

MXview One 1.8.0 User Manual

Version 9.0, September 2026

www.moxa.com/products



© 2026 Moxa Inc. All rights reserved.

MXview One 1.8.0 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

© 2026 Moxa Inc. All rights reserved.

Trademarks

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

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction	9
Key Features	9
Web-based Operation	9
Auto Discovery and Topology Visualization	9
Event Management	9
Configuration and Firmware Management	9
Traffic Monitoring	9
System Requirements	10
Supported Devices	10
2. Installation and Uninstallation	11
Installation Procedure	11
For Windows	11
For Ubuntu	11
Uninstallation	12
For Windows	12
For Ubuntu	12
3. Getting Started	13
MXview One Control Panel	13
Server Control	13
Configuration	14
DB Backup & Restore	17
Plug-in Manager	19
Certificates	26
Starting the MXview One Server and Logging Into MXview One	37
Logging Into MXview One Remotely	38
Switching to the Legacy UI	41
Legacy UI Limitations	41
License Management	42
Checking the License	42
Adding a New License	43
Using Device Discovery	44
Account Management	46
.....	47
Default Accounts and Role Privileges	47
Adding User Accounts	47
Modifying User Accounts	48
Editing Accessible Groups	48
Deactivating User Accounts	49
Activating Deactivated User Accounts	50
Deleting User Accounts	50
Configuring the Password Policy	51
Configuring Login Messages	52
Configuring Login Lockout Settings	52
Configuring Session Control Settings	53
Changing the Display Language	54
Two-factor Authentication	54
Enabling Two-factor Authentication	54
Setting Up Two-factor Authentication Methods	55
Logging In With Two-factor Authentication	55
Changing Login Verification Methods	55
Login Authentication	55
Applying an Authentication Protocol	56
RADIUS Server	56
Viewing the RADIUS Server List	57
Adding a RADIUS Server	57
Editing a RADIUS Server	58
Configuring Server Priority and Failover	58
Deleting a RADIUS Server	58

LDAP Management.....	58
Connection Settings.....	58
Role Mapping.....	60
4. License Management	62
License Management Overview.....	62
License Type	63
Adding a New License	63
Adding an Add-on License.....	66
Deactivating a License.....	69
Reactivating a Deactivated License	70
Transferring a License to a Different Instance of MXview One.....	72
Quantity of Monitored Devices Exceeds the Number of Node-based Licenses	73
5. Dashboard Widgets	75
Dashboard Overview	75
Device Summary	75
Event Highlights	76
6. Device Discovery and Polling	77
Device Discovery Overview	77
Configuring IP Address Scan Ranges	78
Configuring Device Polling Settings	80
Changing the Default SNMP Configuration.....	82
Changing Modbus TCP Settings	83
Changing EtherNet/IP Settings	83
Changing Siemens S7comm Settings	83
7. Topology Management.....	85
Topology Overview	85
Viewing the Topology Map	86
Viewing Recent Events	89
Organizing the Topology Structure By Group Function	91
Redundant Topologies	93
PoE Power Consumption Visualization.....	94
VPN Tunnel Visualization	95
Port Trunking	95
Adding Devices and Links	96
Deleting Devices and Links	99
Updating the Topology Map.....	99
Refreshing the Topology Layout.....	100
Creating a New Topology Map	101
Setting/Editing the Background Image	102
Editing the Topology Appearance	103
Editing the Device Appearance	106
Exporting the Topology Map.....	107
8. Network and Traffic Monitoring	108
Viewing Link Properties	108
Viewing Port Traffic.....	109
Viewing Packet Error Rates	109
Monitoring Traffic Loads	110
Monitoring Network Security	111
Monitoring VLAN.....	116
Viewing the VLAN Distribution.....	116
Viewing the VLAN Report.....	116
Configuring Severity Thresholds for Traffic and Fiber Status Monitoring Events.....	118
Configuring Custom Port Labels	120
9. SFP Fiber Status	121
Viewing the SFP Fiber Status in Table View	121
Synchronize the SFP Threshold From the Device.....	122
10. Device Operation in the Topology	123
Viewing the Device List.....	123
Importing Device Configurations.....	126
Exporting Device Configurations	127
Upgrading Firmware.....	128

Configuring SNMP Trap Server	129
Configuring Port Settings	130
Configuring SNMP Communication Protocol	131
Configuring MXview One Polling Interval	132
Configuring Device Accounts	133
Modifying the Device Alias	134
Changing the Device Icon	135
Signing on to Device Web Consoles	136
Managing and Running Scripts	137
Running a CLI Script	137
Running a Saved CLI Script	140
Changing Device Groups	141
Refreshing the Device Status	142
Deleting Devices	142
11. Device Management	144
Configuration and Control	144
Configuration and Control Overview	144
Account and Password	155
Account Management Overview	155
Password Automation Overview	157
Account Audit Overview	161
Default Password Audit Overview	163
Temporary Accounts Overview	163
12. Saved CLI Scripts	167
Saved CLI Scripts Overview	167
CLI Scripts	168
Adding a CLI Script	168
Searching for a CLI Script	168
Editing a CLI Script	168
Deleting a CLI Script	169
Deleting Multiple CLI Scripts	169
Creating a CLI Script Scheduled Task	169
Execution Results	170
Download All Execution Results	170
Delete All CLI Script Execution Results	171
Delete Execution Results Prior to a Specified Time	171
Script Automation	171
Adding a Script Automation	171
Editing a Script Automation	173
Deleting a Script Automation	173
Deleting Multiple Script Automations	174
Automation Buttons	174
Setting the Automation Button Display Mode	174
Configuring Automation Button Authentication Settings	174
Editing an Automation Button Group	175
Editing an Automation Button	176
Creating an Automation Button Group	178
Changing the Automation Button Widget Size	179
Previewing Affected Devices	180
13. Firmware Management	182
Firmware Management Overview	182
Checking the Firmware Status	182
Model Series Table Overview	183
Selecting a Firmware Version	184
Upgrading Firmware	185
14. Baseline Management	187
Baseline Overview	187
Creating a Configuration and Firmware Baseline	187
Executing a Manual Baseline Audit	188
Configuring Scheduled Baseline Audits	188

Exporting the Baseline	189
Searching the Baseline Data	189
Comparing Configuration Files	189
Executing a Manual Baseline Audit on Selected Devices.....	190
Setting the Current Configuration and Firmware as the New Baseline.....	191
Restoring Devices to the Baseline Settings	192
Removing Device(s) from the Baseline.....	192
Not in Baseline Overview	193
Searching the Not in Baseline Data	194
Adding Device(s) to the Baseline.....	194
15. Events and Notifications	195
Event Monitoring	195
Viewing System Events	195
Viewing Network and Device Events	196
Configuring Event Thresholds and Severity Levels	197
Notification Methods.....	198
Configuring Email Server Settings	198
Notification Management	198
Configuring Notification Actions.....	199
Adding a Microsoft Teams Action	199
Configuring Event Notifications	201
Editing or Exporting Registered Actions	202
Editing or Exporting Notification Configurations	202
Custom Event Management	203
Configuring Custom Events.....	204
Viewing or Exporting Custom Event Settings.....	204
Editing Custom Events	205
Syslog Settings	205
Configuring the Built-in Syslog Server.....	205
Viewing Syslog Events	206
Configuring Syslog Forwarding.....	208
Enabling/Disabling Internal Event Forwarding	209
SNMP Trap Forwarding	209
Enabling Trap Forwarding	210
Viewing the SNMPv3 EngineID	210
Viewing the Destinations List	210
Adding a Destination.....	211
Editing a Destination.....	212
Deleting a Destination.....	212
16. Inventory Management	213
Assets and Warranty	213
Asset List Overview	213
Warranty Management Overview.....	214
Warranty Notifications Overview	218
Rogue Device Detection.....	218
Rogue Device Settings Overview	219
Device Baseline Overview	220
Current Rogue Devices Overview.....	221
Rogue Device History Overview.....	223
17. Backups, Restores, and Compares	225
Backing Up the MXview One Database.....	225
Backing Up Device Configurations	226
Restoring Device Configurations	226
Comparing Archived Configuration Files.....	227
Creating Maintenance Scheduler for Database/Configuration Backups	228
18. Custom Integrations.....	230
OPC UA Server Overview	230
Viewing the OPC Tags Table	230
Adding an OPC Tag.....	230
Editing an OPC Tag.....	231

Deleting an OPC Tag	231
Deleting Multiple OPC Tags	232
Configuring OPC UA Server Settings	232
Managing RESTful API Keys	233
Embedding Web Widgets	234
19. Wireless Add-on Module	236
Introduction	236
System Requirements	236
Supported Devices	236
Getting Started With the Wireless Add-on Module	237
Wireless Module Features	238
Main Dashboard	238
Dynamic Wireless Client Roaming	238
AP/Client Device Dashboard	240
AP Device Dashboard	240
Client Device Dashboard	241
Wireless Device Summary	242
Wireless Roaming Playback	243
20. Power Add-on Module	245
Introduction	245
System Requirements	245
Supported Devices With PRP/HSR Features	245
Getting Started With the Power Add-on Module	246
Power Module Features	247
Topology	247
Ungrouping an IED Group	248
Creating an IED Group	252
Import SCD	253
GOOSE Message	253
21. Security Add-on Module	257
Introduction	257
System Requirements	257
Supported Devices	257
Getting Started With the Security Add-on Module	258
IPS License Management	258
Viewing IPS License Information	259
Adding an IPS License	259
Registering an IPS-licensed Device	260
Deregistering an IPS-licensed Device	261
Transferring an IPS License	261
Configuring IPS License Depletion Notifications	262
Checking Registered Devices	262
Security Module Features	263
Main Dashboard	263
Policy Profile Management	264
Policy Profiles	264
Inspection Objects	269
Interface Objects	271
Policy Profile Deployment	272
Security Package Management	273
Security Package Files	273
Event Logs	275
Scheduled Update Check	276
Security Package Deployment	277
Upgrading the Security Package of Managed Devices	277
Scheduling a Security Package Deployment for Managed Devices	277
Deleting a Scheduled Security Package Deployment	278
Cybersecurity Event Log	278
Viewing Cybersecurity Events	279
Cybersecurity Event Settings	279

Adding a Cybersecurity Event	280
Adding a Cybersecurity Event Notification.....	280
IPS Configuration	281
Configuring IPS Settings	281
A. Network Port Usage.....	282
MXview One Central Manager	282
Inbound Traffic	282
Outbound Traffic	282
MXview One.....	282
Inbound Traffic	282
Outbound Traffic	282
Internal Services.....	283
Device Outbound.....	283
B. Installation Directories.....	284
Windows.....	284
Linux.....	284

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, Windows 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](https://www.moxa.com) for a list of Moxa devices that are supported.

2. Installation and Uninstallation

Installation Procedure

The Windows and Ubuntu versions of MXview One must be installed and operated in their respective operating system environments. Installation packages and backup files are not interchangeable between Windows and Ubuntu.

For Windows



NOTE

If your computer already has MXview installed, uninstall it first before installing MXview One.

1. Download the MXview One software from www.moxa.com and install the program.
2. During installation, agree to the EULA (End-User License Agreement), choose the installation directory, and the default language.
3. After the installation is complete, shortcuts for launching the MXview One server will be created on the desktop and in the start menu.

