MXview One 1.7.0 User Manual

Version 8.0, January 2026

www.moxa.com/products

MXview One 1.6.0 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 four parts: The Main Module, Power Add-on Module, the Wireless Add-on Module, and the Security 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. The MXview Wireless Add-on Module provides additional advanced functions for wireless applications to monitor and troubleshoot your network, and help you minimize downtime. The Security Add-on Module provides additional advanced functions to enhance field security, including centralized management and deployment of firewall policies, and updating cybersecurity packages.

Key Features

Web-based Operation

You will need to install 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, 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, Microsoft Teams, or message box.

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

For Ubuntu installation instructions, please refer to the **MXview One Linux Installation Guide**, which can be downloaded from the Moxa website.

There are two ways to install MXview One on Linux Ubuntu: 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.

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

For Ubuntu users:

Execute the following command to activate MXview One Control Panel:
#sudo /usr/mxview/mxview-control-panel/MXControlPanel

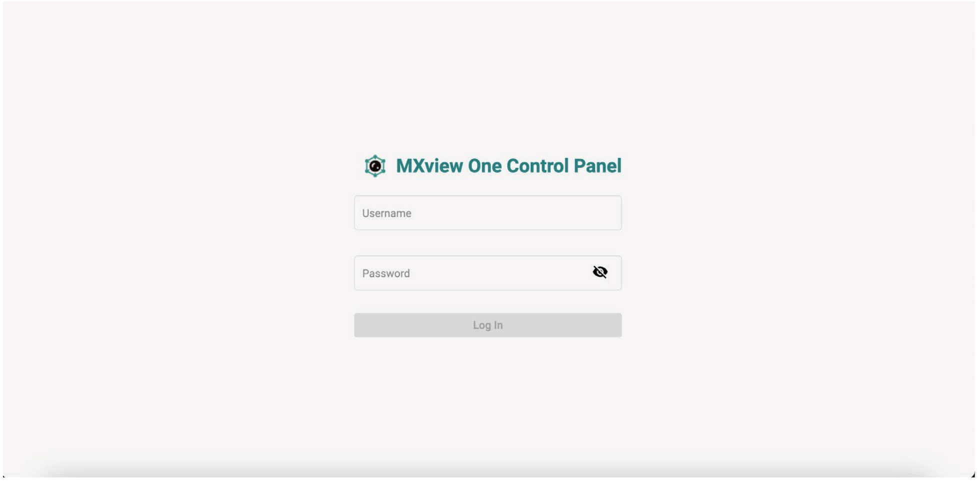
Open a web browser and navigate to https://[host IP address]:7100. The host IP address is the IP of the computer running MXview One. The default IP address is: 127.0.0.1

To stop MXview One in Linux, press CTRL + C.

For Windows users:

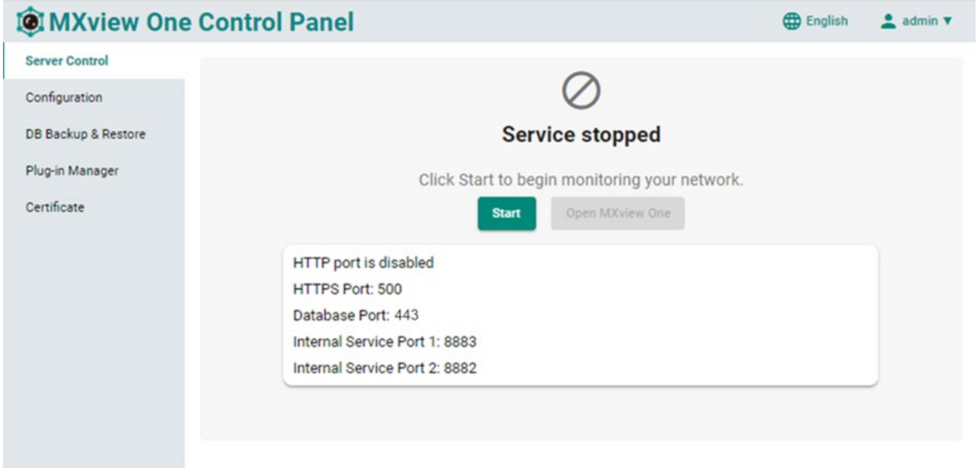
Start the MXview One server on the computer before launching the MXview One web console. On the server computer, double-click the MXview One desktop shortcut in the Windows operating system.

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**.

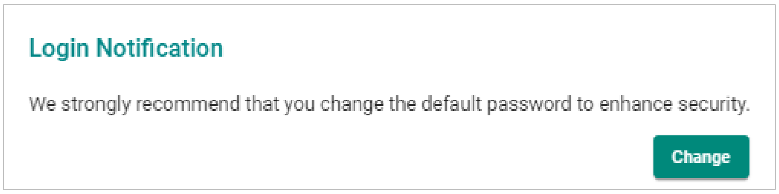


Service stopped

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

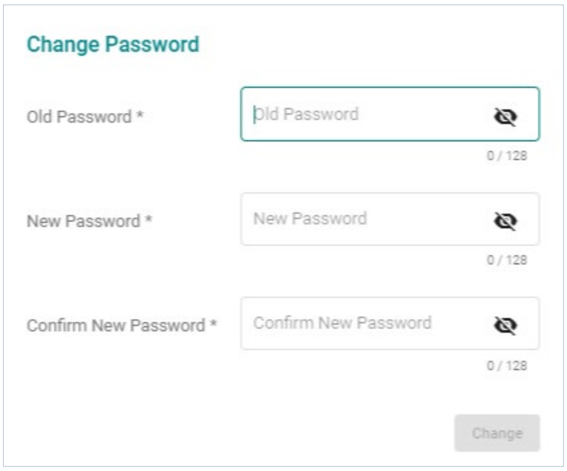
After logging in with the default credentials, the system will display a message asking you to change the default password to enhance security.



Login Notification

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

After clicking the **Change** button, the **Change Password** window will appear.

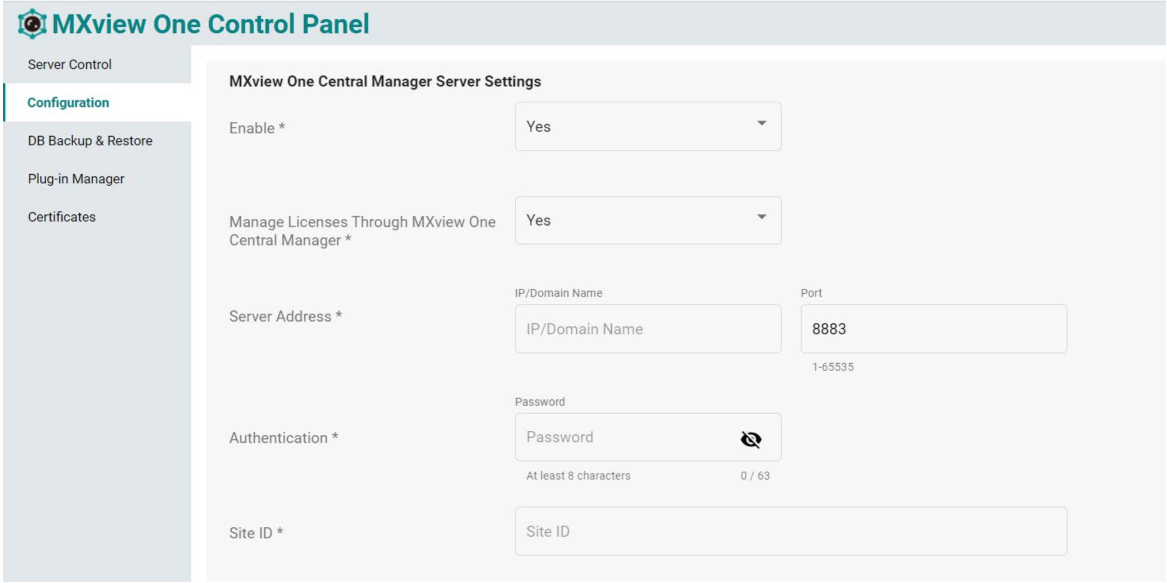


Change Password

Old Password *	Old Password 0 / 128
New Password *	New Password 0 / 128
Confirm New Password *	Confirm New Password 0 / 128

Configuration

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



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)

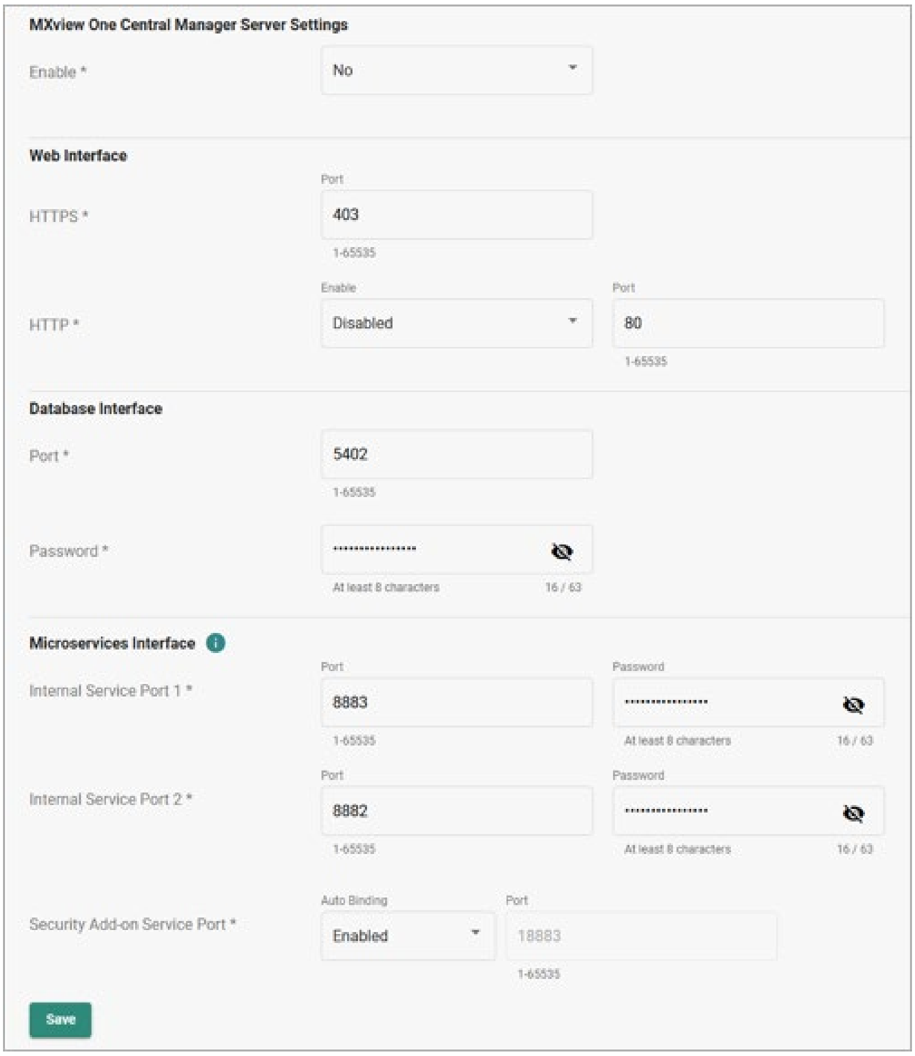
Authentication * Password: Password (At least 8 characters, 0 / 63)

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



MXview One Central Manager Server Settings

Enable * : No

Web Interface

HTTPS * : Port 403 (1-65535)

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

Database Interface

Port * : 5402 (1-65535)

Password * : •••••••••••••••• (At least 8 characters, 16 / 63)

Microservices Interface

Internal Service Port 1 * : Port 8883 (1-65535); Password •••••••••••••••• (At least 8 characters, 16 / 63)

Internal Service Port 2 * : Port 8882 (1-65535); Password •••••••••••••••• (At least 8 characters, 16 / 63)

Security Add-on Service Port * : Auto Binding Enabled; Port 18883 (1-65535)

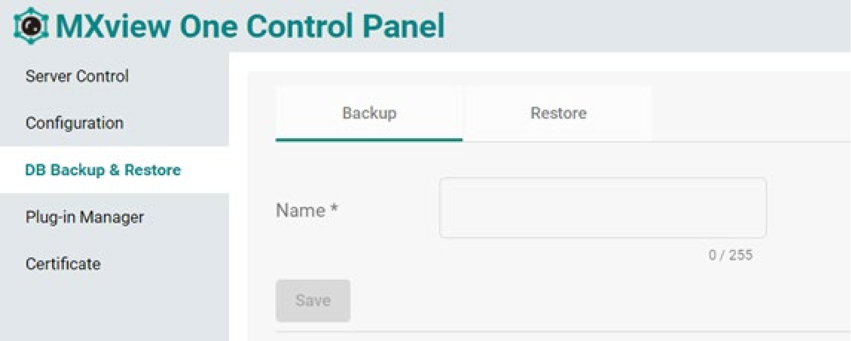
- **Web Interface**
  - **HTTPS:** Specify the HTTPS port of the MXview One Central Manager server. The default port is 443.
  - **HTTP:** Enable or disable HTTP. If enabled, specify the listening port of the server. The default port is 80.
- **Database Interface**
  - **Port:** Specify the service port of the MXview One Central Manager database server. The default port is 5432.
  - **Password:** The password used to connect to MXview One Central Manager. While the default password is randomized, we strongly recommend you to change the password to enhance security.
- **Microservices Interface**
  - **Internal Service Port 1/2:**
    1. **Port:** Specify the communication ports between MXview One and its internal system. The default ports are 8883 and 8882.
    2. **Password:** The password used for the microservices interface. While the default password is randomized, we strongly recommend you changing the password to enhance security.
  - **Security Add-on Service Port:**
    1. **Auto Binding**: Enable or disable the auto-binding feature. When enabled, MXview One will automatically select a random port number for the Security add-on module if the default port number is already in use.
    2. **Port**: Specify the service port of the Security add-on module.

When finished, click **Save**.

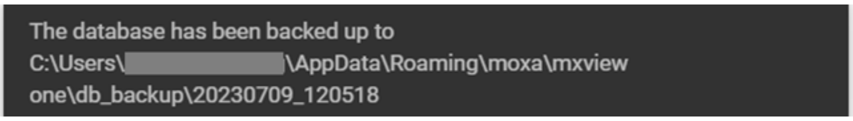
DB Backup & Restore

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.

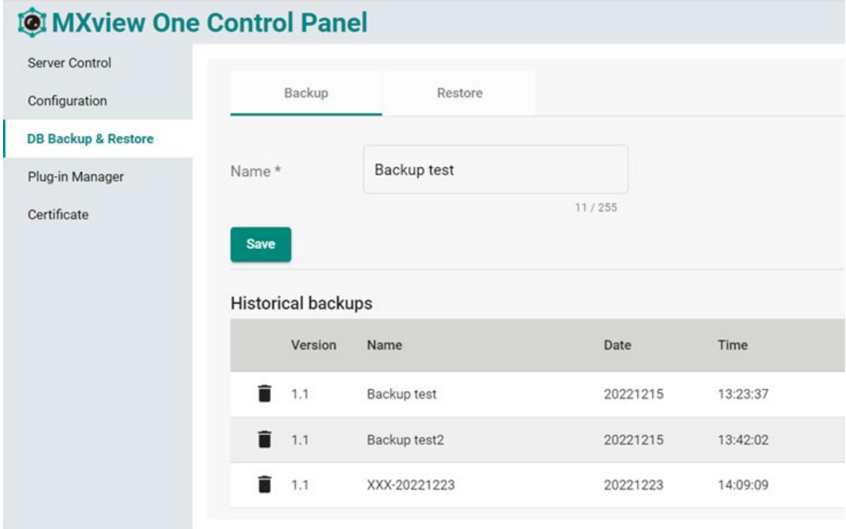


2. Choose the **Backup** tab to start the process of backing up the database.
3. In the **Name** field, specify the backup file name.
4. Click **Save**.
5. The message that the file of the backup database has been stored in the specified directory will be displayed.



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

Historical backups

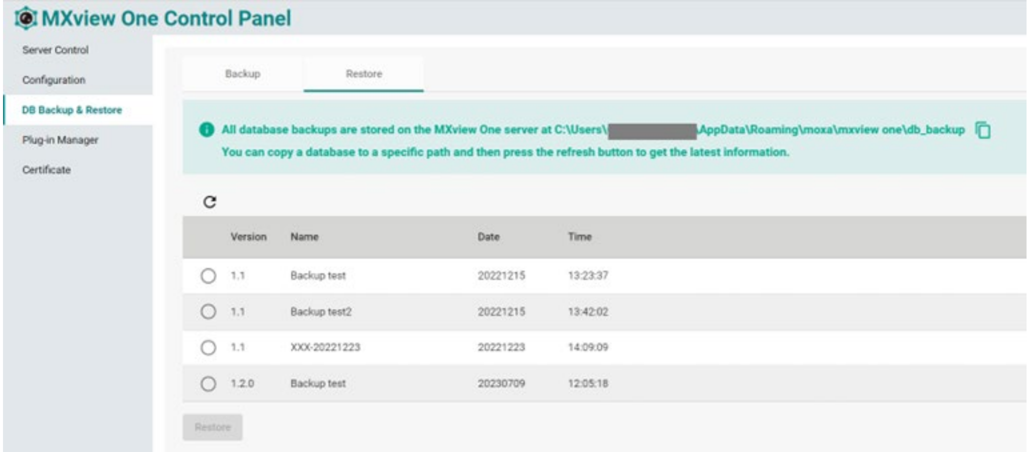
	Version	Name	Date	Time
🗑	1.1	Backup test	20221215	13:23:37
🗑	1.1	Backup test2	20221215	13:42:02
🗑	1.1	XXX-20221223	20221223	14:09:09

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.



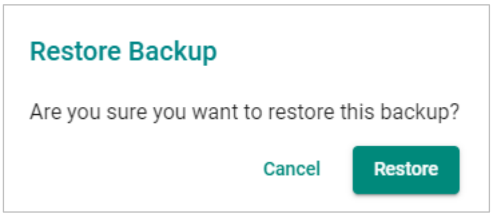
All database backups are stored on the MXview One server at C:\Users\[redacted]AppData\Roaming\moxa\mxview one\db_backup
You can copy a database to a specific path and then press the refresh button to get the latest information.

	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**.

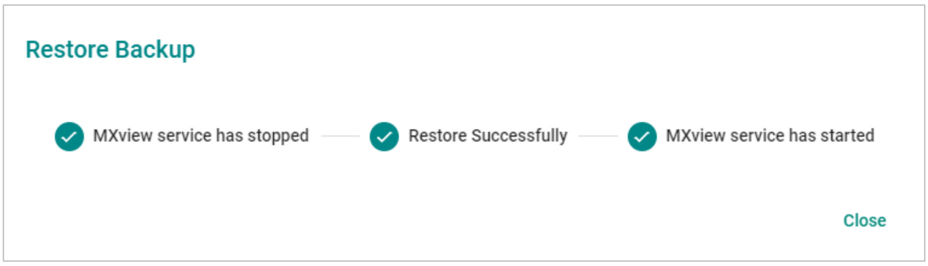
   A confirmation screen will appear.



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

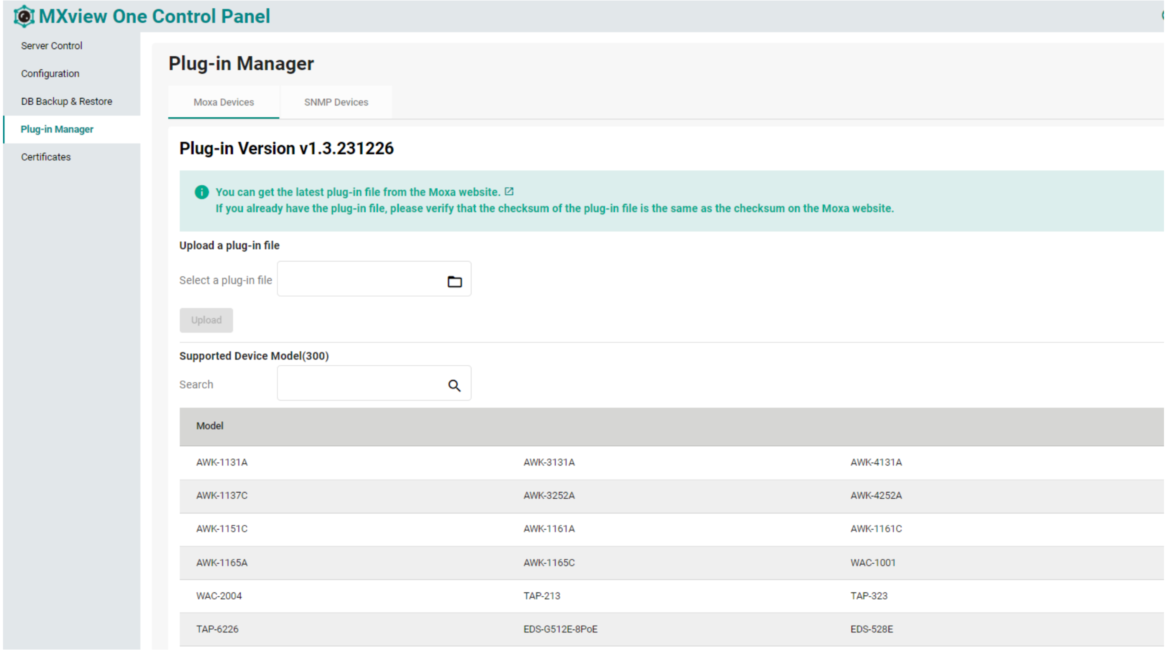
Navigate to **Plug-in Manager** on the **Control Panel**. The Plug-in Manager is a tool that can be used to manage the plug-in files. The **Plug-in Manager** screen features two tabs: **Moxa Devices** and **SNMP Devices**.

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 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

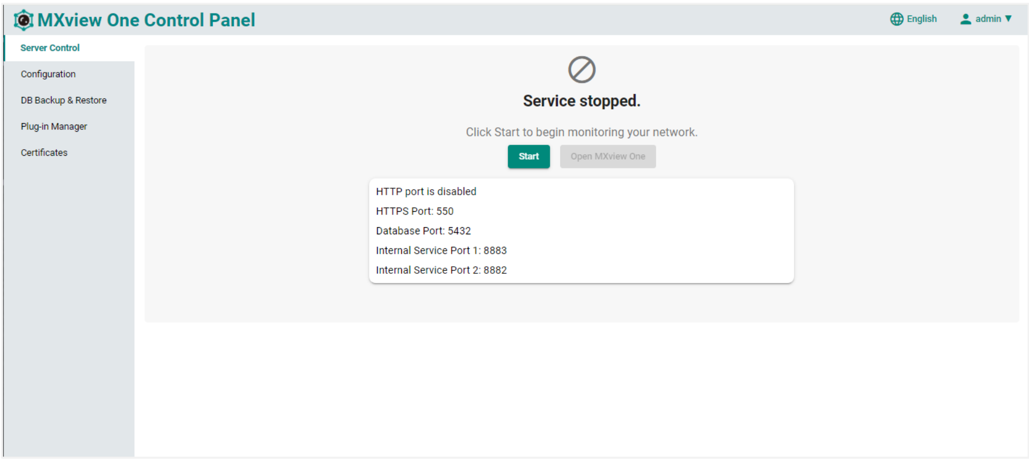
Select a plug-in file

Supported Device Model(300)

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.



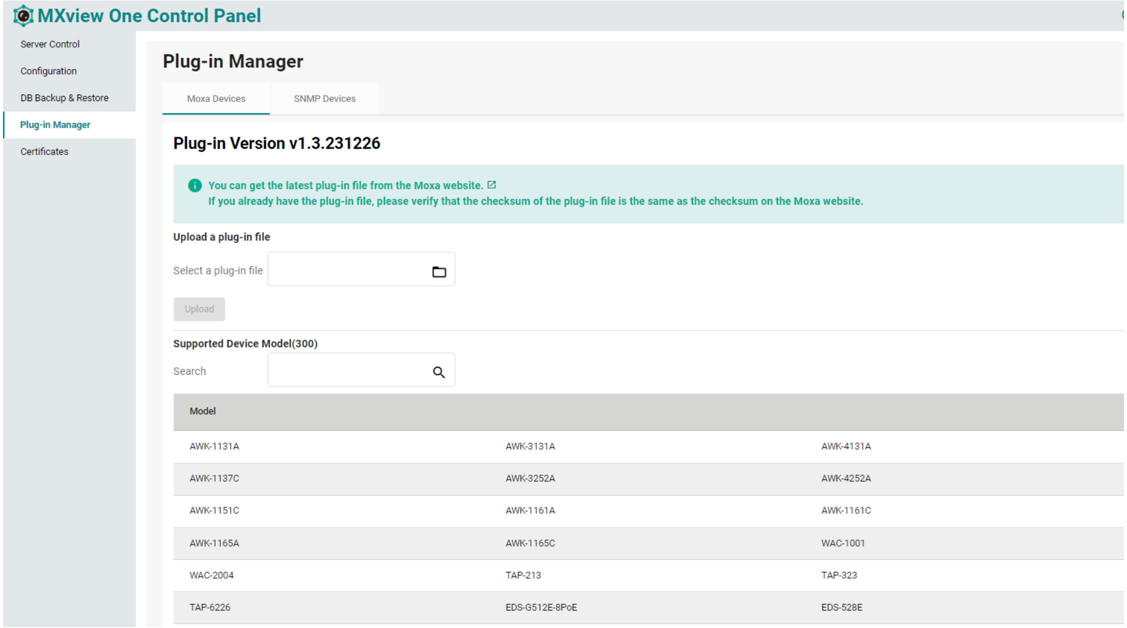
Service stopped.

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 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

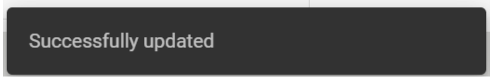
Select a plug-in file

Supported Device Model(300)

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.

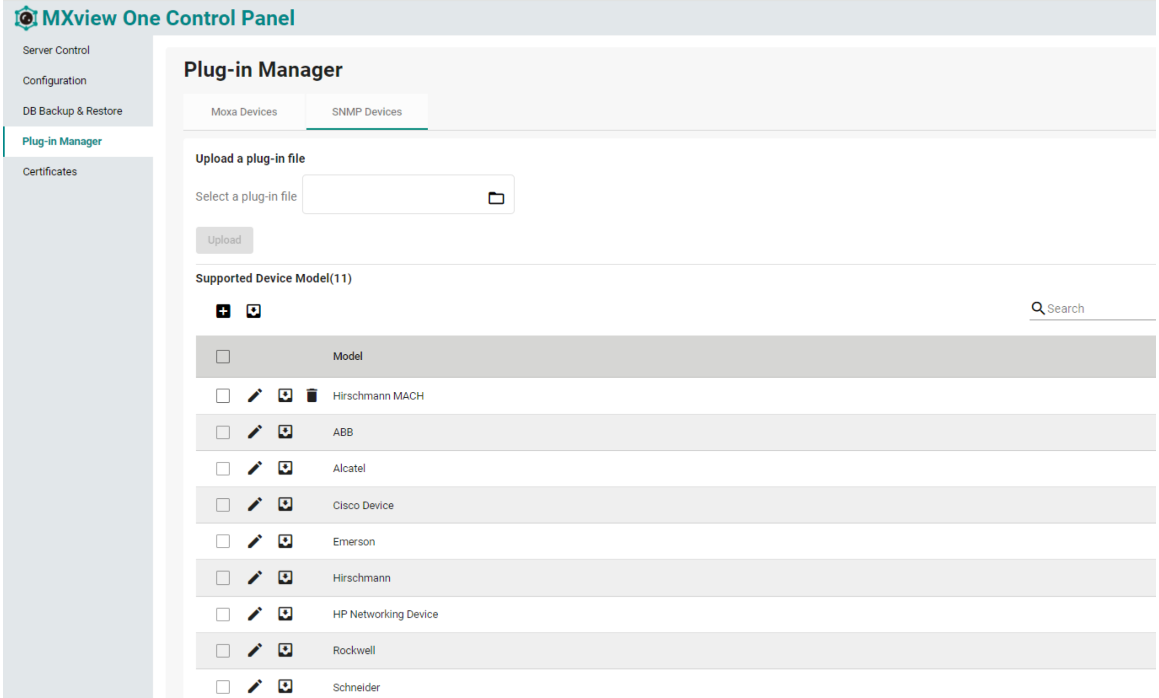


Successfully updated

SNMP Devices

By default, MXview One will show basic information for third-party SNMP devices by polling the RFC-1213 public MIB and does not require users to upload device plug-in files. MXview One can also monitor the status of these SNMP devices.

To show more detailed information for third-party SNMP devices in MXview One, users can create an SNMP device plug-in by uploading the device’s private MIB files and defining the OID and OID syntax mapping.



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

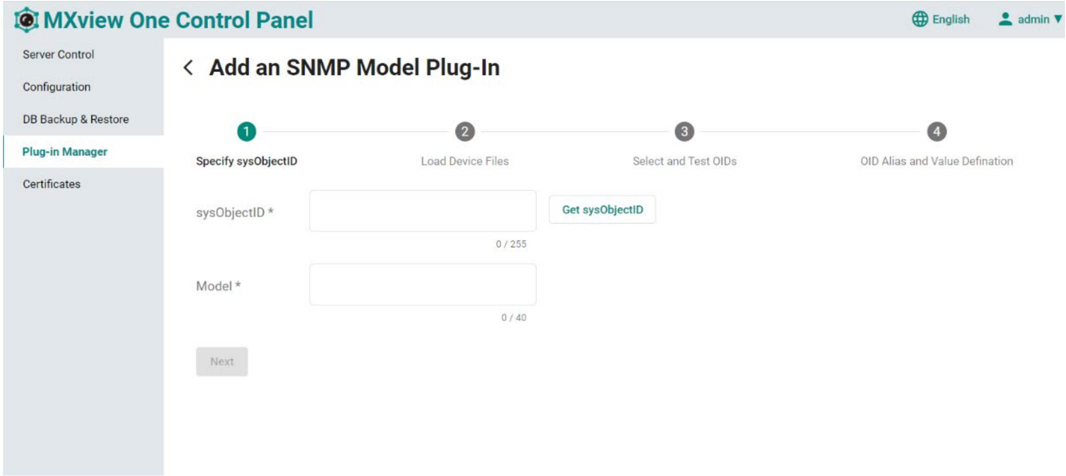
The tab SNMP Devices includes the following information:

- Upload a plug-in file: This function allows users to upload plug-in files for third-party SNMP devices.
- 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.



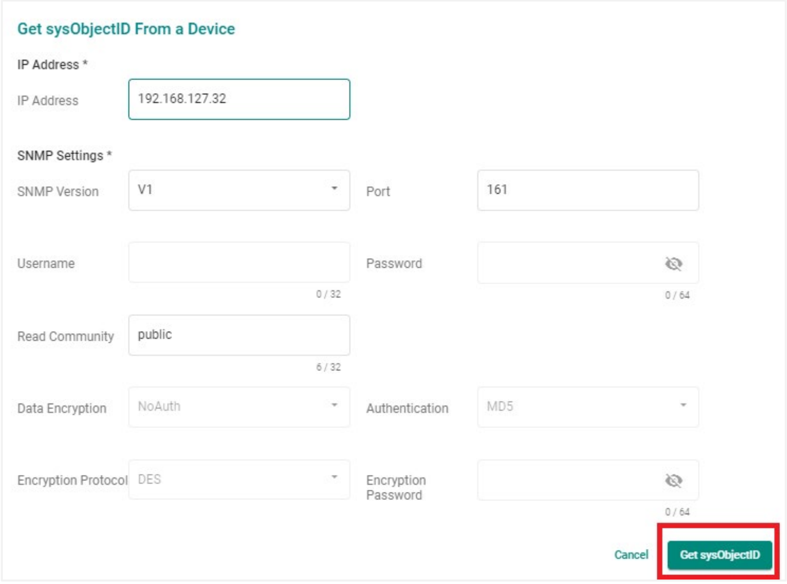
sysObjectID * 0 / 255

Model * 0 / 40

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.



IP Address *

IP Address: 192.168.127.32

SNMP Settings *

SNMP Version: V1

Port: 161

Username: 0 / 32

Password: 0 / 64

Read Community: public 6 / 32

Data Encryption: NoAuth

Authentication: MD5

Encryption Protocol: DES

Encryption Password: 0 / 64

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.

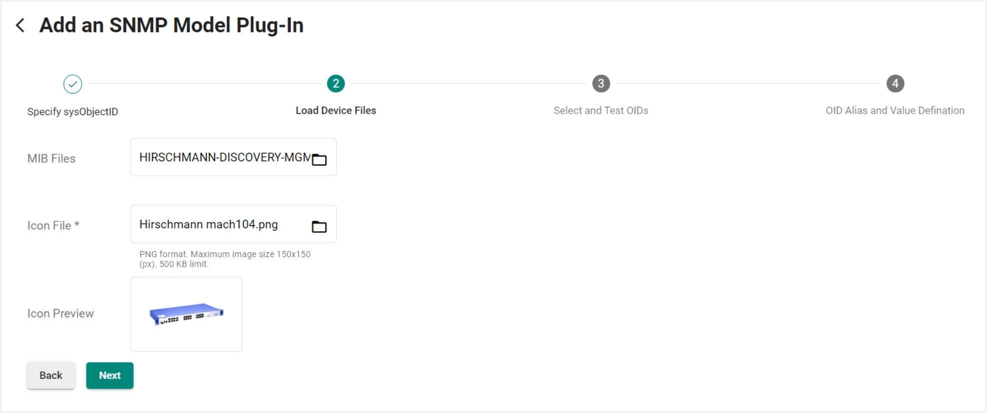
   b. When finished, click **Next**.

4. Load Device Files.

   a. **MIB Files**: Upload all the necessaryYou 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

MIB Files: HIRSCHMANN-DISCOVERY-MGM

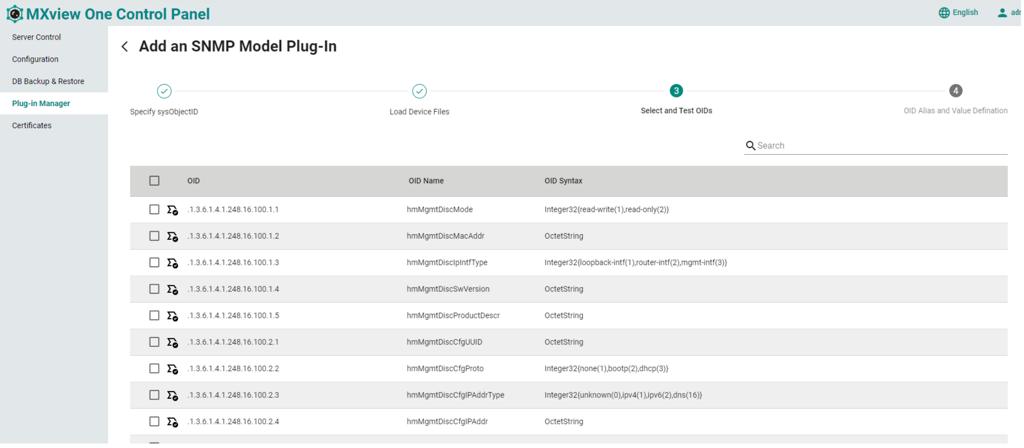
Icon File *: Hirschmann mach104.png

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

Icon Preview

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.



Add an SNMP Model Plug-In

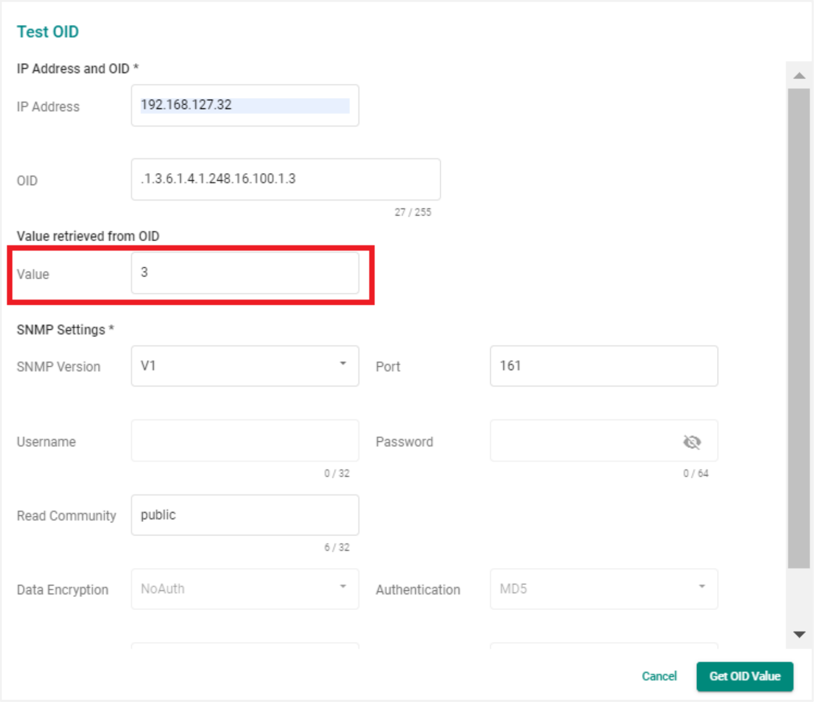
	OID	OID Name	OID Syntax
□ Σ	.1.3.6.1.4.1.248.16.100.1.1	hmMgmtDiscMode	Integer32{read-write(1),read-only(2)}
□ Σ	.1.3.6.1.4.1.248.16.100.1.2	hmMgmtDiscMacAddr	OctetString
□ Σ	.1.3.6.1.4.1.248.16.100.1.3	hmMgmtDiscIpIntfType	Integer32{loopback-intf(1),router-intf(2),mgmt-intf(3)}
□ Σ	.1.3.6.1.4.1.248.16.100.1.4	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)

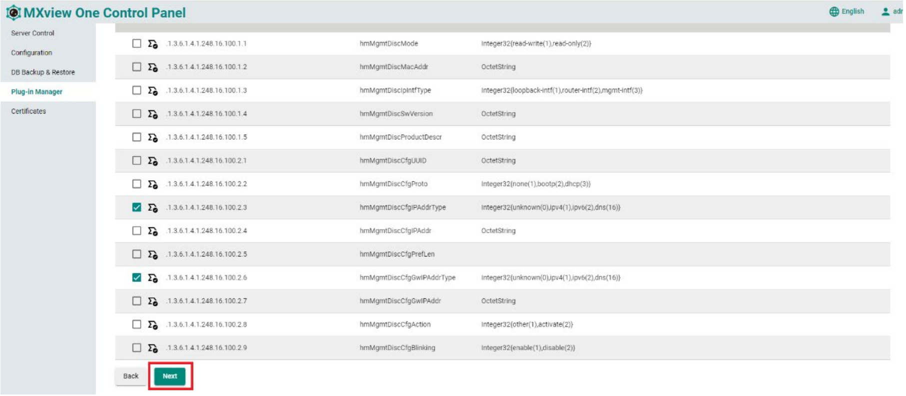
Data Encryption: NoAuth

Authentication: MD5

b. Select OIDs.

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

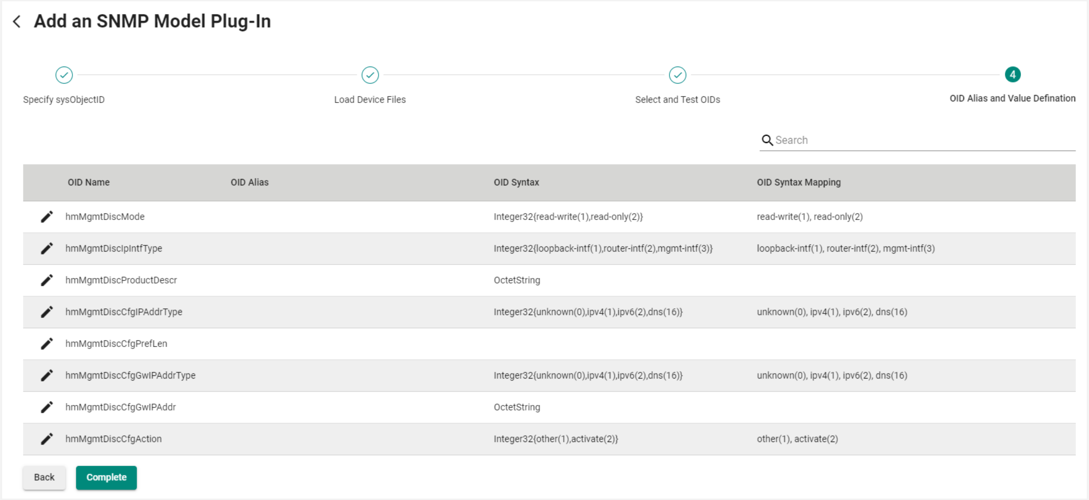
ii. When finished, click **Next**.



☐	.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.

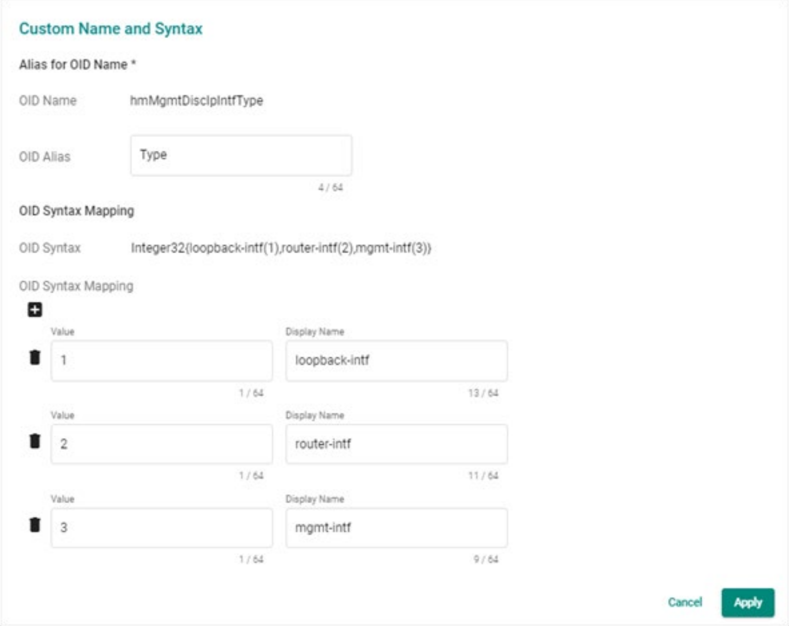


Add an SNMP Model Plug-In

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)

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)}

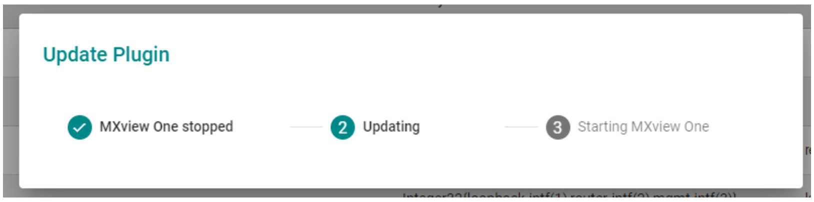
OID Syntax Mapping

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

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

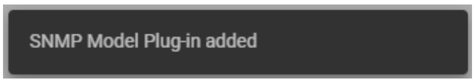
c. When finished, click **Apply**.

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



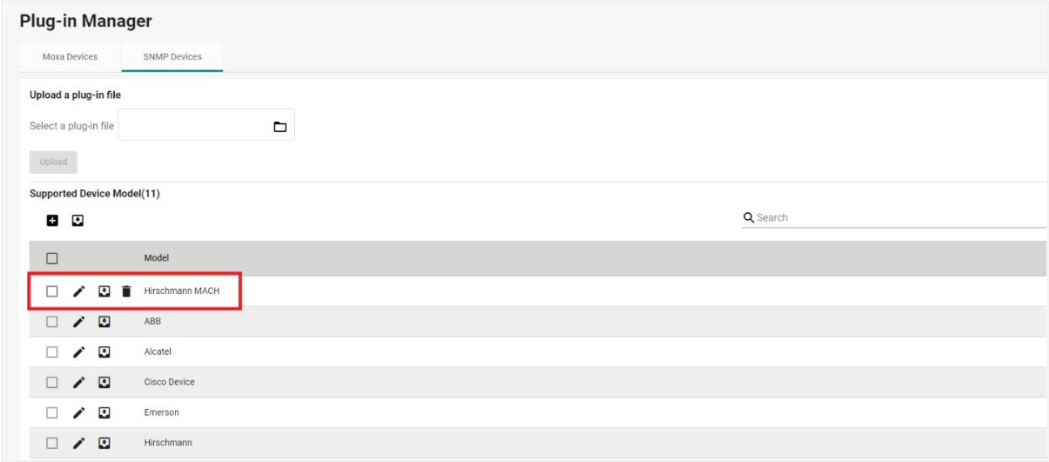
Update Plugin

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

Upload a plug-in file

Select a plug-in file

Supported Device Model(11)

Model
Hirschmann MACH
ABB
Alcatel
Cisco Device
Emerson
Hirschmann

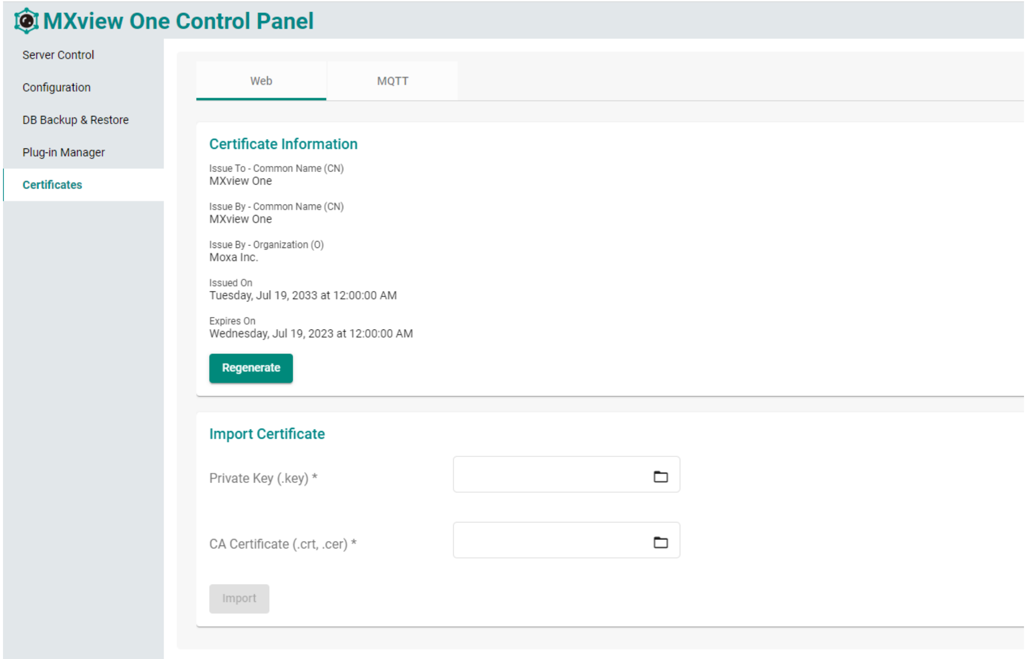
Certificates

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

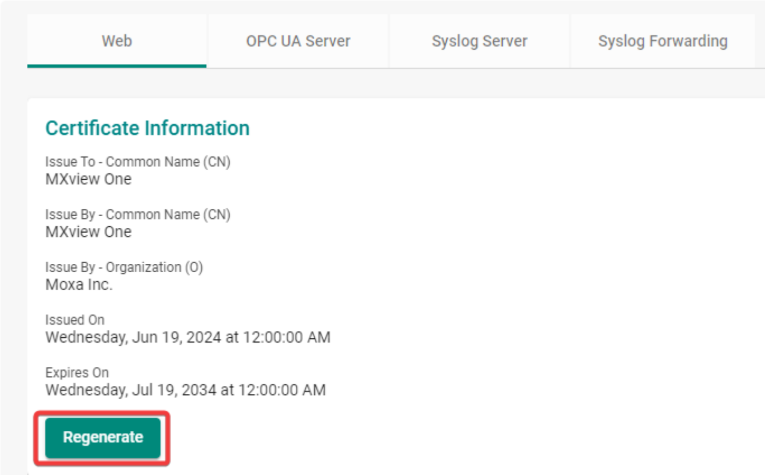
Private Key (.key) *

CA Certificate (.crt, .cer) *

Regenerating the Web Certificate

1. Navigate to **Control Panel > Certificates.**
2. Go to the **Web** tab.
3. Click the **Regenerate** button.

   The **Regenerate Certificate** window will appear.



Certificate Information

Issue To - Common Name (CN)
MXview One

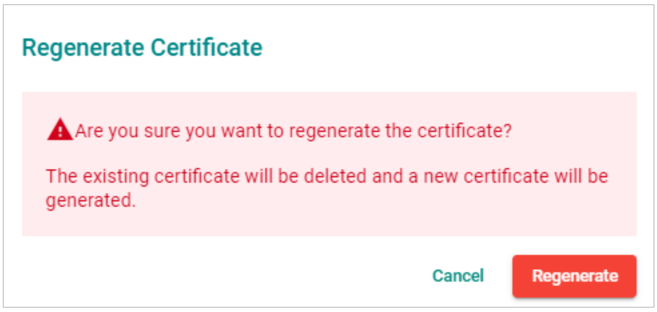
Issue By - Common Name (CN)
MXview One

Issue By - Organization (O)
Moxa Inc.

Issued On
Wednesday, Jun 19, 2024 at 12:00:00 AM

Expires On
Wednesday, Jul 19, 2034 at 12:00:00 AM

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

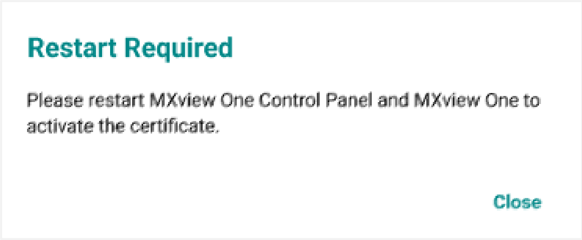


Regenerate Certificate

Are you sure you want to regenerate the certificate?

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

5. 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.



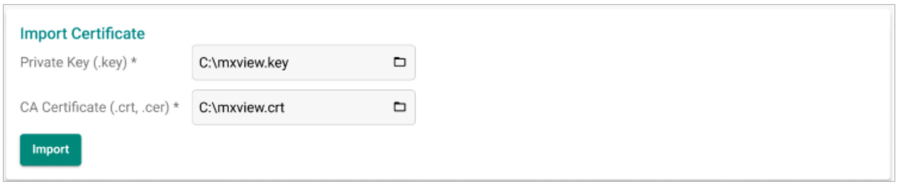
Restart Required

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

Importing a Web Certificate

You can manually important a certificate file and key file.

1. Navigate to **Control Panel > Certificates.**
2. Go to the **Web** tab.
3. In the **Import Certificate** section, 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.

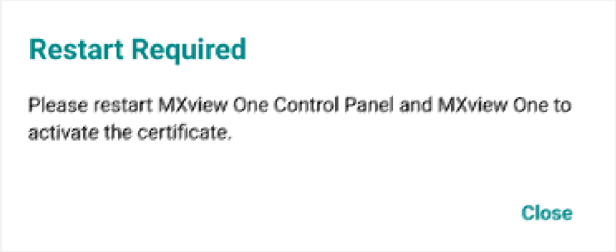


Import Certificate

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

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

4. Click **Import**.
5. 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.

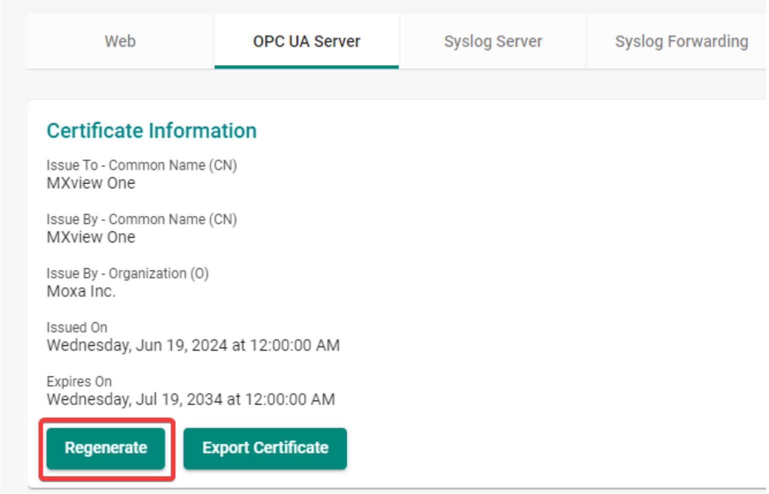
OPC UA Server Certificates

On the **OPC UA Server** tab, you can view the information for the current OPC UA certificates, including:

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

Regenerating the OPC UA Server Certificate

1. Navigate to **Control Panel > Certificates**.
2. Go to the **OPC UA Server** tab.
3. Click the **Regenerate** button.
   The **Regenerate Certificate** window will appear.



Certificate Information

Issue To - Common Name (CN)
MXview One

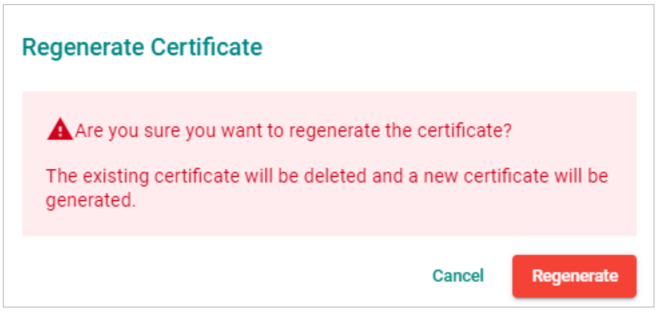
Issue By - Common Name (CN)
MXview One

Issue By - Organization (O)
Moxa Inc.

Issued On
Wednesday, Jun 19, 2024 at 12:00:00 AM

Expires On
Wednesday, Jul 19, 2034 at 12:00:00 AM

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

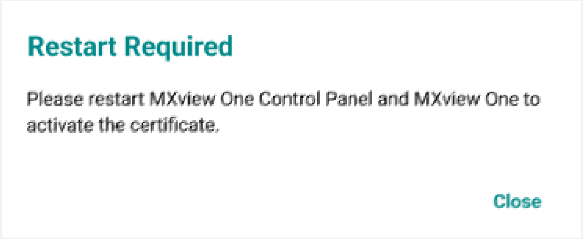


Regenerate Certificate

⚠ Are you sure you want to regenerate the certificate?

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

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

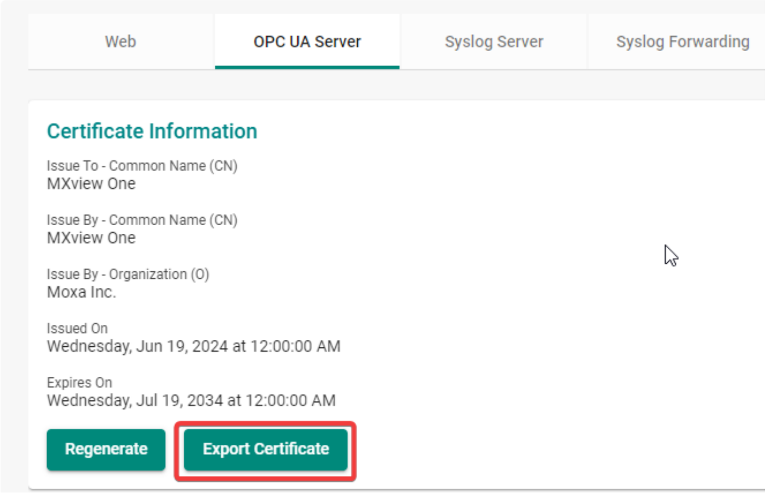


Restart Required

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

Exporting the OPC UA Server Certificate

1. Navigate to **Control Panel > Certificates**.
2. Go to the **OPC UA Server** tab.
3. Click the **Export Certificate** button.
   MXview One will export the OPC UA certificate as a ZIP file.



Certificate Information

Issue To - Common Name (CN)
MXview One

Issue By - Common Name (CN)
MXview One

Issue By - Organization (O)
Moxa Inc.

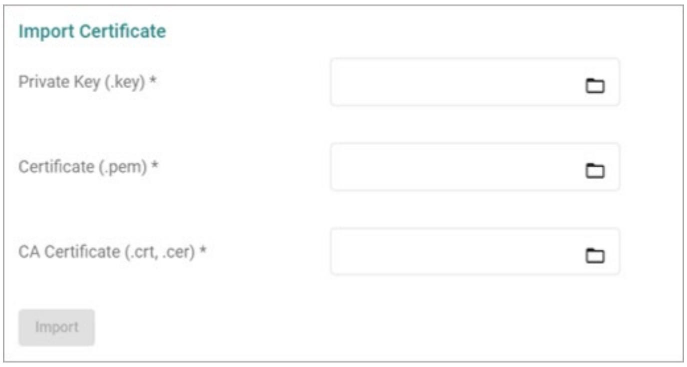
Issued On
Wednesday, Jun 19, 2024 at 12:00:00 AM

Expires On
Wednesday, Jul 19, 2034 at 12:00:00 AM

Importing an OPC UA Server Certificate

1. Navigate to **Control Panel > Certificates.**
2. Go to the **OPC UA Server** tab.
3. In the **Import Certificate** section, click the folder icon for the Private Key, Certificate, and CA Certificate fields and navigate to the CA certificate (.crt, .cer), certificate (.pem), and key (.key) file on

the local host.



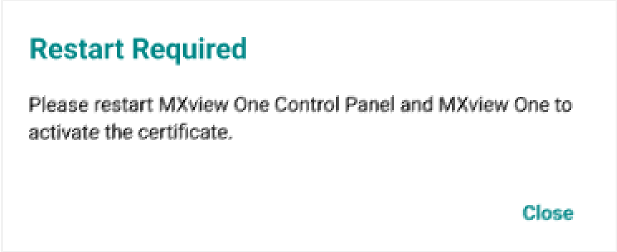
Import Certificate

Private Key (.key) *

Certificate (.pem) *

CA Certificate (.crt, .cer) *

4. Click **Import**.
5. 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.



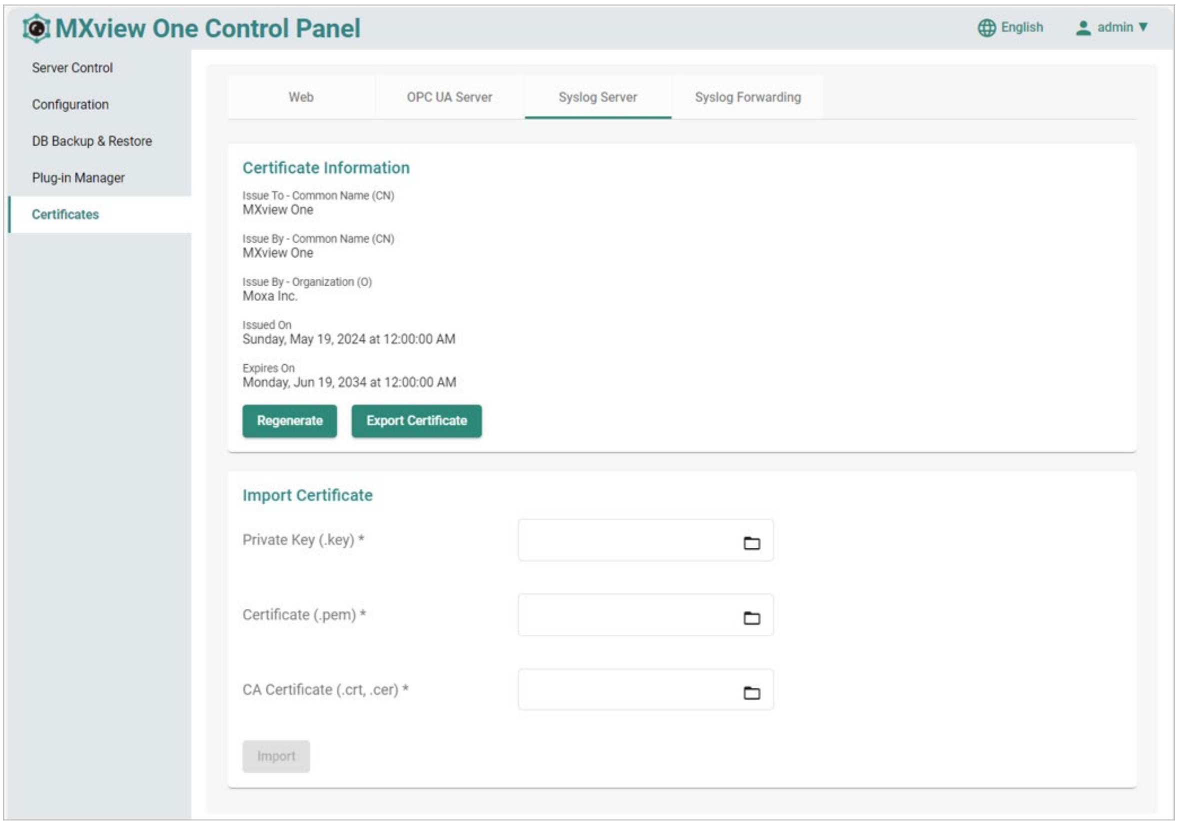
Restart Required

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

Syslog Server Certificates

On the **Syslog Server** tab, you can view the information for the current syslog server 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
Sunday, May 19, 2024 at 12:00:00 AM

Expires On
Monday, Jun 19, 2034 at 12:00:00 AM

Import Certificate

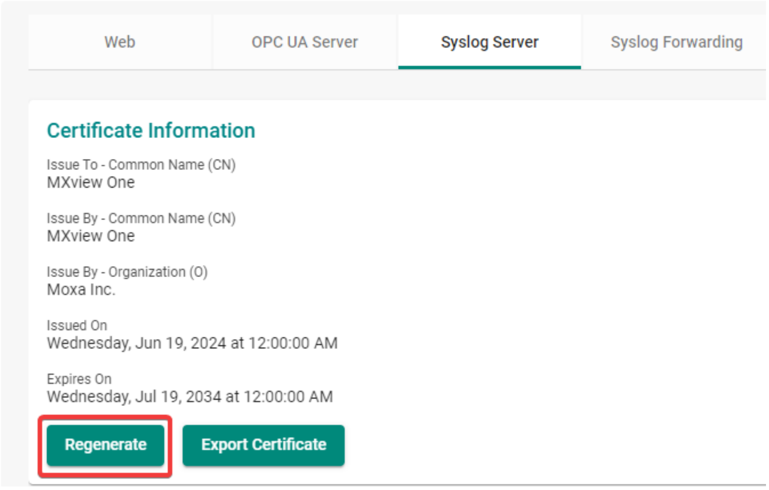
Private Key (.key) *

Certificate (.pem) *

CA Certificate (.crt, .cer) *

Regenerating the Syslog Server Certificate

1. Navigate to **Control Panel > Certificates**.
2. Go to the **Syslog Server** tab.
3. Click the **Regenerate** button.
   The **Regenerate Certificate** window will appear.



Certificate Information

Issue To - Common Name (CN)
MXview One

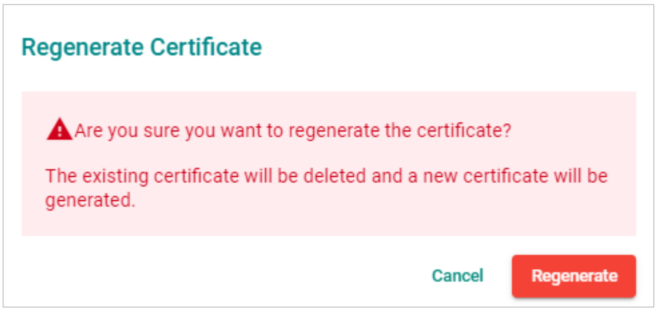
Issue By - Common Name (CN)
MXview One

Issue By - Organization (O)
Moxa Inc.

Issued On
Wednesday, Jun 19, 2024 at 12:00:00 AM

Expires On
Wednesday, Jul 19, 2034 at 12:00:00 AM

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

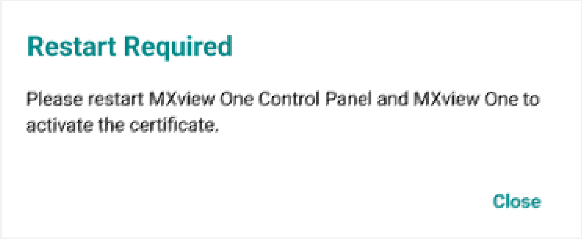


Regenerate Certificate

⚠Are you sure you want to regenerate the certificate?

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

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

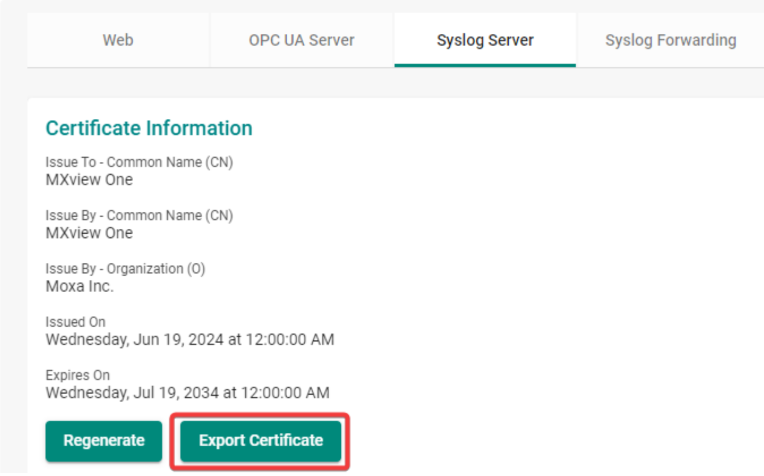


Restart Required

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

Exporting the Syslog Server Certificate

1. Navigate to **Control Panel > Certificates**.
2. Go to the **Syslog Server** tab.
3. Click the **Export Certificate** button.
   MXview One will export the syslog server certificate as a ZIP file.



Certificate Information

Issue To - Common Name (CN)
MXview One

Issue By - Common Name (CN)
MXview One

Issue By - Organization (O)
Moxa Inc.

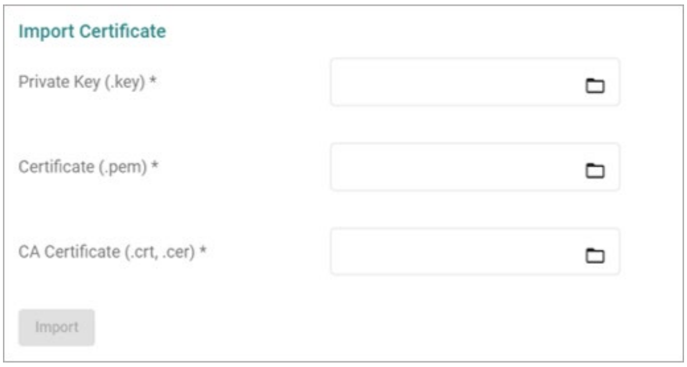
Issued On
Wednesday, Jun 19, 2024 at 12:00:00 AM

Expires On
Wednesday, Jul 19, 2034 at 12:00:00 AM

Importing a Syslog Server Certificate

1. Navigate to **Control Panel > Certificates.**
2. Go to the **Syslog Server** tab.
3. In the **Import Certificate** section, click the folder icon for the Private Key, Certificate, and CA Certificate fields and navigate to the CA certificate (.crt, .cer), certificate (.pem), and key (.key) file on

the local host.



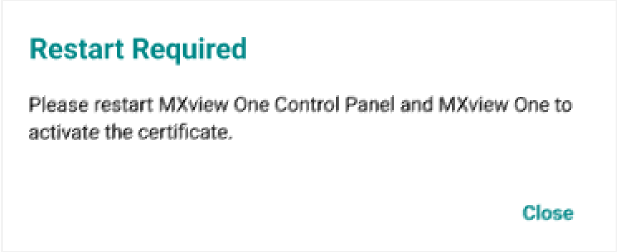
Import Certificate

Private Key (.key) *

Certificate (.pem) *

CA Certificate (.crt, .cer) *

4. Click **Import**.
5. 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.

Syslog Forwarding Certificates

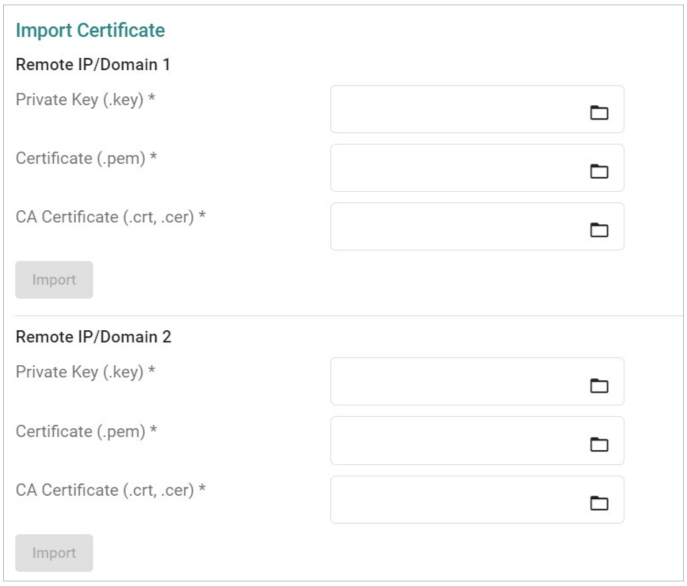
On the **Syslog Forwarding** tab, you can view the information for the current syslog forwarding certificates, including:

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

Importing a Syslog Forwarding Certificate

1. Navigate to **Control Panel > Certificates.**
2. Go to the **Syslog Forwarding** tab.
3. In the **Import Certificate** section, click the folder icon for the Private Key, Certificate, and CA Certificate fields and navigate to the CA certificate (.crt, .cer), certificate (.pem), and key (.key) file on

the local host. Repeat these instructions for both the 1st and 2nd syslog forwarding server.



Import Certificate

Remote IP/Domain 1

Private Key (.key) *

Certificate (.pem) *

CA Certificate (.crt, .cer) *

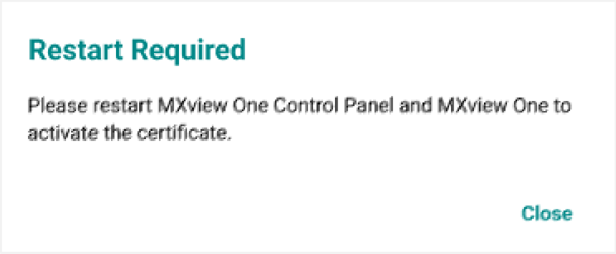
Remote IP/Domain 2

Private Key (.key) *

Certificate (.pem) *

CA Certificate (.crt, .cer) *

4. Click **Import**.
5. 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.

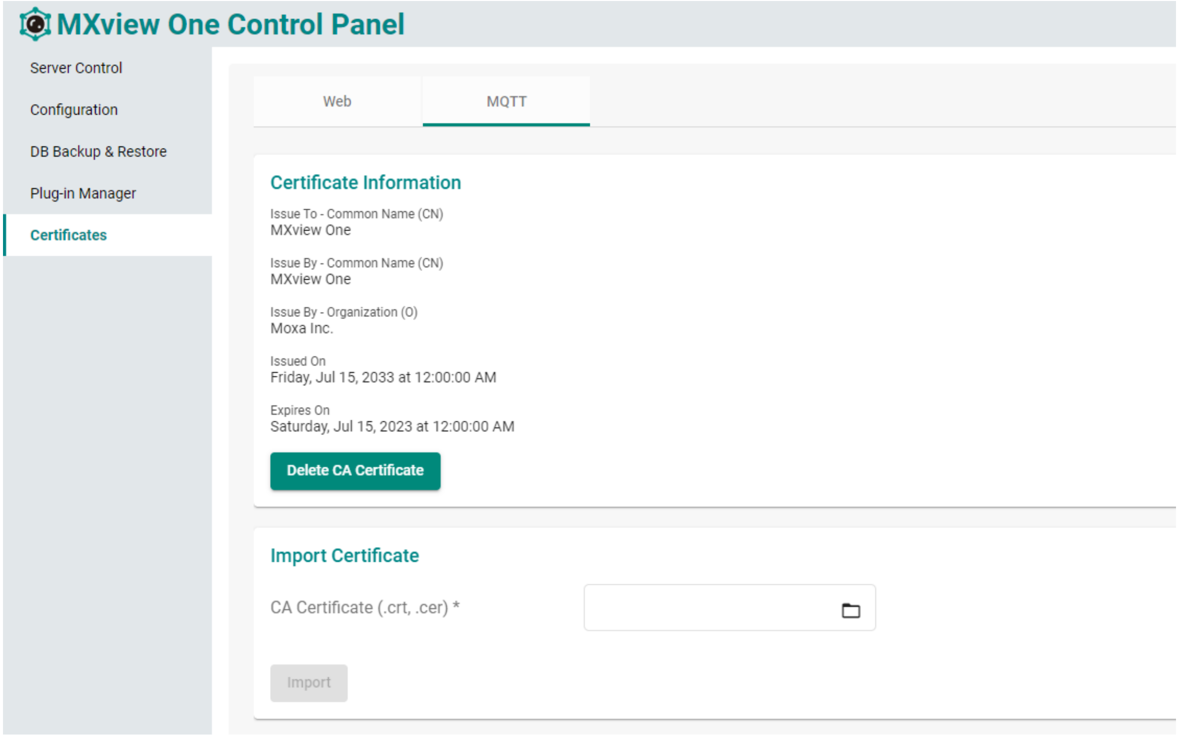
MQTT Certificates

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.

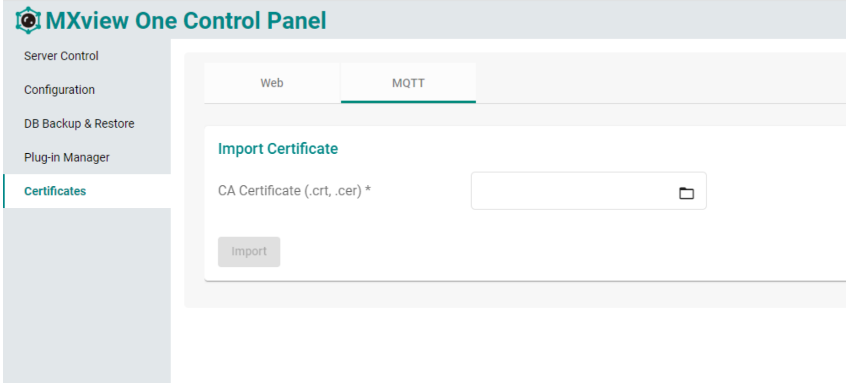
Issued On
Friday, Jul 15, 2033 at 12:00:00 AM

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

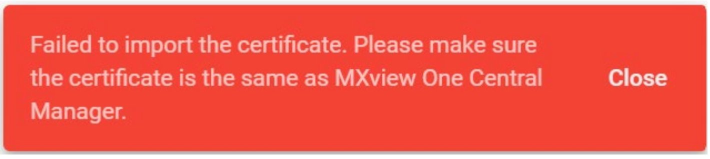
Importing the MXview One Central Manager CA Certificate

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.

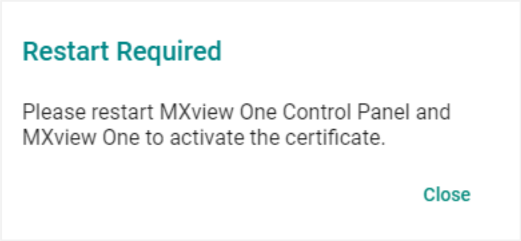


If the uploaded certificate is not from Central Manager, an error message will appear.



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.

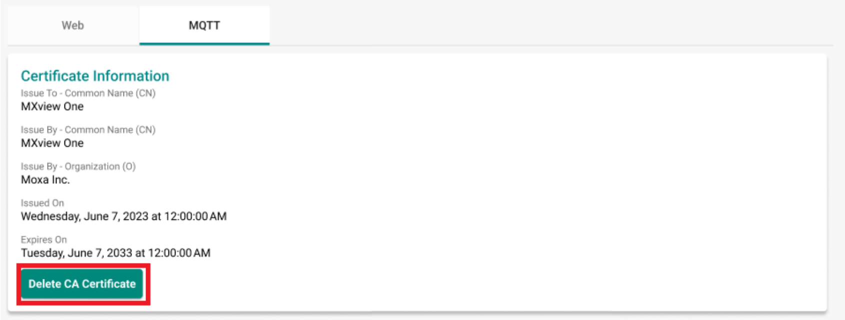


Restart Required

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

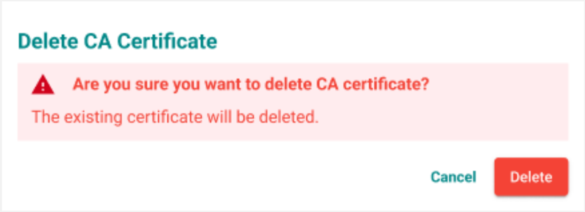
Issue By - Common Name (CN)
MXview One

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**.

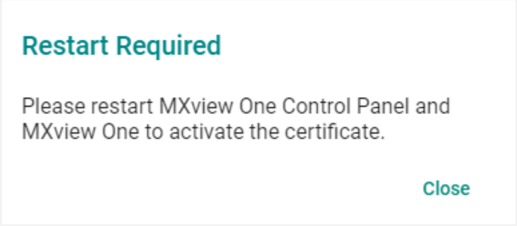


Delete CA Certificate

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.

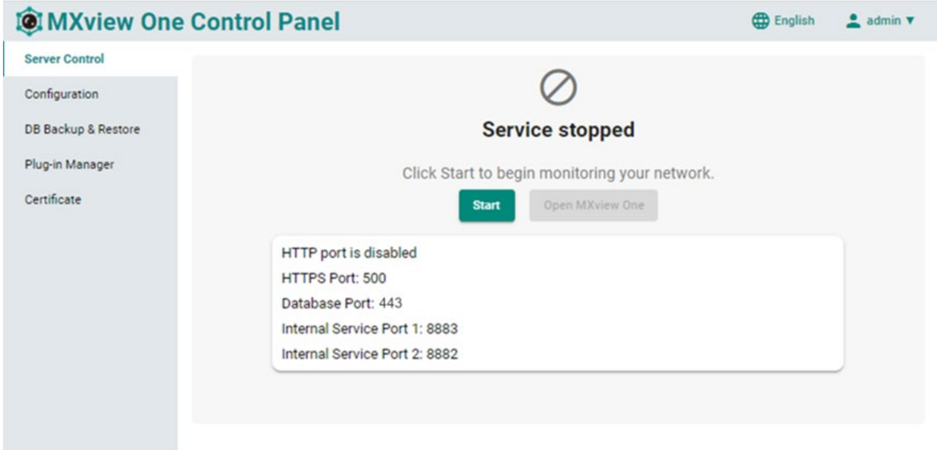


Restart Required

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

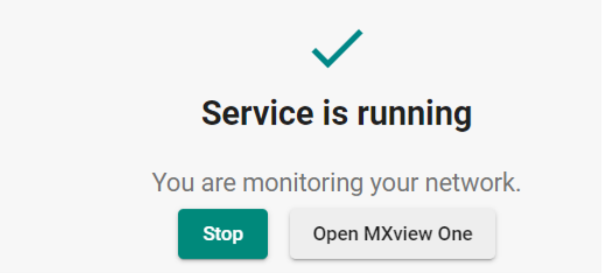
Starting the MXview One Server and Logging Into MXview One

1. On the **Server Control** page, click **Start**. The MXview One server will start running.

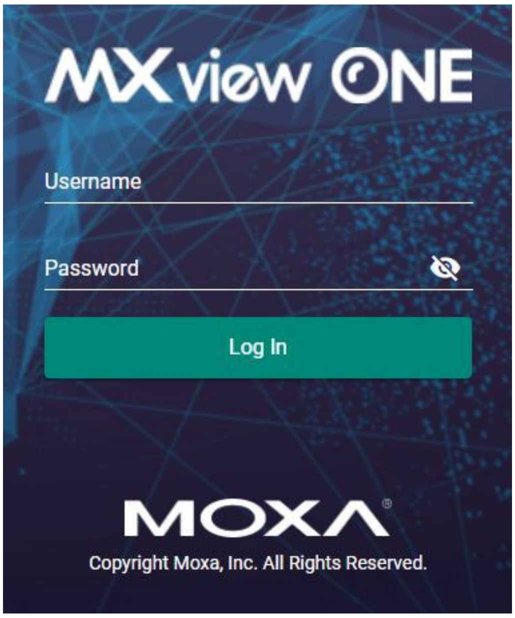


HTTP port is disabled
HTTPS Port: 500
Database Port: 443
Internal Service Port 1: 8883
Internal Service Port 2: 8882

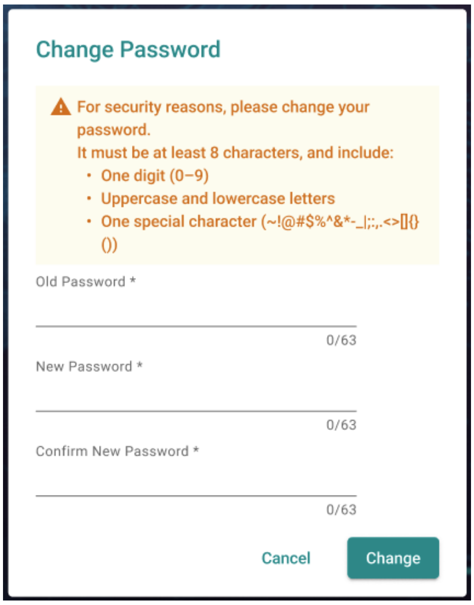
2. Wait for the status to display **Service is running**, then click **Open MXview One**.



3. Enter the login credentials and click **Log In**.
   - Default username: **admin**
   - Default password: **moxa**



4. When logging in using the default credentials. the **Change Password** screen will appear. Enter the old password and specify the new password.



Change Password

For security reasons, please change your password.
It must be at least 8 characters, and include:

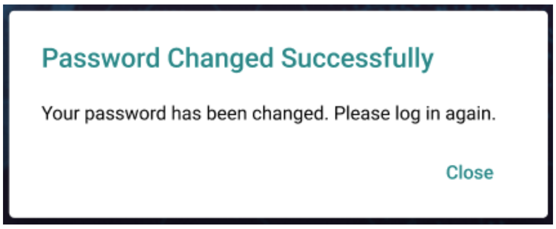
- One digit (0–9)
- Uppercase and lowercase letters
- One special character (~!@#$%^&*-_|;:,.<>[]{}())

Old Password *
0/63

New Password *
0/63

Confirm New Password *
0/63

5. Click **Change**.
The **Password Changed Successfully** screen will appear.



Password Changed Successfully

Your password has been changed. Please log in again.

6. Click **Close** and log in with the updated password.

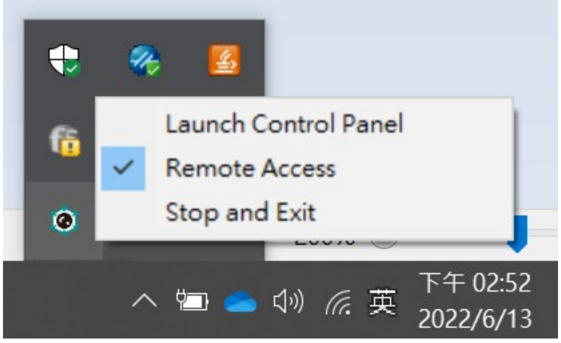
NOTE

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**.

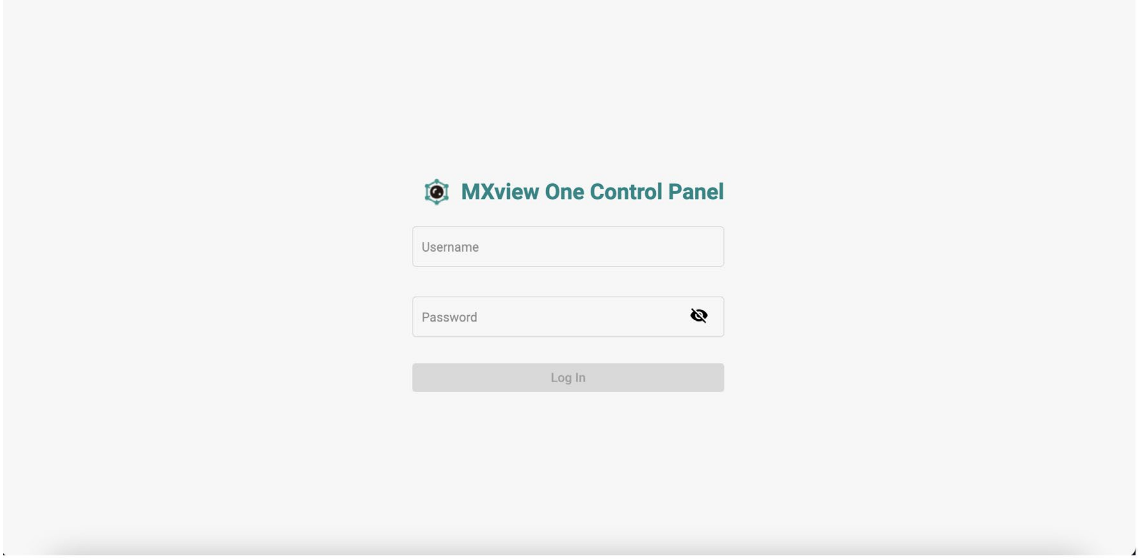


NOTE

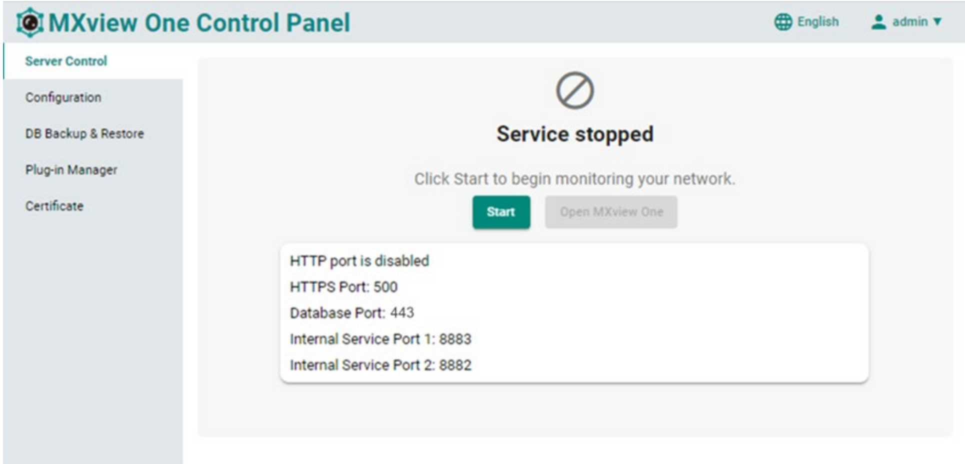
If the **Remote Access** function is enabled, you can access the MXview One Control Panel from another computer. To disable this function, click **Remote Access** again.

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.

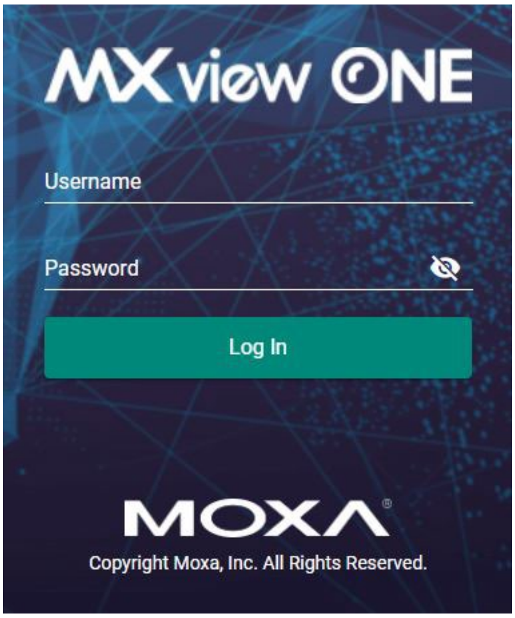
HTTP port is disabled
HTTPS Port: 500
Database Port: 443
Internal Service Port 1: 8883
Internal Service Port 2: 8882

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]**

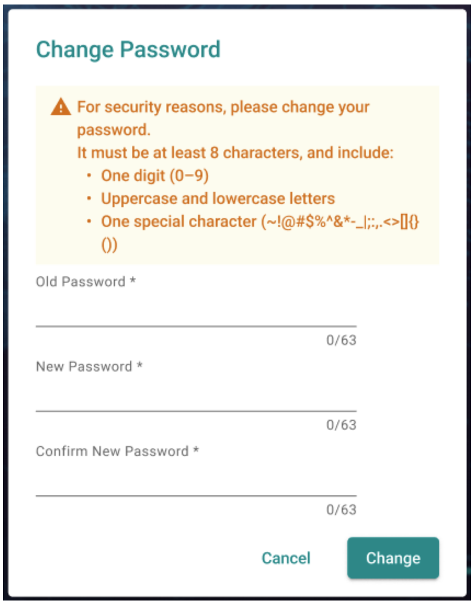
- ➢ Example: https://192.168.1.250

The MXview One web console appears.

7. Enter the login credentials and click **Log In.**
   - ➢ Default username: **admin**
   - ➢ Default password: **moxa**



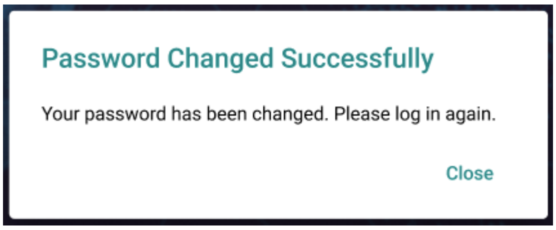
8. When logging in using the default credentials. the **Change Password** screen will appear. Enter the old password and specify the new password.



Change Password

For security reasons, please change your password.
It must be at least 8 characters, and include:
- One digit (0–9)
- Uppercase and lowercase letters
- One special character (~!@#$%^&*-_|;:,.<>[]{}())

9. Click **Change**.
   The **Password Changed Successfully** screen will appear.



Password Changed Successfully

Your password has been changed. Please log in again.

10. Click **Close** and log in with the updated password.

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.

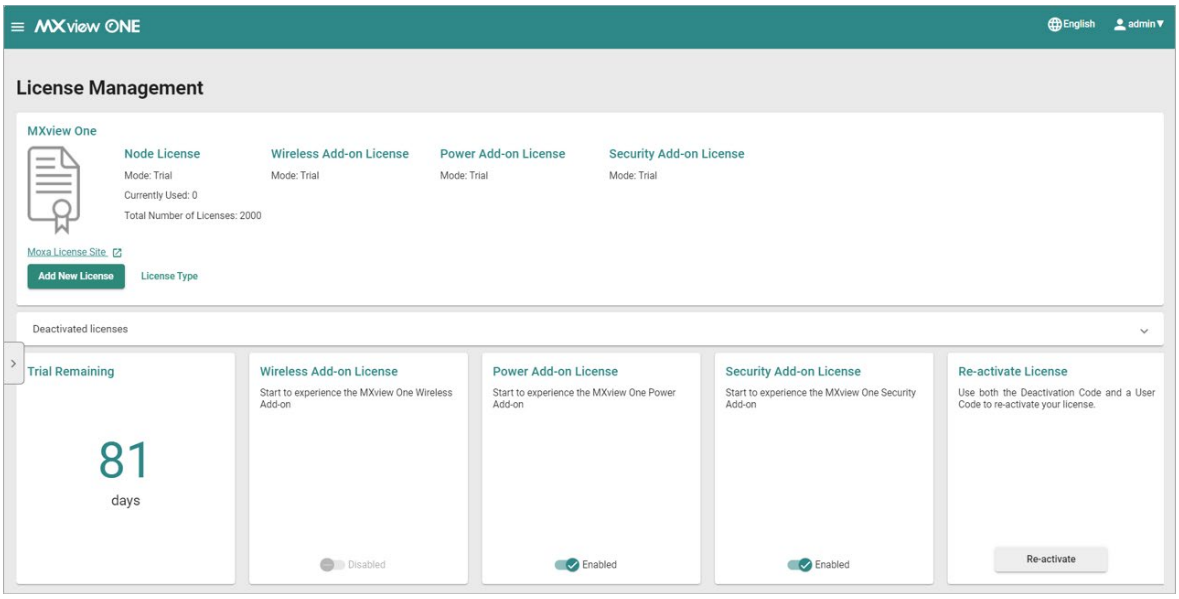
NOTE

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

Node License
Mode: Trial
Currently Used: 0
Total Number of Licenses: 2000

Wireless Add-on License
Mode: Trial

Power Add-on License
Mode: Trial

Security Add-on License
Mode: Trial

Trial Remaining
81
days

Wireless Add-on License
Start to experience the MXview One Wireless Add-on
Disabled

Power Add-on License
Start to experience the MXview One Power Add-on
Enabled

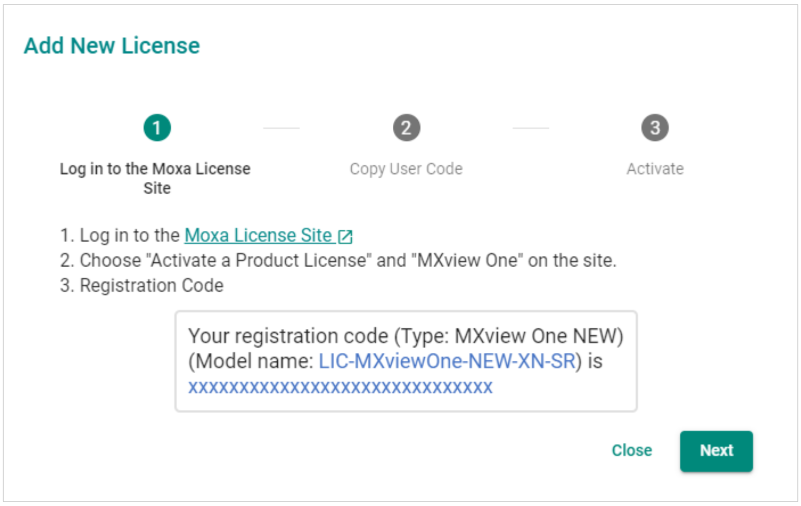
Security Add-on License
Start to experience the MXview One Security Add-on
Enabled

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.

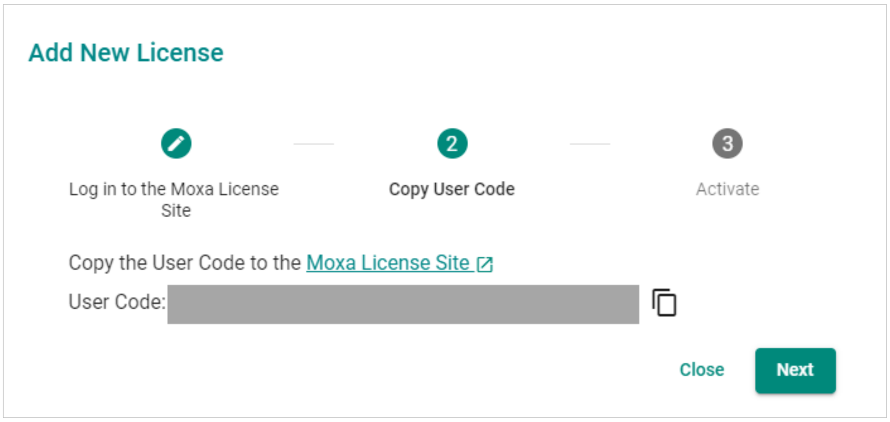
1. Navigate to **Menu** (☰) **> Administration > License Management**.
   The **License Management** screen appears.
   In the **Add New License** section, click **Add New License**.
2. Login to the Moxa License Site to activate the MXview One license. Click **Next** to get the User Code.



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 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

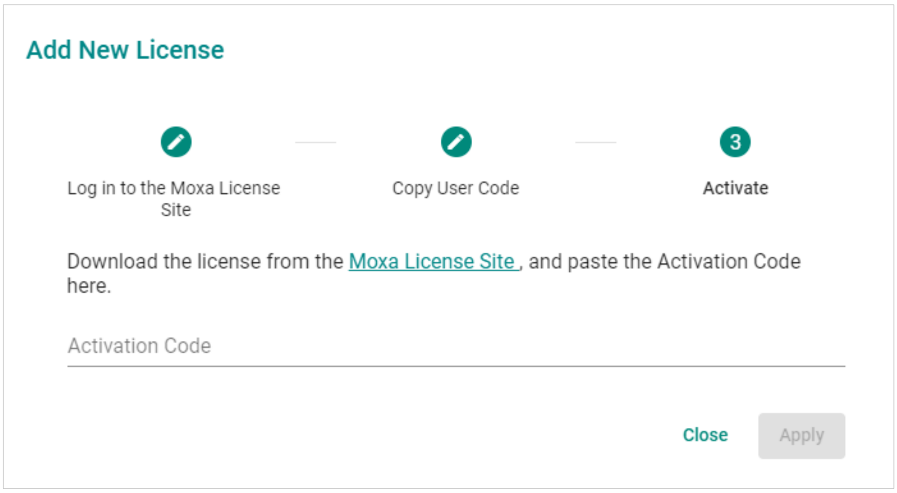
3. Copy the User Code.



Copy the User Code to the Moxa License Site

User Code: [redacted]

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.

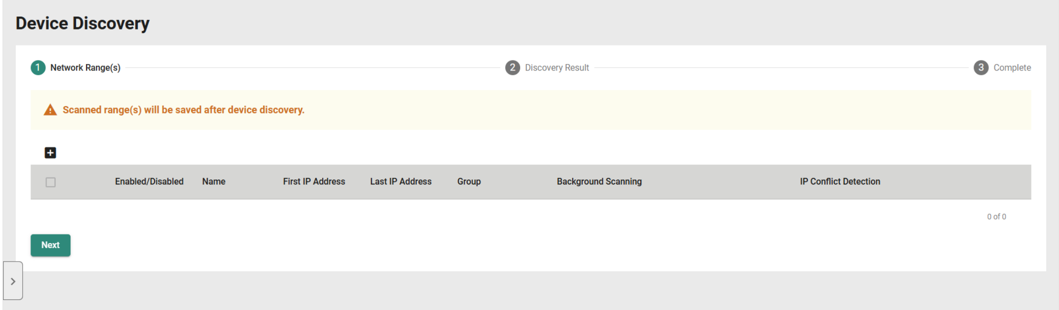
Using Device Discovery

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

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

□	Enabled/Disabled	Name	First IP Address	Last IP Address	Group	Background Scanning	IP Conflict Detection

0 of 0

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

NOTE

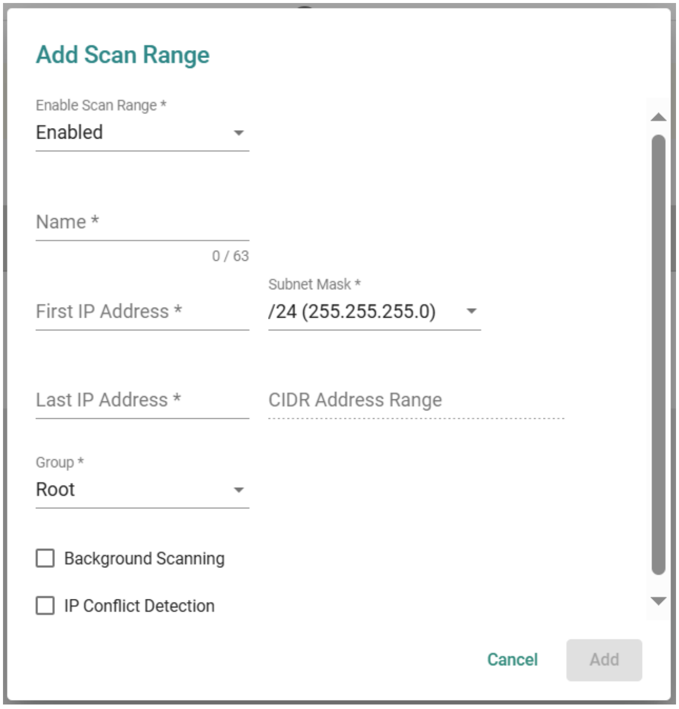
MXview One supports scanning multiple IP address ranges. The selected IP address scan ranges must be enabled in order for MXview One to scan for devices.

NOTE

Moxa devices must have the SNMP function enabled for MXview One to scan the devices.

   a. Click the **Add** (⊞) icon.

The **Add Scan Range** screen appears.



Add Scan Range

Enable Scan Range * Enabled

Name *

0 / 63

First IP Address *

Subnet Mask * /24 (255.255.255.0)

Last IP Address *

CIDR Address Range

Group * Root

□ Background Scanning

□ IP Conflict Detection

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 **Subnet Mask** for the scan range (if applicable).
   - Select the MXview One **Group** to assign the scan range to.
   - Check the **Background Scanning** checkbox (if required). When enabled, MXview One will scan for compatible devices in the background and add them to the topology. An event log will be recorded when a device is added.
   - Check the **IP Conflict Detection** checkbox (if required). When enabled, MXview One will check for IP conflicts among field devices. This feature requires WinPcap/libpcap to be installed.

d. Click **Add**.

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

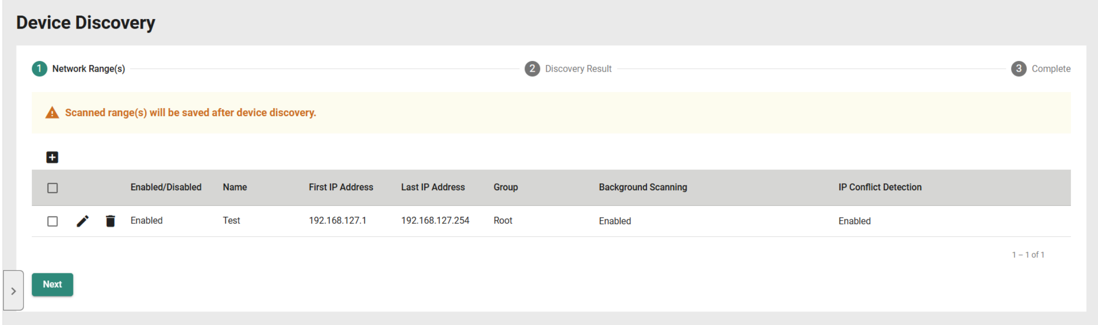
f. (Optional) Modify scan range settings, click the **Edit** (✎) icon next to an added scan range.

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.



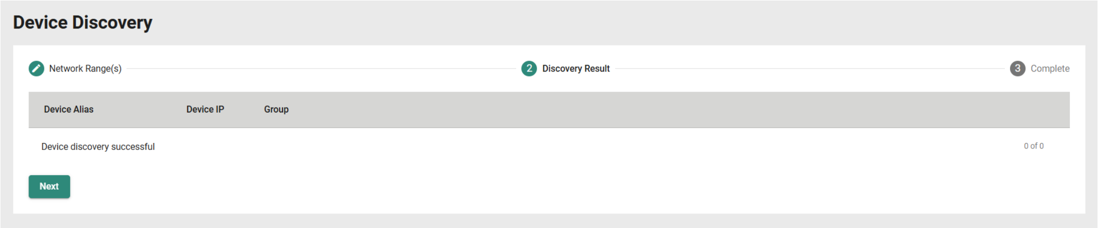
Device Discovery

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

□		Enabled/Disabled	Name	First IP Address	Last IP Address	Group	Background Scanning	IP Conflict Detection
□	✎ 🗑	Enabled	Test	192.168.127.1	192.168.127.254	Root	Enabled	Enabled

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

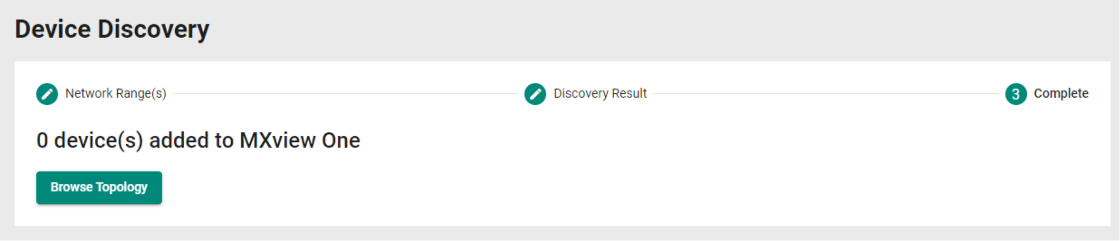
Device Alias	Device IP	Group

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

0 device(s) added to MXview One

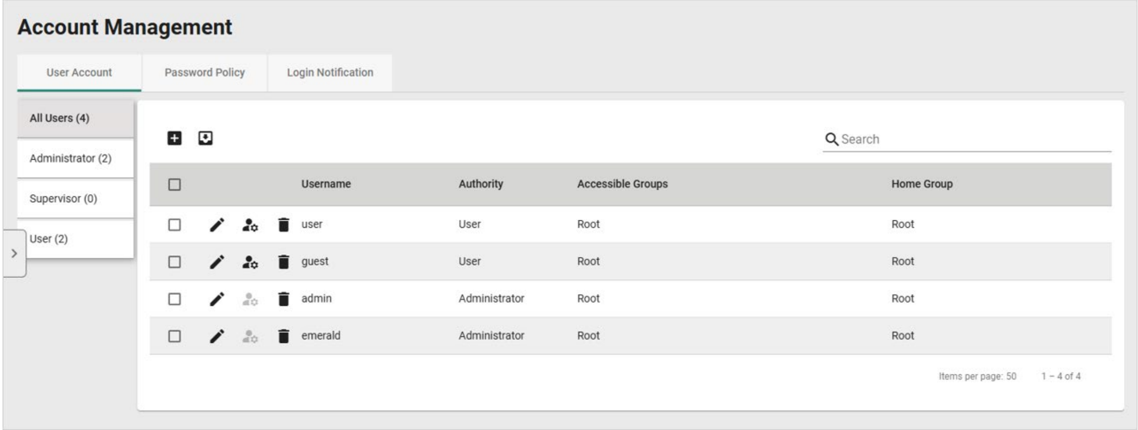
NOTE

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 Groups	Home Group
☐		user	User	Root	Root
☐		guest	User	Root	Root
☐		admin	Administrator	Root	Root
☐		emerald	Administrator	Root	Root

Items per page: 50   1 – 4 of 4

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.

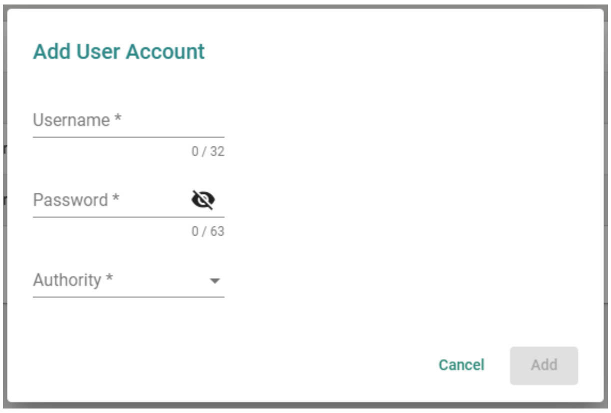
Function	Description
Dashboard	Read-only
Topology	Read-only
Event History	Can do some actions: Export, Filter
Syslog Viewer	Can do some actions: Export, Filter
Inventory Report	Can do some actions: Export
About MXview One	Can check the version
User Manual	Can link to the document
API Documentation	Can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

Adding User Accounts

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

   The **Account Management** screen appears.
2. Go to the **User Account** tab.
3. Click the **Add** (⊞) icon in the top-left corner of the screen.

