ATOP Technologies, Inc.

Network Management Utility

User Manual
V1.5
Nov 8, 2023

This PDF Document contains internal hyperlinks for ease of navigation.
For example, click on any item listed in the **Table of Contents** to go to that page.

Important Announcement

The information contained in this document is the property of ATOP Technologies, Inc., and is supplied for the sole purpose of operation and maintenance of ATOP Technologies, Inc., products.

No part of this publication is to be used for any other purposes, and it is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form, by any means, in whole or in part, without the prior explicit written consent of ATOP Technologies, Inc.,

Offenders will be held liable for damages and prosecution.

All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Disclaimer

We have checked the contents of this manual for agreement with the hardware and the software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual is reviewed regularly and any necessary corrections will be included in subsequent editions.

Suggestions for improvement are welcome. All other product names referenced herein are registered trademarks of their respective companies.

Who Should Use This User Manual

This manual is to be used by qualified network personnel or support technicians who are familiar with network operations and might be useful for system programmers or network planners as well. This manual also provides helpful and handy information for first-time users. For any related problems, please contact your local distributor. If they are unable to assist you, please redirect your inquiries to www.atoponline.com .

Warranty Period

There is no warranty for the software. Please refer to the license agreement.

Documentation Control

Revision:	1.5
Creation Date:	19 April 2021
Last Revision Date:	8 November 2023
Product Reference:	Network Management Utility User Manual
Document Status:	Release

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1   *Purpose of the Manual*

This manual explains the available technical features of the Network Management Utility. During device configuration, users can follow instructions, examples, and guidelines provided in the manual for general and advanced network management. Some general technical information is also given to help users manage their devices. A background in general theory is necessary when reading it. Please refer to the Glossary for technical terms and abbreviations.

1.2   *Who Should Use This User Manual*

This manual should be used by qualified network personnel or support technicians who are familiar with network operations. It can be useful for system programmers and network planners. This manual will also come handy for new users. If there are any issues, please reach us at www.atoponline.com.

1.3   *Scope*

Network Management Utility is a software utility developed by ATOP Technologies. It is a special tool for device management and configuration of our products. It can be used for daily management and for setting tasks on various ATOP network devices, such as:
- Device discovery and listing
- Device grouping
- Login with password
- Network parameter configuration
- Firmware update
- Reset to default
- Backup and restore configuration

1.4   *System Requirements*

- Windows 7/8
- Windows 2008
- Windows Vista
- Windows Professional 2003
- Windows 2000/Windows NT
- Windows 10 is supported and fully functional; however, some issues related to font size have been reported.

Note: All figures herein are intended for illustrative purposes only. Certain features of this software work only on some specific ATOP devices.

2 Getting Started

1.1 Installation of Network Management Utility

The Network Management Utility can be either installed from the CD that comes in your product package, or downloaded from www.atoponline.com. Once the installer is available on your PC, proceed to install it by double clicking on the Network Management Utility program icon, which has the icon as shown in Figure 2.1.
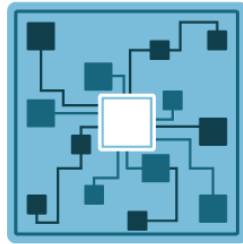
Figure 2.1 Network Management Utility© Program Icon

For Windows 7 users, it is strongly recommended to allow the program to run in Compatibility Mode. This can be done by right-clicking the **Network Management Utility Setup 2.X** program icon and selecting the **Properties** menu as shown in Figure 2.2. Then, click on the **Compatibility** tab and tick on the **"Run this program in compatibility mode for:"** box and tick on the "**Run this program as an administrator"** box, as shown in Figure 2.3. Finally, click **OK** button and proceed to install the program.
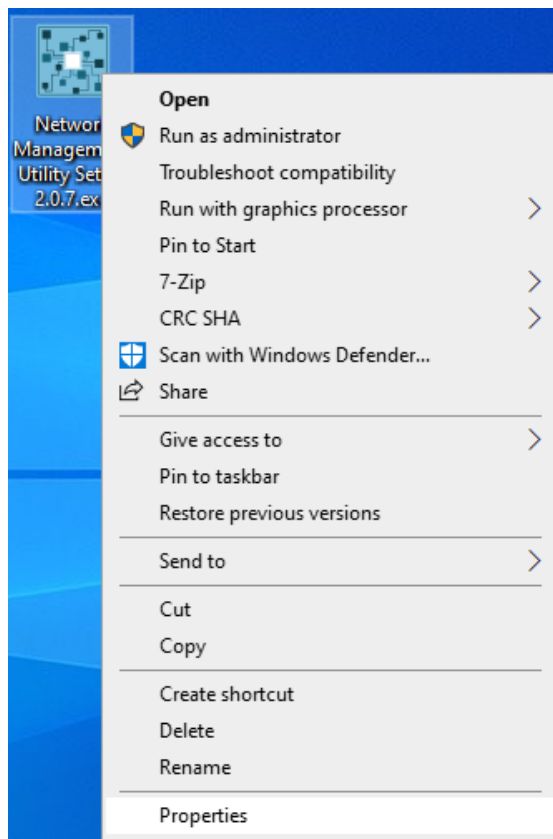
Figure 2.2 Right Click the Network Management Utility© Program Icon
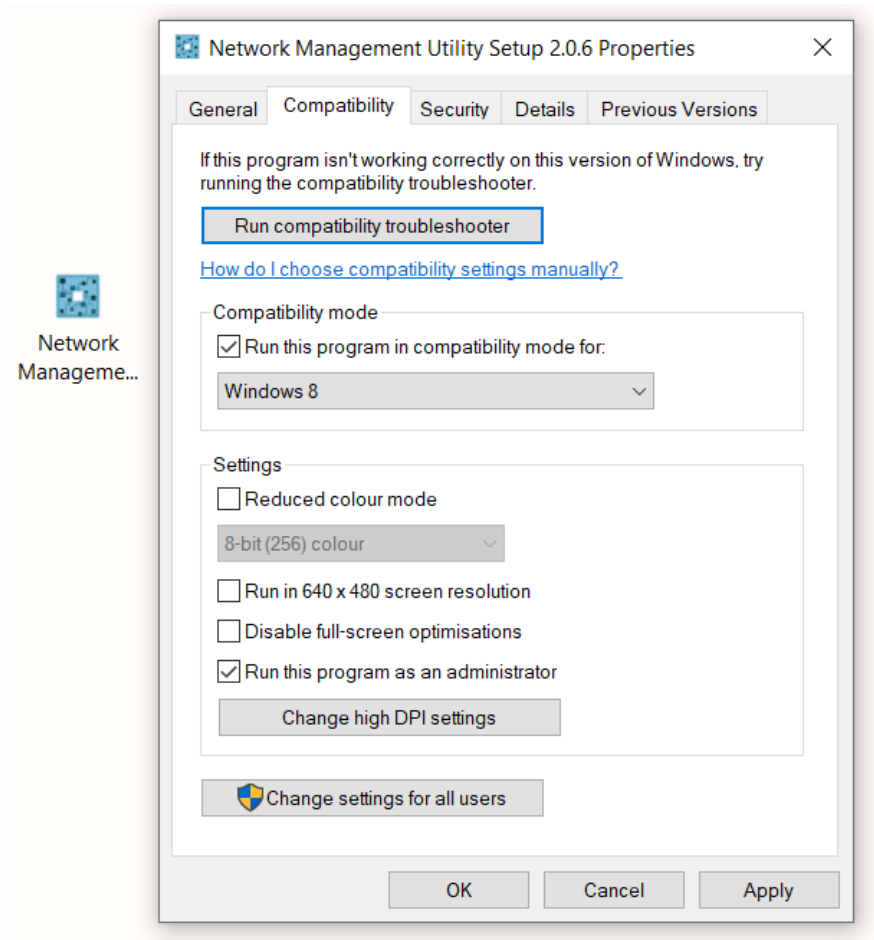
Figure 2.3 Right Click Properties → Compatibility Tab → Tick Two Boxes

1.2   Installation

After clicking on the **OK** button in the setup program's Properties as shown above, double-click on the setup icon, and a pop-up window will be launched, as shown in Figure 2.4. Once the installation completes, the **Network Management Utility Setup** program is installed into your computer system.
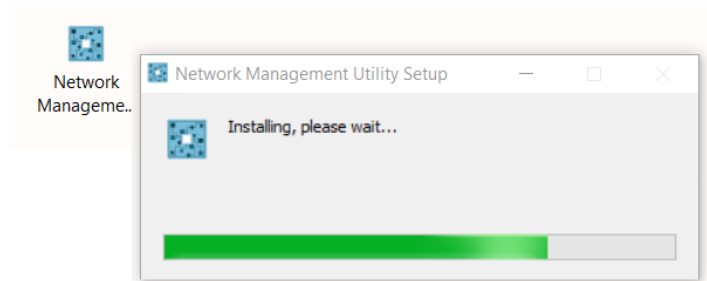
Figure 2.4 An Installing Pop-up Window

3 User Interface

Double click the installed **Network Management Utility Setup 2.X** to launch the program. While loading the program, its logo and version will appear as shown in Figure 3.1 below.

Figure 3.1 Launching After Double-clicking the Network Management Utility Setup

Log in to the **Network Management Utility**. When executing the **Network Management Utility** for the first time, log in with the default user name & password. (User Name: **admin**, Password: **admin123**)
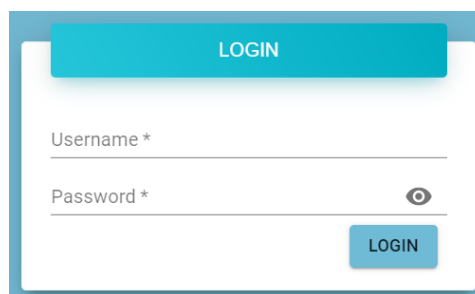
Figure 3.2 Log in to the Network Management Utility

The user interface (UI) of **Network Management Utility Setup 2.X** is depicted in Figure 3.. The window consists of the following: 1) drop-down menus at the top, 2) a vertical left menu, and 3) a working space in the middle. When users click on the magnifier icon on the vertical left menu, a second horizontal icon bar will appear for the **Device List** and **Topology** menus. The following chapters will describe each item and its function in detail. Here, we will explain how to first discover connected devices.
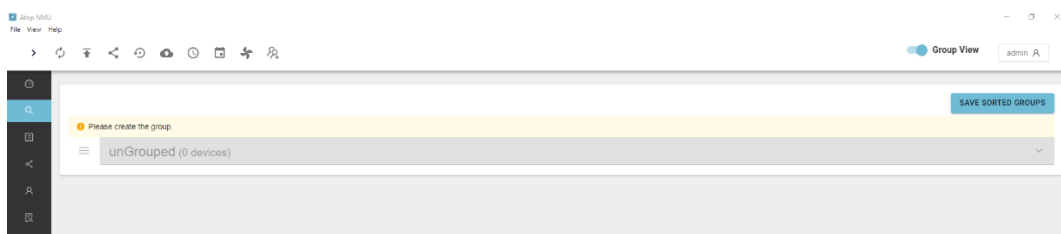
Figure 3.3 First-time Launch of Network Management Utility Setup 2.X

Click on the magnifier icon at the top of the vertical left menu. The number of devices connected to the **Network Management Utility Setup 2.X**. If these devices are not yet grouped together, the number of devices will be showed as unGrouped.
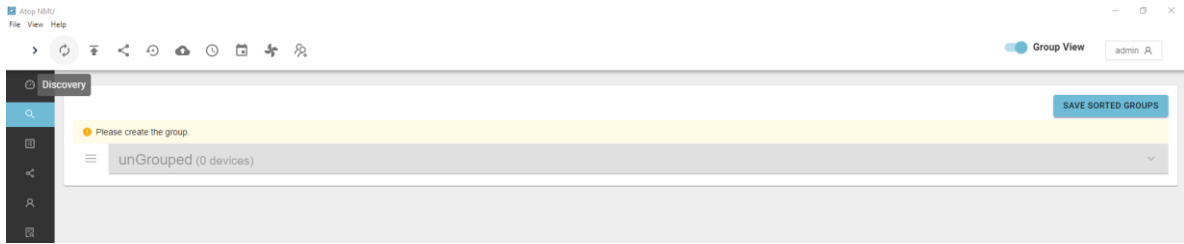
Figure 3.4 Working Space after Clicking on Magnifier Icon

Click on the drop-down icon on the right, and the list of the found device(s) is displayed as a table with the following columns: **Online**, **Device Type**, **Model**, **IP Address**, **MAC Address**, **Host Name**, **Kernel, AP,** and **Access** as shown in Figure 3.5. Click on a column title to sort the devices according to values in that column.

Figure 3.5 List of Connected Devices after Clicking on Magnifier Icon

The first column called **Online** shows the status of each device: active (green dot) or inactive (red dot). The second column, called **Device Type**, shows whether it is a basic or an advanced device. The third column is the **Model** number of the found device(s). The fourth column is the **IP Address** of the corresponding device. The fifth column is the **MAC Address** of the device. The sixth column is the **Host Name** of the device. The seventh column is the **Kernel** version of the device. The eighth column is the **AP information** or application version of the device. Note that ATOP's device firmware generally consists of an application version and a kernel version. The last column, **Access**, indicates whether the device is already accessible by NMU (✓) or not (✗). An accessible device must belong in a group. That is, users have to create a group and add the device to that group first to view it as accessible.

4 Top Drop-down Menus

There are three drop-down menus in the top menu bar: **File**, **View**, and **Help**. In the following sections, we will describe options within each menu in detail.

4.1   *File*

The first drop-down on the bar is **File**, as shown in Figure 4.1. In this menu, there are four options:
- Preferences...
- Import Settings...
- Export Settings...
- Quit
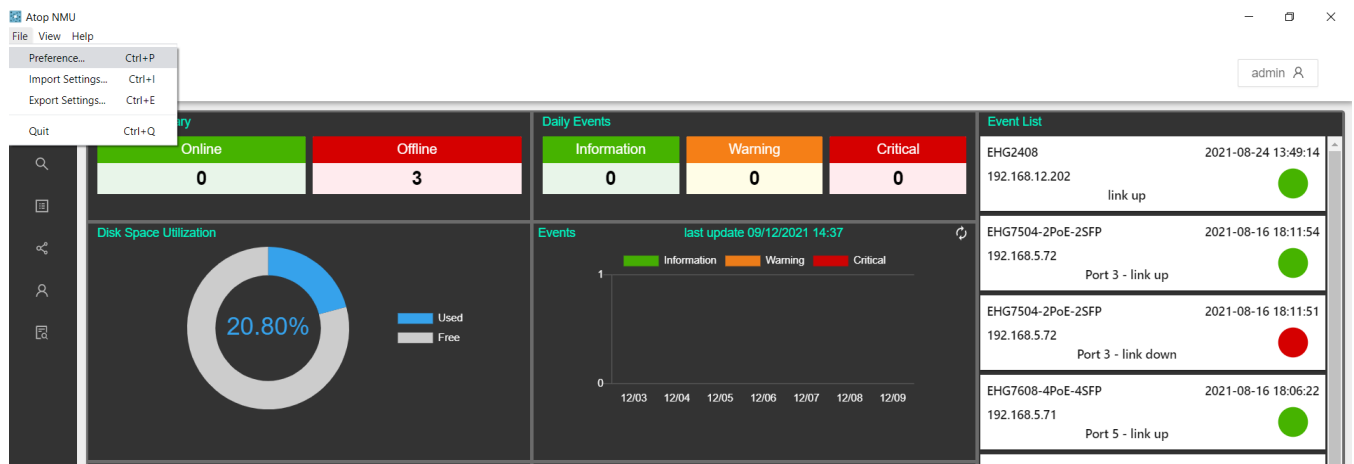
Figure 4.1 Options within File Menu

4.1.1 *Preferences*

As shown in Figure 4.2 below, the **Preferences** option under the **File** menu contains five tabs: **General**, **Mail**, **Telegram, SNMP**, and **Advanced**.
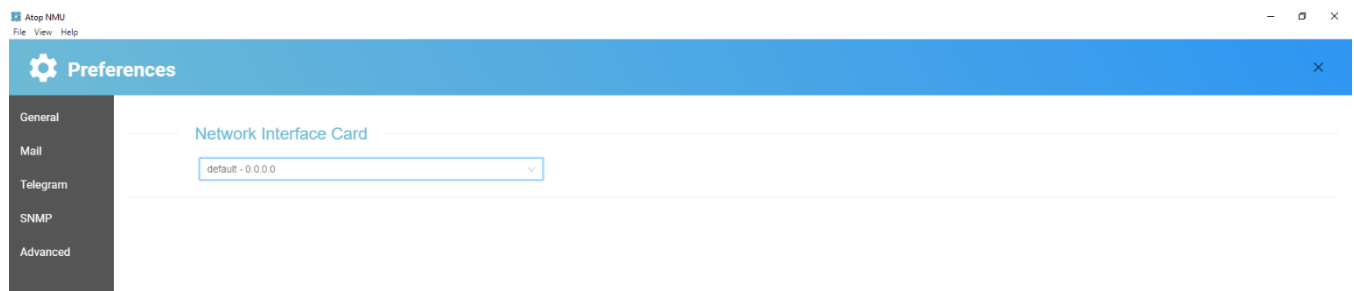
Figure 4.2 File → Preferences Sub-menu

4.1.2   *General Tab*

The **File → Preferences → Genera**l tab displays the **Network Interface Card**. All interfaces, including virtual interfaces, are listed here as shown in Figure 4.3 below.
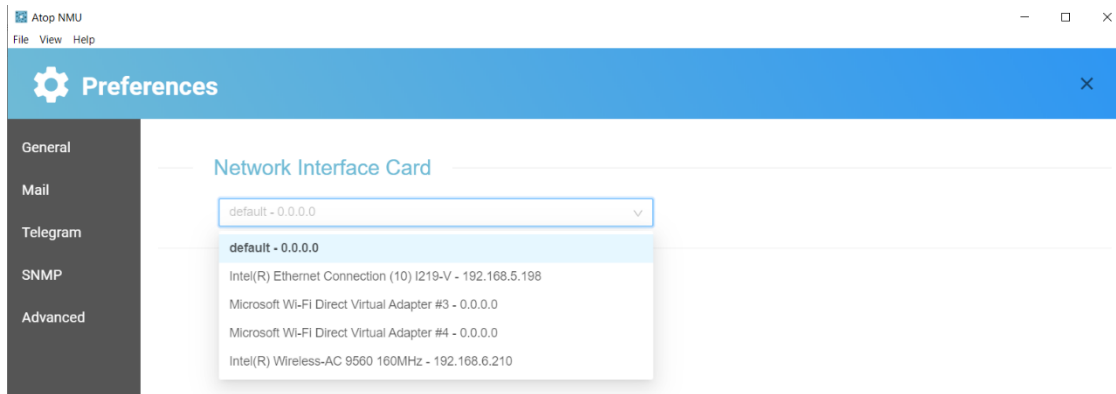
Figure 4.3 File → Preferences → General

4.1.3   *Mail Tab*

Under **File → Preferences → Mail**, users can enable automatic mail notifications, as shown in Figure 4.4 below. Toggle **Enable Notification** to enable the service via providers such as Gmail, Hotmail, or Yahoo. Select option **Mail Service List** if using mail service from an available standard provider; otherwise, select **User Definition** and enter your choice of host mail and port.
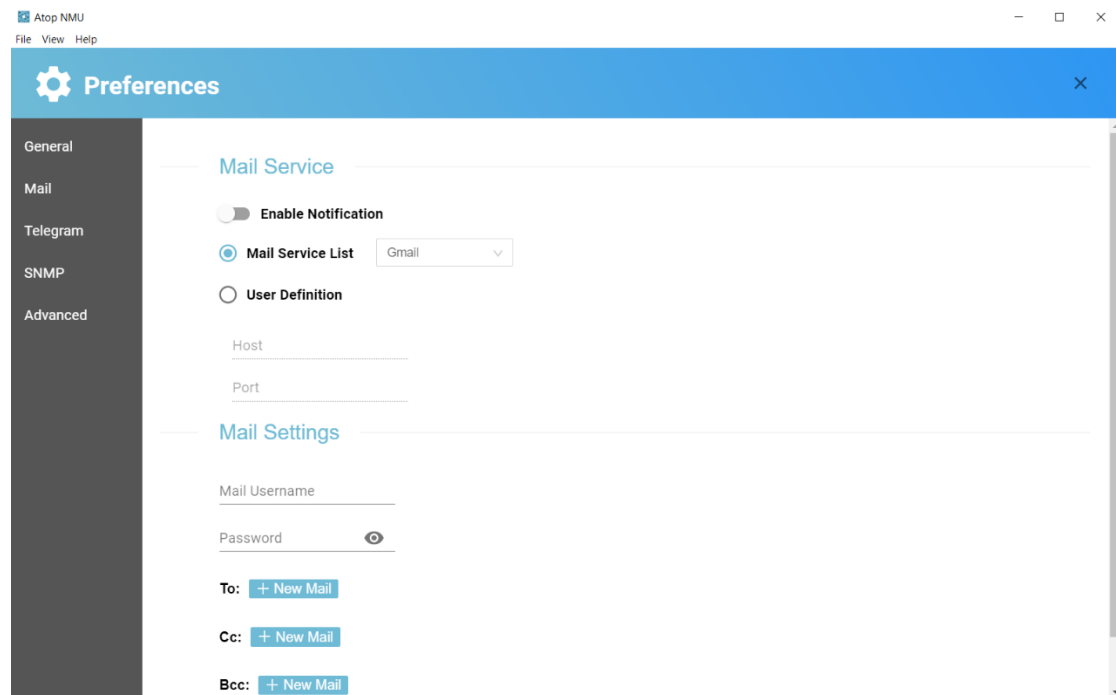
Figure 4.4 File → Preferences → Mail

The various choices of mail services are as shown in Figure 4.5 below.
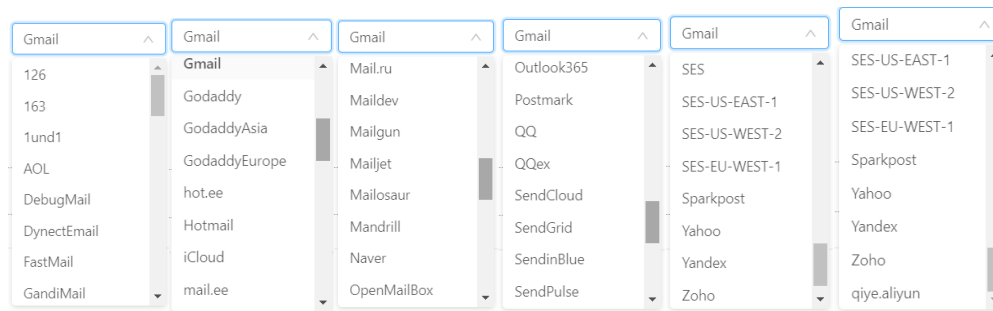
Figure 4.5 List of Mail Services Available within File → Preferences option → Mail tab

Click **+ New Mail** to enter valid email addresses for each email header: **To:**, **CC:**, and **BCC:**.

4.1.4 *Telegram Tab*

In **File → Preferences** option → **Telegram** tab, users can enable Telegram Notifications and configure settings to receive offline notifications. Functions include:

· Saving Telegram Token ID
· Sending test messages
· Adding new users to receive alarm messages
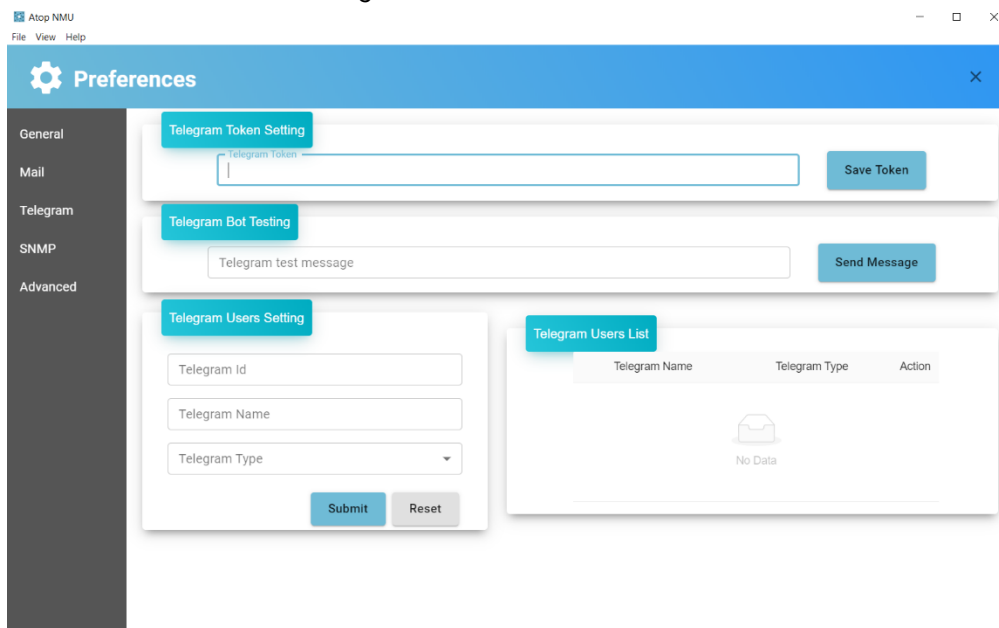
Figure 4.6 Configure the Telegram Notification to Receive Offline Event Messages

Reference: How to Get Your Telegram Token?

