

# MXview One v1.3.0

## New Features

**Ahmed Mabrouk, TS**  
**Branislav Radak, FAE**  
September 19<sup>th</sup>, 2024

**MXview ONE**

# Expect to Gain from This Training

- ❑ Understand customers' challenges from the scenarios and why we design these features
- ❑ Understand new features and how to operate them

# Training Outline

## What's new in MXview One v1.3.0

- New Features Introduction
- Demo

# Overview of New Features



## Enhance Efficiency

- ❑ Run Script / Saved CLI Scripts
- ❑ Device Management
- ❑ Firmware Management

## MXview ONE v1.3.0



## Strengthen Network Visibility

- ❑ User-defined SNMP Device Plug-in
- ❑ Modbus Device Recognition (v1.2.0)



## Cybersecurity Management

- ❑ Device Management Cybersecurity Control
- ❑ Firmware Management Security Patch icon

# MXview One v1.3.0

## Enhance Efficiency



Run Script  
Saved CLI Scripts

# Scenario: I have to do configuration on multiple devices

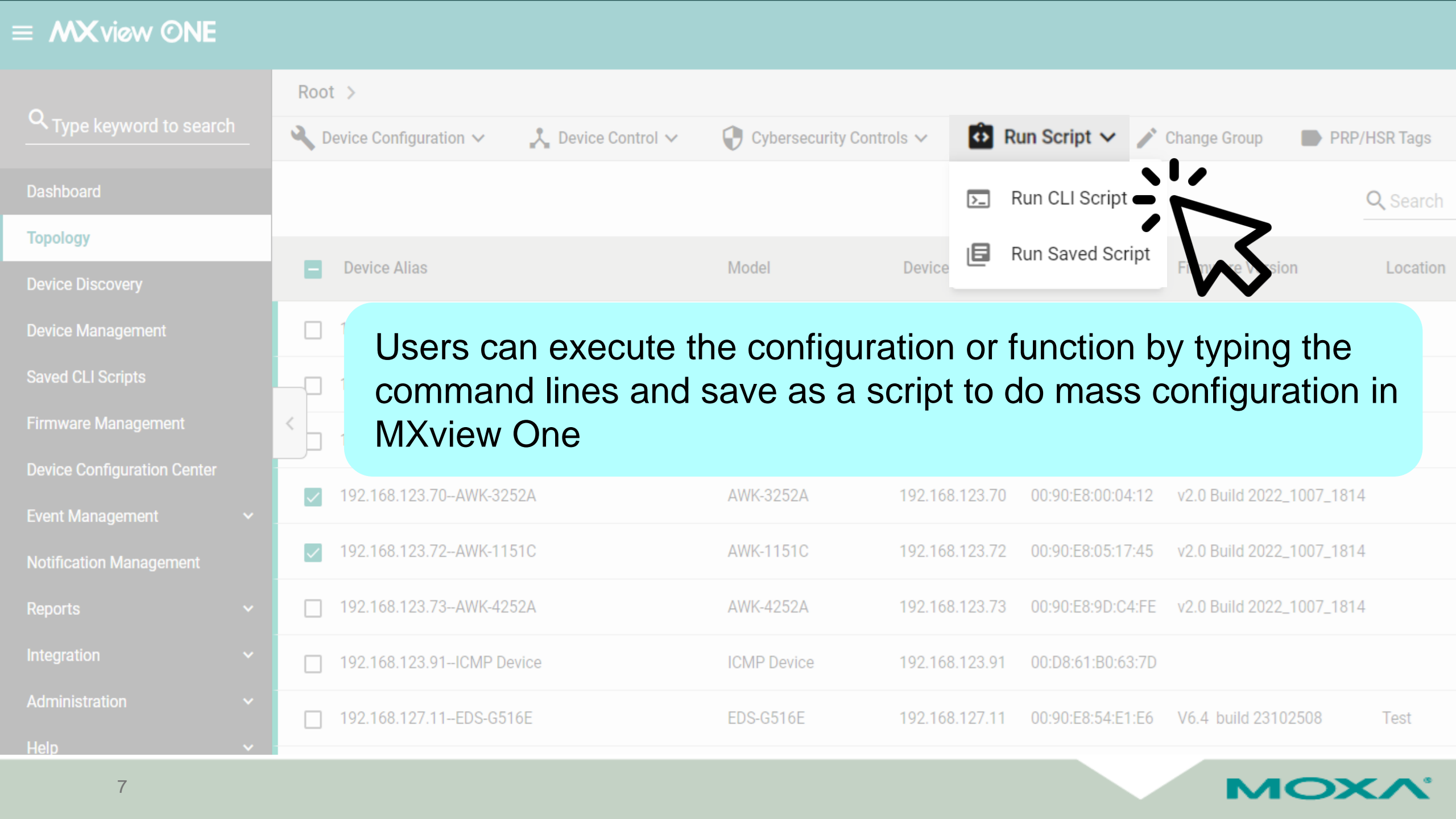


Operator  
MXview One user

As a network operator, I have the need to configure devices.

The current device configuration features available in MXview One are limited, so I need to **log in to device's Web Console** for operations, and it's a **one-by-one** process.