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**.
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
```

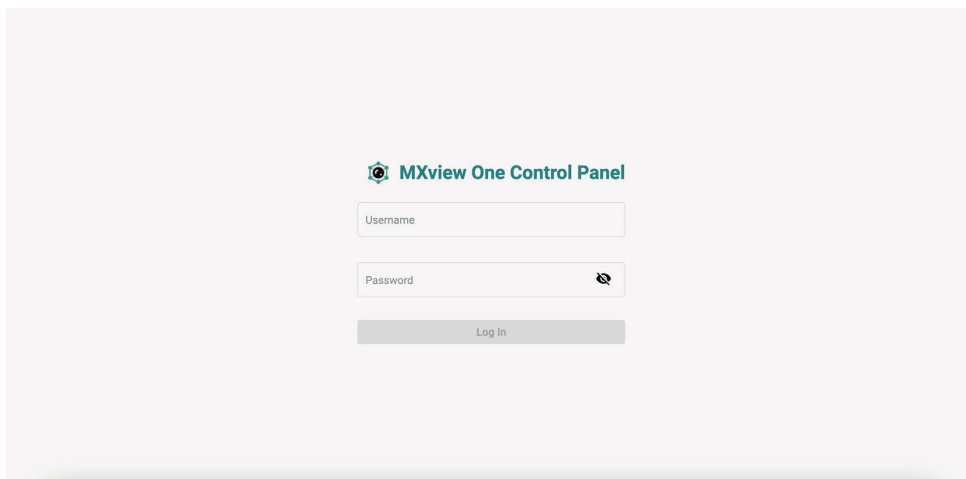
Open a web browser and navigate to [https://\[host IP address\]:7100](https://[host IP address]:7100). The host IP address is the IP of the computer running MXview One. The default IP address is: 127.0.0.1

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

For Windows users:

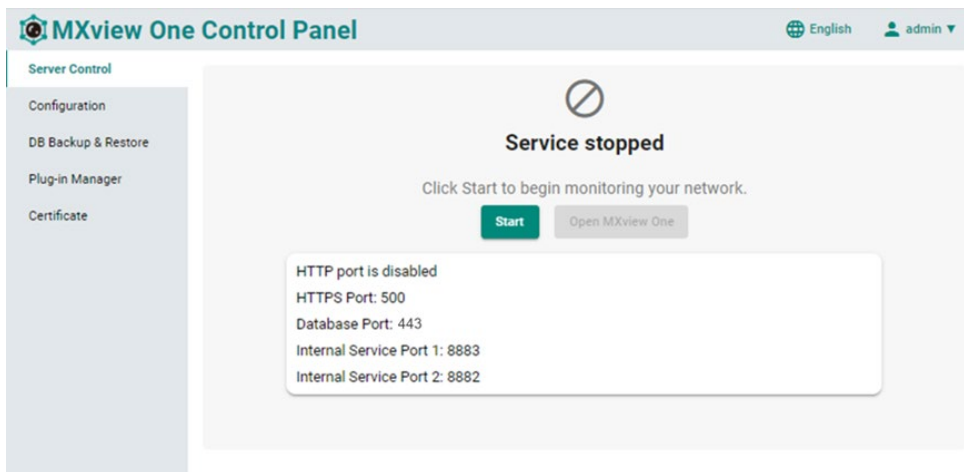
Start the MXview One server on the computer before launching the MXview One web console. On the server computer, double-click the MXview One desktop shortcut in the Windows operating system.

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

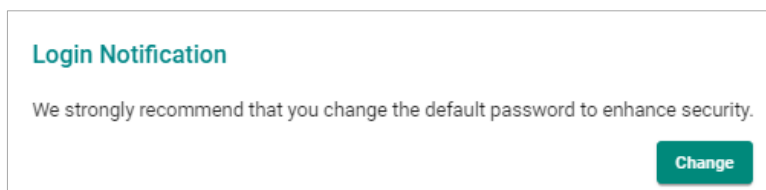


Provide the following login credentials

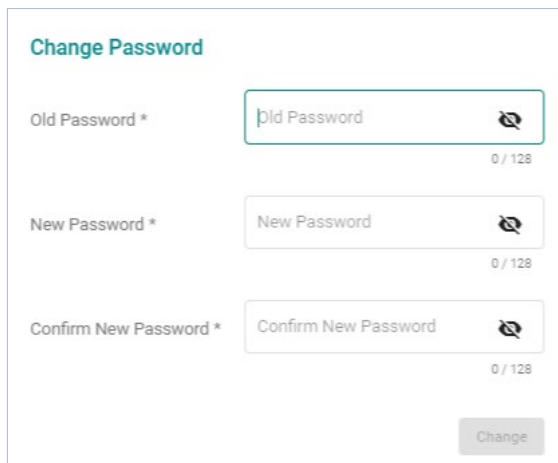
- **Username:** The default username is **admin**.
- **Password:** The default password is **moxa**.



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



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



Configuration

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

The screenshot shows the MXview One Control Panel interface. On the left is a sidebar with navigation links: Server Control, Configuration (highlighted), DB Backup & Restore, Plug-in Manager, and Certificates. The main content area is titled 'MXview One Central Manager Server Settings'. It contains several configuration fields:

- Enable ***: A dropdown menu with 'Yes' selected.
- Manage Licenses Through MXview One Central Manager ***: A dropdown menu with 'Yes' selected.
- Server Address ***: A section with two input fields:
 - IP/Domain Name**: A text input field containing 'IP/Domain Name'.
 - Port**: A text input field containing '8883'. Below it, a small text '1-65535' indicates the valid range.
- Authentication ***: A section with a **Password** input field. Below the field, it says 'At least 8 characters' and '0 / 63'. There is an eye icon to toggle password visibility.
- Site ID ***: A text input field containing '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 Password: *****
1-65535 At least 8 characters 16 / 63

Internal Service Port 2 * Port: 8882 Password: *****
1-65535 At least 8 characters 16 / 63

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

Save

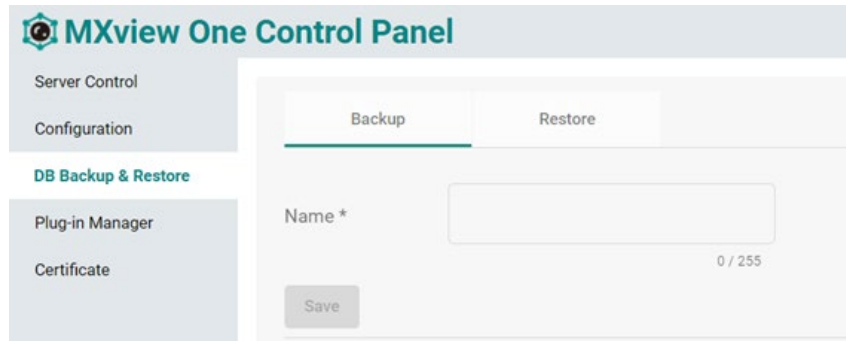
- **Web Interface**
 - **HTTPS:** Specify the HTTPS port of the MXview One Central Manager server. The default port is 443.
 - **HTTP:** Enable or disable HTTP. If enabled, specify the listening port of the server. The default port is 80.
- **Database Interface**
 - **Port:** Specify the service port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

When finished, click **Save**.

DB Backup & Restore

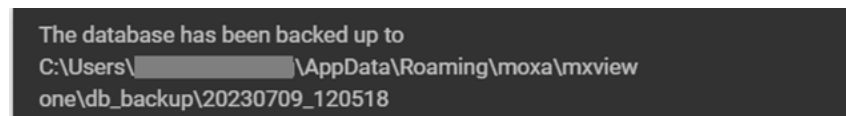
1. Navigate to **DB Backup & Restore** on the MXview One Control Panel.

The Database Backup & Restore screen will appear and includes **Backup** and **Restore** functions.



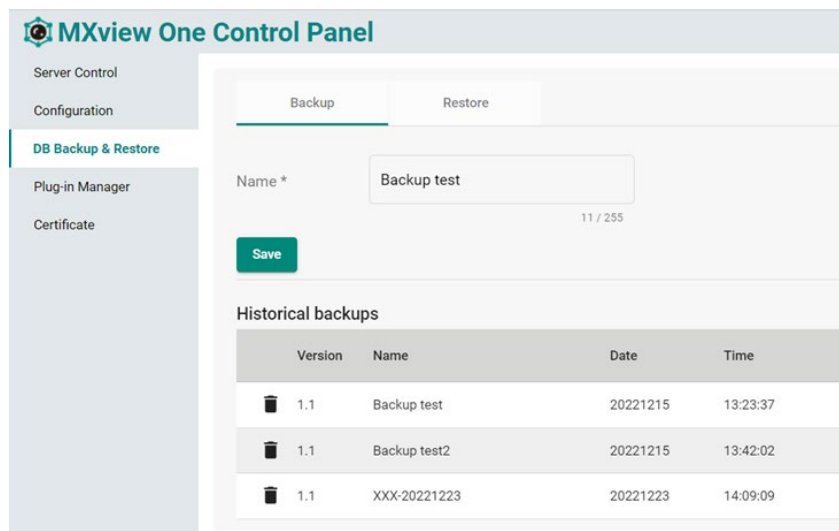
The screenshot shows the MXview One Control Panel interface. On the left is a sidebar with navigation links: Server Control, Configuration, DB Backup & Restore (highlighted), Plug-in Manager, and Certificate. The main area has two tabs: Backup and Restore. The Backup tab is active, showing a form with a 'Name *' label and a text input field. Below the input field is a 'Save' button. A character count '0 / 255' is visible at the bottom right of the input field.

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.



The screenshot shows the MXview One Control Panel interface after a successful backup. The 'Backup' tab is active, and the 'Name' field now contains 'Backup test'. The 'Save' button is green. Below the form is a section titled 'Historical backups' containing a table with the following data:

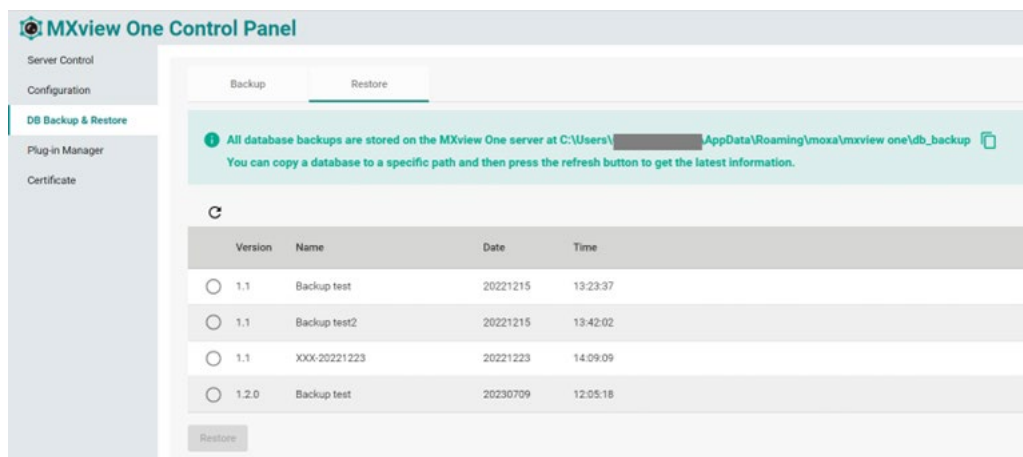
Version	Name	Date	Time
1.1	Backup test	20221215	13:23:37
1.1	Backup test2	20221215	13:42:02
1.1	XXX-20221223	20221223	14:09:09

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.

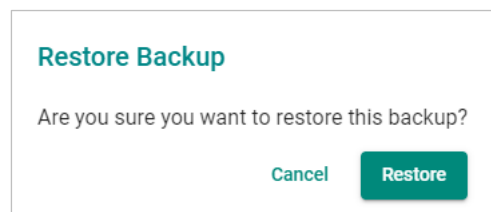
1. Click the **Restore** Tab.



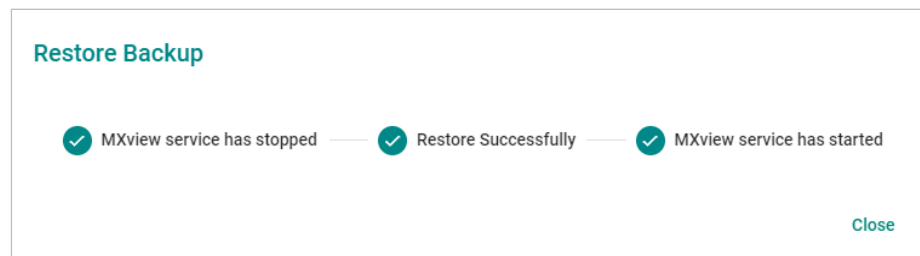
2. Choose the backups you want to restore in the table. You can also copy a database to a specific path and then press the refresh button to get the latest result.

3. Click **Restore**.

A confirmation screen will appear.



4. Displaying the restoration process.



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

The screenshot shows the 'MXview One Control Panel' with a sidebar menu containing 'Server Control', 'Configuration', 'DB Backup & Restore', 'Plug-in Manager' (selected), and 'Certificates'. The main area is titled 'Plug-in Manager' and has two tabs: 'Moxa Devices' (active) and 'SNMP Devices'. Below the tabs, it says 'Plug-in Version v1.3.231226'. A green information box states: '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.' Below this is an 'Upload a plug-in file' section with a 'Select a plug-in file' button and an 'Upload' button. Further down is a 'Supported Device Model(300)' section with a search bar and a table of device models.

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

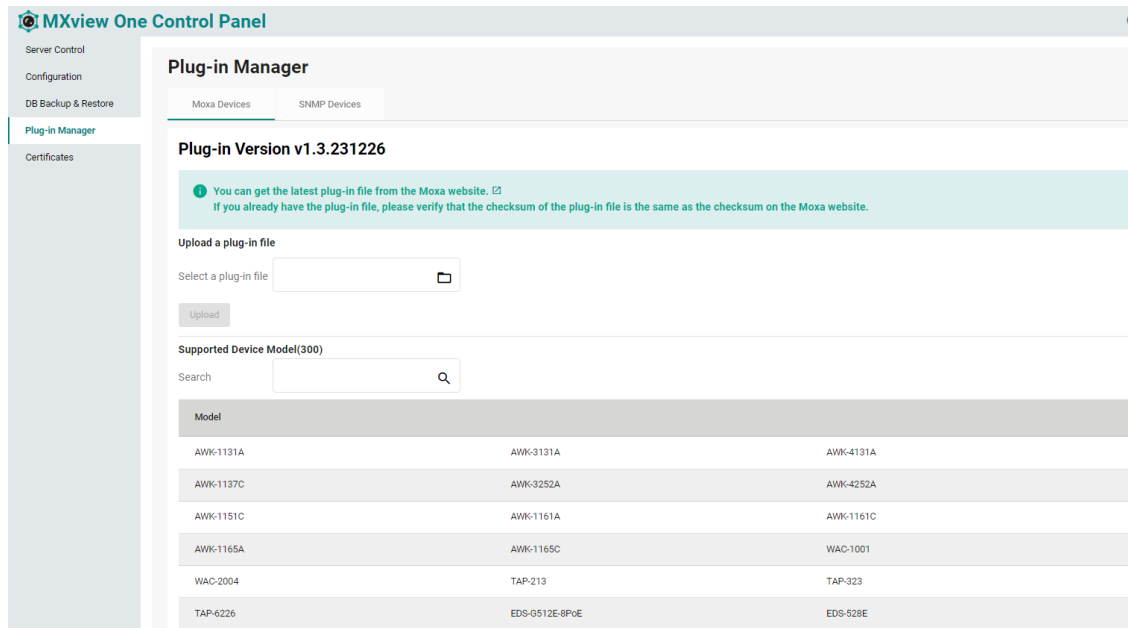
Steps to Upload a Plug-in File:

1. Stop MXview One.

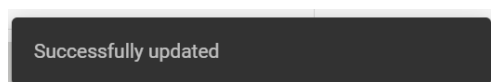
The screenshot shows the 'MXview One Control Panel' with a sidebar menu. The main area displays a 'Service stopped.' message with a 'Start' button and an 'Open MXview One' button. Below the message, it says 'Click Start to begin monitoring your network.' A box lists the following ports: 'HTTP port is disabled', 'HTTPS Port: 550', 'Database Port: 5432', 'Internal Service Port 1: 8883', and 'Internal Service Port 2: 8882'.

2. Download the latest plug-in file from the Moxa website. [Moxa MXview One Series - Resources](#)

3. Navigate to the **Plug-in Manager** on the **Control Panel**.



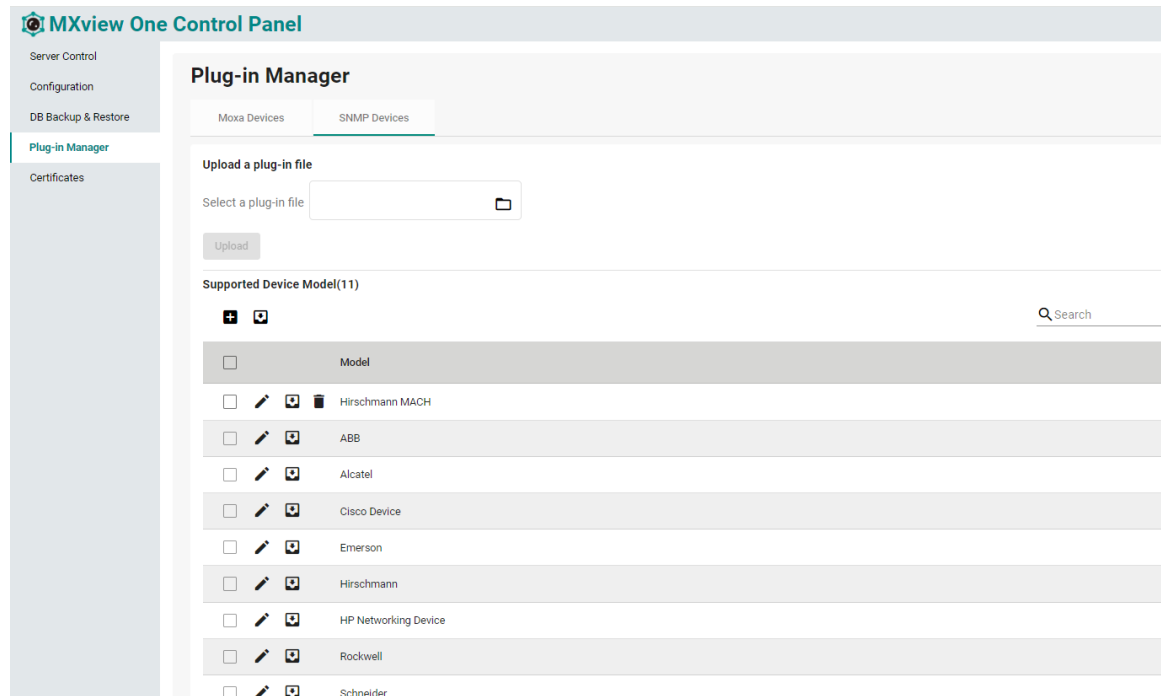
4. Click the folder () icon in **Select a Plug-in File** to upload the file (.zip) from your local machine.
5. Click **Upload** and if successful, the message below will be displayed.
MXview One will upload the plug-in file and display the supported devices.



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.



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.

The screenshot shows the 'Add an SNMP Model Plug-In' interface in the MXview One Control Panel. The top navigation bar includes 'English' and 'admin'. The left sidebar lists 'Server Control', 'Configuration', 'DB Backup & Restore', 'Plug-in Manager' (selected), and 'Certificates'. The main area has a progress bar with four steps: 1. Specify sysObjectID, 2. Load Device Files, 3. Select and Test OIDs, and 4. OID Alias and Value Definition. Step 1 is active, showing input fields for 'sysObjectID *' (with a 'Get sysObjectID' button) and 'Model *'. A 'Next' button is at the bottom.

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.

The 'Get sysObjectID From a Device' dialog box contains the following fields: 'IP Address *' (with a text input containing '192.168.127.32'), 'SNMP Settings *' (including 'SNMP Version' dropdown set to 'V1' and 'Port' input set to '161'), 'Username' (0/32), 'Password' (0/64), 'Read Community' (set to 'public', 6/32), 'Data Encryption' dropdown set to 'NoAuth', 'Authentication' dropdown set to 'MD5', 'Encryption Protocol' dropdown set to 'DES', and 'Encryption Password' (0/64). At the bottom right, there are 'Cancel' and 'Get sysObjectID' buttons, with the latter highlighted by a red rectangle.

After specifying all the necessary information, click **Get sysObjectID**. If successful, a confirmation message will appear.

Model: Specify the model name. The model name only supports A-Z a-z 0-9 _ - , (comma) () and space.

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

4. Load Device Files.

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

< **Add an SNMP Model Plug-In**

Specify sysObjectID Load Device Files Select and Test OIDs OID Alias and Value Definition

MIB Files:

Icon File *: 

Icon Preview: 

Back Next

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

MXview One Control Panel English id

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

< **Add an SNMP Model Plug-In**

Specify sysObjectID Load Device Files **Select and Test OIDs** OID Alias and Value Definition

Search

☐	OID	OID Name	OID Syntax
☐	1.3.6.1.4.1.248.16.100.1.1	hnmMgmtDiscMode	Integer32(read-write(1),read-only(2))
☐	1.3.6.1.4.1.248.16.100.1.2	hnmMgmtDiscMacAddr	OctetString
☐	1.3.6.1.4.1.248.16.100.1.3	hnmMgmtDiscIntfType	Integer32(loopback-intf(1),router-intf(2),mgmt-intf(3))
☐	1.3.6.1.4.1.248.16.100.1.4	hnmMgmtDiscSwVersion	OctetString
☐	1.3.6.1.4.1.248.16.100.1.5	hnmMgmtDiscProductDescr	OctetString
☐	1.3.6.1.4.1.248.16.100.2.1	hnmMgmtDiscCfgUUID	OctetString
☐	1.3.6.1.4.1.248.16.100.2.2	hnmMgmtDiscCfgProto	Integer32(none(1),bootp(2),dhcp(3))
☐	1.3.6.1.4.1.248.16.100.2.3	hnmMgmtDiscCfgIPAddrType	Integer32(unknown(0),ipv4(1),ipv6(2),dms(16))
☐	1.3.6.1.4.1.248.16.100.2.4	hnmMgmtDiscCfgIPAddr	OctetString

- a. Test OIDs.
- Click on the **Test OID** () icon of the OID you want to test.
The **Test OID** window will appear.
 - 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

Value retrieved from OID

Value: 3

SNMP Settings *

SNMP Version: V1 Port: 161

Username: Password: 0 / 64

Read Community: public 6 / 32

Data Encryption: NoAuth Authentication: MD5

Cancel Get OID Value

- b. Select OIDs.
 - i. Select the OIDs you want to monitor in MXview One.
 - ii. When finished, click **Next**.

MXview One Control Panel

Server Control

Configuration

DB Backup & Restore

Plug-in Manager

Certificates

☐	1.3.6.1.4.1.248.16.100.1.1	hnmAgentDiscMode	Integer32(read-write(1),read-only(2))
☐	1.3.6.1.4.1.248.16.100.1.2	hnmAgentDiscMacAddr	OctetString
☐	1.3.6.1.4.1.248.16.100.1.3	hnmAgentDiscPortType	Integer32(loopback-intf(1),router-intf(2),mgmt-net(3))
☐	1.3.6.1.4.1.248.16.100.1.4	hnmAgentDiscSwVersion	OctetString
☐	1.3.6.1.4.1.248.16.100.1.5	hnmAgentDiscProductDescr	OctetString
☐	1.3.6.1.4.1.248.16.100.2.1	hnmAgentDiscCfgyUd	OctetString
☐	1.3.6.1.4.1.248.16.100.2.2	hnmAgentDiscCfgyPhoto	Integer32(rone(1),boots(2),fncp(3))
☒	1.3.6.1.4.1.248.16.100.2.3	hnmAgentDiscCfgyPAddrType	Integer32(unknown(0),ipv4(1),ipv6(2),other(16))
☐	1.3.6.1.4.1.248.16.100.2.4	hnmAgentDiscCfgyPAddr	OctetString
☐	1.3.6.1.4.1.248.16.100.2.5	hnmAgentDiscCfgyPAddrType	Integer32(unknown(0),ipv4(1),ipv6(2),other(16))
☒	1.3.6.1.4.1.248.16.100.2.6	hnmAgentDiscCfgyPAddrType	Integer32(unknown(0),ipv4(1),ipv6(2),other(16))
☐	1.3.6.1.4.1.248.16.100.2.7	hnmAgentDiscCfgyPAddr	OctetString
☐	1.3.6.1.4.1.248.16.100.2.8	hnmAgentDiscCfgyAction	Integer32(other(1),activate(2))
☐	1.3.6.1.4.1.248.16.100.2.9	hnmAgentDiscCfgyBlinking	Integer32(enable(1),disable(2))

Back Next

6. OID Alias and Value Definition

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

< Add an SNMP Model Plug-In

Specify sysObjectID Load Device Files Select and Test OIDs **OID Alias and Value Definition**

Search

OID Name	OID Alias	OID Syntax	OID Syntax Mapping
hmMgmtDiscMode		Integer32(read-write(1),read-only(2))	read-write(1), read-only(2)
hmMgmtDiscIntfType		Integer32(loopback-intf(1),router-intf(2),mgmt-intf(3))	loopback-intf(1), router-intf(2), mgmt-intf(3)
hmMgmtDiscProductDescr		OctetString	
hmMgmtDiscCfIPIAddrType		Integer32(unknown(0),ipv4(1),ipv6(2),dns(16))	unknown(0), ipv4(1), ipv6(2), dns(16)
hmMgmtDiscCfIPrefLen			
hmMgmtDiscCfGwIPAddrType		Integer32(unknown(0),ipv4(1),ipv6(2),dns(16))	unknown(0), ipv4(1), ipv6(2), dns(16)
hmMgmtDiscCfGwIPAddr		OctetString	
hmMgmtDiscCfGwIPAction		Integer32(other(1),activate(2))	other(1), activate(2)

Back Complete

If necessary, you can manually edit the OID information.

- 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 hmMgmtDiscIntfType

OID Alias 4 / 64

OID Syntax Mapping

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

OID Syntax Mapping

+ Value Display Name

1 loopback-intf 1 / 64 13 / 64

2 router-intf 1 / 64 11 / 64

3 mgmt-intf 1 / 64 9 / 64

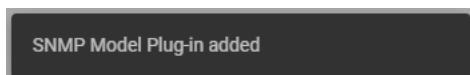
Cancel Apply

- Edit the OID Alias and OID Syntax Mapping information as required.
 - When finished, click **Apply**.
- When finished with all four steps, click **Complete**. The **Update Plug-in** window will appear.

Update Plugin

MXview One stopped **Updating** Starting MXview One

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



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



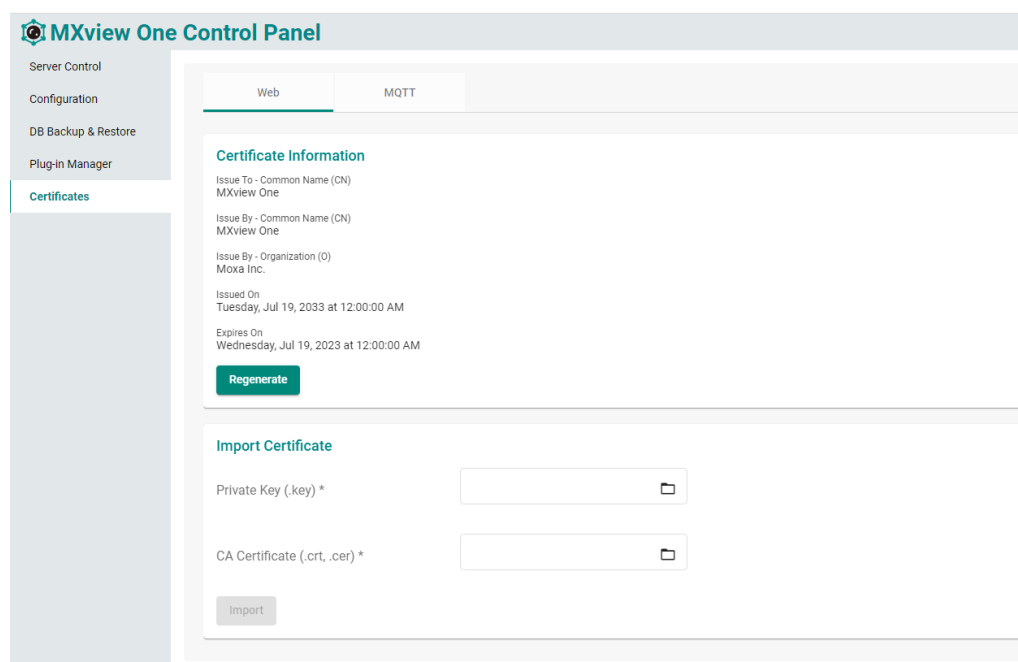
Certificates

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:

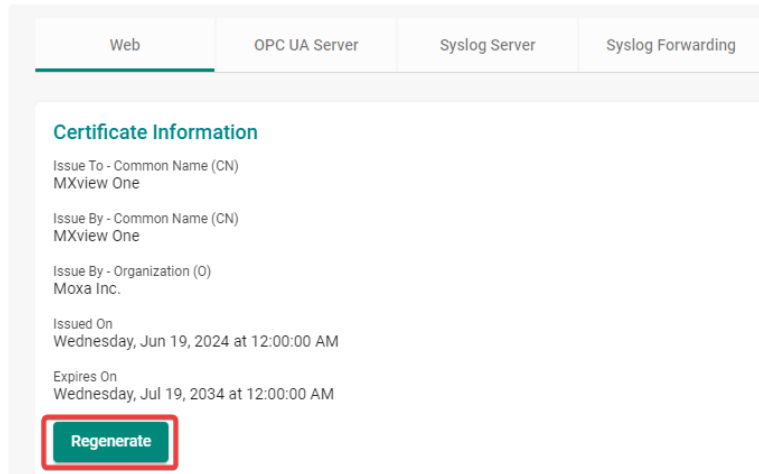
- Issue To - Common Name (CN)
- Issue By - Common Name (CN)
- Issue By - Organization (O)
- Issued On
- Expires On



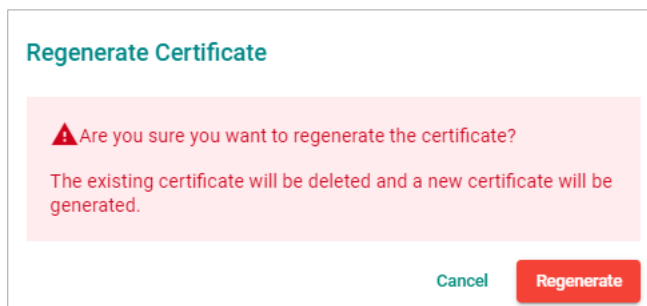
Regenerating the Web Certificate

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

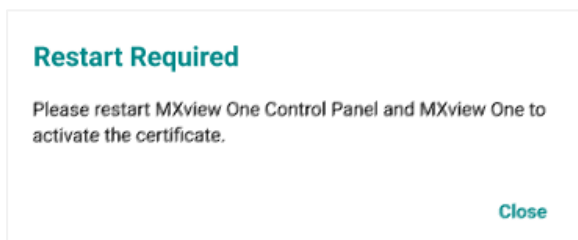
The **Regenerate Certificate** window will appear.



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



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.



Importing a Web Certificate

You can manually import 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.



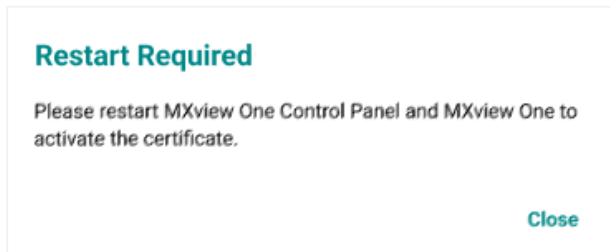
Import Certificate

Private Key (.key) *

CA Certificate (.crt, .cer) *

Import

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.



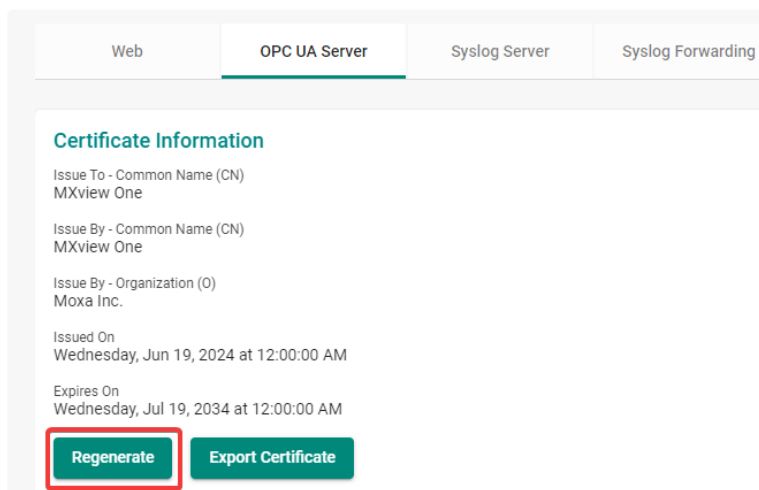
OPC UA Server Certificates

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

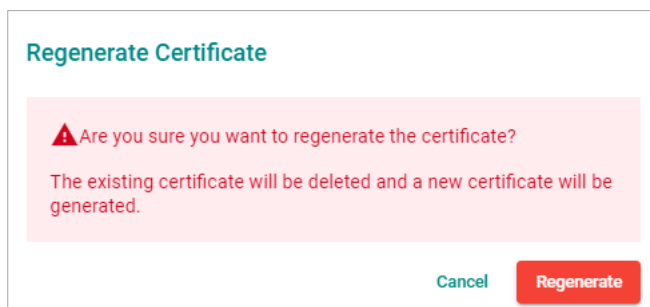
- Issue To – Common Name (CN)
- Issue By – Common Name (CN)
- Issue By – Organization (O)
- Issued On
- Expires On

Regenerating the OPC UA Server Certificate

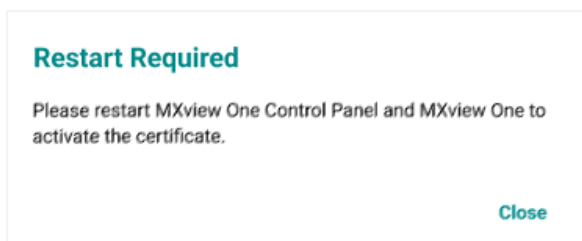
1. Navigate to **Control Panel > Certificates**.
 2. Go to the **OPC UA Server** tab.
 3. Click the **Regenerate** button.
- The **Regenerate Certificate** window will appear.



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

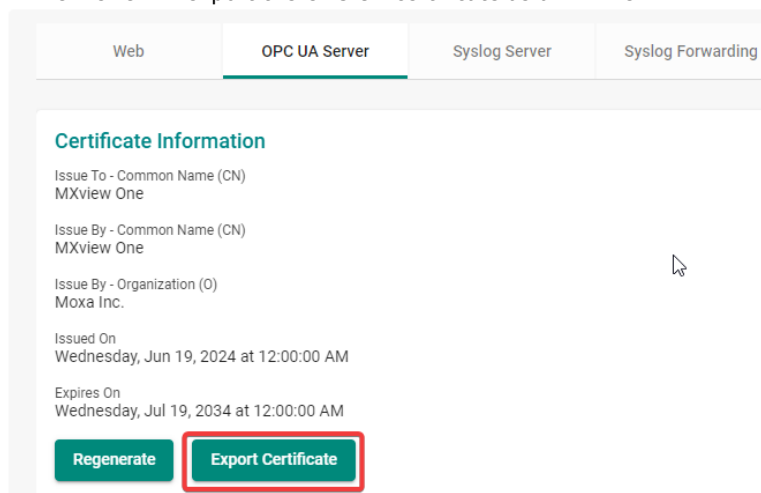


5. After successfully regenerating the certificate, MXview One Control Panel will need to be restarted for the certificate to take effect. Click **Close** and restart the instance.



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.



Importing an OPC UA Server Certificate

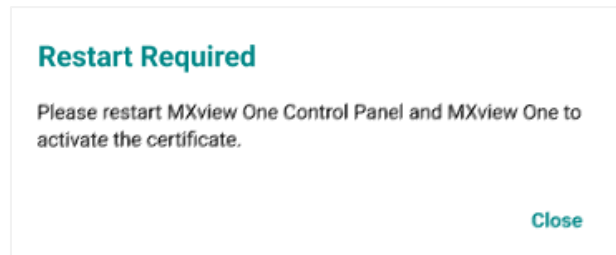
1. Navigate to **Control Panel > Certificates**.
2. Go to the **OPC UA Server** tab.
3. In the **Import Certificate** section, click the folder icon for the Private Key, Certificate, and CA Certificate fields and navigate to the CA certificate (.crt, .cer), certificate (.pem), and key (.key) file on

the local host.



The 'Import Certificate' dialog box contains three input fields for file selection, each with a folder icon on the right. The fields are labeled 'Private Key (.key) *', 'Certificate (.pem) *', and 'CA Certificate (.crt, .cer) *'. At the bottom left is an 'Import' button.

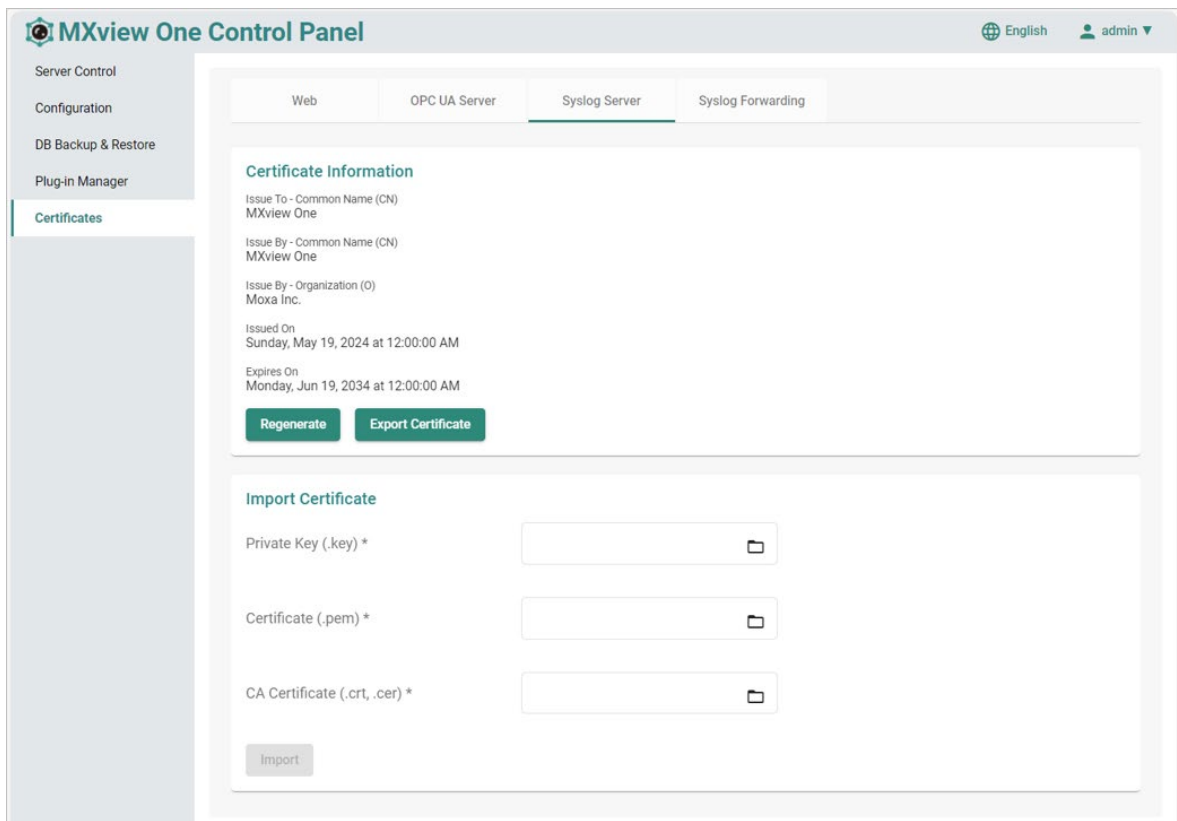
4. Click **Import**.
5. After successfully importing the certificate, MXview One Control Panel will need to be restarted for the certificate to take effect. Click **Close** and restart the instance.



Syslog Server Certificates

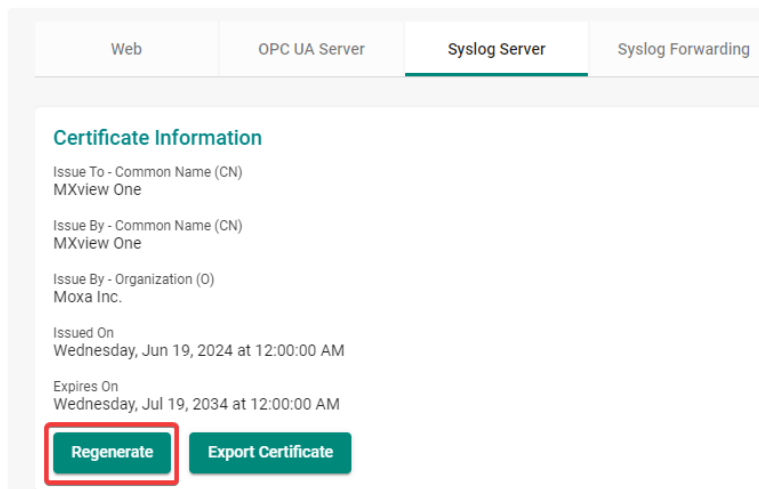
On the **Syslog Server** tab, you can view the information for the current syslog server certificates, including:

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

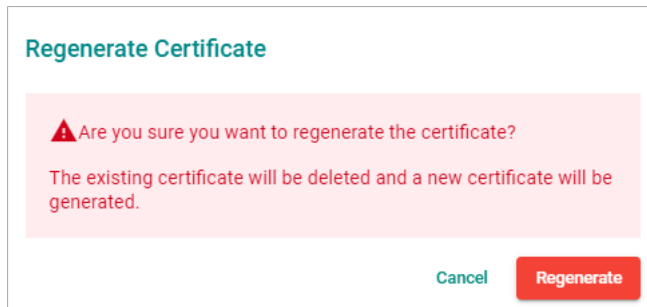


Regenerating the Syslog Server Certificate

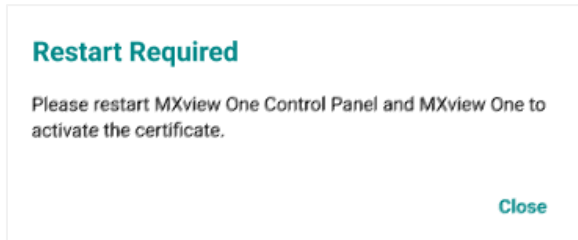
1. Navigate to **Control Panel > Certificates**.
2. Go to the **Syslog Server** tab.
3. Click the **Regenerate** button.
The **Regenerate Certificate** window will appear.



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

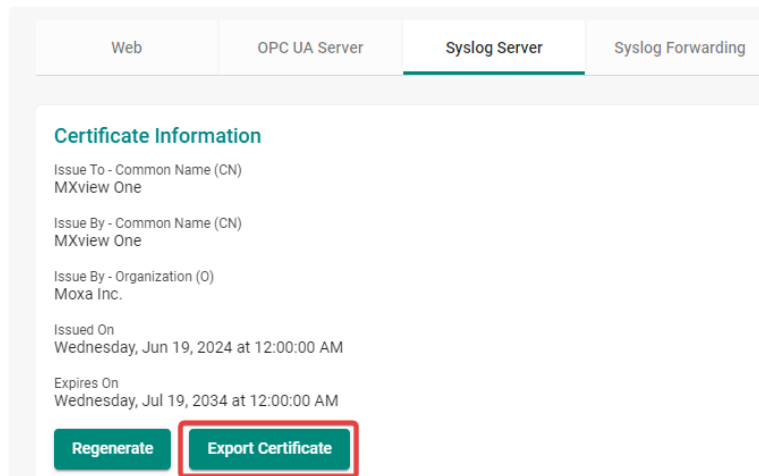


5. After successfully regenerating the certificate, MXview One Control Panel will need to be restarted for the certificate to take effect. Click **Close** and restart the instance.



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.



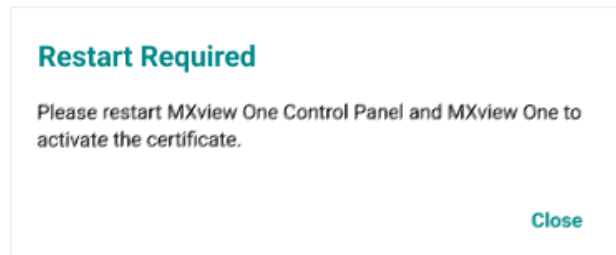
Importing a Syslog Server Certificate

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.

A dialog box titled "Import Certificate" with a light blue header. It contains three input fields, each with a folder icon to its right: "Private Key (.key) *", "Certificate (.pem) *", and "CA Certificate (.crt, .cer) *". At the bottom left is a grey "Import" button.

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.



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) *

Import

Remote IP/Domain 2

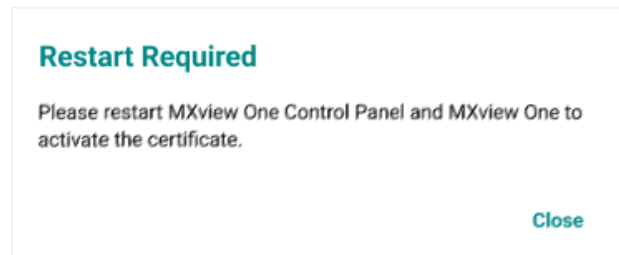
Private Key (.key) *

Certificate (.pem) *

CA Certificate (.crt, .cer) *

Import

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.



MQTT Certificates

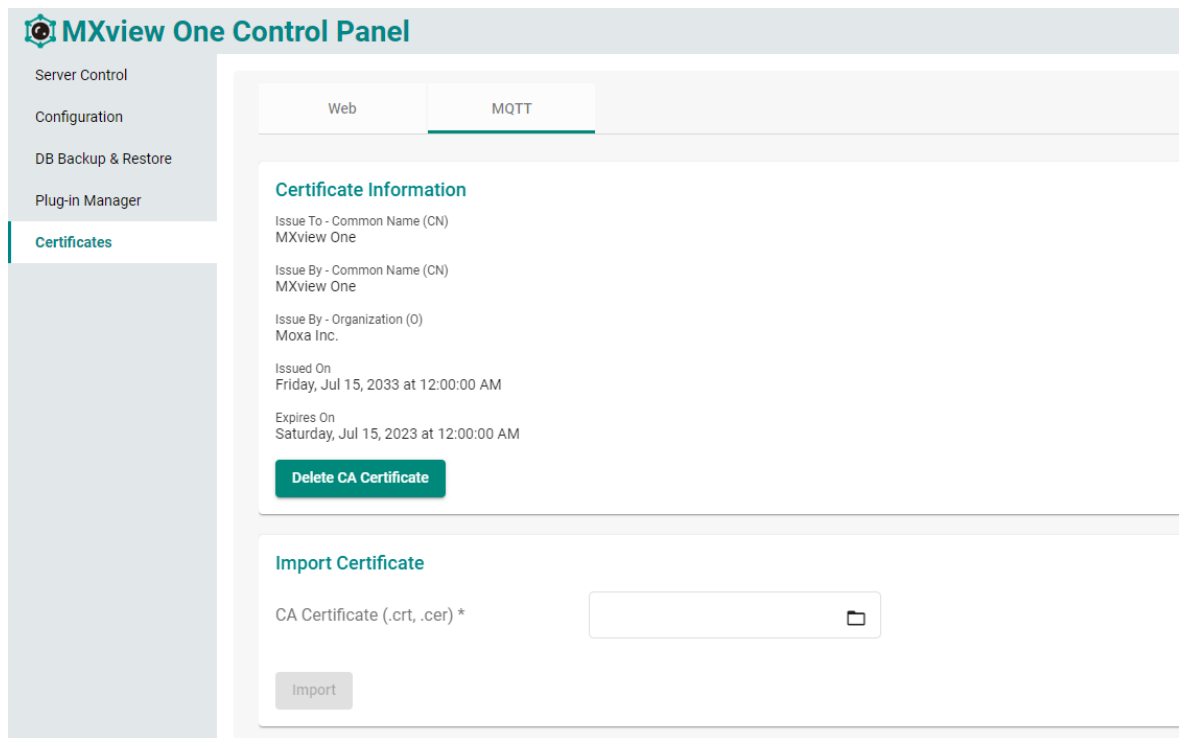


NOTE

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

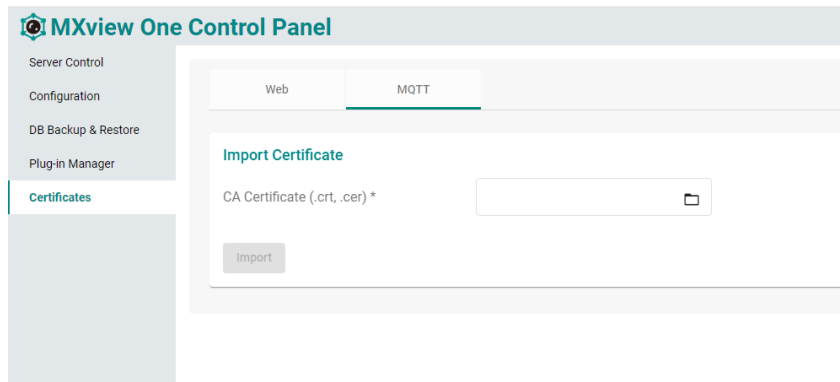


The screenshot shows the 'MXview One Control Panel' interface. On the left is a sidebar menu with options: Server Control, Configuration, DB Backup & Restore, Plug-in Manager, and Certificates (which is highlighted). The main content area has two tabs: 'Web' and 'MQTT' (which is selected). Under the 'MQTT' tab, there are two sections. The first section, 'Certificate Information', displays details for a certificate: 'Issue To - Common Name (CN)' is 'MXview One', 'Issue By - Common Name (CN)' is 'MXview One', 'Issue By - Organization (O)' is 'Moxa Inc.', 'Issued On' is 'Friday, Jul 15, 2023 at 12:00:00 AM', and 'Expires On' is 'Saturday, Jul 15, 2023 at 12:00:00 AM'. Below this information is a green button labeled 'Delete CA Certificate'. The second section, 'Import Certificate', contains a text input field labeled 'CA Certificate (.crt, .cer) *' with a folder icon to its right, and a grey 'Import' button below it.

Importing the MXview One Central Manager CA Certificate

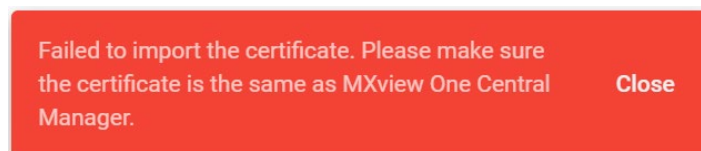
If this MXview One instance is managed through MXview One Central Manager, upload the CA certificate generated through MXview One Central Manager Control Panel here.

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.



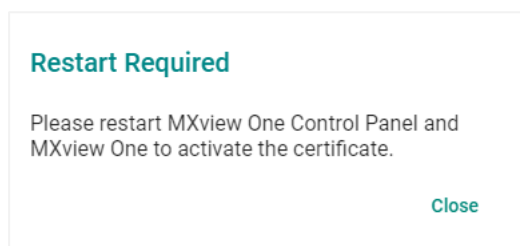
This screenshot shows the 'MXview One Control Panel' interface, specifically the 'Import Certificate' section under the 'MQTT' tab. The sidebar menu is visible on the left. The main content area shows the 'Import Certificate' section with a text input field labeled 'CA Certificate (.crt, .cer) *' and a folder icon to its right. Below the input field is a grey 'Import' button.

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



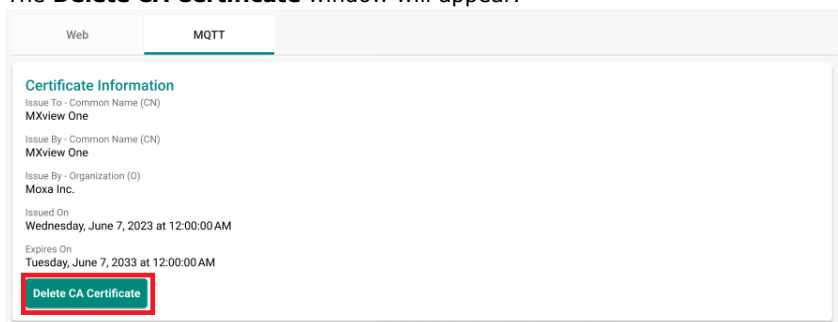
The screenshot shows a red error message dialog box. The text inside reads: 'Failed to import the certificate. Please make sure the certificate is the same as MXview One Central Manager.' To the right of the text is a white button labeled 'Close'.

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.

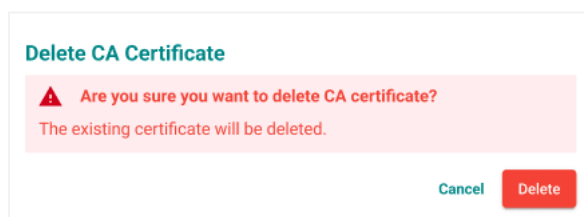


Deleting the CA Certificate

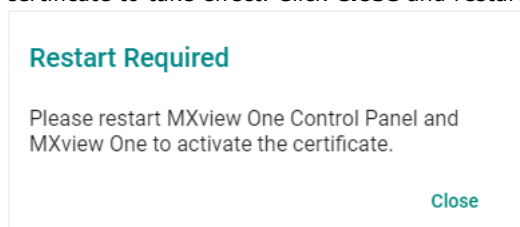
1. Click **Delete CA Certificate** to delete the current CA certificate file. The **Delete CA Certificate** window will appear.



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

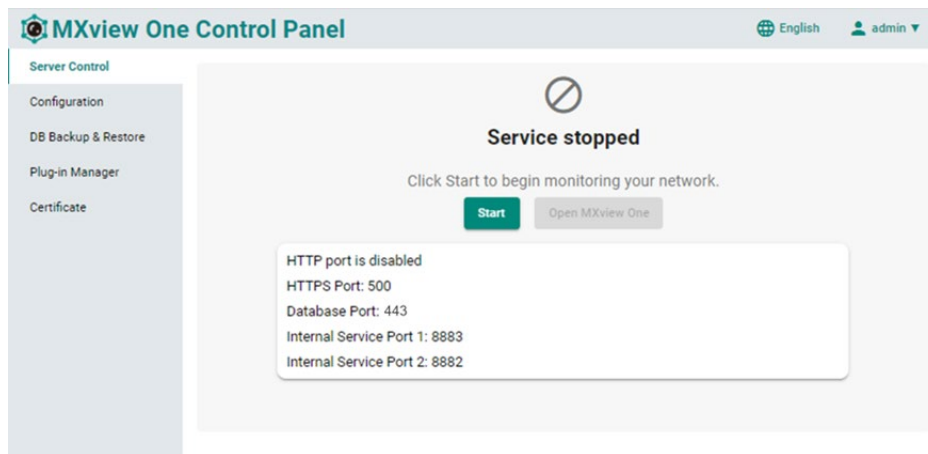


3. After successfully deleting the certificate, MXview One Control Panel will need to be restarted for the certificate to take effect. Click **Close** and restart the instance.

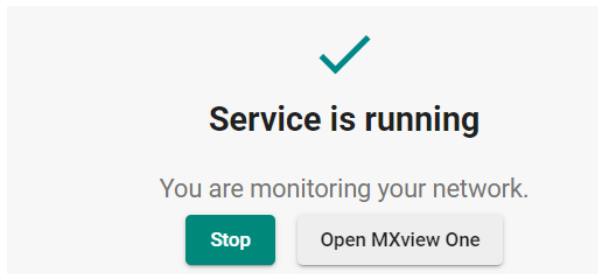


Starting the MXview One Server and Logging Into MXview One

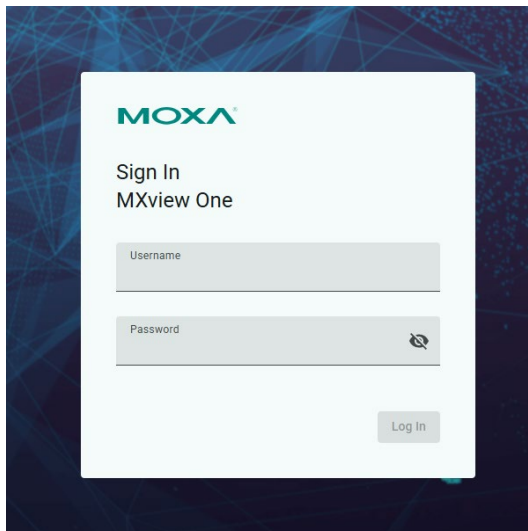
1. On the **Server Control** page, click **Start**. The MXview One server will start running.



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

Cancel

Change

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

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

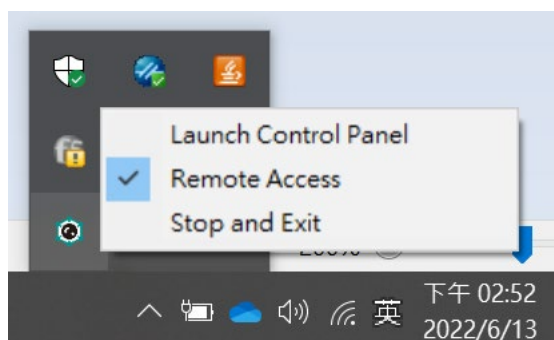
NOTE

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**.

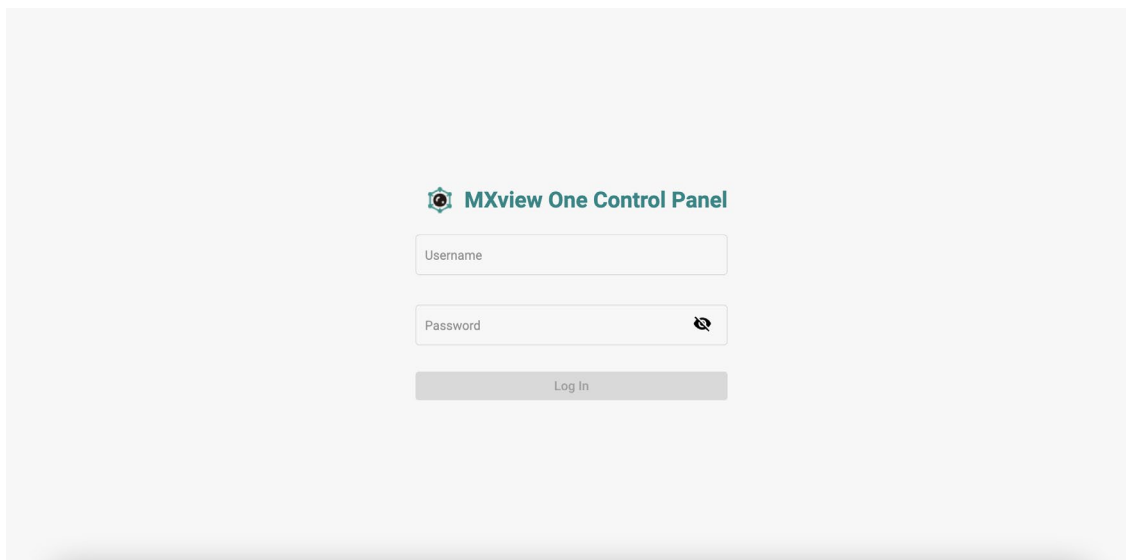




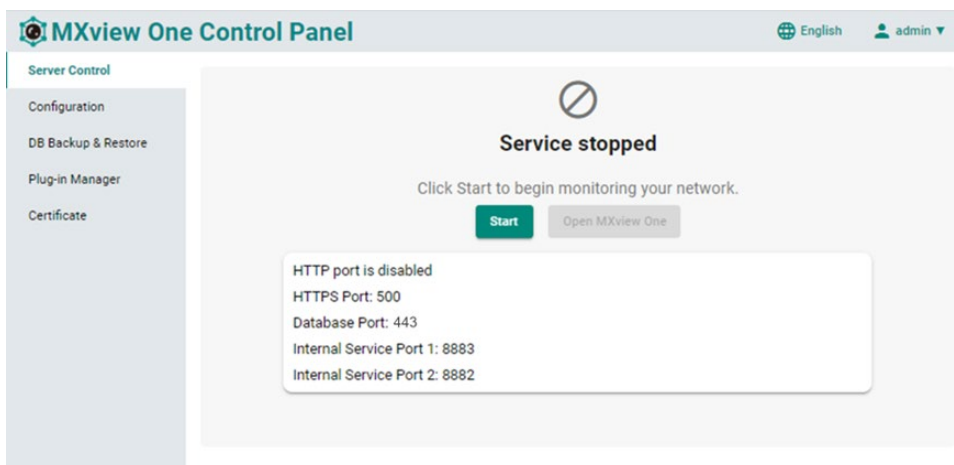
NOTE

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

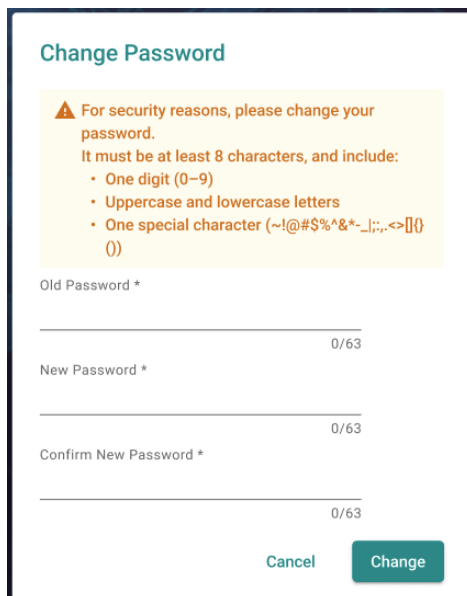


6. To open the MXview One web console, you can type the IP address of the computer at the local site into another web browser once the MXview One Control Panel displays 'Service is running now'.
 - Format: **https://[IP address]**

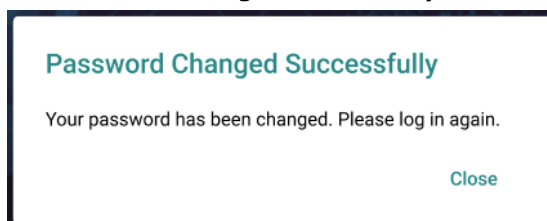
- Example: <https://192.168.1.250>
The MXview One web console appears.
- 7. Enter the login credentials and click **Log In**.
 - Default username: **admin**
 - Default password: **moxa**



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

The image shows the "Change Password" screen. It has a title "Change Password" in teal. Below the title is a warning message: "For security reasons, please change your password. It must be at least 8 characters, and include: One digit (0-9), Uppercase and lowercase letters, and One special character (~!@#\$%^&*-_!;,:.<>[]{}()).". There are three input fields: "Old Password *", "New Password *", and "Confirm New Password *". Each field has a character count "0/63" to its right. At the bottom are two buttons: "Cancel" and "Change".

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



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.

Switching to the Legacy UI

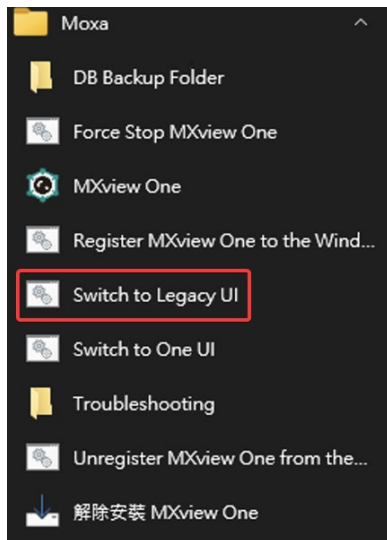
As of v1.8.0, MXview One uses the new One UI by default. When upgrading from an older version of MXview One to v1.8.0, all your existing data will be converted to the latest architecture. If necessary, you can switch back to the legacy interface.



WARNING

When switching from the new One UI to the legacy interface, some functions will be limited or unavailable. Refer to **Legacy UI Limitations** for an overview of all affected features and functions.

1. In the Windows Start menu, navigate to the Moxa folder.
2. Click **Switch to Legacy UI**.



3. Click **Switch to One UI**, to load the new default interface.

Legacy UI Limitations

When switching to the legacy interface, the following limitations will apply:

Limitation	Description
Login Policy	If LDAP , RADIUS , or Two-factor Authentication (2FA) is enabled in the One UI, you cannot log in to the legacy UI. These functions must be disabled in the One UI first before switching back to the legacy UI.
Unsupported features	The legacy UI does not support the following functions introduced in MXview One v1.8.0: • LDAP • RADIUS • Two-factor Authentication (2FA) • VLAN View • Trap Forwarding • Internal Event Forwarding

License Management

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

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



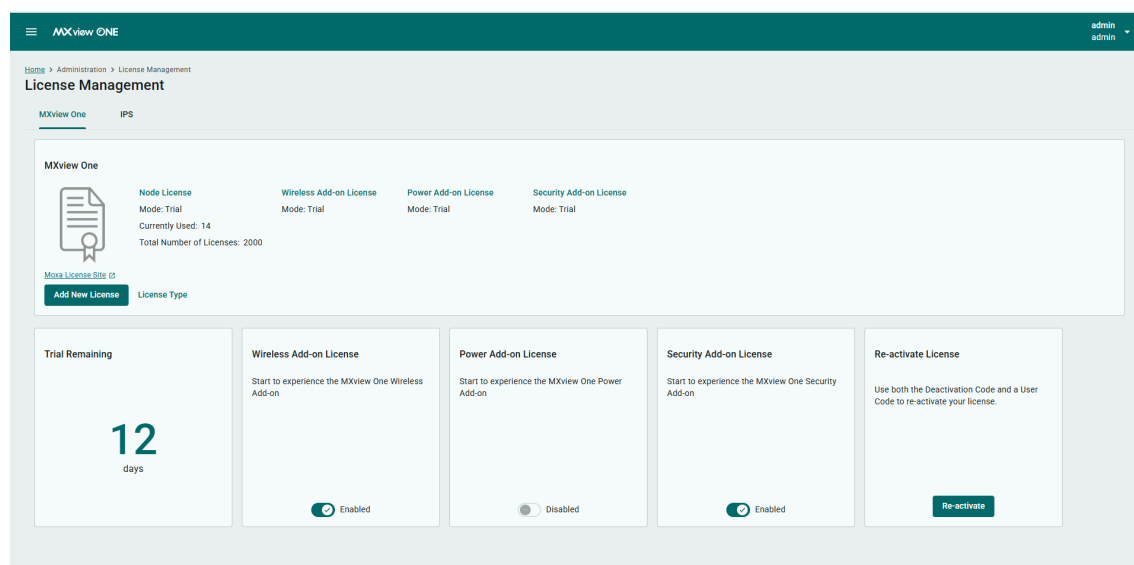
NOTE

Click "Start Trial" to start using MXview One.

Checking the License

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

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



Adding a New License

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

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

The screenshot shows the 'Add New License' dialog box with a progress bar at the top. Step 1, 'Log in to the Moxa License Site', is the active step and is highlighted with a green circle. Step 2, 'Copy User Code', and Step 3, 'Activate', are shown in gray. Below the progress bar, there are instructions: '1. Log in to the [Moxa License Site](#)', '2. Choose "Activate a Product License" and "MXview One" on the site.', and '3. Registration Code'. A text box displays the registration code: 'Your registration code (Type: MXview One NEW) (Model name: LIC-MXviewOne-NEW-XN-SR) is xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx'. At the bottom right, there are 'Close' and 'Next' buttons.

4. Copy the User Code.

The screenshot shows the 'Add New License' dialog box with the progress bar updated. Step 1 is now completed and marked with a green checkmark. Step 2, 'Copy User Code', is the active step and is highlighted with a green circle. Step 3, 'Activate', remains in gray. Below the progress bar, the instruction is 'Copy the User Code to the [Moxa License Site](#)'. A text box labeled 'User Code:' contains a grayed-out field for pasting the code, followed by a copy icon. At the bottom right, there are 'Close' and 'Next' buttons.

5. Input a valid activation code.

Add New License

1

Log in to the Moxa License Site

2

Copy User Code

3

Activate

Download the license from the [Moxa License Site](#), and paste the Activation Code here.

Activation Code

Close

Apply

- Click **Apply**.



NOTE

Please reference **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.

- Navigate to **Menu**  > **Device Discovery**.

Home > Device Discovery

Device Discovery

1

Network Range(s)

2

Discovery Result

3

Complete

⚠

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

+

☐

Enable Scan Range

Name

First IP Address

Last IP Address

Group

Background Scanning

IP Conflict Detection

- Add the IP address ranges to scan for devices.



NOTE

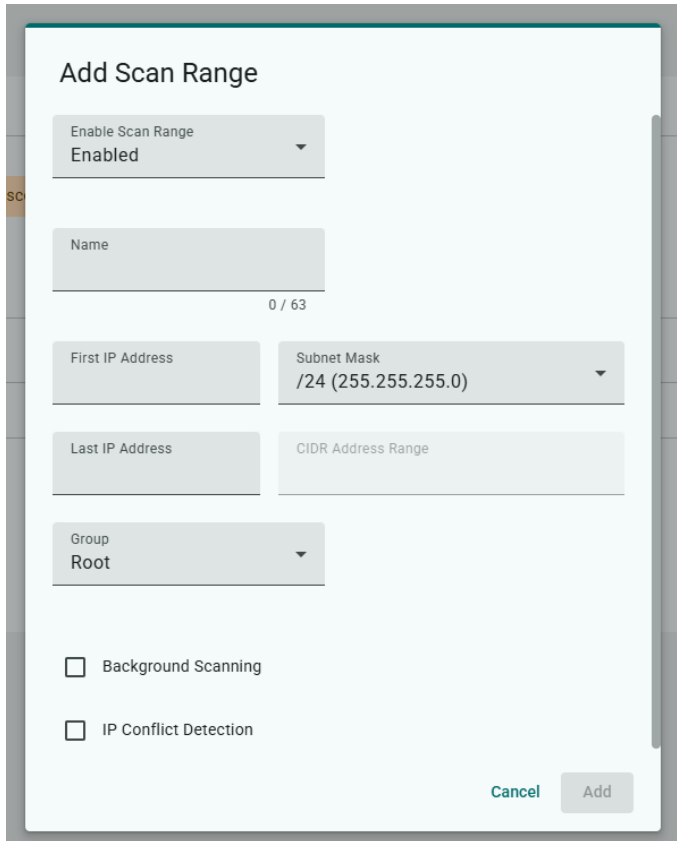
MXview One supports scanning multiple IP address ranges. The selected IP address scan ranges must be enabled in order for MXview One to scan for devices.



NOTE

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

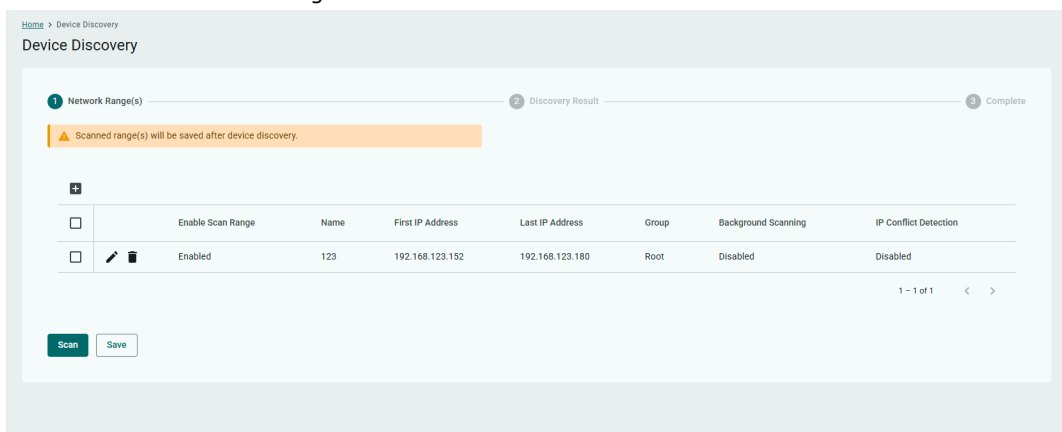
- a. Click the **Add (+)** icon.



The 'Add Scan Range' dialog box contains the following fields and options:

- Enable Scan Range:** A dropdown menu currently set to 'Enabled'.
- Name:** A text input field with a character count '0 / 63' below it.
- First IP Address:** A text input field.
- Subnet Mask:** A dropdown menu currently set to '/24 (255.255.255.0)'.
- Last IP Address:** A text input field.
- CIDR Address Range:** A text input field.
- Group:** A dropdown menu currently set to 'Root'.
- Background Scanning:** An unchecked checkbox.
- IP Conflict Detection:** An unchecked checkbox.
- Buttons:** 'Cancel' and 'Add' buttons at the bottom right.

- b. In the **Add Scan Range** window, configure the following settings:
- ☐ **Enable Scan Range:** Enable or disable scanning of the specified IP address range.
 - ☐ **Name:** Enter a name for the scan range.
 - ☐ **First IP Address:** Specify the starting IP address of the scan range.
 - ☐ **Last IP Address:** Specify the ending IP address of the scan range.
 - ☐ **Subnet Mask:** Specify subnet mask for the scan range.
 - ☐ **Background Scanning:** Enable or disable background scanning. 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.
 - ☐ **IP Conflict Detection:** Enable or disable IP conflict detection. When enabled, MXview One will check for IP conflicts among field devices. This feature requires WinPcap/libpcap to be installed.
- c. Click **Add**. Repeat these steps to add additional scan ranges.
- d. (Optional) To modify scan range settings, click the **Edit (✎)** icon next to an added scan range.
- e. (Optional) To remove a scan range, click the **Delete (🗑)** icon next to the added scan range.
- f. Select one or more scan ranges and click **Next**.



The 'Device Discovery' screen shows a progress bar with three steps: 1. Network Range(s), 2. Discovery Result, and 3. Complete. A warning message states: 'Scanned range(s) will be saved after device discovery.'

	Enable Scan Range	Name	First IP Address	Last IP Address	Group	Background Scanning	IP Conflict Detection
☐	Enabled	123	192.168.123.152	192.168.123.180	Root	Disabled	Disabled

At the bottom, there are 'Scan' and 'Save' buttons. A pagination indicator shows '1 - 1 of 1'.

- Review the devices discovered on the network and click **Next**.

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



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** (☰) > **Administration** > **Account Management**.

The Account Management screen allows you to manage MXview One user accounts, and set up the password and login policies. You can also export a list of user accounts and related information as a CSV file.

Default Accounts and Role Privileges

Default Accounts

MXview One supports the following default accounts:

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

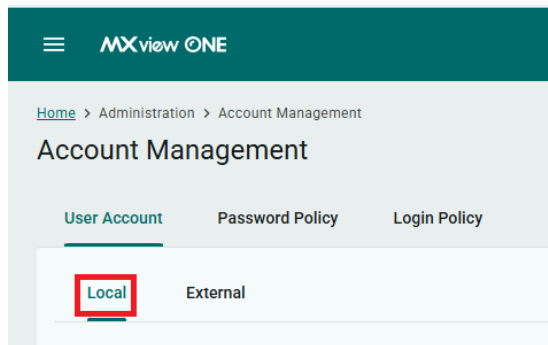
User Roles and Privileges

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

Role	Access Permissions
admin	Full access rights to modify any settings/configurations and can assign authorities to other accounts.
user	Full access rights to modify any settings/configurations on all pages, except Account Management .
guest	Limited access to the following functions: • Dashboard: Read-only access. • Topology: Read-only access. • Event History: Can perform: Export, Filter. • Syslog Viewer: Can perform: Export, Filter. • Inventory Report: Can perform: Export. • About MXview One: View software version. • User Manual: Can access link to document. • API Documentation: Can access link to document.

Adding User Accounts

1. Navigate to **Menu** (☰) > **Administration** > **Account Management**.
2. Go to the **User Account** tab, then go to the **Local** sub-tab.



3. Click **Create** in the top-right corner of the screen.
4. In the **Create User Account** window, configure the following settings:
 - **Username**: Specify the username for the account.
 - **Role**: Select the account role, which determines access permissions. Refer to **Default Accounts and Role Privileges**.
 - **Password**: Enter the login password for the account. The password requirements are determined by the password policy. Refer to **Configuring the Password Policy**.
 - **Confirm Password**: Enter the account password to confirm.
 - **Email**: Enter the email address of the user.
 - **Description**: Enter a description for the user account.
5. Click **Add**.

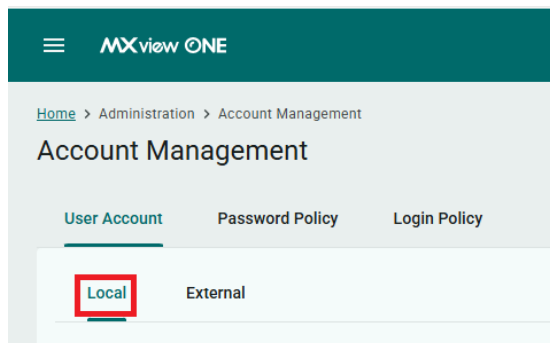
Modifying User Accounts



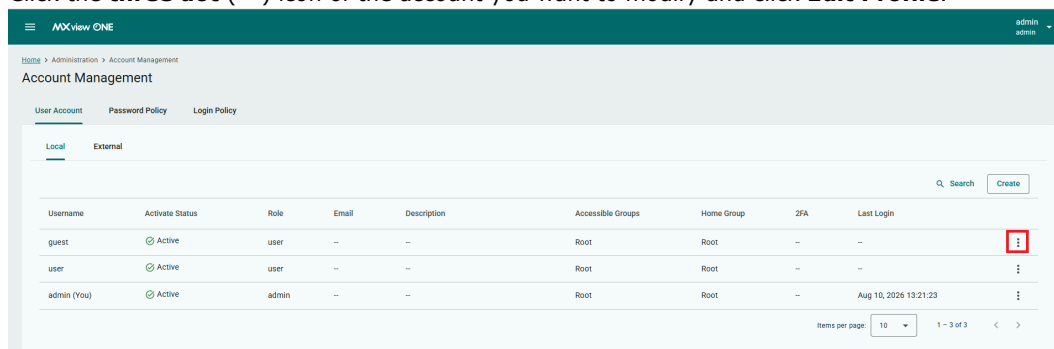
NOTE

This action requires administrator privileges.

1. Navigate to **Menu** (☰) > **Administration** > **Account Management**.
2. Go to the **User Account** tab, then go to the **Local** sub-tab.



3. Click the **three dot** (⋮) icon of the account you want to modify and click **Edit Profile**.



4. Modify the settings. Some settings cannot be modified. Refer to **Adding User Accounts**.
5. Click **Apply**.

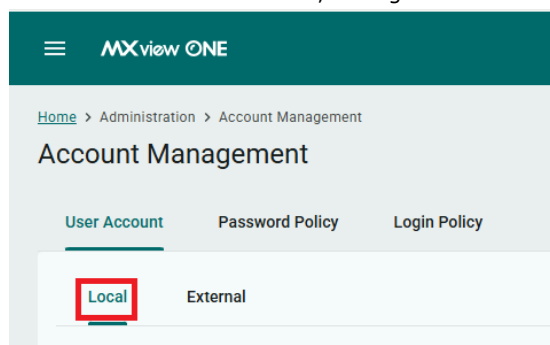
Editing Accessible Groups



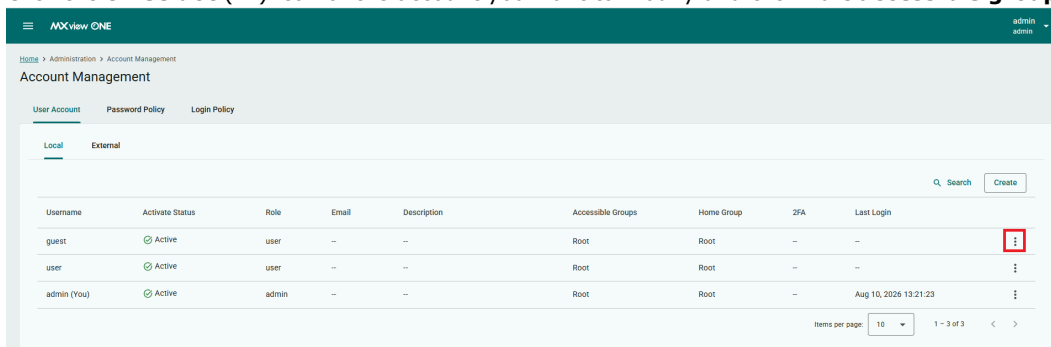
NOTE

This action requires administrator privileges.

1. Navigate to **Menu** (☰) > **Administration** > **Account Management**.
2. Go to the **User Account** tab, then go to the **Local** sub-tab.



- Click the **three dot** (⋮) icon of the account you want to modify and click **Edit accessible groups**.



- In the **Edit Accessible Groups** window, 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.
- Click **Save**.

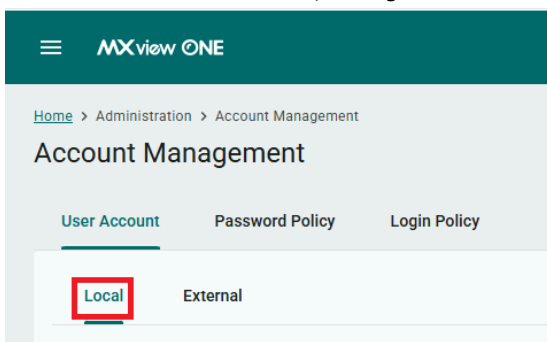
Deactivating User Accounts



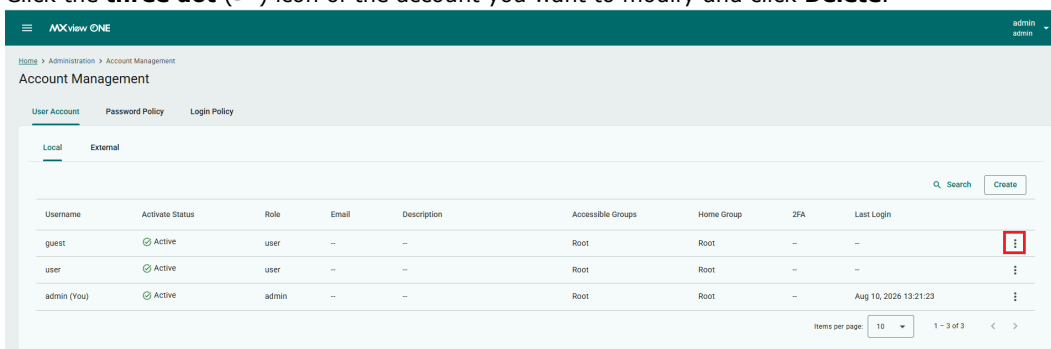
NOTE

This action requires administrator privileges.

- Navigate to **Menu** (☰) > **Administration** > **Account Management**.
- Go to the **User Account** tab, then go to the **Local** sub-tab.



- Click the **three dot** (⋮) icon of the account you want to modify and click **Delete**.



- When prompted, click **Deactivate**.

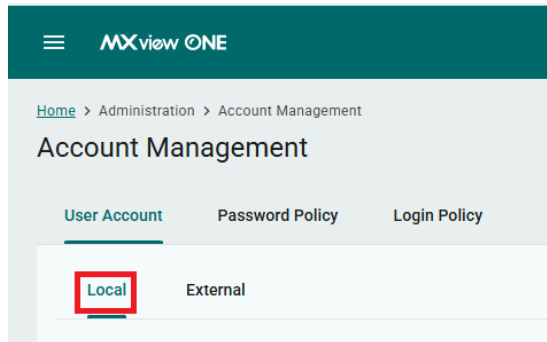
Activating Deactivated User Accounts



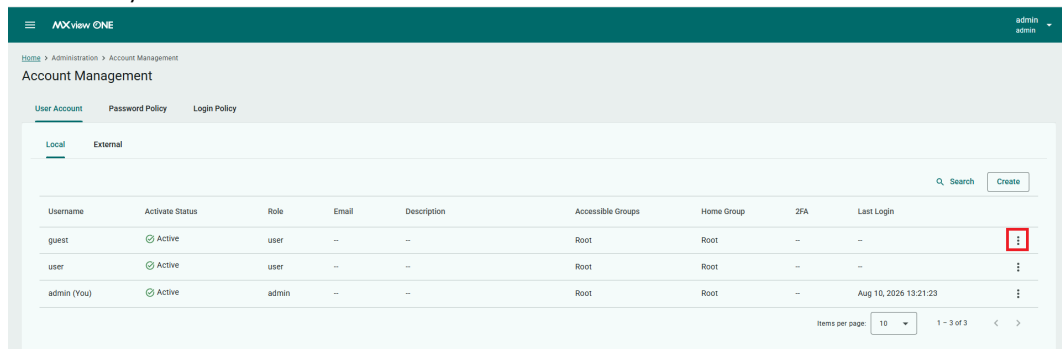
NOTE

This action requires administrator privileges.