   The **Add User Account** screen appears.



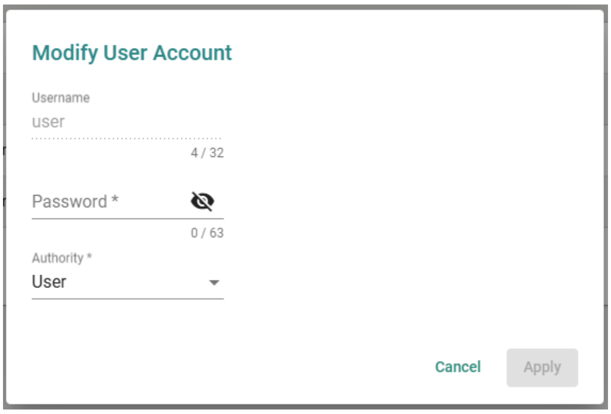
4. Configure the following account details:
   - ➢ **Username:** Specify the username for the account.
   - ➢ **Password:** Specify the login password (minimum length: 4 characters) for the account.
   - ➢ **Authority:** Assign the authority permission (Administrator, Supervisor, or User) for the account.
5. Click **Add**.

Modifying User Accounts

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

The **Account Management** screen appears.

2. Go to the **User Account** tab.
3. Click the **Edit** (✎) icon in front of the account you want to modify.
   The **Modify User Account** screen appears.



Modify User Account

Username
user
4 / 32

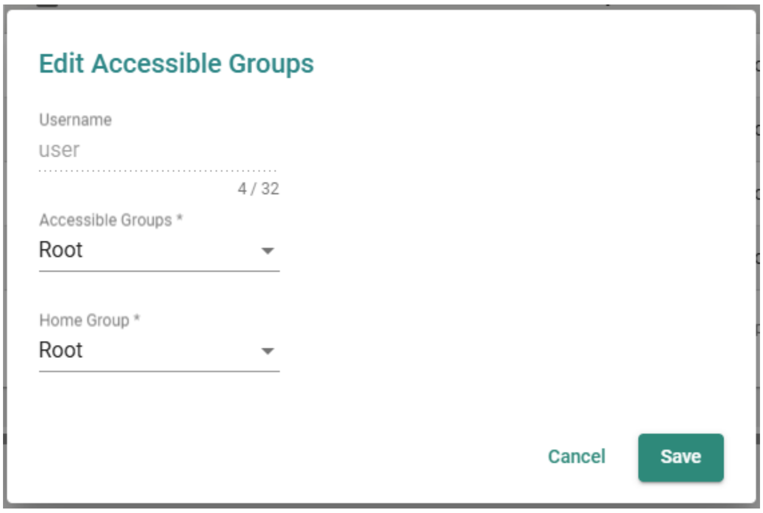
Password *
0 / 63

Authority *
User

4. 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.
5. Click **Apply**.

Editing Accessible Groups

1. Navigate to **Menu** (☰) **> Administration > Account Management**.
   The **Account Management** screen appears.
2. Go to the **User Account** tab.
3. Click the **Edit accessible groups** (👥) icon in front of the user account you want to modify the accessible groups and home group settings for.
   The **Edit Accessible Groups** window will appear.



Edit Accessible Groups

Username
user
4 / 32

Accessible Groups *
Root

Home Group *
Root

4. Configure the following settings:
   - **Accessible Groups**: Select the device group(s) that this user account can access.
   - **Home Group**: Select the default device group(s) that show when this user account logs in.
5. Click **Save**.

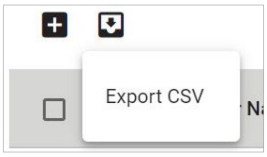
Deleting User Accounts

1. Navigate to **Menu** (☰) **> Administration > Account Management**.
   The **Account Management** screen appears.
2. Go to the **User Account** tab.
3. Click the **Delete** (🗑) icon in front of the account you want to delete.
4. To delete multiple accounts, check the boxes of the accounts you want to delete and click the **Delete** (🗑) icon in the top-left corner of the screen.
   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. Go to the **User Account** tab.
3. Click the **Export** (⬇) icon.

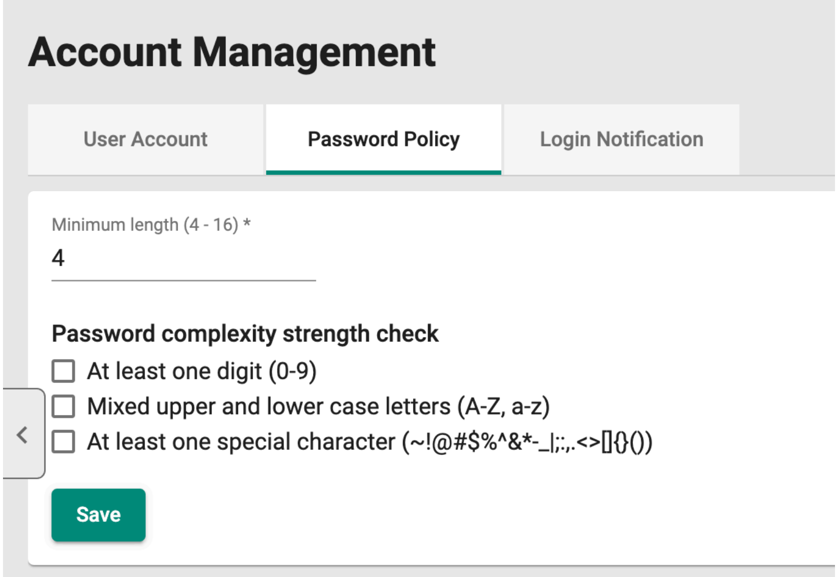


4. Select **Export CSV**.

Configuring the Password Policy

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

1. Navigate to **Menu** (☰) **> Administration > Account Management**.
   The **Account Management** screen appears.
2. Go to the **Password Policy** tab.



Account Management

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 (~!@#$%^&*-_|;:,.<>[]{}())

3. Specify the minimum password length (between 4 to 16 characters).
4. Select one or more of the following password complexity requirements:

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

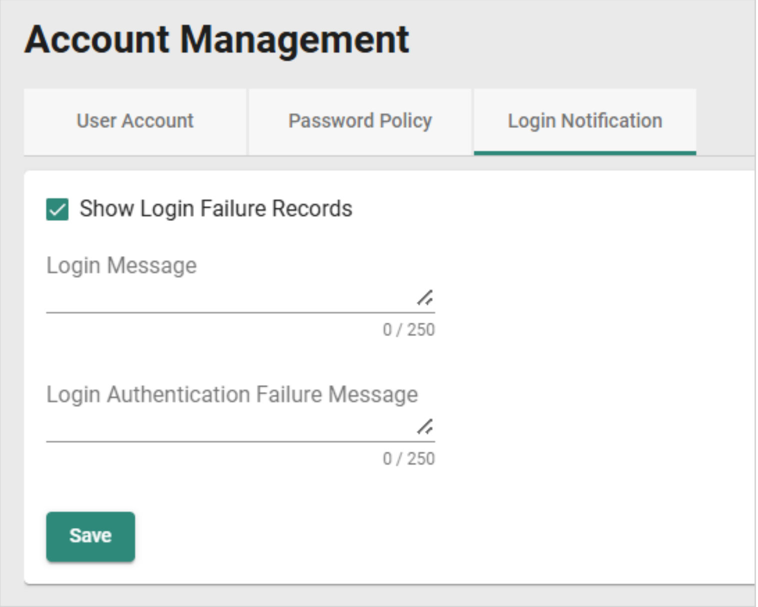
5. Click **Save**.

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

Configuring Login Notifications

Use the **Login Notification** screen to customize the notifications displayed when users log in to MXview One.

1. Navigate to **Menu** (☰) **> Administration > Account Management**.
   The **Account Management** screen appears.
2. Go to the **Login Notification** tab.



☑ Show Login Failure Records

Login Message

0 / 250

Login Authentication Failure Message

0 / 250

3. Check or uncheck the **Show Login Failure Records** box to enable or disable the login message and login failure records when logging in.
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**.

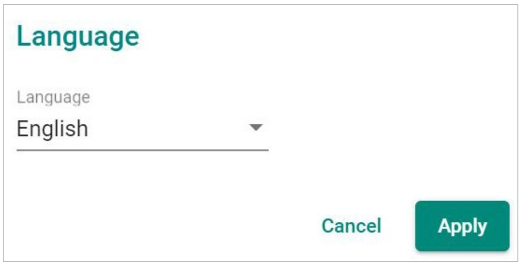
   MXview One displays the configured login notifications the next time a user logs in.

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**.

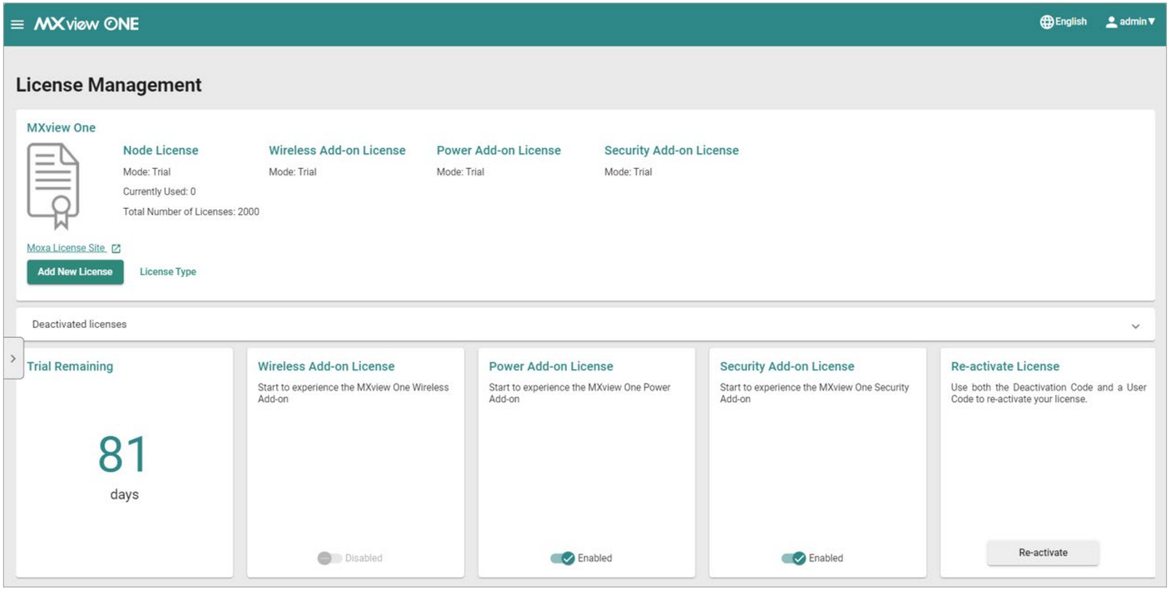
   MXview One updates the display language.

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: 0
Total Number of Licenses: 2000

Wireless Add-on License
Mode: Trial

Power Add-on License
Mode: Trial

Security Add-on License
Mode: Trial

Deactivated licenses

Trial Remaining
81 days

Wireless Add-on License
Start to experience the MXview One Wireless Add-on
Disabled

Power Add-on License
Start to experience the MXview One Power Add-on
Enabled

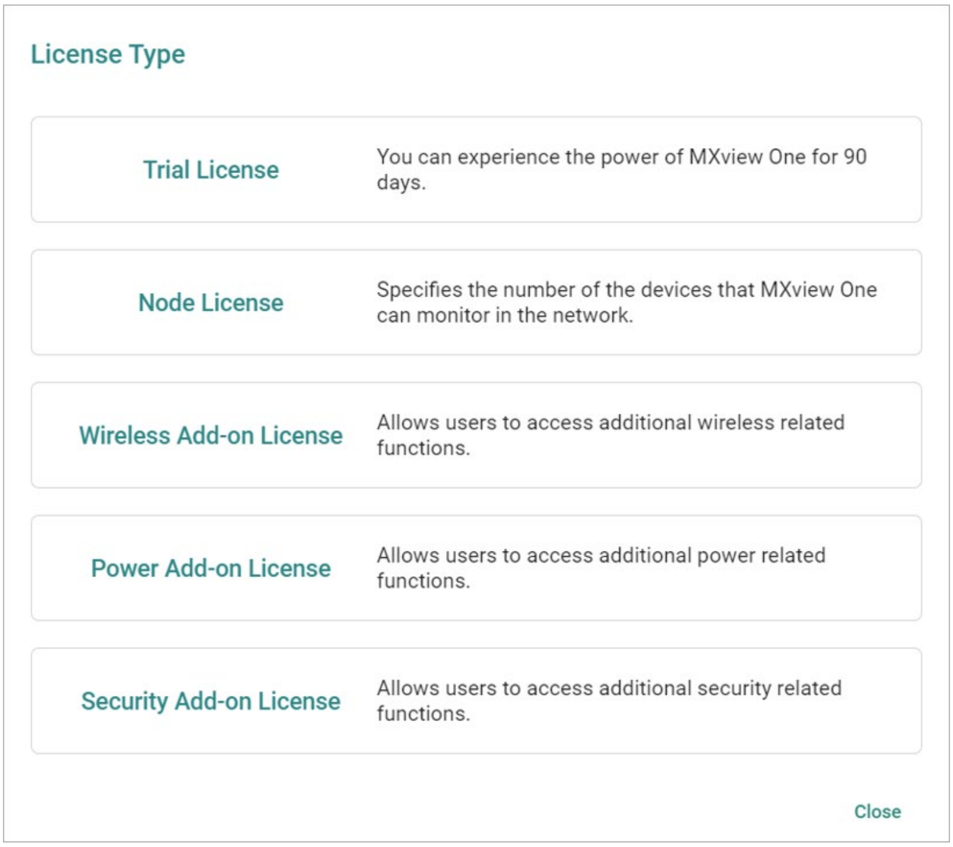
Security Add-on License
Start to experience the MXview One Security Add-on
Enabled

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.
Security Add-on License	Allows users to access additional security related functions.



License Type

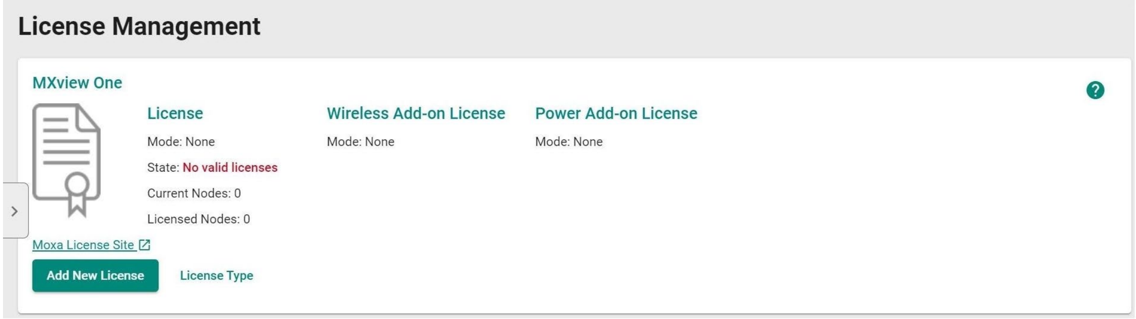
Trial License	You can experience the power of MXview One for 90 days.
Node License	Specifies the number of the devices that MXview One can monitor in the network.
Wireless Add-on License	Allows users to access additional wireless related functions.
Power Add-on License	Allows users to access additional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

Adding a New License

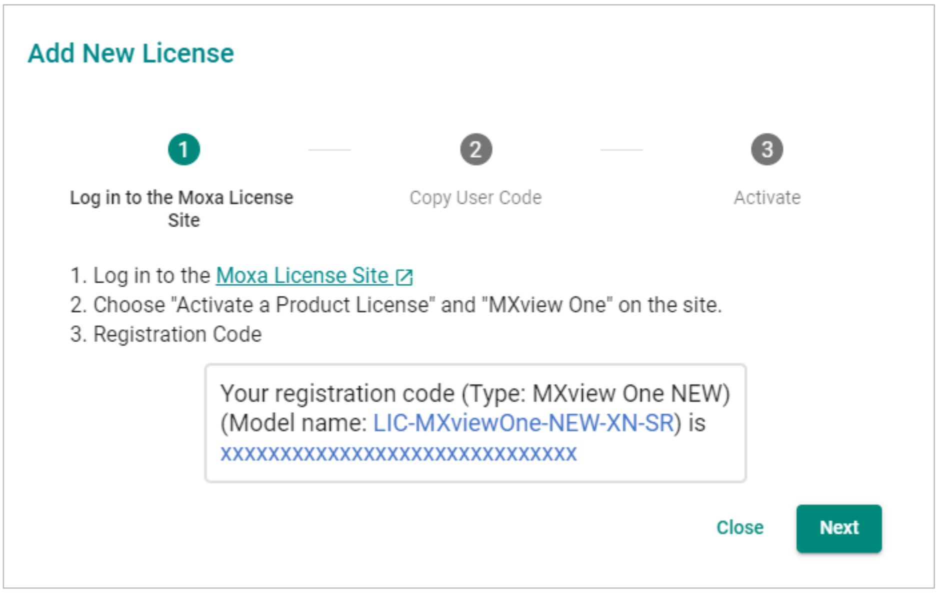
1. Navigate to **Menu** (☰) **> Administration > License Management**.

   The **License Management** screen appears.

2. In the **Add New License** section, click **Add New License**.



The **Add New License** screen appears.

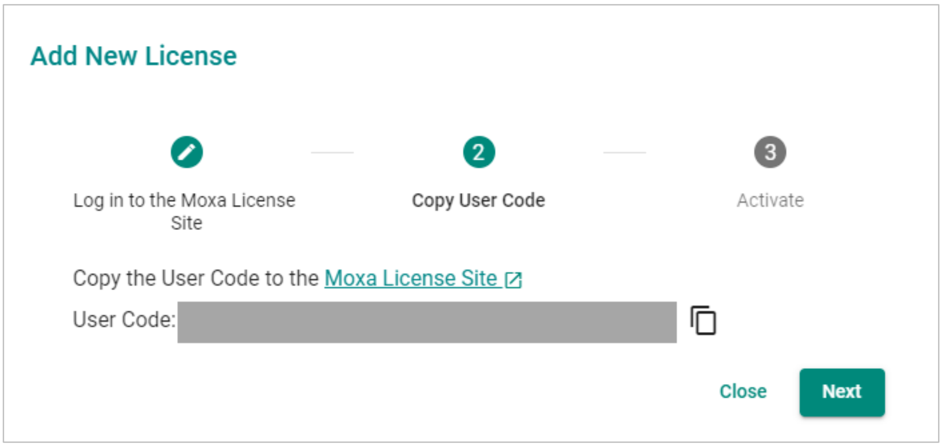


Add New License

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**.



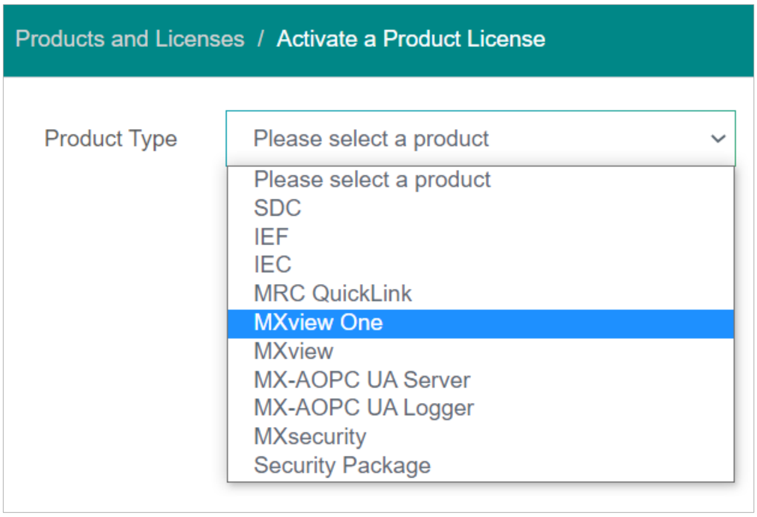
Add New License

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.

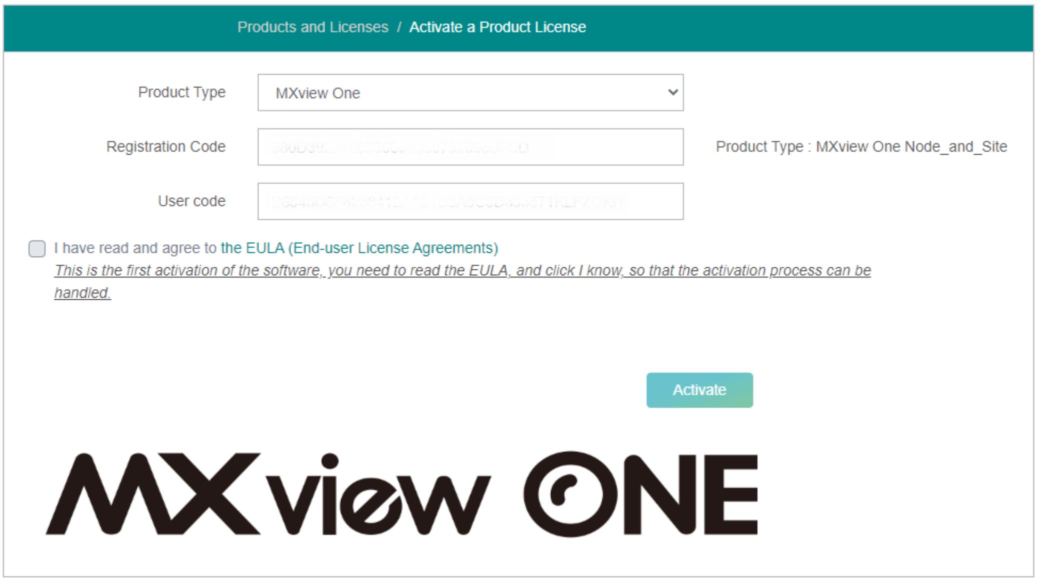
6. Click **Products and Licenses > Activate a Product License**. Then, select **MXview One** from the product type list.



Products and Licenses / Activate a Product License

Product Type: Please select a product

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.



Products and Licenses / Activate a Product License

Product Type: MXview One

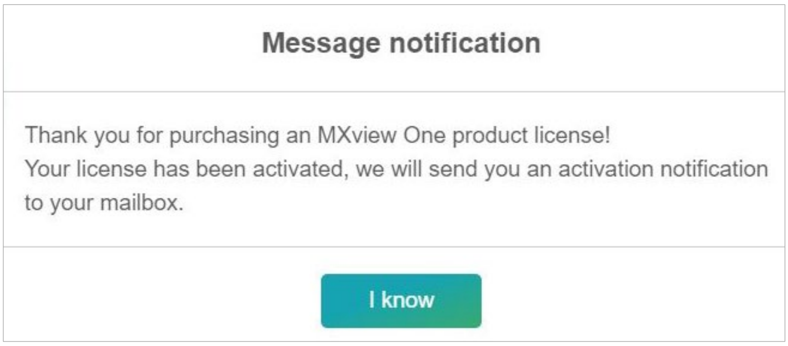
Registration Code: [redacted] Product Type : MXview One Node_and_Site

User code: [redacted]

□ 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.

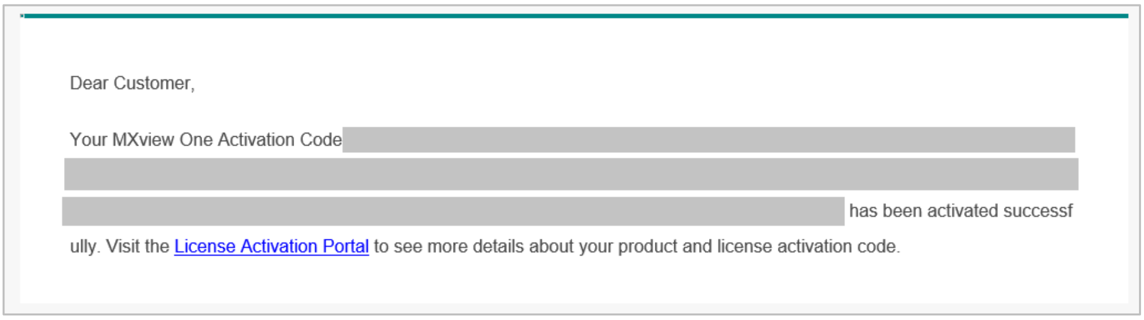
9. Once the process has been successfully completed, a pop-up window will appear to inform you that your license code has been activated. Click **I know** to close the window. If the license failed to activate, enter the correct Registration Code and User code again. If you are still experiencing problems,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



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.

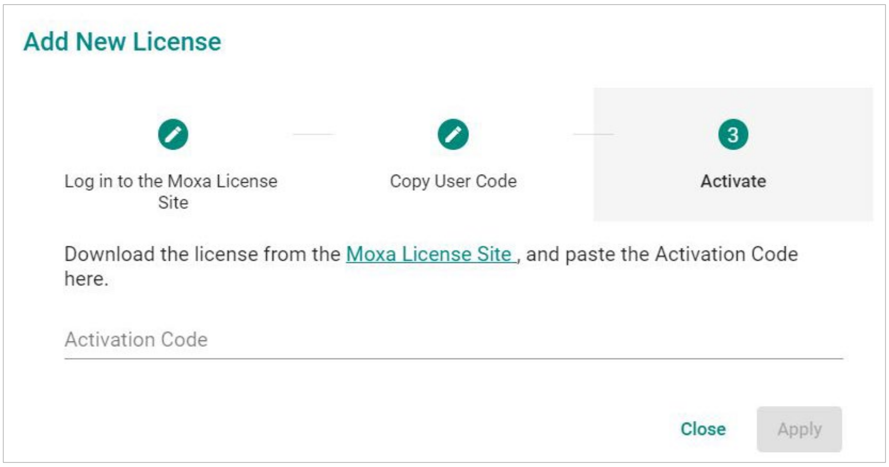
10. Check your email account you used to apply for your moxa account. The activation code will be sent to this email address.



Dear Customer,

Your MXview One Activation Code [redacted] has been activated successf
ully. 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

Log in to the Moxa License Site — Copy User Code — 3 Activate

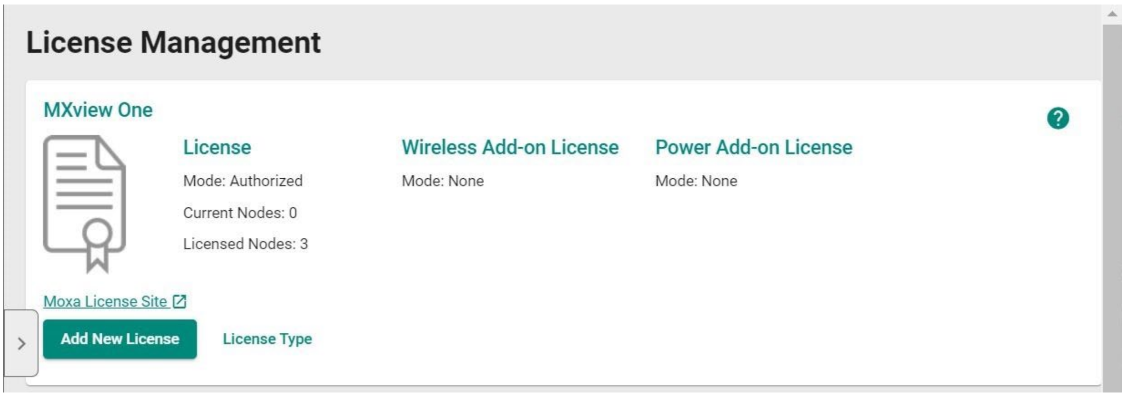
Download the license from the Moxa License Site , and paste the Activation Code here.

Activation Code

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

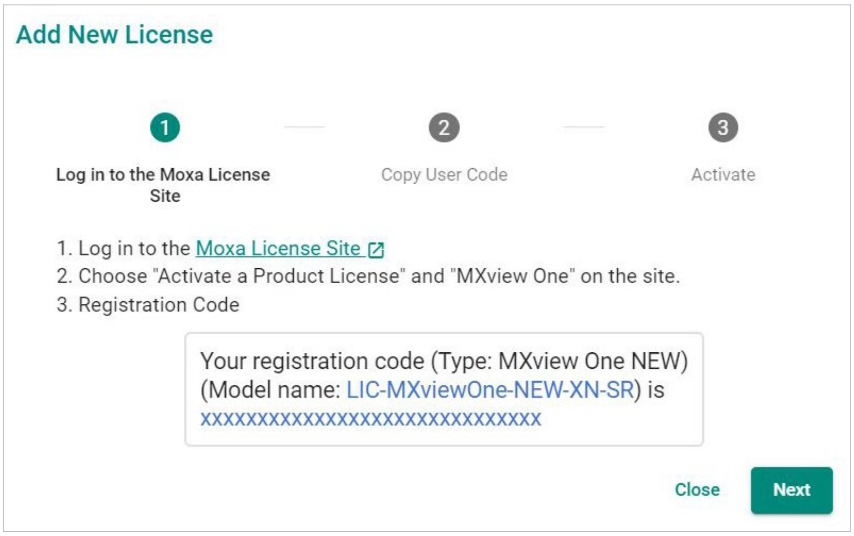
MXview One

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

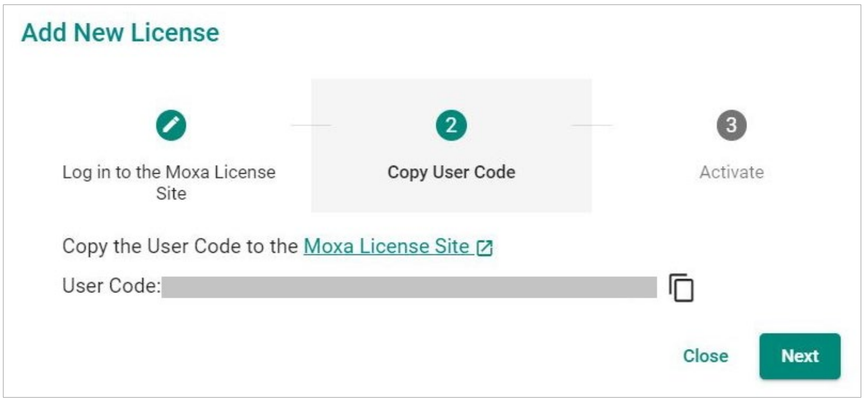
1. Log in to the Moxa License Site
2. Choose "Activate a Product License" and "MXview One" on the site.
3. Registration Code

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.

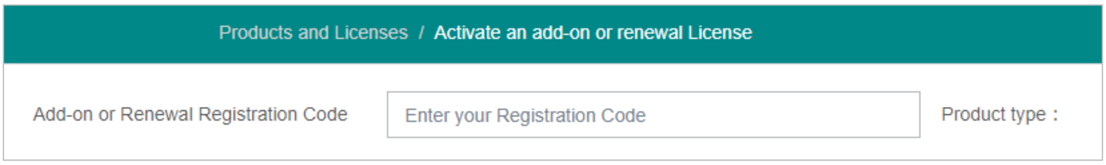


Add New License

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.

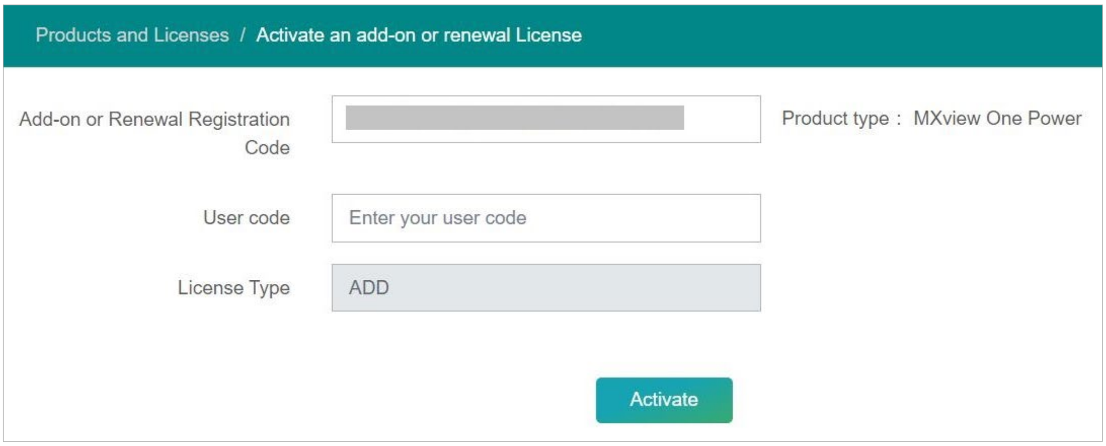


Products and Licenses / Activate an add-on or renewal License

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

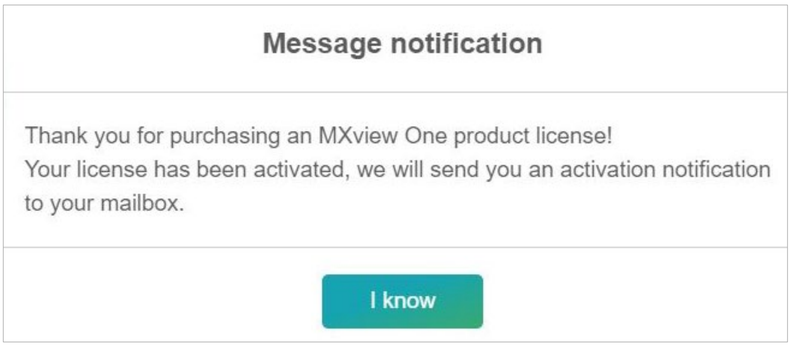
Add-on or Renewal Registration Code: [redacted]

Product type : MXview One Power

User code: Enter your user code

License Type: ADD

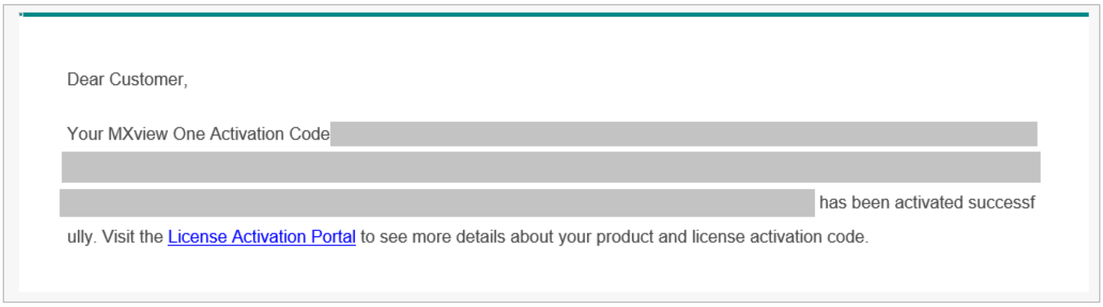
8. Once the process has been successfully completed, a pop-up window will appear to inform you that your license code has been activated. Click **I know** to close the window. If the license failed to activate, enter the correct Registration Code and User code again. If you are still experiencing problems,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

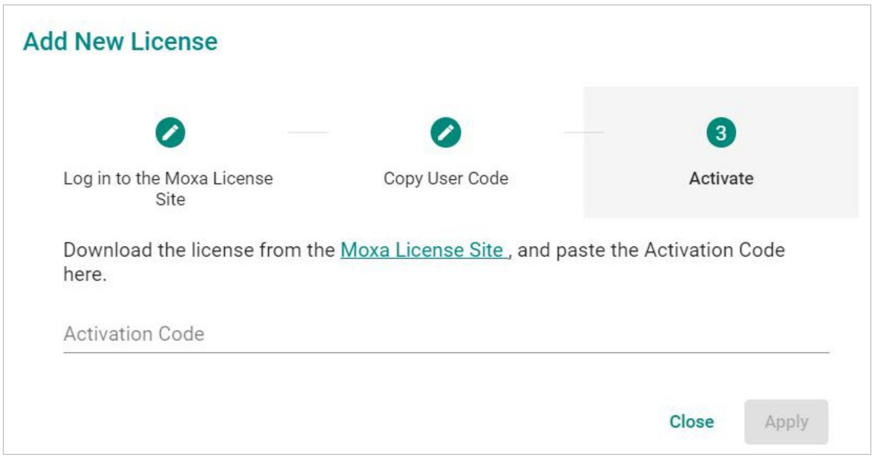


Dear Customer,

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

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

Activation Code

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.

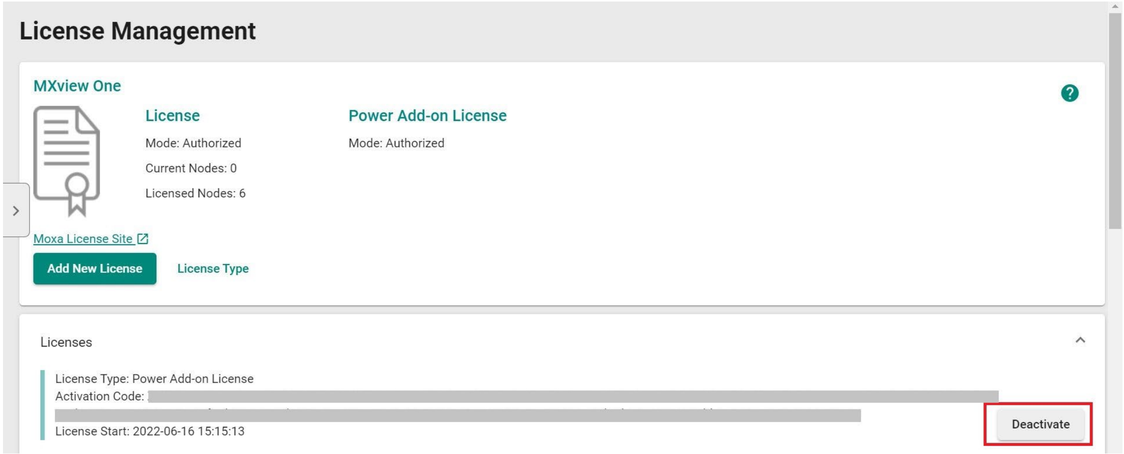
1. Navigate to **Menu** (☰) **> Administration > License Management**.

   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

Licenses

License Type: Power Add-on License

Activation Code: [redacted]

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

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

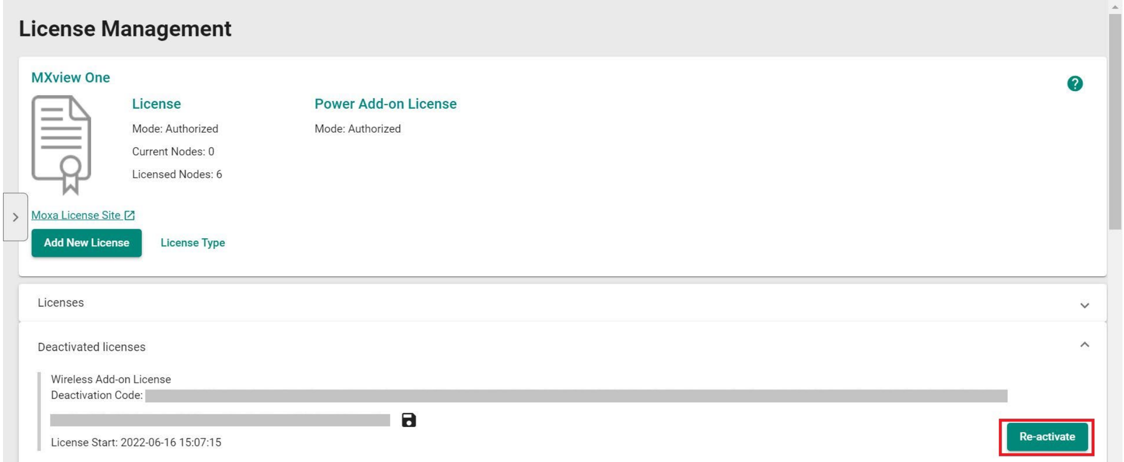
A deactivated license can be reactivated on the current instance of MXview One.

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

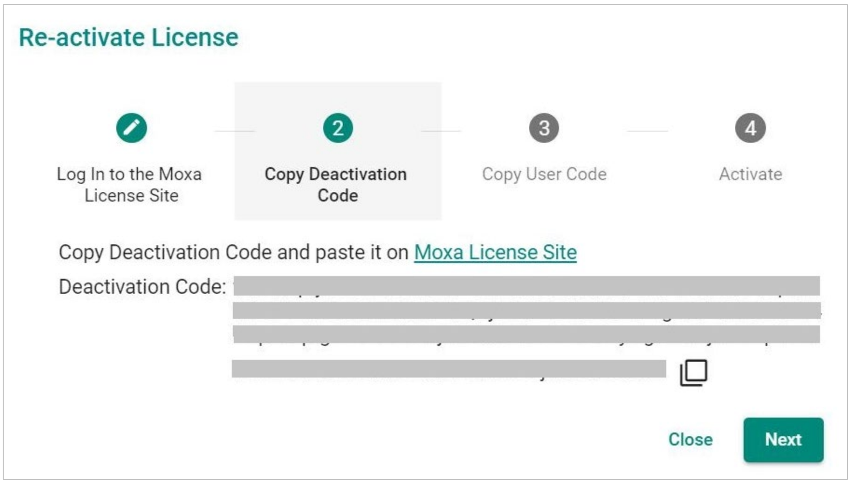
License
Mode: Authorized
Current Nodes: 0
Licensed Nodes: 6

Power Add-on License
Mode: Authorized

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**.



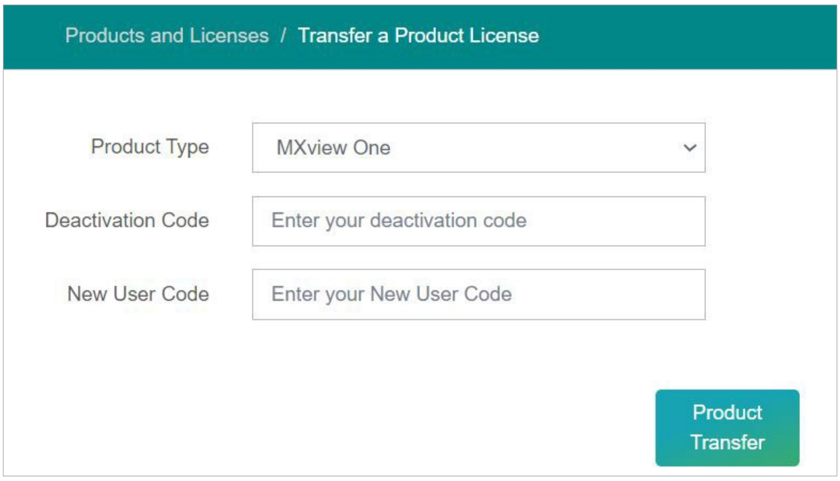
Re-activate License

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

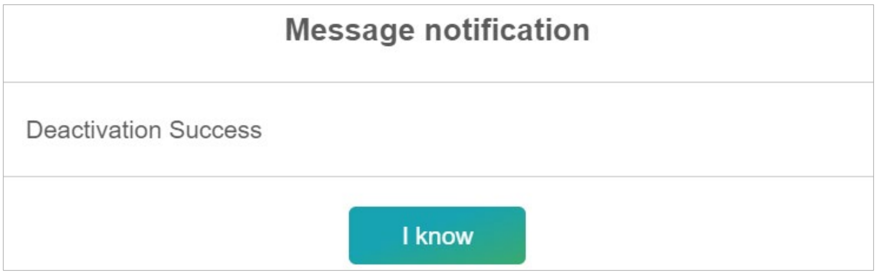
New User Code: Enter your New User Code

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.

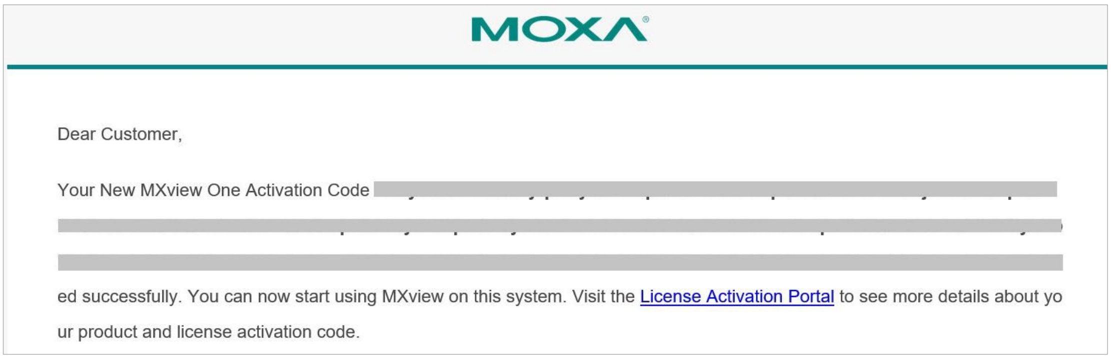
8. Once the process has been successfully completed, a pop-up window will appear to inform you that your license code has been deactivated. Click **I know** to close the window. If the license failed to deactivate, enter the license key again. If you are still experiencing problems, please contact Moxa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

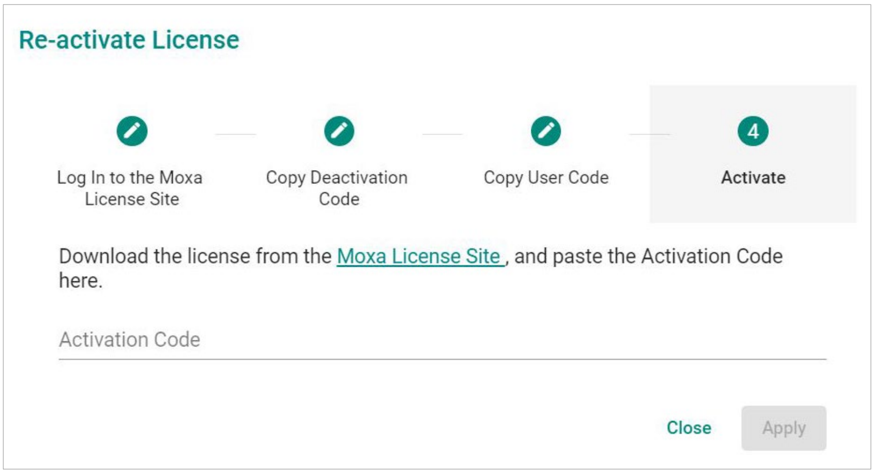


Dear Customer,

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.



Re-activate License

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

Activation Code

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

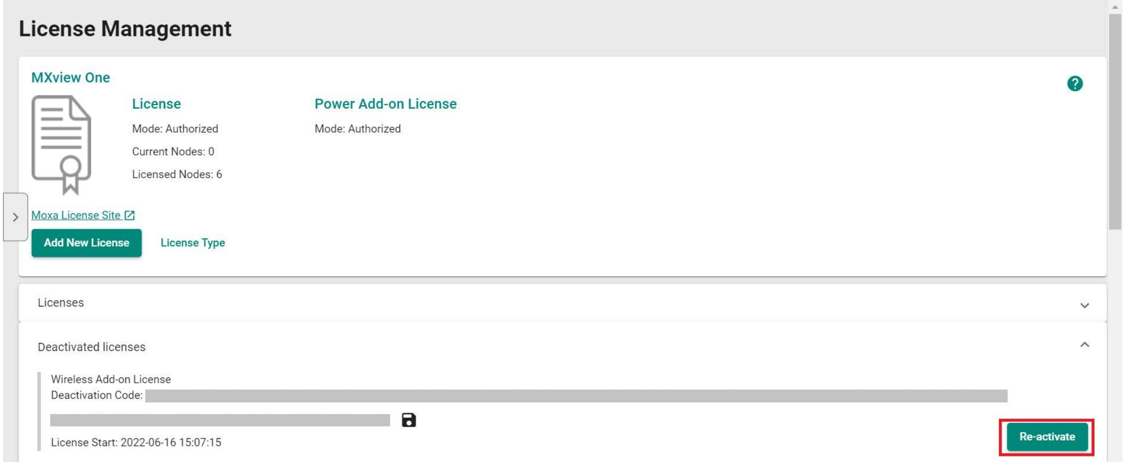
Transferring a License to a Different Instance of MXview One

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 Management

MXview One

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

Power Add-on License
Mode: Authorized

Licenses

Deactivated licenses

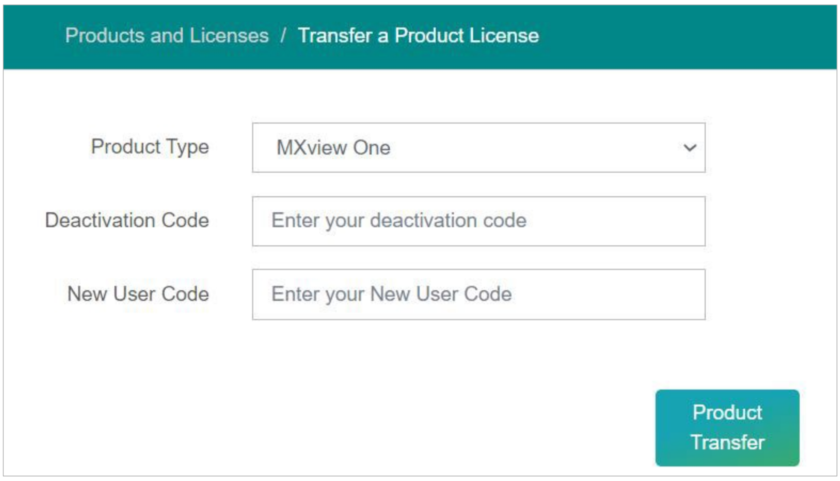
Wireless Add-on License
Deactivation Code: [redacted]

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**.



Product Type: MXview One

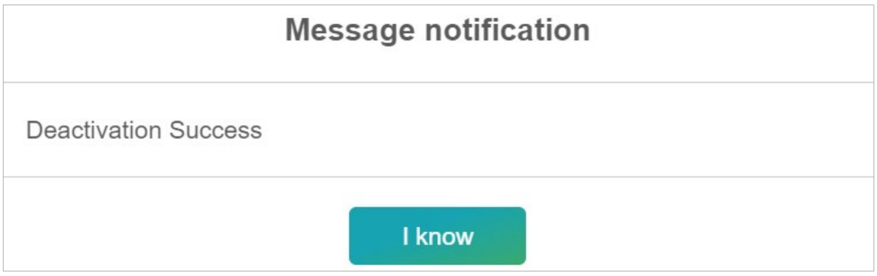
Deactivation Code: Enter your deactivation code

New User Code: Enter your New User Code

NOTE

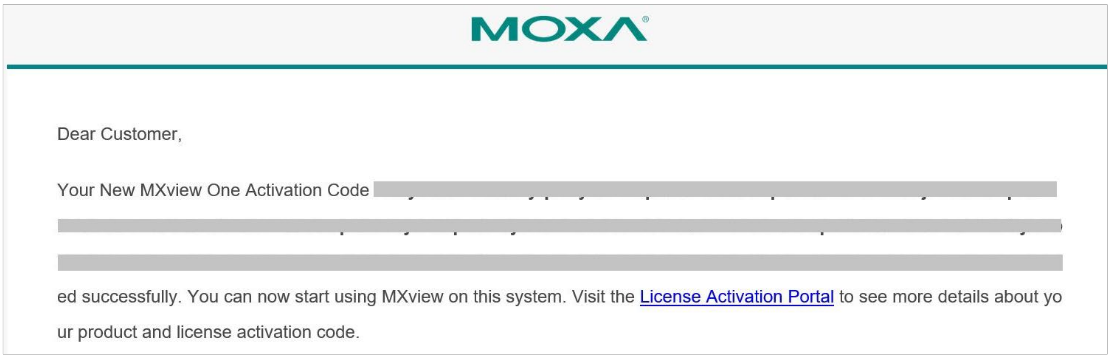
To obtain a new User Code, please visit "**Adding a New License**", and follow steps 1 to 4 to obtain and copy the new User Code.

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.



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.

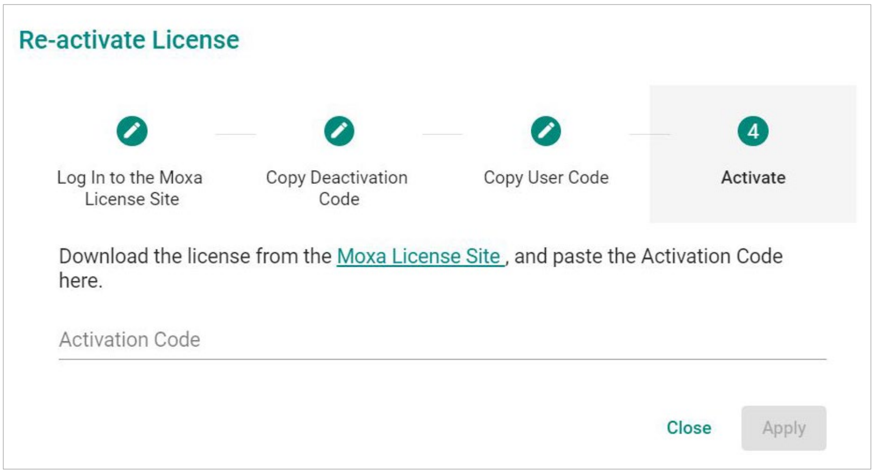


Dear Customer,

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

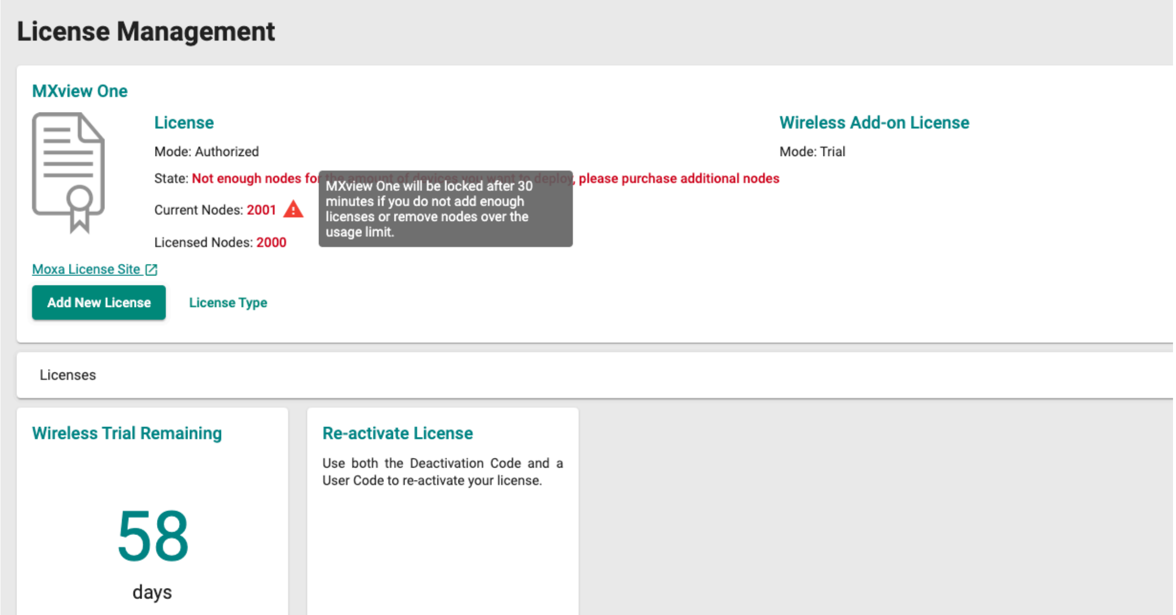
Download the license from the Moxa License Site , and paste the Activation Code here.

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

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

Current Nodes: 2001

Licensed Nodes: 2000

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**

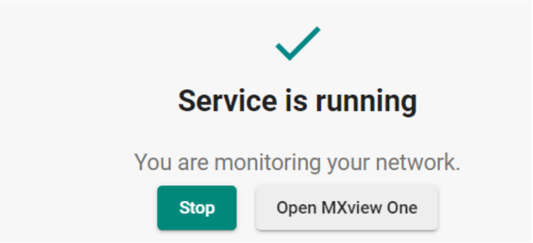
   Order the required quantity of Node-based Licenses from your channel or Moxa Sales Representative. Then, follow the instructions on **Adding a New License** to activate a new license.

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.

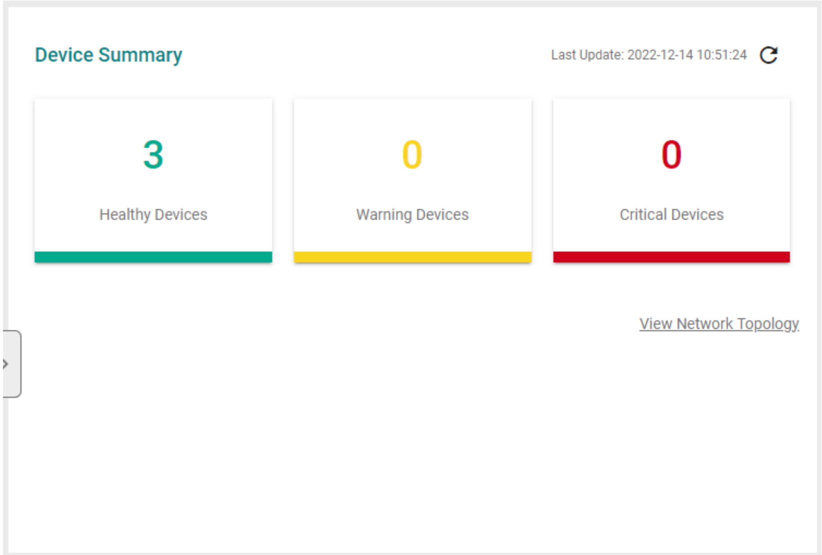
The **Dashboard** displays the following widgets:

- 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:



- **Healthy Devices:** The number of devices with no critical events or warnings.

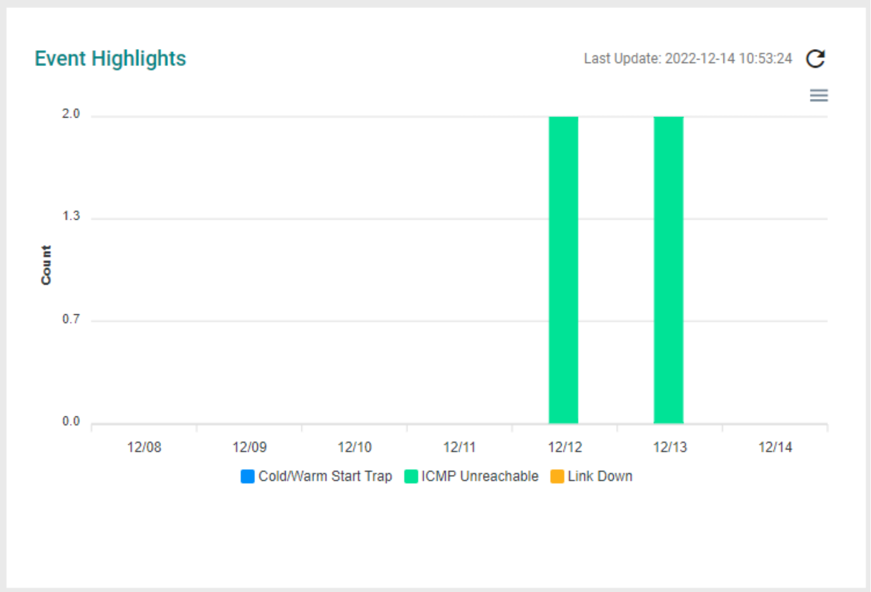
  Click to view additional details about the devices on the **Topology** screen.
- **Warning Devices:** The number of devices with warnings.

  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

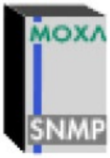
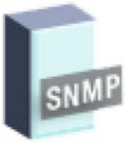
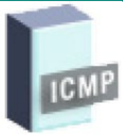
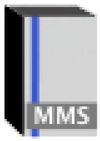
Device Discovery Overview

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

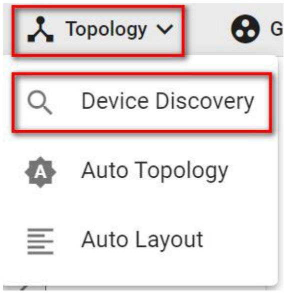
MXview One will display one of the following graphics to indicate devices:

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.	

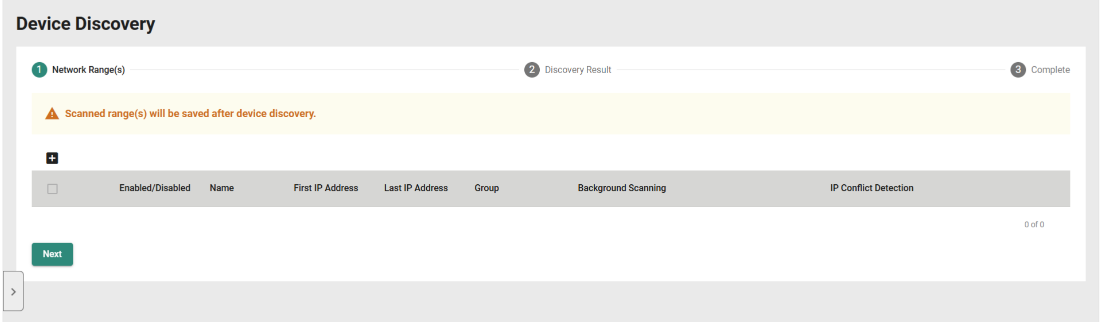
Configuring IP Address Scan Ranges

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.



Device Discovery

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

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

⊞

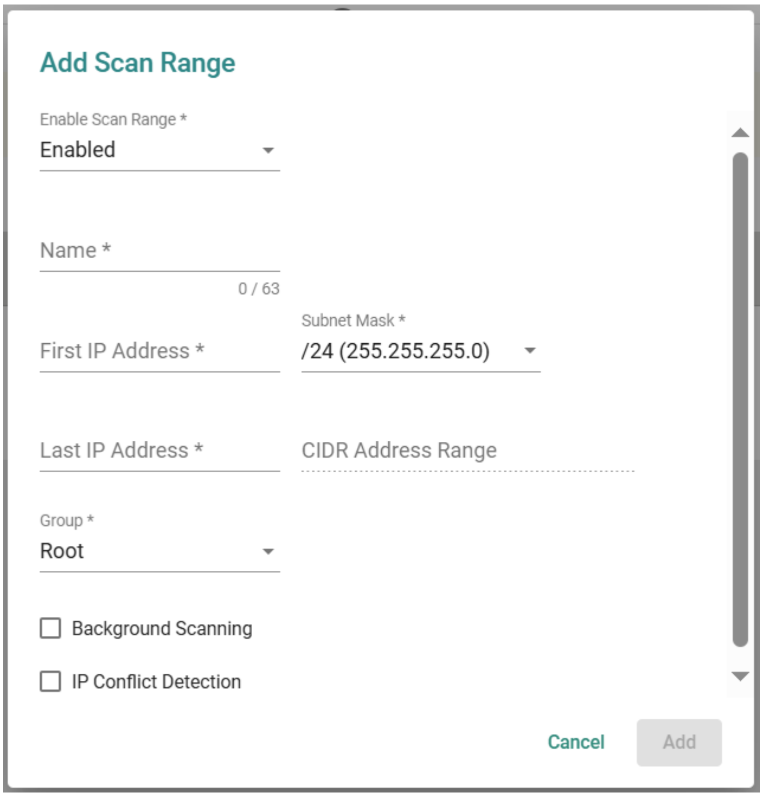
□	Enabled/Disabled	Name	First IP Address	Last IP Address	Group	Background Scanning	IP Conflict Detection

0 of 0

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 *

0 / 63

First IP Address *

Subnet Mask *: /24 (255.255.255.0)

Last IP Address *

CIDR Address Range

Group *: Root

□ Background Scanning

□ IP Conflict Detection

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 **Subnet Mask** (if applicable).

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

h. Check the **Background Scanning** checkbox (if required). When enabled, MXview One will scan for compatible devices in the background and add them to the topology. An event log will be recorded when a device is added.

i. Check the **IP Conflict Detection** checkbox (if required). When enabled, MXview One will check for IP conflicts among field devices. This feature requires WinPcap/libpcap to be installed.

j. 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.

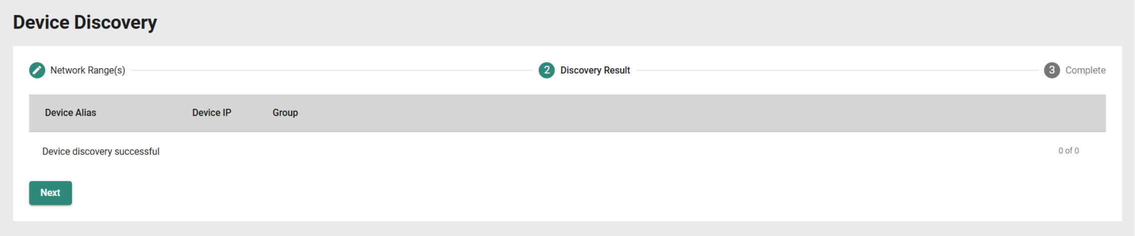
      The **Edit Scan Range** screen appears.

   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 Discovery

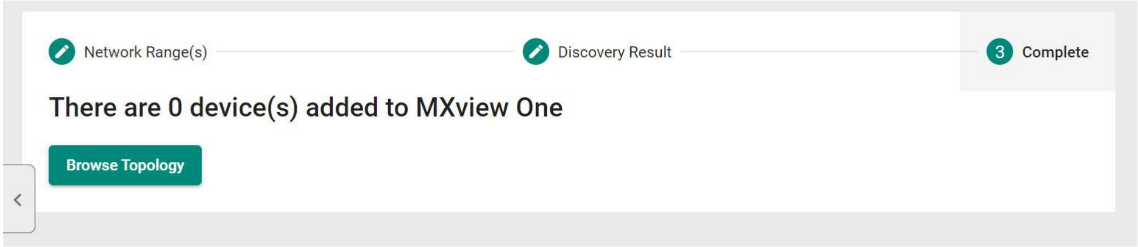
Device Alias	Device IP	Group

Device discovery successful

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:

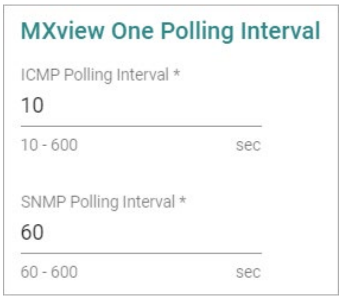
NOTE

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 **MXview One Polling Interval** section.



MXview One Polling Interval

ICMP Polling Interval *
10
10 - 600 sec

SNMP Polling Interval *
60
60 - 600 sec

3. Configure the following ICMP polling settings:

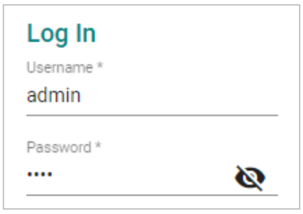
   ICMP polling interval: Specify the time in seconds between polls. MXview One will use ICMP protocol to check if the device is alive.

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.

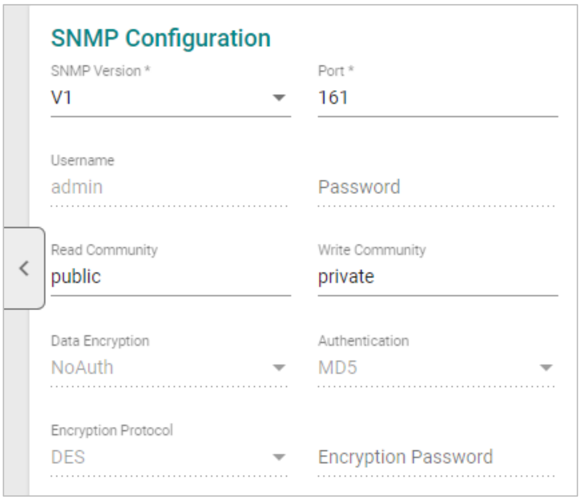
Changing the Default SNMP Configuration

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 settings:

   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.

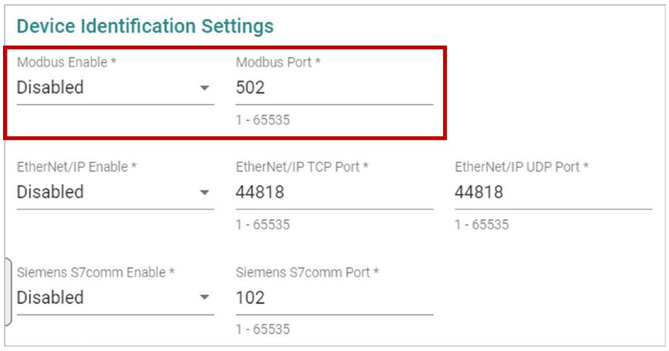
Changing Modbus TCP Settings

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 **Device Identification Settings** section.



Device Identification Settings

Modbus Enable *	Modbus Port *	
Disabled	502 1 - 65535	
EtherNet/IP Enable *	**EtherNet/IP TCP Port ***	**EtherNet/IP UDP Port ***
Disabled	44818 1 - 65535	44818 1 - 65535
Siemens S7comm Enable *	**Siemens S7comm Port ***	
Disabled	102 1 - 65535	

3. Configure the following settings:
   a. **Modbus Enabled:** Enable or disable Modbus TCP settings.
   b. **Modbus Port:** Specify the Modbus TCP port.

4. Click **Save**.

   MXview One updates the modified settings.

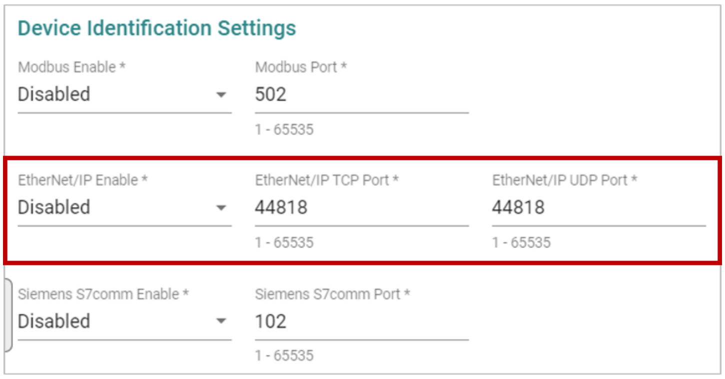
Changing EtherNet/IP Settings

By configuring EtherNet/IP Settings in the Default Device Template section, MXview One will be able to detect whether an ICMP device has EtherNet/IP attributes or not. If an ICMP device supports EtherNet/IP, an EtherNet/IP device icon will be displayed 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 **Device Identification Settings** section.



Device Identification Settings

Modbus Enable *	Modbus Port *	
Disabled	502 1 - 65535	
EtherNet/IP Enable *	**EtherNet/IP TCP Port ***	**EtherNet/IP UDP Port ***
Disabled	44818 1 - 65535	44818 1 - 65535
Siemens S7comm Enable *	**Siemens S7comm Port ***	
Disabled	102 1 - 65535	

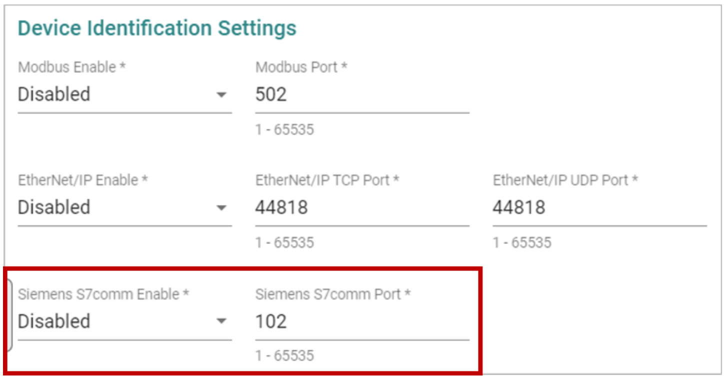
3. Configure the following settings:
   - **EtherNet/IP Enable**: Enable or disable EtherNet/IP settings.
   - **EtherNet/IP TCP Port**: Specify the EtherNet/IP TCP port.
   - **EtherNet/IP UDP Port**: Specify the EtherNet/IP UDP port.
   - Click **Save**.
     MXview One updates the modified settings.

Changing Siemens S7comm Settings

By configuring Siemens S7comm Settings in the Default Device Template section, MXview One will be able to detect whether an ICMP device has Siemens S7comm attributes or not. If an ICMP device supports Siemens S7comm, a Siemens S7comm device icon will be displayed 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 **Device Identification Settings** section.



Device Identification Settings

Modbus Enable * Disabled

Modbus Port * 502 (1 - 65535)

EtherNet/IP Enable * Disabled

EtherNet/IP TCP Port * 44818 (1 - 65535)

EtherNet/IP UDP Port * 44818 (1 - 65535)

Siemens S7comm Enable * Disabled

Siemens S7comm Port * 102 (1 - 65535)

3. Configure the following settings:
   - **Siemens S7comm Enable**: Enable or disable Siemens S7comm settings.
   - **Siemens S7comm Port**: Specify the Siemens S7comm port.
4. Click **Save**.
   MXview One updates the modified settings.

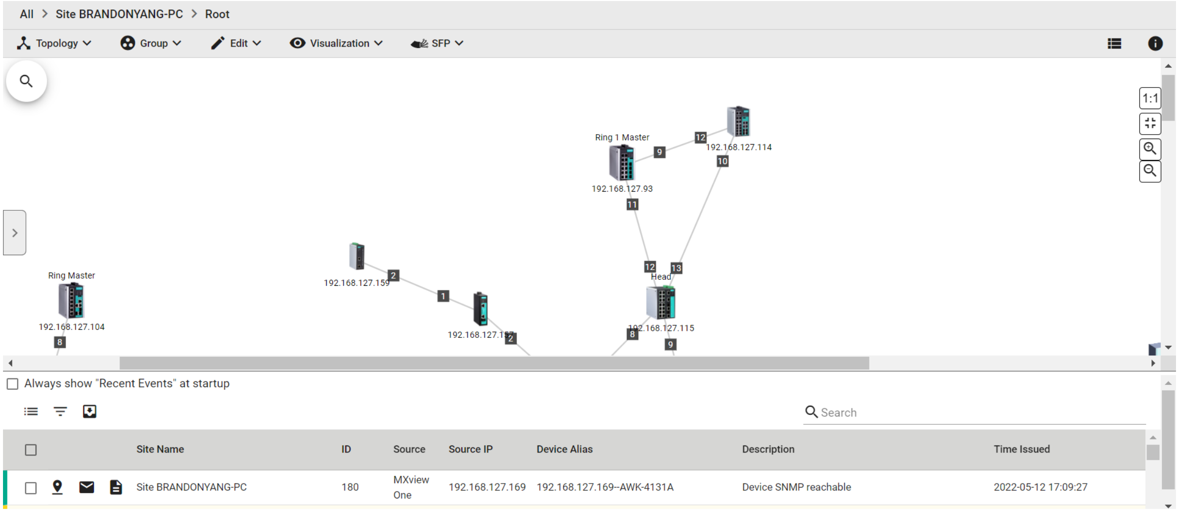
7. Topology Management

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

☐	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.

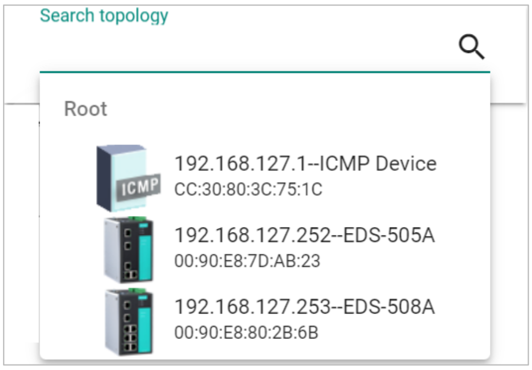
2. If the **List view** is displayed, click the **Topology view** (⅄) icon in the top right corner.

   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

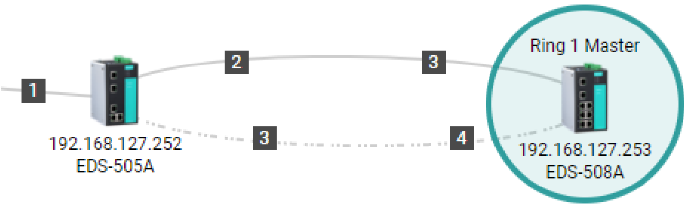
192.168.127.1--ICMP Device
CC:30:80:3C:75:1C

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

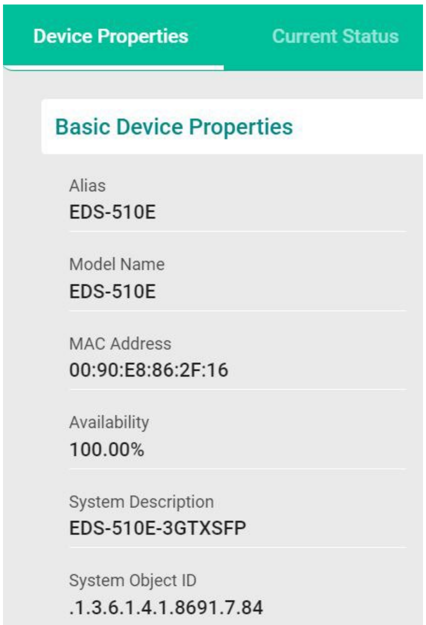
192.168.127.253--EDS-508A
00:90:E8:80:2B:6B

   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

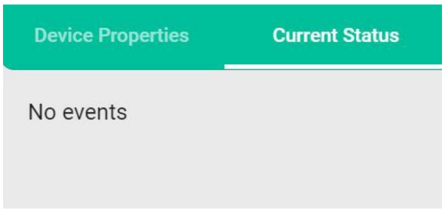
Availability
100.00%

System Description
EDS-510E-3GTXSFP

System Object ID
.1.3.6.1.4.1.8691.7.84

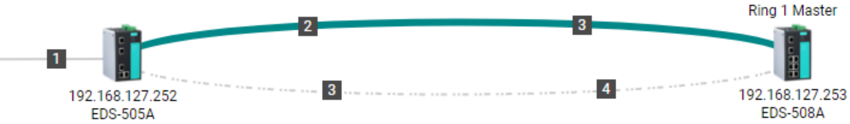
5. To view events associated with the device, click the **Current Status**.

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

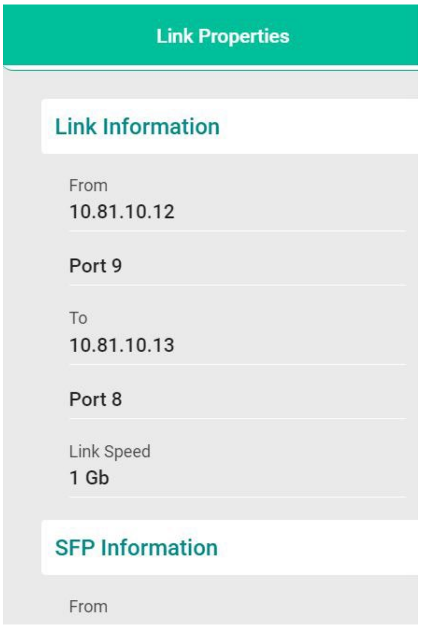


No events

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

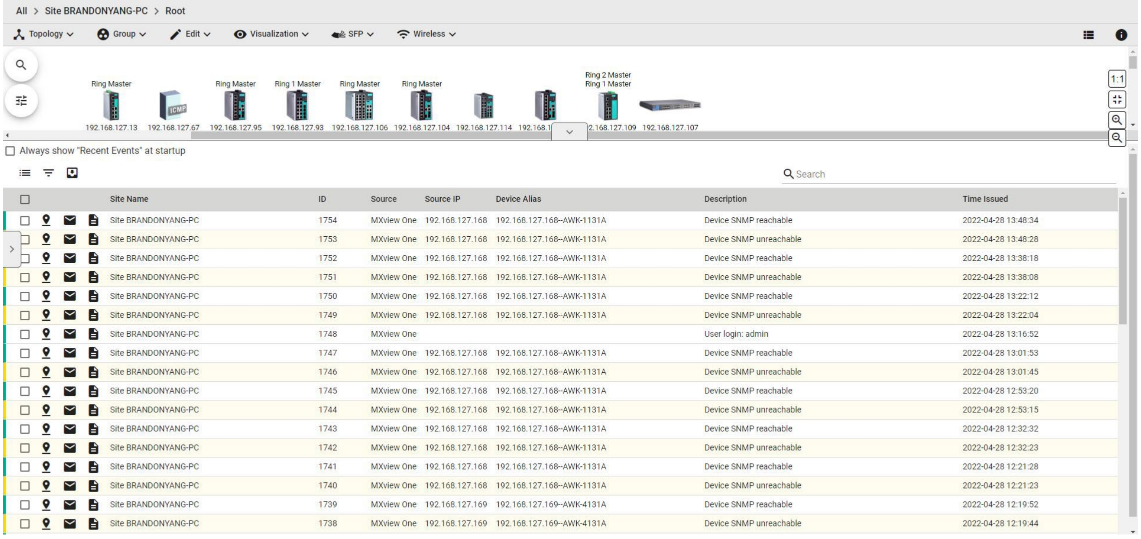
Viewing Recent Events

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

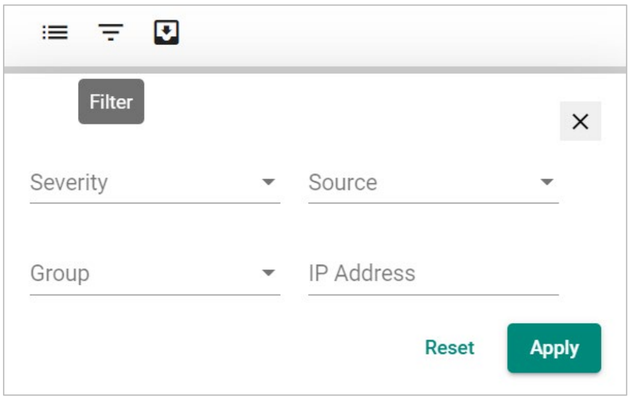
2. To filter the information in the table, type a full or partial string that matches the value in any of the table columns on the right of the search space.

   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.

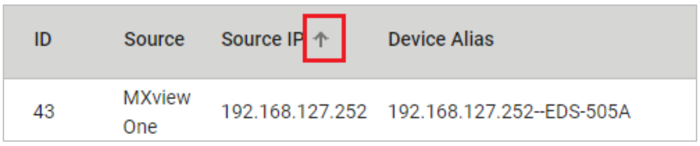
4. To acknowledge the events in the table:

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.

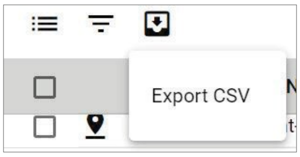
MXview One sorts the table by the column.



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.

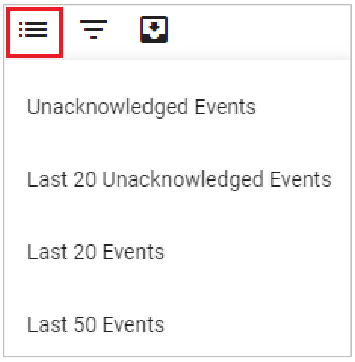
d. Click **Save**.

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

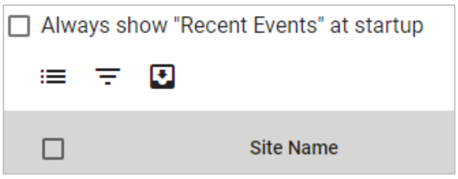
7. To quickly filter event, click the **Quick filter event** (☰) icon to find the events.

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

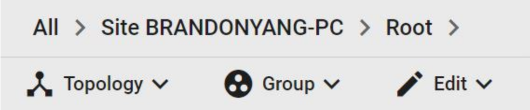
Organizing the Topology Structure By Group Function

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.

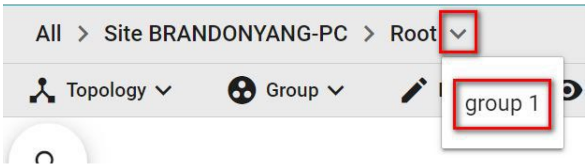
1. Navigate to **Menu** (☰) **> Topology**.

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

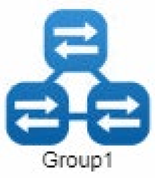
   - MXview One represents the Topology Map structure by a path at the top of the **Topology** screen:

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

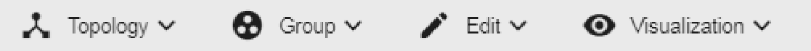
     
     All > Site BRANDONYANG-PC > Root
Topology Group
group 1

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

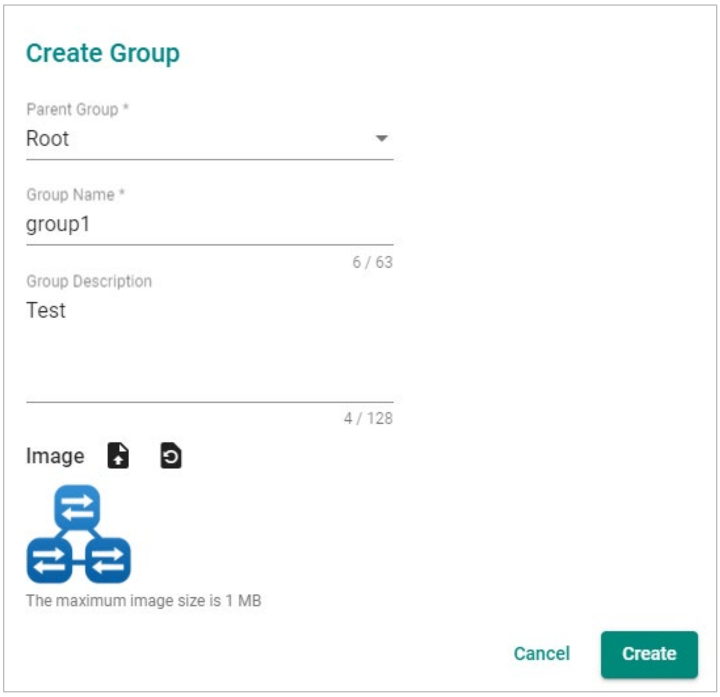
2. If **List view** is displayed, click the **Topology view** (⅄) icon in the top right corner.

   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

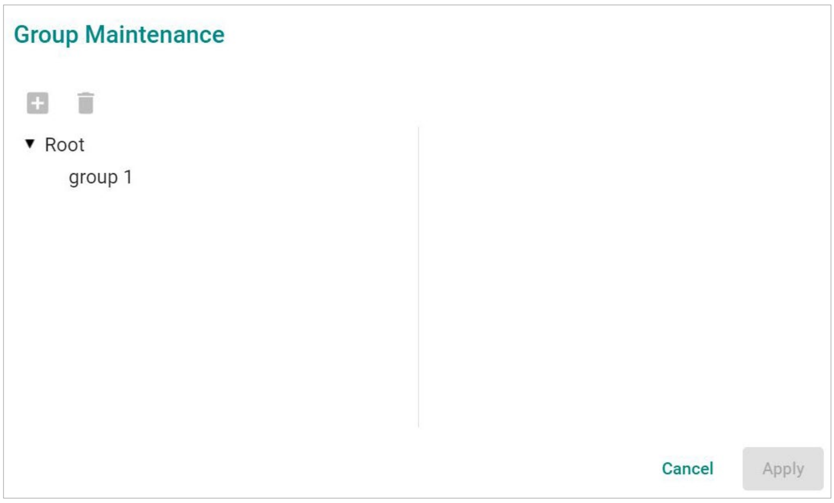
Group Description
Test
4 / 128

    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**.

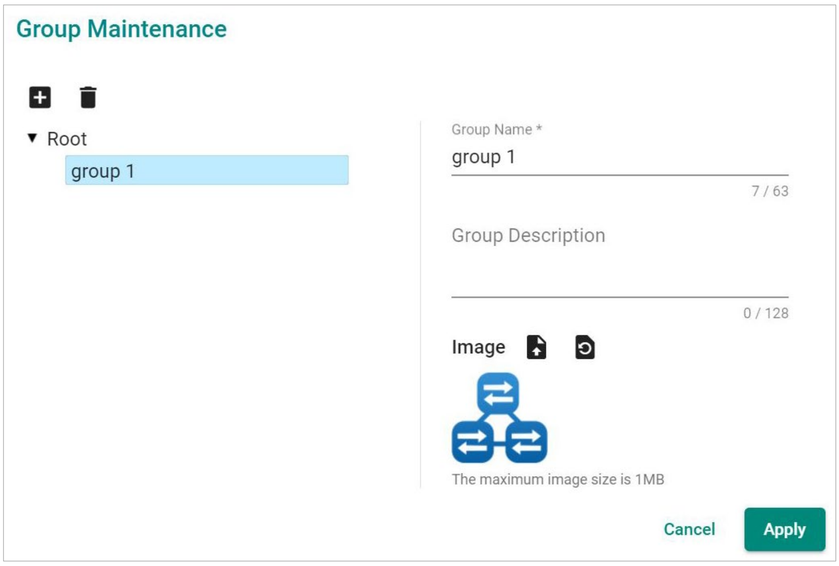
       The **Group Maintenance** screen appears.



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.

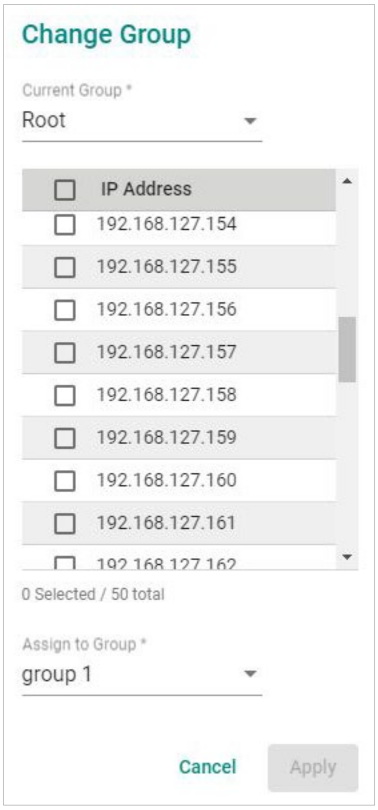
d. Click **Apply**.

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.

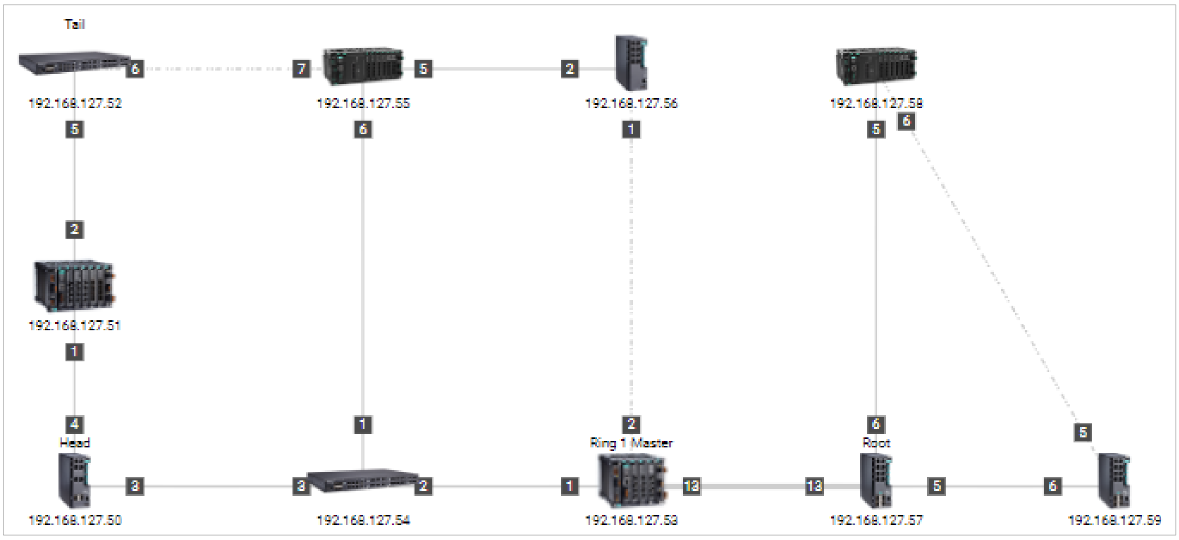
c. Select the IP address(es) of the device(s) that you want to reassign to a different group.

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.

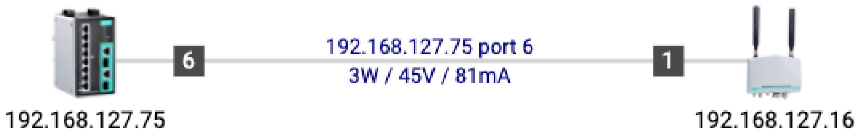
- RSTP has a **Root**
- Turbo Ring has a **Master**
- Turbo Chain has a **Head** and a **Tail**
- Dual Homing

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

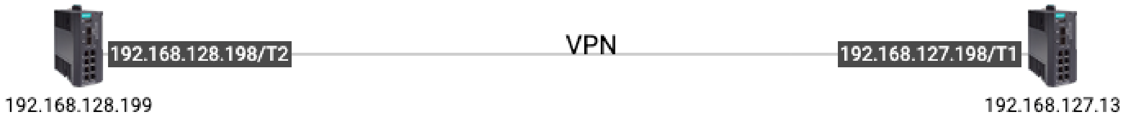
By periodic polling, a PoE link will display the port number, power (watts), voltage (V), and current (mA) directly on the topology map.



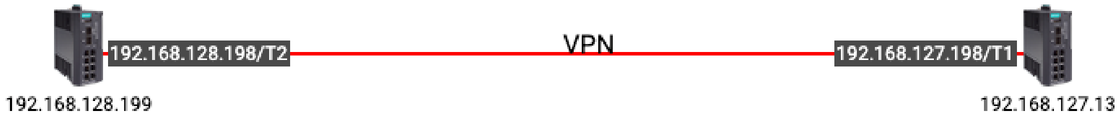
VPN Tunnel Visualization

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

1. The VPN tunnel is connected.



2. The VPN tunnel is disconnected.

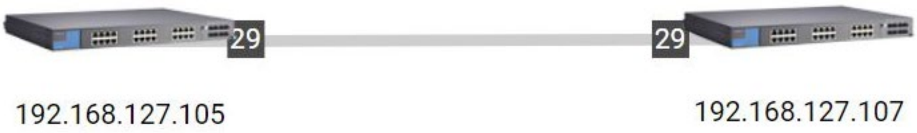


NOTE

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.

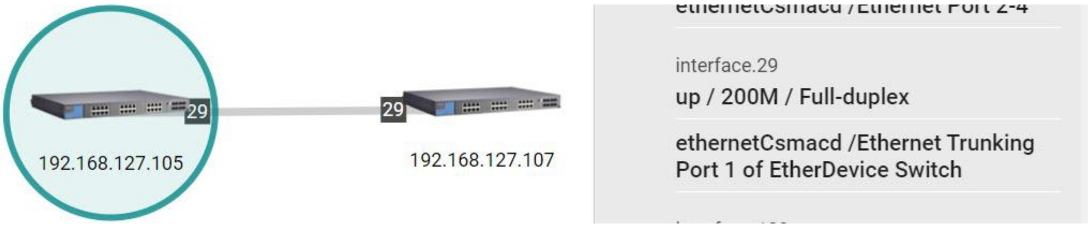


NOTE

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.

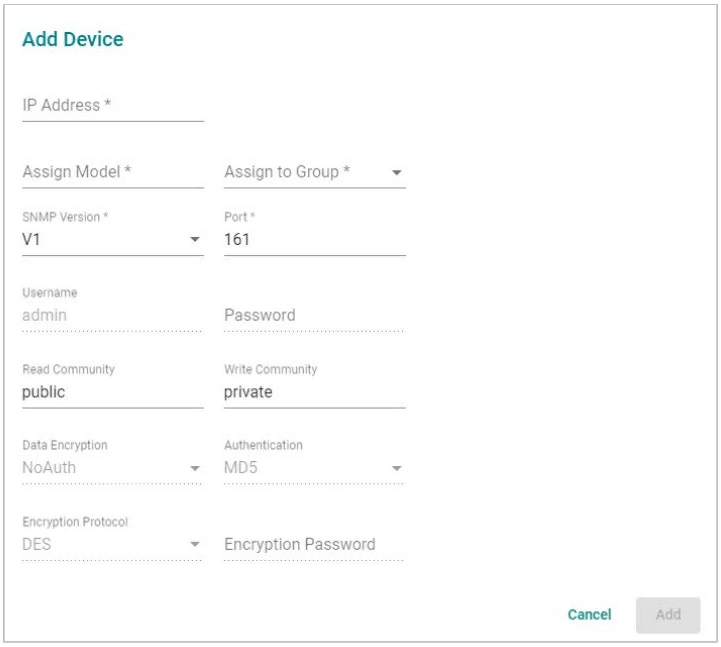
1. Navigate to **Menu** (☰) **> Topology**.

   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**

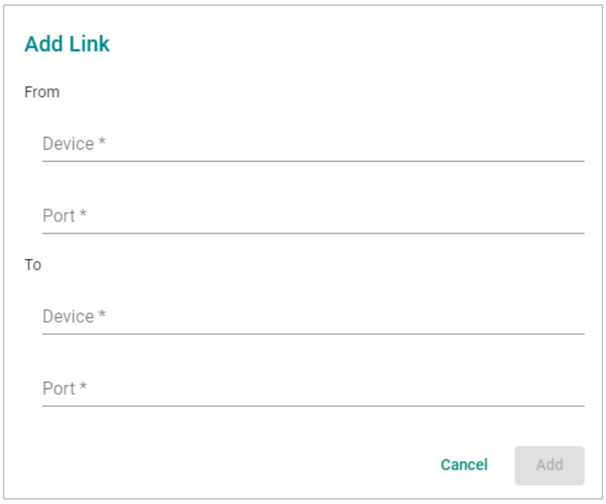
   c. Click **Add**.

   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

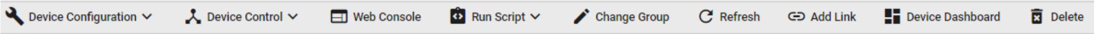
You can delete devices and links from the Topology Map. After a device is deleted, it will be removed from the topology map, and the device will not be polled or located when performing Device Discovery. Deleting a link will delete a link from the topology map, but it will not affect the actual network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

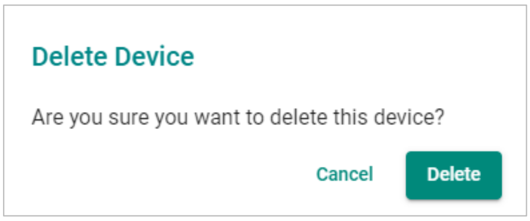
   a. Select the device.

   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?

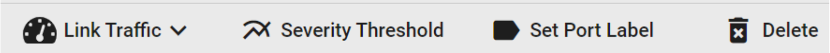
   c. Click **Delete**.

   MXview One deletes the device from the Topology Map.

3. To delete a link from the Topology Map:

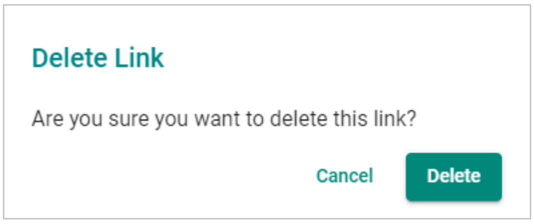
   a. Select the link.

   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**.

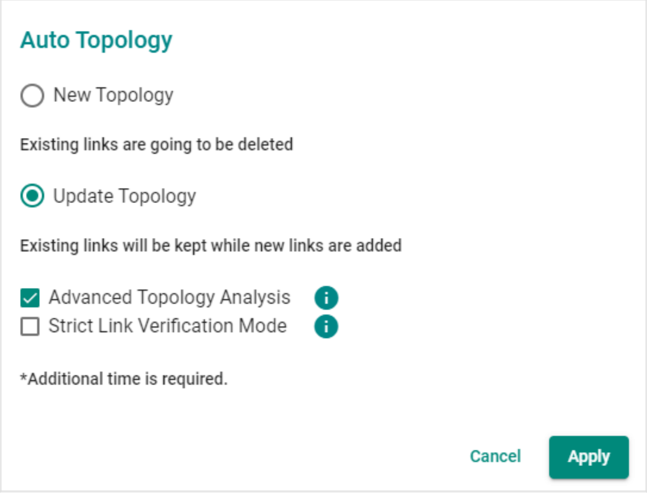
   The **Topology** screen appears and displays the Topology Map by default.

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**.

NOTE

You can create an Auto Topology scheduled task from the **Menu > Administration > Maintenance Scheduler** page.

Refreshing the Topology Layout

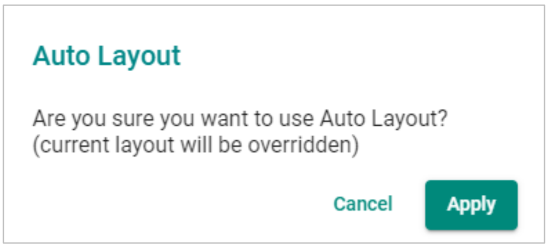
After changes have been made, use the **Auto Layout** feature to refresh the layout of the Topology Map. Auto Layout does not update any devices or links. It only redraws the topology to better fit the screen.

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

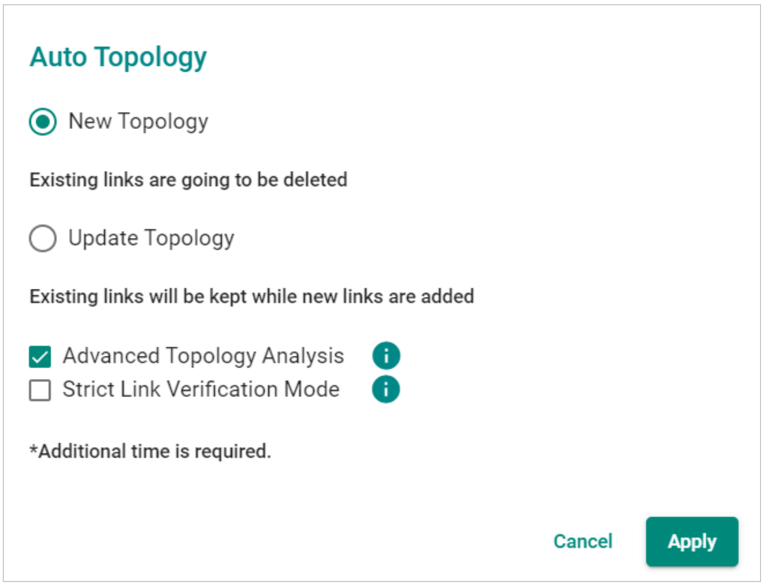
If the Auto Topology function does not create an accurate representation of the actual network, deselect the **Advanced Topology Analysis** check box and try again.

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**.

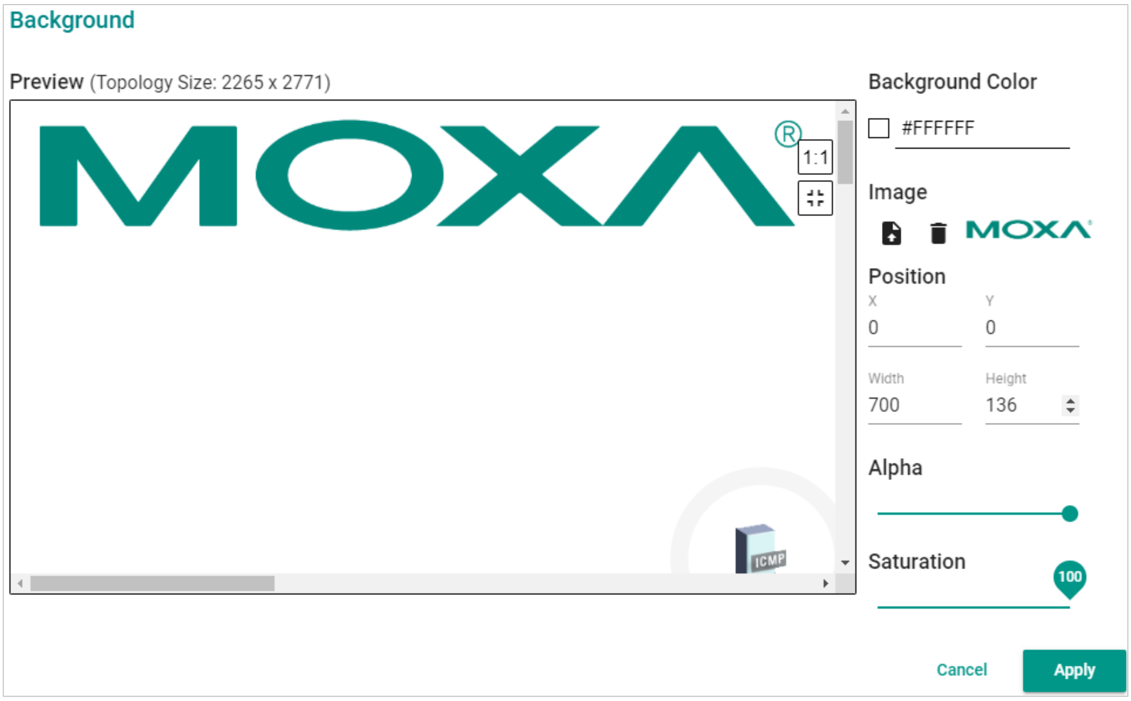
   The **Topology** screen appears and will display the Topology Map by default.