In this tutorial we will look at a quick way to create a bot on Telegram. You can find more detailed information on the **official site.**

You can use your APP, Web or PC version Telegram to complete 4 simple steps to set up your Telegram bot:

Step 1. Find the Telegram bot named "@botfarther", he will help you with creating and managing your bot.

 Figure 4.7 Find the BotFather

Step 2. Send the message "/help" and you will see all possible commands that the Botfather can operate.
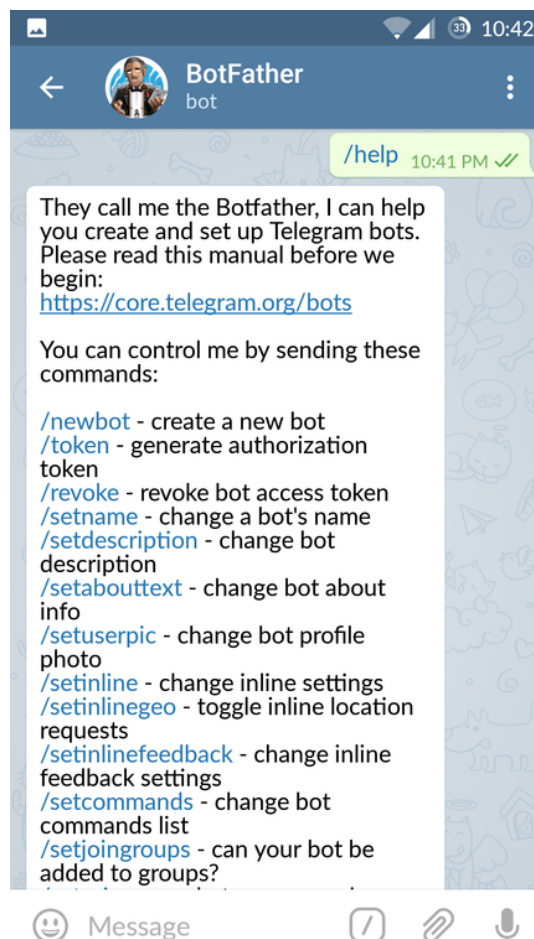
 Figure 4.8 Start Telegram Bot Setup

Step 3. To create a new bot, send "/newbot" or click on the Botfather's /newbot link.

Follow the instructions to create a new name for your bot. The name has to be unique, so if you are creating a trial bot only, you can namespace your bot by placing your own name at the start of its username. Screen names can be anything you like.
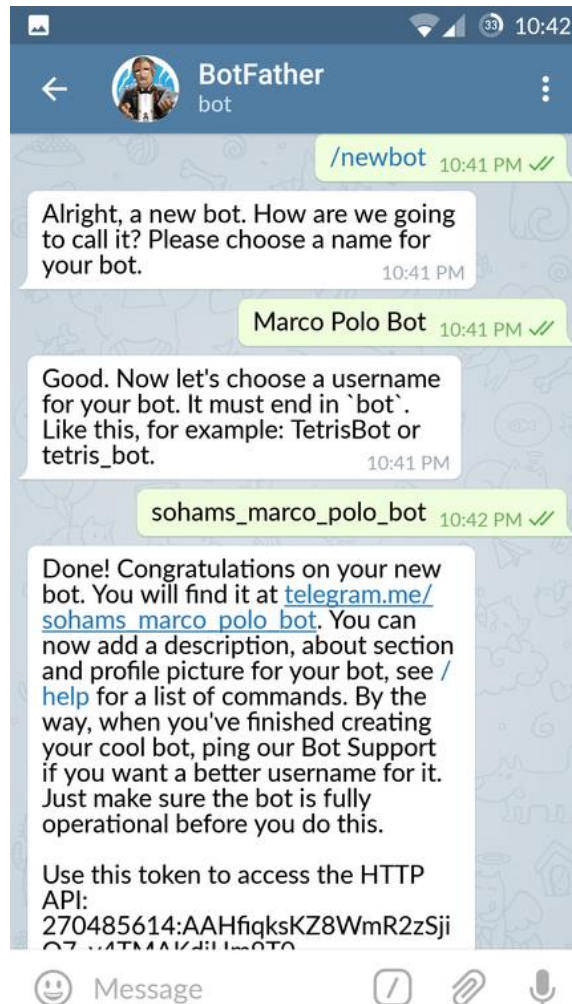
Figure 4.9 Name Your Telegram Bot

Reference: How to get your Telegram ID?

Step1. Start Chat room with your Bot
Step2. Send "/getId" in the chat room
Step3. Your Bot will reply its id, as below "1699644503"
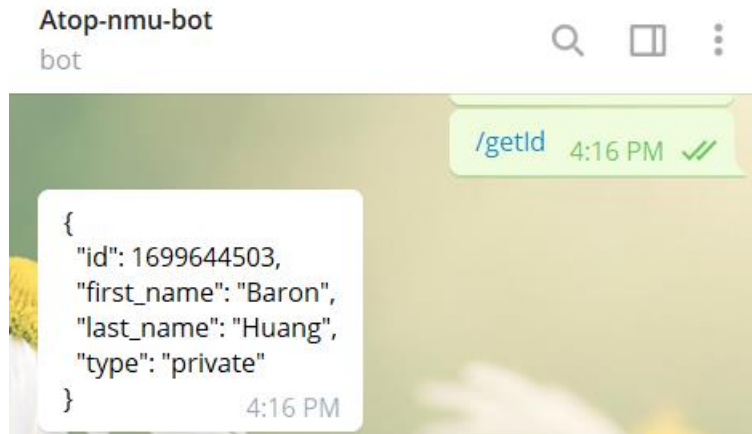
Figure 4.10 Get Telegram ID

4.1.5   *SNMP Tab*

In the **File → Preferences** option → **SNMP** tab, users can enable SMNP service and configure settings such as SNMP Scan, Default Community, and Others, as shown in below.
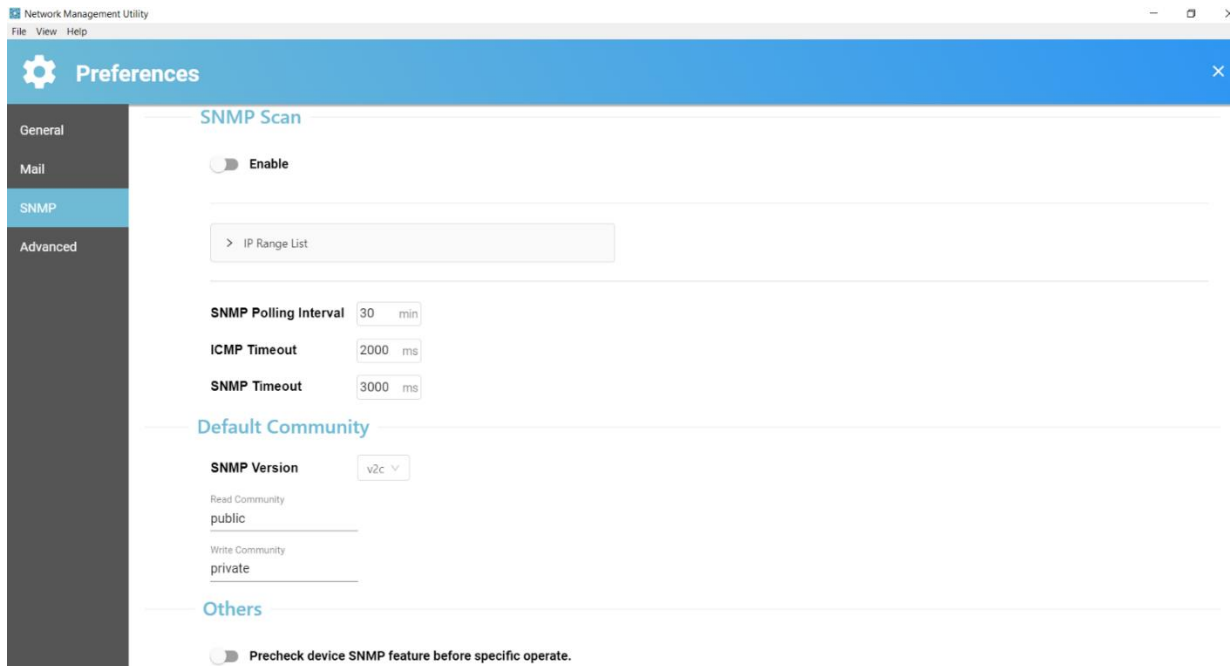
Figure 4.7 SNMP Scan Section View Within File → Preferences → SNMP

In **File → Preferences** option → **SNMP** tab, toggle ⬤ Enable to enable SNMP scan, and click ⊞ ADD to add range of IP addresses in IP Range List, as shown in below.
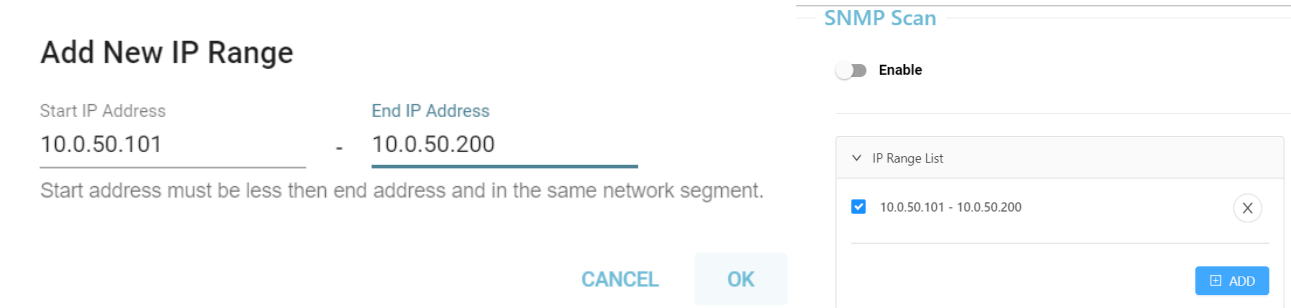
Figure 4.8 SNMP Scan Section within File → Preferences Sub-menu → SNMP

Please refer to Section 4.1.5 if SNMP function cannot be enabled. If the message "This feature only for device with SNMP support" persists, and the **"OK"** link cannot be clicked even when SNMP function is already enabled via the **Network Management Utility Setup 2.X,** the user should enable SNMP function via the device's web interface instead. Follow the instructions in Section 5.6.1 to initialize a web configuration page. Note that when SNMP is enabled, the device type changes from Basic to Basic/SNMP, as shown in Figure 4.9.

Online	Device Type	Model	IP Address	MAC Address	Hostname	Kernel	Ap	Access
🟢	Basic/SNMP	Managed Switch, EHG7508-8PoE	10.0.50.1	00:60:E9:19:53:8B	EHG7508	3.11	3.11	✓

Figure 4.9 Device Type is shown as Basic/SNMP

The description of each field in the SNMP Scan section is shown in Table 4.1.

Table 4.1 Description of each field in File → Preferences → SNMP

Field Name	Description	Default Value
IP Range List	Start and end IP addresses of devices to scan with SNMP messages	N/A
SNMP Polling Interval	The period of time between the end of the previous polling's timeout period and start of the next polling, where polling consists of launching remote queries synchronously, either actively or on demand.	30 mins
ICMP Timeout	The maximum number of milliseconds before an ICMP response is received	2000 ms
SNMP Timeout	The maximum number of milliseconds before an SNMP response is received	3000 ms

In **File → Preferences** option → **SNMP** tab, users can set the **Default Community**, as shown in Figure 4.10 below.

Default Community

SNMP Version   v2c ∨

Read Community
public

Write Community
private

Figure 4.10 Default Community section within File → Preferences → SNMP

The description of each field in the Default Community section is shown in 4.2 below.

Table 4.2 Description of each field in the Default Community Section under File → Preferences → SNMP

Field Name	Description	Default Value
SNMP Version	Version of SNMP available on SNMPv1 and SNMPv2c (with data encryption)	v2c
Read Community	Community string (in clear text) to allow access to read device data	public
Write Community	Community string (in clear text) to allows access to read and write device data or edit its configurations	private

To allow public viewing/editing of device information, enable the **SNMP** function by toggling the **Enable** option and fill in the two passphrases (or SNMP Community Strings) below it. Entering the passphrase for **Read Community** allows other network management software to read the connected device's information. Entering the passphrase for **Write Community** allows other network management software to read/modify the connected device's information. The default SNMP Community Strings (or passphrases) for **Read Community** and **Write Community** are "**public**" and "**private**", respectively.

In the **File → Preferences** option → **SNMP** tab → **Others** section, users can select whether to precheck device SNMP features before specific operations, as shown in Figure 4.11 below.

Others

⬤ **Precheck device SNMP feature before specific operate.**

Figure 4.11 Others section within File → Preferences → SNMP

Before performing specific operations such as network configuration, the program will precheck device SNMP feature, as shown in below Figure 4.12.
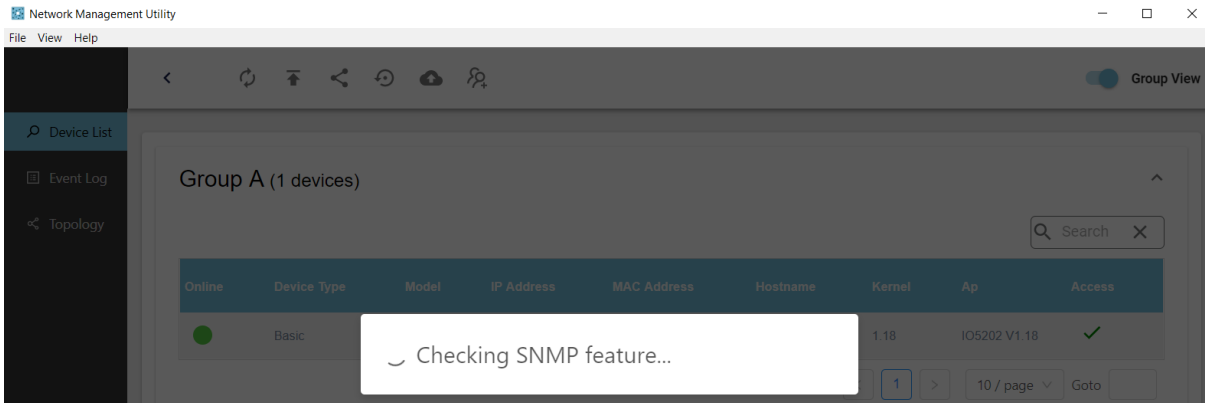
Figure 4.12 Precheck Device SNMP Feature First before Specific Operations

4.2   *View*

The second drop-down menu in the top menu bar is **View**, as shown in Figure 4.13. In this menu, there is one option:
  - Toggle to full screen

Figure 4.13 Toggle Full Screen Option within View Menu

Once **Toggle to Full Screen** is selected, or when the F11 key is pressed, the NMU window will expand to full screen. Re-select the option or press F11 again to reduce the window to its original size.

4.3   *Help*

The third drop-down menu on the top menu bar is **Help**, as shown in Figure 4.14. In this menu, there is one option:
  - About Network Management Utility

Figure 4.14 About Network Management Utility Submenus within Help Menu

When **About Network Management** is selected, the NMU logo and version number will appear, as shown in Figure 4.15 below.

ABOUT
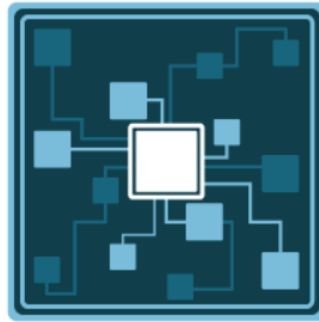
Figure 4.15 About Network Management Utility Window

5 Side Vertical Menu

The **Side Vertical Menu** consists of the following items, as shown in Figure 5.1:
- Dashboard
- Device List
- Event Log
- Topology
- Users
- Device Config
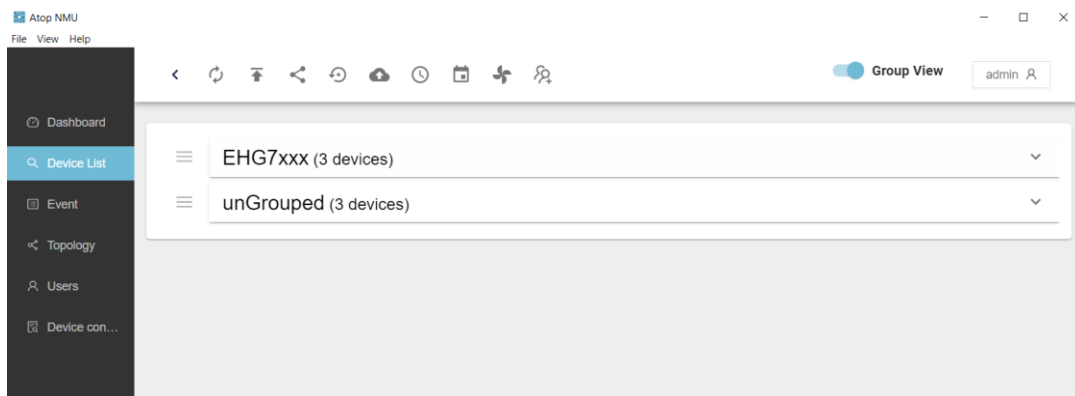
Figure 5.1 Side Verticle Menu

5.1   *Dashboard*

The Dashboard contains several widgets that provide summary information about your network devices, event highlights, and server disk space utilization. A Device Summary table indicates the quantity of Online/Offline devices.
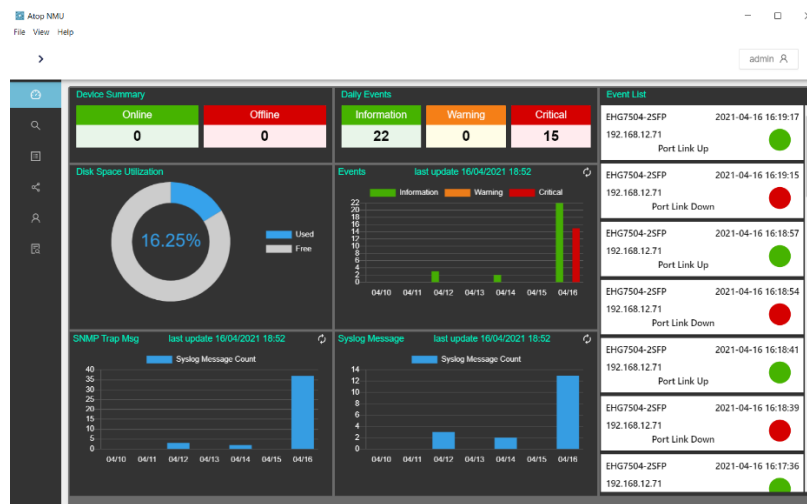
Figure 5.2 Dashboard

Use the Dashboard to gain a quick overview of your network devices, important system events, and server disk space utilization. The Dashboard displays the following widgets:
1) Device Summary
2) Daily Events

3) Disk Space Utilization
4) Events
5) SNMP Trap Msg
6) Syslog Message
7) Event List

Device Summary
The Device Summary table displays the quantity of Online/Offline devices in the Network:

Figure 5.3 Device Summary

Daily Events
The Daily Events table displays the daily number of events in different severities:
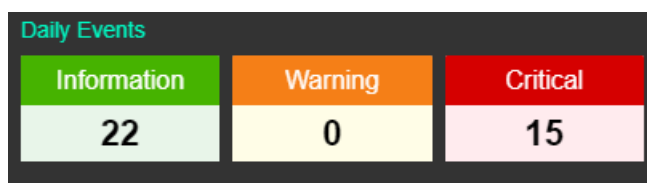
Figure 5.4 Daily Events

Table 5.1 Event Severity Table

Event	Critical	Warning	Information
Cold Start	√		
Warm Start	√		
Port Link Up			√
Port Link Down	√		
Authentication failure		√	
Power Status: OK			√
Power Status: Fault	√		

Disk Space Utilization
The Disk Space Utilization widget displays information about storage capacity available on the NMU server computer.
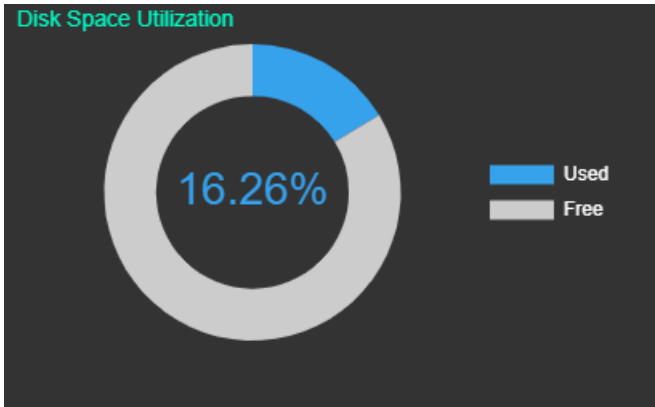
Figure 5.5 Disk Space Utilization

Events

The Events widget displays the number of events issued for your network, and the day on which the events occurred. You can perform the following actions on this widget:

• To view the number of events 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 All Events screen, click a bar on the widget chart.
• To refresh widget data, click the Refresh (⟳) button on the upper right corner.
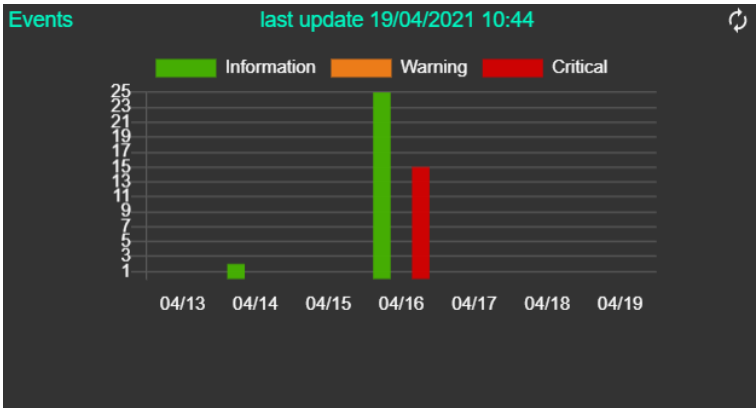
Figure 5.6 Events

SNMP Trap Msg

The SNMP Trap Message widget displays the number of SNMP Trap messages issued for your network, and the date on which the events occurred. You can perform the following actions on this widget:

• To view the number of events 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 All Events screen, click a bar on the widget chart.
• To refresh widget data, click the Refresh (⟳) button on the upper right corner.
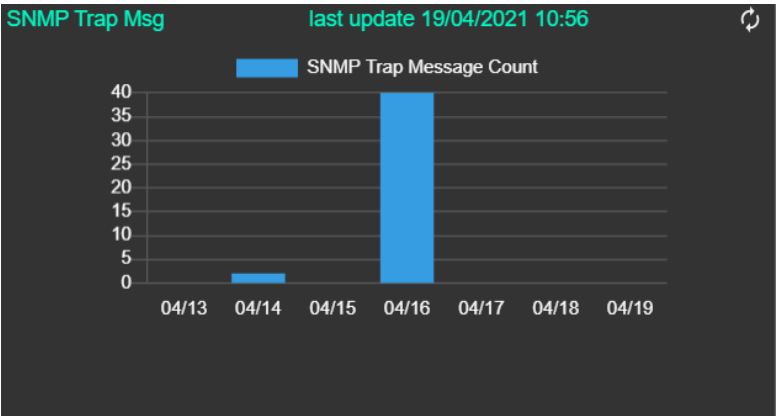
Figure 5.7 SNMP Trap Msg

Syslog Message

The Syslog Message widget displays the number of Syslog messages issued for your network, and the date on which the events occurred. You can perform the following actions on this widget:

• To view the number of events 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 All Events screen, click a bar on the widget chart.
• To refresh widget data, click the Refresh (🗘) button on the upper right corner.
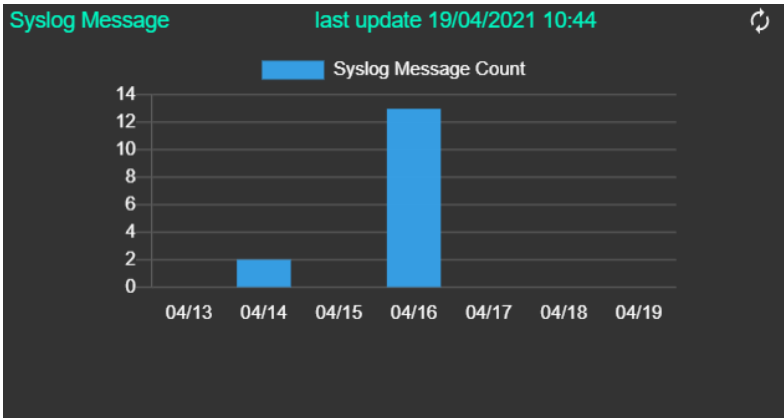
Figure 5.8 Syslog Message

Event List

The Event List widget displays the latest 30 event messages issued for your network, and the date on which the events occurred. You can view the below event details on this widget:

 •IP/
• Model Name
• Event Message

• Date & Time
• Severity

Figure 5.9 Event List

5.2 *Device List*

The **Device List** (Magnifier icon) on the Side Vertical Menu consists of:
1) a device table for each device group's working space and
2) a top horizontal icon bar.
In this section, we will only describe the first part. Details of the top horizontal icon bar will be explained in Chapter 6.