1. Navigate to **Menu** (☰) > **Administration** > **Account Management**.
2. Go to the **User Account** tab, then go to the **Local** sub-tab.



3. Click the **three dot** (⋮) icon of the account you want to modify and click **Activate**. This will immediately reactivate the user account without confirmation.



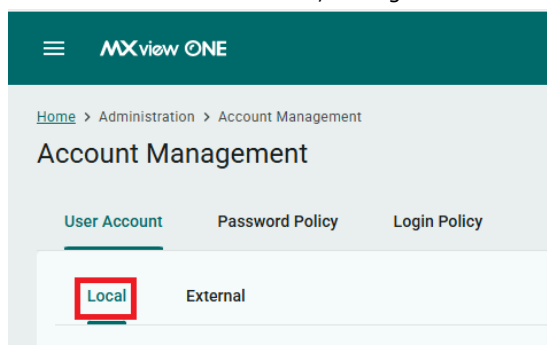
Deleting User Accounts



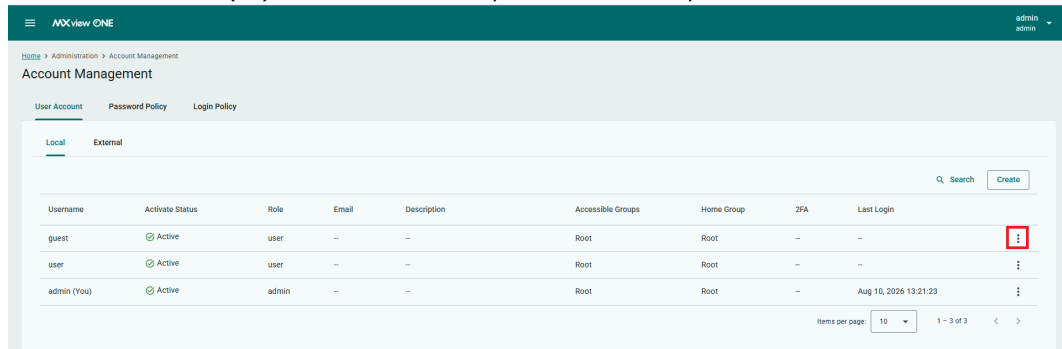
NOTE

This action requires administrator privileges.

1. Navigate to **Menu** (☰) > **Administration** > **Account Management**.
2. Go to the **User Account** tab, then go to the **Local** sub-tab.



- Click the **three dot** (⋮) icon of the account you want to modify and click **Delete**.

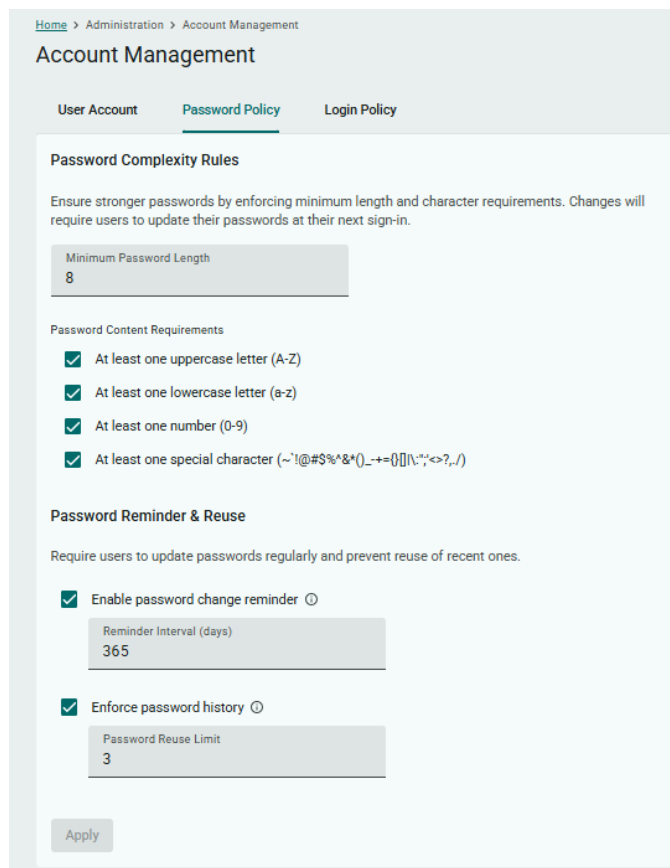


- When prompted, click **Delete**.

Configuring the Password Policy

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

- Navigate to **Menu** (☰) > **Administration** > **Account Management**.
- Go to the **Password Policy** tab.



- Specify the minimum password length (between 4 to 16 characters).
- Select the password complexity strength checks to apply.
- Check **Enable password change reminder** to regularly remind users to update their password.
 - If enabled, specify the reminder interval (in days).
- Check **Enforce password history** to prevent users from reusing previous passwords.
 - If enabled, specify the password reuse limit. For example, if set to 3, users cannot reuse their last 3 passwords.

7. Click **Save**.

Configuring Login Messages

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

1. Navigate to **Menu** (☰) > **Administration** > **Account Management**.
2. Go to the **Login Policy** tab, then go to the **Login Message** sub-tab.

The screenshot shows the 'Login Policy' configuration page. At the top, there are three tabs: 'User Account', 'Password Policy', and 'Login Policy'. The 'Login Policy' tab is selected. Below the tabs, there are three sub-tabs: 'Login Message', 'Login Lockout', and 'Session Control'. The 'Login Message' sub-tab is selected. The main content area is titled 'Login Message' and contains a large text input field with the placeholder text 'Message - optional'. Below this field is a character count '0 / 256'. Underneath the text field is a section titled 'Login Authentication Failure Message'. It contains a 'Mode' dropdown menu with 'Default' selected. Below the dropdown is a 'Message' input field with the text 'The account or password you entered is incorrect.' At the bottom of the page is an 'Apply' button.

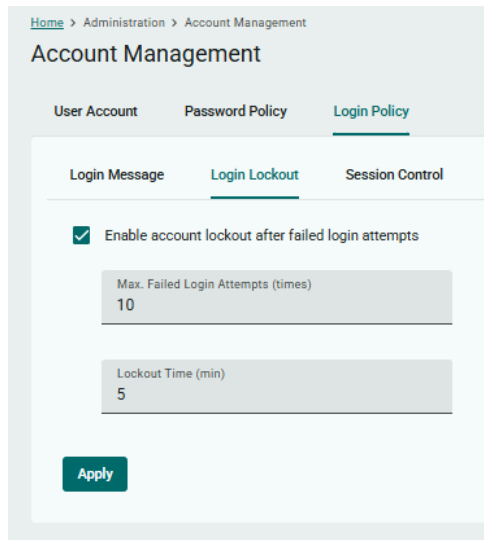
3. (Optional) In the **Login Message** field, enter a custom message of up to 256 characters. This message appears when users successfully logged in to MXview One.
4. Select the **Login Authentication Failure Message** mode. This message appears when users failed to log in.
 - **Default:** Shows the default login failure message.
 - **Custom:** Enter a custom message of up to 256 characters.
5. Click **Apply**.

Configuring Login Lockout Settings

Login Lockout temporarily prevents users from logging in to MXview One after multiple consecutive failed login attempts.

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

2. Go to the **Login Policy** tab, then go to the **Login Lockout** sub-tab.



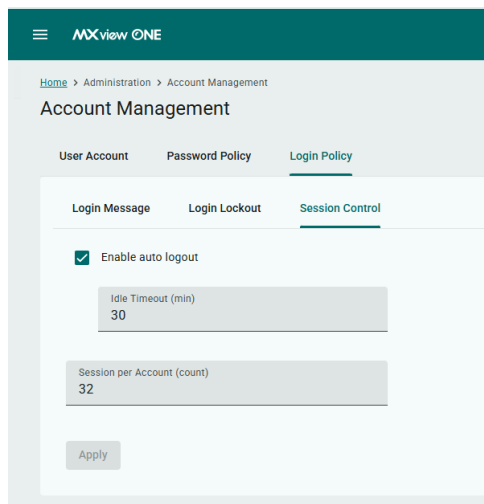
The screenshot shows the 'Account Management' page with the 'Login Policy' tab selected. Under the 'Login Lockout' sub-tab, the 'Enable account lockout after failed login attempts' checkbox is checked. Below it, the 'Max. Failed Login Attempts (times)' is set to 10, and the 'Lockout Time (min)' is set to 5. An 'Apply' button is at the bottom.

3. Check **Enable account lockout after failed login attempts** to enable lockout. If enabled, configure the following settings:
 - **Max. Failed Login Attempts (times)**: Specify the number of consecutive failed login attempts allowed before the user is locked out.
 - **Lockout Time (min)**: Specify the lockout duration.
4. Click **Apply**.

Configuring Session Control Settings

Session Control will automatically log out idle users and limit the number of concurrent sessions for each account.

1. Navigate to **Menu** (☰) > **Administration** > **Account Management**.
2. Go to the **Login Policy** tab, then go to the **Session Control** sub-tab.



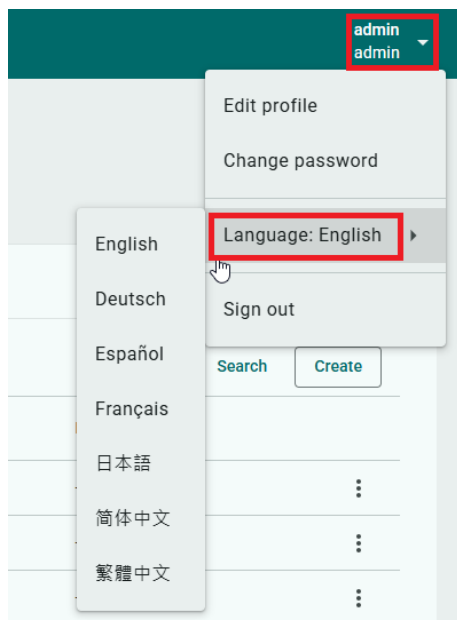
The screenshot shows the 'Account Management' page with the 'Login Policy' tab selected. Under the 'Session Control' sub-tab, the 'Enable auto logout' checkbox is checked. Below it, the 'Idle Timeout (min)' is set to 30, and the 'Session per Account (count)' is set to 32. An 'Apply' button is at the bottom.

3. Check **Enable auto logout** to automatically log out idle users.
 - a. Specify the idle duration (in min) before a user is logged out.
4. Specify the maximum allowed concurrent sessions per user account.
5. Click **Apply**.

Changing the Display Language

Use the **Language** screen to change the display language of the MXview One interface.

1. Expand the account menu in the top-right corner of screen.
2. Hover over **Language** to expand the selection and select an interface language. MXview One will immediately change to the selected language without confirmation.



Two-factor Authentication

Two-factor Authentication (2FA) adds a second verification layer to the standard username and password login to protect accounts from unauthorized access. When 2FA is enabled, users must verify their identity with a one-time code in addition to their password. This code can be delivered by email or generated by an authenticator app using a time-based one-time password (TOTP).

When enabled by the system administrator, the 2FA policy applies to all local and externally authenticated user accounts.

Enabling Two-factor Authentication

1. Navigate to **Menu** (☰) > **Administration** > **Two-Factor Authentication**.
2. Check the **Enable two-factor authentication** checkbox.
3. Select the verification method:
 - **Email**: A verification code will be sent to the user's email.
 - **TOTP (Authenticator app)**: A verification code is generated using the Google Authenticator app.
 - **Email & TOTP (Authenticator app)**: A verification code can be sent by email or via authenticator app.
4. (Optional) Select the local and external user accounts that are exempt from the 2FA policy.
5. Click **Apply**.



NOTE

Users will be prompted to configure the selected 2FA verification method(s) when logging in for the first time after 2FA is enabled. Refer to **Setting Up Two-factor Authentication Methods**.

Setting Up Two-factor Authentication Methods

After 2FA is enabled, users will be required to configure the selected 2FA method(s) when logging in.

1. Enter your username and password and click **Log In**.
2. In the **Edit Two-Factor Authentication** window, click **Set up** to configure the corresponding 2FA method.
3. To set up **Email Verification**:
 - a. Enter the email address to send the verification code to and click **Send code**. The verification code will remain valid for 5 minutes.
 - b. Enter the verification code and click **Confirm**.
If you did not receive the code, confirm the email address is correct or contact your administrator.
 - c. When successfully verified, click **Close**.
4. To set up **TOTP (Authenticator app)**:



NOTE

Because TOTP is time-based, ensure NTP is enabled on the system before setting up TOTP.

- a. Scan the corresponding QR code to download the Google Authenticator app and click **Next**.
- b. Select the cryptographic hash function and click **Regenerate**.
- c. Scan the generated QR code with the authenticator app. If you cannot scan the QR, manually enter the code shown on the screen.
- d. Enter the verification code generated by the authenticator app and click **Confirm**.
- e. When successfully verified, click **Close**.

Logging In With Two-factor Authentication

If 2FA is applied and set up, you will need a verification code to confirm your login identity. Available 2FA methods depend on which methods are enabled and configured. If the required authentication method is not configured yet, you will be prompted to complete the setup first.

1. Enter your username and password and click **Log In**.
2. When prompted, enter the verification code sent to your email or generated by the authenticator app.
3. If you have multiple 2FA methods configured, click **Verify with TOTP** or **Verify with Email** at the bottom of the window to change methods.

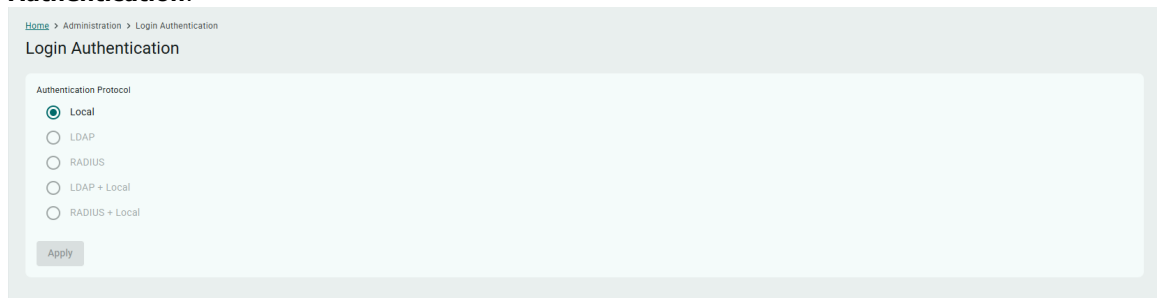
Changing Login Verification Methods

1. Open the account menu in the top-right corner and select **Edit two-factor authentication**.
2. If a verification method is not configured yet, click **Set up**. Refer to **Setting Up Two-factor Authentication Methods**.
3. To modify an authentication method, click **Action** and select one of the following options:
 - **Edit**: Modify the current authentication method settings.
 - **Reset**: Reset the current configuration. You will be required to set up the method again.
 - **Set as default**: Set this method as the default authentication method. This option is only available if more than one method is configured.

Login Authentication

From the **Login Authentication** screen, you can select the protocol used to authenticate users when they log in.

To access the **Login Authentication** screen, navigate to **Menu** (☰) > **Administration** > **Login Authentication**.



Applying an Authentication Protocol



NOTE

Local, LDAP, and RADIUS options require the relevant settings to be configured.

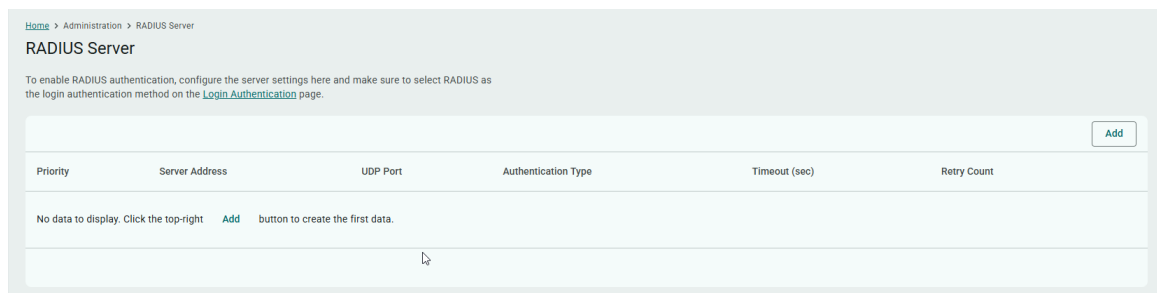
- For local account configuration, refer to **Account Management**.
- For RADIUS server configuration, refer to **RADIUS Server**.
- For LDAP server configuration, refer to **LDAP Management**.

1. Navigate to **Menu** (☰) > **Administration** > **Login Authentication**.
2. Select the authentication protocol:
 - **Local**: Users are authenticated against the account database stored locally in MXview One. This is the default method.
 - **LDAP**: Users are authenticated against the configured LDAP server(s) only. Local accounts cannot be used to log in.
 - **RADIUS**: Users are authenticated against the configured RADIUS server(s) only. Local accounts cannot be used to log in.
 - **LDAP + Local**: Users are authenticated against the configured LDAP server(s) first. If all attempts fail, the system will fall back to local account authentication. If the LDAP server responds with an authentication rejection, the system will not trigger local account authentication.
 - **RADIUS + Local**: Users are authenticated against the configured RADIUS server(s) first. If all attempts fail, the system will fall back to local account authentication. If the RADIUS server responds with an authentication rejection, the system will not trigger local account authentication.
3. Click **Apply**.

RADIUS Server

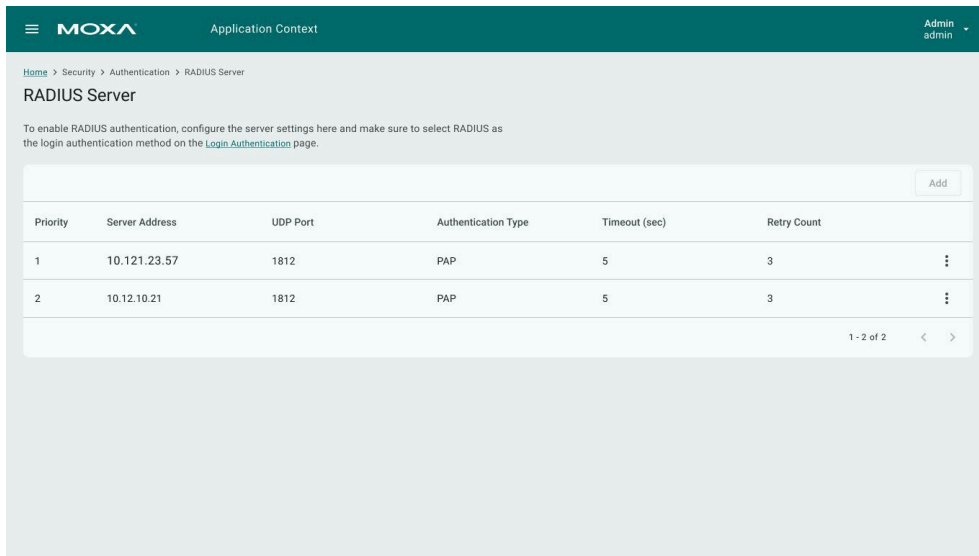
MXview One supports RADIUS (Remote Authentication Dial-in User Service) for centralized login authentication. When configured, RADIUS can be selected as a user authentication method. You can configure up to two RADIUS servers for failover. The primary server acts as the active server. If the primary server does not respond, the system will automatically switch over the secondary server for that request.

To access the **RADIUS Server** screen, navigate to **Menu** (☰) > **Administration** > **RADIUS Server**.



Viewing the RADIUS Server List

The **RADIUS Server** screen lists all configured RADIUS servers. From this screen, you can add, edit, or remove RADIUS servers.



Priority	Server Address	UDP Port	Authentication Type	Timeout (sec)	Retry Count
1	10.121.23.57	1812	PAP	5	3
2	10.12.10.21	1812	PAP	5	3

This page displays the following information in a table format:

Item	Description
Priority	The priority of the server. The primary server is the active server. The secondary server acts as a redundant failover server if the primary server is unavailable.
Server Address	The IPv4 address or domain name of the RADIUS server.
UDP Port	The UDP destination port of the RADIUS server for authentication requests. The default is 1812.
Authentication Type	The authentication protocol used between MXview One and the RADIUS server.
Timeout (sec)	The time (in seconds) that the system waits for a response from the server before retrying.
Retry Count	The number of times the system will attempt to connect to the RADIUS server after timing out. If a secondary server is configured, the system will switch over to the backup server if all retries are exhausted.

Adding a RADIUS Server

1. Navigate to **Menu** (☰) > **Administration** > **RADIUS Server**.
2. Click **Add**.
3. Configure the following settings:
 - **Server Address:** Specify the RADIUS server IP address or domain name.
 - **UDP Port:** Specify the RADIUS server UDP destination port.
 - **Shared Key:** Enter the shared secret. For security reasons, the shared key will be hidden by default. If server settings are retrieved via RESTful API, the shared key info is never returned in plain text.
 - **Authentication Type:** Select the authentication protocol used by MXview One and the RADIUS server.
 - **Timeout:** Specify the duration (in seconds) the system will wait before considering the server unresponsive.
 - **Retry Count:** Specify the number of times the system will attempt to connect to the RADIUS server after timing out. If a secondary server is configured, the system will switch over to the backup server if all retries are exhausted.
4. (Optional) Test the server connection:

- a. Click **Test connection**.
 - b. Enter a username and password that exist on the target RADIUS server.
 - c. Click **Test**. The test result will be shown under the **Test connection** button.
 - d. Modify the server settings and repeat the connection test if necessary. Testing the connection does not apply the configuration changes.
5. Click **Apply**.

Editing a RADIUS Server

1. Navigate to **Menu** (☰) > **Administration** > **RADIUS Server**.
2. From the RADIUS server list, click the menu (⋮) icon of the server you want to modify and select **Edit**.
3. Modify the settings as necessary. Refer to **Adding a RADIUS Server**.
4. To modify the shared key, click the **Edit** (✎) icon next and enter the new shared key.
5. (Optional) Click **Test connection** to verify the modified server settings.
6. Click **Apply**.

Configuring Server Priority and Failover

If a second RADIUS server is configured, you can set the priority for each server. By default, MXview One authenticates users against the primary RADIUS server. If the primary server is unavailable, the system will automatically switch over to the secondary server for that request. Each new request will attempt to contact the primary server first.

1. Navigate to **Menu** (☰) > **Administration** > **RADIUS Server**.
2. From the RADIUS server list, click the menu (⋮) icon of the server you want to change priority and select **Change to Primary** or **Change to Secondary** respectively. The change will apply immediately.

Deleting a RADIUS Server

1. Navigate to **Menu** (☰) > **Administration** > **RADIUS Server**.
2. From the RADIUS server list, click the action menu (⋮) icon of the server you want to remove and select **Delete**.
3. When prompted, click **Delete**.

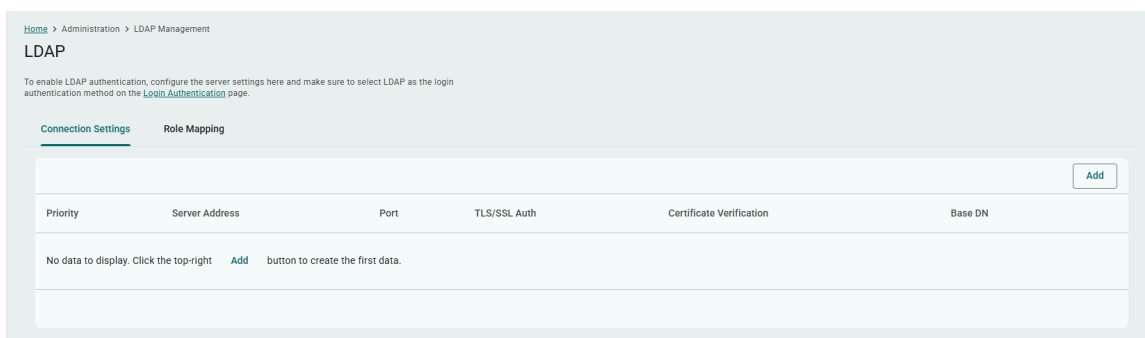
LDAP Management

LDAP (Lightweight Directory Access Protocol) authentication lets users sign in to MXview One with credentials managed in an external LDAP or Active Directory (AD) server. After configuring the connection to the directory server and defining how directory attributes map to MXview One roles, externally authenticated users are signed in automatically with the correct role. You can configure up to two LDAP servers for failover. The primary server acts as the active server. If the primary server does not respond, the system will automatically switch over to the secondary server.

Connection Settings

To access the **Connection Settings** page, in the function tree, navigate to **Menu** (☰) > **Administration** > **LDAP Management** and go to the **Connection Settings** tab.

The **Connection Settings** tab lets you manage LDAP servers.



This page displays the following information in a table format:

Item	Description
Priority	The priority of the server. The primary server is the active server. The secondary server acts as a redundant failover server if the primary server is unavailable.
Server Address	The IPv4 address or domain name of the LDAP server.
Port	The LDAP server port.
TLS/SSL Auth	The connection encryption status.
Certificate Verification	If TLS/SSL authentication is enabled, shows the server certificate verification method.
Base DN	The base Distinguished Name (DN) used to define the scope of the directory search.

Adding an LDAP Server

1. Navigate to **Menu**  > **Administration > LDAP Management**.
2. Go to the **Connection Settings** tab.
3. Click **Add**.
4. Configure the following settings:
 - **Server Address:** Specify the LDAP server IP address or domain name.
 - **Port:** Specify the LDAP server port.
 - **Enable TLS/SSL authentication:** Check to enable connection encryption. When enabled, select the **Certificate Verification** option:
 - ☐ **System default certificate:** Validate the server certificate using the system's built-in CA certificate.
 - ☐ **Self-signed:** Validate the server certificate using a third-party CA certificate. Click **Browse** and navigate to the CA certificate file.
 - ☐ **Skip verify:** Establish an encrypted connection without verifying the server certificate. For security reasons, this is not recommended.
 - **Base DN:** Specify the base distinguished name (DN) the system will use to define the scope of the directory search.
 - **Timeout:** Specify the duration (in seconds) the system will wait before considering the server unresponsive.
 - **Retry Count:** Specify the number of times the system will attempt to connect to the LDAP server after timing out. If a secondary server is configured, the system will switch over to the backup server if all retries are exhausted.
5. (Optional) Test the server connection:
 - a. Click **Test connection**.
 - b. Enter a username and password that exists on the target LDAP server.
 - c. Click **Test**. The test result will be shown under the **Test connection** button.
 - d. Modify the server settings and repeat the connection test if necessary. Testing the connection does not apply the configuration changes.
6. Click **Apply**.

Editing an LDAP Server

1. Navigate to **Menu** (☰) > **Administration** > **LDAP Management**.
2. Go to the **Connection Settings** tab.
3. Click the menu (⋮) icon of the server you want to modify and select **Edit**.
4. Modify the settings as necessary. Refer to **Adding an LDAP Server**.
5. (Optional) Click **Test connection** to verify the modified server settings.
6. Click **Apply**.

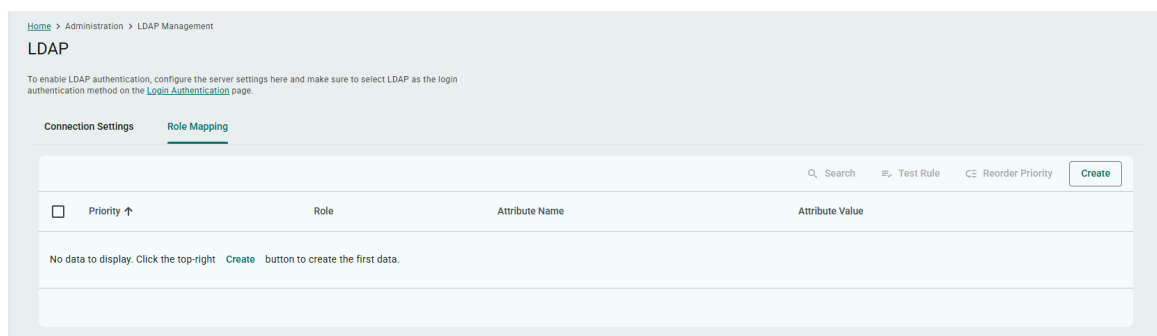
Removing an LDAP Server

1. Navigate to **Menu** (☰) > **Administration** > **LDAP Management**.
2. Go to the **Connection Settings** tab.
3. Click the menu (⋮) icon of the server you want to modify and select **Delete**.
4. When prompted, click **Delete**.

Role Mapping

To access the **Role Mapping** page, in the function tree, navigate to **Menu** (☰) > **Administration** > **LDAP Management** and go to the **Role Mapping** tab.

The **Role Mapping** tab lets configure directory attribute rules. Role mapping rules convert a directory attribute returned by the LDAP server (for example, `memberOf`) into an MXview One role. When a user logs in, the system reads the configured attribute from the directory and evaluates the rules in priority order from highest to lowest. The attributes of the first rule that matches are applied and the corresponding role is assigned to the user. If no rule matches, the login is rejected.



This page displays the following information in a table format:

Item	Description
Priority	The priority of the rule. A higher priority means the rule will be matched against first.
Role	The associated MXview One user role.
Attribute Name	The attribute name in the directory to compare against.
Attribute Value	The attribute value in the directory to match.

Adding a Role Mapping Rule

1. Navigate to **Menu** (☰) > **Administration** > **LDAP Management**.
2. Go to the **Role Mapping** tab.
3. Click **Create**.
4. Configure the following settings:
 - **Role**: Select the MXview One role to assign when the rule is matched.
 - **Attribute Name**: Specify the attribute name in the directory to compare to. The default is **memberOf**.

- **Attribute Value:** Specify the attribute value in the directory to match.
- 5. Click **Apply**.

Reordering Role Mapping Rules

When a user logs in, mapping rules are matched based on priority to determine the role assigned to the user. When multiple rules apply, the higher priority rule is matched first.

1. Navigate to **Menu** (☰) > **Administration** > **LDAP Management**.
2. Go to the **Role Mapping** tab.
3. In the top-right, click **Reorder Priority**.
4. Drag and drop the rule into the desired position.
5. Click **Apply**.



NOTE

The **Priority** and **Role** columns in the role mapping table can be sorted. This only affects the display order and does not change the underlying rule matching priority.

Testing a Role Mapping Rule

1. Navigate to **Menu** (☰) > **Administration** > **LDAP Management**.
2. Go to the **Role Mapping** tab.
3. In the top-right, click **Test Rule**.
4. Select the server to test the rule against.
5. Enter the user account and password of a user in the directory.
6. Click **Test**. The test results will show.
7. Click **Close**.

Editing a Role Mapping Rule

1. Navigate to **Menu** (☰) > **Administration** > **LDAP Management**.
2. Go to the **Role Mapping** tab.
3. Click the menu (⋮) icon of the rule you want to modify and select **Edit**.
4. Modify the settings as necessary. Refer to **Adding a Role Mapping Rule**.
5. Click **Apply**.

Deleting a Role Mapping Rule

1. Navigate to **Menu** (☰) > **Administration** > **LDAP Management**.
2. Go to the **Role Mapping** tab.
3. To delete a single rule:
 - a. Click the menu (⋮) icon of the rule you want to remove and select **Delete**.
 - b. When prompted, click **Delete**.
4. To delete multiple rules:
 - a. Check the box for the rules you want to remove and select **Delete**.
 - b. When prompted, click **Delete**.

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**.

The screenshot displays the MXview ONE License Management interface. At the top, the navigation bar shows 'MXview ONE' and the user 'admin'. The breadcrumb trail is 'Home > Administration > License Management'. The main heading is 'License Management'. Below this, there are two tabs: 'MXview One' (selected) and 'IPS'. The 'MXview One' tab shows a summary of the license: 'Node License', 'Mode: Trial', 'Currently Used: 14', and 'Total Number of Licenses: 2000'. There are also links for 'Wireless Add-on License', 'Power Add-on License', and 'Security Add-on License', all in 'Mode: Trial'. A 'Move License Site ID' link and an 'Add New License' button are also present. Below the summary, there are five cards: 'Trial Remaining' showing '12 days', 'Wireless Add-on License' with an 'Enabled' toggle, 'Power Add-on License' with a 'Disabled' toggle, 'Security Add-on License' with an 'Enabled' toggle, and 'Re-activate License' with a 'Re-activate' button.

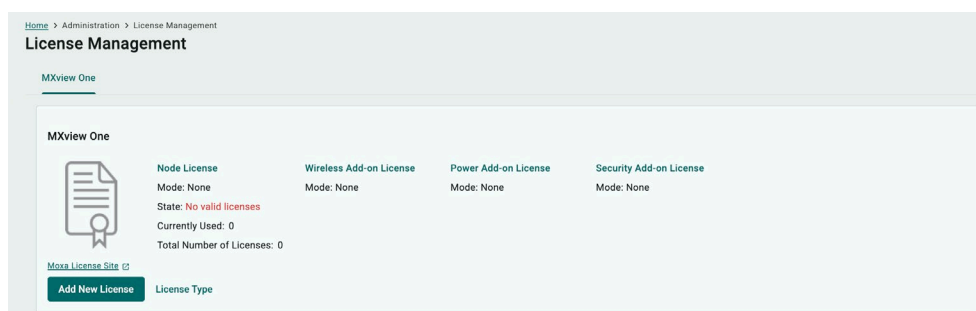
License Type

MXview One supports several types of licenses. Each license has a specific function.

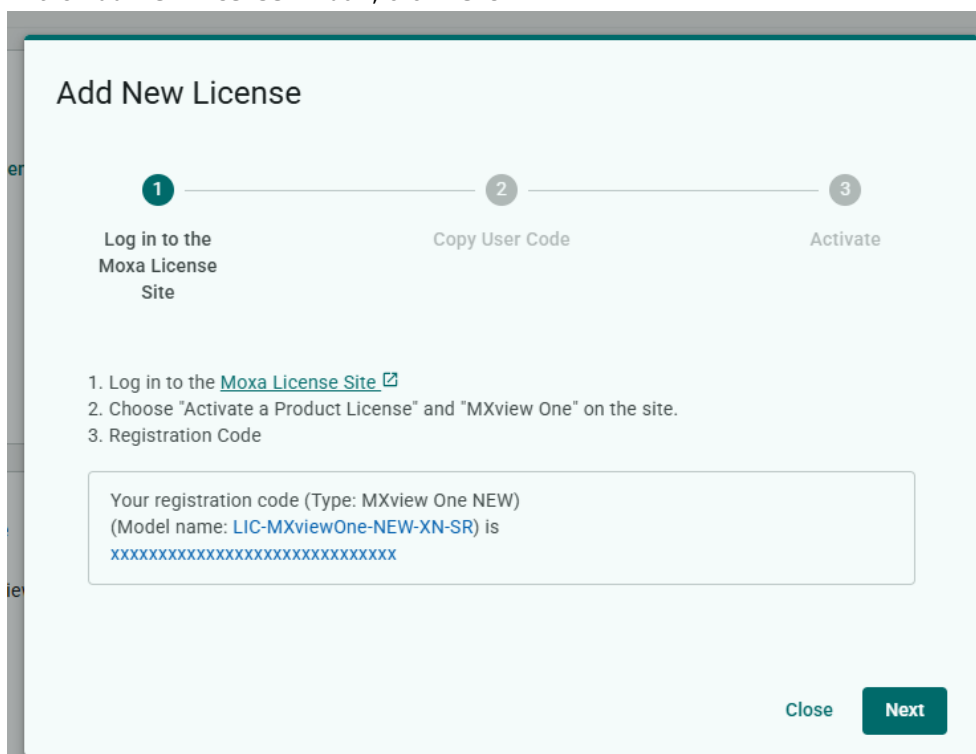
Trial License	Allows you to experience MXview One for 90 days.
Node License	Determines the number of devices that MXview One can monitor in the network.
Wireless Add-on License	Allows you to access additional wireless related functions.
Power Add-on License	Allows you to access additional power related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

Adding a New License

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



3. In the **Add New License** window, click **Next**.



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

Add New License

1 ☒ 2 ☒ 3 ☐

Log in to the Moxa License Site Copy User Code Activate

Copy the User Code to the [Moxa License Site](#)

User Code:

[Close](#) [Next](#)

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

Products and Licenses / Activate a Product License

Product Type:

- Please select a product
- SDC
- IEF
- IEC
- MRC QuickLink
- MXview One**
- MXview
- MX-AOPC UA Server
- MX-AOPC UA Logger
- MXsecurity
- Security Package

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: 00000000000000000000000000000000

User code: 00000000000000000000000000000000

Product Type : MXview One Node_and_Site

☐ 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.

Activate

MXview ONE

- 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.

I know

- 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]
 [REDACTED]
 [REDACTED] has been activated successfully. Visit the [License Activation Portal](#) to see more details about your product and license activation code.

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

Add New License

Log in to the Moxa License Site

Copy User Code

3
Activate

Download the license from the [Moxa License Site](#), and paste the Activation Code here.

Activation Code

Close

Apply

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

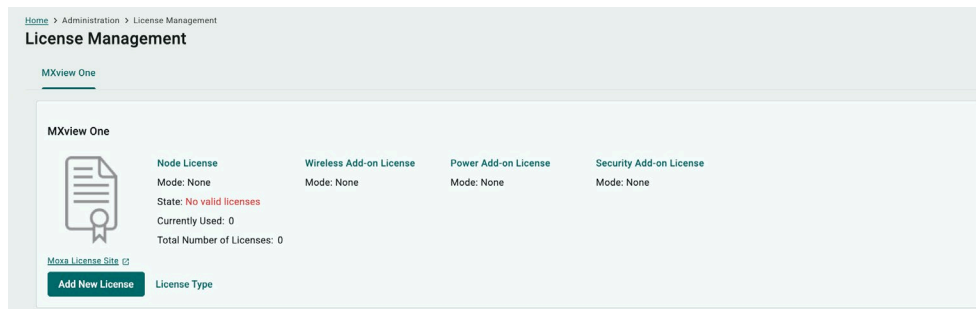
Adding an Add-on License



NOTE

An active node license is required to activate an add-on license.

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



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

The screenshot shows the 'Add New License' window with a progress bar at the top. Step 1, 'Log in to the Moxa License Site', is active and highlighted with a green circle. Step 2, 'Copy User Code', and Step 3, 'Activate', are shown in gray. Below the progress bar, there are instructions: '1. Log in to the [Moxa License Site](#)', '2. Choose "Activate a Product License" and "MXview One" on the site.', and '3. Registration Code'. A text box displays the registration code: 'Your registration code (Type: MXview One NEW) (Model name: LIC-MXviewOne-NEW-XN-SR) is xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx'. At the bottom right, there are 'Close' and 'Next' buttons.

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

The screenshot shows the 'Add New License' window with the progress bar updated. Step 1 is now completed and marked with a green checkmark. Step 2, 'Copy User Code', is active and highlighted with a green circle. Step 3, 'Activate', remains in gray. Below the progress bar, the instruction is 'Copy the User Code to the [Moxa License Site](#)'. A text box labeled 'User Code:' contains the code '1EF0A022C7614F7D93F26EEC4DFC7BA5QGGSIVVQ'. To the right of the text box is a copy icon. At the bottom right, there are 'Close' and 'Next' buttons.

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
Product type :

- 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
Product type : MXview One Power

User code

License Type

Activate

- 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.

I know

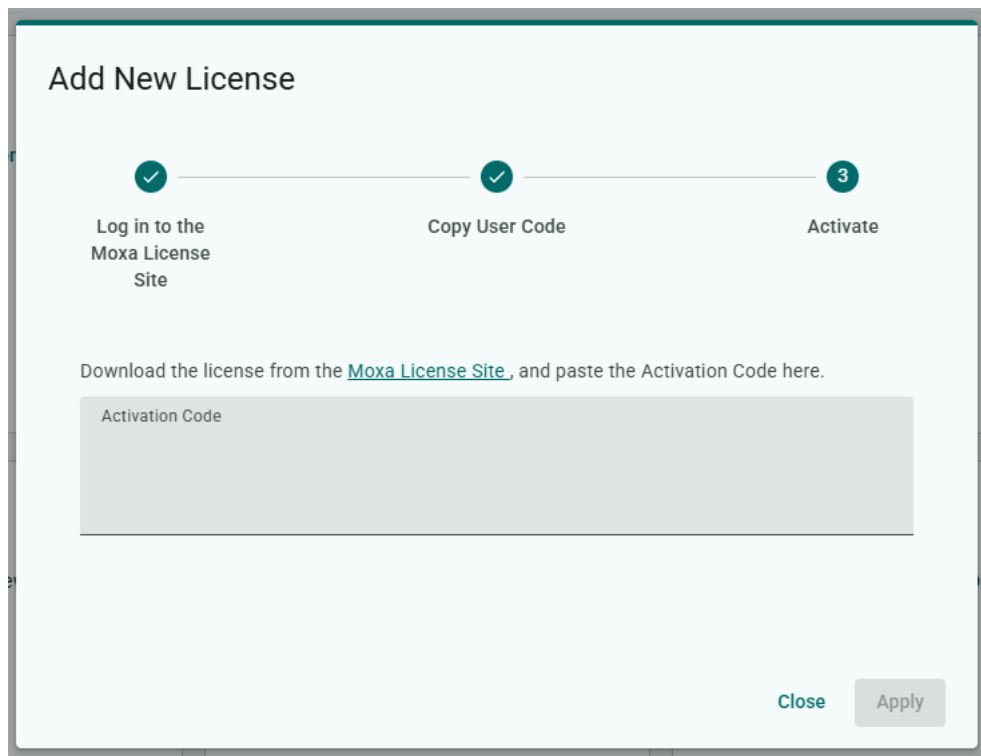
- Check the email account you used to apply for your moxa account. The activation code will be sent to this email address.

Dear Customer,

Your MXview One Activation Code

 has been activated successfully. Visit the [License Activation Portal](#) to see more details about your product and license activation code.

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



Add New License

1. Log in to the Moxa License Site

2. Copy User Code

3. Activate

Download the license from the [Moxa License Site](#), and paste the Activation Code here.

Activation Code

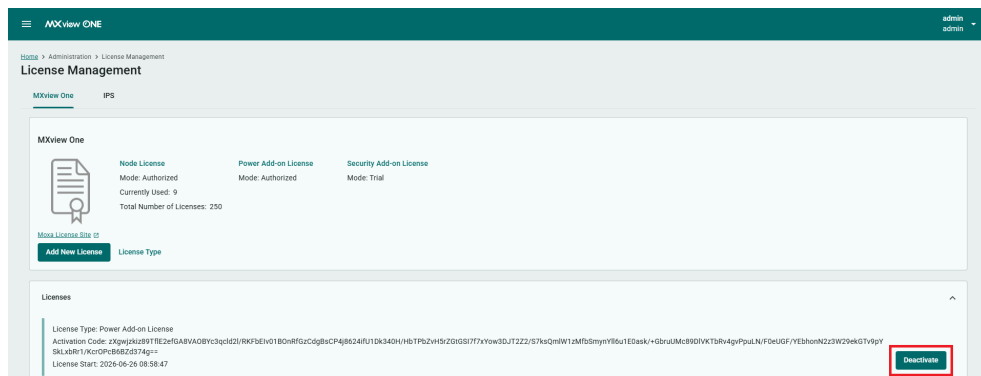
Close Apply

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

Deactivating a License

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

1. Navigate to **Menu** (☰) > **Administration** > **License Management**.
2. Expand the **Licenses** section.
3. Click **Deactivate** and MXview One will deactivate the license.



NOTE

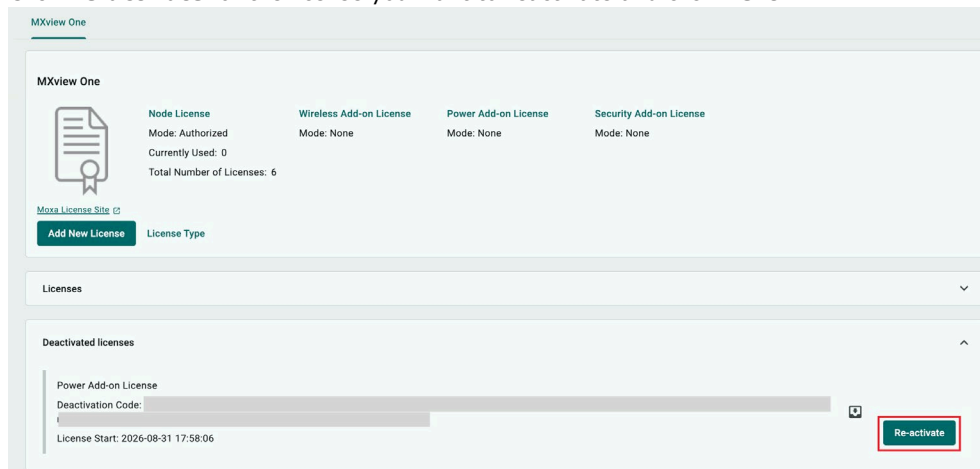
If you only have a single node license with one add-on license, you must deactivate the add-on license first before deactivating the node license next.

If you have multiple node licenses, you can deactivate node and add-on licenses in any order.

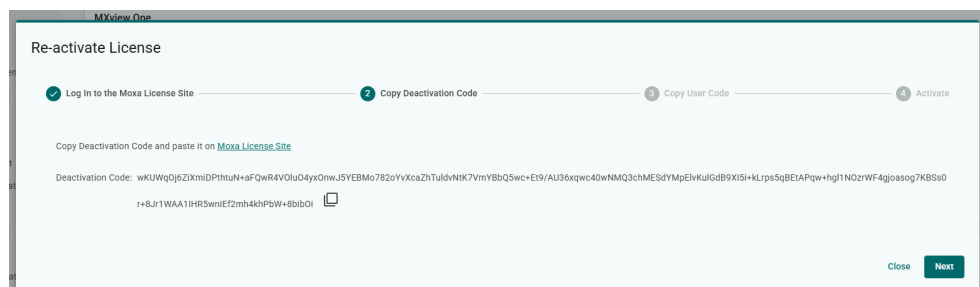
Reactivating a Deactivated License

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

1. Navigate to **Menu** (☰) > **Administration** > **License Management**.
2. Expand the **Deactivated Licenses** section.
3. Click **Re-activate** for the license you want to reactivate and click **Next**.



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



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

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

Product Transfer



NOTE

Reactivating a Deactivated License and **Transfer a Deactivated License to another MXview One instance** use the same menu here.

If you are performing '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.

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

Message notification
Deactivation Success
I know

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

MOXA®
Dear Customer,
Your New MXview One Activation Code
ed successfully. You can now start using MXview on this system. Visit the License Activation Portal to see more details about your product and license activation code.

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

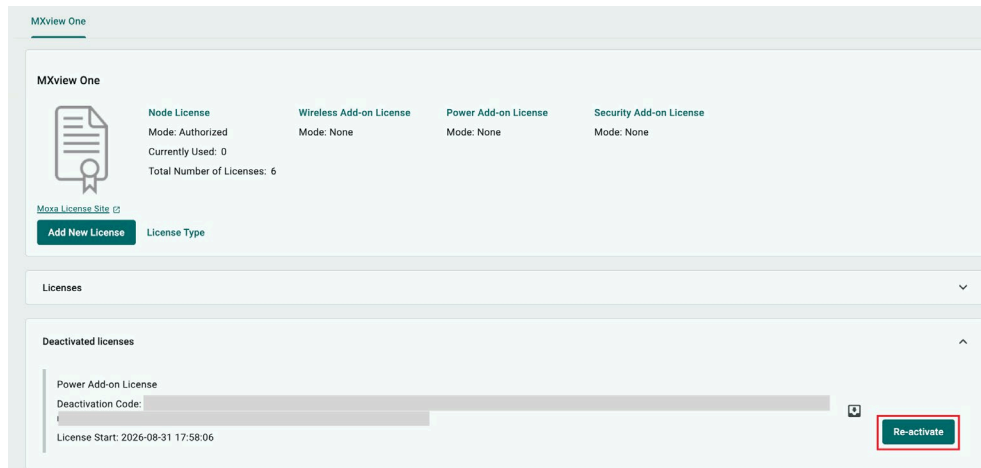
Re-activate License			
Log In to the Moxa License Site	Copy Deactivation Code	Copy User Code	Activate
Download the license from the Moxa License Site , and paste the Activation Code here.			
Activation Code			
			Close Apply

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

Transferring a License to a Different Instance of MXview One

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

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



3. Open a web browser and go to <https://license.moxa.com>. Select **MXview One** and log in using your Moxa account.
4. Select **Products and Licenses** and click **Transfer a Product License**. Then, select **MXview One** from the product type list.
5. Paste the **Deactivation Code** and the **New User Code** from a new installation of MXview One. Then, click **Product Transfer**.



NOTE

To obtain a new User Code, refer to **Adding a New License** and follow the steps to obtain and copy the new User Code.

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

Message notification
Deactivation Success
I know

7. 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

ed successfully. You can now start using MXview on this system. Visit the [License Activation Portal](#) to see more details about your product and license activation code.

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

Re-activate License



Log In to the Moxa License Site



Copy Deactivation Code



Copy User Code



4
Activate

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 licenses and activate them as required. Alternatively, you can delete any devices you do not need to monitor.

License Management

MXview One



License

Mode: Authorized

State: **Not enough nodes for**

Current Nodes: **2001**

Licensed Nodes: **2000**