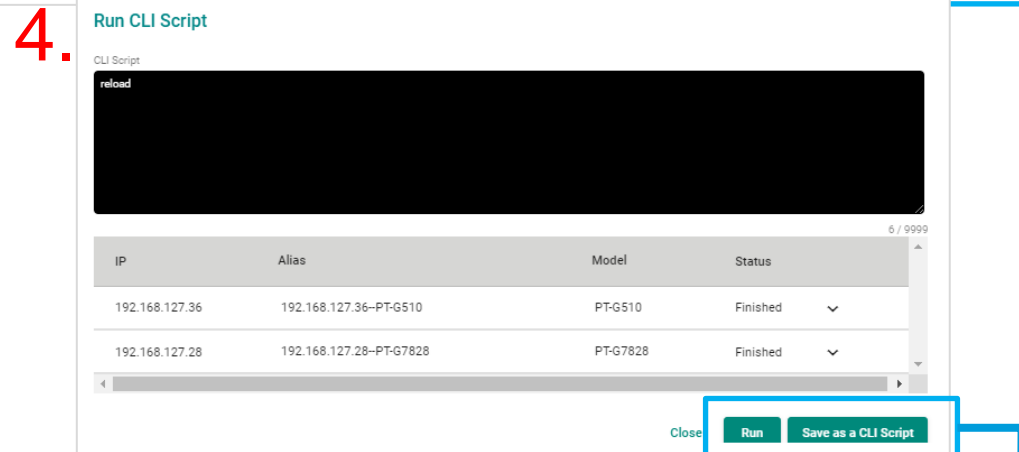
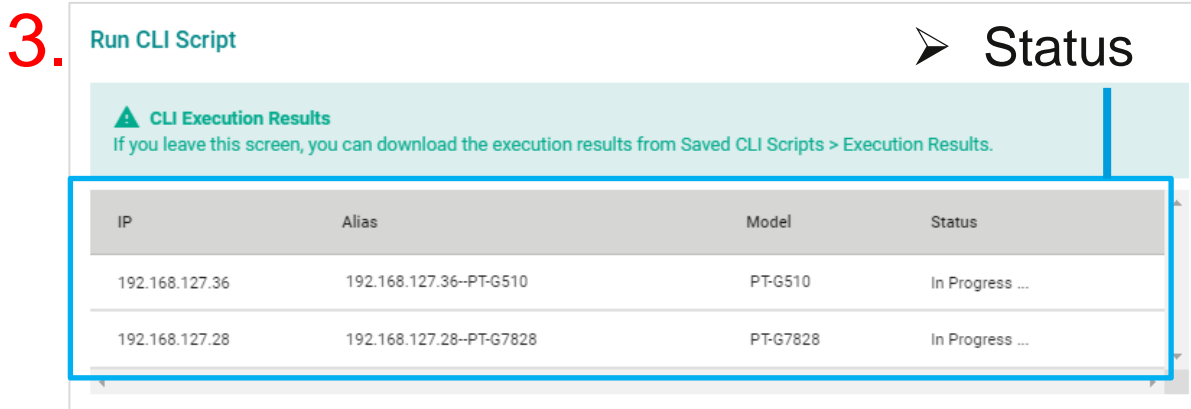
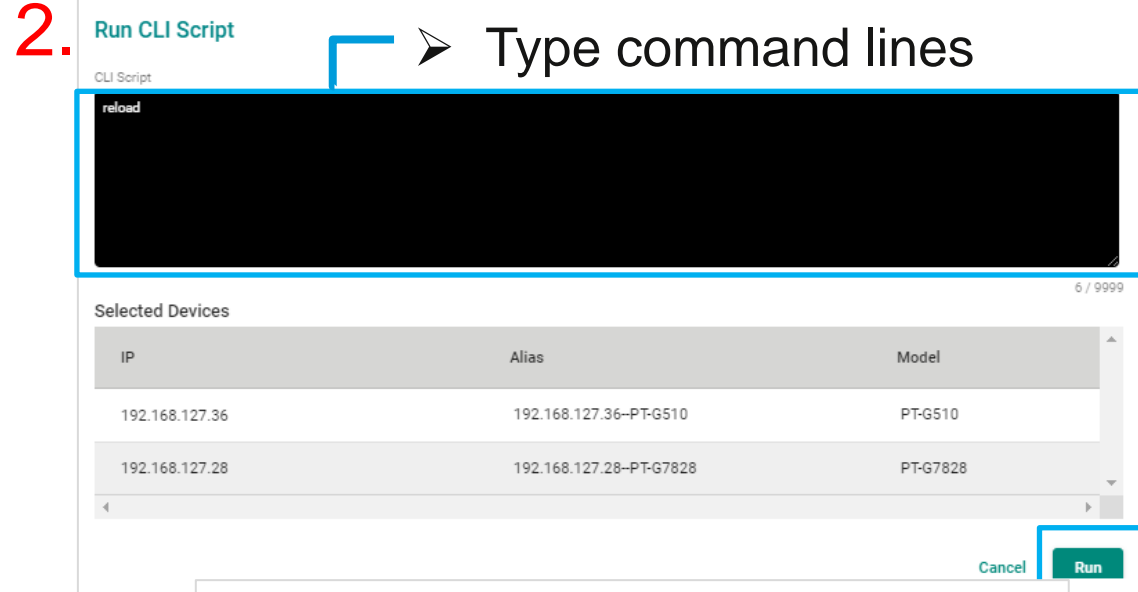
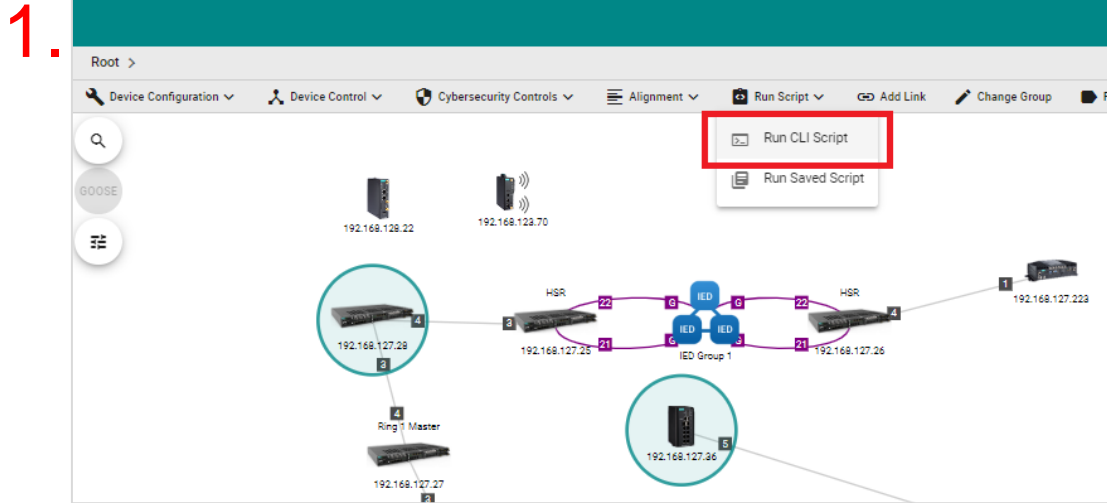
It will be very time-consuming especially when configuring multiple devices individually.



Users can execute the configuration or function by typing the command lines and save as a script to do mass configuration in MXview One

# Run Script

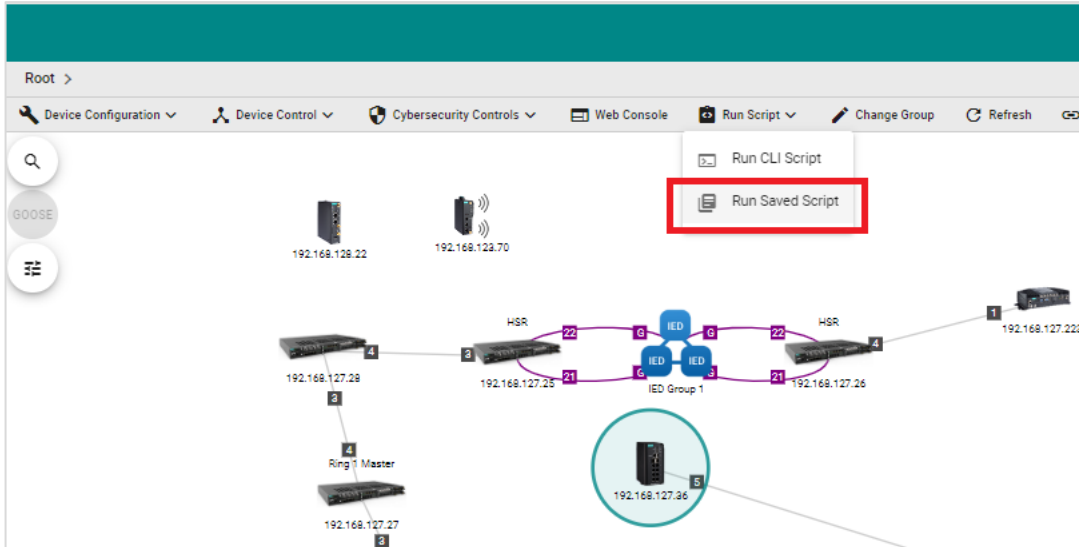
Device Management or Topology -> Run Script-> Run CLI Script



Can Save as a CLI Script or Run again

# Run Saved Scripts

- Device Management or Topology -> **Run Script-> Run Saved Script**



- Scheduling**

**Maintenance Scheduler**

Search:

	Job Name	Action	Description	Scheduled Time	Registered Devices
<input type="checkbox"/>	configuration	Run Saved Script	None	2024-02-19 PM5:31	3
<input type="checkbox"/>	Show memory	Run Saved Script	None	PM2:20, Daily	3

1 - 2 of 2

- Run a saved CLI script

**Run Saved Script**

Select a CLI Script

Search:

CLI Script Name	Description
<input checked="" type="radio"/> Reboot a device	Reboot a device
<input type="radio"/> Disable Port 1	Disable Port 1

CLI Script

```
reload
```

Selected Devices

IP	Alias	Model
192.168.127.16	192.168.127.16-EDS-4012-8P-4GS	EDS-4012-8P-4GS
192.168.127.11	192.168.127.11-EDS-G516E	EDS-G516E
192.168.127.12	192.168.127.12-EDS-G4008	EDS-G4008

Cancel Run

# Run Script – Value Proposition



- **Mass Configuration:** execute multiple devices at once
- **Saved CLI Scripts:** directly select and run the script which has been saved
- **Scheduling**