In the Side Vertical Menu→ **Device List**, connected devices are listed according to its group. Any devices that have not been added to any group will be listed in the unGrouped section, as shown in below. As described in Section 3, the list of found device(s) is displayed as a table with the following columns: **Online**, **Device Type**, **Model**, **IP Address**, **MAC Address**, **Host Name**, **Kernel**, **Ap**, and **Access**. When users click on a column title, the devices are sorted according to values in that column.
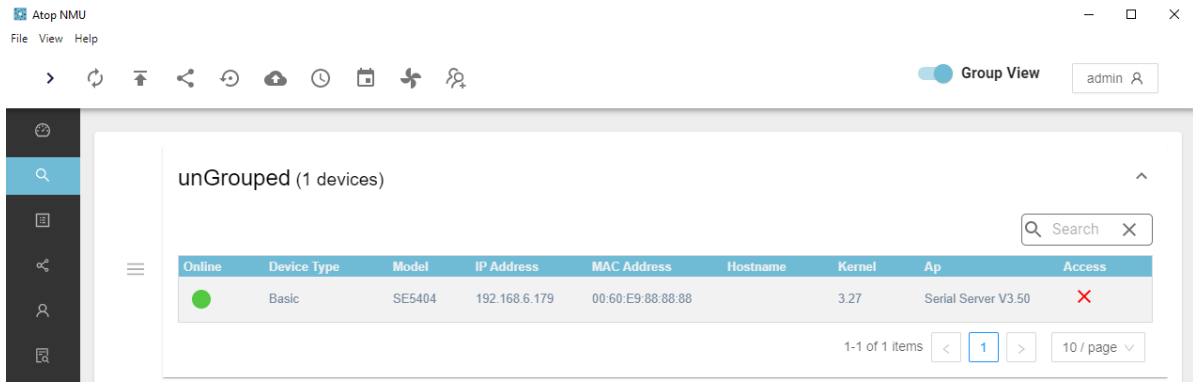
Figure 5.10 List of Connected Devices in Side Vertical Menu → Device List

The description of each field in the Side Menu→Device List is shown in Table 5.2 below.

Table 5.2 Description of each field in the Side Menu → Device List

Field Name	Description
Online	Status of each device: active (green dot) or inactive (red dot)
Device Type	Indicate whether it is a basic or an advanced device
Model	**Model** number of the device
IP Address	**IP Address** of the device
MAC Address	**MAC Address** of the device
Host Name	**Host Name** of the device
Kernel	**Kernel** version of the device
AP Information	Application version of the device
Access	Indicate whether the device is already accessible (✓) or not (✗). Users have to create a group and add the device to that group first to view it as accessible.

5.3   *Add New Group*

As mentioned in Chapter 3, a device must belong in a group before a user can access it. To create/add a new group, click on the **Add New Group** icon on the horizontal icon bar. A new small box will appear for entering a group name, as shown in below. After entering the group name, click on the **APPLY** button.
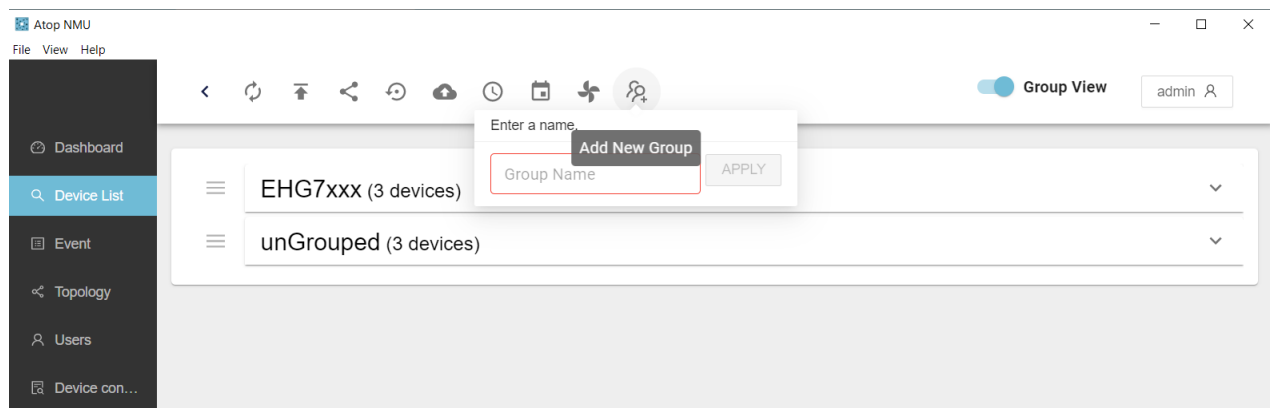
Figure 5.11 Click Add New Group Icon in the Top Horizontal Icon Bar

Once the new group is successfully created, a notification window will appear with a success message, as shown in below.
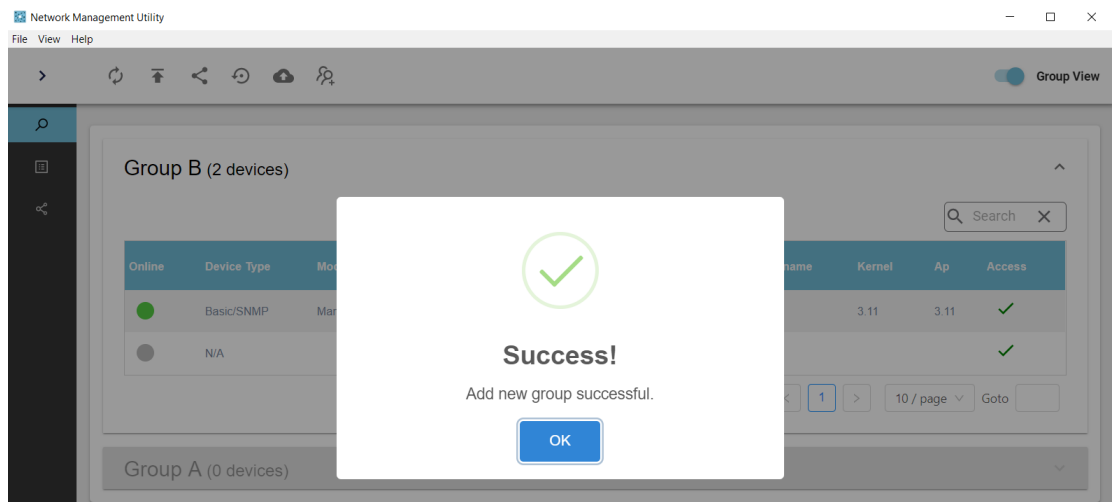
Figure 5.12 Success Window after Successfully Adding a New Group

5.4 *Group View (Toggle Icon)*

On the upper right corner of the screen, there is a toggle menu ⬤ Group View , called **Group View**. If this toggle is enabled, the middle working space will display active devices in group view. If disabled, all connected devices will be displayed in the same working area without classifying into groups. Figure 5.13 (a) shows lists of devices by group, while Figure 5.13 (b) shows a list of devices without grouping. Connected devices that are not yet added to a group will be listed in an **unGrouped** section.
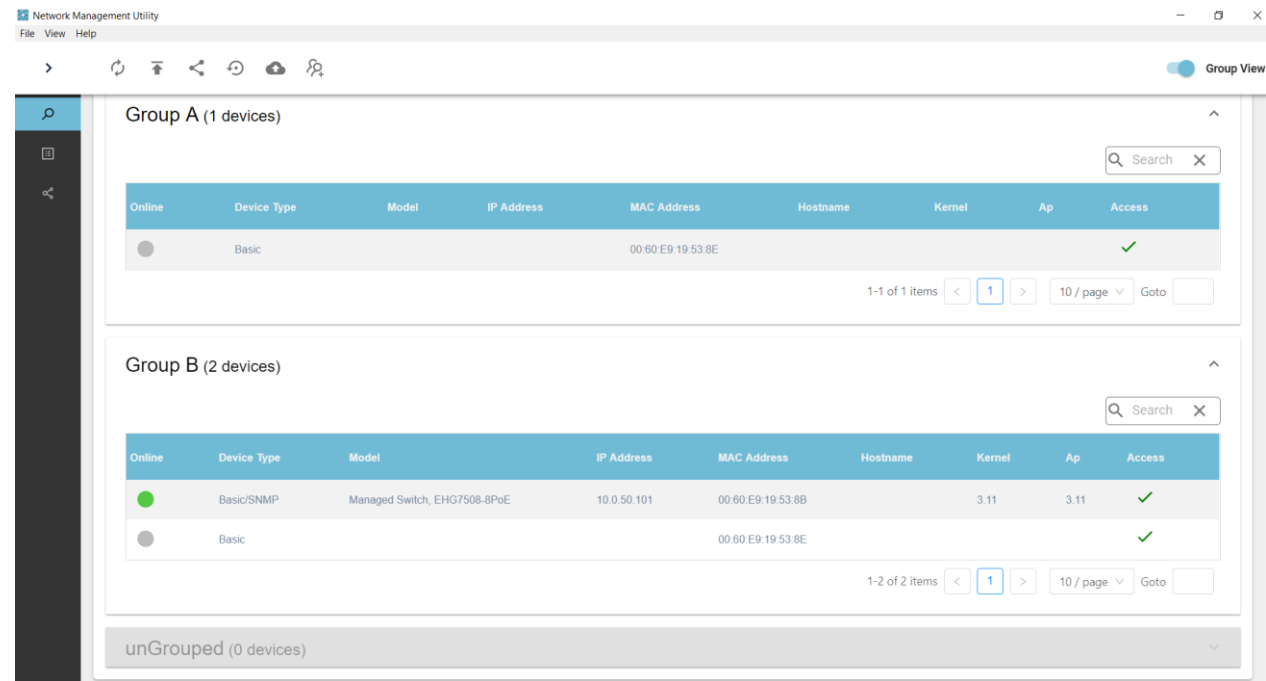
(a)
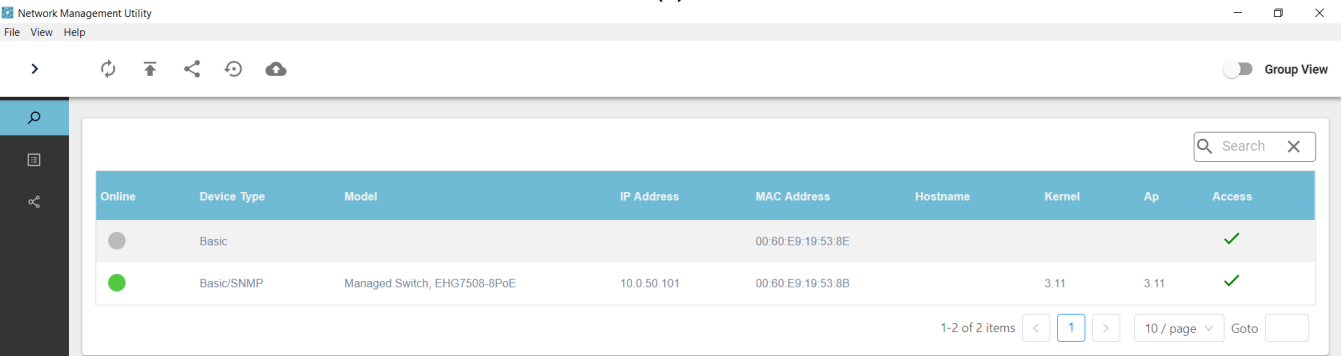
(b)

Figure 5.13 Lists of Devices (a) in Grouping (b) Without Grouping

5.5   *Edit groups*

In the Device List working space, right-click on a group box anywhere outside the device table to display the following menu: **Edit Group Name**, **Remove Group**, and **Edit Member**, as shown in 錯誤! 找不到參照來源。. Note that the unGrouped section does not have this menu available.
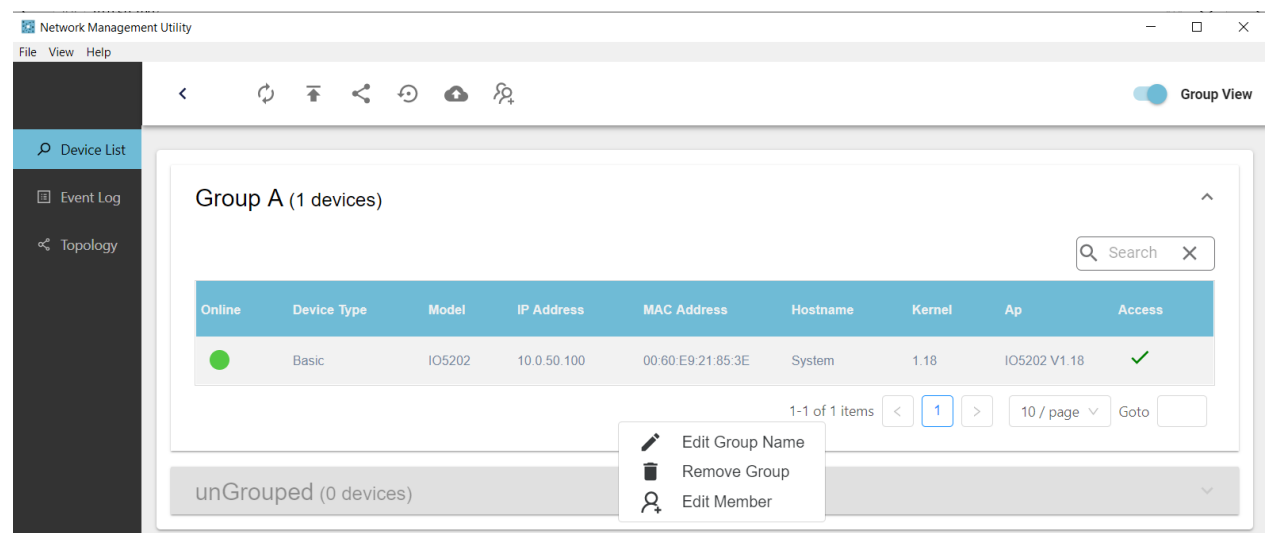
Figure 5.14 Right Click on Any Space in a Group Box but Outside of the Device Table

5.5.1 *Edit Group Name*

Clicking on **Edit Group Name** launches a small new window as shown in below. Enter the new group name and then click **APPLY** button to implement.
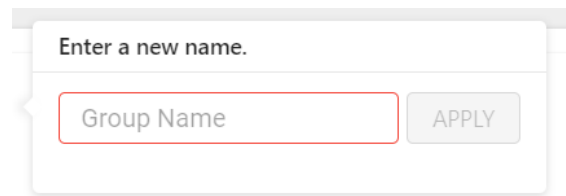
Figure 5.15 Enter a New Name Window

5.5.2 *Remove Group*

Clicking on **Remove Group** will cause a small new window to pop up. Click on **OK** to confirm removal, as shown in below.
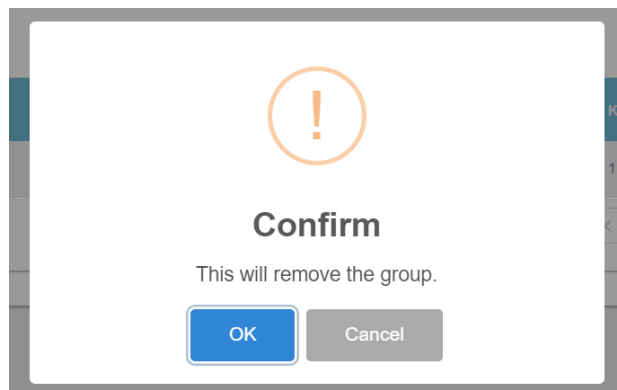
Figure 5.16 Confirmation Dialog for Removing a Group

When the selected group is successfully removed, a new window is initialized to notify its success, as show in below.
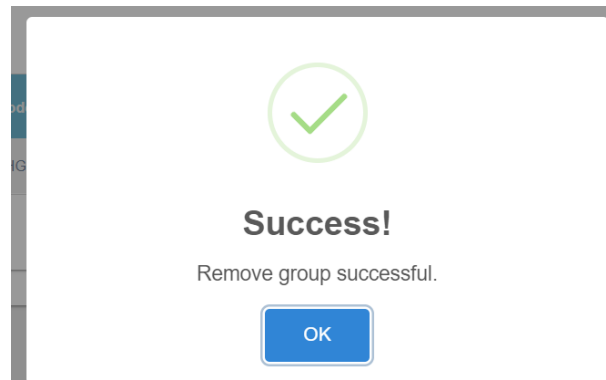
Figure 5.17 Confirmation on Sucessfully Removing a Group

5.5.3 *Edit Member*

Clicking on **Edit Member** will launch a new **Group *x* - Edit Group Member** window. Select devices to add in the **Group *x*** (Group A in this example), and click the **> Add Member** button to move devices from the left sub-window into the right sub-window, as shown in below. Note here that each device can be added into more than one group.
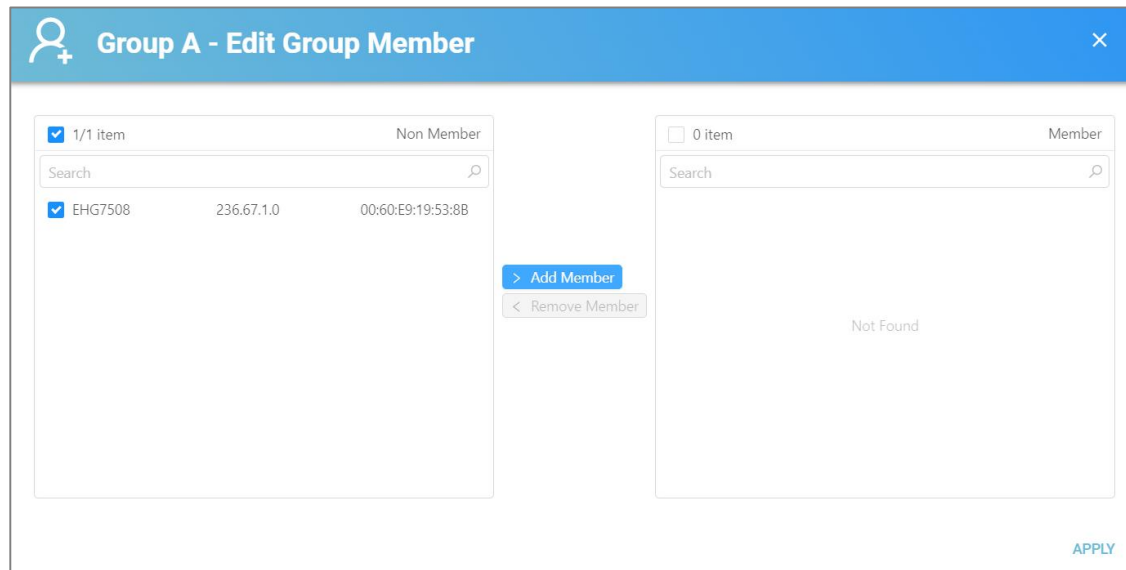
Figure 5.18 Add Member to the Selected Group

To remove any devices from the selected group (**Group A** in this example), click on devices to be removed, and then click the **< Remove Member** button to move devices from the right sub-window into the left sub-window, as shown in below.
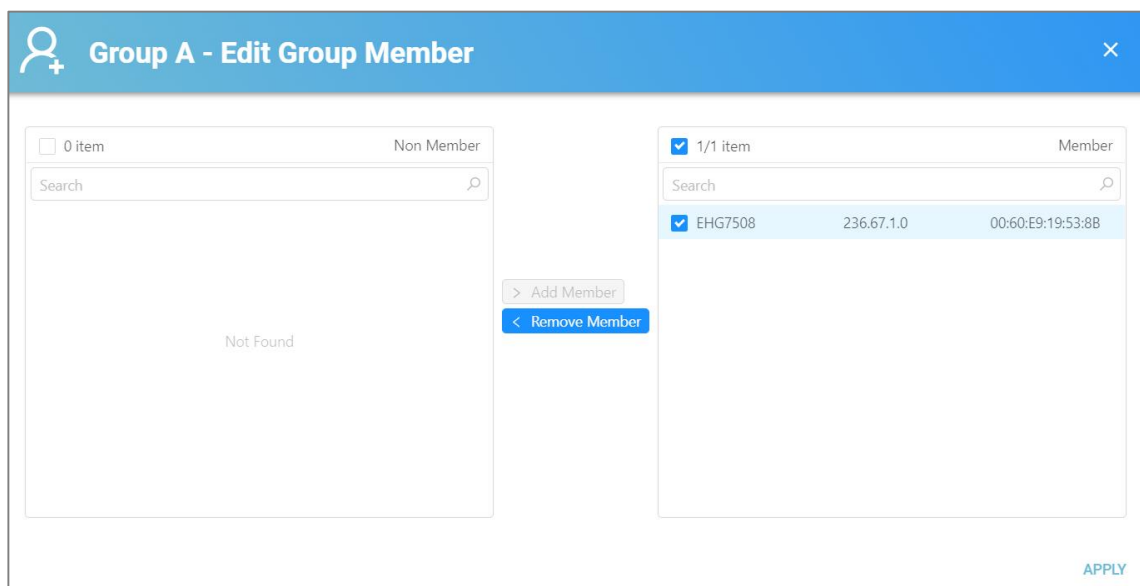
Figure 5.19 Remove Member from the Selected Group

After clicking the **APPLY** button, the **Edit Group Member** window is closed and devices in Group A are shown in the device list. A small notification window for **Device Online** will appear on the bottom right corner, as shown in below
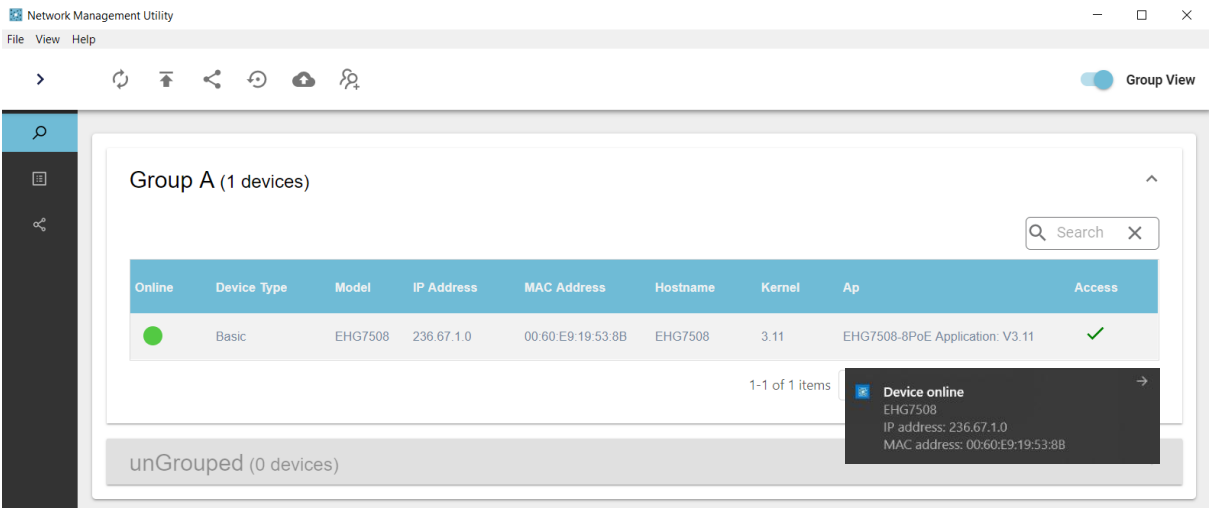
Figure 5.20 Devices Added/Removed To/From Group A