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

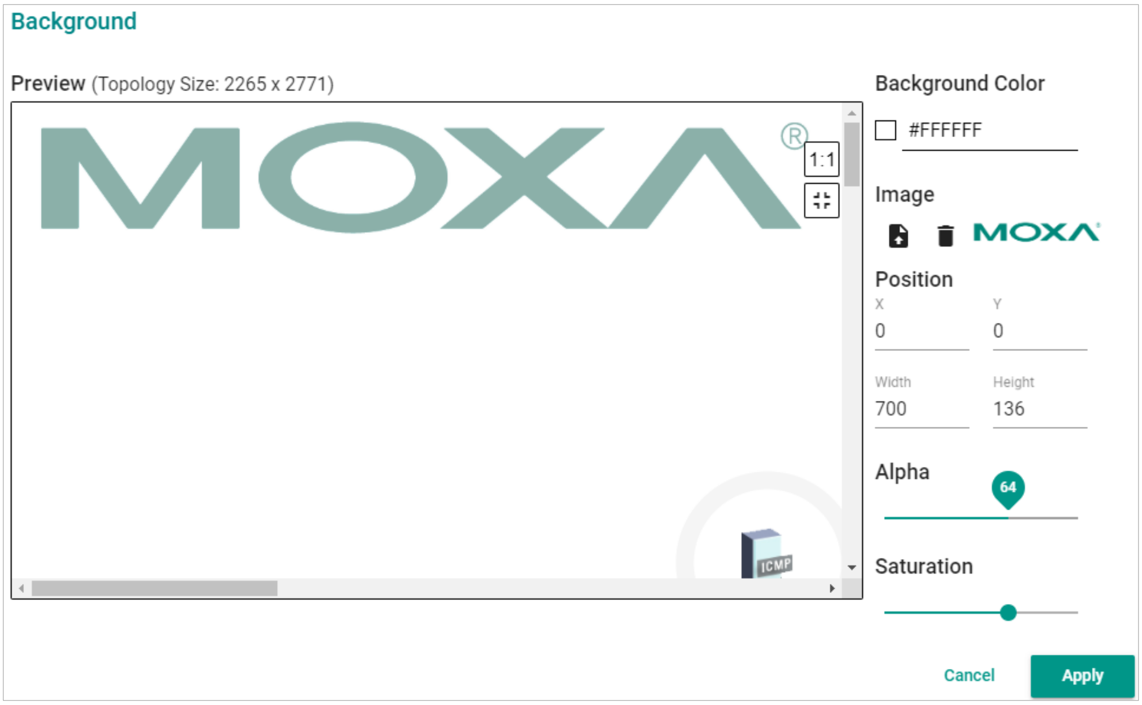
4. Upload the background image by using one of the following methods:

   - 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

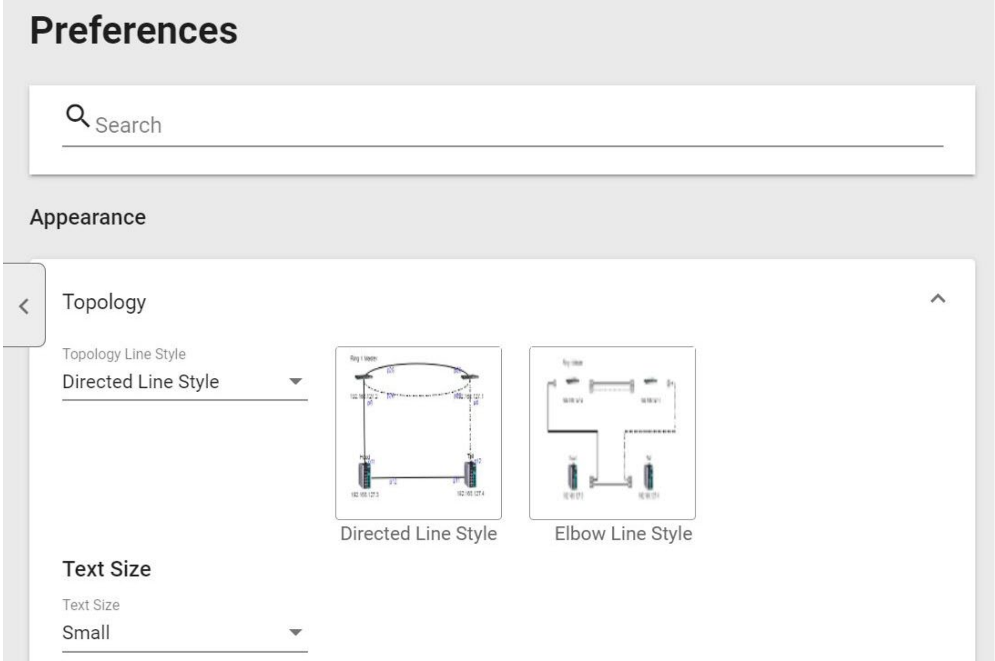
Use the **Preferences** screen to modify how the Topology Map displays the topology line style, PoE status, background color, link status, and traffic load.

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

   The **Preferences** screen appears.

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

   The **Topology** settings appear.



Preferences

Search

Appearance

Topology

Topology Line Style: Directed Line Style

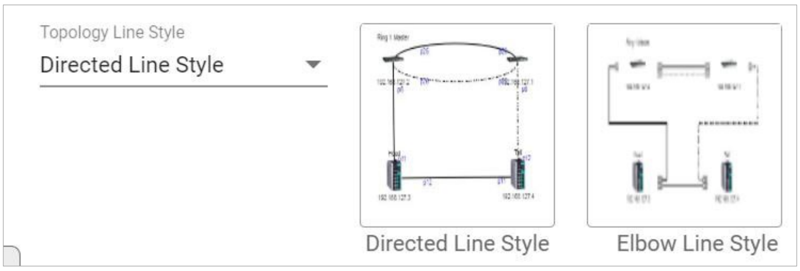
Directed Line Style

Elbow Line Style

Text Size

Text Size: Small

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

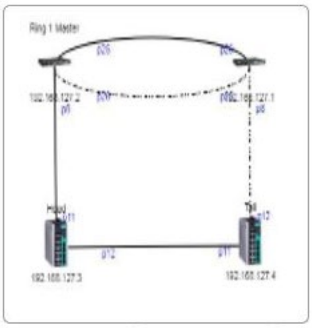


Topology Line Style

Directed Line Style

- **Directed Line Style**

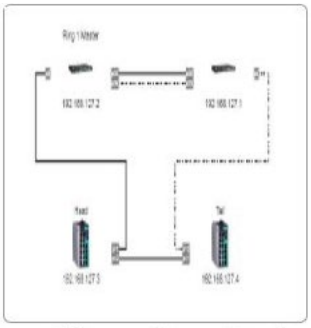
  MXview One applies the following style to the lines indicating the links between devices in the Topology Map:



Directed Line Style

- **Elbow Line Style**

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

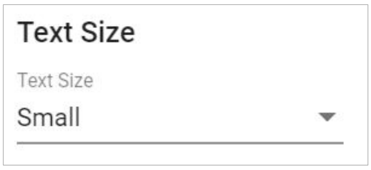


Elbow Line Style

4. To modify the text size in MXview One:

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

   - Large
   - Medium
   - Small

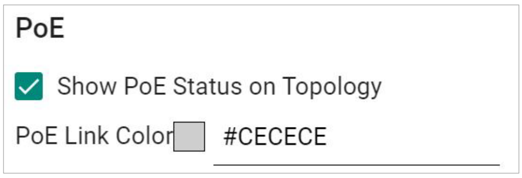


Text Size

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.

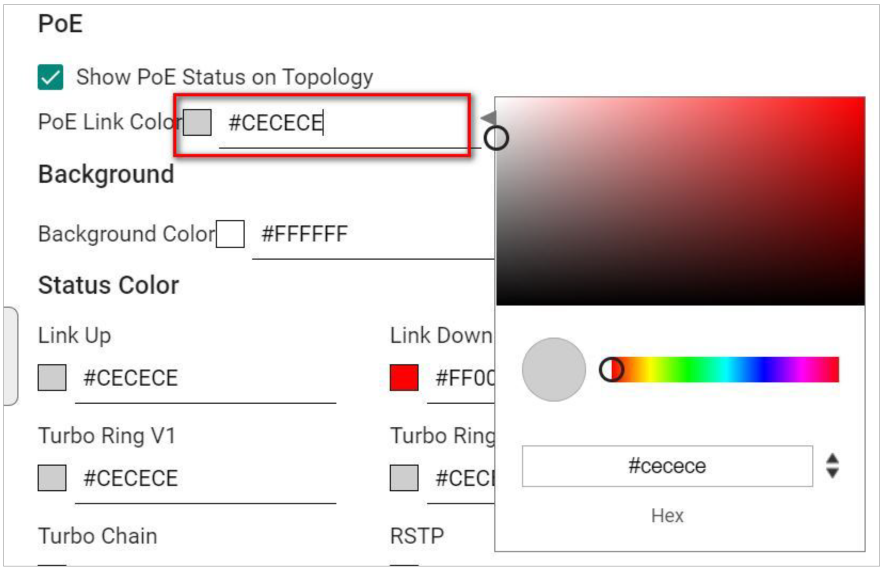


PoE

☑ 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

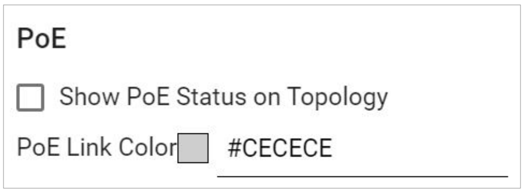
Turbo Ring #CECI

Turbo Chain

RSTP

#cecece

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

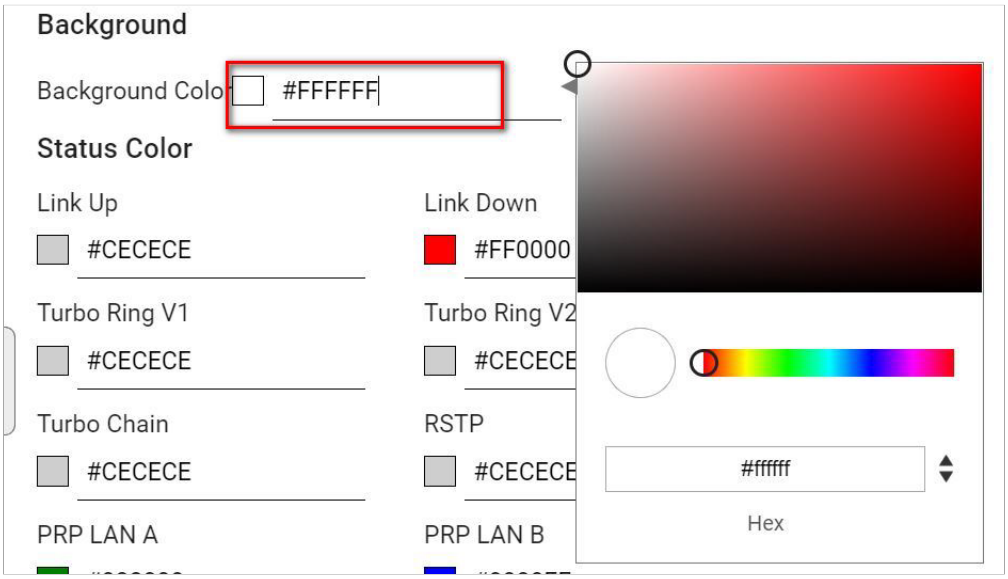


PoE

☐ 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

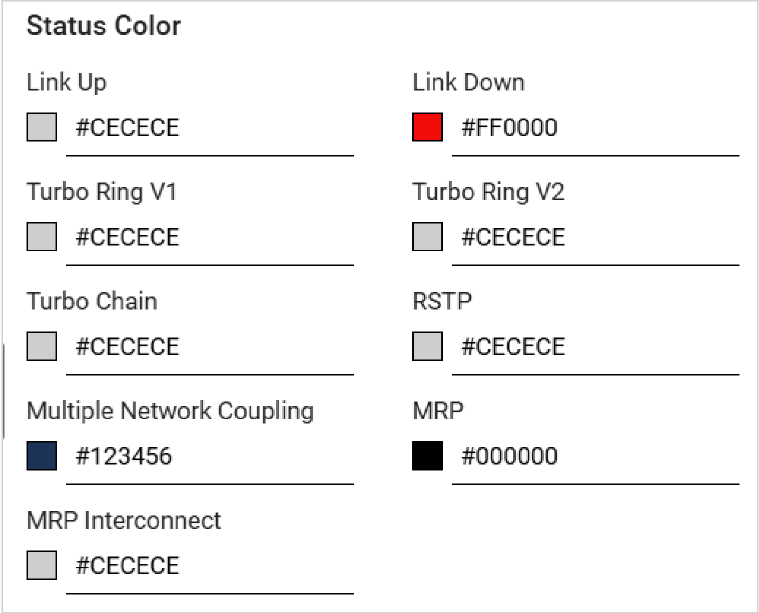
RSTP #CECECE

PRP LAN A

PRP LAN B

#ffffff

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
   - Multiple Network Coupling
   - MRP
   - MRP Interconnect



Status Color

Link Up
□ #CECECE

Link Down
🟥 #FF0000

Turbo Ring V1
□ #CECECE

Turbo Ring V2
□ #CECECE

Turbo Chain
□ #CECECE

RSTP
□ #CECECE

Multiple Network Coupling
■ #123456

MRP
■ #000000

MRP Interconnect
□ #CECECE

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

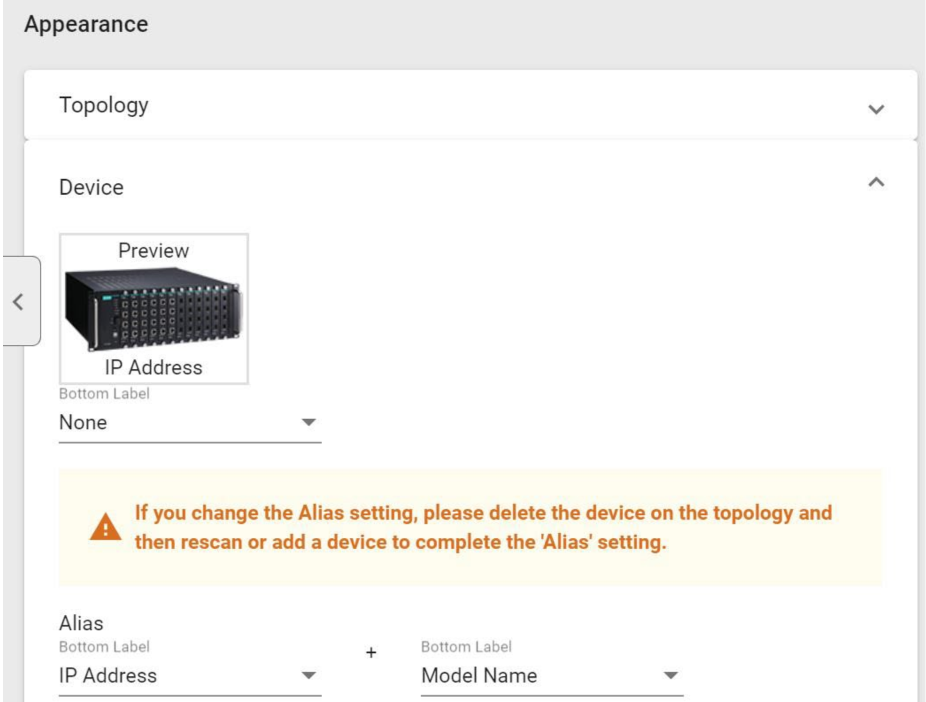
Use the **Preferences** screen to modify how devices appear in the Topology Map.

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

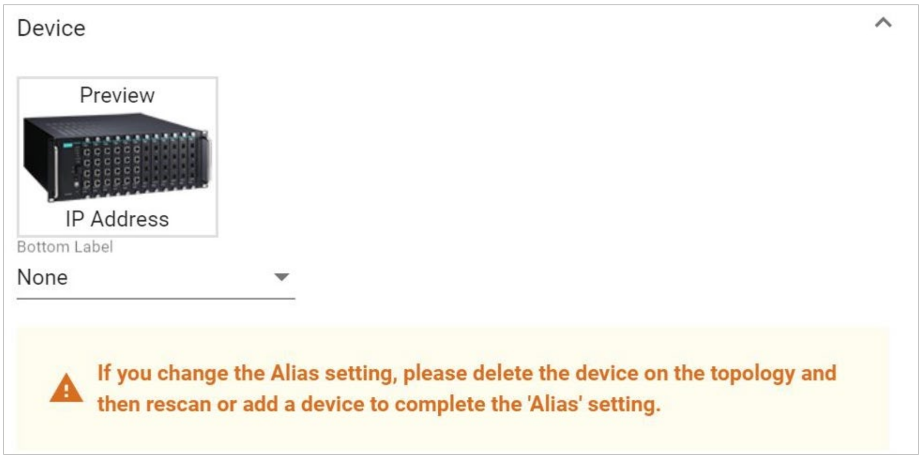
+

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

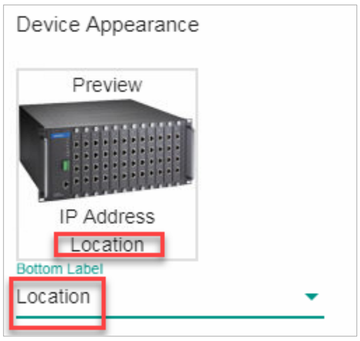
None

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.



Device Appearance

Preview

IP Address

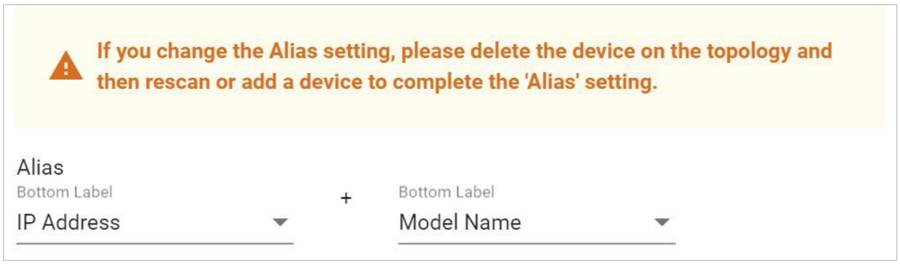
Location

Bottom Label

Location

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

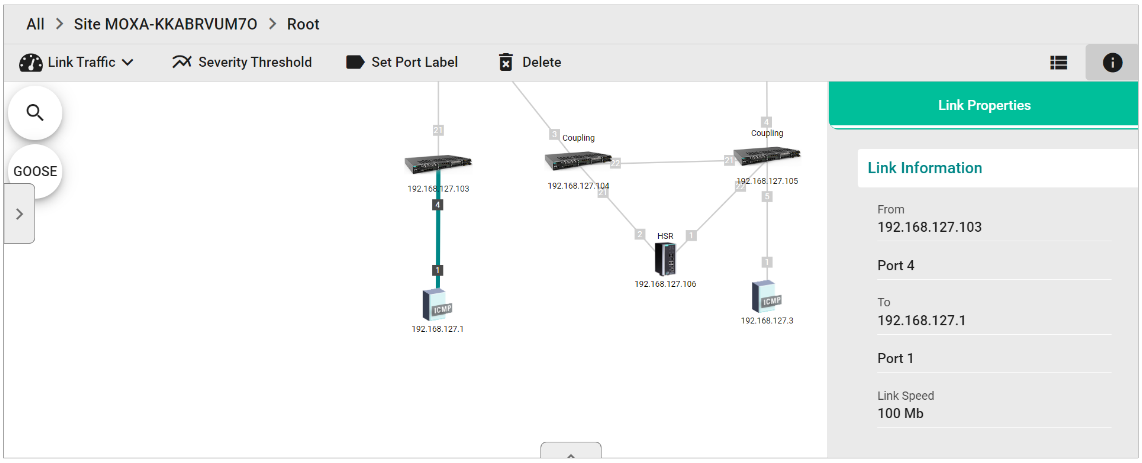
Click a link on the Topology Map to view link properties and perform the following:

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.



Link Information

From
192.168.127.103

Port 4

To
192.168.127.1

Port 1

Link Speed
100 Mb

Viewing Port Traffic

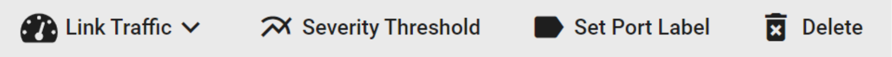
The **Port Traffic** screen displays a graph that shows the utilization percentage (Y-axis) over a specific time period (X-axis). You can also adjust the time period for the data that is displayed by changing the starting date and ending date. The minimum interval you can select is one day and the maximum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

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

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

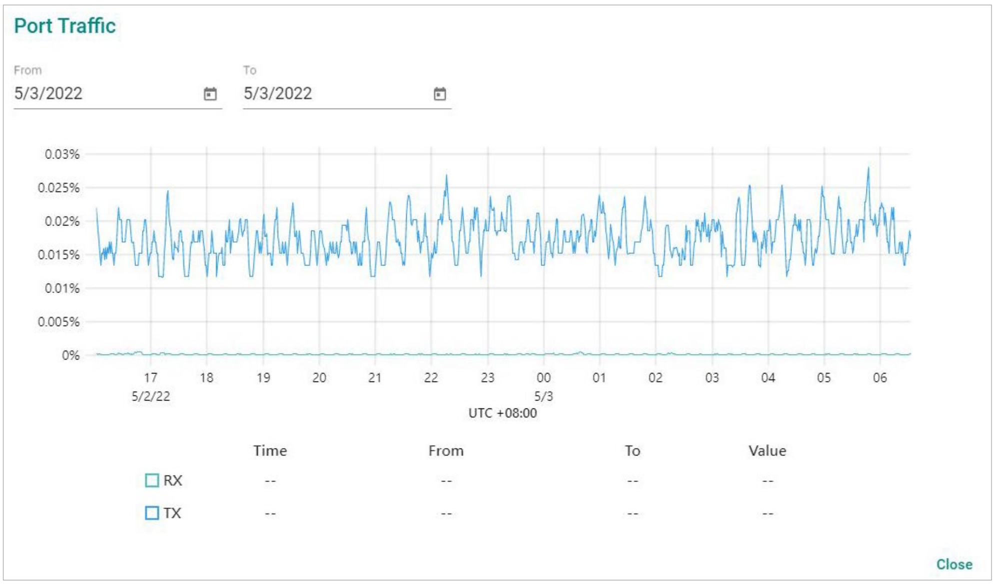
2. Click on a link between devices in the Topology Map.

   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	--	--	--	--

Close

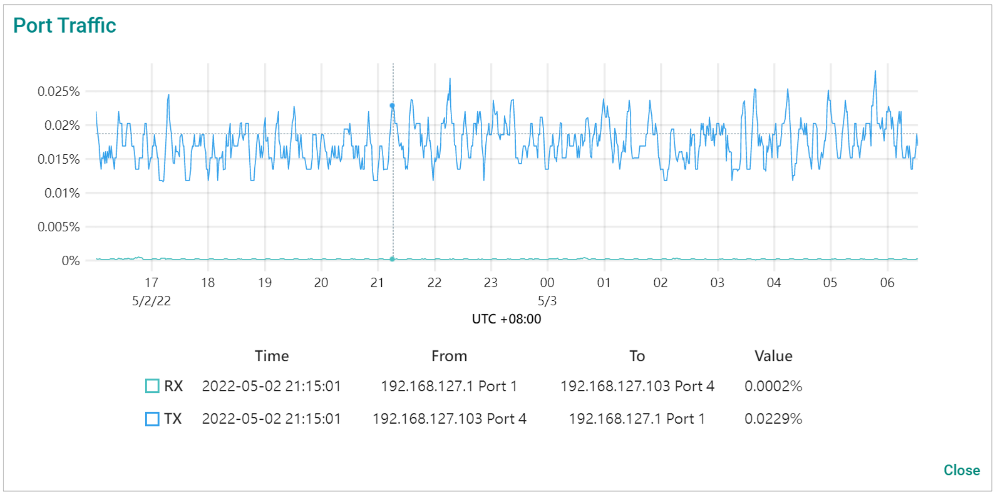
4. To adjust the time period for the graph data:

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

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

5. Hover over a line to view the direction of traffic.

   For example, the green line at the top of the following graph represents traffic from **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%

Close

Viewing Packet Error Rates

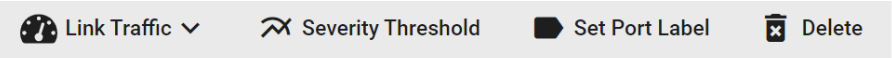
The **Packet Error Rate** screen displays a graph that shows the packet error rate (Y-axis) over a specific time period (X-axis). You can also adjust the time period for the data that is displayed by changing the start and end dates. The minimum interval is one day and the maximum interval you can select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

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

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

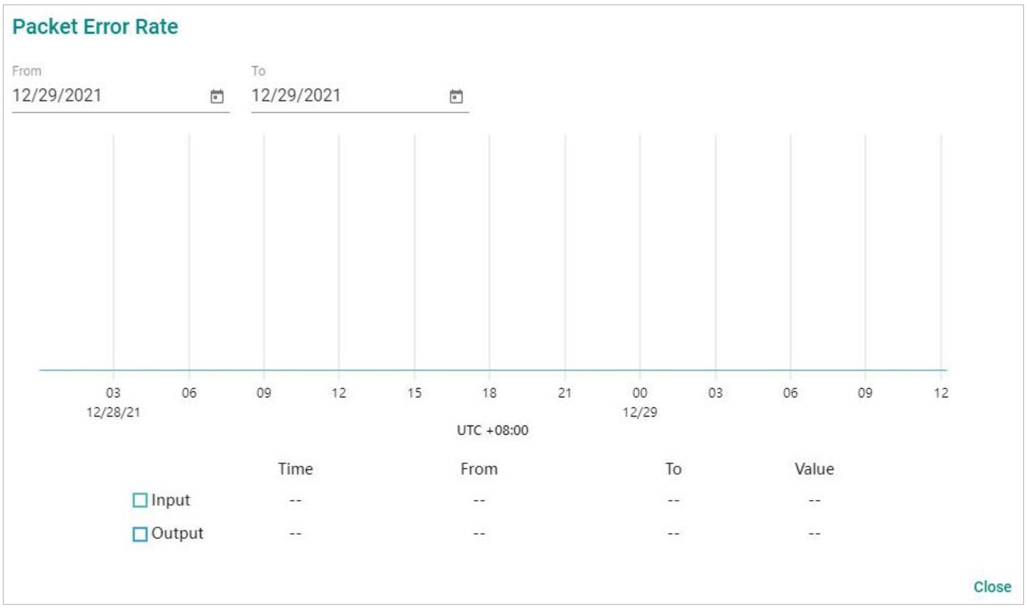
2. Click on a link between devices in the Topology Map.

   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

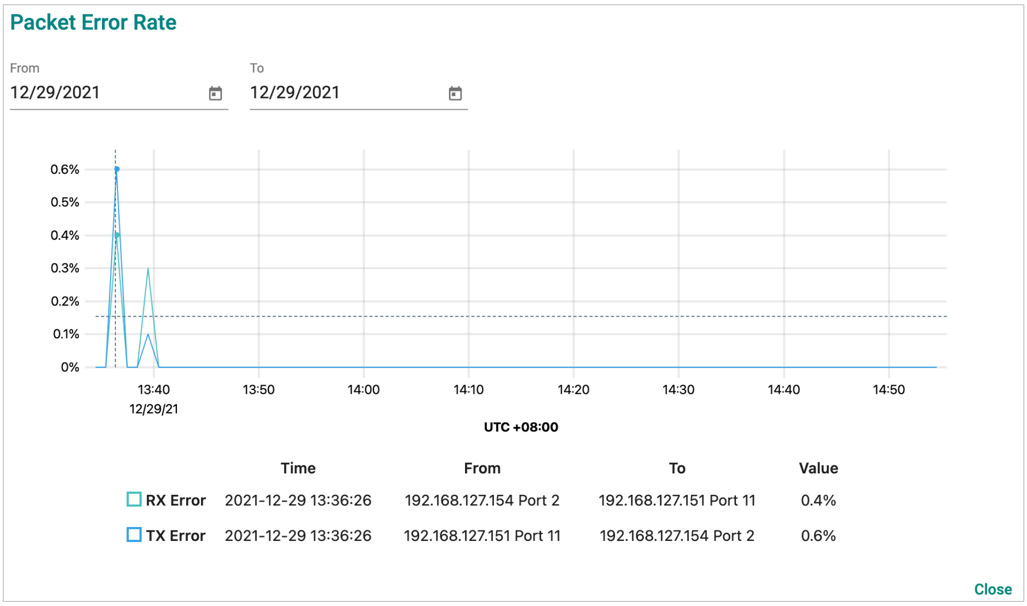
	Time	From	To	Value
□ Input	--	--	--	--
□ Output	--	--	--	--

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%

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.

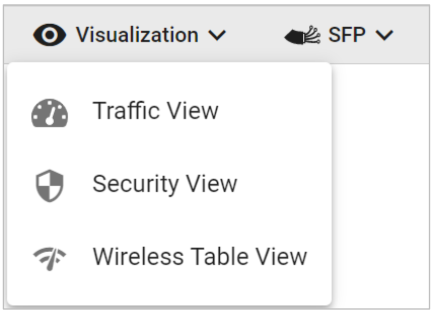
1. Navigate to **Menu** () **> Topology**.

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

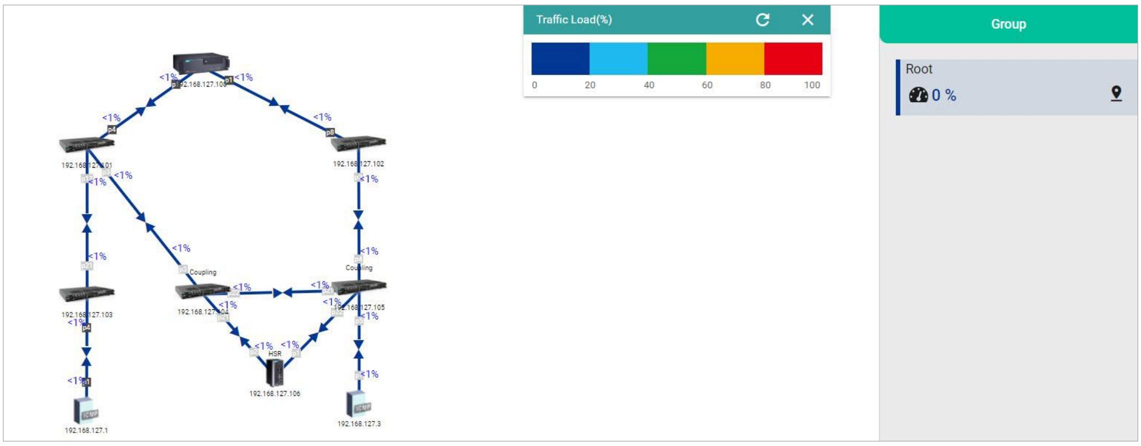
2. If **List view** is selected, click the **Topology view** () icon in the top right corner.

   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.



NOTE

The Group section on the right-hand side of the screen shows the link with the highest traffic load within each group.

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**.

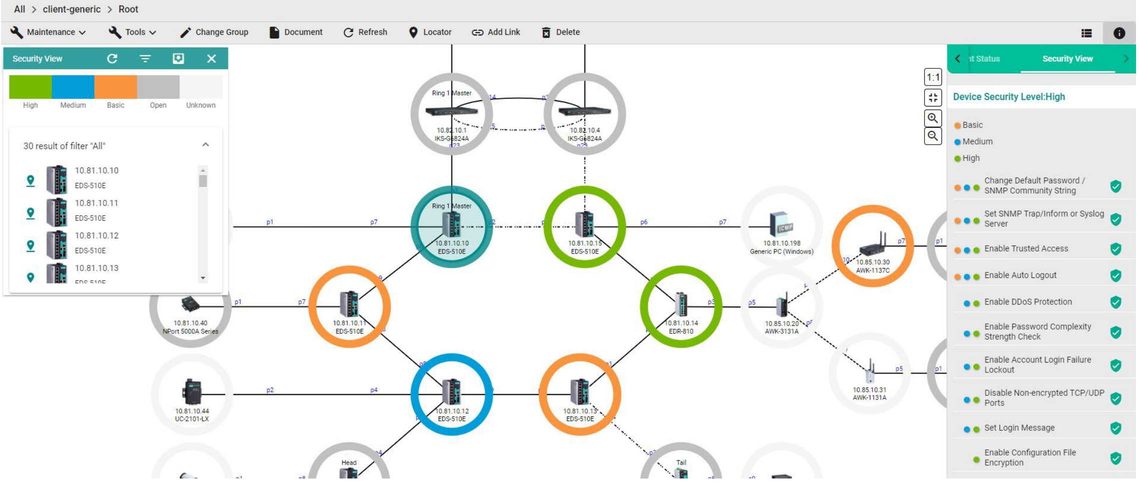
   The **Topology** screen will appear and display the Topology Map by default.

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	✓

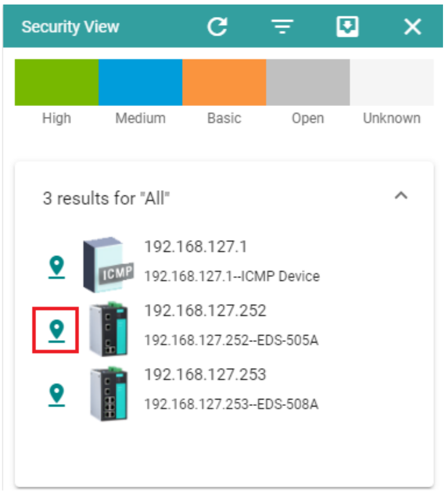
4. To filter the devices in the **Security View** window by security level:

   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.



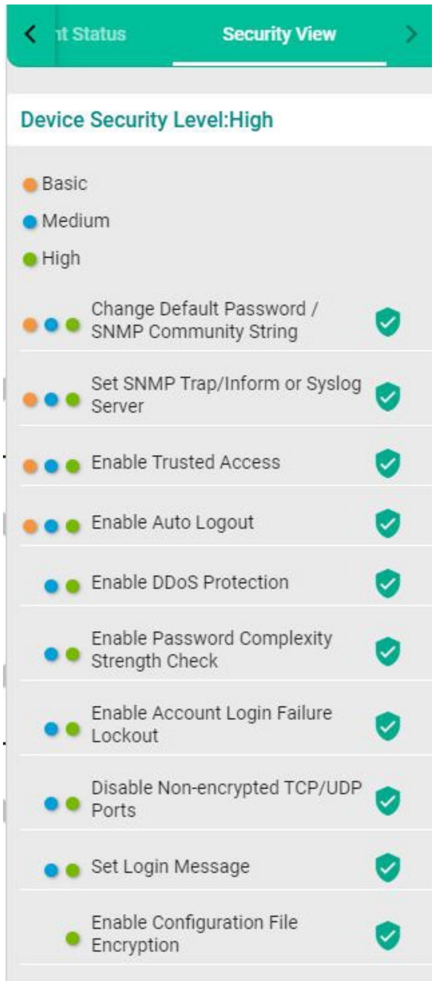
3 results for "All"

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 ✓

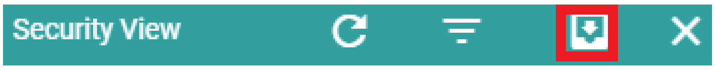
● Enable Configuration File Encryption ✓

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.



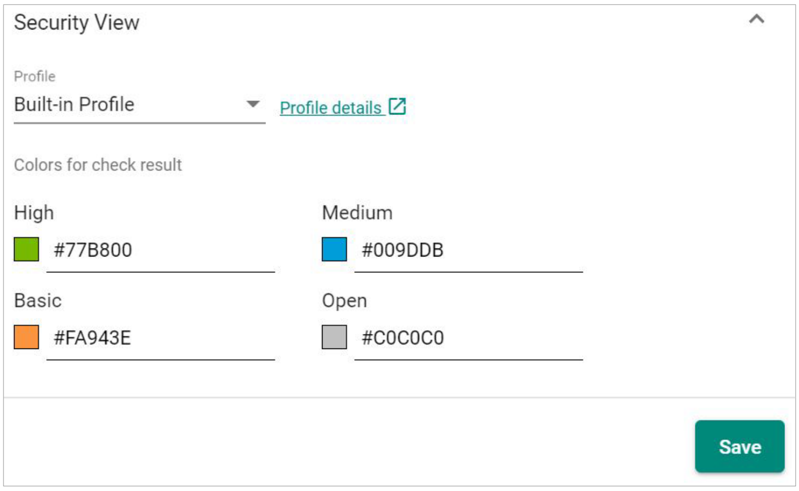
8. Review the following items in the Security View details pane:

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

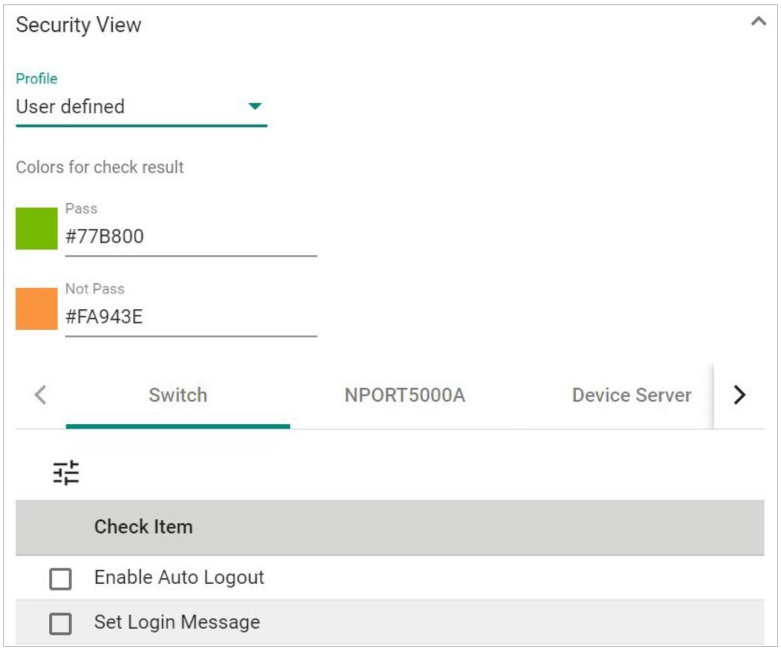
Medium
🟦 #009DDB

Basic
🟧 #FA943E

Open
⬜ #C0C0C0

   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.

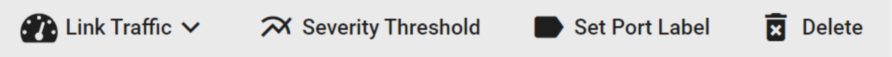
Since a link is bidirectional, the event will be triggered when the traffic condition in either direction satisfies the configured severity threshold.

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

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

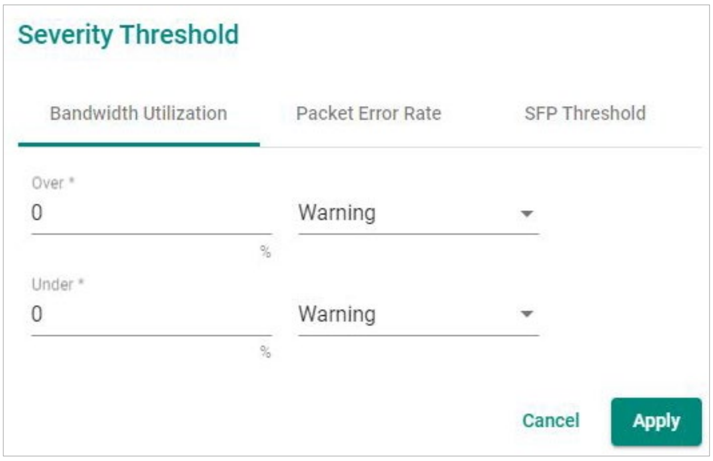
2. Click on a link between devices in the Topology Map.

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



3. Click **Severity Threshold**.

   The **Severity Threshold** screen will appear.

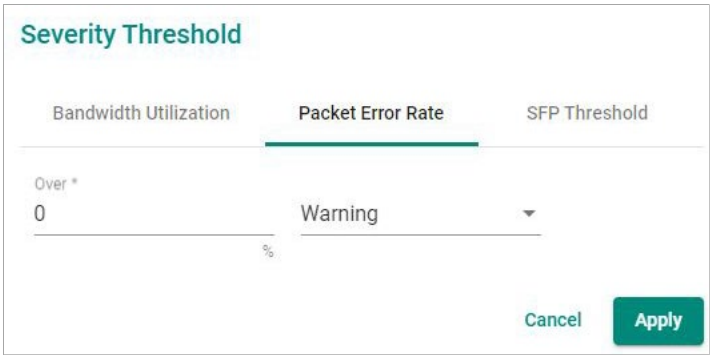


Severity Threshold

Bandwidth Utilization | Packet Error Rate | SFP Threshold

Over *
0 %
Warning

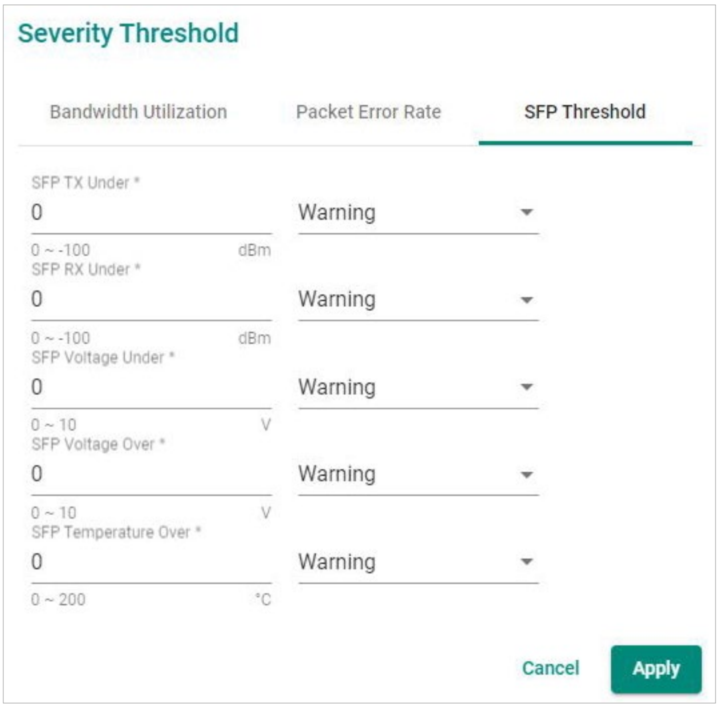
Under *
0 %
Warning



Severity Threshold

Bandwidth Utilization | Packet Error Rate | SFP 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.

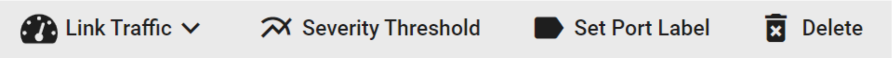
Configuring Custom Port Labels

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

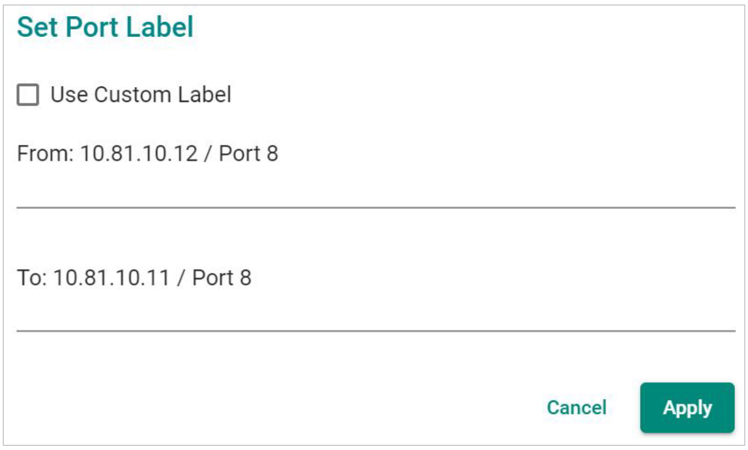
<Device IP Address> / <Port Number>

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

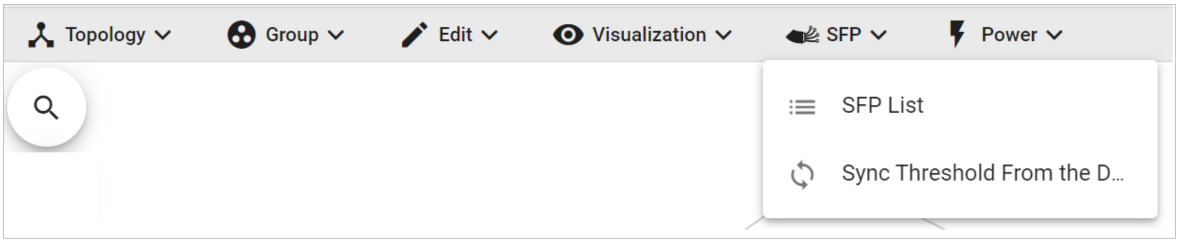
To: 10.81.10.11 / Port 8

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**.

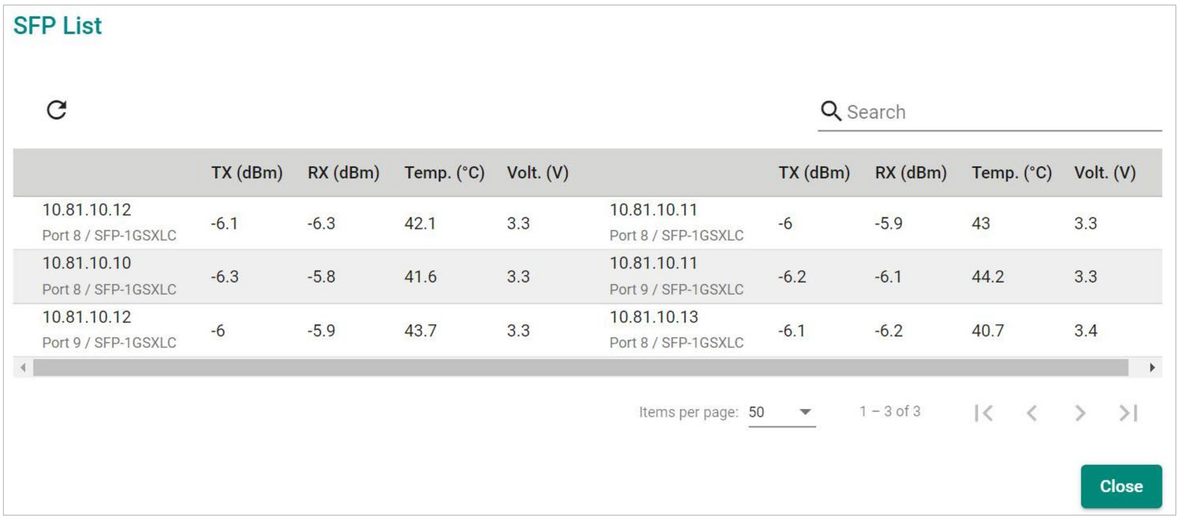
9. SFP Fiber Status

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

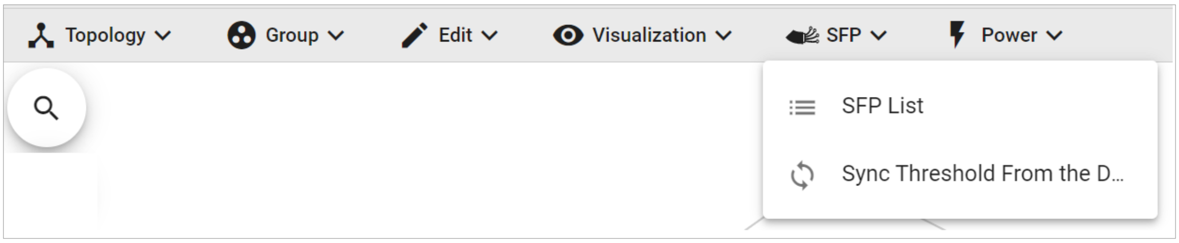
Items per page: 50 1 – 3 of 3

Close

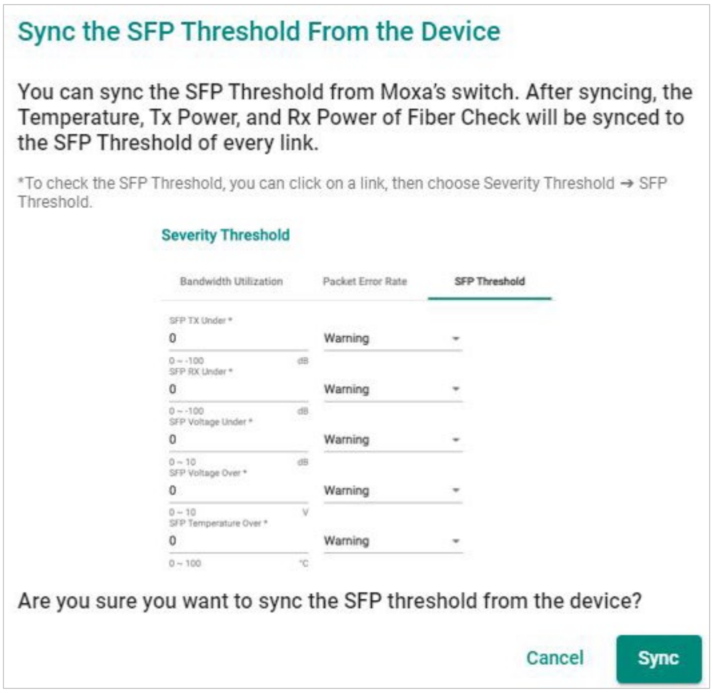
Synchronize the SFP Threshold From the Device

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

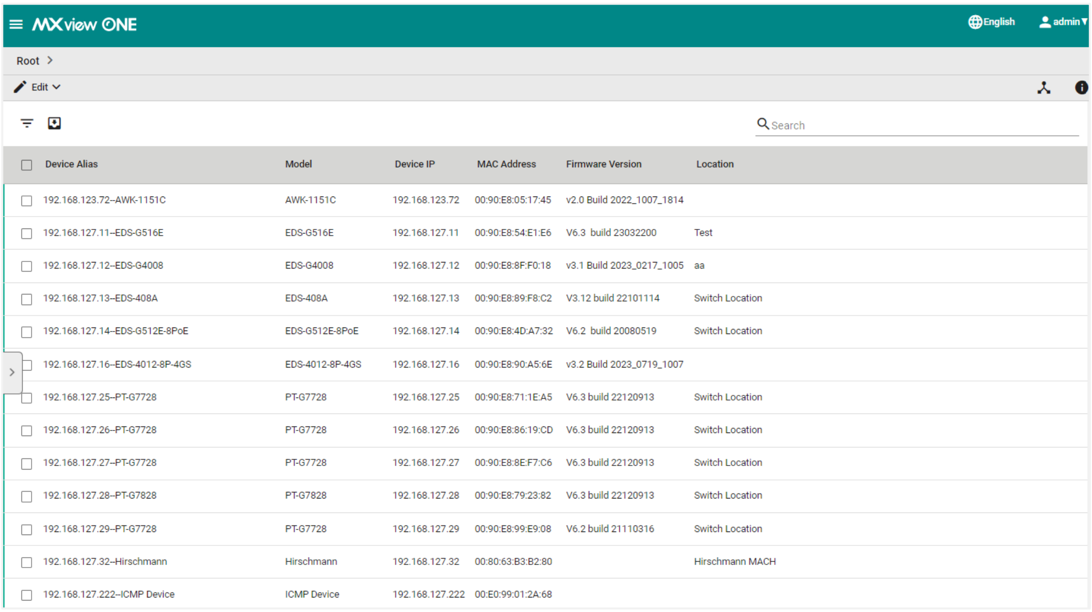
Are you sure you want to sync the SFP threshold from the device?

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.

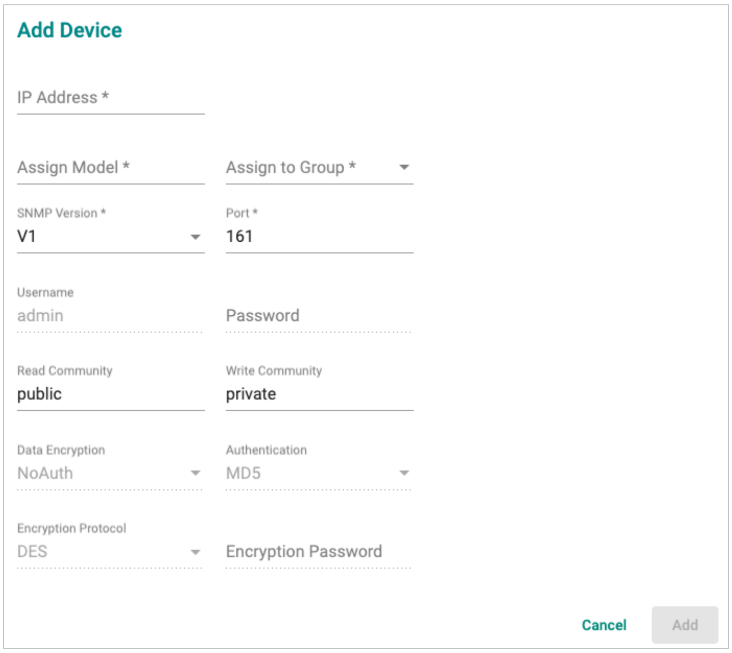
2. Click the **List view** (☰) icon in the top right corner.

   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**.

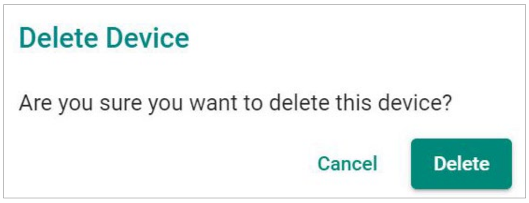
      MXview One adds the device to the topology.

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.

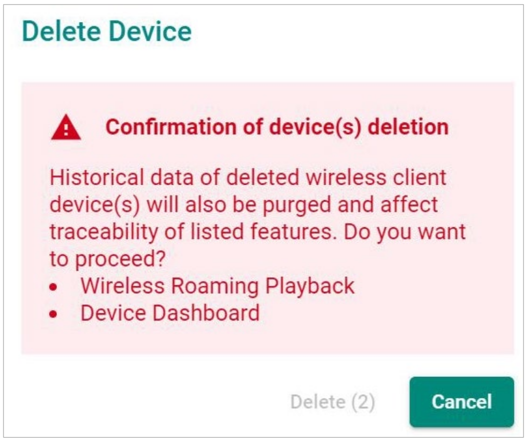
   c. For non AWK devices, read the message and then click **Delete** if you are sure you want to delete the device.



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?

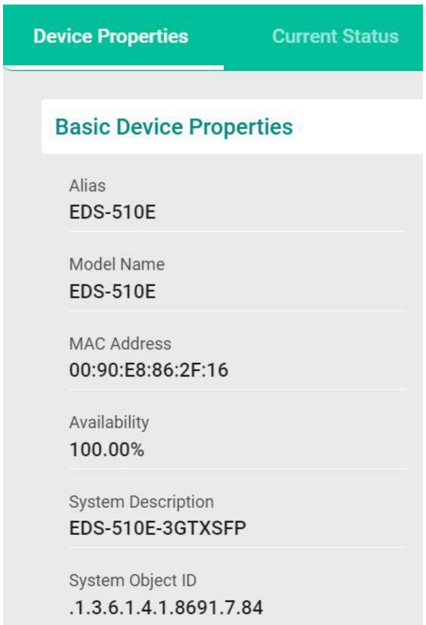
- Wireless Roaming Playback
- Device Dashboard

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%

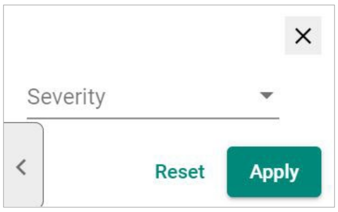
System Description
EDS-510E-3GTXSFP

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:

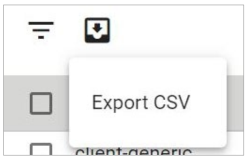
- **Critical**
- **Warning**
- **Information**

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.



Export CSV

client-generic

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.

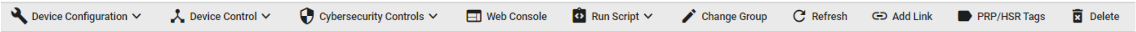
2. Select one of the following views:

   - **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:

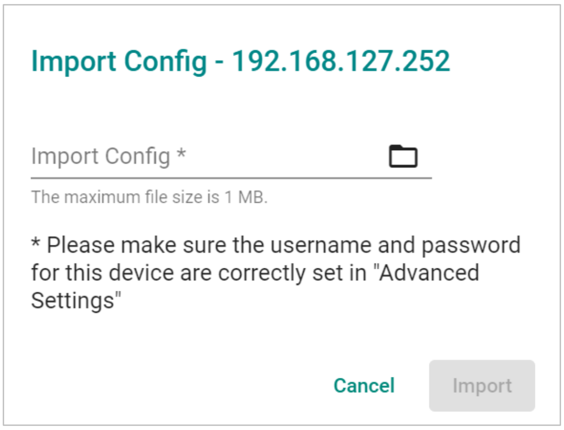
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the site name in the Device List.

   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.

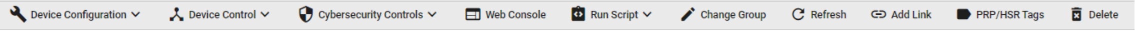
2. Select one of the following views:

   - **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.

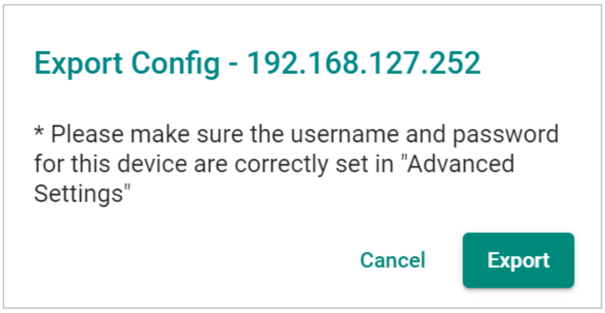
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the device in the Device List.

   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.

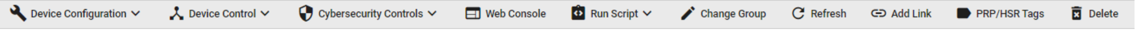
   b. **List view:** Displays a list of the devices in your network topology.

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

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

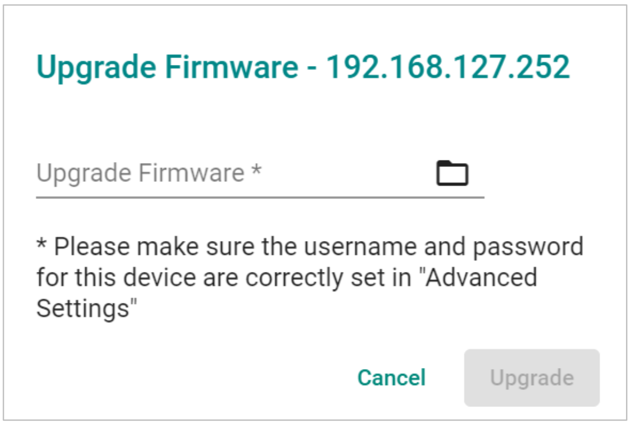
   ➢ **List view:** Select the check box next to the device in the Device List.

   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.

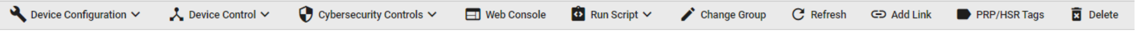
1. Navigate to **Menu** (≡) **> Topology**.

   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.

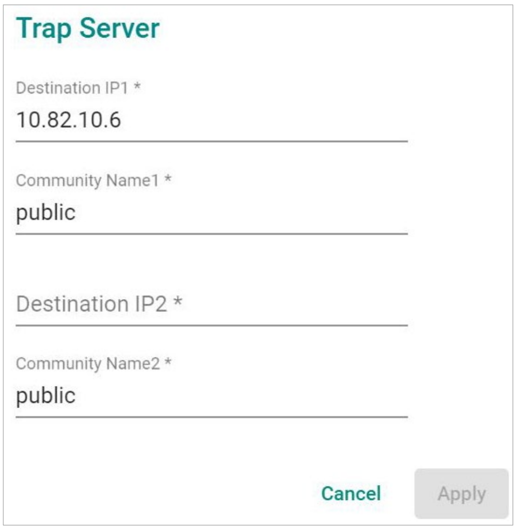
3. Select the device.
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the device in the Device List.

   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.

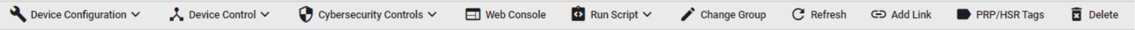
2. Select one of the following views:

   - **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.

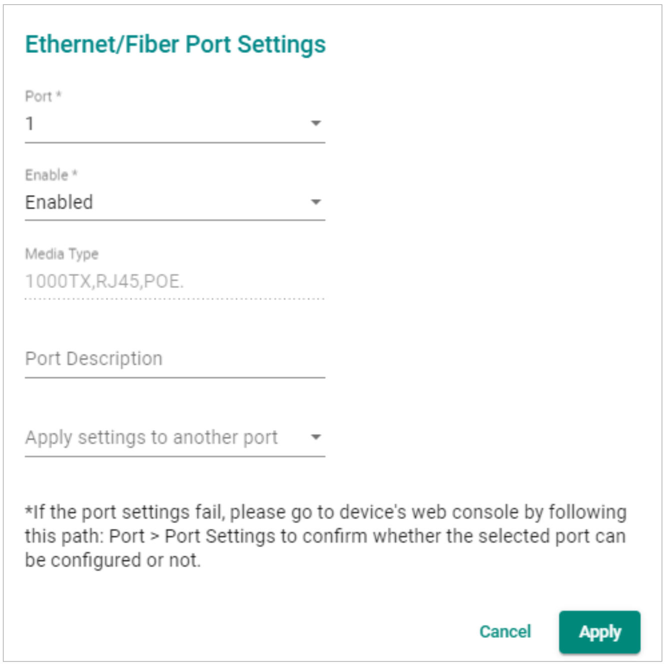
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the device in the Device List.

   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**.

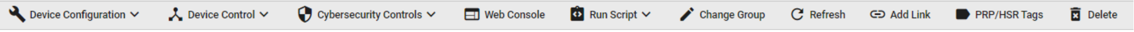
1. Navigate to **Menu** (☰) **> Topology**.

   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.

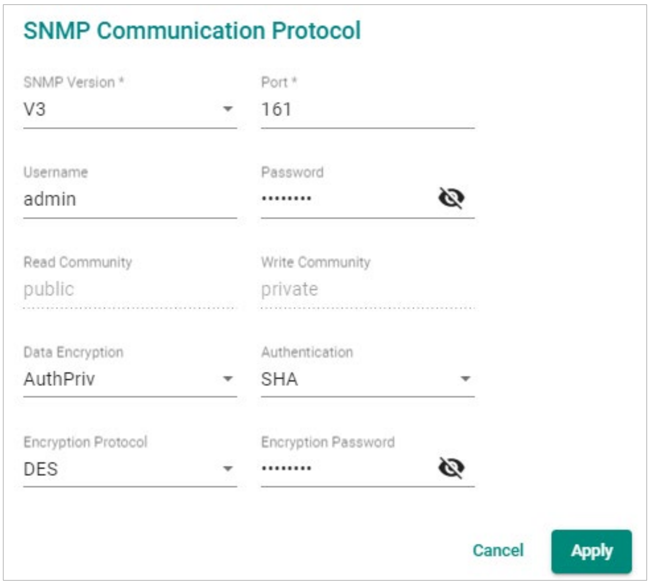
3. Select the device.
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the device in the Device List.

   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**.

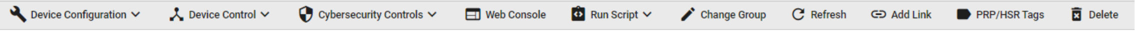
1. Navigate to **Menu** (☰) **> Topology**.

   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.

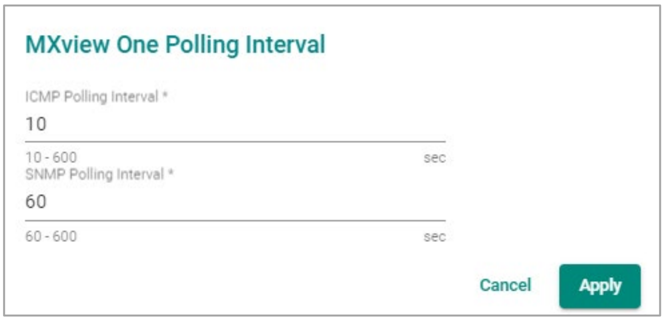
3. Select the device.
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the device in the Device List.

   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**.

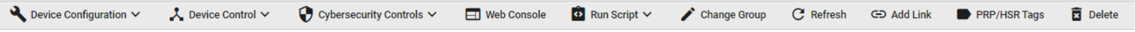
1. Navigate to **Menu** (☰) **> Topology**.

   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.

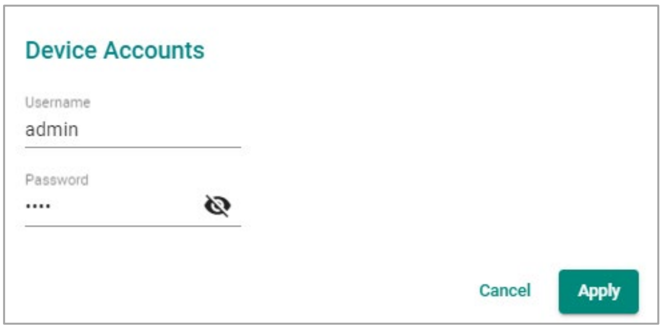
3. Select the device.
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the device in the Device List.

   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.

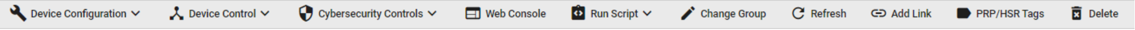
Modifying the Device Alias

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**.

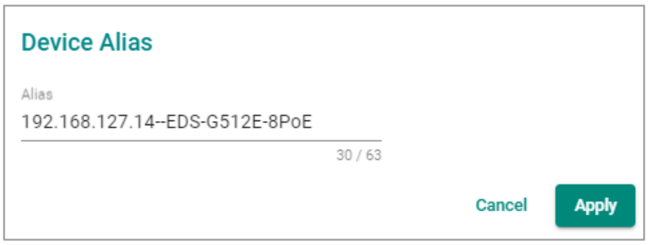
   The **Topology** screen will appear and display the Topology Map by default.
2. Select one of the following views:
   - **Topology view:** Displays a graphical representation of the devices in your network topology.
   - **List view:** Displays a list of the devices in your network topology.
3. Select 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.



Alias: 192.168.127.14--EDS-G512E-8PoE

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. You can change the icon for multiple devices at once.

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

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

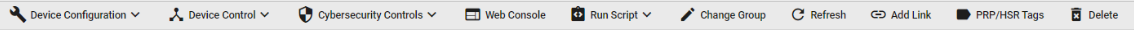
2. Select one of the following views:

   - **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(s).

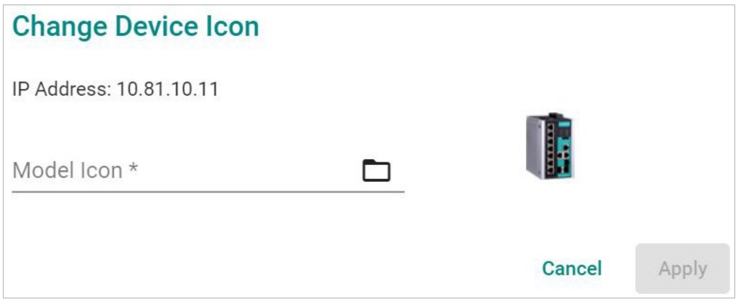
   - **Topology view:** Click the icon of the device in the Topology Map. To select multiple devices, click and drag over the devices or CTRL + left-click the devices individually.
   - **List view:** Select the check box next to the device(s) in the Device List.

   The toolbar options will change.



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

   The **Change Device Icon** screen appears.



Change Device Icon

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(s) to the uploaded JPG, GIF, or PNG image file.

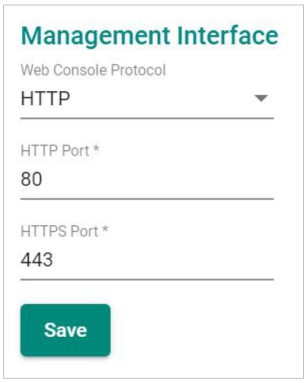
Signing on to Device Web Consoles

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.



Management Interface

Web Console Protocol: HTTP

HTTP Port *: 80

HTTPS Port *: 443

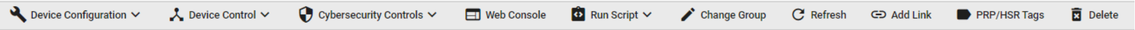
   c. Configure the following:
      - **Web Console Protocol**
      - **HTTP Port**
      - **HTTPS Port**
   d. Click **Save**.
      MXview One updates the web console protocol settings.

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**.

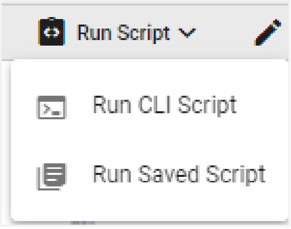
   The device web console will successfully log in.

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.

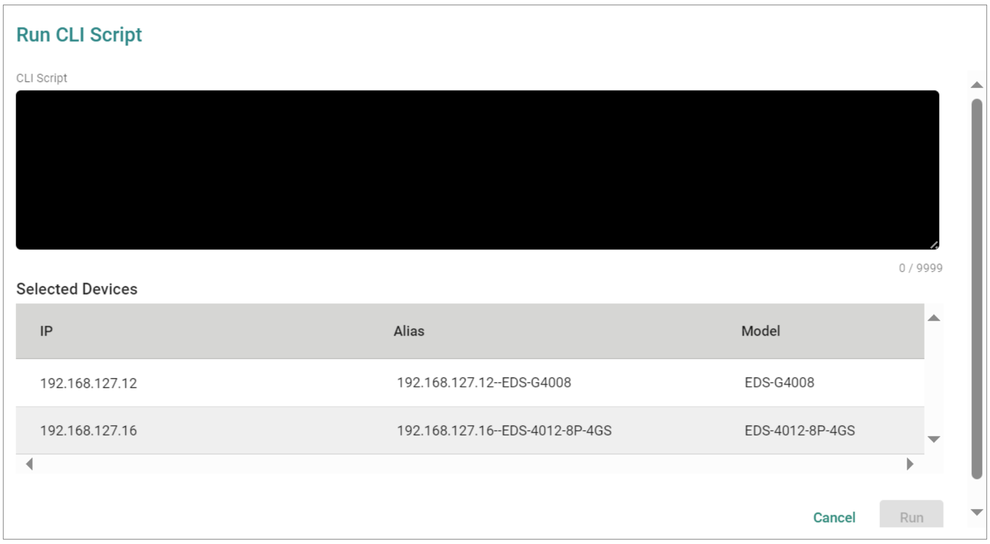
Click the **Run Script** ( ) icon in the menu bar to expand the script functions. There are two main functions:

- **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

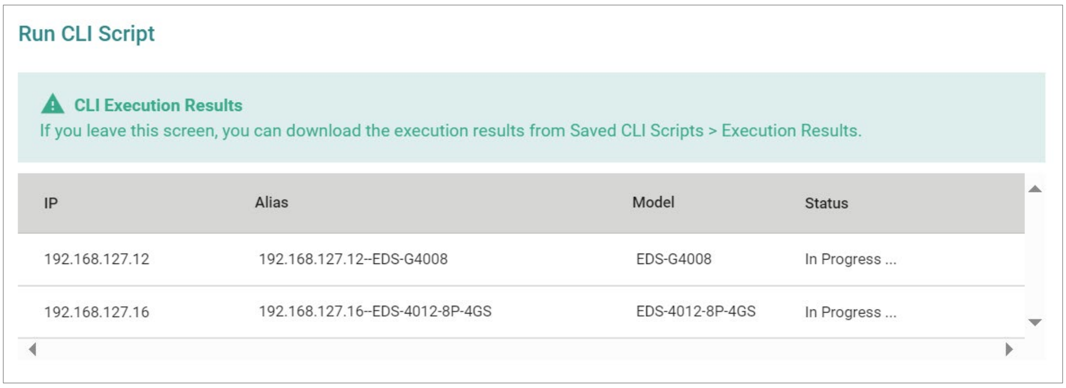
0 / 9999

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.

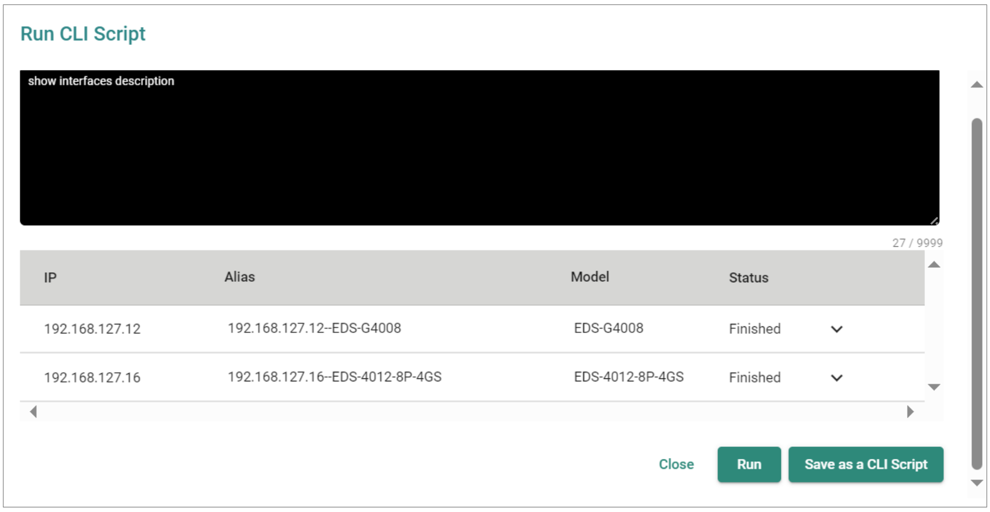
IP	Alias	Model	Status
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008	In Progress ...
192.168.127.16	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	In Progress ...

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
```

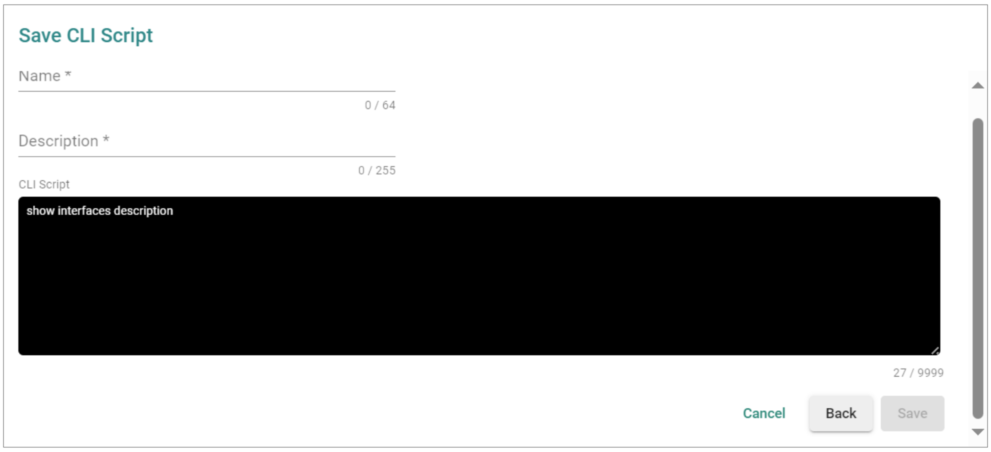
27 / 9999

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
```

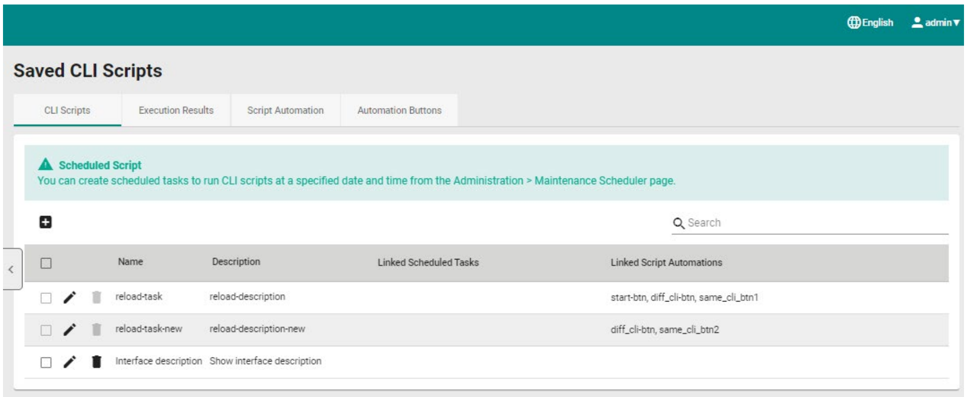
27 / 9999

      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

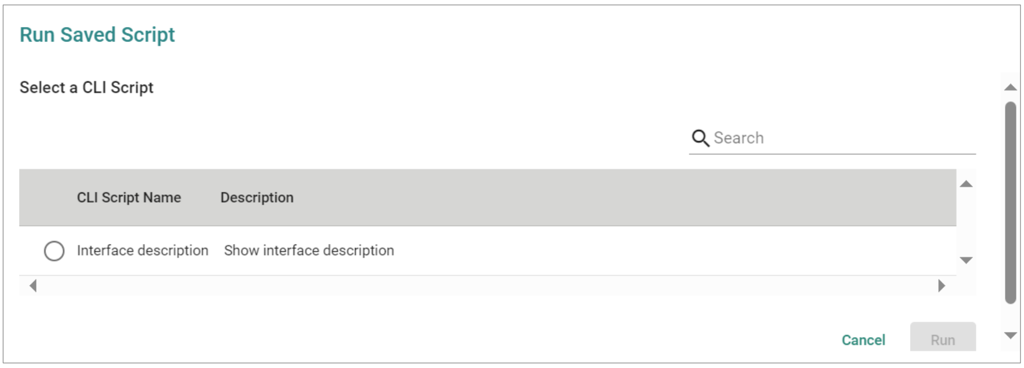
Scheduled Script
You can create scheduled tasks to run CLI scripts at a specified date and time from the Administration > Maintenance Scheduler page.

□	Name	Description	Linked Scheduled Tasks	Linked Script Automations
□	reload-task	reload-description		start-btn, diff_cli-btn, same_cli_btn1
□	reload-task-new	reload-description-new		diff_cli-btn, same_cli_btn2
□	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.



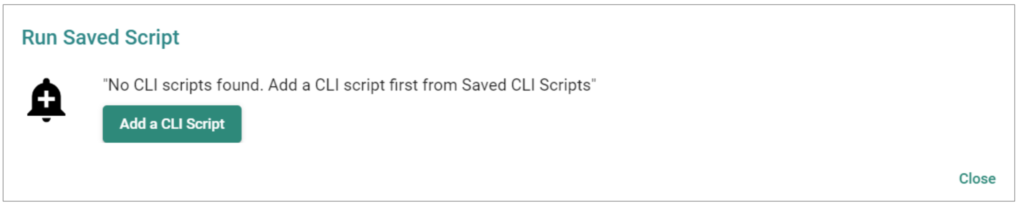
Run Saved Script

Select a CLI Script

Search

	CLI Script Name	Description
○	Interface description	Show interface description

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

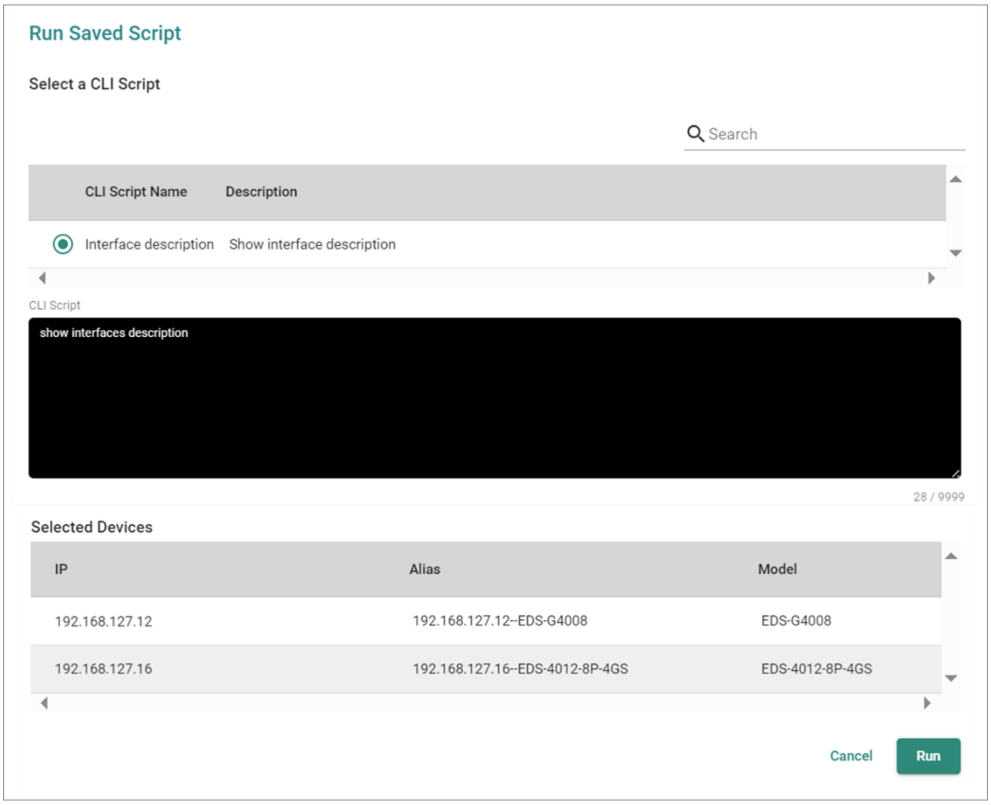


Run Saved Script

"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

Search

	CLI Script Name	Description
●	Interface description	Show interface description

CLI Script

```
show interfaces description
```

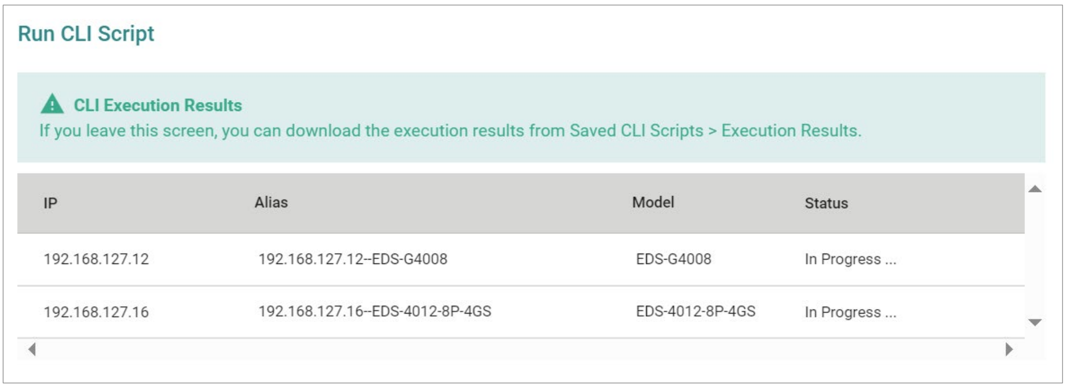
28 / 9999

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.

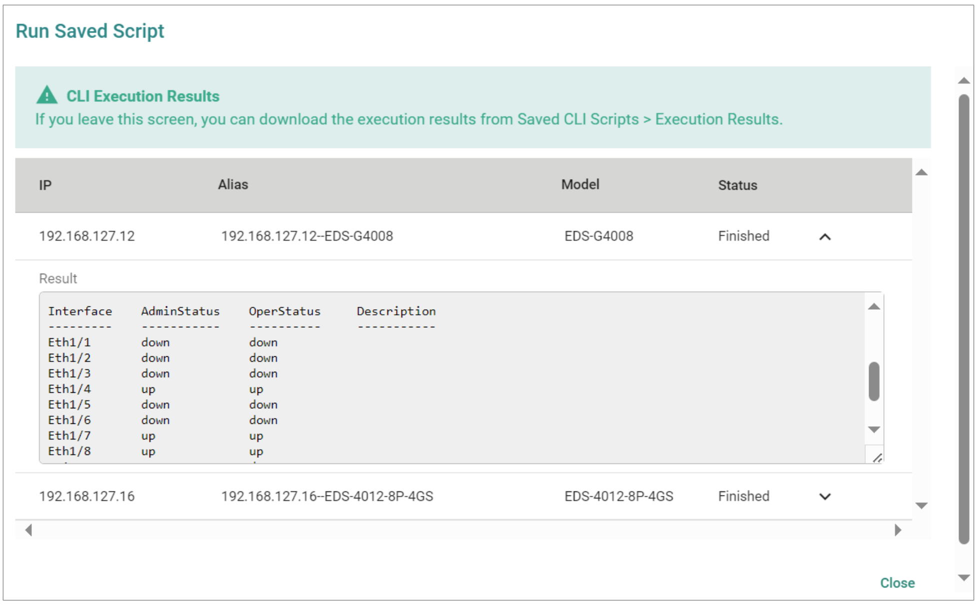
IP	Alias	Model	Status
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008	In Progress ...
192.168.127.16	192.168.127.16--EDS-4012-8P-4GS	EDS-4012-8P-4GS	In Progress ...

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**.

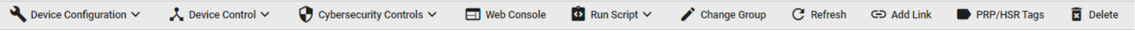
1. Navigate to **Menu** (☰) **> Topology**.

   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.

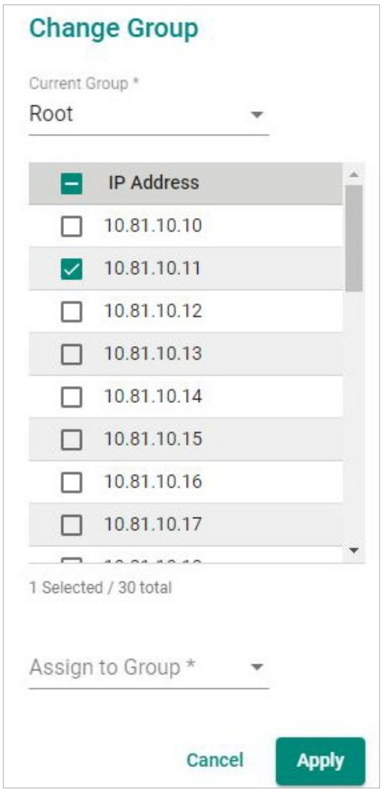
3. Select the device.
   - **Topology view:** Click the icon of the device in the Topology Map.
   - **List view:** Select the check box next to the device in the Device List.

   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**.

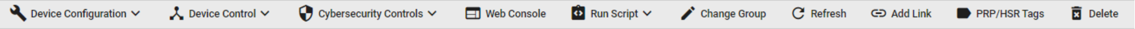
1. Navigate to **Menu** (☰) **> Topology**.

   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.

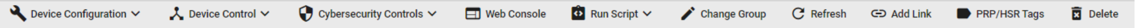
1. Navigate to **Menu** (☰) **> Topology**.

   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** feature lets users perform certain functions directly from within MXview One, without having to enter the device's web console. This feature covers two sections: **Configuration and Control** and **Account and Password**.

The **Device Configuration and Control** section provides quick access buttons to quickly execute commonly used device management functions. Users can perform these functions either from the menu bar on the **Topology** screen, or directly from the **Configuration and Control** page.

The **Account and Password** section allows administrators to check device accounts and perform account and default password audits.

Configuration and Control

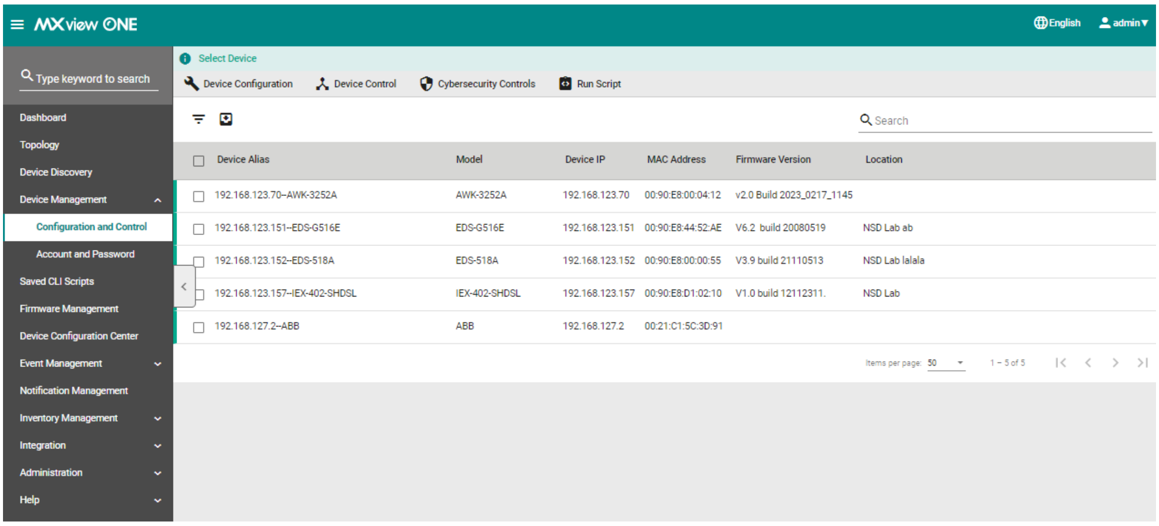
Configuration and Control Overview

To access the Configuration and Control page, in the function tree, navigate to **Menu (☰) > Device Management> Configuration and Control**.

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
□ 192.168.123.70--AWK-3252A	AWK-3252A	192.168.123.70	00:90:E8:00:04:12	v2.0 Build 2023_0217_1145	
□ 192.168.123.151--EDS-G516E	EDS-G516E	192.168.123.151	00:90:E8:44:52:AE	V6.2 build 20080519	NSD Lab ab
□ 192.168.123.152--EDS-518A	EDS-518A	192.168.123.152	00:90:E8:00:00:55	V3.9 build 21110513	NSD Lab lalala
□ 192.168.123.157--IEX-402-SHDSL	IEX-402-SHDSL	192.168.123.157	00:90:E8:D1:02:10	V1.0 build 12112311.	NSD Lab
□ 192.168.127.2--ABB	ABB	192.168.127.2	00:21:C1:5C:3D:91		

Items per page: 50 1 – 5 of 5

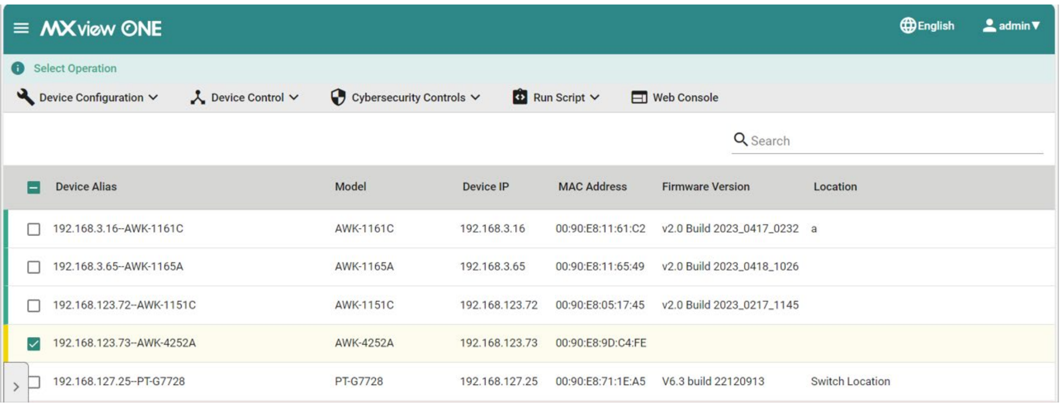
Refer to the following section for an overview of all functions in each category.

Device Configuration

Change Wi-Fi Channel

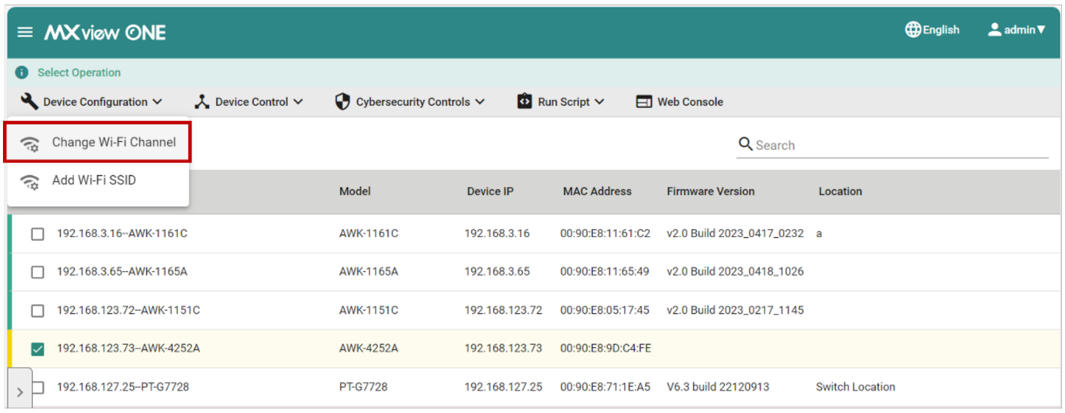
If the performance of your wireless devices is affected by interruptions in the current Wi-Fi channel, you can use the Change Wi-Fi Channel function to switch to another channel to improve performance.

1. Navigate to **Menu** (≡) **> Device Management> Configuration and Control**.
2. Select the device(s) to configure from the device list.



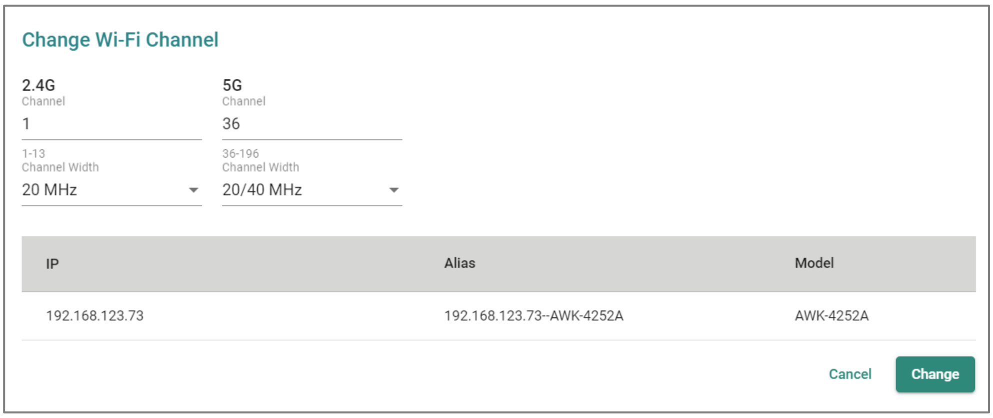
	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.3.16–AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
□	192.168.3.65–AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
□	192.168.123.72–AWK-1151C	AWK-1151C	192.168.123.72	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

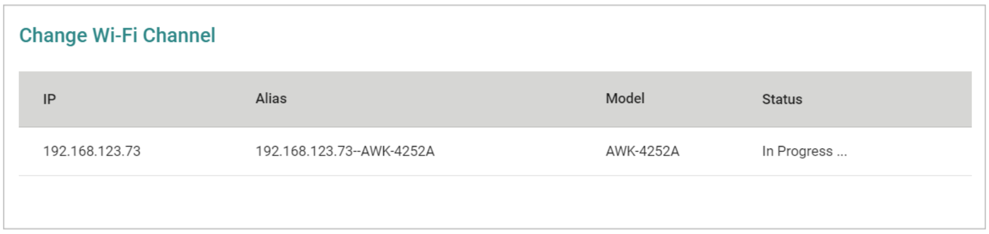
2.4G
Channel: 1
1-13
Channel Width: 20 MHz

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
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

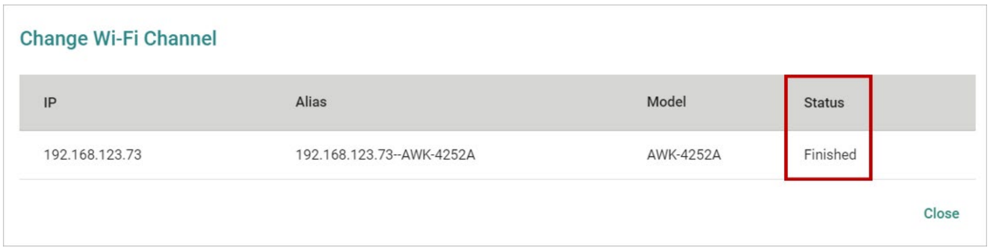
5. When finished, click **Change**. The system will execute the action.



Change Wi-Fi Channel

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

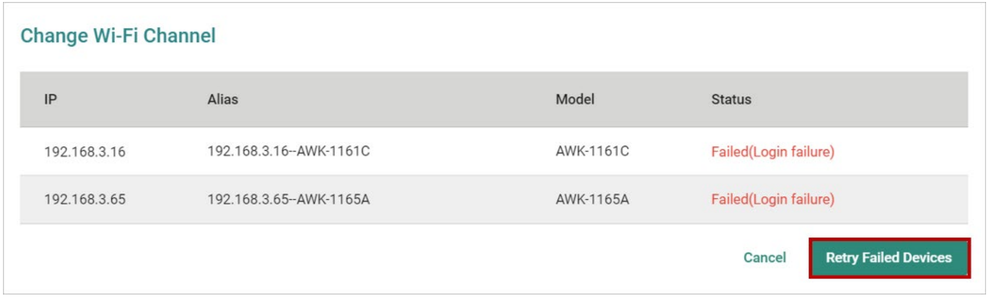
6. If successful, a confirmation will be shown in the Status column.



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.



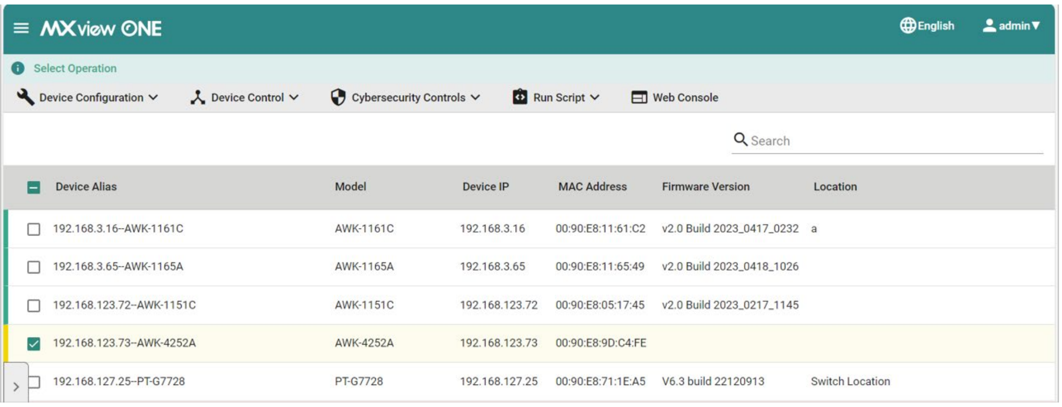
Change Wi-Fi Channel

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

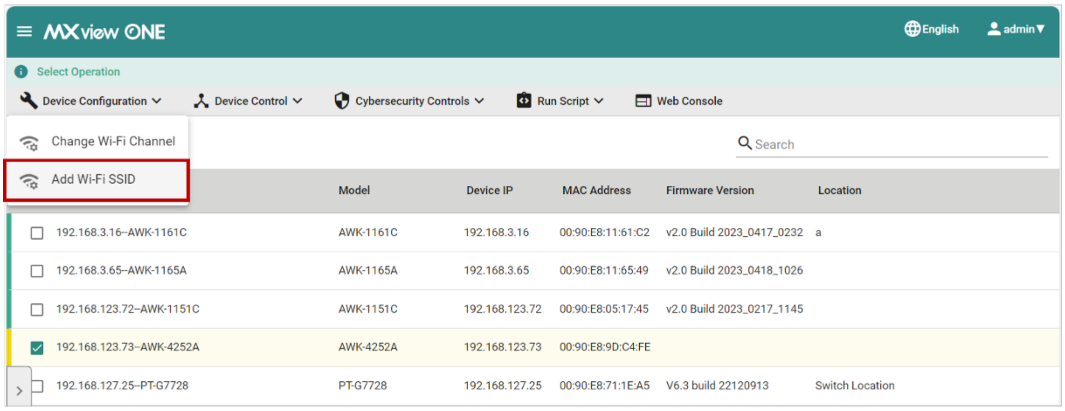
Use the **Add Wi-Fi SSID** function to create additional Wi-Fi SSIDs for your wireless environment.

1. Navigate to **Menu** (≡) **> Device Management > Configuration and Control**.
2. Select the device(s) to configure from the device list.



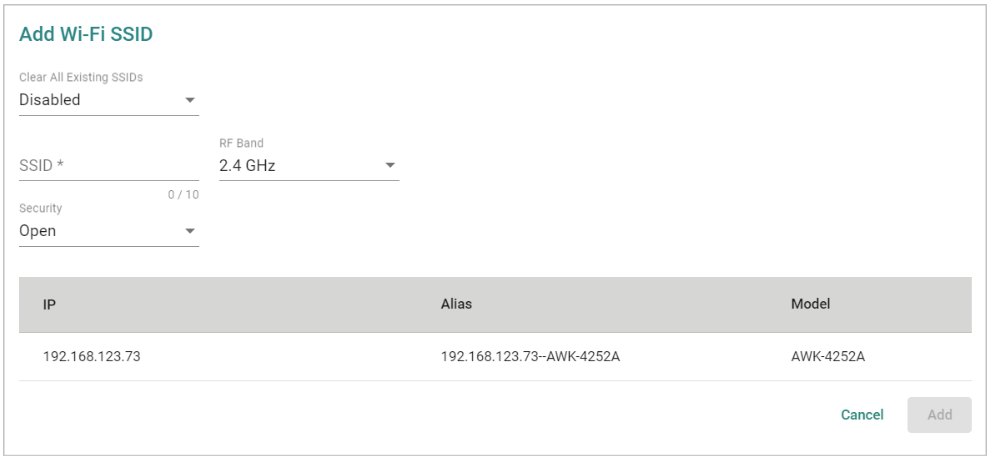
	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.3.16--AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
□	192.168.3.65--AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
□	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	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.

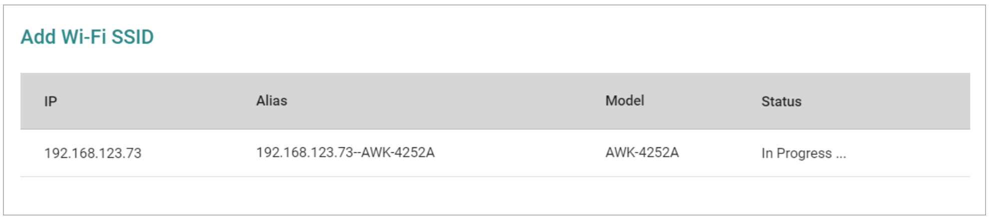
EAPOL Version

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.

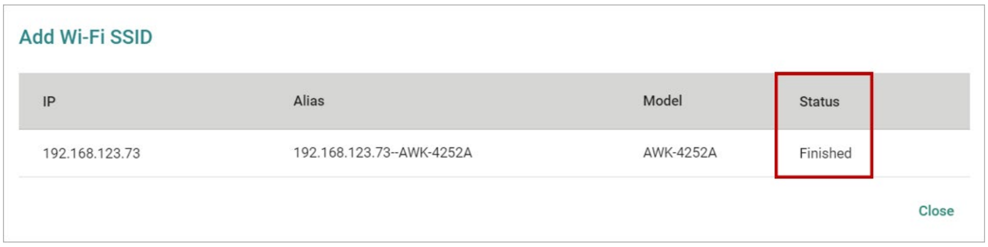
5. When finished, click **Add**. The system will execute the action.



Add Wi-Fi SSID

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

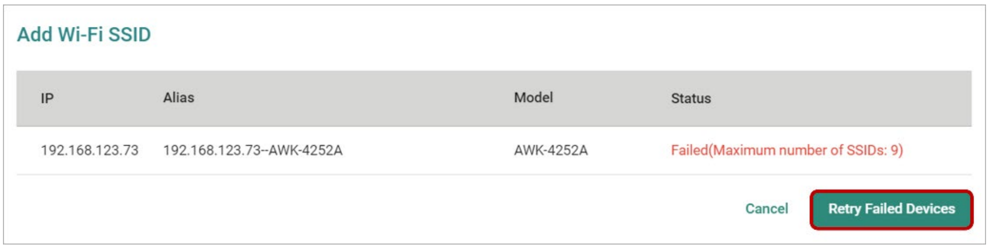
6. If successful, a confirmation will be shown in the Status column.



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

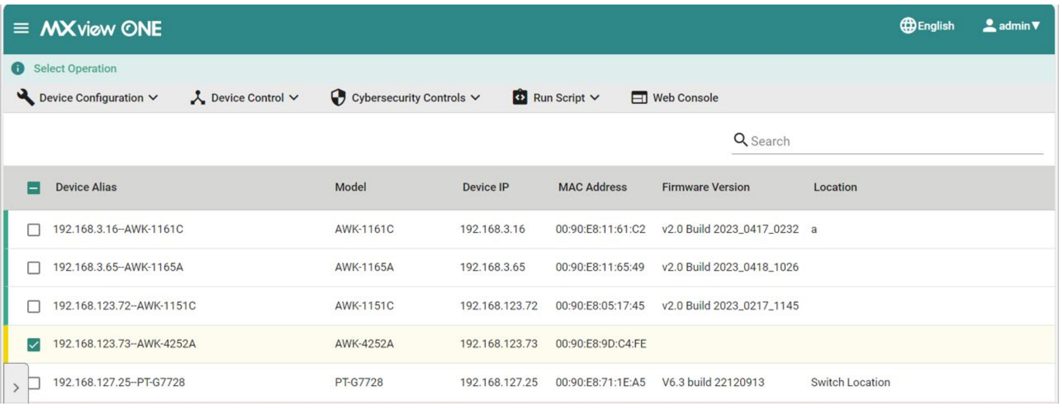
IP	Alias	Model	Status
192.168.123.73	192.168.123.73--AWK-4252A	AWK-4252A	Failed(Maximum number of SSIDs: 9)

Dynamic Sticky MAC

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

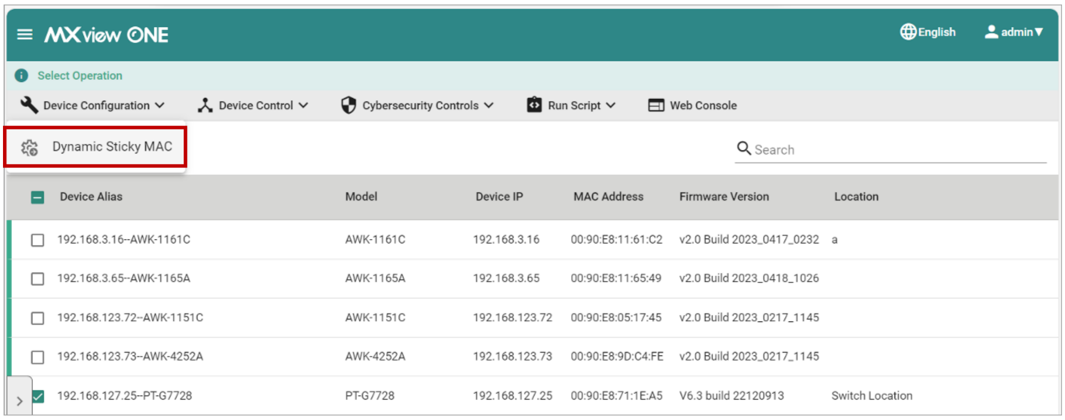
1. Navigate to **Menu** (☰) **> Device Management > Configuration and Control**.

2. Select 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

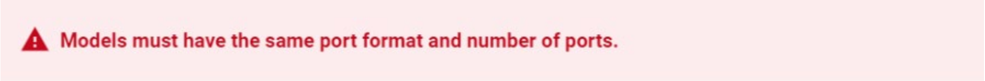
3. From the **Device Configuration** drop-down list, select **Dynamic Sticky MAC**.
The **Dynamic Sticky MAC** screen will appear.