**MXview ONE**  
**v1.3.0**



Strengthen Network Visibility



Cybersecurity Management

# **MXview One v1.3.0**

## **Enhance Efficiency**

## **Cybersecurity Management**

# **Device Management**

Type keyword to search

Dashboard

Topology

Device Discovery

Device Management

Saved CLI Scripts

Firmware Management

Device Configuration Center

Event Management

Notification Management

Reports

Integration

Administration

Help

Select Operation

Device Configuration

Device Control

Cybersecurity Controls


Run Script


Web Console


<input type="checkbox"/>	192.168.127.4-ABB	ABB	192.168.127.4	00:21:C1:50:52:95	
<input type="checkbox"/>	192.168.127.5-ABB	ABB	192.168.127.5	00:21:C1:56:9B:B7	
<input type="checkbox"/>	192.168.127.11-EDS-G516E	EDS-G516E	192.168.127.11	00:90:E8:54:E1:E6	V6.4 build 23102508 Test
<input checked="" type="checkbox"/>	192.168.127.12-PT-G7728	PT-G7728	192.168.127.12	00:90:E8:71:1E:A5	V6.3 build 22120913 Switch Location
<input type="checkbox"/>	192.168.127.16-EDS-4012-8P-4GS	EDS-4012-8P-4GS	192.168.127.16	00:90:E8:90:A5:6E	v3.2 Build 2023_0719_1007
<input type="checkbox"/>	192.168.127.25-PT-G7728	PT-G7728	192.168.127.25	00:90:E8:71:1E:A5	V6.3 build 22120913 Switch Location
<input type="checkbox"/>	192.168.127.26-PT-G7728	PT-G7728	192.168.127.26	00:90:E8:86:19:CD	V6.3 build 22120913 Switch Location
<input type="checkbox"/>	192.168.127.27-PT-G7728	PT-G7728	192.168.127.27	00:90:E8:8E:F7:C6	V6.3 build 22120913 Switch Location
<input type="checkbox"/>	192.168.127.28-PT-G7828	PT-G7828	192.168.127.28	00:90:E8:79:23:82	V6.3 build 22120913 Switch Location

Design commonly used functions into **built-in buttons** to let users execute operations directly in MXview One

# Device Management

 Device Configuration

 Device Control

 Cybersecurity Controls

	Type		
	Device Configuration	Device Control	Cybersecurity Controls
Function	Dynamic Sticky MAC	Reboot	Sticky MAC On/Off
	Change Wi-Fi Channel	Create Snapshot	Relearn Dynamic Sticky MAC
	Add Wi-Fi SSID	Restore from Snapshot	Disable Unused Ethernet and Fiber Ports
			Disable Insecure HTTP and Telnet Console

# Scenario 1: To enhance network security, I need to configure and enable device's Sticky MAC function



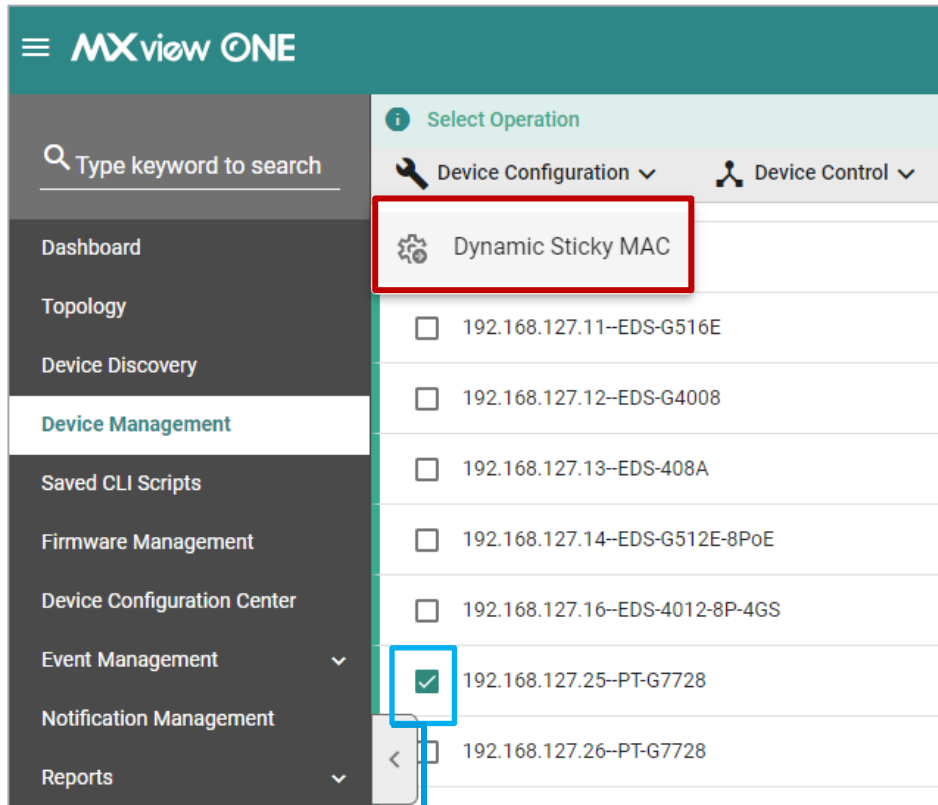
Operator  
Network administrator

- ① Device Deploy stage: configure Sticky MAC parameters on each port
- ② Operate stage: enable Sticky MAC function
- ③ Replace the old end-device

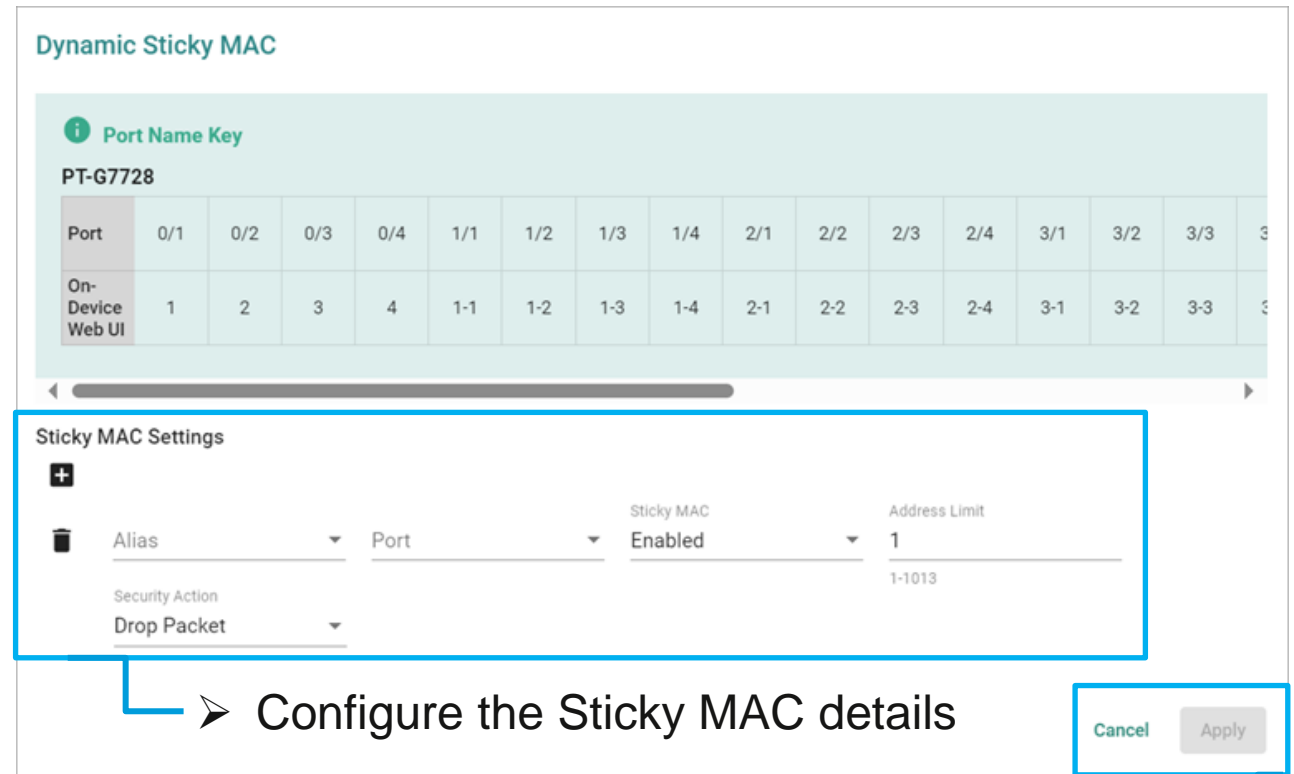
I need to **access the Web Console of each device** to make sure the device only receives the packets from trusted sources.