[Moxa License Site](#)

[Add New License](#)

License Type

Wireless Add-on License

Mode: Trial

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

please purchase additional nodes

Licenses

Wireless Trial Remaining

58

days

Re-activate License

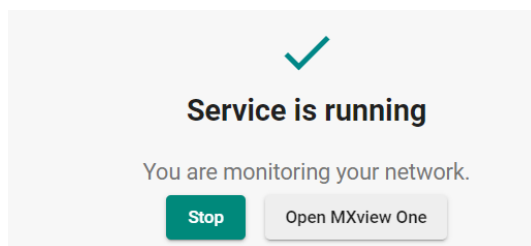
Use both the Deactivation Code and a User Code to re-activate your license.

Buy additional node 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.

Delete extra devices

1. Press the Stop button in the Control Panel.



- 2.
3. After 1 minute, click **Start** and wait for the status to display 'Service is running'.
4. Click **Open MXview One** and log in to MXview One.
5. Navigate to **Menu (☰) > Topology**.
6. Select the devices you want to remove and click **Delete**. MXview One will revoke the nodes on the license.

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.

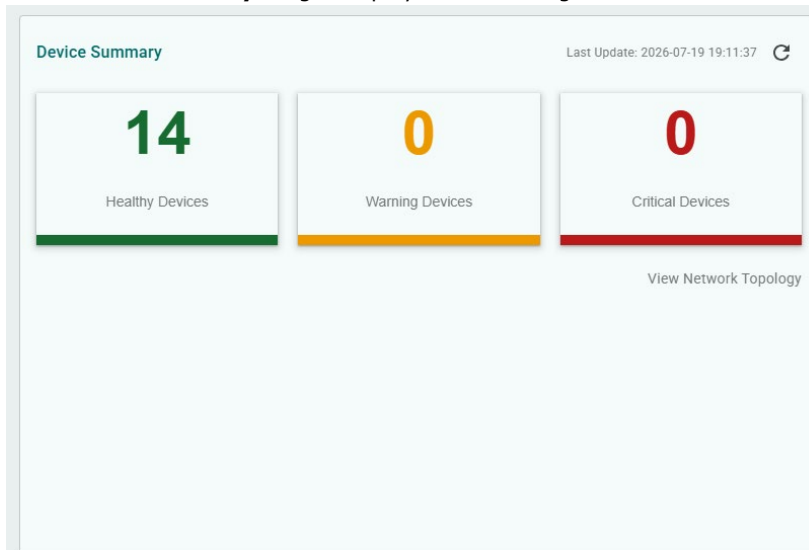
The **Dashboard** displays the following widgets:

- 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

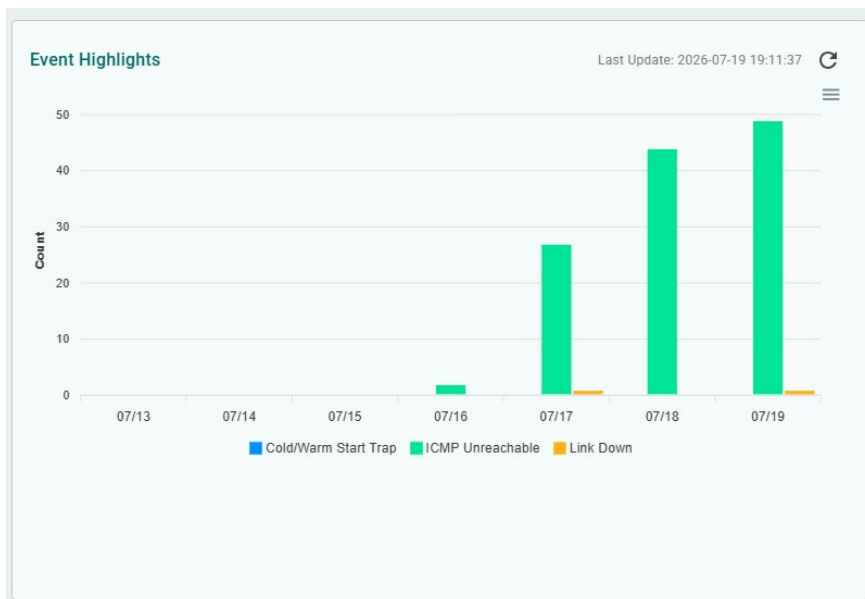
The **Device Summary** widget displays the following information about the devices on your network:



- **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

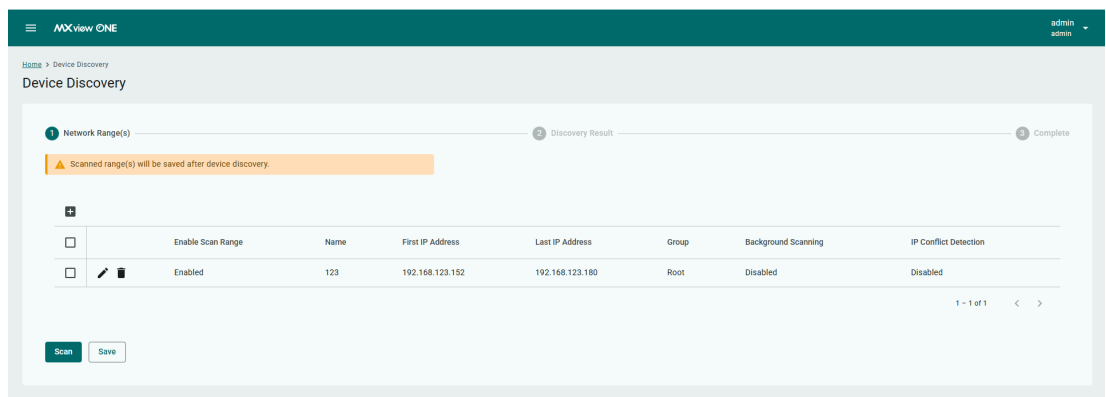
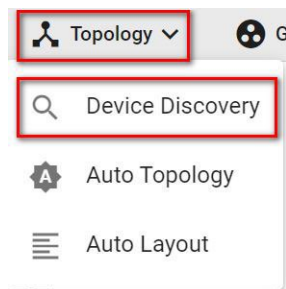
MXview One will display one of the following graphics to indicate devices:

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 select **Device Discovery** from the **Topology** toolbar menu.



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

- 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.
 - c. In the **Edit Scan Range** screen, modify the scan range settings.
 - d. Click **Apply**.
The **Device Discovery** screen displays the **Network Range** table with the updated scan range information.

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

The screenshot shows the 'Device Discovery' progress bar with three steps: 1. Network Range(s) (checked), 2. Discovery Result (active), and 3. Complete. Below the progress bar is a table with three columns: Device Alias, Device IP, and Group. The table contains one row with the following data: Device Alias: 192.168.127.16--EDS-4012-8P-4GS, Device IP: 192.168.127.16, and Group: Root. At the bottom right of the table, it says '1 - 1 of 1' with navigation arrows. A 'Next' button is located at the bottom left of the table.

Device Alias	Device IP	Group
192.168.127.16--EDS-4012-8P-4GS	192.168.127.16	Root

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

The screenshot shows the 'MXview ONE' interface. The top navigation bar is dark green with the 'MXview ONE' logo and a user profile icon labeled 'admin'. Below the navigation bar is a breadcrumb trail: 'Home > Device Discovery'. The main content area is titled 'Device Discovery' and shows a progress bar with three steps: 1. Network Range(s) (checked), 2. Discovery Result (checked), and 3. Complete. Below the progress bar, it says '0 device(s) added to MXview One'. A 'Browse Topology' button is located at the bottom left of the main content area.

- 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**.

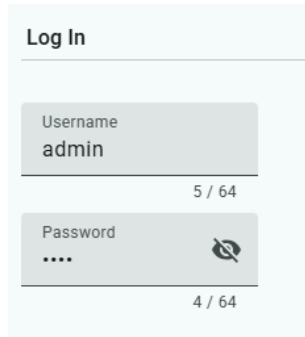
- Navigate to **Menu** (☰) > **Administration** > **Default Device Template**.
- Scroll down to the **MXview One Polling Interval** section.
-

The screenshot shows the 'MXview One Polling Interval' settings. It has two input fields: 'ICMP Polling Interval' with the value '10' and 'SNMP Polling Interval' with the value '60'. Both fields have a 'sec' label below them.

- 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.

5. Configure the following SNMP polling settings:
 - **SNMP polling interval:** Specify the time in seconds between polls.
6. 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
5 / 64

Password
....
4 / 64

7. Click **Save**.

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

The image shows a screenshot of the 'SNMP Configuration' section in a web interface. It contains several input fields and dropdown menus arranged in a grid. The settings shown are: SNMP Version (V1), Port (161), Username (admin), Password (empty), Read Community (public), Write Community (private), Data Encryption (NoAuth), Authentication (MD5), Encryption Protocol (DES), and Encryption Password (empty).

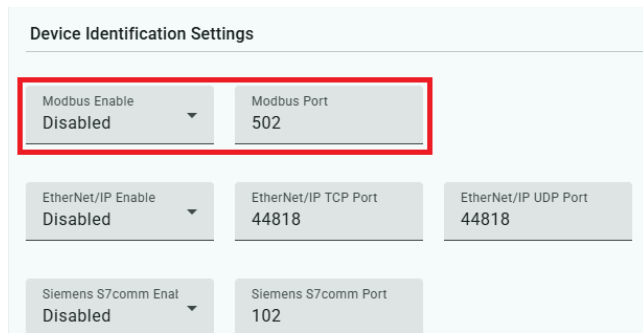
SNMP Configuration	
SNMP Version V1	Port 161
Username admin	Password
Read Community public	Write Community private
Data Encryption NoAuth	Authentication MD5
Encryption Protocol DES	Encryption Password

3. Configure the following settings:
 - **SNMP Version:** Select the SNMP protocol version.
 - **SNMP Port:** Specify the SNMP port.
 - **Username:** Specify the SNMP server username.
 - **Password:** Specify the SNMP server password.
 - **Read Community:** Specify the new community string.
 - **Write Community:** Specify the new community string.
 - **Data Encryption:** Select the data encryption method.
 - ☐ NoAuth
 - ☐ AuthNoPriv
 - ☐ AuthPriv
 - **Authentication:** Select the authentication method.
 - ☐ MD5
 - ☐ SHA
 - ☐ SHA256
 - ☐ SHA512
 - **Encryption Protocol:** Select the encryption protocol and input the Encryption Password.
 - ☐ DES
 - ☐ AES
4. Click **Save**.

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**.
2. Scroll down to the **Device Identification Settings** section.



Device Identification Settings

Modbus Enable Disabled	Modbus Port 502	
EtherNet/IP Enable Disabled	EtherNet/IP TCP Port 44818	EtherNet/IP UDP Port 44818
Siemens S7comm Enal Disabled	Siemens S7comm Port 102	

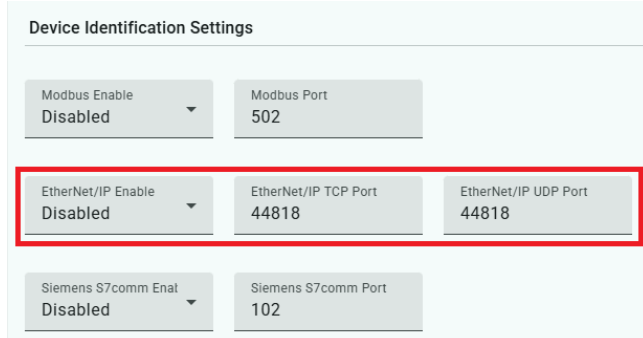
Configure the following settings:

- a. **Modbus Enabled:** Enable or disable Modbus TCP settings.
 - b. **Modbus Port:** Specify the Modbus TCP port.
3. Click **Save**.

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 Disabled	Modbus Port 502	
EtherNet/IP Enable Disabled	EtherNet/IP TCP Port 44818	EtherNet/IP UDP Port 44818
Siemens S7comm Enal Disabled	Siemens S7comm Port 102	

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**.

Changing Siemens S7comm Settings

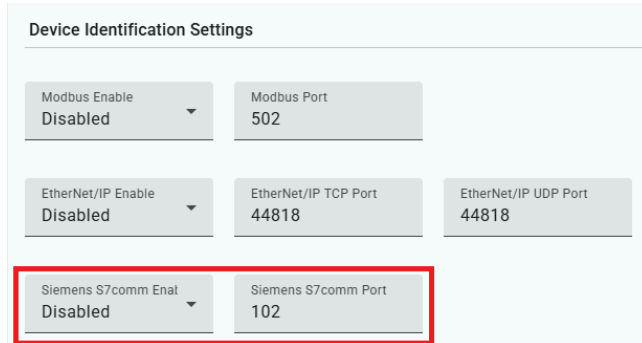
By configuring Siemens S7comm Settings in the Default Device Template section, MXview One will be able to detect whether an ICMP device has Siemens S7comm attributes or not. If an ICMP device supports

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	
EtherNet/IP Enable Disabled	EtherNet/IP TCP Port 44818	EtherNet/IP UDP Port 44818
Siemens S7comm Enal Disabled	Siemens S7comm Port 102	

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**.

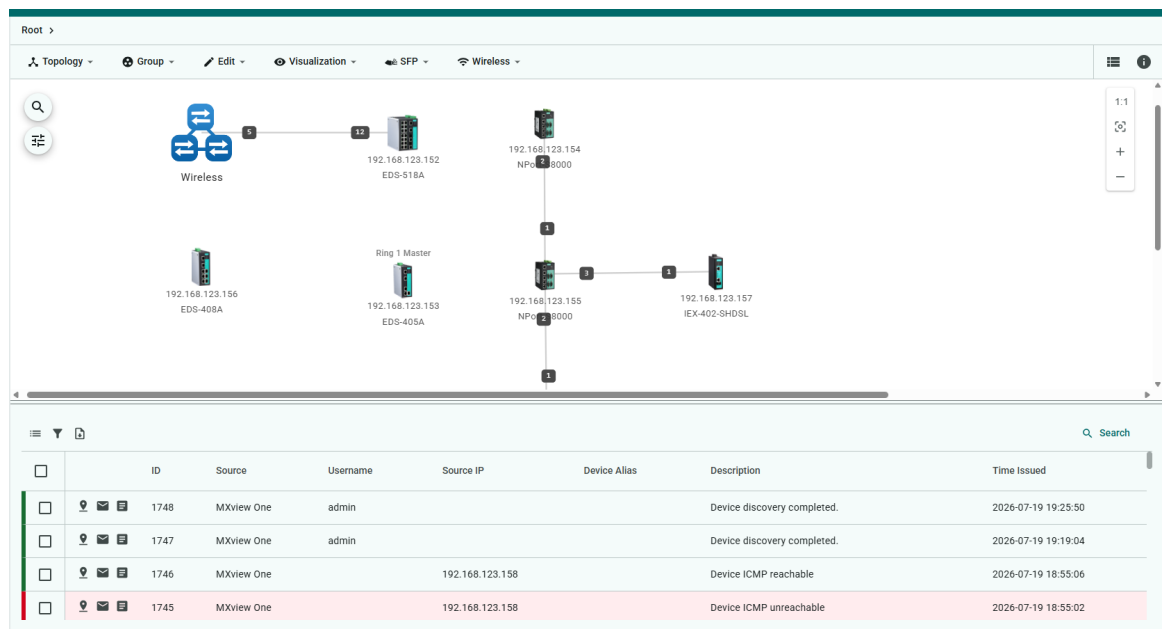
7. Topology Management

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

Topology Overview

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

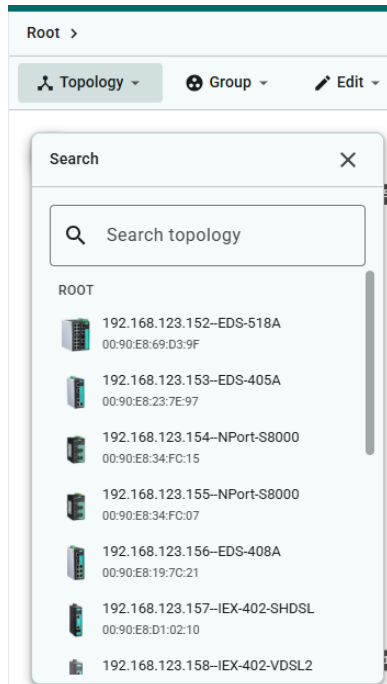
- Display a graphical representation of a real network.
- Show connecting relationships between devices.
- Indicate the status of devices and links.



Viewing the Topology Map

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

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



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



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

Device Properties

Current Status

Basic Device Properties

Alias

192.168.123.153--EDS-405A

Model Name

EDS-405A

MAC Address

00:90:E8:23:7E:97

Availability

96.54%

System Description

EDS-405A

System Object ID

.1.3.6.1.4.1.8691.7.6

System Contact

System Name

Managed Redundant Switch 04619

System Location

NSD Lab

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

Device Properties

Current Status

No events

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



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

Link Properties

Link Information

From

192.168.123.162 Port 11

To

192.168.123.163 Port 10

Link Speed

1 Gb

SFP Information

From

192.168.123.162

TX (dBm)

-6.1

RX (dBm)

-16.3

Temp. (°C)

44.3

Volt. (V)

3.4

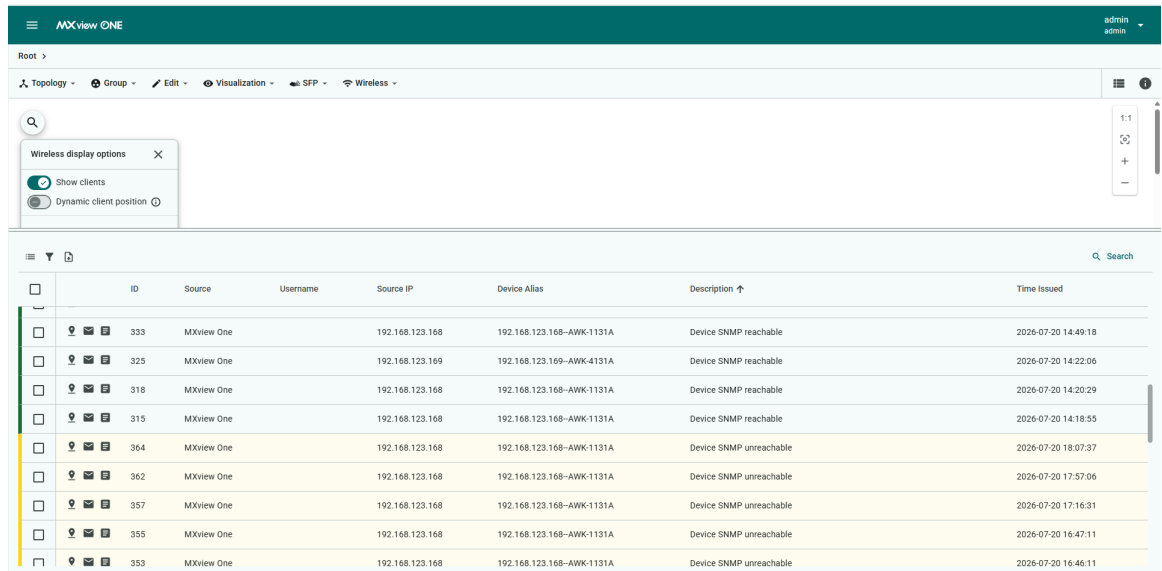
Viewing Recent Events

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.



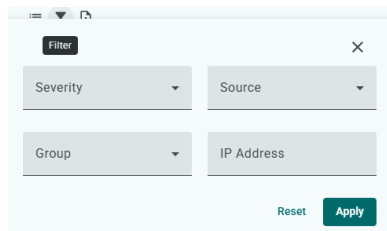
ID	Source	Username	Source IP	Device Alias	Description	Time Issued
333	MXview One		192.168.123.168	192.168.123.168-AWK-1131A	Device SNMP reachable	2026-07-20 14:49:18
325	MXview One		192.168.123.169	192.168.123.169-AWK-4131A	Device SNMP reachable	2026-07-20 14:22:06
318	MXview One		192.168.123.168	192.168.123.168-AWK-1131A	Device SNMP reachable	2026-07-20 14:20:29
315	MXview One		192.168.123.168	192.168.123.168-AWK-1131A	Device SNMP reachable	2026-07-20 14:18:55
364	MXview One		192.168.123.168	192.168.123.168-AWK-1131A	Device SNMP unreachable	2026-07-20 18:07:37
362	MXview One		192.168.123.168	192.168.123.168-AWK-1131A	Device SNMP unreachable	2026-07-20 17:57:06
357	MXview One		192.168.123.168	192.168.123.168-AWK-1131A	Device SNMP unreachable	2026-07-20 17:16:31
355	MXview One		192.168.123.168	192.168.123.168-AWK-1131A	Device SNMP unreachable	2026-07-20 16:47:11
353	MXview One		192.168.123.168	192.168.123.168-AWK-1131A	Device SNMP unreachable	2026-07-20 16:46:11

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.



Filter ✕
Severity ▾ Source ▾
Group ▾ IP Address ▾
Reset Apply

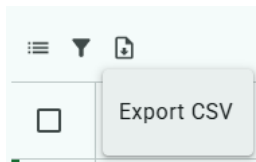
- b. Specify any of the following criteria:

- ☐ **Severity:** Select the event severity level
 - Any
 - Information
 - Warning
 - Critical
 - System Information

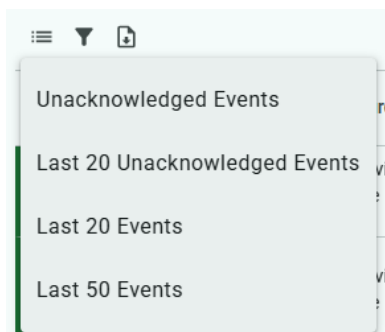
- ☐ **Source:** Select the source that detected the event
 - Any
 - MXview One
 - Trap
 - ☐ **Group:** Select the device group
 - ☐ **IP Address:** Select the device IP address
- c. Click **Apply**.
MXview One filters the table to only display events that match the specified criteria.
4. To acknowledge 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	Username	Source IP
☐	2277	MXview One		192.168.123.168

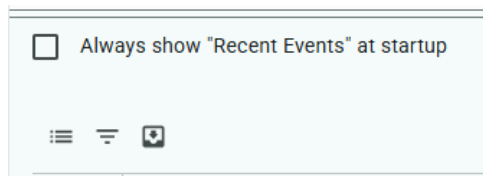
6. To export data displayed in the **Recent Events** tab:
- a. Click the **Export** (📄) icon.



- b. Select **Export CSV**.
 - c. Specify the location to save the exported file.
 - d. Click **Save**.
MXview One exports the displayed event data as a CSV file.
7. To quickly filter event, click the **Quick filter event** (☰) icon to find the events.
The events include the following:
- Unacknowledged Events
 - Last 20 Unacknowledged Events
 - Last 20 Events
 - Last 50 Events.



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

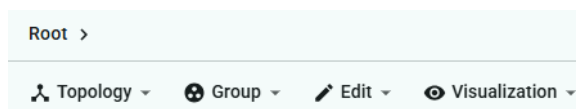


Organizing the Topology Structure By Group Function

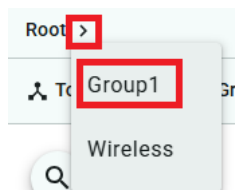
The Topology Map can be organized into a multi-layer tree structure of up to 5 layers. Organizing the topology structure into groups helps manage a large number of nodes on the computer screen. For example, users can move nodes of the same subnet or location into the same group. Root, which is the only group at the first layer, exists by default and cannot be deleted. Groups created by users are in the layer under Root. Devices can be moved between groups.

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

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



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

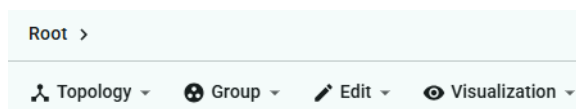


➤ You can also click the following icon used to indicate user-defined groups within the Topology Map:

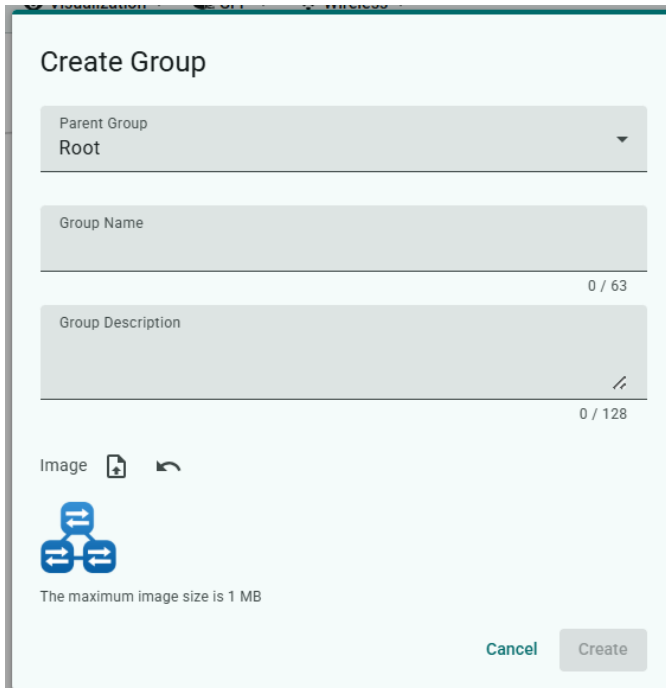


2. If **List view** is displayed, click the **Topology view** (👤) icon in the top right corner.

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



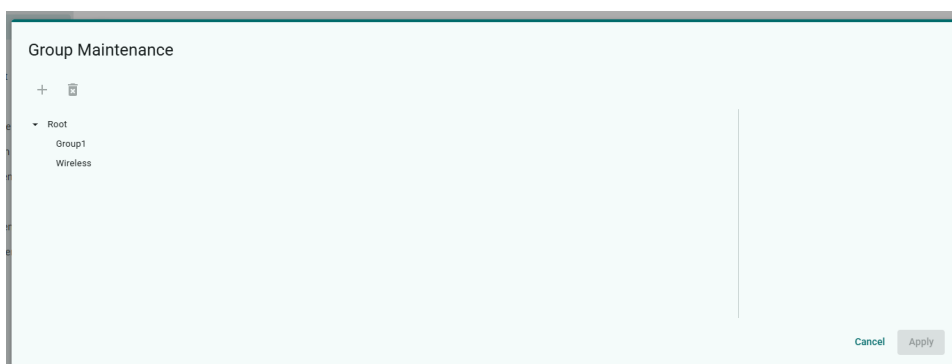
3. To create a group:
 - a. Navigate to **Group > Create Group**.



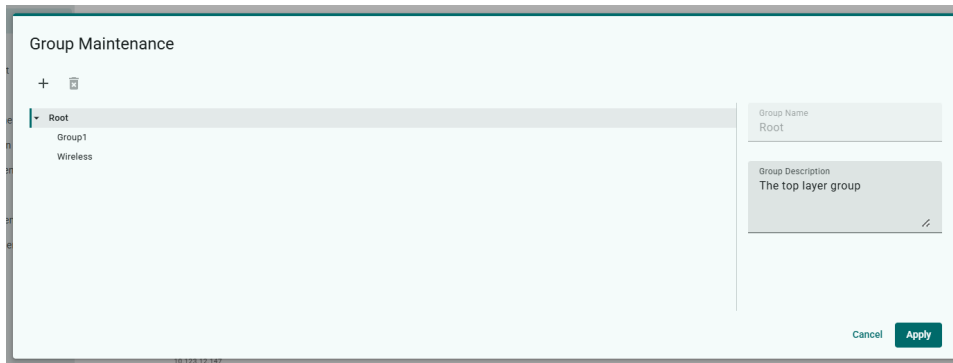
The 'Create Group' dialog box contains the following fields and controls:

- Parent Group:** A dropdown menu currently showing 'Root'.
- Group Name:** A text input field with a character count of '0 / 63'.
- Group Description:** A larger text input field with a character count of '0 / 128' and a small edit icon.
- Image:** A section with an 'Image' label, an upload icon, and a refresh icon. Below it is a placeholder icon showing three connected nodes. A note states 'The maximum image size is 1 MB'.
- Buttons:** 'Cancel' and 'Create' buttons at the bottom right.

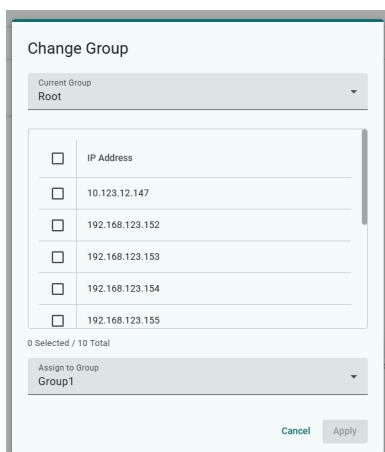
- b. Configure the following settings:
 - ☐ Parent Group
 - ☐ Group Name
 - ☐ Group Description
 - ☐ Group Icon
 - c. Click **Create**.
MXview One will add the group below to the specified parent group.
4. To reorganize the groups within the Topology Map structure:
 - a. Navigate to **Group > Group Maintenance**.



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



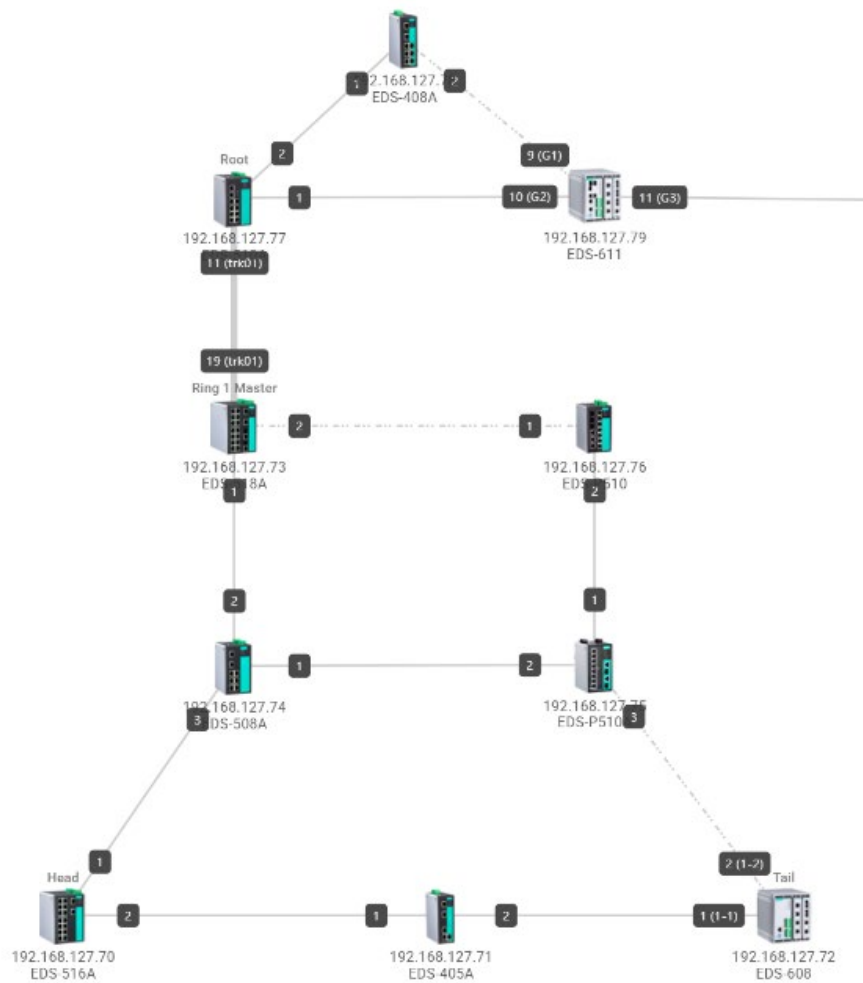
- c. (Optional) Edit the group details or perform one of the following points:
 - i. (Optional) Click **Add** to add a new group below the selected layer.
 - ii. (Optional) Click **Delete** to remove a group from the topology structure.
- d. Click **Apply**.
5. To reassign the device(s) in a group:
 - a. There are two ways to reassign the device(s) in a group:
 - i. Navigate to Group > **Change Group**. The Change Group screen appears.
 - ii. Select the device(s) you want to reassign on the topology and click the Change Group icon on the toolbar.



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

Redundant Topologies

Redundant topologies have at least one backup link, which will be indicated with a dashed line:



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

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



NOTE

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

PoE Power Consumption Visualization

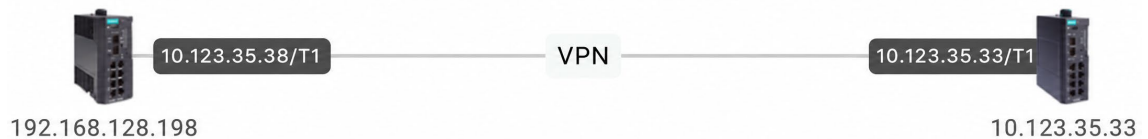
By periodic polling, a PoE link will display the port number, power (watts), voltage (V), and current (mA) directly on the topology map.



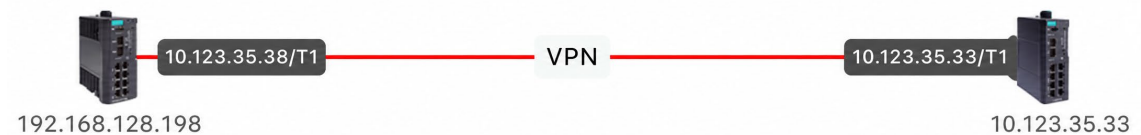
VPN Tunnel Visualization

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

1. The VPN tunnel is connected.



2. The VPN tunnel is disconnected.

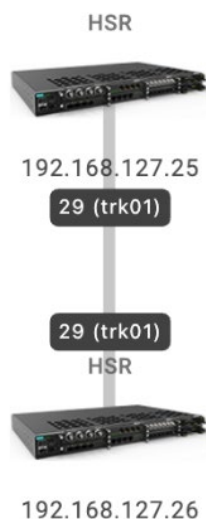


NOTE

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

Port Trunking

Port trunking, also called link aggregation, involves grouping links into a link aggregation group. Trunking links will be indicated with thick, solid lines.





NOTE

Only **Auto Topology** can draw thick lines for trunking links. Trunking links that are added manually will appear as solid lines.



NOTE

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



Adding Devices and Links

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

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 Settings

SNMP Version V1 Port 161

Username Password

Read Community public Write Community private

Data Encryption NoAuth Authentication MD5

Encryption Protocol DES Encryption Password

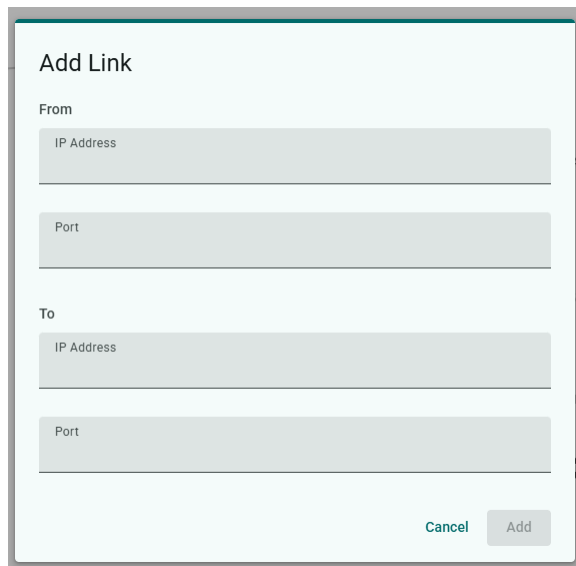
Cancel Add

- 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.



The screenshot shows a modal dialog titled "Add Link". It is divided into two main sections: "From" and "To". Each section contains two text input fields, one labeled "IP Address" and one labeled "Port". At the bottom right of the dialog, there are two buttons: "Cancel" and "Add".

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



NOTE

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



NOTE

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



NOTE

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



NOTE

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

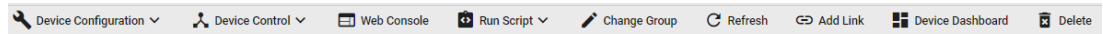
Deleting Devices and Links

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

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

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

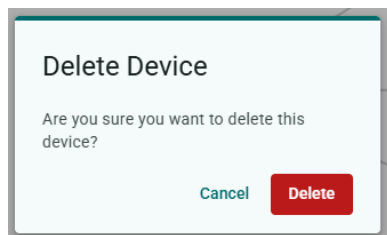
2. To delete a device from the Topology Map:
 - a. Select the device.



The following toolbar menu will appear.

- b. Click **Delete**.

A confirmation screen will appear.

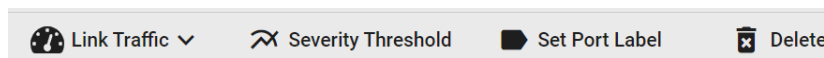


- c. Click **Delete**.
MXview One deletes the device from the Topology Map.

3. To delete a link from the Topology Map:

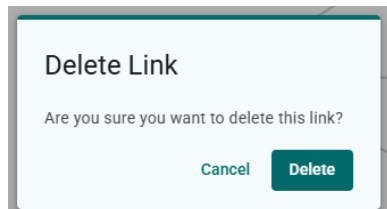
- a. Select the link.

The following toolbar menu will appear.



- b. Click **Delete**.

A confirmation screen will appear.



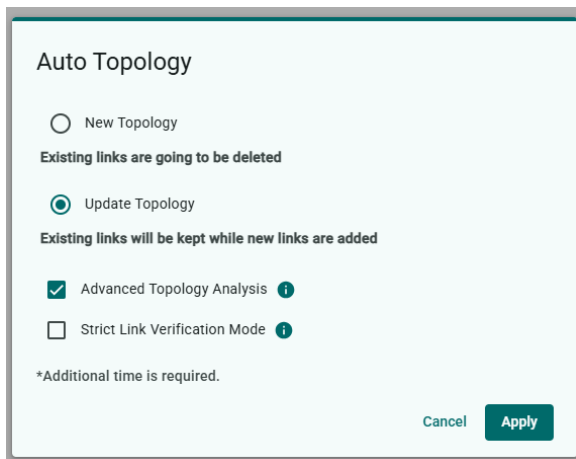
- c. Click **Delete**.
MXview One deletes the link from the Topology Map.

Updating the Topology Map

Updating the existing topology adds new links and updates existing links, but does not change the status of links that are indicated as having been disconnected or links that were drawn manually.

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

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



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**.



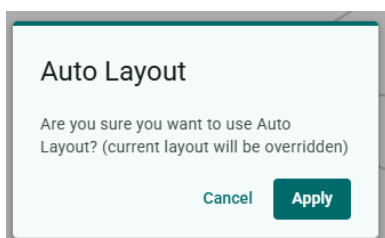
NOTE

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**.
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**.



4. Click **Apply**.

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**.
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**.

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.

Cancel Apply

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



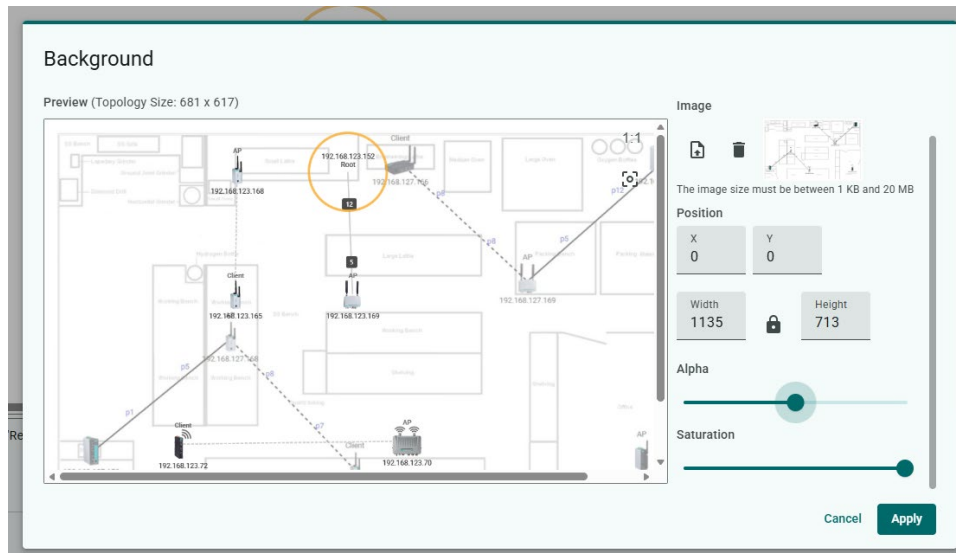
NOTE

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**.
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**.



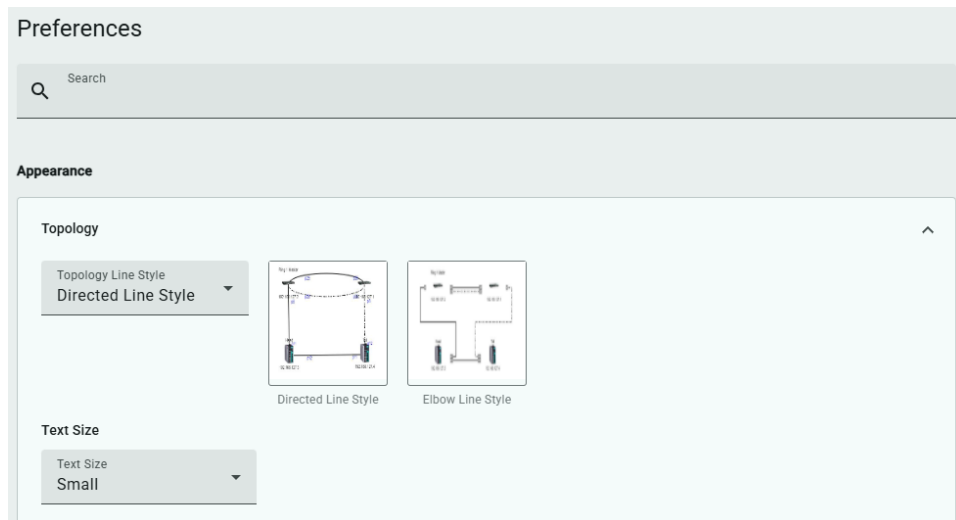
4. Upload the background image by using one of the following methods:
 - The image size must be less than 20 MB.
 - Click **Set Background** (📎) icon to upload the image file.MXview One will set the uploaded image as the Topology Map background.
5. Use the sliders to modify the **Alpha** and **Saturation** value of a background image.

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

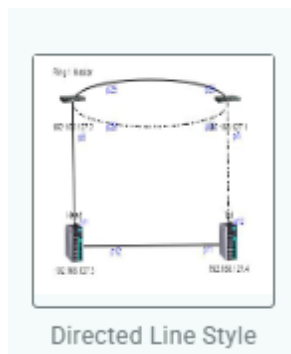
Editing the Topology Appearance

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

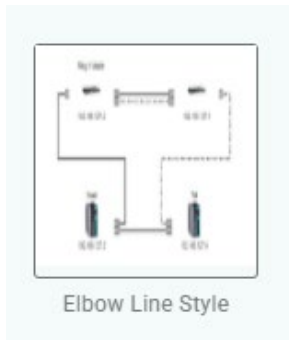
- Navigate to **Menu (☰) > Administration > Preferences**.
- In the **Appearance** section, expand **Topology**.



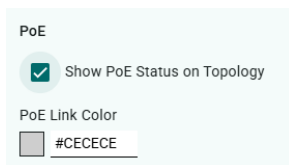
- To modify the Topology Line Style, select one of the following from the drop-down list:
 - **Directed Line Style**
MXview One applies the following style to the lines indicating the links between devices in the Topology Map:



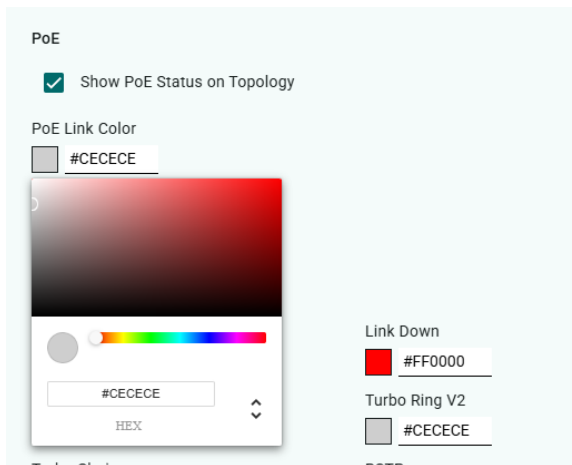
- **Elbow Line Style**
MXview One applies the following style to the lines indicating the links between devices in the Topology Map:



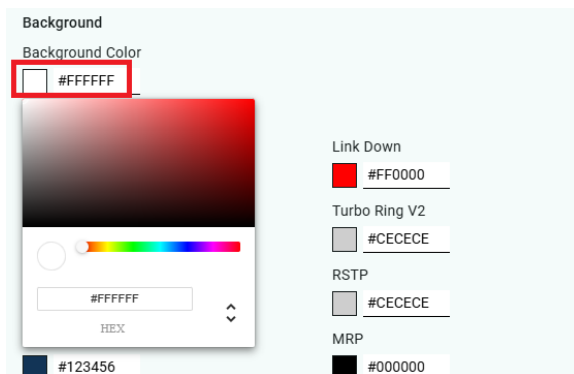
4. To modify the text size in MXview One:
Select one of the following from the drop-down list:
 - Large
 - Medium
 - Small
5. To modify how MXview One displays Power-over-Ethernet (PoE) links:
 - a. Select the **Show PoE Status on Topology** check box to indicate the PoE link status on the Topology Map.



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



- c. (Optional) Clear the **Show PoE Status on Topology** check box to hide the PoE link status on the Topology Map.
6. To modify the Topology Map background, click the Background Color field and specify a new color.



7. To modify the color used to indicate the status of specific links in the Topology Map, click to modify the **Status Color** hex code for any of the following links:
- Link Up
 - Link Down
 - Turbo Ring V1
 - Turbo Ring V2
 - Turbo Chain
 - RSTP
 - PRP/Coupling LAN A
 - PRP/Coupling LAN B
 - HSR Ring
 - Multiple Network Coupling
 - MRP
 - MRP Interconnect

Status Color	
Link Up	Link Down
<input type="color"/> #CECECE	<input type="color"/> #FF0000
Turbo Ring V1	Turbo Ring V2
<input type="color"/> #CECECE	<input type="color"/> #CECECE
Turbo Chain	RSTP
<input type="color"/> #CECECE	<input type="color"/> #CECECE
Multiple Network Coupling	MRP
<input type="color"/> #123456	<input type="color"/> #000000
MRP Interconnect	
<input type="color"/> #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**.

Editing the Device Appearance

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

1. Navigate to **Menu** (☰) > **Administration** > **Preferences**.
2. In the **Appearance** section, expand **Device**.

Device

Preview

IP Address
None

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

Save

3. To modify the label that indicates the device in the Topology Map:
 - a. Select one of the following properties from the **Bottom Label** drop-down under the Preview image:
 - ☐ Location
 - ☐ Alias
 - ☐ Model Name
 - ☐ MAC

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

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. In the Alias section, select a value for both Bottom Label drop-down lists:
 - ☐ IP Address
 - ☐ MAC

- ☐ Model Name
- ☐ Location
- ☐ SysName



NOTE

If you change the Alias values, you must delete and add the device again for the Alias changes to show on the topology.

5. Click **Save**.

Exporting the Topology Map

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

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

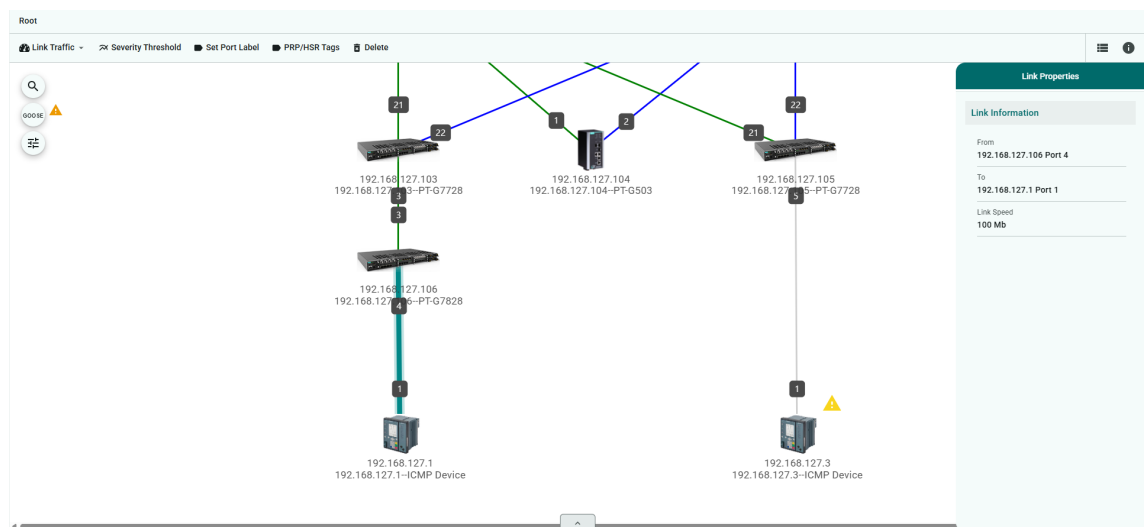
MXview One allows you to monitor the traffic between devices on your network and trigger events for specific traffic conditions. You can apply topology views to monitor traffic load, network security, as well as wireless access points and clients.

Viewing Link Properties

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

1. Navigate to **Menu** (☰) > **Topology**.
2. Click on a link between devices in the Topology Map.

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

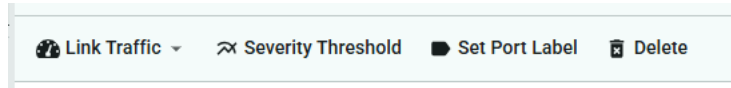


Viewing Port Traffic

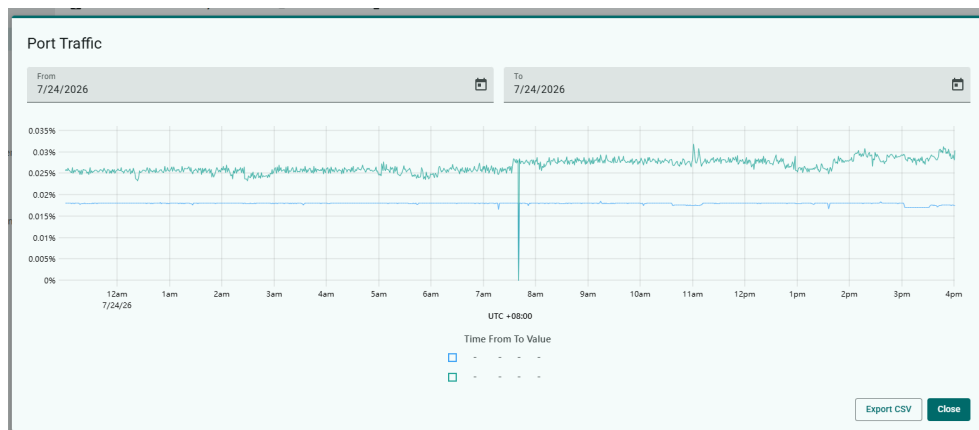
The **Port Traffic** screen displays a graph that shows the utilization percentage (Y-axis) over a specific time period (X-axis). You can also adjust the time period for the data that is displayed by changing the starting date and ending date. The minimum interval you can select is one day and the maximum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

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

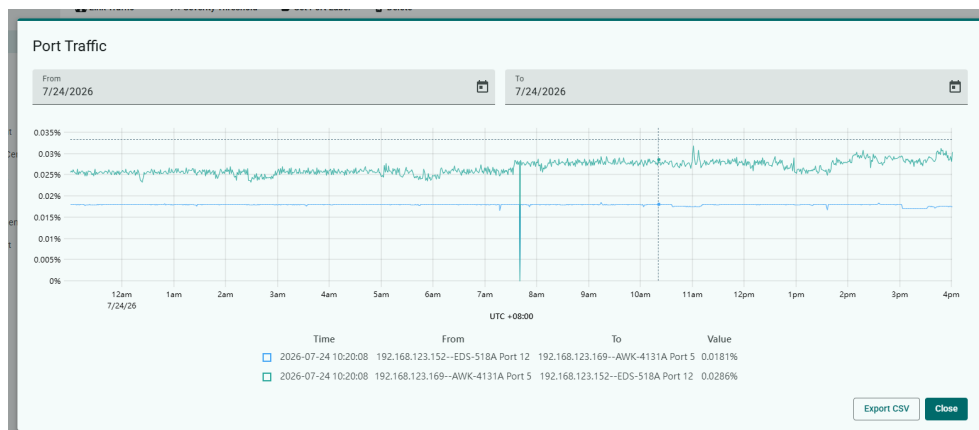


3. Navigate to **Link Traffic** > **Port Traffic**.



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

For example, the green line at the top of the following graph represents traffic from **192.168.127.1 (device IP address) Port 1 to 192.168.127.103 (device IP address) Port 4**.

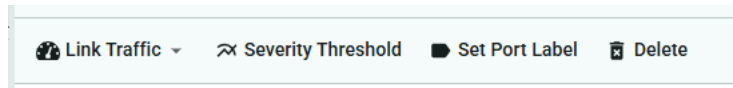


Viewing Packet Error Rates

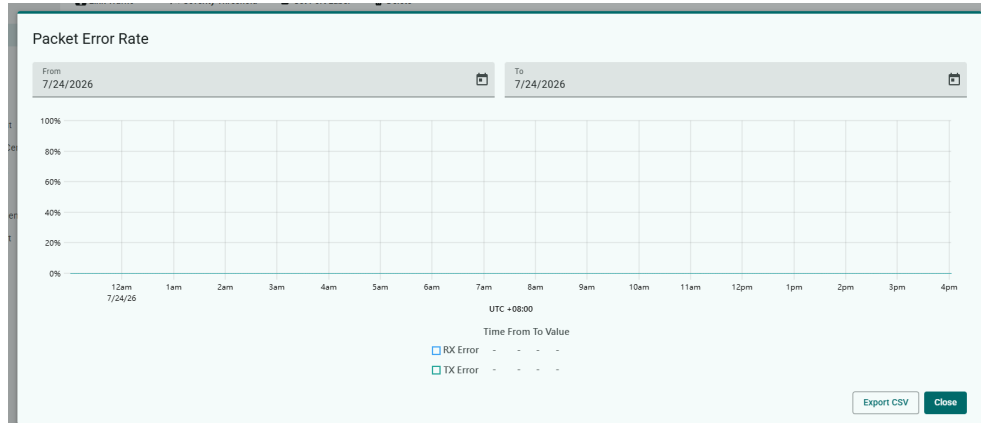
The **Packet Error Rate** screen displays a graph that shows the packet error rate (Y-axis) over a specific time period (X-axis). You can also adjust the time period for the data that is displayed by changing the start and end dates. The minimum interval is one day and the maximum interval you can select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

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

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



- Navigate to **Link Traffic > Packet Error Rate**.



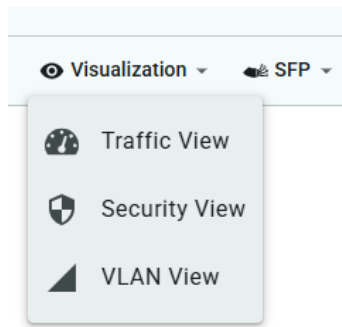
- To adjust the time period for the graph data:
 - Click the **From** date and select a new starting date.
 - Click the **To** date and select a new ending date.
- Hover over a line to view the packet error rate.



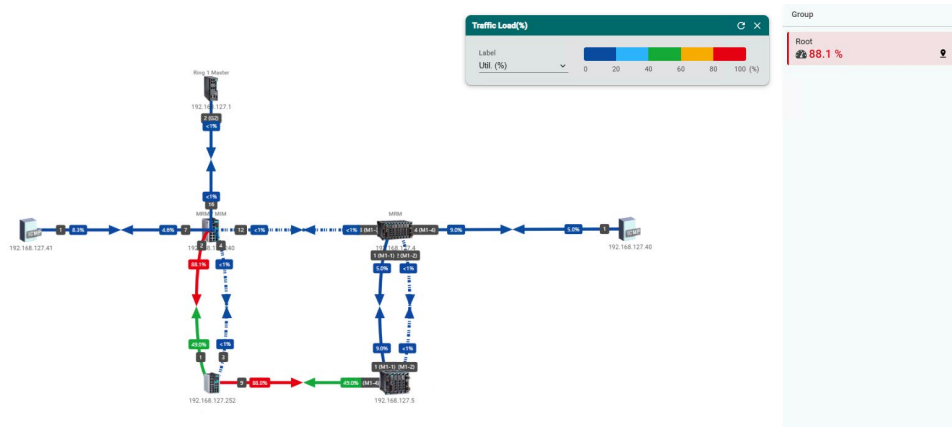
Monitoring Traffic Loads

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

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

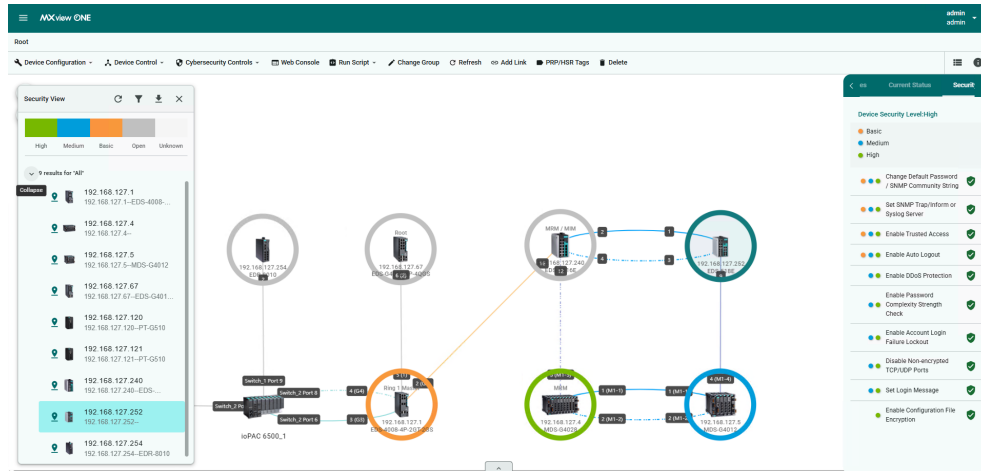


NOTE

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

1. Navigate to **Menu** (☰) > **Topology**.
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.
- From the toolbar menu, navigate to **Visualization > Security View**.
- The **Security View** window will appear. The Topology Map indicates the security level of each device with a color-coded circle.

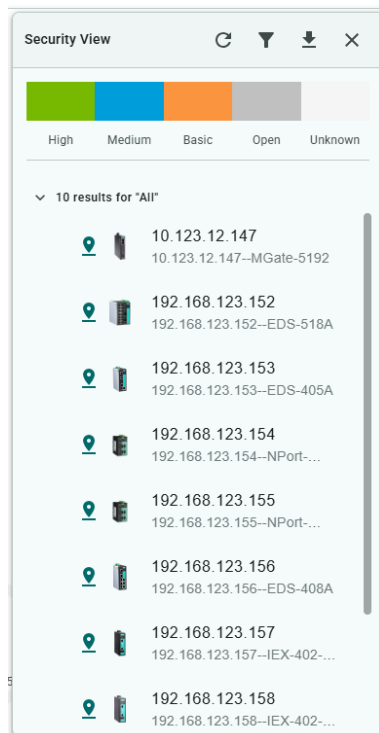


- To filter the devices in the **Security View** window by security level:

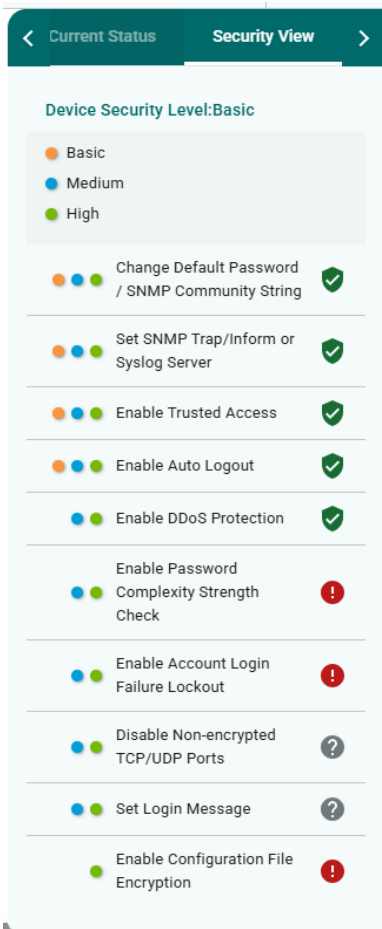
- Click the **Filter** (≡) icon.
- Select the security level.

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

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



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



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

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

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



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

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



NOTE

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

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

Security View

Profile
Built-in Profile [Profile details](#)

Colors for check result

High
#77B800

Medium
#009DDB

Basic
#FA943E

Open
#C0C0C0

Save

- Click **Save**.

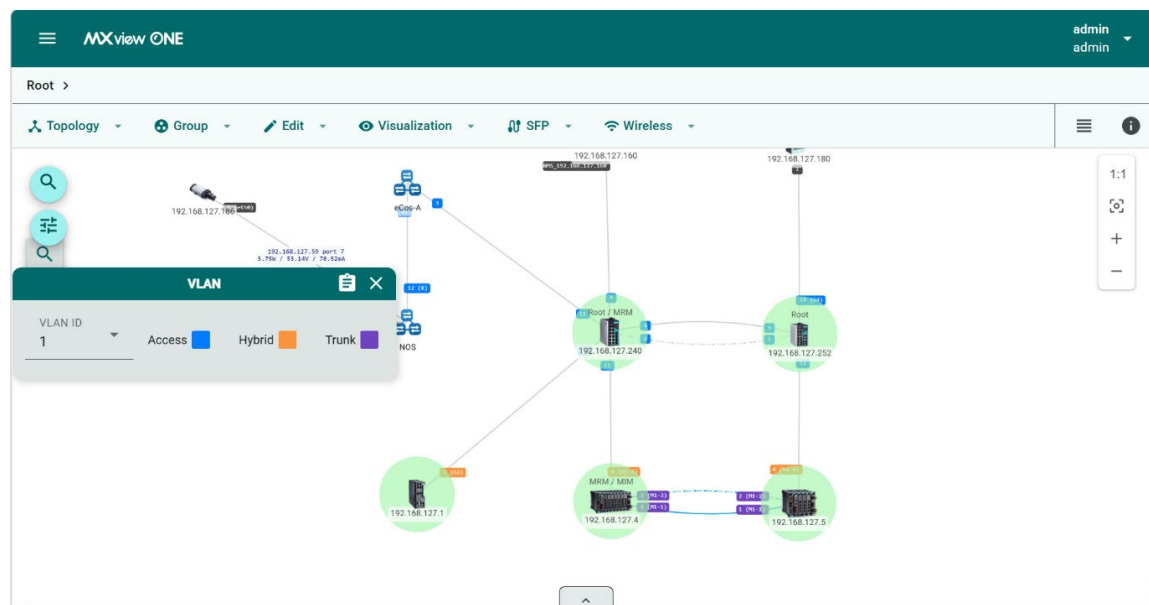
10. To define a custom security profile:
 - a. Navigate to **Menu** (☰) > **Administration** > **Preferences**.
 - b. Under the **Appearance** section, expand **Security View**.
 - c. From the **Profile** drop-down list, select **User defined**.

- 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**.

Monitoring VLAN

VLAN View visualizes the VLAN configuration of every managed device on your network. From this view, you can verify how VLANs are distributed across the topology, inspect the VLAN settings of individual devices, and audit the consistency of the VLAN configuration between connected devices.

To access the **VLAN View** screen, navigate to **Menu** (☰) > **Topology**. In the toolbar, navigate to **Visualization** > **VLAN View**.



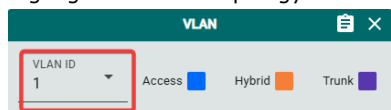
VLAN port types are indicated by color-coded labels:

Port Type	Label Color	Description
Access	Blue	The port carries traffic for a single, untagged VLAN.
Hybrid	Orange	The port carries both tagged and untagged VLAN traffic.
Trunk	Purple	The port carries tagged traffic for multiple VLANs.

Viewing the VLAN Distribution

In VLAN View, you can easily check the VLAN type label of each port and select a VLAN ID to highlight which devices belong to that VLAN.

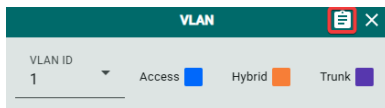
1. Navigate to **Menu** (☰) > **Topology**.
2. In the toolbar, navigate to **Visualization** > **VLAN View**.
3. In the **VLAN** window, select the VLAN ID. All devices belonging to the selected VLAN ID will be highlighted on the topology.



Viewing the VLAN Report

The VLAN Report provides a consolidated overview of the VLAN configuration of all the devices on your network and the connectivity between them. The report audits the VLAN settings on both ends of each link and flags any mismatches to identify misconfigurations and broken VLAN paths.

To access the VLAN report, click the **Report** (📄) icon in the VLAN legend window when in VLAN View.



The report will open in a separate window.

VLAN Report

Warning

VLAN 1 is divided into isolated groups.
Select the corresponding VLAN ID in VLAN view to show more information.

☒ Show Audit Results

Audit Results

All audit results

Export

Search

IP ↑	Port ⓘ	Mode	PVID	Allowlist	Peer Device IP/Port ⓘ	Audit Results
192.168.127.11	1	access	1	1	192.168.127.15/2	Normal
192.168.127.11	2	access	1	1	192.168.127.15/1	Normal
192.168.127.11	3	access	1	1		Normal
192.168.127.11	4	access	1	1		Normal
192.168.127.11	5	access	1	1		Normal

Close

This page displays the following information in a table format:

Item	Description
IP	The IP address of the device.
Port	The local port of the device. If available, hover over the Information (ⓘ) icon to view the port description.
Mode	The VLAN mode of the local port.
PVID	The VLAN ID assigned to the local port.
Allowlist	The VLANs that are allowed on the local port.
Peer Device IP/Port	The IP address and port of the peer device connected to the local port. If available, hover over the Information (ⓘ) icon to view the port description.
Audit Results	The result of the VLAN consistency check between the two ends of the link. This column only shows when Show Audit Results is enabled and will only show the selected results. Refer to Audit Results for more details.

To export the VLAN report, click the Export (ⓘ) icon at the top of the table.

Audit Results

MXview One compares the VLAN settings on both ends of the VLAN connection and includes the result in the VLAN report. The following audit results may show:

Audit Result	Description
Normal	No inconsistencies in VLAN configuration were detected.
Port Mode Mismatch	The port VLAN mode on the local and peer port do not match. The mode of each port is listed in the result.
PVID Mismatch	If both ends are set to Hybrid or Trunk mode, the assigned PVIDs do not match. The PVID of each port is listed in the result.
Allowed List Mismatch	If both ends are set to Hybrid or Trunk mode, but allowed VLANs do not match. The missing VLANs are listed in the result.

Configuring Severity Thresholds for Traffic and Fiber Status Monitoring Events

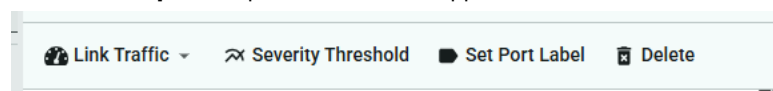
MXview One allows you to configure the following traffic conditions on a link to trigger events:

- 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.

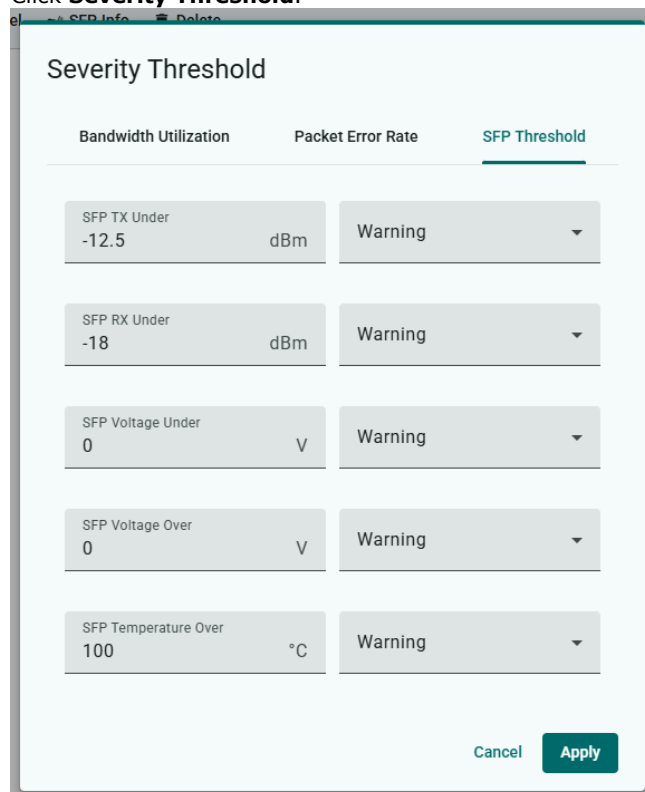
Since a link is bidirectional, the event will be triggered when the traffic condition in either direction satisfies the configured severity threshold.

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

A screenshot of the 'Severity Threshold' configuration dialog box. The dialog has three tabs: 'Bandwidth Utilization', 'Packet Error Rate', and 'SFP Threshold', with 'SFP Threshold' currently selected. It contains five rows of configuration fields. Each row has a text field for a value, a unit field, and a severity level dropdown menu. The rows are: 1. 'SFP TX Under' with value '-12.5' and unit 'dBm', severity 'Warning'. 2. 'SFP RX Under' with value '-18' and unit 'dBm', severity 'Warning'. 3. 'SFP Voltage Under' with value '0' and unit 'V', severity 'Warning'. 4. 'SFP Voltage Over' with value '0' and unit 'V', severity 'Warning'. 5. 'SFP Temperature Over' with value '100' and unit '°C', severity 'Warning'. At the bottom right are 'Cancel' and 'Apply' buttons.

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**.

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**.



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.

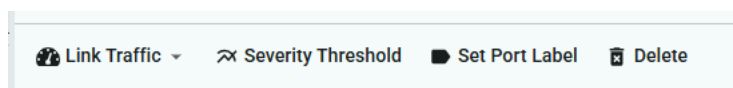
Configuring Custom Port Labels

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

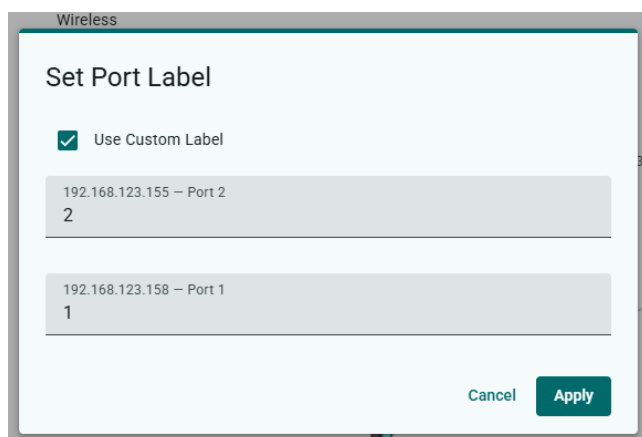
<Device IP Address> / <Port Number>

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

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

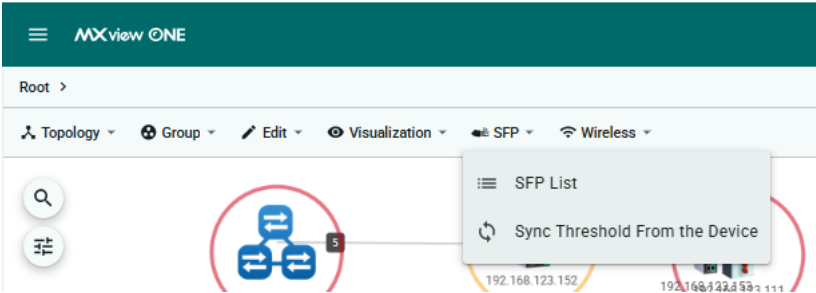


4. Select the **Use Custom Label** check box.
5. In the **From** field, provide a new label for the source port.
6. In the **To** field, provide a new label for the destination port.
7. Click **Apply**.

9. SFP Fiber Status

Viewing the SFP Fiber Status in Table View

MXview One collects and displays the fiber status in **SFP > SFP List**



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

SFP List

Scope *
All Groups

Refresh

Search

	TX (dBm)	RX (dBm)	Temp. (°C)	Volt. (V)		TX (dBm)	RX (dBm)	Temp. (°C)	V (V)
192.168.123.162 Port 11 / SFP- 1GSXLC	-6.0	-6.3	44.4	3.4	192.168.123.163 Port 10 / SFP- 1GSXLC	-6.1	-6.5	43.9	3

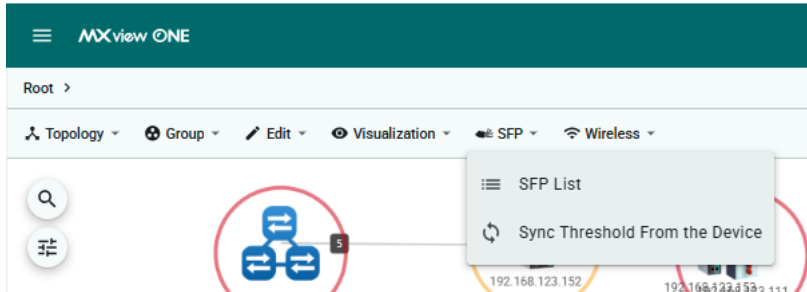
Items per page: 20 1 - 1 of 1 |< < > >|

Close

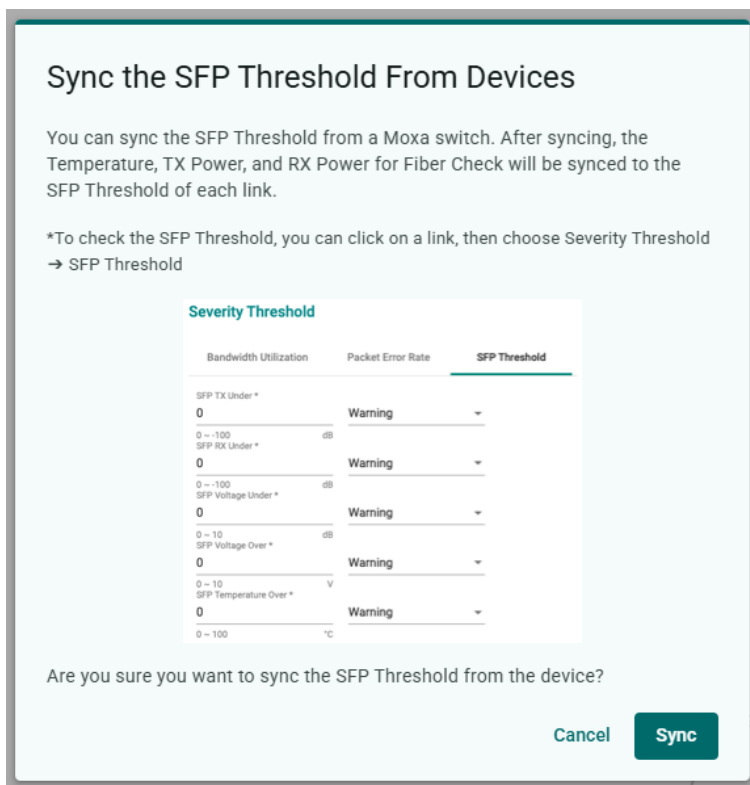
Synchronize the SFP Threshold From the Device

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.