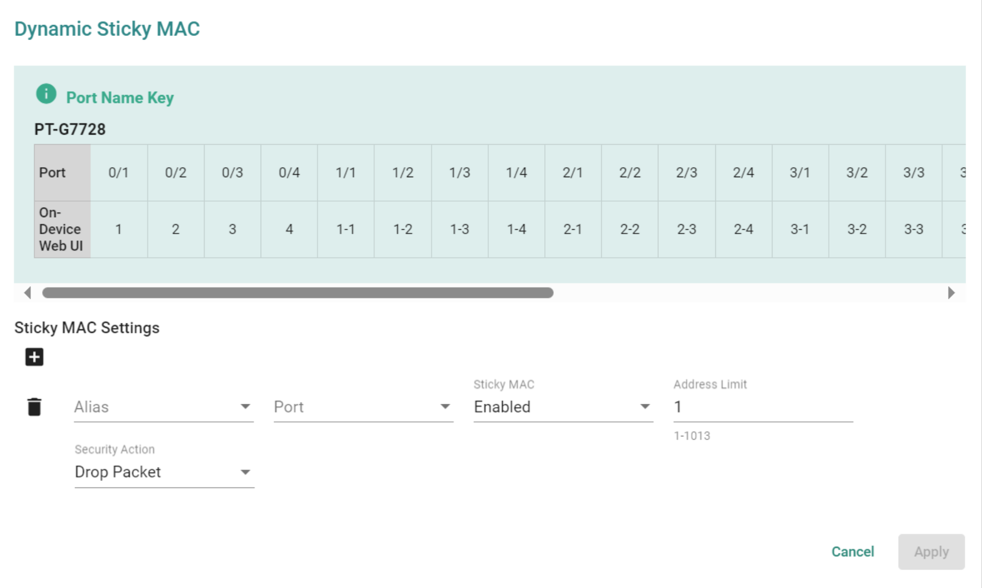
	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.3.16–AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
□	192.168.3.65–AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
□	192.168.123.72–AWK-1151C	AWK-1151C	192.168.123.72	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).

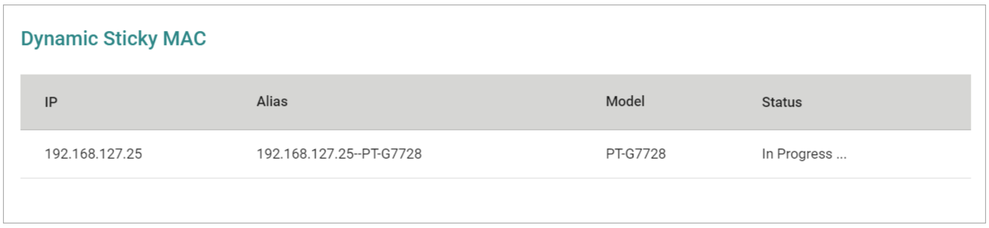
Address Limit

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.

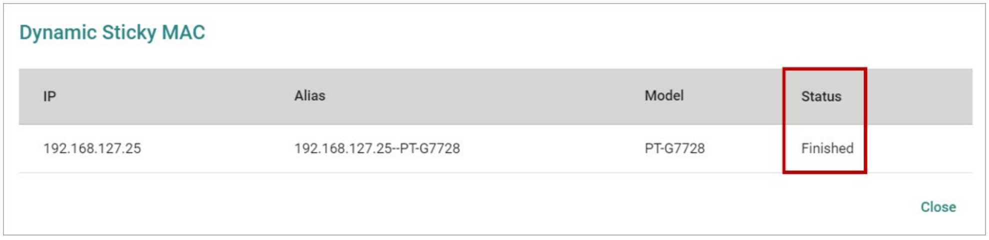
5. When finished, click **Apply**. The system will execute the action.



Dynamic Sticky MAC

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

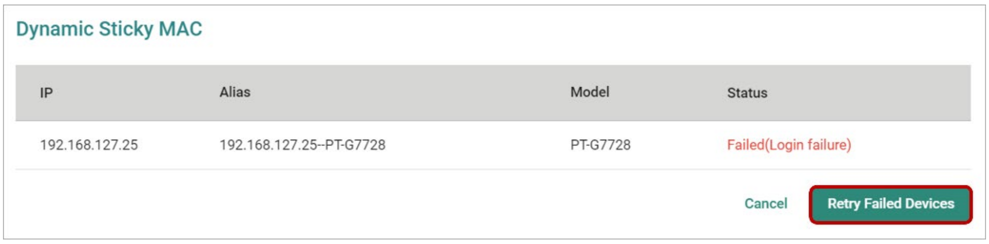
6. If successful, a confirmation will be shown in the Status column.



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)

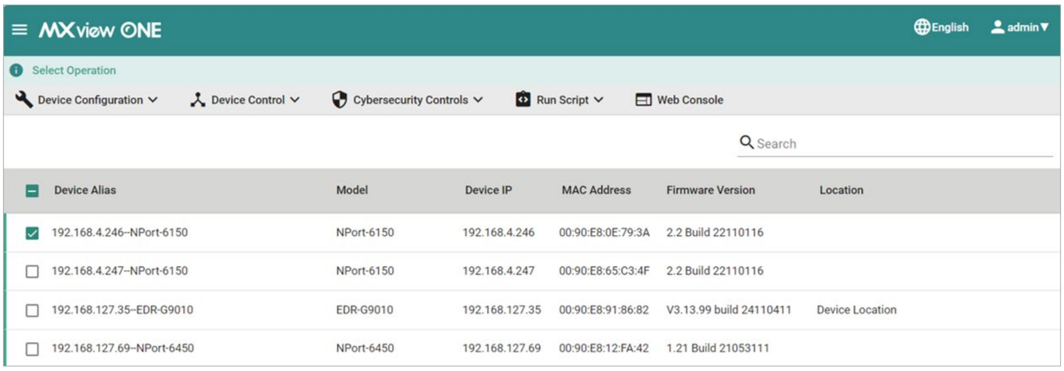
Serial Port Monitoring

NOTE

This function is only supported by the NPort 6000 Series and NPort 6000-G2 Series.

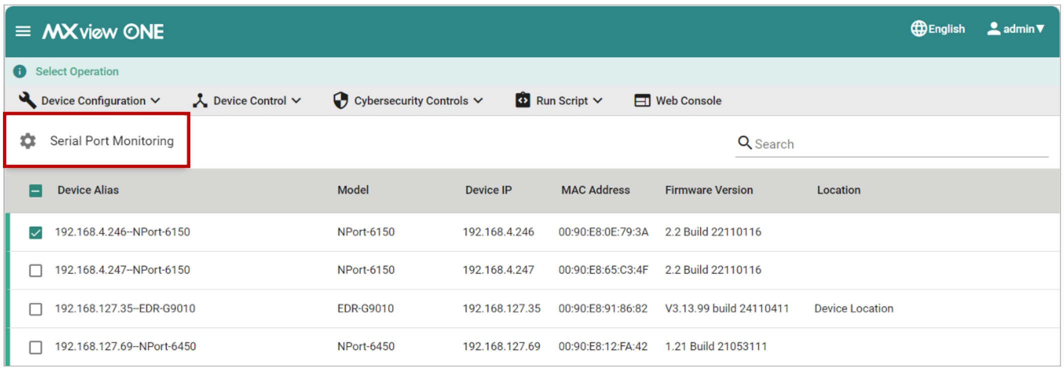
Use the **Serial Port Monitoring** function to configure event trigger rules for triggering serial port events.

1. Navigate to **Menu** (≡) **> Device Management > Configuration and Control**.
2. Select the NPort 6000 Series or NPort 6000-G2 Series device(s) to configure from the device list.



	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
☑	192.168.4.246--NPort-6150	NPort-6150	192.168.4.246	00:90:E8:0E:79:3A	2.2 Build 22110116	
□	192.168.4.247--NPort-6150	NPort-6150	192.168.4.247	00:90:E8:65:C3:4F	2.2 Build 22110116	
□	192.168.127.35--EDR-G9010	EDR-G9010	192.168.127.35	00:90:E8:91:86:82	V3.13.99 build 24110411	Device Location
□	192.168.127.69--NPort-6450	NPort-6450	192.168.127.69	00:90:E8:12:FA:42	1.21 Build 21053111	

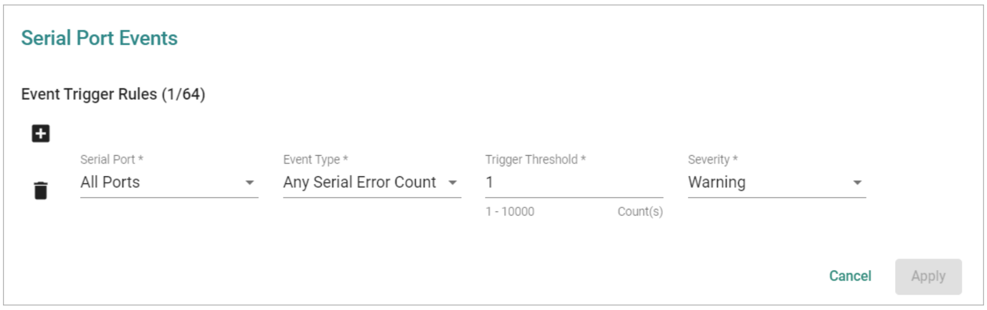
3. From the **Device Configuration** drop-down list, select **Serial Port Monitoring**.
The **Serial Port Events** screen will appear.



	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
☑	192.168.4.246--NPort-6150	NPort-6150	192.168.4.246	00:90:E8:0E:79:3A	2.2 Build 22110116	
□	192.168.4.247--NPort-6150	NPort-6150	192.168.4.247	00:90:E8:65:C3:4F	2.2 Build 22110116	
□	192.168.127.35--EDR-G9010	EDR-G9010	192.168.127.35	00:90:E8:91:86:82	V3.13.99 build 24110411	Device Location
□	192.168.127.69--NPort-6450	NPort-6450	192.168.127.69	00:90:E8:12:FA:42	1.21 Build 21053111	

4. In the **Event Trigger Rules** section, configure the event trigger rules.
5. To add an event trigger rule:

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



Serial Port Events

Event Trigger Rules (1/64)

Serial Port *: All Ports

Event Type *: Any Serial Error Count

Trigger Threshold *: 1 (1 - 10000, Count(s))

Severity *: Warning

- ❒ **Serial Port**: Select the device port(s) to apply the event trigger rule to.
- ❒ **Event Type**: Select the rule event property.
- ❒ **No Data Period**: If the Event Type is set to RX Inactivity, TX Inactivity, or TX & RX Inactivity, specify the duration the port does not transmit or receive data before triggering a no data event.
- ❒ **Trigger Threshold**: If the Serial Port Properties to any Error Count type, specify the number of consecutive error counts the serial can receive before triggering an error event.
- ❒ **Severity**: Select the event severity for this rule.

b. (Optional) If there are other devices of the model type in the topology, use the **Condition Copy** option to copy the event trigger rules to these devices.

c. Click **Apply**.

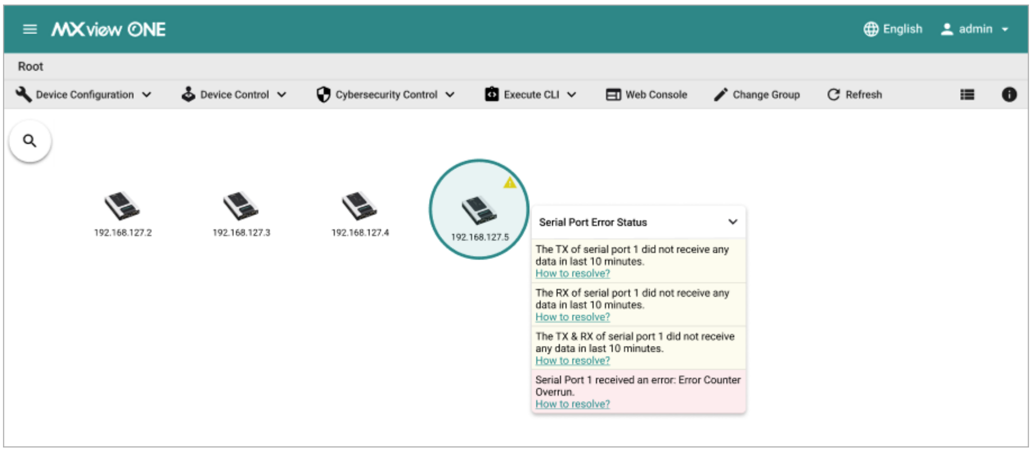
NOTE

MXview One supports a maximum of 64 event trigger rules. Different rules cannot have identical Serial Port and Event Type settings.

6. To delete an event trigger rule:

   a. Click the Delete (🗑) icon next to the rule you want to delete.

7. When a serial port event is triggered, a yellow triangle icon will appear the above affected devices in the Topology screen. Click the device icon to show the event list.



Serial Port Error Status

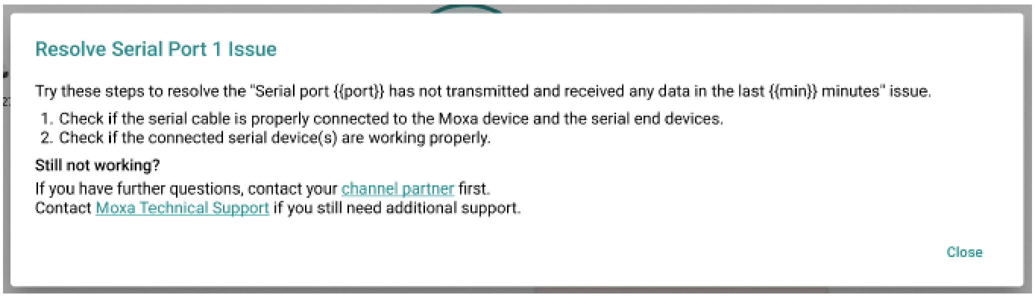
The TX of serial port 1 did not receive any data in last 10 minutes.
How to resolve?

The RX of serial port 1 did not receive any data in last 10 minutes.
How to resolve?

The TX & RX of serial port 1 did not receive any data in last 10 minutes.
How to resolve?

Serial Port 1 received an error: Error Counter Overrun.
How to resolve?

8. Click the **How to resolve?** link to open a pop-up window with step-by-step instructions to resolve the issue.



Resolve Serial Port 1 Issue

Try these steps to resolve the "Serial port {{port}} has not transmitted and received any data in the last {{min}} minutes" issue.

1. Check if the serial cable is properly connected to the Moxa device and the serial end devices.
2. Check if the connected serial device(s) are working properly.

Still not working?

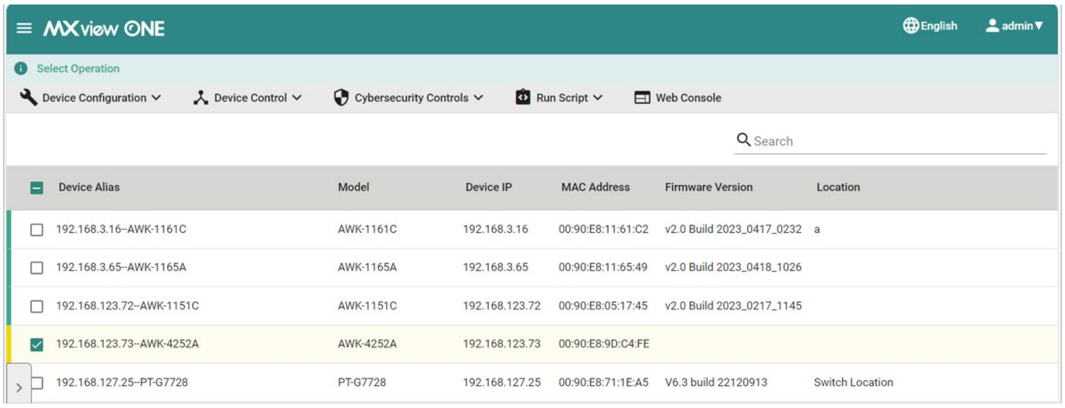
If you have further questions, contact your channel partner first.
Contact Moxa Technical Support if you still need additional support.

Device Control

Reboot

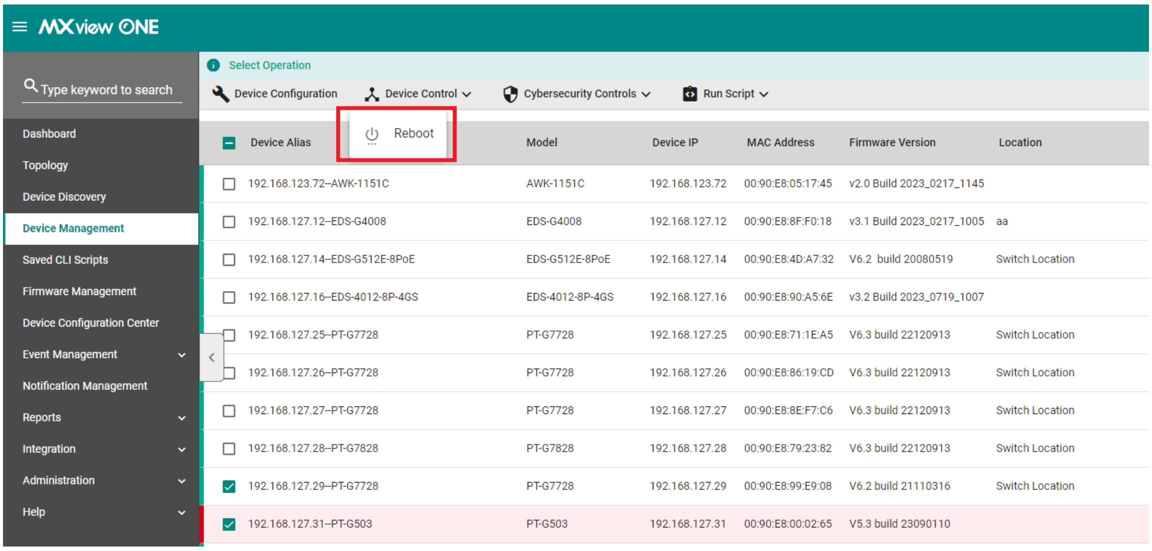
Use the **Reboot** function to manually reboot devices or configure a reboot schedule.

1. Navigate to **Menu** (☰) **> Device Management > Configuration and Control**.
2. Select the device(s) to configure from the device list.



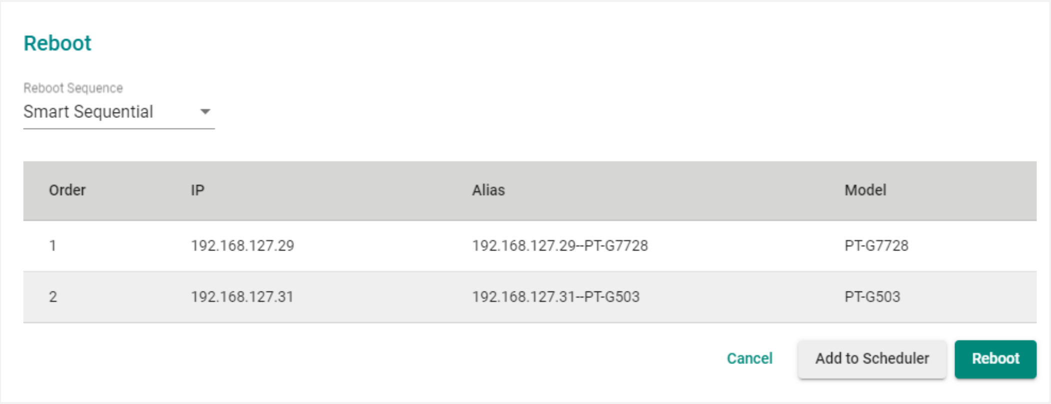
	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.3.16--AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
□	192.168.3.65--AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
□	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	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

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

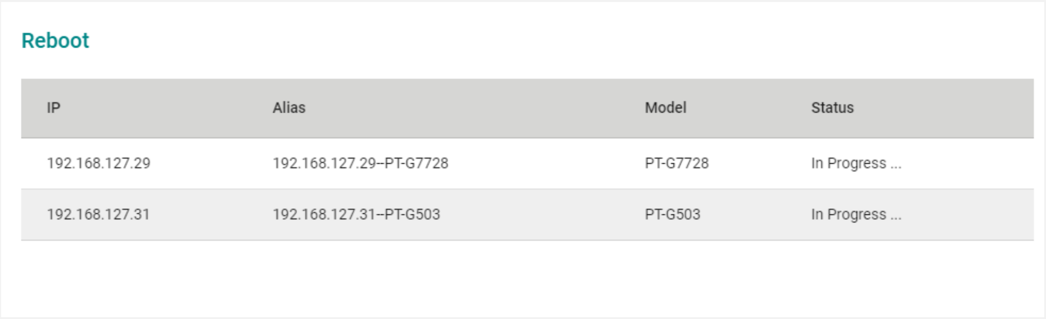
a. Select the reboot sequence:

- **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.

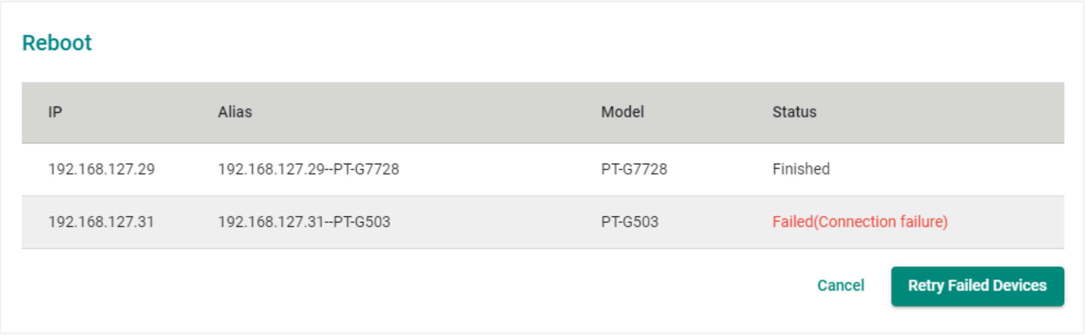
5. To reboot devices instantly, click **Reboot**. The system will execute the action.



Reboot

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

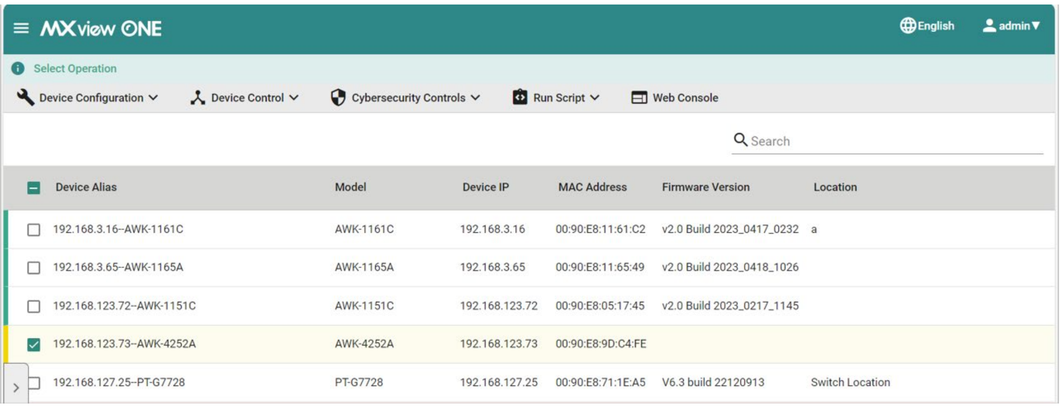
IP	Alias	Model	Status
192.168.127.29	192.168.127.29--PT-G7728	PT-G7728	Finished
192.168.127.31	192.168.127.31--PT-G503	PT-G503	Failed(Connection failure)

Create Snapshot

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

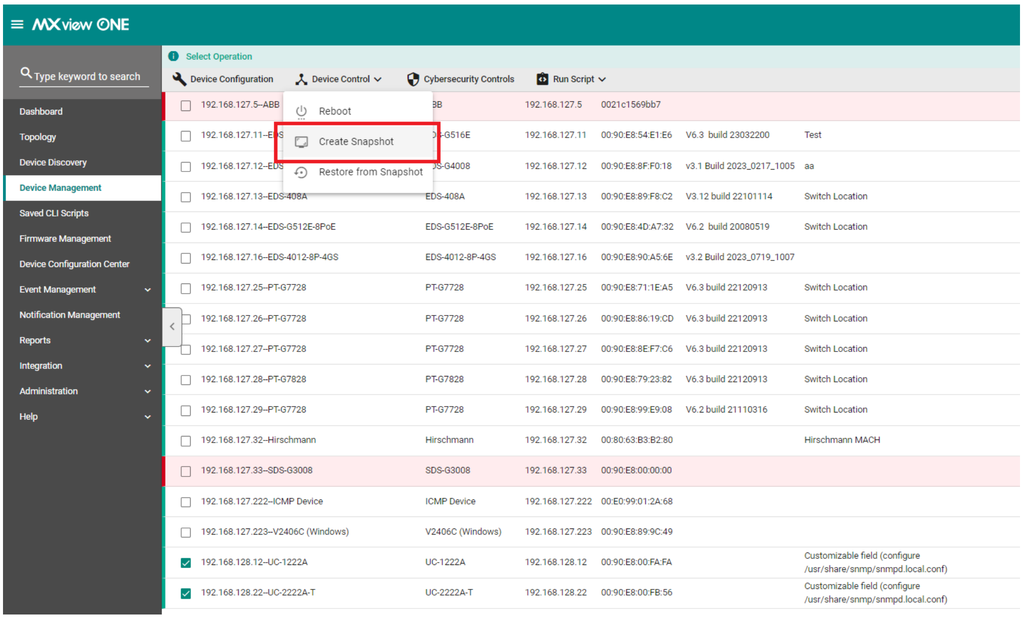
1. Navigate to **Menu** (☰) **> Device Management > Configuration and Control**.

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



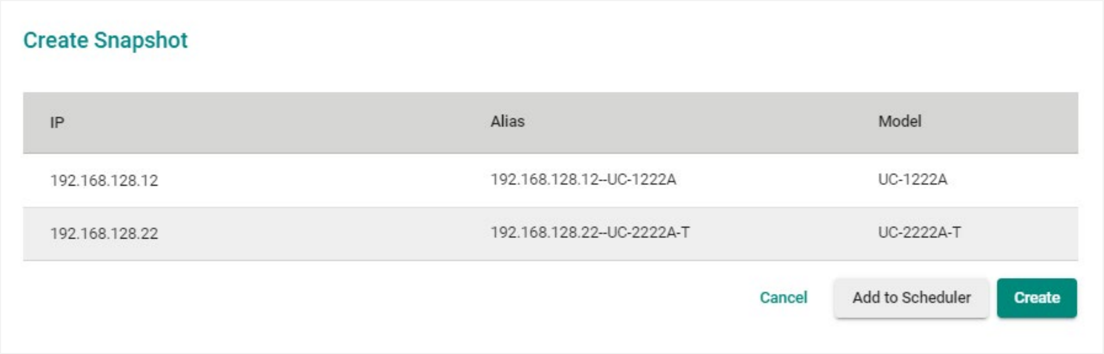
	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.3.16–AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
□	192.168.3.65–AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
□	192.168.123.72–AWK-1151C	AWK-1151C	192.168.123.72	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.

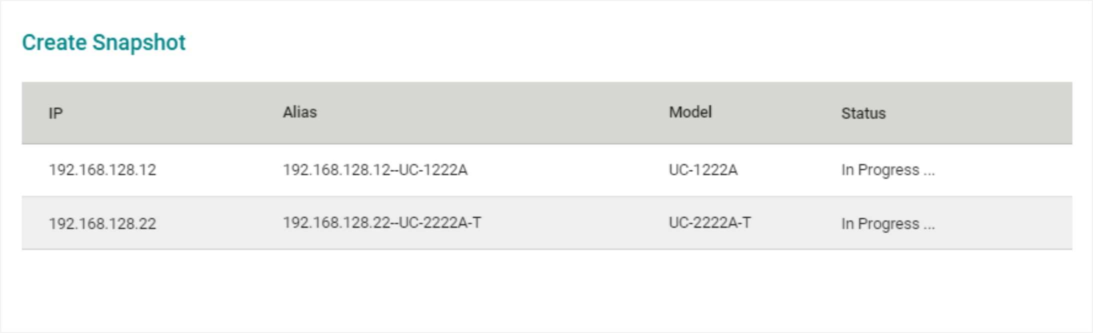


Create Snapshot

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.

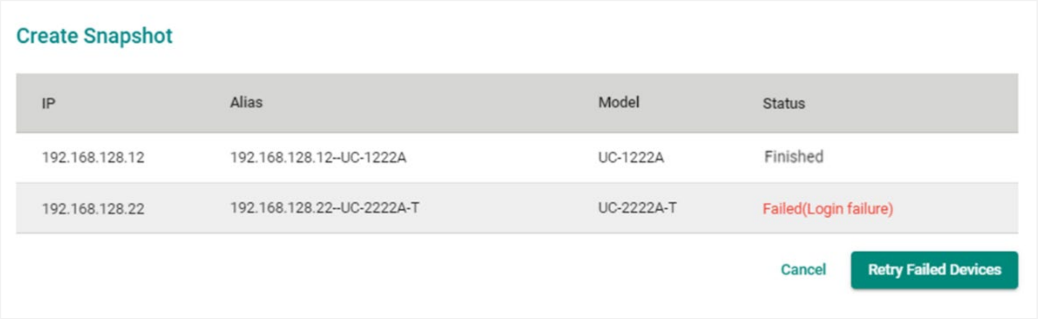
5. To create a snapshot instantly, click **Create**. The system will execute the action.



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.



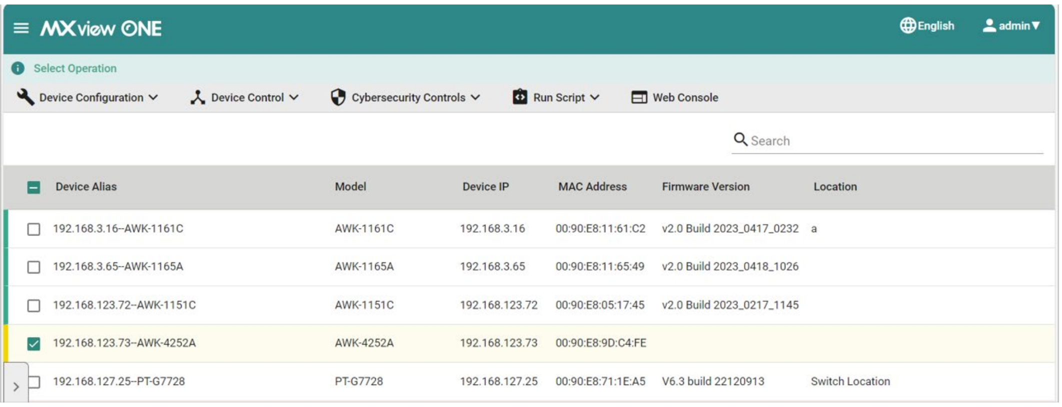
Create Snapshot

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

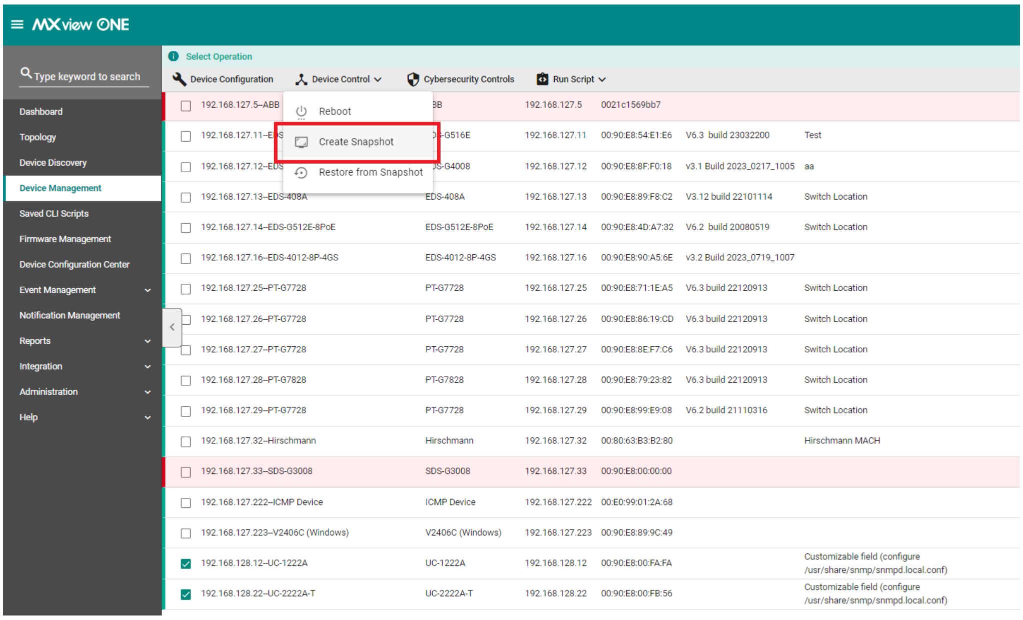
Use the **Restore from Snapshot** to restore the configuration from a previously created snapshot.

1. Navigate to **Menu** (☰) **> Device Management > Configuration and Control**.
2. Select the device(s) to configure from the device list.



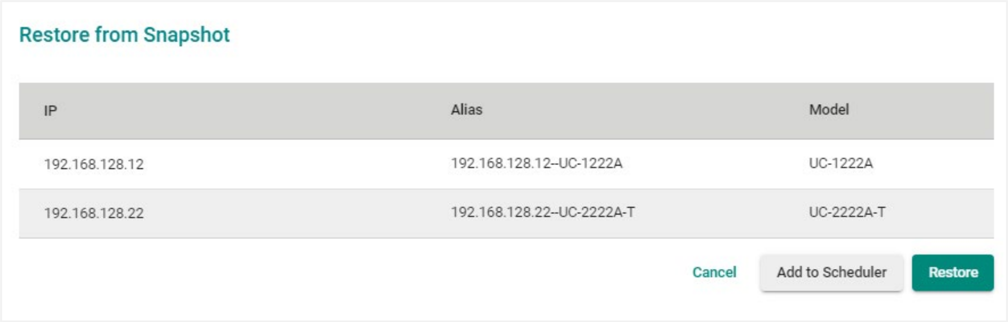
	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.3.16–AWK-1161C	AWK-1161C	192.168.3.16	00:90:E8:11:61:C2	v2.0 Build 2023_0417_0232	a
□	192.168.3.65–AWK-1165A	AWK-1165A	192.168.3.65	00:90:E8:11:65:49	v2.0 Build 2023_0418_1026	
□	192.168.123.72–AWK-1151C	AWK-1151C	192.168.123.72	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	BB	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)

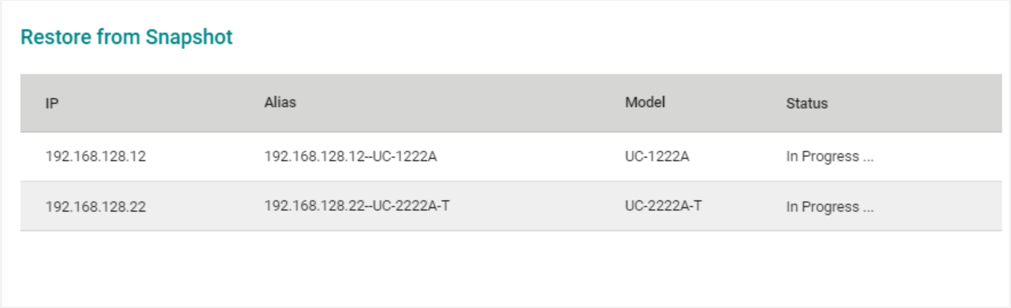
4. Configure the execution time.



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.

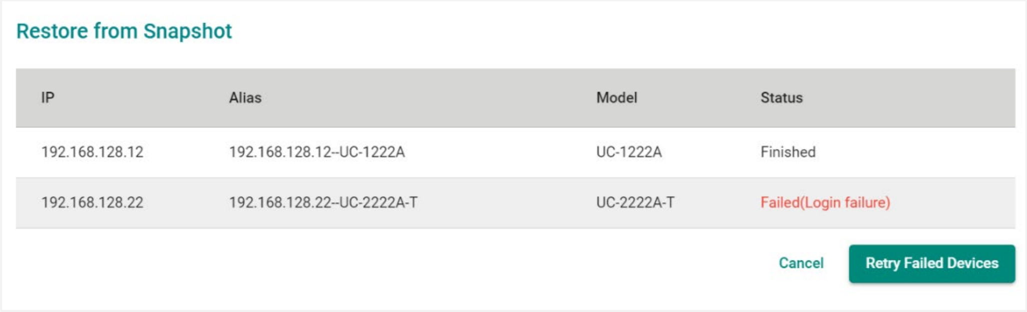
5. To restore the snapshot instantly, click **Restore**. The system will execute the action.



Restore from 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.



Restore from Snapshot

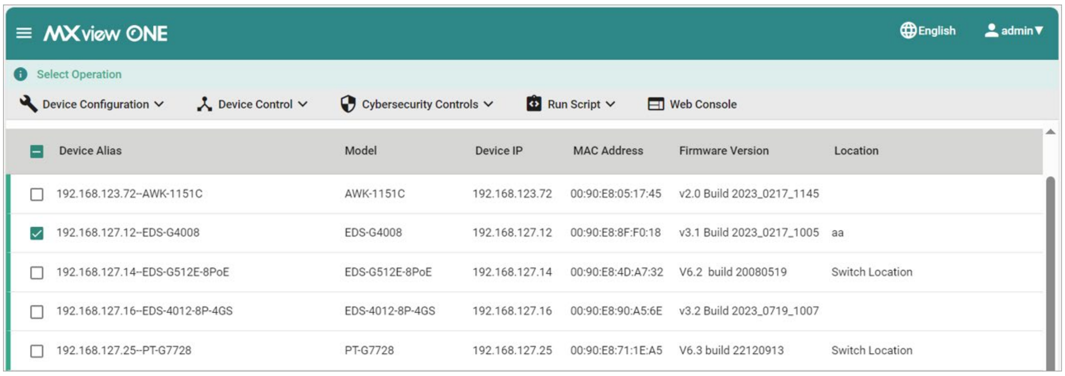
IP	Alias	Model	Status
192.168.128.12	192.168.128.12--UC-1222A	UC-1222A	Finished
192.168.128.22	192.168.128.22--UC-2222A-T	UC-2222A-T	Failed(Login failure)

Cybersecurity Controls

Sticky MAC On/Off

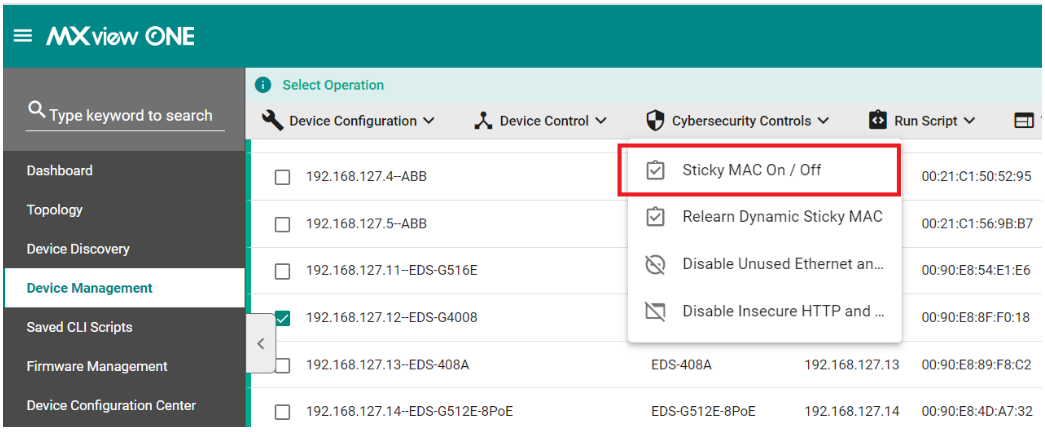
Use the **Sticky MAC On/Off** function to enable or disable Sticky MAC for the selected device(s).

1. Navigate to **Menu** (☰) **> Device Management > Configuration and Control**.
2. Select the device(s) to configure from the device list.



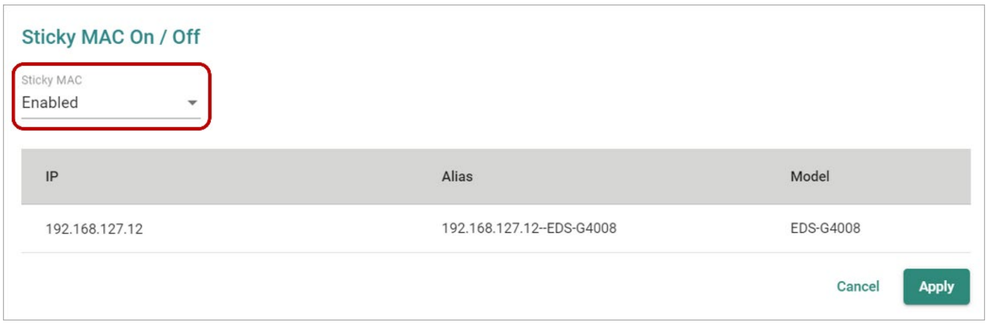
☐	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
☐	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
☑	192.168.127.12--EDS-G4008	EDS-G4008	192.168.127.12	00:90:E8:8F:F0:18	v3.1 Build 2023_0217_1005	aa
☐	192.168.127.14--EDS-G512E-8PoE	EDS-G512E-8PoE	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

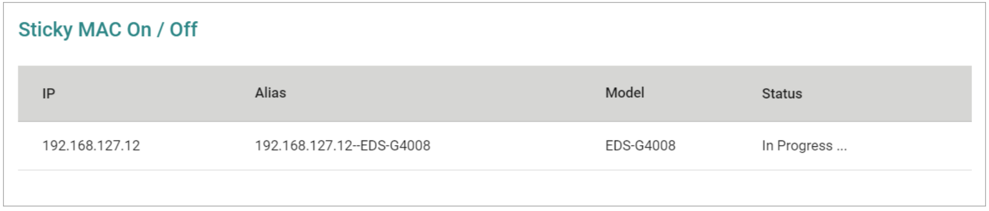
4. Choose to enable or disable Sticky MAC.


Sticky MAC On / Off

Sticky MAC: Enabled

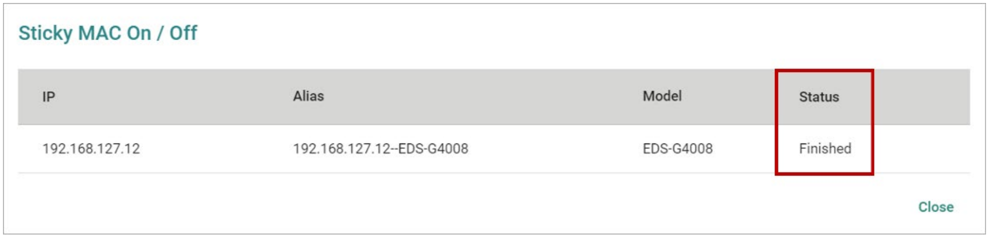
IP	Alias	Model
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008

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

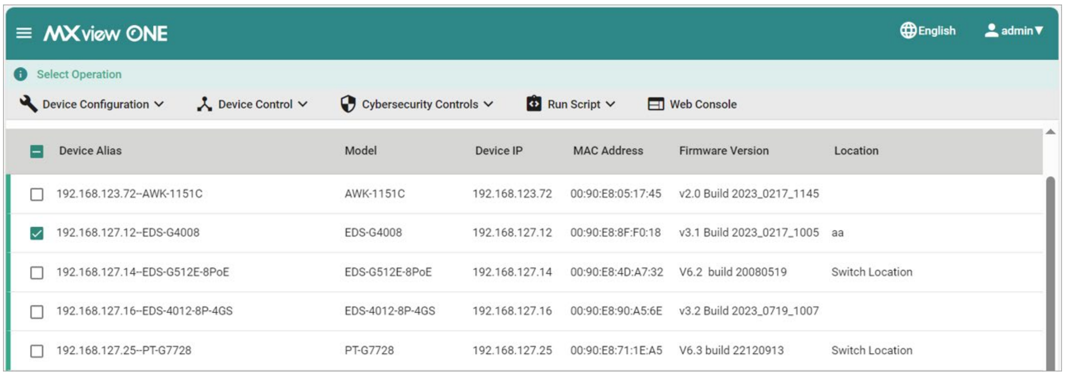
IP	Alias	Model	Status
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008	Finished

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

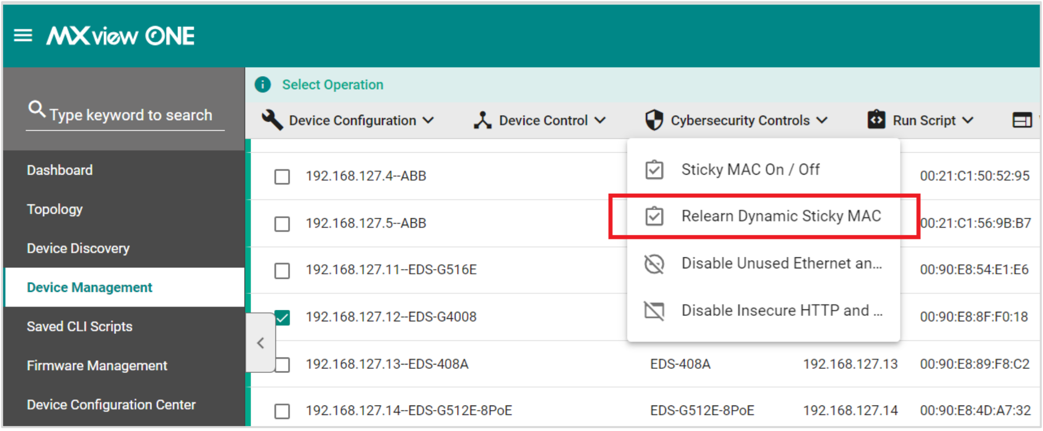
Use the **Relearn Dynamic Sticky MAC** function to reset all previously learned MAC addresses and relearn them again for the selected device(s).

1. Navigate to **Menu** (☰) **> Device Management > Configuration and Control**.
2. Select the device(s) to configure from the device list.



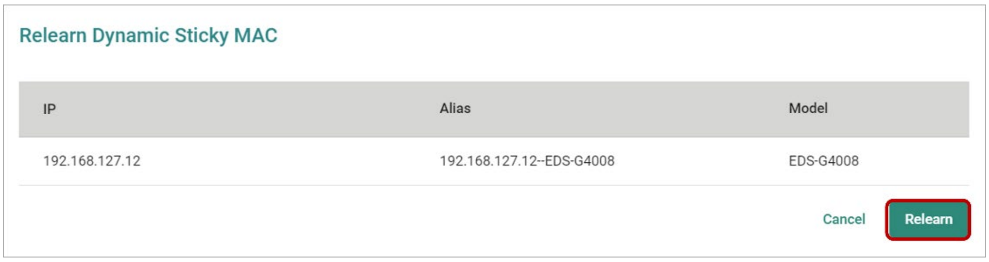
	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
☐	192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2023_0217_1145	
☑	192.168.127.12--EDS-G4008	EDS-G4008	192.168.127.12	00:90:E8:8F:F0:18	v3.1 Build 2023_0217_1005	aa
☐	192.168.127.14--EDS-G512E-8PoE	EDS-G512E-8PoE	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

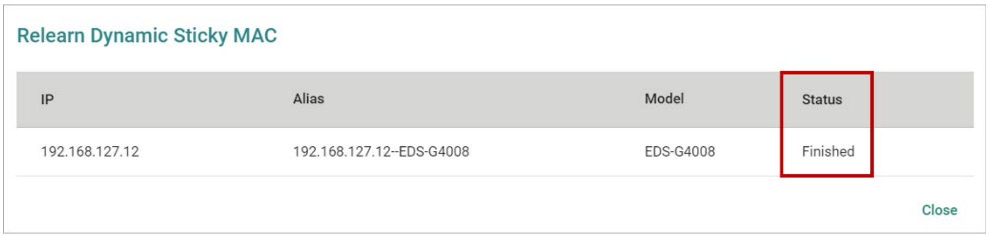
4. Click **Relearn**. The system will execute the action.



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

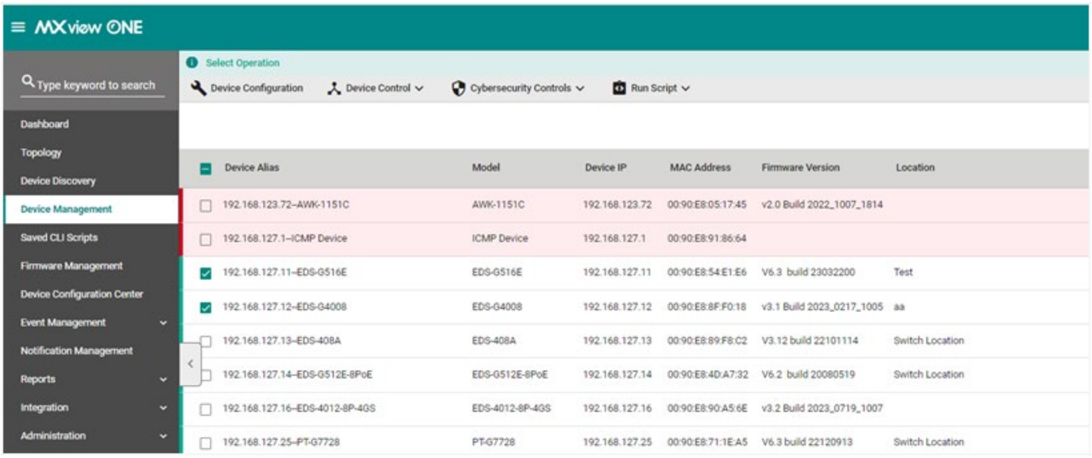
IP	Alias	Model	Status
192.168.127.12	192.168.127.12--EDS-G4008	EDS-G4008	Finished

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

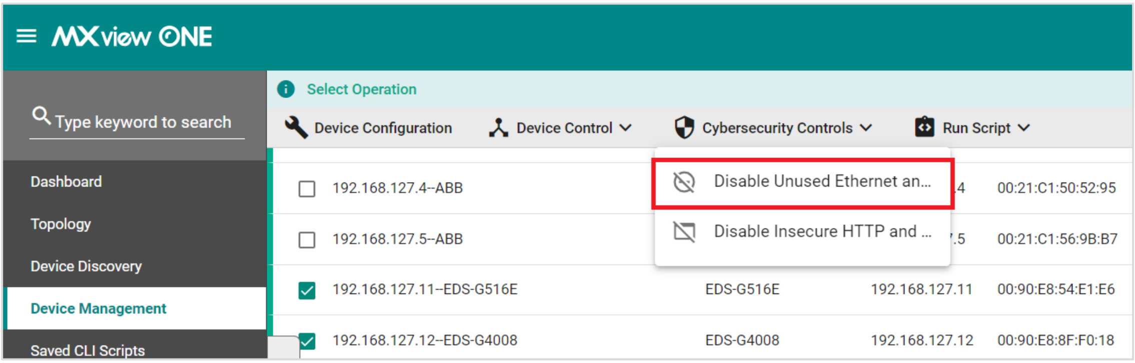
Use the **Disable Unused Ethernet and Fiber Ports** function to disable any unused Ethernet or fiber ports to make sure these ports cannot be exploited to gain unauthorized access to the device.

1. Navigate to **Menu** (☰) **> Device Management > Configuration and Control**.
2. Select the device(s) to configure from the device list.

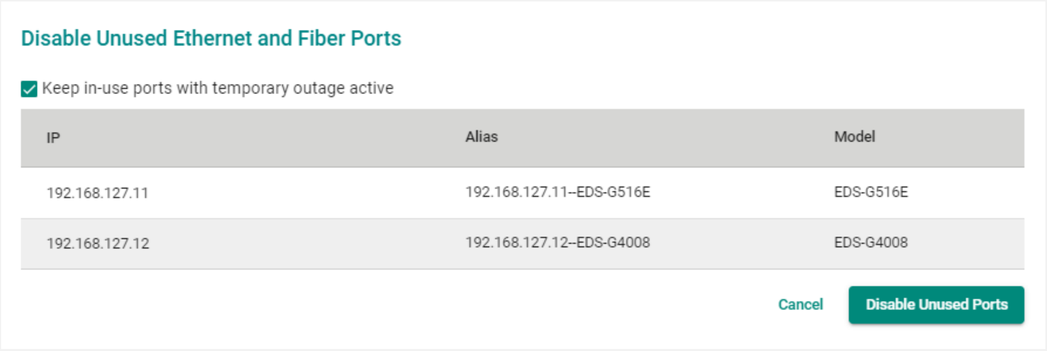


	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.123.72–AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2022_1007_1814	
□	192.168.127.1–ICMP Device	ICMP Device	192.168.127.1	00:90:E8:91:86:64		
☑	192.168.127.11–EDS-G516E	EDS-G516E	192.168.127.11	00:90:E8:54:E1:E6	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.



4. Choose to keep ports with temporary inactivity active.

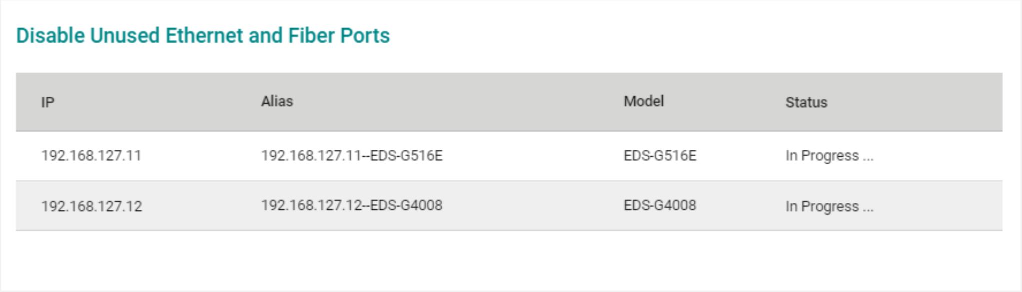


Disable Unused Ethernet and Fiber Ports

☑ 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

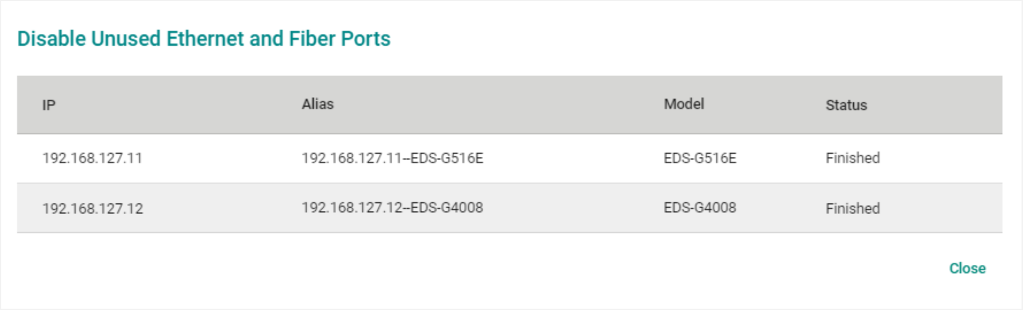
5. Click **Disable Unused Ports**. The system will execute the action.



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

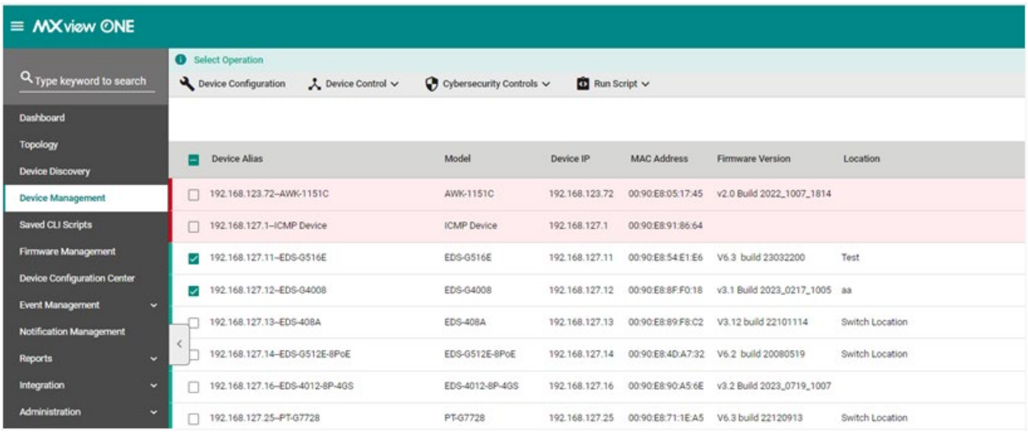
IP	Alias	Model	Status
192.168.127.11	192.168.127.11–EDS-G516E	EDS-G516E	Finished
192.168.127.12	192.168.127.12–EDS-G4008	EDS-G4008	Finished

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

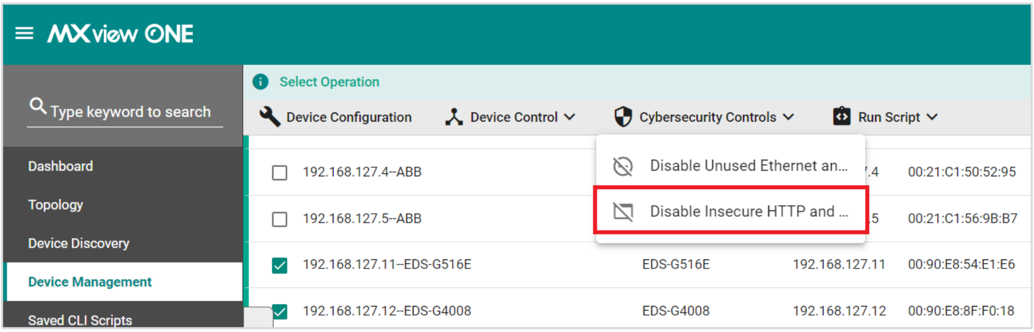
Use the **Disable Insecure HTTP and Telnet Console** function to disable the non-secure HTTP and Telnet connection interfaces.

1. Navigate to **Menu** (☰) **> Device Management > Configuration and Control**.
2. Select the device(s) to configure from the device list.



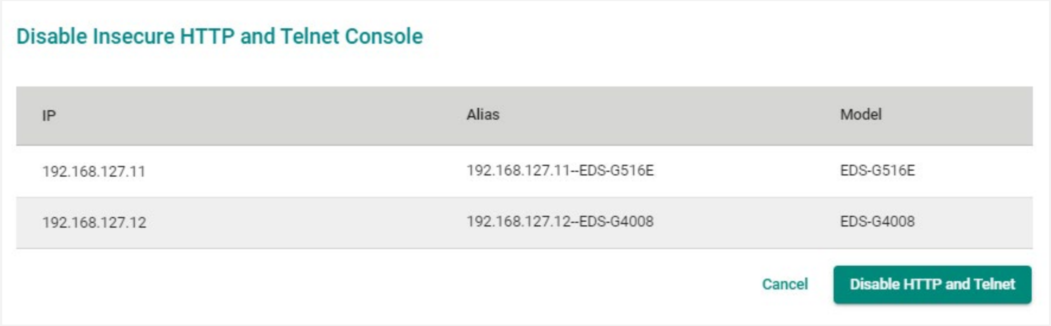
☐	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
☐	192.168.123.72–AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2022_1007_1814	
☐	192.168.127.1–ICMP Device	ICMP Device	192.168.127.1	00:90:E8:91:86:64		
☑	192.168.127.11–EDS-G516E	EDS-G516E	192.168.127.11	00:90:E8:54:E1:E6	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

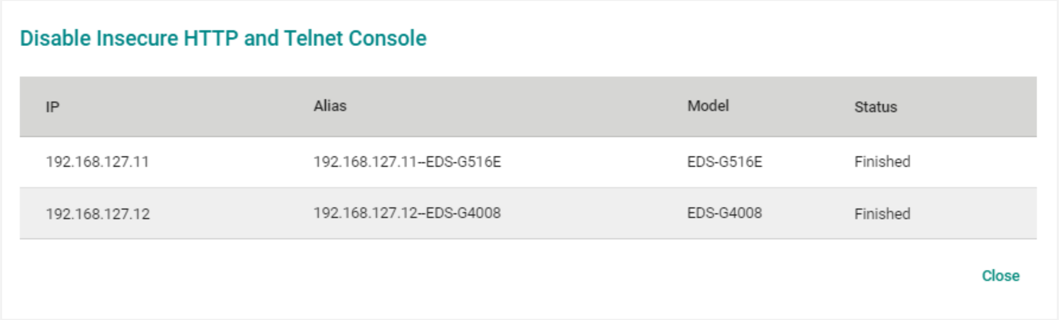
4. Click **Disable HTTP and Telnet**. The system will execute the action.



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

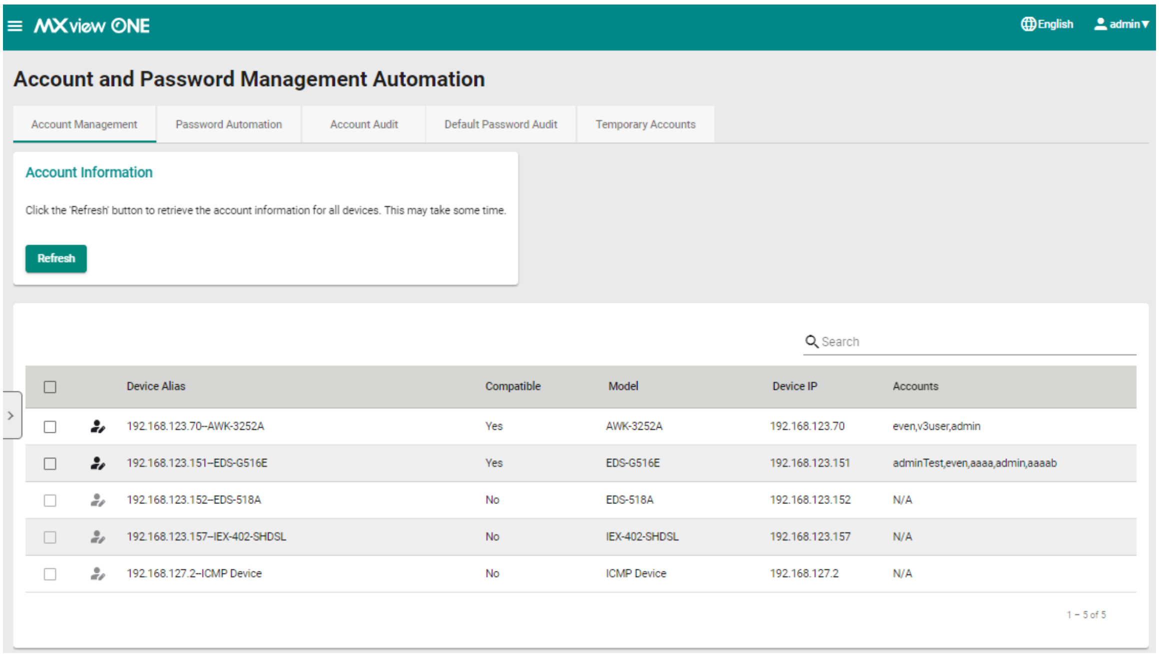
Refer to the Managing and Running Scripts section.

Account and Password

Account Management Overview

To access the **Account Management** page, in the function tree, navigate to **Menu** (☰) **> Device Management > Account and Password** and go to the **Account Management** tab.

The **Account Management** tab shows an overview of all user accounts on each device.



Account and Password Management Automation

Account Information

Click the 'Refresh' button to retrieve the account information for all devices. This may take some time.

□		Device Alias	Compatible	Model	Device IP	Accounts
□		192.168.123.70–AWK-3252A	Yes	AWK-3252A	192.168.123.70	even,v3user,admin
□		192.168.123.151–EDS-G516E	Yes	EDS-G516E	192.168.123.151	adminTest,even,aaaa,admin,aaaab
□		192.168.123.152–EDS-518A	No	EDS-518A	192.168.123.152	N/A
□		192.168.123.157–IEX-402-SHDSL	No	IEX-402-SHDSL	192.168.123.157	N/A
□		192.168.127.2–ICMP Device	No	ICMP Device	192.168.127.2	N/A

This page displays the following information in a table format:

Column	Description
Device Alias	The unique name of the device.
Compatible	Shows if the device supports MXview One retrieving account information.
Model	The device model name.
Device IP	The IP address of the device.
Accounts	The list of accounts associated with the device. Under certain conditions, the following statuses can show: • **Unable to retrieve accounts**: The device supports this feature, but MXview One was unable to successfully retrieve account information from the device. • **N/A**: MXview One cannot retrieve account information because the device does not support this feature.

Click **Refresh** at the top of the page to update the account information in the table.

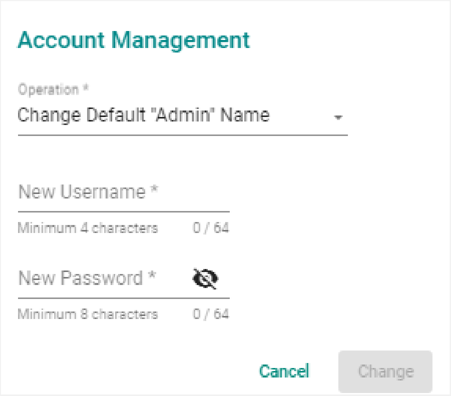
Editing Accounts on a Device

NOTE

This function is only available for compatible devices. If the device is incompatible, this function will be greyed out.

1. Navigate to **Menu** (☰) **> Device Management > Account and Password**.
2. Go to the **Account Management** tab.

3. Click the **Edit** ( ) icon next to the device account you want to edit.
   The **Account Management** window will appear.



Account Management

Operation *
Change Default "Admin" Name

New Username *
Minimum 4 characters 0 / 64

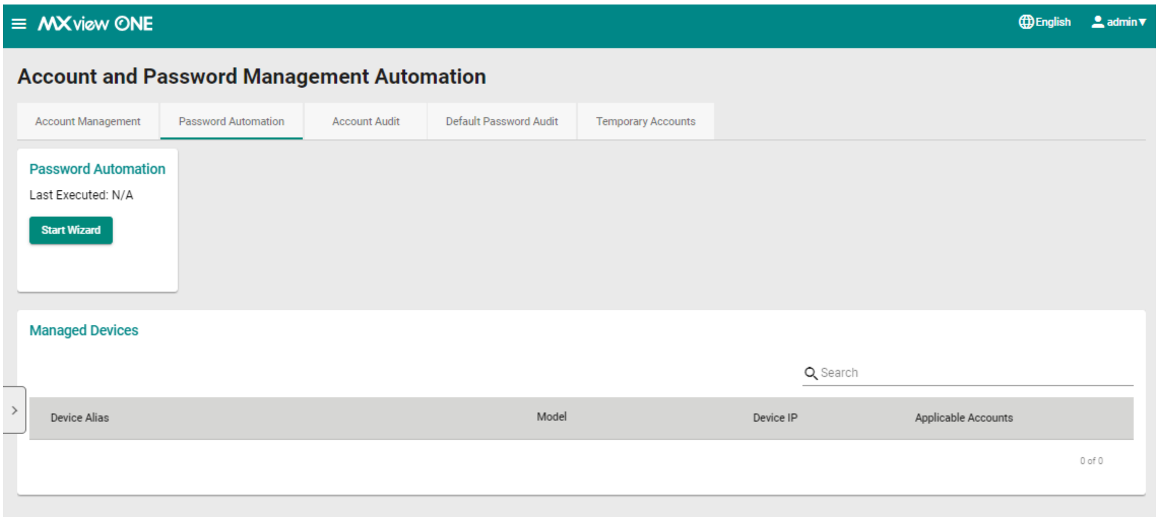
New Password *
Minimum 8 characters 0 / 64

4. To change the default admin account credentials:
   a. Select **Change Default ''Admin'' Name** as the operation.
   b. Specify the new username and password.
   c. Click **Change**.
5. To add an account:
   a. Select **Edit Account** as the operation.
   b. Select the **Add Account** radio button.
   c. Specify the username, password, and authority of the account.
   d. Click **Add**.
6. To delete an account:
   a. Select **Edit Account** as the operation.
   b. Select the **Delete Account** radio button.
   a. Enter the username of the account you want to delete.
   b. Click **Delete**.

Password Automation Overview

To access the **Account Management** page, in the function tree, navigate to **Menu** (☰) **> Device Management > Account and Password** and go to the **Password Automation** tab.

The **Password Automation** tab shows an overview of all user accounts on each device.



Account and Password Management Automation

Password Automation
Last Executed: N/A

Managed Devices

Device Alias	Model	Device IP	Applicable Accounts

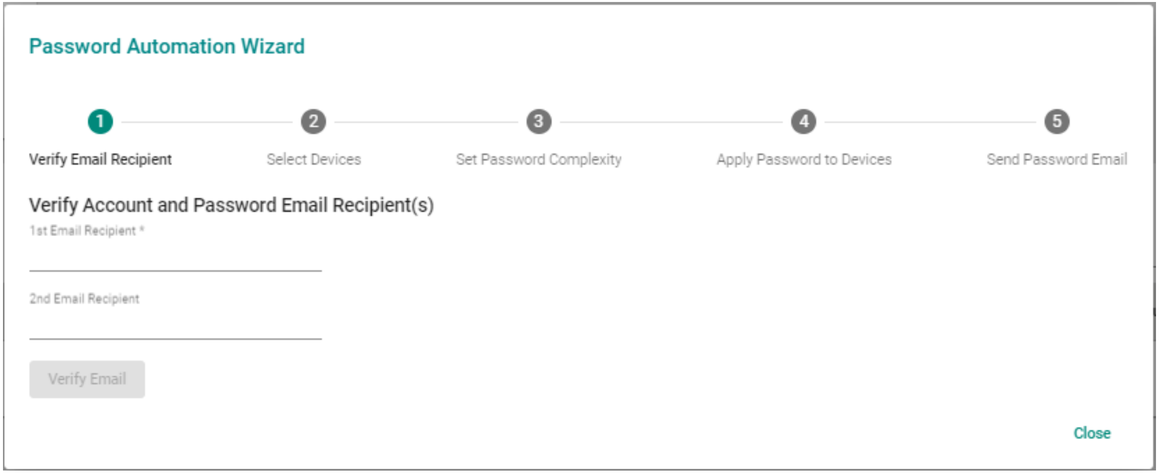
0 of 0

This page displays the following information in a table format:

Column	Description
Device Alias	The unique name of the device.
Model	The device model name.
Device IP	The IP address of the device.
Applicable Accounts	Shows the device accounts that the password automation functions are applied to.

Running the Password Automation Wizard

1. Navigate to **Menu** (☰) **> Device Management > Account and Password**.
2. Go to the **Password Automation** tab.
3. In the **Password Automation** section, click **Start Wizard**.
4. When prompted, verify your MXview One account.
   The **Password Automation Wizard** screen will appear.



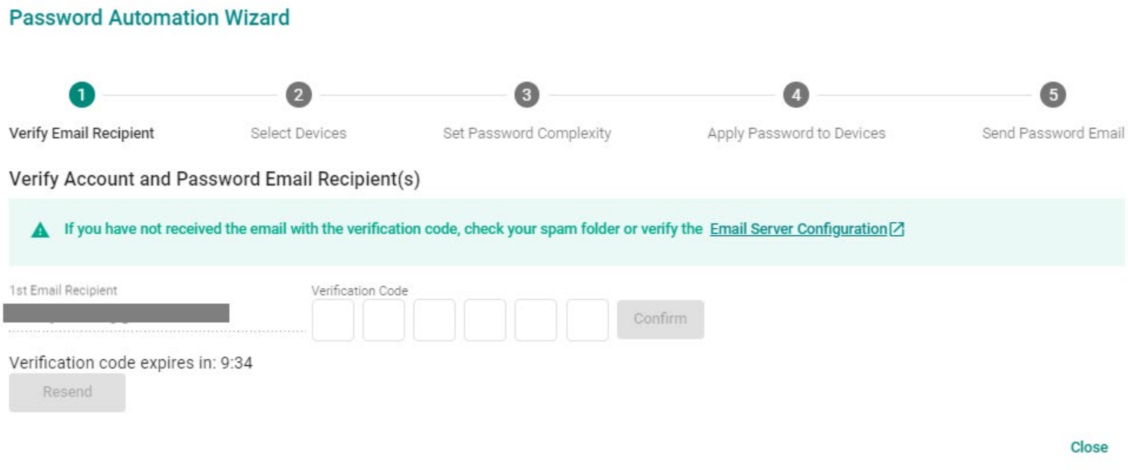
Password Automation Wizard

Verify Account and Password Email Recipient(s)

1st Email Recipient *

2nd Email Recipient

5. Enter the 1st and 2nd recipient email addresses and click **Verify Email**.
   MXview One will send a verification code to these addresses.
6. Enter the verification code in the Wizard to continue.
   If you have not received an email, check your Spam folder or confirm the Email Server Configuration settings in MXview One.



Password Automation Wizard

Verify Account and Password Email Recipient(s)

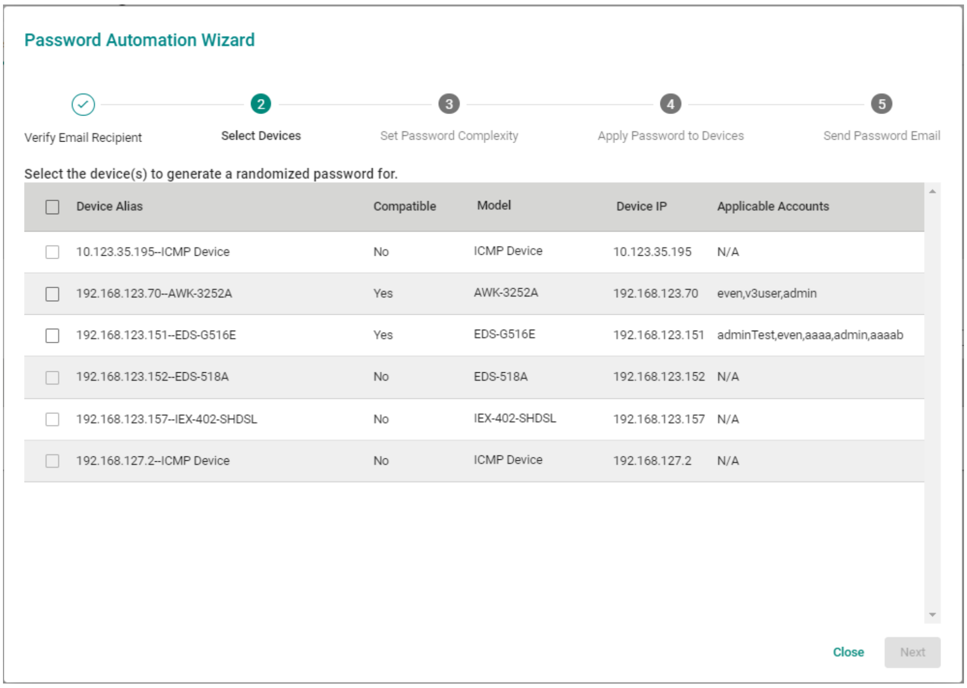
If you have not received the email with the verification code, check your spam folder or verify the Email Server Configuration

1st Email Recipient [redacted]

Verification Code

Verification code expires in: 9:34

7. Select the device(s) to generate a randomized password for and click **Next**.

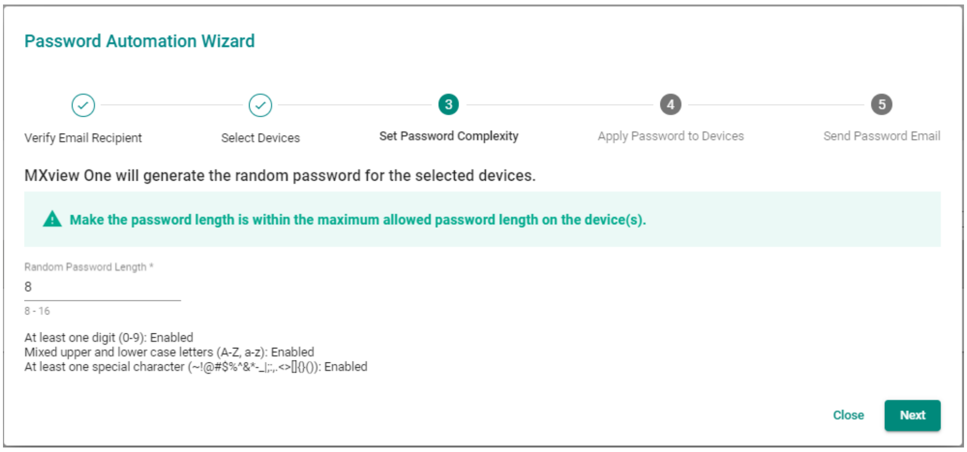


Password Automation Wizard

Select the device(s) to generate a randomized password for.

□ Device Alias	Compatible	Model	Device IP	Applicable Accounts
□ 10.123.35.195--ICMP Device	No	ICMP Device	10.123.35.195	N/A
□ 192.168.123.70--AWK-3252A	Yes	AWK-3252A	192.168.123.70	even,v3user,admin
□ 192.168.123.151--EDS-G516E	Yes	EDS-G516E	192.168.123.151	adminTest,even,aaaa,admin,aaaab
□ 192.168.123.152--EDS-518A	No	EDS-518A	192.168.123.152	N/A
□ 192.168.123.157--IEX-402-SHDSL	No	IEX-402-SHDSL	192.168.123.157	N/A
□ 192.168.127.2--ICMP Device	No	ICMP Device	192.168.127.2	N/A

8. Specify the randomized password length and click **Next**.
   MXview One will generate a random password of the specified length containing:
   - At least one digit (0-9).
   - Mixed upper and lowercase letters (A-Z, a-z).
   - At least one special character (~!@#$%^&*-_|;:,.<>[]{}())



Password Automation Wizard

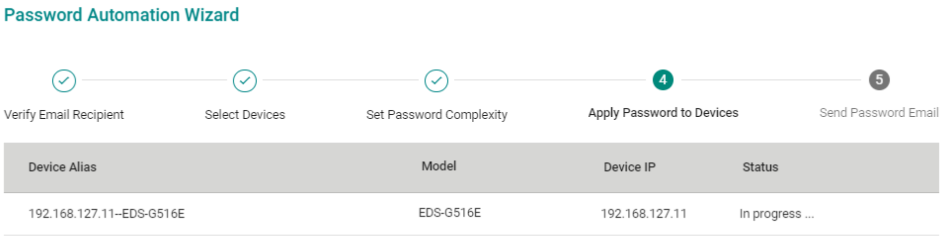
MXview One will generate the random password for the selected devices.

Make the password length is within the maximum allowed password length on the device(s).

Random Password Length *
8
8 - 16

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

9. MXview One will start generating new passwords for the selected devices.

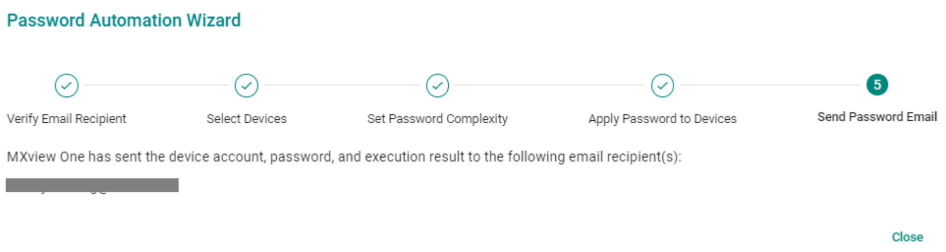


Password Automation Wizard

Device Alias	Model	Device IP	Status
192.168.127.11--EDS-G516E	EDS-G516E	192.168.127.11	In progress ...

10. When finished, MXview One will send the device account and password information to the email recipients specified at the beginning of the Wizard.
    Users will receive two emails. One email containing the account information and execution results and

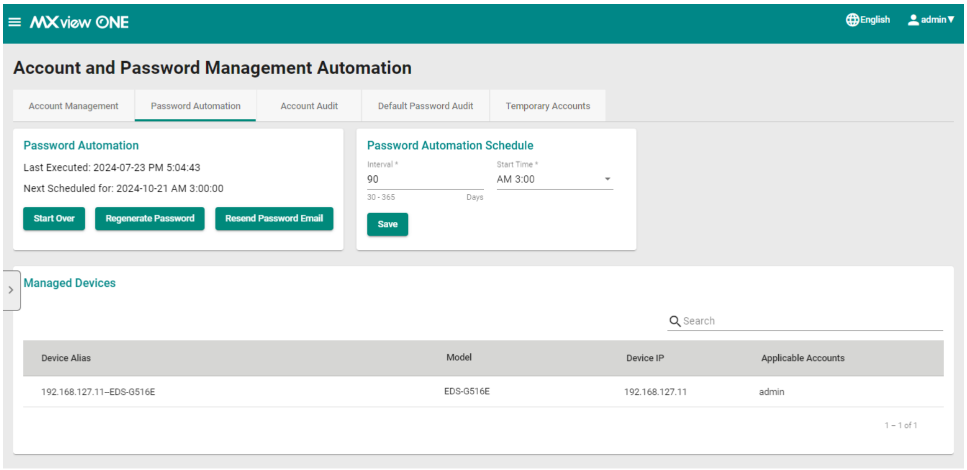
another email containing the string to unzip the account information file.



MXview One has sent the device account, password, and execution result to the following email recipient(s):

[redacted]

11. Click **Close**.
12. The table will show all the devices and associated accounts that password automation is applied to.



Password Automation

Last Executed: 2024-07-23 PM 5:04:43

Next Scheduled for: 2024-10-21 AM 3:00:00

Password Automation Schedule

Interval *: 90 (30 - 365 Days)

Start Time *: AM 3:00

Managed Devices

Device Alias	Model	Device IP	Applicable Accounts
192.168.127.11-EDS-G516E	EDS-G516E	192.168.127.11	admin

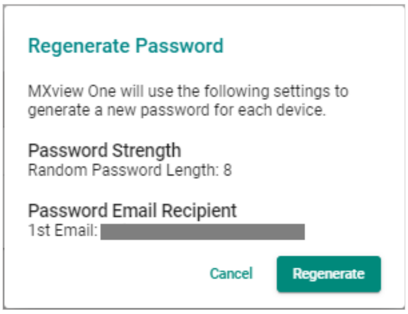
1 – 1 of 1

> **NOTE**
>
> Click **Start Over** to run the Password Automation Wizard again.

Regenerating Device Passwords

> **NOTE**
>
> This function is only available after completing the Password Automation Wizard at least once. Refer to Running the Password Automation Wizard.

1. Navigate to **Menu** (≡) **> Device Management > Account and Password**.
2. Go to the **Password Automation** tab.
3. In the **Password Automation** section, click **Regenerate Password**.
4. When prompted, verify your MXview One account.
   The **Regenerate Password** screen will appear.



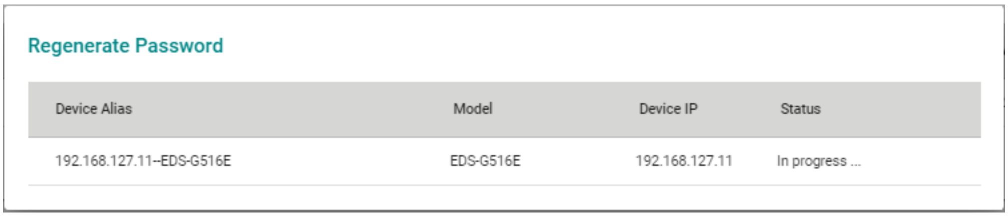
Regenerate Password

MXview One will use the following settings to generate a new password for each device.

Password Strength
Random Password Length: 8

Password Email Recipient
1st Email: [redacted]

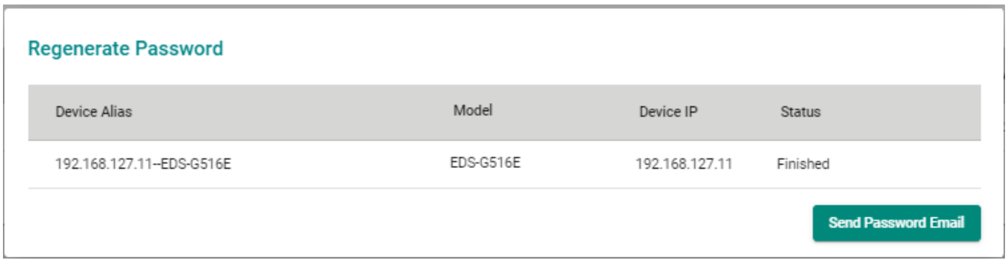
5. Click **Regenerate**.
   MXview One will generate a new password for all applicable devices.



Regenerate Password

Device Alias	Model	Device IP	Status
192.168.127.11--EDS-G516E	EDS-G516E	192.168.127.11	In progress ...

6. Click **Send Password Email** to receive an email with the new randomized passwords to the recipients specified in the Password Automation Wizard.



Regenerate Password

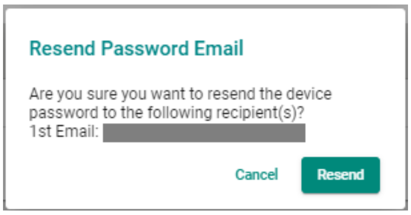
Device Alias	Model	Device IP	Status
192.168.127.11--EDS-G516E	EDS-G516E	192.168.127.11	Finished

Resending the Password Email

NOTE

This function is only available after completing the Password Automation Wizard at least once. Refer to Running the Password Automation Wizard.

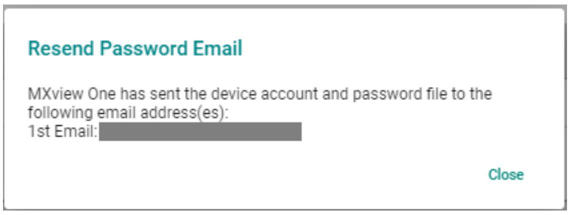
1. Navigate to **Menu** (☰) **> Device Management > Account and Password**.
2. Go to the **Password Automation** tab.
3. In the **Password Automation** section, click **Resend Password Email**.
4. When prompted, verify your MXview One account.
   The **Resend Password Email** screen will appear.



Resend Password Email

Are you sure you want to resend the device password to the following recipient(s)?
1st Email: [redacted]

5. Click **Resend**.
   MXview One will send an email with the device account credentials to the recipients specified in the Password Automation Wizard.



Resend Password Email

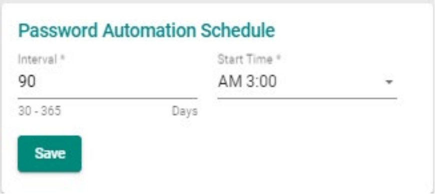
MXview One has sent the device account and password file to the following email address(es):
1st Email: [redacted]

Configuring a Password Automation Schedule

With the password automation schedule function, you can configure a specific interval at which MXview One will generate new randomized passwords for all applicable devices.

> **NOTE**
>
> This function is only available after completing the Password Automation Wizard at least once. Refer to Running the Password Automation Wizard.

1. Navigate to **Menu** (☰) **> Device Management > Account and Password**.
2. Go to the **Password Automation** tab.
3. In the **Password Automation Schedule** section, configure the following settings:



Password Automation Schedule

Interval *
90
30 - 365 Days

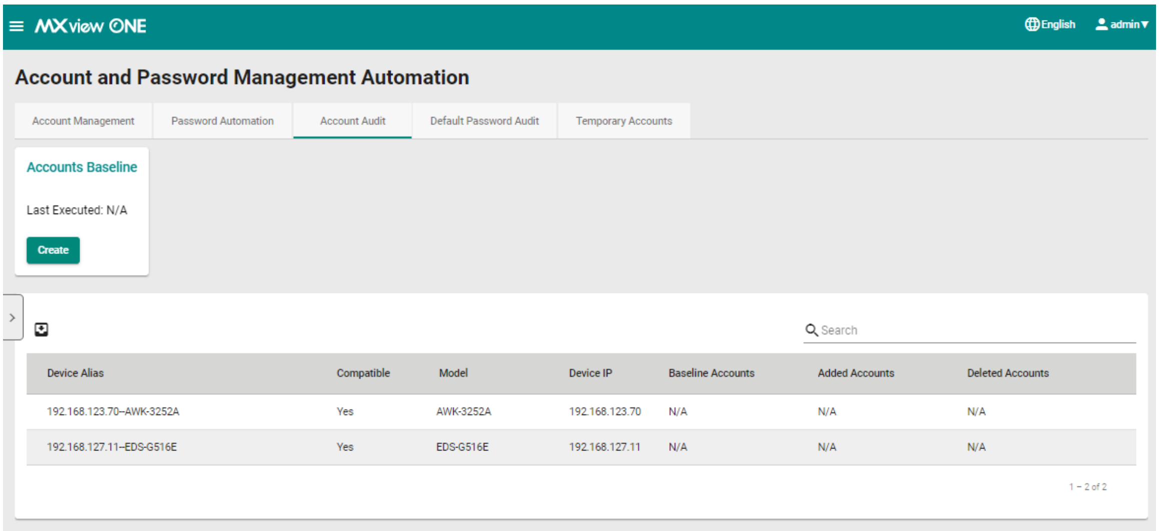
Start Time *
AM 3:00

   - **Interval**: Select the interval (in days) at which MXview One will randomize device passwords.
   - **Start Time**: Specify the day of time when MXview One will execute the password automation.
4. Click **Save**.

Account Audit Overview

To access the **Account Audit** page, in the function tree, navigate to **Menu** (☰) **> Device Management > Account and Password** and go to the **Account Audit** tab.

The **Account Audit** tab lets users create a device account baseline and perform an account audit to easily identify newly added or deleted accounts.



Account and Password Management Automation

Accounts Baseline

Last Executed: N/A

Device Alias	Compatible	Model	Device IP	Baseline Accounts	Added Accounts	Deleted Accounts
192.168.123.70--AWK-3252A	Yes	AWK-3252A	192.168.123.70	N/A	N/A	N/A
192.168.127.11--EDS-G516E	Yes	EDS-G516E	192.168.127.11	N/A	N/A	N/A

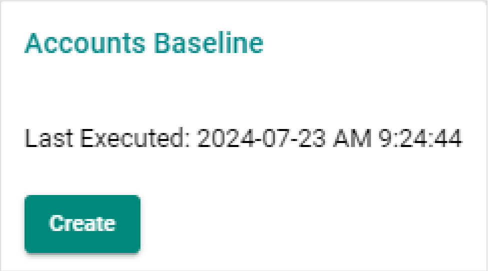
1 – 2 of 2

This page displays the following information in a table format:

Column	Description
Device Alias	The unique name of the device.
Compatible	Shows if the device supports MXview One retrieving account information. If the device does not support this function, the **Accounts** column will show **N/A**.
Model	The device model name.
Device IP	The IP address of the device.
Baseline Accounts	Shows the user accounts associated with the device when creating the baseline.
Added Accounts	Shows the user accounts that were added compared to the baseline after performing an account audit.
Deleted Accounts	Shows the user accounts that were deleted compared to the baseline after performing an account audit.

Creating an Account Baseline

1. Navigate to **Menu** (☰) **> Device Management > Account and Password**.
2. Go to the **Account Audit** tab.
3. The **Accounts Baseline** section includes the following information:

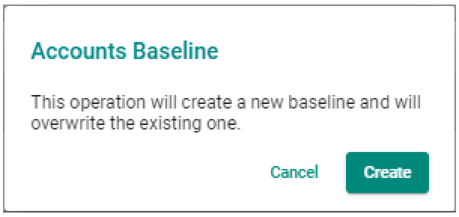


Accounts Baseline

Last Executed: 2024-07-23 AM 9:24:44

   - **Last Executed**: Shows the date and time when the most recent baseline was created. If no baseline has been created before, this will show **N/A**.

4. Click **Create**.
   The **Device Baseline** window will appear.



Accounts Baseline

This operation will create a new baseline and will overwrite the existing one.

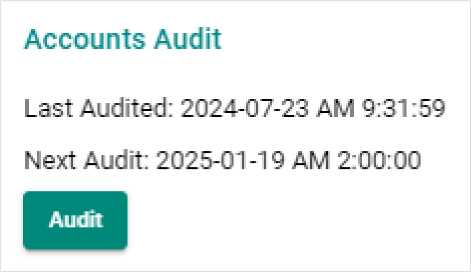
5. Click **Create**.

Executing a Manual Account Audit

NOTE

This function is only available after creating an account baseline. Refer to Creating an Account Baseline.

1. Navigate to **Menu** (☰) **> Device Management > Account and Password**.
2. Go to the **Account Audit** tab.
3. The **Accounts Audit** section shows the following information:



Accounts Audit

Last Audited: 2024-07-23 AM 9:31:59

Next Audit: 2025-01-19 AM 2:00:00

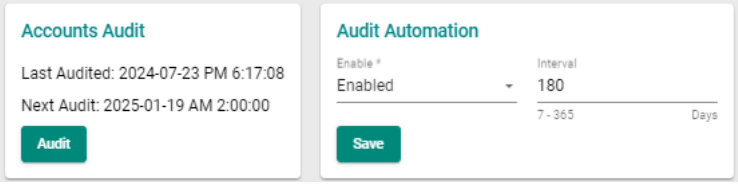
   - **Last Audited**: Shows the date and time of the most recent account audit.
   - **Next Audit**: If automatic account auditing is enabled, this shows the time and date of the next scheduled audit.

4. Click **Audit**.
   MXview One will compare the current accounts to the baseline and will show any added or deleted accounts in the table.

Configuring an Automatic Account Audit Schedule

> **NOTE**
>
> This function is only available after creating an account baseline. Refer to Creating an Account Baseline.

1. Navigate to **Menu** (☰) **> Device Management > Account and Password**.
2. Go to the **Account Audit** tab.
3. In the **Audit Automation** section, configure the following settings:



Accounts Audit

Last Audited: 2024-07-23 PM 6:17:08

Next Audit: 2025-01-19 AM 2:00:00

Audit Automation

Enable *: Enabled

Interval: 180

7 - 365 Days

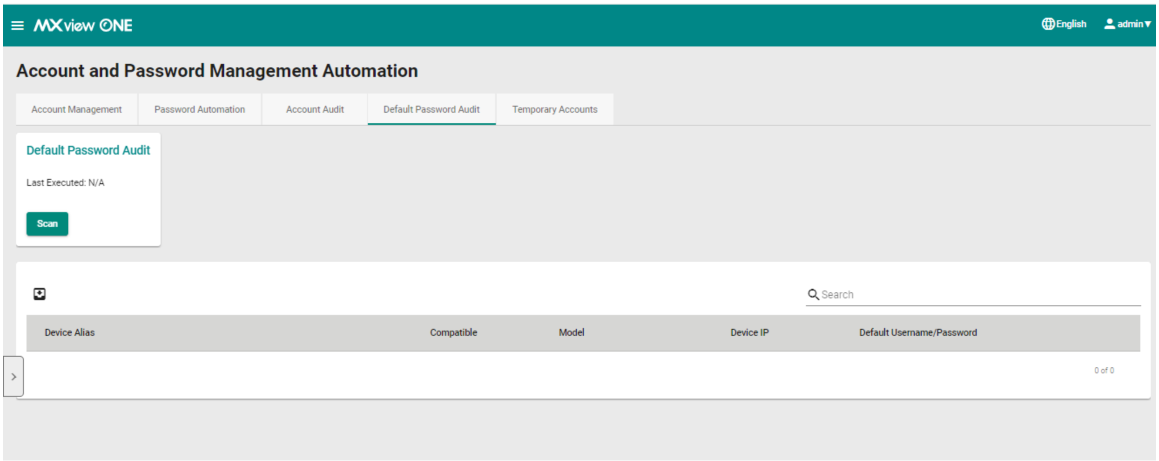
   - ➢ **Enable**: Enable or disable the automatic account auditing function.
   - ➢ **Interval**: Specify the interval (in days) when MXview One will perform an account audit.

4. Click **Save**.

Default Password Audit Overview

To access the **Default Password Audit** page, in the function tree, navigate to **Menu** (☰) **> Device Management > Account and Password** and go to the **Default Password Audit** tab.

The **Default Password Audit** tab lets users quickly check for any accounts that are using the default password.



Account and Password Management Automation

Default Password Audit

Last Executed: N/A

Device Alias	Compatible	Model	Device IP	Default Username/Password

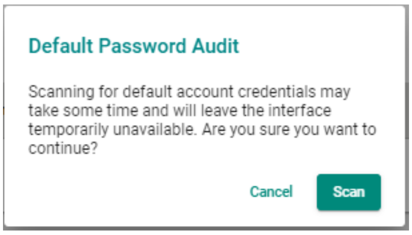
0 of 0

This page displays the following information in a table format:

Column	Description
Device Alias	The unique name of the device.
Compatible	Shows if the device supports MXview One retrieving account information.
Model	The device model name.
Device IP	The IP address of the device.
Default Account/Password	Shows if the account is using the default credentials: • **Yes**: The device uses the default username and password. For security reasons, it is highly recommended to change the default credentials. • **No**: The device is not using the default credentials. • **N/A**: MXview One cannot retrieve account information because the device does not support this feature.

Performing a Default Password Audit

1. Navigate to **Menu** (☰) **> Device Management > Account and Password**.
2. Go to the **Default Password Audit** tab.
3. In the **Default Password Audit** section, click **Scan**.
   The **Default Password Audit** window will appear.



Default Password Audit

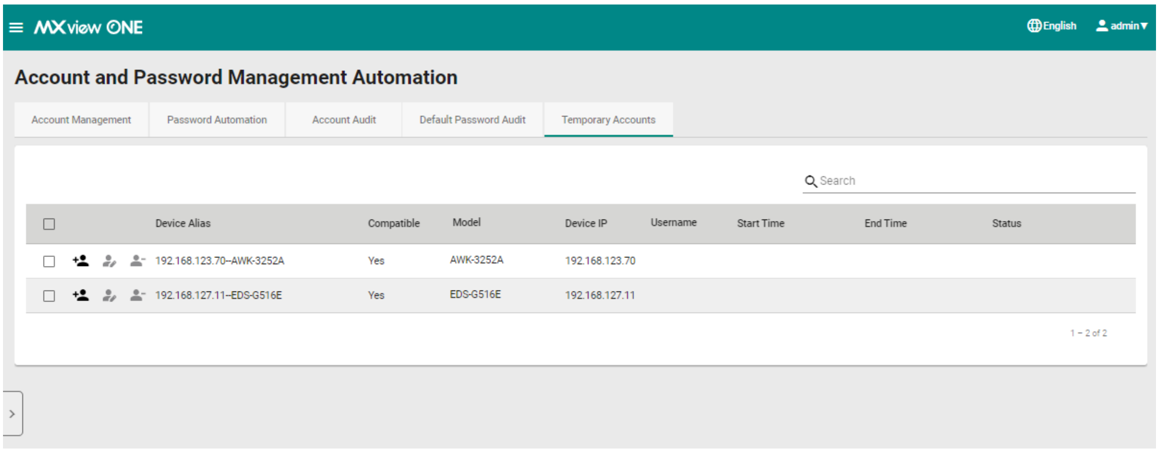
Scanning for default account credentials may take some time and will leave the interface temporarily unavailable. Are you sure you want to continue?

4. Click **Scan**.
   MXview One will scan for any accounts using the default credentials and list them in the table.

Temporary Accounts Overview

To access the **Temporary Accounts** page, in the function tree, navigate to **Menu** (☰) **> Device Management > Account and Password** and go to the **Temporary Accounts** tab.

The **Temporary Accounts** tab allows users to create, edit, and delete temporary accounts for devices.



Account and Password Management Automation

□	Device Alias	Compatible	Model	Device IP	Username	Start Time	End Time	Status
□	192.168.123.70--AWK-3252A	Yes	AWK-3252A	192.168.123.70				
□	192.168.127.11--EDS-G516E	Yes	EDS-G516E	192.168.127.11				

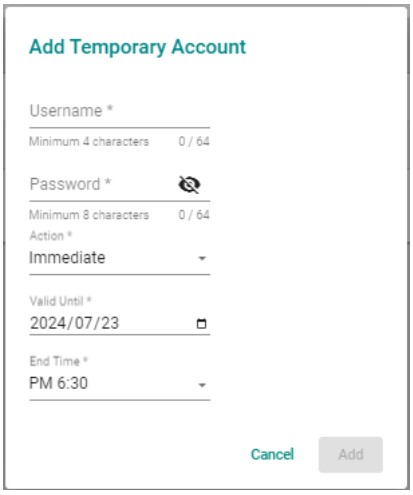
1 – 2 of 2

This page displays the following information in a table format:

Column	Description
Device Alias	The unique name of the device.
Compatible	Shows if the device supports the temporary accounts function.
Model	The device model name.
Device IP	The IP address of the device.
Username	The username of the account.
Start Time	The account validity start time.
End Time	The account validity end time.
Status	The status of the account.

Adding a Temporary Account

1. Navigate to **Menu** (☰) **> Device Management > Account and Password**.
2. Go to the **Temporary Accounts** tab.
3. Click the **Add** (+👤) icon next to the device you want to create a temporary account for.
   The **Add Temporary Account** window will appear.



Add Temporary Account

Username *

Minimum 4 characters 0 / 64

Password *

Minimum 8 characters 0 / 64

Action *

Immediate

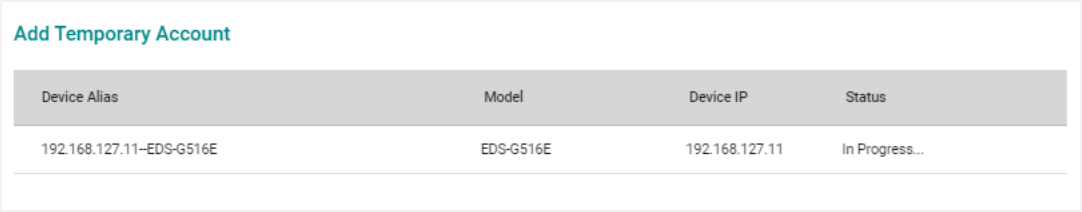
Valid Until *

2024/07/23

End Time *

PM 6:30

4. Configure the following settings:
   - **Username**: Enter a username for the account.
   - **Password**: Enter the password for the account.
   - **Action**: Select the type of account.
     - **Immediate**: The account will be active immediately until the specified end date.
     - **Scheduled**: The account will only be active during the specified time period.
   - **Active From**: If you selected **Scheduled**, specify the date the account will be valid from.
   - **Start Time**: If you selected **Scheduled**, specify the starting time the account will be valid from.
   - **Valid Until**: Specify the date the account expires.
   - **End Time**: Specify the time of day the account expires.
5. Click **Add**.
   MXview One will show the status of the account creation.

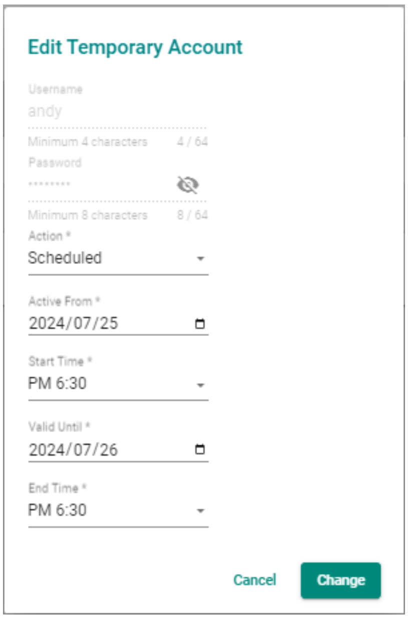


Add Temporary Account

Device Alias	Model	Device IP	Status
192.168.127.11--EDS-G516E	EDS-G516E	192.168.127.11	In Progress...

Editing a Temporary Account

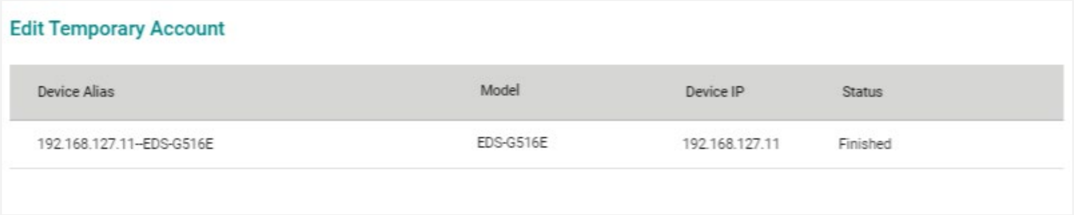
1. Navigate to **Menu** (☰) **> Device Management > Account and Password**.
2. Go to the **Temporary Accounts** tab.
3. Click the **Edit** ( ) icon next to the device you want to edit the temporary account for.
   The **Edit Temporary Account** window will appear.



Edit Temporary Account

Username
andy
Minimum 4 characters 4 / 64
Password
****
Minimum 8 characters 8 / 64
Action *
Scheduled
Active From *
2024/07/25
Start Time *
PM 6:30
Valid Until *
2024/07/26
End Time *
PM 6:30

4. Configure the following settings:
   - **Action**: Select the type of account.
     - **Immediate**: The account will be active immediately until the specified end date.
     - **Scheduled**: The account will only be active during the specified time period.
   - **Active From**: If you selected **Scheduled**, specify the date the account will be valid from.
   - **Start Time**: If you selected **Scheduled**, specify the starting time the account will be valid from.
   - **Valid Until**: Specify the date the account expires.
   - **End Time**: Specify the time of day the account expires.
5. Click **Change**.
   MXview One will show the status of the account modification.

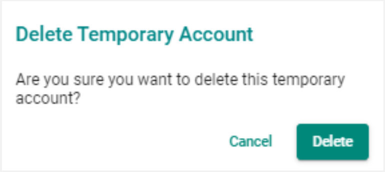


Edit Temporary Account

Device Alias	Model	Device IP	Status
192.168.127.11–EDS-G516E	EDS-G516E	192.168.127.11	Finished

Deleting a Temporary Account

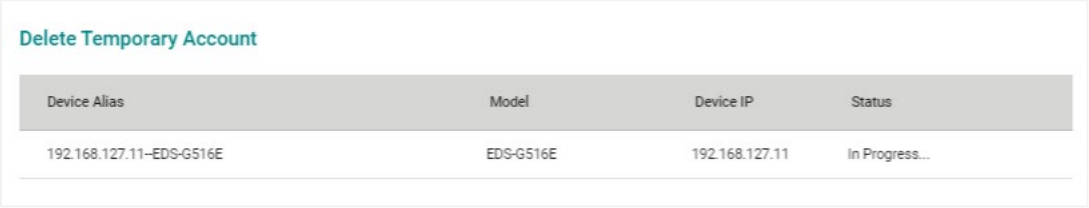
1. Navigate to **Menu** (☰) **> Device Management > Account and Password**.
2. Go to the **Temporary Accounts** tab.
3. Click the **Delete** (👤-) icon next to the device you want to delete the temporary account of.
   The **Delete Temporary Account** window will appear.



Delete Temporary Account

Are you sure you want to delete this temporary account?

4. Click **Delete**.
   MXview One will show the status of the account deletion.



Delete Temporary Account

Device Alias	Model	Device IP	Status
192.168.127.11--EDS-G516E	EDS-G516E	192.168.127.11	In Progress...

12. Saved CLI Scripts

The CLI Scripts function allows users to generate and execute CLI scripts from within MXview One. After creating and saving CLI scripts, users can create script automations and automation buttons to quickly execute batch configurations on multiple devices at once.