# Dynamic Sticky MAC

- Device Management or Topology -> **Device Configuration** -> **Dynamic Sticky MAC**



➤ Select one or multiple devices

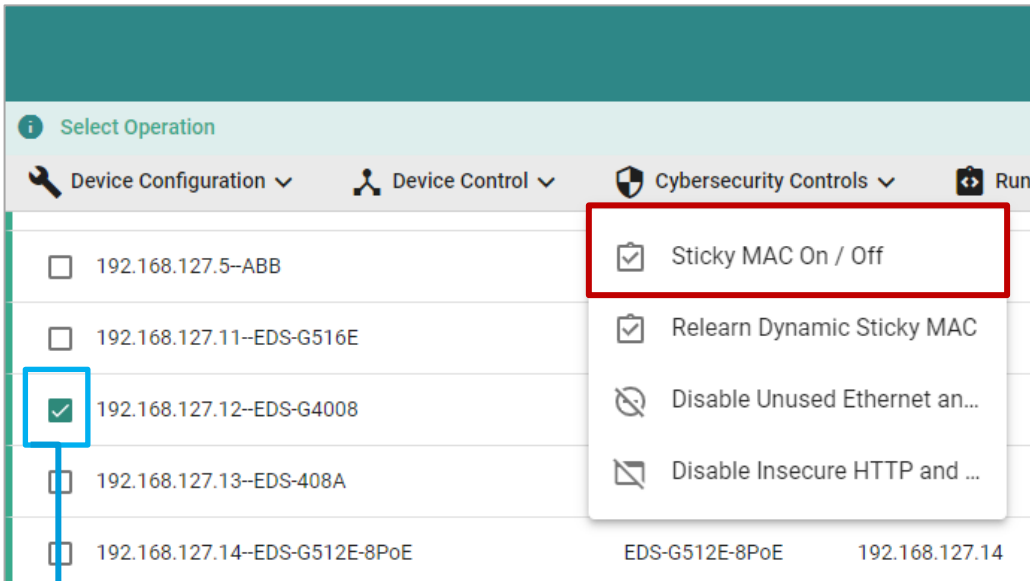


➤ Configure the Sticky MAC details

➤ Click Apply to execute

# Sticky MAC On / Off

- Device Management or Topology -> **Cybersecurity Controls** -> **Sticky MAC On / Off**



➤ Select one or multiple devices

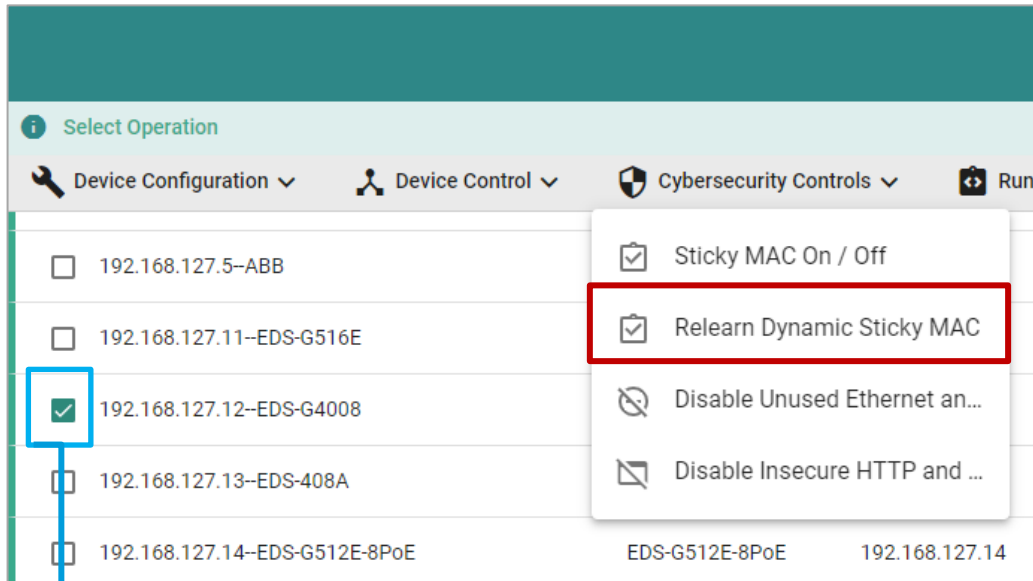


➤ Enable/Disable Sticky MAC function

➤ Click Apply to execute

# Relearn Dynamic Sticky MAC

- Device Management or Topology -> **Cybersecurity Controls** -> **Relearn Dynamic Sticky MAC**



➤ Select one or multiple devices



➤ Click Relearn to execute

# Scenario 2: In the Wi-Fi field, I need to efficiently modify the Wi-Fi parameters



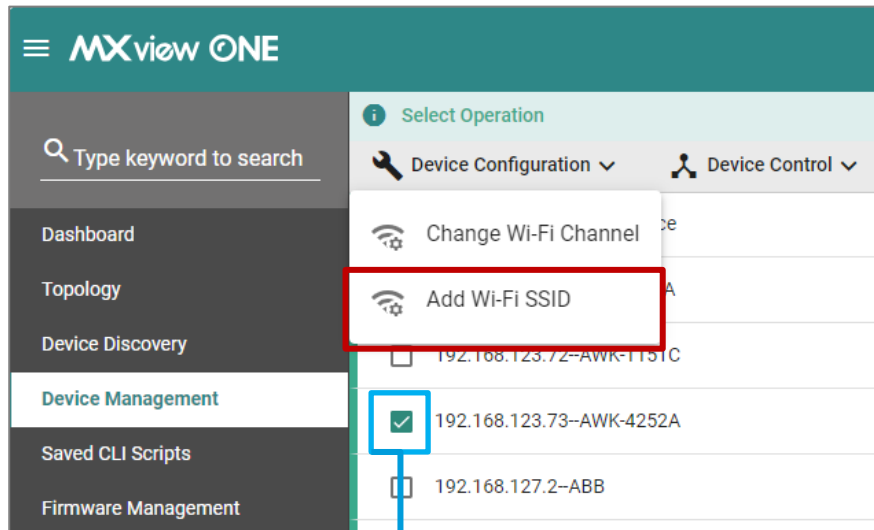
Operator  
Network administrator

- ① To add new devices to the wireless field
- ② Switch devices to another Wi-Fi channel for improved performance

I need to **adjust settings in each device's Web Console.**

# Add Wi-Fi SSID

- Device Management or Topology -> **Device Configuration** -> **Add Wi-Fi SSID**



➤ Select one or multiple devices

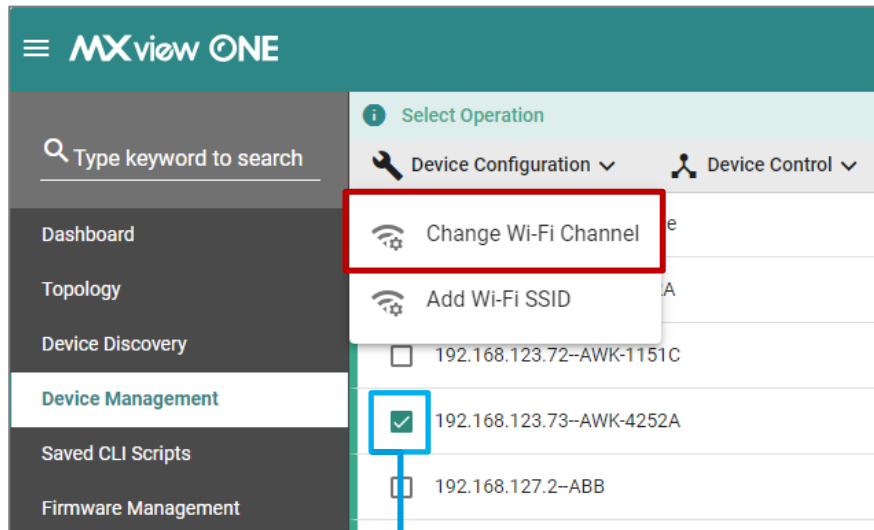
The screenshot shows the 'Add Wi-Fi SSID' configuration form. It includes a 'Clear All Existing SSIDs' dropdown set to 'Disabled'. The 'SSID \*' field is empty, with a character count '0 / 10'. The 'RF Band' dropdown is set to '2.4 GHz'. The 'Security' dropdown is set to 'Open'. A blue box highlights these three fields, with an arrow pointing to the text 'Modify the Wi-Fi SSID details'. Below the form is a table with columns 'IP', 'Alias', and 'Model'. The table contains one row: IP: 192.168.123.73, Alias: 192.168.123.73-AWK-4252A, Model: AWK-4252A. At the bottom right, there are 'Cancel' and 'Add' buttons. A blue box highlights these buttons, with an arrow pointing to the text 'Click Add to execute'.