5.6   *Perform actions on devices assigned to groups*

Right click on a device in the device table of any group, and a drop-down menu will appear as shown in below: **Open Web**, **Telnet**, **Beep**, **Reboot**, **Network Setting**, **Device Advanced Setting**, **Port Information**, and **Backup and Restore**. Note that if a connected device does not belong in a group, this right click feature will not function.
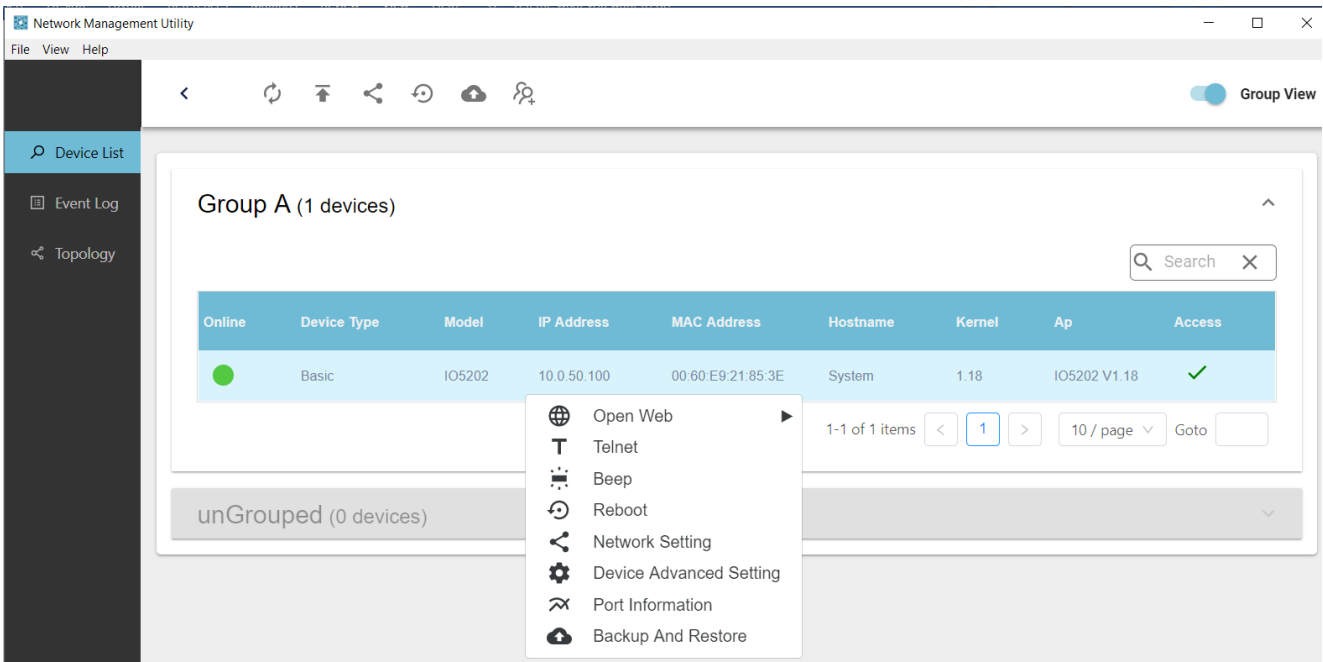
Figure 5.21 Drop-down Menu when Right Click on the Device List in any Group

5.6.1 *Open Web*

Selecting **Open Web → Open on OS browser** will initiate configuration of the device through a web browser, as shown in below. User will be prompted to log in, as shown in below. The default username and password are "admin" and "default".
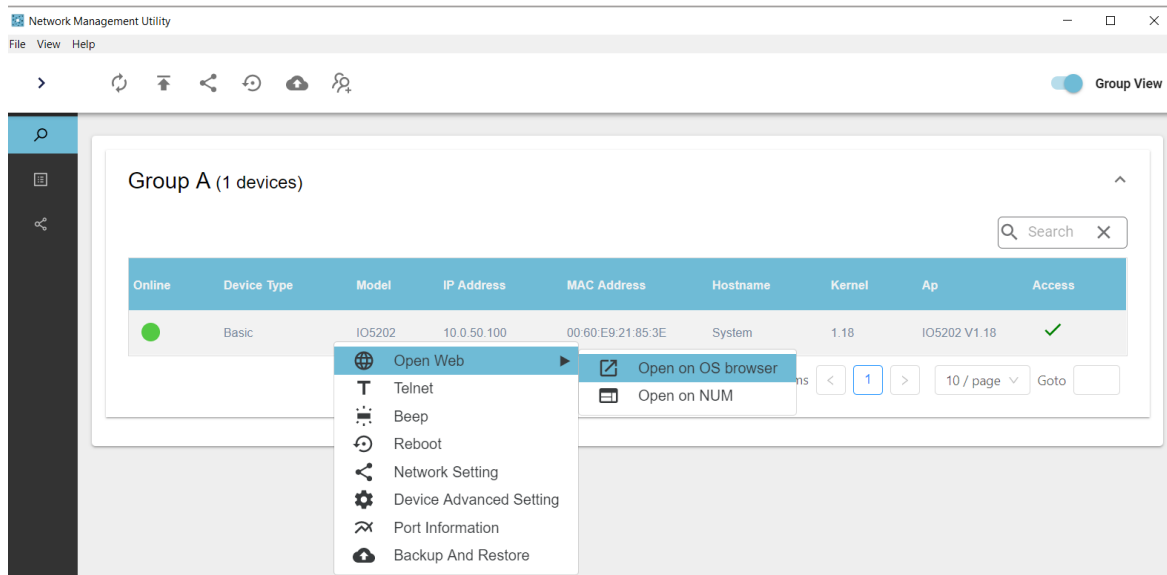
Figure 5.22 Device List → Right Clicka Device in Any Group → Open Web → Open on OS browser
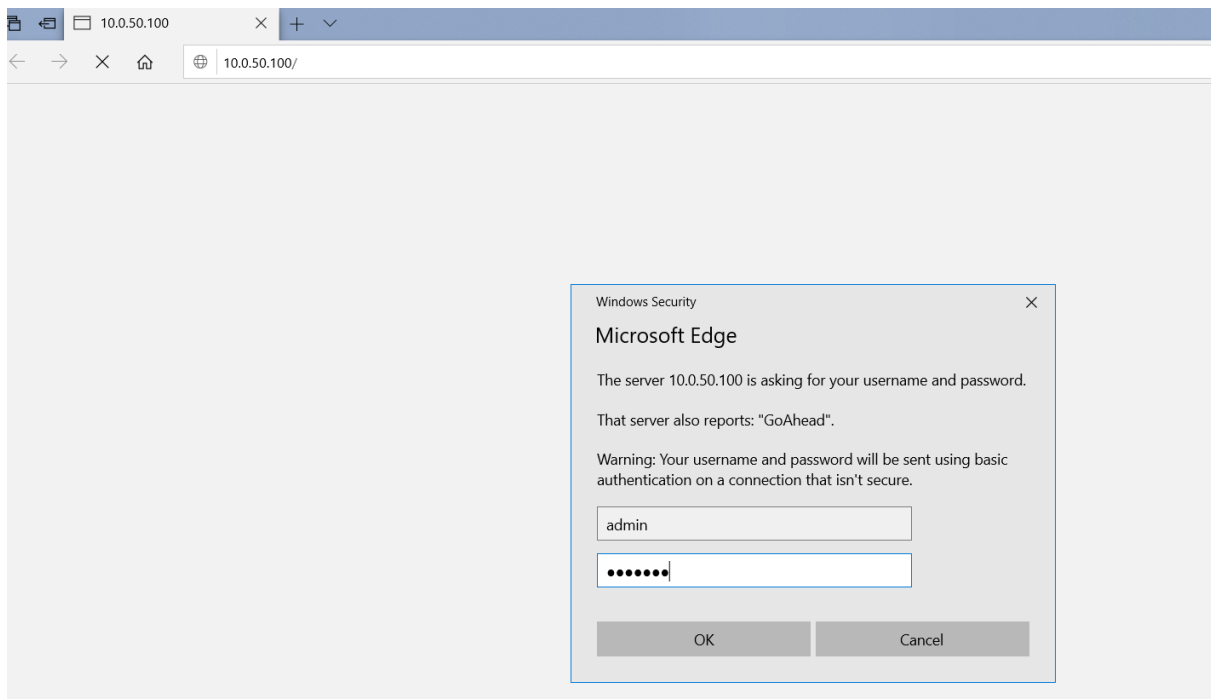
Figure 5.23 Log In to Web-based Configuration

Selecting **Open Web → Open on NMU** will initiate web configuration of the device through NMU, as shown in below. Click the grey circled cross ⊗ on the upper right corner to close the web configuration and return to the Device List working space.
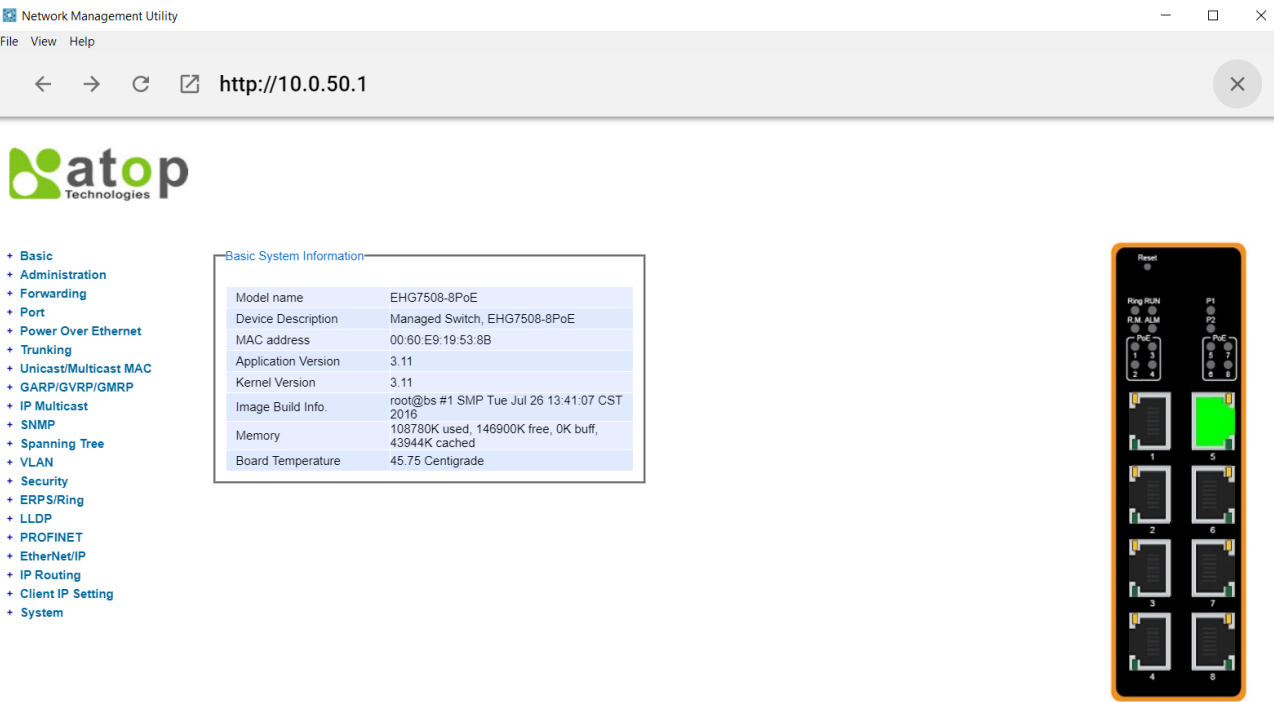
Figure 5.24 Right Click on the Device List in any Group and Select Open Web → Open on NUM

5.6.2 *Telnet*

Selecting **Telnet** will initiate Telnet program.

5.6.3 *Beep*

Selecting **Beep** will initialize the Beep confirm window, as shown in below. Click on the OK button and the device will beep twice.
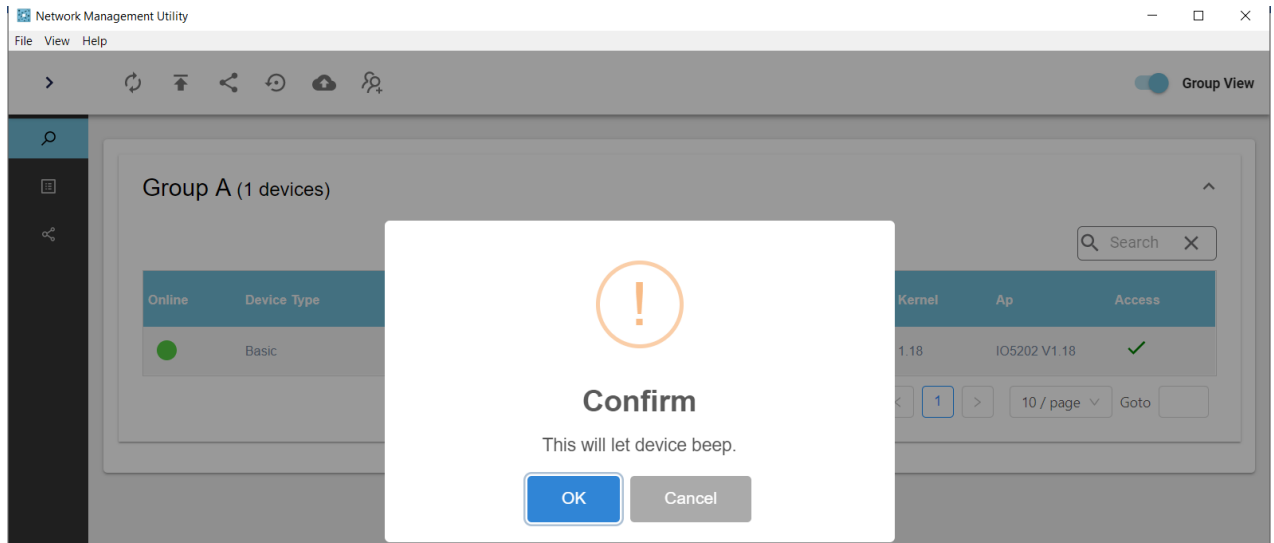
Figure 5.25 Select Beep to Launch the Beep Confirm Window

5.6.4 *Reboot*

Selecting **Reboot** will initialize the Reboot confirm window, as shown in below. Click on the OK button to reboot the device. After the device finishes rebooting, a reboot success window will appear, as shown in below.
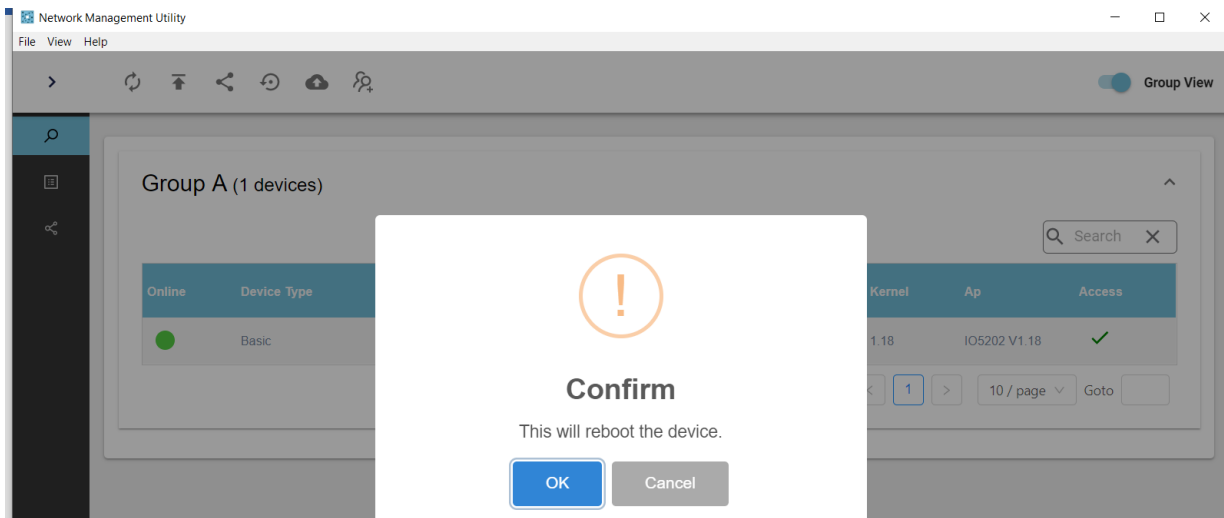
Figure 5.26 Select Reboot to Launch Restart Confirm Window
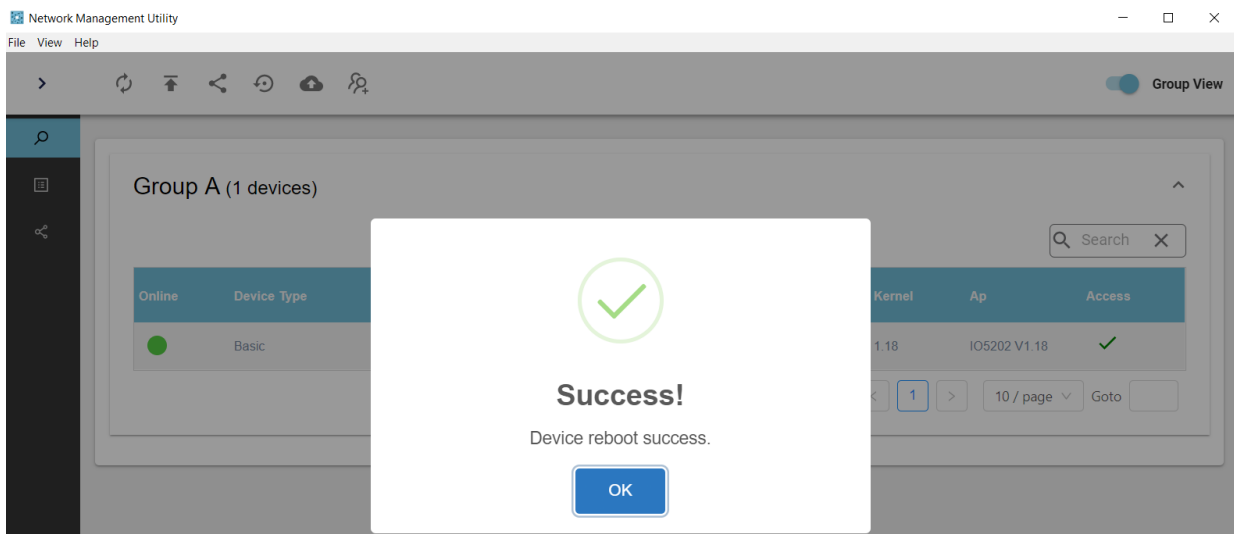
Figure 5.27 Notification of Reboot Success Window

5.6.5 *Network Settings*

Once **Network Settings** is selected, NMU will **Precheck Device SNMP Feature First before Specific Operations** and then initialize the Network Settings window, as shown in below. The display here is a summary of network settings, which is a bit different from the full settings that users can configure through **Network Settings** in the **Top Horizontal Icon Bar**.
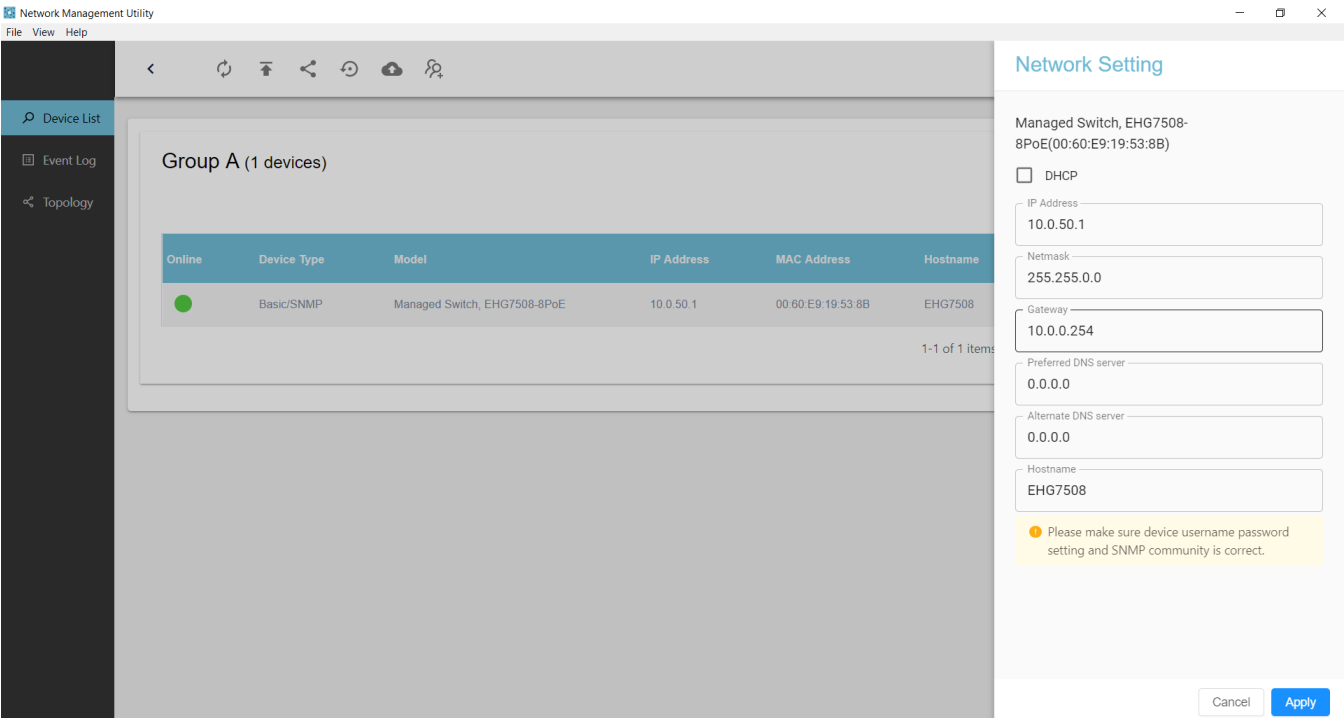
Figure 5.28 Network Settings Window

Enable **DHCP** (Dynamic Host Configuration Protocol) in the first option to allow the device to retrieve its network settings automatically from a DHCP server, which should be available in your LAN. Consult your local network administrator about DHCP server, if necessary. If the **DHCP** option is selected, the other settings within this **Network Settings** window will be disabled, except **Hostname**. If the **DHCP** option is not selected, the **IP Address**, **Subnet Mask**, **Default Gateway,** and the **Preferred DNS** and **Alternate DNS** addresses can be modified. Fill in these settings for LAN interface of the device. After completing all IP network information on this web page, click on the **Apply** button after making sure that the device username, password and SNMP community settings are correct. The **Network Settings** window will close and settings will display in the **Device List** window, as shown in the figure below.
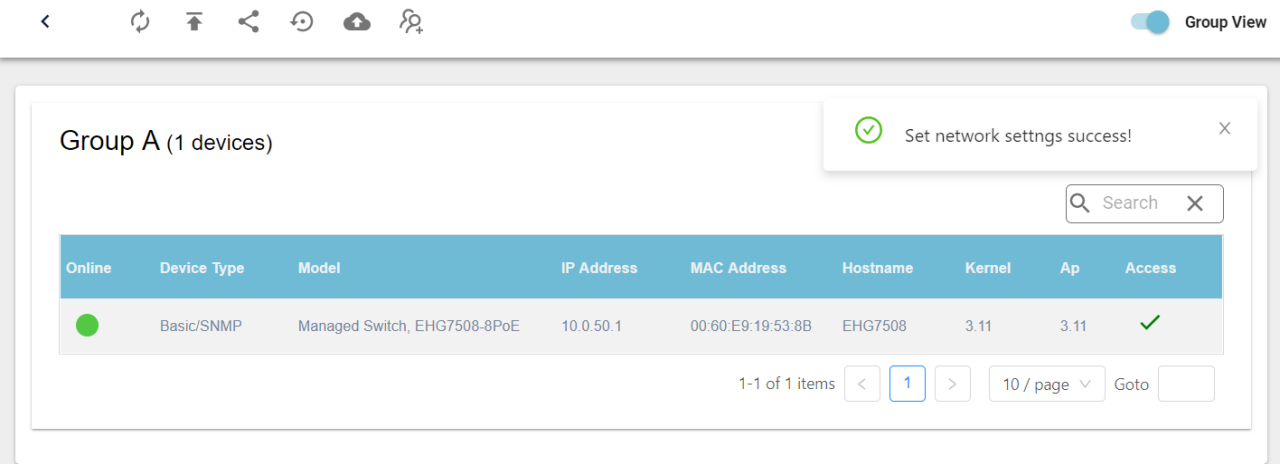
Figure 5.29 Notification of Successful Settings in the Device List Window