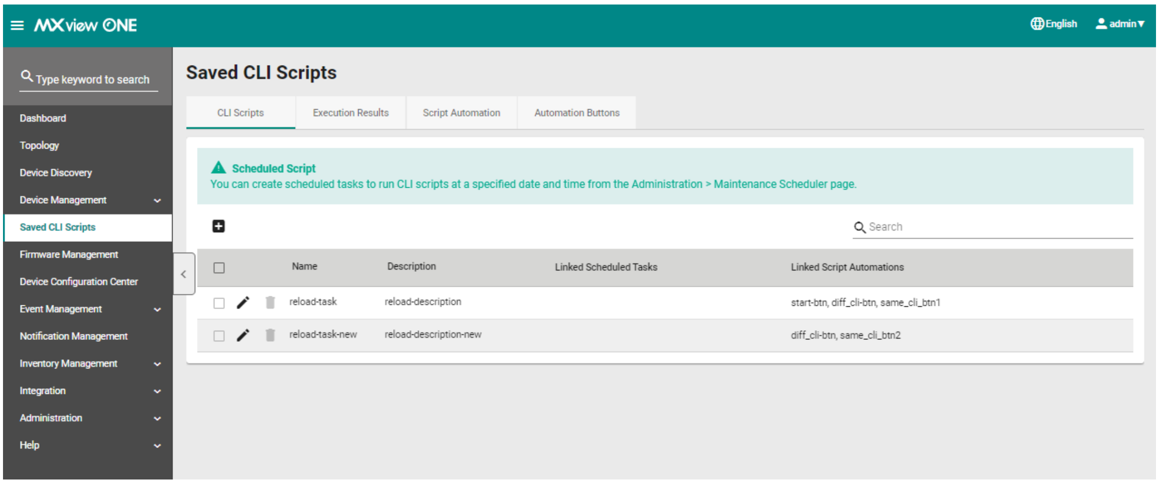
Saved CLI Scripts Overview

To access the **Saved CLI Scripts** page, in the function tree, navigate to **Menu** (☰) > **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.
- **Script Automation**: From this tab, you can view, create, edit, or delete script automations.
- **Automation Buttons**: Each script automation you create will generate an automation button. From this tab, you can manage script automation buttons.



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	Linked Scheduled Tasks	Linked Script Automations
□	reload-task	reload-description		start-btn, diff_cli-btn, same_cli_btn1
□	reload-task-new	reload-description-new		diff_cli-btn, same_cli_btn2

CLI Scripts

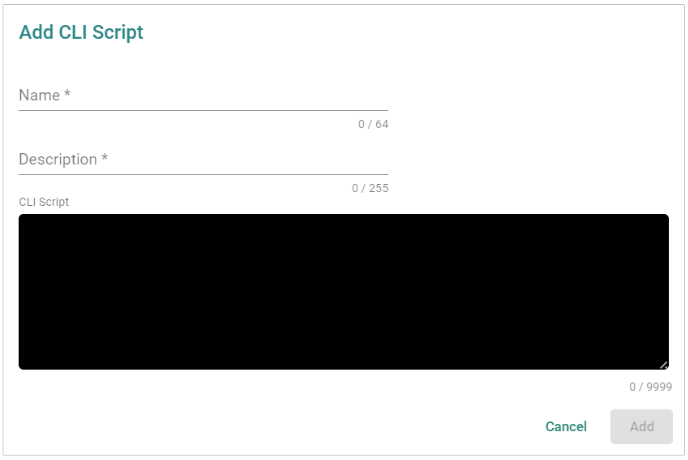
Adding a CLI Script

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

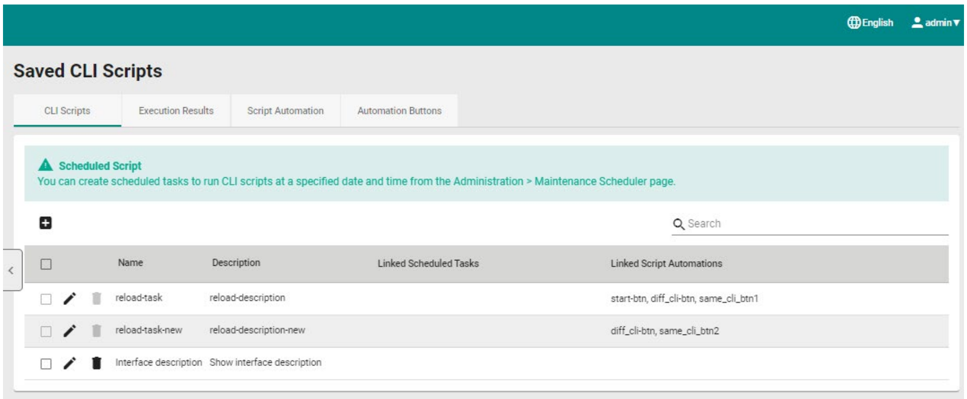
3. Configure the following settings:

   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	Linked Scheduled Tasks	Linked Script Automations
□	reload-task	reload-description		start-btn, diff_cli-btn, same_cli_btn1
□	reload-task-new	reload-description-new		diff_cli-btn, same_cli_btn2
□	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.

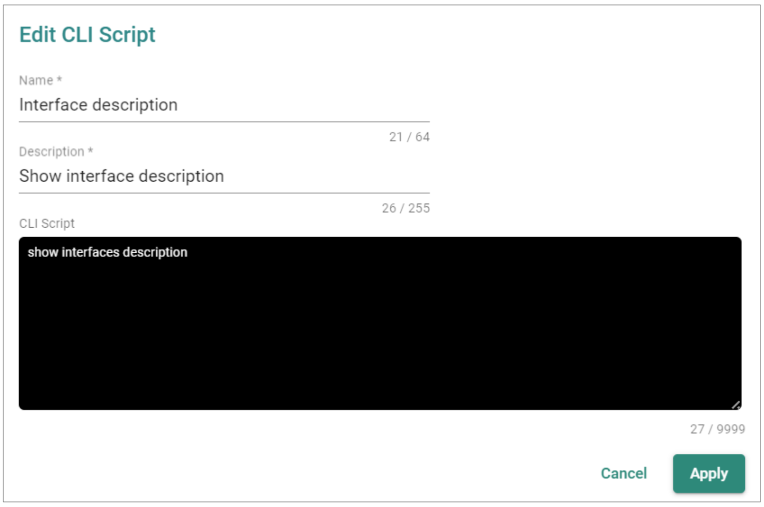
Editing a CLI Script

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

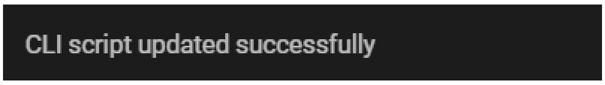
3. Configure the following settings:

   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

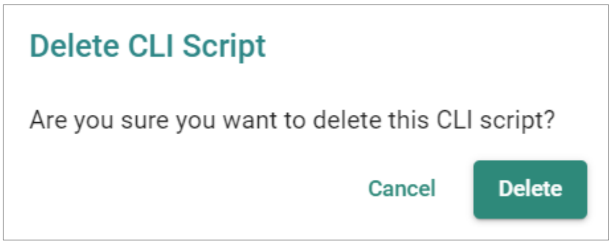
Deleting a CLI Script

> **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

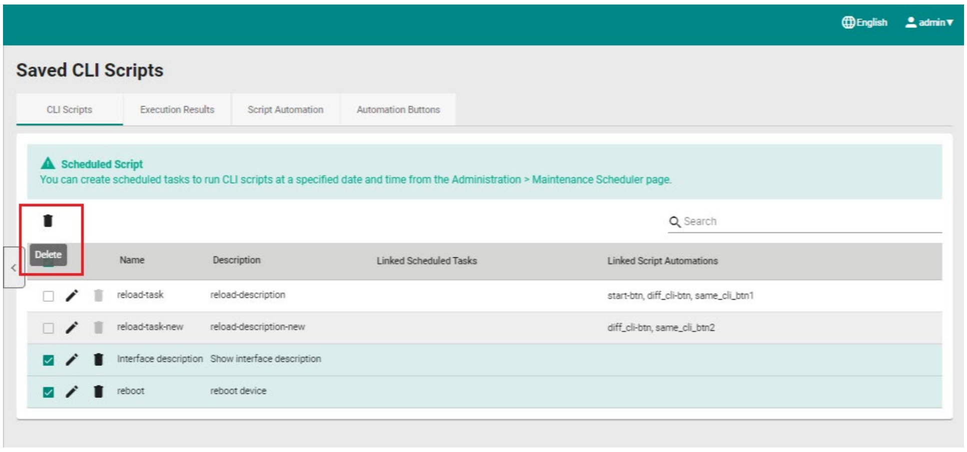
> **NOTE**
>
> A CLI script cannot be deleted if it is linked to a scheduled task. To delete the script, modify or delete the scheduled task first on the **Administration> Maintenance Scheduler** page.

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.

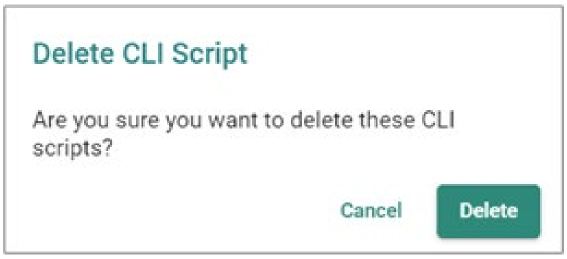
3. Click the **Delete** (🗑) icon at the top-left corner of the page.



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	Linked Scheduled Tasks	Linked Script Automations
☐	✎	🗑	reload-task	reload-description		start-btn, diff_cli-btn, same_cli_btn1
☐	✎	🗑	reload-task-new	reload-description-new		diff_cli-btn, same_cli_btn2
☑	✎	🗑	Interface description	Show interface description		
☑	✎	🗑	reboot	reboot device		

4. A confirmation window will appear.



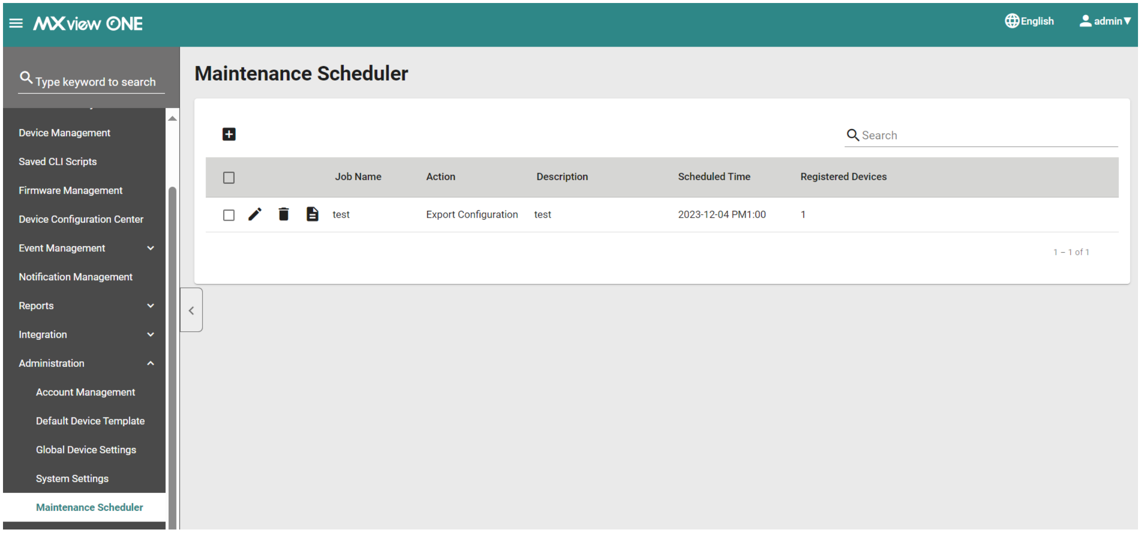
Delete CLI Script

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.

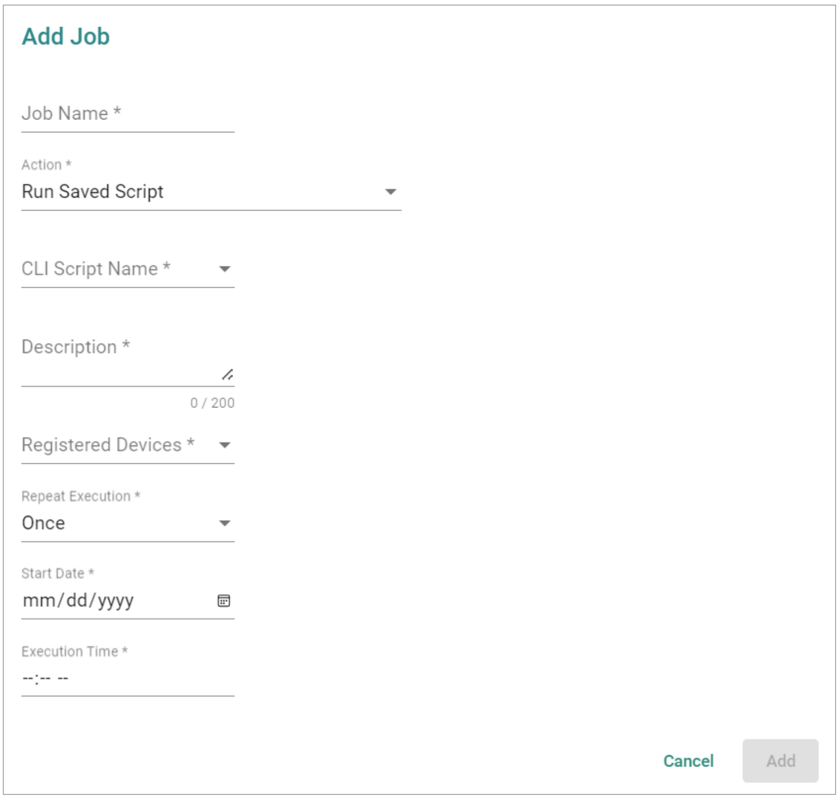


Maintenance Scheduler

□		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

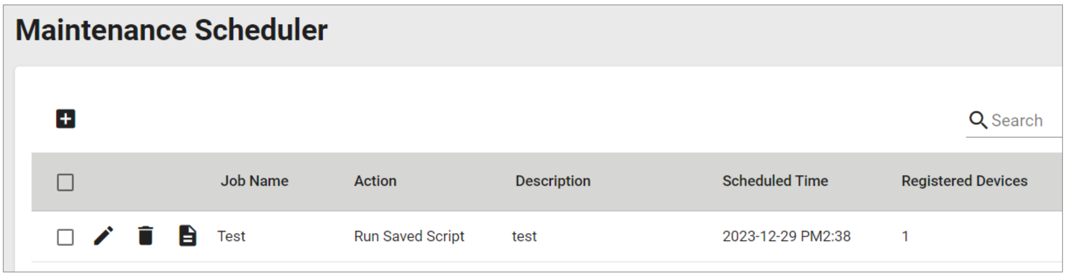
Registered Devices *

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

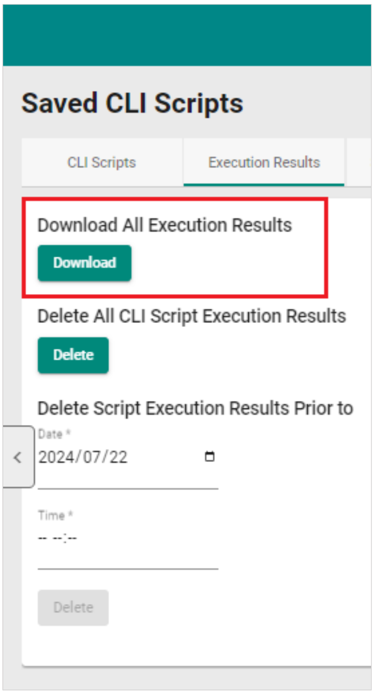
Execution Results

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.



Saved CLI Scripts

CLI Scripts
Execution Results
Download All Execution Results
Download
Delete All CLI Script Execution Results
Delete
Delete Script Execution Results Prior to
Date *
2024/07/22
Time *
-- --:--
Delete

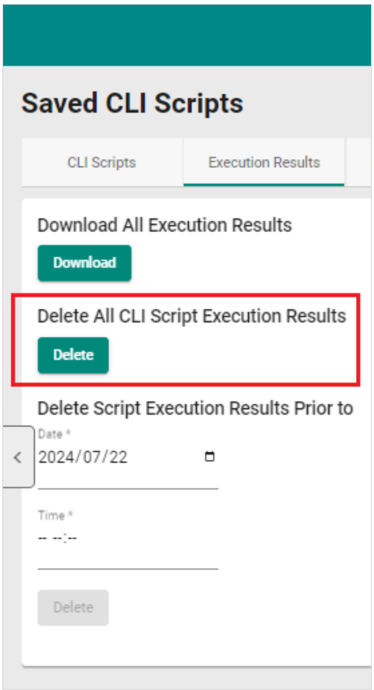
3. Click **Download**.
   MXview One will download all the CLI script execution results as a ZIP file.

Delete All CLI Script Execution Results

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

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

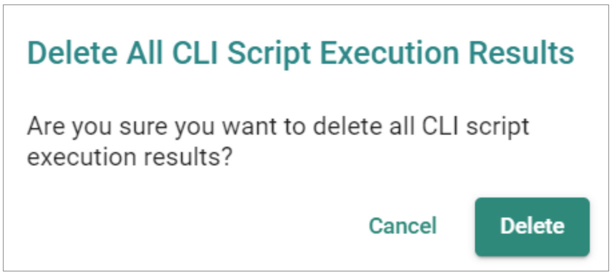
2. Go to the **Execution Results** tab.


Saved CLI Scripts
CLI Scripts
Execution Results
Download All Execution Results
Download
Delete All CLI Script Execution Results
Delete
Delete Script Execution Results Prior to
Date *
Time *
Delete

Date * 2024/07/22

Time * -- --:--

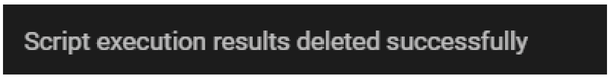
3. Click **Delete**.
   A confirmation window will appear.



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.

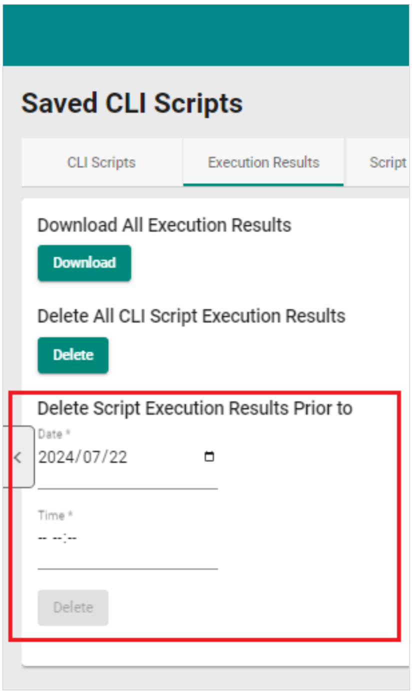


Script execution results deleted successfully

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.



Saved CLI Scripts

Download All Execution Results

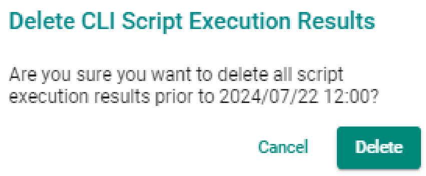
Delete All CLI Script Execution Results

Delete Script Execution Results Prior to

Date * 2024/07/22

Time * -- --:--

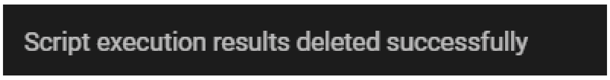
3. Specify the **Date** and **Time**. All execution results prior to this time will be deleted.
4. Click **Delete**.
   A confirmation window will appear.



Delete CLI Script Execution Results

Are you sure you want to delete all script execution results prior to 2024/07/22 12:00?

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



Script execution results deleted successfully

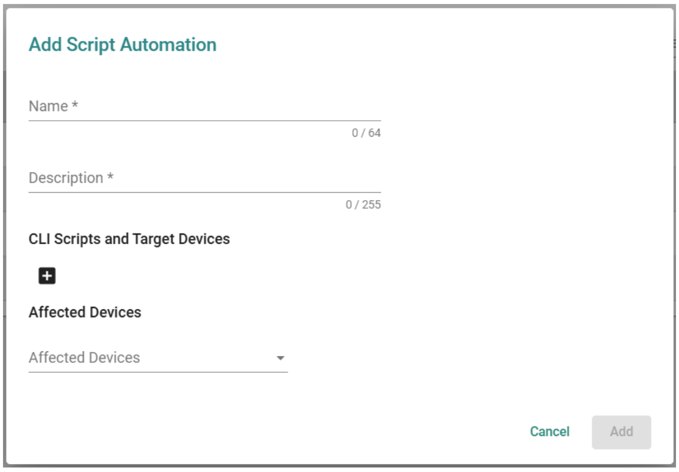
Script Automation

From the **Script Automation** screen, you can create and manage script automations. A script automation allows you to combine multiple saved CLI scripts into a single script. A corresponding automation button then lets you quickly execute the included commands to the specified devices with just a single click.

Adding a Script Automation

1. Navigate to **Menu** (☰) **> Saved CLI Scripts**.
   The **Saved CLI Scripts** screen will appear.
2. Go to the **Script Automation** tab.

3. Click the **Add** (⊞) icon.
   The **Add Script Automation** screen will appear.



4. Configure the following settings:
   - **Name**: Enter a name for the script automation.
   - **Description**: Enter a description for the script automation.
   - **CLI Scripts and Target Devices**: Select the saved CLI script and devices to include in this automation. You can add a maximum of 50 scripts in a single script automation.
     This requires a previously created saved CLI script. Refer to the Adding a CLI Script section.

     Click the **Add** (⊞) icon to add additional entries to the automation.

NOTE

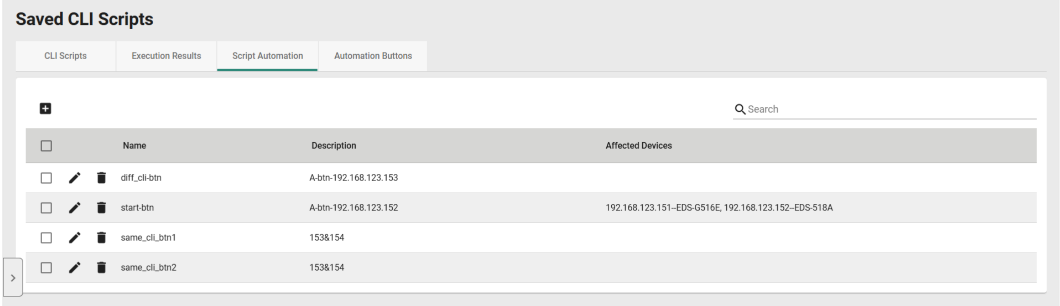
Only one saved CLI script can be assigned to an individual target device.

   - **Affected Devices**: Select the device(s) that will be affected by executing the CLI script(s) in the automation. A warning reminder with a list of affected devices will show when attempting to execute the automation button. If left blank, relevant devices will still be affected, but no warning will be shown in the Topology.

NOTE

If the **Automation Button Display Mode** is set to **Panel**, devices affected by CLI script automations can be visually highlighted in the topology. Refer to Previewing Affected Devices.

5. Click **Add**.
   The script automation will be added to the table. Each script automation entry will also create an individual button in the Automation Buttons section. Refer to the Automation Buttons section.



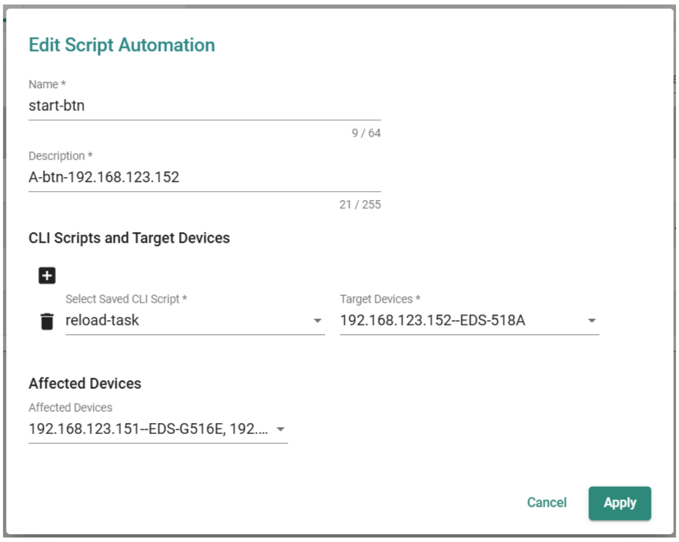
	Name	Description	Affected Devices
□	diff_cli-btn	A-btn-192.168.123.153	
□	start-btn	A-btn-192.168.123.152	192.168.123.151--EDS-G516E, 192.168.123.152--EDS-518A
□	same_cli_btn1	153&154	
□	same_cli_btn2	153&154	

NOTE

MXview One supports a maximum of 200 script automations.

Editing a Script Automation

1. Navigate to **Menu** (☰) **> Saved CLI Scripts**.
   The **Saved CLI Scripts** screen will appear.
2. Go to the **Script Automation** tab.
3. Click the **Edit** (✎) icon next to the script automation you want to edit.
   The **Edit Script Automation** screen will appear.



Edit Script Automation

Name *
start-btn
9 / 64

Description *
A-btn-192.168.123.152
21 / 255

CLI Scripts and Target Devices

Select Saved CLI Script *
reload-task

Target Devices *
192.168.123.152--EDS-518A

Affected Devices

Affected Devices
192.168.123.151--EDS-G516E, 192....

4. Configure the following settings:
   - **Name**: Enter a name for the script automation.
   - **Description**: Enter a description for the script automation.
   - **CLI Script and Target Devices**: Select the saved CLI script and device(s) to include in this automation. You can add a maximum of 50 scripts in a single script automation.
     This requires a previously created saved CLI script. Refer to the Adding a CLI Script section.

     Click the **Add** (⊞) icon to add additional entries to the automation.

     Click the **Delete** (🗑) icon to remove an entry.
   - **Affected Devices**: Select the device(s) that will be affected by executing the CLI script(s) in the automation. A warning reminder with a list of affected devices will show when attempting to execute the automation button. If left blank, relevant devices will still be affected, but no warning will be shown in the Topology.

NOTE

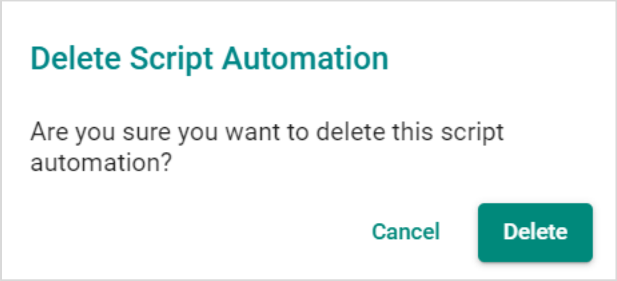
If the **Automation Button Display Mode** is set to **Panel**, devices affected by CLI script automations can be visually highlighted in the topology. Refer to Previewing Affected Devices.

5. Click **Apply**.
   A confirmation will appear to verify the script automation was updated

Updated successfully

Deleting a Script Automation

1. Navigate to **Menu** (☰) **> Saved CLI Scripts**.
2. Go to the **Script Automation** tab.
   The **Script Automation** screen will appear. A list of configured script automation will show.
3. Click the **Delete** (🗑) icon next to the script automation you want to delete.
   A confirmation window will appear.



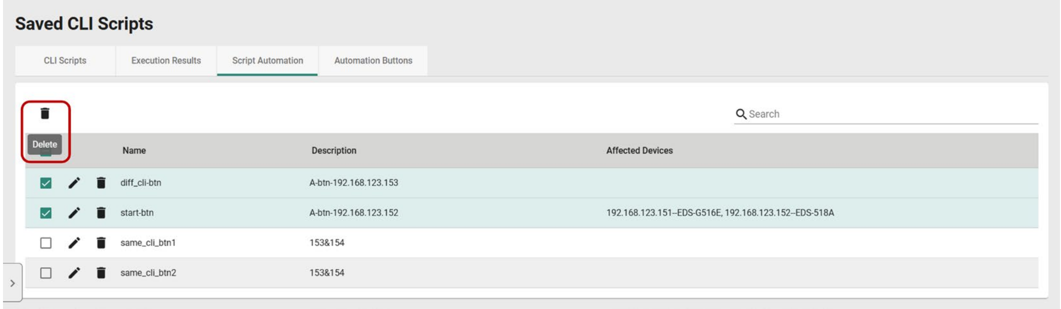
Delete Script Automation

Are you sure you want to delete this script automation?

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

Deleting Multiple Script Automations

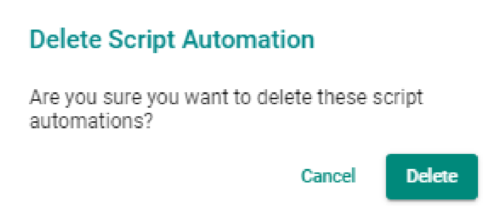
1. Navigate to **Menu** (☰) **> Saved CLI Scripts**.
2. Go to the **Script Automation** tab.
   The **Script Automation** screen will appear. A list of configured script automation will show in the CLI Scripts list (if any).
3. Select the checkbox of the script automations you want to delete in the list.
4. Click the **Delete** (🗑) icon at the top of the page.



Saved CLI Scripts

	Name	Description	Affected Devices
☑	diff_cli-btn	A-btn-192.168.123.153	
☑	start-btn	A-btn-192.168.123.152	192.168.123.151--EDS-G516E, 192.168.123.152--EDS-518A
□	same_cli_btn1	153&154	
□	same_cli_btn2	153&154	

5. A confirmation window will appear.



Delete Script Automation

Are you sure you want to delete these script automations?

6. Click **Delete**.
   A confirmation will appear to verify the script automations were deleted.

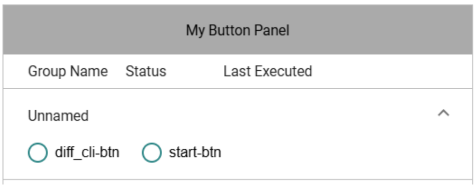
Automation Buttons

From the **Automation Buttons** screen, you can manage automation buttons for configured script automations.

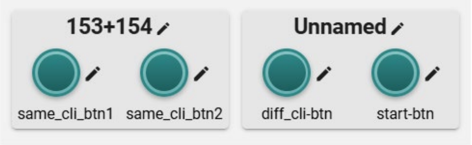
Each newly added automation script will automatically generate an automation button that is placed in the default Unnamed group.

Setting the Automation Button Display Mode

1. Navigate to **Menu** (☰) **> Saved CLI Scripts**.
2. Go to the **Automation Buttons** tab.
3. Select the automation button display mode from the **Display Mode** drop-down list.
   - **Panel**: Show automation buttons in a panel format. This mode also allows you to preview devices affected by CLI script automations on the Topology screen. Refer to Previewing Affected Devices.



   - **Widget**: Show automation in a widget format. The widget size can be adjusted. Refer to Changing the Automation Button Widget Size.



4. Click **Apply**.

Configuring Automation Button Authentication Settings

1. Navigate to **Menu** (☰) **> Saved CLI Scripts**.
2. Go to the **Automation Buttons** tab.
3. Enable or disable the admin authentication using the **Require Admin Authentication** drop-down list.
   - **Enable**: Users need to enter the password of currently logged in account to execute the automation button.
   - **Disable**: Users can execute automation buttons without any authentication.
4. Click **Apply**.

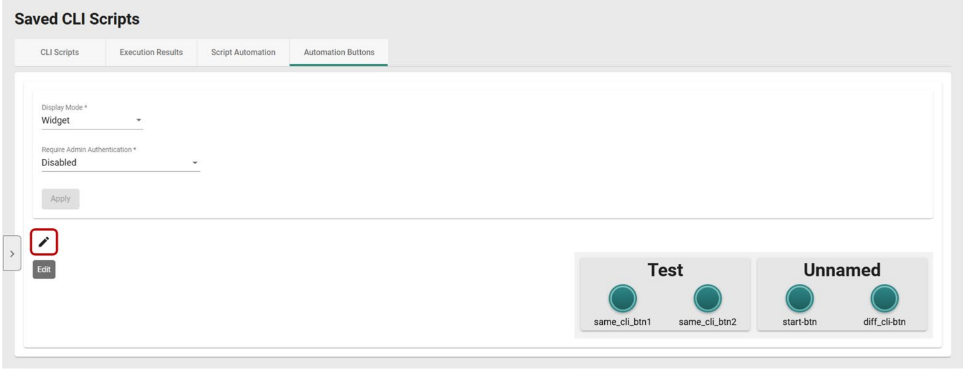
Editing an Automation Button Group

NOTE

The interface elements may appear slightly different depending on the selected **Automation Button Display Mode**, but the process is the same for both view modes. The images in the instructions use **Widget** mode.

1. Navigate to **Menu** (☰) **> Saved CLI Scripts**.
2. Go to the **Automation Buttons** tab.

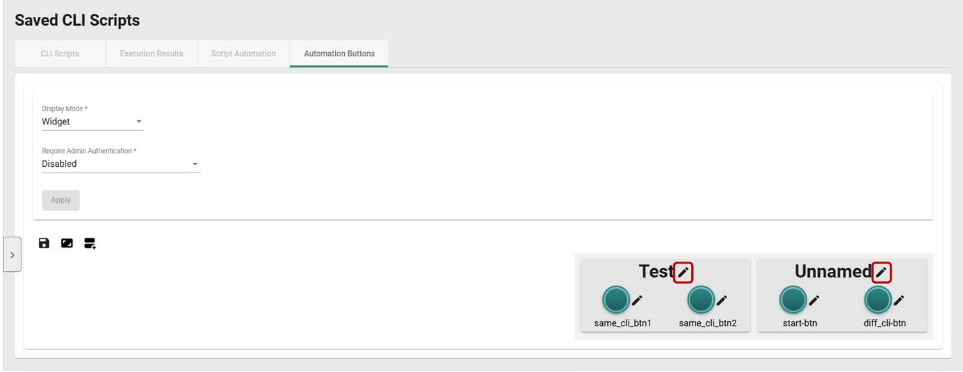
3. Click the **Edit** (✎) icon in the top-left corner of the screen to enter edit mode.



Display Mode *
Widget

Require Admin Authentication *
Disabled

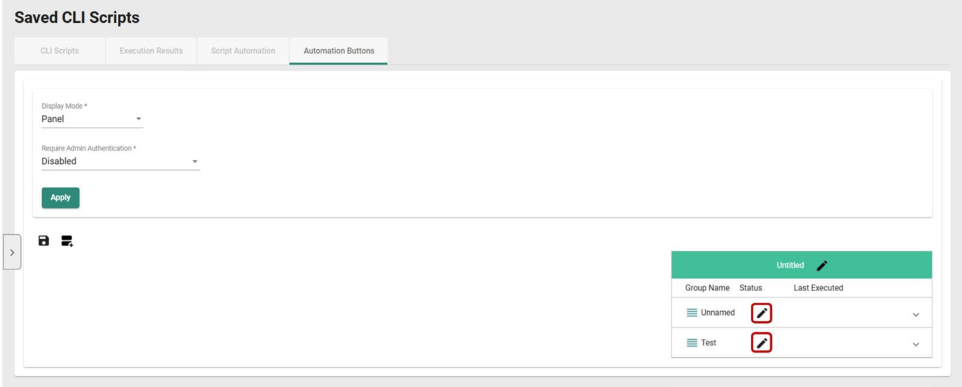
4. Click the **Edit** (✎) icon next to the group name of the group you want to edit.
   Widget mode:



Display Mode *
Widget

Require Admin Authentication *
Disabled

Panel mode:

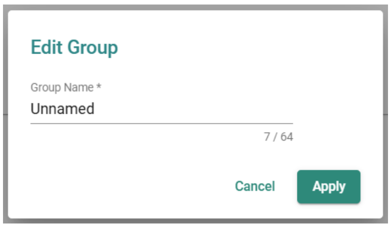


Display Mode *
Panel

Require Admin Authentication *
Disabled

Group Name	Status	Last Executed
Unnamed		
Test		

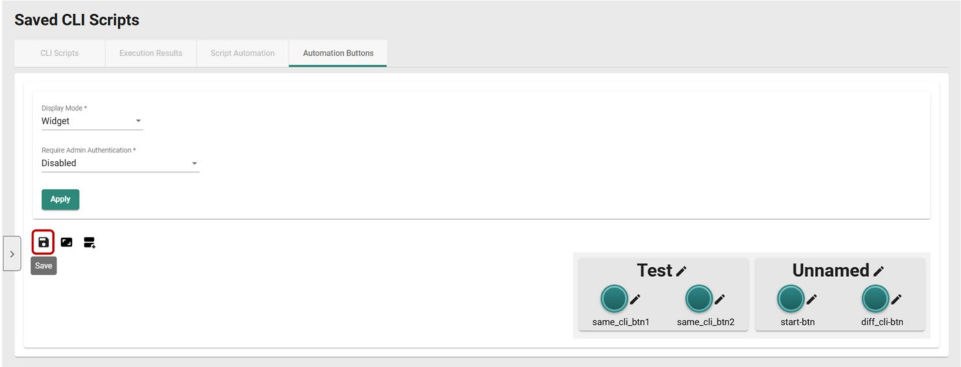
The **Edit Group** will appear.



Group Name *
Unnamed

5. Configure the following settings:
   - **Group Name**: Enter a name for the group.
   - **Reorder Buttons**: (For Widget mode only) Click and drag the buttons to adjust their position.
6. Click **Apply**.
   The changes will appear on the **Automation Buttons** page.

7. Click the **Save** (🖫) icon to save your changes and leave edit mode.

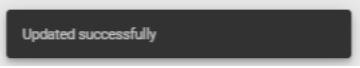


Saved CLI Scripts

Display Mode *: Widget

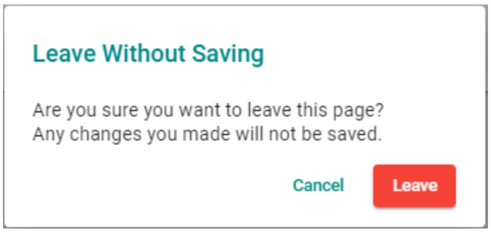
Require Admin Authentication *: Disabled

8. A confirmation will appear to verify the button group was updated.



Updated successfully

If you leave the **Automation Buttons** page without saving, a confirmation window will appear.



Leave Without Saving

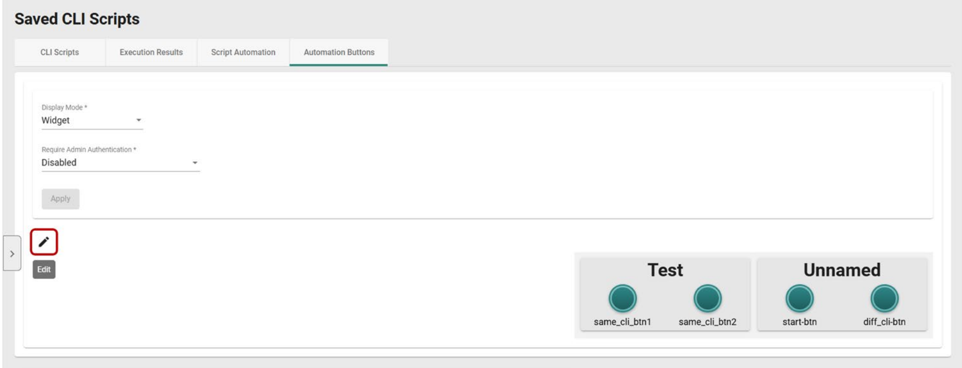
Are you sure you want to leave this page?
Any changes you made will not be saved.

Editing an Automation Button

NOTE

The interface elements may appear slightly different depending on the selected **Automation Button Display Mode**, but the process is the same for both view modes. The images in the instructions use **Widget** mode.

1. Navigate to **Menu** (☰) **> Saved CLI Scripts**.
2. Go to the **Automation Buttons** tab.
3. Click the **Edit** (✎) icon in the top-left corner of the screen to enter edit mode.

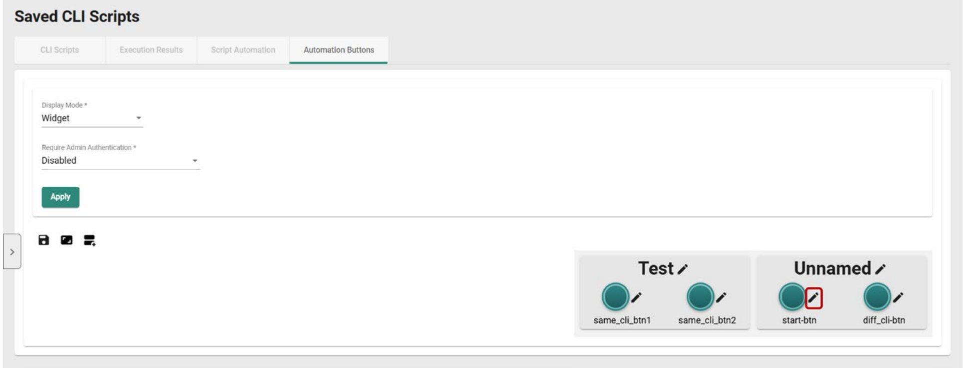


Saved CLI Scripts

Display Mode *: Widget

Require Admin Authentication *: Disabled

4. Click the **Edit** (✎) icon next to the button you want to edit.
Widget home:

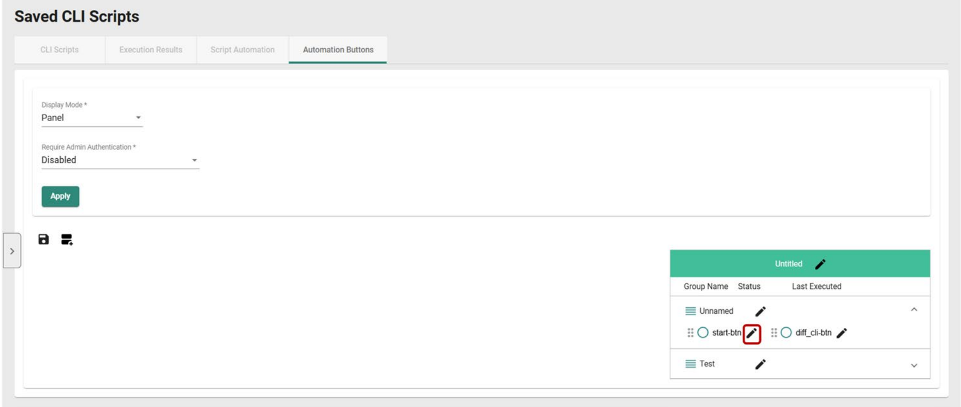


Saved CLI Scripts

Display Mode * Widget

Require Admin Authentication * Disabled

Panel mode:

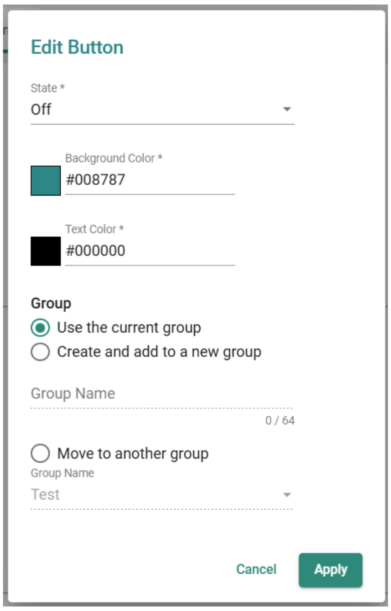


Saved CLI Scripts

Display Mode * Panel

Require Admin Authentication * Disabled

The **Edit Button** window will appear.



Edit Button

State * Off

Background Color * #008787

Text Color * #000000

Group

● Use the current group

○ Create and add to a new group

Group Name

0 / 64

○ Move to another group

Group Name Test

5. Configure the following settings:

   a. **State**: (For Panel mode only) Enable or disable the automation button.

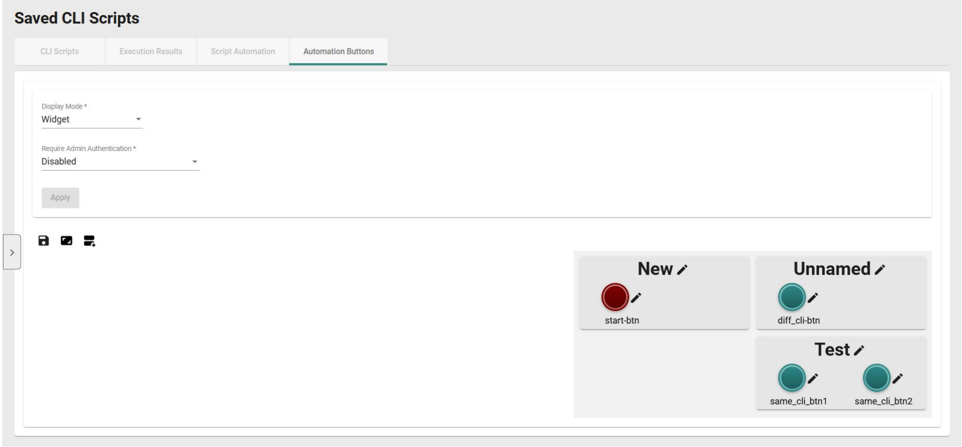
   b. **Background Color**: Click the value to open the color picker. Select the preferred background color on the color picker or enter the color's hex value.

   c. **Text Color**: Click the value to open the color picker. Select the preferred text color on the color picker or enter the color's hex value.

   d. **Group**: Select the group to assign this button to.

      - **Use the current group**: Leave the button in its currently assigned group.
      - **Create and add to a new group**: Create and assign the button to a new group.
      - **Move to another group**: Select an existing group to assign the button to.

6. Click **Apply**.
   The changes will appear on the **Automation Buttons** page.

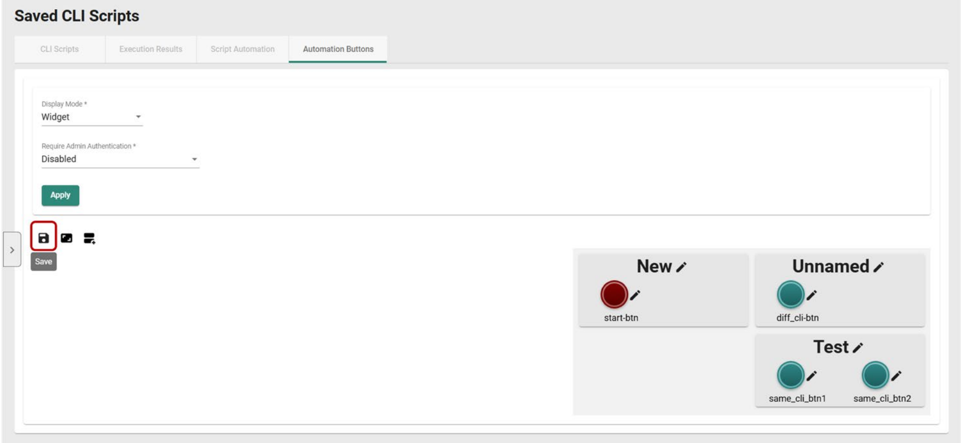


Saved CLI Scripts

Display Mode *: Widget

Require Admin Authentication *: Disabled

7. Click the **Save** (💾) icon to save your changes and leave edit mode.

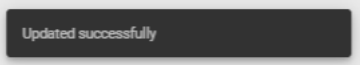


Saved CLI Scripts

Display Mode *: Widget

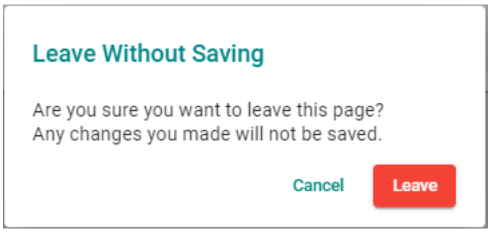
Require Admin Authentication *: Disabled

8. A confirmation will appear to verify the button was updated.



Updated successfully

If you leave the **Automation Buttons** page without saving, a confirmation window will appear.



Leave Without Saving

Are you sure you want to leave this page?
Any changes you made will not be saved.

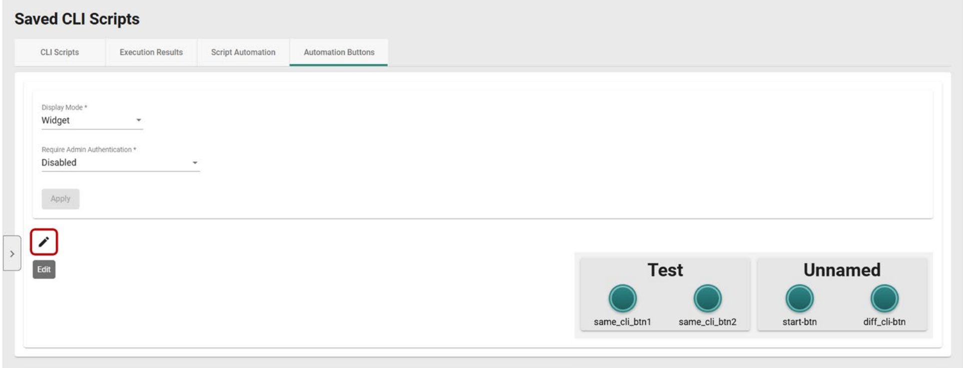
Creating an Automation Button Group

NOTE

The interface elements may appear slightly different depending on the selected **Automation Button Display Mode**, but the process is the same for both view modes. The images in the instructions use **Widget** mode.

1. Navigate to **Menu** (☰) **> Saved CLI Scripts**.
2. Go to the **Automation Buttons** tab.

3. Click the **Edit** (✎) icon in the top-left corner of the screen to enter edit mode.

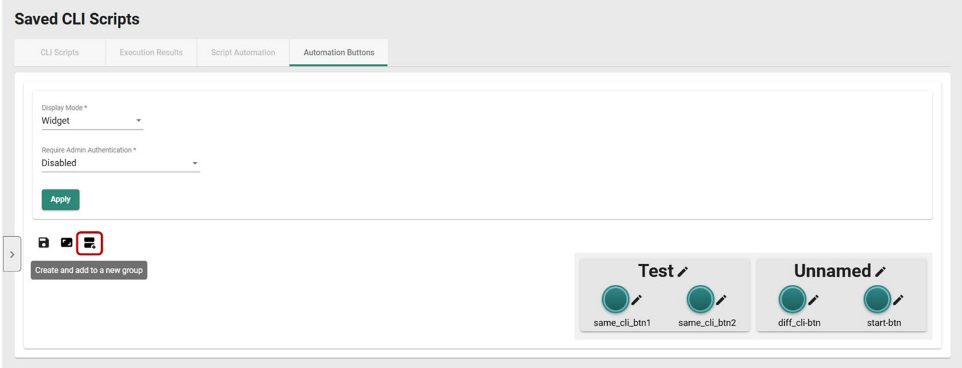


Saved CLI Scripts

Display Mode *: Widget

Require Admin Authentication *: Disabled

Click the **Create and add to a new group** ( ) icon in the top-left corner of the screen.

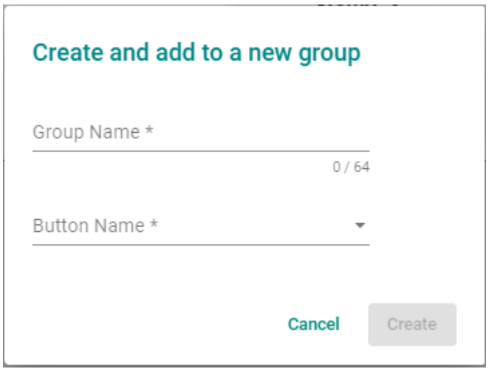


Saved CLI Scripts

Display Mode *: Widget

Require Admin Authentication *: Disabled

The **Create and add to a new group** window will appear.



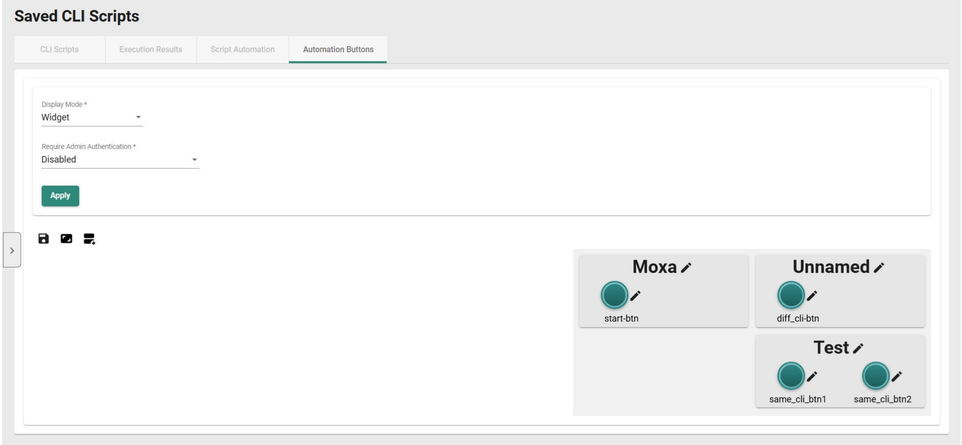
Create and add to a new group

Group Name *

0 / 64

Button Name *

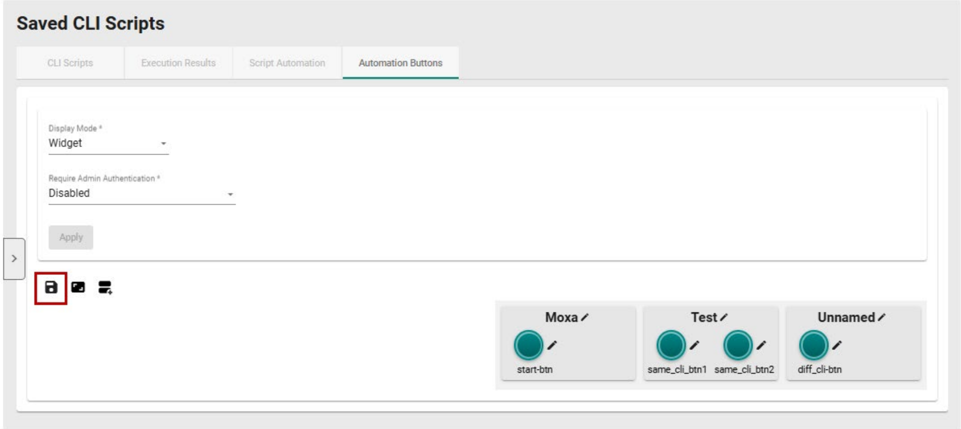
4. Configure the following settings:
   - **Group Name**: Enter a name for the group.
   - **Button Name**: Select the button(s) to add to this group.
5. Click **Create**.
   The changes will appear on the **Automation Buttons** page.


Saved CLI Scripts

Display Mode *: Widget

Require Admin Authentication *: Disabled

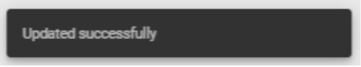
6. Click the **Save** (🖫) icon to save your changes and leave edit mode.


Saved CLI Scripts

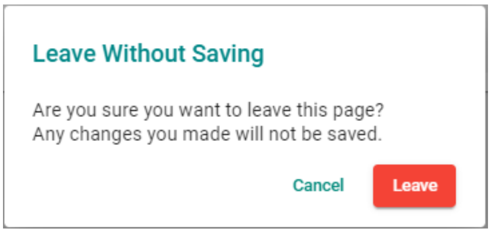
Display Mode *: Widget

Require Admin Authentication *: Disabled

7. A confirmation will appear to verify the button was updated.


Updated successfully

If you leave the **Automation Buttons** page without saving, a confirmation window will appear.


Leave Without Saving

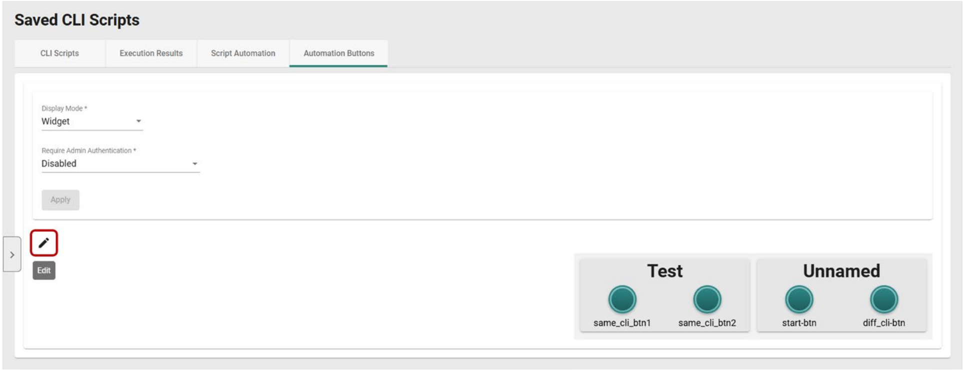
Are you sure you want to leave this page?
Any changes you made will not be saved.

Changing the Automation Button Widget Size

NOTE

This function is only available if the **Automation Button Display Mode** is set to **Widget**. Changes to the widget size will reflect on both the **Automation Buttons** and **Topology** pages.

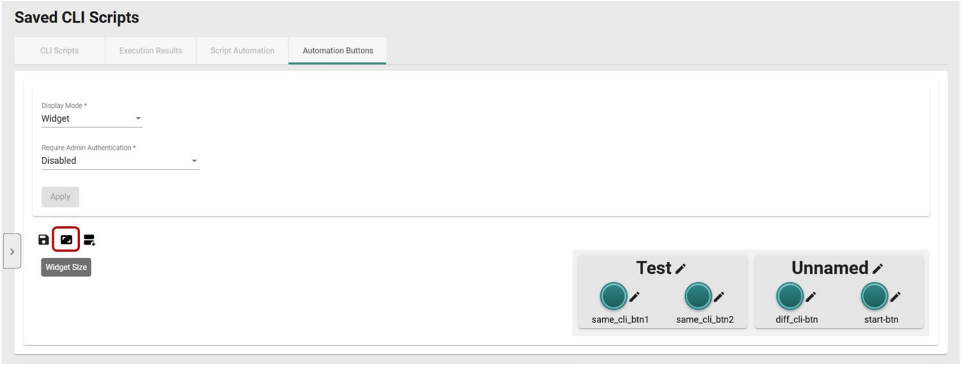
1. Navigate to **Menu** (☰) **> Saved CLI Scripts**.
2. Go to the **Automation Buttons** tab.
3. Click the **Edit** (✎) icon in the top-left corner of the screen to enter edit mode.



Display Mode * Widget

Require Admin Authentication * Disabled

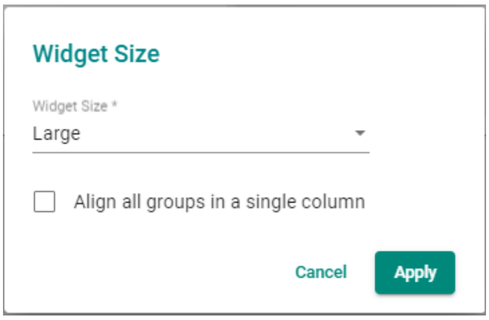
Click the **Widget Size** ( ) icon in the top-left corner of the screen.



Display Mode * Widget

Require Admin Authentication * Disabled

The **Widget Size** window will appear.



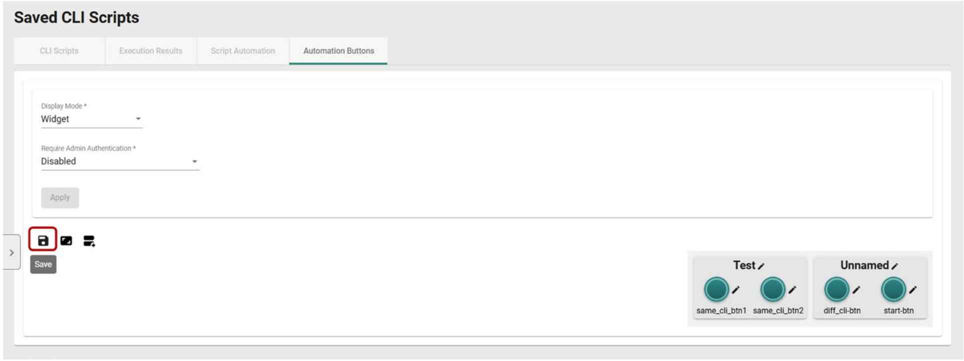
Widget Size

Widget Size * Large

□ Align all groups in a single column

4. Configure the following settings:
   - **Widget Size**: Select the size of the automation button widgets on the **Automation Buttons** and **Topology** pages.
   - **Align all groups in a single column**: Check to align automation button group widgets in a single column.

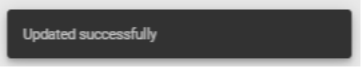
5. Click the **Save** ( ) icon to save your changes and leave edit mode



Display Mode * Widget

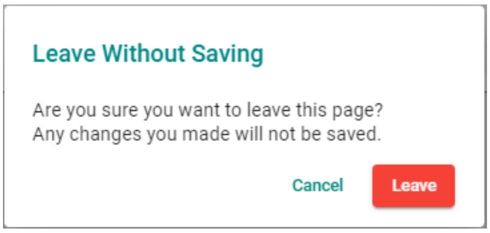
Require Admin Authentication * Disabled

6. A confirmation will appear to verify the button was updated.



Updated successfully

If you leave the **Automation Buttons** page without saving, a confirmation window will appear.



Leave Without Saving

Are you sure you want to leave this page?
Any changes you made will not be saved.

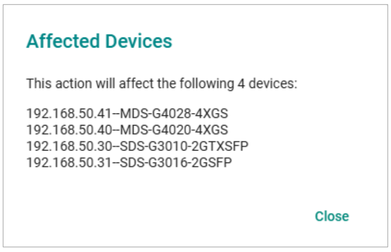
Previewing Affected Devices

You can highlight any devices affected by CLI script automations in the topology screen. Only devices listed as Affected Devices of a script automation will be highlighted. Refer to Adding a Script Automation.

NOTE

This function is only available if the **Automation Button Display Mode** is set to **Panel**. Refer to Setting the Automation Button Display Mode.

1. Navigate to **Menu** (☰) **> Topology**.
2. Hover over the automation button you want to execute.
   A hint message box will appear next to the button.
3. Click **more ...** to show a list of all affected devices.

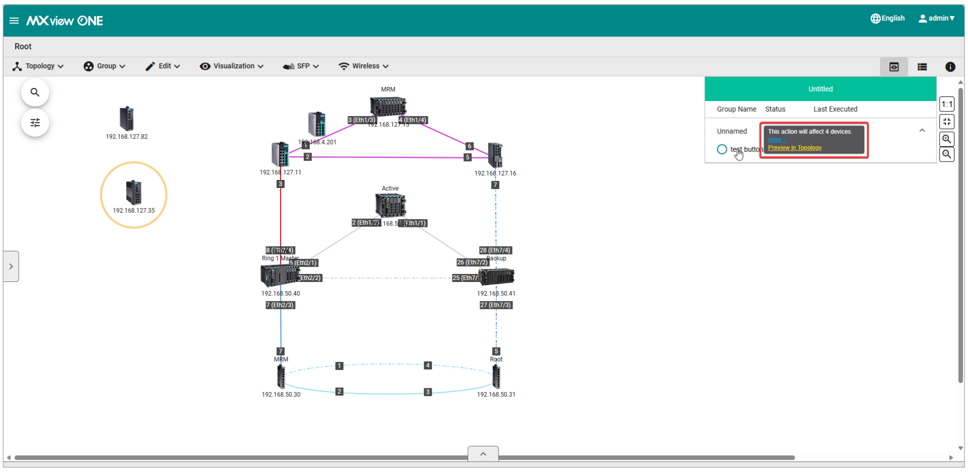


Affected Devices

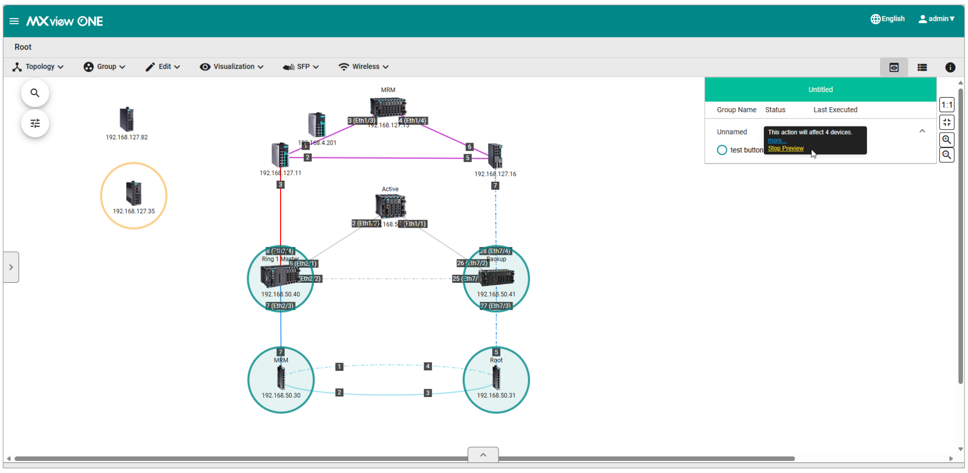
This action will affect the following 4 devices:

192.168.50.41–MDS-G4028-4XGS
192.168.50.40–MDS-G4020-4XGS
192.168.50.30–SDS-G3010-2GTXSFP
192.168.50.31–SDS-G3016-2GSFP

4. Click **Preview in Topology** to highlight the affected devices in the topology.



5. The affected devices will be highlighted in the topology. Click **Stop Preview** to close the preview.



Untitled

Group Name	Status	Last Executed
Unnamed		
○ test button		

This action will affect 4 devices.
more...
Stop Preview

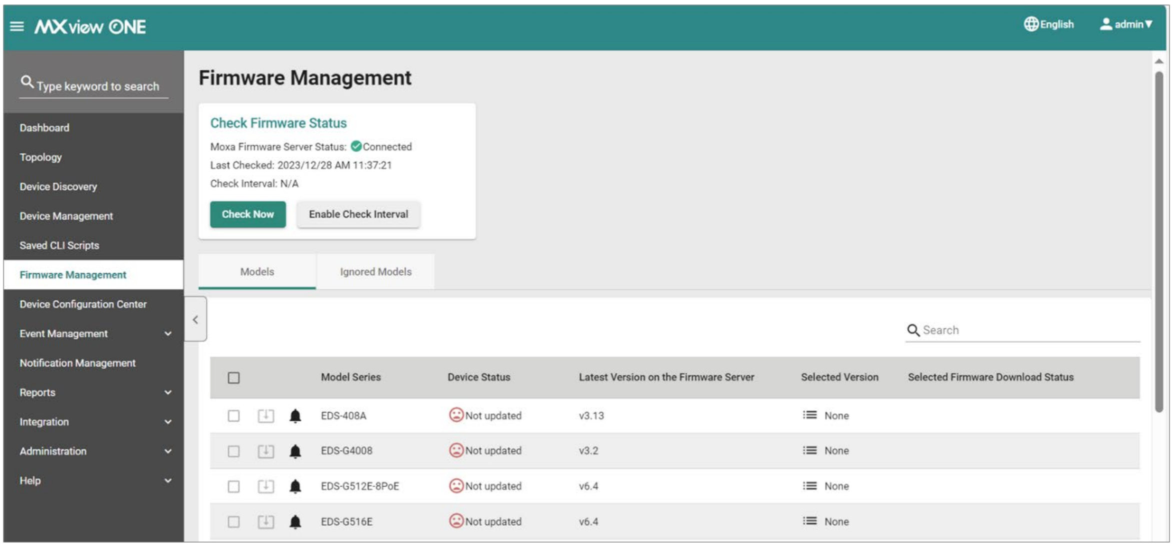
13. Firmware Management

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 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

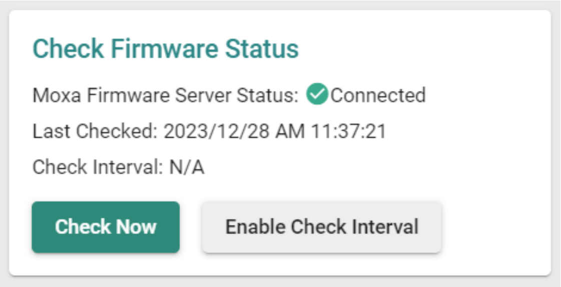
Check Interval: N/A

□		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	

NOTE

Before using the Firmware Management function, make sure that the URL: https://api.moxa-srs.thingsprocloud.com and port 443 are allowed through the firewall.

Check Firmware Status



Check Firmware Status

Moxa Firmware Server Status: ✓Connected

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

Check Interval: N/A

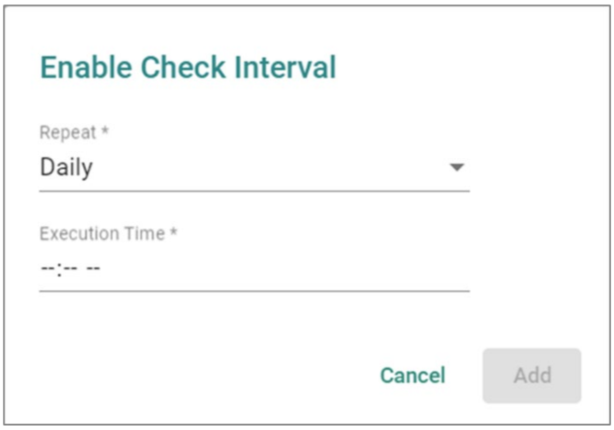
The **Check Firmware Status** section includes the following the information:

- **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

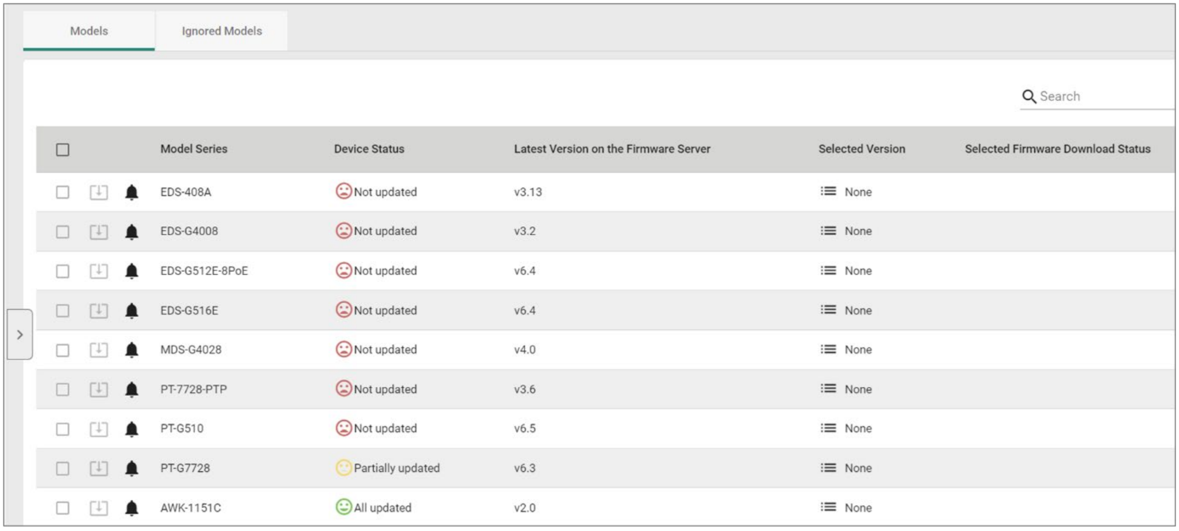
Execution Time *
--:-- --

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:

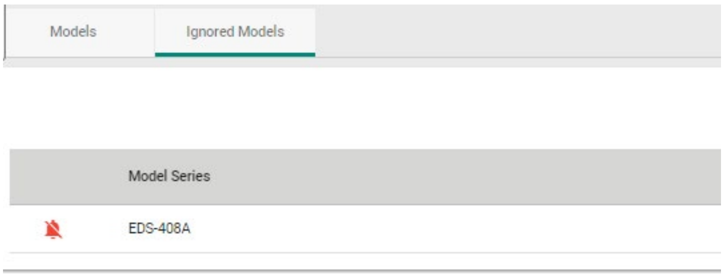
Itom	Description
Model Series	The model name. All identical models will be represented by a single entry. For example, if there are multiple EDS-408A devices, only one EDS-408A entry will appear in the table.
Device Status	The current firmware version status of the model series. The following statuses 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.

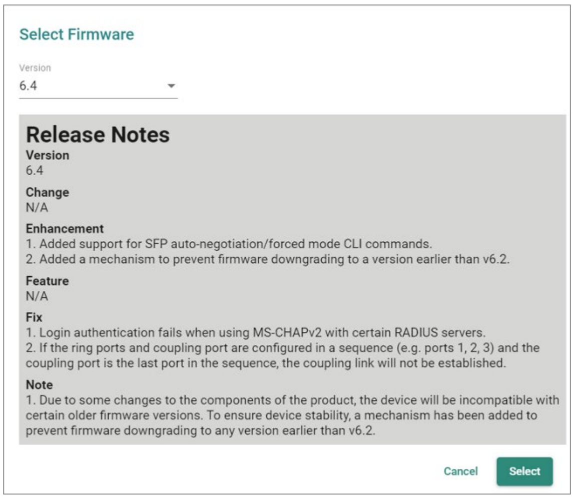


	Model Series
🔕	EDS-408A

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

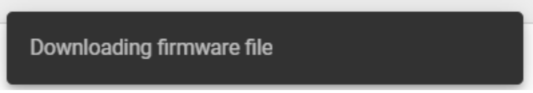
Enhancement
1. Added support for SFP auto-negotiation/forced mode CLI commands.
2. Added a mechanism to prevent firmware downgrading to a version earlier than v6.2.

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.

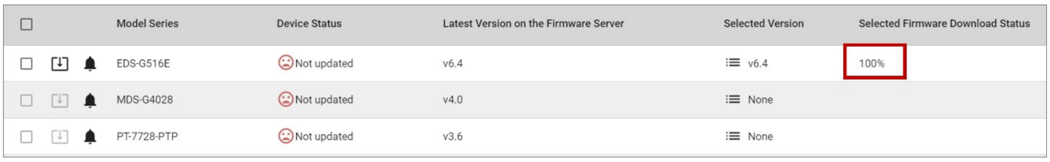
Note
1. Due to some changes to the components of the product, the device will be incompatible with certain older firmware versions. To ensure device stability, a mechanism has been added to prevent firmware downgrading to any version earlier than v6.2.

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.

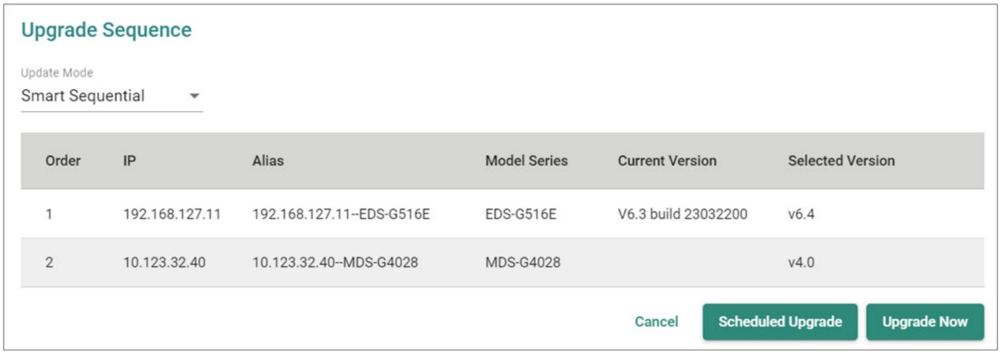


□			Model Series	Device Status	Latest Version on the Firmware Server	Selected Version	Selected Firmware Download Status
□	⤓	🔔	EDS-G516E	☹ Not updated	v6.4	☰ v6.4	100%
□	⤓	🔔	MDS-G4028	☹ Not updated	v4.0	☰ None	
□	⤓	🔔	PT-7728-PTP	☹ Not updated	v3.6	☰ None	

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

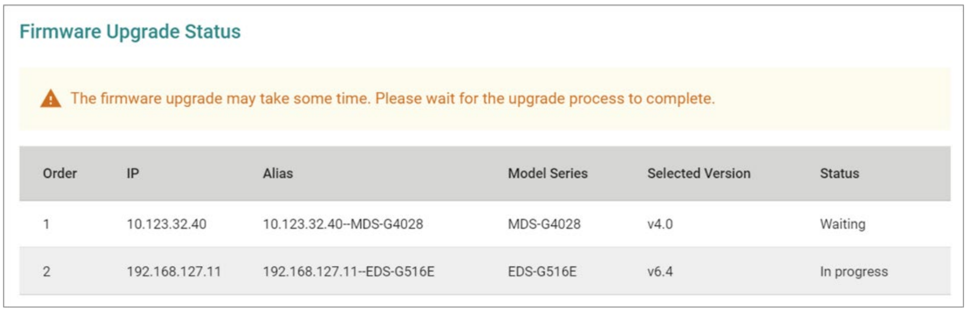
   a. Select the reboot sequence:
      - **Strict Sequential**: Upgrade the devices based on the device sequence in the topology starting from the device furthest away from the computer running MXview One, proceeding to the nearest one.
      - **Smart Sequential:** Upgrade the devices based on the device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



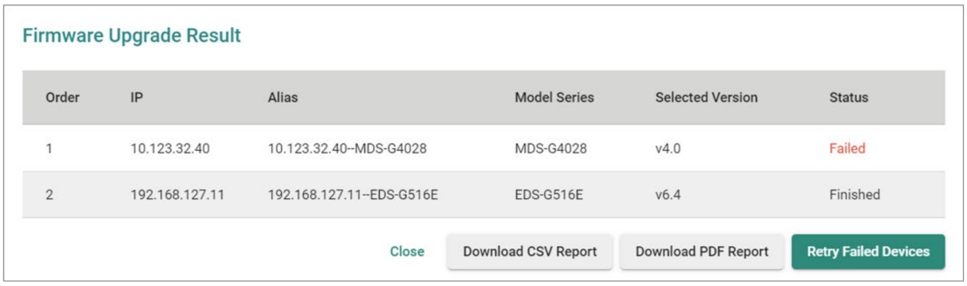
Firmware Upgrade Status

⚠ 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.

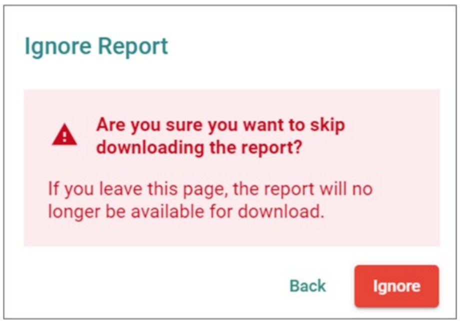
8. If the firmware upgrade was unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.



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?

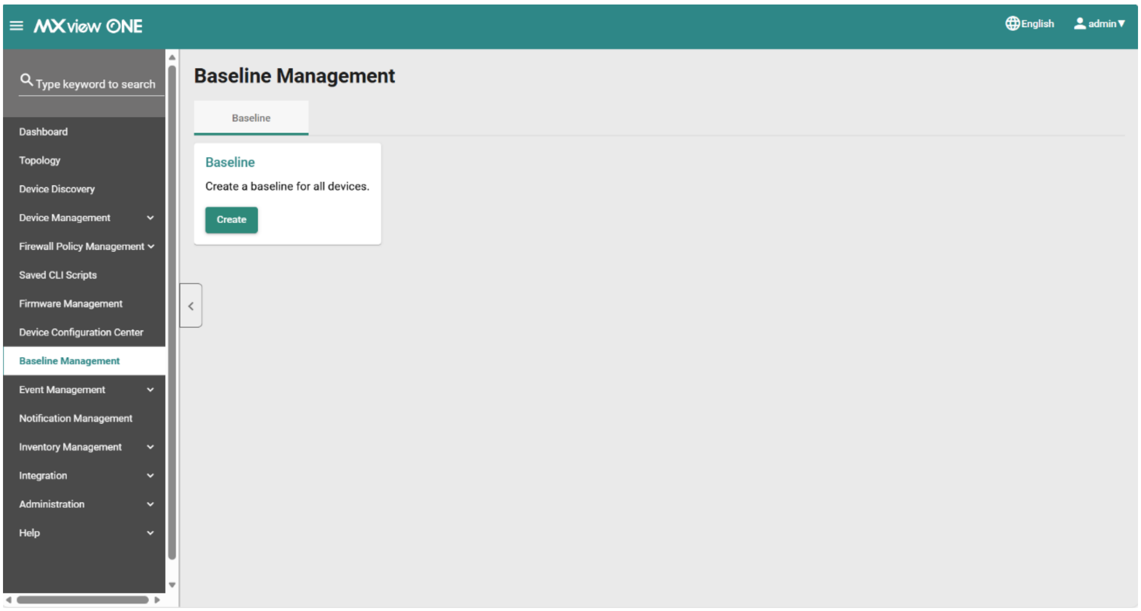
If you leave this page, the report will no longer be available for download.

14. Baseline Management

The **Baseline Management** feature helps users detect whether a device's configuration and firmware settings have been modified.

Baseline Overview

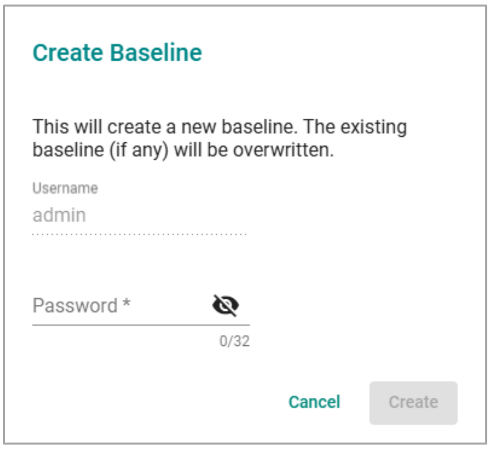
To access the **Baseline** page, in the function tree, navigate to **Menu (☰) > Baseline Management** and go to the **Baseline** tab. From this screen, users can create a device configuration and firmware baseline and perform a baseline audit to easily identify changes to device settings.



Creating a Configuration and Firmware Baseline

1. Navigate to **Menu** (☰) **> Baseline Management**.
2. Go to the **Baseline** tab.

3. In the Baseline section, click **Create**.
   The **Create Baseline** window will appear.



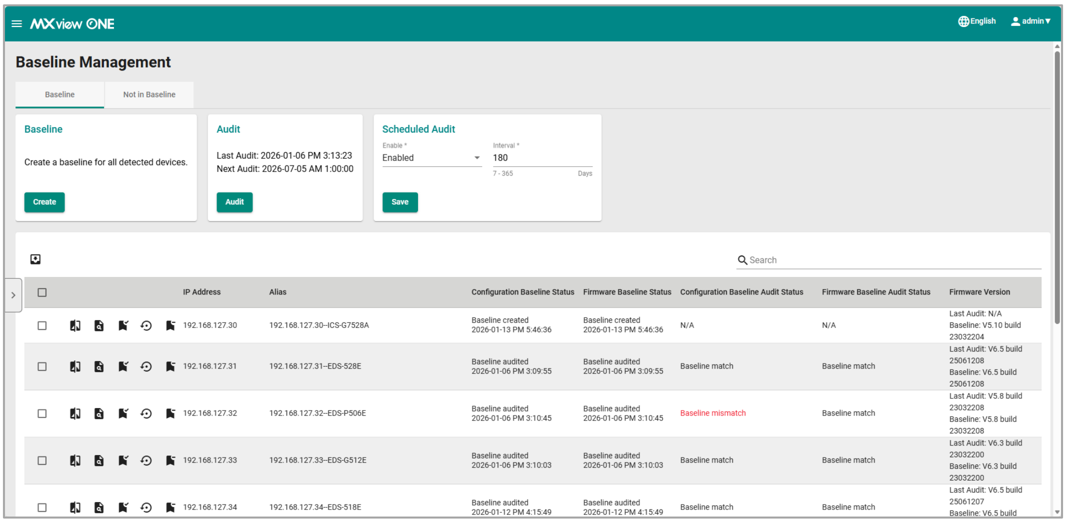
Create Baseline

This will create a new baseline. The existing baseline (if any) will be overwritten.

Username: admin

Password *: 0/32

4. Enter the password of the currently logged in user.
5. Click **Create**.
   MXview One will create a configuration and firmware baseline for all detected devices.



Baseline Management

Baseline

Create a baseline for all detected devices.

Audit

Last Audit: 2026-01-06 PM 3:13:23
Next Audit: 2026-07-05 AM 1:00:00

Scheduled Audit

Enable *: Enabled
Interval *: 180 Days (7 - 365)

IP Address	Alias	Configuration Baseline Status	Firmware Baseline Status	Configuration Baseline Audit Status	Firmware Baseline Audit Status	Firmware Version
192.168.127.30	192.168.127.30–ICS-G7528A	Baseline created 2026-01-13 PM 5:46:36	Baseline created 2026-01-13 PM 5:46:36	N/A	N/A	Last Audit: N/A Baseline: V5.10 build 23032204
192.168.127.31	192.168.127.31–EDS-528E	Baseline audited 2026-01-06 PM 3:09:55	Baseline audited 2026-01-06 PM 3:09:55	Baseline match	Baseline match	Last Audit: V6.5 build 25061208 Baseline: V6.5 build 25061208
192.168.127.32	192.168.127.32–EDS-P506E	Baseline audited 2026-01-06 PM 3:10:45	Baseline audited 2026-01-06 PM 3:10:45	Baseline mismatch	Baseline match	Last Audit: V5.8 build 23032208 Baseline: V5.8 build 23032208
192.168.127.33	192.168.127.33–EDS-G512E	Baseline audited 2026-01-06 PM 3:10:03	Baseline audited 2026-01-06 PM 3:10:03	Baseline match	Baseline match	Last Audit: V6.3 build 23032200 Baseline: V6.3 build 23032200
192.168.127.34	192.168.127.34–EDS-518E	Baseline audited 2026-01-12 PM 4:15:49	Baseline audited 2026-01-12 PM 4:15:49	Baseline match	Baseline match	Last Audit: V6.5 build 25061207 Baseline: V6.5 build

The page displays the following information in a table format:

Column	Description
IP Address	The IP address of the device.
Alias	The unique name of the device.
Configuration Baseline Status	Configuration baseline creation and audit record of the device.
Firmware Baseline Status	Firmware baseline creation and audit record of the device.
Configuration Baseline Audit Status	The configuration baseline audit result of the device.
Firmware Baseline Audit Status	The firmware baseline audit result of the device.
Firmware Version	The last audit date and baseline firmware version of the device.

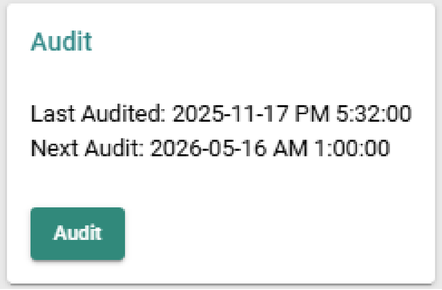
Executing a Manual Baseline Audit

NOTE

This function is only available after creating a configuration and firmware baseline. Refer to Creating a Configuration and Firmware Baseline.

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

2. Go to the **Baseline** tab.
3. In the Audit section, click **Audit**.
4. When prompted to confirm, click **Audit**.
5. MXview One will compare the current configuration and firmware version to the baseline and will show the audit result for each device in the table.



Audit

Last Audited: 2025-11-17 PM 5:32:00
Next Audit: 2026-05-16 AM 1:00:00

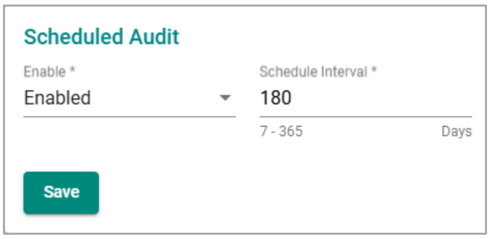
If scheduled auditing is enabled, the next scheduled audit date will be shown. Refer to Configuring Scheduled Baseline Audits.

Configuring Scheduled Baseline Audits

NOTE

This function is only available after creating a configuration and firmware baseline. Refer to Creating a Configuration and Firmware Baseline.

1. Navigate to **Menu** (☰) **> Baseline Management**.
2. Go to the **Baseline** tab.
3. In the **Scheduled Audit** section, configure the following settings:



Scheduled Audit

Enable *: Enabled
Schedule Interval *: 180 Days (7 - 365)

   - **Enable**: Enable or disable scheduled auditing.
   - **Schedule Interval**: Specify the interval (in days) when MXview One will perform a baseline audit. The audit is always performed at 1 AM, based on the configured MXview One system time.
4. Click **Save**.

Exporting the Baseline

NOTE

This function is only available after creating a configuration and firmware baseline. Refer to Creating a Configuration and Firmware Baseline.

1. Navigate to **Menu** (☰) **> Baseline Management**.
2. Go to the **Baseline** tab.
3. Click the **Export** (⊞) icon in the top-left corner.

4. Click **Export CSV**.
   MXview One exports all baseline data as a CSV file.

Searching the Baseline Data

> **NOTE**
>
> This function is only available after creating a configuration and firmware baseline. Refer to Creating a Configuration and Firmware Baseline.

1. Navigate to **Menu** (☰) **> Baseline Management**.
2. Go to the **Baseline** tab.
3. In the **Search** (🔍) field, type the full or partial information.
   All items matching the entered string will be shown in the table.

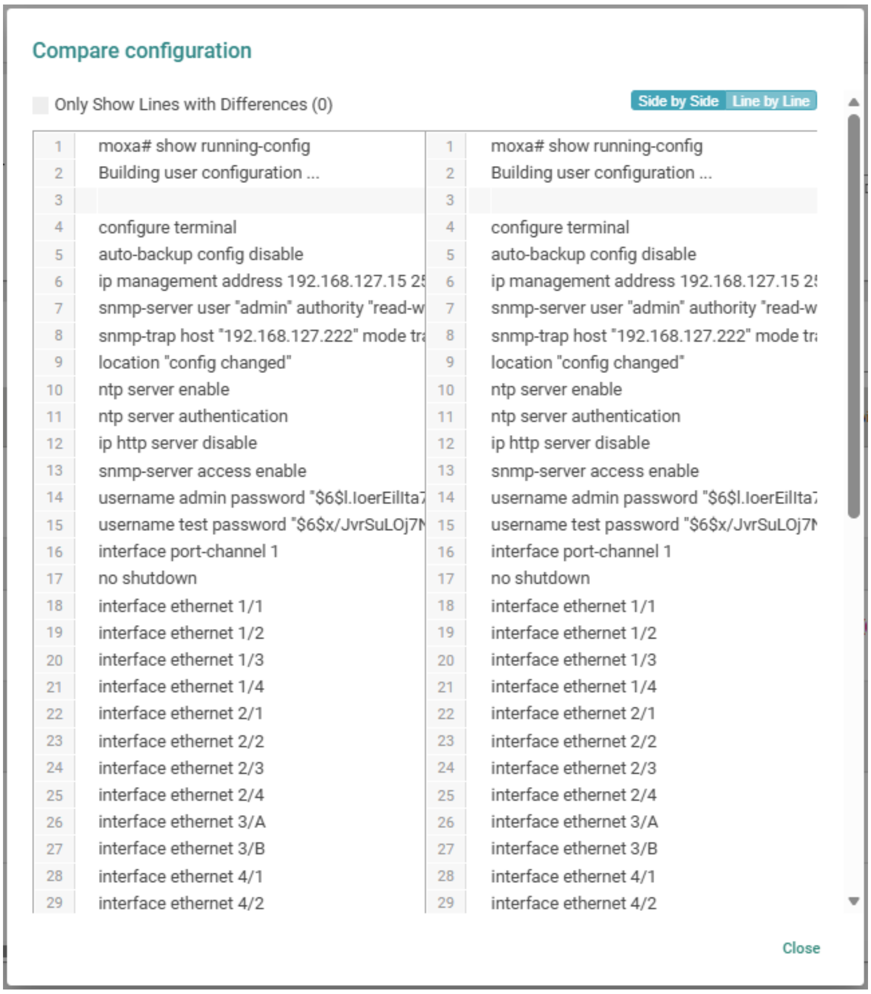
Comparing Configuration Files

Use the **Compare Configuration** feature to compare changes between the current device configuration and baseline configuration.

> **NOTE**
>
> This function is only available after creating a configuration and firmware baseline. Refer to Creating a Configuration and Firmware Baseline.

1. Navigate to **Menu** (☰) **> Baseline Management**.
2. Go to the **Baseline** tab.
3. Click the **Compare configuration** (⇆) icon next to the device you want to compare configurations for.
   The **Compare configuration** screen will appear and show a comparison between the current device

and baseline configuration.



```
 1  moxa# show running-config                      1  moxa# show running-config
 2  Building user configuration ...                2  Building user configuration ...
 3                                                 3
 4  configure terminal                             4  configure terminal
 5  auto-backup config disable                     5  auto-backup config disable
 6  ip management address 192.168.127.15 25        6  ip management address 192.168.127.15 2
 7  snmp-server user "admin" authority "read-w     7  snmp-server user "admin" authority "read-w
 8  snmp-trap host "192.168.127.222" mode tr       8  snmp-trap host "192.168.127.222" mode tr
 9  location "config changed"                      9  location "config changed"
10  ntp server enable                             10  ntp server enable
11  ntp server authentication                     11  ntp server authentication
12  ip http server disable                        12  ip http server disable
13  snmp-server access enable                     13  snmp-server access enable
14  username admin password "$6$l.IoerEillta7     14  username admin password "$6$l.IoerEillta7
15  username test password "$6$x/JvrSuLOj7N       15  username test password "$6$x/JvrSuLOj7N
16  interface port-channel 1                      16  interface port-channel 1
17  no shutdown                                   17  no shutdown
18  interface ethernet 1/1                        18  interface ethernet 1/1
19  interface ethernet 1/2                        19  interface ethernet 1/2
20  interface ethernet 1/3                        20  interface ethernet 1/3
21  interface ethernet 1/4                        21  interface ethernet 1/4
22  interface ethernet 2/1                        22  interface ethernet 2/1
23  interface ethernet 2/2                        23  interface ethernet 2/2
24  interface ethernet 2/3                        24  interface ethernet 2/3
25  interface ethernet 2/4                        25  interface ethernet 2/4
26  interface ethernet 3/A                        26  interface ethernet 3/A
27  interface ethernet 3/B                        27  interface ethernet 3/B
28  interface ethernet 4/1                        28  interface ethernet 4/1
29  interface ethernet 4/2                        29  interface ethernet 4/2
```

4. Click the **Side by Side** or **Line by Line** buttons to change the view mode.
5. (Optional) Check the **Only Show Lines with Differences** checkbox to only show configuration lines with differences.

Executing a Manual Baseline Audit on Selected Devices

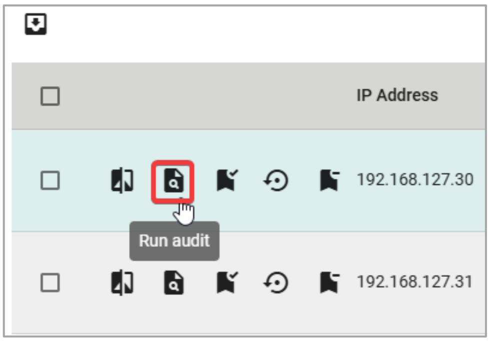
Use the **Audit now** feature to immediately perform a baseline audit on the selected device(s).

NOTE

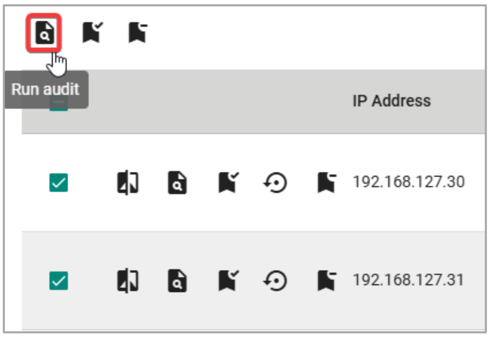
This function is only available after creating a configuration and firmware baseline. Refer to Creating a Configuration and Firmware Baseline.

1. Navigate to **Menu** (☰) **> Baseline Management**.
2. Go to the **Baseline** tab.
3. To perform a manual baseline audit on a single device:

a. Click the **Run audit** ( ) icon of the device you want to perform the audit for.



4. To perform a manual baseline audit on multiple devices:
   a. Check the checkbox of the devices you want to perform the audit for.
   b. Click the **Run audit** ( ) icon in the top-left corner of the table.



5. MXview will compare the current device configuration with the baseline configuration. The result (match or mismatch) will show in the table.

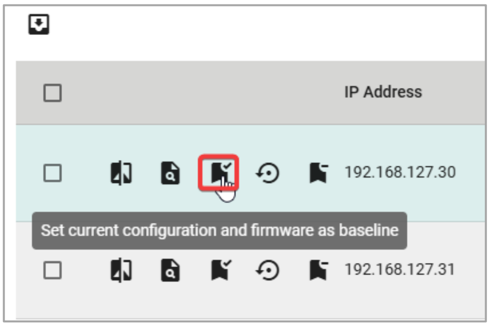
Setting the Current Configuration and Firmware as the New Baseline

This function allows users to set the current configuration and firmware of one or more devices as the new baseline for those devices. This action will overwrite any existing baseline for the selected device(s).

NOTE

This function is only available after creating a configuration and firmware baseline. Refer to Creating a Configuration and Firmware Baseline.

1. Navigate to **Menu** ( ) **> Baseline Management**.
2. Go to the **Baseline** tab.
3. To set the current configuration and firmware as the baseline for a single device:
   a. Click the **Set current configuration and firmware as baseline** ( ) icon of the device you want to update the baseline for.



The **Set New Baseline** window will appear.

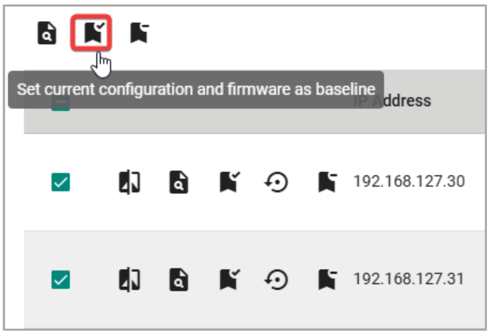
b. When prompted, enter the account credentials of the currently logged in users.

c. Click **Set**.

4. To set the current configuration and firmware as the baseline for multiple devices:

a. Check the checkbox of the devices you want to update the baseline for.

b. Click the **Set current configuration and firmware as baseline** ( ) icon in the top-left corner of the table.



The **Set New Baseline** window will appear.

c. When prompted, enter the account credentials of the currently logged in user.

d. Click **Set**.

5. MXview One will update the baseline with the current device configuration and firmware version.

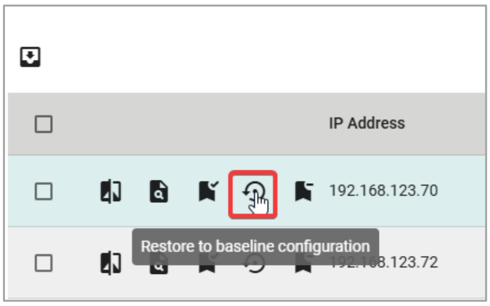
Restoring Devices to the Baseline Settings

This function allows users to restore the device configuration and firmware to the baseline configuration and firmware version.

NOTE

This function is only available after creating a configuration and firmware baseline. Refer to Creating a Configuration and Firmware Baseline.

1. Navigate to **Menu** ( ) **> Baseline Management**.
2. Go to the **Baseline** tab.
3. Click the **Restore to baseline configuration** ( ) icon of the device you want to restore to the baseline configuration and firmware.



The **Restore to Baseline Configuration** window will appear.

4. When prompted, enter the account credentials of the currently logged in user.
5. Click **Restore**.
6. MXview One will restore the current device configuration and firmware to the baseline version.

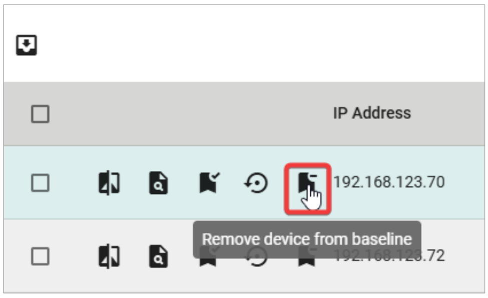
Removing Device(s) from the Baseline

NOTE

This function is only available after creating a configuration and firmware baseline. Refer to Creating a Configuration and Firmware Baseline.

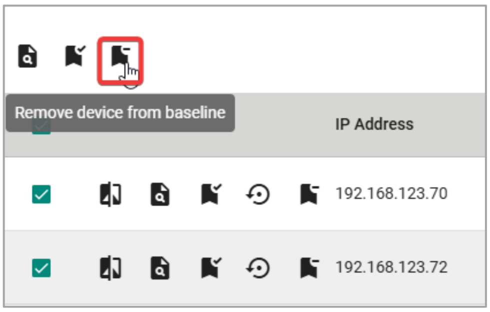
1. Navigate to **Menu** (☰) **> Baseline Management**.
2. Go to the **Baseline** tab.
3. To remove a single device from the baseline:

   a. Click the **Remove device from baseline** (⚑) icon of the device you want to remove.



4. To remove multiple devices from the baseline:
   a. Check the checkbox of the devices you want to remove.

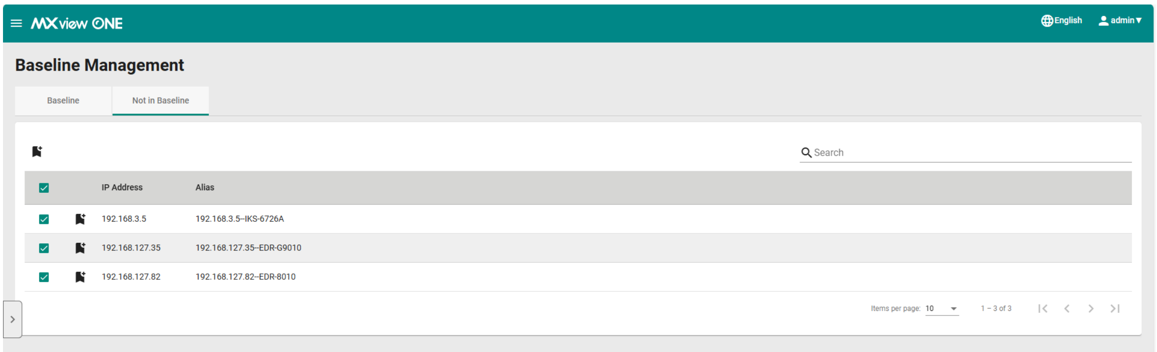
   b. Click the **Remove device from baseline** (⚑) icon in the top-left corner of the table.



5. MXview will move the device(s) to the **Not in Baseline** tab. Audits and baseline actions will no longer apply to these devices. Refer to **Not in Baseline Overview**.

Not in Baseline Overview

To access the **Not in Baseline** page, in the function tree, navigate to **Menu (☰) > Baseline Management** and go to the **Not in Baseline** tab. This screen shows any devices that are not included in the baseline. Baseline auditing actions do not apply to these devices.



☑		IP Address	Alias
☑	🔖	192.168.3.5	192.168.3.5–IKS-6726A
☑	🔖	192.168.127.35	192.168.127.35–EDR-G9010
☑	🔖	192.168.127.82	192.168.127.82–EDR-8010

Searching the Not in Baseline Data

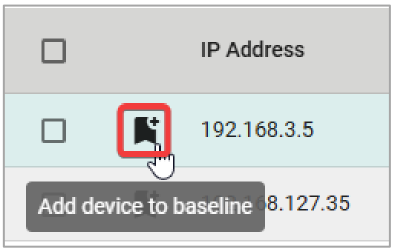
1. Navigate to **Menu** (☰) **> Baseline Management**.
2. Go to the **Not in Baseline** tab.
3. In the **Search** (🔍) field, type the full or partial information.

   All items matching the entered string will be shown in the table.

Adding Device(s) to the Baseline

1. Navigate to **Menu** (☰) **> Baseline Management**.
2. Go to the **Not in Baseline** tab.
3. To add a single device to the baseline:

   a. Click the **Add device to baseline** (🔖) icon of the device you want to add.

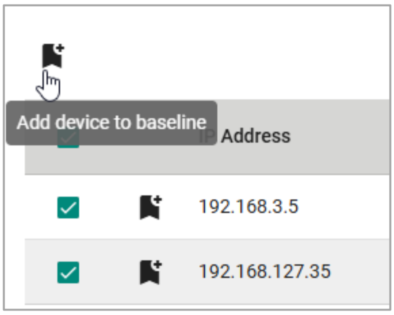


□		IP Address
□	🔖	192.168.3.5
		8.127.35

4. To add multiple devices to the baseline:

   a. Check the checkbox of the devices you want to add.

   b. Click the **Add device to baseline** (🔖) icon in the top-left corner of the table.



☑		IP Address
☑	🔖	192.168.3.5
☑	🔖	192.168.127.35

5. MXview will move the device(s) to the **Baseline** tab. Refer to **Baseline Overview**.

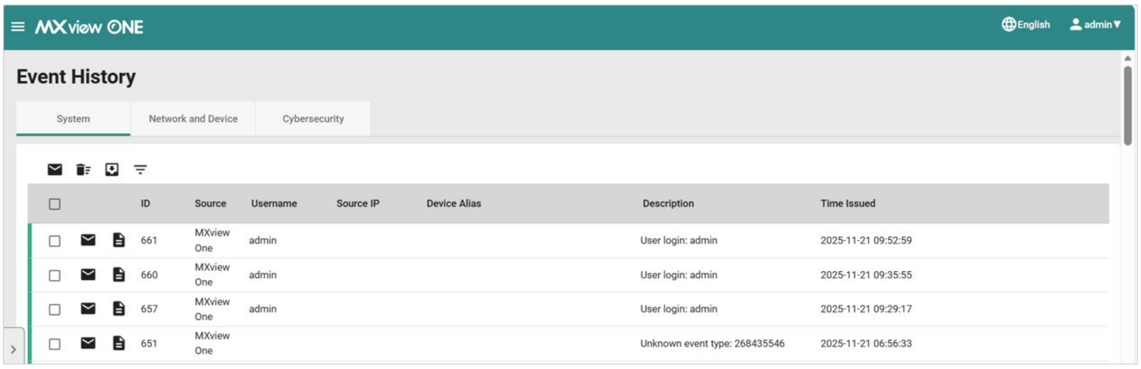
15. Events and Notifications

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

Event Monitoring

Viewing System Events

To access the **System** page, in the function tree, navigate to **Menu** (☰) **> Event Management > Event History** and go to the **System** tab. The **System** tab shows information about MXview One system events. Use the filters to customize the information displayed in the table. You can also export the data as a CSV file.



			ID	Source	Username	Source IP	Device Alias	Description	Time Issued
□	✉	🗎	661	MXview One	admin			User login: admin	2025-11-21 09:52:59
□	✉	🗎	660	MXview One	admin			User login: admin	2025-11-21 09:35:55
□	✉	🗎	657	MXview One	admin			User login: admin	2025-11-21 09:29:17
□	✉	🗎	651	MXview One				Unknown event type: 268435546	2025-11-21 06:56:33

1. Navigate to **Menu** (☰) **> Event Management > Event History**.
2. Go to the **System** tab.

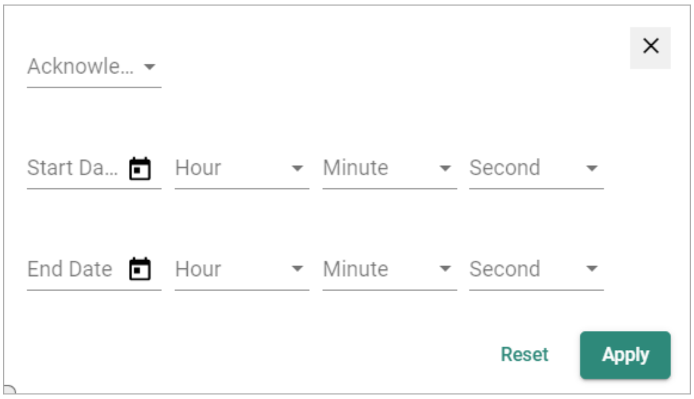
   The **System** tab will display the following information in a table format:

Column	Description
Acknowledge	Acknowledge status of the event
Show Details	The detailed information of this event
ID	The unique identifier of the event
Source	The source of the event
Username	The username of the account associated with the event
Source IP	The IP address of the device that issued the event
Device Alias	The unique name of the device
Description	The description of the event
Time Issued	The time the event was issued

3. 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
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**.