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

➤ Click Add to execute

# Change Wi-Fi Channel

- Device Management or Topology -> **Device Configuration** -> **Change Wi-Fi Channel**



➤ Select one or multiple devices

➤ Modify the Wi-Fi channel details

### Change Wi-Fi Channel

<b>2.4G</b> Channel	<b>5G</b> Channel
1	36
1-13 Channel Width	36-196 Channel Width
20 MHz	20/40 MHz

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

Cancel Change

➤ Click Change to execute

# Scenario 3: Efficiently Rebooting Devices That Are Functioning Abnormally



Operator  
MXview One user

When devices begin to malfunction, the workaround procedure sometimes involves manually rebooting each device. This process requires accessing the web console for each device individually to perform a restart. Unfortunately, this method is time-consuming, especially when dealing with multiple devices.



# Reboot

- Device Management or Topology -> **Device Control** -> **Reboot**

MXview ONE

Select Operation

Device Configuration Device Control

Reboot

192.168.127.4--ABB

192.168.127.5--ABB

192.168.127.11--EDS-G516E

192.168.127.12--EDS-G4008

192.168.127.13--EDS-408A

192.168.127.14--EDS-G512E-8PoE

192.168.127.16--EDS-4012-8P-4GS

192.168.127.25--PT-G7728

- Select Sequence:
  - Strict Sequential
  - Smart Sequential\*

*\***Smart Sequential:** Reboot the devices based on the devices sequence, but will concurrently reboot devices in the same layer of the topology.*

Reboot

Reboot Sequence  
Strict Sequential

Order	IP	Alias	Model
1	192.168.127.11	192.168.127.11--EDS-G516E	EDS-G516E
2	192.168.127.13	192.168.127.13--EDS-408A	EDS-408A
3	192.168.127.36	192.168.127.36--PT-G510	PT-G510

Cancel Add to Scheduler Reboot

➤ Select one or multiple devices

➤ Execute now or set to scheduler

# Scenario 4: In the field that using industrial computer, I need to do snapshot backup or restore



Operator  
MXview One user

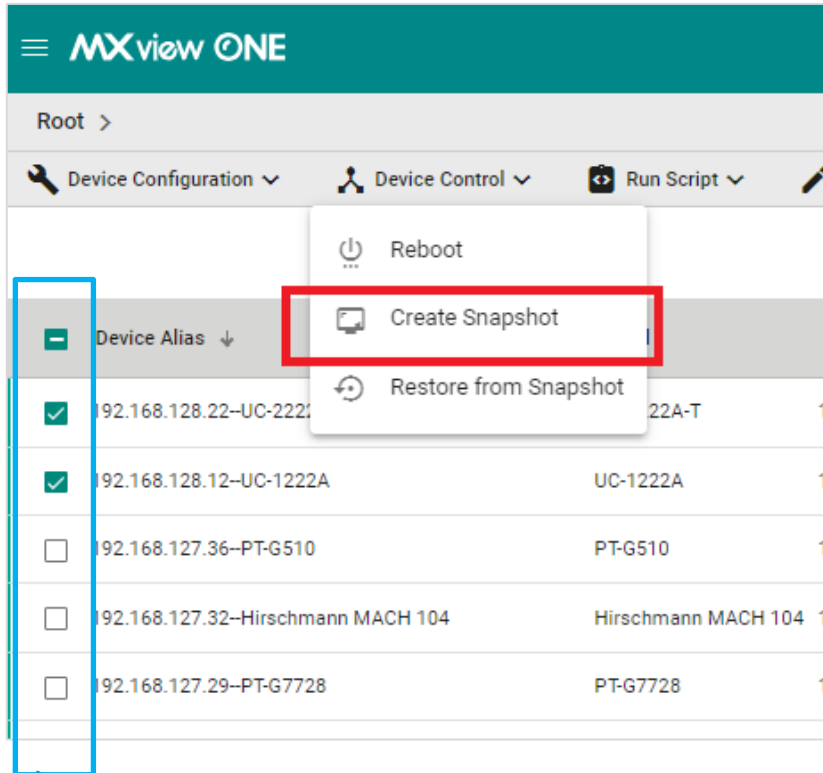
I take snapshots for **industrial computers** regularly.

When I find the status of the industrial computer is abnormal in MXview One, I will try to restore it to a previous snapshot to bring it back to its previous operational state.

However, the current process of executing and restoring snapshots **requires command line operations through the terminal**, which is inconvenient for me.

# Create Snapshot

- Device Management or Topology -> **Device Control-> Create Snapshot**

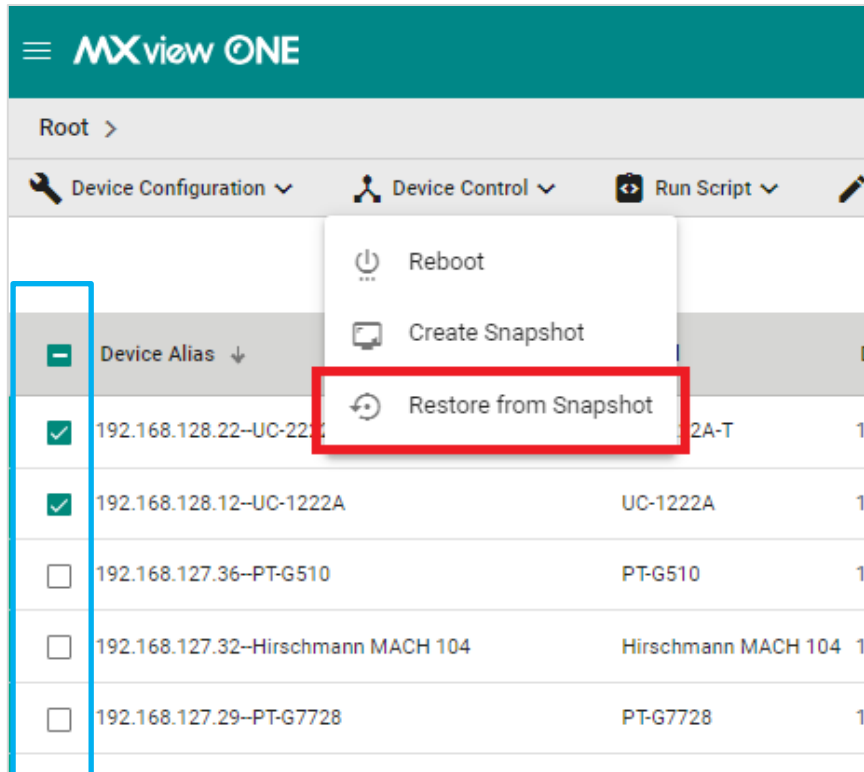


➤ Execute now or set to scheduler

➤ Select one or multiple UC devices

# Restore from Snapshot

- Device Management or Topology -> **Device Control-> Restore from Snapshot**



➤ Select one or multiple UC devices



➤ Execute now or set to scheduler

# Scenario 5: Manage devices from the perspective of network security management to reduce the probability of being attacked

