How to Set Up and Monitor UC-2100 Computers in MXview

Moxa Technical Support Team
support@moxa.com

Contents

 Released on May 07, 2021

About Moxa

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things (IIoT). With over 30 years of industry experience, Moxa has connected more than 57 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industries with reliable networks and sincere service. Information about Moxa's solutions is available at www.moxa.com.

How to Contact Moxa

Tel: +886-2-8919-1230

1 Introduction

This document provides a tutorial on how to set up the SNMP service in UC-2100 computers and use MXview to monitor them.

2 Prerequisites

The following firmware and MXview versions are required:

- UC-2100 firmware version v1.7 and higher
- MXview v3.1.20 and higher

Note:	The abovementioned firmware and MXview versions are required for the SNMP service to work. If a higher level of security needs to be set up on the UC-2100 computer, you can enable and configure SNMPv3. For additional details, refer to the instructions in the following sections.

3 Restart the SNMP and LLDP Services on the UC-2100

1. Enable the SNMP and LLDP services on the computer.

```
sudo systemctl enable snmpd
Sudo systemctl enable lldpd
```

2. Modify the `snmpd.conf` file to include the configuration required to monitor the computer remotely.

   - Open the `/etc/snmp/snmpd.conf` file in the vim editor

```
sudo vim /etc/snmp/snmpd.conf
```

   - Modify the `snmpd.conf` file as follows:

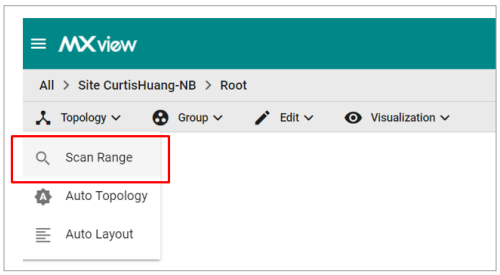
```
#  Listen for connections from the local system only
#  agentAddress  udp:127.0.0.1:161
#  Listen for connections on all interfaces (both IPv4 *and*
IPv6)
agentAddress udp:161,udp6:[::1]:161
```

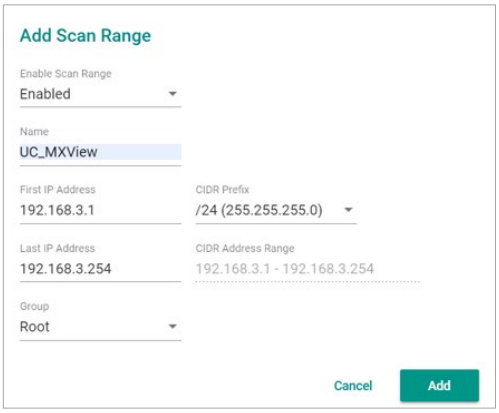
3. Restart the SNMP and LLDP services.

```
sudo systemctl enable snmpd
Sudo systemctl enable lldpd
```