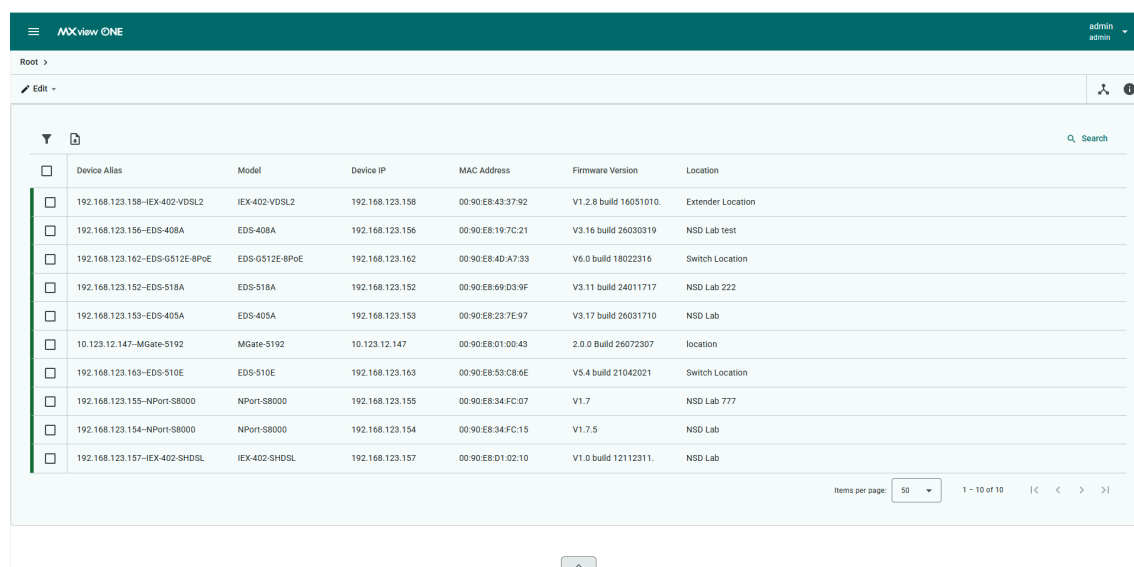


10. Device Operation in the Topology

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.



The screenshot shows the MXview ONE interface with the 'Topology' screen selected. The 'List view' icon is active. The table displays the following data:

☐	Device Alias	Model	Device IP	MAC Address	Firmware Version	Location
☐	192.168.123.158-IEK-402-VDSL2	IEK-402-VDSL2	192.168.123.158	00:90:E8:43:37:92	V1.2.8 build 16051010.	Extender Location
☐	192.168.123.156-EDS-408A	EDS-408A	192.168.123.156	00:90:E8:19:7C:21	V3.16 build 26030319	NSD Lab test
☐	192.168.123.162-EDS-G512E-8PoE	EDS-G512E-8PoE	192.168.123.162	00:90:E8:4D:A7:33	V6.0 build 18022316	Switch Location
☐	192.168.123.152-EDS-S18A	EDS-S18A	192.168.123.152	00:90:E8:69:D3:9F	V3.11 build 24011717	NSD Lab 222
☐	192.168.123.153-EDS-405A	EDS-405A	192.168.123.153	00:90:E8:23:7E:97	V3.17 build 26031710	NSD Lab
☐	10.123.12.147-MGate-S192	MGate-S192	10.123.12.147	00:90:E8:01:00:43	2.0.0 Build 26072307	location
☐	192.168.123.163-EDS-S10E	EDS-S10E	192.168.123.163	00:90:E8:53:C8:6E	V5.4 build 21042021	Switch Location
☐	192.168.123.155-NPort-S8000	NPort-S8000	192.168.123.155	00:90:E8:34:FC:07	V1.7	NSD Lab 777
☐	192.168.123.154-NPort-S8000	NPort-S8000	192.168.123.154	00:90:E8:34:FC:15	V1.7.5	NSD Lab
☐	192.168.123.157-IEK-402-SHDSL	IEK-402-SHDSL	192.168.123.157	00:90:E8:D1:02:10	V1.0 build 12112311.	NSD Lab

At the bottom right of the table, there is a pagination control showing 'Items per page: 50' and '1 - 10 of 10'.

1. Navigate to **Menu** (☰) > **Topology**.
2. Click the **List view** (📄) icon in the top right corner.
3. To add a device to your network topology:

- a. Click **Edit > Add Device**.

Add Device

IP Address

Assign Model

Assign to Group ▼

SNMP Settings

SNMP Version ▼
V1

Port
161

Username

Password

Read Community
public

Write Community
private

Data Encryption ▼
NoAuth

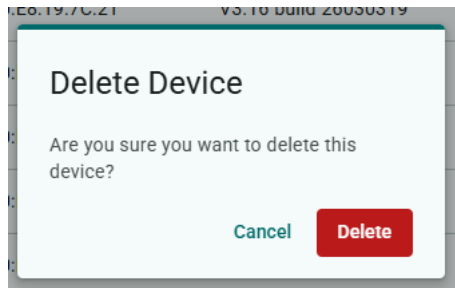
Authentication ▼
MD5

Encryption Protocol ▼
DES

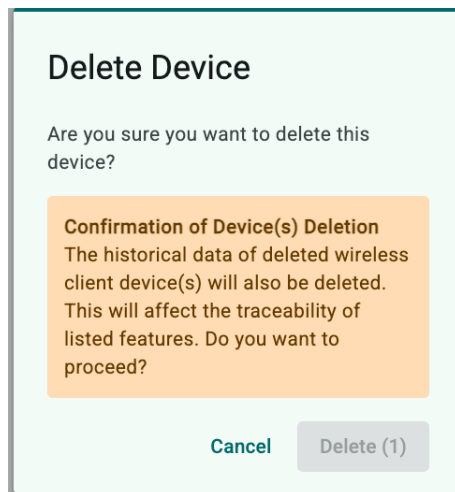
Encryption Password

Cancel Add

- b. Configure the following:
 - ☐ **IP Address:** Specify the IP address of the device
 - ☐ **Assign Model:** Select the model of the device
 - ☐ **Assign To Group:** Select the group to assign the device to
 - ☐ **SNMP Version:** Select the SNMP version
 - ☐ **Username:** Specify the device login Username
 - ☐ **Password:** Create a password
 - ☐ **Read Community:** Specify the SNMP read community string
 - ☐ **Write Community:** Specify the SNMP write community string
 - ☐ **Data Encryption:** Select the data encryption method
 - ☐ **Authentication:** Select the authentication method
 - ☐ **Encryption Key:** Specify the encryption key
- c. Click **Add**.
MXview One adds the device to the topology.
4. To delete devices in your network topology:
 - a. Check the box on the first column of devices.
 - b. Click the **Delete** () icon on the menu bar. The **Delete Device** screen appears.
 - c. For non AWK devices, read the message and then click **Delete** if you are sure you want to delete the device.



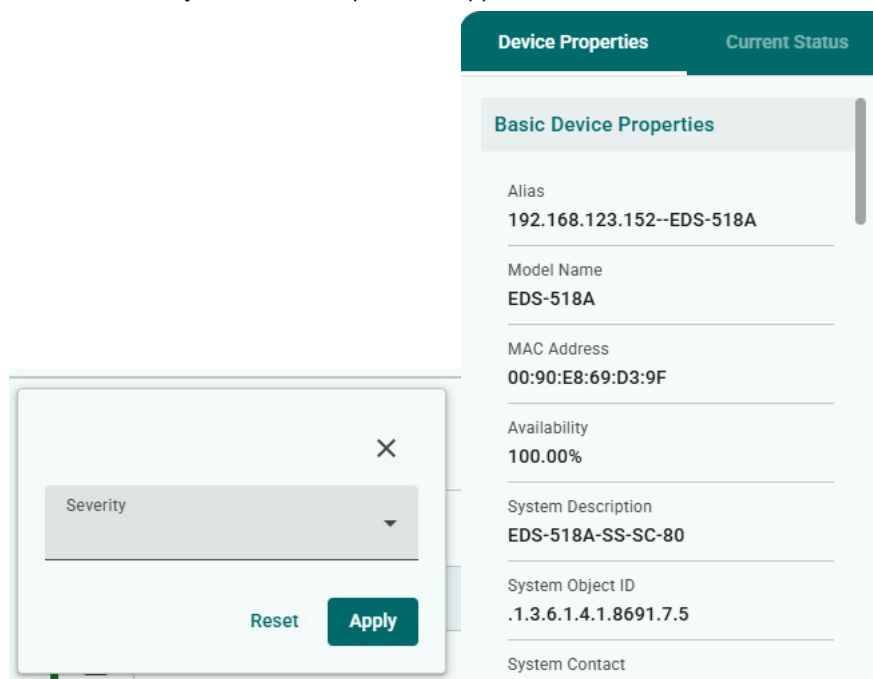
- d. For AWK devices, read the message and wait for the countdown. Click **Delete** if you are sure you want to delete the device.



NOTE

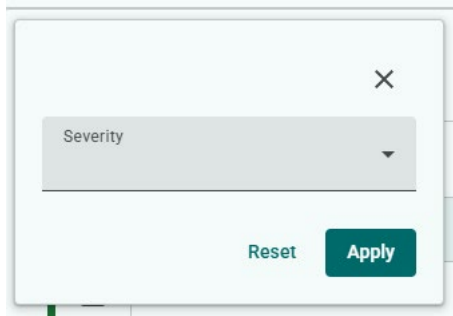
If you click the check box for all the devices, when you click the Delete icon, you will delete all the devices in the topology.

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



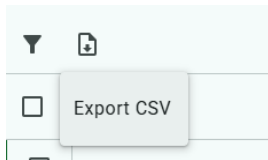
6. To filter the device list by severity level:

- a. Click the **Filter** () icon in the top left corner.



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

MXview One filters the device list to only display devices with the selected severity level.
7. To export the device list:
- a. Click the **Export** () icon.



- b. Select **Export CSV**.

MXview One will export the displayed data as a CSV file.

Importing Device Configurations

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

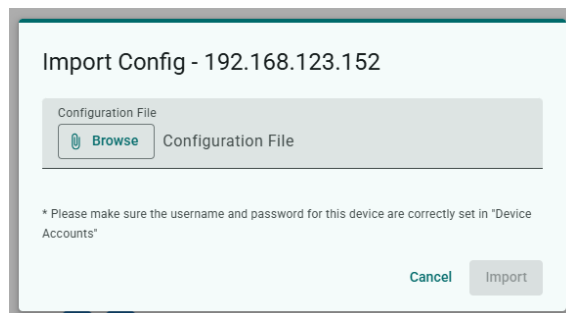
1. Navigate to **Menu** () > **Topology**.
2. Select one of the following views:
 - **Topology view:** Displays a graphical representation of devices in your network topology.
 - **List view:** Displays a list of the devices in your network topology.
3. Select the device that you want to import configurations 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.



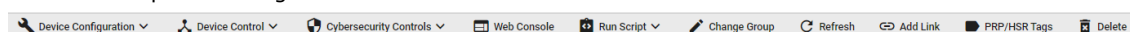
5. Click the folder (■) icon to upload the configuration file from your local machine.
6. Click **Import**.

Exporting Device Configurations

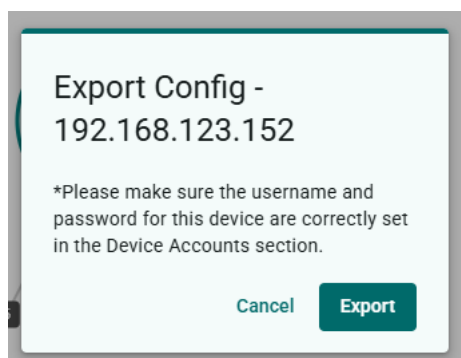
Use the **Topology** screen to export an INI-formatted configuration file from a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

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



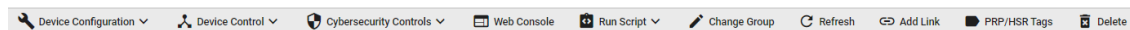
5. Click **Export**.
MXview One exports the device configurations as an INI file in the specified location.

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**.

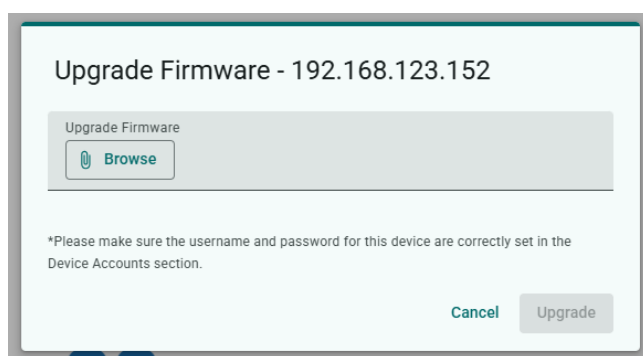
1. Navigate to **Menu** (☰) > **Topology**.
2. Select one of the following views:
 - **Topology view:** Displays a graphical representation of the devices in your network topology.
 - b. **List view:** Displays a list of the devices in your network topology.
3. Select the device that you want to upgrade 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.



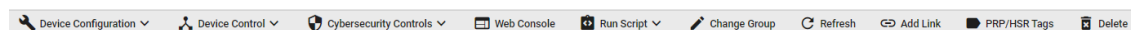
5. Click the folder (📁) icon to upload the ROM-formatted firmware file from your local machine.
6. Click **Upgrade**.

Configuring SNMP Trap Server

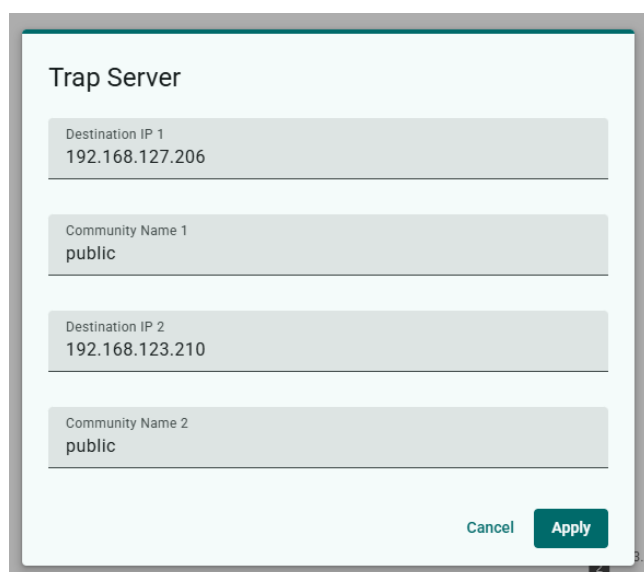
MXview One can collaborate with other network management software and send SNMP Traps to non-Moxa NMS. MXview One supports up to two trap servers depending on the device.

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



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

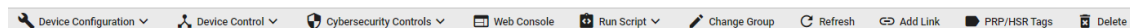
When a device fails to reply within seven seconds, MXview One will display the message "Failed to update device Trap server settings." Please confirm the execution results via the same settings page or go to the web page of the devices.

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**.
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**.

A dialog box titled 'Ethernet/Fiber Port Settings'. It contains several input fields: 'Port' with a dropdown menu showing '1'; 'Enable' with a dropdown menu showing 'Enabled'; 'Media Type' with a text field showing '100TX,RJ45'; 'Port Description - optional' with a text field; and 'Apply settings to another port' with a dropdown menu. At the bottom, there is a note: '*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.' Below the note are two buttons: 'Cancel' and 'Apply'.

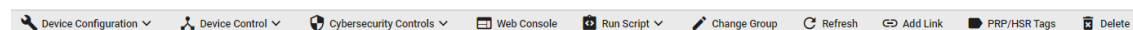
5. Configure the following port settings for the device:
 - **Port:** Select the port number.
 - **Enable:** Enable or disable the port.
 - **Port Description:** Provide a description of the port.
 - **Apply settings to another port:** Select to apply the configured settings to other ports on the device.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

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**.
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**.

A configuration window titled "SNMP Communication Protocol". It contains several input fields and dropdown menus arranged in a grid. The fields are: SNMP Version (V1), Port (161), Username (admin), Password (with a toggle icon), Read Community (public), Write Community (private), Data Encryption (NoAuth), Authentication (MD5), Encryption Protocol (DES), and Encryption Password (with a toggle icon). At the bottom right, there are "Cancel" and "Apply" buttons.

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

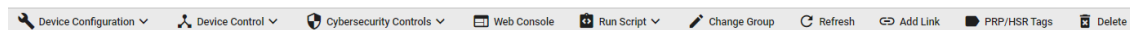
For the first time, users can use the Default Device Template function to set the function template. For more information, see **Changing Default SNMP Configuration**.

Configuring MXview One Polling Interval

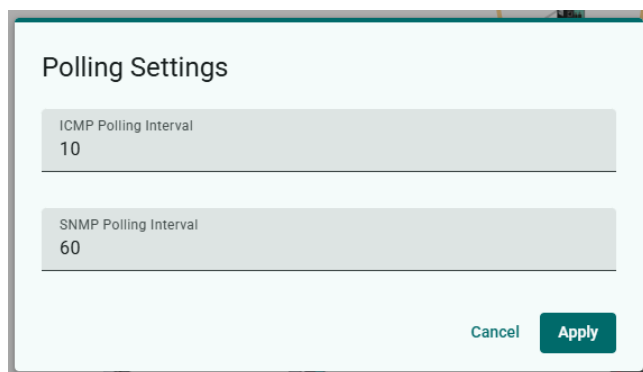
Use the **Topology** screen to configure ICMP or SNMP polling settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

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



5. Configure the following polling settings for the device:
 - **ICMP polling interval**
 - **SNMP polling interval**
6. Click **Apply**.



NOTE

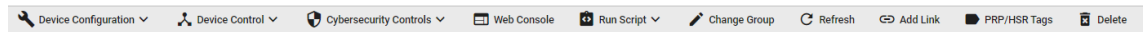
For the first time, users can use the Default Device Template function to set the function template. For more information, see **Default Device Template**.

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**.
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**.

A dialog box titled "Device Accounts" with a light blue header. It contains two input fields: "Username" with the text "admin" and "Password" with masked characters "....". A toggle icon for password visibility is on the right of the password field. At the bottom right are "Cancel" and "Apply" buttons.

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

Modifying the Device Alias

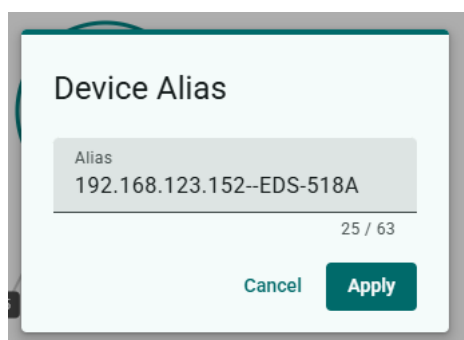
Use the **Topology** screen to configure advanced settings for a device in your network topology by selecting the device from the **Topology Map** or **Device List**.

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



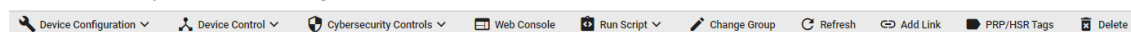
5. Edit the **Alias** field.
6. Click **Apply**.

Changing the Device Icon

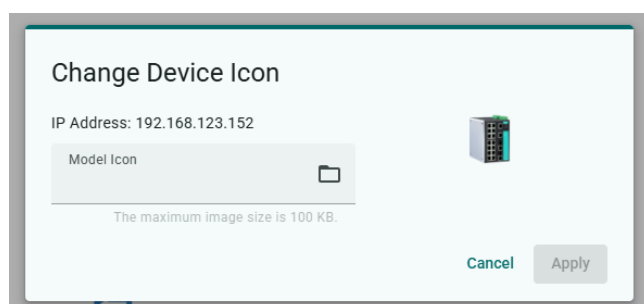
Use the **Topology** screen to change the device icon by selecting the device from the **Topology Map** or **Device List**, and then upload a JPG, GIF, or PNG image file. You can change the icon for multiple devices at once.

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



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

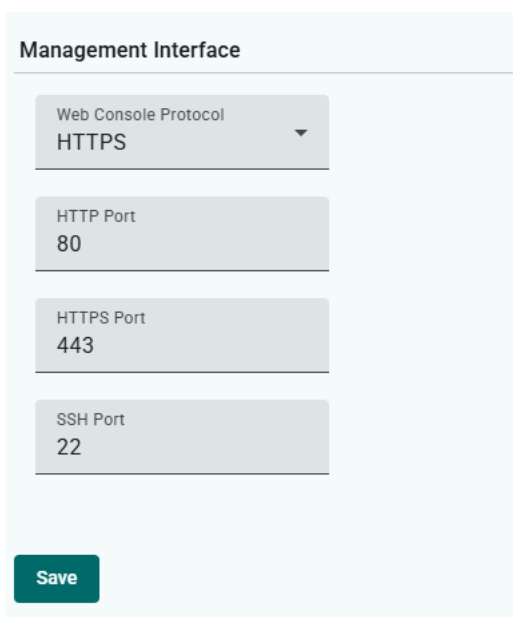
MXview One allows you to use the **Topology** screen to the web console for a device from the **Topology Map** or **Device List**.



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**.
 - b. Find the **Management Interface** to complete the settings.



Management Interface

Web Console Protocol
HTTPS

HTTP Port
80

HTTPS Port
443

SSH Port
22

Save

- c. Configure the following:
 - ☐ **Web Console Protocol**
 - ☐ **HTTP Port**
 - ☐ **HTTPS Port**
 - ☐ **SSH Port**
 - d. Click **Save**.



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**.
 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.

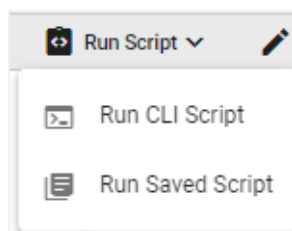
6. Enter the **Username** and **Password** for the device web console.
7. Click **Login**.

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.

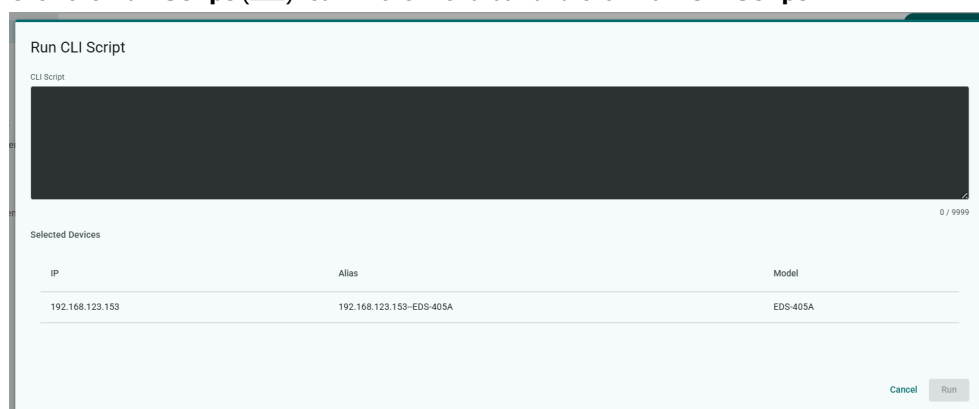
Click the **Run Script** () icon in the menu bar to expand the script functions. There are two main functions:

- **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.



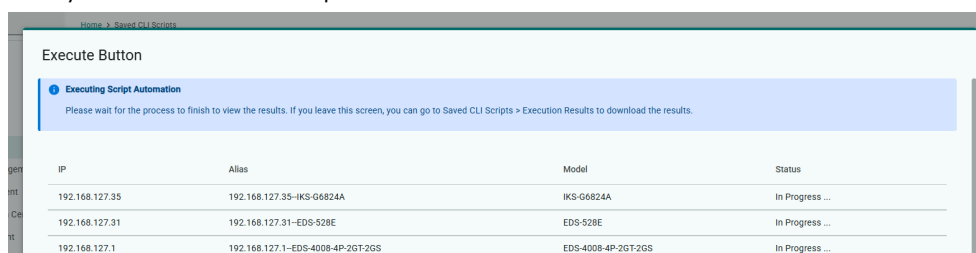
Running a CLI Script

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**.



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.



IP	Alias	Model	Status
192.168.127.35	192.168.127.35-IKS-G6824A	IKS-G6824A	In Progress ...
192.168.127.31	192.168.127.31-EDS-528E	EDS-528E	In Progress ...
192.168.127.1	192.168.127.1-EDS-4008-4P-2GT-2GS	EDS-4008-4P-2GT-2GS	In Progress ...

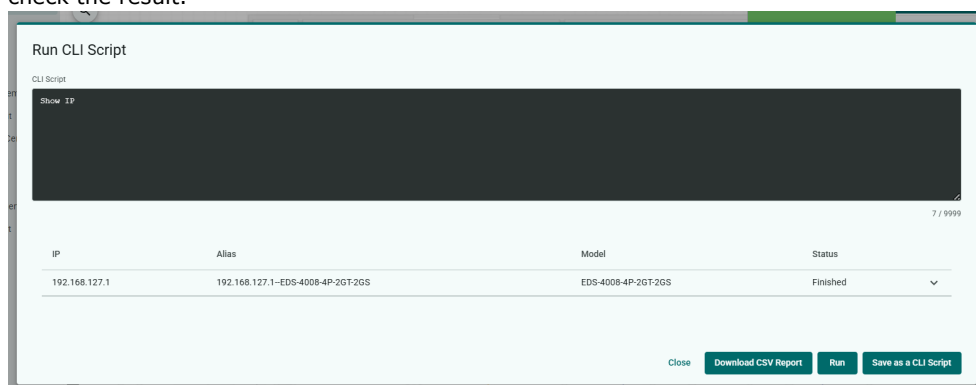


NOTE

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.

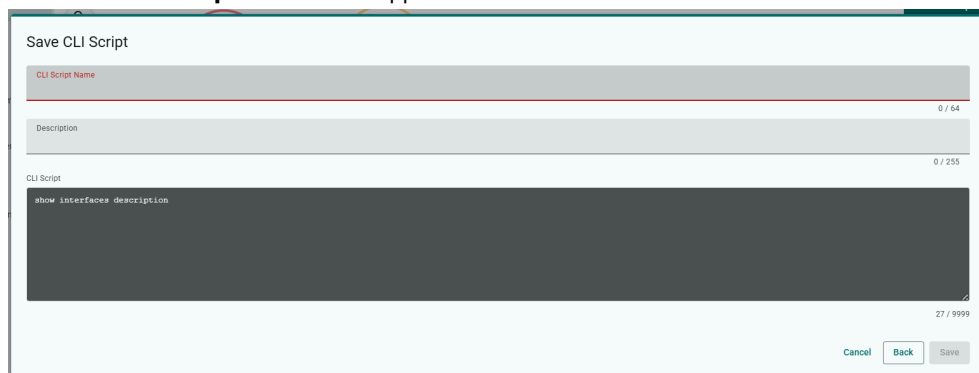
5. Check the script results.

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



IP	Alias	Model	Status
192.168.127.1	192.168.127.1-EDS-4008-4P-2GT-2GS	EDS-4008-4P-2GT-2GS	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.



The 'Save CLI Script' dialog box contains the following fields:

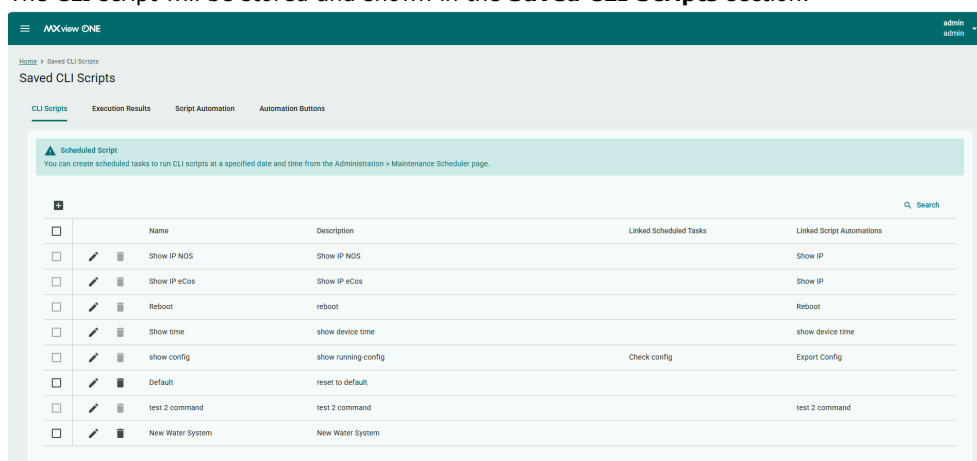
- CLI Script Name:** A text input field with a character count of 0 / 64.
- Description:** A text input field with a character count of 0 / 255.
- CLI Script:** A large text area containing the command 'show interfaces description' and a character count of 27 / 9999.

At the bottom right, there are three buttons: 'Cancel', 'Back', and 'Save'.

- 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.

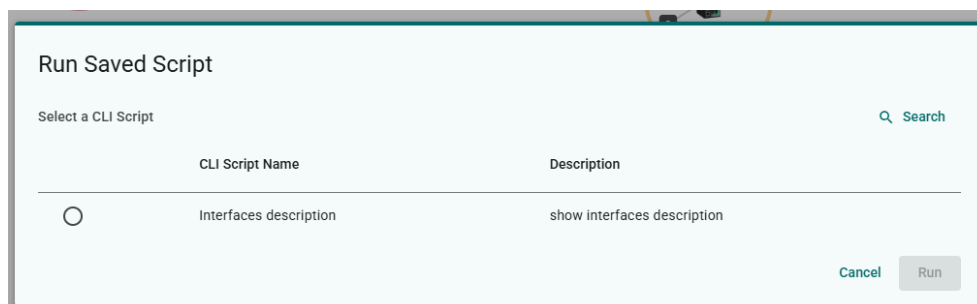


The 'Saved CLI Scripts' page shows a table of saved scripts. Above the table is a 'Scheduled Script' section with a note: 'You can create scheduled tasks to run CLI scripts at a specified date and time from the Administration > Maintenance Scheduler page.'

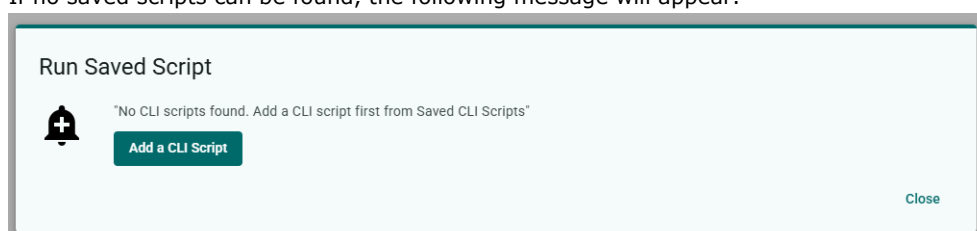
	Name	Description	Linked Scheduled Tasks	Linked Script Automations
☐	Show IP NOS	Show IP NOS		Show IP
☐	Show IP eCos	Show IP eCos		Show IP
☐	Reboot	reboot		Reboot
☐	Show time	show device time		show device time
☐	show config	show running-config	Check config	Export Config
☐	Default	reset to default		
☐	test 2 command	test 2 command		test 2 command
☐	New Water System	New Water System		

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.

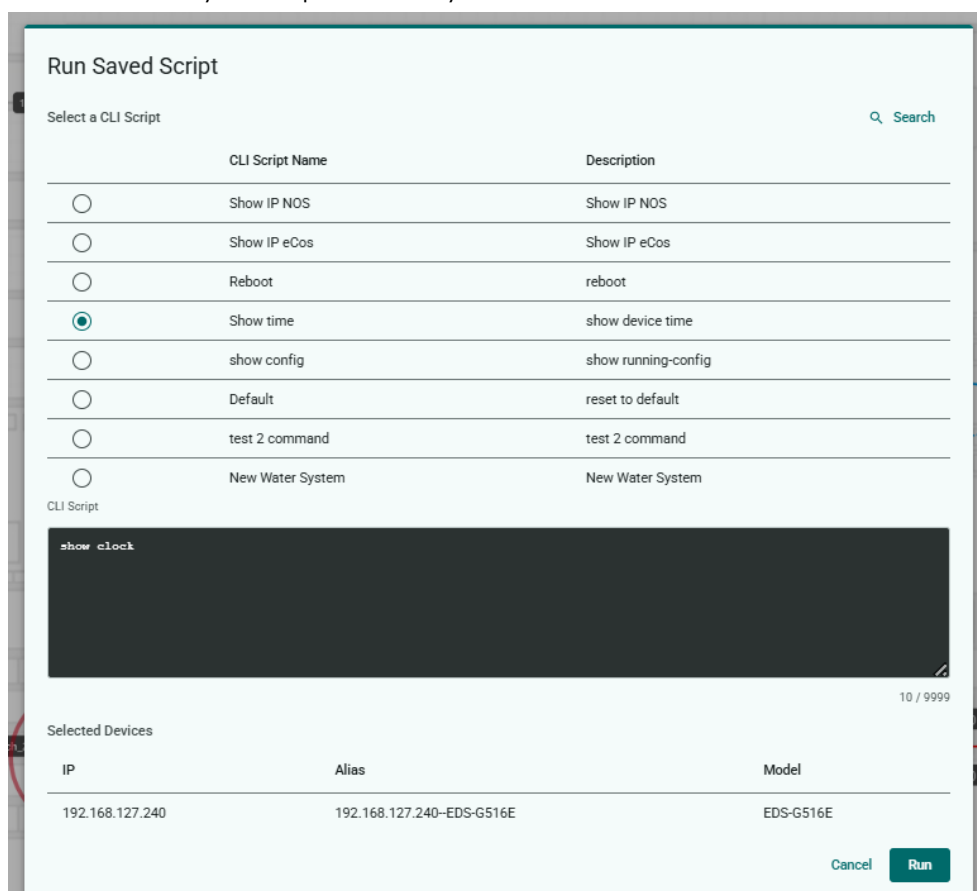


If no saved scripts can be found, the following message will appear.



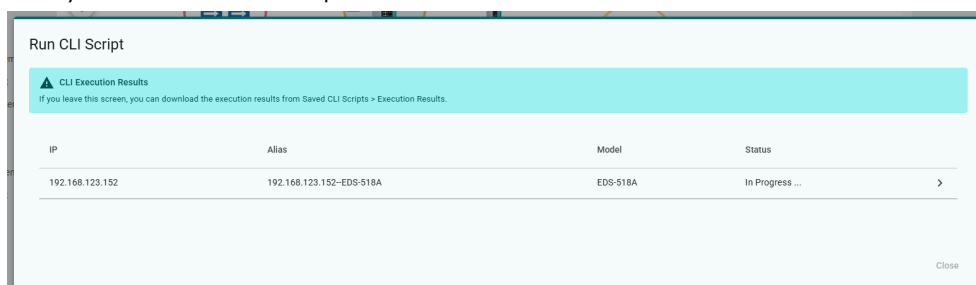
Click the **Add a CLI Script** to create a script. Refer to **Adding a CLI Script**.

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.



4. Click **Run**.

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



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.

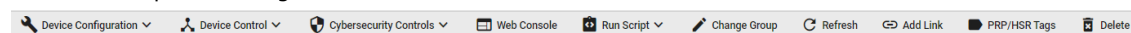


Changing Device Groups

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**.
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**.

Change Group

Current Group
Root

	IP Address
☐	10.123.12.147
☐	192.168.123.152
☒	192.168.123.153
☐	192.168.123.154
☐	192.168.123.155

1 Selected / 10 Total

Assign to Group
Group1

Cancel Apply

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**.

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**.
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**.

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**.
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**.

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

MXview ONE

adminadmin

Search

Dashboard

Topology

Device Discovery

Device Management

Configuration and Control

Account and Password

Saved CLI Scripts

Firmware Management

Device Configuration Center

Baseline Management

Event Management

Notification Management

Inventory Management

Integration

Administration

Help

Home

Device Management

Configuration and Control

Configuration and Control

Select Device

Device ConfigurationDevice ControlCybersecurity ControlsRun Script

☐	192.168.123.70-AWK-4252A	AWK-4252A	192.168.123.70	00:90:E8:9D:C4:FE	v2.0 Build 2023_0217_1145	
☐	192.168.123.72-AWK-1151C	AWK-1151C	192.168.123.72	00:90:E8:05:17:45	v2.0 Build 2022_1007_1814	
☐	192.168.123.152-EDS-518A	EDS-518A	192.168.123.152	00:90:E8:69:D3:9F	V3.11 build 24011717	NSD Lab 222
☐	192.168.123.153-EDS-405A	EDS-405A	192.168.123.153	00:90:E8:23:7E:97	V3.17 build 26031710	NSD Lab
☐	192.168.123.154-NPort-S8000	NPort-S8000	192.168.123.154	00:90:E8:34:FC:15	V1.7.5	NSD Lab
☐	192.168.123.155-NPort-S8000	NPort-S8000	192.168.123.155	00:90:E8:34:FC:07	V1.7	NSD Lab 777
☐	192.168.123.156-EDS-408A	EDS-408A	192.168.123.156	00:90:E8:19:7C:21	V3.16 build 26030319	NSD Lab test
☐	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
☐	192.168.123.158-IEX-402-VDSL2	IEX-402-VDSL2	192.168.123.158	00:90:E8:43:37:92	V1.2.8 build 16051010	Extender Location
☐	192.168.123.162-EDS-G512E-8PoE	EDS-G512E-8PoE	192.168.123.162	00:90:E8:4D:A7:33	V6.0 build 18022316	Switch Location
☐	192.168.123.163-EDS-510E	EDS-510E	192.168.123.163	00:90:E8:53:C8:6E	V5.4 build 21042021	Switch Location
☐	192.168.123.165-AWK-1131A	AWK-1131A	192.168.123.165	00:90:E8:52:39:75	1.21.1 Build 21031116	NSD Lab
☐	192.168.123.168-AWK-1131A	AWK-1131A	192.168.123.168	00:90:E8:52:39:50	1.24 Build 23010916	NSD Lab qq
☐	192.168.123.169-AWK-4131A	AWK-4131A	192.168.123.169	00:90:E8:7C:C3:01	1.16 Build 21020511	

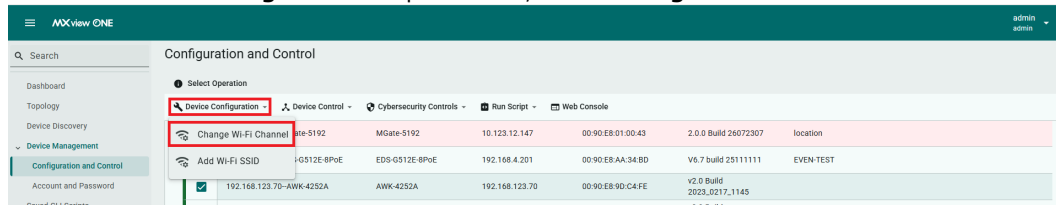
Refer to the following section for an overview of all functions in each category.

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



4. Configure the following Wi-Fi channel settings for the 2.4 and 5 GHz bands.

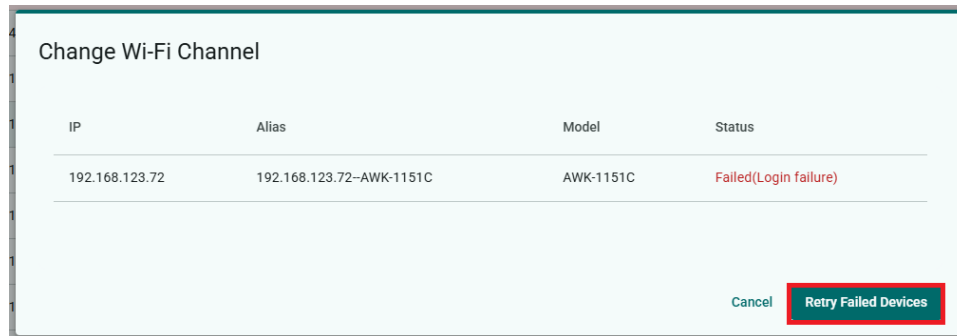
The 'Change Wi-Fi Channel' dialog box is shown. It has two sections for 2.4G and 5G. For 2.4G, the Channel is set to 1 and the Channel Width is 20 MHz. For 5G, the Channel is set to 36 and the Channel Width is 20 MHz. Below these settings is a table with columns for IP, Alias, and Model. The table contains one entry: IP 192.168.123.70, Alias 192.168.123.70-AWK-4252A, and Model AWK-4252A. At the bottom right are 'Cancel' and 'Change' buttons.

- **Channel:** Select the channel for each band.
 - **Channel Width:** Select the channel bandwidth.
5. When finished, click **Change**.
If successful, a confirmation will be shown in the Status column.

The 'Change Wi-Fi Channel' dialog box is shown after successful completion. The table now includes a 'Status' column, and the entry for IP 192.168.123.70 shows a status of 'Finished'. A 'Close' button is at the bottom right.

If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry**

Failed Devices to try again.



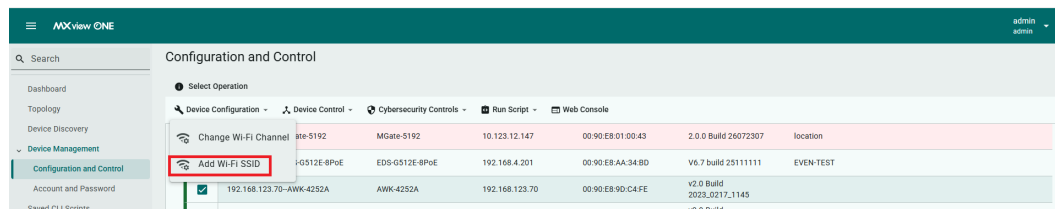
A dialog box titled "Change Wi-Fi Channel" with a table listing devices. The table has columns for IP, Alias, Model, and Status. One device is listed with a status of "Failed(Login failure)". At the bottom right, there are "Cancel" and "Retry Failed Devices" buttons.

IP	Alias	Model	Status
192.168.123.72	192.168.123.72-AWK-1151C	AWK-1151C	Failed(Login failure)

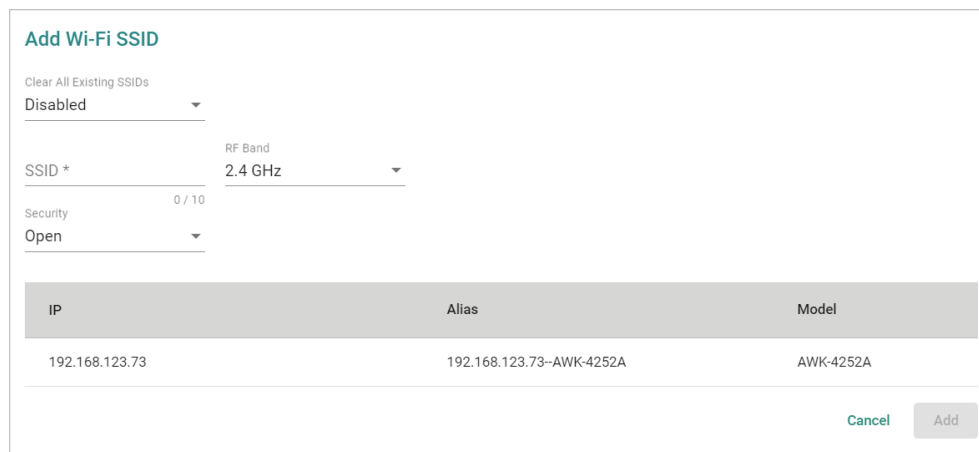
Add Wi-Fi SSID

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



4. Configure the following Wi-Fi SSID settings:



A form titled "Add Wi-Fi SSID" with fields for "Clear All Existing SSIDs" (Disabled), "SSID *" (0 / 10), "RF Band" (2.4 GHz), and "Security" (Open). Below the form is a table with columns for IP, Alias, and Model. The table contains one row with the following data:

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

At the bottom right, there are "Cancel" and "Add" buttons.

- **Clear All Existing SSIDs:** (Optional) If enabled, all existing SSIDs on the selected devices will be removed.
- **SSID:** Enter a name for the SSID.
- **RF Band:** Select the RF band for the SSID.
- **Security:** Select the security mode for the SSID. If you select any mode other than Open, also configure the following settings:
- **WPA Mode:** Select the WPA mode.
- **Protected Management Frame:** Disable or use 802.11w protected management frames.
- **Encryption:** Select the encryption mode. TKIP/AES Mixed mode is mainly to support legacy AP devices.
- **EAPOL:** Select the EAPOL authentication version.
- **Passphrase:** Enter the passphrase.

- When finished, click **Add**. The system will execute the action.
If successful, a confirmation will be shown in the Status column.

IP	Alias	Model	Status
192.168.123.70	192.168.123.70-AWK-4252A	AWK-4252A	Finished

Close

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

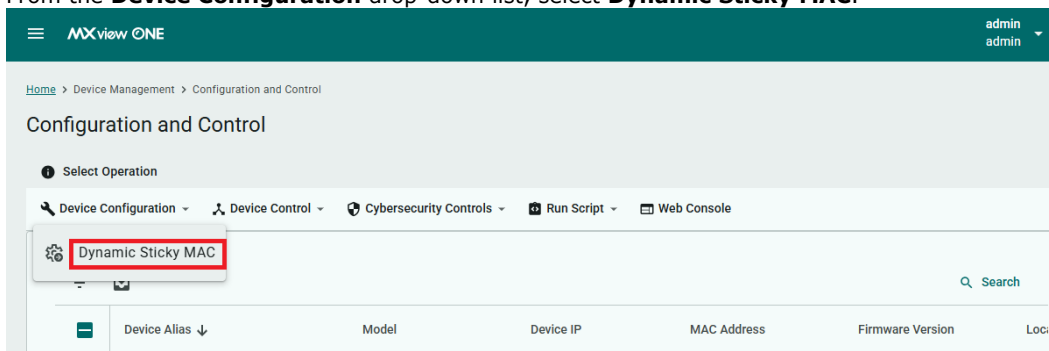
IP	Alias	Model	Status
192.168.123.70	192.168.123.70-AWK-4252A	AWK-4252A	Failed(Login failure)

Cancel **Retry Failed Devices**

Dynamic Sticky MAC

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

- Navigate to **Menu** (☰) > **Device Management** > **Configuration and Control**.
- Select the device(s) to configure from the device list.
- From the **Device Configuration** drop-down list, select **Dynamic Sticky MAC**.

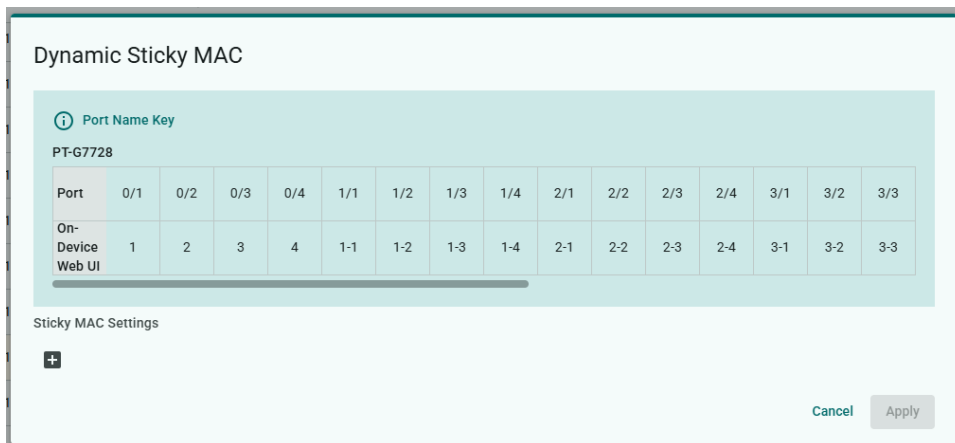


NOTE

Due to port format differences, 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. 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

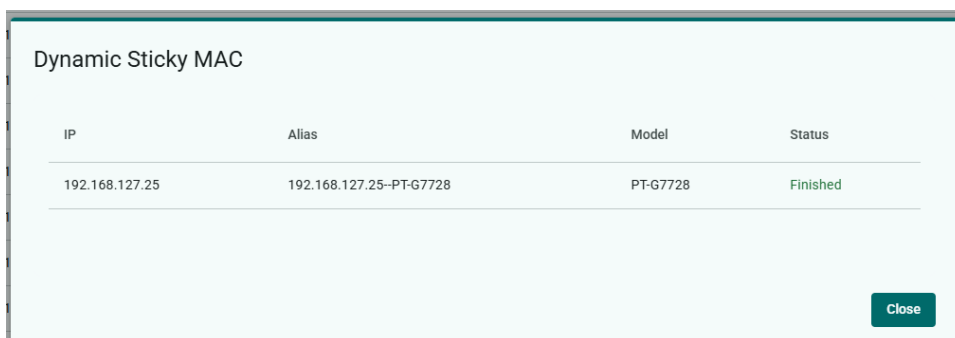
Port	0/1	0/2	0/3	0/4	1/1	1/2	1/3	1/4	2/1	2/2	2/3	2/4	3/1	3/2	3/3
On-Device	1	2	3	4	1-1	1-2	1-3	1-4	2-1	2-2	2-3	2-4	3-1	3-2	3-3
Web UI															

Sticky MAC Settings



Cancel Apply

- **Alias:** Select the devices the configure Sticky MAC for.
 - **Port:** Select the device ports to configure Sticky MAC for. Refer to the Port Name Key section at the top for the web UI port mapping.
 - **Sticky MAC:** Enable or disable Sticky MAC for the selected ports.
 - **Address Limit:** Specify the maximum number of learned MAC addresses.
 - **Security Action:** Select whether the system will drop the packet or shut down the port when a violation occurs.
5. When finished, click **Apply**. The system will execute the action. If successful, a confirmation will be shown in the Status column.

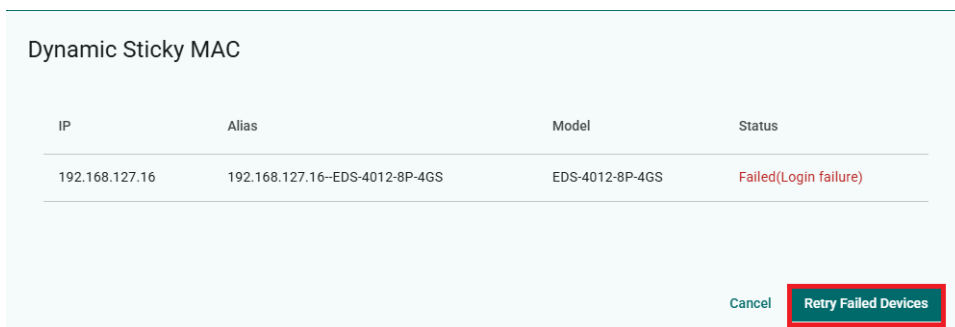


Dynamic Sticky MAC

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

Close

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



Dynamic Sticky MAC

IP	Alias	Model	Status
192.168.127.16	192.168.127.16-EDS-4012-8P-4GS	EDS-4012-8P-4GS	Failed(Login failure)

Cancel **Retry Failed Devices**

Serial Port Monitoring

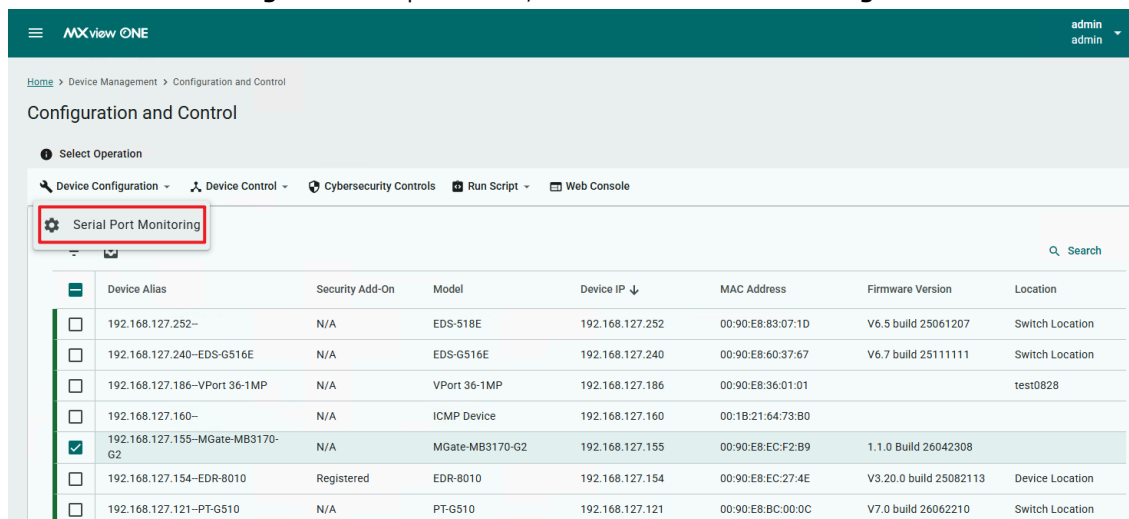


NOTE

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.
3. From the **Device Configuration** drop-down list, select **Serial Port Monitoring**.



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

TX Inactivity

No Data Period

1

Minutes

Severity

Warning

Cancel

Apply

- ☐ **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 **Event Type** is set to **Any Serial Error Count**, 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**.



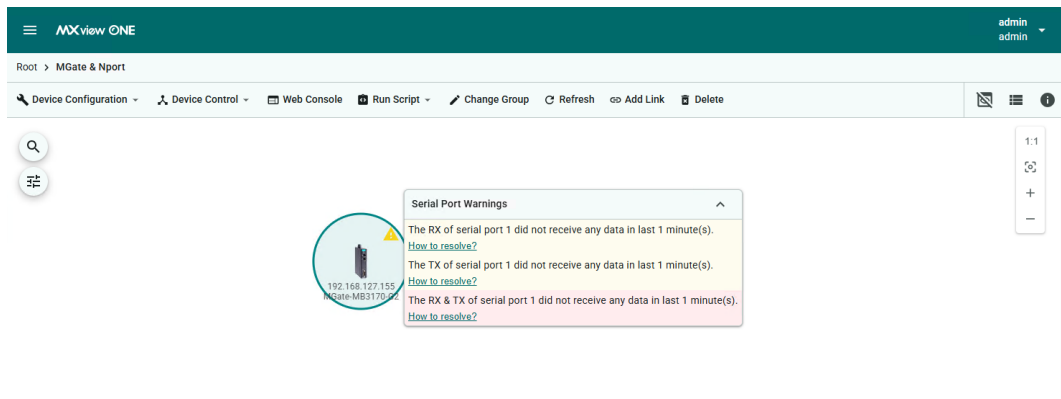
NOTE

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

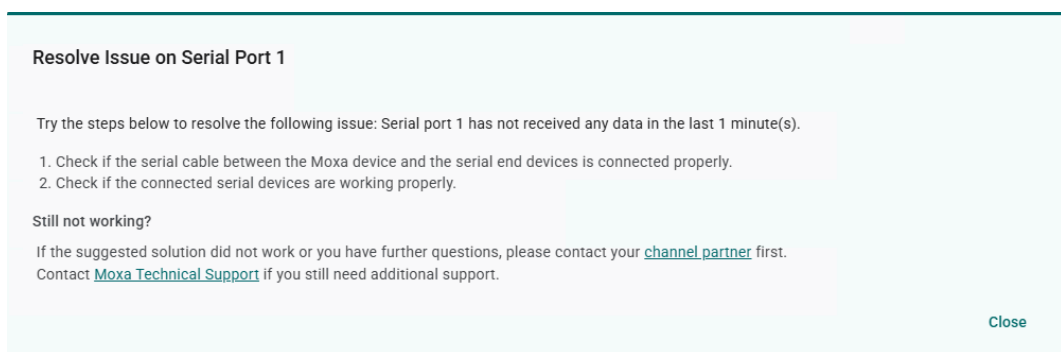
6. To delete an event trigger rule:

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

- 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.



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

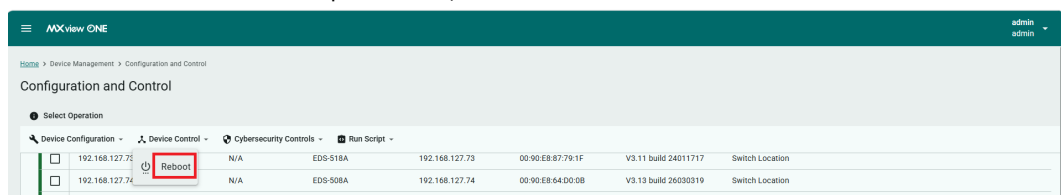


Device Control

Reboot

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

- Navigate to **Menu** (☰) > **Device Management** > **Configuration and Control**.
- Select the device(s) to configure from the device list.
- From the **Device Control** drop-down list, select **Reboot**.



4. Configure the reboot sequence and execution time.

Reboot

Reboot Sequence
Smart Sequential

Order	IP	Alias	Model
1	192.168.127.52	192.168.127.52-RKS-G4028-L3-PoE-4GS-HV-T	RKS-G4028-L3-PoE-4GS-HV-T
2	192.168.127.121	192.168.127.121-PT-G510	PT-G510
3	192.168.127.120	192.168.127.120-PT-G510	PT-G510

Cancel Add to Scheduler Reboot

- 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.
 - Select an execution time:
 - ☐ **Reboot:** Click **Reboot** to restart the devices instantly.
 - ☐ **Add to Scheduler:** Click **Add to Scheduler** to create a new scheduled task. MXview One will reboot the devices based on the specified time and date in the schedule.
- To reboot devices instantly, click **Reboot**. The system will execute the action. 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 try again.

Reboot

IP	Alias	Model	Status
192.168.127.52	192.168.127.52-RKS-G4028-L3-PoE-4GS-HV-T	RKS-G4028-L3-PoE-4GS-HV-T	Finished
192.168.127.121	192.168.127.121-PT-G510	PT-G510	Failed(Login failure)
192.168.127.120	192.168.127.120-PT-G510	PT-G510	Finished

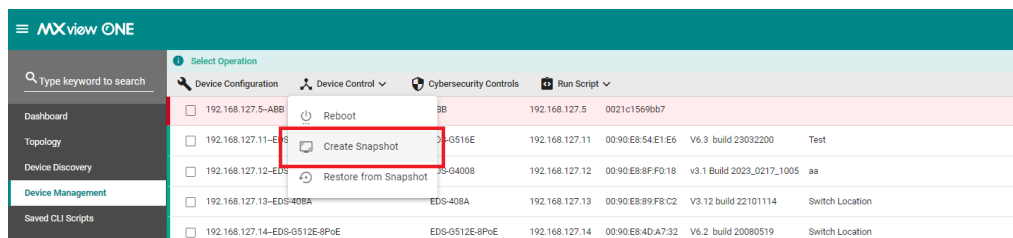
Cancel Retry Failed Devices

Create Snapshot

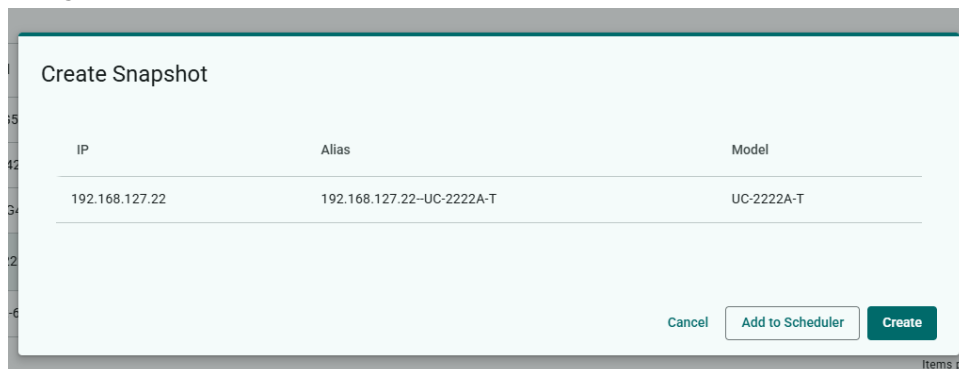
Use the **Snapshot** function to create a snapshot of the current configuration. The snapshot can be used to restore the configuration later.

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

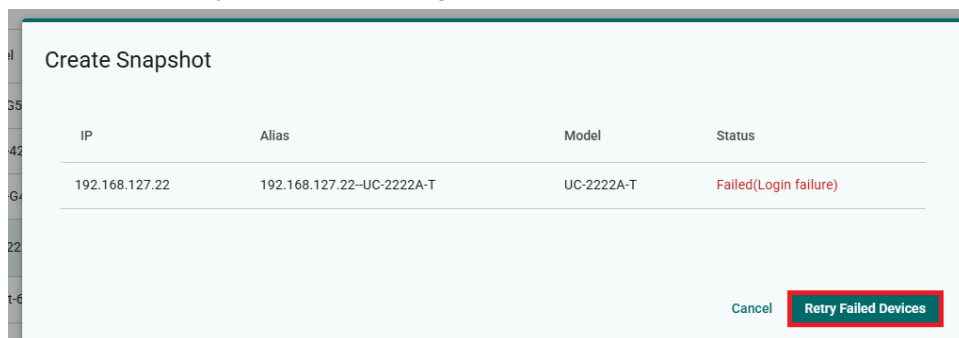
- From the **Device Control** drop-down list, select **Create Snapshot**.



- Configure the execution time.



- **Create:** Click **Create** to create a snapshot instantly.
 - **Add to Scheduler:** Click **Add to Scheduler** to create a new scheduled task. MXview One will create a snapshot based on the specified time and date in the schedule.
- To create a snapshot instantly, click **Create**. The system will execute the action. 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.



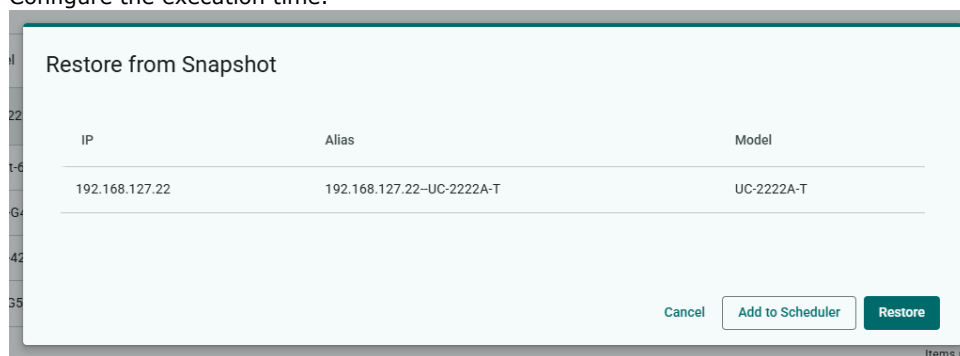
Restore From Snapshot

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

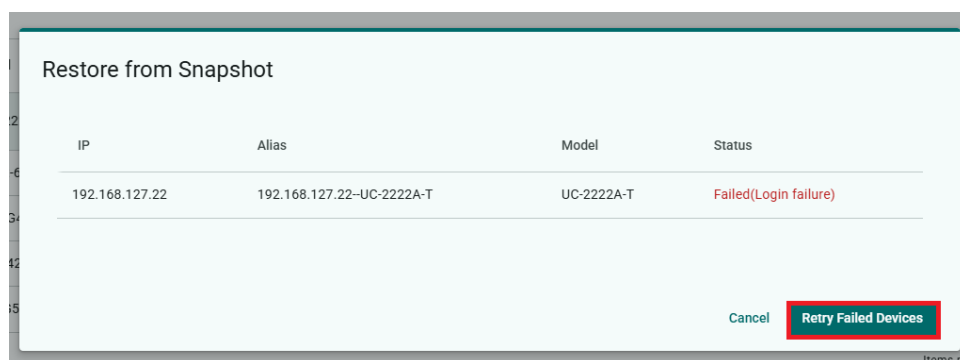
- Navigate to **Menu** (☰) > **Device Management** > **Configuration and Control**.
- Select the device(s) to configure from the device list.
- From the **Device Control** drop-down list, select **Restore from Snapshot**.



4. Configure the execution time.



- **Restore:** Click **Restore** to restore the snapshot instantly.
 - **Add to Scheduler:** Click **Add to Scheduler** 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. If successful, a confirmation will be shown in the Status column.
 6. If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.

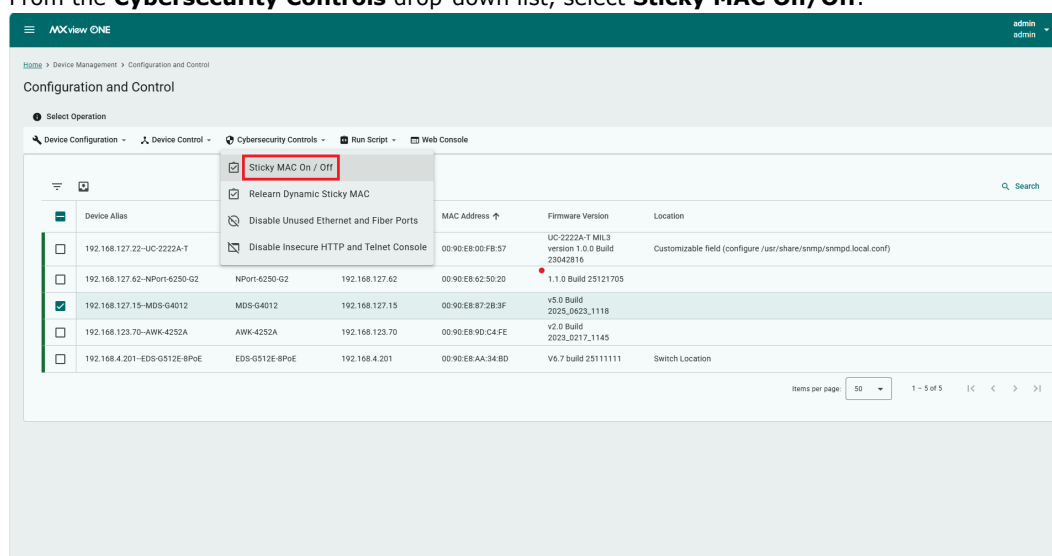


Cybersecurity Controls

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. From the **Cybersecurity Controls** drop-down list, select **Sticky MAC On/Off**.

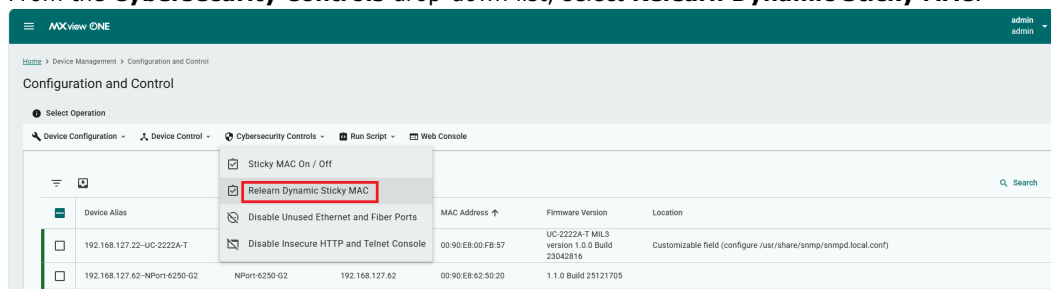


3. Enable or disable Sticky MAC.
4. Click **Apply**. The system will execute the action.
If successful, a confirmation will be shown in the Status column.
5. If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.

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

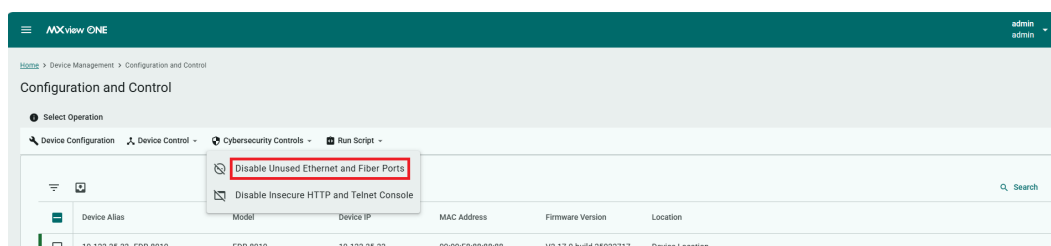


4. Click **Relearn**. The system will execute the action.
5. If successful, a confirmation will be shown in the Status column.
6. If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.

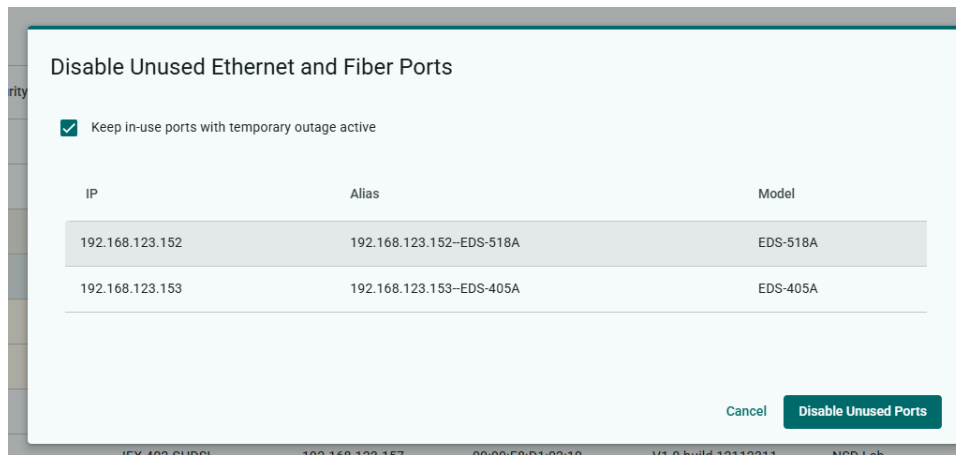
Disable Unused Ethernet and Fiber Ports

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



4. Choose to exempt active ports with temporary inactivity.

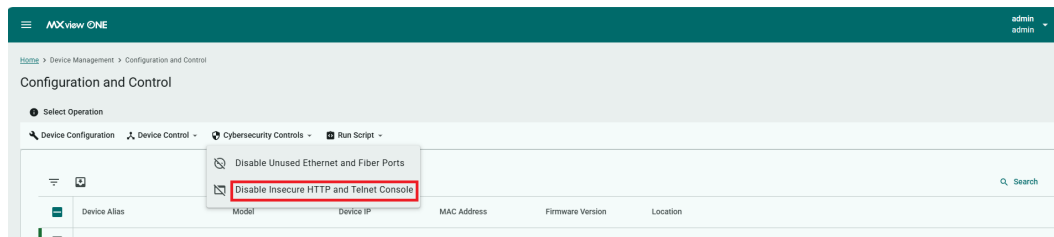


5. Click **Disable Unused Ports**. The system will execute the action. If successful, a confirmation will be shown in the Status column.
6. If unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.

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



4. Click **Disable HTTP and Telnet**. If successful, a confirmation will be shown in the Status column.
5. 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

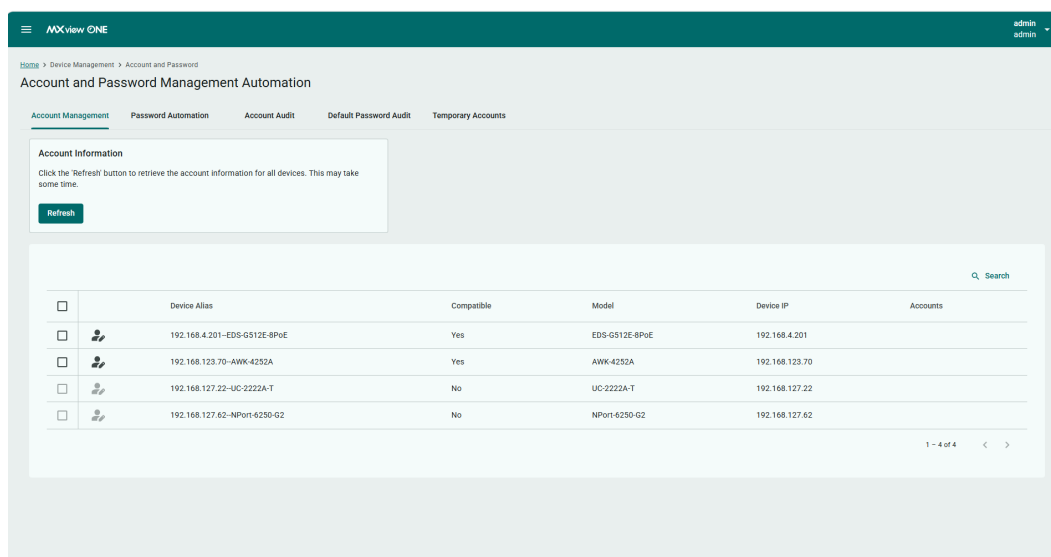
Refer to the **Managing and Running Scripts** section.

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.



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.

Account Management

Operation *

Change Default "Admin" Name

New Username *

Minimum 4 characters 0 / 64

New Password *

Minimum 8 characters 0 / 64

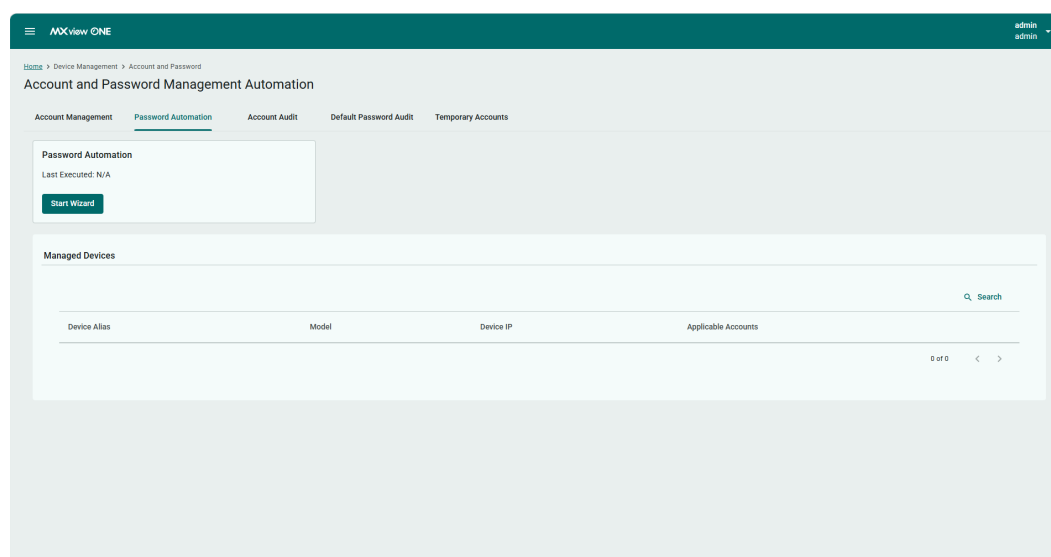
Cancel Change

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 **Password Automation** 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.



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**.

- When prompted, verify your MXview One account.

The screenshot shows the 'Password Automation Wizard' interface. At the top, a progress bar has five steps: 1. Verify Email Recipient (active), 2. Select Devices, 3. Set Password Complexity, 4. Apply Password to Devices, and 5. Send Password Email. Below the progress bar, the title 'Verify Account and Password Email Recipient(s)' is followed by three input fields: '1st Email Recipient', '2nd Email Recipient', and a 'Verify Email' button. A 'Close' button is in the bottom right corner.

- Enter the 1st and 2nd recipient email addresses and click **Verify Email**. MXview One will send a verification code to these addresses.
- Enter the verification code from the email in the Wizard and click **Confirm**. If you have not received an email, check your Spam folder or confirm the Email Server Configuration settings in MXview One.
- Select the device(s) to generate a randomized password for and click **Next**.
- Specify the randomized password length and click **Next**. MXview One will generate a random password of the specified length that complies with the complexity requirements.

The screenshot shows the 'Password Automation Wizard' interface at Step 3: Set Password Complexity. The progress bar shows steps 1 and 2 completed, step 3 active, and steps 4 and 5 pending. Below the progress bar, the text 'MXview One will generate the random password for the selected devices.' is followed by an orange warning box: 'Make the password length is within the maximum allowed password length on the device(s)'. Below this is a 'Random Password Length' input field with the value '8'. At the bottom, three complexity requirements are listed as 'Enabled': 'At least one digit (0-9)', 'Mixed upper and lower case letters (A-Z, a-z)', and 'At least one special character (~!@#%&*~.;,:<>[]{}())'. 'Close' and 'Next' buttons are in the bottom right.

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

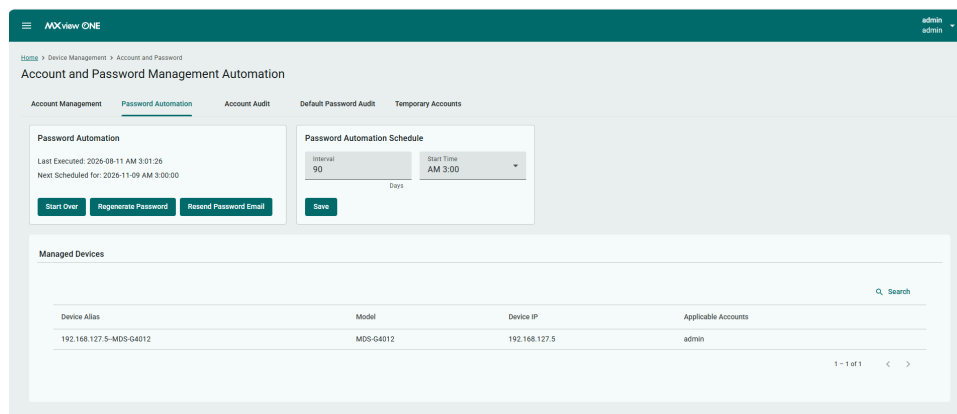
The screenshot shows the 'Password Automation Wizard' interface at Step 4: Apply Password to Devices. The progress bar shows steps 1, 2, and 3 completed, step 4 active, and step 5 pending. Below the progress bar, a table displays the status of password generation for selected devices.

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

- 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.

11. Click **Close**.

The table will show all the devices and associated accounts that password automation is applied to.



NOTE

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

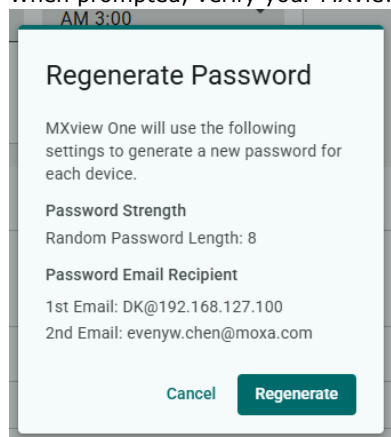
Regenerating Device Passwords



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.



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

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

Device Alias	Model	Device IP	Status
192.168.127.240-EDS-G516E	EDS-G516E	192.168.127.240	Finished

Send Password Email

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**.

- Navigate to **Menu** (☰) > **Device Management** > **Account and Password**.
- Go to the **Password Automation** tab.
- In the **Password Automation** section, click **Resend Password Email**.
- When prompted, verify your MXview One account.

Resend Password Email

Are you sure you want to resend the device password to the following recipient(s)?

1st Email: DK@192.168.127.100
2nd Email: evenyw.chen@moxa.com

Cancel **Resend**

- 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]
2nd Email: [Redacted]

Close

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**.

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

3. In the **Password Automation Schedule** section, configure the following settings:

Password Automation Schedule

Interval: 90 Days

Start Time: AM 3:00

Save

- **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.

MXview ONE

Home > Device Management > Account and Password

Account and Password Management Automation

Account Management Password Automation **Account Audit** Default Password Audit Temporary Accounts

Accounts Baseline

Last Executed: N/A

Create

Device Alias	Compatible	Model	Device IP	Baseline Accounts	Added Accounts	Deleted Accounts
192.168.4.201-EDS-GS12E-8PoE	Yes	EDS-GS12E-8PoE	192.168.4.201	N/A	N/A	N/A
192.168.123.70-AWK-4252A	Yes	AWK-4252A	192.168.123.70	N/A	N/A	N/A
192.168.127.22-UC-2222A-T	No	UC-2222A-T	192.168.127.22	N/A	N/A	N/A
192.168.127.62-NPort-6250-G2	No	NPort-6250-G2	192.168.127.62	N/A	N/A	N/A

1 - 4 of 4

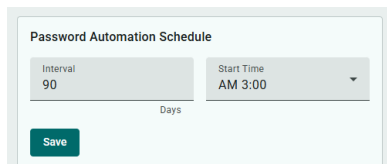
This page displays the following information in a table format:

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. In the **Accounts Baseline** section, click **Create**.



