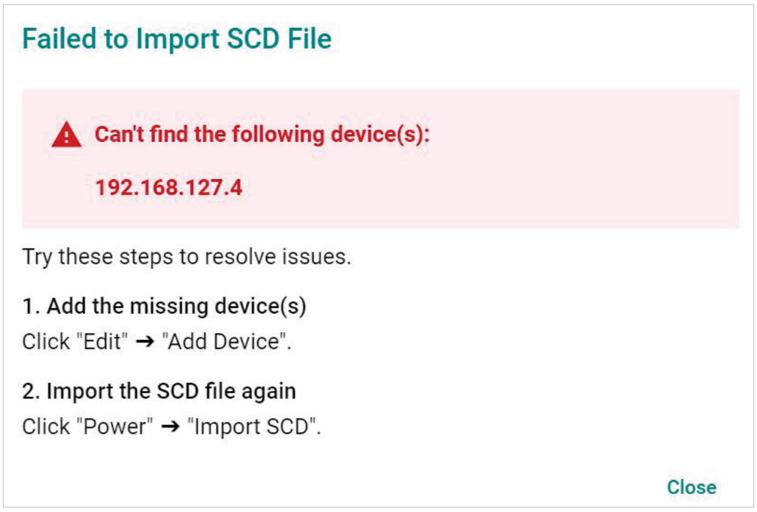


SCD File Import Successful

GOOSE messages and flow design successfully built into the network topology.

Close

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.



Failed to Import SCD File

⚠ Can't find the following device(s):

192.168.127.4

Try these steps to resolve issues.

1. Add the missing device(s)
Click "Edit" ➔ "Add Device".

2. Import the SCD file again
Click "Power" ➔ "Import SCD".

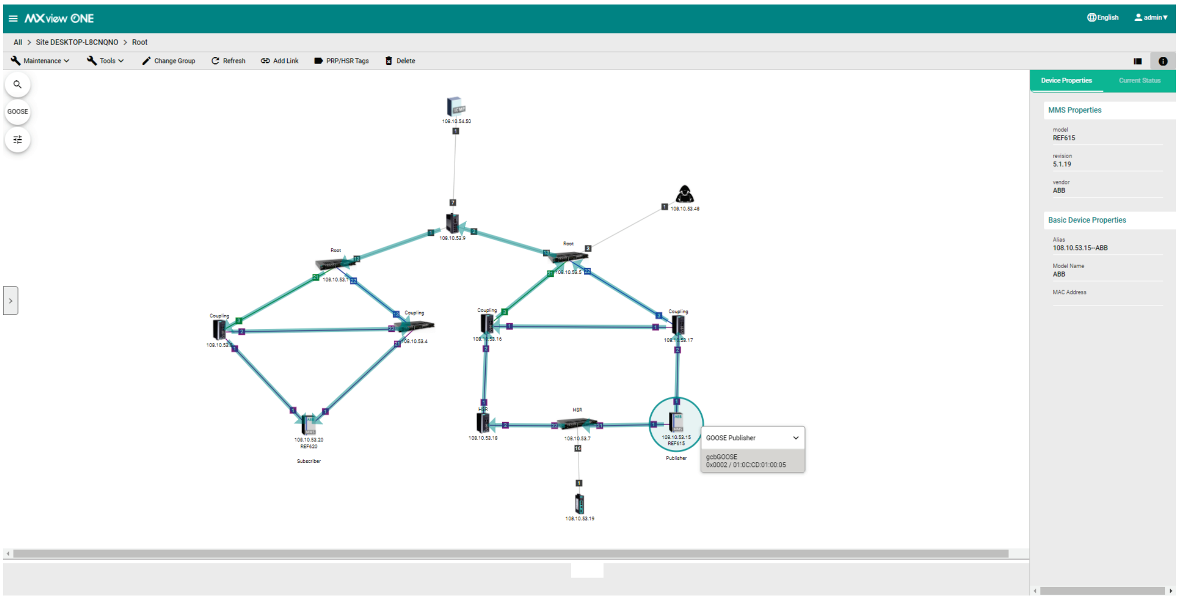
Close

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 Publisher
gcbGOOSE
0x0002 / 01:0C:CD:01:00:05

