

# MXview One v1.4.0

## New Features

**Ahmed Mabrouk, TS**

**Branislav Radak, FAE**

January 30<sup>th</sup>, 2025

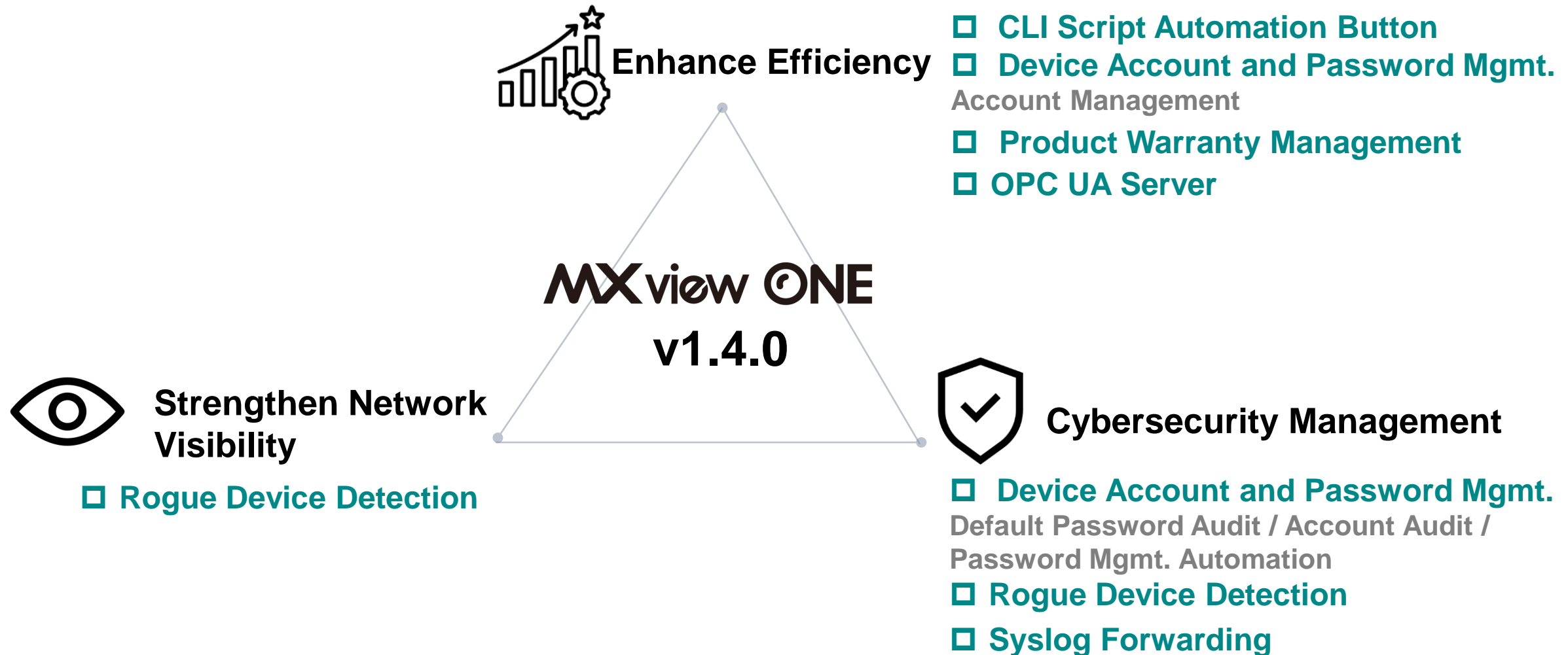
**MXview ONE**

**MOXA®**  
Reliable Networks ▲ Sincere Service

# 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

# Overview of New Features





OT-Tailored Operation

# MXview One v1.4.0 New Feature

## CLI Script Automation Button

**Demo**

# Scenarios

1

When an emergency occurs, clients hope there is a function to assist operators in quickly and effectively resolving it.



SI

Customers hope that when an emergency occurs, the operator can quickly and effectively resolve it.

I think this requirement can be met with the Run Script function, but currently, they need to select devices to apply the saved script.

It will take time to select devices and may be prone to errors since there are many devices in the field.

2

OT engineers are more used to operating and controlling devices with the SCADA button type method.



OT  
Engineer

I am used to operating and controlling devices with the SCADA button type method. However, MXview One does not have this functionality, so I use the Run Script function to do mass configuration.

Since I am less familiar with scripts, I need to put more effort into learning it, and it is more prone to operational errors.

Type keyword to search

Dashboard

Topology

Device Discovery

Device Management

Saved CLI Scripts

Firmware Management

Device Configuration Center

Event Management

Notification Management

Inventory Management

Integration

Administration

Help

## Saved CLI Scripts

CLI Scripts

Execution Results

Script Automation

Automation Button



Search



same\_cli\_btn2

153&154

Customized one-click button to execute the operations defined by users on multiple saved CLI scripts and corresponding devices

# Create the Script Automation



- Saved CLI Scripts-> **Script Automation**
- A Script Automation is composed of multiple CLI scripts and corresponding devices

The screenshot displays the MXview ONE interface. On the left, the 'Saved CLI Scripts' table lists several scripts. A blue box highlights the '+' icon in the top-left corner of the table, with an arrow pointing to the text 'Select scripts from Saved CLI Script'. On the right, the 'Add Script Automation' dialog is open. A blue box highlights the 'Name' and 'Description' fields, with an arrow pointing to the text 'Configure the script automation name and description'. Another blue box highlights the 'CLI Script and Target Device' section, which contains a list of scripts and their target devices. An arrow points from this section to the text 'Select the corresponding devices'. The dialog also includes 'Close' and 'Apply' buttons at the bottom right.

**MXview ONE**

**Saved CLI Scripts**

	Name	Description
<input type="checkbox"/>	start-btn	A-btn-192.168.123.152
<input type="checkbox"/>	diff_cli-btn	A-btn-192.168.123.153
<input type="checkbox"/>	same_cli_btn1	153&154
<input type="checkbox"/>	same_cli_btn2	153&154

**Add Script Automation**

Name: 關閉純水系統  
Description: 一鍵讓所有跟純水系統系統連接的交換機port enable

**CLI Script and Target Device**

Select Saved CLI Script *	Target Device *
Disable Port 1	192.168.127.11-EDS-G516E, 192.1..
Disable Port 2	192.168.127.12-EDS-G4008
Disable Port 3	192.168.127.13-EDS-408A