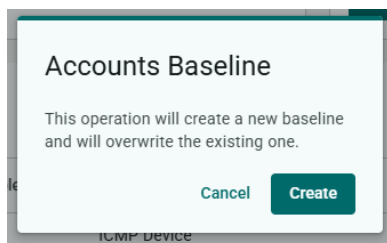
Password Automation Schedule

Interval: 90 Days

Start Time: AM 3:00

Save

4. When prompted, click **Create**. This action will overwrite the current baseline, if present.



Accounts Baseline

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

Cancel Create

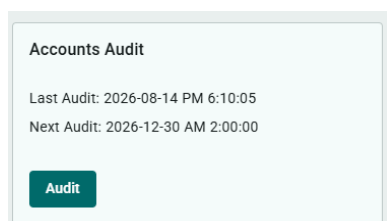
Executing a Manual Account Audit



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. In the **Accounts Audit** section, click **Audit**.
MXview One will compare the current accounts to the baseline and will show any added or deleted accounts in the table.



Accounts Audit

Last Audit: 2026-08-14 PM 6:10:05

Next Audit: 2026-12-30 AM 2:00:00

Audit

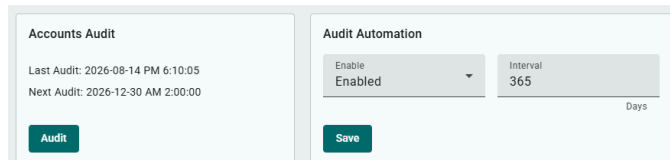
Configuring an Automatic Account Audit Schedule



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 Audit: 2026-08-14 PM 6:10:05

Next Audit: 2026-12-30 AM 2:00:00

Audit

Audit Automation

Enable: Enabled

Interval: 365 Days

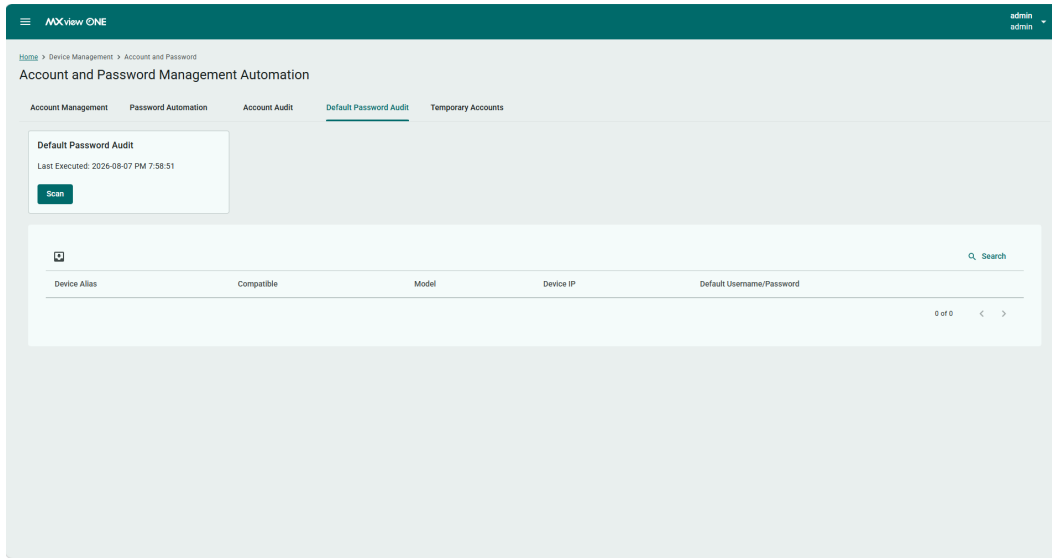
Save

- **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.

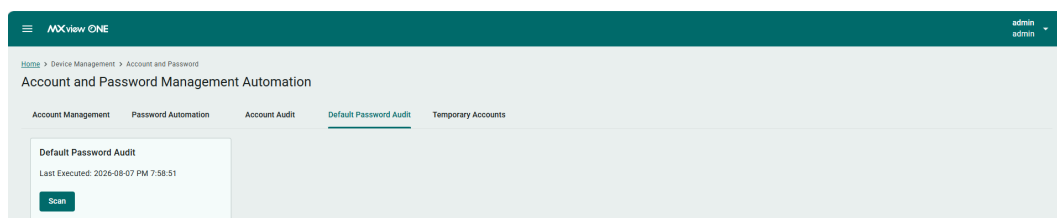


This page displays the following information in a table format:

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**.



4. When prompted, 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.

Device Alias	Compatible	Model	Device IP	Username	Start Time	End Time	Status
10.90.24.83-ICMP Device	No	ICMP Device	10.90.24.83	N/A	N/A	N/A	N/A
10.90.26.167-MGate-S242	No	MGate-S242	10.90.26.167	N/A	N/A	N/A	N/A
10.90.26.169-MGate-S442	No	MGate-S442	10.90.26.169	N/A	N/A	N/A	N/A
192.168.127.1-EDS-4008-4P-2GT-2GS	Yes	EDS-4008-4P-2GT-2GS	192.168.127.1				
192.168.127.2-ABB	No	ABB	192.168.127.2	N/A	N/A	N/A	N/A
192.168.127.4-	Yes	MDS-G4028	192.168.127.4				
192.168.127.5-MDS-G4012	Yes	MDS-G4012	192.168.127.5				
192.168.127.30-ICS-G7528A	Yes	ICS-G7528A	192.168.127.30				
192.168.127.31-EDS-S28E	Yes	EDS-S28E	192.168.127.31				
192.168.127.32-EDS-P506E	Yes	EDS-P506E	192.168.127.32				
192.168.127.33-EDS-G512E	Yes	EDS-G512E	192.168.127.33				
192.168.127.34-EDS-S18E	Yes	EDS-S18E	192.168.127.34				
192.168.127.35-IKS-G6824A	Yes	IKS-G6824A	192.168.127.35				
192.168.127.36-EDS-S10E	Yes	EDS-S10E	192.168.127.36				
192.168.127.37-IKS-6728A	Yes	IKS-6728A	192.168.127.37				

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

- Navigate to **Menu** > **Device Management** > **Account and Password**.
- Go to the **Temporary Accounts** tab.
- Click the **Add** () icon next to the device you want to create a temporary account for.

- 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.

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 screenshot shows the 'Edit Temporary Account' dialog box. It contains the following fields and values:

- Username:** temp
- Password:** 8 / 64 (masked with dots)
- Action:** Scheduled (dropdown menu)
- Active From:** 2026/09/11 (calendar icon)
- Start Time:** PM 3:00 (dropdown menu)
- Valid Until:** 2026/09/11 (calendar icon)
- End Time:** PM 4:30 (dropdown menu)

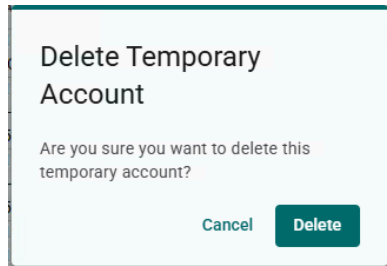
At the bottom right, there are two buttons: 'Cancel' and 'Change'.

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.

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.



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

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.

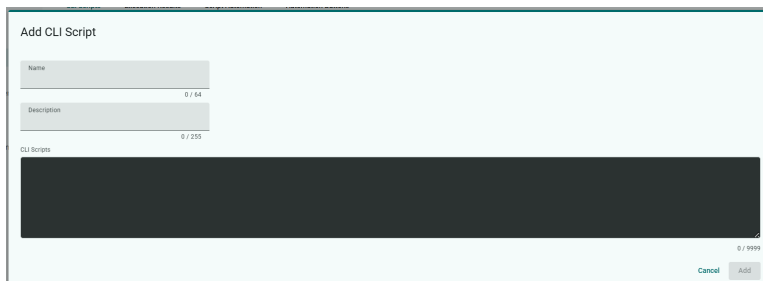
The screenshot displays the 'Saved CLI Scripts' page in the MXview ONE interface. The page has a sidebar on the left with a search bar and a list of navigation items. The main content area shows a table of saved CLI scripts. At the top of the table area, there is a notification about 'Scheduled Script' and a note about creating scheduled tasks. The table has four columns: 'Name', 'Description', 'Linked Scheduled Tasks', and 'Linked Script Automations'. The table lists several scripts, each with a checkbox, an edit icon, and a delete icon. The scripts are: 'Show IP NOS', 'Show IP eCos', 'Reboot', 'show time', 'show config', 'Default', and 'test 2 command'. The 'show config' script is linked to 'Check config' and 'Export Config'. The 'Default' script is linked to 'reset to default'. The 'test 2 command' script is linked to 'test 2 command'.

	Name	Description	Linked Scheduled Tasks	Linked Script Automations
☐	Show IP NOS	Show IP NOS		Show IP
☐	Show IP eCos	Show IP eCos		Show IP
☐	Reboot	reboot		Reboot
☐	show time	show device time		show device time
☐	show config	show running-config	Check config	Export Config
☐	Default	reset to default		
☐	test 2 command	test 2 command		test 2 command

CLI Scripts

Adding a CLI Script

1. Navigate to **Menu** (☰) > **Saved CLI Scripts** > **CLI Scripts**.
2. Click the **Add** (+) icon.



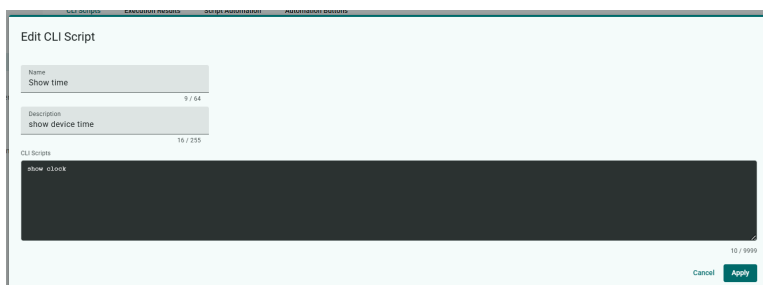
3. Configure the following settings:
 - a. **Name:** Enter a name for the CLI script.
 - b. **Description:** Enter a description for the CLI script.
 - c. **CLI Script:** Enter the CLI command(s) to execute.
4. Click **Add**. The script will be added to the table.

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



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**.

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.
3. When prompted, click **Delete**.

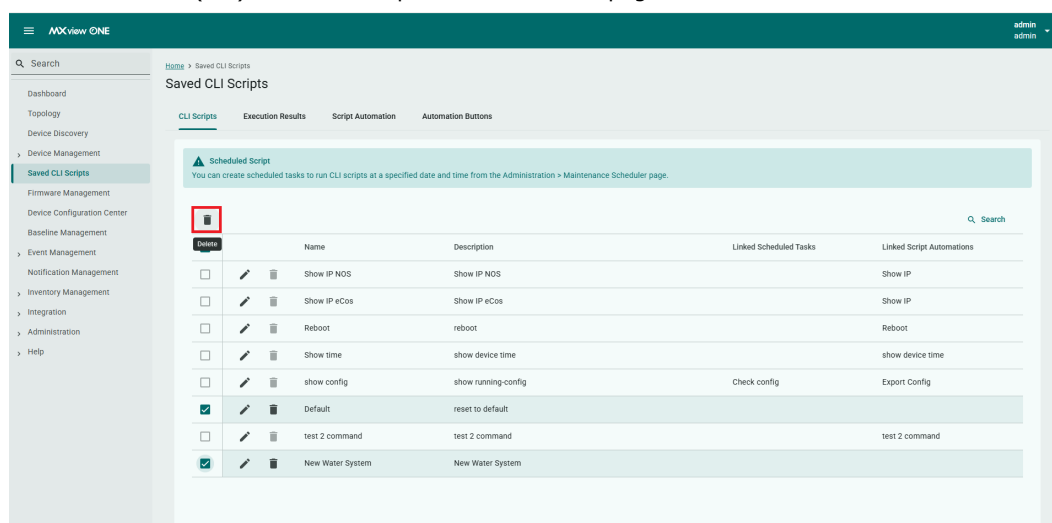
Deleting Multiple CLI Scripts



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**.
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.

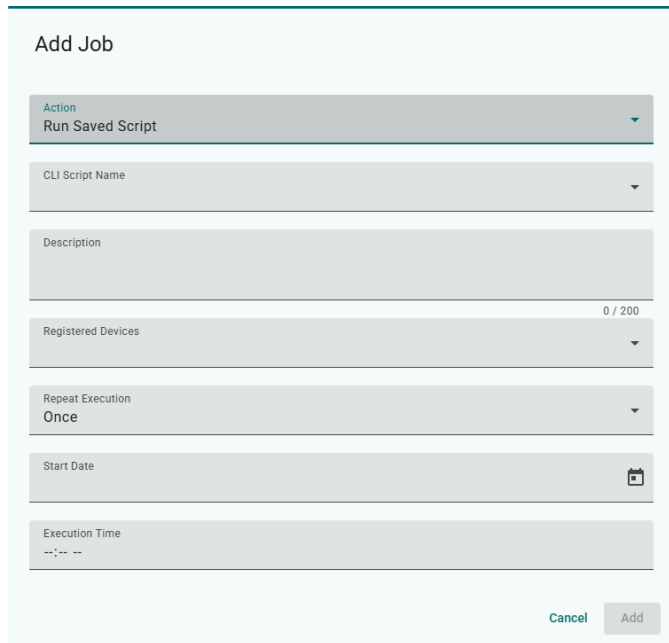


4. When prompted, click **Delete**.

Creating a CLI Script Scheduled Task

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

2. Click the **Add** (+) icon.



The 'Add Job' form is a light blue modal window. It contains several input fields: a dropdown for 'Action' with 'Run Saved Script' selected, a dropdown for 'CLI Script Name', a text area for 'Description' with a '0 / 200' character count, a dropdown for 'Registered Devices', a dropdown for 'Repeat Execution' with 'Once' selected, a date picker for 'Start Date', and a time picker for 'Execution Time' showing '--:-- --'. At the bottom right are 'Cancel' and 'Add' buttons.

3. Configure the following settings:
 - **Job Name:** Enter a name for the job.
 - **Action:** Select **Run Saved Script** from the Action drop-down list.
 - **CLI Script Name:** Select the CLI script that you want to execute.
 - **Description:** Enter a description for the job.
 - **Registered Devices:** Select the devices that you want to run the selected CLI script on.
 - **Repeat Execution:** Select the job execution frequency: Once, Daily, Weekly, Monthly.
 - **Start Date:** If you select **Once** in the Repeat Execution field, specify the start date to begin executing the scheduled job.
 - **On:** If you select **Weekly** or **Monthly** in the Repeat Execution field, specify when to begin executing the scheduled job.
 - **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.

Execution Results

Download All Execution Results

1. Navigate to **Menu** (☰) > **Saved CLI Scripts**.
2. Go to the **Execution Results** tab.
3. Under **Download All Execution Results**, click **Download**.

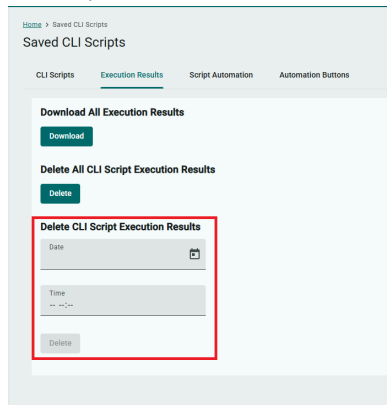
MXview One will download all the CLI script execution results as a ZIP file.

Delete All CLI Script Execution Results

1. Navigate to **Menu** (☰) > **Saved CLI Scripts**.
2. Go to the **Execution Results** tab.
3. Under **Delete All CLI Script Execution Results**, click **Delete**.
4. When prompted, click **Delete**.

Delete Execution Results Prior to a Specified Time

1. Navigate to **Menu** (☰) > **Saved CLI Scripts**.
2. Go to the **Execution Results** tab.
3. In the **Delete Script Execution Results Prior to** section, specify the **Date** and **Time**. All execution results prior to this date and time will be deleted.



4. Click **Delete**.
5. When prompted, click **Delete**.

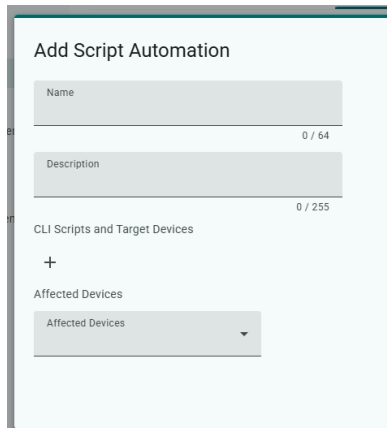
Script Automation

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**.
2. Go to the **Script Automation** tab.

- Click the **Add (+)** icon.



The form titled "Add Script Automation" contains the following fields and options:

- Name:** A text input field with a character count of 0 / 64.
- Description:** A text input field with a character count of 0 / 255.
- CLI Scripts and Target Devices:** A section with a plus icon (+) to add items.
- Affected Devices:** A dropdown menu labeled "Affected Devices".

- 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.

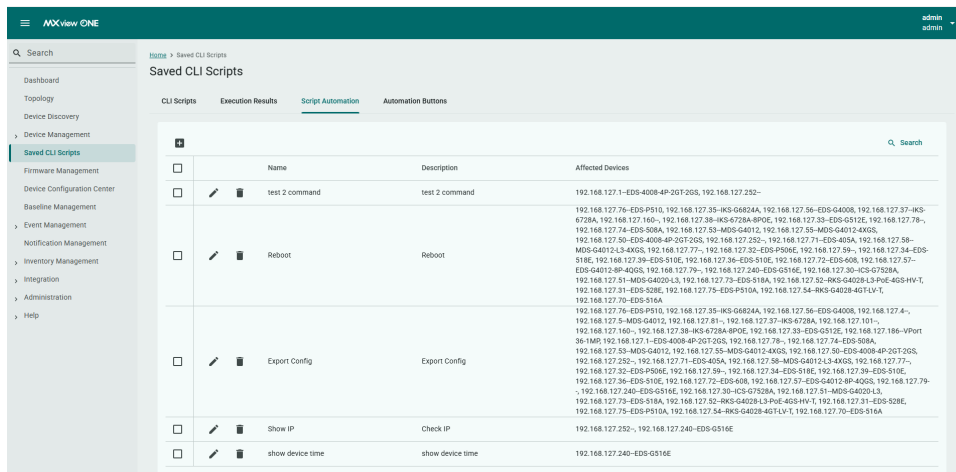
- **Affected Devices:** Select the device(s) that will be affected by executing the CLI script(s) in the automation. A warning reminder with a list of affected devices will show when attempting to execute the automation button. If left blank, relevant devices will still be affected, but no warning will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

- 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.



The screenshot shows the "Saved CLI Scripts" section in the MXview ONE interface. It includes a table with columns for Name, Description, and Affected Devices. The table lists several scripts, including "test 2 command", "Reboot", "Export Config", "Show IP", and "show device time". Each script has a checkbox in the first column and a plus icon in the second column.

	Name	Description	Affected Devices
☐	test 2 command	test 2 command	192.168.127.1-EDS-4008-4P-20T-20S, 192.168.127.252-
☐	Reboot	Reboot	192.168.127.76-EDS-P510, 192.168.127.35-IXS-G6824A, 192.168.127.56-EDS-G4008, 192.168.127.37-IXS-G728A, 192.168.127.166-, 192.168.127.38-IXS-G728A-8P0E, 192.168.127.39-EDS-G510E, 192.168.127.78-, 192.168.127.74-EDS-S08A, 192.168.127.53-MDS-G4012, 192.168.127.55-MDS-G4012-4X0S, 192.168.127.50-EDS-4008-4P-20T-20S, 192.168.127.252-, 192.168.127.71-EDS-405A, 192.168.127.58-MDS-G4012-3-4X0S, 192.168.127.77-, 192.168.127.32-EDS-P506E, 192.168.127.59-, 192.168.127.34-EDS-S18E, 192.168.127.39-EDS-S10E, 192.168.127.34-EDS-S10E, 192.168.127.72-EDS-K08, 192.168.127.57-EDS-G4012-8P-400S, 192.168.127.79-, 192.168.127.240-EDS-G516E, 192.168.127.30-IXS-G7328A, 192.168.127.51-MDS-G4020-L3, 192.168.127.73-EDS-S18A, 192.168.127.52-IXS-G4020-L3-PoE-40S-HV-T, 192.168.127.31-EDS-S28E, 192.168.127.75-EDS-P510A, 192.168.127.54-IXS-G4020-40-FLV-T, 192.168.127.70-EDS-S16A
☐	Export Config	Export Config	192.168.127.76-EDS-P510, 192.168.127.35-IXS-G6824A, 192.168.127.56-EDS-G4008, 192.168.127.4-, 192.168.127.5-MDS-G4012, 192.168.127.81-, 192.168.127.37-IXS-G728A, 192.168.127.101-, 192.168.127.160-, 192.168.127.38-IXS-G728A-8P0E, 192.168.127.39-EDS-G510E, 192.168.127.78-, 192.168.127.74-EDS-S08A, 36-MDP 192.168.127.1-EDS-4008-4P-20T-20S, 192.168.127.78-, 192.168.127.74-EDS-S08A, 192.168.127.53-MDS-G4012, 192.168.127.55-MDS-G4012-4X0S, 192.168.127.50-EDS-4008-4P-20T-20S, 192.168.127.252-, 192.168.127.71-EDS-405A, 192.168.127.58-MDS-G4012-3-4X0S, 192.168.127.77-, 192.168.127.32-EDS-P506E, 192.168.127.59-, 192.168.127.34-EDS-S18E, 192.168.127.39-EDS-S10E, 192.168.127.34-EDS-S10E, 192.168.127.72-EDS-K08, 192.168.127.57-EDS-G4012-8P-400S, 192.168.127.79-, 192.168.127.240-EDS-G516E, 192.168.127.30-IXS-G7328A, 192.168.127.51-MDS-G4020-L3, 192.168.127.73-EDS-S18A, 192.168.127.52-IXS-G4020-L3-PoE-40S-HV-T, 192.168.127.31-EDS-S28E, 192.168.127.75-EDS-P510A, 192.168.127.54-IXS-G4020-40-FLV-T, 192.168.127.70-EDS-S16A
☐	Show IP	Check IP	192.168.127.252-, 192.168.127.240-EDS-G516E
☐	show device time	show device time	192.168.127.240-EDS-G516E



NOTE

MXview One supports a maximum of 200 script automations.

Editing a Script Automation

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

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**.

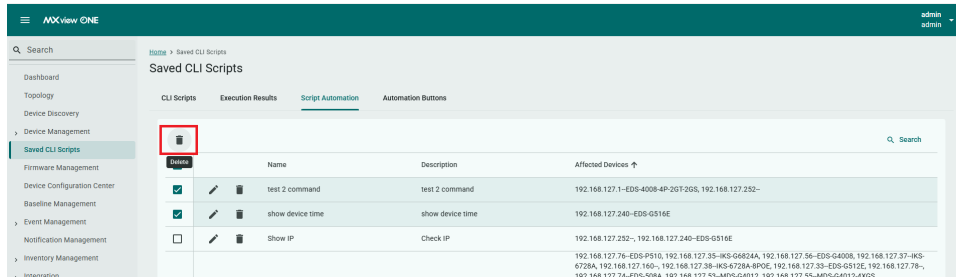
5. Click **Apply**.

Deleting a Script Automation

1. Navigate to **Menu** (☰) > **Saved CLI Scripts**.
2. Go to the **Script Automation** tab.
3. Click the **Delete** (🗑) icon next to the script automation you want to delete.
4. When prompted, click **Delete**.

Deleting Multiple Script Automations

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



5. When prompted, click **Delete**.

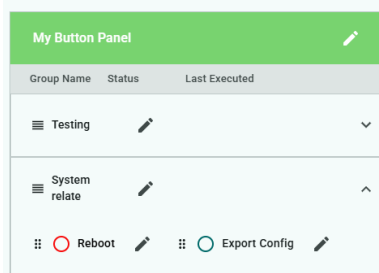
Automation Buttons

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

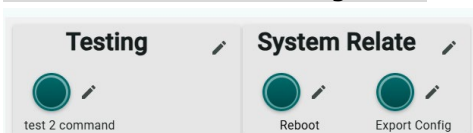
Each newly added automation script will automatically generate an automation button that is placed in the default Unnamed group.

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**.

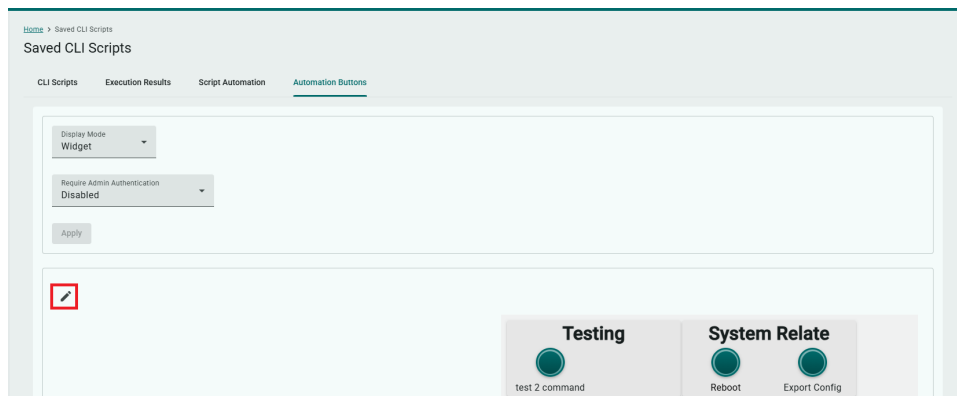
Editing an Automation Button Group



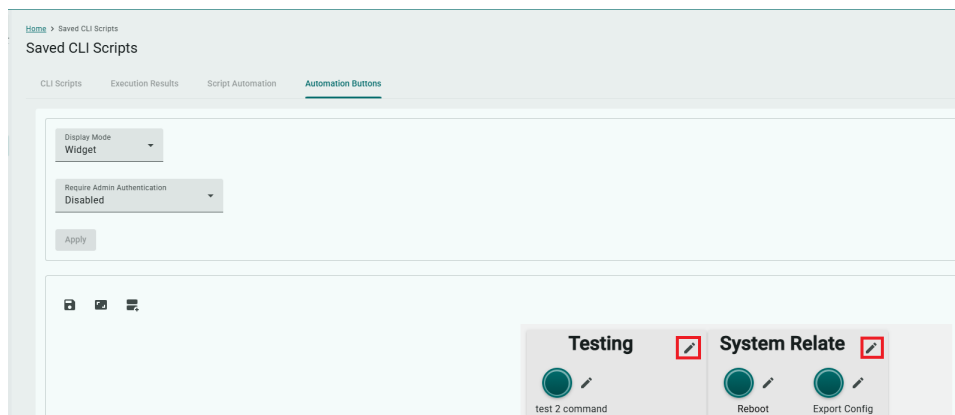
NOTE

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.

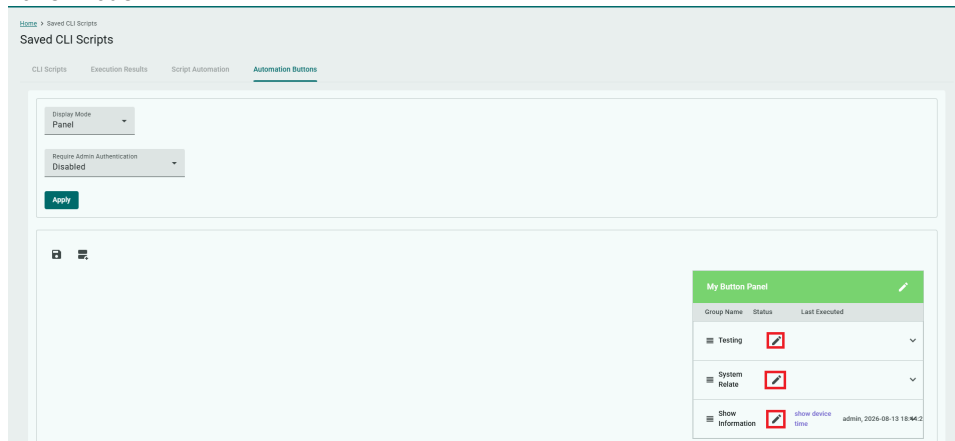
1. Navigate to **Menu** (☰) > **Saved CLI Scripts**.
2. Go to the **Automation Buttons** tab.
3. Click the **Edit** (✎) icon in the top-left corner of the screen to enter edit mode.



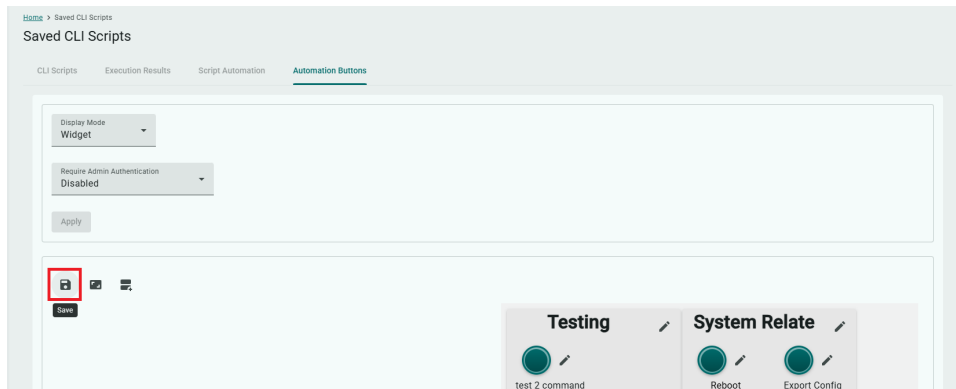
4. In edit mode, Click the **Edit** (✎) icon next to the group name of the group you want to edit.
 - **Widget mode:**



➤ Panel mode:



5. In the **Edit Group** window, 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.



Editing an Automation Button

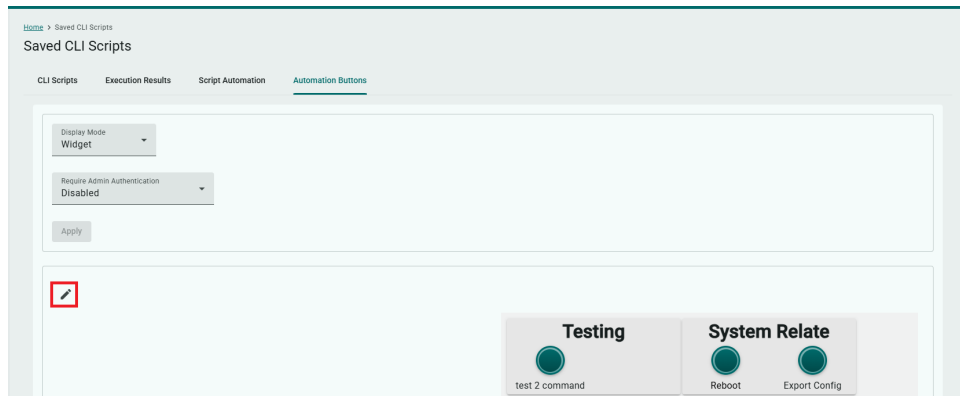


NOTE

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.

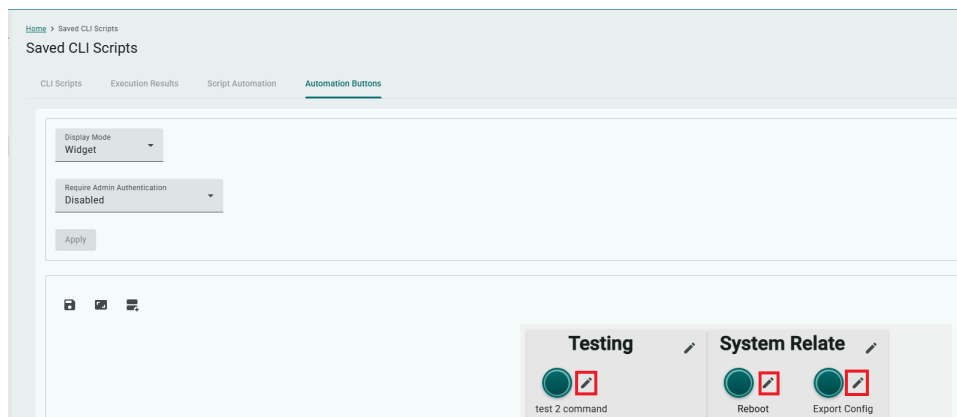
1. Navigate to **Menu** () > **Saved CLI Scripts**.
2. Go to the **Automation Buttons** tab.

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

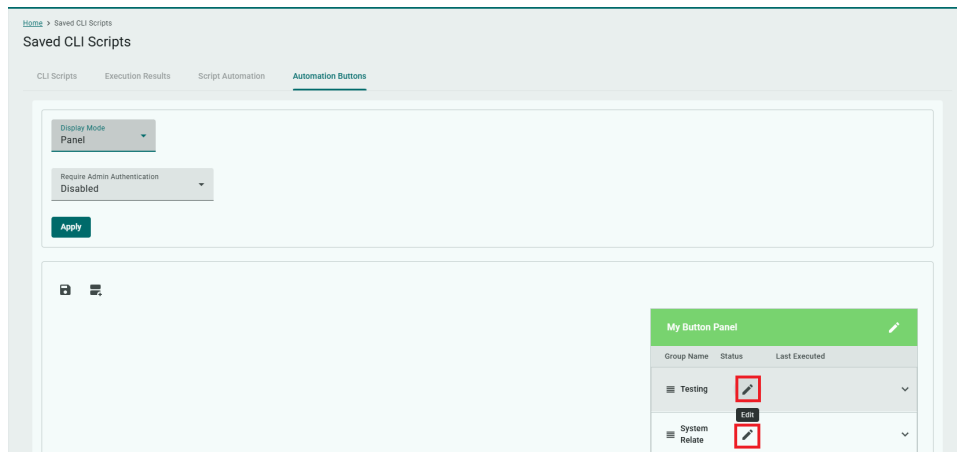


- In edit mode, click the **Edit** (✎) icon next to the button you want to edit.

➤ Widget mode:

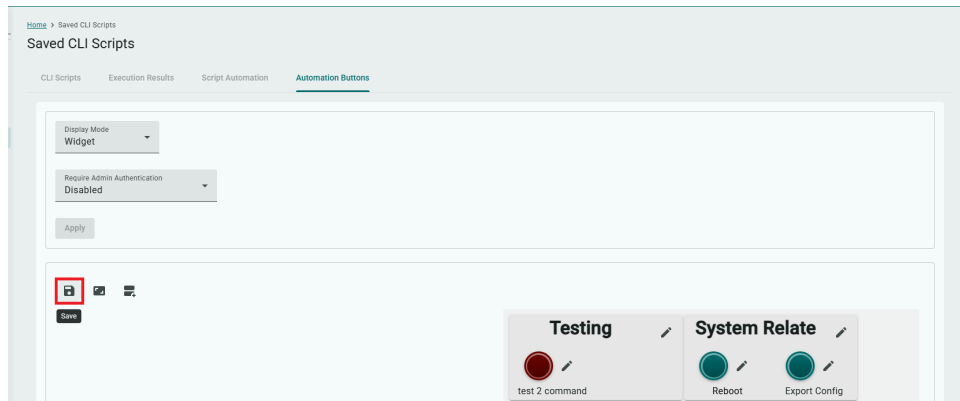


➤ Panel mode:



- In the **Edit Button** window, configure the following settings:
 - **State:** (For Panel mode only) Enable or disable the automation button.
 - **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.
 - **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.
 - **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.
- Click **Apply**.

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



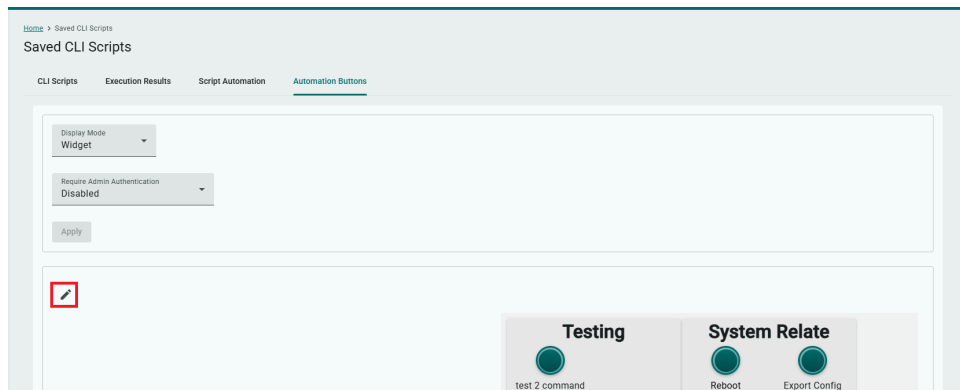
Creating an Automation Button Group



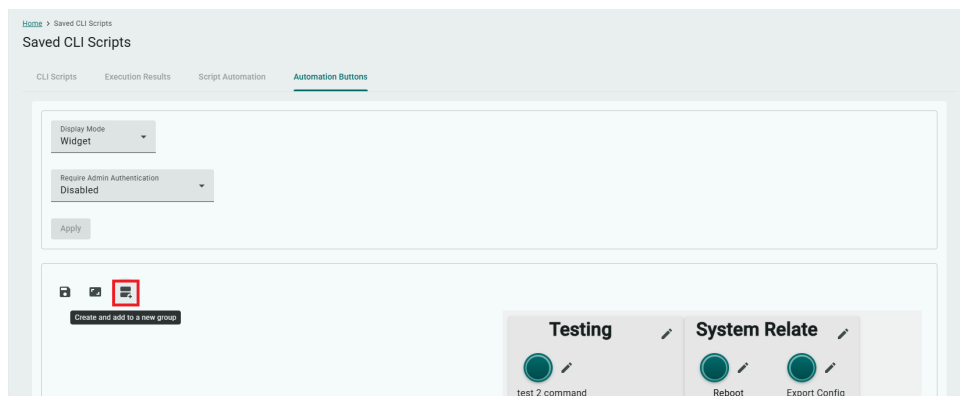
NOTE

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.

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



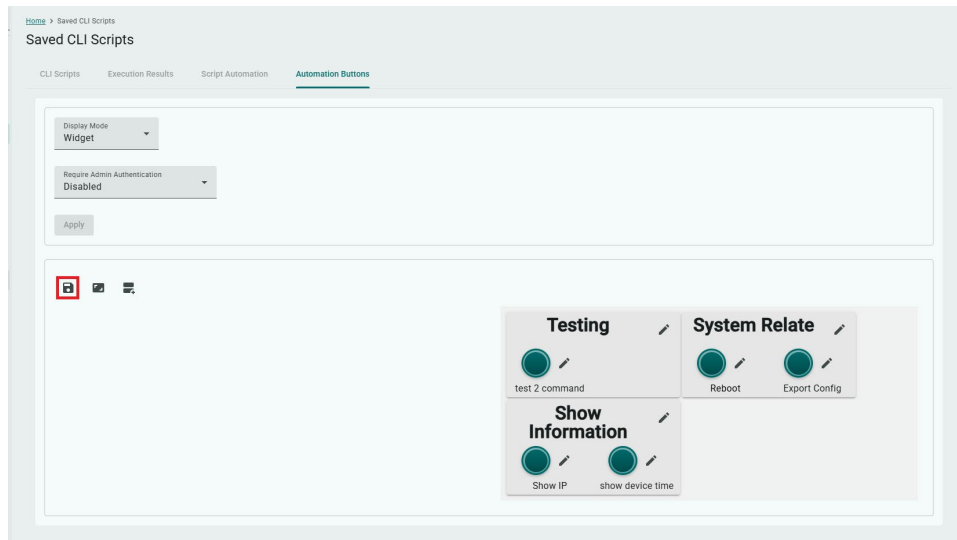
- Click the **Create and add to a new group** () icon in the top-left corner of the screen.



In the **Create and add to a new group** window, 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 new group will appear on the **Automation Buttons** page.
- 6. Click the **Save** () icon to save your changes and leave edit mode.



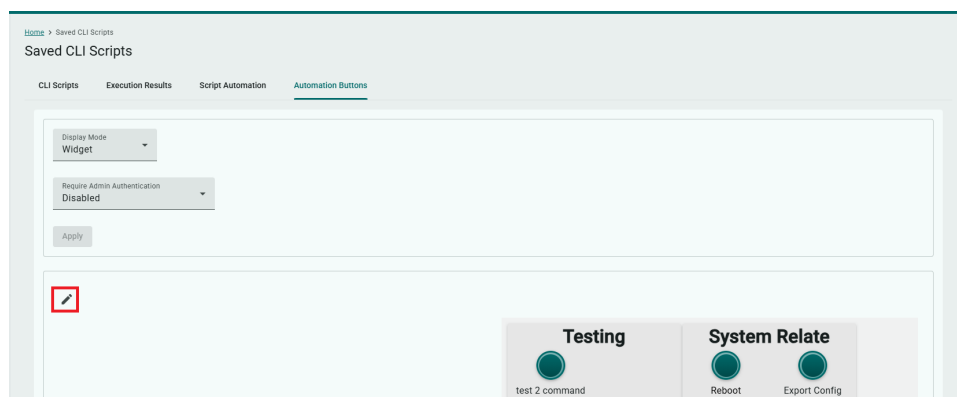
Changing the Automation Button Widget Size



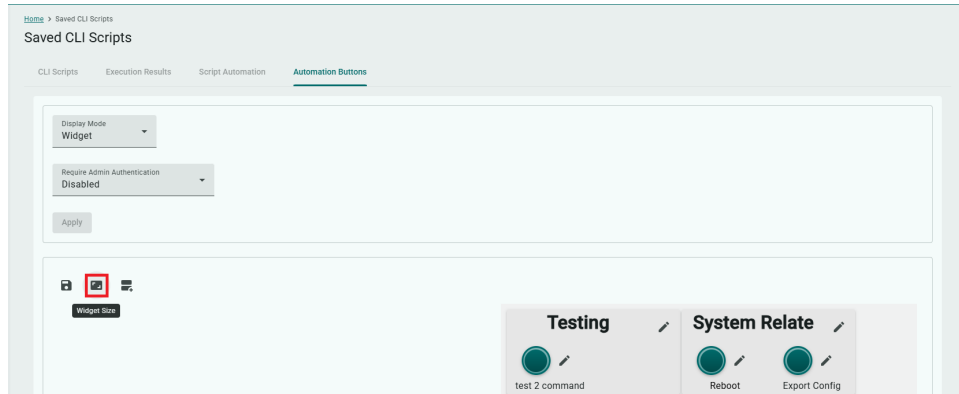
NOTE

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

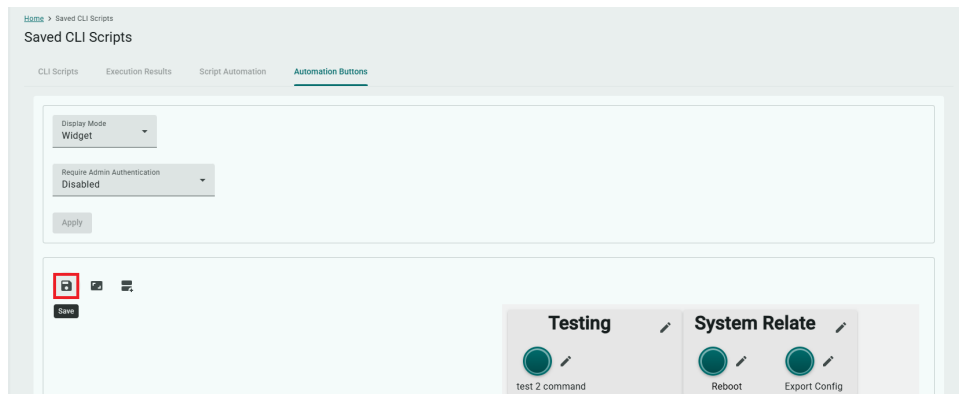
1. Navigate to **Menu** () > **Saved CLI Scripts**.
2. Go to the **Automation Buttons** tab.
3. Click the **Edit** () icon in the top-left corner of the screen to enter edit mode.



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



5. In the **Widget Size** window, 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.
6. Click the **Save** () icon to save your changes and leave edit mode.



Previewing Affected Devices

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

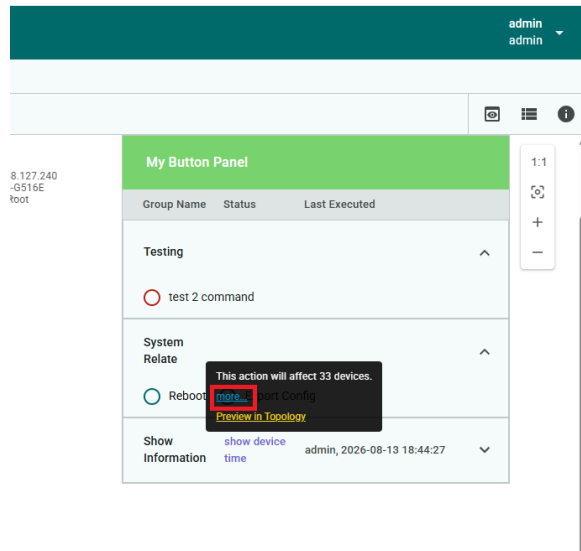


NOTE

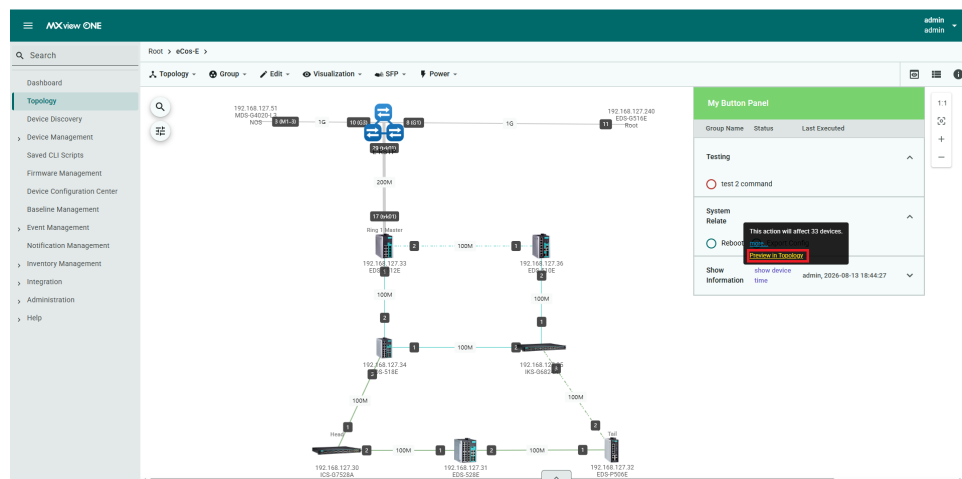
This function is only available if the **Automation Button Display Mode** is set to **Panel**. Refer to **Setting the Automation Button Display Mode**.

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.

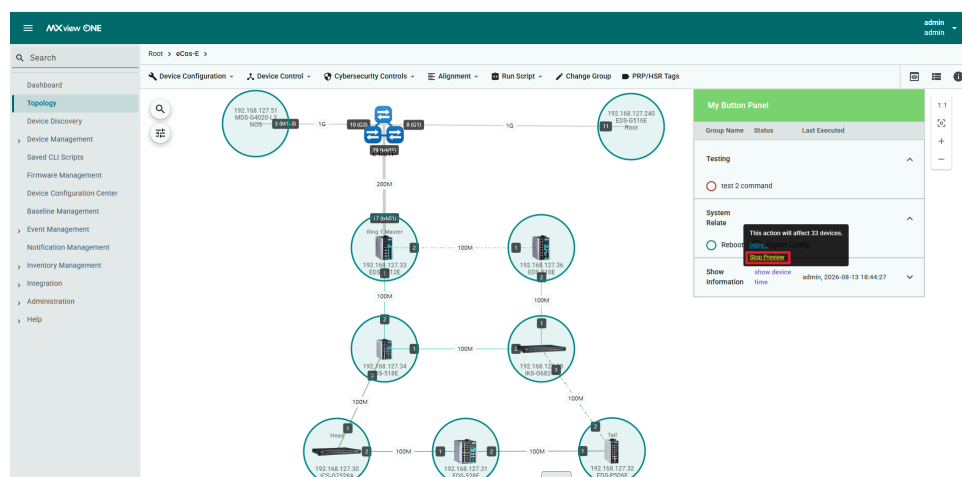
- Click **more ...** to show a list of all affected devices.



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



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

	Model Series	Device Status	Latest Version on the Firmware Server	Selected Version	Selected Firmware Download Status
☐	PT-G7728	Not updated	v6.6	None	
☐	PT-G503	All updated	v5.3	None	
☐	PT-G7828	All updated	v6.6	None	
☐	DA820C (Windows)	No Information	No Information	No Information	



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.

Checking the Firmware Status

The **Check Firmware Status** section includes the following 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.

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
☐	PT-G7728	Not updated	v6.6	None	
☐	PT-G503	All updated	v5.3	None	
☐	PT-G7828	All updated	v6.6	None	
☐	DA820C (Windows)	No Information	No Information	No Information	

This screen includes the following information:

Item	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.

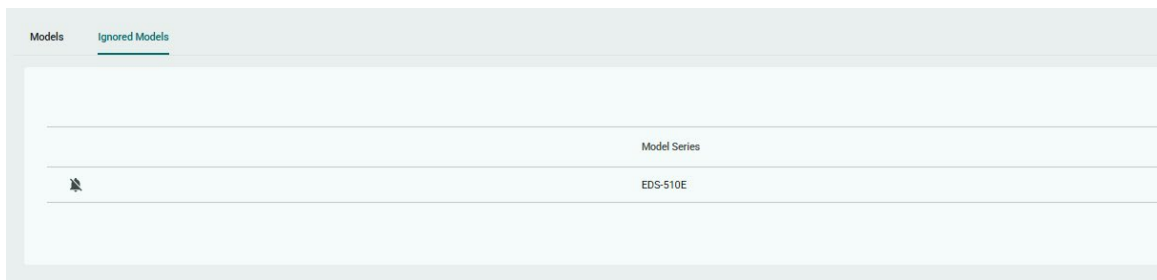
The following actions are available from this screen:

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

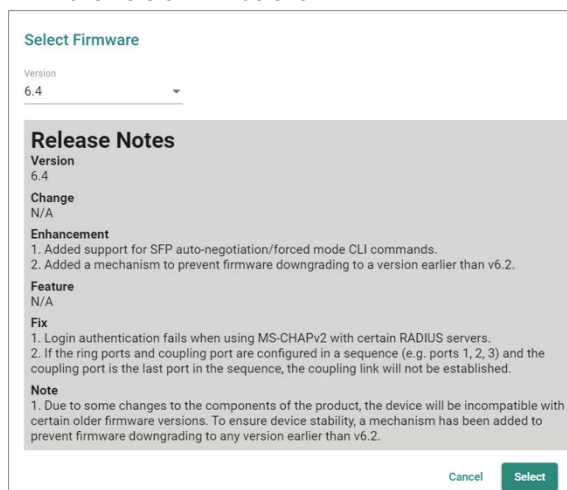
The Ignored Models lists all models for which MXview One is not checking for new firmware and is not sending notifications. To add a model series to the Ignored Models list, click the bell () icon on the Models tab next to the model series.



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 the **Models** tab.
3. In the device list, click the **Select Firmware** () icon of the corresponding model series in the Selected Version column.
4. Select a firmware version from the **Version** drop-down menu. The release notes for the selected firmware version will be shown.

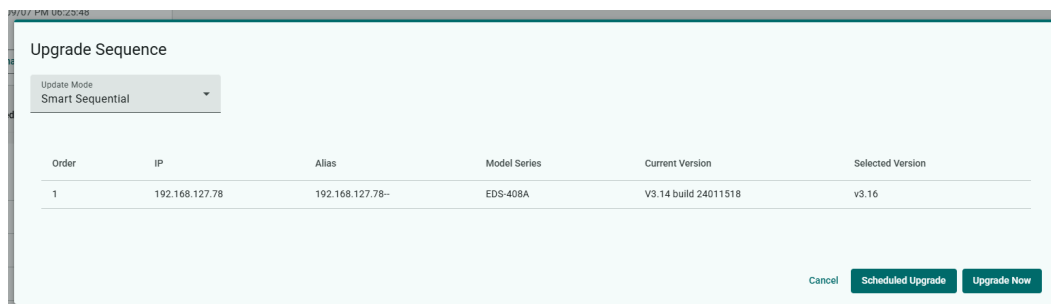


5. Click **Select**.
MXview One will begin downloading the selected firmware. The download progress will be shown in the Selected Firmware Download Status column.

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	192.168.127.78	192.168.127.78--	EDS-408A	V3.14 build 24011518	v3.16

Cancel Scheduled Upgrade Upgrade Now

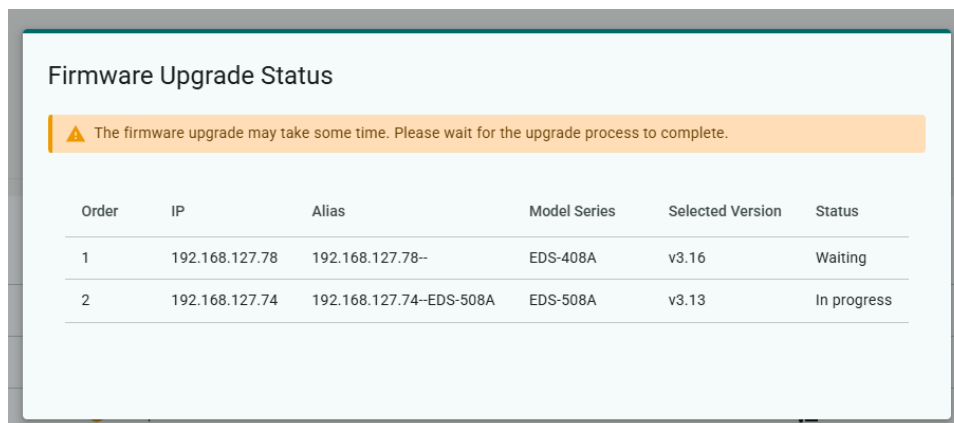
- a. Select the reboot sequence:
 - ☐ **Strict Sequential:** Upgrade the devices based on the device sequence in the topology starting from the device furthest away from the computer running MXview One, proceeding to the nearest one.
 - ☐ **Smart Sequential:** Upgrade the devices based on the device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



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	192.168.127.78	192.168.127.78--	EDS-408A	v3.16	Waiting
2	192.168.127.74	192.168.127.74--EDS-508A	EDS-508A	v3.13	In progress

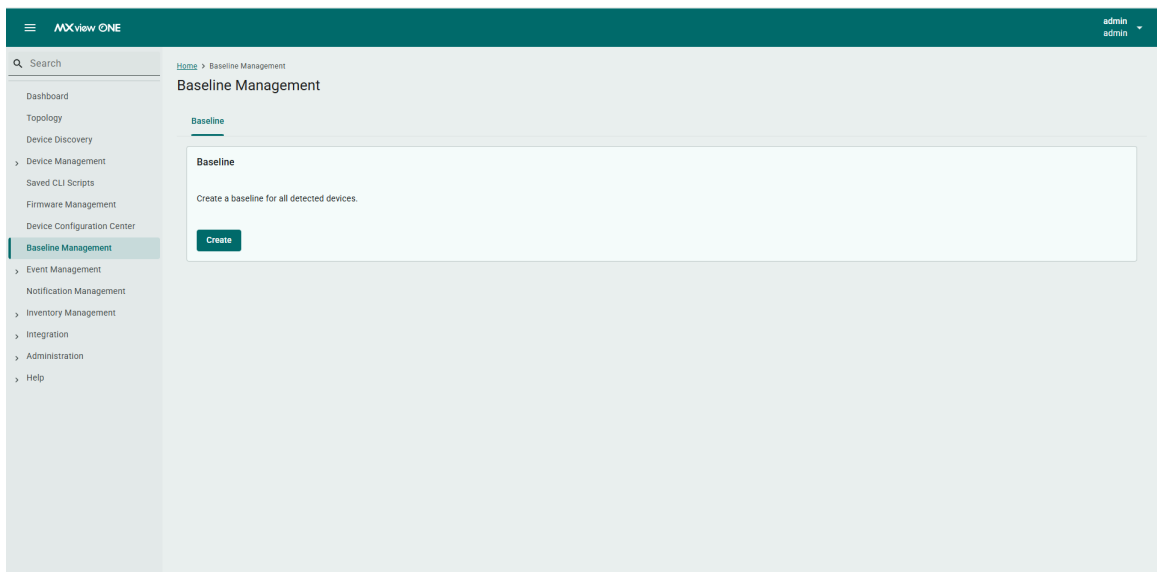
7. When the upgrade is finished, click **Download CSV Report** or **Download PDF Report** to download a summary report of the firmware upgrade.
8. If the firmware upgrade was unsuccessful, check the error description in the Status column to identify the issue. Click **Retry Failed Devices** to perform the action again.
9. If you close this page without downloading the results report, a confirmation will appear. Clicking **Ignore** will delete the results report permanently.

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**.
4. In the **Create Baseline** window, enter the password of the currently logged in user.

- Click **Create**.
MXview One will create a configuration and firmware baseline for all detected devices.

The screenshot shows the MXview ONE Baseline Management interface. It includes a 'Baseline' section with a 'Create' button, an 'Audit' section with 'Last Audit' and 'Next Audit' dates, and a 'Scheduled Audit' section with 'Enable' and 'Interval' settings. Below these sections is a table listing devices with columns for IP Address, Alias, Configuration Baseline Status, Firmware Baseline Status, Configuration Baseline Audit Status, and Firmware Baseline Audit Status.

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**.

- Navigate to **Menu** (☰) > **Baseline Management**.
- Go to the **Baseline** tab.
- In the **Audit** section, click **Audit**.
- When prompted to confirm, click **Audit**.

Configuring Scheduled Baseline Audits

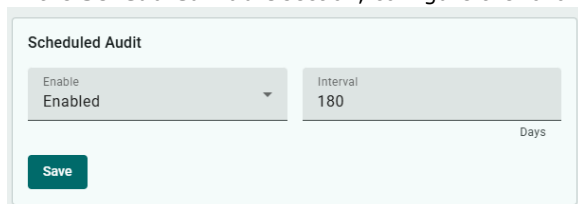


NOTE

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

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

3. In the **Scheduled Audit** section, configure the following settings:



Scheduled Audit

Enable
Enabled

Interval
180

Days

Save

- **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**.
The **Next Audit** field in the **Audit** section will show the next scheduled audit.

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.

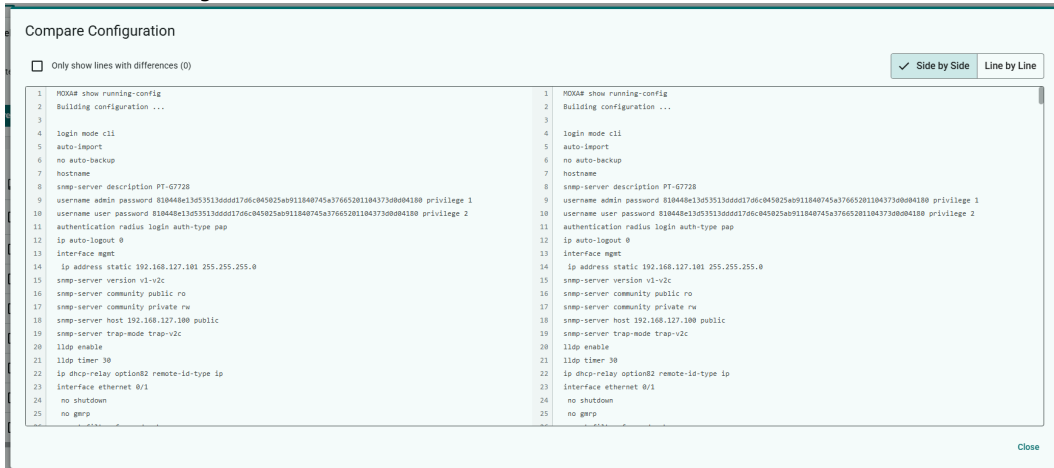


NOTE

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.



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

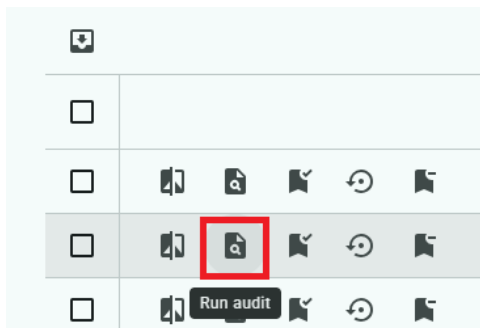
Use the **Audit now** feature to immediately perform a baseline audit on the selected device(s).



NOTE

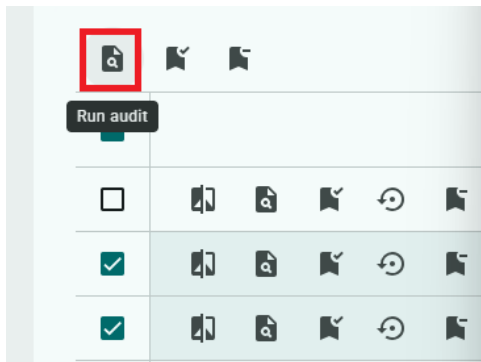
This function is only available after creating a configuration and firmware baseline. Refer to **Creating a Configuration and Firmware Baseline**.

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

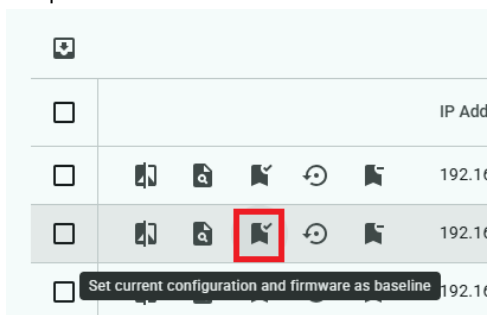
This function allows users to set the current configuration and firmware of one or more devices as the new baseline for those devices. This action will overwrite any existing baseline for the selected device(s).



NOTE

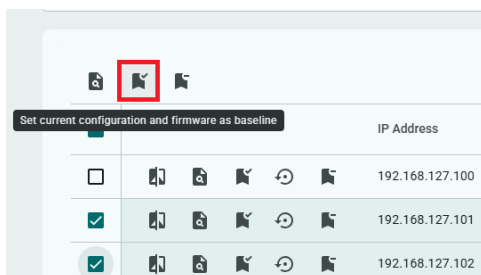
This function is only available after creating a configuration and firmware baseline. Refer to **Creating a Configuration and Firmware Baseline**.

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

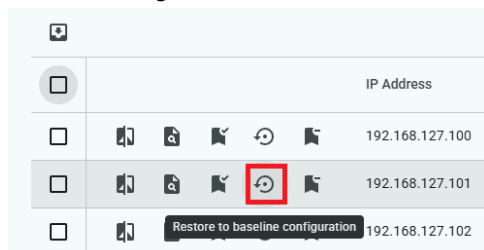
This function allows users to restore the device configuration and firmware to the baseline configuration and firmware version.



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.

The screenshot shows the 'Device' tab in the 'Network' section. The table lists three devices with IP addresses 192.168.127.100, 192.168.127.101, and 192.168.127.102. The third device is highlighted in grey, and its 'Remove' icon (a trash can) is circled in red. A tooltip 'Remove device from baseline' is visible over the fourth device's 'Remove' icon.

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.



Remove device from baseline

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.

MXview ONE

adminadmin

Home > Baseline Management

Baseline Management

BaselineNot in Baseline

Search

☒		IP Address	Alias
☒		192.168.123.70	192.168.123.70-AWK-4252A
☒		192.168.123.72	192.168.123.72-AWK-1151C
☒		192.168.123.152	192.168.123.152-EDS-518A

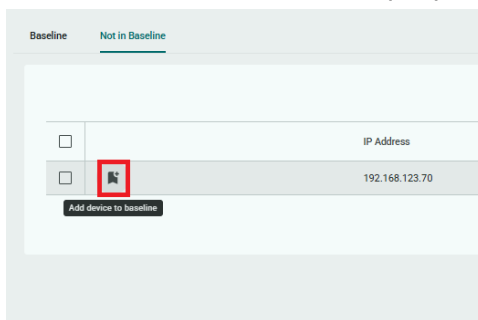
Items per page: 101 - 3 of 3<<>>

Searching the Not in Baseline Data

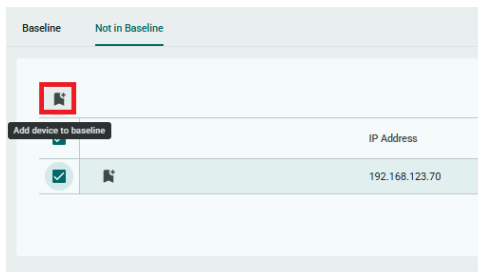
1. Navigate to **Menu** () > **Baseline Management**.
2. Go to the **Not in Baseline** tab.
3. In the **Search** () field, type the full or partial information.
All items matching the entered string will be shown in the table.

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.



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.



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

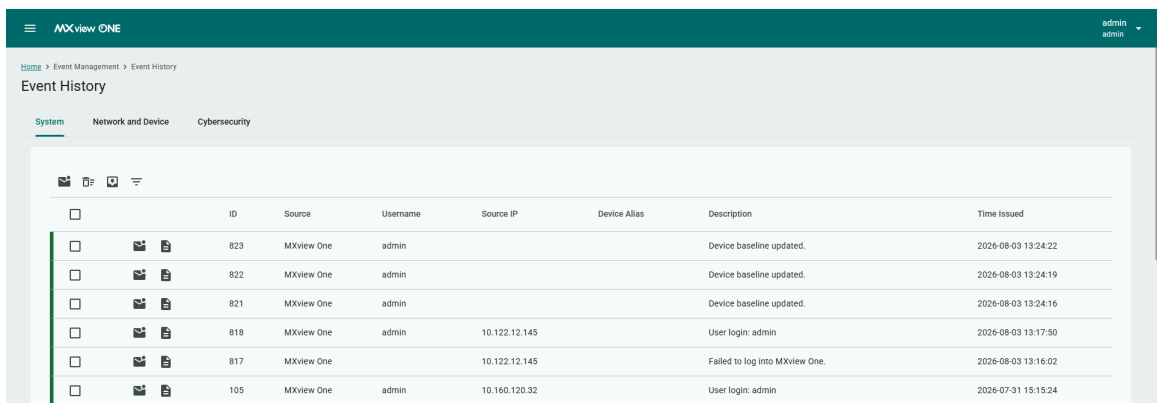
15. Events and Notifications

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

Event Monitoring

Viewing System Events

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
823	MXview One	admin			Device baseline updated.	2026-08-03 13:24:22
822	MXview One	admin			Device baseline updated.	2026-08-03 13:24:19
821	MXview One	admin			Device baseline updated.	2026-08-03 13:24:16
818	MXview One	admin	10.122.12.145		User login: admin	2026-08-03 13:17:50
817	MXview One		10.122.12.145		Failed to log into MXview One.	2026-08-03 13:16:02
105	MXview One	admin	10.160.120.32		User login: admin	2026-07-31 15:15:24

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

The **System** tab shows 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.
 - b. Specify any of the following criteria:
 - ☐ **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
 - b. Click **Apply**.
2. To sort the data in the table by a specific column, click the column heading.
3. 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.

Viewing Network and Device Events

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
☐	602	MXview One		192.168.123.158	192.168.123.158-HEX-402-VDSL2	Device ICMP reachable	2026-08-02 19:27:17
☐	601	MXview One		192.168.123.158	192.168.123.158-HEX-402-VDSL2	Device ICMP unreachable	2026-08-02 19:27:13
☐	566	MXview One		192.168.123.156	192.168.123.156-EDS-408A	Device SNMP reachable	2026-08-02 06:09:17
☐	564	MXview One		192.168.123.156	192.168.123.156-EDS-408A	Device SNMP unreachable	2026-08-02 06:08:26
☐	563	MXview One		192.168.123.162	192.168.123.162-EDS-GS12E-8PoE	Device ICMP reachable	2026-08-02 06:08:19
☐	561	MXview One		192.168.123.162	192.168.123.162-EDS-GS12E-8PoE	Device ICMP unreachable	2026-08-02 06:08:15

The **Network and Device** tab shows 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** tab shows 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.

Column	Description
Description	The description of the event.
Time Issued	The date and time the event was issued.

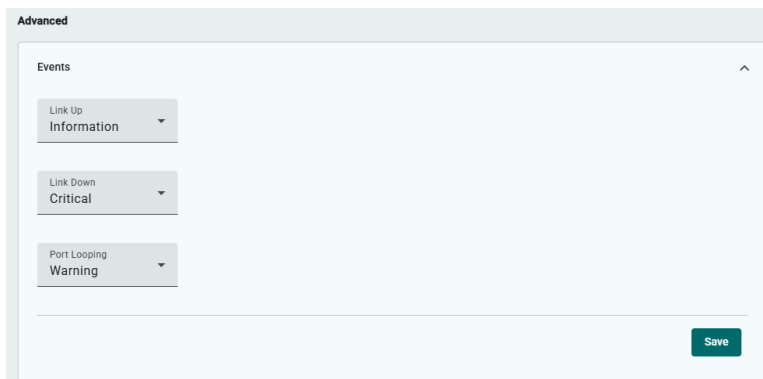
3. To filter the information in the table according to specific criteria:
 - a. Click the **Filter** () icon in the top-left corner.
 - b. Specify any of the following criteria:
 - ☐ **Severity**: Select the severity level of the event.
 - ☐ **Group**: Select the group the device is assigned to.
 - ☐ **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.
 - b. When prompted to confirm, click **Apply**.
6. To delete all events:
 - a. Click the **Clear All Events** () icon in the top-left corner.
 - b. When prompted to confirm, click **Apply**.
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.

Configuring Event Thresholds and Severity Levels

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



3. Assign a severity level to each type of event.
 - **Information**
 - **Warning**
 - **Critical**

4. Click **Save**.
5. Navigate to **Menu** (☰) > **Administration** > **Global Device Settings**.



NOTE

Once saved, changes to **Global Device Settings** will synchronize to each device in the topology.

6. Enable and configure the threshold values and severity levels for the conditions you want to trigger events for.
 - **Bandwidth Utilization**: Triggers an event if bandwidth usage exceeds or falls below the set threshold.
 - **Packet Error Rate**: Triggers an event if the packet error rate exceeds the set threshold.
 - **SFP Threshold**: Triggers an event if SFP TX, RX, or voltage exceeds or falls below the set threshold, or if the transceiver temperature exceeds the set threshold.
7. Click **Save**.



NOTE

If the threshold is set to 0, the threshold will be disabled.

8. Click **Save**.

Notification Methods

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

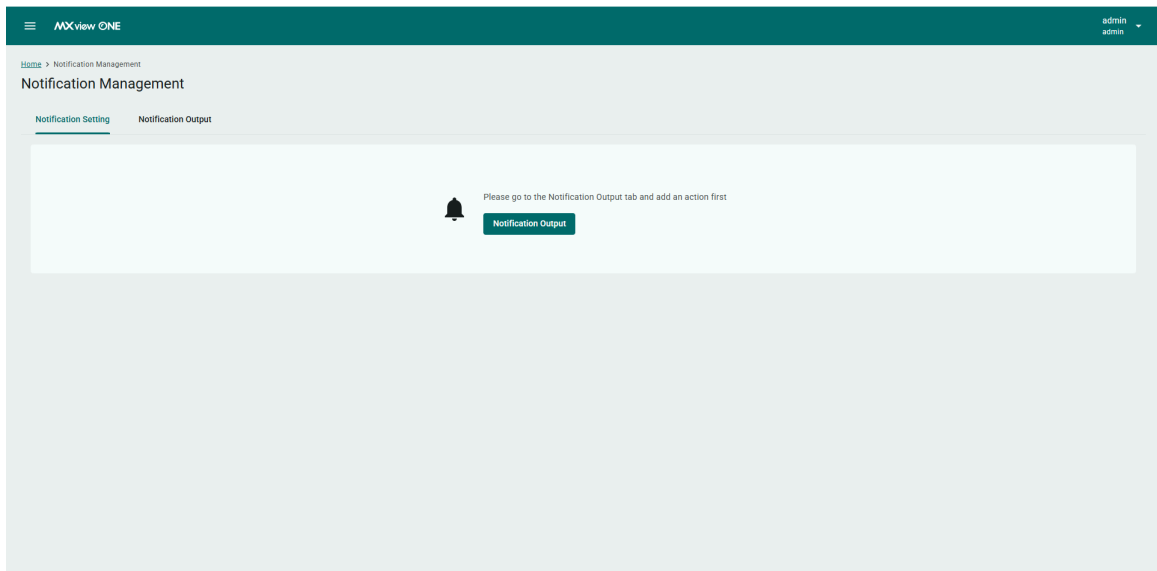
Configuring Email Server Settings

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

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

Notification Management

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



Configuring Notification Actions

Before MXview One can send notifications, you must configure notification actions that determine how notifications are sent.

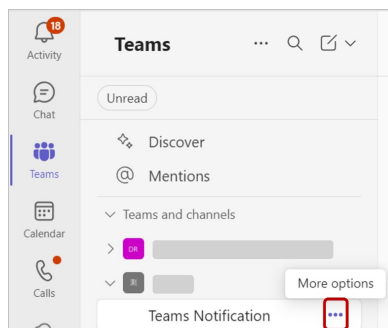
1. Navigate to **Menu** (☰) > **Notification Management**.
2. Go to the **Notification Output** tab.
3. Click the **Add** (+) icon.
4. In the **Add Notification Output** window, configure the following settings:
 - a. **Name**: Enter a name to describe the action.
 - b. **Type**: Choose the method for sending the notifications. For Microsoft Teams notifications, additional configuration is required. Refer to **Adding a Microsoft Teams Action**.
 - c. **Information**: Provide additional information required for the action, if any.
- b. Click **Add**.

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

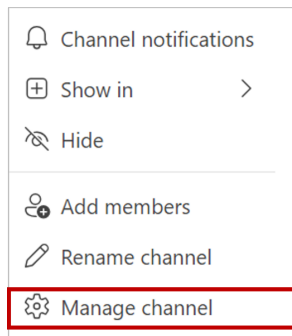
Adding a Microsoft Teams Action

MXview One can send event notifications directly to a specific Microsoft Teams channel.

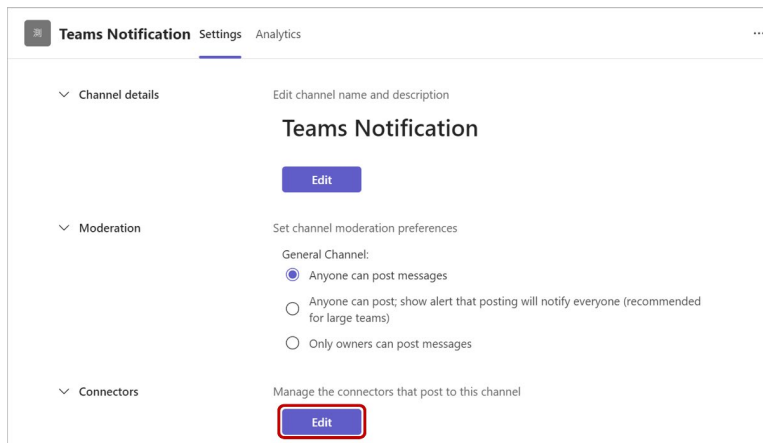
1. In Microsoft Teams, go to the channel you want to add the incoming webhook to.
2. Click **More options (...)** next to the channel name.



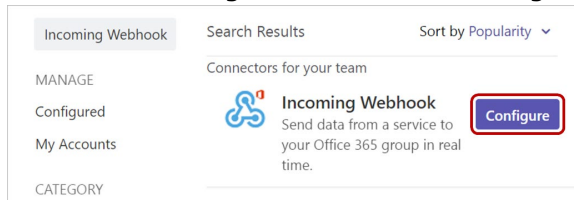
3. Select **Manage channel**.



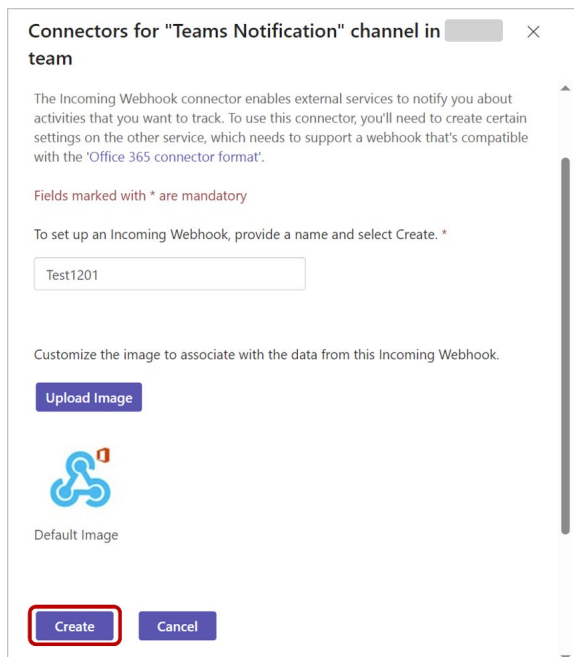
4. On the **Settings** tab, click **Edit** in the **Connectors** section.



5. Search for **Incoming Webhook** and click **Configure**.

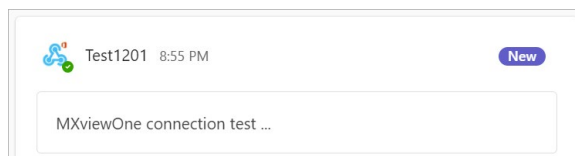


6. Enter a name for the webhook, upload a custom icon (optional), and click **Create**.



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.
11. In the **Add Notification Output** window, configure the following settings:
 - **Name:** Enter a name to describe the action.
 - **Type:** Select **Microsoft Teams**.
 - **Webhook:** Paste the URL copied from Microsoft Teams.
12. Click **Test Connection** to verify the webhook works properly.

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



13. Click **Add**.

Configuring Event Notifications

MXview One can send event notifications whenever a specific event is detected on a monitored device.



NOTE

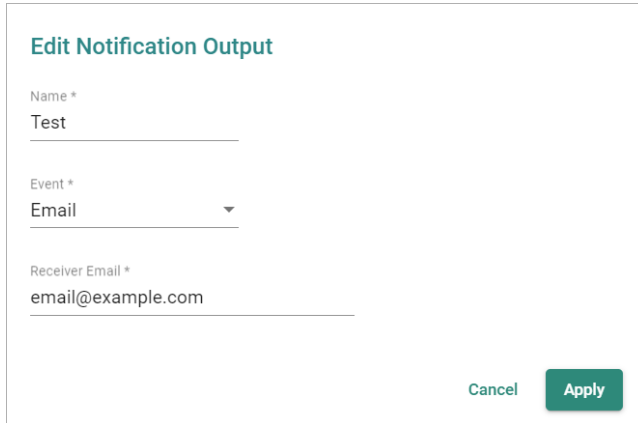
Setting up event notifications requires a configured notification action. Refer to **Configuring Notification Actions**.

1. Navigate to **Menu** (☰) > **Notification Management**.
2. Go to the **Notification Setting** tab.
3. Click the **Add** (+) icon.
4. In the **Create Notification** window, configure the following settings:
 - **Notification Name:** Enter a name for the notification.
 - **Event:** Select the event type.
 - **Registered Devices:** Select the devices to monitor.
 - **Registered Outputs:** Select a previously configured notification action MXview One will perform when the specified event is detected on the registered devices.
5. Click **Add**.

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**.
2. Go to the **Notification Output** tab.
3. To edit a registered action:
 - a. Click the **Edit** () icon next to the action you want to edit.



- b. Modify the settings. Refer to **Configuring Notification Actions**.
 - c. Click **Apply**.
4. To export data displayed on the **Notification Output** tab:
 - a. Click the **Export** () icon.
 - b. Select **Export CSV**.

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**.
2. Click the **Notification Setting** tab.
3. To edit a notification:
 - a. Click the **Edit** () icon next to the notification you want to edit.

Edit Notification

Notification Name *

Test

Event *

Device ICMP unreachable

Registered Devices *

All devices

Registered Outputs *

Test

Content

0 / 2000

Cancel Apply

- b. Modify the settings. Refer to **Configuring Event Notifications**.
- c. Click **Apply**.
4. To export data displayed on the **Notification Setting** tab:
 - a. Click the **Export** (📄) icon.
 - b. Select **Export CSV**.

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.

MXview ONE

admin

Home > Event Management > Event Settings

Event Settings

Custom Event

Cybersecurity Event

All (2)

Critical (1)

Warning (1)

Information (0)

+

📄

	Event Name	Enabled/Disabled	Condition	Description	Recovery Description	Duration	Registered Devices
☐	IpAddr	Enabled	Not Equal 192.168.123.153			0	4
☐	IpMask	Enabled	Not Equal 255.255.255.0			0	14

Items per page: 50

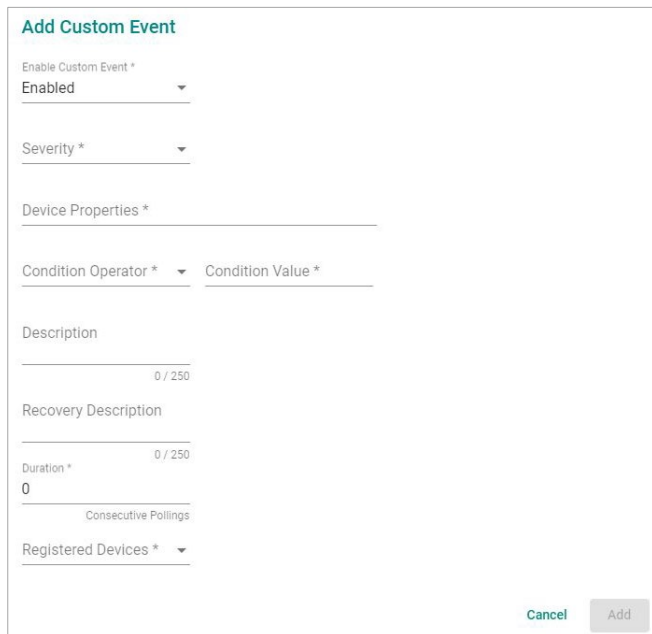
1 - 2 of 2

[< >]

Configuring Custom Events

Custom events allow you to define your own events to monitor with flexible detection thresholds, severity levels, and durations.