5.6.6 *Device Advanced Settings*

Once **Device Advanced Settings** is selected, NMU will **Precheck Device SNMP Feature First before Specific Operations** and then initialize the Advanced Settings window, as shown in below
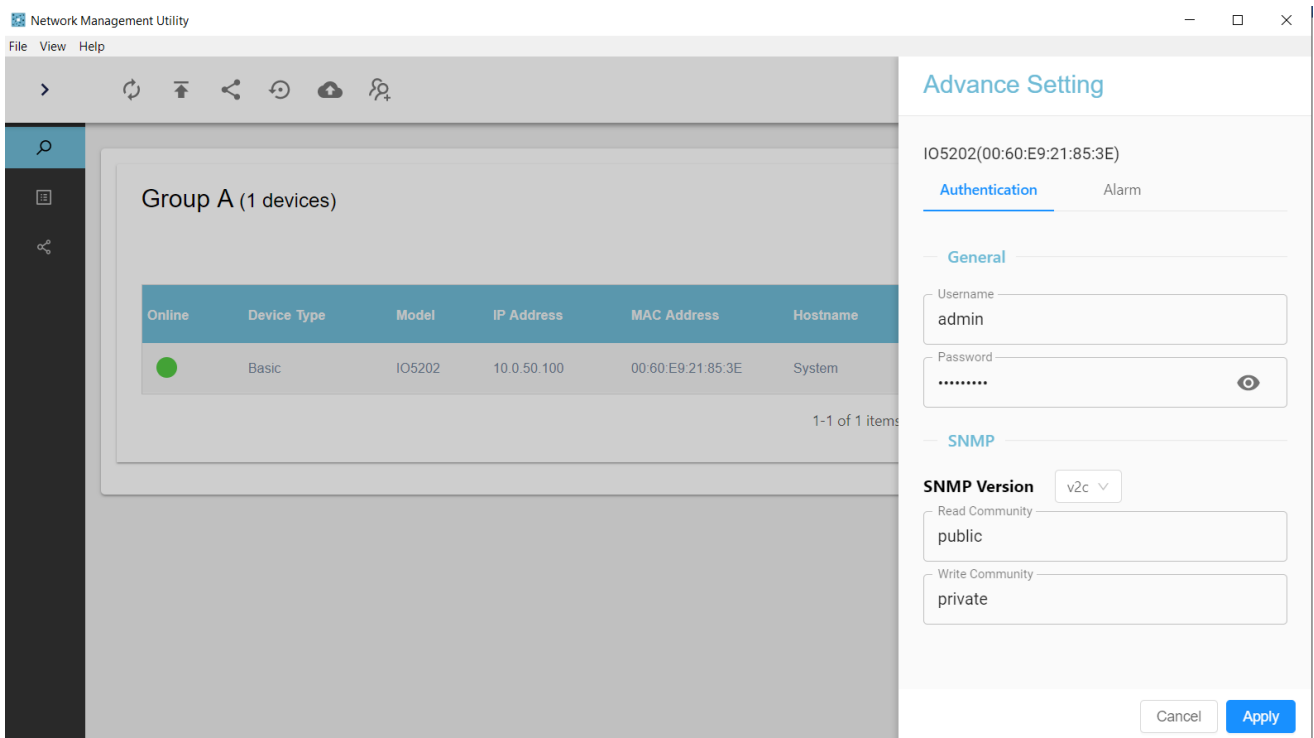
Figure 5.30 Authentication Tab in Advanced Settings Window

The description of each field in the Advanced Setting-Authentication Tab is shown in Table 5.3 below.

Table 5.3 Description of Each Field in Device List → Advanced Settings → Authentication Tab

Sections within Advance Setting	Field Name	Description	Default Value
General	Username	Username to access the device	admin
	Password	Password to access the device	admin123
SNMP	SNMP version	Version of SNMP available for the device (v1 or v2c)	v2c
	Read community	The community string to access device statistics (concept similar to a password)	public
	Write community	The community string to config device (concept similar to a password)	private

The Alarm tab in Device List → Advanced Settings is displayed as below.
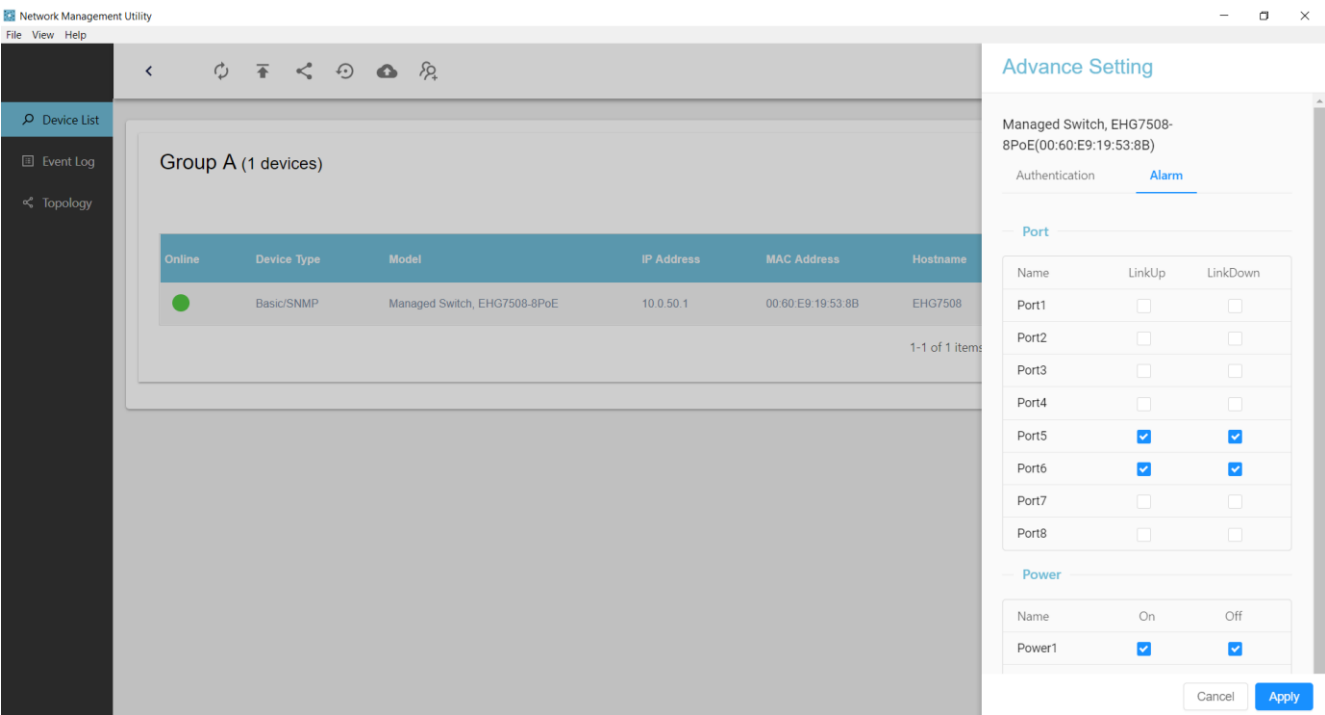
Figure 5.31 Right Click on Device List → Advanced Settings → Alarm Tab

Check the **LinkUp** and **LinkDown** boxes for any port to receive its notifications. Similarly, check the **On** and **Off** boxes for any power source to get notifications on its status change. Below are examples of notifications which will appear individually at the bottom right corner when a change in the chosen port or power source occurs.
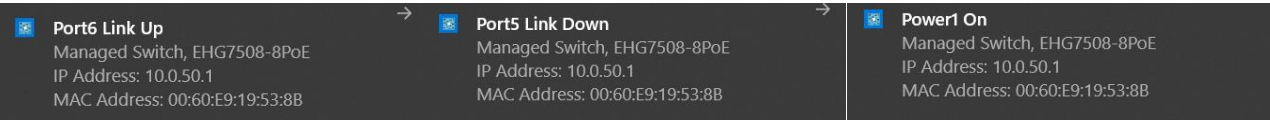
Figure 5.32 Alarm Notifications at the Bottom Right Corner (Appearing One at a Time)

5.6.7   *Port Information*

Once **Port Information** is selected, NMU will **Precheck Device SNMP Feature First before Specific Operations** and then initialize the **Port Information** window, as shown in below. If the SNMP feature fails, enable SNMP through the NMU or web configuration (refer to Section 4.1.5 for detailed settings).
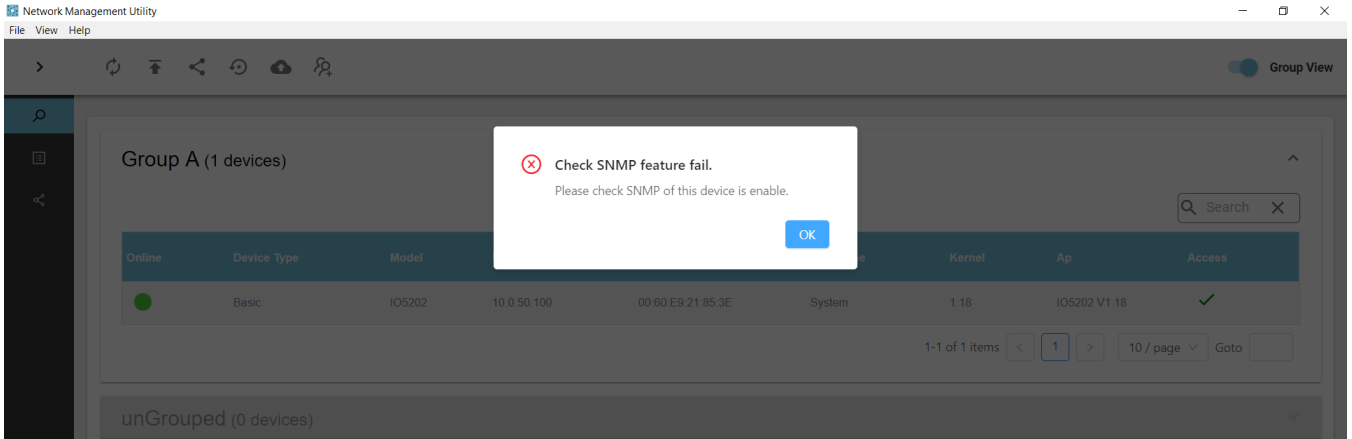
Figure 5.33 Notification of SNMP Feature Fail

The Port Information screen shows device information, graphical real-time traffic, and port status.
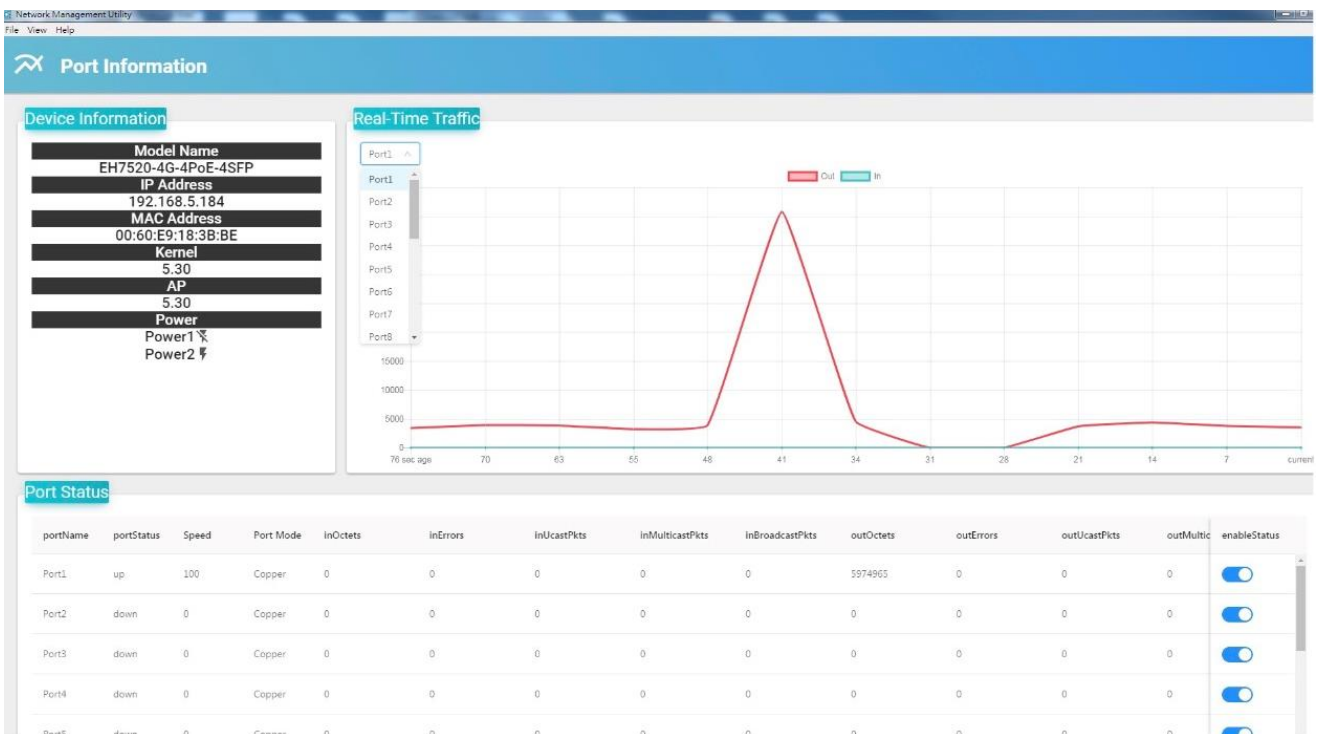
Figure 5.34 Right Click on Device List → Port Information

5.6.8 *Backup and Restore*

Selecting **Backup and Restore** after right clicking on the Device List will initialize the **Backup and Restore** window. Back-up the device configuration by clicking on **SELECT FOLDER** button to select the destination folder, entering a file name, and then clicking on the **BACKUP** button. Make sure that your selected NIC has a real external IP address by clicking on File → Preferences → General → Network Interface Card. If the backup process is successful, a success notification will appear, as shown in below.
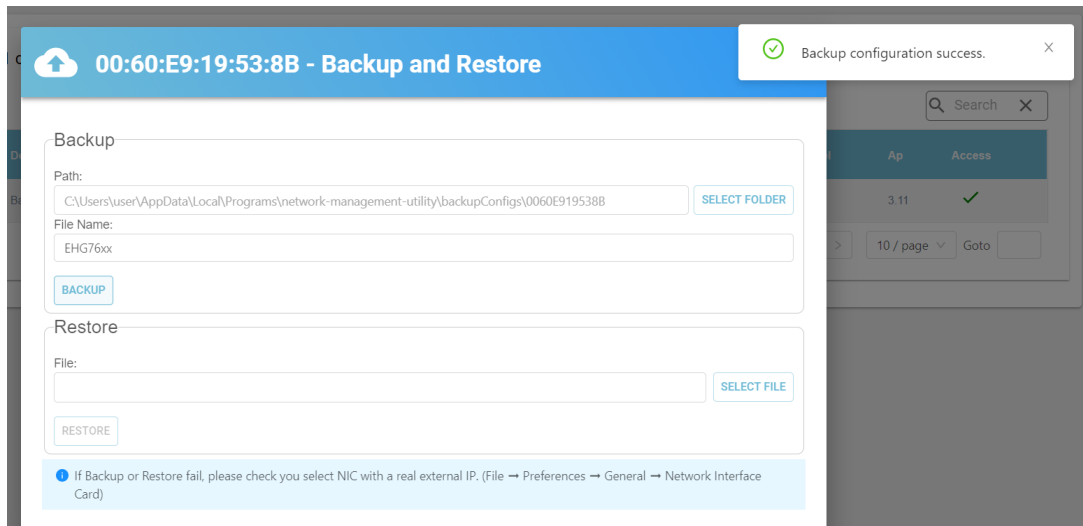
Figure 5.35 Backup View in Backup and Restore

To restore a configuration, select a previously saved configuration filename and then click on the **RESTORE** button. Again, ensure that your selected NIC has a real external IP address by clicking on File → Preferences → General → Network Interface Card. Here, a new small window will be launched. Confirm to restore the configuration by clicking on the **OK** button, as shown in

.
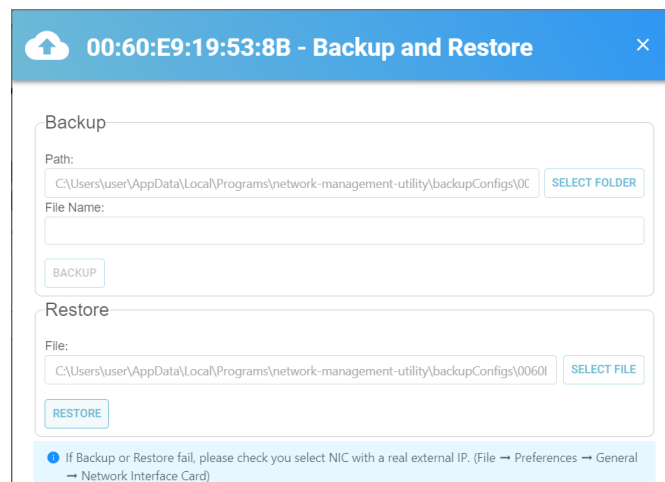
Figure 5.36 Restore View in Backup and Restore

Figure 5.37 Confirmation Window for the Restore Function

If the restoration process is successful, a success notification will appear, as shown in below. The device will then restart automatically, with a few beeps indicating its restart. Notifications will appear on the bottom right corner, alerting of the device becoming offline and then online again.
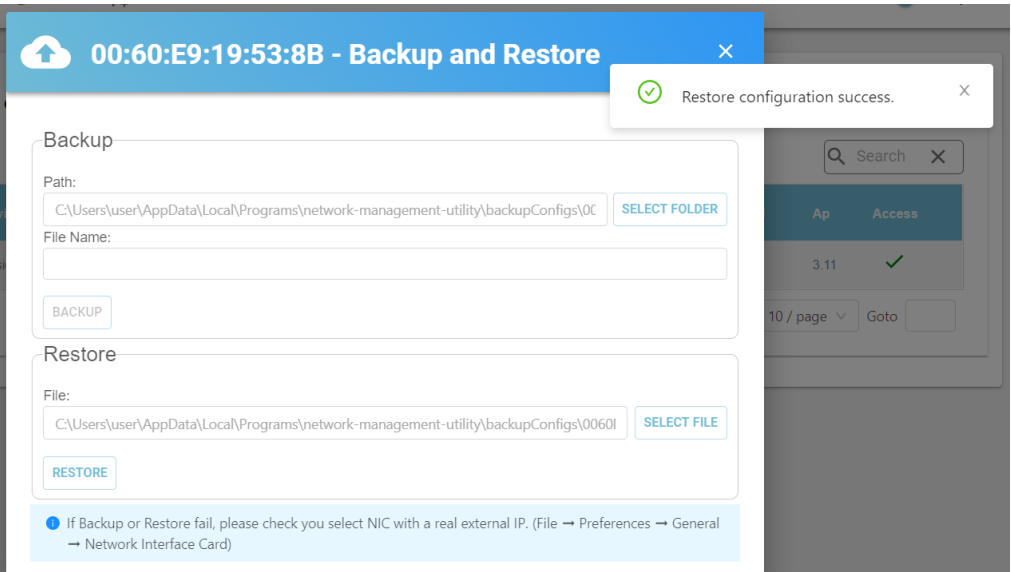
Figure 5.38 Configuration Restore Success Notification

5.7   *Event Log*

Clicking on **Event Log** within the Side Vertical Menu will present three tabs: **Event**, **SNMP trap**, and **Syslog**.

5.7.1   *Event Tab*

The **Event** tab displays history events and can be sorted by **Time** or **SOURCE IP** address. Events can be cleared by clicking on the **CLEAR** button. Historic events are listed in a table which consists of the following columns: **Time**, **Source IP**, **Mode**, **MAC Address**, and **Message**. The **Time** column indicates the timestamp when the event occurred. **Source IP**, **Model**, and **MAC Address** list the IP address, model, and MAC address of the device respectively. **Message** displays whether the device is online or offline at time the event occurred.
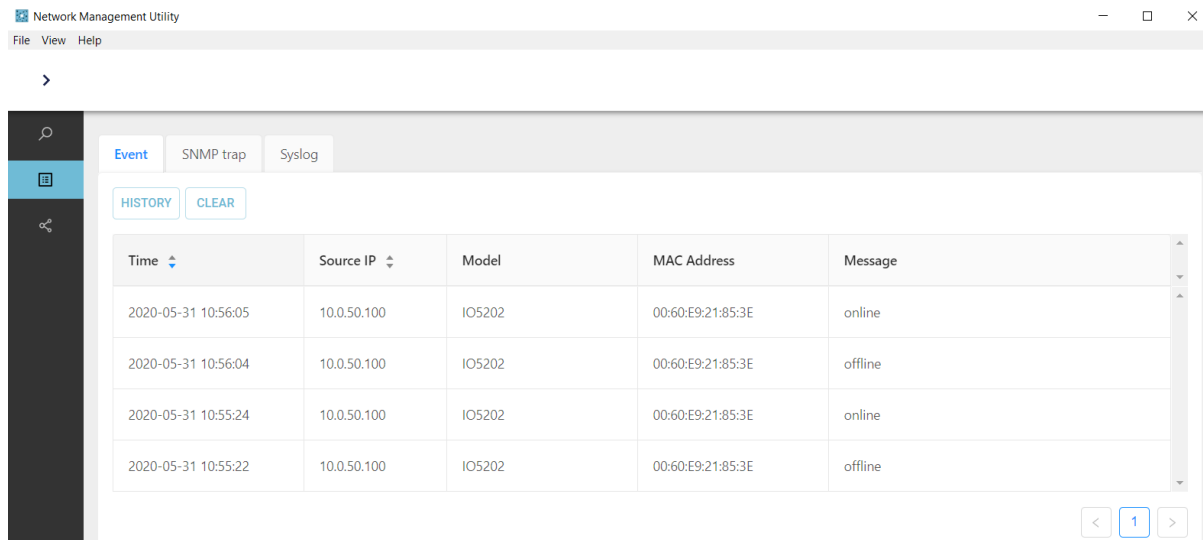
Figure 5.39 Historic Events in the Side Vertical Menu → Event Log → Event Tab

When the **HISTORY** button is clicked, a new window launches, as shown in below. Filter out unwanted events by entering a MAC Address and a Date/Time range of events to **view**. Make sure that the entered MAC address contains no spaces. Click the **REFRESH** button to see filtered events only.

Figure 5.40 Historic Events inside the Side Vertical Menu → Event Log → Event Tab → HISTORY Button

5.7.2 *SNMP Trap Tab*

Figure 5.41 shows the **SNMP Trap** tab. Click on the **HISTORY** button to see SNMP Trap history, and clear historic events by clicking on the **CLEAR** button.

Figure 5.41 Historic Events in the Side Vertical Menu → Event Log → SNMP Trap Tab

The SNMP Trap history is listed in a table which consists of the following columns: **Time, Source IP, Up Time, GT, ST, Version, Enterprise, Community, and Description.** The details of each field are described in Table 5.4 below.

Table 5.4 Description of Each Field in the Side Vertical Menu → Event Log → SNMP Tab

Field in SNMP Trap Tab	Description
Time	Timestamp when the SNMP Trap event occurred
Source IP	IP address of the device
Up time	The active time of the device
GT	The SNMP generic type
ST	The SNMP specified type
Version	The SNMP version used at the time of SNMP trap
Enterprise	The SNMP Enterprise OID
Community	The SNMP community
Description	The event description of SNMP packet

When the **HISTORY** button is clicked, a new window launches as shown in below. Filter out unwanted SNMP Trap events by entering a **SOURCE IP** Address and a Date/Time range of events to **view**. Make sure that the entered MAC address contains no spaces. Click the **REFRESH** button to see filtered events only.