☐ All Devices  
☐ 192.168.127.11-EDS-G516E  
☐ 192.168.127.12-EDS-G4008

Close Apply

➤ Select scripts from Saved CLI Script

➤ Configure the script automation name and description

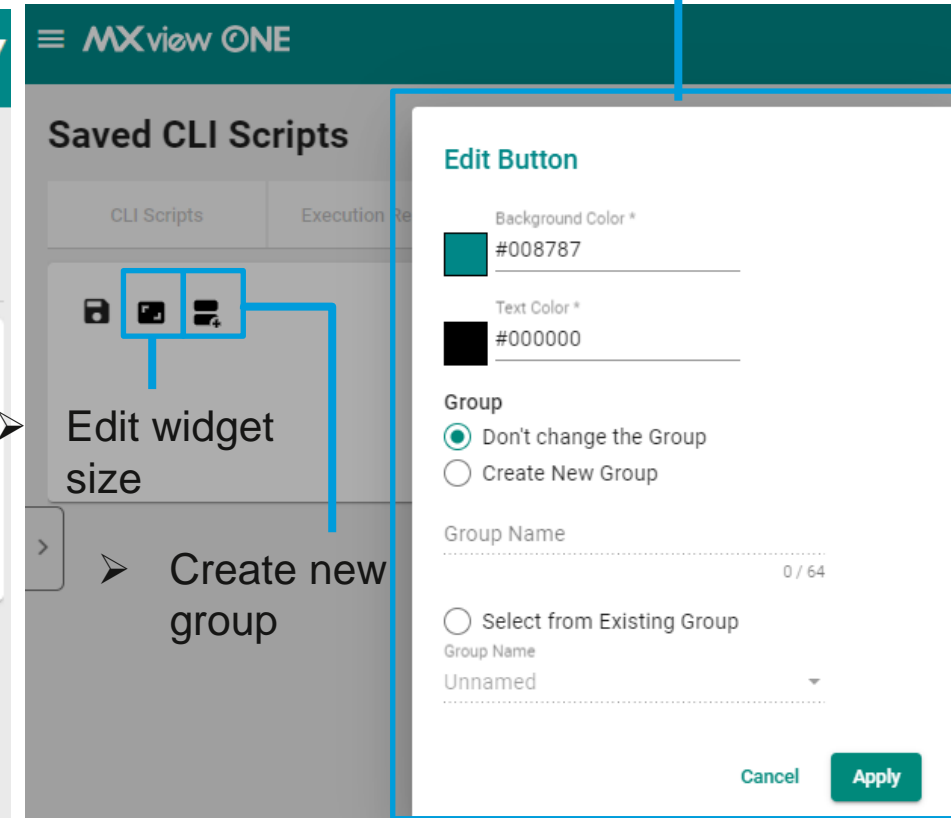
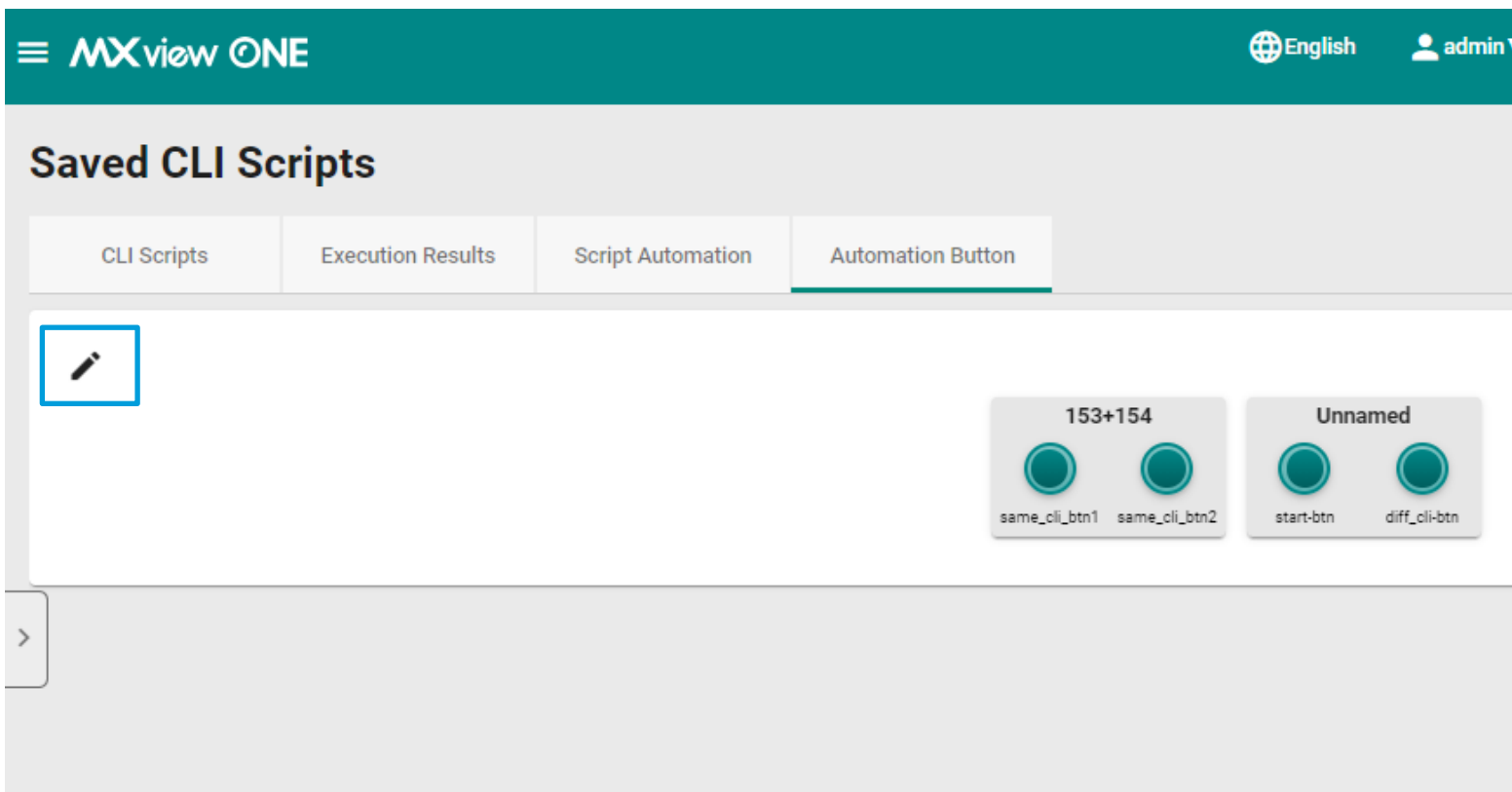
➤ Select the corresponding devices

# Automation Button



- Saved CLI Scripts-> **Automation Button**
- Each created Script Automation will be an automation button
- The appearance will be accurately displayed in the topology

➤ Edit the button color, text color or located group





# Execute the Automation Button

- Click on the button to execute the operation
- Automation Button page can be set as the Start Page

MXview ONE English admin

Saved CLI Scripts

CLI Scripts Execution Results Script Automation Automation Button

Execute a Button : start-btn

Confirm to proceed.

Cancel Confirm

MXview ONE English admin

Root

Topology Group Edit Visualization SFP Power

GOOSE

192.168.123.165 192.168.127.1

Ring 1 Master Modbus

153+154

same\_cli\_btn1 same\_cli\_btn2

Unnamed

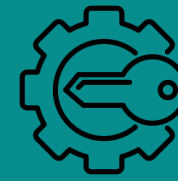
start-btn diff\_cli\_btn

Execute a Button : start-btn

Confirm to proceed.

Cancel Confirm

<input type="checkbox"/>	ID	Source	Source IP	Device Alias	Description	Time Issued
<input type="checkbox"/>	1020		MXview One		admin from IP: 127.0.0.1 starts to execute the button: start-btn, and the execution result is All Finished.	2024-06-09 21:50:53
<input type="checkbox"/>	1019		MXview One		admin from IP: 127.0.0.1 starts to execute the button: start-btn.	2024-06-09 21:50:40



Password Management

# MXview One v1.4.0 New Feature

## Device Account and Password Management

**Demo**

# Scenarios

1

## Manage all accounts of devices

It's difficult to effectively manage all devices' accounts. I need to log into device's Web Console to check the status. It is also hard to know if there are any suspicious accounts in the devices.

2

## Regularly change passwords on each device

To comply with regulations, I regularly change the device passwords. However, logging into each device's web console to check if the default password is still used and to change the passwords individually is very time-consuming.

3

## Provide the device credentials to the operator

When there are issues, I need to provide a temporary account and password to maintenance person for troubleshooting. However, after the maintenance is completed, the passwords need to be changed again, causing management difficulties



### Network administrator

(Moxa total solution users: buy Moxa devices and use MXview One to manage)

Type keyword to search

Dashboard  
Topology  
Device Discovery  
Device Management  
Configuration and Control  
Account and Password  
Saved CLI Scripts  
Firmware Management  
Device Configuration Center  
Event Management  
Notification Management  
Inventory Management  
Integration  
Administration  
Help  
About MXview One  
User Manual

## Account and Password Management Automation

Account Management

Password Automation

Account Audit

Default Password Audit

Temporary Account

## Accounts Information

Click the 'Refresh' button to retrieve all device accounts. This will take time to process.

Refresh



Only the MXview One authority **Administrator** can use it.

Device account and password management function lets administrators easily monitor and manage the devices accounts. There are also functions to help them regularly change default passwords.

<input type="checkbox"/>	Dev				
<input type="checkbox"/>		192			
<input type="checkbox"/>		192			
<input type="checkbox"/>		192.168.127.15-ICMP Device	NO	ICMP Device	192.168.127.15
<input type="checkbox"/>		192.168.127.16-EDS-4012-8P-4GS	Yes	EDS-4012-8P-4GS	192.168.127.16
<input type="checkbox"/>		192.168.127.25-PT-G7728	Yes	PT-G7728	192.168.127.25
<input type="checkbox"/>		192.168.127.27-PT-G7728	Yes	PT-G7728	192.168.127.27

# 1. Account Management

1

Manage all accounts of devices



- Device Management-> Account and Password-> **Account Management**
- Account Management displays an overview of all accounts of the Moxa devices

## ➤ Add / Delete account

**Add Account**

Operation \*  
Edit Account ▼

☒ Add Account ☐ Delete Account

Username \*  
0 / 64

Password \*  
0 / 64

Authority \*  
Admin ▼

## ➤ Edit default admin name and its password

**Account Management**

Operation \*  
Change Default "Admin" Name ▼

New Username \*  
0 / 64

New Password \*  
0 / 64

## Account and Password Management Automation

Account Management

Password Automation

Account Audit

Default Password Audit

Temporary Account

### Accounts Information

Click the 'Refresh' button to retrieve all device accounts. This will take time to process.