1. Navigate to **Menu** (☰) > **Event Management** > **Event Settings**.
2. Go to the **Custom Event** tab.
3. Click the **Add** (+) button.



4. In the **Add Custom Event** window, configure the following settings:
 - **Enable Custom Event:** Enable or disable the custom event.
 - **Severity:** Select the severity for the event.
 - **Device Properties:** Select the device property to monitor.
 - **Condition Operator:** Select the criteria operator for matching the condition value.
 - **Condition Value:** Specify the value for the criteria operator to match.
 - **Description:** Enter a description for the custom monitoring event.
 - **Recovery Description:** Enter a description of how to recover from the event.
 - **Duration:** Specify how many times an event can occur without any action being taken. If the event occurs more times than the specified duration, MXview One will send an alert.
 - **Registered Devices:** Select the devices to monitor for the custom event.
5. Click **Add**.



NOTE

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

Viewing or Exporting Custom Event Settings

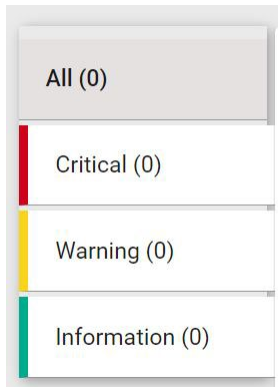
1. Navigate to **Menu** (☰) > **Event Management** > **Event Settings**.
2. Go to the **Custom Event** tab.

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

Column	Description
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 of registered devices that the event applies to

- To search for information in the table, type a full or partial string that matches the value in any of the table columns.
- To filter the information in the table by event severity, click one of the color-coded severity levels in the left-side panel.



- To sort the data in the table by a specific column, click the column heading.
- To export data displayed on the **Custom Event** tab:
 - Click the **Export** (📄) icon.
 - Select **Export CSV**.

Editing Custom Events

- Navigate to **Menu** (☰) > **Event Management** > **Event Settings**.
- Go to the **Custom Event** tab.
- Click the **Edit** (✎) icon next to the event you want to modify.
- Modify the settings. Refer to [Configuring Custom Events](#).
- Click **Apply**.

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.

Configuring the Built-in Syslog Server

- Navigate to **Menu** (☰) > **Event Management** > **Syslog Settings**.

2. Go to the **Syslog Server Settings** tab.

MXview ONE

Home > Event Management > Syslog Settings

Syslog Settings

Syslog Server Settings Syslog Viewer Syslog Forwarding

Built-in Syslog Server
Disabled

UDP Port
514

TCP Port
5143

Authentication
Disabled

Save

3. Configure the following settings:
 - **Built-in Syslog Server:** Enable or disable the built-in syslog server. When enabled, select the 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.
 - **UDP:** Specify the syslog server's UDP port. The default port number is 514.
 - **TCP:** Specify the syslog server's TCP port. The default port number is 5143.
 - **Authentication:** 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.



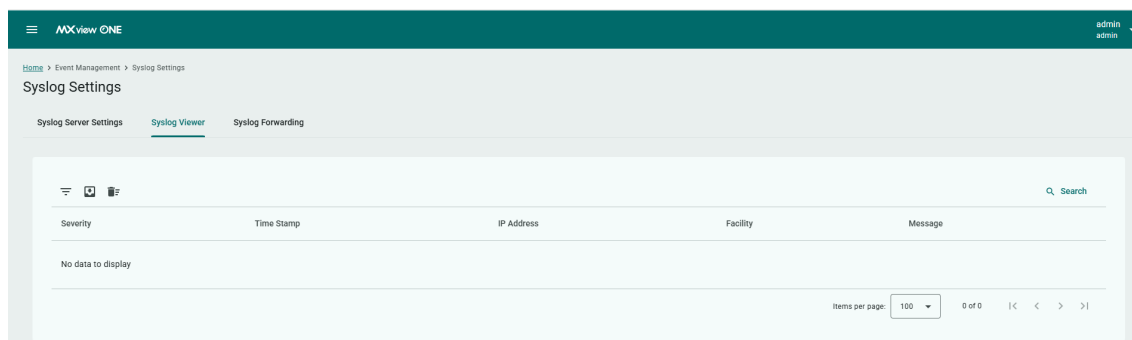
NOTE

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. 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**.
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.
4. To filter the information in the table by specific criteria:
 - a. Click the **Filter** (≡) icon in the top-left corner.

- 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.
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.
7. To clear all syslog data, click the **Clear All Events** (🗑️) icon.

Configuring 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.

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

The screenshot shows the 'Syslog Settings' page with the 'Syslog Forwarding' tab selected. The settings are as follows:

- Syslog Forwarding:** Disabled
- Protocol:** UDP
- Remote IP/Domain Name 1:** 0 / 253
- Port 1:** 514
- Remote IP/Domain Name 2:** 0 / 253
- Port 2:** 514
- Syslog Filters (1/128):**
 - Source IP:** Any IP
 - Severity:** All
- Event Log Forwarding:** Disabled
- Format:** Traditional
- Save** button

3. Configure the following settings:
 - **Syslog Forwarding:** Enable or disable syslog forwarding.
 - **Protocol:** Select the communication protocol.
 - **Authentication:** If you selected **TCP** as the **Protocol**, select an authentication method (**Disabled**, **TLS only**, **TLS + certificate**).
 - ☐ **Disabled:** Do not require authentication.
 - ☐ **TLS only:** Use TLS authentication.
 - ☐ **TLS + certificate:** Use a combination of TLS and certificates for authentication.



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.
- 4. 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.

a. 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.

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

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



NOTE

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

5. Click **Save**.

Enabling/Disabling Internal Event Forwarding

In addition to forwarding device syslog messages, you can forward internal MXview One event logs to an external SIEM over syslog.



NOTE

Since internal event forwarding reuses the same syslog destination information, this function requires Syslog forwarding to be enabled and a configured forwarding destination. Refer to **Configuring Syslog Forwarding**.

1. Navigate to **Menu** (☰) > **Event Management** > **Syslog Settings**.
2. Go to the **Syslog Forwarding** tab.
3. In the **Internal Event Forwarding** section, configure the following settings:
 - **Internal Event Forwarding:** Enable or disable forwarding internal MXview One event logs.
 - **Format:** Select the message format for forwarded logs.
 - ☐ **Traditional:** Use plain syslog text.
 - ☐ **CEF:** Use Common Event Format.
4. Click **Save**.

SNMP Trap Forwarding

MXview One can forward the SNMP traps it receives from managed devices to upstream network management or SIEM systems. With trap forwarding, your NOC or SIEM can collect alarms from all devices centrally without communicating with each device directly. You can configure up to three forwarding destinations, each with its own SNMP version and credentials. Traps can be relayed in their original form or

re-encoded to SNMPv3 to apply authentication and encryption to meet security compliance requirements such as NIS2.



NOTE

This function requires editing rights and is only available to users with **Administrator** or **Supervisor** privileges.

Enabling Trap Forwarding



NOTE

Enabling SNMP Trap forwarding requires at least one configured destination. Refer to **Adding a Destination**.

1. Navigate to **Menu** (☰) > **Event Management** > **Trap Forwarding**.
2. Select **Enable** from the **Enable Trap Forwarding** drop-down menu.
3. Click **Apply**.

Viewing the SNMPv3 EngineID

MXview One reports the SNMPv3 EngineID as the source of forwarded SNMPv3 traps and should be provided to the downstream SIEM administrator when configuring the corresponding SNMP USM user that receives the forwarded traps. The EngineID is a lowercase hexadecimal string (without a 0x prefix) and remains the same after restarts. If MXview One could not obtain the EngineID, this value will be blank.

1. Navigate to **Menu** (☰) > **Event Management** > **Trap Forwarding**.
2. The EngineID is shown in the **Polling Engine** section.
3. Click **Copy** to copy the EngineID to your clipboard.

Viewing the Destinations List

The **Destinations List** shows all configured SNMP trap forwarding destinations. You can configure up to three destinations.

Home > Event Management > Trap Forwarding

Trap Forwarding

Trap Forwarding Disabled

Apply

Polling Engine

SNMPv3 Engine ID

80001f8880a2000000df2d62ea00000000

Use this engine ID when configuring SNMPv3 USM users on downstream NMS and SIEM systems.

Copy

Destinations (1 / 3)

+

Host	Port	SNMP Version	Security
1.1.1.1	162	v1 / v2c	community: public

This page displays the following information in a table format:

Item	Description
Host	The IP address of the destination that receives the forwarded traps.
Port	The port of the destination. The default is 162.
SNMP Version	The SNMP version used to forward traps to the destination.
Security	The security settings configured for the destination, depending on the SNMP version and security mode.

Adding a Destination

- Navigate to **Menu** (☰) > **Event Management** > **Trap Forwarding**.
- In the **Destinations** section, click the **Add** (+) icon.
- Configure the basic settings:
 - **Host:** Specify the destination host address.
 - **Port:** Specify the destination port.
- Configure the SNMP version:
 - **v1 / v2c:** Forward SNMPv1/v2c traps unaltered. Also configure the following settings:
 - ☐ **Community:** Specify the SNMP community.
 - **v3:** Convert all traps to SNMPv3 before forwarding.
 - **Security Name:** Specify the SNMPv3 security name. In v1/v2c mode, the security name is optional and is used to re-encode incoming v3 traps.
- Configure the **Security Mode** (for v3 only):
 - **NoAuth:** Do not apply any authentication or encryption. For security reasons, this is not recommended.
 - **AuthNoPriv:** Apply authentication without encryption. Also configure the following settings:
 - ☐ **Authentication:** Select the cryptographic hash function.
 - ☐ **Authentication Password:** Enter the authentication password.
 - **AuthPriv:** Apply both authentication and encryption. Also configure the following settings:
 - ☐ **Authentication:** Select the cryptographic hash function.
 - ☐ **Authentication Password:** Enter the authentication password.
 - ☐ **Encryption:** Select the encryption algorithm.
 - ☐ **Encryption Password:** Enter the encryption password.
- Click **Save**.

Editing a Destination

1. Navigate to **Menu** () > **Event Management** > **Trap Forwarding**.
2. In the **Destinations** section, click the **Edit** () icon of the entry you want to edit.
3. Modify the settings as necessary. Refer to **Adding a Destination**.
4. If an authentication or encryption password is already configured, click **Change** to modify it. Click **Keep current** to retain the original password.
5. Click **Save**.

Deleting a Destination

1. Navigate to **Menu** () > **Event Management** > **Trap Forwarding**.
2. In the **Destinations** section, click the **Delete** () icon of the entry you want to delete.
3. When prompted, click **Delete**.

16. Inventory Management

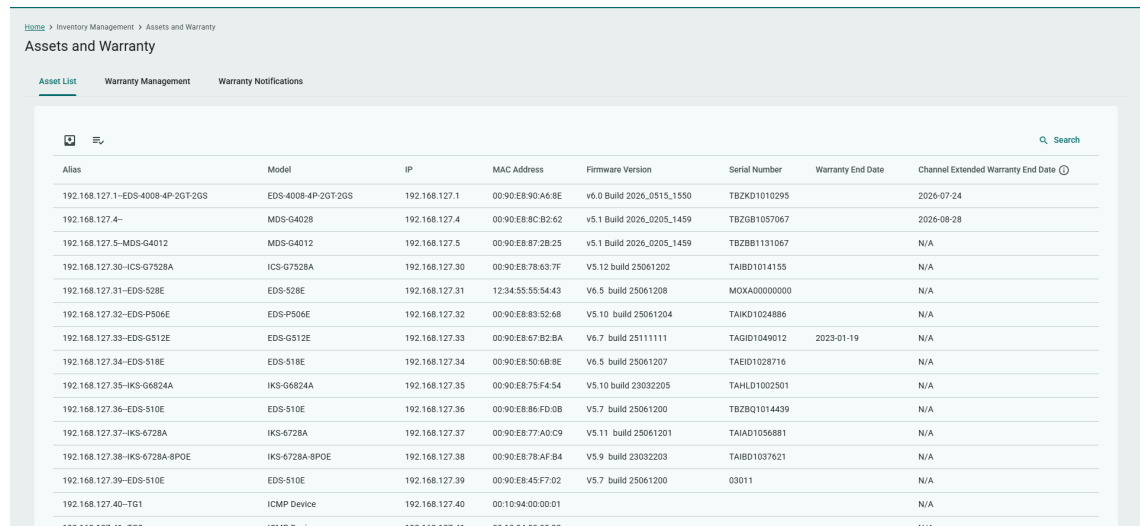
The **Inventory Management** section allows users to manage device inventory, check warranty information, and manage rogue devices.

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
192.168.127.1-EDS-4008-4P-2GT-2GS	EDS-4008-4P-2GT-2GS	192.168.127.1	00:90:E8:90:A6:8E	v6.0 Build 2026_0515_1550	TBZKD1010295		2026-07-24
192.168.127.4~	MDS-G4028	192.168.127.4	00:90:E8:8C:B2:62	v5.1 Build 2026_0205_1459	TBZGB1057067		2026-08-28
192.168.127.5-MDS-G4012	MDS-G4012	192.168.127.5	00:90:E8:87:2B:25	v5.1 Build 2026_0205_1459	TBZBB1131067		N/A
192.168.127.30-ICS-G7528A	ICS-G7528A	192.168.127.30	00:90:E8:78:63:7F	V5.12 build 25061202	TAIBD1014155		N/A
192.168.127.31-EDS-528E	EDS-528E	192.168.127.31	12:34:55:55:54:43	V6.5 build 25061208	MOXA00000000		N/A
192.168.127.32-EDS-P506E	EDS-P506E	192.168.127.32	00:90:E8:83:52:68	V5.10 build 25061204	TAIKD1024886		N/A
192.168.127.33-EDS-G512E	EDS-G512E	192.168.127.33	00:90:E8:67:B2:BA	V6.7 build 25111111	TAGID1049012	2023-01-19	N/A
192.168.127.34-EDS-518E	EDS-518E	192.168.127.34	00:90:E8:30:6B:8E	V6.9 build 25061207	TAED1028716		N/A
192.168.127.35-IKS-G6824A	IKS-G6824A	192.168.127.35	00:90:E8:75:F4:54	V5.10 build 23032205	TAHLD1002501		N/A
192.168.127.36-EDS-510E	EDS-510E	192.168.127.36	00:90:E8:86:FD:0B	V5.7 build 25061200	TBZBQ1014439		N/A
192.168.127.37-IKS-6728A	IKS-6728A	192.168.127.37	00:90:E8:77:A0:C9	V5.11 build 25061201	TAIAD1056881		N/A
192.168.127.38-IKS-6728A-8POE	IKS-6728A-8POE	192.168.127.38	00:90:E8:78:AF:B4	V5.9 build 23032203	TAIBD1037621		N/A
192.168.127.39-EDS-510E	EDS-510E	192.168.127.39	00:90:E8:45:F7:02	V5.7 build 25061200	03011		N/A
192.168.127.40-TG1	ICMP Device	192.168.127.40	00:10:94:00:00:01				N/A
192.168.127.41-TG2	ICMP Device	192.168.127.41	00:10:94:00:00:02				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

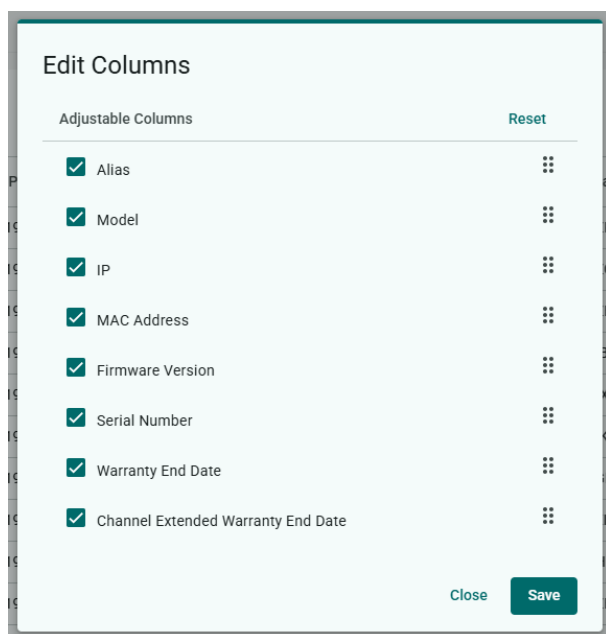
1. Navigate to **Menu** (☰) > **Inventory Management** > **Assets and Warranty**.
2. Go to the **Asset List** tab.
3. In the **Search** (🔍) field, type the full or partial information.
All items matching the entered string will be shown in the table.

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.



4. Check or uncheck the box next to the column value to show or hide the column.
 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: 2026-05-20 18:37:49 UTC+08:00

Retrieve Data

Manually Check Warranty

Serial Number Serial Number

0 / 12

Check

Alias	IP	MAC Address	Serial Number	Warranty Duration	Warranty Start Date	Warranty End Date	Channel Extended Warranty End Date	Warranty Status
192.168.127.1-EDS-4008-4P-2GT-2GS	192.168.127.1	00:90:E8:90:A6:8E	TBZKD1010295		2021-01-13		2026-07-24	Expired
192.168.127.4-	192.168.127.4	00:90:E8:8C:82:62	TBZGB1057067				2026-08-28	Expires soon
192.168.127.5-MDS-G4012	192.168.127.5	00:90:E8:87:2B:25	TBZBB1131067		2020-04-16		N/A	N/A
192.168.127.30-ICS-G7528A	192.168.127.30	00:90:E8:78:63:7F	TAIBD1014155		2020-03-25		N/A	N/A
192.168.127.31-EDS-528E	192.168.127.31	12:34:55:55:54:43	MOXA00000000				N/A	N/A
192.168.127.32-EDS-P506E	192.168.127.32	00:90:E8:83:52:68	TAIKD1024886		2020-03-25		N/A	N/A
192.168.127.33-EDS-G512E	192.168.127.33	00:90:E8:67:82:BA	TAGID1049012	61	2017-12-19	2023-01-19	N/A	Expired

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 below 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**.



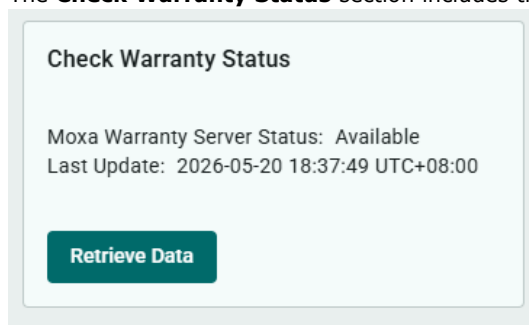
NOTE

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:



Check Warranty Status

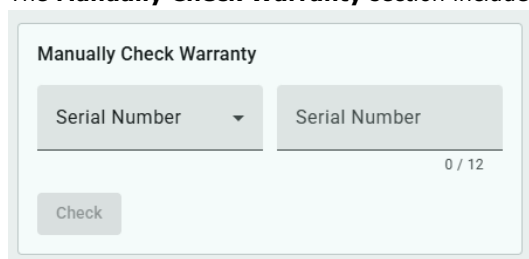
Moxa Warranty Server Status: Available
Last Update: 2026-05-20 18:37:49 UTC+08:00

Retrieve Data

- **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:



Manually Check Warranty

Serial Number Serial Number 0 / 12

Check

- **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

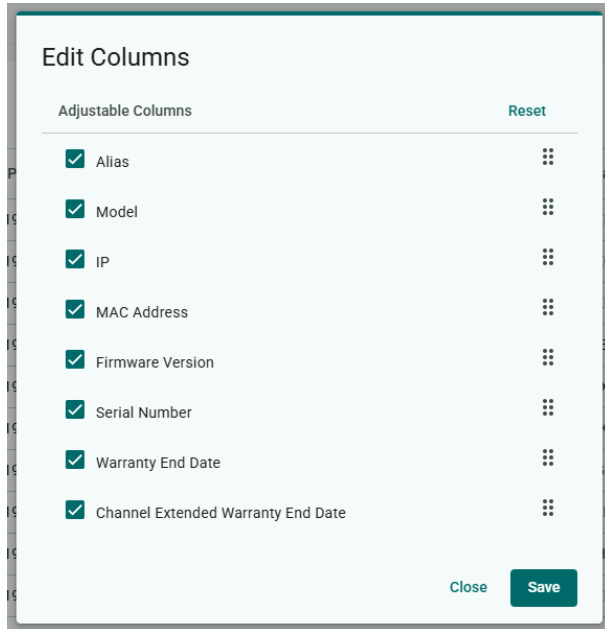
1. Navigate to **Menu** (☰) > **Inventory Management** > **Assets and Warranty**.
2. Go to the **Warranty Management** tab.
3. In the **Search** (🔍) field, type the full or partial information.
All items matching the entered string will be shown in the table.

Exporting the Warranty Management List

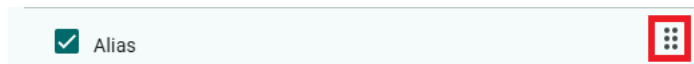
1. Navigate to **Menu** (☰) > **Inventory Management** > **Assets and Warranty**.
2. Go to the **Warranty Management** tab.
3. Click the **Export** (📄) icon in the top-left corner of the table.
MXview One exports the warranty management table as a CSV file.

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. Check or uncheck the box next to the column value to show or hide the column.
5. To change the column order:
 - a. Click and drag the **Drag** (⋮) icon of the column you want to move.



6. To revert all changes to column visibility and order, click **Reset**.
7. Click **Save**.

Editing the Channel Extended Warranty End Date

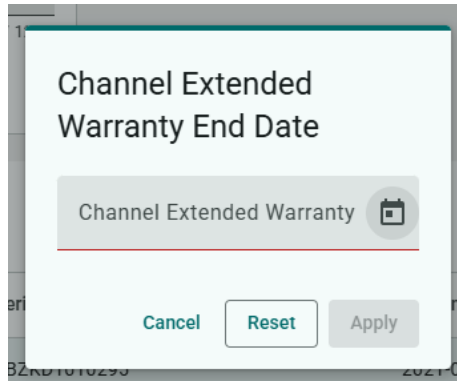
1. Navigate to **Menu** (☰) > **Inventory Management** > **Assets and Warranty**.
2. Go to the **Warranty Management** tab.
3. Check the box of the device(s) you want to edit the Channel Extended Warranty End Date for.
4. Click the **Edit** (✎) icon in the **Channel Extended Warranty End Date** column of the device you want to edit.

☒	Alias	IP	MAC Address	Serial Number	Warranty Duration	Warranty Start Date	Warranty End Date	Channel Extended Warranty End Date	Warranty Status
☒	192.168.127.1-EDS-4008-4P-2GT-2GS	192.168.127.1	00:90:E8:90:A6:BE	TBZKD1010295		2021-01-13		 2026-07-24	Expired
☐	192.168.127.4-	192.168.127.4	00:90:E8:8C:B2:62	TBZGB1057067				 2026-08-28	Expires soon

If you selected multiple devices, click the **Edit** (✎) icon in the top-left corner of the page.

	Alias	IP	MAC Address	Serial Number	Warranty Duration	Warranty Start Date	Warranty End Date	Channel Extended Warranty End Date	Warranty Status
☒	192.168.127.1-EDS-4008-4P-2GT-2GS	192.168.127.1	00:90:E8:90:A6:BE	TBZKD1010295		2021-01-13		 2026-07-24	Expired
☐	192.168.127.4-	192.168.127.4	00:90:E8:8C:B2:62	TBZGB1057067				 2026-08-28	Expires soon

The **Channel Extended Warranty End Date** window will appear.



5. To update the channel extended warranty end date:
 - a. Click the **Calendar** (📅) icon to select the new warranty end date.
 - b. Click **Apply**.
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**.

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.

Creating a Device Baseline

1. Navigate to **Menu** (☰) > **Inventory Management** > **Rogue Device Detection**.
2. Go to the **Rogue Device Settings** tab.
3. In the **Device Baseline** section, click **Create**.

4. When prompted, click **Create**.
MXview One will create a baseline of the currently monitored devices and enable the **Rogue Device Detection** function.

Enabling/Disabling Rogue Device Detection

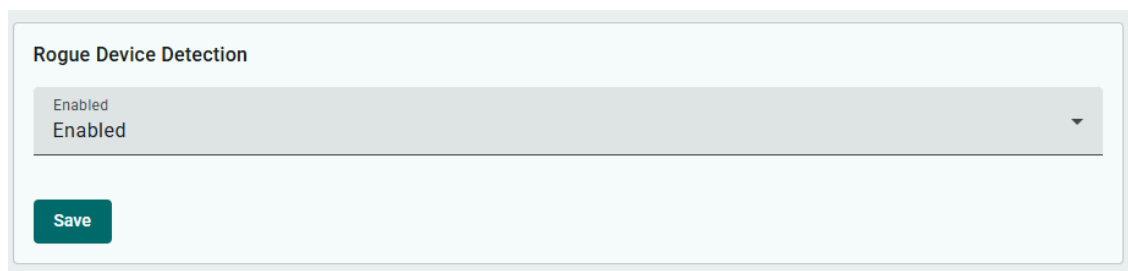


NOTE

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

Save

- **Enabled:** Enable or disable the Rogue Device Detection function.

4. Click **Save**.



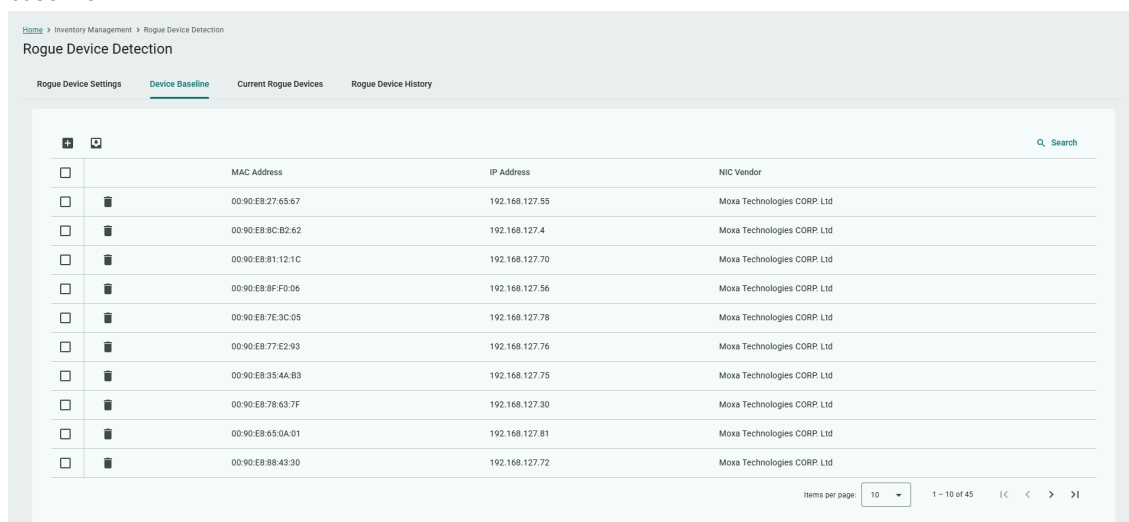
NOTE

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.



Home > Inventory Management > Rogue Device Detection

Rogue Device Detection

Rogue Device Settings **Device Baseline** Current Rogue Devices Rogue Device History

	MAC Address	IP Address	NIC Vendor
☐	00:90:E8:27:65:67	192.168.127.55	Moxa Technologies CORP. Ltd
☐	00:90:E8:8C:82:62	192.168.127.4	Moxa Technologies CORP. Ltd
☐	00:90:E8:81:12:1C	192.168.127.70	Moxa Technologies CORP. Ltd
☐	00:90:E8:8F:F0:06	192.168.127.56	Moxa Technologies CORP. Ltd
☐	00:90:E8:7E:3C:05	192.168.127.78	Moxa Technologies CORP. Ltd
☐	00:90:E8:77:62:93	192.168.127.76	Moxa Technologies CORP. Ltd
☐	00:90:E8:35:4A:B3	192.168.127.75	Moxa Technologies CORP. Ltd
☐	00:90:E8:78:63:7F	192.168.127.30	Moxa Technologies CORP. Ltd
☐	00:90:E8:65:0A:01	192.168.127.81	Moxa Technologies CORP. Ltd
☐	00:90:E8:88:43:30	192.168.127.72	Moxa Technologies CORP. Ltd

Items per page: 10 1 - 10 of 45

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.
3. To delete a single device:
 - a. Click the **Delete** () icon next to the device you want to delete from the baseline.
 - b. When prompted, click **Delete**.
4. 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.
 - c. When prompted, 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.

Home > Inventory Management > Rogue Device Detection

Rogue Device Detection

Rogue Device Settings Device Baseline **Current Rogue Devices** Rogue Device History

Q Search

	MAC Address	IP Address	First Seen	Last Seen	Connected Switch/Port	NIC Vendor
☐	00:01:02:03:04:05	192.168.127.50	2026-07-31 PM 05:49:49	2026-08-28 PM 05:19:34	192.168.127.57/Port15	3com
☐	00:90:E8:7A:01:9A	192.168.127.51	2026-08-04 PM 02:42:45	2026-08-28 PM 05:19:34	192.168.127.50/Port14	Moxa Technologies CORP. Ltd
☐	00:10:94:00:00:01	192.168.127.40	2026-08-06 PM 04:12:45	2026-08-28 PM 05:19:32	192.168.127.121/Port2	Performance Analysis Broadband, Spirent plc
☐	00:90:E8:65:0A:06	192.168.127.81	2026-08-04 PM 04:06:28	2026-08-28 PM 05:19:32	192.168.127.121/Port2	Moxa Technologies CORP. Ltd
☐	00:90:E8:EC:27:4E	192.168.127.254	2026-07-31 PM 05:49:36	2026-08-28 PM 05:19:24	192.168.127.101/Port9	Moxa Technologies CORP. Ltd
☐	00:1B:21:64:73:6B	192.168.127.100	2026-07-31 PM 05:49:22	2026-08-28 PM 05:19:21	192.168.127.57/Port15	Intel Corporate
☐	00:90:E8:87:80:7B	192.168.127.57	2026-07-31 PM 05:49:34	2026-08-28 PM 05:19:20	192.168.127.58/Port15	Moxa Technologies CORP. Ltd
☐	00:90:E8:90:A6:1C	192.168.127.59	2026-07-31 PM 05:49:34	2026-08-28 PM 05:19:20	192.168.127.58/Port16	Moxa Technologies CORP. Ltd
☐	00:0C:29:AC:60:2D	192.168.127.195	2026-08-21 PM 03:35:09	2026-08-28 PM 05:19:17	192.168.127.57/Port15	Vmware Inc
☐	00:0C:29:DA:F4:6E	192.168.127.161	2026-08-21 PM 02:08:34	2026-08-28 PM 05:19:17	192.168.127.57/Port15	Vmware Inc
☐	00:90:E8:36:47:3A	192.168.127.58	2026-08-04 PM 02:43:16	2026-08-28 PM 05:19:17	192.168.127.57/Port15	Moxa Technologies CORP. Ltd
☐	CC:96:E5:50:3F:18	192.168.127.180	2026-07-31 PM 05:49:30	2026-08-28 PM 05:19:17	192.168.127.57/Port15	Dell 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.

- Click the **Add** (+) icon next to the rogue device you want to add to the baseline.

	MAC Address	IP Address	First Seen	Last Seen	Connected Switch/Port	NIC Vendor
☒	00:01:02:03:04:05	192.168.127.50	2026-07-31 PM 05:49:49	2026-08-28 PM 05:19:34	192.168.127.57/Port15	3com
☒	00:90:E8:7A:01:9A	192.168.127.51	2026-08-04 PM 02:42:45	2026-08-28 PM 05:19:34	192.168.127.50/Port4	Moxa Technologies CORP. Ltd

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.

	MAC Address	IP Address	First Seen	Last Seen	Connected Switch/Port	NIC Vendor
☒	00:01:02:03:04:05	192.168.127.50	2026-07-31 PM 05:49:49	2026-08-28 PM 05:19:34	192.168.127.57/Port15	3com
☒	00:90:E8:7A:01:9A	192.168.127.51	2026-08-04 PM 02:42:45	2026-08-28 PM 05:19:34	192.168.127.50/Port4	Moxa Technologies CORP. Ltd

- When prompted, click **Add**.

Exporting the Current Rogue Devices List

- Navigate to **Menu** (☰) > **Inventory Management** > **Rogue Device Detection**.
- Go to the **Current Rogue Devices** tab.
- 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.

Sequence No.	MAC Address	IP Address	First Seen	Last Seen	NIC Vendor
15	00:90:E8:90:A6:90	192.168.127.1	2026-07-31 PM 05:50:00	2026-08-28 PM 05:15:23	Moxa Technologies CORP. Ltd
14	A8:E7:7D:E5:1B:04		2026-07-31 PM 05:50:41	2026-08-28 PM 05:15:13	Texas Instruments
13	A8:E7:7D:E4:FE:18		2026-08-07 PM 05:38:36	2026-08-28 PM 05:08:15	Texas Instruments
12	B4:32:A9:97:7A:84		2026-07-31 PM 05:49:34	2026-08-28 PM 04:58:16	Texas Instruments
11	B4:32:A9:98:11:B6		2026-07-31 PM 06:40:39	2026-08-28 PM 04:56:48	Texas Instruments
10	A8:E7:7D:E6:96:D8		2026-07-31 PM 06:40:34	2026-08-28 PM 04:43:27	Texas Instruments
9	B4:32:A9:95:3C:44		2026-07-31 PM 06:10:16	2026-08-28 PM 04:36:17	Texas Instruments
8	00:90:E8:8C:82:63	192.168.127.4	2026-07-31 PM 05:49:22	2026-08-26 PM 05:43:48	Moxa Technologies CORP. Ltd
7	00:90:E8:8C:82:64	192.168.127.4	2026-08-03 PM 06:56:15	2026-08-25 PM 06:30:42	Moxa Technologies CORP. Ltd

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.
4. When prompted, click **Delete**.

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 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.



NOTE

When upgrading MXview One, you can choose to retain the existing database backup files. If retained, the backup files will be added to the **Historical backups** list after the upgrade. If not retained, no backup record will be kept.

1. In MXview One Control Panel, navigate to **DB Backup & Restore** and go to the **Backup** tab.

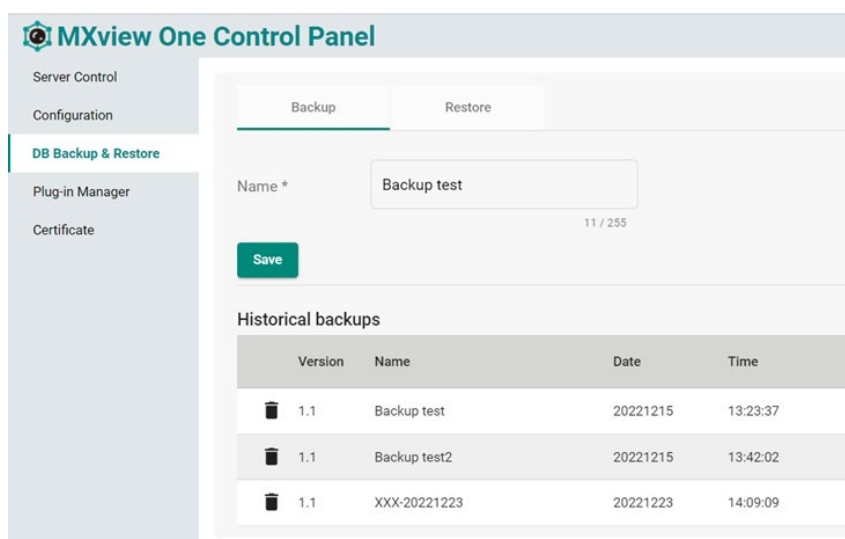
The screenshot shows the MXview One Control Panel interface. On the left is a sidebar with navigation links: Server Control, Configuration, DB Backup & Restore (highlighted), Plug-in Manager, and Certificate. The main content area has two tabs: 'Backup' (active) and 'Restore'. Under the 'Backup' tab, there is a form with a 'Name *' label, a text input field, and a 'Save' button. A character count '0 / 255' is visible next to the input field.

2. Choose the **Backup** tab to start the process of backing up the database.
3. Specify the name for the backup file.
4. Click **Save**.

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\██████████\AppData\Roaming\moxa\mxview
one\db_backup\20230709_120518

5. A record will show in the **Historical backups** list.



Backing Up Device Configurations

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

1. Navigate to **Menu** (☰) > **Device Configuration Center**.
2. Go to the **Backup** tab.
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**.
4. To back up configurations from specific devices:
 - a. For a single device, click the **Backup** (📁) next to the selected device.
 - b. For multiple devices, select the devices and click the **Backup** (📁) icon in the upper left corner of the screen.
 - c. In the **Back Up Configuration** window, 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. Refer to **Comparing Archived Configuration Files**.



NOTE

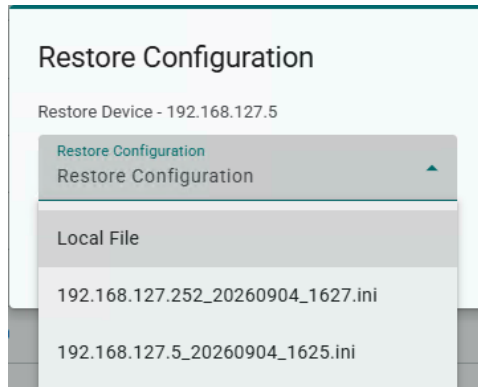
If MXview One compares two configuration files and they are the same, it will only leave the latest one. If the two configuration files are different, MXview One will keep both in the **Records** tab.

Restoring Device Configurations

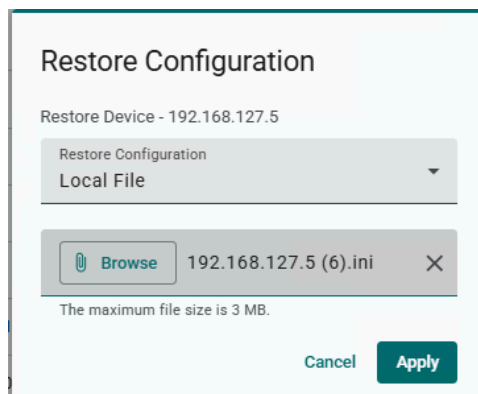
Use the **Configuration Center** screen to restore configurations to one or more devices by restoring an archived configuration from the MXview One server or importing a local configuration backup file (in INI format).

1. Navigate to **Menu** (☰) > **Device Configuration Center**.

2. Go to the **Restore** tab.
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**.
4. 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**.
 - b. From the **Restore Configuration** drop-down list, select the archived device configuration to restore.



- c. Click **Apply**.
MXview One imports the configuration file to the selected device.
5. 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**.
 - b. From the **Restore Configuration** drop-down list, select **Local File**.
 - c. Click the **Configuration File** field to browse to the local configuration file.

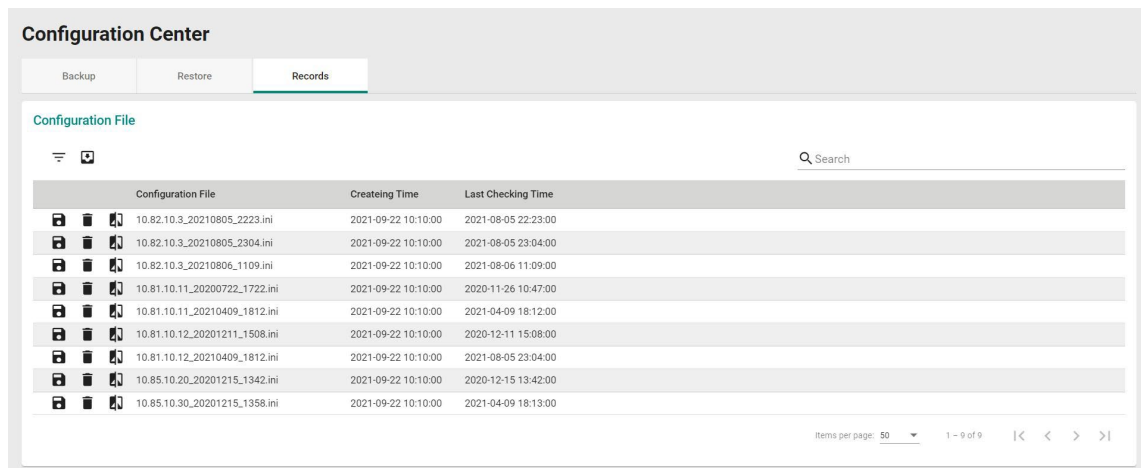


- d. Click **Apply**.

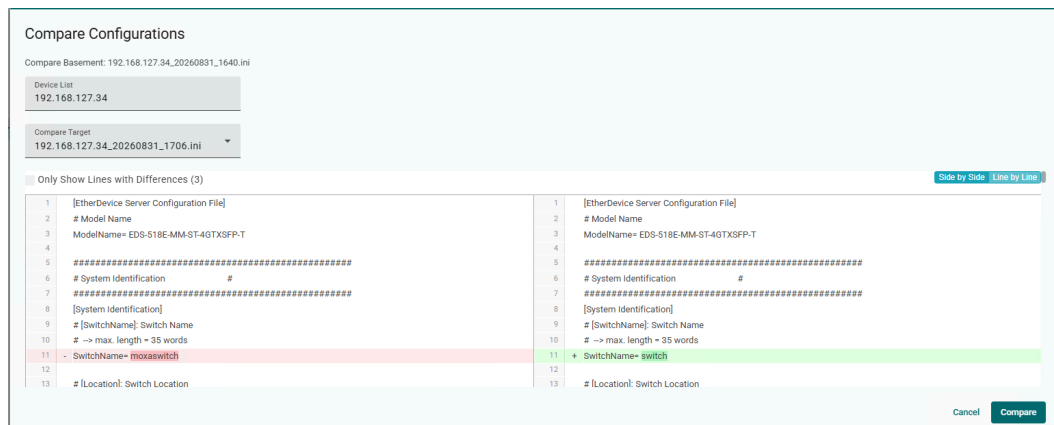
Comparing Archived Configuration Files

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

1. Navigate to **Menu** (≡) > **Device Configuration Center**.
2. Go to the **Records** tab.



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. Click the **Compare** (🔍) icon next to the configuration file you want to compare.
5. Select the device from the **Device List** drop-down list.
6. Select the target configuration file to compare from the **Compare Target** drop-down list.
7. Click **Compare**. Any inserted, deleted, and modified lines in the configuration will be where red lines indicate the source configuration and green lines indicate the target configuration.



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**.
2. (Optional) Search a previously saved scheduled job, type a job name in the search box.
3. Click the **Add** (+) button.
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.

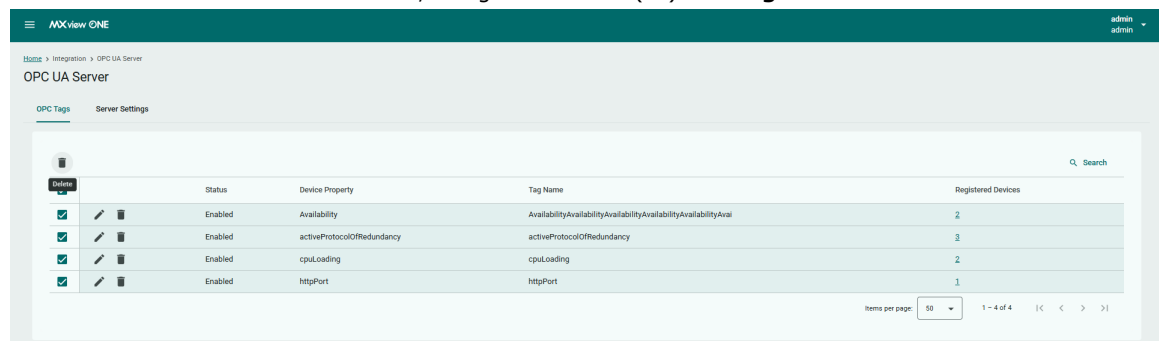
18. Custom Integrations

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

OPC UA Server Overview

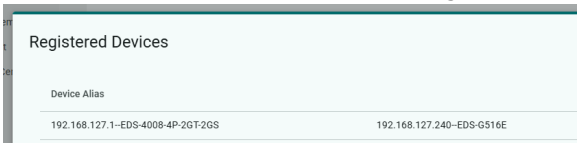
MXview One supports integrated OPC UA Server functionality to integrate with OPC clients such as SCADA systems. From this section, users can configure OPC tags and server settings.

To access the **OPC UA Server** screen, navigate to **Menu** (☰) > **Integration** > **OPC UA Server**.



Viewing the OPC Tags Table

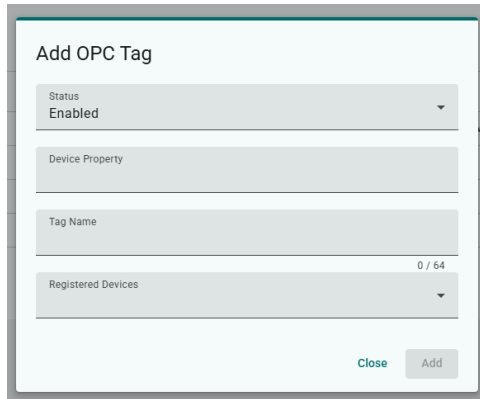
1. Navigate to **Menu** (☰) > **Integration** > **OPC UA Server**.
2. Go to the **OPC Tags** tab.
3. The OPC tags table includes the following information:

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. 

Adding an OPC Tag

1. Navigate to **Menu** (☰) > **Integration** > **OPC UA Server**.
2. Go to the **OPC Tags** tab.

3. Click the **Add** (+) icon.



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**.

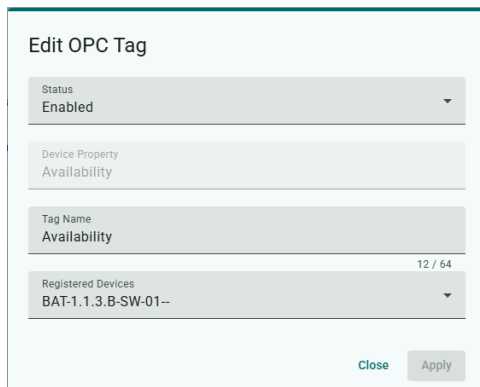


NOTE

MXview One supports a maximum of 2000 OPC tags and up to 4000 registered devices per tag.

Editing an OPC Tag

1. Navigate to **Menu** (☰) > **Integration** > **OPC UA Server**.
2. Go to the **OPC Tags** tab.
3. Click on the **Edit** (✎) icon next to the tag you want to edit.



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**.

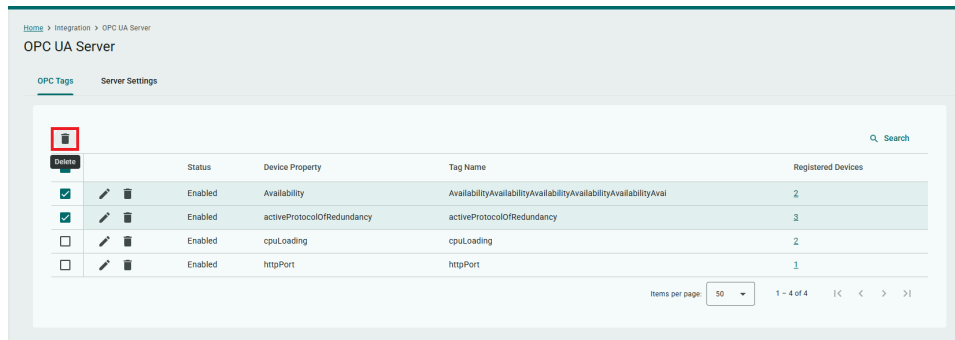
Deleting an OPC Tag

1. Navigate to **Menu** (☰) > **Integration** > **OPC UA Server**.
2. Go to the **OPC Tags** tab.

3. Click the **Delete** () icon next to the tag you want to delete.
4. When prompted, click **Delete**.

Deleting Multiple OPC Tags

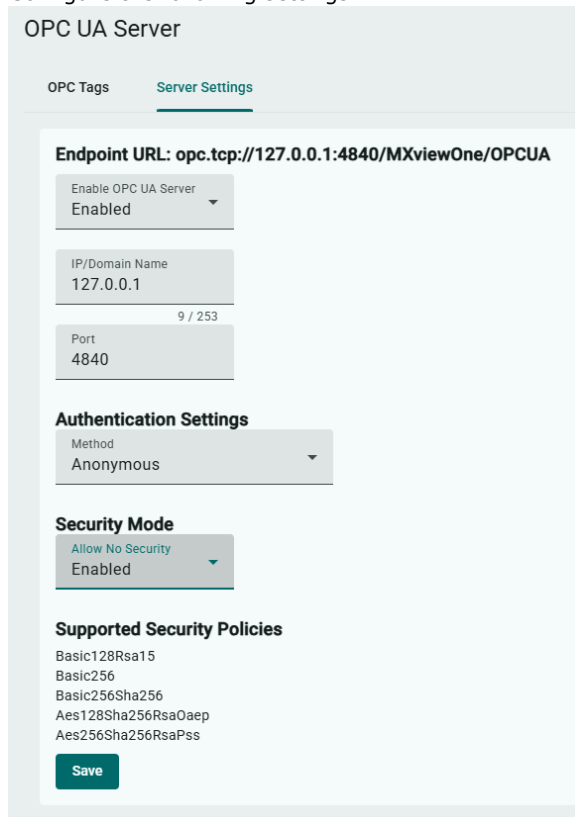
1. Navigate to **Menu** () > **Integration** > **OPC UA Server**.
2. Go to the **OPC Tags** tab
3. Select the checkbox of the OPC tags you want to delete in the list.
4. Click the **Delete** () icon at the top of the page.



5. When prompted, click **Delete**.

Configuring OPC UA Server Settings

1. Navigate to **Menu** () > **Integration** > **OPC UA Server**.
2. Go to the **Server Settings** tab.
3. Configure the following settings:



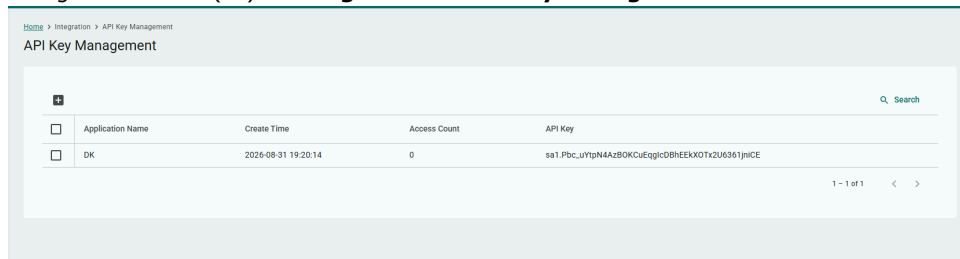
- **Enable OPC UA Server:** Enable or disable OPC UA server functionality.

- **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.
4. Click **Save**.

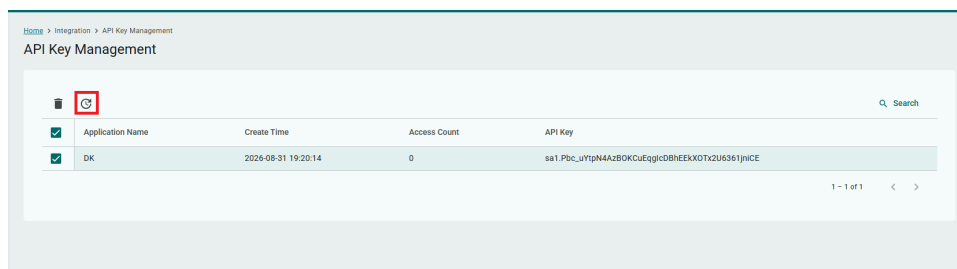
Managing RESTful API Keys

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**.



2. (Optional) Search the list of applications, type a string in the search box.
3. To add a new API key for an application:
- Click the **Add** (+) icon in the top-left corner of the screen.
 - In the **Add New Token** window, specify an **Application Name**.
 - Click **Add**.
4. To regenerate an API key for an existing application:
- Select the check box next to the application you want to regenerate the API key for.
 - Click the **Regenerate the API Key** (↻) icon.



NOTE

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

5. To delete an application:
- Select the check box next to the **Application Name**.
 - Click the **Delete** (🗑️) icon in the top-left corner of the screen.



NOTE

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

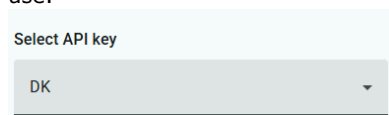
- To view API reference documentation, navigate to **Menu** (☰) > **Help** > **API Documentation**. On the **Moxa One API** page, click **API user guide** to find the guidelines for using the RESTful API functions.



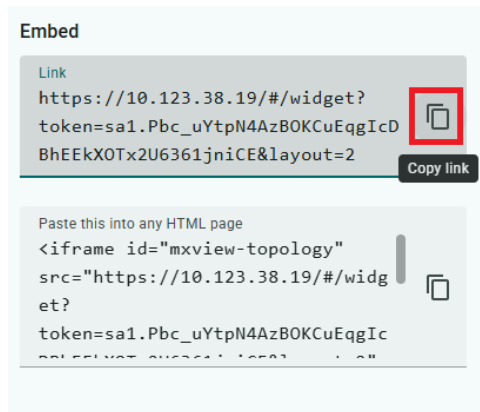
Embedding Web Widgets

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

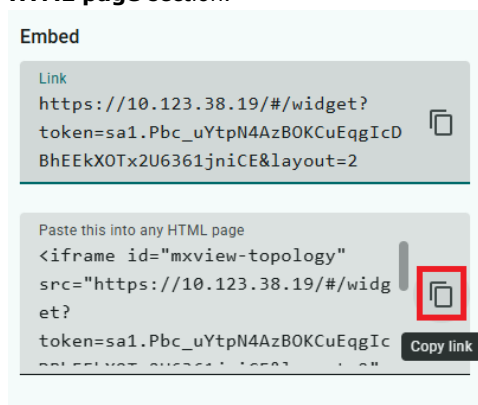
- Navigate to **Menu** (☰) > **Integration** > **Embedded Web Widget**.
- From the **Select API Key** drop-down list, select the **Application Name** for the API key you want to use.



- 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
- Copy and paste the widget link for the target application:
 - To embed the widget in a web application, click the **Copy link** (📄) icon in the **Link** section.



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



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

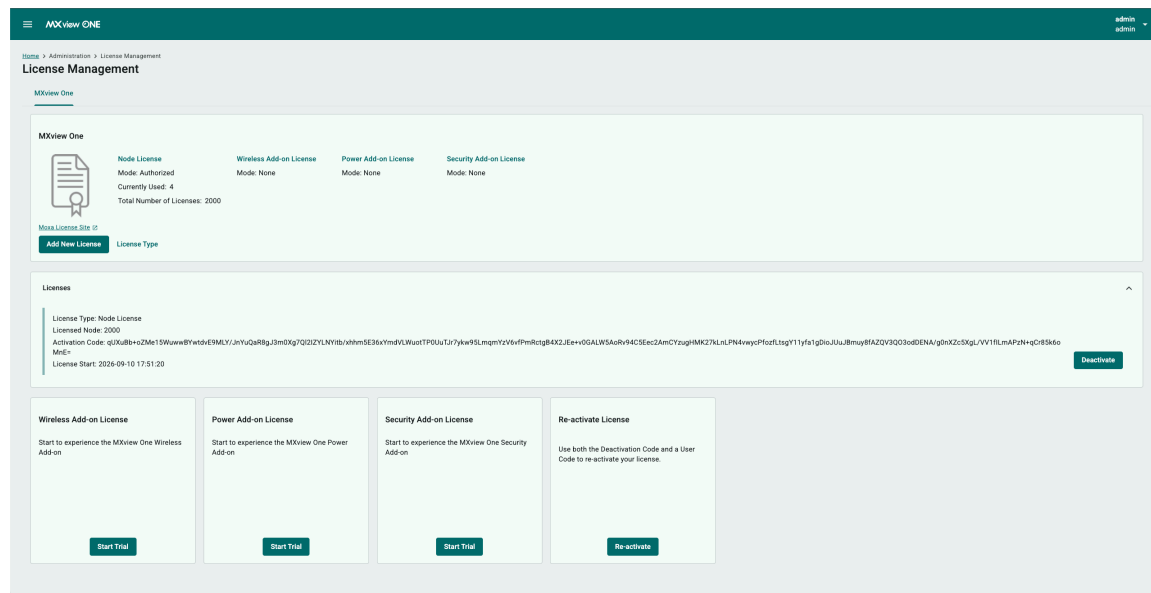
Supported Devices

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.



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 Wireless Add-on features.

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



NOTE

Activate the Node-based License first before activating 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**.

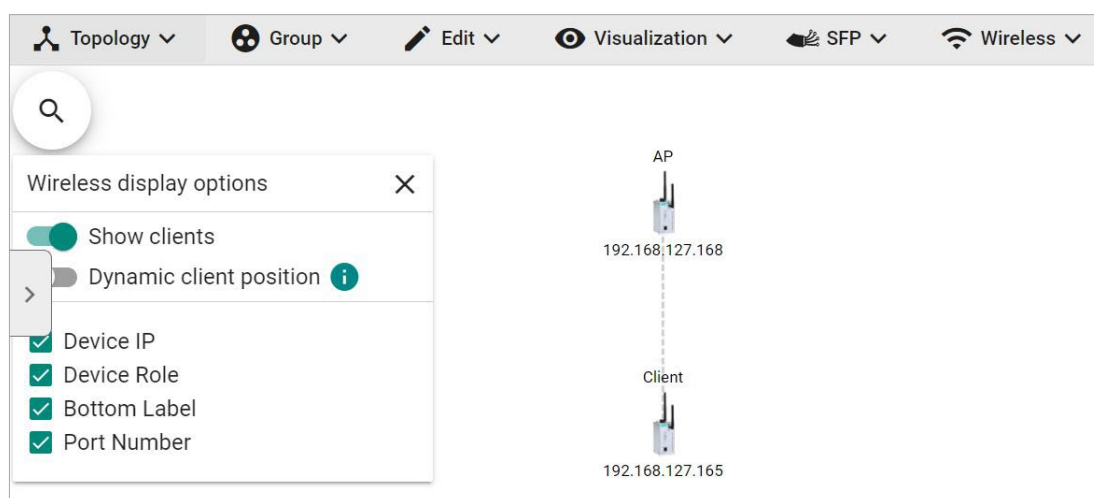
Dynamic Wireless Client Roaming

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.

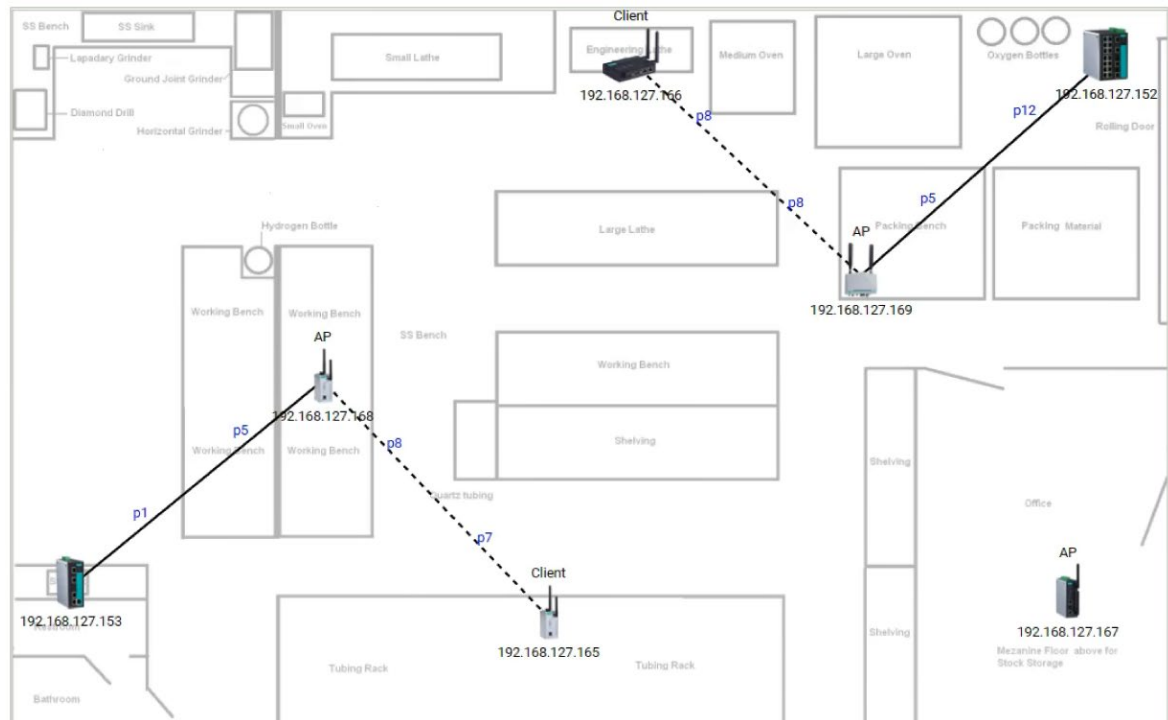
Refer to the table below for a description of each display option.

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

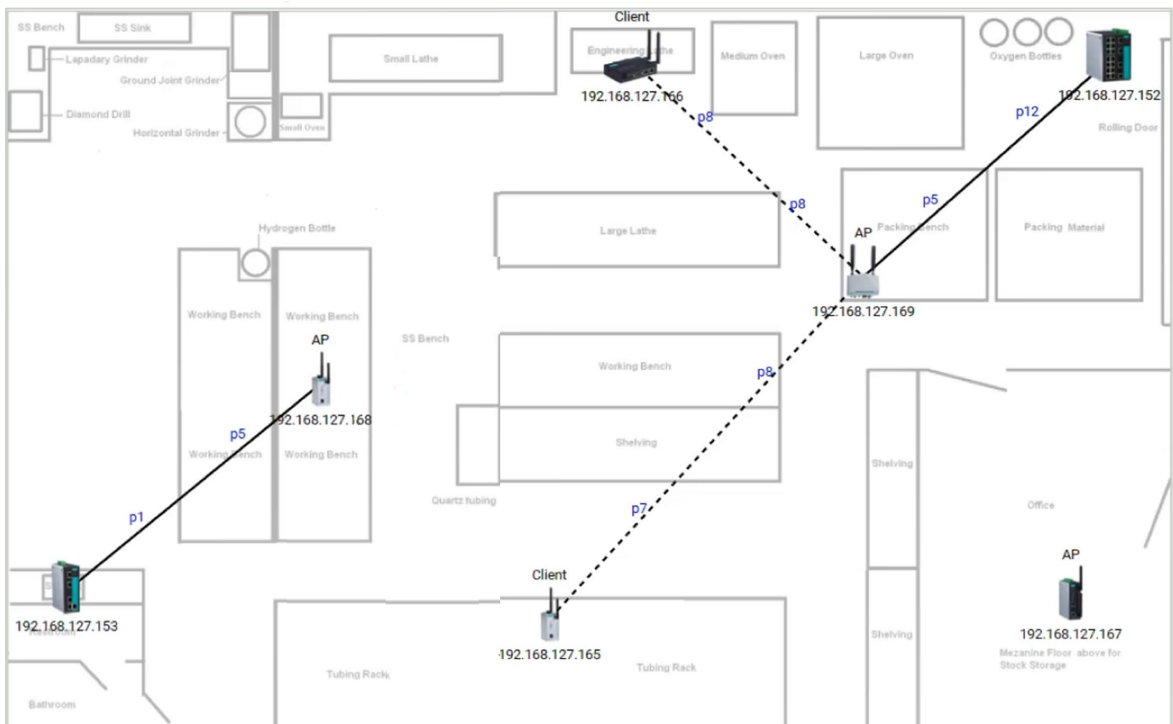


The following diagrams are an example of the dynamic roaming display showing dynamic client-AP link changes.