(a)
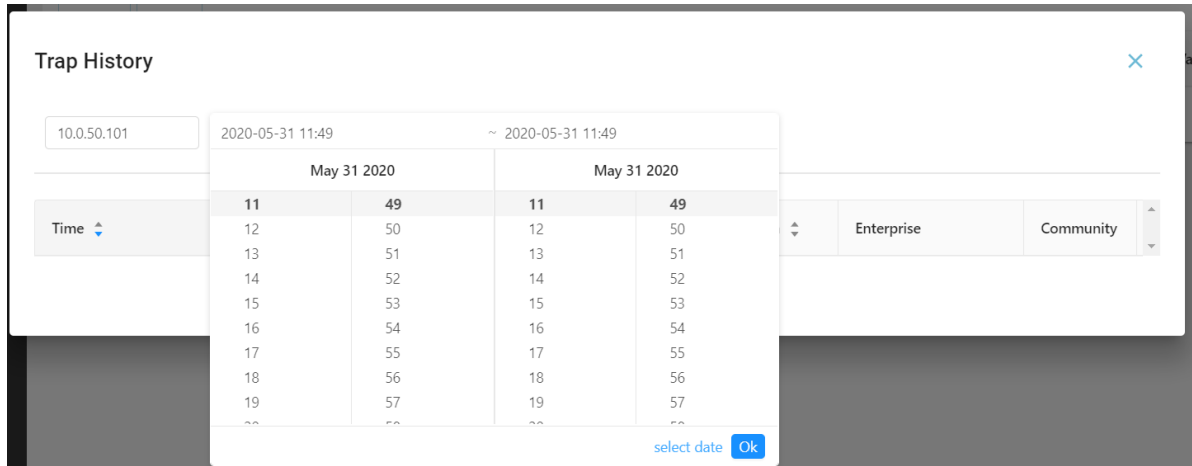
(b)

Figure 5.42 Date (a) and Time (b) Selection in the SNMP Trap Tab → HISTORY window

Figure 5.43 shows the **Syslog** tab. Click on the **HISTORY** button to see Syslog event history, and clear historic events by clicking on the **CLEAR** button.
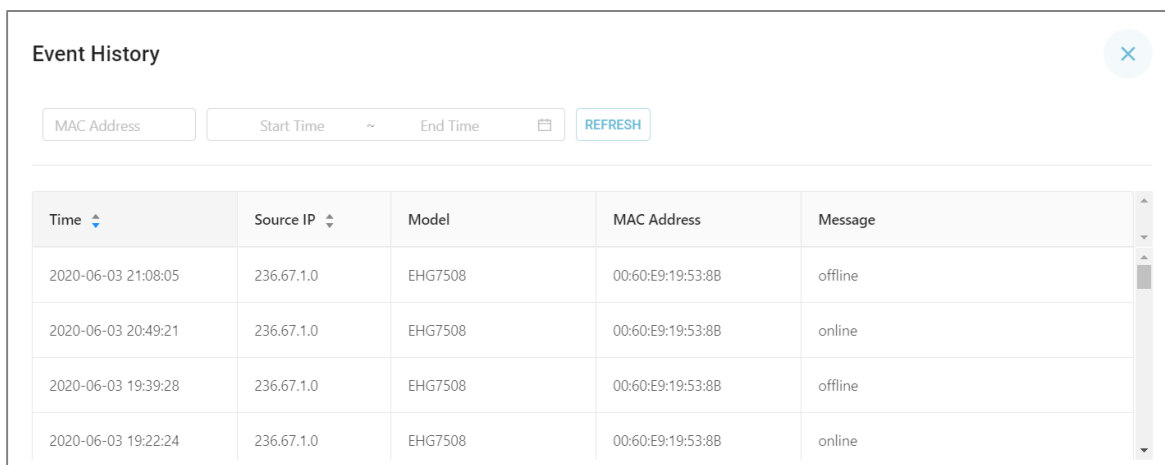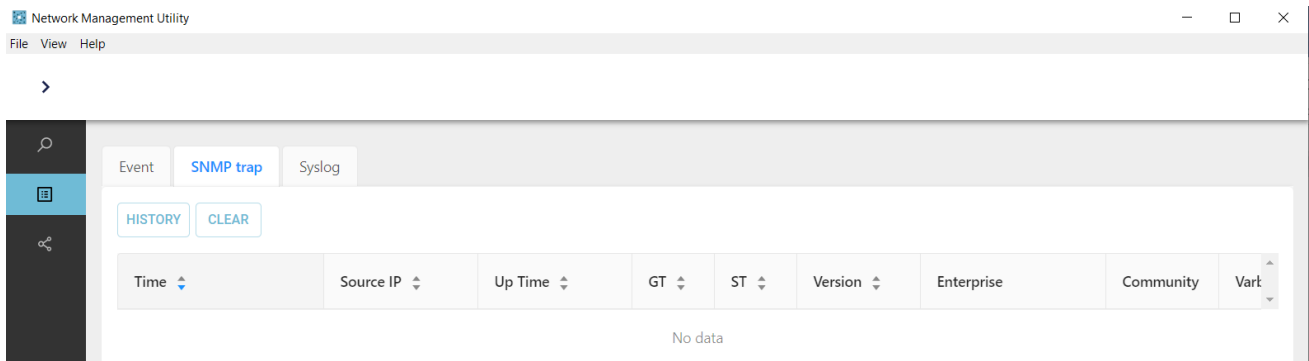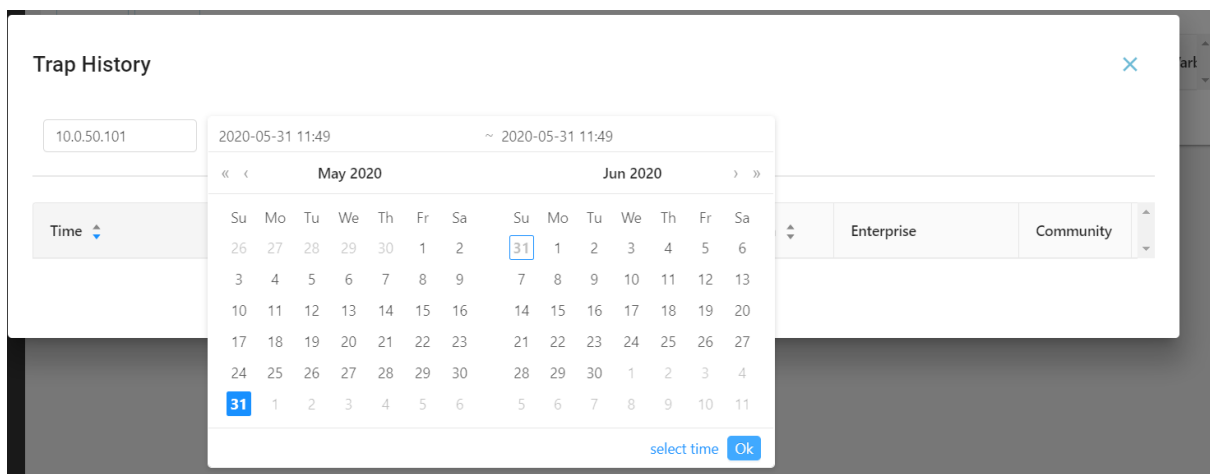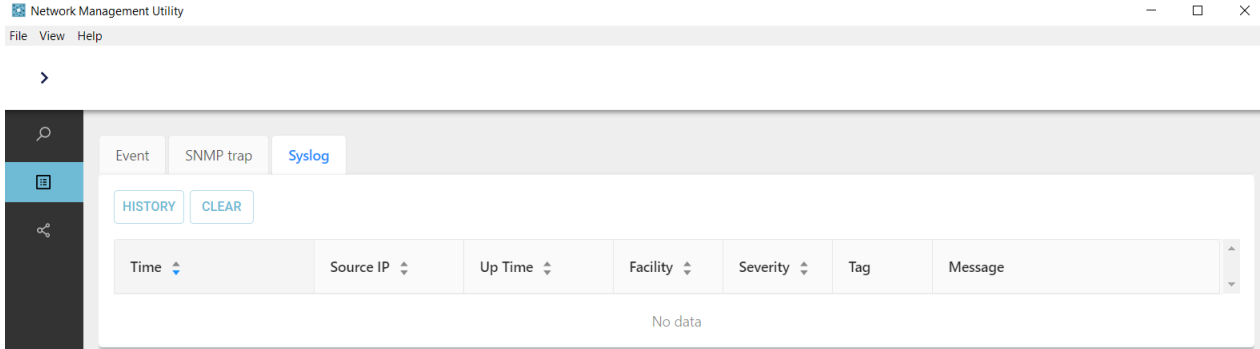

Figure 5.43 Historic Events inside the Side Vertical Menu → Event Log → Syslog Tab

The description of each field in the Syslog table is shown in Table 5.5 below.

Table 5.5 Description of Each Field in the Side Vertical Menu → Event Log → Syslog Tab

Field in Syslog Tab	Description
Time	Timestamp when the Syslog event occurred
Source IP	IP address of the device
Up time	The active time of the device
Facility	Type of process that created the syslog event, e.g., kernel, mail system, or security/authorization
Severity	Critical level of the information, e.g., emergency or alert
Tag	Name of the program or process that generated the message
Message	Details of the syslog information

When the **HISTORY** button is clicked, a new window launches as shown in below. Filter out unwanted Syslog events by entering a **SOURCE IP** Address and a Date/Time range of events to **view**. Make sure that the entered MAC address contains no spaces. Click the **REFRESH** button to see filtered events only.

Figure 5.44 Historic Events in the Side Vertical Menu → Event Log → Syslog Tab → HISTORY Button

5.8   *Topology*

There are two parts within the Vertical Menu → Topology section: 1) Drawing Space, and 2) Top bar.

5.8.1 *Drawing Space*

Click on the icon of a device (e.g., EHG7608 in this picture) to display the device properties, as shown in below. If the device icon is in grey colour and displays a cross mark ⊗, the device is not yet available for accessing and settings reconfiguration. Check the Device List to see if the device's SNMP is enabled (refer to Section 4.1.5 if not). If the problem persists, enable the SNMP function for the device via web interface instead. Follow the instructions in Section 5.6.1 to initialize a web configuration page. Note that when SNMP is enabled, the device type changes from Basic to Basic/SNMP.
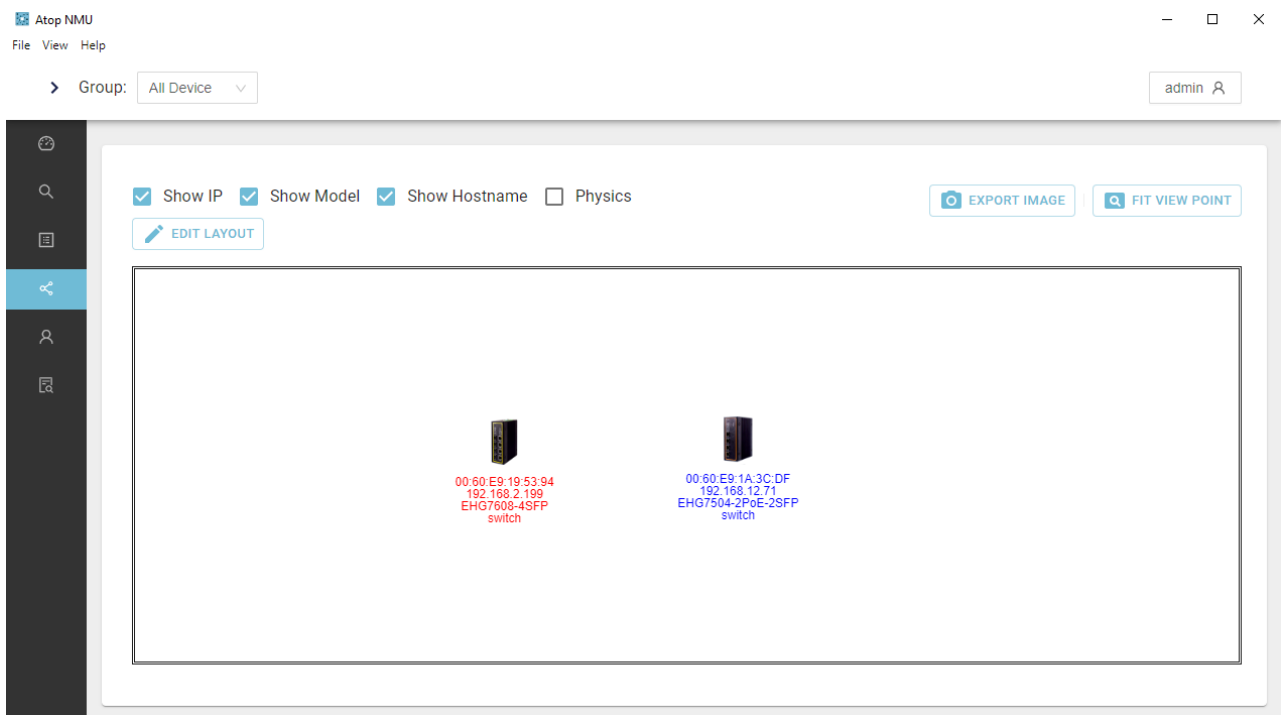
Figure 5.45 Side Vertical Menus → Topology (SNMP Disabled)

After SNMP is enabled, the device's icon becomes green-blue in colour and the text underneath becomes blue, as shown in below. Check the boxes for **Show IP**, **Show Model**, and **Show Hostname** to display text information on IP address, device model name and device hostname respectively, underneath the device's icon. Clicking the Edit Layout button will call up a new set of buttons: Add Node, Add Link, Save, and Cancel, as shown in Figure 5.46.
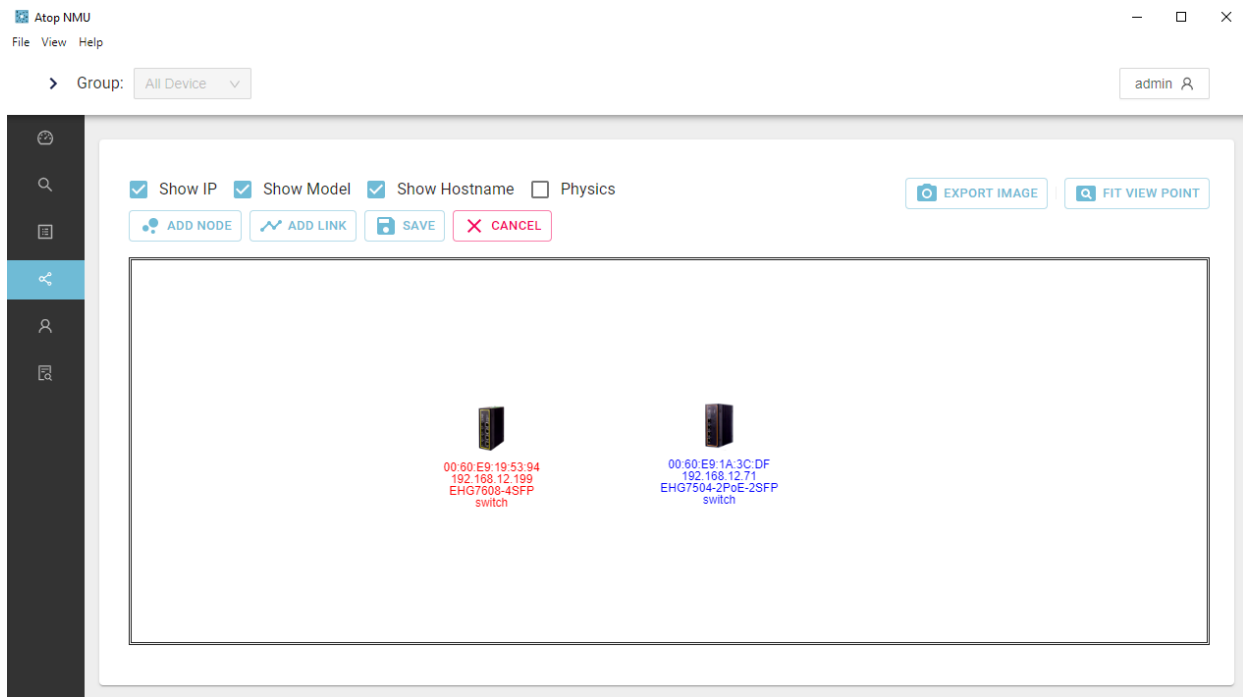
Figure 5.47 Working Space for Drawing a Topology: Side Menus → Topology (SNMP Enabled)

When the ADD NODE or ADD LINK button is clicked, a new small window is launched, as shown in below. To add a new node, click anywhere on the working space, and enter the MAC address for the new node or check the Virtual Node box. To add a link, click on the two nodes that the new link will connect. Click OK to implement new node or new link addition.

(a)   (b)
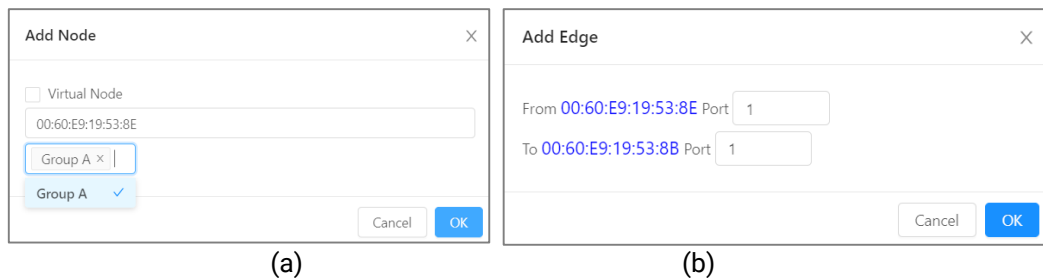
Figure 5.48 Drawing a Topology in the Side Menu → Topology section: (a) ADD NODE and (b) ADD LINK

The color coding used in the drawing is:
- Blue: User defined, matched with actual topology.
- Black: Real edge and user without defined.
- Dotted Line: User defined but does not exist.
- Red-X: Device offline.

Checking the Physics option to illustrate moving simulation so that user can see nodes and edges more clearly. This is shown in below.
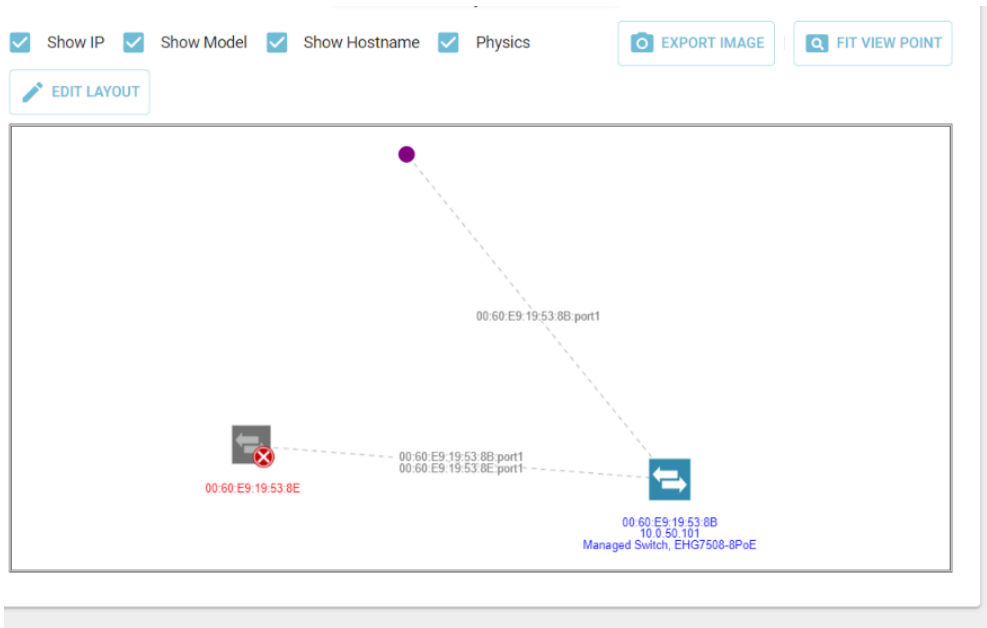
Figure 5.49 Topology Drawing Example

When any node or link on the topology's working space is clicked, a DELETE button will appear, as show in below. Click on the button to delete the node or link. Click on the CANCEL button to return to the EDIT LAYOUT Button.
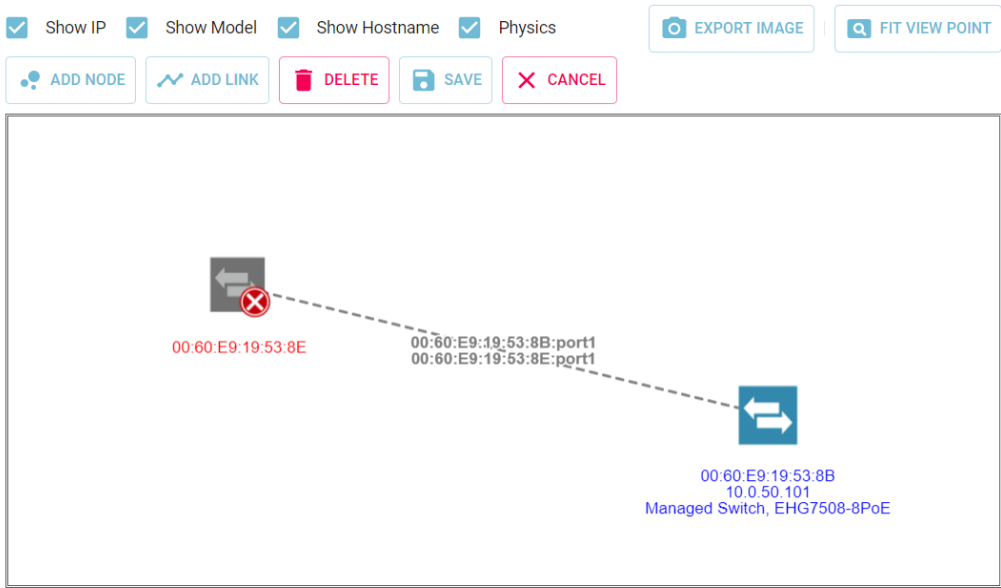
Figure 5.50 DELETE Button insider the Side Vertical Menu → Topology

If a new device is added in any group using a MAC address, its details are shown in the table inside the Device List. However, if a newly added device is a virtual node, nothing will be added in the Device List. In the below example, the new device is added using a MAC address in the drawing topology in Group A. Thus, the new device can be seen in Group A in the Device List, as shown in Figure 5.51 below.
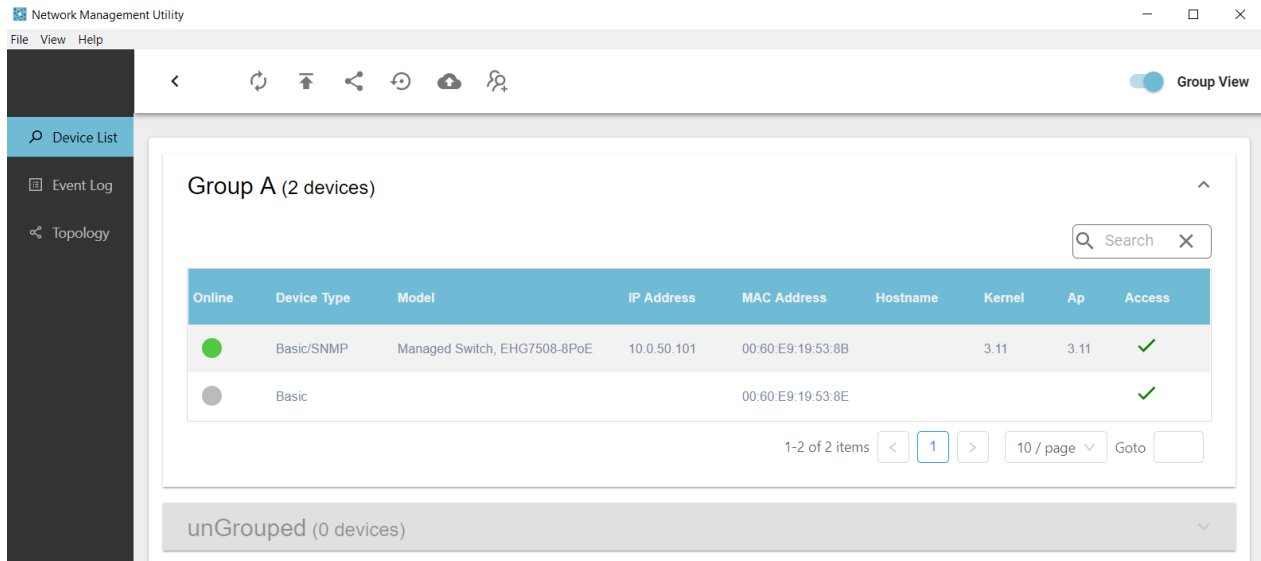
Figure 5.51 Device List After Adding a New Device using a MAC Address in Topology

When leaving the page after adding nodes and/or links, click on the Save button to save the changes. The drawing topology will disappear if left without first saving. If topology is successfully saved, a notification will appear on the top right corner, as shown in Figure 5.52.
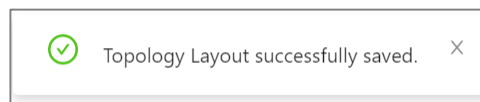
Figure 5.52 Notification of Successfully Saving Topology Layout

You can also click on the EXPORT IMAGE button to save the topology. Select the destination folder to save the image file, as shown in Figure 5.53.
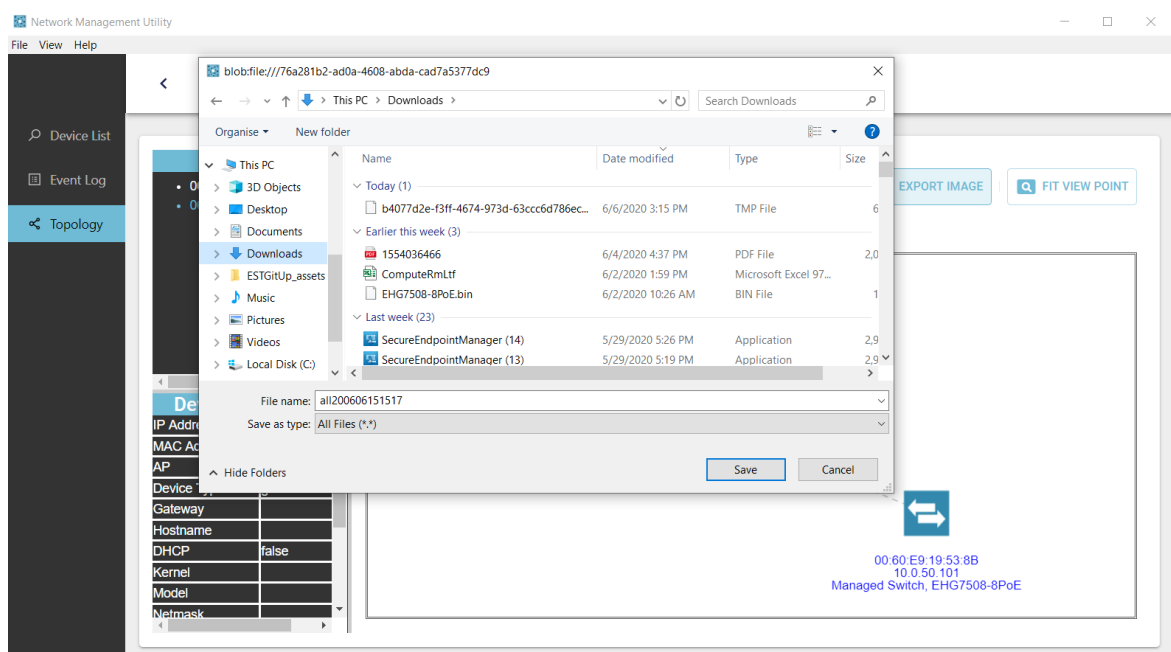
Figure 5.53 Export Image function in the Side Vertical Menu → Topology

The exported image file format is .svg, and can be viewed on an web browser.