Refresh

## ➤ Display accounts of supported Moxa devices

	Device Alias ↑	Compatibility	Model	Device IP	Accounts
<input type="checkbox"/>	10.123.35.120-ICMP Device	No	ICMP Device	10.123.35.120	N/A
<input type="checkbox"/>	192.168.127.11-EDS-G516E	Yes	EDS-G516E	192.168.127.11	admin,user,test-0529,even
<input type="checkbox"/>	192.168.127.14-EDS-G512E-8PoE	Yes	EDS-G512E-8PoE	192.168.127.14	admin,user,test0520
<input type="checkbox"/>	192.168.127.15-ICMP Device	No	ICMP Device	192.168.127.15	N/A
<input type="checkbox"/>	192.168.127.16-EDS-4012-8P-4GS	Yes	EDS-4012-8P-4GS	192.168.127.16	admin,user
<input type="checkbox"/>	192.168.127.29-PT-G7728	Yes	PT-G7728	192.168.127.29	admin,user,abc

## 2. Account Audit

1

Manage all accounts of devices



- Device Management-> Account and Password-> **Account Audit**
- Account Audit displays whether there are accounts change in the device

➤ Retrieve account list for Moxa devices and establish it as a baseline

**Account and Password Management Automation**

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

Account Status Baseline  
Creation Time: N/A  
**Create**

Device Alias	Compatibility	Model	Device IP	Baseline Account	Added Account	Deleted Account
192.168.127.14-EDS-G512E-8PoE	Yes	EDS-G512E-8PoE	192.168.127.14	N/A	N/A	N/A
192.168.127.16-EDS-4012-8P-4GS	Yes	EDS-4012-8P-4GS	192.168.127.14	N/A	N/A	N/A
192.168.127.25-PT-G7728	Yes	PT-G7728	192.168.127.14	N/A	N/A	N/A
192.168.127.26-PT-G7728	Yes	PT-G7728	192.168.127.14	N/A	N/A	N/A
192.168.127.40-NPort-6250	No	NPort-6250	192.168.127.40	N/A	N/A	N/A

# 2. Account Audit

1 Manage all accounts of devices

### Account and Password Management Automation

Account ManagementPassword AutomationAccount AuditDefault Password AuditTemporary Account

#### Account Status Baseline

Creation Time: 2024-11-25 PM 04:47:05

Create

#### Account Status Audit

Last Audit Time: 2024-12-25 PM 04:47:05

Next Audit Start Time: 2024-11-25 PM 04:47:05

Audit

#### Audit Automation

Enable \*

Enabled

Schedule Interval \*

180

7-365 Days

Save

Search

Device Alias	Compatibility	Model	Device IP	Baseline Account	Added Account	Deleted Account
192.168.127.14-EDS-G512E-8PoE	Yes	EDS-G512E-8PoE	192.168.127.14	admin, user	test1, test2	admin
192.168.127.16-EDS-4012-8P-4GS	Yes	EDS-4012-8P-4GS	192.168.127.14	admin, user	N/A	N/A
192.168.127.25-PT-G7728	Yes	PT-G7728	192.168.127.14	admin, user	test1, test2	admin
192.168.127.26-PT-G7728	Yes	PT-G7728	192.168.127.14	admin, user	N/A	N/A
192.168.127.40-NPort-6250	No	NPort-6250	192.168.127.40	N/A	N/A	N/A

➤ Manual or scheduling to execute account audit

➤ Display the differences from the baseline, including which accounts have been added or deleted

# 3. Password Automation

2

Regularly change passwords on each device



- Device Management-> Account and Password-> **Password Automation**
- Password Automation function can generate randomized passwords and apply them to the selected devices automatically and periodically.

## • Password Automation Settings

- Email receiver
- Managed devices
- Random password length

**Automation Password Settings**

1 Verify Email Receiver   2 Select Device   3 Random Password Complexity   4 Set Password to Device

**Verify Account and Password Email Receiver**

⚠ If you do not see verification code, check your spam folder or [Email Server Configuration](#)

1st Email Receiver \*  
brandon.yang@moxa.com

Verification Code  
3 7 7 9 0 1 **Confirm**

Verification code expiration: 9:59  
**Resend**

**Automation Password Settings**

1 Verify Email Receiver   2 **Select Device**   3 Random Password Complexity   4 Set Password to Device   5 Send Password Email

Select the device to use a random password.

<input checked="" type="checkbox"/> Device Alias	Compatibility	Model	Device IP	Applied Accounts
<input checked="" type="checkbox"/> 192.168.127.14-EDS-G512E-8PoE	Yes	EDS-G512E-8PoE	192.168.127.14	admin, user, test...
<input checked="" type="checkbox"/> 192.168.127.16-EDS-4012-8P-4GS	Yes	EDS-4012-8P-4GS	192.168.127.16	admin, user, test...
<input checked="" type="checkbox"/> 192.168.127.25-PT-G7728	Yes	PT-G7728	192.168.127.25	admin, user, test...
<input checked="" type="checkbox"/> 192.168.127.26-PT-G7728	Yes	PT-G7728	192.168.127.26	admin, user, test...
<input type="checkbox"/> 192.168.127.40-NPort-6250	No	NPort-6250	192.168.127.40	N/A

**Close** **Next**

**Automation Password Settings**

1 Verify Email Receiver   2 Select Device   3 **Random Password Complexity**   4 Set Password to Device

MXview One generates a random password, which is managed by MXview One.

⚠ Must check the maximum password length of devices.

Random Password Length \*  
8  
8-63

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

➤ Verify the email recipient and enter the verification code

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

➤ Set the length of randomized password



# 3. Password Automation

2

Regularly change passwords on each device

- **Start Over:** Reset and start from scratch
- **Regenerate Password:** Regenerate random passwords for selected devices and set passwords to each device
- **Resend Password Email:** Resend the current random passwords list to the receiver's email address

### Account and Password Management Automation

Account Management

Password Automation

Account Audit

Default Password Audit

Temporary Account

#### Password Automation

Last Execution Time: 2024-05-25 AM 11:00

Next Scheduled Start Time: 2024-11-25 AM 03:00

Start Over

Regenerate Password

Resend Password Email

#### Password Automation Schedule

Schedule Interval \*

180

30-365

Start Time \*

AM 6:00

Days

Save

Search

Device Alias	Model	Device IP	Applied Accounts
192.168.127.14-EDS-G512E-8PoE	EDS-G512E-8PoE	192.168.127.14	admin, user, test...
192.168.127.16-EDS-4012-8P-4GS	EDS-4012-8P-4GS	192.168.127.16	admin, user, test...
192.168.127.25-PT-G7728	PT-G7728	192.168.127.25	admin, user, test...
192.168.127.26-PT-G7728	PT-G7728	192.168.127.26	admin, user, test...

- Set scheduler to generate and set random passwords to selected devices automatically

- Display the selected devices which will be applied with password automation

# 4. Default Password Audit

2

Regularly change passwords on each device



- Device Management-> Account and Password-> **Default Password Audit**
- Default Password Audit can detect whether devices are still using default account passwords

Account and Password Management Automation

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

Default Password Audit

Last Execution Time: 2024-05-25 PM 04:47:05

Scan

Device Alias	Compatibility	Model	Device IP	Default Account/Password
192.168.127.14-EDS-G512E-8PoE	Yes	EDS-G512E-8PoE	192.168.127.14	Yes
192.168.127.16-EDS-4012-8P-4GS	Yes	EDS-4012-8P-4GS	192.168.127.16	Yes
192.168.127.25-PT-G7728	Yes	PT-G7728	192.168.127.25	Yes
192.168.127.26-PT-G7728	Yes	PT-G7728	192.168.127.26	No
192.168.127.40-NPort-6250	No	NPort-6250	192.168.127.40	N/A

1 - 5 of 5

➤ Display whether the devices are using default passwords

# 5. Temporary Account

3 Provide the device credentials to the operator



- Device Management-> Account and Password-> **Temporary Account**
- Temporary Accounts lets administrators create the temporary account for device.