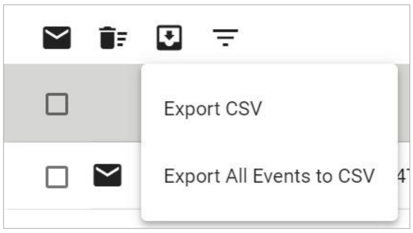
   MXview One filters the table to only display events that match the specified criteria.

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 **System** tab:

   a. Click the **Export** (⤓) icon.



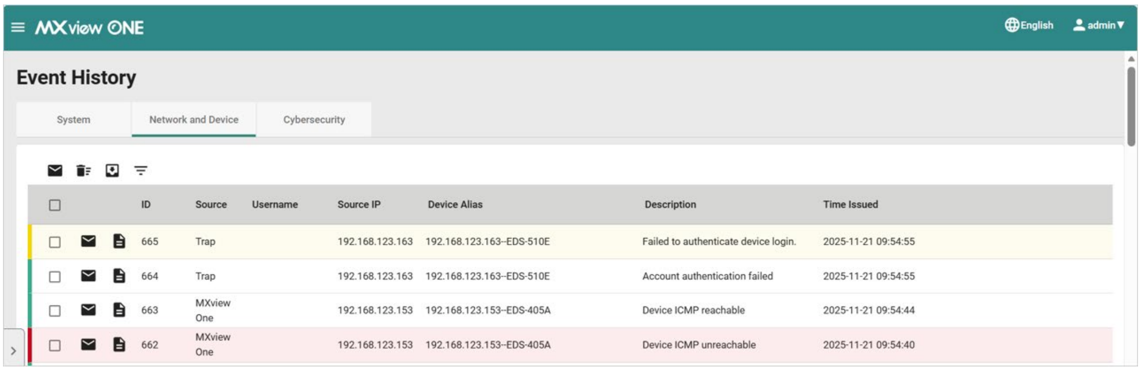
   b. Select **Export CSV** for just the events on the first page or **Export All Events to CSV** for all event pages.

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

Viewing Network and Device Events

To access the **Network and Device** page, in the function tree, navigate to **Menu (☰) > Event Management > Event History** and go to the **Network and Device** tab.

The **Network and Device** tab shows information about all the network and device events in your topology. Use the filters to customize the information displayed in the table. You can also export the data as a CSV file.



☐			ID	Source	Username	Source IP	Device Alias	Description	Time Issued
☐	✉	🗎	665	Trap		192.168.123.163	192.168.123.163--EDS-510E	Failed to authenticate device login.	2025-11-21 09:54:55
☐	✉	🗎	664	Trap		192.168.123.163	192.168.123.163--EDS-510E	Account authentication failed	2025-11-21 09:54:55
☐	✉	🗎	663	MXview One		192.168.123.153	192.168.123.153--EDS-405A	Device ICMP reachable	2025-11-21 09:54:44
☐	✉	🗎	662	MXview One		192.168.123.153	192.168.123.153--EDS-405A	Device ICMP unreachable	2025-11-21 09:54:40

The page will display the following information in a table format:

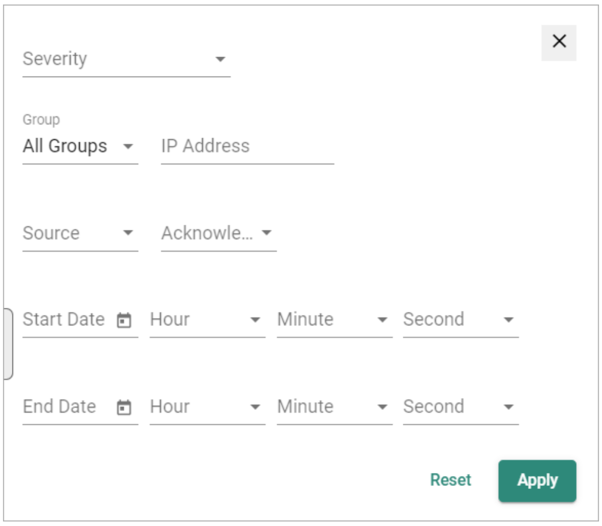
Column	Description
Acknowledge	The acknowledgement status of the event.
Show Details	Detailed information about the event.
ID	The unique identifier of the event
Source	The source of the event.
Username	The username of the account associated with the event
Source IP	The IP address of the device that issued the event.
Device Alias	The unique name of the device.
Description	The description of the event.
Time Issued	The date and time the event was issued.

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

2. Go to the **Network and Device** tab.
   The **Network and Device** screen will appear:

3. To filter the information in the table according to specific criteria:

   a. Click the **Filter** (☰) icon in the top-left corner.
   The filter window will appear.



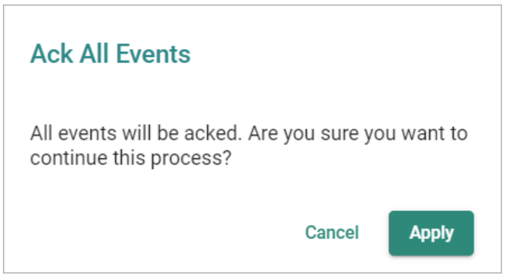
   b. Specify any of the following criteria:
   - ❒ Severity: Select the severity level of the event.
   - ❒ Group: Select the group the device is assigned to.
   - ❒ IP Address: Specify the IP address of the device.
   - ❒ Source: Select the source of the event.
   - ❒ Acknowledge: Select the acknowledgement status of the event.
   - ❒ Start Date: Specify the start date and time for which to display event data.
   - ❒ End Date: Specify the end date and time for which to display event data.

c. Click **Apply**.

4. To sort the data in a specific column, click the column header.
5. To acknowledge all events:

a. Click the **Ack All Events** (✉) icon in the top-left corner.

The **Ack All Events** screen will appear.



Ack All Events

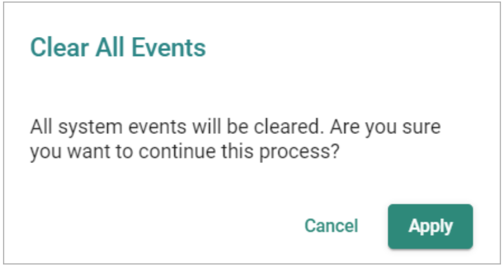
All events will be acked. Are you sure you want to continue this process?

b. When prompted to confirm, click **Apply**.
MXview One will acknowledge all events displayed in the table.

6. To delete all events:

a. Click the **Clear All Events** (🗑) icon in the top-left corner.

The **Clear All Events** screen will appear.



Clear All Events

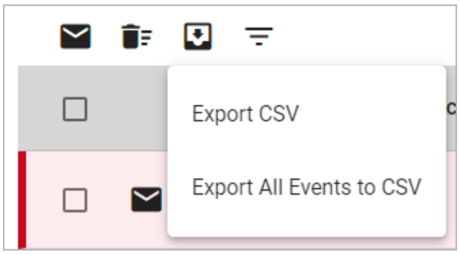
All system events will be cleared. Are you sure you want to continue this process?

b. When prompted to confirm, click **Apply**.

MXview One will delete all events displayed in the table

7. To export data displayed on the **Network and Device** tab:

a. Click the **Export** (⤓) icon.



b. Click **Export CSV** to only export the events on the first page or **Export All Events to CSV** to export all events.
MXview One exports the displayed event data as a CSV file.

Configuring Event Thresholds and Severity Levels

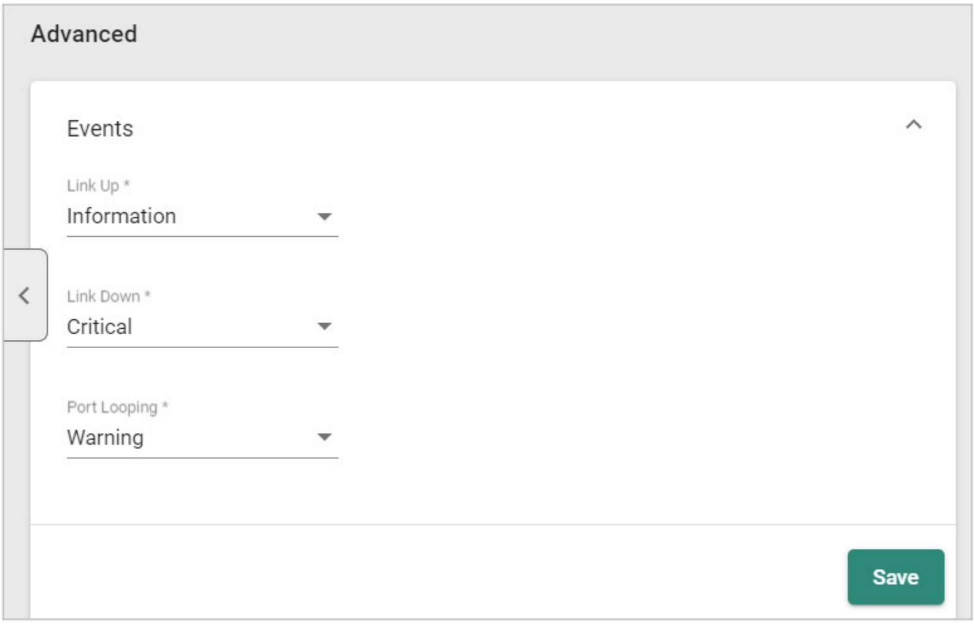
Use the **Preferences** and **Global Device Settings** screen to configure default event thresholds and severity levels.

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 *: Critical

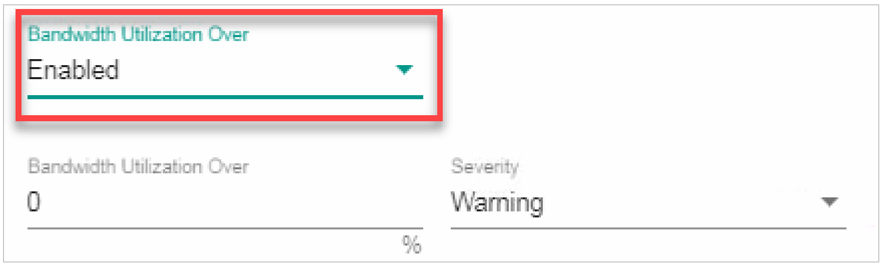
Port Looping *: Warning

3. Select one of the following severity levels for **Link Up** events:
   - **Information**
   - **Warning**
   - **Critical**
4. Select one of the following severity levels for **Link Down** events:
   - **Information**
   - **Warning**
   - **Critical**
5. Select one of the following severity levels for **Port Looping** events:
   - **Information**
   - **Warning**
   - **Critical**
6. Click **Save**.
   MXview One will update the event severity settings.
7. 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.

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

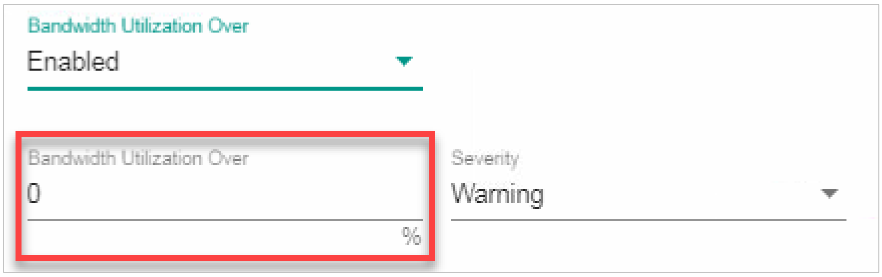


Bandwidth Utilization Over: Enabled

Bandwidth Utilization Over: 0 %

Severity: Warning

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



Bandwidth Utilization Over
Enabled

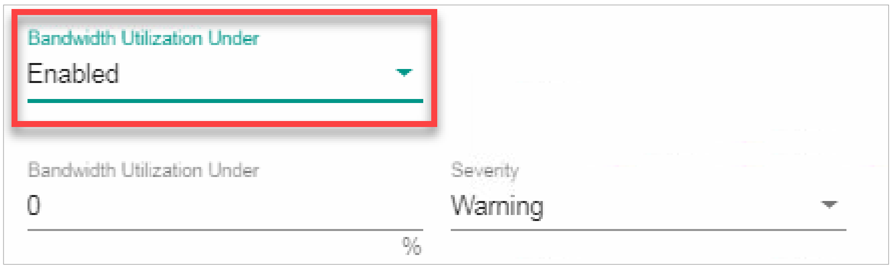
Bandwidth Utilization Over
0 %

Severity
Warning

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

9. To trigger events when network bandwidth utilization falls below a threshold:

a. Select **Enabled** from the first **Bandwidth Utilization Under** drop-down list.

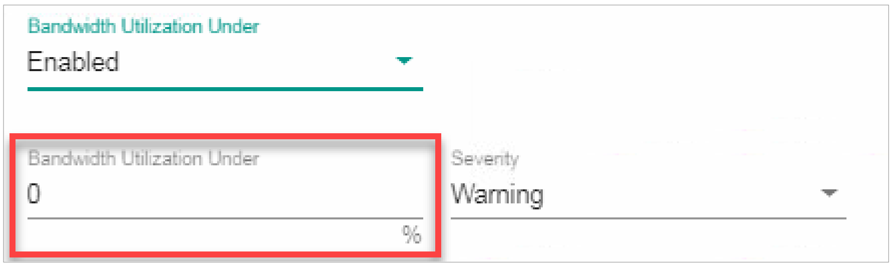


Bandwidth Utilization Under
Enabled

Bandwidth Utilization Under
0 %

Severity
Warning

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



Bandwidth Utilization Under
Enabled

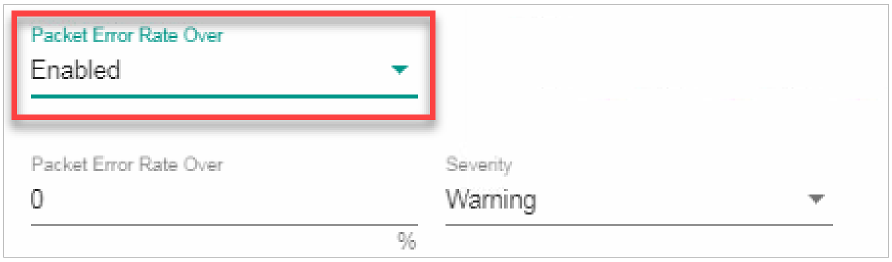
Bandwidth Utilization Under
0 %

Severity
Warning

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

10. To trigger events when the packet error rate exceeds a threshold:

a. Select **Enabled** from the first **Packet Error Rate Over** drop-down list.

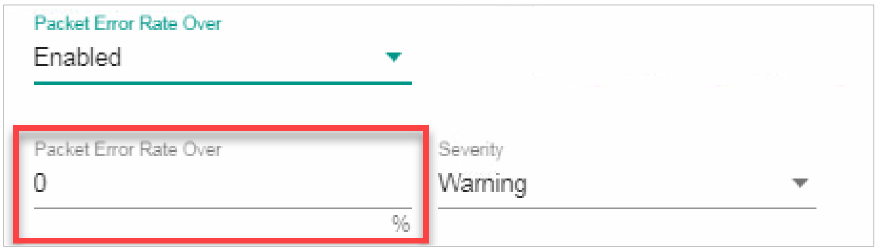


Packet Error Rate Over
Enabled

Packet Error Rate Over
0 %

Severity
Warning

b. Specify the packet error rate for the threshold.



Packet Error Rate Over
Enabled

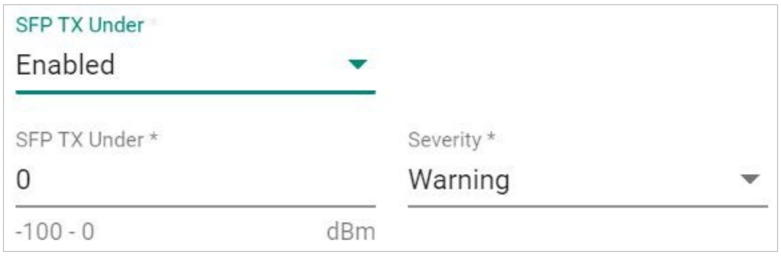
Packet Error Rate Over
0 %

Severity
Warning

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

11. 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.

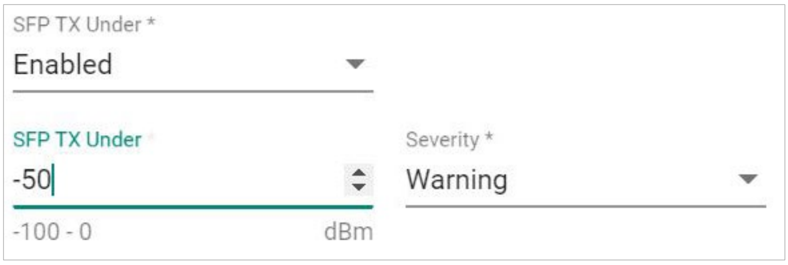


SFP TX Under
Enabled

SFP TX Under * 0 -100 - 0 dBm

Severity * Warning

b. Specify the SFP TX threshold level.

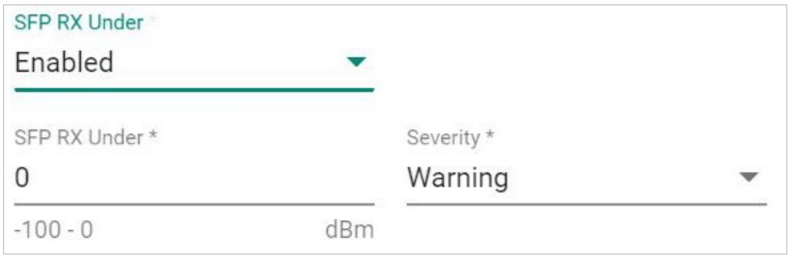


SFP TX Under * Enabled

SFP TX Under -50 -100 - 0 dBm

Severity * Warning

12. 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.

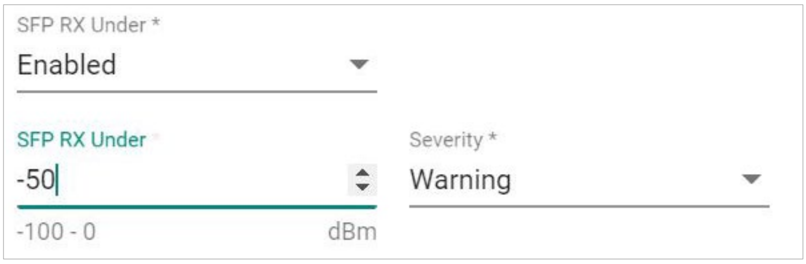


SFP RX Under
Enabled

SFP RX Under * 0 -100 - 0 dBm

Severity * Warning

    b. Specify the SFP RX threshold level.

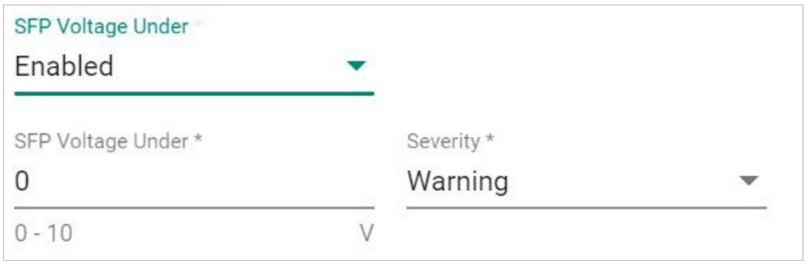


SFP RX Under * Enabled

SFP RX Under -50 -100 - 0 dBm

Severity * Warning

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

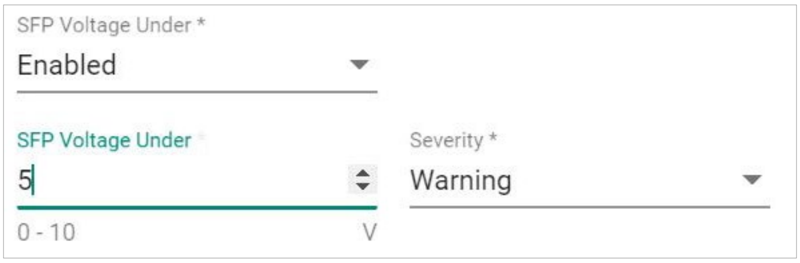


SFP Voltage Under
Enabled

SFP Voltage Under * 0 0 - 10 V

Severity * Warning

    b. Specify the SFP Voltage threshold level.

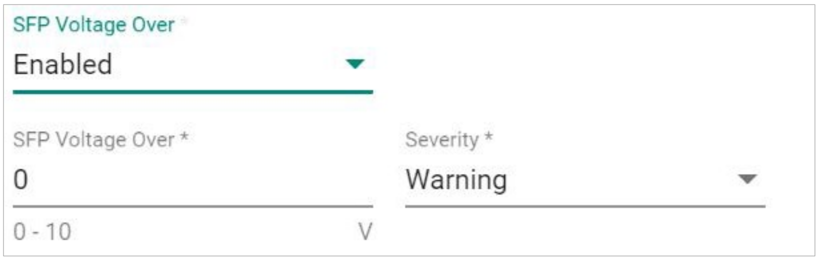


SFP Voltage Under *
Enabled

SFP Voltage Under
5
0 - 10 V

Severity *
Warning

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

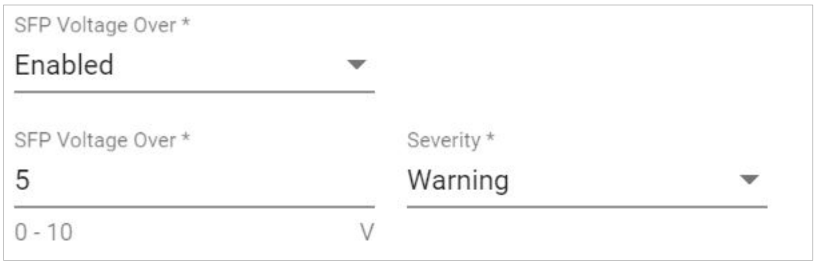


SFP Voltage Over
Enabled

SFP Voltage Over *
0
0 - 10 V

Severity *
Warning

    b. Specify the SFP Voltage threshold level.

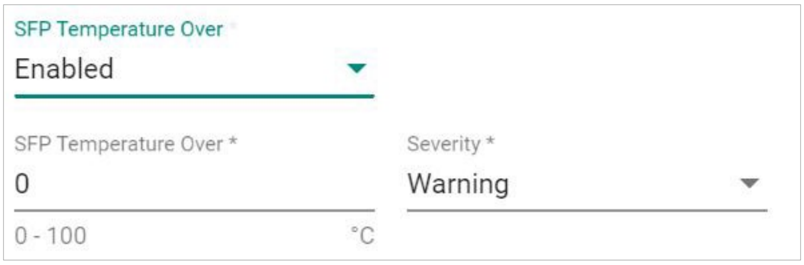


SFP Voltage Over *
Enabled

SFP Voltage Over *
5
0 - 10 V

Severity *
Warning

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

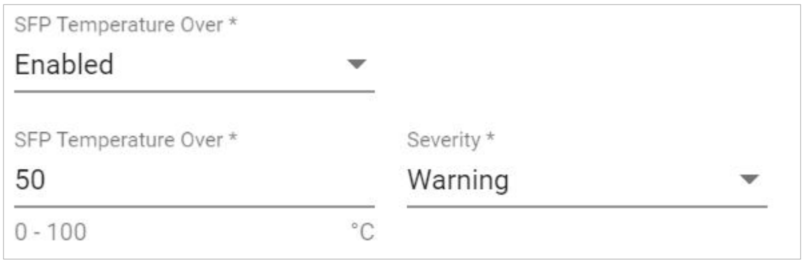


SFP Temperature Over
Enabled

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.

16. 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.

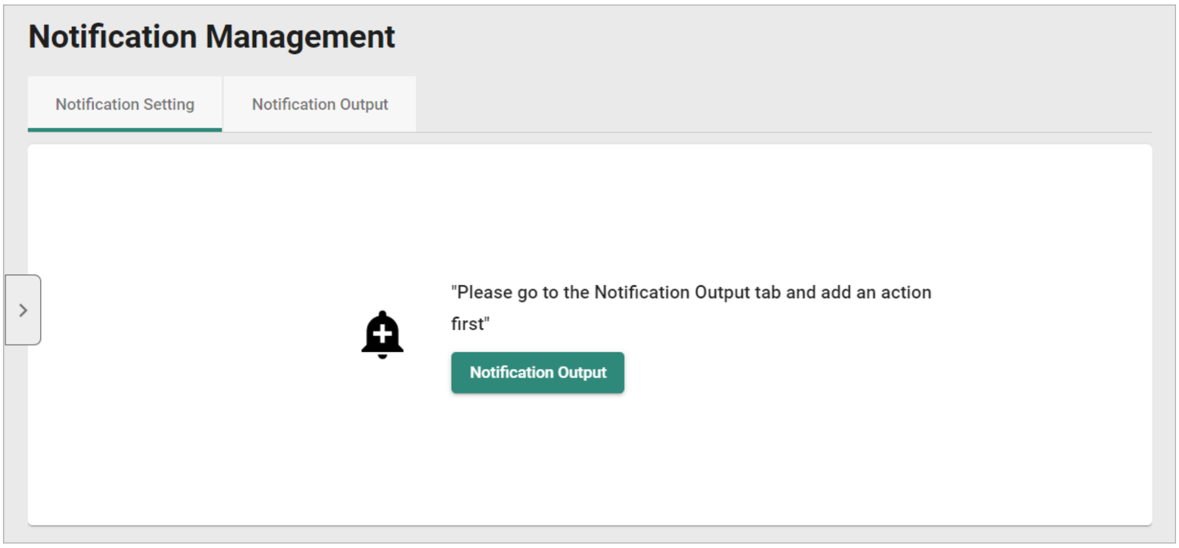
1. Navigate to **Menu** (☰) **> Administration > System Settings**.

   The **System Settings** screen will appear.
2. Find the **Email Server Configuration** section.
3. Configure the following:
   - **Server Domain Name/IP**
   - **Port number**
   - **Encryption**
   - **Allow Self-signed Certificate**
   - **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.



"Please go to the Notification Output 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.

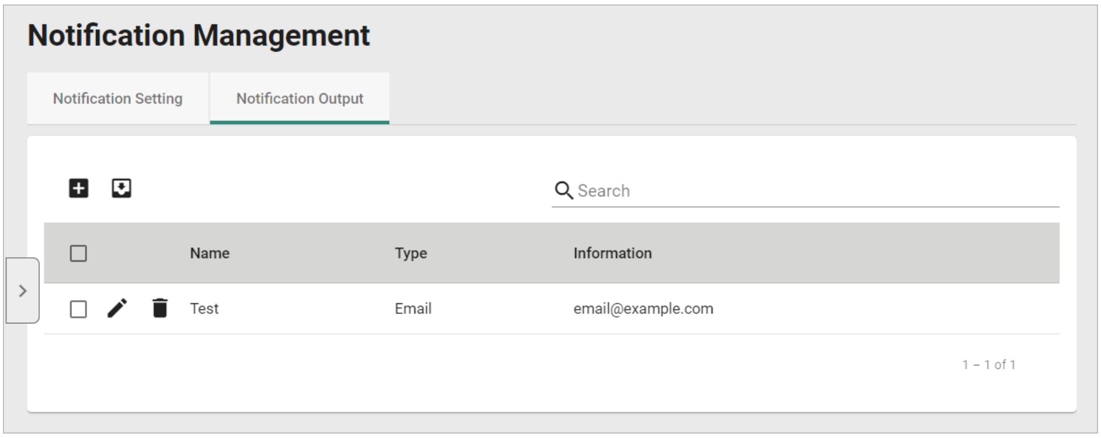
1. Navigate to **Menu** (☰) **> Notification Management**.

   The **Notification Management** screen appears.

2. To register an action:

   a. Click the **Notification Output** tab.

   The **Notification Output** tab displays a list of registered actions (if any).

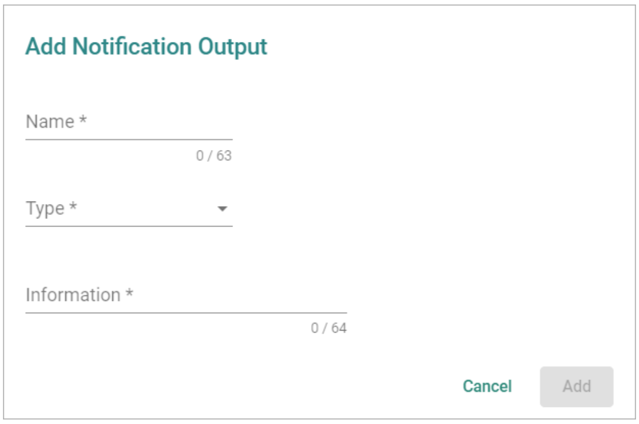


Notification Management

☐	Name	Type	Information
☐	Test	Email	email@example.com

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

   The **Add Notification Output** screen will appear.



Add Notification Output

Name *
0 / 63

Type *

Information *
0 / 64

   c. In the **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.
   - **Microsoft Teams:** Sends a message through Microsoft Teams.
   - **Message Box:** Displays a message box when the event occurs.

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

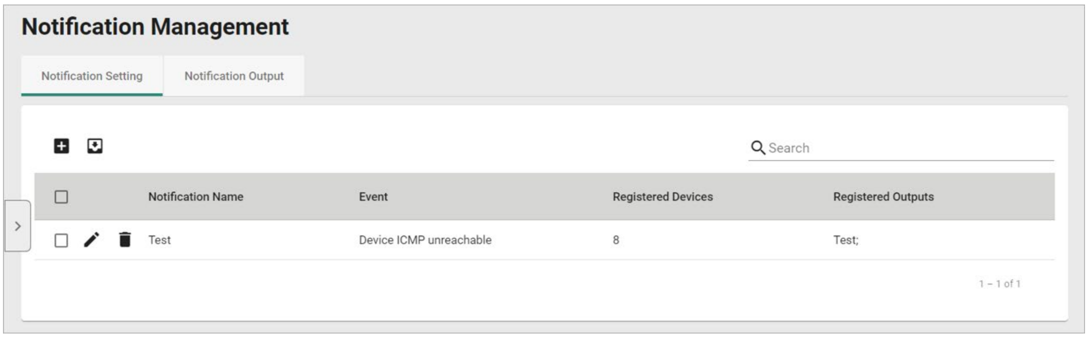
   f. Click **Add**.

   The registered action appears in the table on the **Notification Output** tab.

3. To add a new event notification:

   a. Click the **Notification Setting** tab.

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



Notification Management

Notification Setting | Notification Output

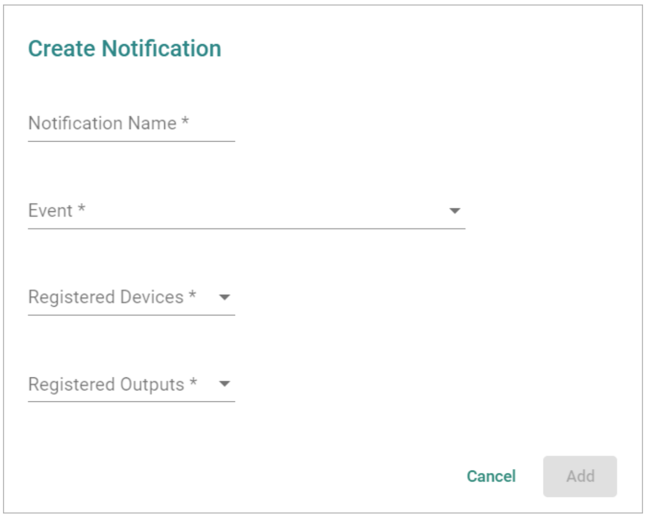
Search

□	Notification Name	Event	Registered Devices	Registered Outputs
□	Test	Device ICMP unreachable	8	Test;

1 – 1 of 1

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

The **Create Notification** screen appears.



Create Notification

Notification Name *

Event *

Registered Devices *

Registered Outputs *

Cancel Add

c. In the **Notification Name** field, type a name to describe the event notification.

d. From the **Event** 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 Outputs** 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**.

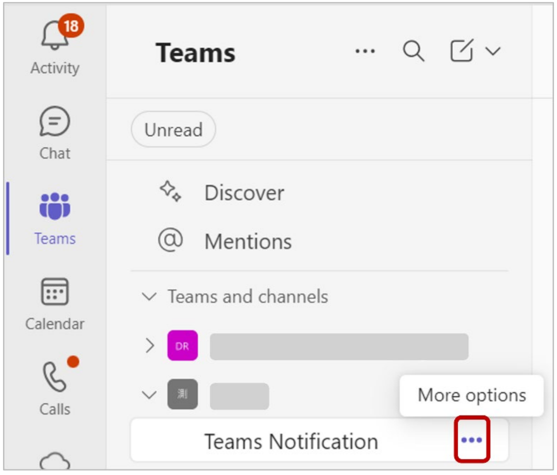
The event notification appears in the table on the **Notification Setting** tab.

Adding a Microsoft Teams Action

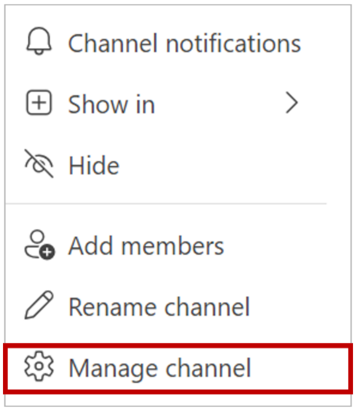
Use the **Notification Output** tab on the **Notification Management** screen to add a Microsoft Teams notification action.

1. In Microsoft Teams, go to the channel you want to add the incoming webhook to.

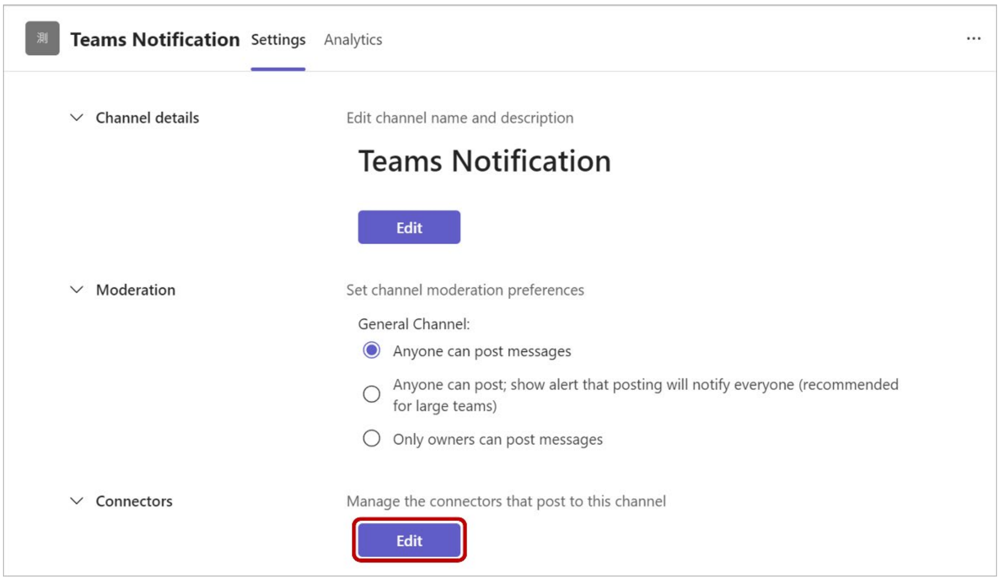
2. Click **More options (...)** next to the channel name.



3. Select **Manage channel**.



4. In the **Connectors** section on the **Settings** tab, click the **Edit** button.


Teams Notification Settings Analytics

Channel details

Edit channel name and description

Teams Notification

Edit

Moderation

Set channel moderation preferences

General Channel:

● Anyone can post messages

○ Anyone can post; show alert that posting will notify everyone (recommended for large teams)

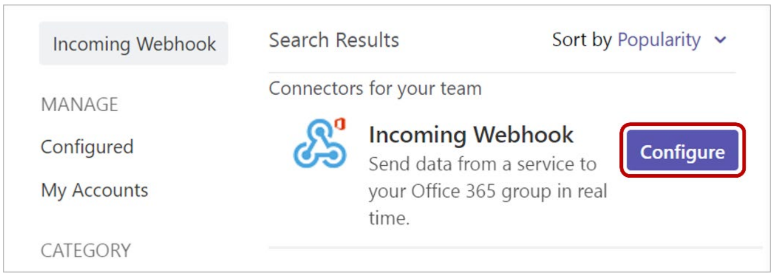
○ Only owners can post messages

Connectors

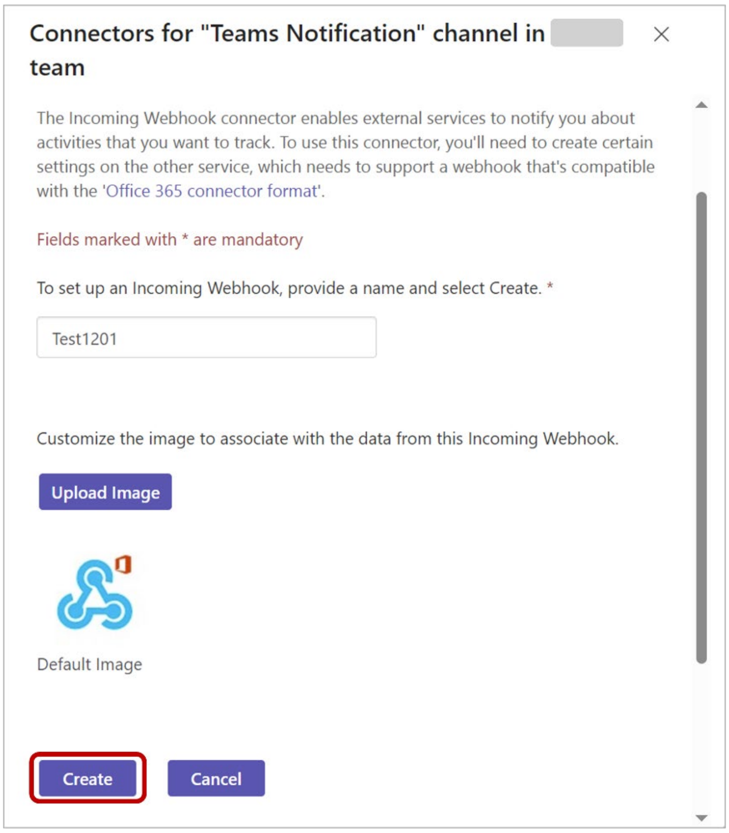
Manage the connectors that post to this channel

Edit

5. Search for **Incoming Webhook** and click the **Configure** button.
   The **Incoming Webhook** will appear.



6. Enter a name for the webhook and upload a custom icon (optional), then click **Create**.



Connectors for "Teams Notification" channel in [redacted] team

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

Fields marked with * are mandatory

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

Test1201

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

7. Copy the URL shown in the pop-up window to your clipboard and click **Done**.

8. In MXview One, navigate to **Menu (≡) > Notification Management**.

9. Click the **Notification Output** tab.

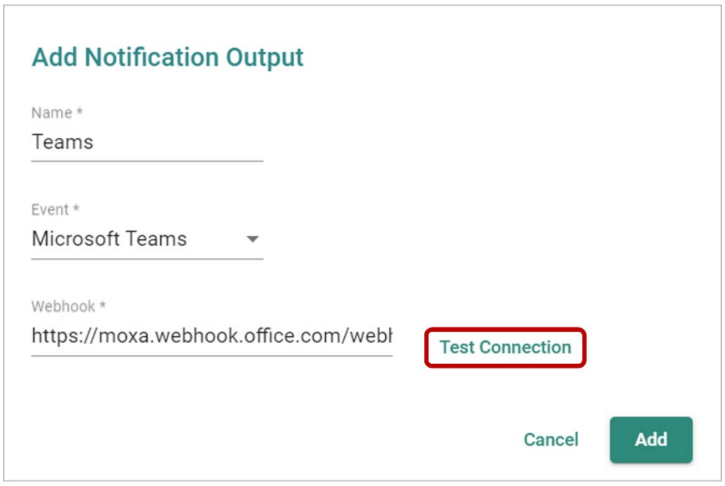
10. Click the **Add** (+) icon in the top-left corner.
    The **Add Notification Output** screen will appear.

11. In the **Name** field, enter a descriptive name for action.

12. From the **Type** drop-down menu, select **Microsoft Teams**.

13. In the **Webhook** field, paste the webhook URL copied from the Microsoft Teams.

14. Click **Test Connection** to verify the webhook works properly.



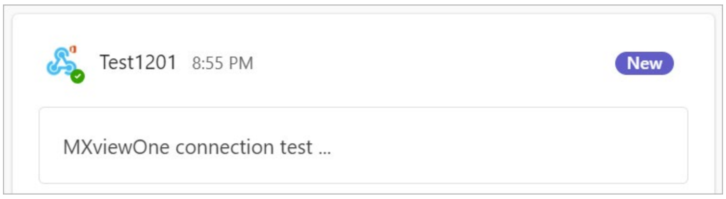
Add Notification Output

Name * Teams

Event * Microsoft Teams

Webhook * https://moxa.webhook.office.com/webl

If successful, you will receive a message in the linked Microsoft Teams channel.



Test1201 8:55 PM

MXviewOne connection test ...

15. Click **Add**.
    The registered action appears in the table on the **Notification Output** tab.

Editing or Exporting Registered Actions

Use the **Notification Output** 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.

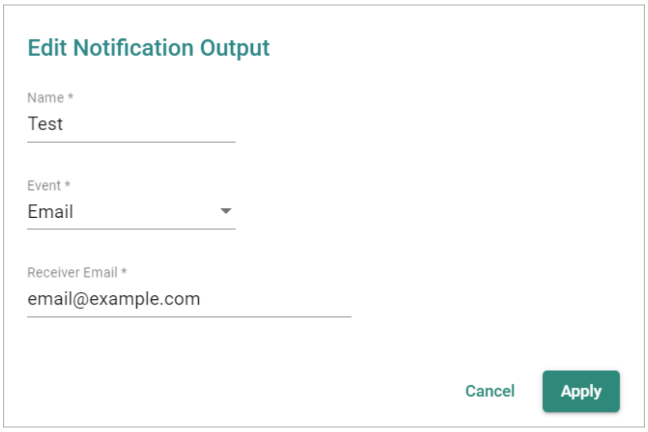
2. Click the **Notification Output** tab.

   The **Notification Output** 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 Output** screen will appear.



Edit Notification Output

Name * Test

Event * Email

Receiver Email * email@example.com

   b. Modify the following settings:

   - Name
   - Type

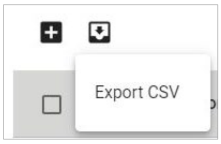
- ❐ Information

c. Click **Apply**.

The **Notification Output** screen appears and displays the updated action information.

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

a. Click the **Export** (⊡) icon.



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

Editing or Exporting Notification Configurations

Use the **Notification Setting** 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.

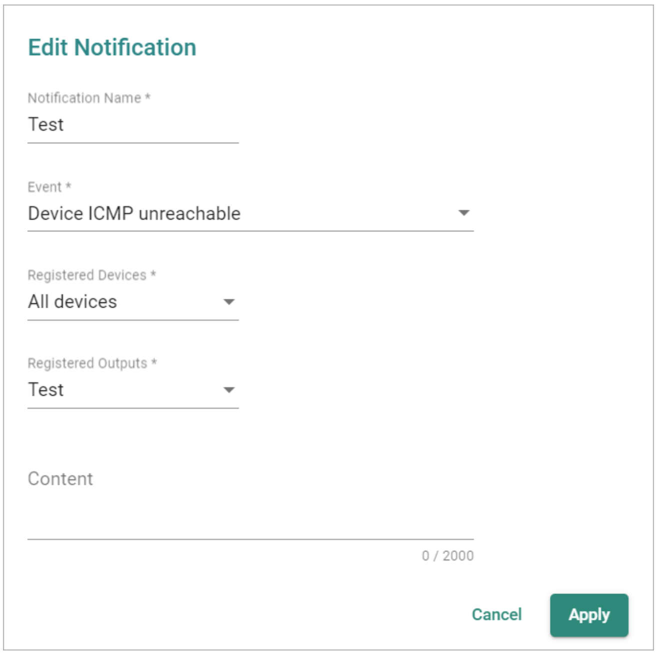
2. Click the **Notification Setting** tab.

The **Notification Setting** tab displays a list of configured notifications.

3. To edit a notification:

a. Click the **Edit** (✎) icon next to the notification you want to edit.

The **Edit Notification** screen will appear.



Edit Notification

Notification Name * Test

Event * Device ICMP unreachable

Registered Devices * All devices

Registered Outputs * Test

Content

0 / 2000

b. Modify the following settings:

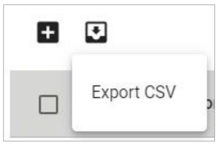
- ❐ Notification Name
- ❐ Event
- ❐ Registered Devices
- ❐ Registered Outputs

c. Click **Apply**.

The **Notification Setting** screen appears and displays the updated notification information.

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

   a. Click the **Export** (⇩) icon.



Export CSV

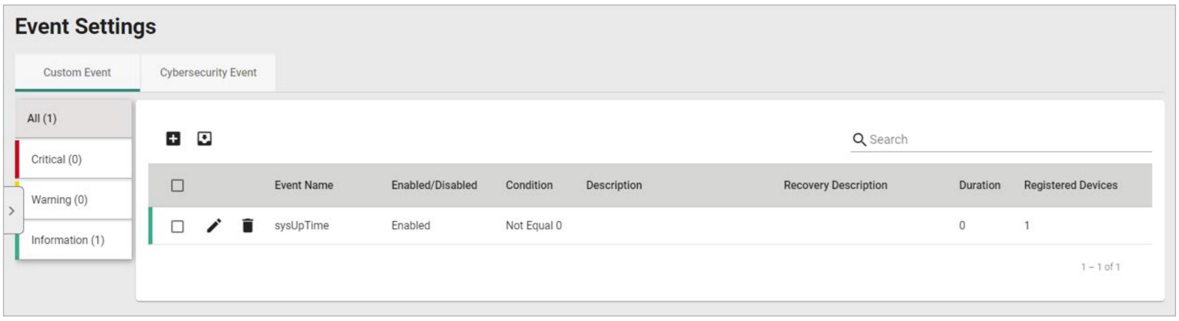
   b. Select **Export CSV**.

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

Custom Event Management

To access the **Custom Event** tab, in the function tree, navigate to **Menu (☰) > Event Management > Event Settings** and go to the **Custom Event** tab.

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



Event Settings

Custom Event | Cybersecurity Event

All (1)
Critical (0)
Warning (0)
Information (1)

Search

□		Event Name	Enabled/Disabled	Condition	Description	Recovery Description	Duration	Registered Devices
□		sysUpTime	Enabled	Not Equal 0			0	1

1 – 1 of 1

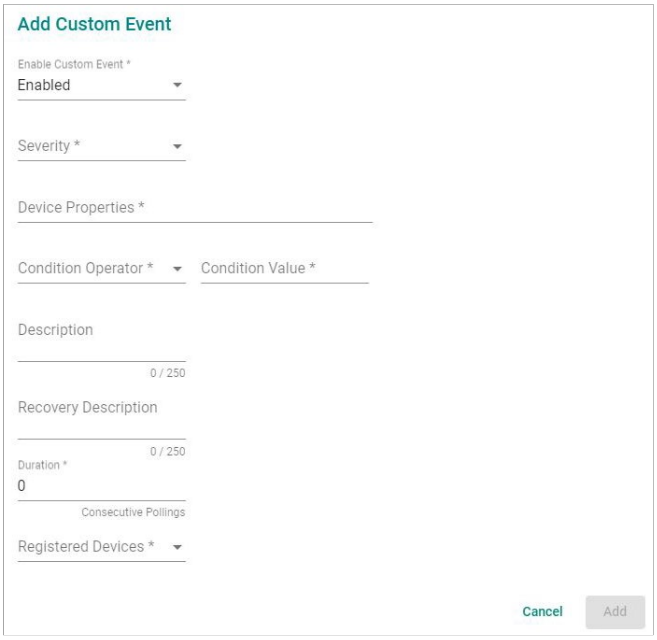
Configuring Custom Events

The **Custom Event** tab allows you to define your own events to monitor with flexible detection thresholds, severity levels, and duration times.

1. Navigate to **Menu** (☰) **> Event Management > Event Settings**.
2. Go to the **Custom Event** tab.

   The **Custom Event** screen will appear.
3. 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

4. Select the default event status:
   - **Enabled:** MXview One monitors the event
   - **Disabled:** MXview One does not monitor the event
5. Select one of the following severity levels for the event:
   - Information
   - Warning
   - Critical
6. Click the **Device Properties** and select the device property to monitor.
7. 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
8. (Optional) In the **Description** field, type a string (up to 250 characters in length) to describe the custom monitoring.
9. (Optional) In the **Recovery Description** field, type a string (up to 250 characters in length) to describe how to recover from the event.
10. 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.
11. From the **Register Devices** drop-down list, select the devices to monitor for the custom event.
12. 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

1. Navigate to **Menu** (☰) **> Event Management > Event Settings**.
2. Go to the **Custom Event** tab.

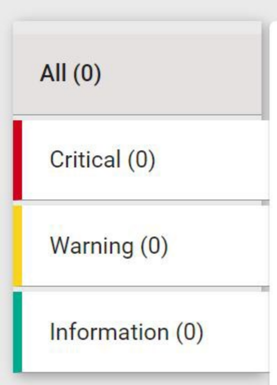
   The **Custom Event** screen will appear and displays the following information in a table format:

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

3. 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.

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

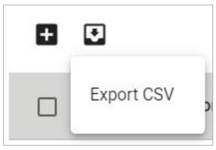
   MXview One filters the table to only display events that match the selected severity level.

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 **Custom Event** tab:

   a. Click the **Export** (⬇) icon.

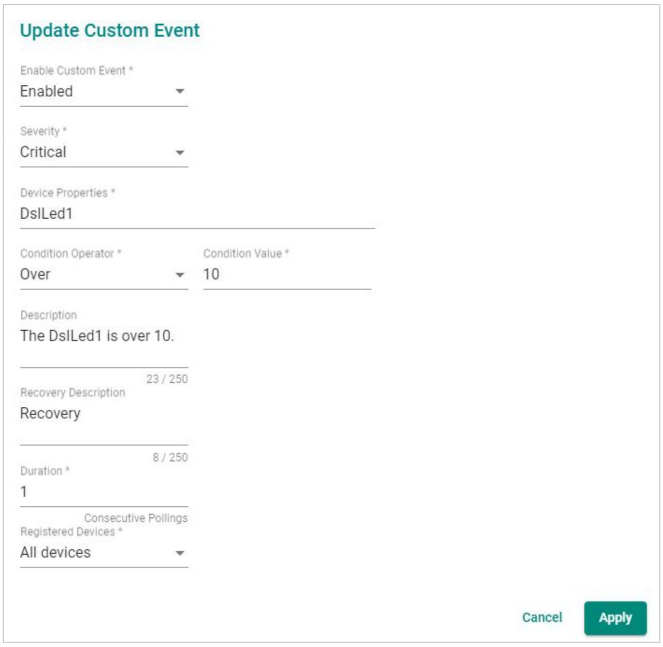


   b. Select **Export CSV.**
   MXview One exports the displayed event data as a CSV file.

Enabling/Disabling or Editing Custom Events

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

1. Navigate to **Menu** (☰) **> Event Management > Event Settings**.
2. Go to the **Custom Event** tab.
   The **Custom Event** screen will appear and display a list of configured custom events.
3. Click the **Edit** (✎) icon next to the event you want to enable/disable.
   The **Update Custom Event** screen will appear.



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

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

NOTE

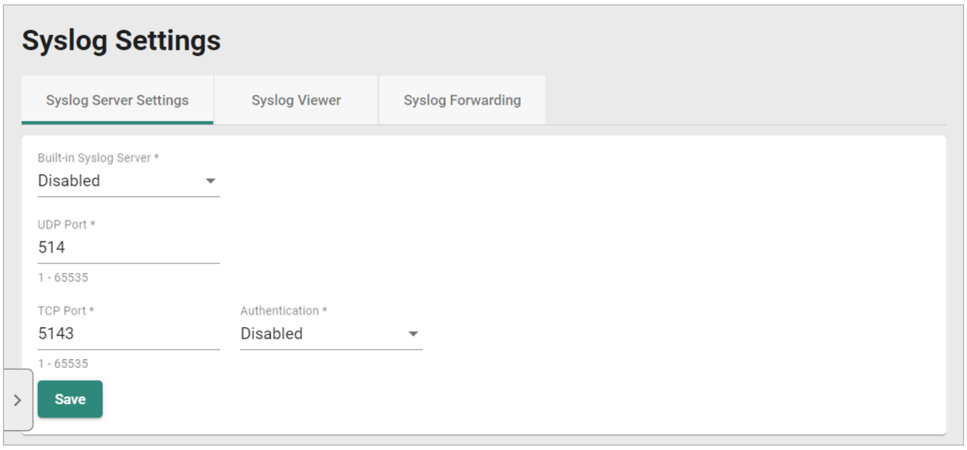
If the threshold is set as '0', the threshold function will be disabled.

Syslog Settings

MXview One features a built-in syslog server to receive and log syslog events from devices. Users can also define filtering rules, allowing MXview One to forward syslog events that match these rules to one or multiple external syslog servers.

Enabling/Disabling the Built-in Syslog Server

1. Navigate to **Menu** (☰) **> Event Management > Syslog Settings**.
   The **Syslog Settings** screen appears.
2. Go to the **Syslog Server Settings** tab.



Syslog Settings

Built-in Syslog Server * Disabled

UDP Port * 514 (1 - 65535)

TCP Port * 5143 (1 - 65535)

Authentication * Disabled

3. To enable the syslog server:
   a. In the **Built-in Syslog Server** field, select a syslog mode.
      - ❐ **Enable (UDP only)**: Enable the syslog server and restrict it to UDP only.
      - ❐ **Enable (TCP only)**: Enable the syslog server and restrict it to TCP only.
      - ❐ **Enable (UDP & TCP)**: Enable the syslog server and make it accessible via TCP and UDP.

   b. Specify the syslog server's UDP port. The default port number is 514.
   c. Specify the syslog server's TCP port. The default port number is 5143.
   d. Select an authentication mode:
      - ❐ **Disabled**: Do not require authentication.
      - ❐ **TLS only**: Use TLS authentication.
      - ❐ **TLS + certificate**: Use a combination of TLS and certificates for authentication.

   e. Click **Save**.

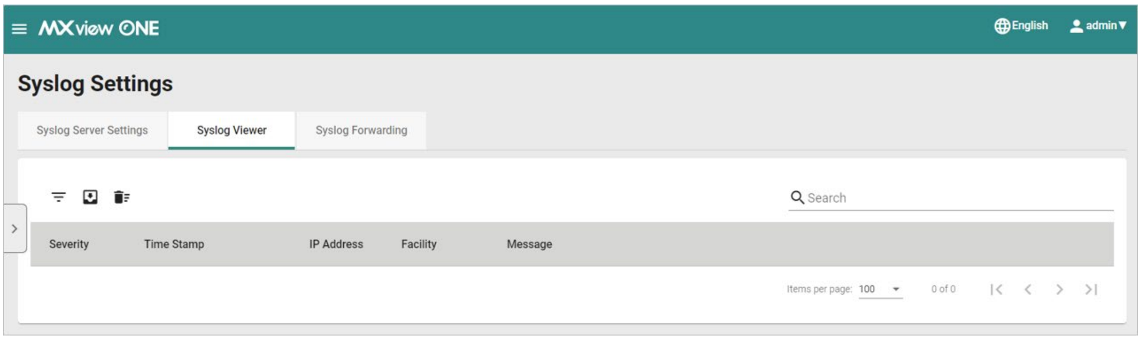
NOTE

If you selected **TLS + certificate** as the authentication method, the **Download and manage certificates from the MXview One Control Panel** message will show. Click the link to go to MXview One Control Panel for managing the syslog server certificate.

4. To disable the syslog server:
   a. In the **Built-in Syslog Server** field, select **Disabled**.
   b. Click **Save**.

Viewing Syslog Events

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



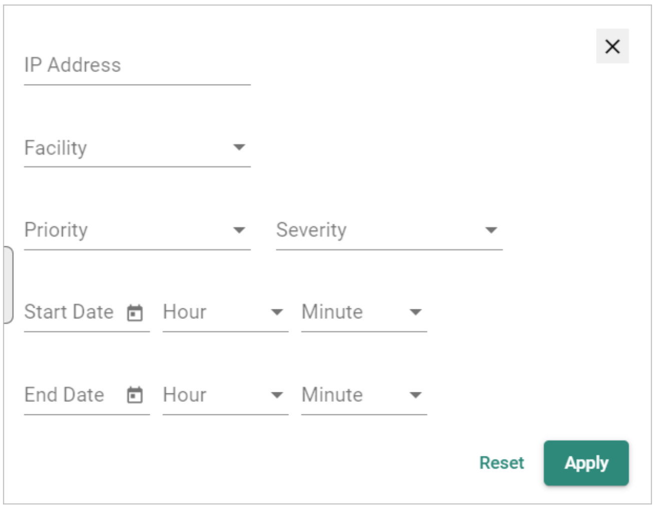
1. Navigate to **Menu** (☰) **> Event Management > Syslog Settings**.
   The **Syslog Settings** screen appears.
2. Go to the **Syslog Viewer** tab.
   The **Syslog Viewer** screen displays the following information in a table format:

Column	Description
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.



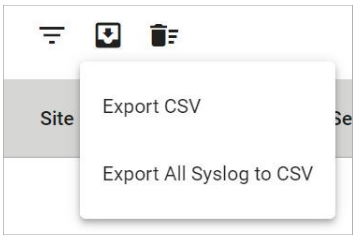
   b. Specify any of the following criteria:

Criteria	Description
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.

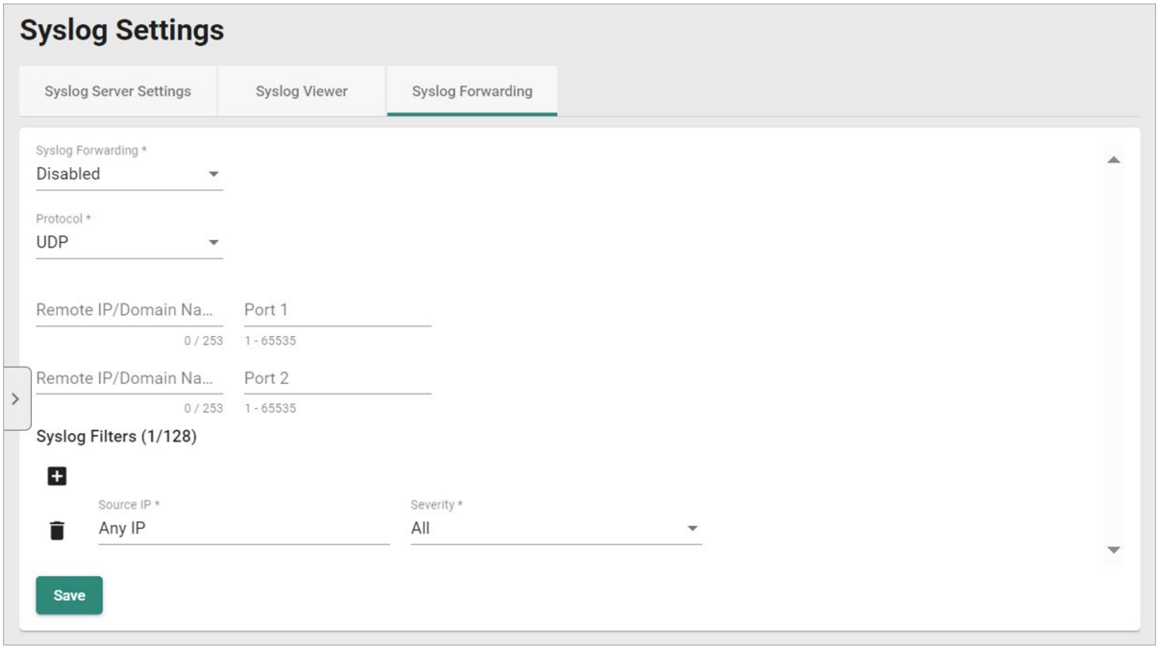
5. To sort the data in the table by a specific column, click the column heading.
   MXview One sorts the table by the column.
6. To export data displayed on the **Syslog Viewer** screen:
   a. Click the **Export** (⬇) icon.



   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.
7. To clear all syslog data, click the **Clear All Events** (🗑) icon.
   MXview One clears all syslog data on the **Syslog Viewer** screen.

Enabling/Disabling Syslog Forwarding

From the **Syslog Forwarding** tab on the **Syslog Settings** screen, you can enable or disable the syslog forwarding function and define the filtering rules. MXview One will act as a syslog forwarder and forward the syslog events that match the configured rules to one or multiple external syslog servers.



Syslog Forwarding *: Disabled
Protocol *: UDP
Remote IP/Domain Na... 0 / 253 | Port 1 1 - 65535
Remote IP/Domain Na... 0 / 253 | Port 2 1 - 65535
Syslog Filters (1/128)
Source IP *: Any IP | Severity *: All

1. Navigate to **Menu** (☰) **> Event Management > Syslog Settings**.
   The **Syslog Settings** screen appears.
2. Go to the **Syslog Forwarding** tab.
3. To enable syslog forwarding:
   a. Configure the following settings:
      ❒ **Syslog Forwarding:** Select **Enabled**.
      ❒ **Protocol**: Select the communication protocol (**UDP** or **TCP**).

- **Authentication**: If you selected **TCP** as the **Protocol**, select an authentication method (**Disabled**, **TLS only**, **TLS + certificate**).

NOTE

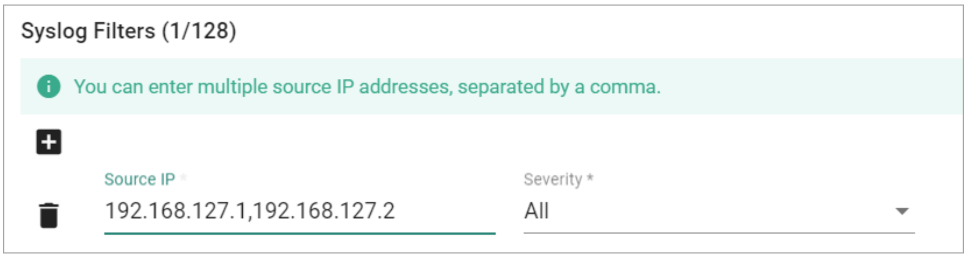
If you selected **TLS + certificate** as the authentication method, the **Download and manage certificates from the MXview One Control Panel** message will show. Click the link to go to MXview One Control Panel for managing the syslog forwarding certificate.

- **Remote IP/Domain Name 1/2**: Specify the IP address or domain name of the 1st and 2nd syslog server.
- **Port 1/2**: Specify the port number of the 1st and 2nd syslog server.

b. In the **Syslog Filters** section, configure the syslog filtering rules. The default rule is **Source IP=Any IP, Severity=All**, meaning MXview One will forward all syslog events from all sources and all severities.

To add a filtering rule, click the **Add** (⊞) icon and configure the following settings:

- **Source IP**: Specify the IP addresses of the device(s) you want to forward syslog events for. You can enter multiple IP addresses, separated by a comma.



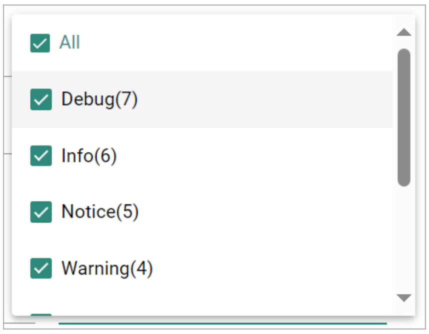
Syslog Filters (1/128)

You can enter multiple source IP addresses, separated by a comma.

Source IP: 192.168.127.1,192.168.127.2

Severity *: All

- **Severity**: Select the event severity level(s) that will be forwarded.



☑ All

☑ Debug(7)

☑ Info(6)

☑ Notice(5)

☑ Warning(4)

NOTE

MXview One supports a maximum of 128 syslog forwarding filtering rules.

c. To delete a filtering rule, click the **Delete** (🗑) icon next to the rule you want to delete.

d. Click **Save**.
MXview One will forward any syslog events that match the configured rules.

4. To disable syslog forwarding:

a. In the **Syslog Forwarding** field, select **Disabled**.

b. Click **Save**.

16. Inventory Management

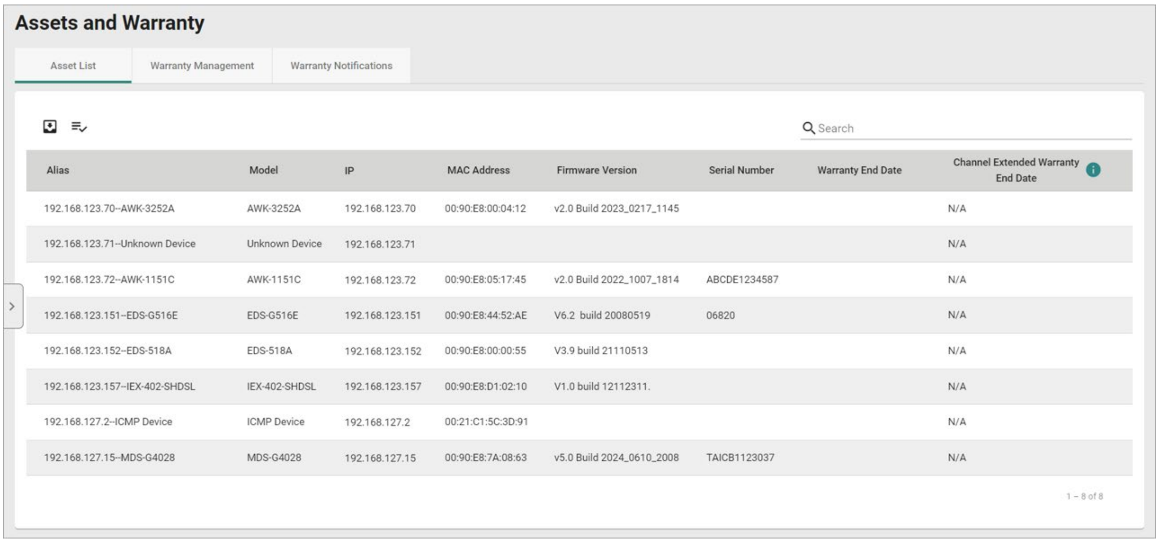
The **Inventory Management** section allows users to manage device inventory, check warranty information, and manage rogue devices.

Assets and Warranty

Asset List Overview

To access the **Asset List** page, in the function tree, navigate to **Menu** (☰) **> Inventory Management > Assets and Warranty** and go to the **Asset List** tab.

The **Asset List** section provides a summary of key information about your network devices.



Alias	Model	IP	MAC Address	Firmware Version	Serial Number	Warranty End Date	Channel Extended Warranty End Date
192.168.123.70--AWK-3252A	AWK-3252A	192.168.123.70	00:90:E8:00:04:12	v2.0 Build 2023_0217_1145			N/A
192.168.123.71--Unknown Device	Unknown Device	192.168.123.71					N/A
192.168.123.72--AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2022_1007_1814	ABCDE1234587		N/A
192.168.123.151--EDS-G516E	EDS-G516E	192.168.123.151	00:90:E8:44:52:AE	V6.2 build 20080519	06820		N/A
192.168.123.152--EDS-518A	EDS-518A	192.168.123.152	00:90:E8:00:00:55	V3.9 build 21110513			N/A
192.168.123.157--IEX-402-SHDSL	IEX-402-SHDSL	192.168.123.157	00:90:E8:D1:02:10	V1.0 build 12112311.			N/A
192.168.127.2--ICMP Device	ICMP Device	192.168.127.2	00:21:C1:5C:3D:91				N/A
192.168.127.15--MDS-G4028	MDS-G4028	192.168.127.15	00:90:E8:7A:08:63	v5.0 Build 2024_0610_2008	TAICB1123037		N/A

This page displays the following information in a table format:

Column	Description
Alias	The unique name of the device.
Model	The model number of the device.
IP	The IP address of the device.
MAC Address	The MAC address of the device.
Firmware Version	The firmware version of the device.
Serial Number	The serial number of the device.
Warranty End Date	The date the device warranty expires.
Channel Extended Warranty End Date	The expiration date of the extended device warranty provided by your channel representative.

NOTE

The **Channel Extended Warranty End Date** value is provided by the channel partner and must be entered by the user. Refer to Editing the Channel Extended Warranty End Date.

Searching the Asset List

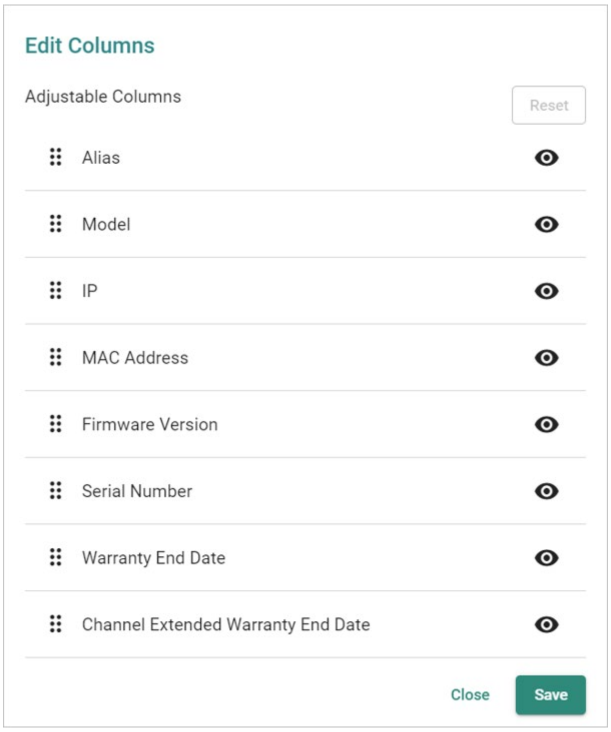
1. Navigate to **Menu** (☰) **> Inventory Management > Assets and Warranty**.
2. Go to the **Asset List** tab.
3. In the **Search** (🔍) field, type the full or partial information.
   All items matching the entered string will be shown in the table.

Exporting the Asset List

1. Navigate to **Menu** (☰) **> Inventory Management > Assets and Warranty**.
2. Go to the **Asset List** tab.
3. Click the **Export** (📥) icon in the top-left corner of the table.
   MXview One exports the asset list as a CSV file.

Editing the Asset List Layout

1. Navigate to **Menu** (☰) **> Inventory Management > Assets and Warranty**.
2. Go to the **Asset List** tab.
3. Click the **Edit Columns** (☰✓) icon in the top-left corner of the table.
   The **Edit Columns** window will appear.

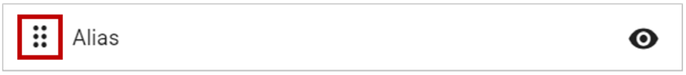


Edit Columns

Adjustable Columns

- Alias
- Model
- IP
- MAC Address
- Firmware Version
- Serial Number
- Warranty End Date
- Channel Extended Warranty End Date

4. To show or hide a column:
   a. Click the **Visible** (👁) and **Hidden** (⊘) icons to toggle column visibility.
5. To change the column order:
   a. Click and drag the **Drag** (⠿) icon of the column you want to move.



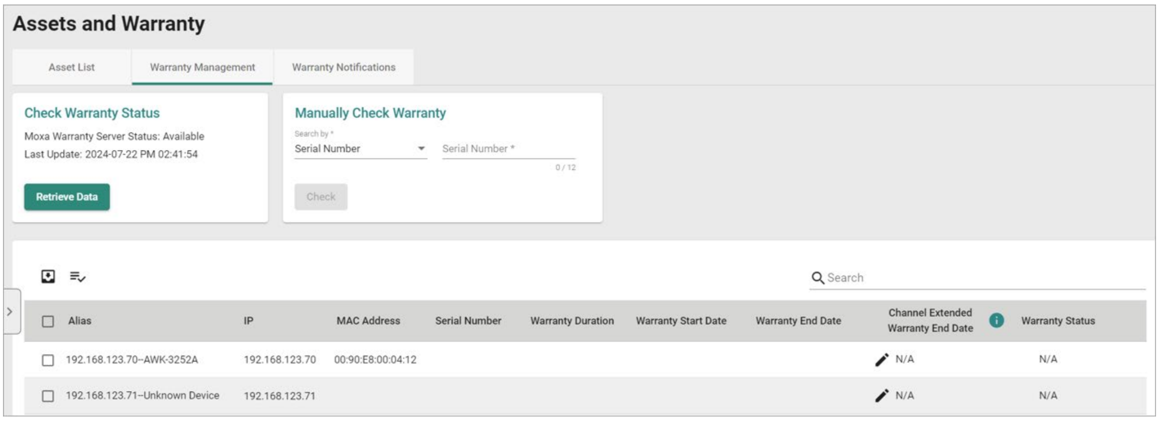
   b. Drag the column to the desired position and release the mouse.
6. To revert all changes to column visibility and order, click **Reset**.

7. Click **Save**.

Warranty Management Overview

To access the **Warranty Management** page, in the function tree, navigate to **Menu** (☰) **> Inventory Management > Assets and Warranty** and go to the **Warranty Management** tab.

The **Warranty Management** section shows warranty information for your devices.



Assets and Warranty

Asset List | Warranty Management | Warranty Notifications

Check Warranty Status

Moxa Warranty Server Status: Available

Last Update: 2024-07-22 PM 02:41:54

Retrieve Data

Manually Check Warranty

Search by *: Serial Number

Serial Number *

0 / 12

Check

Search

□	Alias	IP	MAC Address	Serial Number	Warranty Duration	Warranty Start Date	Warranty End Date	Channel Extended Warranty End Date	Warranty Status
□	192.168.123.70--AWK-3252A	192.168.123.70	00:90:E8:00:04:12					N/A	N/A
□	192.168.123.71--Unknown Device	192.168.123.71						N/A	N/A

This page displays the following information in a table format:

Column	Description
Alias	The unique name of the device.
IP	The IP address of the device.
MAC Address	The MAC address of the device.
Serial Number	The serial number of the device.
Warranty Duration	The warranty duration of the device.
Warranty Start Date	The date the device warranty starts.
Warranty End Date	The date the device warranty expires.
Channel Extended Warranty End Date	The expiration date of the extended device warranty provided by your channel representative.
Warranty Status	The current warranty status of the device. **Valid**: The warranty is active and valid. The remaining duration (in days) between the current date and the **Warranty End Date/Channel Extended Warranty End Date** is greater than the threshold value configured for the **Send Reminder** field on the **Warranty Notifications** tab. Refer to Enabling Warranty Expiration Notifications. **Expires soon**: The warranty is active and valid. The remaining duration (in days) between the current date and the **Warranty End Date/Channel Extended Warranty End Date** is equal to or less than the threshold value configured for the **Send Reminder** field on the **Warranty Notifications** tab. Refer to Enabling Warranty Expiration Notifications. **Expired**: The device warranty has exceeded the warranty period.

NOTE

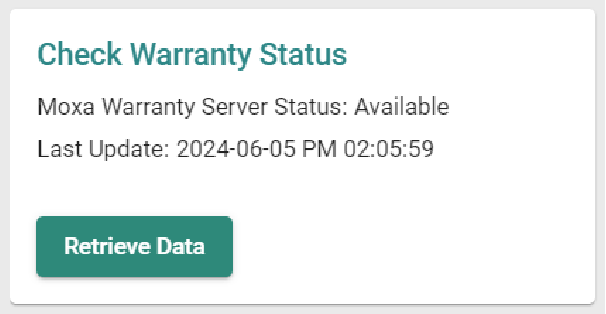
The **Channel Extended Warranty End Date** value is provided by the channel partner and must be entered by the user. Refer to Editing the Channel Extended Warranty End Date.

NOTE

Before using the Warranty Management function, make sure that the URL: https://api.common.thingsprocloud.com and port 443 are allowed through the firewall.

Checking the Warranty Status of All Devices

1. Navigate to **Menu** (☰) **> Inventory Management > Assets and Warranty**.
2. Go to the **Warranty Management** tab.
3. The **Check Warranty Status** section includes the following information:



Moxa Warranty Server Status: Available

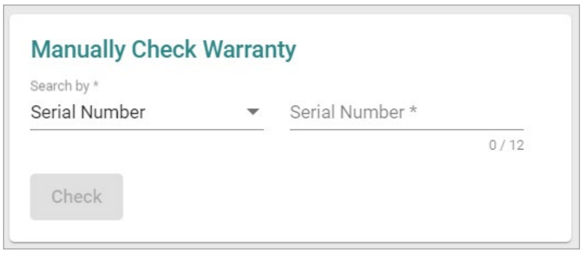
Last Update: 2024-06-05 PM 02:05:59

   - **Moxa Warranty Server Status**: This indicates the status of the connection to the Moxa warranty server. If this connection is unavailable, the warranty table cannot be updated until the connection to the warranty server is restored.
   - **Last Update**: Shows the date and time the warranty table was last checked and updated.

4. Click **Retrieve Data**.
   MXview One will check for updates and refresh the table.

Checking the Warranty Status of a Specific Device

1. Navigate to **Menu** (☰) **> Inventory Management > Assets and Warranty**.
2. Go to the **Warranty Management** tab.
3. The **Manually Check Warranty** section includes the following information:



   - **Search by**: Select the criteria to search for warranty information, either based on serial number or MAC address.
   - **Serial Number**: If **Serial Number** is selected in the **Search by** field, specify the serial number of the device to check warranty information for.
   - **MAC Address**: If **MAC Address** is selected in the **Search by** field, specify the MAC address of the device to check warranty information for.

4. Click **Check**.
   MXview One will check and show the warranty information for the specified criteria.

Searching the Warranty Management List

1. Navigate to **Menu** (☰) **> Inventory Management > Assets and Warranty**.
2. Go to the **Warranty Management** tab.
3. In the **Search** (🔍) field, type the full or partial information.
   All items matching the entered string will be shown in the table.

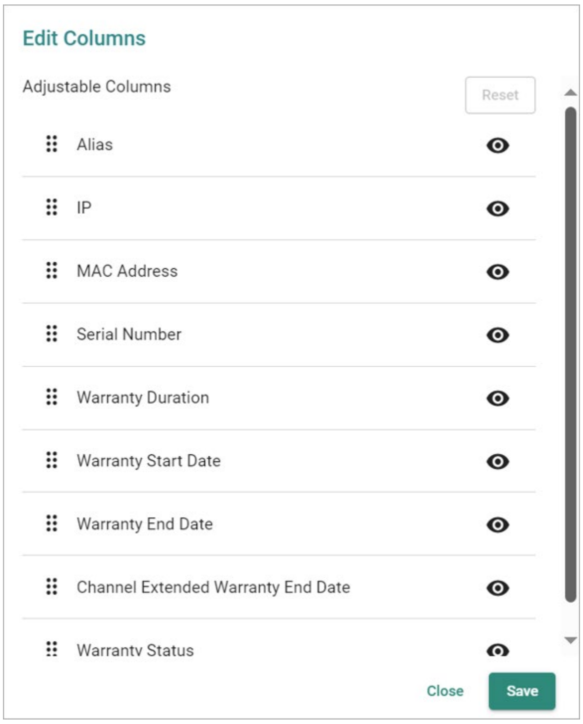
Exporting the Warranty Management List

1. Navigate to **Menu** (☰) **> Inventory Management > Assets and Warranty**.
2. Go to the **Warranty Management** tab.

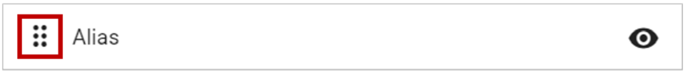
3. Click the **Export** (⤓) icon in the top-left corner of the table.
   MXview One exports the warranty management table as a CSV file.

Editing the Warranty Management List Layout

1. Navigate to **Menu** (☰) **> Inventory Management > Assets and Warranty**.
2. Go to the **Warranty Management** tab.
3. Click the **Edit Columns** (☰✓) icon in the top-left corner of the table.
   The **Edit Columns** window will appear.



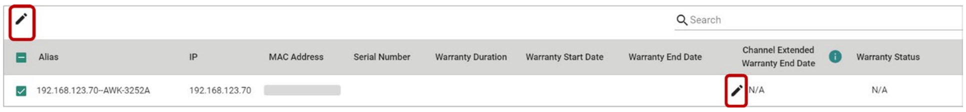
4. To show or hide columns:
   a. Click the **Visible** (👁) and **Hidden** (⊘) icons to toggle column visibility.
5. To change the column order:
   a. Click and drag the **Drag** (⠿) icon of the column you want to move.



   b. Drag the column to the desired position and release the mouse.
6. To revert all changes to column visibility and order, click **Reset**.
7. Click **Save**.

Editing the Channel Extended Warranty End Date

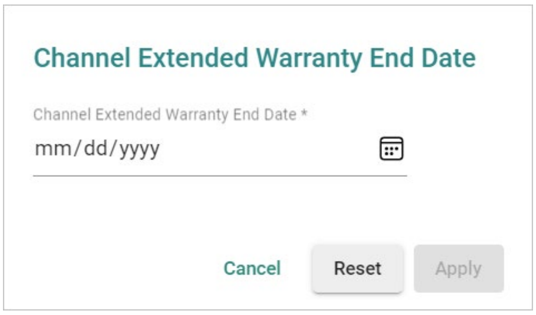
1. Navigate to **Menu** (☰) **> Inventory Management > Assets and Warranty**.
2. Go to the **Warranty Management** tab.
3. Check the box of the device(s) you want to edit the Channel Extended Warranty End Date for.
4. Click the **Edit** (✎) icon in the **Channel Extended Warranty End Date** column of the device you want to edit.
   If you selected multiple devices, click the **Edit** (✎) icon in the top-left corner of the page.



Search

	Alias	IP	MAC Address	Serial Number	Warranty Duration	Warranty Start Date	Warranty End Date	Channel Extended Warranty End Date	Warranty Status
☑	192.168.123.70–AWK-3252A	192.168.123.70	[redacted]					N/A	N/A

The **Channel Extended Warranty End Date** window will appear.



Channel Extended Warranty End Date

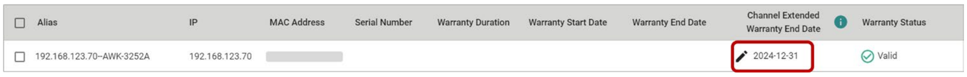
Channel Extended Warranty End Date *

mm/dd/yyyy

5. To update the channel extended warranty end date:

   a. Click the **Calendar** (▦) icon to select the new warranty end date.

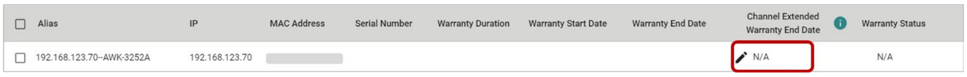
   b. Click **Apply**.
   MXview One will update the channel extended warranty end date value and warranty status according to the new end date.



□	Alias	IP	MAC Address	Serial Number	Warranty Duration	Warranty Start Date	Warranty End Date	Channel Extended Warranty End Date	Warranty Status
□	192.168.123.70–AWK-3252A	192.168.123.70	[redacted]					2024-12-31	✓ Valid

6. To reset the channel extended warranty end date:

   a. Click **Reset**.
   MXview One will update the channel extended warranty end date value to its default value of **N/A**.



□	Alias	IP	MAC Address	Serial Number	Warranty Duration	Warranty Start Date	Warranty End Date	Channel Extended Warranty End Date	Warranty Status
□	192.168.123.70–AWK-3252A	192.168.123.70	[redacted]					N/A	N/A

Warranty Notifications Overview

To access the **Warranty Notifications** page, in the function tree, navigate to **Menu** (☰) **> Inventory Management > Assets and Warranty** and go to the **Warranty Notifications** tab.

From the **Warranty Notifications** tab, you can enable and configure warning notifications to inform you when a device's warranty is about to expire.

Enabling Warranty Expiration Notifications

1. Navigate to **Menu** (☰) **> Inventory Management > Assets and Warranty**.
2. Go to the **Warranty Notifications** tab.
3. Configure the following settings:
   a. **Enabled**: Enable or disable warranty expiration notifications.
   b. **Send Reminder**: Specify how many days before the Warranty End Date/Channel Extended Warranty End Date you want to receive a notification.
   c. **Email to**: Enter the email address of the warranty notification recipient(s).

NOTE

You can add multiple recipient email addresses, separated by a comma.

4. Click **Save**.
   MXview One will send an email notification to the specified recipients when the number of days from the current date to the device Warranty End Date/Channel Extended Warranty End Date is equal to the value set in the **Send Reminder** field.

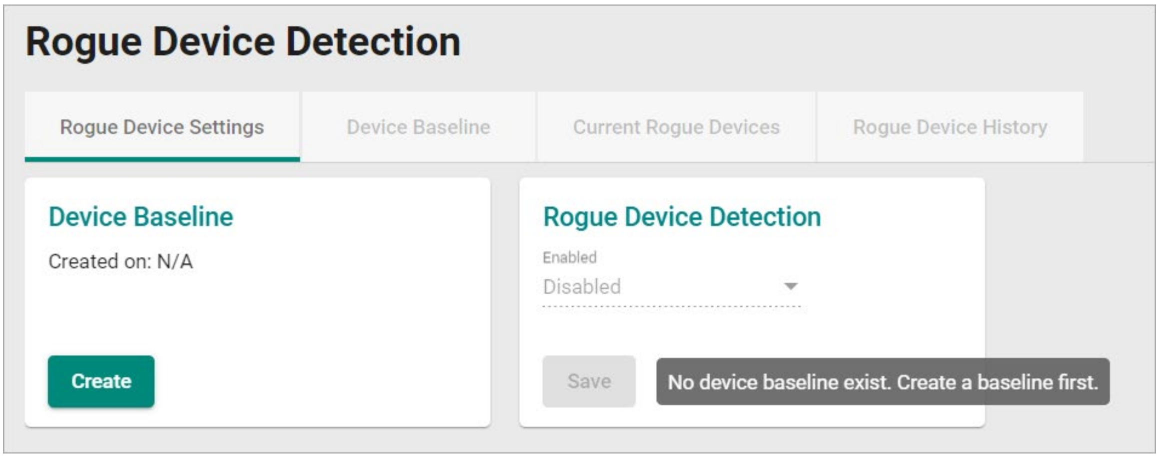
Rogue Device Detection

From the **Rogue Device Detection** section, users can create a baseline of the currently monitored devices. When MXview One detects an unknown device connection that is not part of this baseline, the system will identify and show information about this rogue device. This feature can help users manage the connection status of devices within their network, preventing unknown devices from gaining access to the network.

Rogue Device Settings Overview

To access the **Rogue Device Settings** page, in the function tree, navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection** and go to the **Rogue Device Settings** tab.

From the **Rogue Device Settings** tab, you can create a device baseline and enable the rogue device detection function.



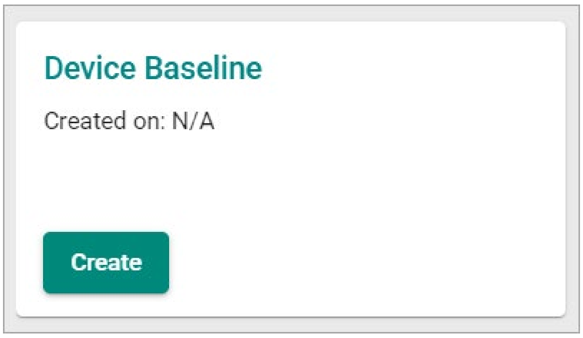
Created on: N/A

Enabled: Disabled

No device baseline exist. Create a baseline first.

Creating a Device Baseline

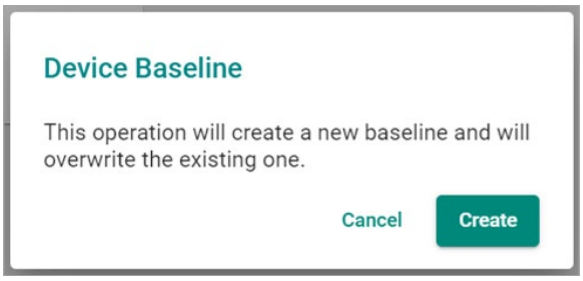
1. Navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection**.
2. Go to the **Rogue Device Settings** tab.
3. The **Device Baseline** section includes the following information:



Created on: N/A

- **Created on**: Shows the date and time when the most recent baseline was created. If no baseline has been created before, this will show **N/A**.

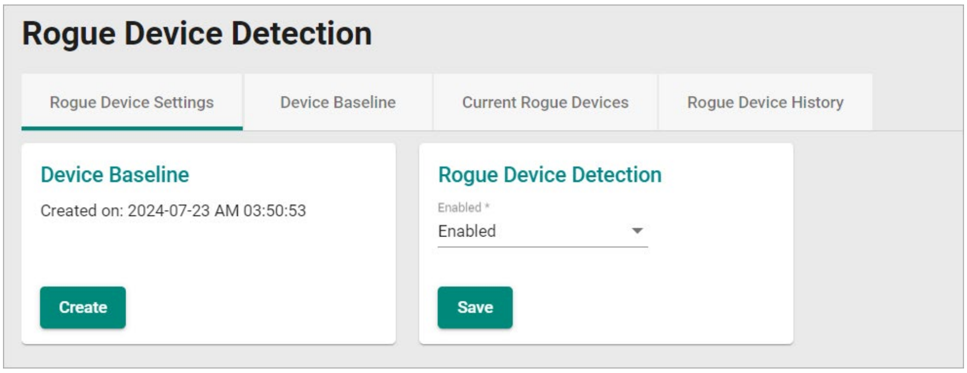
4. Click **Create**.
   The **Device Baseline** window will appear.



Device Baseline

This operation will create a new baseline and will overwrite the existing one.

5. Click **Create**.
   MXview One will create a baseline of the currently monitored devices and enable the **Rogue Device Detection** function.



Rogue Device Detection

Device Baseline

Created on: 2024-07-23 AM 03:50:53

Rogue Device Detection

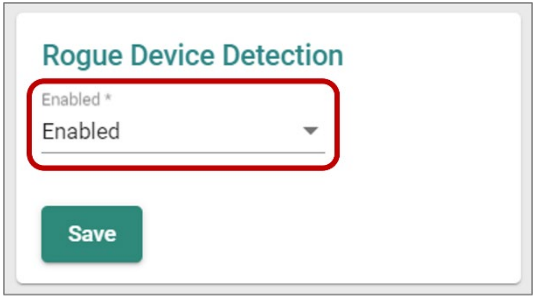
Enabled *: Enabled

Enabling/Disabling Rogue Device Detection

NOTE

To enable or disable **Rogue Device Detection**, a device baseline must be created first. Refer to Creating a Device Baseline.

1. Navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection**.
2. Go to the **Rogue Device Settings** tab.
3. In the **Rogue Device Detection** section, configure the following settings:



Rogue Device Detection

Enabled *: Enabled

   - **Enabled**: Enable or disable the Rogue Device Detection function.
4. Click **Save**.

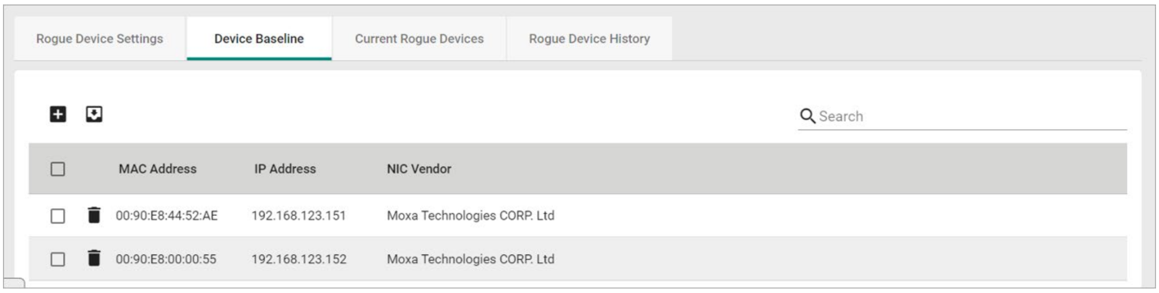
NOTE

After creating a device baseline and enabling the **Rogue Device Detection** function, you can add devices to the baseline via the **Device Discovery** function or by **Adding a Rogue Device to the Baseline**.

Device Baseline Overview

To access the **Device Baseline** page, in the function tree, navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection** and go to the **Device Baseline** tab.

From the **Device Baseline** tab, you can view information about the devices included in the most recent baseline. From this screen, you can also add or remove devices from the baseline and export the device baseline.



□		MAC Address	IP Address	NIC Vendor
□	🗑	00:90:E8:44:52:AE	192.168.123.151	Moxa Technologies CORP. Ltd
□	🗑	00:90:E8:00:00:55	192.168.123.152	Moxa Technologies CORP. Ltd

This page displays the following information in a table format:

Column	Description
MAC Address	The MAC address of the device.
IP Address	The IP address of the device.
NIC Vendor	The vendor of the device's network interface card.

Searching the Device Baseline

1. Navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection**.
2. Go to the **Device Baseline** tab.
3. In the **Search** (🔍) field, type the full or partial information.
   All items matching the entered string will be shown in the table.

Adding a Device to the Baseline

1. Navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection**.
2. Go to the **Device Baseline** tab.
3. Click the **Add** (⊞) icon in the top-left corner of the screen.
   The **Add Device to Baseline** screen will appear.
4. Specify the MAC address of the device you want to add to the baseline.
5. Click **Add**.

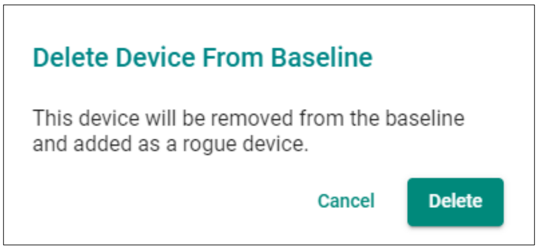
Deleting Devices From the Baseline

NOTE

If a device that was removed from the baseline attempts to reconnect, MXview One will identify the device as a rogue device and add it to the **Current Rogue Devices** list. Refer to Current Rogue Devices Overview.

1. Navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection**.
2. Go to the **Device Baseline** tab.
   To delete a single device:

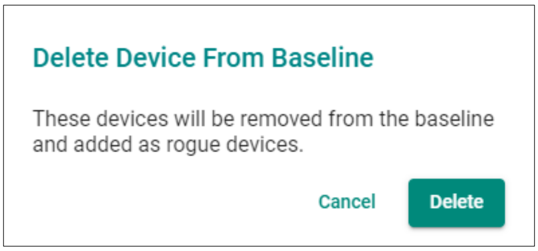
a. Click the **Delete** (🗑) icon next to the device you want to delete from the baseline.
The **Delete Device From Baseline** screen will appear.



Delete Device From Baseline

This device will be removed from the baseline and added as a rogue device.

3. To delete multiple devices:
   a. Check the box of the devices you want to delete from the baseline.
   b. Click the **Delete** (🗑) icon in the top-left corner of the screen.
   The **Delete Device From Baseline** screen will appear.



Delete Device From Baseline

These devices will be removed from the baseline and added as rogue devices.

4. Click **Delete**.

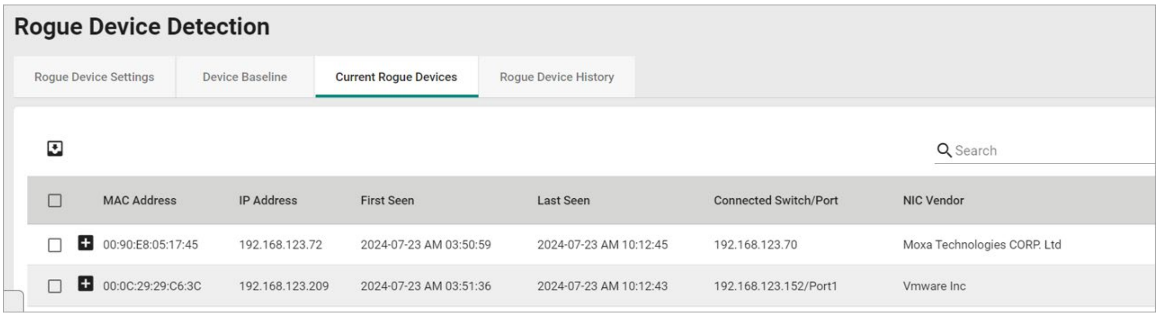
Exporting the Device Baseline

1. Navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection**.
2. Go to the **Device Baseline** tab.
3. Click the **Export** (⬇) icon in the top-left corner of the table.
   MXview One exports the device baseline as a CSV file.

Current Rogue Devices Overview

To access the **Current Rogue Devices** page, in the function tree, navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection** and go to the **Current Rogue Devices** tab.

From the **Current Rogue Devices** tab, you can view information about rogue devices detected on your network.



Rogue Device Detection

☐	MAC Address	IP Address	First Seen	Last Seen	Connected Switch/Port	NIC Vendor
☐	00:90:E8:05:17:45	192.168.123.72	2024-07-23 AM 03:50:59	2024-07-23 AM 10:12:45	192.168.123.70	Moxa Technologies CORP. Ltd
☐	00:0C:29:29:C6:3C	192.168.123.209	2024-07-23 AM 03:51:36	2024-07-23 AM 10:12:43	192.168.123.152/Port1	Vmware Inc

This page displays the following information in a table format:

Column	Description
MAC Address	The MAC address of the rogue device.
IP Address	The IP address of the rogue device.
First Seen	The date and time MXview One first detected the rogue device.

Last Seen	The date and time MXview One last detected the rogue device.
Connected Switch/Port	The switch device and port the rogue device is connected to.
NIC Vendor	The vendor of the rogue device’s network interface card.

NOTE

It is possible to see the same IP listed with different MAC addresses in the rogue device list. This could indicate one of the following situations:

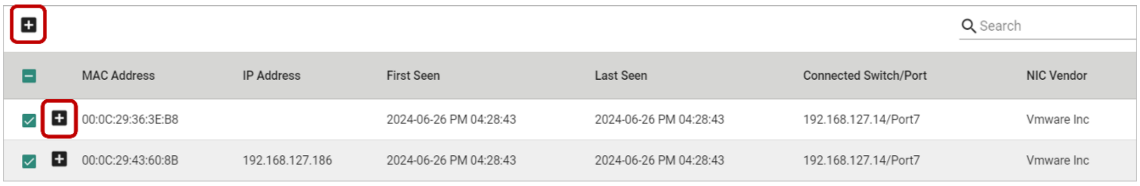
- A single device with multiple MAC addresses: In addition to a CPU MAC address, certain Moxa products (e.g. EDS-(G)4000 Series, MDS-G4028 Series, etc.) and some third-party devices have an individual MAC address for each port.
- Different devices using the same IP address: Different devices using an identical IP address indicate a possible IP conflict. To avoid issues, identify and resolve any IP conflicts.

Searching the Current Rogue Devices List

1. Navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection**.
2. Go to the **Current Rogue Devices** tab.
3. In the **Search** (🔍) field, type the full or partial information.
   All items matching the entered string will be shown in the table.

Adding a Rogue Device to the Baseline

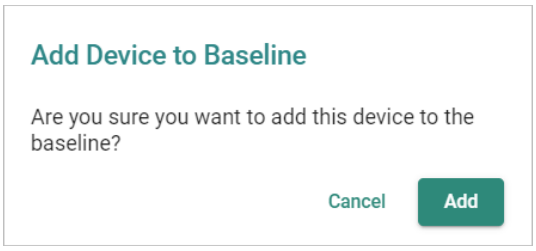
1. Navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection**.
2. Go to the **Current Rogue Devices** tab.
3. Click the **Add** (⊞) icon next to the rogue device you want to add to the baseline.
   To add multiple rogue devices to the baseline, check the box of the devices you want to add and click the **Add** (⊞) icon in the top-left corner of the screen.



⊞ Search

☐		MAC Address	IP Address	First Seen	Last Seen	Connected Switch/Port	NIC Vendor
☑	⊞	00:0C:29:36:3E:B8		2024-06-26 PM 04:28:43	2024-06-26 PM 04:28:43	192.168.127.14/Port7	Vmware Inc
☑	⊞	00:0C:29:43:60:8B	192.168.127.186	2024-06-26 PM 04:28:43	2024-06-26 PM 04:28:43	192.168.127.14/Port7	Vmware Inc

The **Add Device to Baseline** window will appear.



Add Device to Baseline

Are you sure you want to add this device to the baseline?

4. Click **Add**.

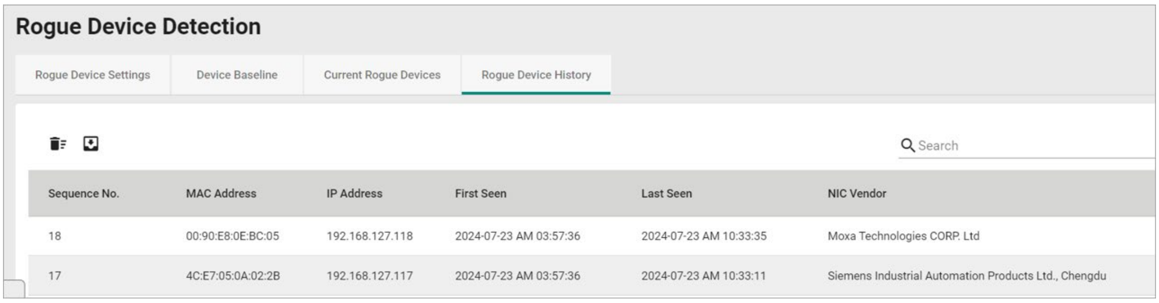
Exporting the Current Rogue Devices List

1. Navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection**.
2. Go to the **Current Rogue Devices** tab.
3. Click the **Export** (⤓) icon in the top-left corner of the table.
   MXview One exports the current rogue devices list as a CSV file.

Rogue Device History Overview

To access the **Rogue Device History** page, in the function tree, navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection** and go to the **Rogue Device History** tab.

From the **Rogue Device History** tab, you can view information about rogue devices that were originally in the Current Rogue Devices list but are currently no longer detected by MXview One.



Rogue Device Detection

Sequence No.	MAC Address	IP Address	First Seen	Last Seen	NIC Vendor
18	00:90:E8:0E:BC:05	192.168.127.118	2024-07-23 AM 03:57:36	2024-07-23 AM 10:33:35	Moxa Technologies CORP. Ltd
17	4C:E7:05:0A:02:2B	192.168.127.117	2024-07-23 AM 03:57:36	2024-07-23 AM 10:33:11	Siemens Industrial Automation Products Ltd., Chengdu

This page displays the following information in a table format:

Column	Description
Sequence No.	The index of the history record.
MAC Address	The MAC address of the rogue device.
IP Address	The IP address of the rogue device.
First Seen	The date and time MXview One first detected the rogue device.
Last Seen	The date and time MXview One last detected the rogue device.
NIC Vendor	The vendor of the rogue device’s network interface card.

Searching the Rogue Device History

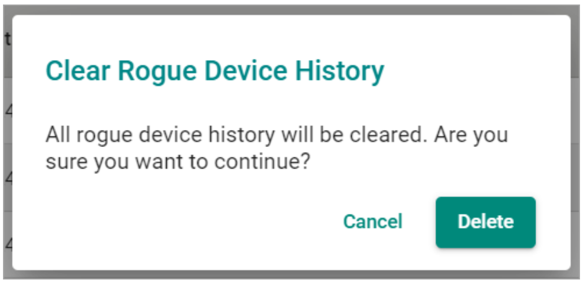
1. Navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection**.
2. Go to the **Rogue Device History** tab.
3. In the **Search** (🔍) field, type the full or partial information.
   All items matching the entered string will be shown in the table.

Exporting the Rogue Device History

1. Navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection**.
2. Go to the **Rogue Device History** tab.
3. Click the **Export** (⬇) icon in the top-left corner of the table.
   MXview One exports the rogue device history as a CSV file.

Clearing the Rogue Device History

1. Navigate to **Menu** (☰) **> Inventory Management > Rogue Device Detection**.
2. Go to the **Rogue Device History** tab.
3. Click the **Delete** (🗑) icon in the top-left corner of the screen.
   The **Clear Rogue Device History** window will appear.



Clear Rogue Device History

All rogue device history will be cleared. Are you sure you want to continue?

4. Click **Delete**.
   MXview One will clear the rogue device history.

17. Backups, Restores, and Compares

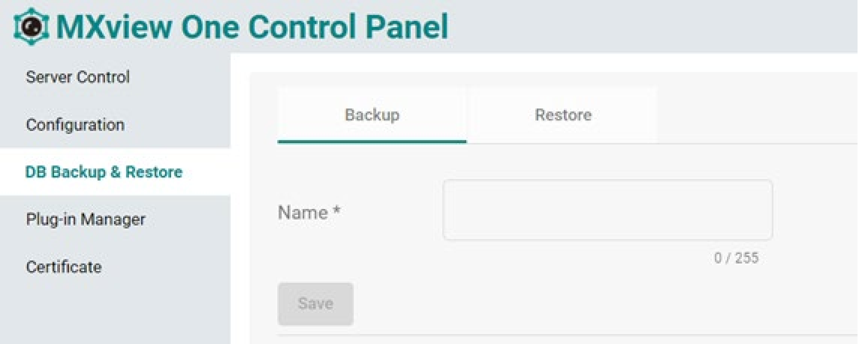
The MXview One web console provides several features to assist database backups and device configuration migrations. MXview One allows you to back up or restore configurations for multiple devices, and also compare changes between different versions of archived configuration files. You can also create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

Backing Up the MXview One Database

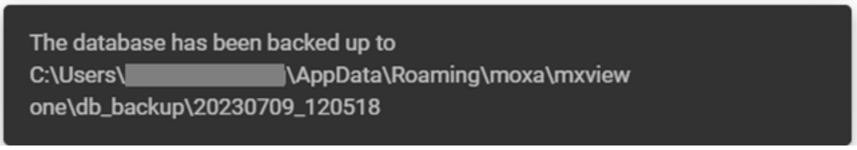
Use the **DB Backup & Restore** screen on the **Control Panel** to back up the MXview One database.

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

   The Database Backup & Restore screen appears.

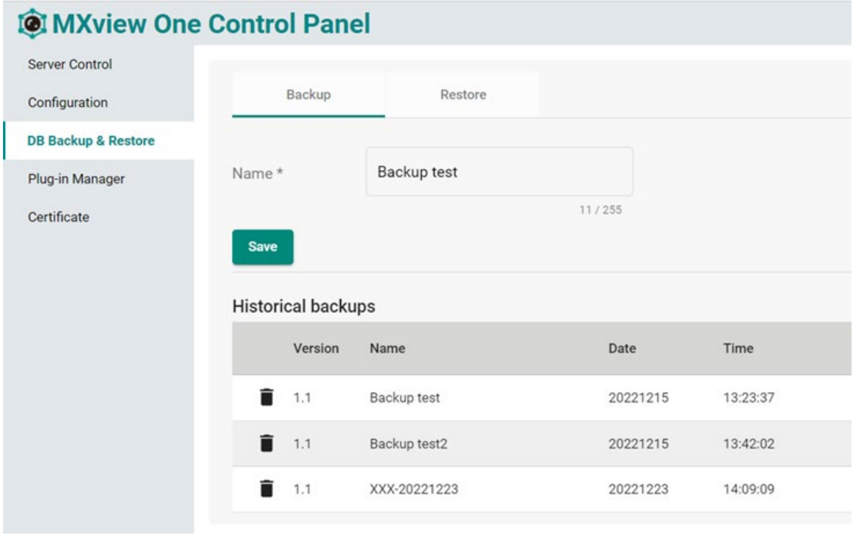


2. Choose the **Backup** tab to start the process of backing up the database.
3. In the **Name** field, specify the backup file name.
4. Click **Save**.
5. The message that the file of the backup database has been stored in the specified directory will be displayed.