Demo



Operator  
MXview One user

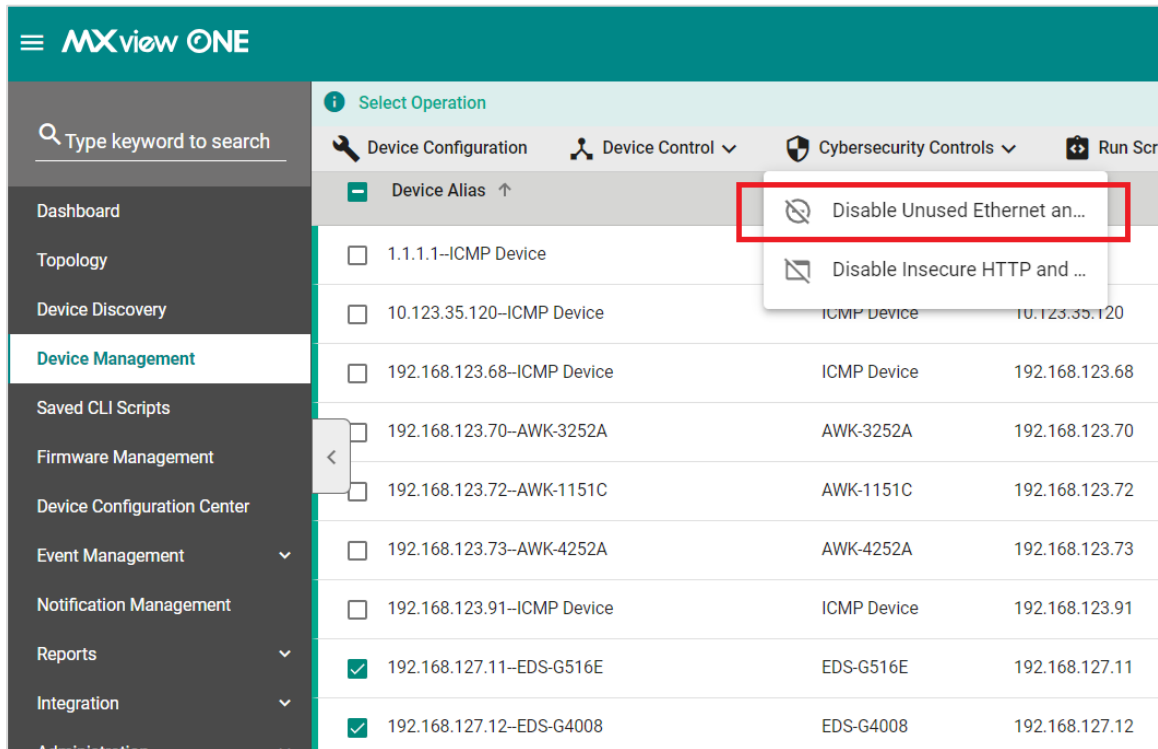
In order to ensure the devices communicate in a secure environment and to prevent them from becoming entry points for attacks.

- ① Check and disable unused physical ports during maintenance operations.
- ② Verify whether insecure HTTP and telnet consoles have been disabled on the devices.

Currently, I need to **access each device's Web console to check and set individually.**

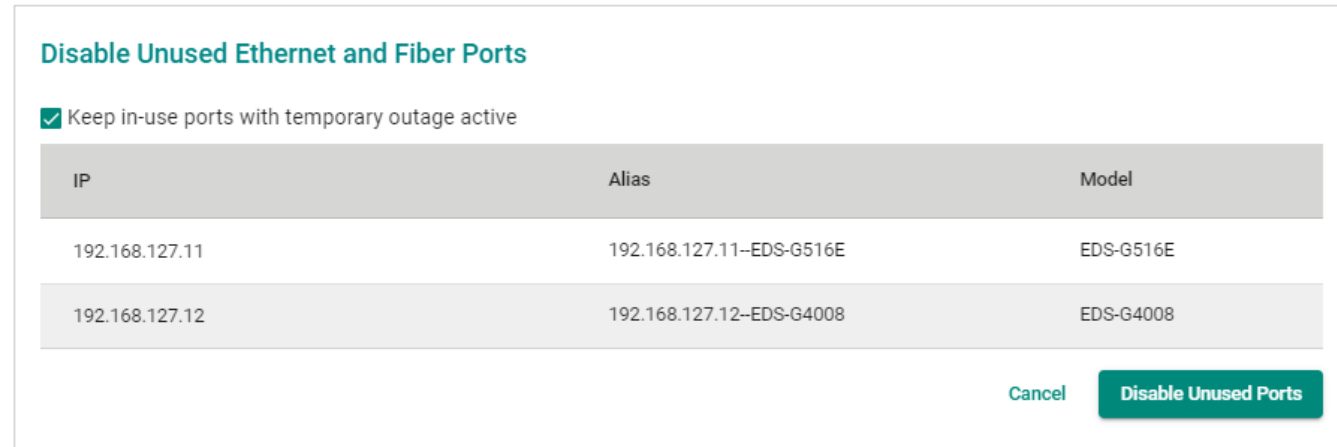
# Disable Unused Ethernet and Fiber Ports

- Device Management or Topology -> **Cybersecurity Controls** -> **Disable Unused Ethernet and Fiber Ports**



The screenshot shows the MXview ONE web interface. On the left is a sidebar with navigation links: Dashboard, Topology, Device Discovery, Device Management (highlighted), Saved CLI Scripts, Firmware Management, Device Configuration Center, Event Management, Notification Management, Reports, Integration, and Administration. The main content area has a 'Select Operation' header with tabs for Device Configuration, Device Control, Cybersecurity Controls (selected), and Run Scripts. Under Cybersecurity Controls, a dropdown menu is open, showing 'Device Alias' and 'Disable Unused Ethernet and Fiber Ports' (highlighted with a red box). Below this, a table lists various devices with checkboxes for selection.

IP	Alias	Model
1.1.1.1	ICMP Device	ICMP Device
10.123.35.120	ICMP Device	ICMP Device
192.168.123.68	ICMP Device	ICMP Device
192.168.123.70	AWK-3252A	AWK-3252A
192.168.123.72	AWK-1151C	AWK-1151C
192.168.123.73	AWK-4252A	AWK-4252A
192.168.123.91	ICMP Device	ICMP Device
192.168.127.11	EDS-G516E	EDS-G516E
192.168.127.12	EDS-G4008	EDS-G4008



The dialog box titled 'Disable Unused Ethernet and Fiber Ports' contains a checkbox 'Keep in-use ports with temporary outage active' which is checked. Below it is a table with three columns: IP, Alias, and Model. The table lists two devices: 192.168.127.11 (EDS-G516E) and 192.168.127.12 (EDS-G4008). At the bottom right, there are 'Cancel' and 'Disable Unused Ports' buttons.

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

# Disable Insecure HTTP and Telnet Console

- Device Management or Topology -> **Cybersecurity Controls** -> **Disable Insecure HTTP and Telnet Console**

The screenshot shows the MXview ONE interface. On the left is a sidebar with navigation options: Dashboard, Topology, Device Discovery, Device Management (highlighted), Saved CLI Scripts, Firmware Management, Device Configuration Center, Event Management, Notification Management, Reports, and Integration. The main area has a 'Select Operation' header with tabs for Device Configuration, Device Control, Cybersecurity Controls (selected), and Run Scripts. Below the tabs is a table of devices. A dropdown menu is open from the 'Cybersecurity Controls' tab, showing two options: 'Disable Unused Ethernet an...' and 'Disable Insecure HTTP and ...' (highlighted with a red box).

IP	Alias	Model
1.1.1.1	ICMP Device	
10.123.35.120	ICMP Device	
192.168.123.68	ICMP Device	
192.168.123.70	AWK-3252A	
192.168.123.72	AWK-1151C	
192.168.123.73	AWK-4252A	
192.168.123.91	ICMP Device	
192.168.127.11	EDS-G516E	
192.168.127.12	EDS-G4008	

The dialog box is titled 'Disable Insecure HTTP and Telnet Console'. It contains a table with the following data:

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

At the bottom right of the dialog are two buttons: 'Cancel' and 'Disable HTTP and Telnet'.

# Device Management - Value

	Type		
	Device Configuration	Device Control	Cybersecurity Controls
Function	Dynamic Sticky MAC	Reboot	Sticky MAC On/Off
	Change Wi-Fi Channel	Create Snapshot	Relearn Dynamic Sticky MAC
	Add Wi-Fi SSID	Restore from Snapshot	Disable Unused Ethernet and Fiber Ports
			Disable Insecure HTTP and Telnet Console



**Enhance Efficiency**

- Built-in button
- Mass Configuration
- Scheduling

**MXview ONE**  
v1.3.0



**Strengthen  
Network Visibility**



**Cybersecurity  
Management**

- Rapidly configure network access

# **MXview One v1.3.0**

## **Enhance Efficiency**

## **Cybersecurity Management**



## **Firmware Management**

# Scenario: I have the need to verify firmware versions and update for many devices



Operator  
MXview One user

As an OT operator, I hope devices in the field operate in a low risk environment. So when the firmware release fixes cybersecurity issues, I tend to update the firmware.