MXview ONE

English admin

Account and Password Management Automation

Account Management

Password Automation

Account Audit

Default Password Audit

Temporary Account

➤ Display the info and status for temporary account
















Device Alias	Compatibility	Model	Device IP	Username	Start Time	End Time	Status
192.168.127.14-EDS-G512E-8PoE	Yes	EDS-G512E-8PoE	192.168.127.14	temp	2024-04-18 AM 9:30	2024-04-18 PM 6:30	Not Activate
192.168.127.16-EDS-4012-8P-4GS	Yes	EDS-4012-8P-4GS	192.168.127.16	temp	2024-03-20 AM 9:30	2024-04-18 PM 6:30	Activate
192.168.127.25-PT-G7728	Yes	PT-G7728	192.168.127.25				
192.168.127.26-PT-G7728	Yes	PT-G7728	192.168.127.26				
192.168.127.40-NPort-6250	No	NPort-6250	192.168.127.40	N/A	N/A	N/A	N/A

1 - 5 of 5

➤ Add, Edit, Delete device temporary account

# 5. Temporary Account

3 Provide the device credentials to the operator

<input type="checkbox"/>	Device Alias
<input type="checkbox"/>	   192.168.127.14-EDS-G512E-8PoE
<input type="checkbox"/>	   192.168.127.16-EDS-4012-8P-4GS
<input type="checkbox"/>	   192.168.127.25-PT-G7728
<input type="checkbox"/>	   192.168.127.26-PT-G7728
<input type="checkbox"/>	   192.168.127.40-NPort-6250

### Add Temporary Account

Username \*

temp

Minimum 4 characters 4/64

Password \*

.....

Minimum 8 characters 8/64

Creation Time \*

Schedule

Start Date

2024/12/12

Start Time \*

AM 9:30

End Date

2024/12/12

End Time \*

PM 6:30

Cancel

Add

Add a device temporary account

- Username
- Password
- Creation Time
  - Now
  - Schedule
- Start / End Date and Time



Inventory Management

# MXview One v1.4.0 New Feature

## Rogue Device Detection

**Demo**

# Scenario :

**Hard to identify any unexpected devices being connected to the network in the field**



Network Operator

I need to ensure the field network operates normally and prevent any suspicious or unexpected devices from being connected, which could disrupt operations.

However, there are numerous devices in the field, making it difficult to identify any new connections. This poses a high risk of attacks or intrusions within the network.

Type keyword to search

Device Discovery

Device Management

Saved CLI Scripts

Device Configuration Center

Event Management

Notification Management

Inventory Management

Assets and Warranty

Rogue Device Detection

Integration

Administration

Help

## Rogue Device Detection

Rogue Device Settings

Device Baseline

Current Rogue Device

Rogue Device History



Search



MAC Address

IP Address

NIC Vendor



00:90:E8:86:71:DA

192.168.127.14

Moxa



00:80:63:83:82:80

192.168.127.16

Hirschmann



00:07:EC:E1:5D:18

192.168.127.25

Cisco



00:90:E8:86:71:DA

192.168.127.26

Unknown

1-5 of 5

Detect and notify if there are devices connected to the network

# Rogue Device Settings



- Inventory Management-> Rogue Device Detection -> **Rogue Device Settings**
- Create Baseline and enable Rogue Device Detection
- Display device list in the Baseline

**MXview ONE**

## Rogue Device Detection

Rogue Device Settings | Device Baseline | Current Rogue Device | Rogue Device History

### Device Baseline

Creation Time: 2024-06-06 PM 01:05:00

Create

### Rogue Device Detection

Enabled \*

Enabled

Save

- Create the baseline based on the devices in the topology

**MXview ONE**

## Rogue Device Detection

Rogue Device Settings | Device Baseline | Current Rogue Device | Rogue Device History

<input type="checkbox"/>	MAC Address	IP Address	NIC Vendor
<input type="checkbox"/>	00:90:E8:00:00:55	192.168.123.152	Moxa Technologies CORP. Ltd
<input type="checkbox"/>	00:90:E8:52:39:75	192.168.123.165	Moxa Technologies CORP. Ltd
<input type="checkbox"/>	00:90:E8:79:23:82	192.168.127.28	Moxa Technologies CORP. Ltd
<input type="checkbox"/>	00:90:E8:23:7E:97	192.168.123.153	Moxa Technologies CORP. Ltd



# Current Rogue Device



- Inventory Management-> Rogue Device Detection -> **Current Rogue Device**
- When the device not in the Baseline is detected on the network, it will be displayed in “Current Rogue Device” list

MXview ONE

### Rogue Device Detection

Rogue Device Settings | Device Baseline | **Current Rogue Device** | Rogue Device History

Search

	MAC Address	IP Address ↓	First Seen	Last Seen	Connected Switch/Port	NIC Vendor
<input type="checkbox"/>	<input type="checkbox"/> + 50:3E:AA:25:0F:E7	192.168.128.222	2024-06-06 PM 01:05:19	2024-06-06 PM 02:29:29	192.168.123.153/Port2	Tp-link Technologies Ltd
<input type="checkbox"/>	<input type="checkbox"/> + 60:A4:B7:75:4A:FB	192.168.128.68	2024-06-06 PM 01:05:19	2024-06-06 PM 02:29:29	192.168.123.153/Port2	Tp-link Corporation Limited
<input type="checkbox"/>	<input type="checkbox"/> + 00:0C:29:74:92:EC	192.168.127.201	2024-06-06 PM 01:05:19	2024-06-06 PM 02:29:29	192.168.123.153/Port2	Vmware Inc
<input type="checkbox"/>	<input type="checkbox"/> + 00:0C:29:D7:B6:A0	192.168.127.200	2024-06-06 PM 01:05:19	2024-06-06 PM 02:29:29	192.168.123.153/Port2	Vmware Inc
<input type="checkbox"/>	<input type="checkbox"/> + 00:0C:29:68:8D:78	192.168.127.198	2024-06-06 PM 01:05:19	2024-06-06 PM 02:29:29	192.168.123.153/Port2	Vmware Inc
<input type="checkbox"/>	<input type="checkbox"/> + 00:0C:29:43:60:8B	192.168.127.186	2024-06-06 PM 01:43:20	2024-06-06 PM 02:29:17	192.168.123.152/Port1	Vmware Inc
<input type="checkbox"/>	<input type="checkbox"/> + 00:1B:21:63:DF:E2	192.168.127.128	2024-06-06 PM 01:05:19	2024-06-06 PM 02:29:29	192.168.123.153/Port2	Intel Corporate
<input type="checkbox"/>	<input type="checkbox"/> + 00:90:E8:12:FA:42	192.168.127.69	2024-06-06 PM 01:05:19	2024-06-06 PM 02:29:29	192.168.123.153/Port2	Moxa Technologies CORP. Ltd

## ➤ Device Information

- MAC Address
- IP Address
- First Seen
- Last Seen
- Connected Switch/Port
- NIC Vendor