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
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

Backing Up Device Configurations

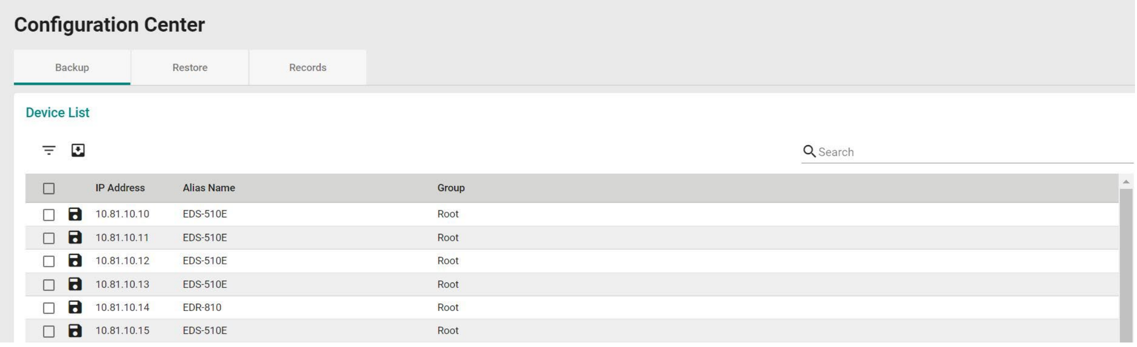
Use the **Device Configuration Center** screen to export configuration backup files from one or more devices.

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:

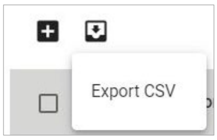
   - **Group:** The group in the MXview One tree structure that the device is assigned to
   - **IP Address:** The IP address of the device

   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:

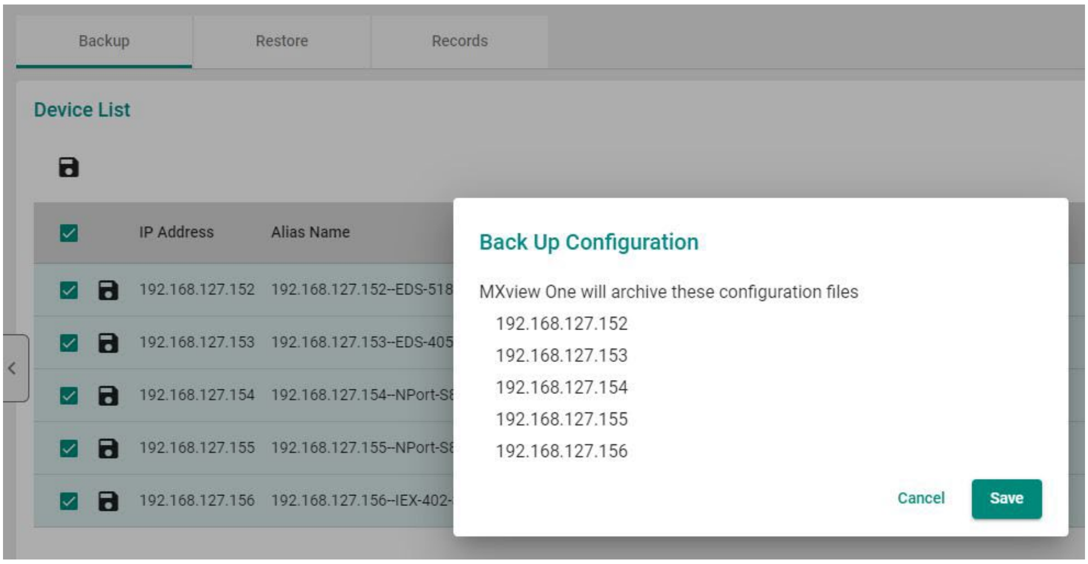
   a. Select the check box next to the device(s) you want to back up.

   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

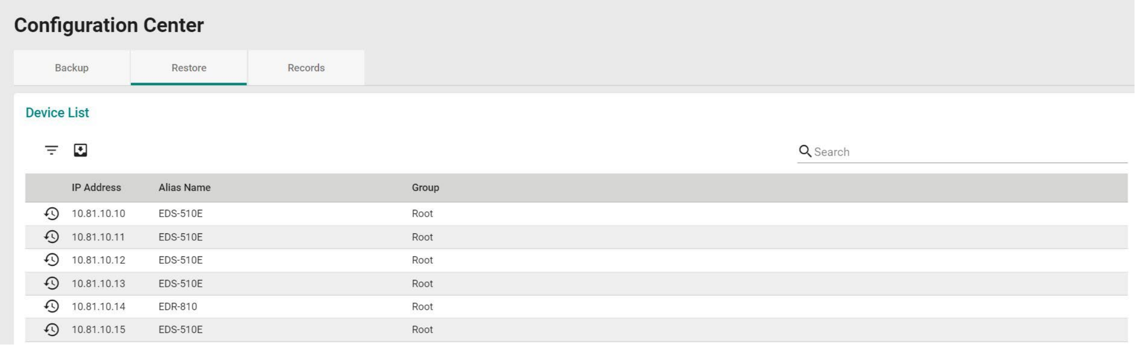
Use the **Configuration Center** screen to restore configurations to one or more devices by restoring an archived configuration from the MXview One server or importing a local configuration backup file (in INI format).

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**.



	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

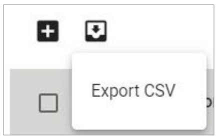
      ❒ **IP Address:** The IP address of the device

   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.



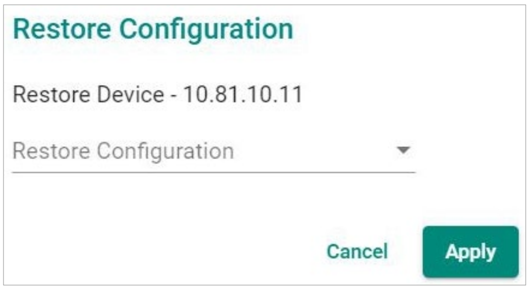
   b. Select **Export CSV**.

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

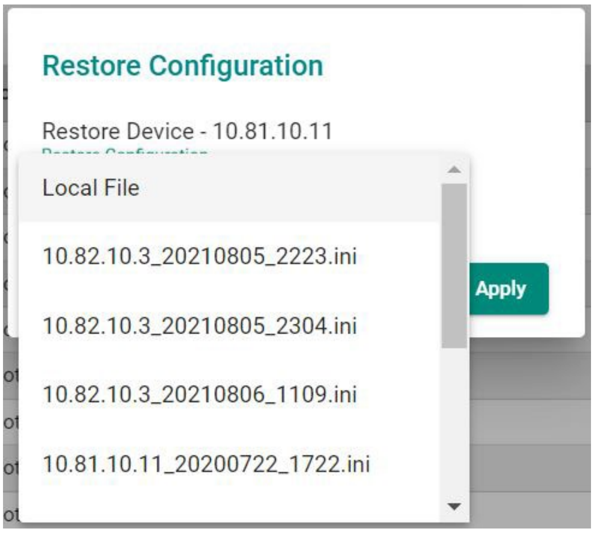
5. To restore an archived configuration file to a device:

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

      The **Restore Configuration** screen will appear.



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

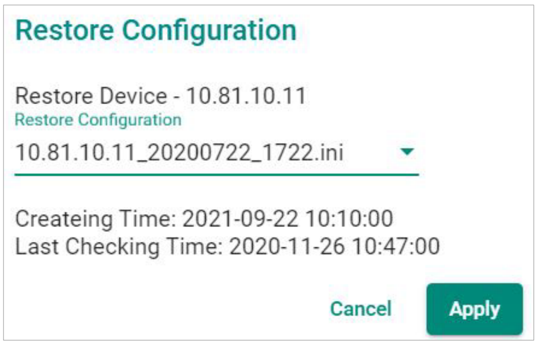


Restore Configuration

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

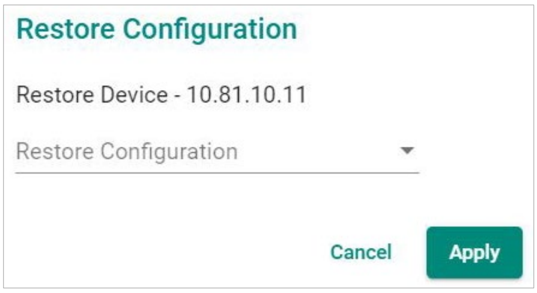
Createing Time: 2021-09-22 10:10:00
Last Checking Time: 2020-11-26 10:47:00

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.



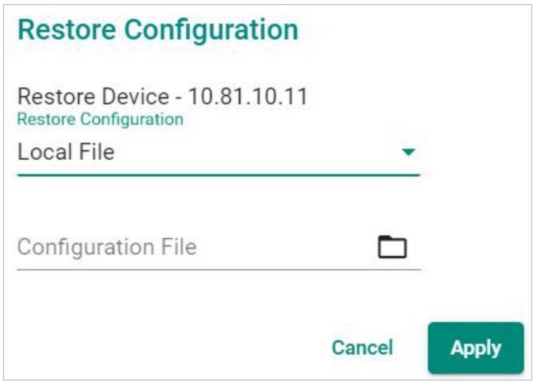
Restore Configuration

Restore Device - 10.81.10.11

Restore Configuration

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

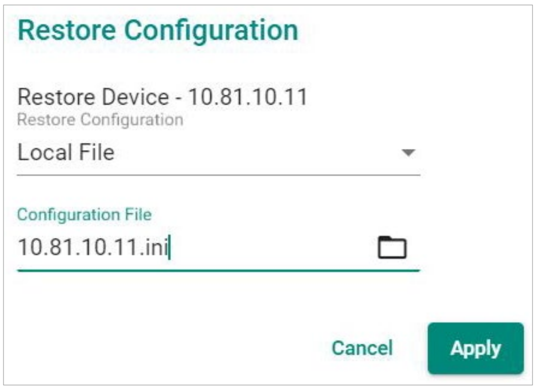
Restore Device - 10.81.10.11

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

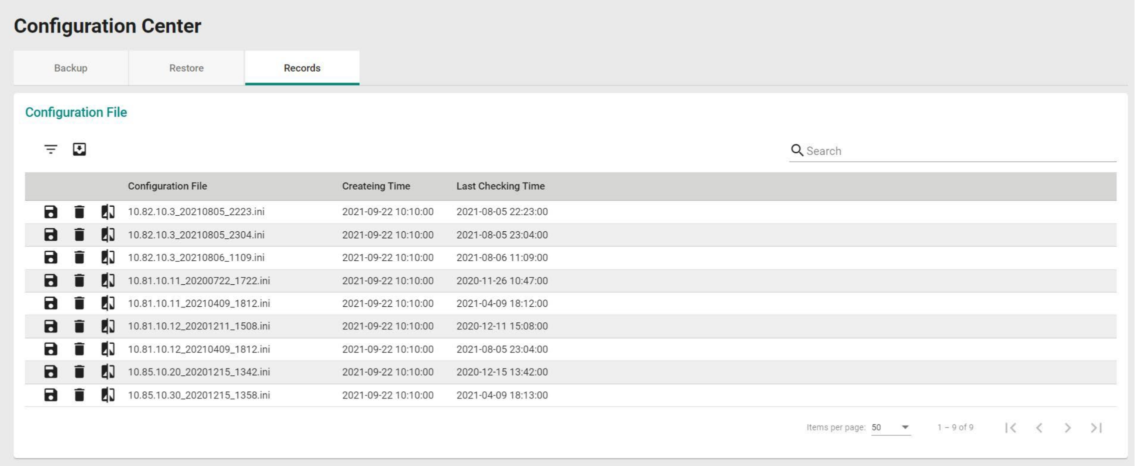
Configuration File: 10.81.10.11.ini

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.



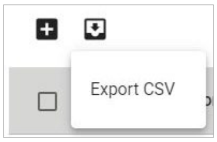
Configuration Center

Configuration File

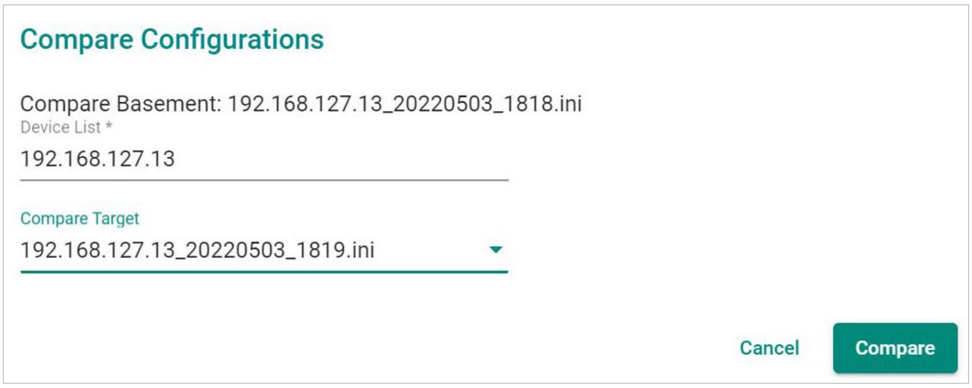
			Configuration File	Createing Time	Last Checking Time
			10.82.10.3_20210805_2223.ini	2021-09-22 10:10:00	2021-08-05 22:23:00
			10.82.10.3_20210805_2304.ini	2021-09-22 10:10:00	2021-08-05 23:04:00
			10.82.10.3_20210806_1109.ini	2021-09-22 10:10:00	2021-08-06 11:09:00
			10.81.10.11_20200722_1722.ini	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

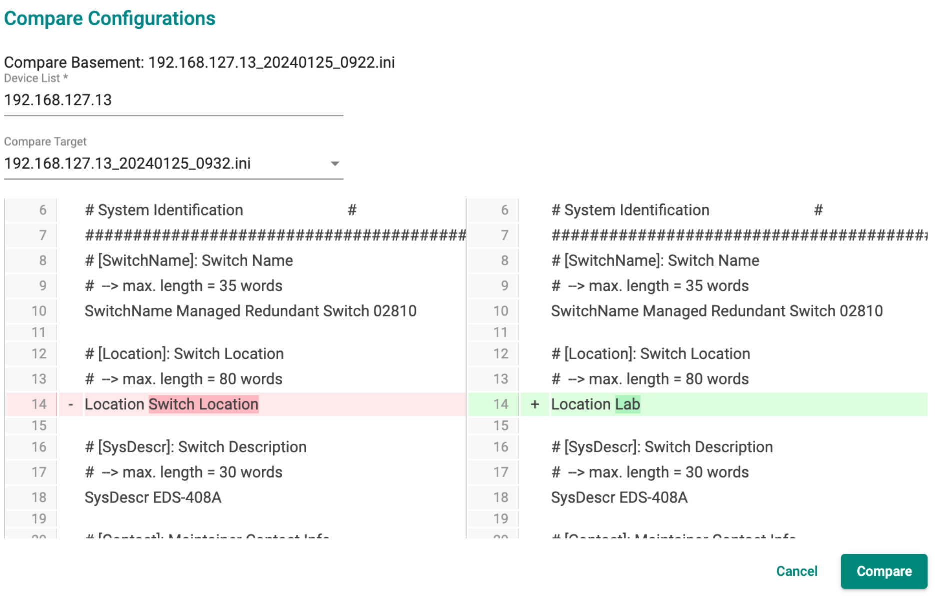
Device List *
192.168.127.13

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.

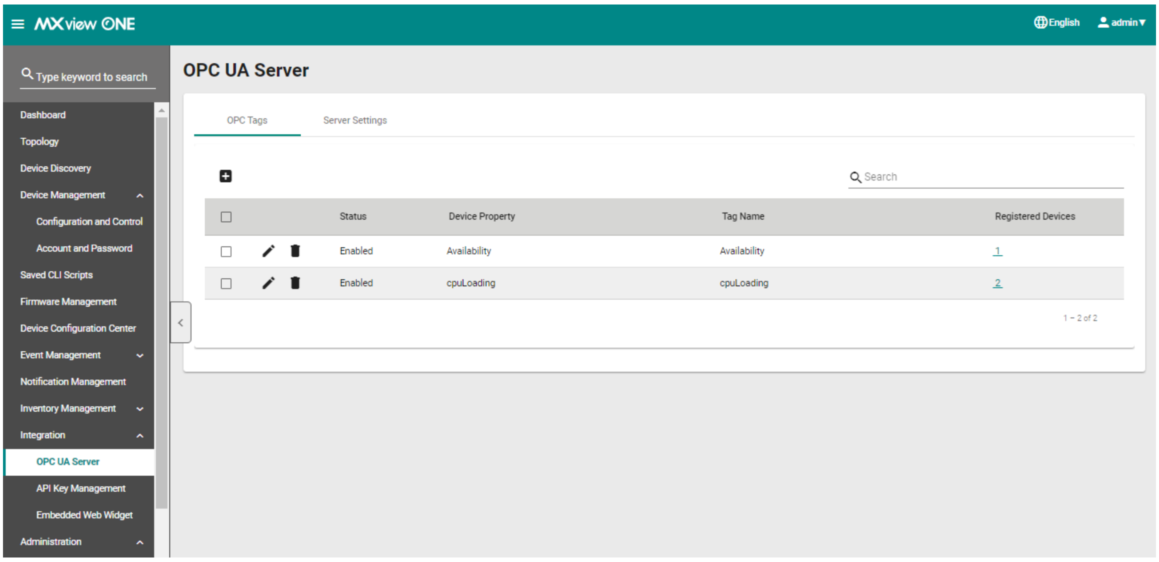
18. Custom Integrations

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

OPC UA Server Overview

MXview One supports integrated OPC UA Server functionality to integrate with OPC clients such as SCADA systems. From this section, users can configure OPC tags and server settings.

To access the **OPC UA Server** screen, navigate to **Menu** (☰) **> Integration > OPC UA Server**.



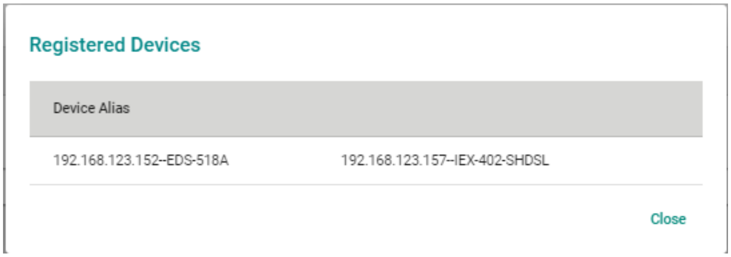
OPC UA Server

□		Status	Device Property	Tag Name	Registered Devices
□	✎ 🗑	Enabled	Availability	Availability	1
□	✎ 🗑	Enabled	cpuLoading	cpuLoading	2

1 – 2 of 2

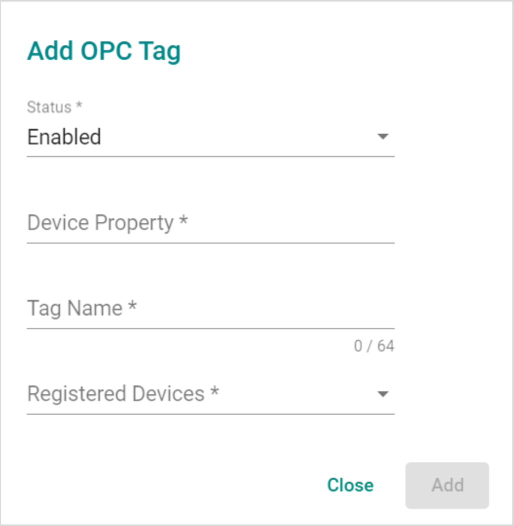
Viewing the OPC Tags Table

1. Navigate to **Menu** (☰) **> Integration > OPC UA Server**.
   The **OPC UA Server** screen appears.
2. Go to the **OPC Tags** tab.
3. The OPC tags table includes the following information:

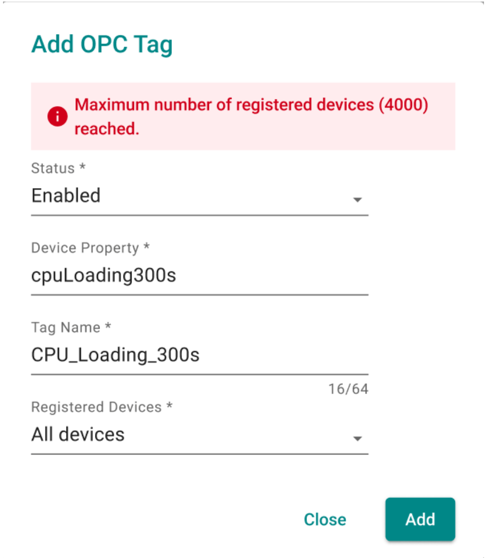
Column	Description
Status	Shows the status of the OPC tag.
Device Property	Shows the SNMP device property of the tag name.
Tag Name	Shows the tag name.
Registered Devices	Shows the devices registered to the tag. Click the hyperlink number in this column to show an overview of all registered devices.  Registered Devices Device Alias 192.168.123.152--EDS-518A 192.168.123.157--IEX-402-SHDSL Close

Adding an OPC Tag

1. Navigate to **Menu (☰) > Integration > OPC UA Server**.
   The **OPC UA Server** screen appears.
2. Go to the **OPC Tags** tab.
3. Click the **Add** (⊞) icon.
   The **Add OPC Tag** screen will appear.



4. Configure the following settings:
   - **Status**: Select to enable or disable the OPC tag.
   - **Device Property**: Select the SNMP property to generate the OPC tag.
   - **Tag Name**: Enter a name for the OPC tag.
   - **Registered Devices**: Select the devices to register to this tag.
5. Click **Add**.
   If the total number of registered devices exceeds 4000, an error message will show.



Add OPC Tag

Maximum number of registered devices (4000) reached.

Status *
Enabled

Device Property *
cpuLoading300s

Tag Name *
CPU_Loading_300s
16/64

Registered Devices *
All devices

A confirmation will appear to verify tag was created.

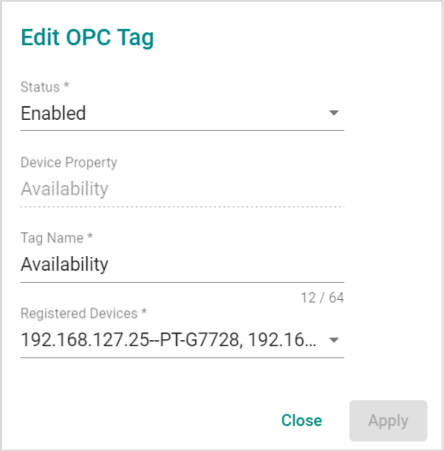
Tag created successfully

NOTE

MXview One supports a maximum of 2000 OPC tags.

Editing an OPC Tag

1. Navigate to **Menu (☰) > Integration > OPC UA Server**.
   The **OPC UA Server** screen appears.
2. Go to the **OPC Tags** tab.
3. Click on the **Edit** (✎) icon next to the tag you want to edit
   The **Edit OPC Tag** screen will appear.



Edit OPC Tag

Status *
Enabled

Device Property
Availability

Tag Name *
Availability
12 / 64

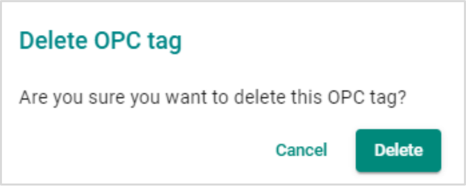
Registered Devices *
192.168.127.25--PT-G7728, 192.16...

4. Configure the following settings:
   - **Status**: Select to enable or disable the OPC tag.
   - **Tag Name**: Enter a name for the OPC tag.
   - **Registered Devices**: Select the devices to associate this tag with.
5. Click **Apply**.
   A confirmation will appear to verify the tag was updated.

Tag updated successfully

Deleting an OPC Tag

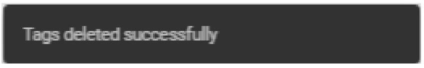
1. Navigate to **Menu (☰) > Integration > OPC UA Server**.
   The **OPC UA Server** screen appears.
2. Go to the **OPC Tags** tab.
3. Click the **Delete** (🗑) icon next to the tag you want to delete.
   A confirmation window will appear.



Delete OPC tag

Are you sure you want to delete this OPC tag?

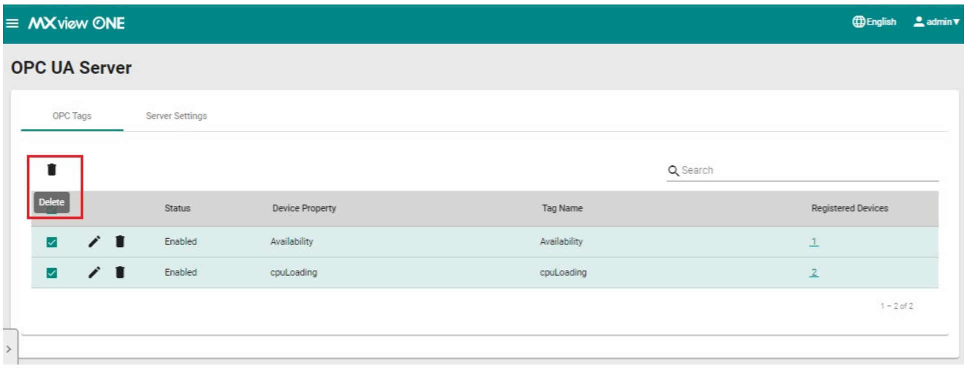
4. Click **Delete**.
   A confirmation will appear to verify the tag was deleted.



Tags deleted successfully

Deleting Multiple OPC Tags

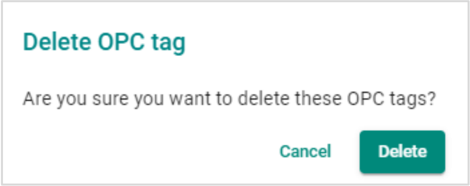
1. Navigate to **Menu (☰) > Integration > OPC UA Server**.
   The **OPC UA Server** screen appears.
2. Go to the **OPC Tags** tab
3. Select the checkbox of the OPC tags you want to delete in the list.
4. Click the **Delete** (🗑) icon at the top of the page.



		Status	Device Property	Tag Name	Registered Devices
☑		Enabled	Availability	Availability	1
☑		Enabled	cpuLoading	cpuLoading	2

1 – 2 of 2

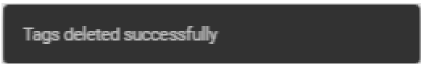
5. A confirmation window will appear.



Delete OPC tag

Are you sure you want to delete these OPC tags?

6. Click **Delete**.
   A confirmation will appear to verify the tags were deleted.

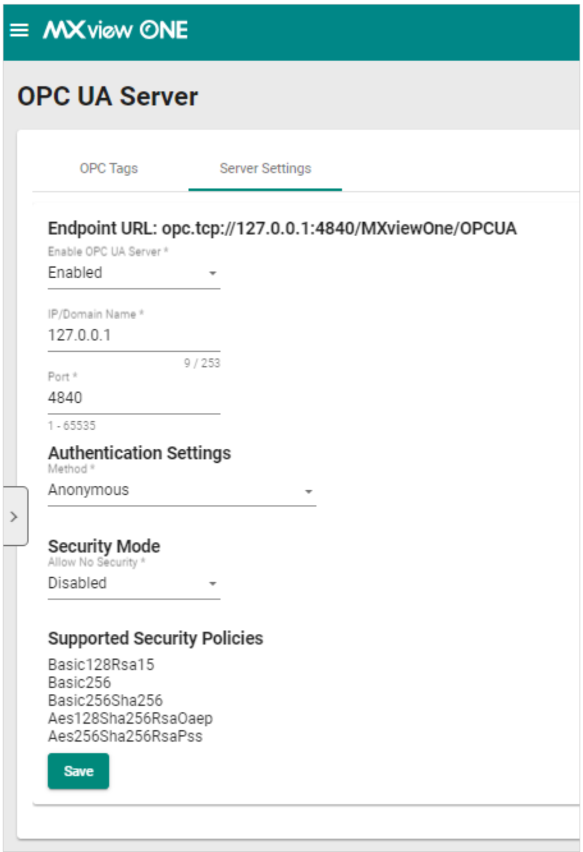


Tags deleted successfully

Configuring OPC UA Server Settings

1. Navigate to **Menu (☰) > Integration > OPC UA Server**.
   The **OPC UA Server** screen appears.
2. Go to the **Server Settings** tab.
3. Enable the OPC UA server.

4. Configure the following settings:



OPC UA Server

Endpoint URL: opc.tcp://127.0.0.1:4840/MXviewOne/OPCUA

Enable OPC UA Server *: Enabled

IP/Domain Name *: 127.0.0.1 (9 / 253)

Port *: 4840 (1 - 65535)

Authentication Settings

Method *: Anonymous

Security Mode

Allow No Security *: Disabled

Supported Security Policies

Basic128Rsa15
Basic256
Basic256Sha256
Aes128Sha256RsaOaep
Aes256Sha256RsaPss

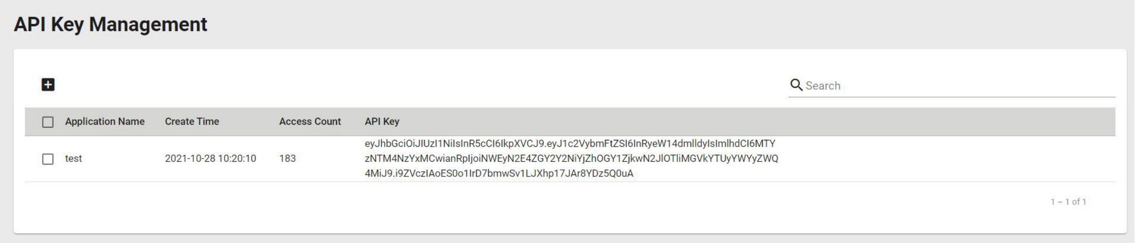
- **IP/Domain Name**: Specify the OPC UA server's IP or domain name.
- **Port**: Enter the server port.
- **Authentication Settings**: Select an authentication method.
  - **Anonymous**: OPC clients can connect to the OPC UA server anonymously without authentication.
  - **Account and Password**: Specify an account and password for OPC clients to connect to the OPC UA server (MXview One).
  - **Certificate**: Authenticate OPC clients using a certificate provided by MXview One Control Panel.
- **Allow No Security**: Enable or disable allowing no security.
  - **Disabled**: The connection requires encryption.
  - **Enabled**: The connection can be established without encryption.

5. Click **Save**.

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

Search

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

1 – 1 of 1

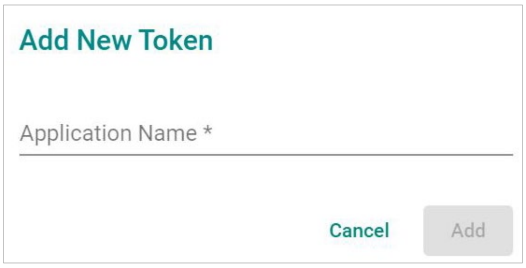
2. (Optional) Search the list of applications, type a string in the search box.

   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**.

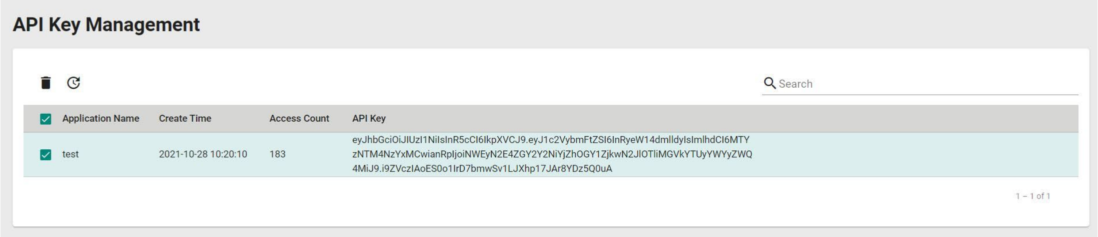
   c. Click **Add**.

      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

Search

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

1 – 1 of 1

   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.

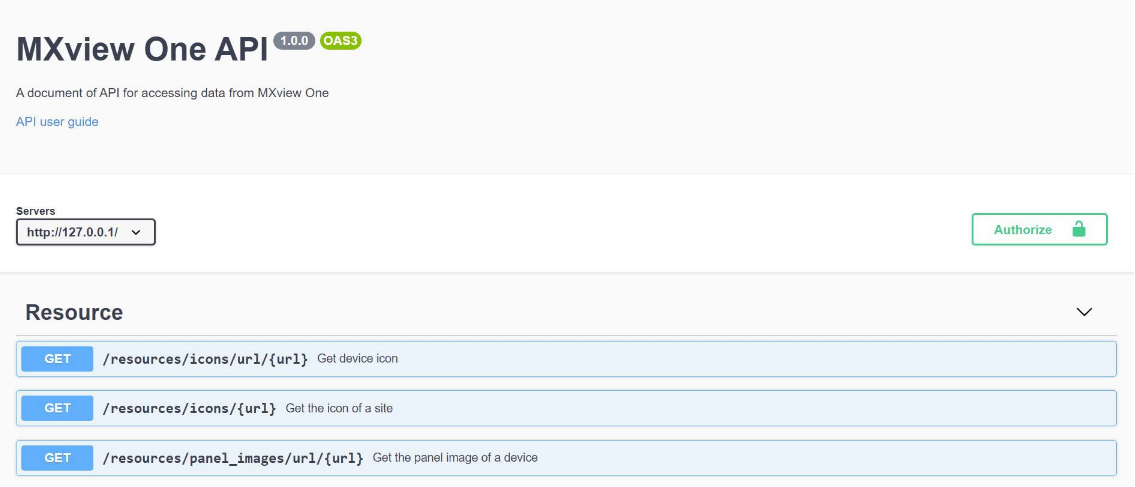
      MXview One will delete the application.

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/

   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

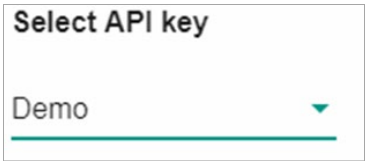
Embedding Web Widgets

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**.

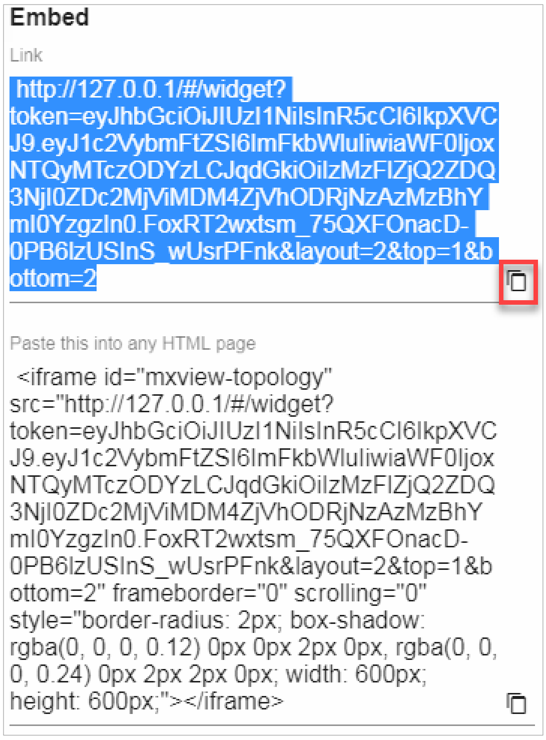
   The **Embedded Web Widget** screen will appear.

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

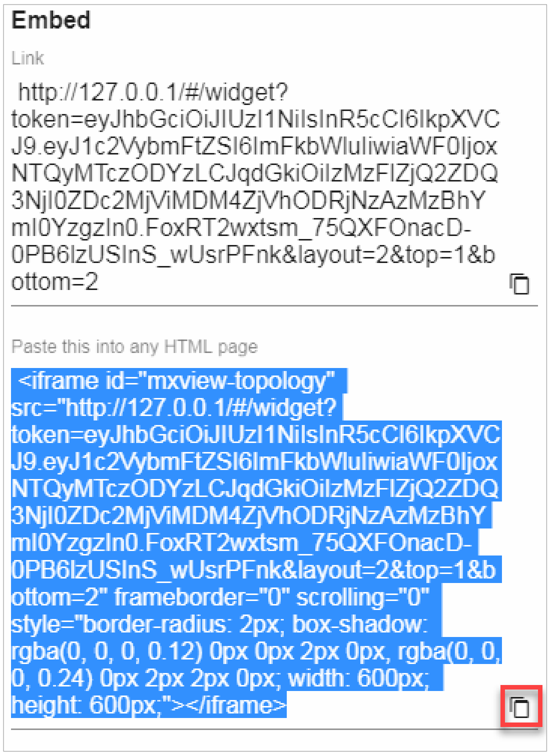
Link

```
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>
```

19. 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

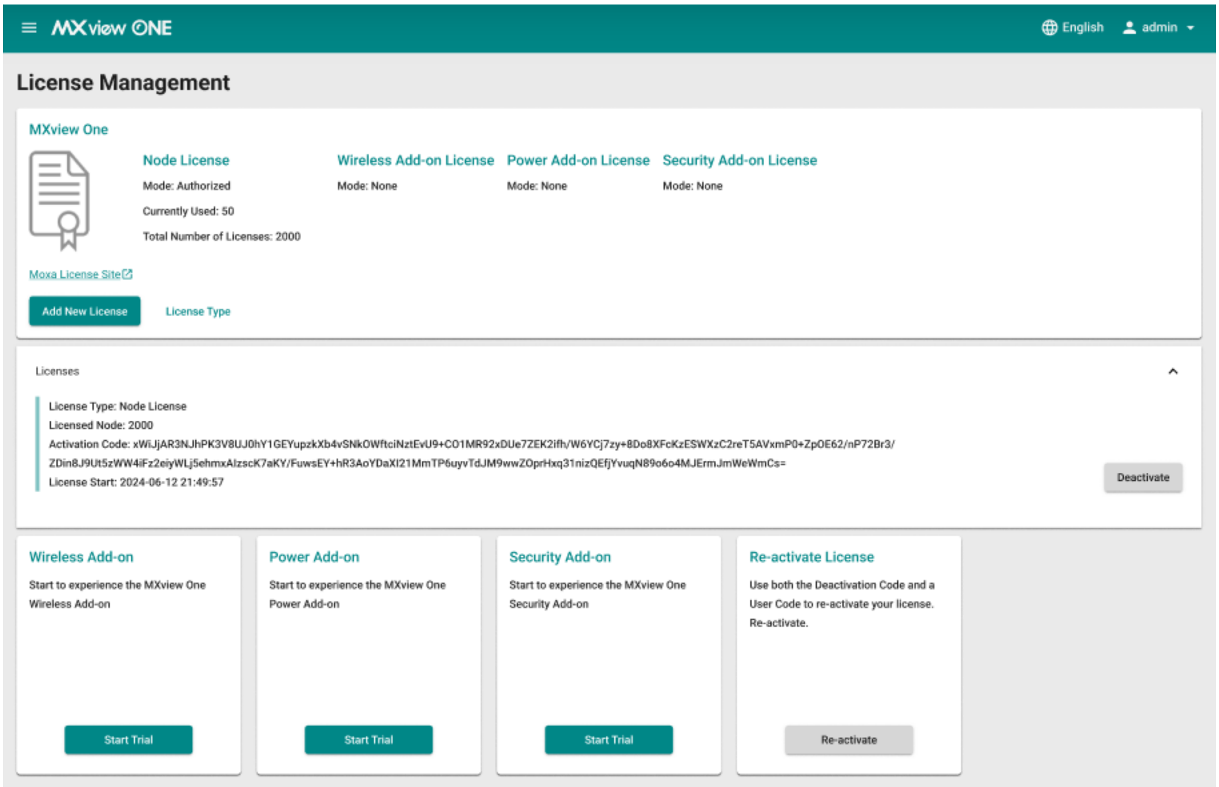
Supported Devices

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

- AWK-1131A Series (firmware v1.22 or higher)
- AWK-1137C Series (firmware v1.6 or higher)
- AWK-1151C Series (firmware v2.0 or higher)
- AWK-1161A Series (firmware v1.0 or higher)
- AWK-1161C Series (firmware v1.0 or higher)
- AWK-1165A Series (firmware v1.0 or higher)
- AWK-1165C Series (firmware v1.0 or higher)
- AWK-3131A Series (firmware v1.16 or higher)
- AWK-3252A Series (firmware v2.0 or higher)
- AWK 3262A Series (firmware v1.1 or higher)
- AWK-4131A Series (firmware v1.16 or higher)
- AWK-4252A Series (firmware v2.0 or higher)
- AWK 4262A Series (firmware v1.1 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 Add-on 90-Day free trial through the license management page.



License Management

MXview One

Node License
Mode: Authorized
Currently Used: 50
Total Number of Licenses: 2000

Wireless Add-on License
Mode: None

Power Add-on License
Mode: None

Security Add-on License
Mode: None

Licenses

License Type: Node License
Licensed Node: 2000
Activation Code: xWiJjAR3NJhPK3V8UJ0hY1GEYupzkXb4vSNkOWftciNztEvU9+CO1MR92xDUe7ZEK2ifh/W6YCj7zy+8Do8XFcKzESWXzC2reT5AVxmP0+ZpOE62/nP72Br3/ZDin8J9Ut5zWW4iFz2eiyWLj5ehmxAlzscK7aKY/FuwsEY+hR3AoYDaXI21MmTP6uyvTdJM9wwZOprHxq31nizQEfjYvuqN89o6o4MJErmJmWeWmCs=
License Start: 2024-06-12 21:49:57

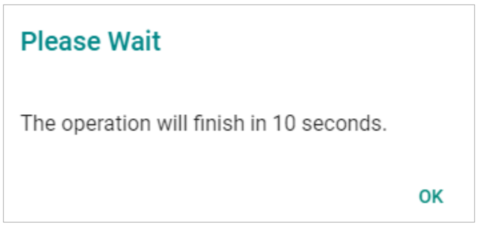
Wireless Add-on
Start to experience the MXview One Wireless Add-on

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

Security Add-on
Start to experience the MXview One Security Add-on

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

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



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 include a **Wireless** tab and show AP Traffic Load and the Wireless Device Summary information.

To access the **Dashboard**, navigate to **Menu** (☰) **> Dashboard** and go to the **Wireless** tab.

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.

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

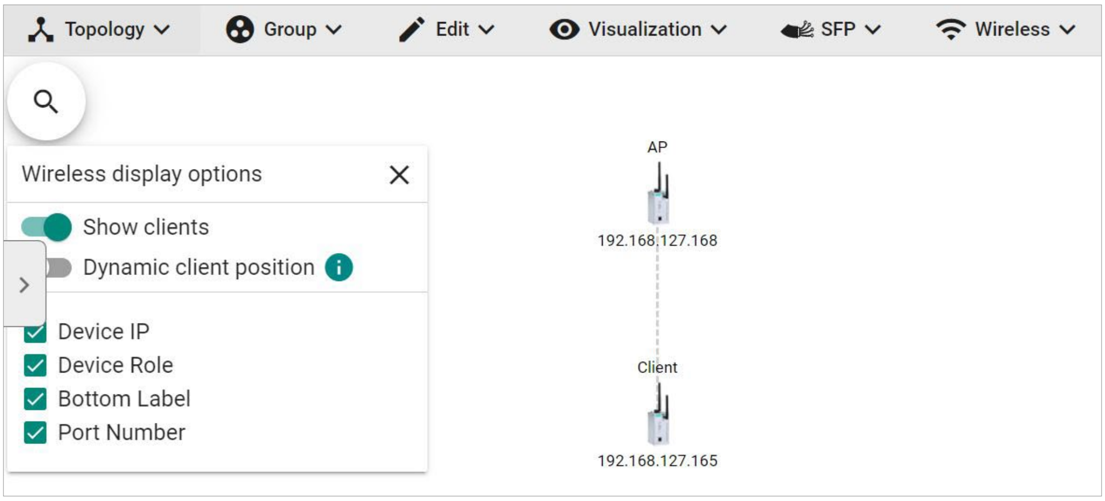
Dynamic Wireless Client Roaming

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

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

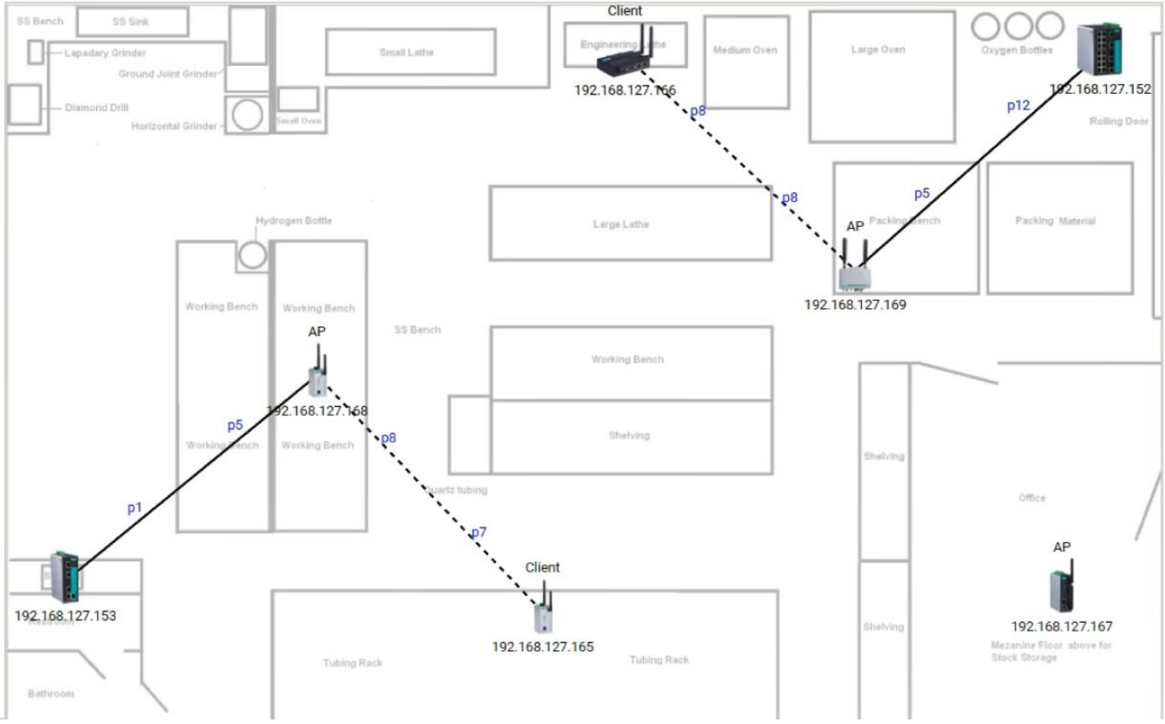
Refer to the table below for a description of each display option.

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

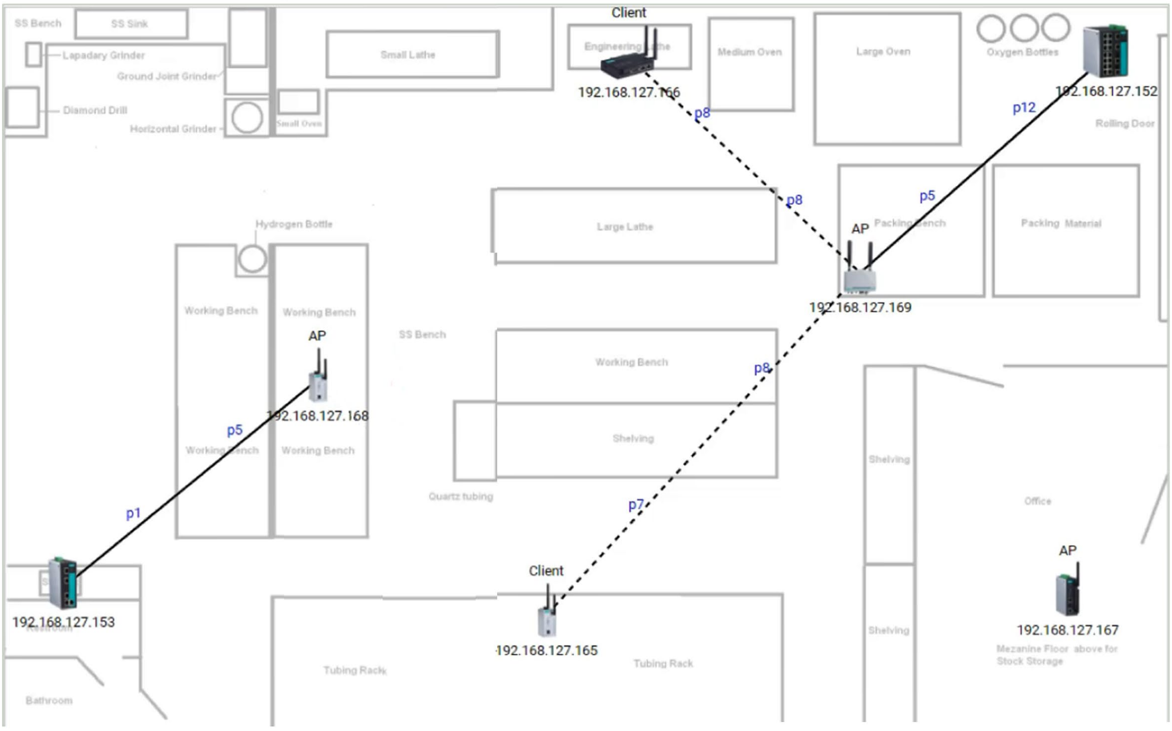


The following diagrams are an example of the dynamic roaming display showing dynamic client-AP link changes.

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



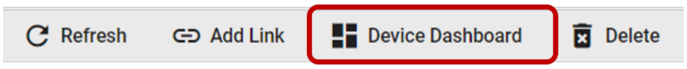
When the client roams to another AP, MXview One will automatically redraw the link to the new AP on the wireless topology diagram.



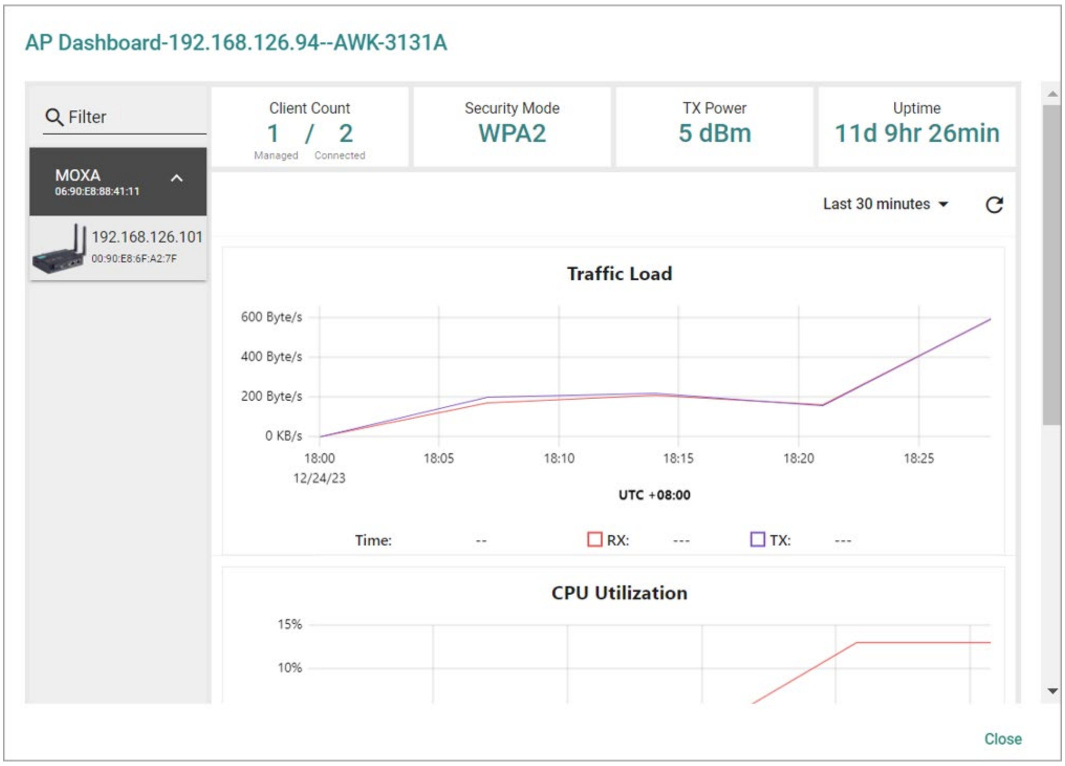
AP/Client Device Dashboard

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

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



AP Device Dashboard


AP Dashboard-192.168.126.94--AWK-3131A

Client Count: 1 / 2 (Managed / Connected)

Security Mode: WPA2

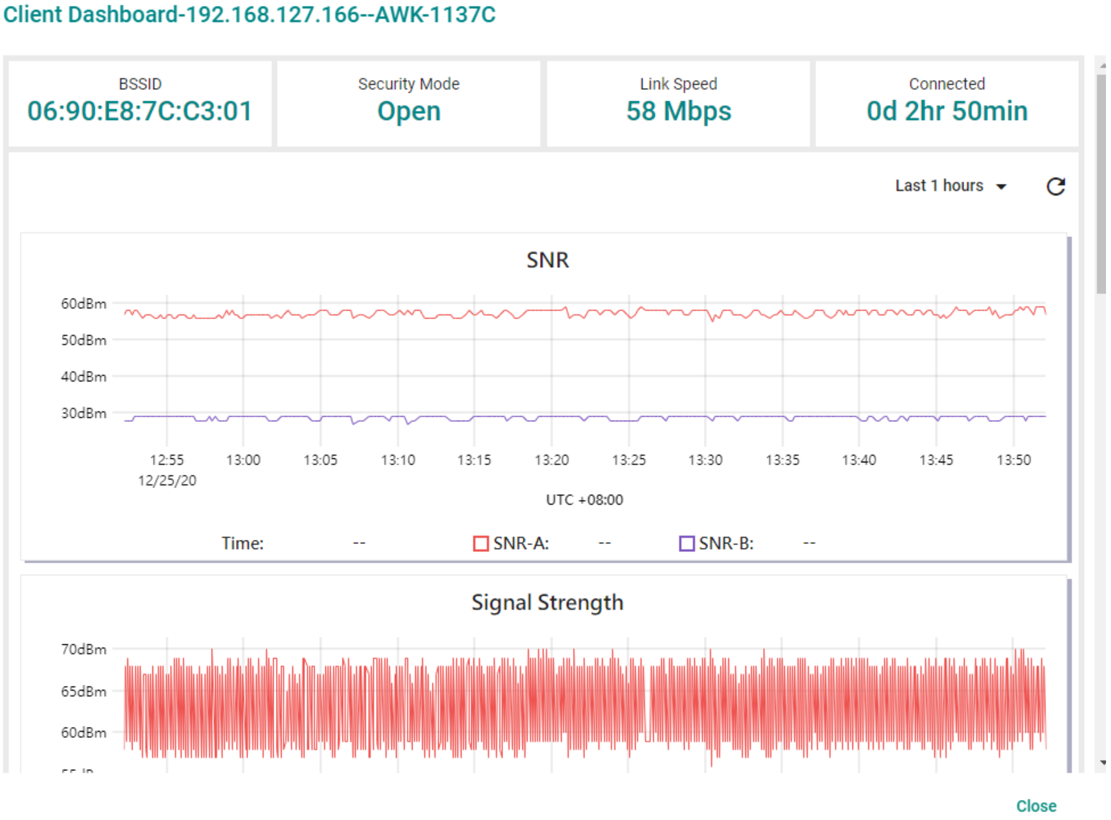
TX Power: 5 dBm

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

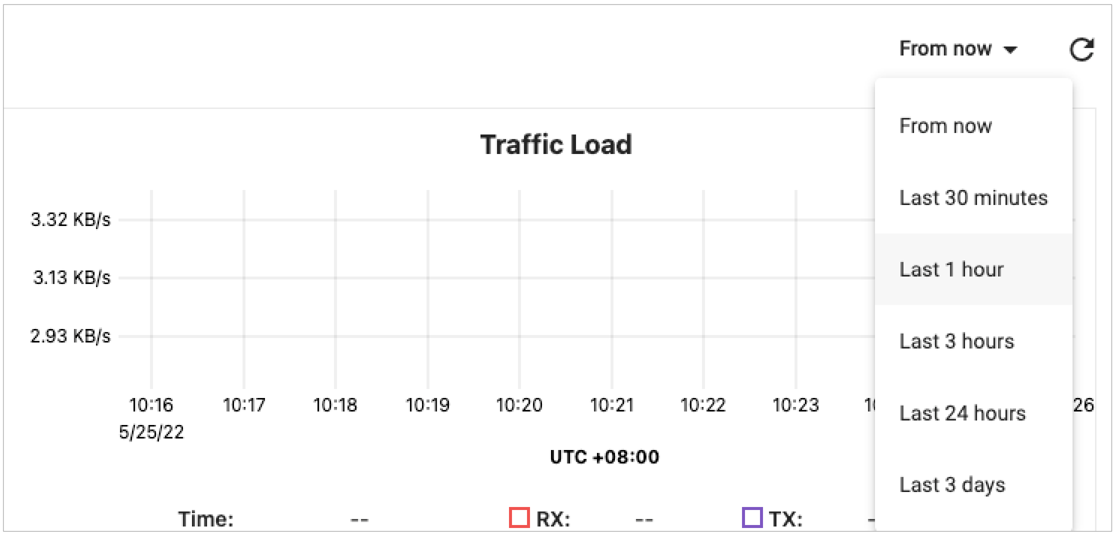
Link Speed
58 Mbps

Connected
0d 2hr 50min

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.

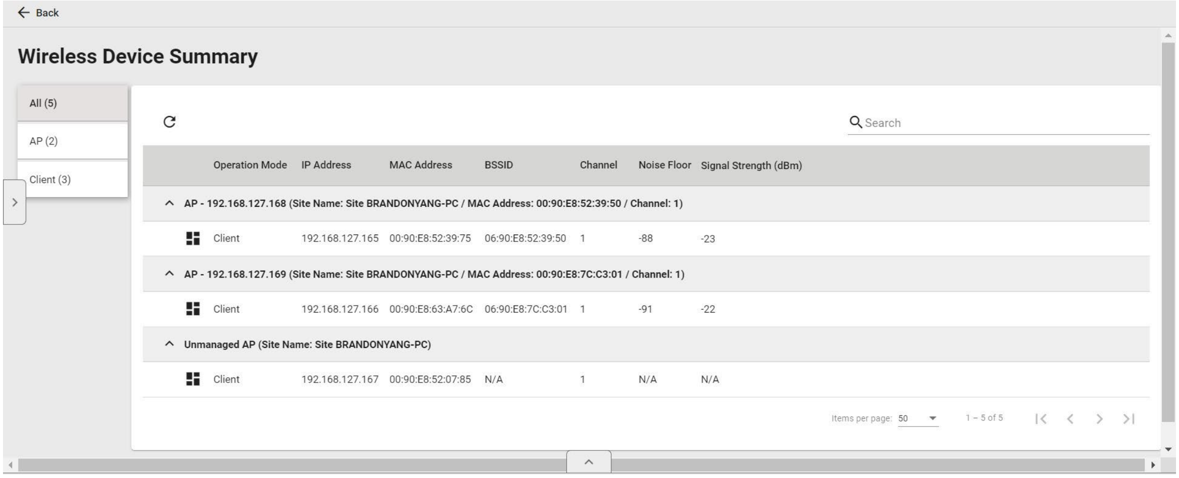


Wireless Device Summary

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.



Wireless Device Summary

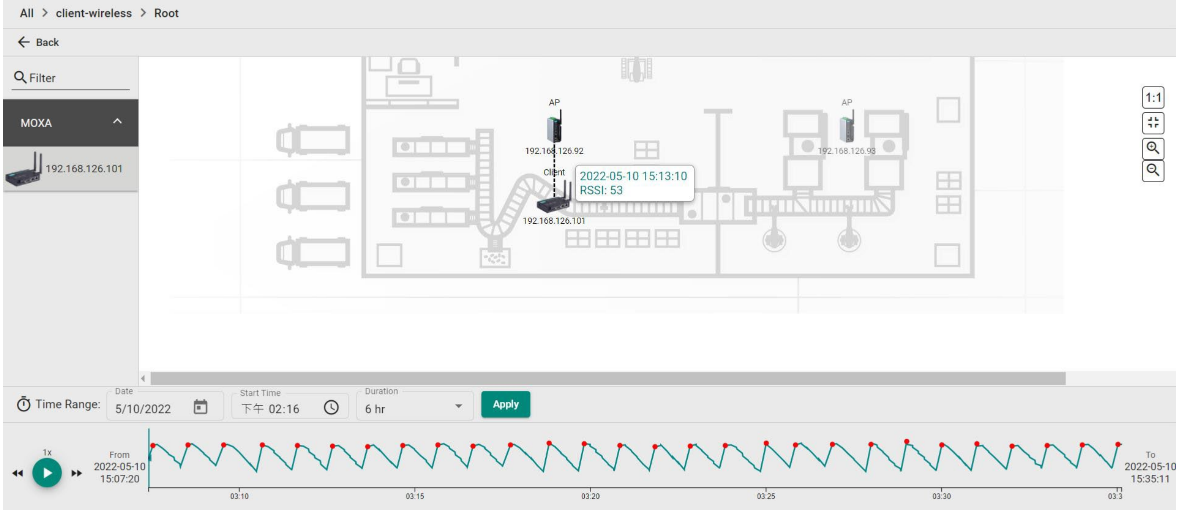
Operation Mode	IP Address	MAC Address	BSSID	Channel	Noise Floor	Signal Strength (dBm)
AP - 192.168.127.168 (Site Name: Site BRANDONYANG-PC / MAC Address: 00:90:E8:52:39:50 / Channel: 1)						
Client	192.168.127.165	00:90:E8:52:39:75	06:90:E8:52:39:50	1	-88	-23
AP - 192.168.127.169 (Site Name: Site BRANDONYANG-PC / 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.



2022-05-10 15:13:10
RSSI: 53

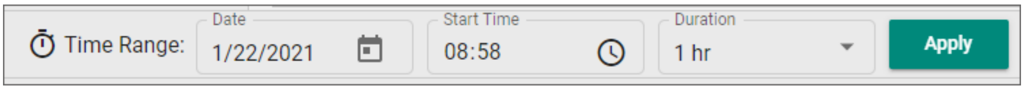
Time Range: Date 5/10/2022 Start Time 下午 02:16 Duration 6 hr

From 2022-05-10 15:07:20

To 2022-05-10 15:35:11

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**.

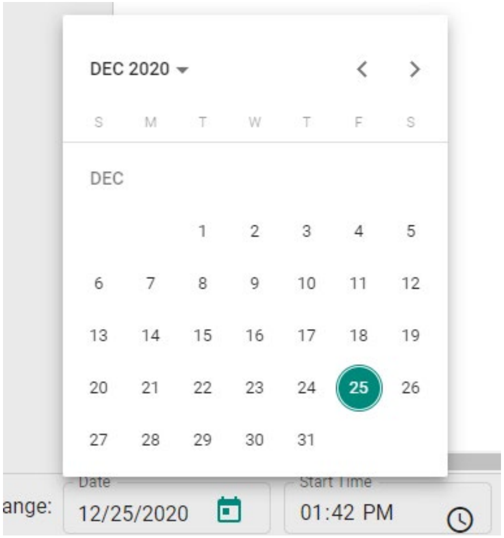


Time Range:

Date: 1/22/2021

Start Time: 08:58

Duration: 1 hr



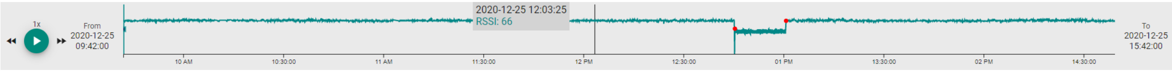
DEC 2020

S	M	T	W	T	F	S
DEC						
		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.



20. 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.

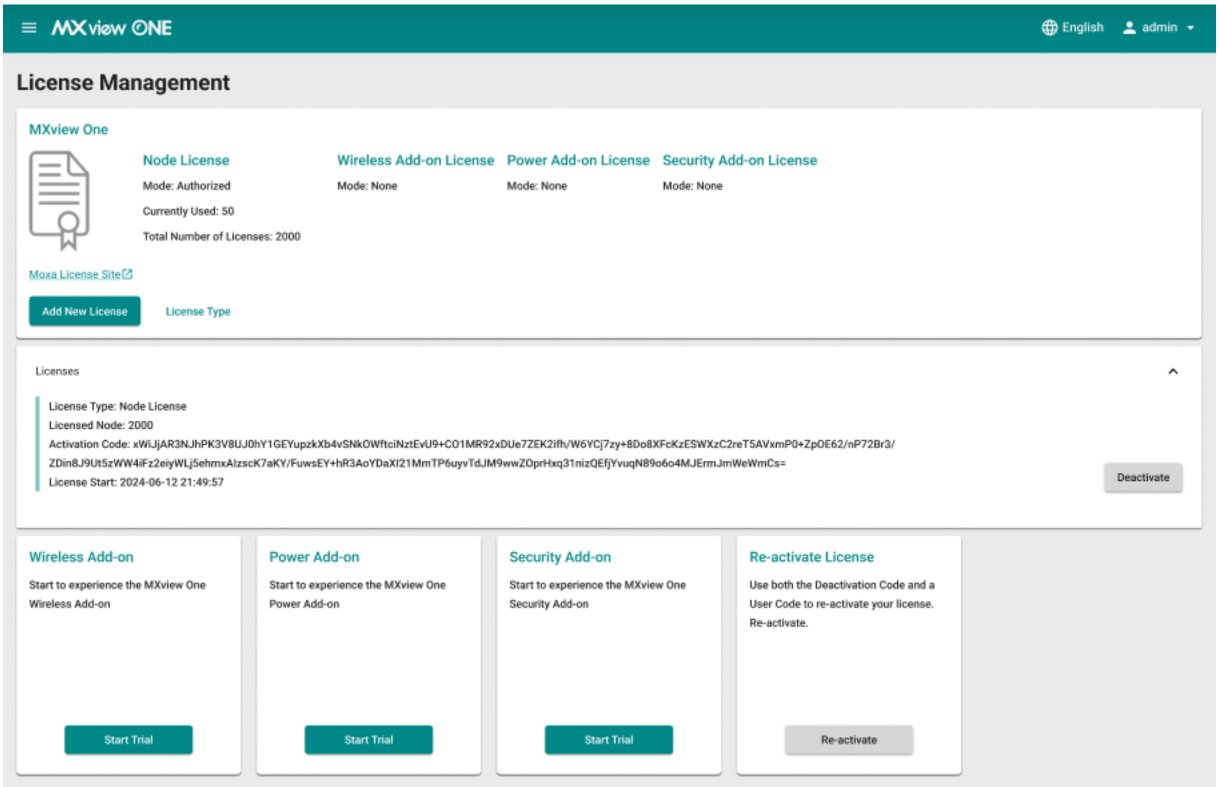
Supported Devices With PRP/HSR Features

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 with LM-7000H-2GPHR modules (firmware v6.2 or higher)
- DA-820C Series and DN-PRP-HSR-I210 or DA-PRP-HSR-I210 (OS Win 10 or higher)
- MDS-G4000 Series (L2 models only) with LM-7000H-2GPHR modules (firmware v5.0 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 Add-on 90-day free version through the License Management page.



License Management

MXview One

Node License
Mode: Authorized
Currently Used: 50
Total Number of Licenses: 2000

Wireless Add-on License
Mode: None

Power Add-on License
Mode: None

Security Add-on License
Mode: None

Licenses

License Type: Node License
Licensed Node: 2000
Activation Code: xWiJjAR3NJhPK3V8UJ0hY1GEYupzkXb4vSNkOWftciNztEvU9+CO1MR92xDUe7ZEK2ifh/W6YCj7zy+8Do8XFcKzESWXzC2reT5AVxmP0+ZpOE62/nP72Br3/ZDin8J9Ut5zWW4iFz2eiyWLj5ehmxAlzscK7aKY/FuwsEY+hR3AoYDaXI21MmTP6uyvTdJM9wwZOprHxq31nizQEfjYvuqN89o6o4MJErmJmWeWmCs=
License Start: 2024-06-12 21:49:57

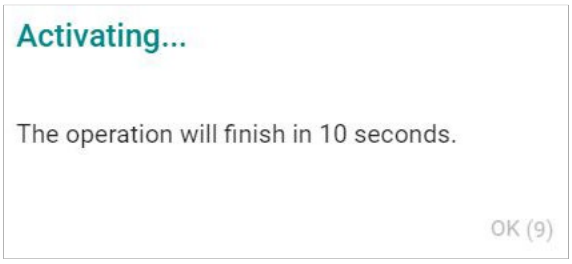
Wireless Add-on
Start to experience the MXview One Wireless Add-on

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

Security Add-on
Start to experience the MXview One Security Add-on

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

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



Activating...

The operation will finish in 10 seconds.

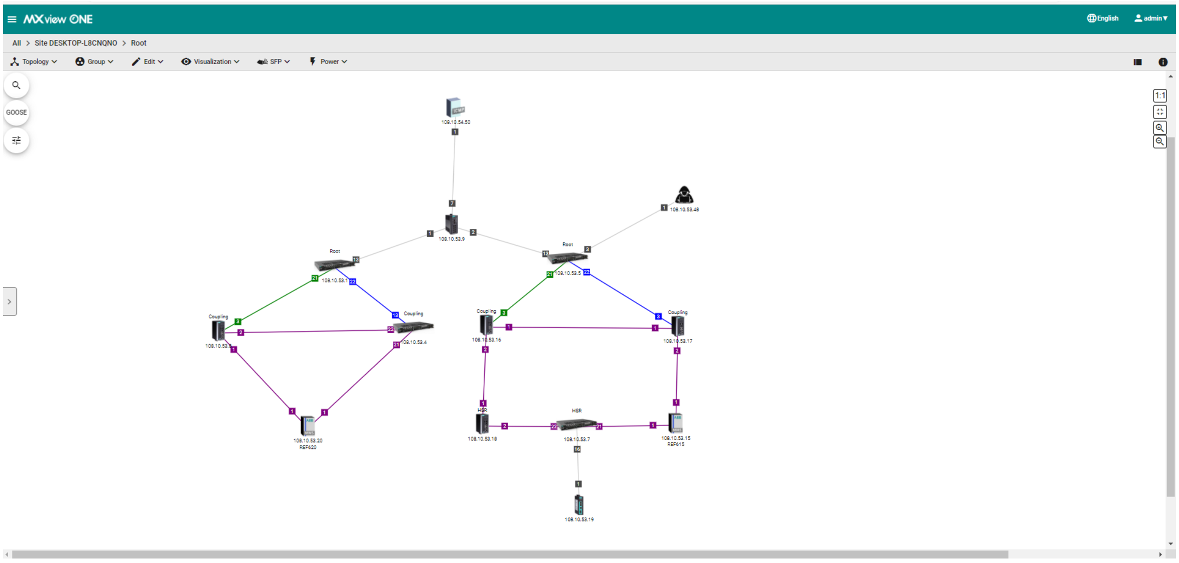
- For detailed information on how to activate the MXview Power Add-on Module, refer to **Chapter 4: License Management**.
- To add power devices to your MXview One network, refer to **Using Device Discovery**.

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.

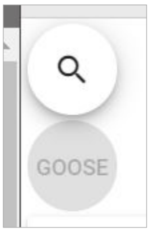


Topology

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

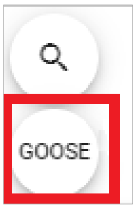
GOOSE panel

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

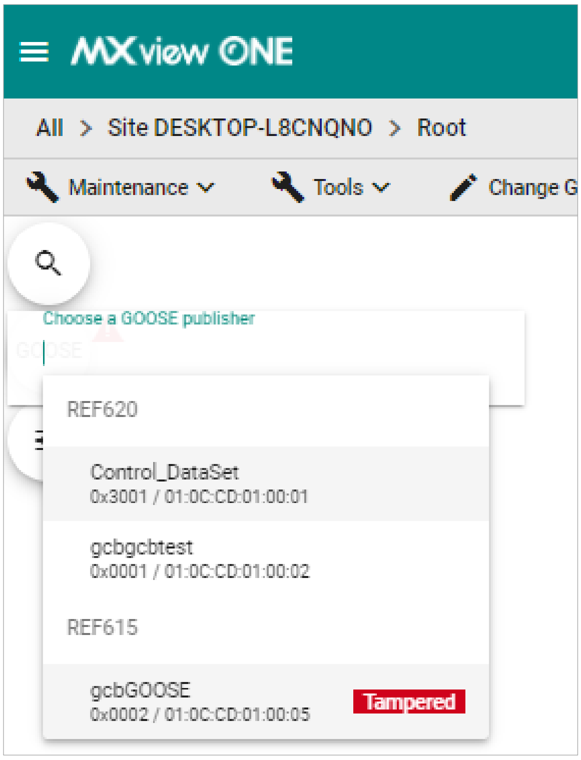


2. Once you have imported the SCD file via **Power > Import SCD**, you can find the IED as a GOOSE publisher identity via the GOOSE panel.

   a. Click **GOOSE panel**.

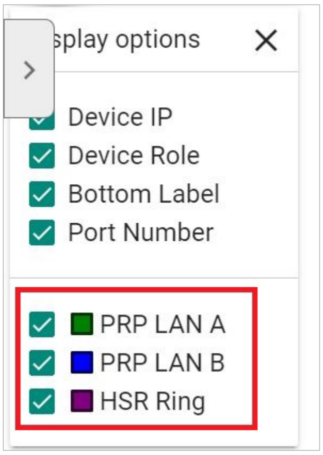


b. Scroll down or type the GOOSE-related information, such as IED name or GoCB name.



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

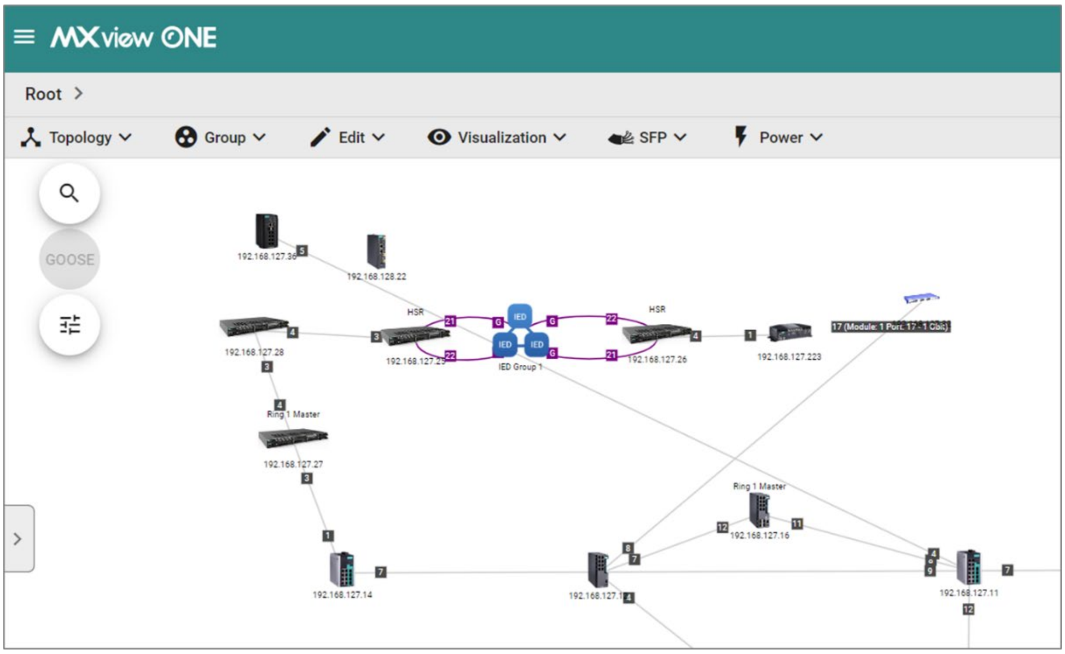
PRP LAN A is represented by a green line, PRP LAN B by a blue line, and HSR Ring by a purple line.

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

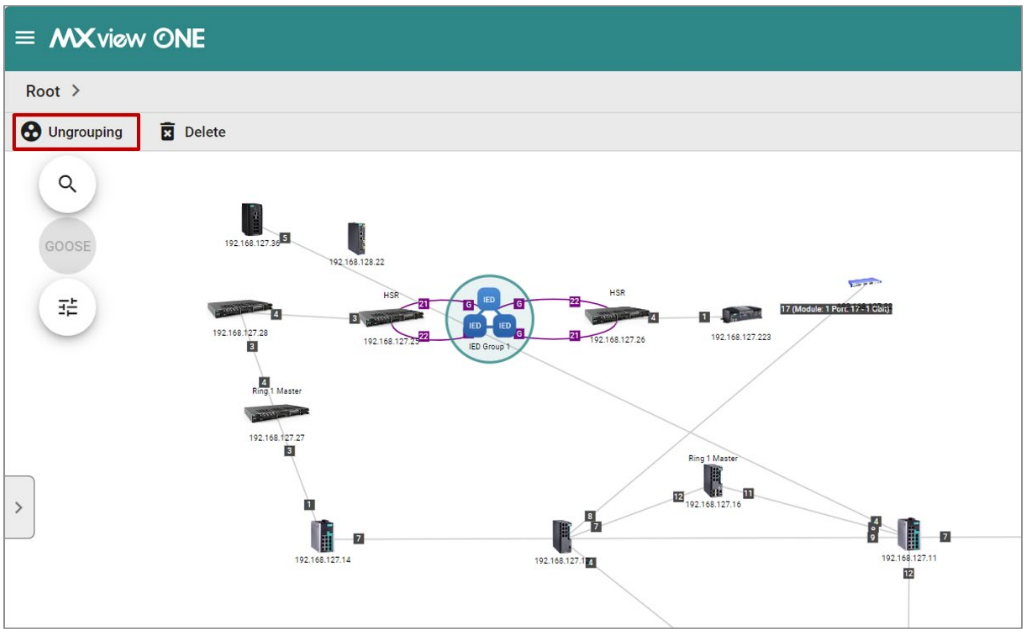
After executing the **Auto Topology** function, MXview One will automatically group the IEDs within the same HSR ring into an IED Group and represent the HSR link with a purple line. If you want to display the IEDs within the Root group or display GOOSE Message information in the topology, you can use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



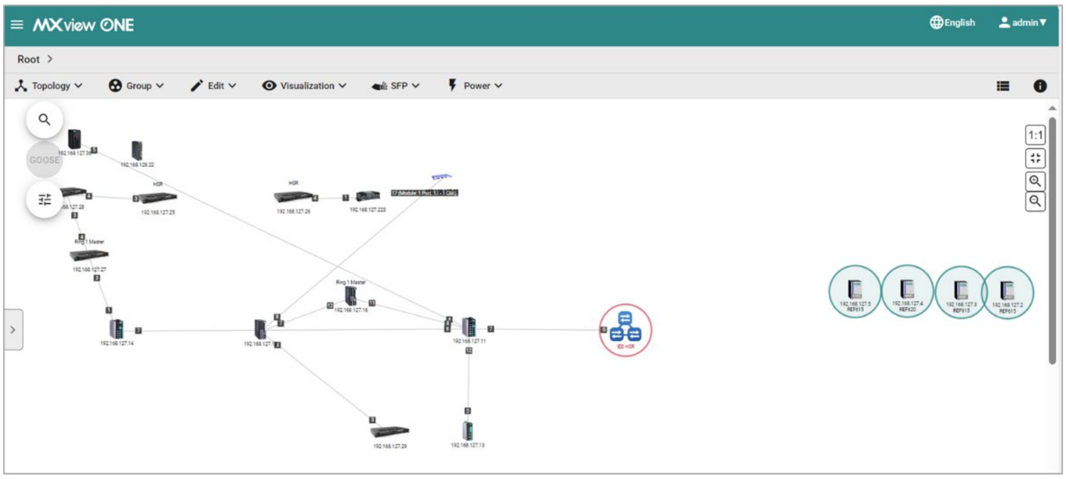
1. Navigate to **Menu** (☰) **> Topology**

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

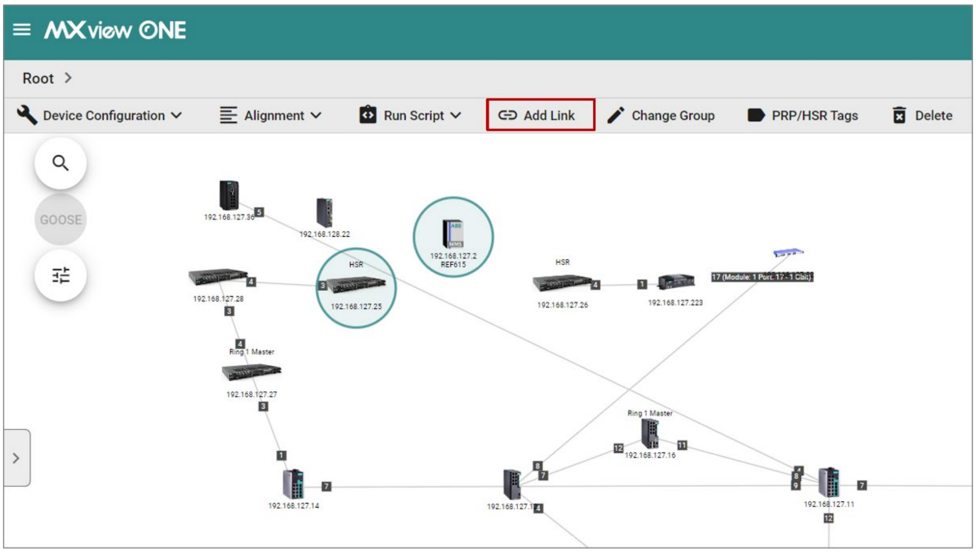
2. Click on the IED group in the topology that you want to ungroup.
3. Click **Ungrouping**.



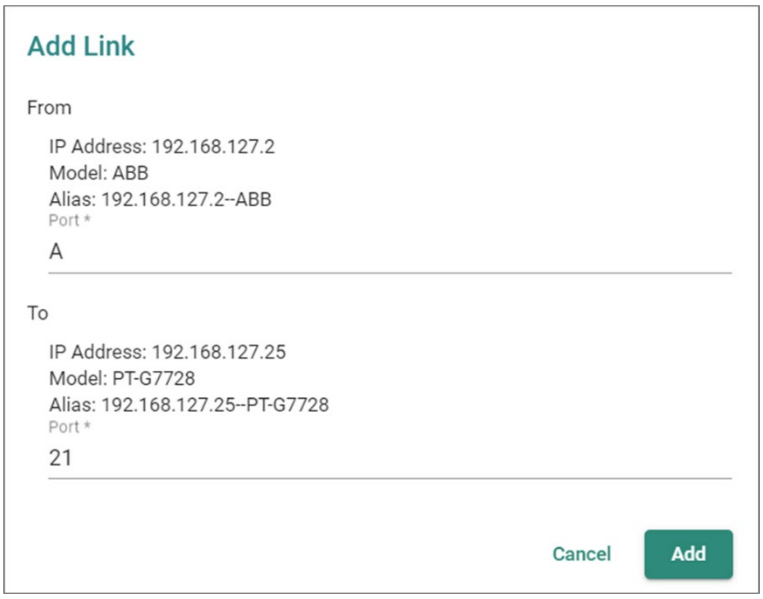
4. After ungrouping an IED group, the individual IEDs will be shown on the right-hand side of the topology.



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

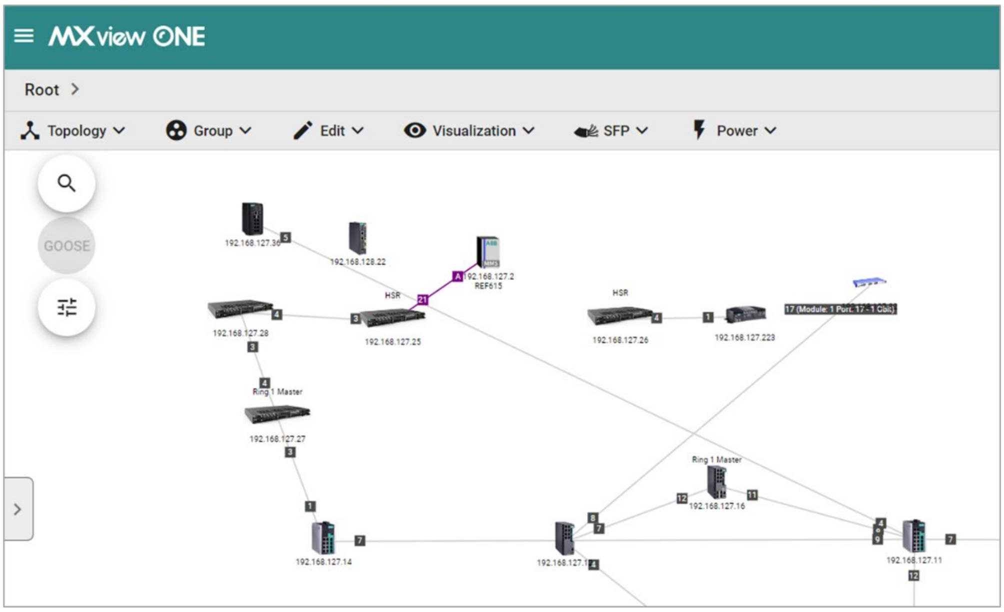
From

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.

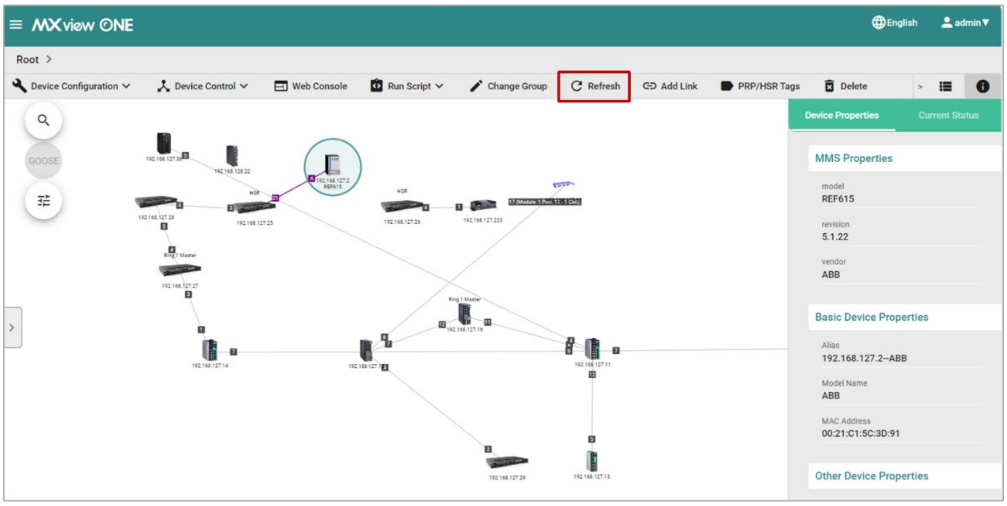


e. Repeat this process for any other remaining IED connections.

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.



model
REF615

revision
5.1.22

vendor
ABB

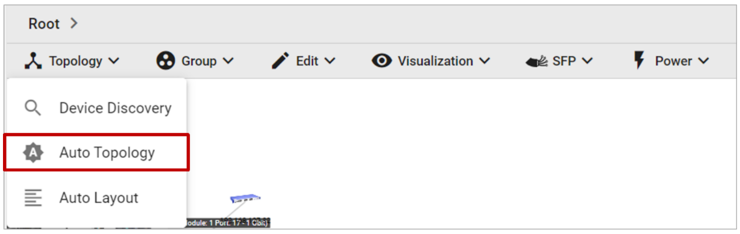
Alias
192.168.127.2--ABB

Model Name
ABB

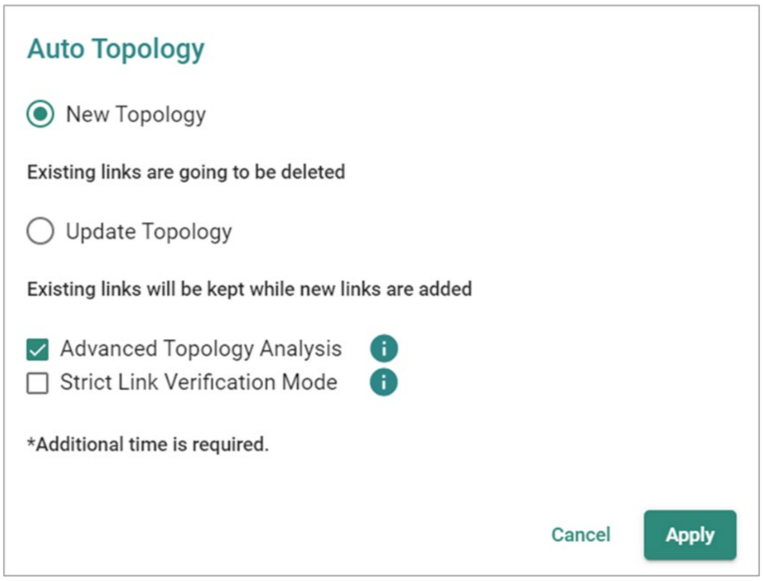
MAC Address
00:21:C1:5C:3D:91

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.

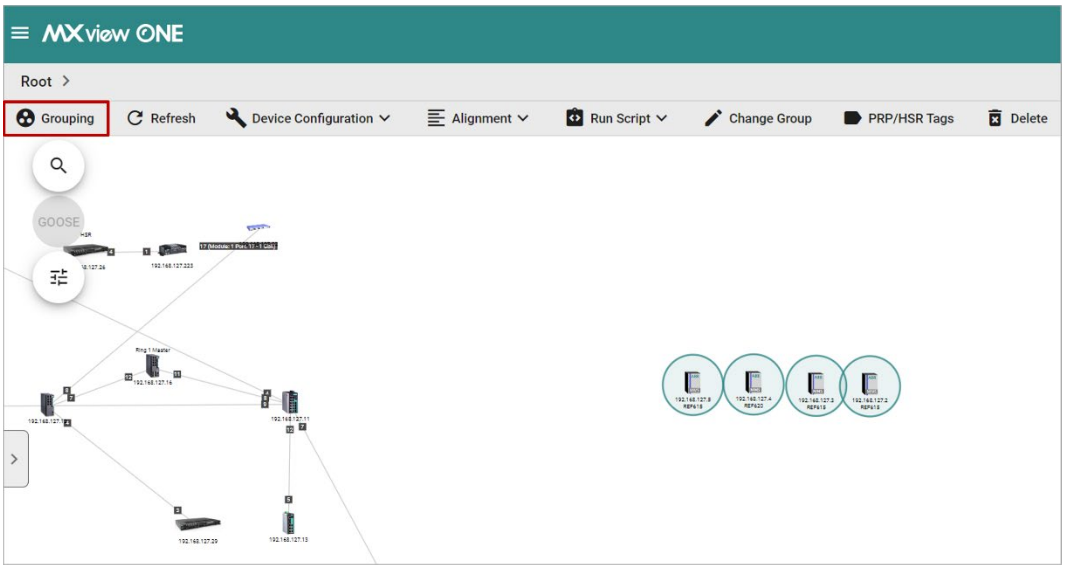
NOTE

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.

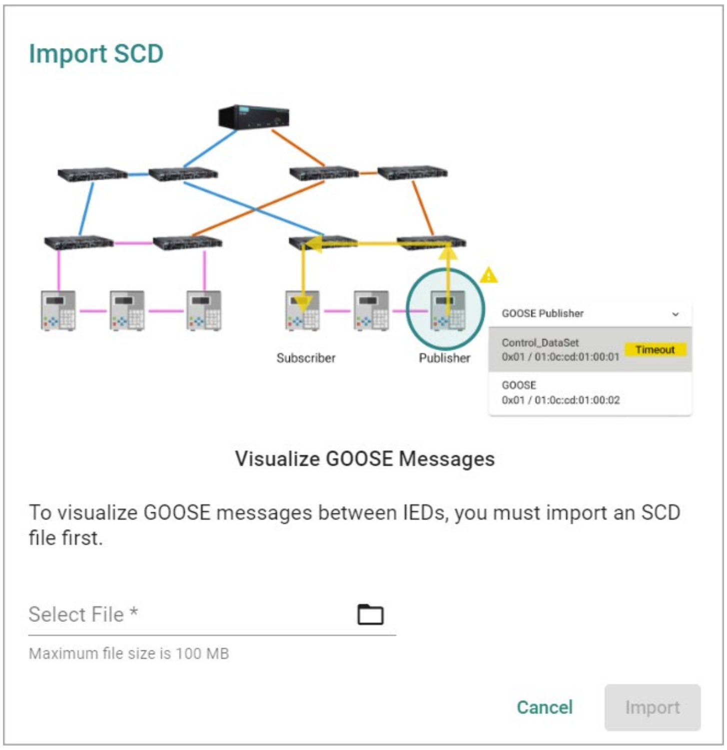
1. Navigate to **Menu** (☰) **> Topology**

   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

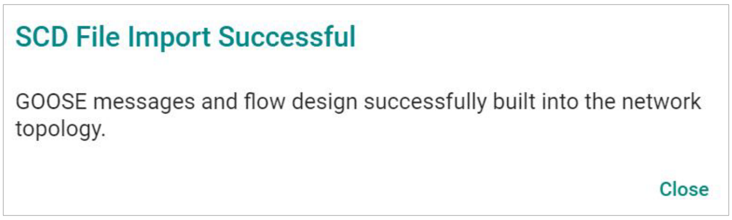
Cancel Import

   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.

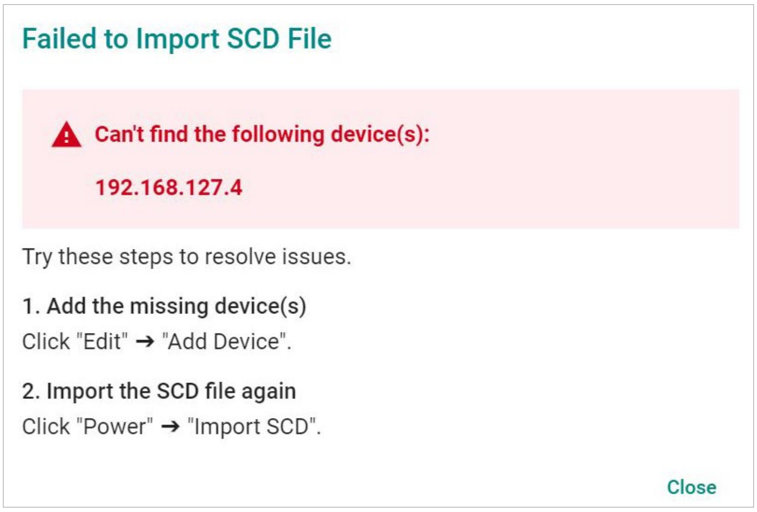


SCD File Import Successful

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".

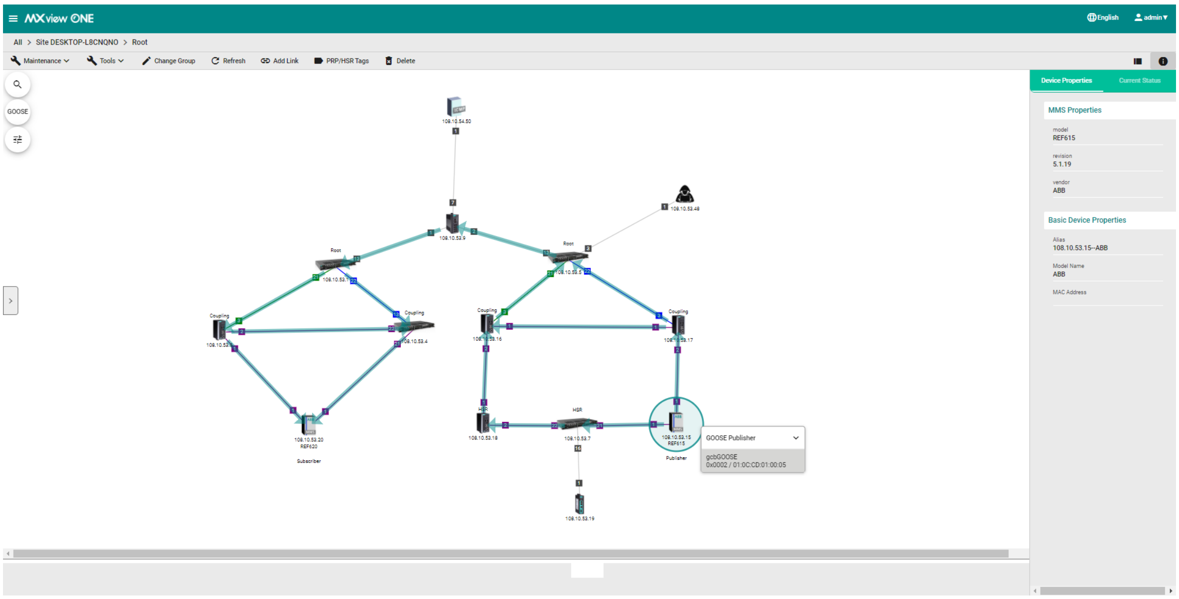
Close

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.



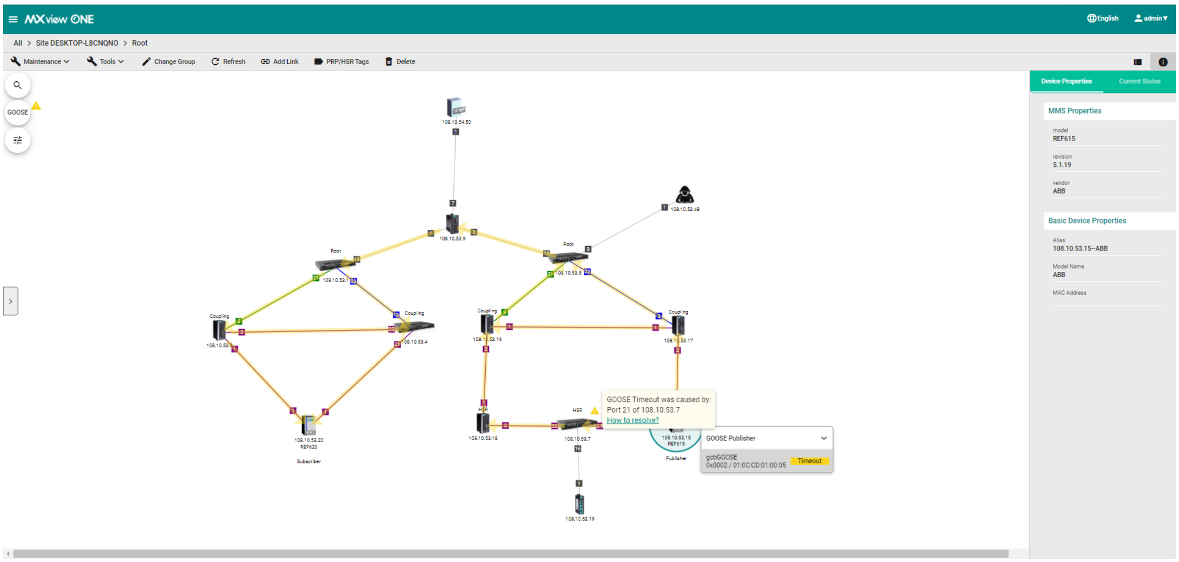
GOOSE Publisher
gcbGOOSE
0x0002 / 01:0C:CD:01:00:05

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.



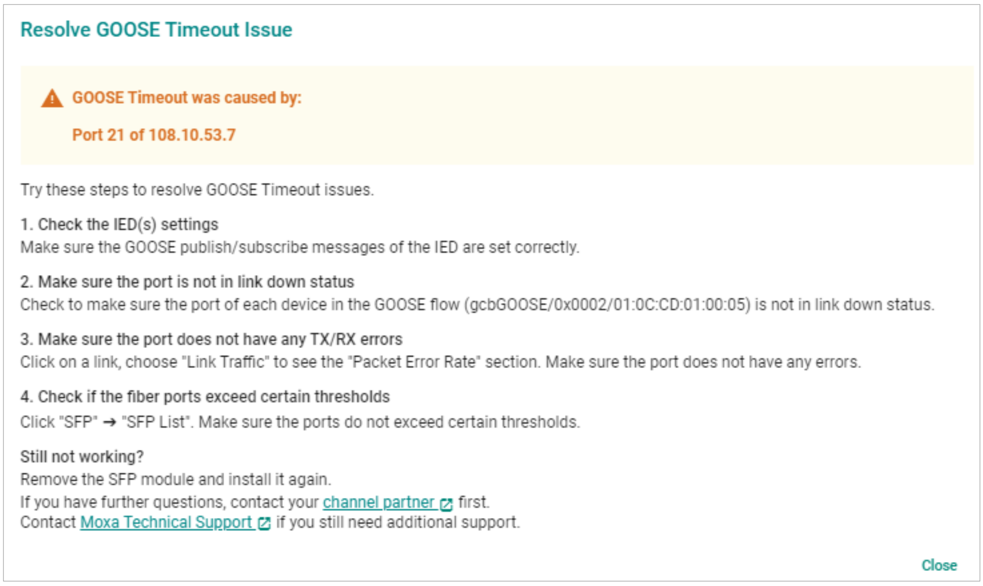
GOOSE Timeout was caused by:
Port 21 of 108.10.53.7
How to resolve?

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.

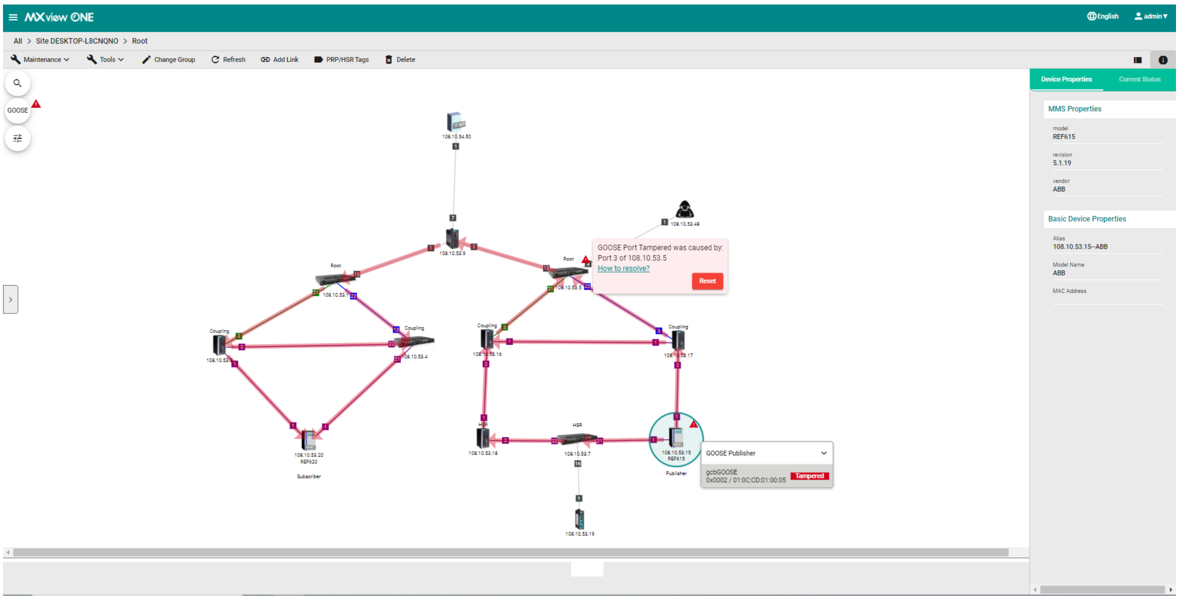
Still not working?
Remove the SFP module and install it again.
If you have further questions, contact your channel partner first.
Contact Moxa Technical Support if you still need additional support.

Close

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.



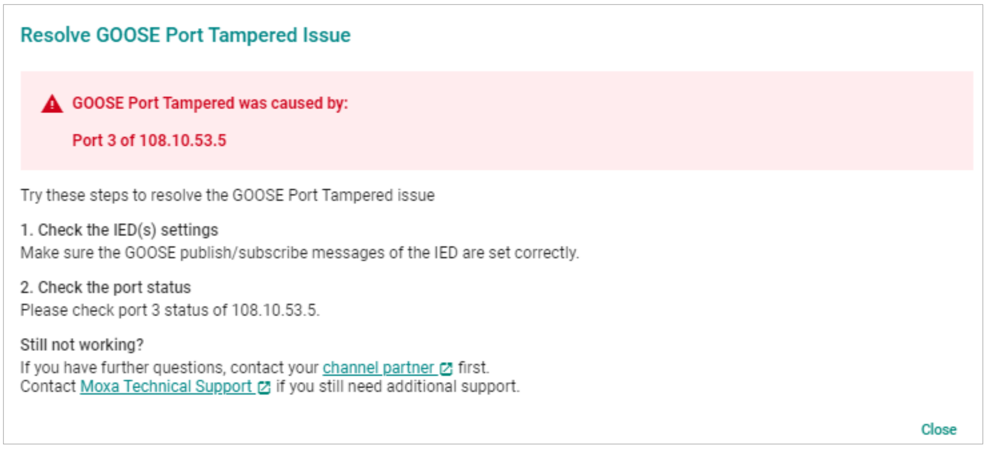
GOOSE Port Tampered was caused by:
Port 3 of 108.10.53.5
How to resolve?
Reset

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

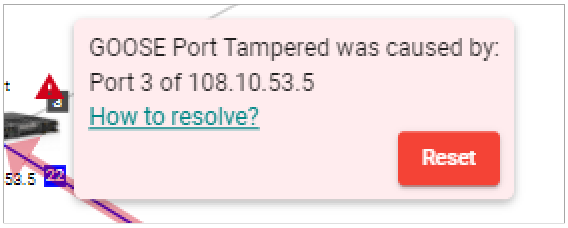
1. Check the IED(s) settings
Make sure the GOOSE publish/subscribe messages of the IED are set correctly.

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

21. Security 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 Security Add-on Module provides a set of features to help you easily monitor and manage the overall cybersecurity condition of your network. The add-on enables you to manage and deploy firewall policy rules and security packages to multiple devices simultaneously. Through the security dashboard featuring statistical charts, users can get important information at a glance and take necessary actions.

Additionally, the Security module instantly notifies you of any security-related issues on your network, enabling quick and easy troubleshooting.

System Requirements

The computer that the MXview Security 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.