MMS Properties

model
REF615

revision
5.1.19

vendor
ABB

Basic Device Properties

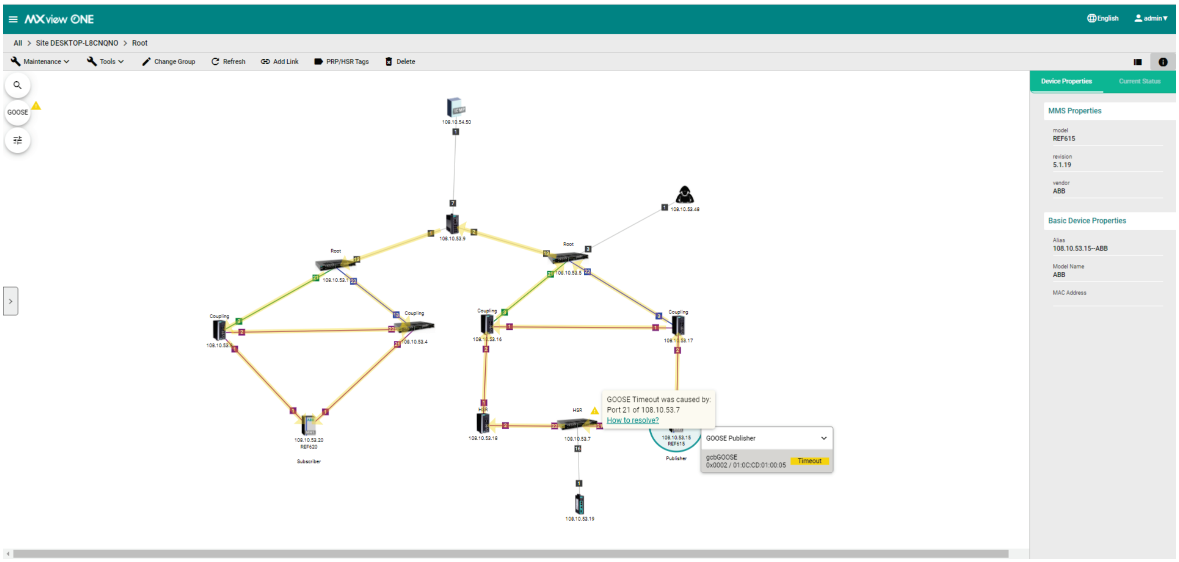
Alias
108.10.53.15--ABB

Model Name
ABB

MAC Address

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.



GOOSE Timeout was caused by:
Port 21 of 108.10.53.7
How to resolve?

GOOSE Publisher

gcbGOOSE
0x0002 / 01:0C:CD:01:00:05 Timeout

MMS Properties

model
REF615

revision
5.1.19

vendor
ABB

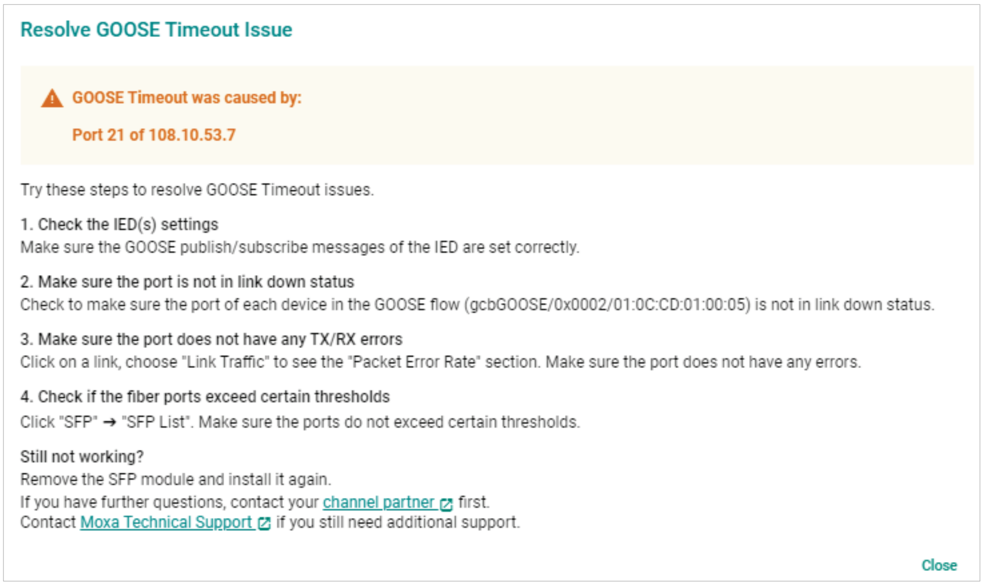
Basic Device Properties

Alias
108.10.53.15--ABB

Model Name
ABB

MAC Address

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



Resolve GOOSE Timeout Issue

GOOSE Timeout was caused by:

Port 21 of 108.10.53.7

Try these steps to resolve GOOSE Timeout issues.

1. Check the IED(s) settings
Make sure the GOOSE publish/subscribe messages of the IED are set correctly.

2. Make sure the port is not in link down status
Check to make sure the port of each device in the GOOSE flow (gcbGOOSE/0x0002/01:0C:CD:01:00:05) is not in link down status.

3. Make sure the port does not have any TX/RX errors
Click on a link, choose "Link Traffic" to see the "Packet Error Rate" section. Make sure the port does not have any errors.