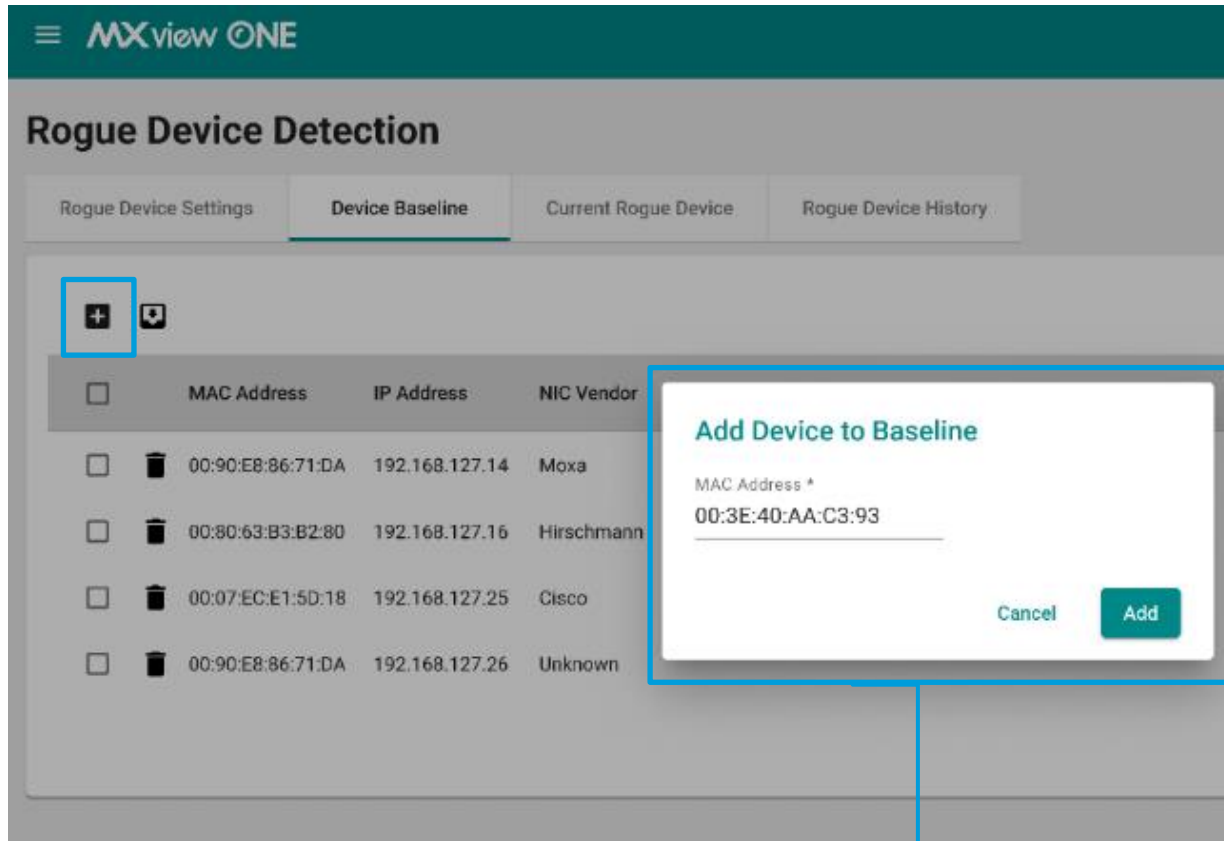
➔ Can add current rogue devices to Baseline list



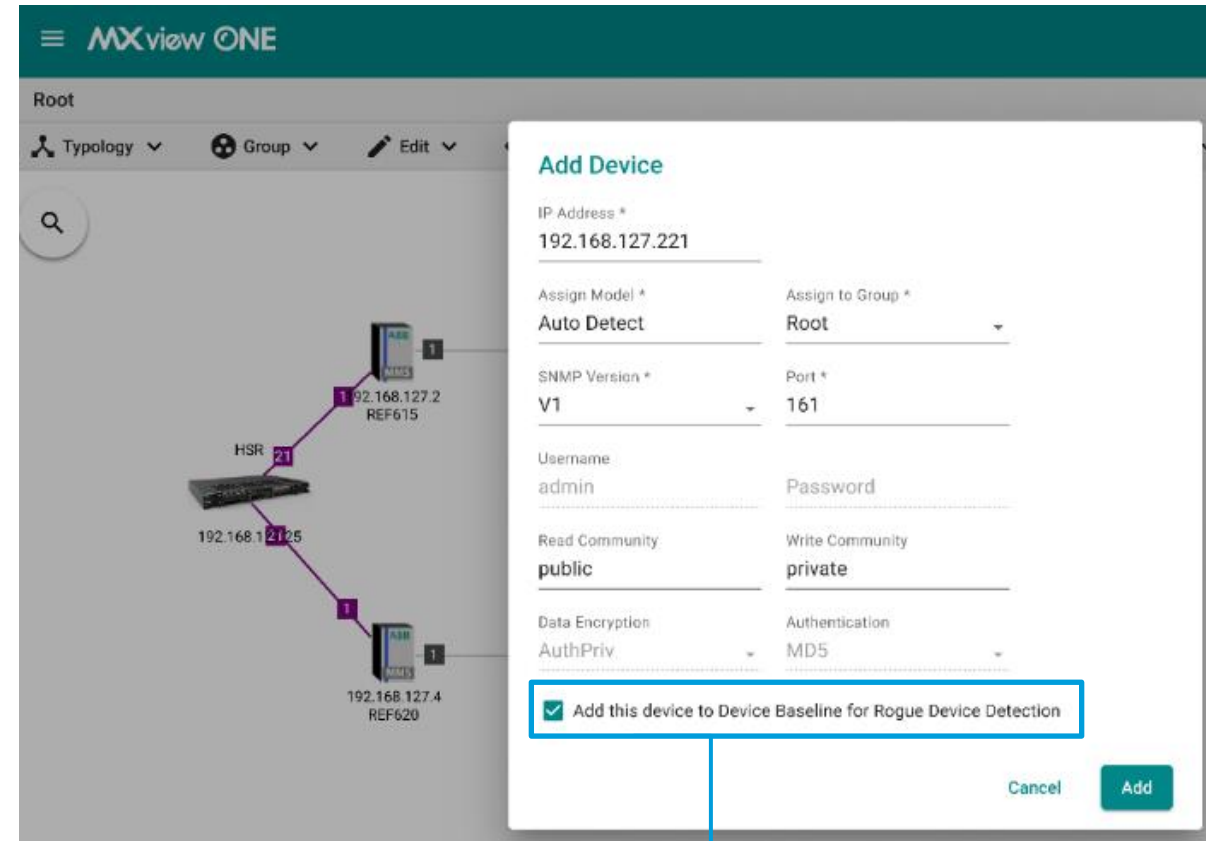
An unknown device has been detected.

# Change Device Baseline- Add Device

- Add the device to the Device Baseline



- Add device to the Baseline list



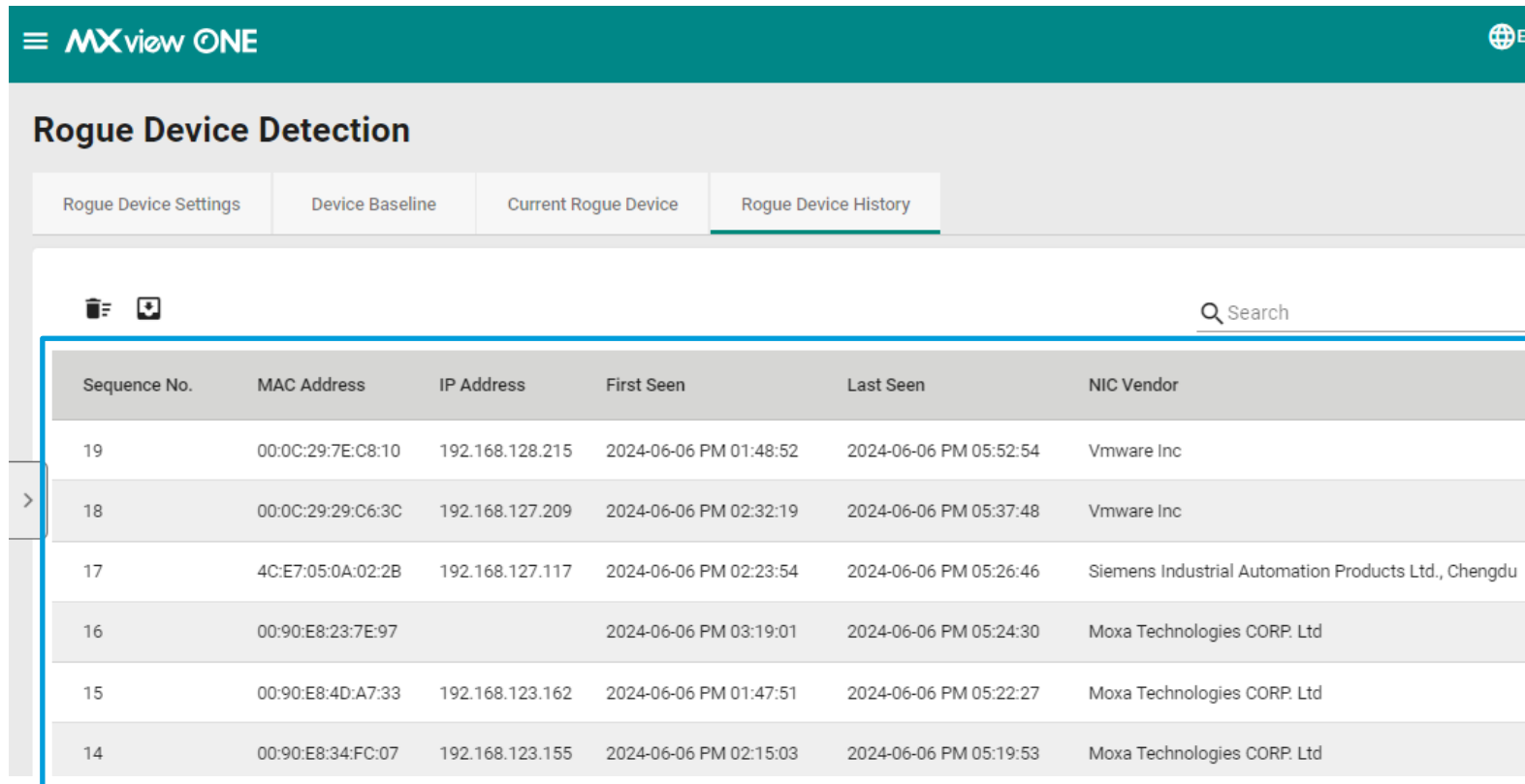
- Decide to add the device to the Baseline list when adding a device in the topology