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



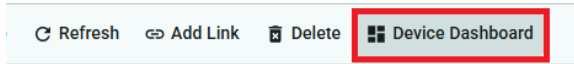
When the client roams to another AP, MXview One will automatically redraw the link to the new AP on the wireless topology diagram.



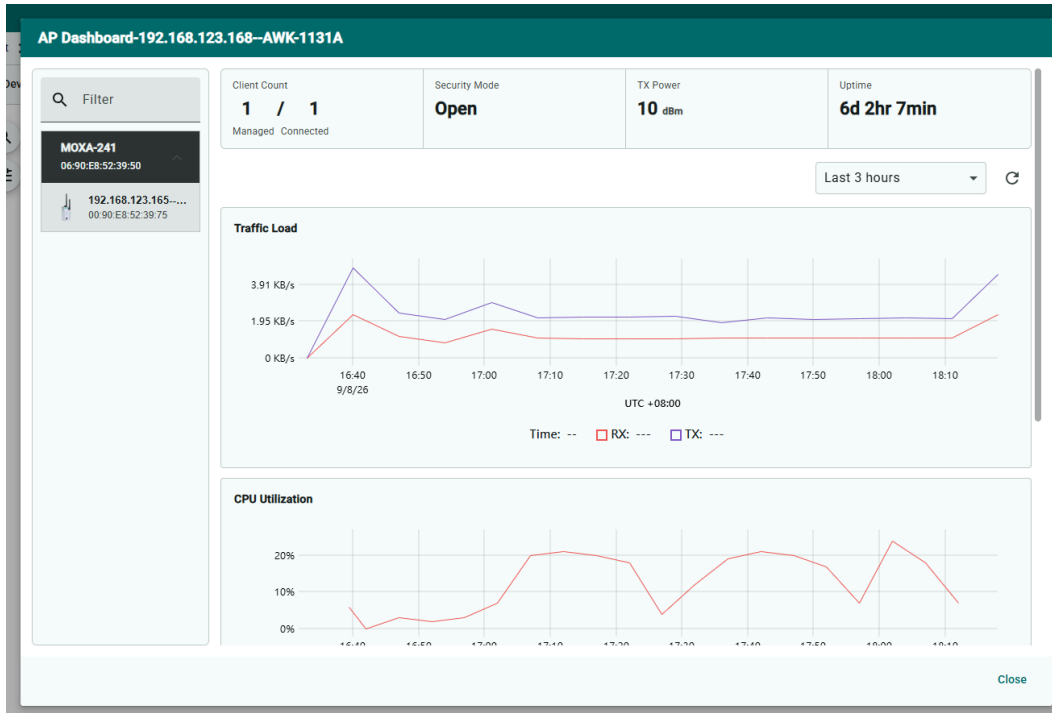
AP/Client Device Dashboard

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.



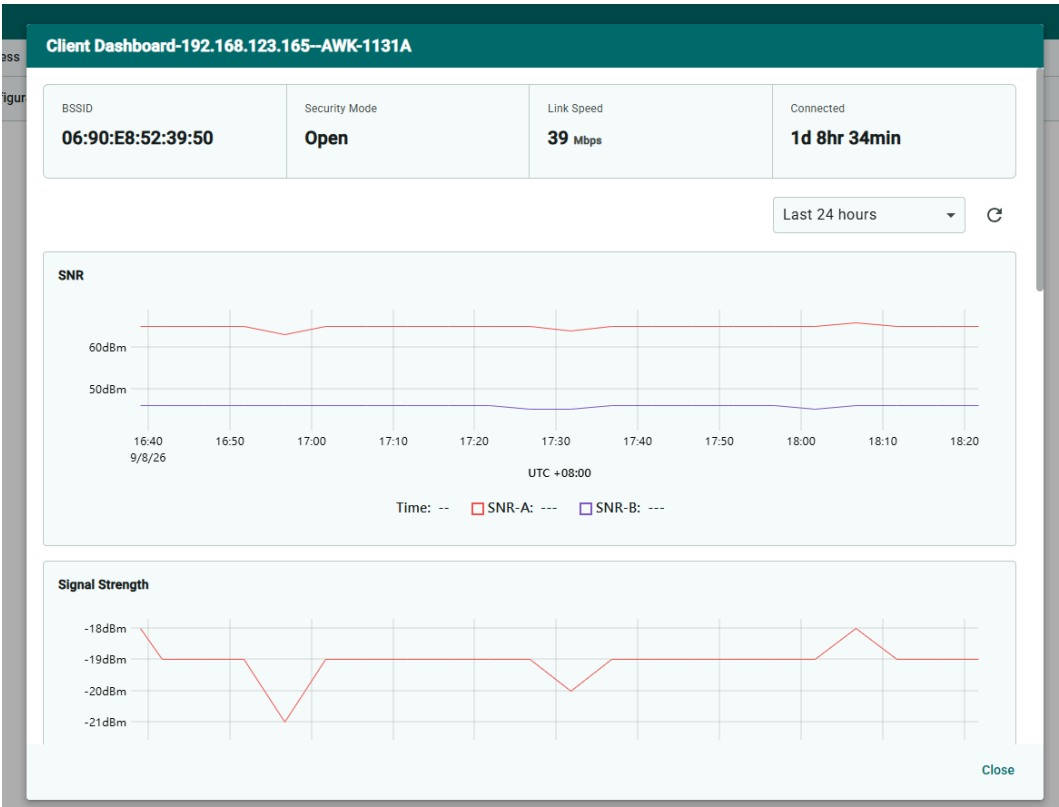
AP Device Dashboard



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)

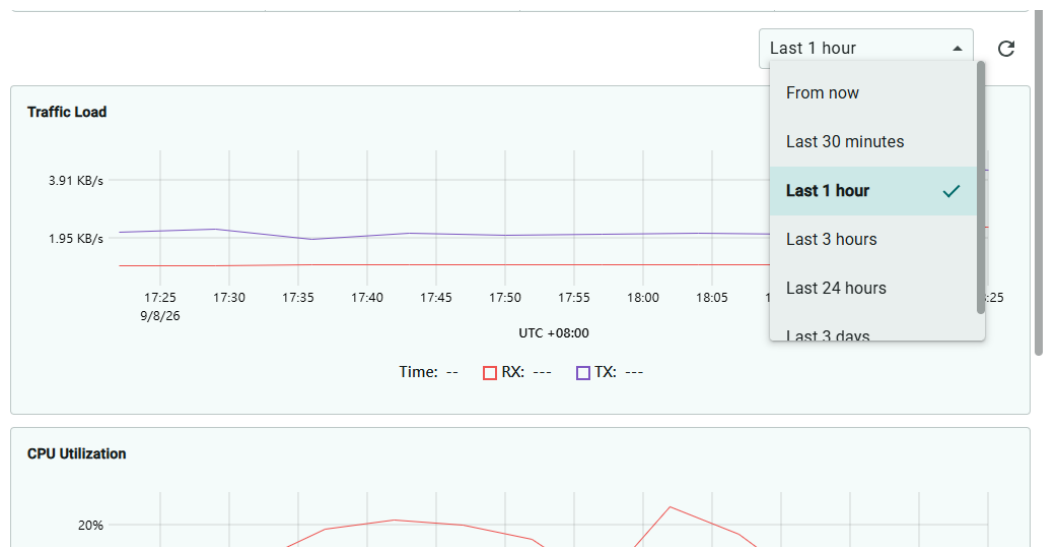
Client Device Dashboard



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.

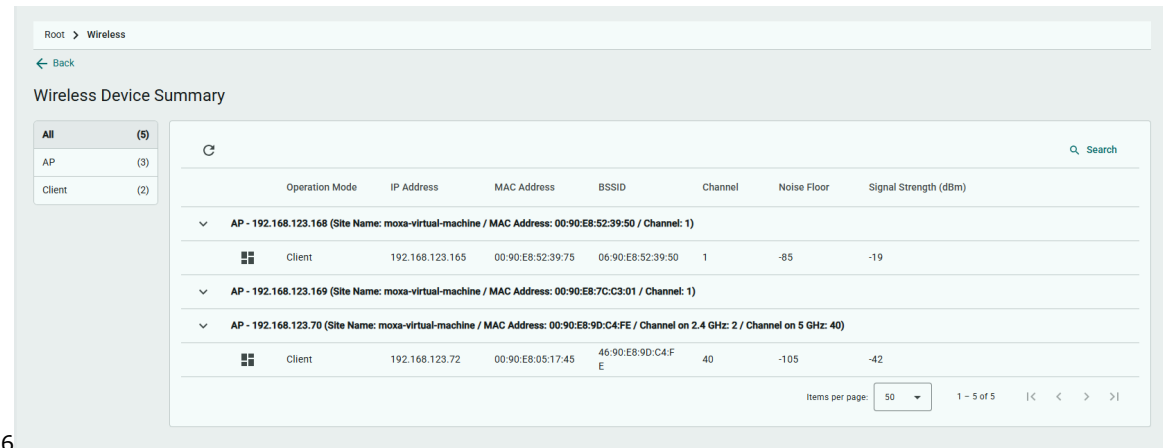


Wireless Device Summary

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.

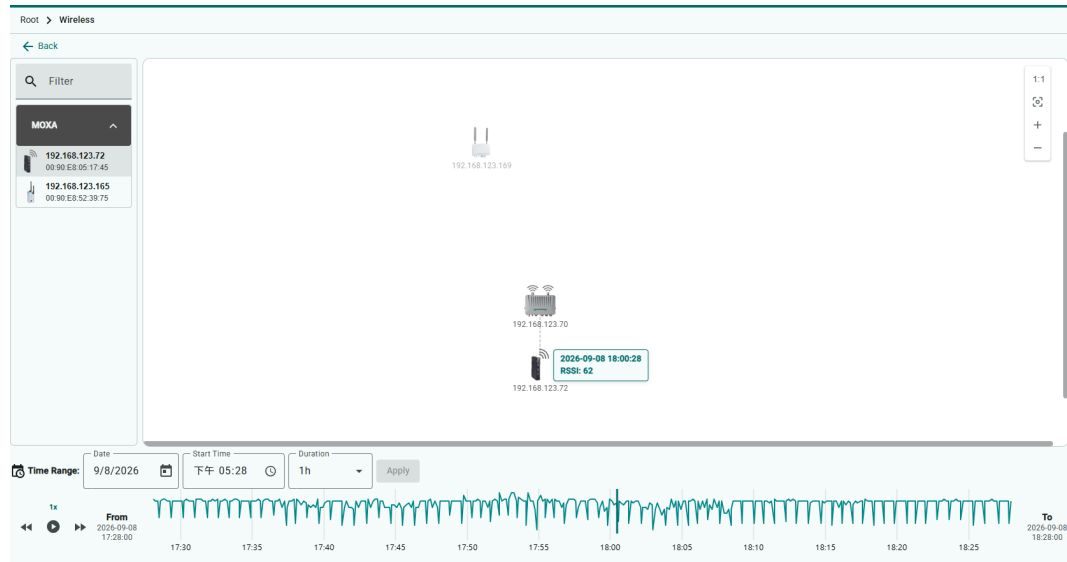


Wireless Roaming Playback

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

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

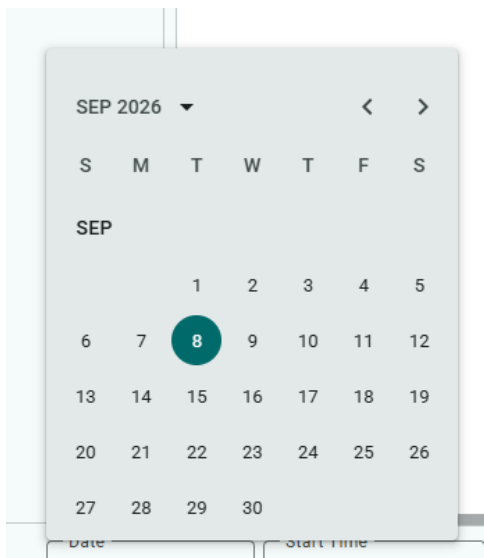
Click **Back** in the top-left corner to return to the topology view.



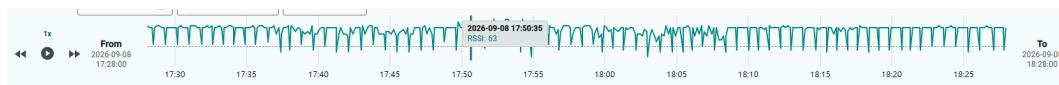
On the left-hand side is a list of wireless clients, in the center is the topology map, and located at the bottom is the playback progress bar. Select any client from the list and click **Play** (▶) to start playing the wireless roaming history for the selected time range. You can adjust the playback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

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

Time Range: 1/22/2021  08:58  1 hr 



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.

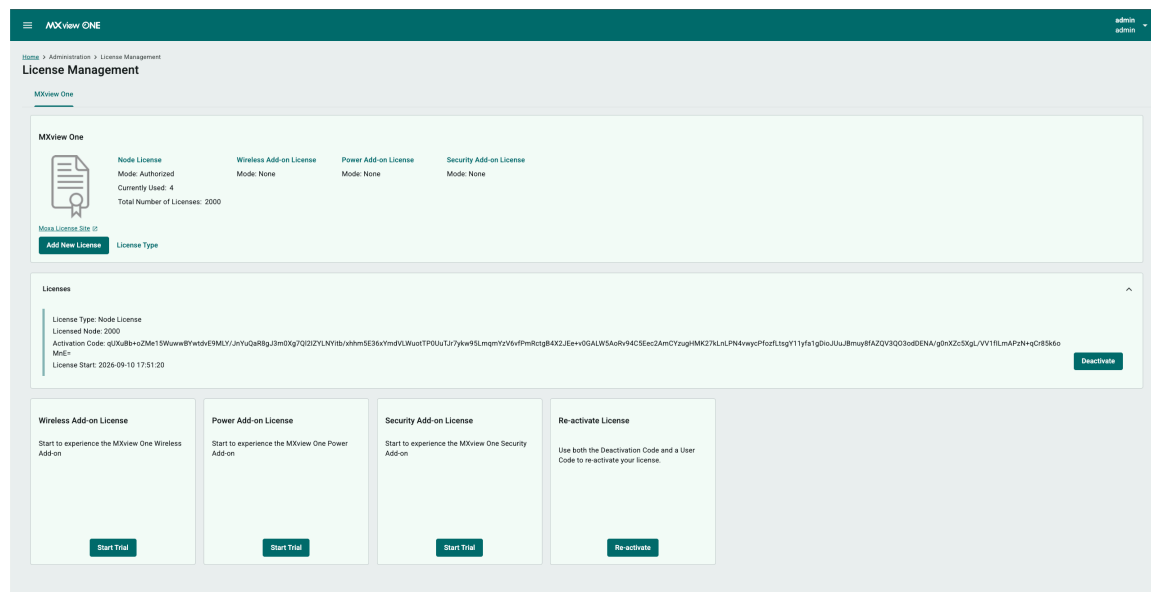
Supported Devices With PRP/HSR Features

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.



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 Power Add-on features.

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

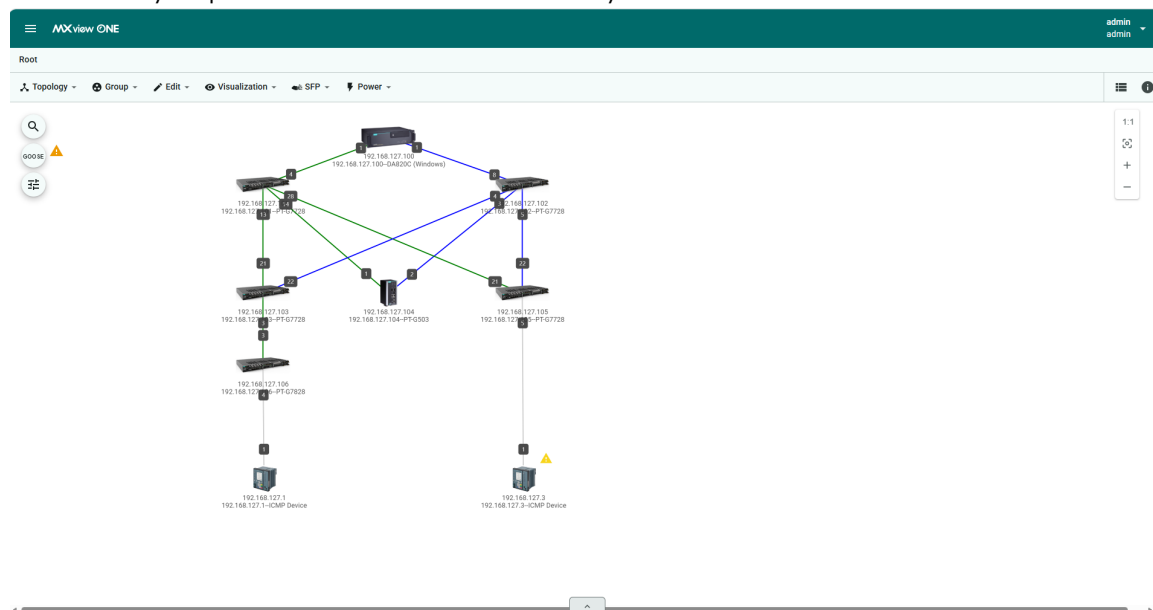


NOTE

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

Power Module Features

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



Topology

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

GOOSE panel

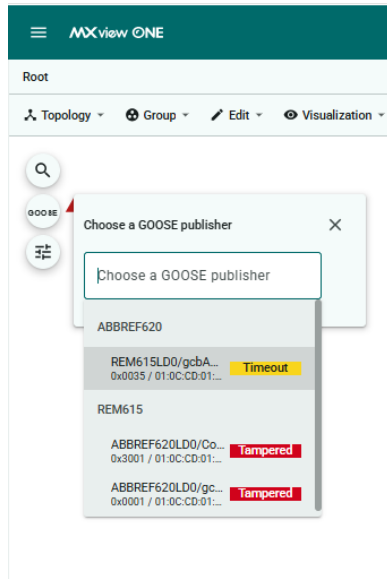
1. Before you import the SCD file, the GOOSE panel will be displayed in light gray. At this point, it has limited functionality.



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

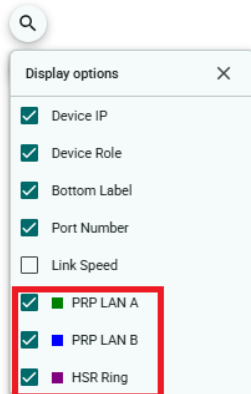


- b. Scroll down or type the GOOSE-related information, such as IED name or GoCB name.



Display Options

1. Once you have activated the MXview Power add-on module, you can see the display options include extra functions such as PRP LAN A, PRP LAN B, and HSR Ring.
2. If the box is checked, you can see the corresponding 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.

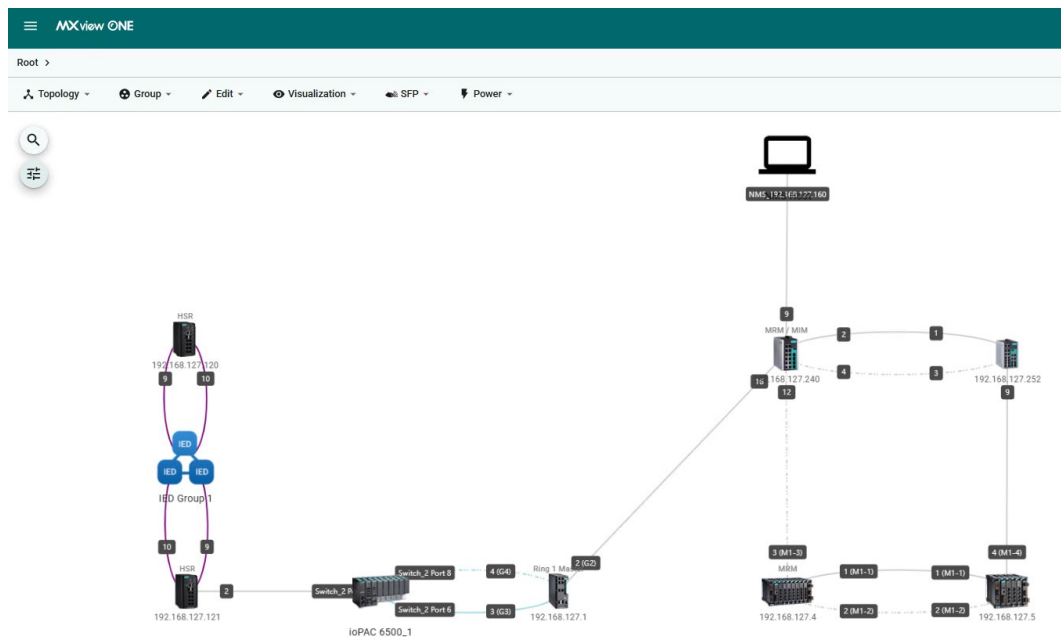


NOTE

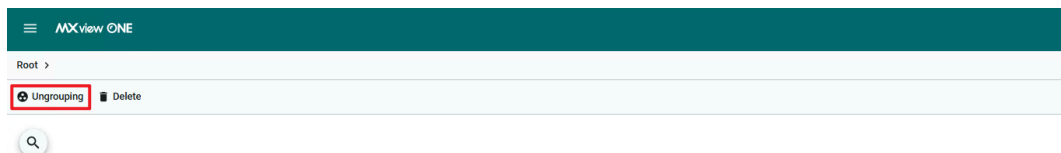
MXview One cannot guarantee that it can draw the link of the topology for non-LLDP devices, such as an IED device. However, you can draw the link of the topology manually by clicking **Add Link**.

Ungrouping an IED Group

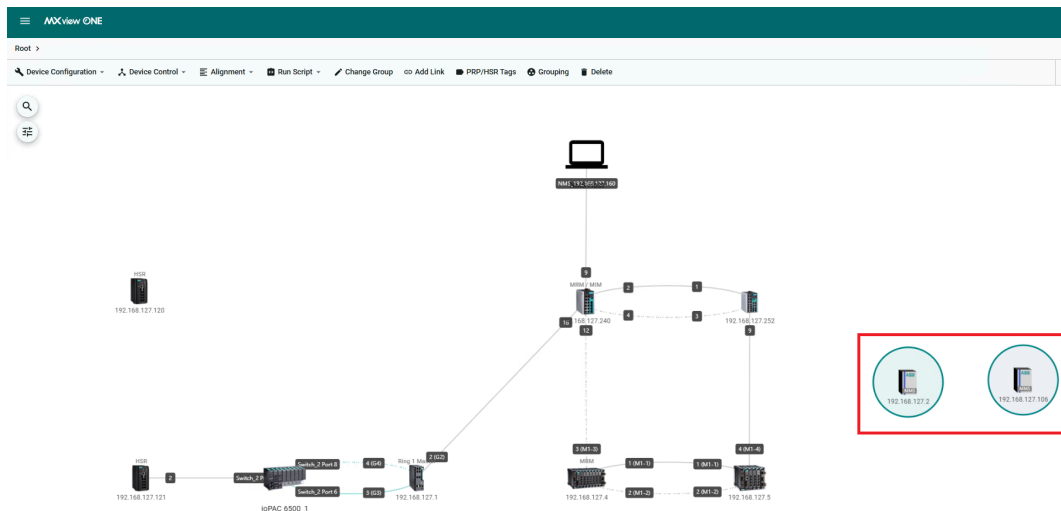
After executing the **Auto Topology** function, MXview One will automatically group the IEDs within the same HSR ring into an IED Group and represent the HSR link with a purple line. If you want to display the IEDs within the Root group or display GOOSE Message information in the topology, you can use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



1. Navigate to **Menu** (☰) > **Topology**
2. Click on the IED group in the topology that you want to ungroup.
3. With the group selected, click **Ungrouping** in the toolbar.

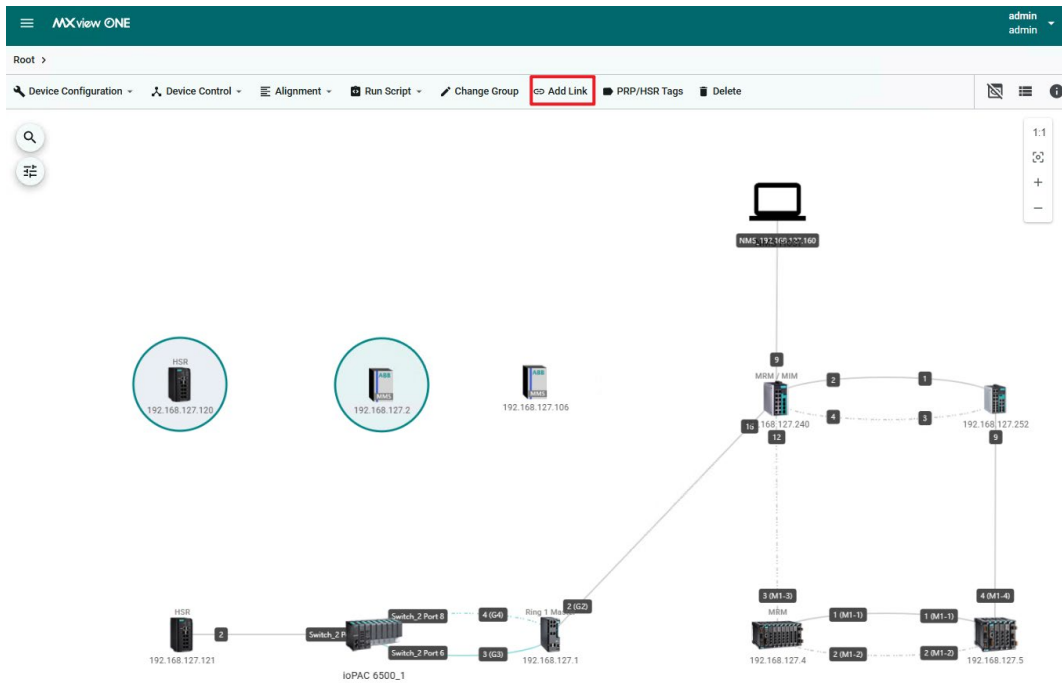


4. After ungrouping an IED group, the individual IEDs will be shown on the right-hand side of the topology.



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** in the toolbar.



- c. In the **Add Link** window, specify the device port number and click **Add**. You can set the port number as non-numerical (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: 192.168.127.120

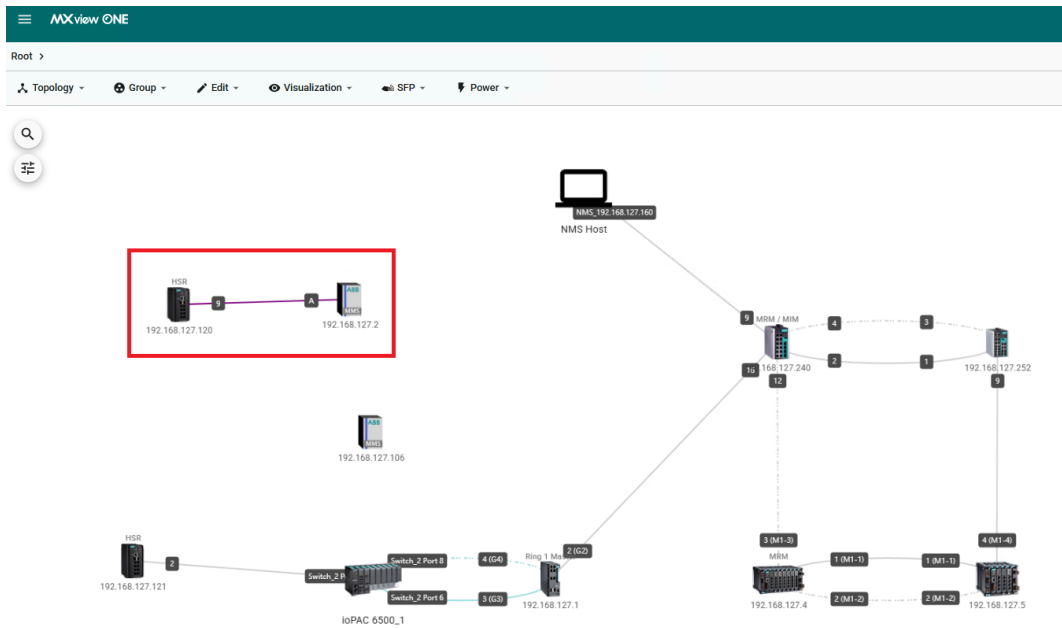
Model: PT-G510

Alias: 192.168.127.120-PT-G510

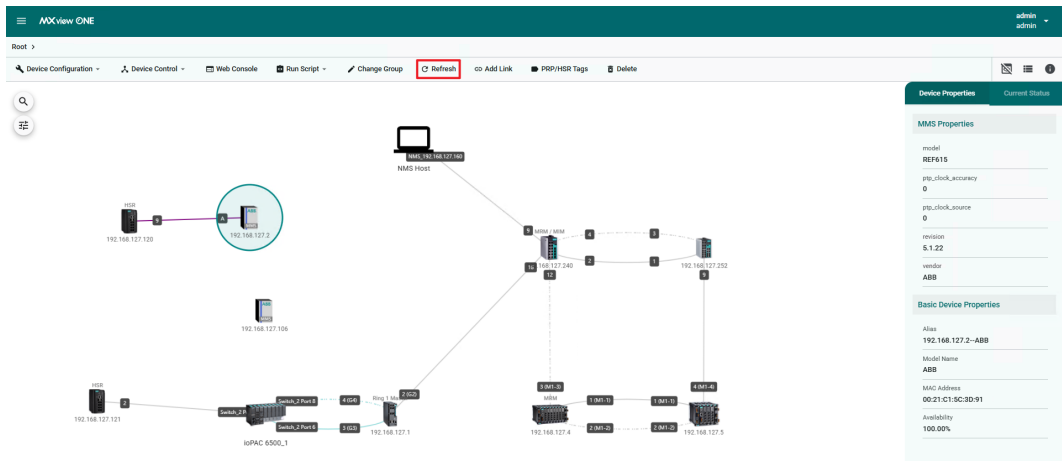
Port
9

Cancel
Add

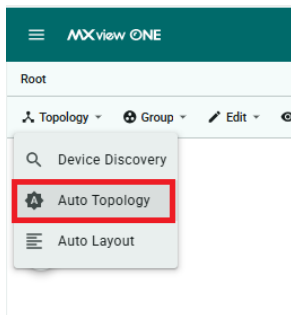
- d. Review the IED connection on the topology, indicated by a purple line.



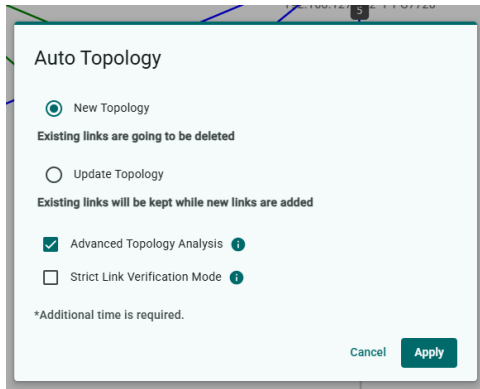
- e. Repeat this process for any other remaining IED connections.
6. (Optional) Refresh the IED information.
- Select one or multiple IEDs.
 - Click **Refresh** in the toolbar. MXview One will retrieve the latest information from the IED.



7. (Optional) Restore the original IED group.
- Go to **Topology > Auto Topology**.



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



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



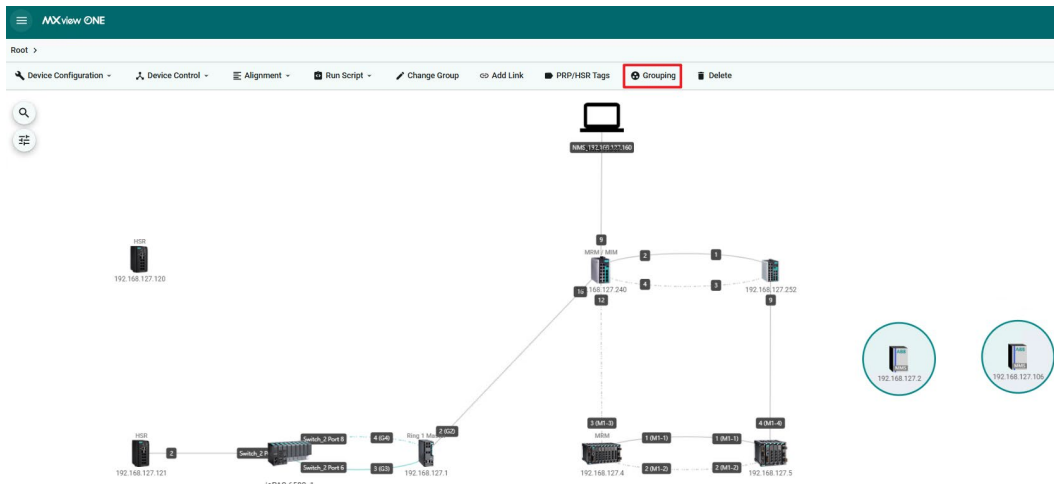
NOTE

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**
2. Select the IEDs in the topology that you want to group together.
3. With the IEDs selected, click **Grouping** in the toolbar.



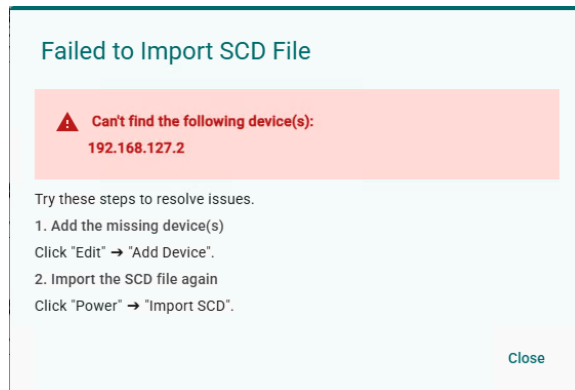
4. MXview One will combine the selected IEDs together and show them as a single group on the topology.
To ungroup an IED group, refer to **Ungrouping an IED Group**.

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**
2. Go to **Power** > **Import SCD** in the toolbar.
3. In the **Import SCD** window, click the **Select File** (📁) icon and navigate to the SCD file. The maximum file size is 100 MB.
4. Click **Import**. If successful, a confirmation will show.

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

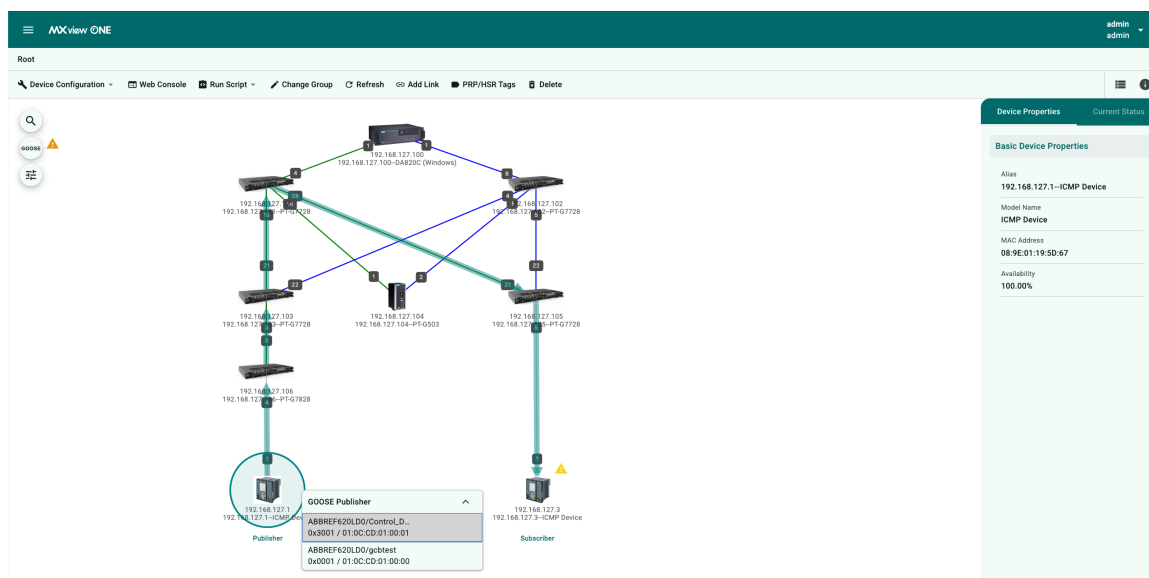


GOOSE Message

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

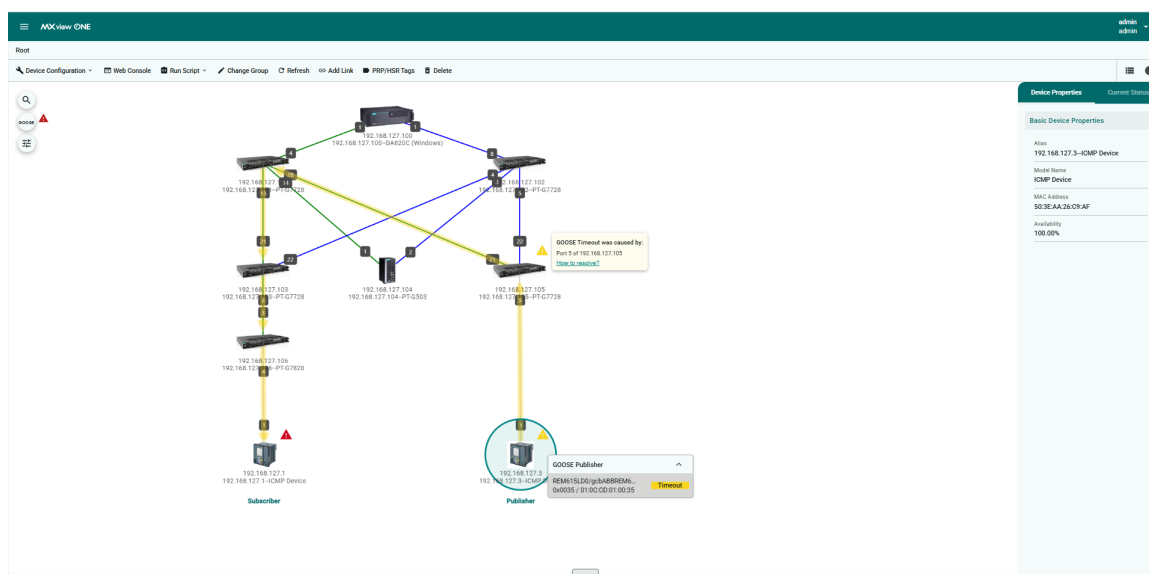
GOOSE Flow

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



GOOSE Timeout

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



Click the **How to resolve?** link in the warning box to show step-by-step instructions on how to resolve the issue.

Resolve GOOSE Timeout Issue

 **GOOSE Timeout was caused by:**
Port 5 of 192.168.127.105

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 (REM615LD0/gcbABBREM615_1/0x0035/01:0C:CD:01:00:35) is not in link down status.
- 3. Make sure the port does not have any TX/RX errors**
Click on a link, choose "Link Traffic" to see the "Packet Error Rate" section. Make sure the port does not have any errors.
- 4. Check if the fiber ports exceed certain thresholds**
Click "SFP" → "SFP List". Make sure the ports do not exceed certain thresholds.

Still not working?
Remove the SFP module and install it again.

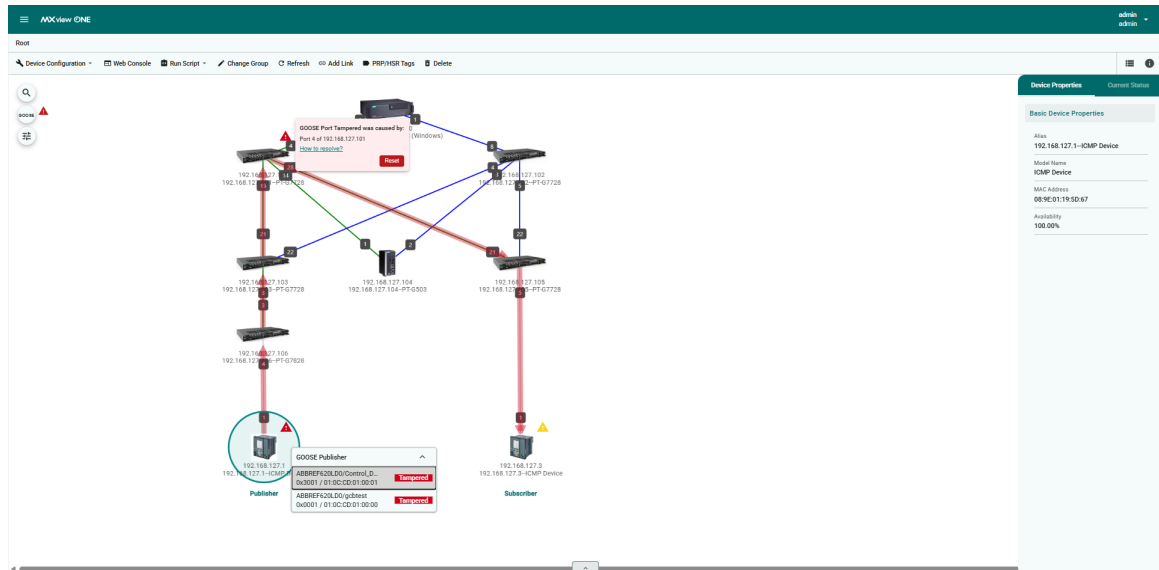
If you have further questions, contact your [channel partner](#) first.

Contact [Moxa Technical Support](#) if you still need additional support.

Once the issue is resolved, the recovery status will show in the **Recent Event** panel and the warning icon will disappear.

GOOSE Tampered

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

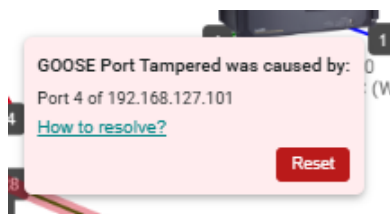


Click the **How to resolve?** link in the warning box to show step-by-step instructions on how to resolve the issue.

The screenshot shows a guide titled 'Resolve GOOSE Port Tampered Issue'. It contains the following information:

- GOOSE Port Tampered was caused by:** Port 4 of 192.168.127.101
- 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 4 status of 192.168.127.101.
- Still not working?**
If you have further questions, contact your [channel partner](#) first.
- Contact [Moxa Technical Support](#) if you still need additional support.

To enhance security, click **Reset** in the warning box to clear the event log for the devices. Once the event logs are cleared, the recovery status will show in the **Recent Event** panel and the warning icon will disappear.



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.

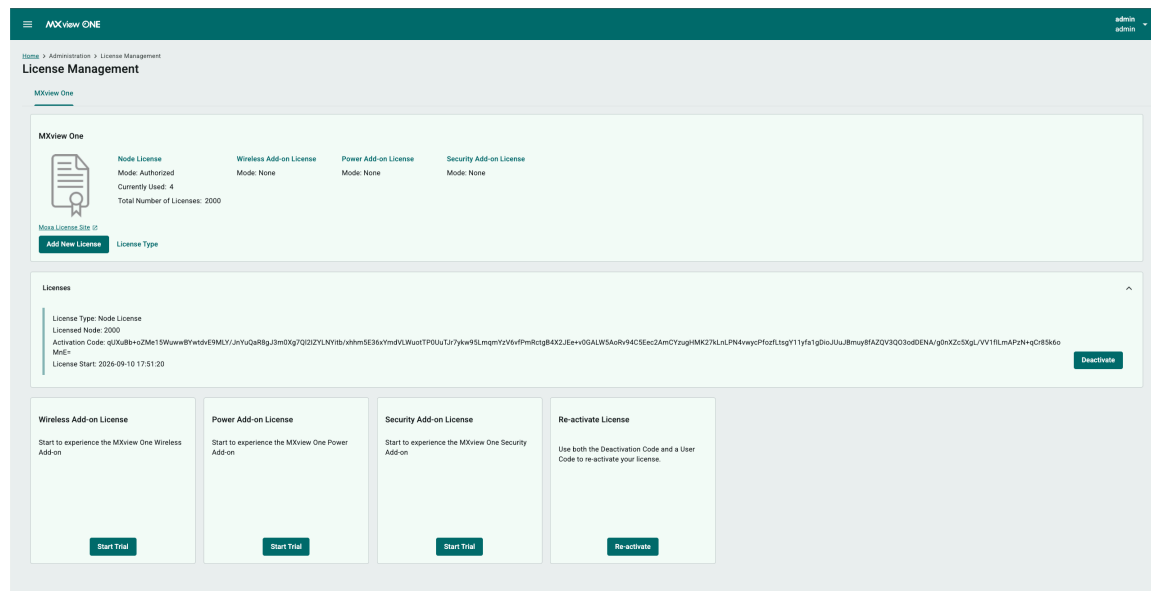
Supported Devices

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.



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 **License Management**.
- To add secure devices to your MXview One network, refer to **Using Device Discovery**.



NOTE

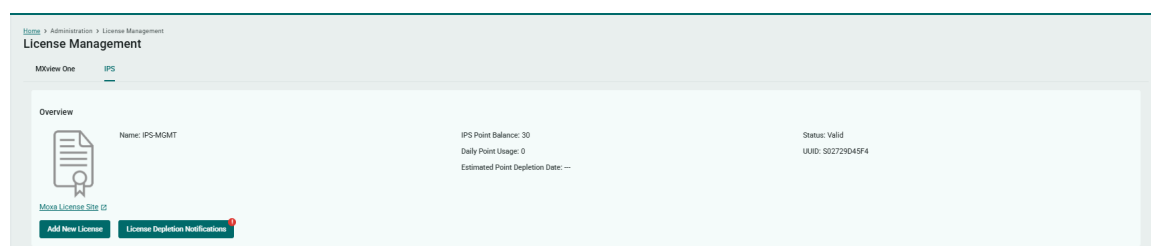
Please activate the Node-based License and then the Security Add-on License.

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.

The screenshot shows the 'License Management' interface. At the top, there are tabs for 'MXview One' and 'IPS'. The 'Overview' section displays a document icon, a 'Name: IPS-MGMT' label, and a summary of license details: 'IPS Point Balance: 60', 'Daily Point Usage: 1', 'Status: Valid', and 'Estimated Point Depletion Date: 2025-09-05'. Below this, there are buttons for 'Add New License' and 'License Depletion Notifications', and a link to 'More License Site'. The 'License History' section below features a search bar and a table with columns: 'Date Created', 'Activation Code', 'License Type', and 'License Points'. The table contains one entry with a date of '2025-07-07 10:05:44', a masked activation code, a 'Trial' license type, and '60' license points. At the bottom right of the table, it shows 'Items per page: 10' and '1 - 1 of 1'.

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**.

Add New License

1 Go to the Moxa License Site — 2 Copy UUID — 3 Activate

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.

Cancel Next

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

Go to the Moxa License Site — Copy UUID — 3 Activate

Download the license from the [Moxa License Site](#), and paste the Activation Code here.

Activation Code

Back Apply

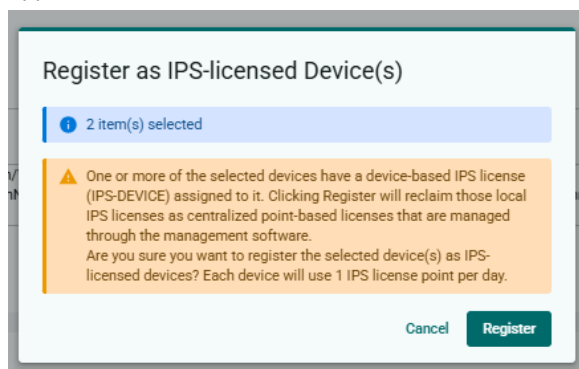
5. Click **Apply**.
6. Verify the license is correct.

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.
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.



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.
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.

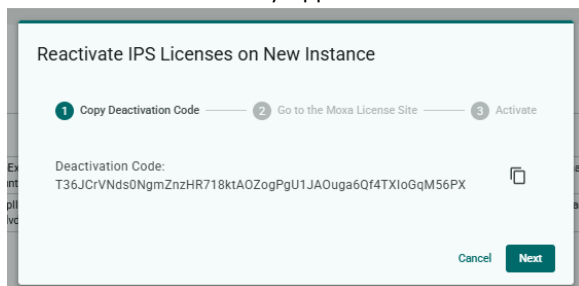


NOTE

If more than one IPS license was deactivated, all remaining license points will be combined into a single license.

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.

- When prompted to confirm, click **Deactivate**. The **Reactivate IPS Licenses on New Instance** window will automatically appear.

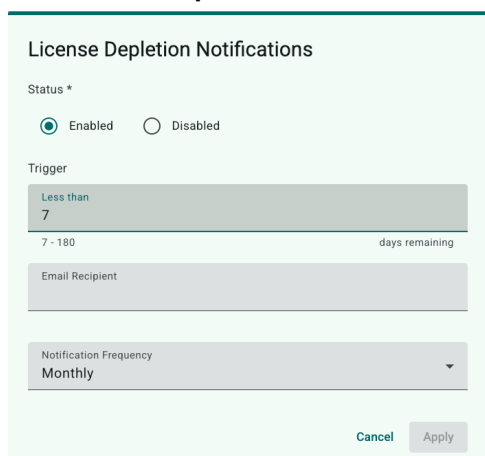


- If you closed this window, you can reopen it at any time by clicking **Reactivate** in the **Deactivated Licenses** section on the **License Management** page.
- Follow the steps in the reactivation wizard to complete the license transfer process.

Configuring IPS License Depletion Notifications

You can set up notifications to inform you when your IPS license point balance is about to run out.

- Navigate to **Menu** (☰) > **Administration** > **License Management**.
- Go to the **IPS** tab.
- Click **License Depletion Notifications**.



- Configure the following settings:
 - **Status:** Enable or disable license depletion notifications.
 - **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.
- 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.

- To check the device registration status from the **Topology** screen:
 - Navigate to **Menu** (☰) > **Topology**.

- b. Click the **List View** () icon in the top-right corner of the screen.
2. To check the device registration status from the **Device Management** screen:
 - a. Navigate to **Menu** () > **Device Management** > **Configuration and Control**.
3. Check the registration status of the device in the **Security Add-on** column:
 - **Registered**: The device can be managed via the Security Add-on module and has been successfully registered.
 - **Unregistered**: The device can be managed via 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 via 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.

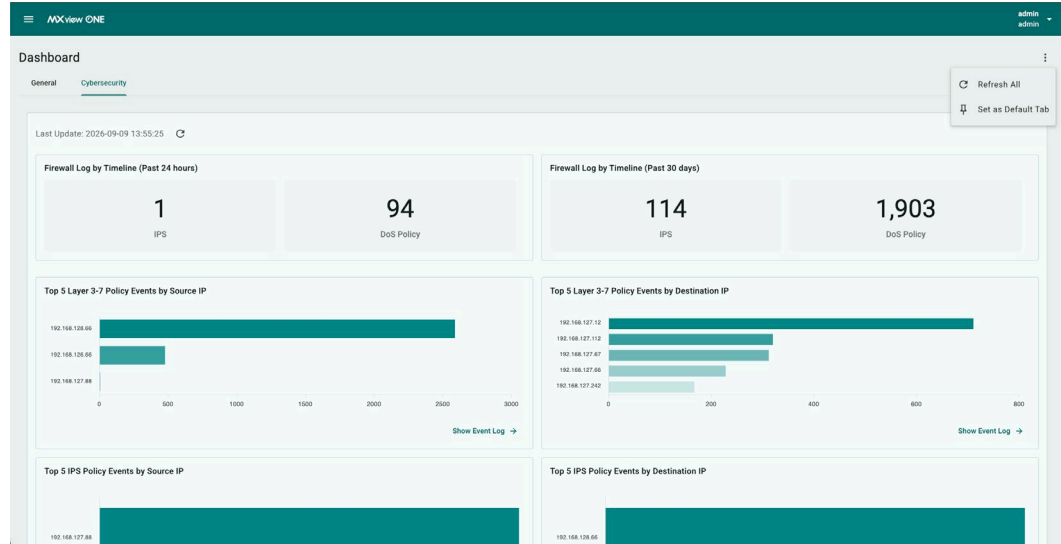
Security Module Features

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**.



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 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.

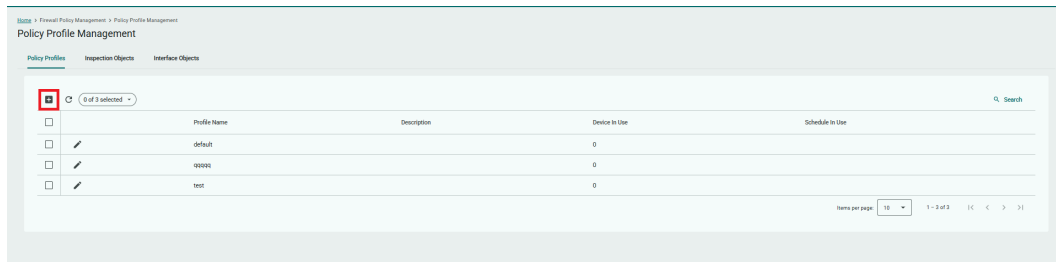
Profile Name	Description	Device in Use	Schedule in Use
default		0	
q22222		0	
test		0	

This page shows the following information in table format:

Field	Description
Profile Name	The name of the policy profile.
Description	The description of the policy profile.
Device in Use	Indicates the number of devices the policy profile is being used by. Click the ... icon in the column to see details about the referenced device(s). Policy profiles applied to devices cannot be deleted.
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.



4. In the **Create Policy Profile** window, enter a name and description for the profile and expand the **Layer 3-7** profile options.
5. Configure global firewall settings:
 - **Enforcement:** Enable or disable Layer 3-7 policy profiles.
 - **Event Log:** Enable or disable logging Layer 3-7 policy events.
6. 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**.
7. In the **Layer 3-7** section, click the **Add** (+) icon to add a Layer 3-7 policy.

The screenshot shows the 'Create Layer 3-7 Policy' window. It contains the following fields and options:

- Index:** 4
- Status:** Enabled
- Name:** (empty field, 0 / 32 characters)
- Description - optional:** (empty field, 0 / 128 characters)
- Event Log:** Disabled
- Severity:** Warning
- Log Destination - optional:** Local Storage
- Incoming Interface:** Any
- Outgoing Interface:** Any
- Action:** Allow
- Filter Mode:** IP and Port Filtering
- Source IP Address:** Any
- Source Port:** Any

At the bottom right, there are 'Cancel' and 'Create' buttons.

8. 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**.

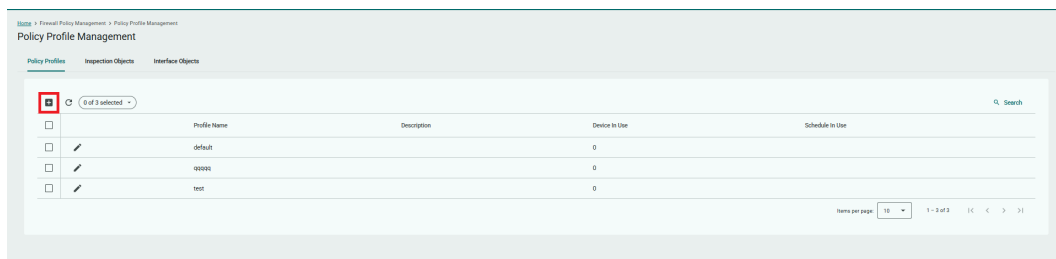
Source MAC Filtering:

- ☐ **Source MAC Address:** Specify the source MAC address.

9. Click **Create** to create the Layer 3-7 policy.
10. In the **Create Policy Profile** window, 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.



4. In the **Create Policy Profile** window, enter a name and description for the profile and expand the **Session Control** profile options.

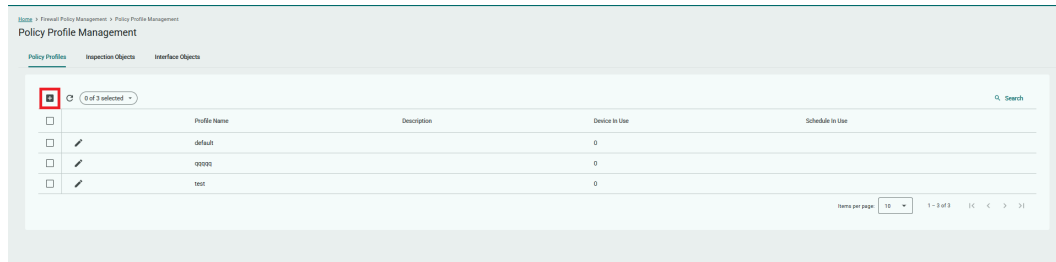
5. In the **Session Control** section, click the **Add (+)** icon to add a Session Control policy.

6. 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.
7. Click **Create** to create the Session Control policy.
8. In the **Create Policy Profile** window, click **Apply**.

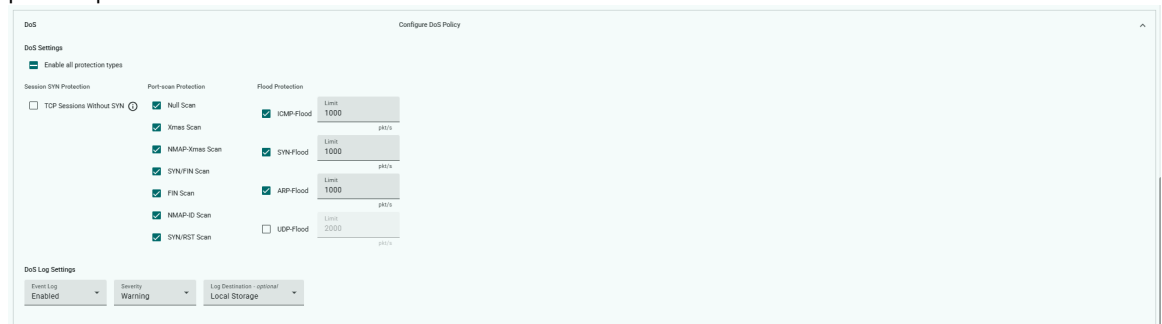
Creating a DoS Policy Profile

1. Navigate to **Menu (☰) > Firewall Policy Management > Policy Profile Management**.
2. Go to the **Policy Profile** tab.

- Click the **Add (+)** icon.



- In the **Create Policy Profile** window, enter a name and description for the profile and expand the **DoS** profile options.



- Configure the following settings:
 - **DoS Settings:** Check the box of the DoS types you want to enable. Where applicable, 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.
- Click **Apply**.

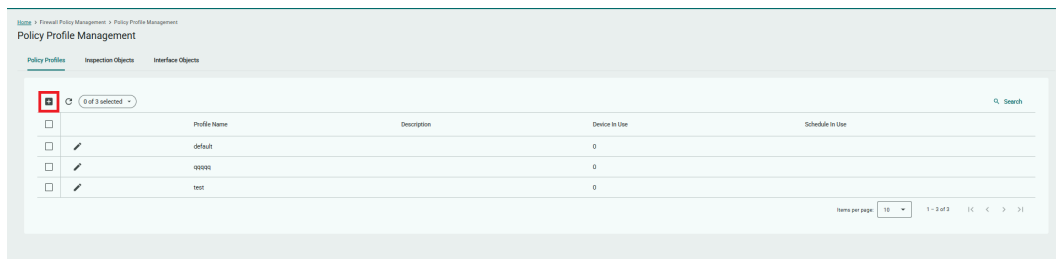
Creating an IPS Policy Profile



NOTE

IPS policy profiles require a valid security software package. Refer to **Security Package Management**.

- Navigate to **Menu (☰) > Firewall Policy Management > Policy Profile Management**.
- Go to the **Policy Profile** tab.
- Click the **Add (+)** icon.

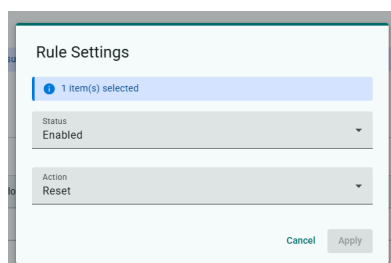


- In the **Create Policy Profile** window, enter a name and description for the profile and expand the **IPS** profile options.

- From the Package Version drop-down menu, select a previously uploaded IPS software package version. Refer to **Security Package Management** for more information.



- In the IPS rule table, check the box of the rule(s) you want to configure. You can select multiple rules at once.
- Click the **Rule Settings** (⚙️) icon.



- Configure the following settings:
 - **Status:** Enable or disable the selected rule(s).
 - **Action:** Select the action when traffic matches the policy rule.
- Click **Apply**.
- In the **Create Policy Profile** window, click **Apply**.

Editing a Policy Profile

- Navigate to **Menu** (☰) > **Firewall Policy Management** > **Policy Profile Management**.
- Go to the **Policy Profile** tab.
- Click the **Edit** (✎) icon of the profile you want to edit.
- 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**
- Click **Apply**.

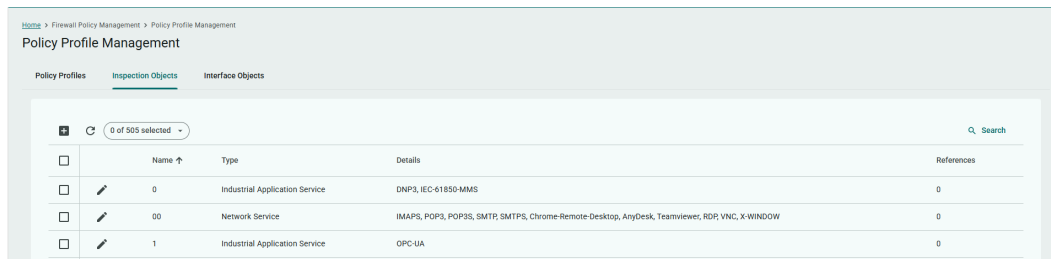
Deleting a Policy Profile

- Navigate to **Menu** (☰) > **Firewall Policy Management** > **Policy Profile Management**.
- Go to the **Policy Profile** tab.
- Check the box of the policy profile(s) you want to delete.
- Click the **Delete** (🗑️) icon.
- 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.

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.



4. In the **Create Object** window, 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. Refer to **Creating an Inspection Object**.
5. Click **Apply**.

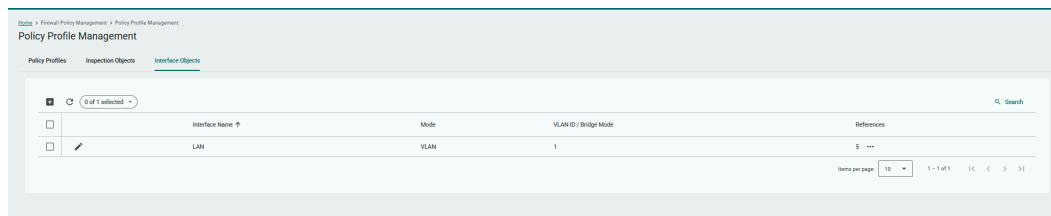
Deleting an Inspection Object

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

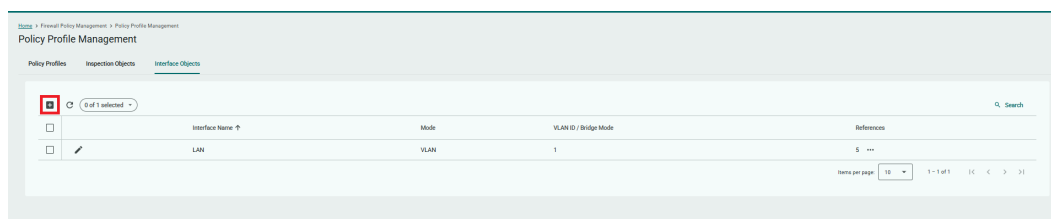
To access the **Interface Object** page, in the function tree, navigate to **Menu** (☰) > **Firewall Policy Management** > **Policy Profile Management** and go to the **Interface Object** tab.

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.



4. In the **Create Interface** window, 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. Refer to **Creating an Interface Object**.
5. Click **Apply**.

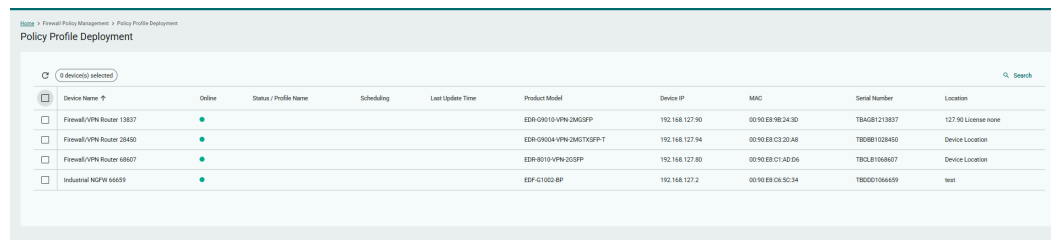
Deleting an Interface Object

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**.

From this screen, users can deploy policy profiles to multiple managed devices at a time and check the synchronization status.



The screenshot shows the 'Policy Profile Deployment' interface. At the top, there's a breadcrumb trail: 'Home > Firewall Policy Management > Policy Profile Deployment'. Below this is a sub-header 'Policy Profile Deployment'. A search bar on the right says 'Search'. On the left, there's a filter section with a dropdown '0 device(s) selected' and a checkbox icon. The main area is a table with columns: 'Device Name', 'Online', 'Status / Profile Name', 'Scheduling', 'Last Update Time', 'Product Model', 'Device IP', 'MAC', 'Serial Number', and 'Location'. There are four rows of device data, each with a checkbox in the 'Device Name' column.

Device Name	Online	Status / Profile Name	Scheduling	Last Update Time	Product Model	Device IP	MAC	Serial Number	Location
☐ Firewall/VPN Router 13837	●				EDR-0910-VPN-2M5GFP	192.168.127.50	00:90:EB:9B:24:3D	TBAG081213837	127.00 License none
☐ Firewall/VPN Router 28400	●				EDR-0904-VPN-2M5GFP-T	192.168.127.54	00:90:EB:C3:2D:A8	TB0081028400	Device Location
☐ Firewall/VPN Router 68607	●				EDR-0910-VPN-2G5GFP	192.168.127.80	00:90:EB:C1:AD:06	TBCL81068607	Device Location
☐ Industrial NCFW 66659	●				EDF-01003-8P	192.168.127.2	00:90:EB:06:5C:34	TB0001066659	test

Deploying Policy Profiles to Managed Devices



NOTE

To deploy policy profiles to devices, a configured policy profile is required. Refer to **Policy Profiles Management**.

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.
4. In the **Sync Profile to Device(s)** window, select a previously configured policy profile. Refer to **Policy Profile Management**.
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.
4. In the **Schedule Settings** window, 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.

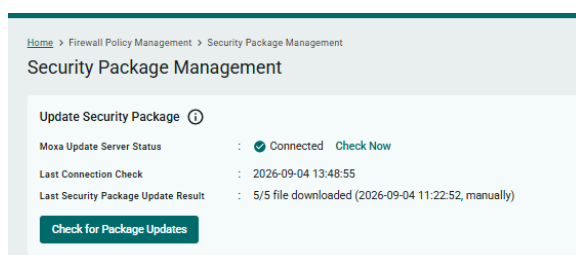
Security Package Files

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**.

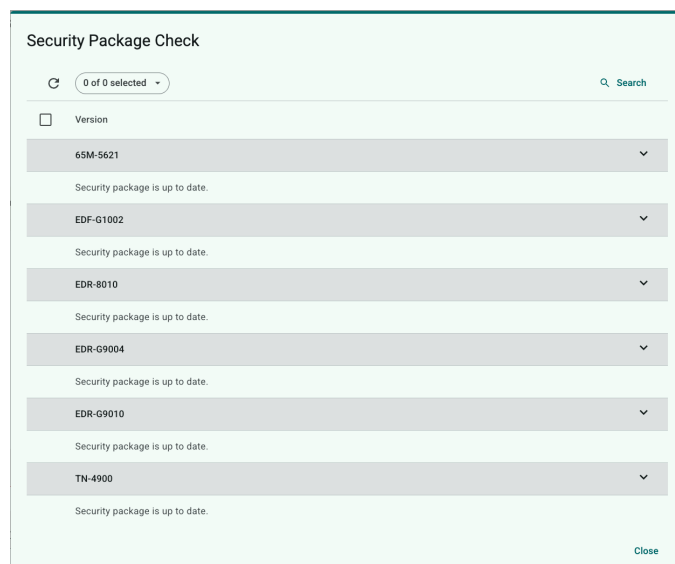


This section shows the following information:

Field	Description
Moxa Update Server Status	Shows the current status of the connection to the Moxa update server. Click Check Now to refresh the connection status.
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.



The 'Security Package Check' dialog box displays a list of security packages with their versions and status. At the top, there is a search bar and a selection indicator showing '0 of 0 selected'. The list includes packages like 65M-5621, EDF-G1002, EDR-8010, EDR-G9004, EDR-G9010, and TN-4900, each with a status of 'Security package is up to date.' A 'Close' button is located at the bottom right.

Version	Status
65M-5621	Security package is up to date.
EDF-G1002	Security package is up to date.
EDR-8010	Security package is up to date.
EDR-G9004	Security package is up to date.
EDR-G9010	Security package is up to date.
TN-4900	Security package is up to date.

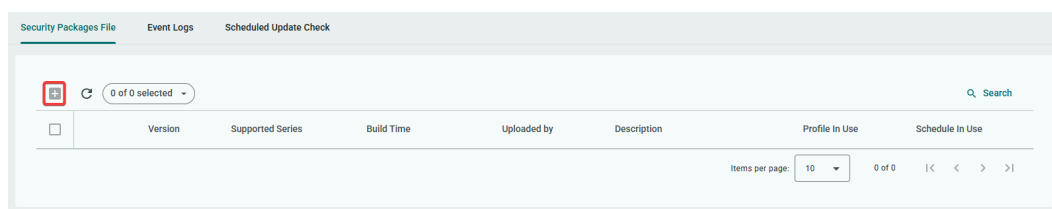
Uploading a Security Package



NOTE

Security software packages for supported products can be downloaded from the relevant product pages on the Moxa website.

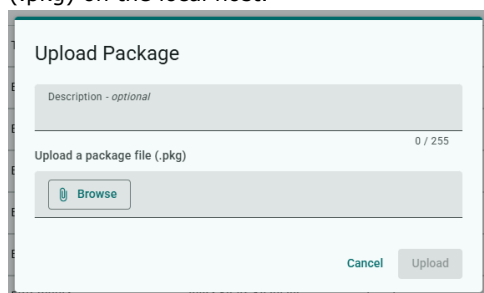
1. Navigate to **Menu** (☰) > **Firewall Policy Management** > **Security Package Management**.
2. Go to the **Security Package Files** tab.
3. Click the **Add** (+) icon.



The 'Security Packages File' tab shows a table with columns: Version, Supported Series, Build Time, Uploaded by, Description, Profile in Use, and Schedule in Use. A search bar and a selection indicator '0 of 0 selected' are at the top. The table is currently empty.

Version	Supported Series	Build Time	Uploaded by	Description	Profile in Use	Schedule in Use
---------	------------------	------------	-------------	-------------	----------------	-----------------

4. In the **Upload Package** window, enter a description and drag and drop or browse to the package file (.pkg) on the local host.



The 'Upload Package' dialog box has a 'Description - optional' text field and a file upload section labeled 'Upload a package file (.pkg)' with a 'Browse' button. At the bottom are 'Cancel' and 'Upload' buttons.

5. Click **Upload**.

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

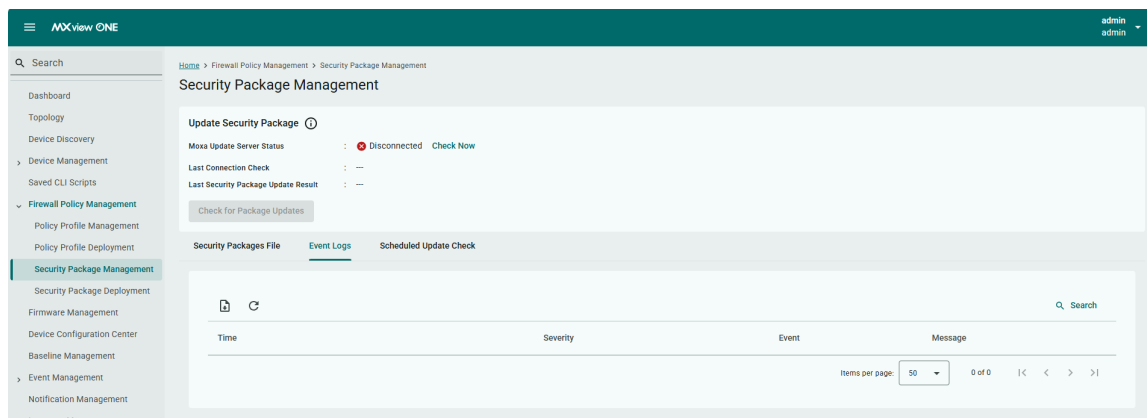
1. Navigate to **Menu** (☰) > **Firewall Policy Management** > **Security Package Management**.
2. Go to the **Security Package Files** tab.
3. In the package file list, click the **Download** (⬇) icon of the package file you want to download.

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

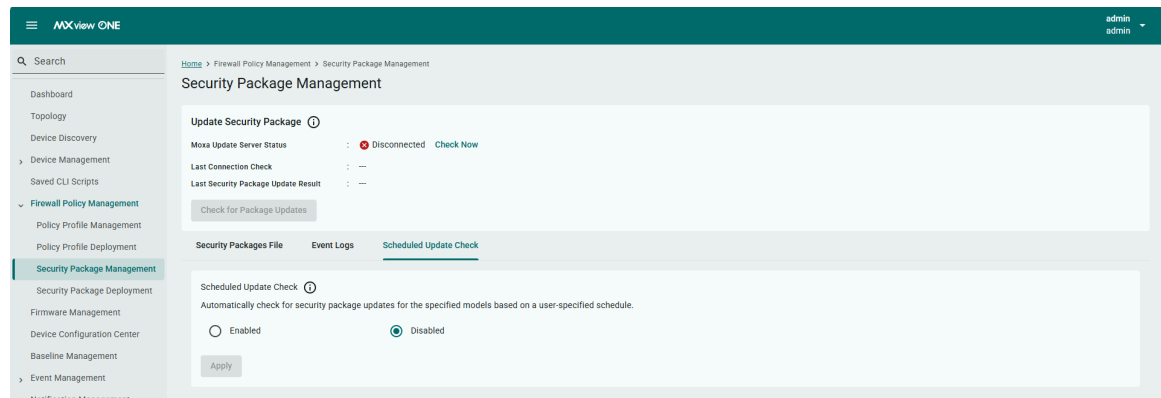
1. Navigate to **Menu** (☰) > **Firewall Policy Management** > **Security Package Management**.
2. Go to the **Event Logs** tab.
3. You can perform the following actions:
 - a. Click the **Download All Logs** (⬇) icon to export the current search results as a CSV file.
 - b. Click the **Refresh** (↻) 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.

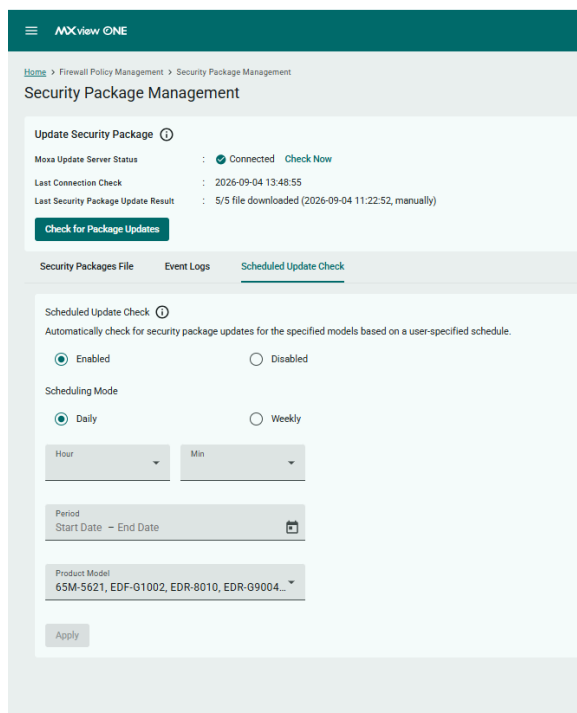
Scheduled Update Check

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 **Scheduled Update Check** tab.
3. Set **Scheduled Update Check** to **Enabled**. Additional options will be available.



4. Choose a **Scheduling Mode**:
 - **Daily**: Schedule daily checks.
 - **Weekly**: Schedule weekly checks.
5. Configure the update period. The system will only perform update checks at 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

From this screen, you can deploy security packages to managed devices. 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											
1 2 device(s) selected											
Search											
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-2G5FP	192.168.127.82	TBZKB1155166	00:90:EB:80:10:A4	v10.0.0023	V3.13.99				25.058, 121.453
Firewall/VPN Router 55165	●	EDR-G9010-VPN-2M05FP	192.168.127.35	TBZKB1155165	00:90:EB:91:86:82	v10.0.0023	V3.13.99				Device Location

Upgrading the Security Package of Managed Devices

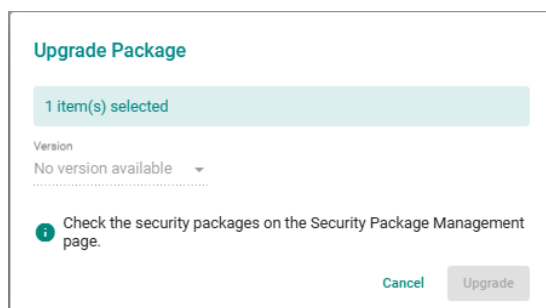
You can manually upgrade the security package of managed devices and check basic security package version information.



NOTE

To upgrade security packages for devices, the relevant security package must be uploaded first. Refer to **Uploading a Security Package**.

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.



4. In the **Upgrade Package** window, select a previously uploaded security package to upgrade to.
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 be executed only once, or on a daily or weekly recurring basis.

You 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.

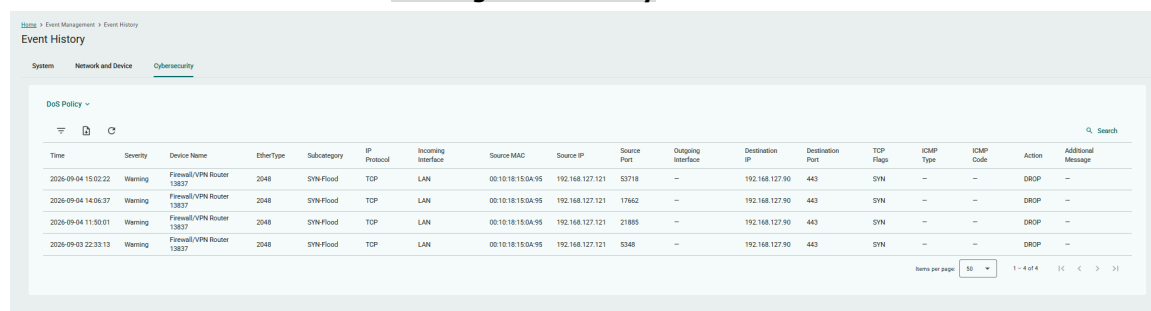
3. Click the **Schedule Settings** (📅) icon.
4. In the **Schedule Settings** window, configure the following settings:
 - **Select File:** Select a security package version to apply to the selected device(s).
 - **Scheduling Mode:** Select a scheduling mode. Depending on the selected mode, configure 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**.



The screenshot shows the 'Event History' page with the 'Cybersecurity' tab selected. It displays a table of security events under the 'DoS Policy' filter. The table includes columns for 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, and Additional Message. Four events are listed, all with a 'Warning' severity and 'DROP' action.

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
2026-09-04 15:02:22	Warning	Firewall/VPN Router 13837	2048	SYN Flood	TCP	LAN	00:10:18:15:0A:95	192.168.127.121	53718	--	192.168.127.90	443	SYN	--	--	DROP	--
2026-09-04 14:06:37	Warning	Firewall/VPN Router 13837	2048	SYN Flood	TCP	LAN	00:10:18:15:0A:95	192.168.127.121	17662	--	192.168.127.90	443	SYN	--	--	DROP	--
2026-09-04 11:50:01	Warning	Firewall/VPN Router 13837	2048	SYN Flood	TCP	LAN	00:10:18:15:0A:95	192.168.127.121	21885	--	192.168.127.90	443	SYN	--	--	DROP	--
2026-09-03 22:33:13	Warning	Firewall/VPN Router 13837	2048	SYN Flood	TCP	LAN	00:10:18:15:0A:95	192.168.127.121	5348	--	192.168.127.90	443	SYN	--	--	DROP	--

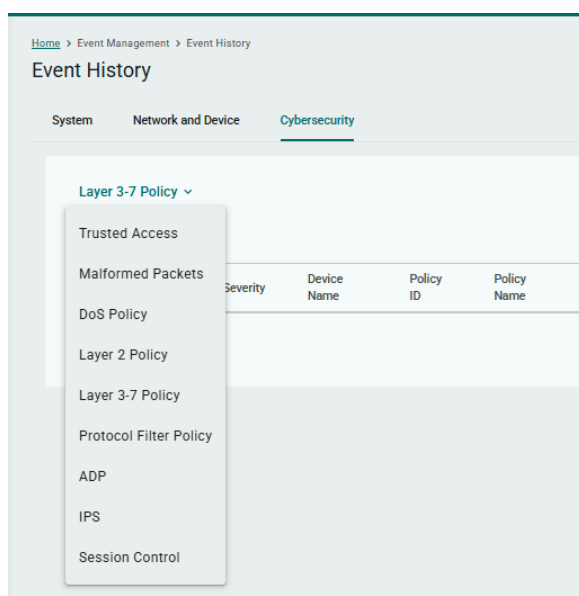
The table shows the following information:

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.

Field	Description
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

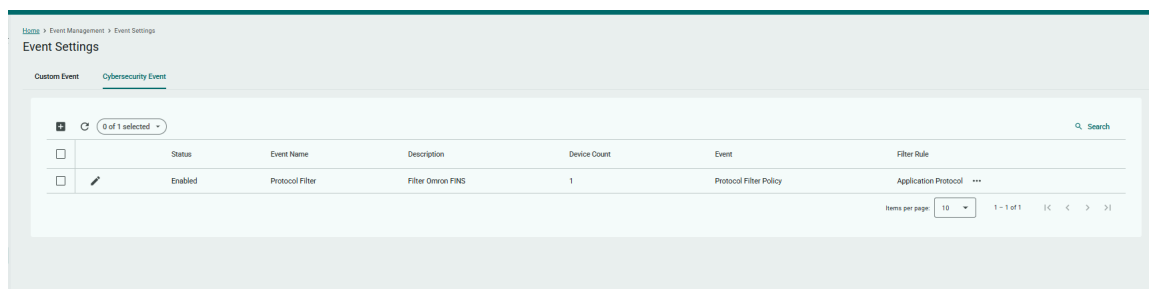
1. Navigate to **Menu** (☰) > **Event Management** > **Event History**.
2. Go to the **Cybersecurity** tab.
3. Select the event type from the drop-down menu.



4. 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.
5. To export logs:
 - a. Click the **Download All Logs** (📄) icon to export the current results as a CSV file
6. To refresh the event log data:
 - a. Click the **Refresh** (🔄) icon to renew the search results.

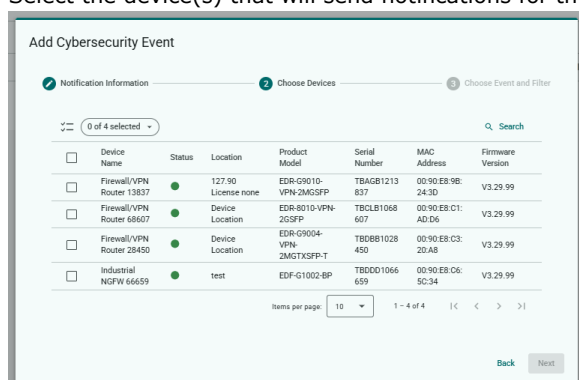
Cybersecurity Event Settings

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**.

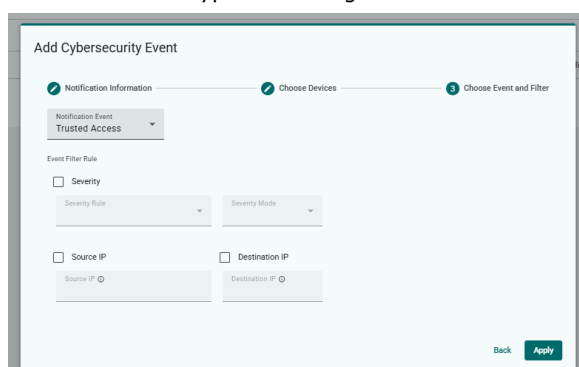


Adding a Cybersecurity Event

1. Navigate to **Menu** (☰) > **Event Management** > **Event Settings**.
2. Go to the **Cybersecurity Event** tab.
3. Click the **Add** (+) icon.
4. In the **Add Cybersecurity Event** window, enter a name and description for the event and click **Next**.
5. Select the device(s) that will send notifications for the specified event(s) and click **Next**.



6. Select the event type and configure the filter rules:



- a. Select the notification event type from the drop-down menu.
 - 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.
7. 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



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.

1. Navigate to **Menu** (☰) > **Device Management** and select **IPS Configuration** from the **Cybersecurity Controls** menu in the toolbar.
2. In the **IPS Configuration** window, 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. If unsuccessful, an error description will be shown for troubleshooting.

IP	Alias	Model	Status
192.168.127.90	192.168.127.90-EDR-G9010	EDR-G9010	Failed(No IPS license assigned)

5. Click **Close** to close the status window.

A. Network Port Usage

This section lists the TCP/UDP ports used by MXview One and MXview One Central Manager services. The following types can be attributed:

- **Fixed:** The assigned port is fixed and cannot be changed.
- **Configurable:** The port can be modified by the user via the relevant configuration page. Available ports depend on the function.

MXview One Central Manager

Inbound Traffic

Port	Protocol	Usage	Type
8883	MQTT (TLS)	MXview One Central Manager server; waits for MXview One to send MQTT messages to the Central Manager.	Configurable
443	HTTPS	Access the MXview One Central Manager web GUI.	Configurable
80	HTTP	Access the MXview One Central Manager web GUI.	Configurable
6601	MQTT (TLS)	Connect to a local MXview One web console from MXview One Central Manager.	Configurable

Outbound Traffic

Port	Protocol	Usage	Type
8883	MQTT (TLS)	Retrieve and set the MXview One server settings via encrypted MQTT.	Configurable
587	SMTP	Send emails with TLS/SSL encryption via SMTP.	Configurable

MXview One

Inbound Traffic

Port	Protocol	Usage	Type
443	HTTPS	Access the MXview One web GUI.	Configurable
80	HTTP	Access the MXview One web GUI. This service is disabled by default.	Configurable
162	UDP	Used by MXview One to receive SNMP traps from devices.	Configurable
514 / 5143	UDP / TCP (TLS)	Built-in syslog server.	Configurable
4840	TCP (TLS)	OPC UA server.	Configurable
18883	MQTT + TLS	Used by the MXview Security add-on.	Configurable
123	NTP / SNTP	Sync the device time after enabling the MXview Security add-on.	Fixed

Outbound Traffic

Port	Protocol	Usage	Type
161	UDP	Poll Moxa devices.	Configurable

8883	MQTT (TLS)	Update network data to MXview One Central Manager via MQTT.	Configurable
22	SSH	Execute CLI commands.	Configurable
User-defined	UDP / TCP (TLS)	Syslog forwarding. This service is disabled by default.	Configurable
502	TCP	Modbus traffic. This service is disabled by default.	Fixed
102	TCP	MMS traffic.	Fixed
102	TCP	Siemens S7 Comm. traffic. This service is disabled by default.	Fixed
44818	TCP / UDP	EtherNet/IP traffic. This service is disabled by default.	Fixed
User-defined	SMTP	Send email notifications. This service is disabled by default.	Configurable
443	HTTPS	RESTful API for firmware automation, warranty management. Connects to https://api.common.thingsprocloud.co by request.	Fixed

Internal Services

Port	Protocol	Usage	Type
5432	Database Interface	Save device and network status information.	Configurable
8883	MQTT + TLS	MXview One internal services.	Configurable
18883	MQTT + TLS	Used by the MXview Security add-on.	Configurable
7100 to 7105 (auto-detected)	HTTPS	Access the MXview One Control Panel.	Configurable
30000 to 50000 (auto-detected)	HTTPS	Internal HTTPS servers. Randomly assigns 4 ports from the valid port range.	Configurable

Device Outbound

Port	Protocol	Usage	Type
4800	UDP	NPort / MGate: search.	Fixed
5353	UDP	NPort / MGate: search.	Fixed
29168	UDP	NPort / MGate: search.	Fixed
4001~ (depends on used ports)	UDP	UDP Mode.	Fixed
4900	TCP	NPort / MGate: configuration.	Fixed
10124	TCP	IO: configuration.	Fixed
443	TCP	NPort / MGate: configuration.	Fixed
502	TCP	IO: configuration.	Fixed
4001~ and 966~ (depends on used ports)	TCP	Server Mode.	Fixed
950 to 1012	TCP	Real COM Mode.	Fixed
1029	UDP	NPort: security view.	Fixed

B. Installation Directories

Installing MXview One will create the necessary directories on the host system. Directory paths may vary depending on the selected options during installation. The following table lists the default installation paths.

Windows

Directory	Description
C:\Users\<username>\AppData\Roaming\moxa\mxview one	Stores user-specific configuration and application data. <username> is the Windows account used to run MXview One.
C:\Program Files (x86)\Moxa\MXview One	The MXview One program installation directory.

Linux

Directory	Description
/usr/mxview/	The default MXview One installation directory.