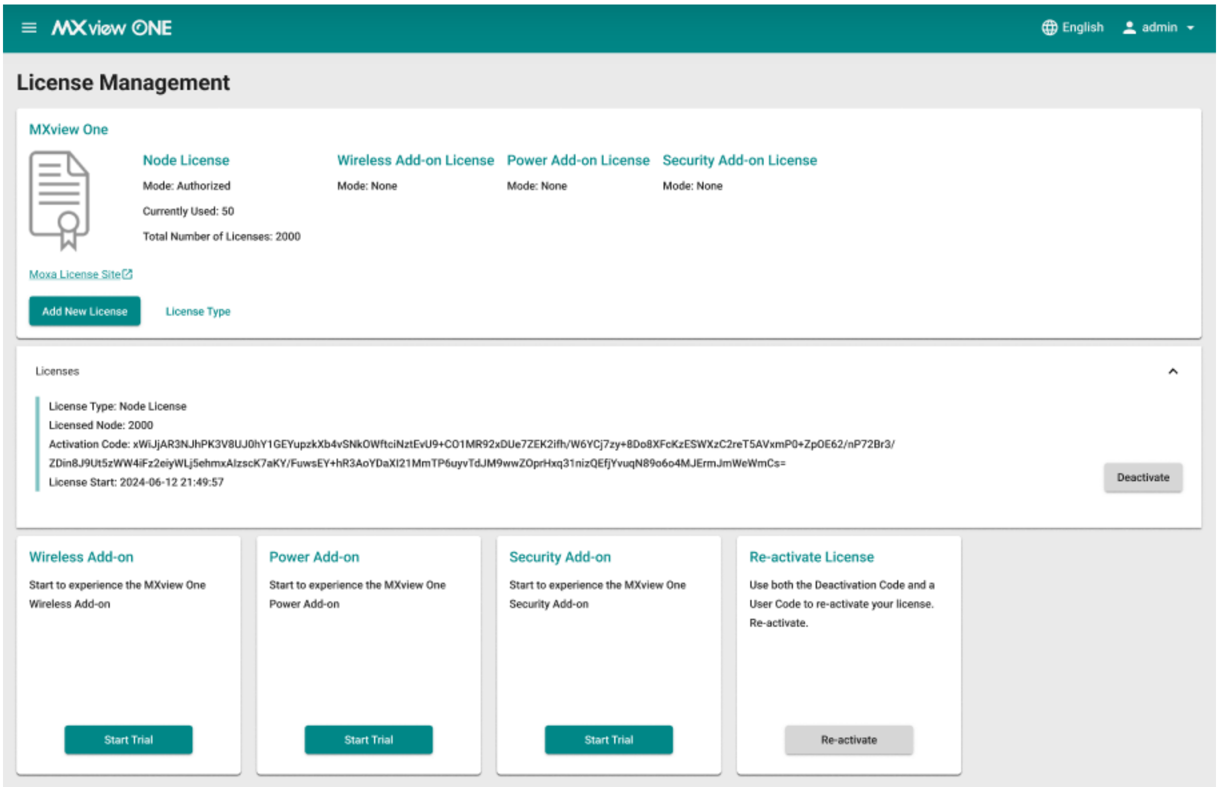
Supported Devices

The MXview Security Add-on Module supports the following devices:

- EDR-8010 Series
- EDR-G9004 Series
- EDR-G9010 Series
- EDF-G1002-BP Series
- TN-4900 Series

Getting Started With the Security Add-on Module

In order to use the MXview Security Add-on module, you will need to activate it first. You can choose to activate a new license or enable the Security Add-on 90-day free version through the License Management page.



License Management

MXview One

Node License
Mode: Authorized
Currently Used: 50
Total Number of Licenses: 2000

Wireless Add-on License
Mode: None

Power Add-on License
Mode: None

Security Add-on License
Mode: None

Licenses

License Type: Node License
Licensed Node: 2000
Activation Code: xWiJjAR3NJhPK3V8UJ0hY1GEYupzkXb4vSNkOWftciNztEvU9+CO1MR92xDUe7ZEK2ifh/W6YCj7zy+8Do8XFcKzESWXzC2reT5AVxmP0+Zp0E62/nP72Br3/ZDin8J9Ut5zWW4iFz2eiyWLj5ehmxAIzscK7aKY/FuwsEY+hR3AoYDaXI21MmTP6uyvTdJM9wwZOprHxq31nizQEfjYvuqN89o6o4MJErmJmWeWmCs=
License Start: 2024-06-12 21:49:57

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

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

Security Add-on
Start to experience the MXview One Security Add-on

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

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

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

NOTE

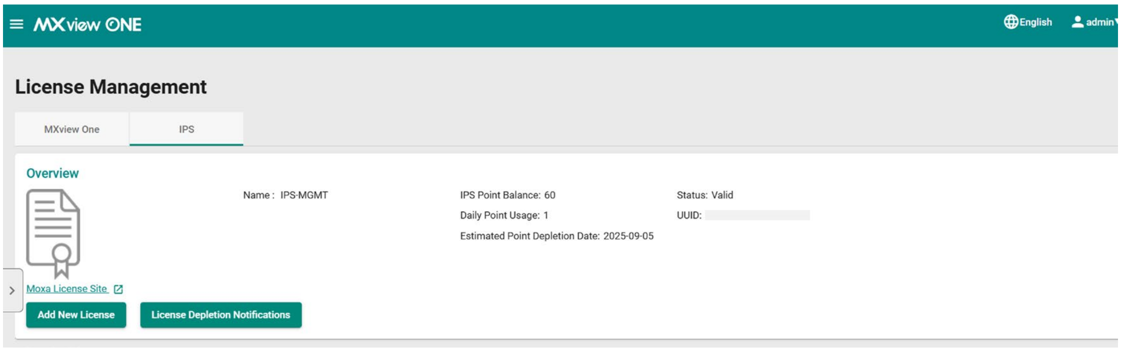
Please activate the Node-based License and then the Security Add-on License.

IPS License Management

After successfully enabling a Security Add-on license, an additional **IPS** tab will become available on the **License Management** page. From this tab, users can view IPS license information and manage IPS license allocation.

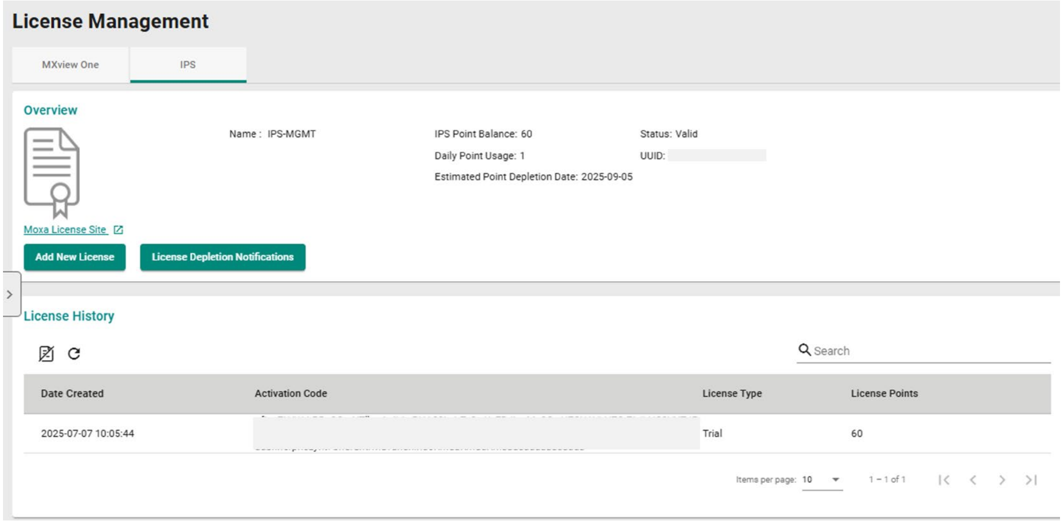
IPS licenses are point-based. The combined total of all IPS license points is added to the available IPS Point Balance.

Each device with a registered IPS license will consume one IPS license point per day. The Daily Point Usage indicates the combined number of IPS license points that will be deducted from the IPS Point Balance per day.



Viewing IPS License Information

1. Navigate to **Menu** (☰) **> Administration > License Management**.
2. Go to the **IPS** tab.



Date Created	Activation Code	License Type	License Points
2025-07-07 10:05:44	[redacted]	Trial	60

The **Overview** section shows the following information:

Field	Description
Name	The name of the license.
IPS Point Balance	The available IPS license points. This is the total combined points of all active IPS licenses.
Daily Point Usage	The number of points consumed per day by IPS-registered devices.
Estimated Point Depletion Date	The estimated date that the points will be depleted. This estimate is based on the available IPS points and daily IPS point usage.
Status	The status of the license.
UUID	The unique ID of this instance.

The **License History** section shows the following information:

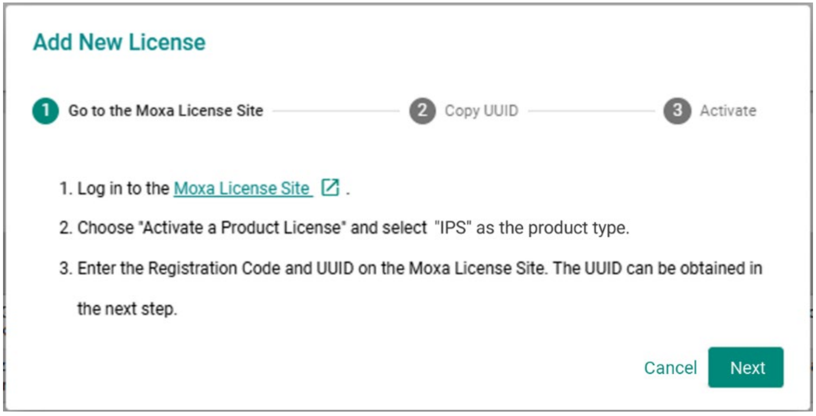
Field	Description
Date Created	The date of this license was added.
Activation Code	The activation code of the license.
License Type	The type of license.
License Points	The number of IPS points on the license.

Adding an IPS License

Adding an IPS license requires a valid license activation code.

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

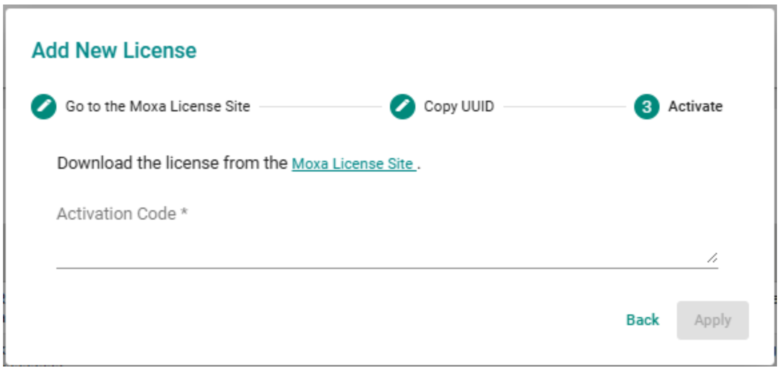
2. Click **Add New License**.
   The **Add New License** screen will appear.



Add New License

1. Log in to the Moxa License Site .
2. Choose "Activate a Product License" and select "IPS" as the product type.
3. Enter the Registration Code and UUID on the Moxa License Site. The UUID can be obtained in the next step.

3. Follow the on-screen instructions for activating the license on the Moxa License Site.
4. Enter the activation code provided by the Moxa License Site into MXview One.



Add New License

Download the license from the Moxa License Site .

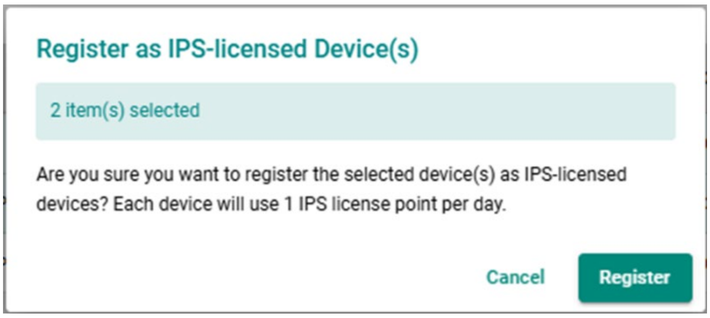
Activation Code *

5. Click **Apply**.
6. Verify the license is correct.

Registering an IPS-licensed Device

To enable full IPS functionality on a device, you must register the device as an IPS-licensed device. Once registered, the device will consume one IPS license point per day.

1. Navigate to **Menu** (☰) **> Administration > License Management**.
2. Go to the **IPS** tab.
3. In the IPS License Management section, check the box of the device(s) you want to register as IPS-licensed.
4. Click the **Register** ( ) icon.
   The **Register as IPS-licensed Device(s)** screen will appear.



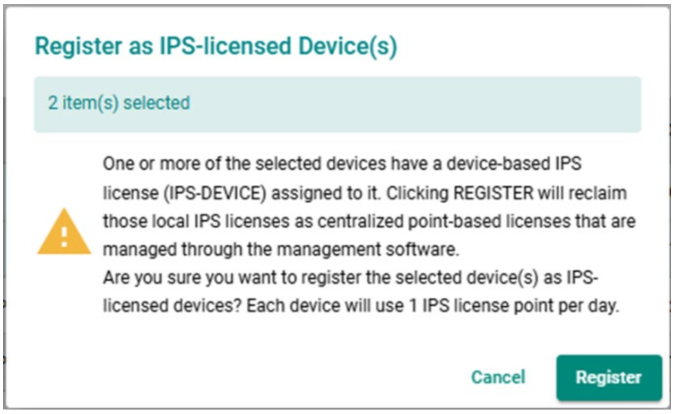
Register as IPS-licensed Device(s)

2 item(s) selected

Are you sure you want to register the selected device(s) as IPS-licensed devices? Each device will use 1 IPS license point per day.

5. When prompted to confirm, click **Register**.

6. If a device already has a device-based IPS (IPS-DEVICE) license assigned to it, a notification will appear.



Register as IPS-licensed Device(s)

2 item(s) selected

One or more of the selected devices have a device-based IPS license (IPS-DEVICE) assigned to it. Clicking REGISTER will reclaim those local IPS licenses as centralized point-based licenses that are managed through the management software.
Are you sure you want to register the selected device(s) as IPS-licensed devices? Each device will use 1 IPS license point per day.

7. Click **Register** to reclaim the device-based IPS licenses and register the device(s) as IPS-licensed.

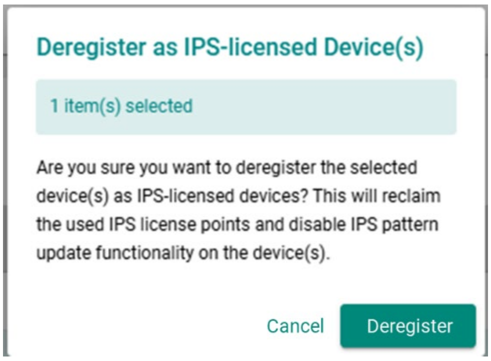
NOTE

When reclaiming a device-based IPS (IPS-DEVICE) license, MXview One will reclaim and reassign the license as a centrally managed IPS license. The original license will be added to the total IPS point balance.

Deregistering an IPS-licensed Device

You can deregister an IPS license from a managed device to assign it to another device. Deregistering an IPS license will cause IPS pattern updates to become unavailable on that device until it is registered as an IPS-licensed device again.

1. Navigate to **Menu** (☰) **> Administration > License Management**.
2. Go to the **IPS** tab.
3. In the IPS License Management section, check the box of the device(s) you want to deregister the IPS license for.
4. Click the **Deregister** ( ) icon.



Deregister as IPS-licensed Device(s)

1 item(s) selected

Are you sure you want to deregister the selected device(s) as IPS-licensed devices? This will reclaim the used IPS license points and disable IPS pattern update functionality on the device(s).

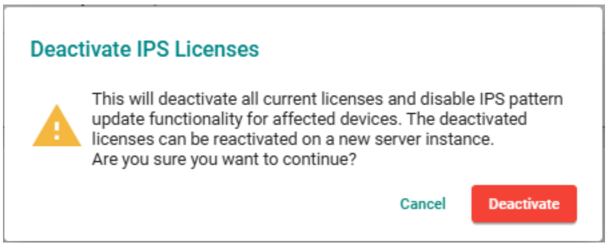
5. When prompted to confirm, click **Deregister**.

Transferring an IPS License

Under some circumstances, you may need to migrate MXview One to a new host system. To transfer your IPS licenses to another instance of MXview One, you must deactivate them on the current system first and reactivate the license(s) on the new MXview One instance.

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

2. Go to the **IPS** tab.
3. In the License History section, click the **Deactivate** (☒) icon to deactivate all active IPS licenses.



Deactivate IPS Licenses

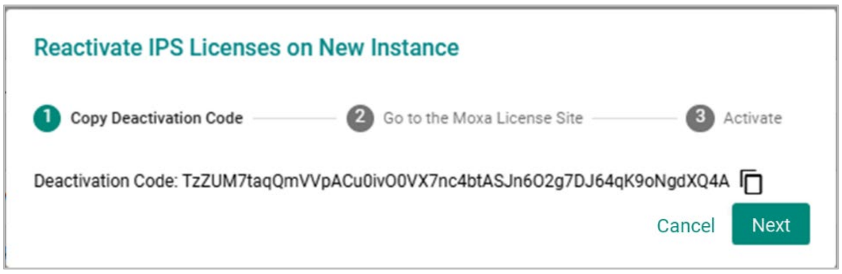
This will deactivate all current licenses and disable IPS pattern update functionality for affected devices. The deactivated licenses can be reactivated on a new server instance.
Are you sure you want to continue?

4. When prompted to confirm, click **Deactivate**.

NOTE

If more than one IPS license was deactivated, all remaining license points will be combined into a single license.

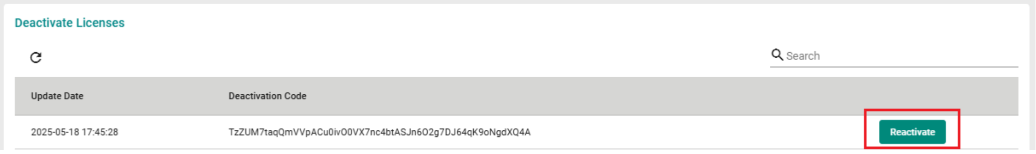
5. The **Reactivate IPS Licenses on New Instance** window will automatically appear.



Reactivate IPS Licenses on New Instance

Deactivation Code: TzZUM7taqQmVVpACu0ivO0VX7nc4btASJn6O2g7DJ64qK9oNgdXQ4A

If you closed this window, you can reopen it at any time by clicking **Reactivate** in the Deactivated Licenses section.



Deactivate Licenses

Update Date	Deactivation Code	
2025-05-18 17:45:28	TzZUM7taqQmVVpACu0ivO0VX7nc4btASJn6O2g7DJ64qK9oNgdXQ4A	Reactivate

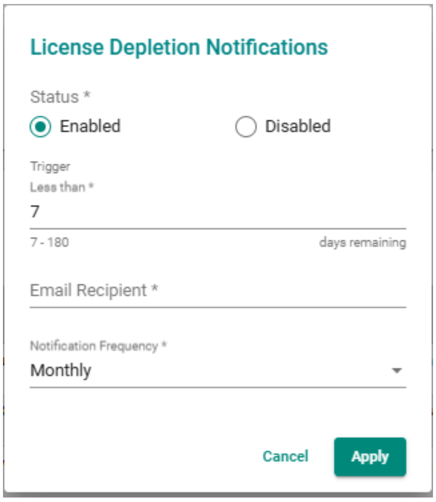
6. Follow the steps in the reactivation wizard to complete the license transfer process.

Configuring IPS License Depletion Notifications

You can set up notifications to inform you when your IPS license point balance is about to run out.

1. Navigate to **Menu** (☰) **> Administration > License Management**.
2. Go to the **IPS** tab.

3. Click **License Depletion Notifications**.
   The **License Depletion Notifications** screen will appear.



License Depletion Notifications

Status *

● Enabled ○ Disabled

Trigger
Less than *
7
7 - 180 days remaining

Email Recipient *

Notification Frequency *
Monthly

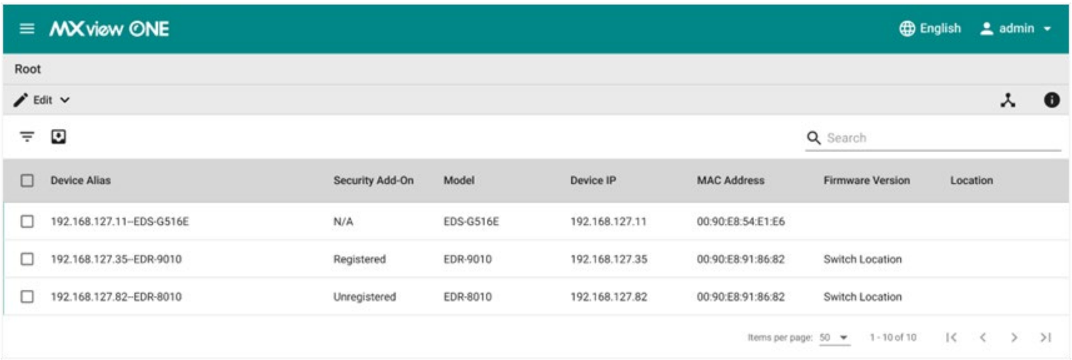
4. Select the notification status. If set to **Enabled**, configure the following settings:
   - **Trigger**: Specify the number of days before the IPS point balance is depleted. A notification will be sent when this threshold is reached. Days remaining are calculated based on the total available IPS point balance divided by the daily point usage.
   - **Email Recipient**: Enter the email address of the notification recipient. SMTP settings must be configured first before notifications can be set up. Refer to **Configuring Email Server Settings**.
   - **Notification Frequency**: Select the frequency at which notifications will be sent.
5. Click **Apply**.

Checking Registered Devices

MXview One can automatically check for and register devices that support MXview Security features.

You can see the registration status on the **Topology** or **Device Management** page.

1. To check the device registration status from the **Topology** screen:
   a. Navigate to **Menu** (☰) **> Topology**.
   b. Click the **List View** (☰) icon.
   Devices in the topology will be shown in a list.

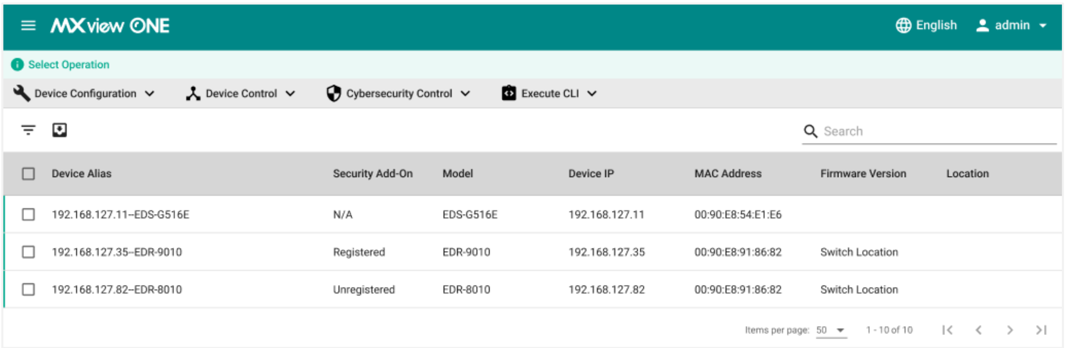


□	Device Alias	Security Add-On	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.127.11–EDS-G516E	N/A	EDS-G516E	192.168.127.11	00:90:E8:54:E1:E6		
□	192.168.127.35–EDR-9010	Registered	EDR-9010	192.168.127.35	00:90:E8:91:86:82	Switch Location	
□	192.168.127.82–EDR-8010	Unregistered	EDR-8010	192.168.127.82	00:90:E8:91:86:82	Switch Location	

Items per page: 50 1 - 10 of 10

2. To check the device registration status from the **Device Management** screen:

a. Navigate to **Menu** (☰) **> Device Management> Configuration and Control**.



□	Device Alias	Security Add-On	Model	Device IP	MAC Address	Firmware Version	Location
□	192.168.127.11–EDS-G516E	N/A	EDS-G516E	192.168.127.11	00:90:E8:54:E1:E6		
□	192.168.127.35–EDR-9010	Registered	EDR-9010	192.168.127.35	00:90:E8:91:86:82	Switch Location	
□	192.168.127.82–EDR-8010	Unregistered	EDR-8010	192.168.127.82	00:90:E8:91:86:82	Switch Location	

Items per page: 50 1 - 10 of 10

3. Check the registration status of the device in the **Security Add-on** column:

- **Registered**: The device can be managed in the Security Add-on module and has been successfully registered.
- **Unregistered**: The device can be managed in the Security Add-on module, but it has not been successfully registered yet. Some functions such as firewall policies cannot be deployed on unregistered devices.
- **N/A**: The device cannot be managed in the Security Add-on module.

NOTE

If the status is **Unregistered**, confirm the device account and password in **Device Configuration > Device Accounts** are correct or reboot the device.

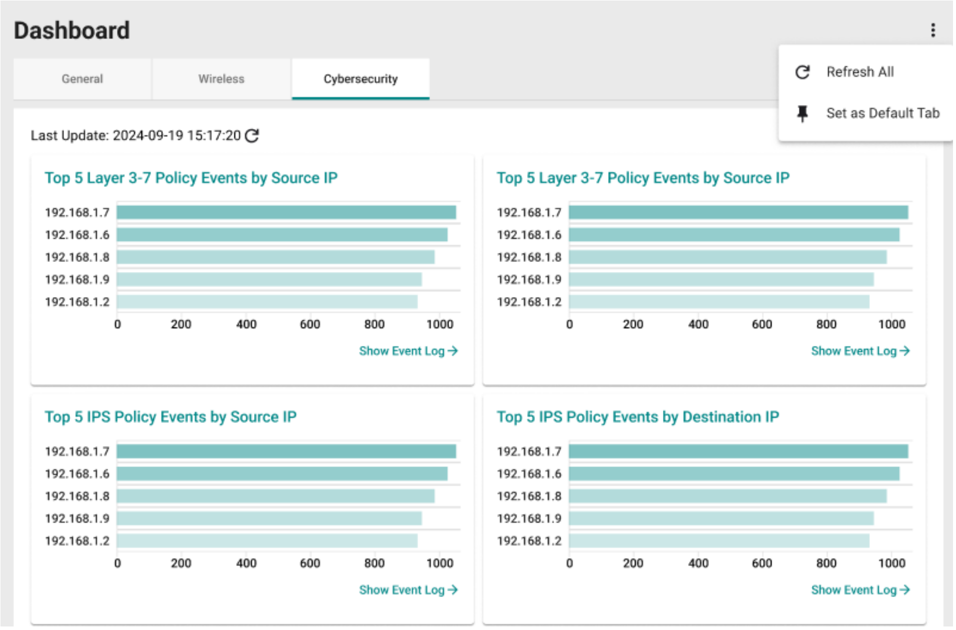
Security Module Features

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

Main Dashboard

If the Security module is activated, the MXview One Dashboard will include a Cybersecurity tab with widgets showing cybersecurity event statistics.

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


Dashboard
General
Wireless
Cybersecurity
Refresh All
Set as Default Tab
Last Update: 2024-09-19 15:17:20
Top 5 Layer 3-7 Policy Events by Source IP
Top 5 Layer 3-7 Policy Events by Source IP
Top 5 IPS Policy Events by Source IP
Top 5 IPS Policy Events by Destination IP
192.168.1.7
192.168.1.6
192.168.1.8
192.168.1.9
192.168.1.2
0
200
400
600
800
1000
Show Event Log →

The following widgets will appear in the Cybersecurity tab, depending on the types of security events that have occurred on the network. Click the **Refresh All** (↻) icon in the top-right to update the data of all the widgets.

- Top 5 Layer 3-7 Policy Events by Source IP
- Top 5 Layer 3-7 Policy Events by Destination IP
- Top 5 IPS Policy Events by Source IP
- Top 5 IPS Policy Events by Destination IP
- Top 5 Protocol Filter Policy Events by Source IP
- Top 5 Protocol Filter Policy Events by Destination IP
- Top 5 ADP Policy Events by Source IP
- Top 5 ADP Policy Events by Destination IP

To check detailed information, click the bar of the corresponding IP address in the widget, or click **Show Event Log** at the bottom of each widget to jump to the cybersecurity event log.

Policy Profile Management

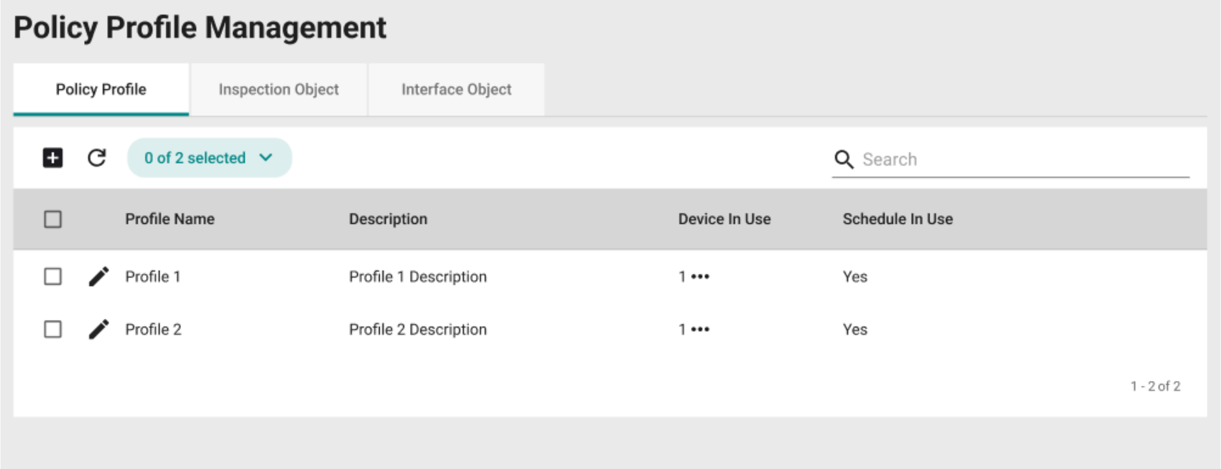
This section allows users to manage policy profiles, inspection objects, and interface objects that can be applied to multiple devices.

This section contains the following tabs:

- **Policy Profile**: Manage policy profiles for devices.
- **Inspection Object**: Manage inspection objects for policy profiles.
- **Interface Object**: Manage interface objects for policy profiles.

Policy Profiles

To access the **Policy Profile** page, in the function tree, navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Management** and go to the **Policy Profile** tab.



Policy Profile Management

Policy Profile | Inspection Object | Interface Object

0 of 2 selected

Search

□		Profile Name	Description	Device In Use	Schedule In Use
□	✎	Profile 1	Profile 1 Description	1 •••	Yes
□	✎	Profile 2	Profile 2 Description	1 •••	Yes

1 - 2 of 2

Policy profiles aggregate various firewall policies and can be deployed to devices based on network security requirements.

You can configure the following types of policies:

- **Layer 3-7 Policy**: Provides secure traffic control, allowing users to control network traffic based on security needs.
- **Session Control**: Protects network hosts or services from exceeding performance limitations.
- **DoS Policy**: Provides different DoS protection functions for detecting or defining abnormal packet formats or traffic flows.
- **IPS Policy**: Performs intrusion detection and prevention to protect networks from security threats.

NOTE

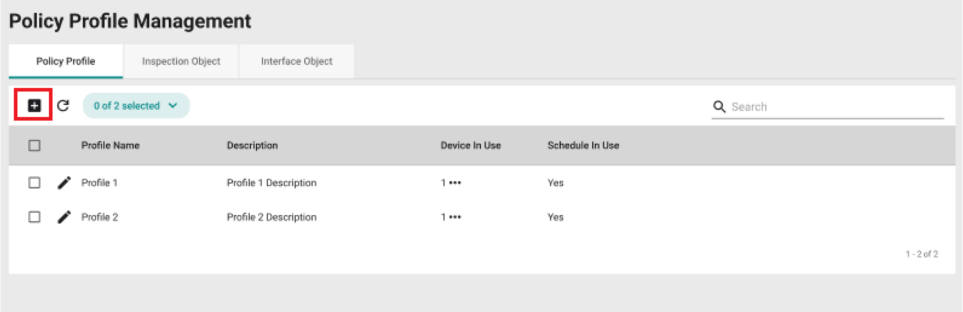
"**Device in Use**" indicates the number of devices the policy profile is being used by. Policy profiles applied to devices cannot be deleted. Click the "**...**" icon in the column to see details about the referenced device(s).

NOTE

"**Schedule in Use**" indicates there is an upcoming scheduled deployment to apply this policy profile to the referenced device(s). To avoid any disruptions or deployment failures, policy profiles with planned deployments cannot be deleted.

Creating a Layer 3-7 Policy Profile

1. Navigate to **Menu** (≡) **> Firewall Policy Management > Policy Profile Management**.
2. Go to the **Policy Profile** tab.
3. Click the **Add** (⊞) icon in the top-left corner to create a new policy profile.



Policy Profile Management

Policy Profile | Inspection Object | Interface Object

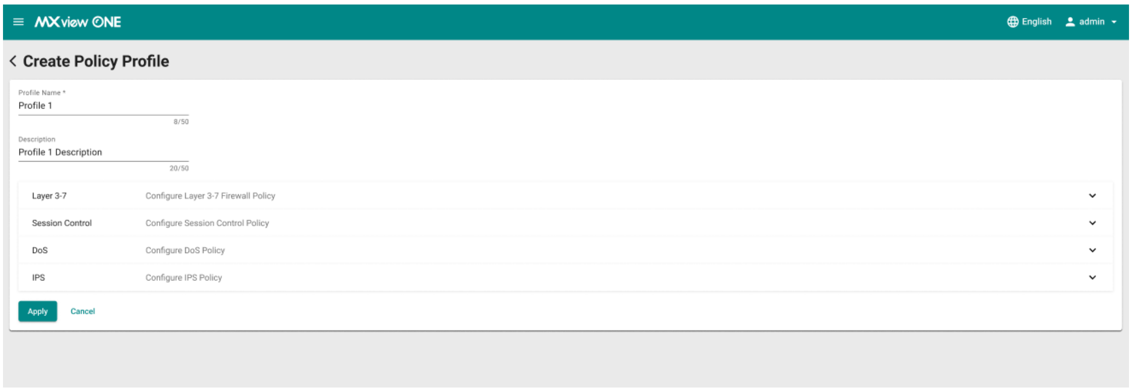
0 of 2 selected

Search

□		Profile Name	Description	Device In Use	Schedule In Use
□	✎	Profile 1	Profile 1 Description	1 •••	Yes
□	✎	Profile 2	Profile 2 Description	1 •••	Yes

1 - 2 of 2

The **Create Policy Profile** will appear.



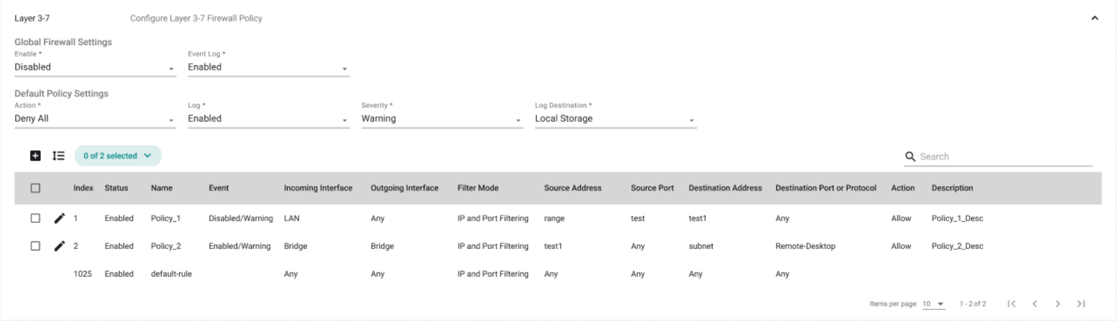
Create Policy Profile

Profile Name *
Profile 1
8/50

Description
Profile 1 Description
20/50

Layer 3-7	Configure Layer 3-7 Firewall Policy
Session Control	Configure Session Control Policy
DoS	Configure DoS Policy
IPS	Configure IPS Policy

4. Enter a name and description for the profile.
5. Expand the Layer 3-7 profile options.



Layer 3-7 Configure Layer 3-7 Firewall Policy

Global Firewall Settings

Enable *: Disabled

Event Log *: Enabled

Default Policy Settings

Action *: Deny All

Log *: Enabled

Severity *: Warning

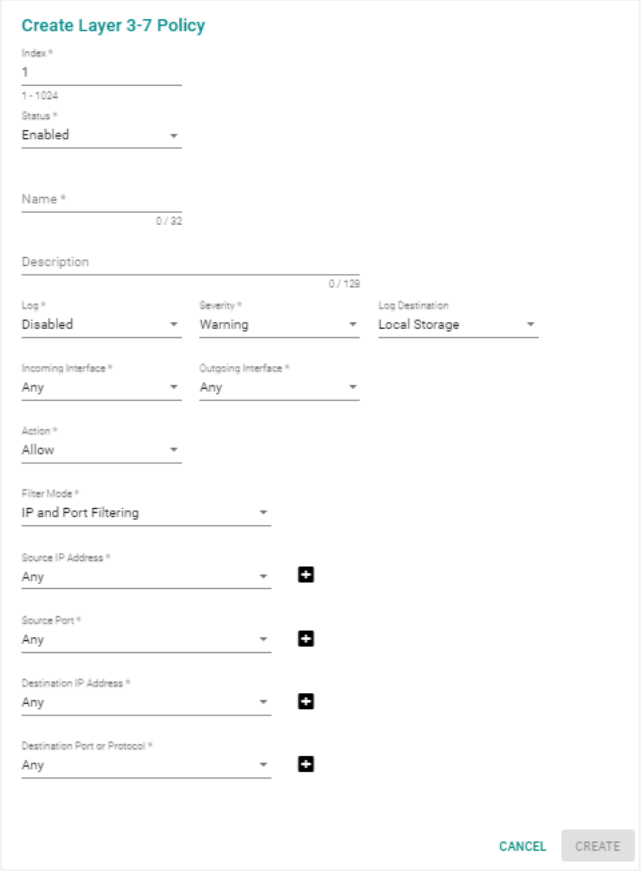
Log Destination *: Local Storage

□		Index	Status	Name	Event	Incoming Interface	Outgoing Interface	Filter Mode	Source Address	Source Port	Destination Address	Destination Port or Protocol	Action	Description
□	✎	1	Enabled	Policy_1	Disabled/Warning	LAN	Any	IP and Port Filtering	range	test	test1	Any	Allow	Policy_1_Desc
□	✎	2	Enabled	Policy_2	Enabled/Warning	Bridge	Bridge	IP and Port Filtering	test1	Any	subnet	Remote-Desktop	Allow	Policy_2_Desc
		1025	Enabled	default-rule		Any	Any	IP and Port Filtering	Any	Any	Any	Any		

6. Configure global firewall settings:
   - **Enforcement**: Enable or disable Layer 3-7 policy profiles.
   - **Event Log**: Enable or disable logging Layer 3-7 policy events.
7. Configure the default policy settings:
   - **Action**: Choose to allow or deny packets that do not match any configured policy rules.
   - **Log**: Enable or disable logging Layer 3-7 policy events.
   - **Severity**: Select the severity level for the event. The default is **Warning**.
   - **Log Destination**: Choose where to store the event logs. The default is **Local Storage**.

8. Click the **Add** (⊞) icon to add a Layer 3-7 policy.

   The **Create Layer 3-7 Policy** screen will appear.



Create Layer 3-7 Policy

Index * 1 (1 - 1024)

Status * Enabled

Name * (0 / 32)

Description (0 / 128)

Log * Disabled

Severity * Warning

Log Destination Local Storage

Incoming Interface * Any

Outgoing Interface * Any

Action * Allow

Filter Mode * IP and Port Filtering

Source IP Address * Any

Source Port * Any

Destination IP Address * Any

Destination Port or Protocol * Any

9. Configure the following settings:
   - **Index**: Specify the index for the policy profile.
   - **Status**: Enable or disable the policy profile.
   - **Name**: Enter a name for the policy profile.
   - **Description**: Enter a description for the policy profile.
   - **Log**: Enable or disable event logs.
   - **Severity**: Select the log severity level.
   - **Log Destination**: If logging is enabled, choose where the logs will be stored. Multiple options can be selected.
   - **Incoming/Outgoing Interface**: Select the incoming and outgoing interfaces.
   - **Action**: Select the action when traffic matches the policy rule.
   - **Filter Mode**: Select a filtering mode. Depending on the selected mode, configure the following settings:

     IP and Port Filtering:

     - **Source/Destination IP Address**: Select **Any** or a preconfigured filter object. Refer to Creating an Inspection Object.
     - **Source Port/Destination Port or Protocol**: Select **Any** or a preconfigured interface object. Refer to Creating an Interface Object.

     IP and Source MAC Binding:

     - **Source MAC Address**: Specify the source MAC address.
     - **Source IP Address**: Select a preconfigured filter object. Refer to Creating an Inspection Object.

     Source MAC Filtering:

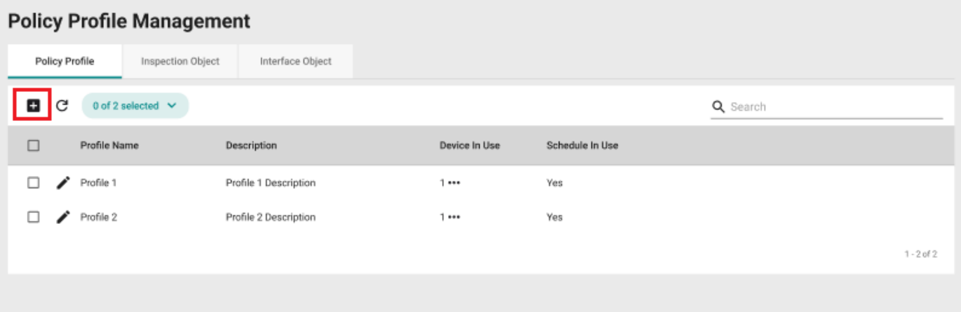
     - **Source MAC Address**: Specify the source MAC address.

10. Click **Create** to create the Layer 3-7 policy.

11. Click **Apply**.

Creating a Session Control Policy Profile

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Management**.
2. Go to the **Policy Profile** tab.
3. Click the **Add** (⊞) icon in the top-left corner to create a new policy profile.

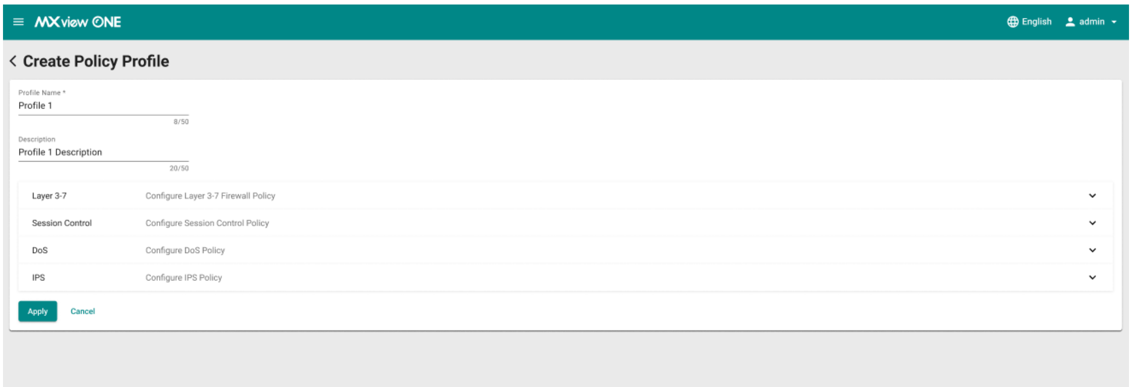


Policy Profile Management

☐		Profile Name	Description	Device In Use	Schedule In Use
☐	✎	Profile 1	Profile 1 Description	1 •••	Yes
☐	✎	Profile 2	Profile 2 Description	1 •••	Yes

1 - 2 of 2

The **Create Policy Profile** will appear.



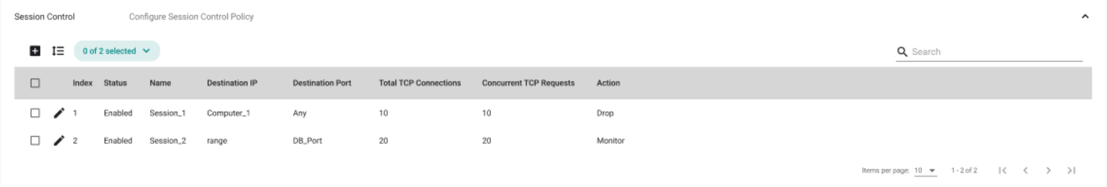
Create Policy Profile

Profile Name *
Profile 1
8/50

Description
Profile 1 Description
20/50

Layer 3-7	Configure Layer 3-7 Firewall Policy
Session Control	Configure Session Control Policy
DoS	Configure DoS Policy
IPS	Configure IPS Policy

4. Enter a name and description for the profile.
5. Expand the Session Control profile options.



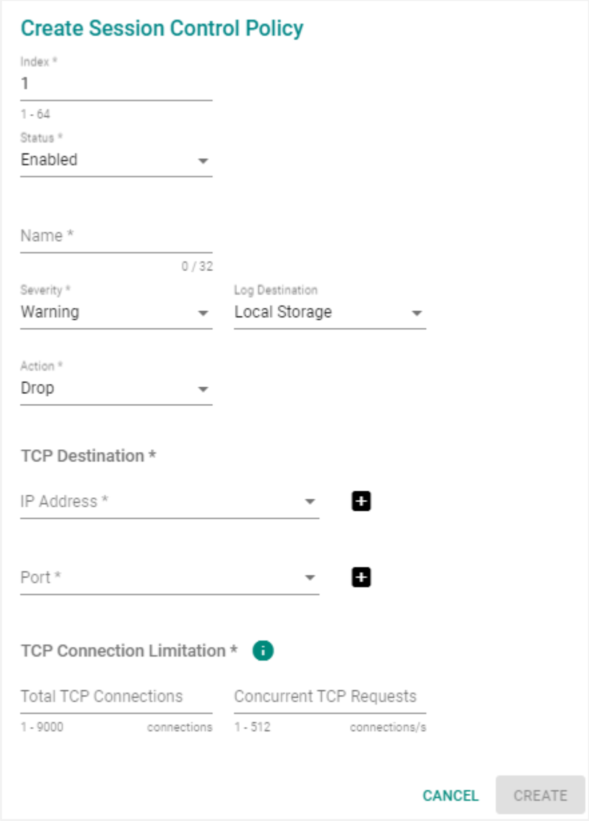
Session Control   Configure Session Control Policy

☐		Index	Status	Name	Destination IP	Destination Port	Total TCP Connections	Concurrent TCP Requests	Action
☐	✎	1	Enabled	Session_1	Computer_1	Any	10	10	Drop
☐	✎	2	Enabled	Session_2	range	DB_Port	20	20	Monitor

Items per page: 10   1 - 2 of 2

6. Click the **Add** (⊞) icon to add a Session Control policy.

   The **Create Session Control Policy** screen will appear.



Create Session Control Policy

Index *: 1 (1 - 64)

Status *: Enabled

Name * (0 / 32)

Severity *: Warning

Log Destination: Local Storage

Action *: Drop

TCP Destination *

IP Address * ⊞

Port * ⊞

TCP Connection Limitation *

Total TCP Connections (1 - 9000 connections)

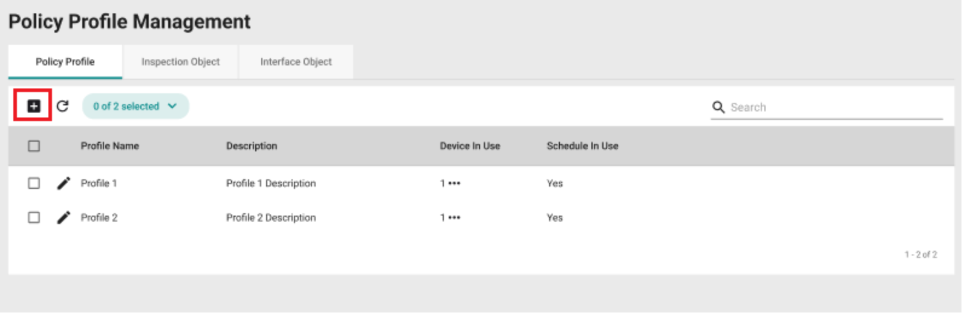
Concurrent TCP Requests (1 - 512 connections/s)

7. Configure the following settings:
   - **Index**: Specify the index for the policy profile.
   - **Status**: Enable or disable the policy profile.
   - **Name**: Enter a name for the policy profile.
   - **Severity**: Select the log severity level.
   - **Log Destination**: If logging is enabled, choose where the logs will be stored. Multiple options can be selected.
   - **Action**: Select the action when traffic matches the policy rule.
   - **IP Address**: Select **Any** or a preconfigured inspection object. Refer to Creating an Inspection Object.
   - **Port**: Select **Any** or a preconfigured interface object. Refer to Creating an Interface Object.
   - **Total TCP Connections**: Specify the maximum allowed TCP connections.
   - **Concurrent TCP Requests**: Specify the maximum allowed concurrent connections.
8. Click **Create** to create the Session Control policy.
9. Click **Apply**.

Creating a DoS Policy Profile

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Management**.
2. Go to the **Policy Profile** tab.

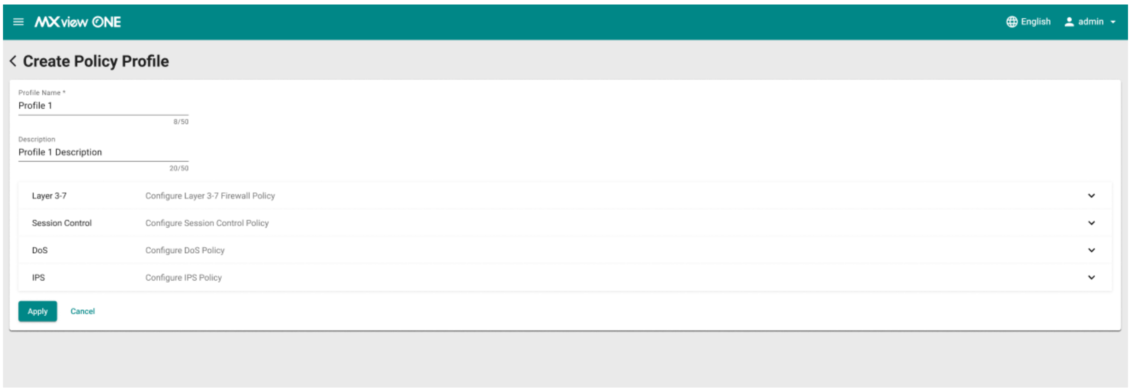
3. Click the **Add** (⊞) icon in the top-left corner to create a new policy profile.



Policy Profile Management

□	Profile Name	Description	Device In Use	Schedule In Use
□	Profile 1	Profile 1 Description	1 •••	Yes
□	Profile 2	Profile 2 Description	1 •••	Yes

The **Create Policy Profile** will appear.



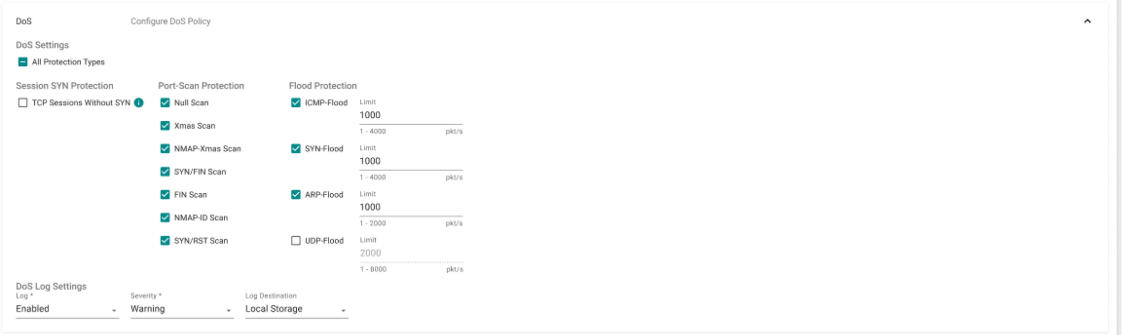
Create Policy Profile

Profile Name * Profile 1 8/50

Description Profile 1 Description 20/50

Layer 3-7	Configure Layer 3-7 Firewall Policy
Session Control	Configure Session Control Policy
DoS	Configure DoS Policy
IPS	Configure IPS Policy

4. Enter a name and description for the profile.
5. Expand the **DoS** profile options.



DoS Configure DoS Policy

DoS Settings

▣ All Protection Types

Session SYN Protection	Port-Scan Protection	Flood Protection	
□ TCP Sessions Without SYN	☑ Null Scan	☑ ICMP-Flood	Limit 1000 (1 - 4000 pkt/s)
	☑ Xmas Scan		
	☑ NMAP-Xmas Scan	☑ SYN-Flood	Limit 1000 (1 - 4000 pkt/s)
	☑ SYN/FIN Scan		
	☑ FIN Scan	☑ ARP-Flood	Limit 1000 (1 - 2000 pkt/s)
	☑ NMAP-ID Scan		
	☑ SYN/RST Scan	□ UDP-Flood	Limit 2000 (1 - 8000 pkt/s)

DoS Log Settings

Log * Enabled

Severity * Warning

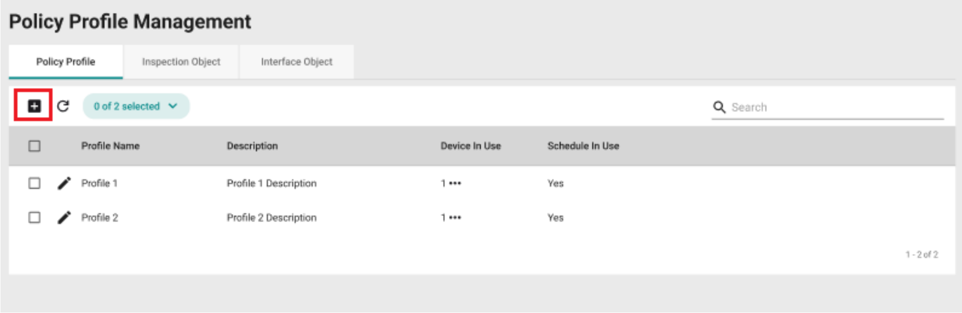
Log Destination Local Storage

6. Configure the following settings:
   - **DoS Settings**: Check the box of the DoS types you want to enable. If necessary, specify the packet limit.
   - **Log**: Enable or disable event logs.
   - **Severity**: Select the log severity level.
   - **Destination**: If logging is enabled, choose where the logs will be stored. Multiple options can be selected.
7. Click **Apply**.

Creating an IPS Policy Profile

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Management**.
2. Go to the **Policy Profile** tab.

3. Click the **Add** (⊞) icon in the top-left corner to create a new policy profile.

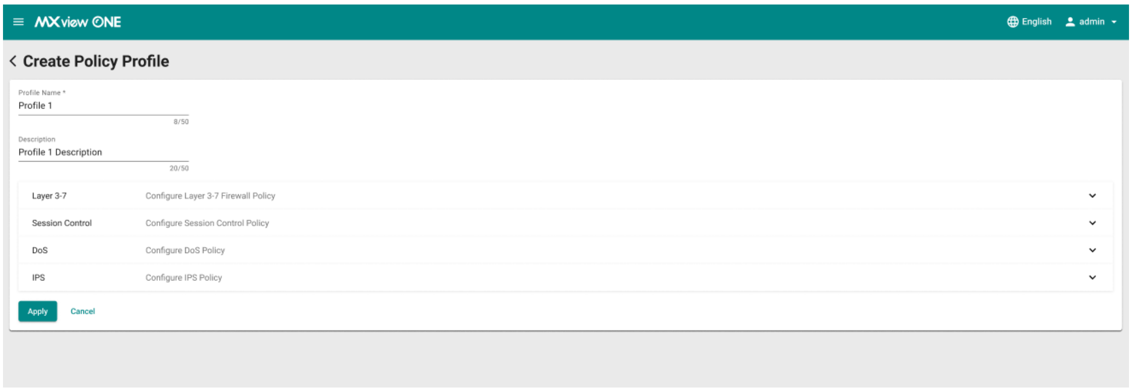


Policy Profile Management

□		Profile Name	Description	Device In Use	Schedule In Use
□	✎	Profile 1	Profile 1 Description	1 •••	Yes
□	✎	Profile 2	Profile 2 Description	1 •••	Yes

1 - 2 of 2

The **Create Policy Profile** will appear.



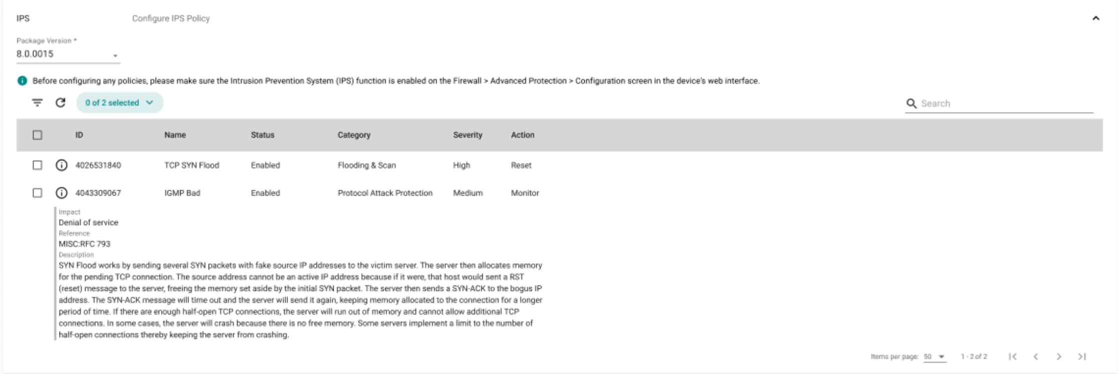
Create Policy Profile

Profile Name *
Profile 1
8/50

Description
Profile 1 Description
20/50

Layer 3-7	Configure Layer 3-7 Firewall Policy
Session Control	Configure Session Control Policy
DoS	Configure DoS Policy
IPS	Configure IPS Policy

4. Enter a name and description for the profile.
5. Expand the **IPS** profile options.



IPS Configure IPS Policy

Package Version *
8.0.0015

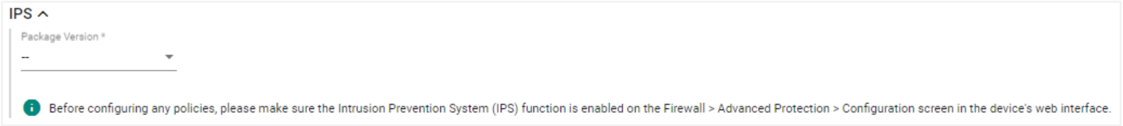
Before configuring any policies, please make sure the Intrusion Prevention System (IPS) function is enabled on the Firewall > Advanced Protection > Configuration screen in the device's web interface.

□		ID	Name	Status	Category	Severity	Action
□	ⓘ	4026531840	TCP SYN Flood	Enabled	Flooding & Scan	High	Reset
□	ⓘ	4043309067	IGMP Bad	Enabled	Protocol Attack Protection	Medium	Monitor

Impact
Denial of service
Reference
MISC:RFC 793
Description
SYN Flood works by sending several SYN packets with fake source IP addresses to the victim server. The server then allocates memory for the pending TCP connection. The source address cannot be an active IP address because if it were, that host would sent a RST (reset) message to the server, freeing the memory set aside by the initial SYN packet. The server then sends a SYN-ACK to the bogus IP address. The SYN-ACK message will time out and the server will send it again, keeping memory allocated to the connection for a longer period of time. If there are enough half-open TCP connections, the server will run out of memory and cannot allow additional TCP connections. In some cases, the server will crash because there is no free memory. Some servers implement a limit to the number of half-open connections thereby keeping the server from crashing.

Items per page: 50 1 - 2 of 2

6. Select a previously uploaded IPS software package version. Refer to Security Package Management for more information.



IPS

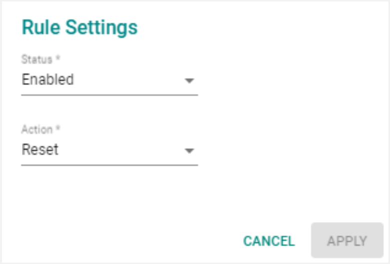
Package Version *
--

Before configuring any policies, please make sure the Intrusion Prevention System (IPS) function is enabled on the Firewall > Advanced Protection > Configuration screen in the device's web interface.

7. In the IPS rule table, check the box of the rule(s) you want to configure. You can select multiple rules at once.

8. Click the **Rule Settings** (⚙) icon.

   The **Rule Settings** screen will appear.



Rule Settings

Status *
Enabled

Action *
Reset

CANCEL APPLY

9. Configure the following settings:
   - **Status**: Enable or disable the selected rule(s).
   - **Action**: Select the action when traffic matches the policy rule.
10. Click **Apply**.
11. On the **Policy Profile** screen, click **Apply**.

Editing a Policy Profile

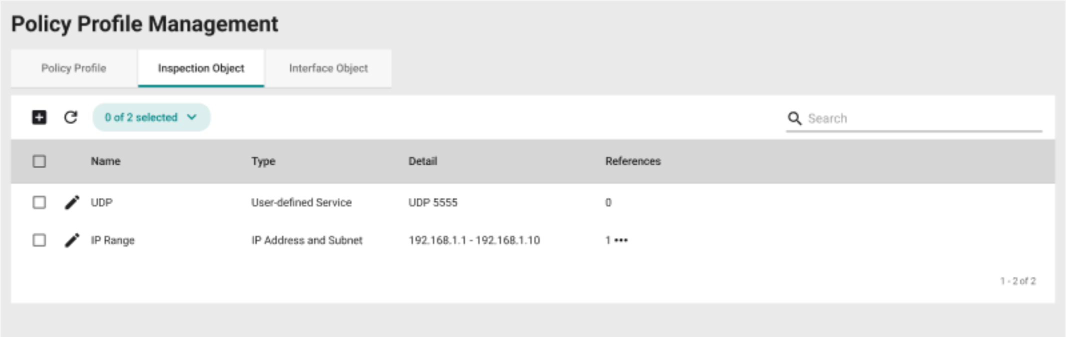
1. Navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Management**.
2. Go to the **Policy Profile** tab.
3. Click the **Edit** (✎) icon of the profile you want to edit.
4. Modify the profile settings. Refer to the corresponding section for settings information:
   - Creating a Layer 3-7 Policy Profile
   - Creating a Session Control Policy Profile
   - Creating a DoS Policy Profile
   - Creating an IPS Policy Profile
5. Click **Apply**.

Deleting a Policy Profile

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Management**.
2. Go to the **Policy Profile** tab.
3. Check the box of the policy profile(s) you want to delete.
4. Click the **Delete** (🗑) icon.
5. When prompted to confirm, click **Delete**.

Inspection Objects

To access the **Inspection Object** page, in the function tree, navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Management** and go to the **Inspection Object** tab.



Policy Profile Management

Policy Profile | Inspection Object | Interface Object

0 of 2 selected

Search

□		Name	Type	Detail	References
□	✎	UDP	User-defined Service	UDP 5555	0
□	✎	IP Range	IP Address and Subnet	192.168.1.1 - 192.168.1.10	1 •••

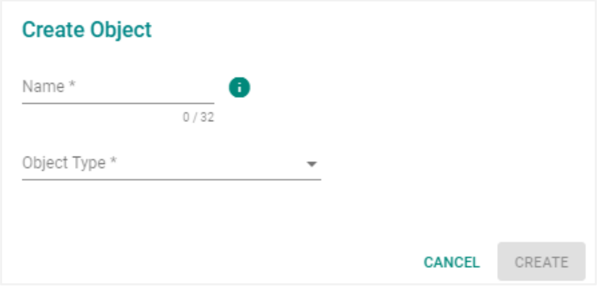
1 - 2 of 2

Inspection objects contain the IP address and subnet, network services, industrial application services, and user-defined services that are applied to policy rules using the object.

Creating an Inspection Object

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Management**.
2. Go to the **Inspection Object** tab.
3. Click the **Add** (➕) icon in the top-left corner to create a new inspection object.

   The **Create Object** window will appear.



Create Object

Name *

0 / 32

Object Type *

4. Configure the following settings:
   - **Name**: Enter a name for the object.
   - **Object Type**: Select the object type. Depending on the selected object, configure the following settings:
     - **IP Address and Subnet**: Depending on the selected IP Type, enter the IP address, IP range, or subnet.
     - **Network Service**: Check the box of the service(s) you want to add to the object.
     - **Industrial Application Service**: Check the box of the industrial application service(s) you want to add to the object.
     - **User-defined Service**: Select the IP protocol. Depending on the selected protocol, specify the port, port range, ICMP Type and Code, or protocol decimal
5. Click **Create**.

Editing an Inspection Object

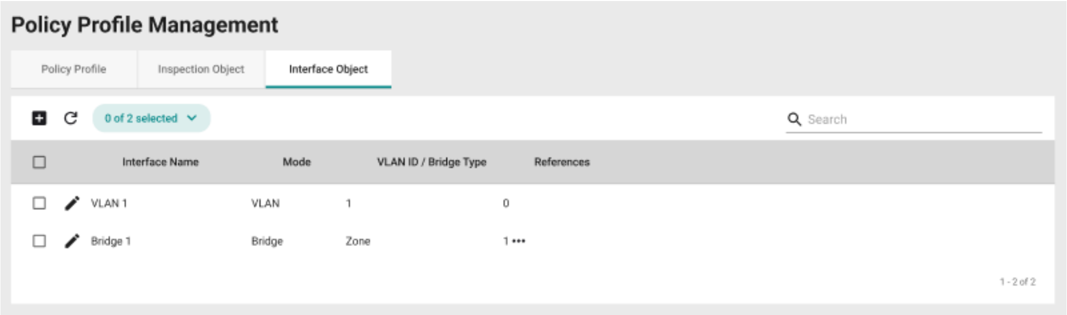
1. Navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Management**.
2. Go to the **Inspection Object** tab.
3. Click the **Edit** (✎) icon of the object you want to edit.
4. Modify the object settings.
5. Click **Apply**.

Deleting an Inspection Object

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Management**.
2. Go to the **Inspection Object** tab.
3. Check the box of the object(s) you want to delete.
4. Click the **Delete** (🗑) icon.
5. When prompted to confirm, click **Delete**.

Interface Objects

To access the **Interface Object** page, in the function tree, navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Management** and go to the **Interface Object** tab.


Policy Profile Management

Policy Profile | Inspection Object | Interface Object

0 of 2 selected

Search

□	Interface Name	Mode	VLAN ID / Bridge Type	References
□	VLAN 1	VLAN	1	0
□	Bridge 1	Bridge	Zone	1 •••

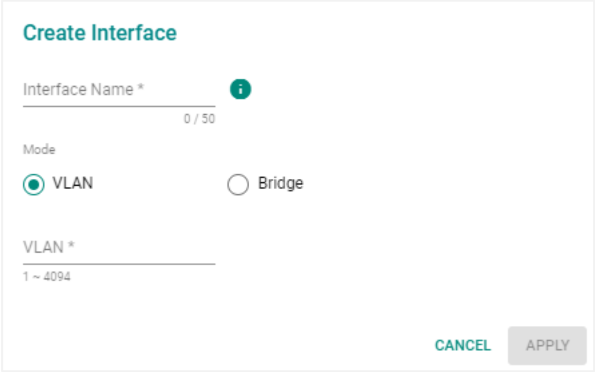
1 - 2 of 2

Interface objects contain the VLAN interface and bridge interface that are applied to policy rules using the object.

Creating an Interface Object

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Management**.
2. Go to the **Interface Object** tab.
3. Click the **Add** (⊞) icon in the top-left corner to create a new interface object.

   The **Create Interface** window will appear.


Create Interface

Interface Name *

0 / 50

Mode

● VLAN ○ Bridge

VLAN *

1 ~ 4094

CANCEL APPLY

4. Configure the following settings:
   - **Name**: Enter a name for the object.
   - **Mode**: Select the interface mode. If set to VLAN, specify the VLAN ID. If set to Bridge, select the Bridge mode.
5. Click **Apply**.

Editing an Interface Object

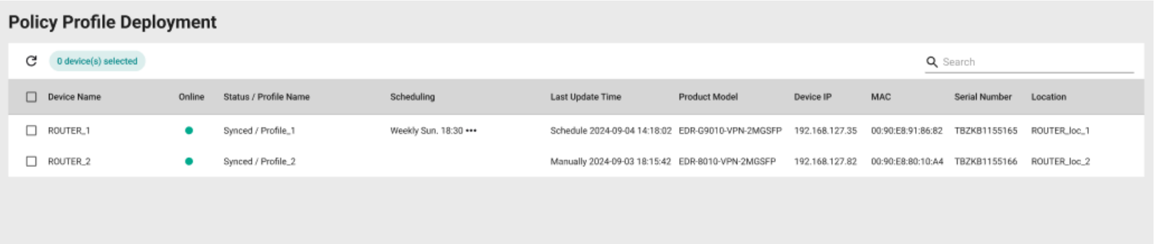
1. Navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Management**.
2. Go to the **Interface Object** tab.
3. Click the **Edit** (✎) icon of the object you want to edit.
4. Modify the object settings.
5. Click **Apply**.

Deleting an Interface Object

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Management**.
2. Go to the **Interface Object** tab.
3. Check the box of the object(s) you want to delete.
4. Click the **Delete** (🗑) icon.
5. When prompted to confirm, click **Delete**.

Policy Profile Deployment

To access the **Policy Profile Deployment** page, in the function tree, navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Deployment**.



Policy Profile Deployment

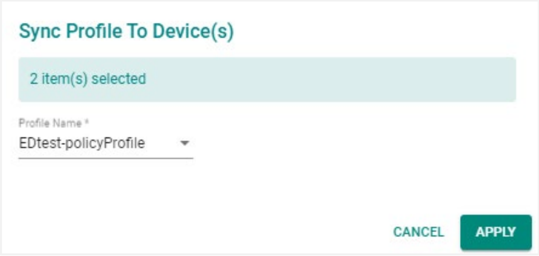
☐ Device Name	Online	Status / Profile Name	Scheduling	Last Update Time	Product Model	Device IP	MAC	Serial Number	Location
☐ ROUTER_1	●	Synced / Profile_1	Weekly Sun. 18:30 •••	Schedule 2024-09-04 14:18:02	EDR-G9010-VPN-2MGSFP	192.168.127.35	00:90:E8:91:86:82	TBZKB1155165	ROUTER_loc_1
☐ ROUTER_2	●	Synced / Profile_2		Manually 2024-09-03 18:15:42	EDR-8010-VPN-2MGSFP	192.168.127.82	00:90:E8:80:10:A4	TBZKB1155166	ROUTER_loc_2

From this screen, users can deploy policy profiles to multiple managed devices at a time and check the synchronization status.

Deploying Policy Profiles to Managed Devices

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Deployment**.
2. Check the box of the device(s) you want to apply a policy profile to.
3. Click the **Sync Profile** (⟳) icon in the top-left corner.

   The **Sync Profile to Device(s)** window will appear.



Sync Profile To Device(s)

2 item(s) selected

Profile Name *: EDtest-policyProfile

4. Select a previously configured policy profile. Refer to Policy Profile Management for instructions on how to create policy profiles.
5. Click **Apply**.

NOTE

You can also deploy policy profiles via **Topology > Cybersecurity Controls > Policy Profile Deployment** or via **Device Management > Configuration and Control > Cybersecurity Controls > Policy Profile Deployment**.

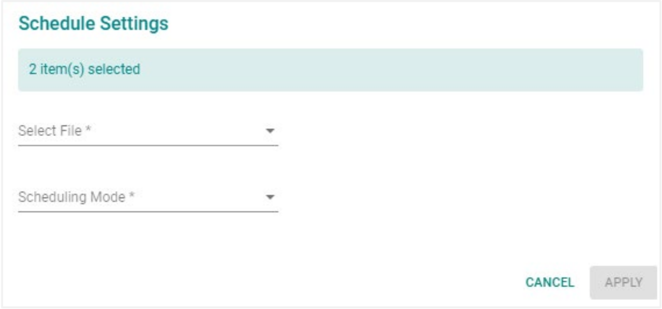
Scheduling a Policy Profile Deployment for Managed Devices

Deploying a policy profile to a device may disrupt services or operations. To minimize the potential impact of policy profile deployments, users can schedule the deployment for specific times where they are least likely to affect operations. Schedules can be configured to execute only once, or on a daily or weekly recurring basis.

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Deployment**.
2. Check the box of the device(s) you want to configure a scheduled deployment for.

3. Click the **Schedule Settings** ( ) icon in the top-left corner.

   The **Schedule Settings** window will appear.



Schedule Settings

2 item(s) selected

Select File *

Scheduling Mode *

4. Configure the following settings:
   - **Select File**: Select a policy profile to apply to the selected device(s).
   - **Scheduling Mode**: Select a scheduling mode. Depending on the selected mode, configure the following settings:
     - **One Time**: Select the date and time. One-time schedules can be configured for up to 30 days in the future.
     - **Daily**: Select the time and the schedule period. Daily schedules can be configured for up to 90 days in the future.
     - **Weekly**: Select the day of the week, the time, and schedule period. Weekly schedules can be configured for up to 90 days in the future.
5. Click **Apply**.

Deleting a Scheduled Profile Policy Deployment

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Policy Profile Deployment**.
2. Check the box of the device(s) with the scheduled deployment you want to delete.
3. Click the **Delete Schedule** (☒) icon.
4. When prompted to confirm, click **Delete**.

Security Package Management

This section describes how to manage the security package either manually from a local PC or automatically by updating to the Moxa Update Server.

This section contains the following tabs:

- **Security Package Files**: Manage security package files for supported devices.
- **Log**: Shows security package-related event logs.
- **Update Settings**: Configure scheduled security package update checks.

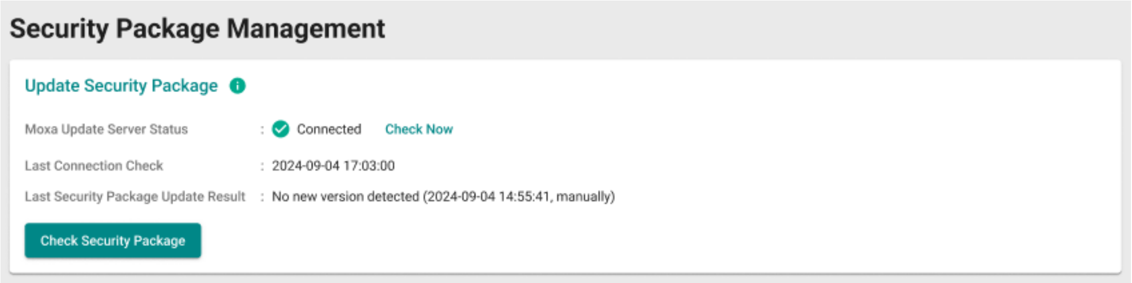
Security Package Files

From the **Security Package Files** tab, you can update and manage security package files.

Checking the Security Package Status

The **Update Security Package** section provides information about the Moxa Update Server connection status, the time and date of the last update check, and the result of the last check.

To access this section, navigate to **Menu** (☰) **> Firewall Policy Management > Security Package Management**.



Security Package Management

Update Security Package

Moxa Update Server Status : Connected Check Now

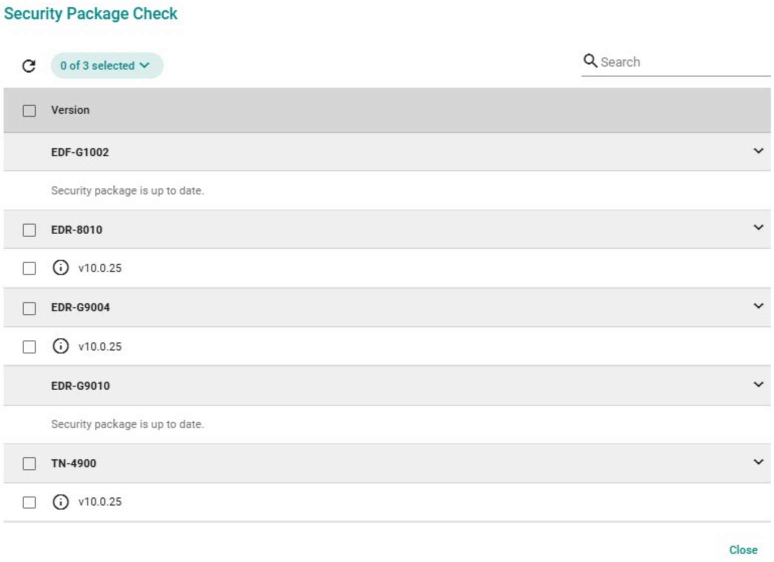
Last Connection Check : 2024-09-04 17:03:00

Last Security Package Update Result : No new version detected (2024-09-04 14:55:41, manually)

The widget shows the following information:

Field	Description
Moxa Update Server Status	Shows the current status of the connection to the Moxa update server.
Last Connection Check	Shows the date and time of the last connection check.
Last Security Package Update Result	Shows the result of the most recent security package update check.

To manually check for security package updates, click the **Check Security Package** button. A list of models and any available security package updates will be shown. The models shown in the list are configured in the **Update Settings** tab. To set up a scheduled update check, refer to Scheduling a Security Package Update Check.



Security Package Check

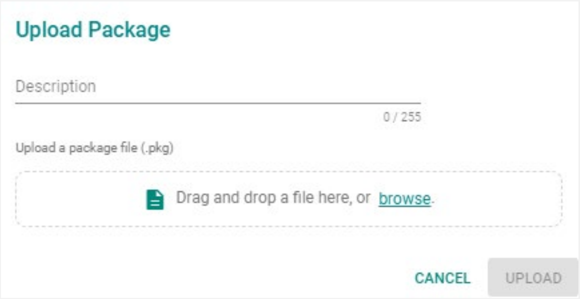
	Version
	EDF-G1002
	Security package is up to date.
□	EDR-8010
□	v10.0.25
□	EDR-G9004
□	v10.0.25
	EDR-G9010
	Security package is up to date.
□	TN-4900
□	v10.0.25

Uploading a Security Package

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Security Package Management**.
2. Go to the **Security Package Files** tab.
3. Click the **Add** (+) icon in the top-left corner to upload a security package.

   The **Upload Package** window will appear.

4. Drag and drop or browse to the package file on the local computer and enter a description for the file.



Upload Package

Description

0 / 255

Upload a package file (.pkg)

Drag and drop a file here, or browse.

CANCEL UPLOAD

5. Click **Upload**.

> **NOTE**
>
> "**Profile in Use**" indicates the number of policy profiles using the corresponding security package. Package files used by policy profiles cannot be deleted. Click the "**...**" icon in the column to see details about the referenced policy profile(s).

> **NOTE**
>
> "**Schedule in Use**" indicates there is an upcoming scheduled deployment to apply this security package to the referenced device(s). To avoid any disruptions or deployment failures, security packages with planned deployments cannot be deleted.

Viewing Detailed Security Package Information

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Security Package Management**.
2. Go to the **Security Package Files** tab.
3. In the package file list, click the **Info** (ⓘ) icon of the package file you want to view details for.
4. Click the **Info** (ⓘ) icon again to close the details section.

Downloading a Security Package

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Security Package Management**.
2. Go to the **Security Package Files** tab.
3. In the package file list, click the **Download** (⤓) icon of the package file you want to download.

Deleting a Security Package

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Security Package Management**.
2. Go to the **Security Package Files** tab.
3. Check the box of the package(s) you want to delete.
4. Click the **Delete** (🗑) icon.
5. When prompted to confirm, click **Delete**.

Event Logs

From the **Event Logs** tab, you can view security package files event logs.

Viewing Security Package Logs

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Security Package Management**.
2. Go to the **Event Logs** tab.
3. You can perform the following actions:

   a. Click the **Download All Logs** (⤓) icon to export the current search results as a CSV file.

   b. Click the **Refresh** (⟳) icon to update the event log table.

The event log table shows the following information:

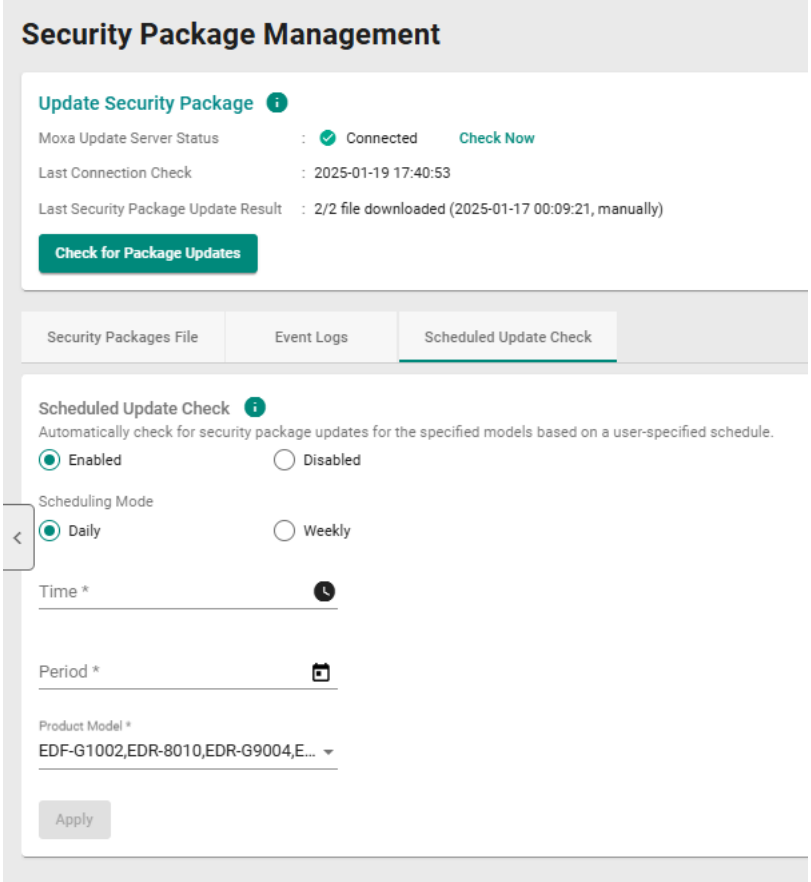
Field	Description
Time	The time the log entry was created.
Severity	The severity level assigned to the event.
Event	The category of the event.
Message	Additional details about the event.

Scheduled Update Check

From the **Scheduled Update Check** tab, you can configure a scheduled time and period to automatically check the Moxa server for security package updates.

Scheduling a Security Package Update Check

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Security Package Management**.
2. Go to the **Update Settings** tab.



Security Package Management

Update Security Package

Moxa Update Server Status : Connected Check Now

Last Connection Check : 2025-01-19 17:40:53

Last Security Package Update Result : 2/2 file downloaded (2025-01-17 00:09:21, manually)

Scheduled Update Check

Automatically check for security package updates for the specified models based on a user-specified schedule.

● Enabled ○ Disabled

Scheduling Mode

● Daily ○ Weekly

Time *

Period *

Product Model *

EDF-G1002,EDR-8010,EDR-G9004,E...

3. Set **Scheduled Update Check** to **Enabled**.
4. Choose a scheduling mode:

- ➢ **Daily**: Set the time of the day to perform the check.
- ➢ **Weekly**: Set the day of the week and time of the day to perform the check.

5. Configure the update period. The system will only perform update checks on the specified time and date during this period.
6. Select the product model(s). The system will only check for security package updates applicable to the select product models.
7. Click **Apply**.

Security Package Deployment

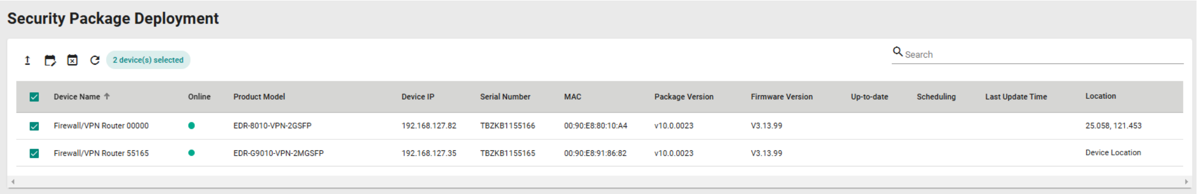
This section allows users to deploy security packages to managed devices.

Upgrading the Security Package of Managed Devices

Users can manually upgrade the security package of managed devices and check basic security package version information.

The table shows the following security package information:

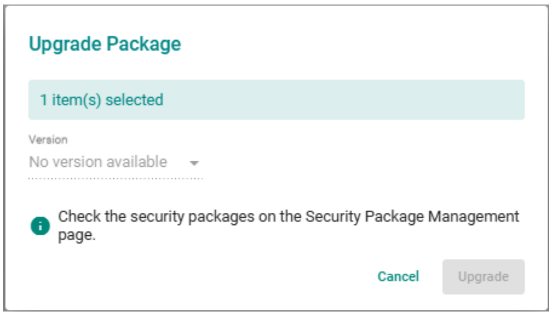
- **Package Version**: Shows the version of the security package currently installed on the device.
- **Up-to-date**: Indicates if the currently installed version is up to date. If not, the latest available version will be shown.


Security Package Deployment

☑	Device Name ↑	Online	Product Model	Device IP	Serial Number	MAC	Package Version	Firmware Version	Up-to-date	Scheduling	Last Update Time	Location
☑	Firewall/VPN Router 00000	●	EDR-8010-VPN-2GSFP	192.168.127.82	TBZKB1155166	00:90:E8:80:10:A4	v10.0.0023	V3.13.99				25.058, 121.453
☑	Firewall/VPN Router 55165	●	EDR-G9010-VPN-2MGSFP	192.168.127.35	TBZKB1155165	00:90:E8:91:86:82	v10.0.0023	V3.13.99				Device Location

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Security Package Deployment**.
2. Check the box of the device(s) you want to upgrade the security package for.
3. Click the **Upgrade** (↥) icon to upgrade the security package for the selected device(s).

   The **Upgrade Package** window will appear.


Upgrade Package

1 item(s) selected

Version
No version available

Check the security packages on the Security Package Management page.

4. Select a previously uploaded security package to upgrade to. Refer to Uploading a Security Package for instructions on how to upload security packages.
5. Click **Upgrade**.

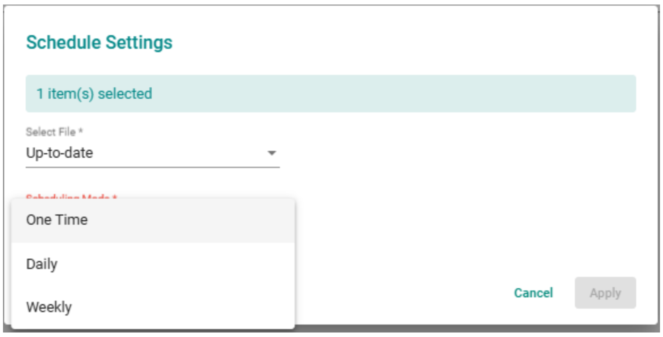
Scheduling a Security Package Deployment for Managed Devices

Deploying a security package to a device may disrupt services or operations. To minimize the potential impact of security package deployments, users can schedule the deployment for specific times where they are least likely to affect operations. Schedules can be configured to execute only once, or on a daily or weekly recurring basis.

Users can choose to deploy a specific version or the most-recent version of the security package available in the management database.

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Security Package Deployment**.
2. Check the box of the device(s) you want to configure a scheduled deployment for.
3. Click the **Schedule Settings** (📅) icon in the top-left corner.

   The **Schedule Settings** window will appear.



Schedule Settings

1 item(s) selected

Select File *: Up-to-date

Scheduling Mode *

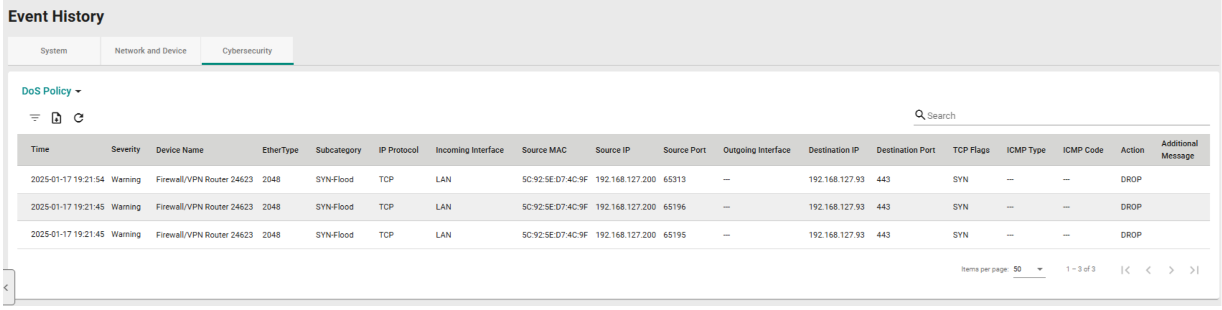
4. Configure the following settings:
   - **Select File**: Select a security package version to apply to the selected device(s).
   - **Scheduling Mode**: Select a scheduling mode. Depending on the selected mode, configure the following settings:
     - **One Time**: Select the date and time. One-time schedules can be configured for up to 30 days in the future.
     - **Daily**: Select the time and the schedule period. Daily schedules can be configured for up to 90 days in the future.
     - **Weekly**: Select the day of the week, the time, and schedule period. Weekly schedules can be configured for up to 90 days in the future.
5. Click **Apply**.

Deleting a Scheduled Security Package Deployment

1. Navigate to **Menu** (☰) **> Firewall Policy Management > Security Package Deployment**.
2. Check the box of the device(s) with the scheduled deployment you want to delete.
3. Click the **Delete Schedule** (☒) icon.
4. When prompted to confirm, click **Delete**.

Cybersecurity Event Log

If the MXview Security add-on license is activated, an additional Cybersecurity tab will be available on the **Event History** page, showing security events occurring on devices. The events include logs detected by the Trusted Access, Malformed Packets, DoS Policy, L2 Policy, L3-L7 Policy, Protocol Filter Policy, ADP, IPS, and Session Control functions. Refer to Viewing Event History.



Event History

Time	Severity	Device Name	EtherType	Subcategory	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP Flags	ICMP Type	ICMP Code	Action	Additional Message
2025-01-17 19:21:54	Warning	Firewall/VPN Router 24623	2048	SYN-Flood	TCP	LAN	5C:92:5E:D7:4C:9F	192.168.127.200	65313	---	192.168.127.93	443	SYN	---	---	DROP	
2025-01-17 19:21:45	Warning	Firewall/VPN Router 24623	2048	SYN-Flood	TCP	LAN	5C:92:5E:D7:4C:9F	192.168.127.200	65196	---	192.168.127.93	443	SYN	---	---	DROP	
2025-01-17 19:21:45	Warning	Firewall/VPN Router 24623	2048	SYN-Flood	TCP	LAN	5C:92:5E:D7:4C:9F	192.168.127.200	65195	---	192.168.127.93	443	SYN	---	---	DROP	

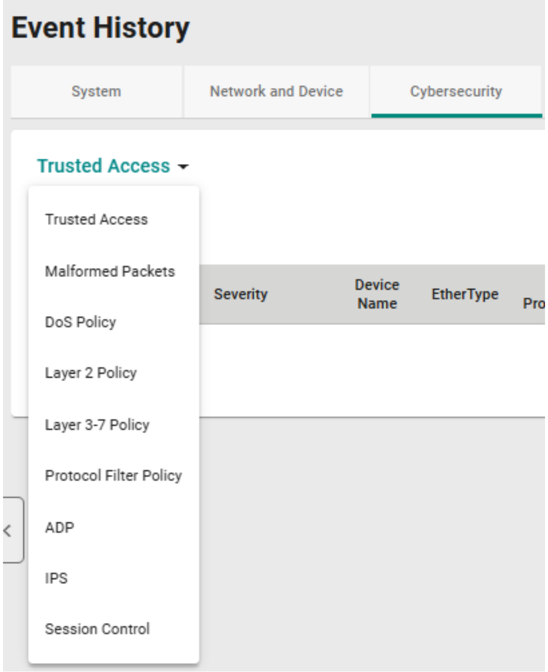
Items per page: 50 1 – 3 of 3

The table shows the following information:

Field	Description
Time	The time the event entry was created.
Severity	The severity level assigned to the event.
Device Name	The host name of the device that generated the event.
IPS Severity	The severity level assigned to the IPS event.
IPS Category	The category of the IPS event.
Ether Type	The Ethernet type of the connection.
IP Protocol	The IP protocol of the connection.
Incoming Interface	The name of the incoming interface where the event was registered.
Source MAC	The source MAC address of the connection.
Source IP	The source IP address of the connection.
Source Port	The source port of the connection.
Outgoing Interface	The name of the outgoing interface where the event was registered.
Destination IP	The destination IP address of the connection.
Destination Port	The destination port of the connection.
TCP Flags	The TCP flags of the TCP protocol.
ICMP Type	The ICMP type of the ICMP protocol.
ICMP Code	The ICMP Code of the ICMP protocol.
Action	The action performed based on the policy settings.
Additional Message	The additional message provided with the event.

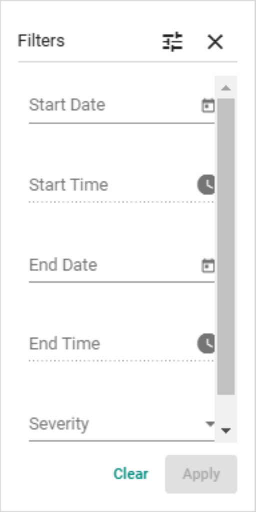
Viewing Cybersecurity Events

1. Navigate to **Menu** (☰) **> Event Management > Event History > Cybersecurity**.
2. Select the event type from the drop-down menu.



3. To filter event logs:

a. Click the **Filter** ( ) icon to open the filter menu. Select a start/end date and time or severity from the respective drop-menu.



b. Click the **Options** ( ) icon to configure advanced filters. Check the box of the specific event(s) you want to filter and click **Apply**. The event log will refresh immediately to reflect the selected criteria.

4. To export logs:

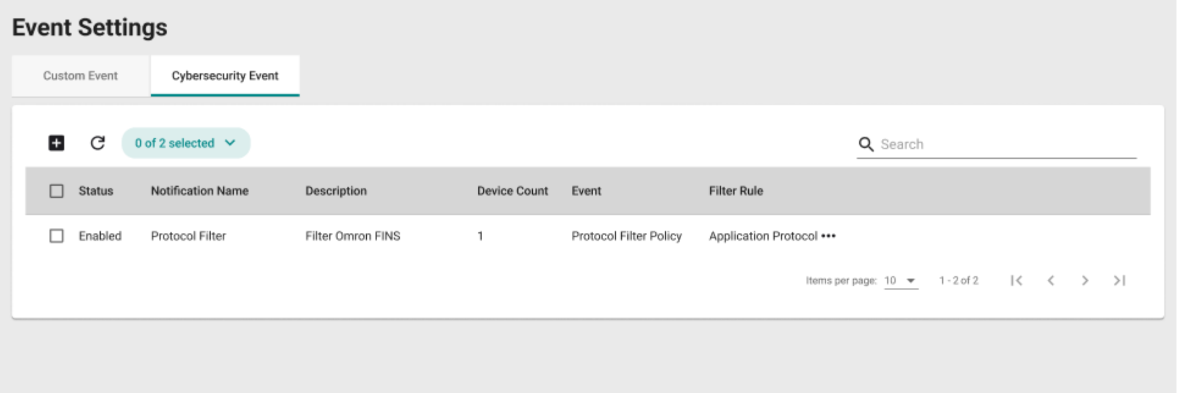
   a. Click the **Download All Logs** ( ) icon to export the current results as a CSV file

5. To refresh the event log data:

   a. Click the **Refresh** ( ) icon to renew the search results.

Cybersecurity Event Settings

If the MXview Security add-on license is activated, an additional **Cybersecurity Event** tab will be added to the **Event Settings** screen. From this tab, users can configure events for specific cybersecurity events. Refer to Events and Notifications.



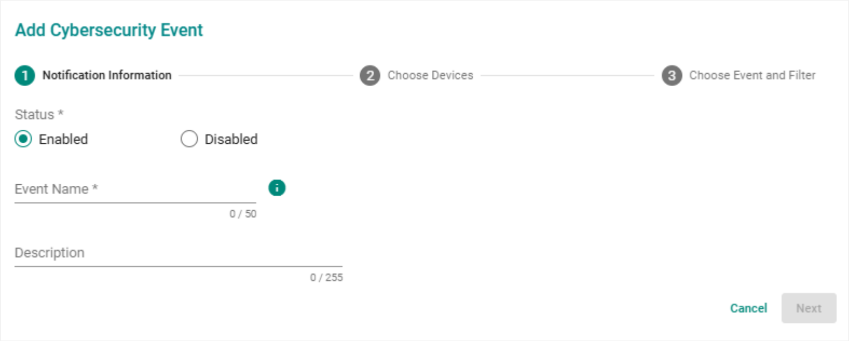
□	Status	Notification Name	Description	Device Count	Event	Filter Rule
□	Enabled	Protocol Filter	Filter Omron FINS	1	Protocol Filter Policy	Application Protocol •••

Adding a Cybersecurity Event

1. Navigate to **Menu** ( ) **> Event Management > Event Settings > Cybersecurity Event**.

2. Click the **Add** (⊞) icon in the top-left corner.

   The **Add Cybersecurity Event** window will appear.



Add Cybersecurity Event

1 Notification Information — 2 Choose Devices — 3 Choose Event and Filter

Status *

● Enabled ○ Disabled

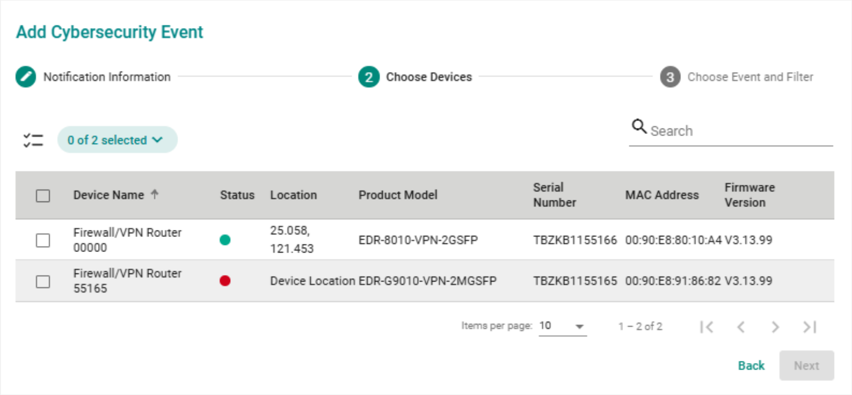
Event Name *

0 / 50

Description

0 / 255

3. Enter a name and description for the event.
4. Click **Next**.
5. Select the device(s) that will send notifications for the specified event(s).



Add Cybersecurity Event

✓ Notification Information — 2 Choose Devices — 3 Choose Event and Filter

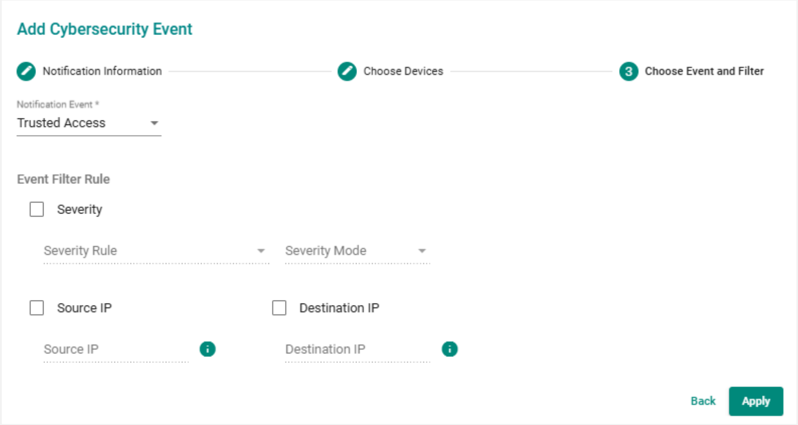
0 of 2 selected

Search

□	Device Name ↑	Status	Location	Product Model	Serial Number	MAC Address	Firmware Version
□	Firewall/VPN Router 00000	●	25.058, 121.453	EDR-8010-VPN-2GSFP	TBZKB1155166	00:90:E8:80:10:A4	V3.13.99
□	Firewall/VPN Router 55165	●	Device Location	EDR-G9010-VPN-2MGSFP	TBZKB1155165	00:90:E8:91:86:82	V3.13.99

Items per page: 10   1 – 2 of 2

6. Click **Next**.
7. Select the event type and configure the filter rules.
   a. Select the notification event type from the drop-down menu.



Add Cybersecurity Event

✓ Notification Information — ✓ Choose Devices — 3 Choose Event and Filter

Notification Event *

Trusted Access

Event Filter Rule

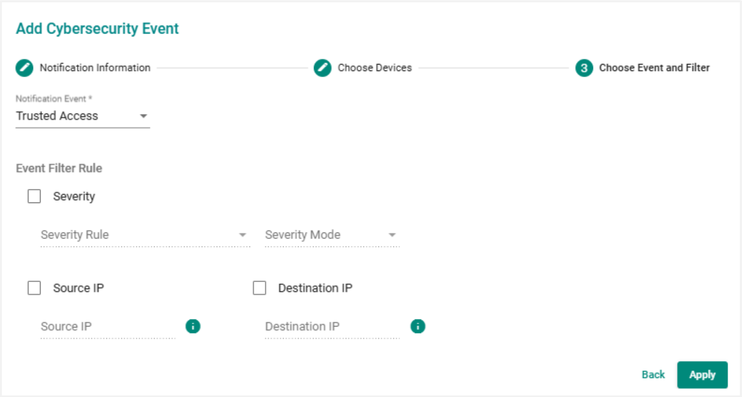
□ Severity

Severity Rule   Severity Mode

□ Source IP   □ Destination IP

Source IP   Destination IP

b. Specify the notification filter rules to determine when the device will send a notification for the event. Filter rule options may differ depending on the selected event type.



Add Cybersecurity Event

Notification Information — Choose Devices — 3 Choose Event and Filter

Notification Event *
Trusted Access

Event Filter Rule

□ Severity

Severity Rule — Severity Mode

□ Source IP □ Destination IP

Source IP — Destination IP

8. Click **Apply**.

Adding a Cybersecurity Event Notification

If the MXview Security is enabled, an additional **Cybersecurity Event** category will be added to the **Notification Management** function. This allows users to set up notifications to alert users when specific cybersecurity events occur on the network.

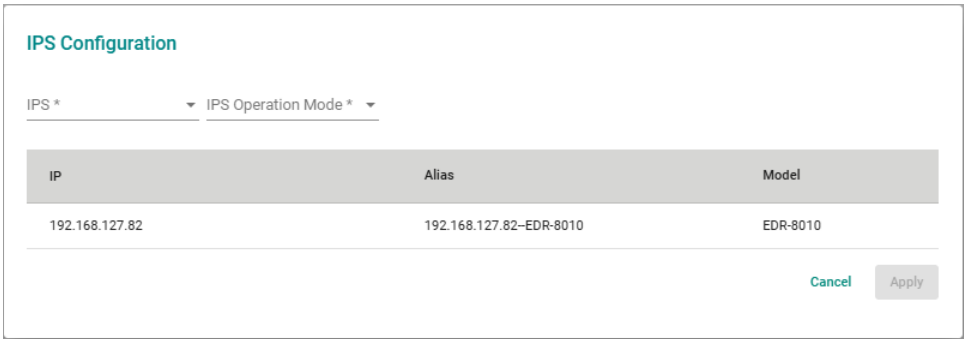
Refer to Configuring New Event Notifications for information and instructions on how to configure event notifications.

IPS Configuration

Use the **IPS Configuration** function to configure IPS settings for one or multiple selected devices at once.

Configuring IPS Settings

1. Navigate to **Menu** (☰) **> Device Management > Cybersecurity Controls > IPS Configuration**. The **IPS Configuration** window will appear.



IPS Configuration

IPS * — IPS Operation Mode *

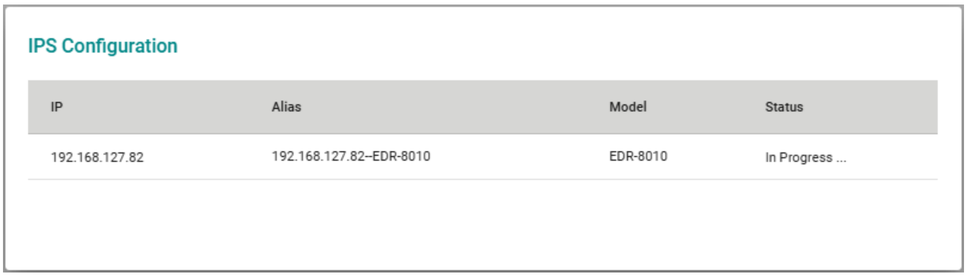
IP	Alias	Model
192.168.127.82	192.168.127.82–EDR-8010	EDR-8010

> **NOTE**
>
> To configure IPS settings for multiple devices, navigate to **Topology**. On the topology screen, select the devices and navigate to **Cybersecurity Controls > IPS Configuration** in the function bar.

2. Configure the following settings:
   - **IPS**: Enable or disable IPS functionality.
   - **IPS Operation Mode**: Select an IPS operation mode.
     - **Detection Mode**: In this mode, the system monitors traffic matching IPS rules configured on the selected device(s) to generate event logs but will not block any traffic.

- ❒ **Prevention Mode**: In this mode, the system will block any traffic that matches IPS rules configured on the selected device(s).

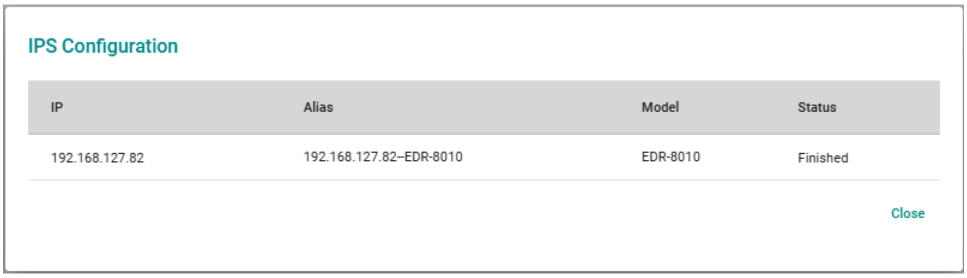
3. Click **Apply**.
4. The **Status** column will show the progress of the IPS configuration.



IPS Configuration

IP	Alias	Model	Status
192.168.127.82	192.168.127.82–EDR-8010	EDR-8010	In Progress ...

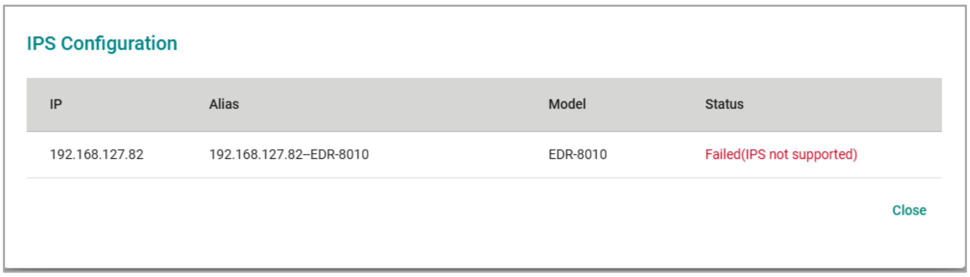
If successful, the status will show as **Finished**.



IPS Configuration

IP	Alias	Model	Status
192.168.127.82	192.168.127.82–EDR-8010	EDR-8010	Finished

If unsuccessful, an error description will be shown for troubleshooting.



IPS Configuration

IP	Alias	Model	Status
192.168.127.82	192.168.127.82–EDR-8010	EDR-8010	Failed(IPS not supported)

5. Click **Close** to close the status window.