# Rogue Device History



• Inventory Management-> Rogue Device Detection -> **Rogue Device History**

• Display rogue device history list



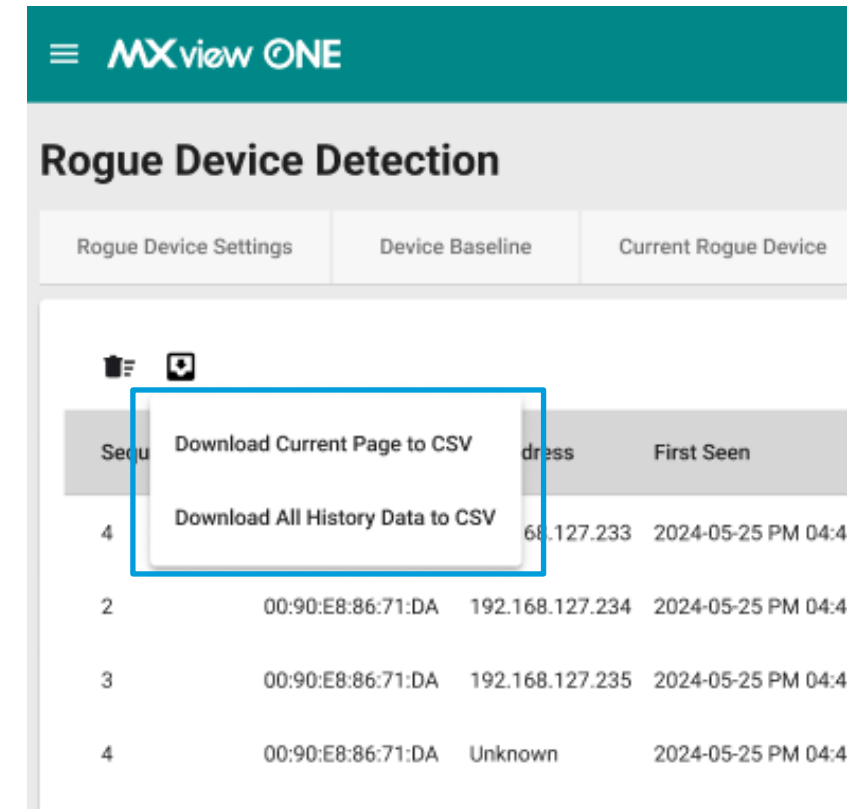
**Rogue Device Detection**

Rogue Device Settings | Device Baseline | Current Rogue Device | **Rogue Device History**

Search

Sequence No.	MAC Address	IP Address	First Seen	Last Seen	NIC Vendor
19	00:0C:29:7E:C8:10	192.168.128.215	2024-06-06 PM 01:48:52	2024-06-06 PM 05:52:54	Vmware Inc
18	00:0C:29:29:C6:3C	192.168.127.209	2024-06-06 PM 02:32:19	2024-06-06 PM 05:37:48	Vmware Inc
17	4C:E7:05:0A:02:2B	192.168.127.117	2024-06-06 PM 02:23:54	2024-06-06 PM 05:26:46	Siemens Industrial Automation Products Ltd., Chengdu
16	00:90:E8:23:7E:97		2024-06-06 PM 03:19:01	2024-06-06 PM 05:24:30	Moxa Technologies CORP. Ltd
15	00:90:E8:4D:A7:33	192.168.123.162	2024-06-06 PM 01:47:51	2024-06-06 PM 05:22:27	Moxa Technologies CORP. Ltd
14	00:90:E8:34:FC:07	192.168.123.155	2024-06-06 PM 02:15:03	2024-06-06 PM 05:19:53	Moxa Technologies CORP. Ltd

• Download to .CSV

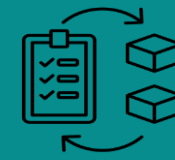


**Rogue Device Detection**

Rogue Device Settings | Device Baseline | Current Rogue Device

Download Current Page to CSV  
Download All History Data to CSV

Sequence No.	MAC Address	IP Address	First Seen
4	00:90:E8:86:71:DA	192.168.127.233	2024-05-25 PM 04:4
2	00:90:E8:86:71:DA	192.168.127.234	2024-05-25 PM 04:4
3	00:90:E8:86:71:DA	192.168.127.235	2024-05-25 PM 04:4
4	00:90:E8:86:71:DA	Unknown	2024-05-25 PM 04:4



Inventory Management

# MXview One v1.4.0 New Feature

## Product Warranty Management

**Demo**

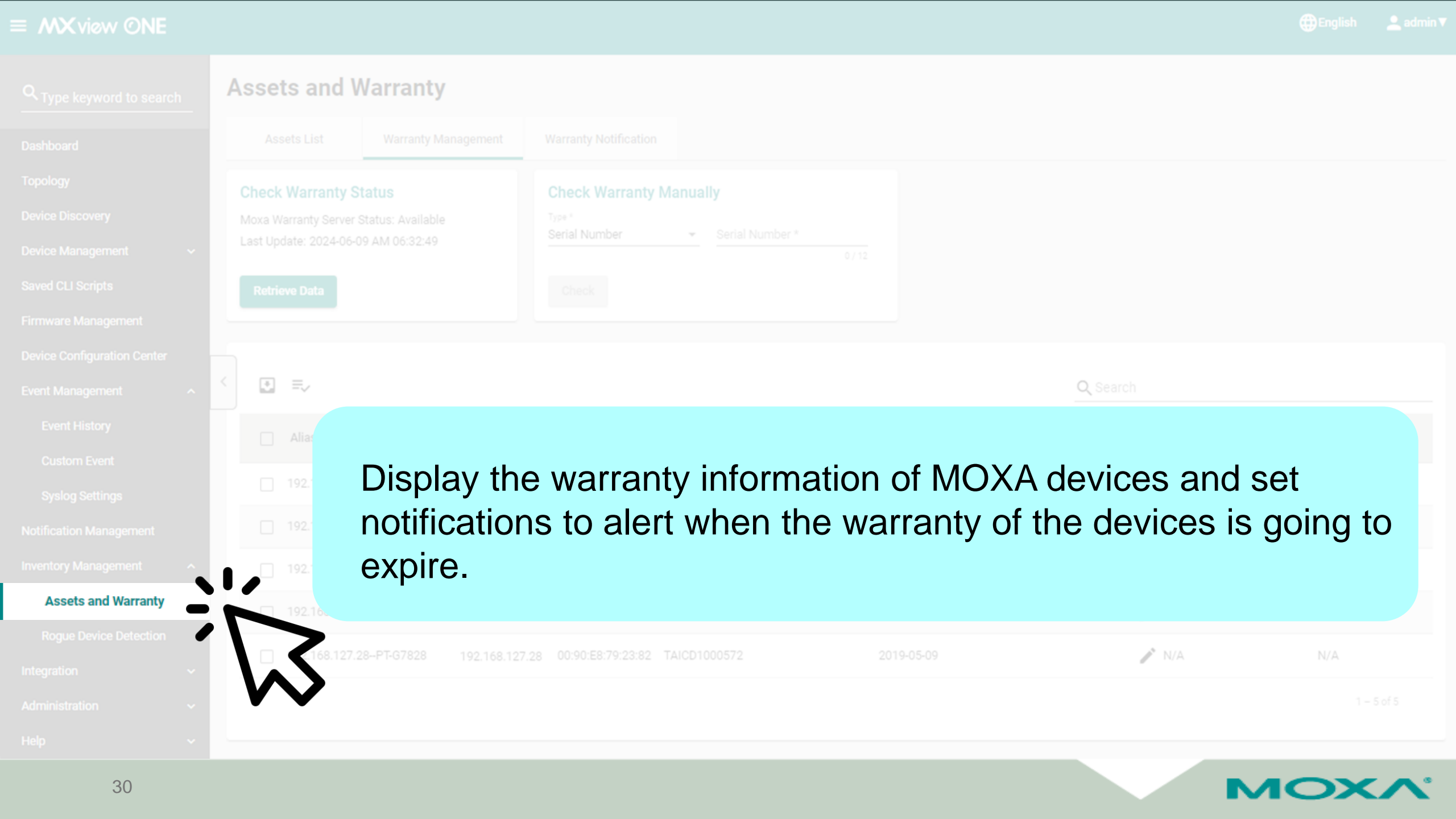
# Scenario: Know the device warranty information to achieve preventive maintenance



Users of Moxa devices who also use MXview One for device management

MXview One helps me manage and monitor devices in the field. I hope to do further inventory management in MXview One, allowing me to know the warranty information of Moxa devices.