Currently, I have to **individually check the Moxa website to review release notes, download the files, and then return to MXview One for the update.**

The whole process for updating firmware is time-consuming.

🔍 Type keyword to search

Dashboard

Topology

Device Discovery

Device Management

Saved CLI Scripts

**Firmware Management**

Device Configuration Center

Event Management

Notification Management

Reports

Integration

Administration

Help

## Firmware Management

### Check Firmware Status

Moxa Firmware Server Status: ✔ Connected

Last Checked: 2024/01/09 AM 12:46:09

Check Interval: N/A

Check Now

Enable Check Interval

MXview One integrates with Moxa Software Release Service (**Moxa SRS**) to check whether the monitored devices run the latest firmware. Users can check each firmware version's release notes before downloading and executing firmware updates.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Models	Status	Current Version	Release Notes	Progress
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	PT-G510	<span style="color: red;">⚠</span> Not updated	v6.5		None
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	PT-G7728	<span style="color: orange;">⚠</span> Partially updated	v6.3		v6.3 100%
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	AWK-1151C	<span style="color: green;">😊</span> All updated	v2.0		None
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	AWK-4252A	<span style="color: green;">😊</span> All updated	v2.0		None

# Firmware Management

➤ Check version's release note

**MXview ONE**

Search: Type keyword to search

**Firmware Management**

Check Firmware Status

Moxa Firmware Server Status: Connected  
Last Checked: 2024/01/16 PM 11:48:18  
Check Interval: N/A

[Check Now](#) [Enable Check Interval](#)

Models Ignored Models

**Hint for security patch**

	Model Series	Device Status	Latest Version on the Firmware Server	Selected Version	Selected Firmware Download Status
<input type="checkbox"/>	EDS-408A	Not updated	v3.13	None	
<input type="checkbox"/>	EDS-G512E-8PoE	Not updated	v6.4	None	
<input type="checkbox"/>	PT-G510	Not updated	v6.5	None	
<input type="checkbox"/>	PT-G7728	Partially updated	v6.3	v6.3	
<input type="checkbox"/>	AWK-1151C	All updated	v2.0	None	
<input type="checkbox"/>	AWK-3252A	All updated	v2.0	None	
<input type="checkbox"/>	AWK-4252A	All updated	v2.0	None	
<input type="checkbox"/>	EDS-4012-8P-4GS	All updated	v3.2	None	
<input type="checkbox"/>	EDS-G4008	All updated	v3.2	None	

**Select Firmware**

Version: 6.3

**Release Notes**

**Version**  
6.3

**Change**  
1. Updated the PT-G7X28 panel image to match the EC version appearance which has no Micro USB on the front panel.

**Enhancement**  
1. [PTP] The PTP domain number will change depending on the parameters of the PTP profile.

**Feature**  
N/A

**Fix**  
1. [PTP] The "UTC Offset Valid" field shows incorrectly on the System Time page.  
2. [PTP] The path delay is calculated twice.  
3. [PTP] The system does not send inaccurate power profile TLV received from the Master to the Slave.  
4. [PTP] When the device is configured for one-step sync but receives two-step sync, the correction field is not properly updated.  
5. [OpenSSL] [CVE-2022-0778] Vulnerability in OpenSSL.  
6. [PoE] Navigating to the PoE Diagnostic page through HTTPS causes a memory leak.  
7. [Fiber Check] TX/RX power warnings are shown on the SFP-RJ45 module.  
8. [Fiber Check] The event for low RX power does not trigger correctly.  
9. [MMS] The character restrictions for the IED name are not applied.  
10. [MMS] Changing the IED name will cause the system to reboot.  
11. [GPNSE Check] The GPNSE tempered port event is recorded incorrectly in the event log.

[Cancel](#) [Select](#)

# Firmware Management

➤ Select one or multiple devices

The screenshot shows the 'Models' tab in the Firmware Management interface. A red box highlights the 'Add' icon (a square with a plus sign) in the top left corner. A blue box highlights the 'Select Devices' dialog box, which is open over the device list. The dialog box contains a table with columns: IP, Alias, Model Series, Current Version, and Selected Version. The table lists several devices, some of which are selected with a green checkmark. The 'Next' button is visible at the bottom right of the dialog box.

IP	Alias	Model Series	Current Version	Selected Version
<input type="checkbox"/> 1.1.1.5	1.1.1.5-PT-G7728	PT-G7728		v6.3
<input checked="" type="checkbox"/> 192.168.127.29	192.168.127.29-PT-G7728	PT-G7728	V6.2 build 21110316	v6.3
<input checked="" type="checkbox"/> 192.168.127.25	192.168.127.25-PT-G7728	PT-G7728	V6.3 build 22120913	v6.3
<input type="checkbox"/> 1.1.1.6	1.1.1.6-PT-G7728	PT-G7728		v6.3
<input checked="" type="checkbox"/> 1.1.1.7	1.1.1.7-PT-G7728	PT-G7728		v6.3
<input type="checkbox"/> 192.168.127.26	192.168.127.26-PT-G7728	PT-G7728	V6.3 build 22120913	v6.3
<input type="checkbox"/> 192.168.127.27	192.168.127.27-PT-G7728	PT-G7728	V6.3 build 22120913	v6.3
<input checked="" type="checkbox"/> 192.168.127.11	192.168.127.11-EDS-G516E	EDS-G516E	V6.4 build 23102508	v6.4

➤ Select Sequence:  
- Smart Sequential\*  
- Strict Sequential

\***Smart Sequential:** based on the devices sequence, but will concurrently execute in the same layer of the topology

## Upgrade Sequence

Update Mode  
Strict Sequential

Order	IP	Alias	Model Series	Current Version	Selected Version
1	192.168.127.11	192.168.127.11-EDS-G516E	EDS-G516E	V6.4 build 23102508	v6.4
2	192.168.127.25	192.168.127.25-PT-G7728	PT-G7728	V6.3 build 22120913	v6.3
3	192.168.127.26	192.168.127.26-PT-G7728	PT-G7728	V6.3 build 22120913	v6.3
4	192.168.127.27	192.168.127.27-PT-G7728	PT-G7728	V6.3 build 22120913	v6.3
5	192.168.127.29	192.168.127.29-PT-G7728	PT-G7728	V6.2 build 21110316	v6.3

Cancel

Scheduled Upgrade

Upgrade Now

➤ Execute now or set to scheduler

# Firmware Management- Value



**Enhance Efficiency**

- Instant update notification from Moxa official release
- Automatically download and deploy by user control or scheduling

**MXview ONE**  
**v1.3.0**



**Strengthen Network Visibility**



**Cybersecurity Management**

- Raise the efficiency of vulnerability management

# **MXview One v1.3.0**

## **Strengthen Network Visibility**

User-defined SNMP  
Device Plug-in

# Scenario: I hope to monitor more third-party device information in MXview One



Operator  
MXview One user

MXview One enables me to use a single network management software to monitor both Moxa and third-party network devices.

However, MXview One can only displays the information in the Public MIB for the third-party devices. There is more device information that I wish to monitor which are not visible, requiring me to **use other tools such as MIB Browser or the other manufacturer's network management software to confirm.**

Server Control

Configuration

DB Backup & Restore

Plug-in Manager

Certificates

## < Add an SNMP Model Plug-In

1

Specify sysObjectID

2

Load Device Files

3

Select and Test OIDs

4

OID Alias and Value Definition

sysObjectID \*

Model \*

Next

For the third-party SNMP devices monitored in MXview One, users can upload MIB files and define OIDs and OID syntax mapping. This information can then be used to monitor additional third-party device properties in MXview One.

# User-defined SNMP Device Plug-In

- MXview One Control Panel -> **Plug-in Manager** -> **SNMP Devices**

The screenshot displays the MXview One Control Panel interface. On the left is a sidebar with navigation links: Server Control, Configuration, DB Backup & Restore, Plug-in Manager (highlighted), and Certificates. The main content area is titled 'Plug-in Manager' and has two tabs: 'Moxa Devices' and 'SNMP Devices' (which is active). Under the 'SNMP Devices' tab, there is a section 'Upload a plug-in file' with a text input field labeled 'Select a plug-in file' and a file selection icon, followed by an 'Upload' button. Below this is a section 'Supported Device Model(11)' with a search bar. A table lists 11 supported device models, each with a checkbox, edit, add, and delete icon, and the device name.