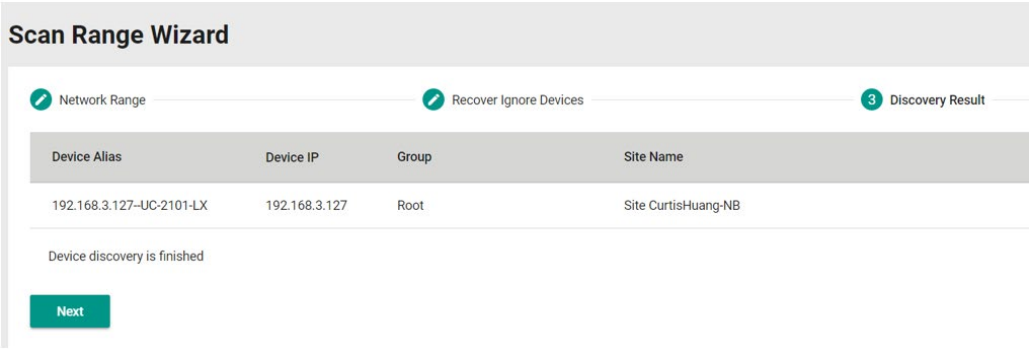
4 Set Up and Monitor UC-2100 in MXview

1. Set up the IP **Scan Range** to include UC-2100's default IP (192.168.3.127).

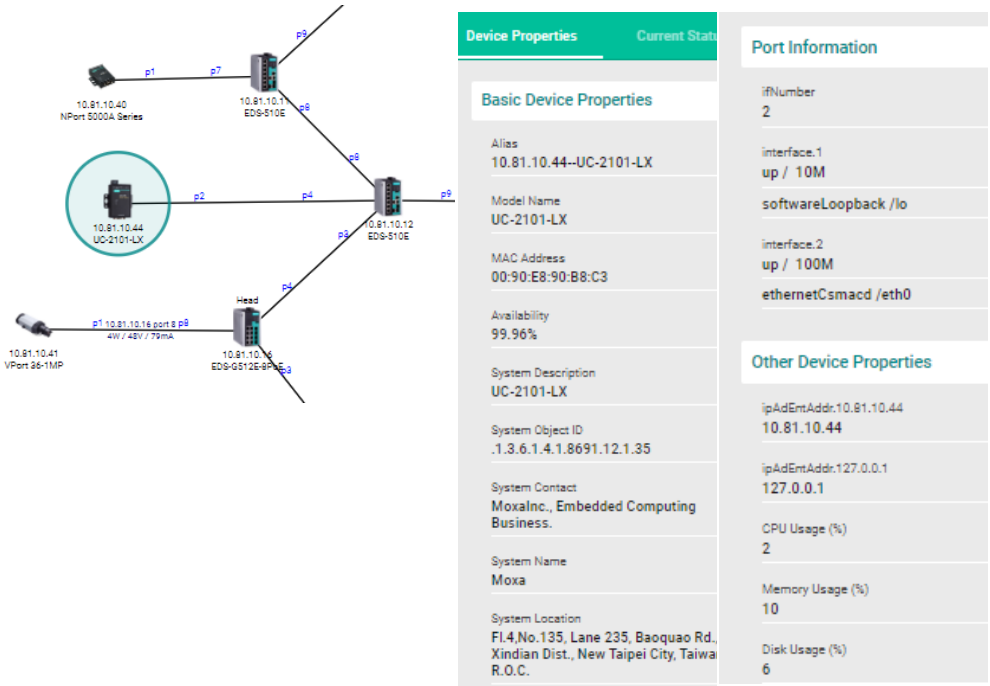




2. Use MXview to scan for and discover the UC-2100 computer.



The UC-2100 computer will be shown in the MXview topology. You can click on the computer icon to view the device properties and hardware statuses such as CPU loading, memory usage, and disk usage.

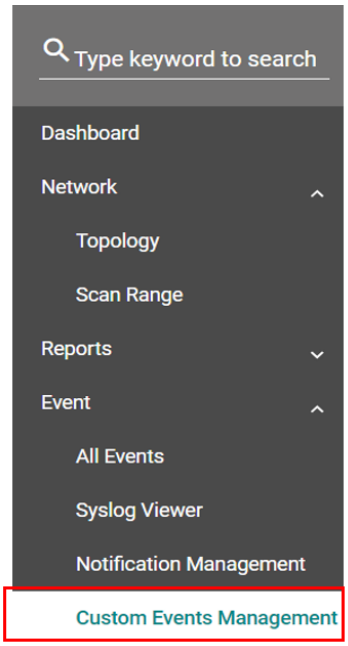


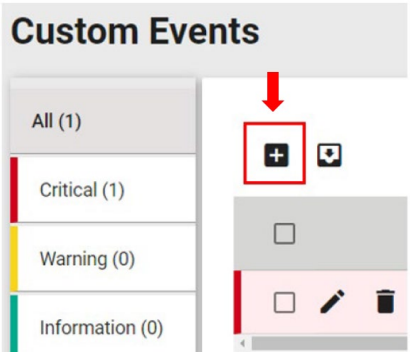
4.1 Setting Up Customized Events in MXview

You can also set up customized events in MXview to monitor computer properties such as CPU, memory, and disk usage.

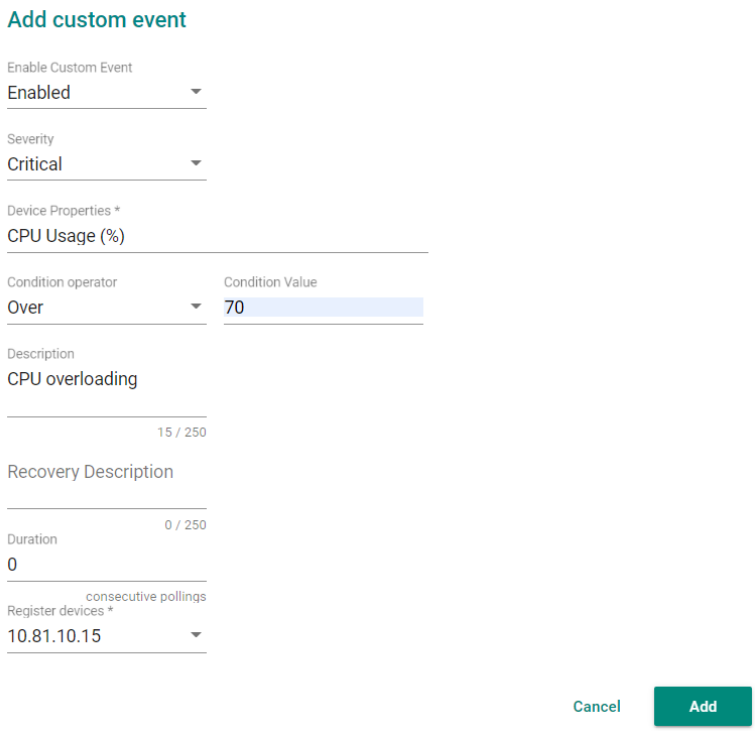
To set up a custom event in MXview, do the following:

1. Open the **Custom Events Management** page and add a custom event.

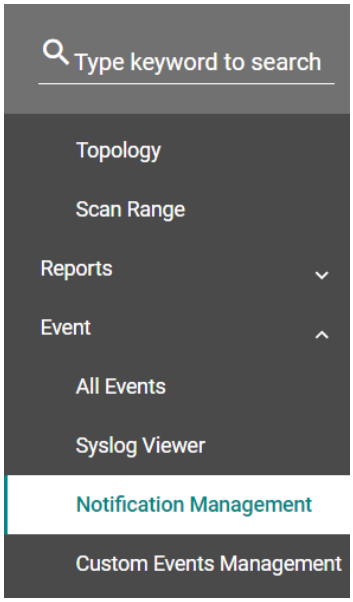


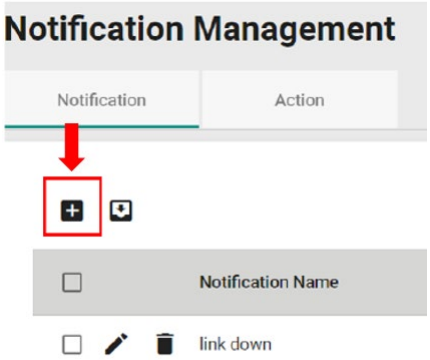


2. Set up the event.
   Specify the severity of the event, the device property to be monitored, the alert conditions, the message to be displayed, and the IP address of the device to monitor.

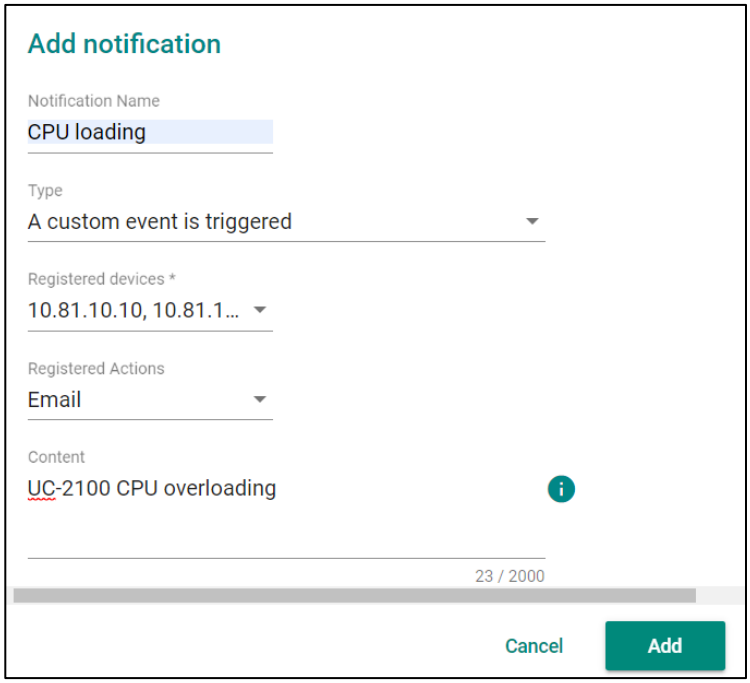


3. Click **Add**.
4. Open the **Notification Management** page and add a new notification.





5. Set up the notification.
   Select the **A custom event is triggered** option for the notification method and specify the notification method; the options include Email, SNMP trap, and Teams.



MXview will send out notifications when the conditions set for the events are reached. You can use these notifications to monitor your device.

5 Enabling and Configuring SNMPv3 on the UC-2100 (optional)

The default SNMP version is **SNMP v2c**. If you want to enable the SNMP v3 service, you must first create a user account, assign a security model with an authentication and encryption algorithm to the account, and restart the SNMP and LLDP services.

The procedure to create a new user account that supports SNMP v3 and remove existing user accounts is covered in the following sections.

5.1 Creating a New User Account

SNMP v3 has 3 security models that can be assigned to the new user account.