5.8.1　*Top Bar*

Menu items in the **Top Bar** of the Topology icon in the **Side Vertical Menu** consists of the following:
- All Devices
- Group x
- …

Click on a group to create the topology and save it for each group, as shown in Figure 5.54.
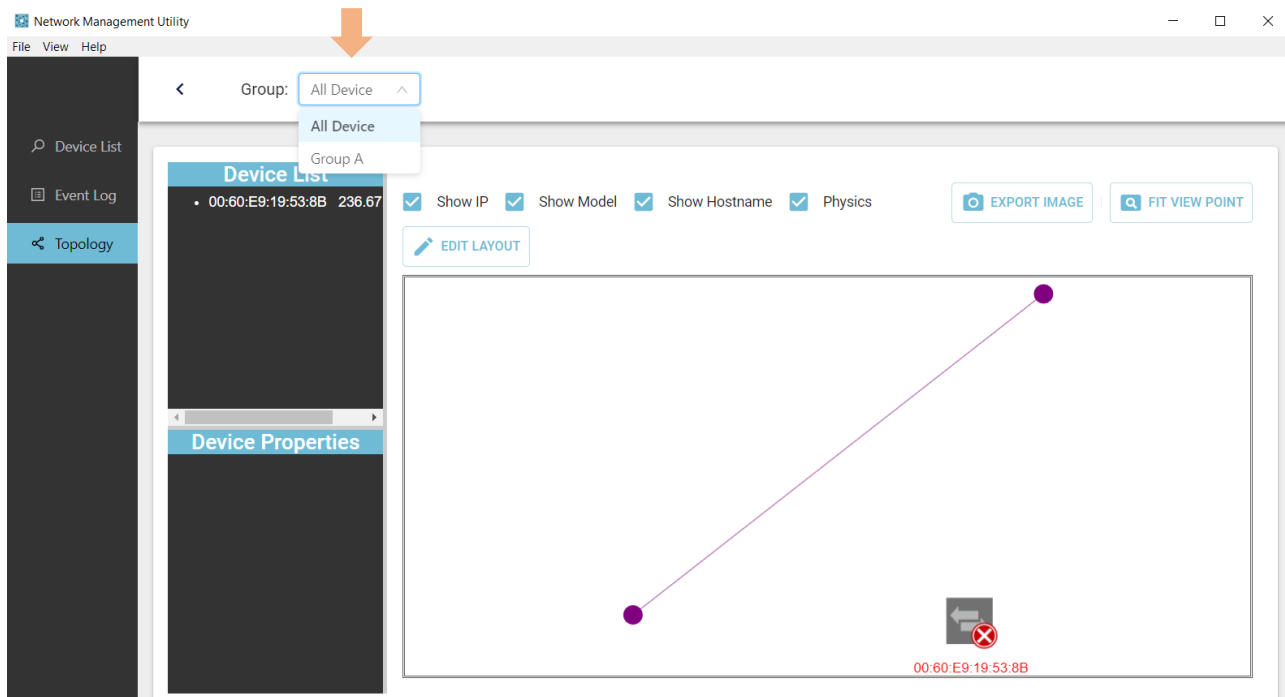
Figure 5.54 Group Selection Menu in the Side Vertical Menu → Topology

5.9   *Account Management*

Create new accounts in the Users section with the appropriate username and password, and select the suitable user role for the account.
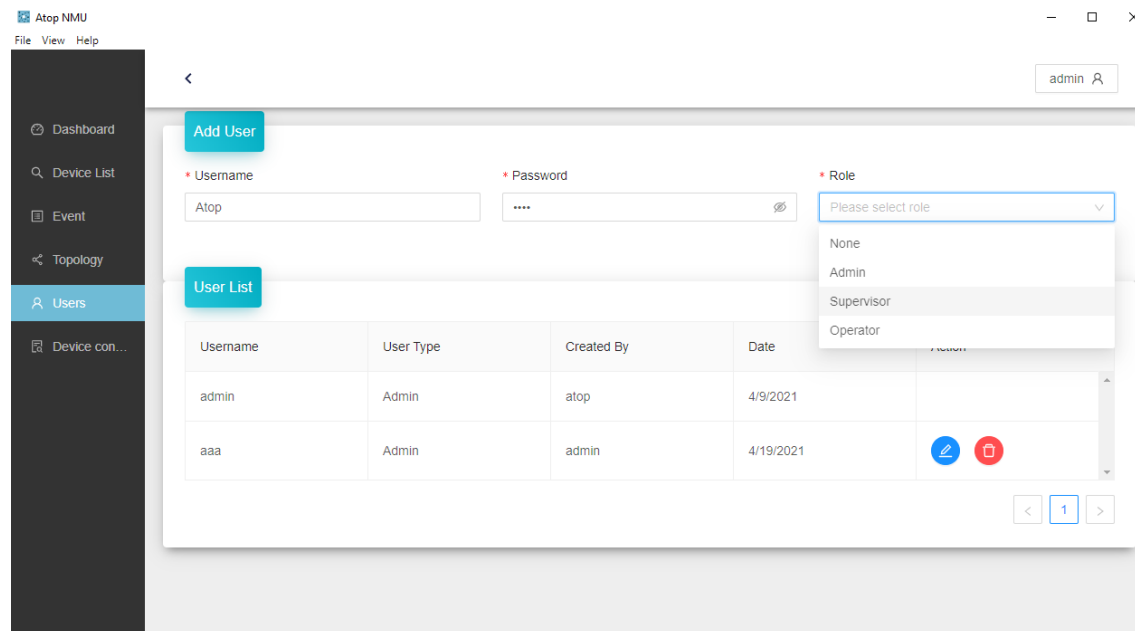
Figure 5.55 Creating New Account

Table 5.6 Permissions of Different Roles

No.	Function	Role		
		Admin	**Supervisor**	**Operator**
1	Add users	W/R	W/R	R
2	Edit and delete users	W/R	R	R
3	Firmware update	W/R	W/R	R
4	Network configuration	W/R	W/R	R
5	Reset to default	W/R	W/R	R
6	Backup and restore	W/R	W/R	R
7	Schedule backup	W/R	W/R	R
8	Syslog server configuration	W/R	W/R	R
9	Trap server configuration	W/R	W/R	R
10	Add new groups	W/R	W/R	R
11	Edit topology layout	W/R	W/R	R
	**W/R - Write and read permission **R - Read permission only			

Edit existing accounts: Click the Edit/Delete icons to modify existing accounts as below.

Figure 5.56 Editing Existing Accounts

5.10   *Device Config Comparison*

Files exported via Backup and Restore (refer to chapter 5.6.8) can be compared for differences in the Device Config Comparison section.
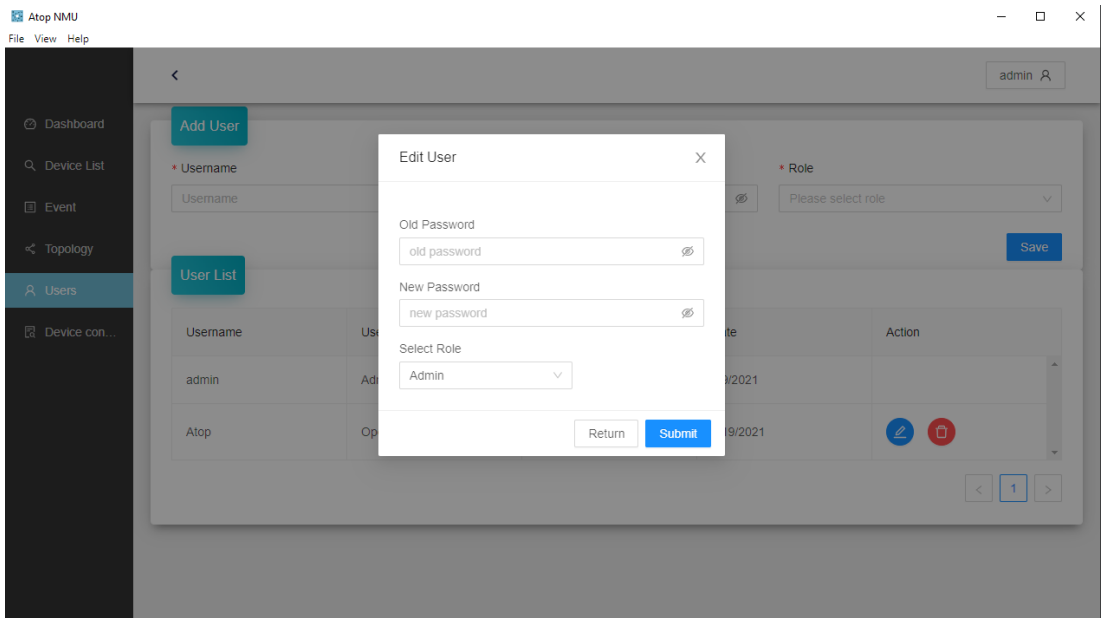
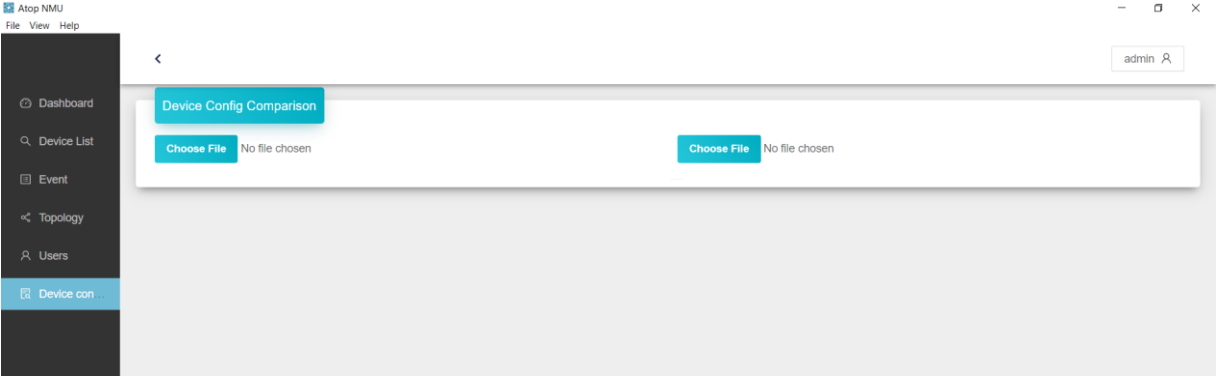Select.txt files produced through the backup process.

Figure 5.57 Device Config Comparison

NMU will highlight any differences between the two files as below.
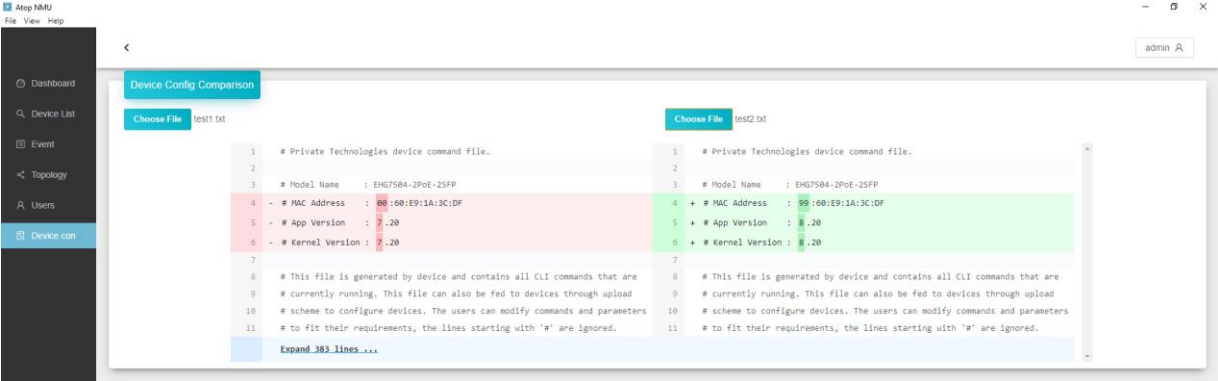
Figure 5.58 Configuration Comparison

6 Top Horizontal Icon Bar - Device List

Menu icons on the **Top Horizontal Icon Bar** consist of the following:

- ⟩ or ⟨ Icon
- Discovery
- Firmware Update
- Network Settings
- Reset to Default
- Backup and Restore
- Add new group
- Group View

6.1 > or < Icon

On the most left is an icon ⟩ . Clicking it will expand the area of the **Side Vertical Menu** and show the name of each icon, as shown in Figure 6.1 below. To shrink the area of the **Side Vertical Menu**, click the ⟨ icon as shown in Figure 6.2.
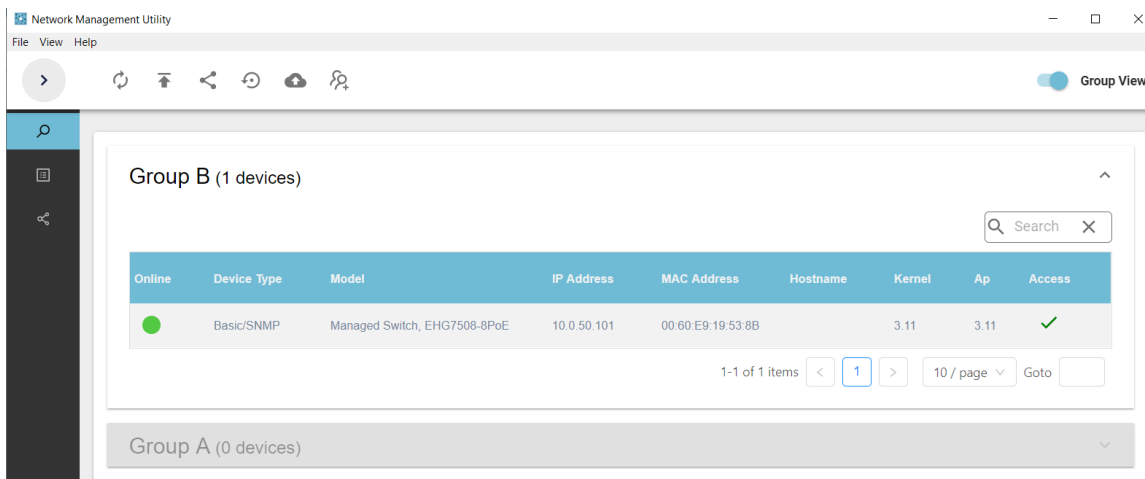
Figure 6.1 Click on > Icon to Expand the Area of the Side Vertical Menu
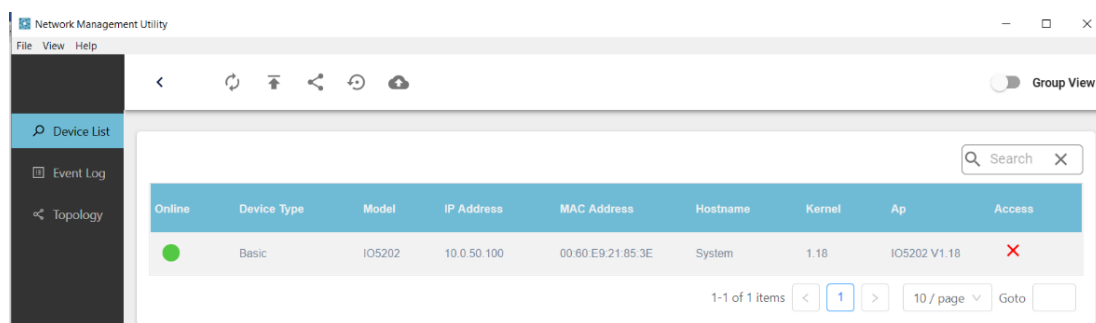
Figure 6.2 Click on < Icon to Shrink the Area of the Side Vertical Menu

6.2   *Discovery*

Before discovering any connected devices, the working space will be as shown in Figure 6.3 below.
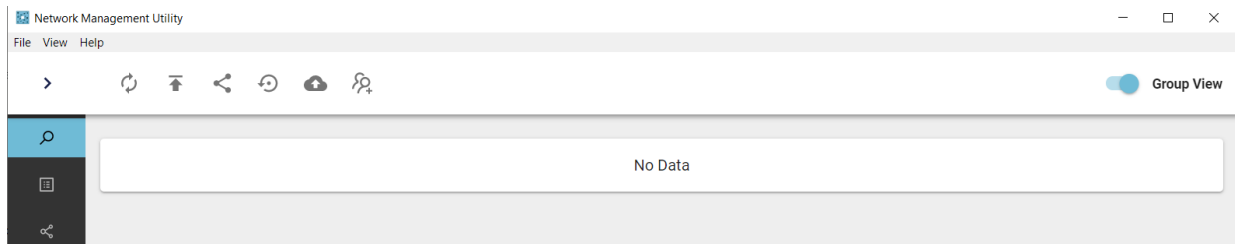
Figure 6.3 First-time Launch of Network Management Utility Setup 2.X

Once the discovery icon on the top icon bar is clicked, and if the SNMP function is on, a pop-up window will appear to notify that an SNMP Scan is in process, as shown in Figure 6.4.
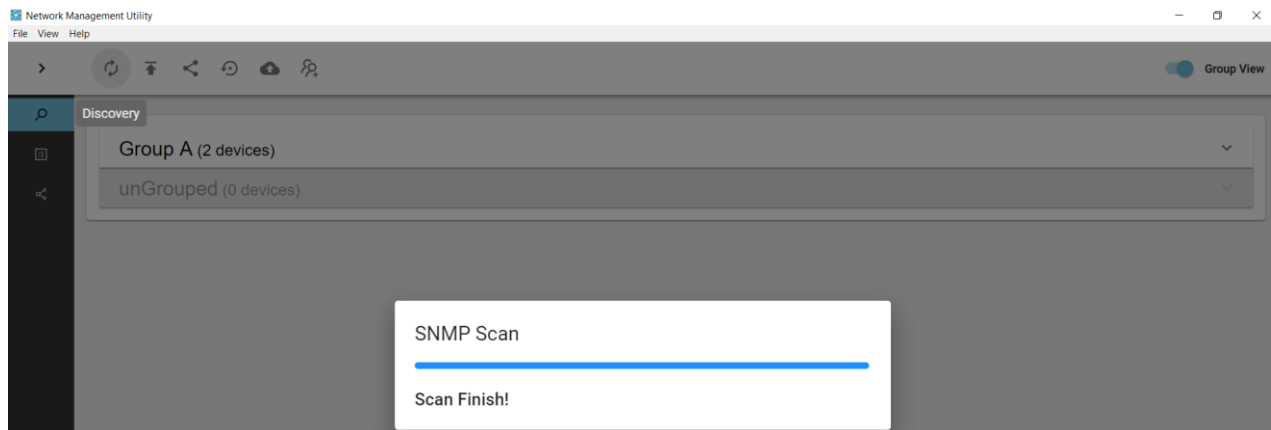
Figure 6.4 SNMP Scan

When the scan finishes, connected devices will be displayed in the Device List, as shown in Figure 6.5. If these devices are not yet grouped together, they will be in the ungrouped section. If the device already belongs to a group, it will be in the device table of that group. Refer to Section 5.3 on how to add a new group and how to add devices into a group. Note that one device can be added to more than one group.
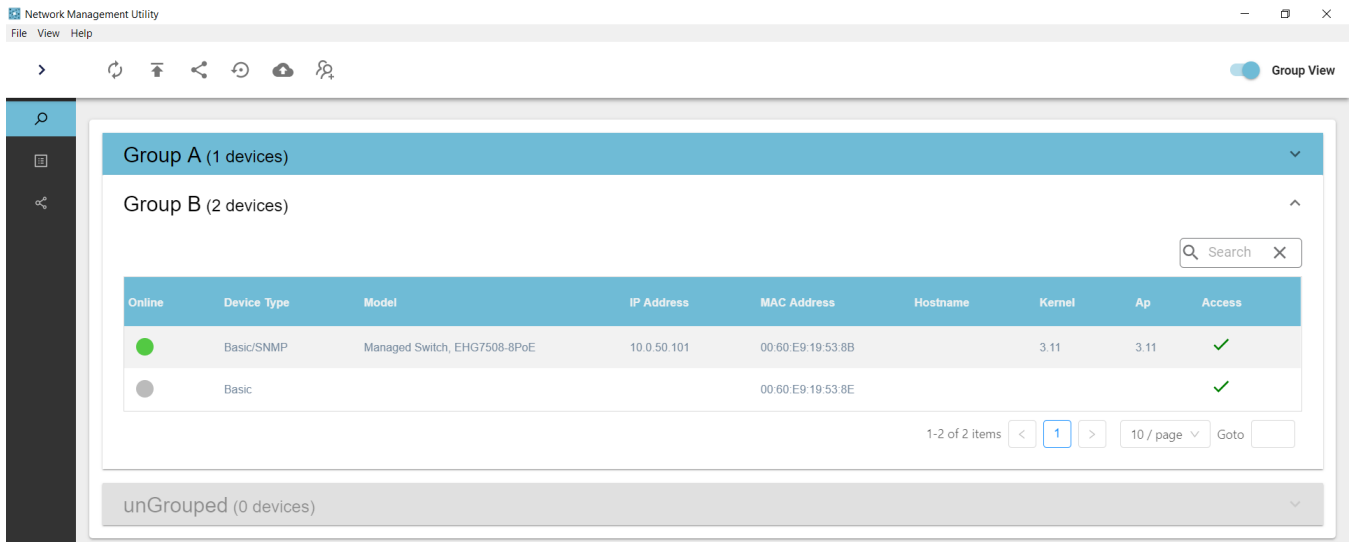
Figure 6.5 Devices in the Device Table in Each Group

Table 6.1 below explains each field in the device table in detail.