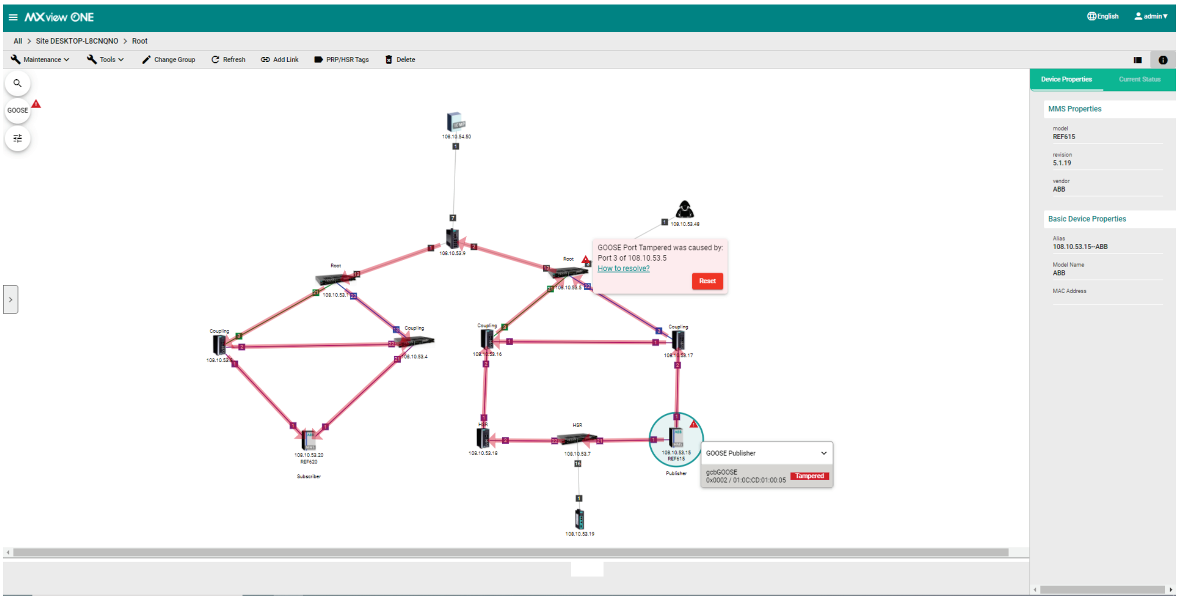
4. Check if the fiber ports exceed certain thresholds
Click "SFP" → "SFP List". Make sure the ports do not exceed certain thresholds.

Still not working?
Remove the SFP module and install it again.
If you have further questions, contact your channel partner first.
Contact Moxa Technical Support if you still need additional support.

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.



GOOSE Port Tampered was caused by:
Port 3 of 108.10.53.5
How to resolve?
Reset

GOOSE Publisher
gcbGOOSE
0x0002 / 01:0C:CD:01:00:05 Tampered

MMS Properties

model
REF615

revision
5.1.19

vendor
ABB

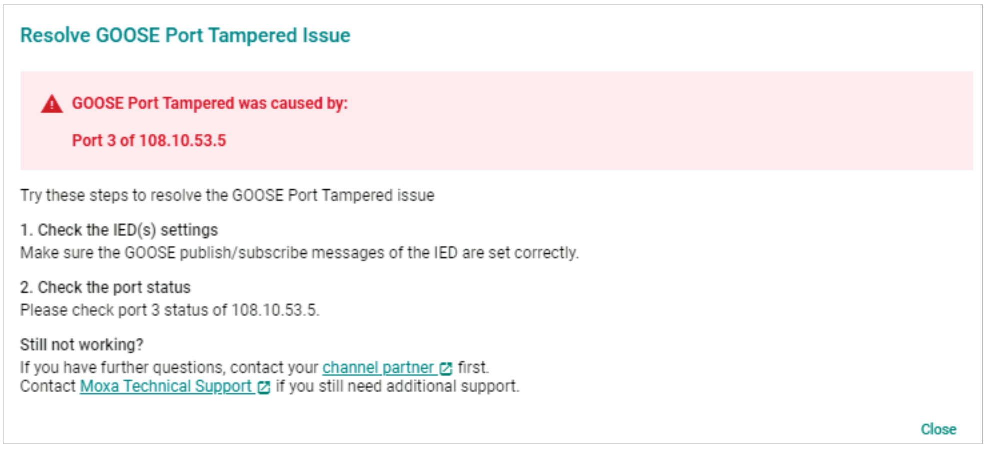
Basic Device Properties

Alias
108.10.53.15--ABB

Model Name
ABB

MAC Address

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



Resolve GOOSE Port Tampered Issue

GOOSE Port Tampered was caused by:

Port 3 of 108.10.53.5

Try these steps to resolve the GOOSE Port Tampered issue

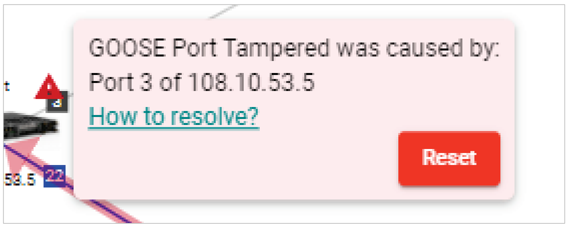
1. Check the IED(s) settings
Make sure the GOOSE publish/subscribe messages of the IED are set correctly.

2. Check the port status
Please check port 3 status of 108.10.53.5.

Still not working?
If you have further questions, contact your channel partner first.
Contact Moxa Technical Support if you still need additional support.

Close

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.



GOOSE Port Tampered was caused by:
Port 3 of 108.10.53.5
How to resolve?
Reset