- **noauth:** Group using the **noAuthNoPriv** security model; no authentication and encryption is required in this group.
- **auth:** Group using the **authNoPriv** security model; an authentication algorithm needs to be designated to this group.
- **priv:** Group using the **authPriv** security model; has the highest security level, both authentication and encryption algorithm need to be designated in this group.

The following authentication and encryption algorithms can be assigned when creating new user accounts that support SNMP v3.

- MD5: Uses HMAC MD5 algorithm for authentication
- SHA: Uses HMAC SHA1 algorithm for authentication
- AES: Uses AES 128 bit algorithm for encryption
- DES: Uses DES algorithm for encryption

The changes to be made in the `snmpd.conf` file (for a user account that supports SNMP v3) is given below:

```
##################################################################
#
#  SNMPv3 AUTHENTICATION
#
#  Note that these particular settings don't actually belong here.
#  They should be copied to the file /var/lib/snmp/snmpd.conf
#    and the passwords changed, before being uncommented in that
file *only*.
#  Then restart the agent


createUser username1
createUser username2 MD5 userpassword2
createUser username3 SHA userpassword3 AES privacypassword


##################################################################

#ACCESS CONTROL
#

rouser username1 noauth
rouser username2 auth
rouser username3 priv
```

- To create an user account with **noauthNoPriv** security model, use the following:

```
createUser username1
rouser username1 noauth
```

- To create an user account with **authNoPriv** security model and **MD5** algorithm for authentication, use the following:

```
createUser username2 MD5 userpassword2
rouser username2 auth
```

- To create an user account with **authPriv** security model, **SHA1** algorithm for authentication, and **AES 128 bit** algorithm for encryption, use the following:

```
createUser username3 SHA userpassword3 AES privacypassword
rouser username3 priv
```

IMPORTANT: SNMP v3 password must be at least 8 characters long.

Note: If the privacy password is not specified, it is assumed to be the same as the user password

5.2 Removing Existing User Accounts

To remove a user account, follow these steps and then restart the SNMP service.

1. Stop the SNMP service.

```
sudo systemctl stop snmpd
```

2. Open the `/etc/snmp/snmpd.conf` file.

```
sudo vim /etc/snmp/snmpd.conf
```

3. Remove the entries for creating a new user account.

```
create User username1
rouser username1 noauth
```

4. Open the `/var/lib/snmp/snmpd.conf` file.

```
sudo vim /var/lib/snmp/snmpd.conf
```

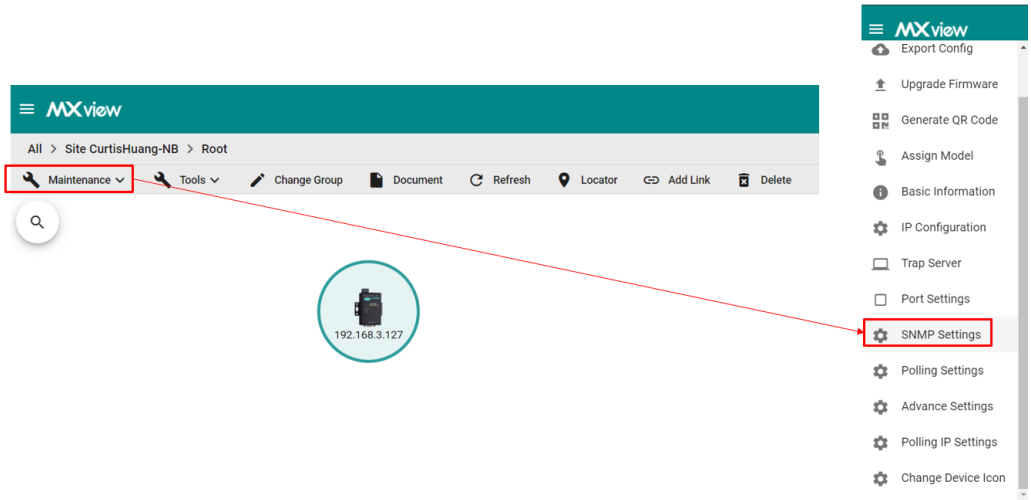
5. Remove the entries that has a specific user name included.

   For example, the following entry includes the user name **username1** and hence should be removed.

```
...
usmUser 1 3 0x80001f8880aa253671d354aa5f "username1"
"username1" NULL .1.3.6.1.6.3.10.1.1.1
"" .1.3.6.1.6.3.10.1.2.1 "" ""
...
```

6 Configuring MXview for SNMPv3 (optional)

1. In MXview, select the UC-2100 computer and enter the SNMP settings.



2. Specify the SNMP Configuration.
   Select SNMP v3 for the SNMP version and choose the corresponding **Data Encryption** method, **Authentication** method, and **Encryption Protocol**.