When devices in the field are nearing the end of their warranty, I want to be notified in advance so that I can adopt preventive maintenance plans (such as budgeting for equipment procurement).



Display the warranty information of MOXA devices and set notifications to alert when the warranty of the devices is going to expire.



# Display Moxa Devices Warranty Information

- 💡 • Inventory Management-> Assets and Warranty-> **Warranty Management**

- Retrieve devices warranty info from server

- Display devices warranty information

**Assets and Warranty**

Assets List | **Warranty Management** | Warranty Notification

**Check Warranty Status**  
Moxa Warranty Server Status: Available  
Last Update: 2024-06-09 AM 06:32:49  
**Retrieve Data**

**Check Warranty Manually**  
Type \*  
Serial Number  Serial Number \*  0 / 12  
**Check**

Search

<input type="checkbox"/>	Alias	IP	MAC Address	Serial Number	Warranty Period	Warranty Start Date	Warranty End Date	Channel Extended Warranty End Date	Warranty Status
<input type="checkbox"/>	192.168.123.152-EDS-518A	192.168.123.152	00:90:E8:00:00:55					2024-07-10	Active
<input type="checkbox"/>	192.168.123.153-EDS-405A	192.168.123.153	00:90:E8:23:7E:97	TAAA01024619		2011-02-14		N/A	N/A
<input type="checkbox"/>	192.168.123.165-AWK-1131A	192.168.123.165	00:90:E8:52:39:75	815		2015-12-04		2024-06-09	Expire soon
<input type="checkbox"/>	192.168.127.2-ABB	192.168.127.2	00:21:C1:5C:3D:91					N/A	N/A
<input type="checkbox"/>	192.168.127.28-PT-G7828	192.168.127.28	00:90:E8:79:23:82	TAICD1000572		2019-05-09		N/A	N/A

1 - 5 of 5

# Set Warranty Notification



- Inventory Management-> Assets and Warranty-> **Warranty Notification**

- Warranty Notification Configuration
  - **Enabled:** Enable or disable notification
  - **Notify Before:** Set how many days to notify before warranty expires
  - **Email To:** Set the email address to receive the device list

MXview ONE

## Assets and Warranty

Assets List   Warranty Management   **Warranty Notification**

### Warranty End Date Notification

Enabled \*  
Enabled

Notify Before \*  
30  
30 - 365   Days

Email To  
tester@192.168.127.198

22 / 512

Save





Northbound Interface

# MXview One v1.4.0 New Feature

## Syslog Forwarding

# Scenario: I hope to forward syslog to an independent server to achieve event analysis



Network administrator

I hope to forward syslogs collected from different network management software to an independent server to achieve event analysis and security management.

However, if all unfiltered information is transmitted to the server, there will be too much information, making it hard to identify what is really important. Therefore, I hope to do the initial filtering in the network management software to define which information to send to the server, so that management on the server can be more efficient.

Type keyword to search

- Dashboard
- Topology
- Device Discovery
- Device Management
- Saved CLI Scripts
- Firmware Management
- Device Configuration Center
- Event Management
  - Event History
  - Custom Event
- Syslog Settings**
- Notification Management
- Inventory Management
- Integration
- Administration
- Help

## Syslog Settings

Syslog Server Settings

Syslog Viewer

Syslog Forwarding

Enable Syslog Forwarding \*

Disabled

Protocol \*

UDP

Remote IP/Domain Na...

Port 1

0 / 253

1 - 65535

Rem

Sys

+

Save

Forward the device syslogs to the specific syslog server.

# Syslog Server Settings



- Event Management-> Syslog Settings-> **Syslog Server Settings**
- MXview One as a syslog server to receive the syslog from devices

MXview ONE English admin

## Syslog Settings

Syslog Server Settings Syslog Viewer Syslog Forwarding

Enable Built-in Syslog Server \*  
Enable UDP & TCP

UDP Port \*  
514  
1 - 65535

TCP Port \*  
5143  
1 - 65535

Authentication \*  
Disabled

> Save

- Enable Built-in Syslog Server
- UDP Port
- TCP Port
- Authentication

# Syslog Forwarding Settings



- Event Management-> Syslog Settings-> **Syslog Forwarding**
- Forward the syslog to another server

- Enable Syslog Forwarding
- Protocol
  - UDP
  - TCP
- Remote IP/Domain Name
- Port
- Syslog Filter Settings

**MXview ONE**

### Syslog Settings

Syslog Server Settings   Syslog Viewer   **Syslog Forwarding**

Enable Syslog Forwarding \*  
Enabled

Protocol \*  
UDP

Remote IP/Domain Name 1   Port 1  
10.123.35.195   514  
13 / 253   1 - 65535

Remote IP/Domain Name 2   Port 2  
0 / 253   1 - 65535

Syslog Filter Settings(1/128)

+   Source IP \*   Severity \*  
Any IP   All Severity

Save



Northbound Interface

# MXview One v1.4.0 New Feature

## OPC UA Server

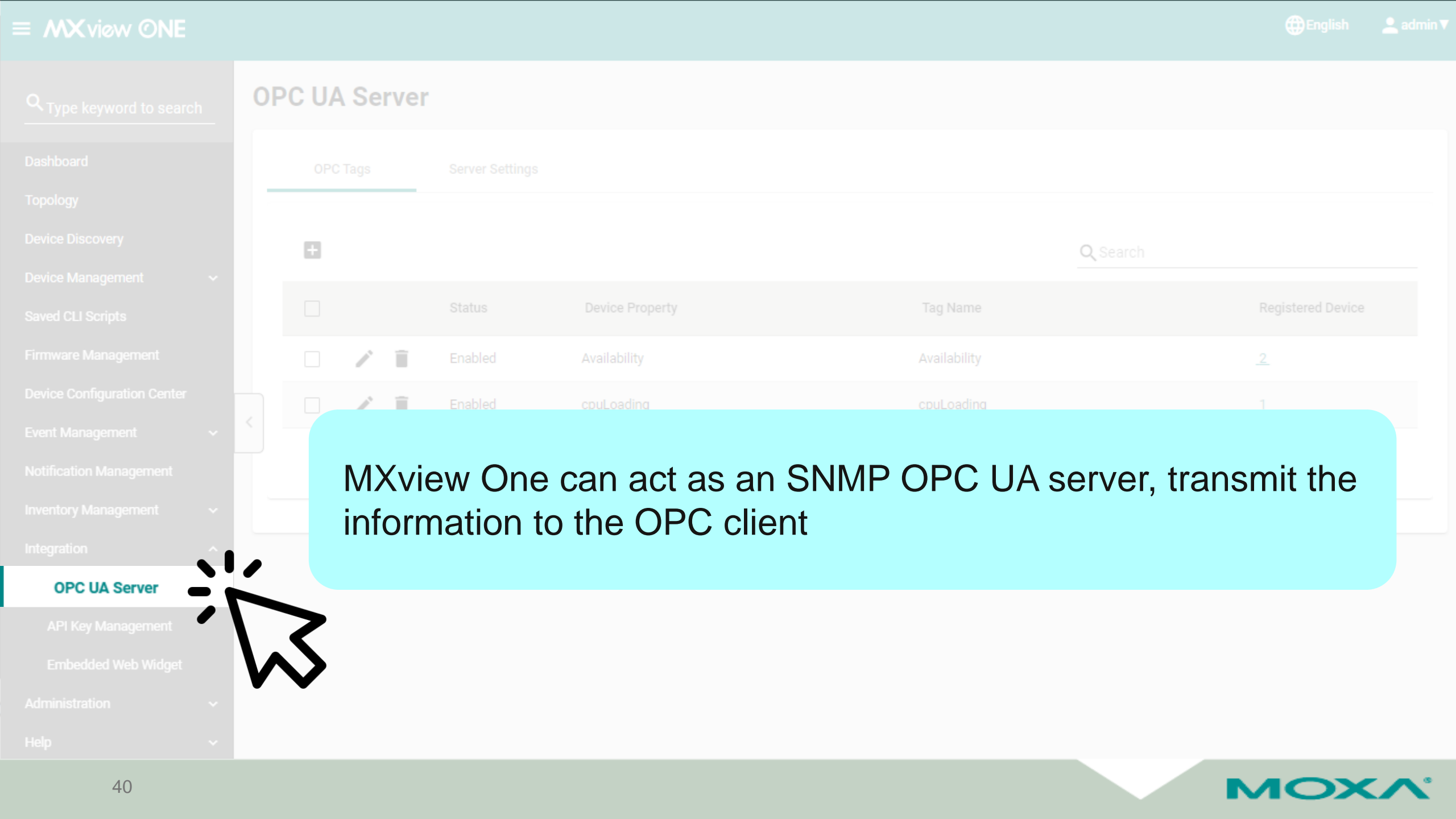
# Scenario: I hope MXview One can be an OPC Server to transmit device information to SCADA