Model
<input type="checkbox"/> Hirschmann MACH
<input type="checkbox"/> ABB
<input type="checkbox"/> Alcatel
<input type="checkbox"/> Cisco Device
<input type="checkbox"/> Emerson
<input type="checkbox"/> Hirschmann
<input type="checkbox"/> HP Networking Device
<input type="checkbox"/> Rockwell
<input type="checkbox"/> Schneider

# User-defined SNMP Device Plug-In

➤ 4 steps to add an SNMP Model Plug-In

**MXview One Control Panel** English admin ▼

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

## < Add an SNMP Model Plug-In

- 1** Specify sysObjectID
- 2 Load Device Files
- 3 Select and Test OIDs
- 4 OID Alias and Value Definition

sysObjectID \*  Get sysObjectID  
0 / 255

Model \*   
0 / 40

Next

# User-defined Device Plug-in- Value



**MXview ONE**  
**v1.3.0**



**Strengthen Network Visibility**

- Monitor more information for third-party devices



Cybersecurity Management

# Key Takeaways

# Takeaways



Enhance Efficiency

Strengthen Network Visibility

Cybersecurity Management



2024-01-31

# Thank You



# FAQ

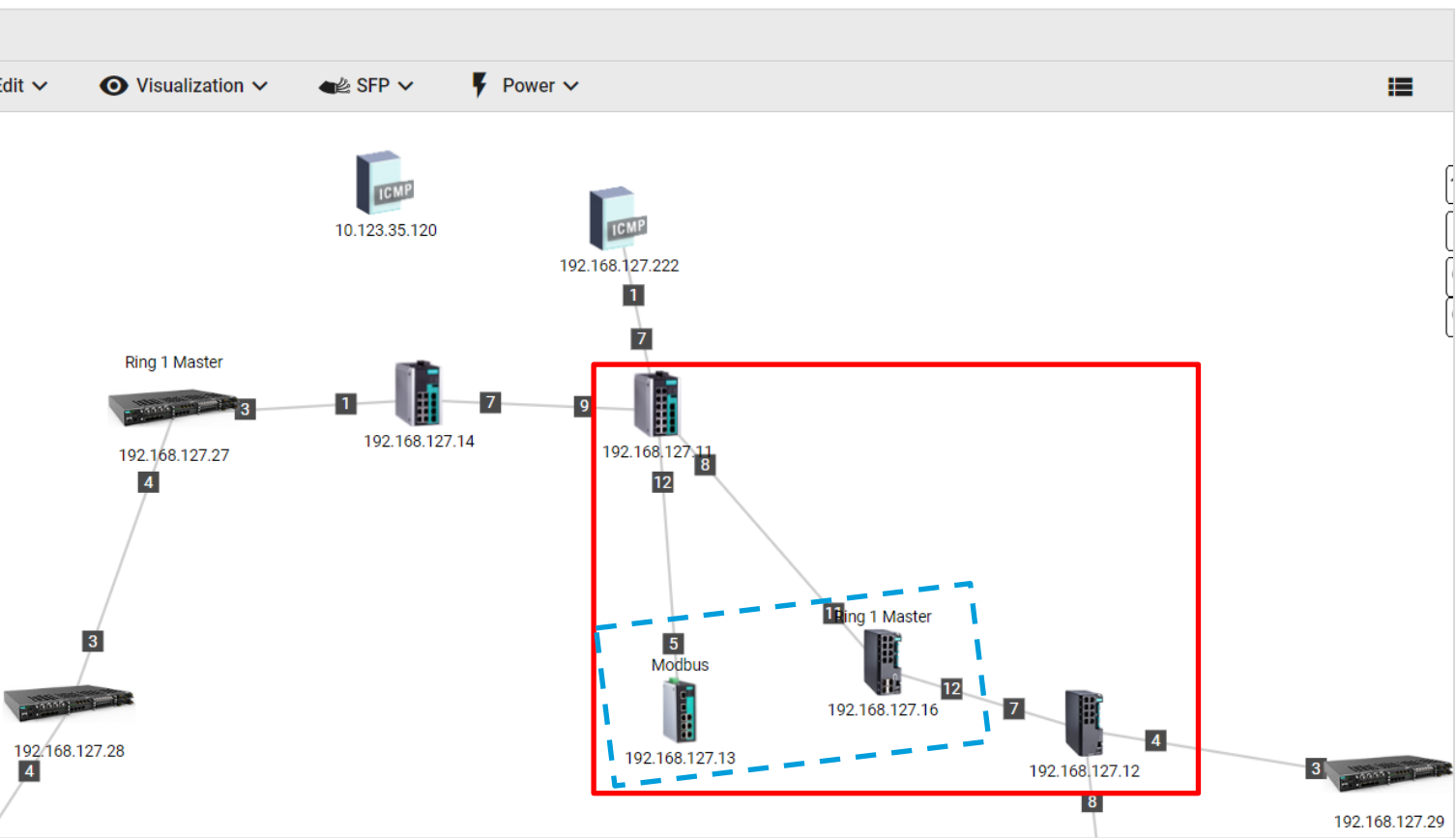
# Q: Is there the supported device list for device management functions?

Type	Function	Supported Device
Device Configuration	Dynamic Sticky MAC	- MX-NOS Switches - PT-G7728 - PT-G510
	Change Wi-Fi Channel	- AWK-3252A,AWK-3262A,AWK-4252A,AWK-4262A,AWK-1151C,AWK-1161A AWK-1161C, AWK-1165A,AWK-1165C
	Add Wi-Fi SSID	- AWK-3252A, AWK-3262A, AWK-4252A, AWK-4262A, AWK-1151C, AWK-1161A AWK-1161C, AWK-1165A, AWK-1165C
Device Control	Reboot	- eCos Switch ( <i>*Not included SDS Series</i> ) - MX-NOS Switch - EDR Series (EDR, OnCell-G4302, TN-4908, TN-4916) - UC Series - AWK New Series - NPort 6000 Series - PT-G503
	Create Snapshot	- UC Series (UC-8200 Series, UC-2200A Series, UC-1200A Series)
	Restore from Snapshot	- UC Series (UC-8200 Series, UC-2200A Series, UC-1200A Series)

# Q: Is there the supported device list for device management functions?

Type	Function	Supported Device
Cybersecurity Controls	Sticky MAC On/Off	- MX-NOS Switches
	Relearn Dynamic Sticky MAC	- MX-NOS Switches - PT-G7728 - PT-G510
	Disable Unused Ethernet and Fiber Ports	- eCos Switches ( <i>*Not include SDS Series</i> ) - MX-NOS Switches - EDR Series (EDR, OnCell-G4302, TN-4908, TN-4916) - PT-G503
	Disable Insecure HTTP and Telnet Console	- eCos Switches ( <i>*Not include SDS Series</i> ) - MX-NOS Switches - EDR Series (EDR, OnCell-G4302, TN-4908, TN-4916) - New AWK Series - NPort 6000 Series - PT-G503

# Q: Can explain more details on what is “Smart Sequential”?



**Smart Sequential:** based on the devices sequence, but will concurrently execute in the same layer of the topology

## Upgrade Sequence

Update Mode

Smart Sequential

Order	IP	Alias	Model Series
1	192.168.127.12	192.168.127.12-EDS-G4008	EDS-G4008
2	192.168.127.13	192.168.127.13-EDS-408A	EDS-408A
2	192.168.127.16	192.168.127.16-EDS-4012-8P-4GS	EDS-4012-8P-4GS
3	192.168.127.11	192.168.127.11-EDS-G516E	EDS-G516E

## Upgrade Sequence

Update Mode

Strict Sequential

Order	IP	Alias	Model Series
1	192.168.127.12	192.168.127.12-EDS-G4008	EDS-G4008
2	192.168.127.13	192.168.127.13-EDS-408A	EDS-408A
3	192.168.127.16	192.168.127.16-EDS-4012-8P-4GS	EDS-4012-8P-4GS
4	192.168.127.11	192.168.127.11-EDS-G516E	EDS-G516E