Operator, SI

In industrial field, we are used to monitor devices status by graphical dashboards. However, currently, to transmit network devices information to the dashboard, we will need to prepare an additional OPC Server to act as an intermediary.

Since MXview One can obtain network device information through SNMP, I hope MXview One can also be configured to act as an OPC Server (OPC UA Server) to help transmit device information to a SCADA (client-side) for data display.



Type keyword to search

- Dashboard
- Topology
- Device Discovery
- Device Management
- Saved CLI Scripts
- Firmware Management
- Device Configuration Center
- Event Management
- Notification Management
- Inventory Management
- Integration
- OPC UA Server**
- API Key Management
- Embedded Web Widget
- Administration
- Help

## OPC UA Server

OPC Tags Server Settings

Search

	Status	Device Property	Tag Name	Registered Device
<div><div></div><div><div></div><div></div><div></div></div></div>	Enabled	Availability	Availability	<a href="#">2</a>
<div><div></div><div><div></div><div></div><div></div></div></div>	Enabled	cpuLoading	cpuLoading	1

MXview One can act as an SNMP OPC UA server, transmit the information to the OPC client



# OPC UA Server Settings



- Integration-> OPC UA Server-> **Server Settings**

- Configure the OPC UA Server
  - IP/ Domain Name
  - Port
  - Authentication Mode  
(The way that OPC client makes the connection to OPC server )
  - Security Mode  
(Encrypt when transmit the data)

MXview ONE English admin

## OPC UA Server

OPC Tags Server Settings

Endpoint URL: `opc.tcp://127.0.0.1:4840/MXviewOne/OPCUA`

Enable OPC UA Server \*  
Enabled

IP/Domain Name \*  
127.0.0.1  
9 / 253

Port \*  
4840  
1 - 65535

Authentication Settings  
Authentication Settings \*  
Anonymous

Security Mode  
Allow None Security \*  
Disabled

Support Security Policy  
Basic128Rsa15  
Basic256  
Basic256Sha256  
Aes128Sha256RsaOaep  
Aes256Sha256RsaPss

Save

# OPC Tags



- Integration-> OPC UA Server-> **OPC Tags**

## ➤ Device Property

Availability  
activeProtocolOfRedundancy  
cpuLoading  
defaultGateway  
dhEnabled

- ## ➤ Add OPC tag
- Status
  - Device Property
  - Tag Name
  - Registered Devices

## Add OPC Tag

Status \*

Enabled

Device Property \*

Tag Name \*

0 / 64

Registered Devices \*

Close

Add

MXview ONE

### OPC UA Server

OPC Tags Server Settings

+ Search

	Status	Device Property	Tag Name
<input type="checkbox"/>	Enabled	Availability	Availability
<input type="checkbox"/>	Enabled	cpuLoading	cpuLoading

# Appendix

# Support Model List

Function	Supported Devices
CLI Script Automation Button	List of supported models in MXview One
Device Account and Password Management	<ul style="list-style-type: none"><li>• eCos Switch 【Exclude SDS Series (SDS-3008, SDS-3016, SDS-G3000), EDS A Series】</li><li>• MX-NOS Switch</li><li>• Router Series 【EDR, OnCell-G4302, TN-4908, TN-4916】</li><li>• AWK Series 【AWK-3252A,AWK-3262A,AWK-4252A,AWK-4262A,AWK-1151C,AWK-1161A, AWK-1161C, AWK-1165A,AWK-1165C】</li><li>• PT-G503</li></ul>
Product Warranty	List of supported models in MXview One
Rogue Device Detection	N/A
Syslog Forwarding	N/A
SNMP OPC UA Server	List of supported models in MXview One (and support SNMP)

# Demo site

MXview One CM: (trymxview/ freedemo)

\*\*for the **remote access** function, please use the site : **Generic Demo Site**

- <https://trycm.mxview.io/#/login>

MXview One: (trymxview/ freedemo)

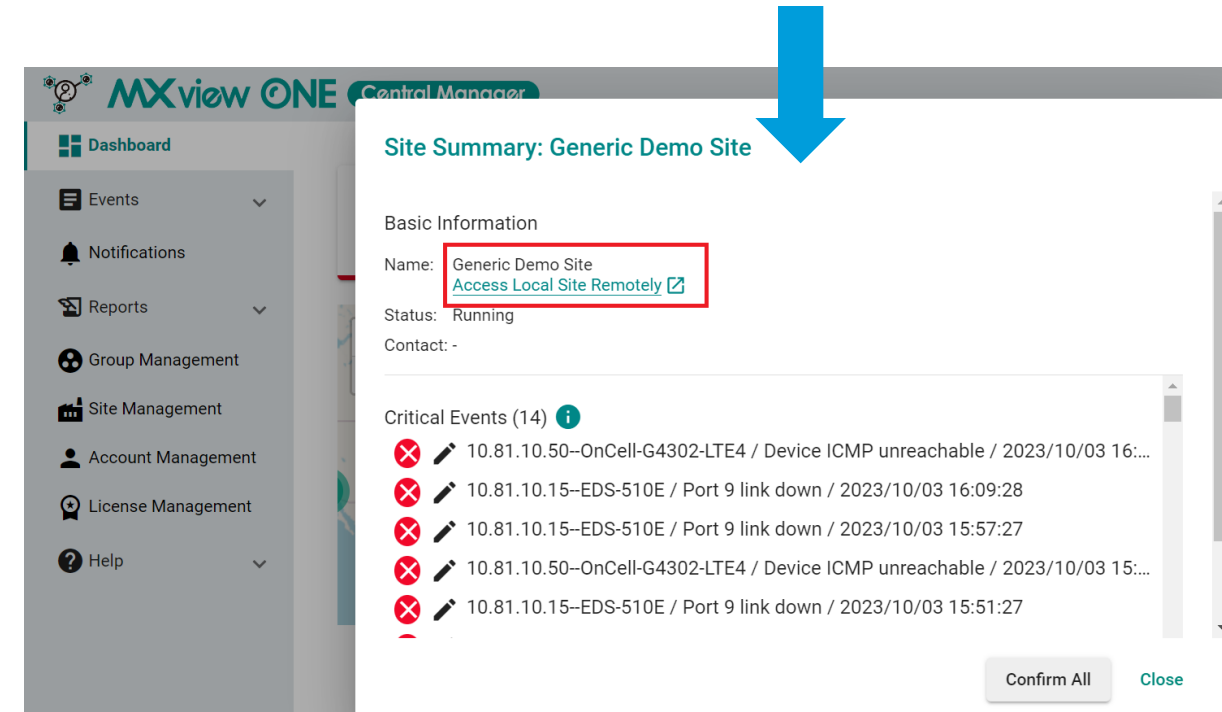
- <https://tryone.mxview.io/>

Wireless: (trymxview/ freedemo)

- <https://trywireless.mxview.io/>

Power: (trymxview/ freedemo)

- <https://trypower.mxview.io/>



# Thank You