Table 6.1 Definition of Each Field in the Device Table

Field	Description
Online	Status of each device: active (green dot) or inactive (red dot)
Device Type	Basic or Advanced
Model number	The model number of the found device(s).
IP Address	The IP Address of the corresponding device
MAC Address	The MAC Address of the device.
Host Name	The Host Name of the device.
Kernel	The Kernel version of the device
AP Information	The AP information or application version of the device. Note that ATOP's device firmware generally consists of an application version and a kernel version.
Access	Indicates whether the device is already accessible (✓) or not (✗).An accessible device must belong in a group. That is, users have to create a group and add the device to that group first to view it as accessible.

6.3　　　*Firmware Update*

Clicking on the **Firmware Update** icon on the **Top Horizontal Icon Bar** will open a notification box on the top of the working space, as shown in Figure 6.6 below.
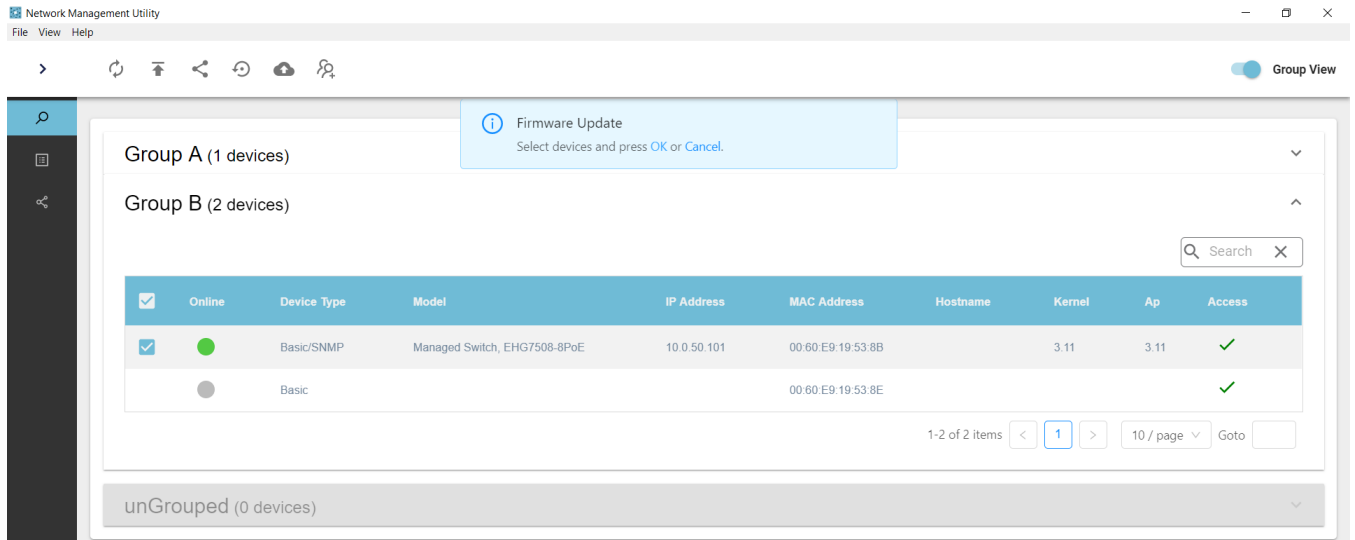
Figure 6.6 Firmware Update Notification Box

After selecting the device that you want to update firmware for and clicking **OK** in the notification box, a new window is launched as shown in Figure 6.7. Press the **BROWSE** button and go through your file directory to select the update firmware file (.dld).

Figure 6.7 Go Through the File Directory to Select Firmware File (.dld)

Click the **Open** button after selecting the correct firmware file. The **START** button at the bottom right corner of the Firmware Update window will then be activated. Click the **START** button to start updating.

Firmware update progress is displayed in the **Progress** field and the update status is shown in the **Status** field, as shown in Figure 6.8. To stop updating the firmware, press the red STOP button in the bottom right corner.
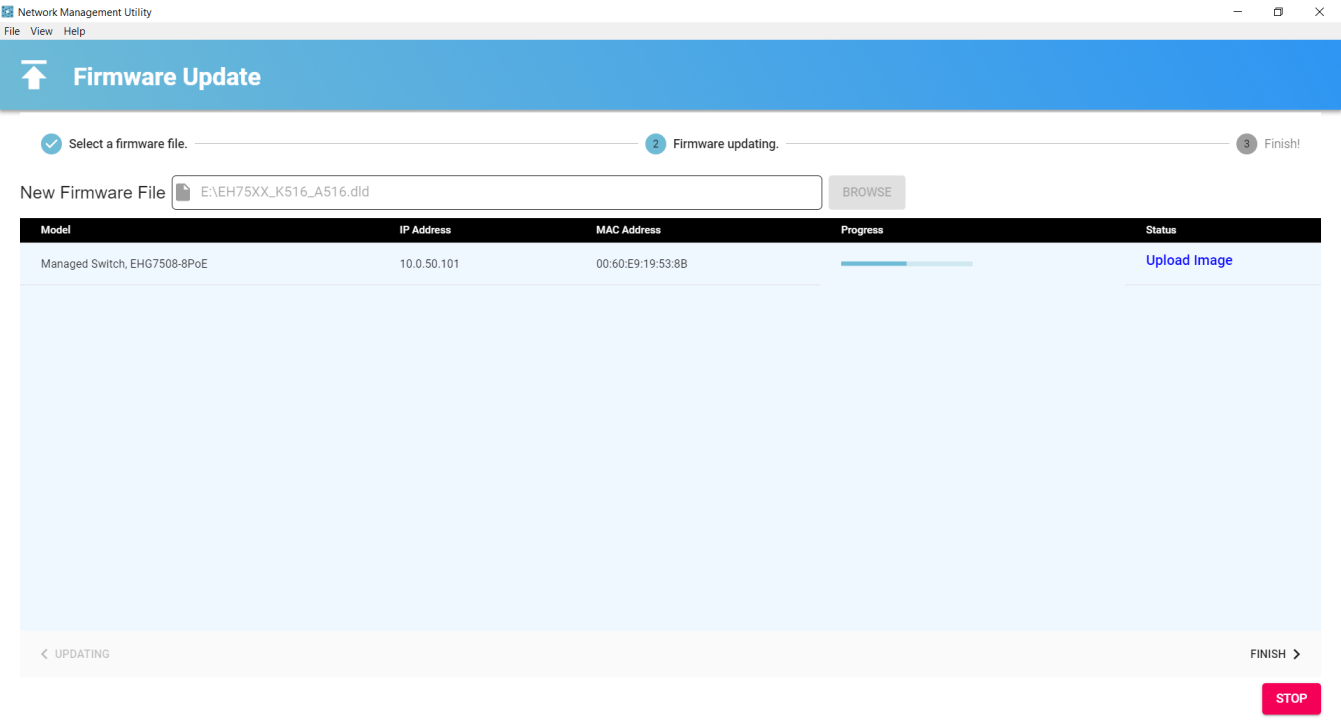
Figure 6.8 Firmware Updating View

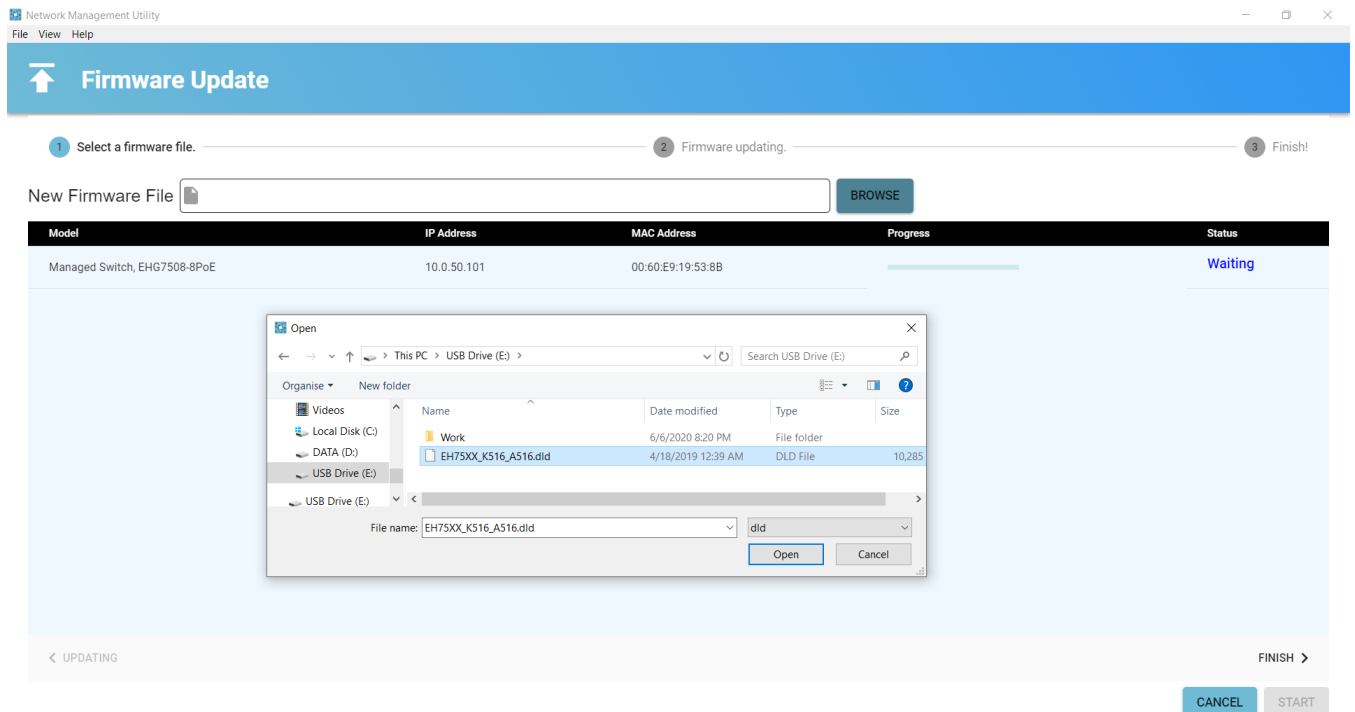Completion of the updating process is indicated by the moving progress line reaching its end point. The status will display either Upload Success or Upload Fail. Figure 6.9 illustrates an example when the firmware updating process failed on completion. The error code is E007.

Figure 6.9 Failed Firmware Update (Code E007)

Click the FINISH button to close the Firmware Update window and return to the Device List's working space.

6.4   *Network Settings*

Clicking the **Network Settings** icon on the **Top Horizontal Icon Bar** of the **Device List** launches a new window, as shown in Figure 6.10. The left side of the window is the Network Settings section, where users can choose whether to obtain a device's IP address automatically or manually. Checking the box for DHCP (Obtain IP automatically) will allow the device to set its IP address an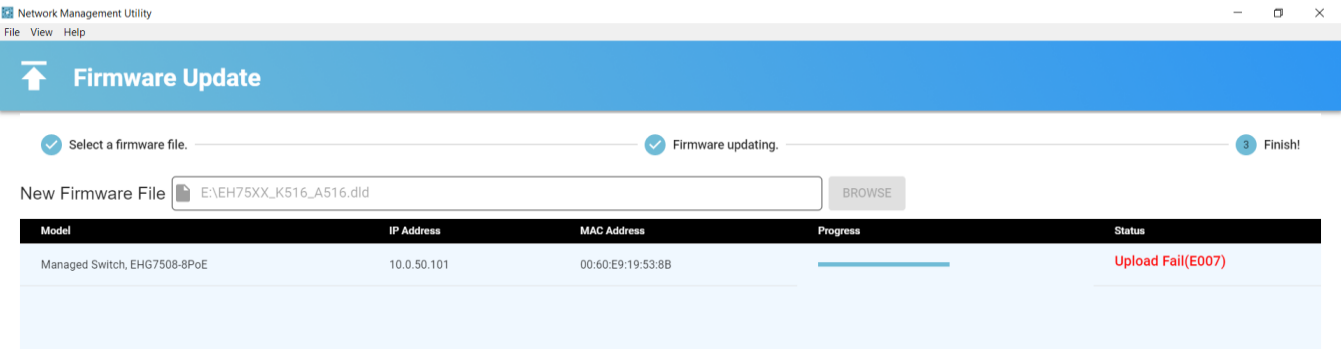d other parameters automatically. If the DHCP option is checked, ignore the IP Assign section on the right side of the window; the START button on the bottom right will be activated for use. Before clicking the START button, Progress will display as 0%.

Figure 6.10 Network Settings Window – Automatic Setting

If the DHCP option is unchecked, the network parameters must be manually entered. Figure 6.11 shows the Network Settings window when the DHCP option is unchecked.

Fill in the Netmask, Gateway, Hostname, Preferred DNS server, and Alternate DNS server fields. The IP address on the right side (IP Assign) also requires input, as shown in Figure 6.11. Press the CALCULATE button next to the IP address input box named "Start Address" to check if the input IP address is valid. If yes, the START button at the bottom right corner will be activated. Once the START button is clicked, device information will display, including Model, MAC Address, IP Address, and Progress. If the configuration is successful, the Progress field will show a green check sign.

Figure 6.11 Network Settings Window – Manual Setting

6.5   *Reset to Default*

In order to reset device configuration to the default values, 1) enable SNMP function for the connected device, 2) create a group if none are available or if a new group is required for the connected device, 3) add the device into the newly created group (refer to Section 5.3). If the SNMP function is not enabled yet, refer to Section 4.1.4. to enable it. If the message "(This feature only for device with SNMP support.)" persists and the **OK** link cannot be clicked even when SNMP function is already enabled via the **Network Management Utility Setup 2.X,** try enabling the SNMP function via our web interface instead. Follow the instructions in Section 5.6.1 to initialize the web configuration page.

After enabling the SNMP function, select connected devices that you want to reset configuration settings to factory default for, and then press **"OK"**, as shown in Figure 6.12 below.
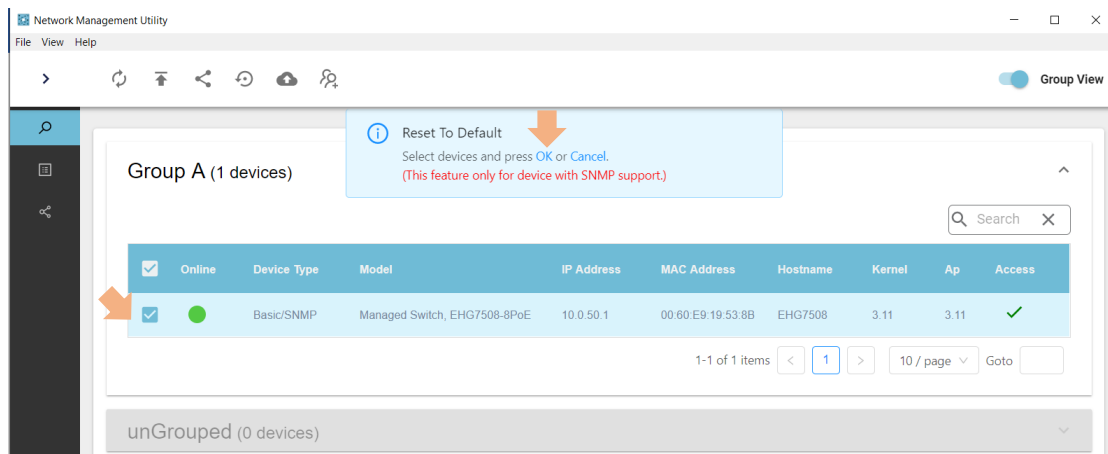

Figure 6.12 Select Devices and Click OK to Reset to Default

A new window displaying device details (i.e., Model, MAC address, IP address, and status) will appear , as shown in Figure 6.13. Before starting, the STATUS will be WAITING. If confirmed that the selected device is the correct one, click the START button to start the reset process.
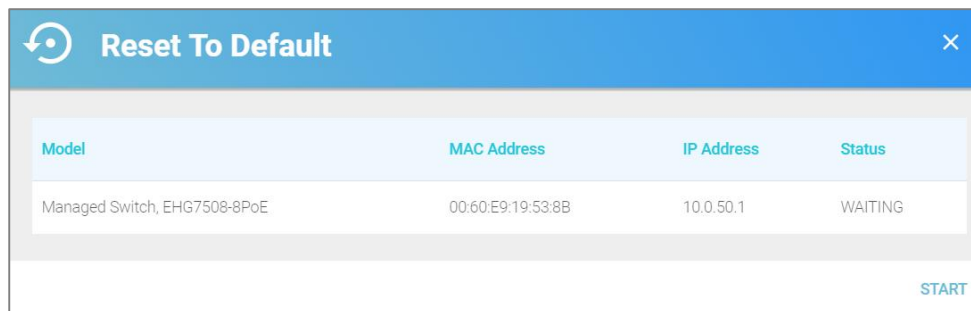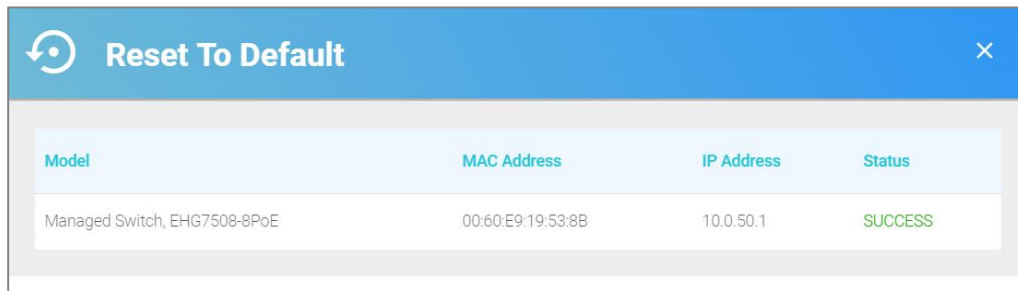

Figure 6.13 Confirm Window to Reset to Default Setting

When the "reset to default" process is finished, the STATUS will change to SUCCESS, as shown in Figure 6.14. Click [×] in the top right corner to close the window.

Figure 6.14 Successful Reset to Default Setting

6.6   *Backup and Restore*

Similar to the **Reset to Default** function icon, before backing up or restoring configurations, 1) enable SNMP function for the connected device, 2) create a group if none are available or if a new group is required for the connected device, 3) add the device into the newly created group (refer to Section 5.3). If the SNMP function is not enabled yet, refer to Section 4.1.4. to enable it. If the message "(This feature only for device with SNMP support.)" persists and the **OK** link cannot be clicked even when SNMP function is already enabled via the **Network Management Utility Setup 2.X,** try enabling the SNMP function via our web interface instead. Follow the instructions in Section 5.6.1 to initialize the web configuration page.

After enabling the SNMP function, select connected devices that you want to Backup and Restore the configuration for, and then press **"OK",** as shown in Figure 6.15.
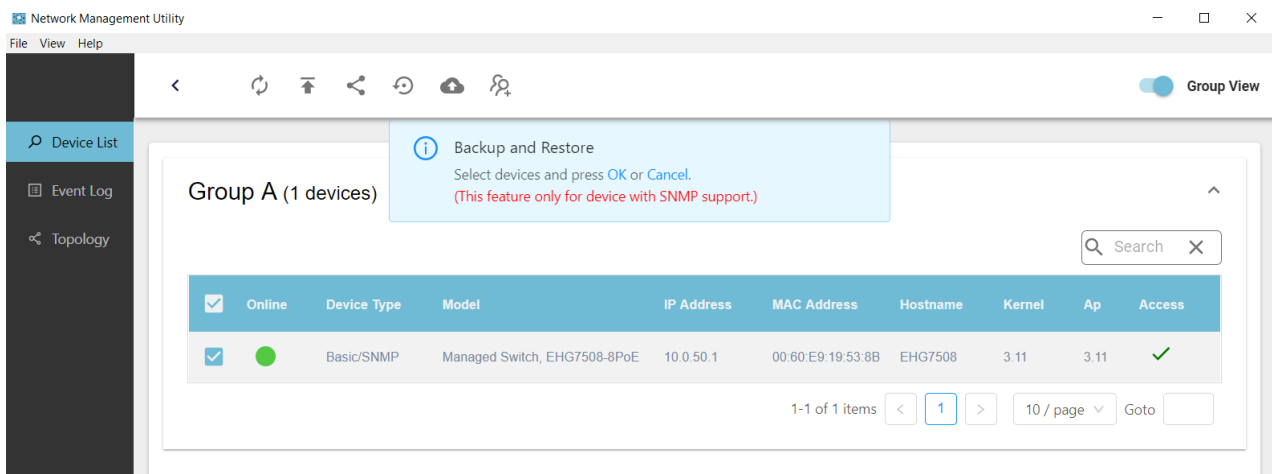

Figure 6.15 Clicking on the Backup and Restore icon in the Top Horizontal Icon Bar

Once the **OK** button is clicked, a new **Backup and Restore** window will launch, as shown in Figure 6.16. Here, the window is divided to two parts, **Devices** and **Files**.
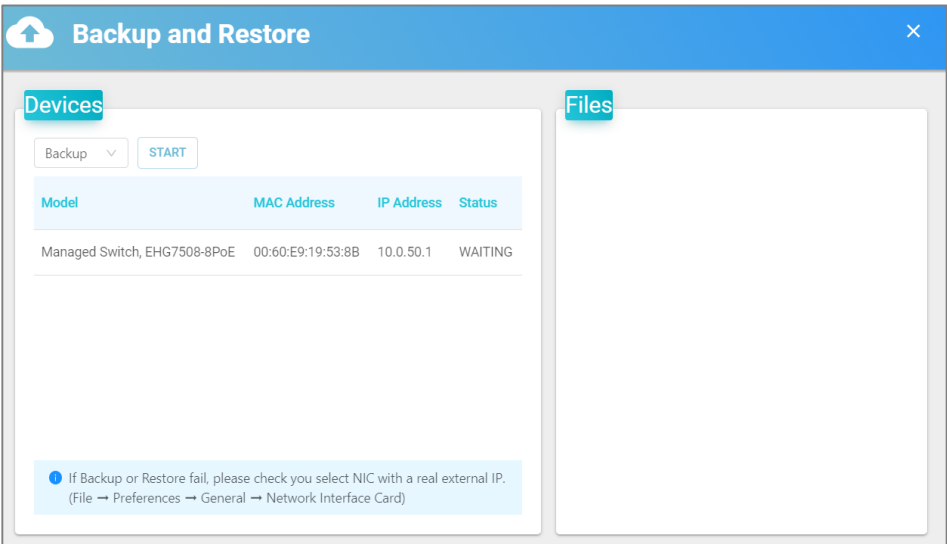
Figure 6.16 Backup and Restore Window

The **Devices** part displays device information such as Model, MAC Address, IP Address, and Status. Before clicking START button, the **Status** is WAITING. To back-up a configuration, select **Backup** from the drop-down box and click the START button. Figure 6.17 shows the **Backup and Restore** window after successfully finishing the Backup process. The device will restart and a notification window will appear on the bottom right corner for the device going offline and online again, respectively. If backup fails, go to File → Preferences → General → Network Interface Card to check if your selected Network Interface Card (NIC) is the one with a real external IP address.. Figure 6.18 illustrates the screen when Backup fails.
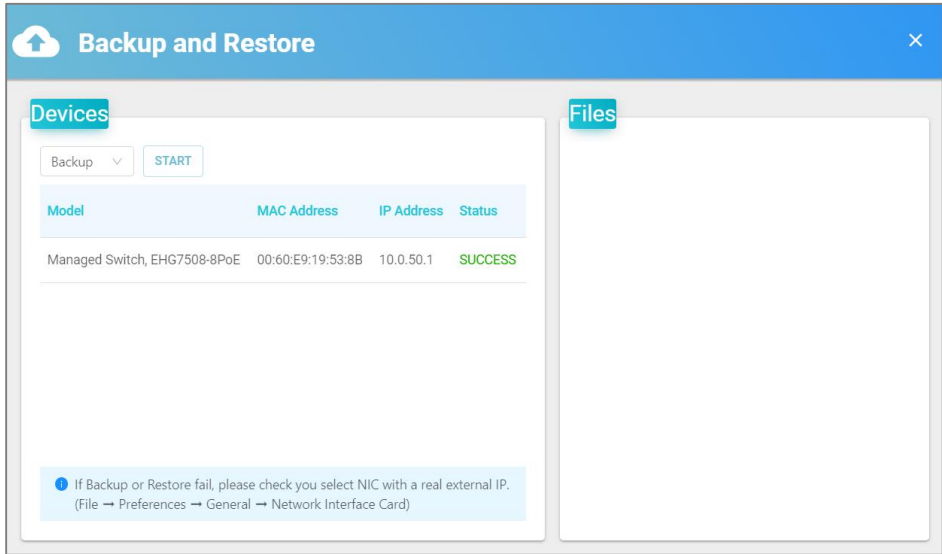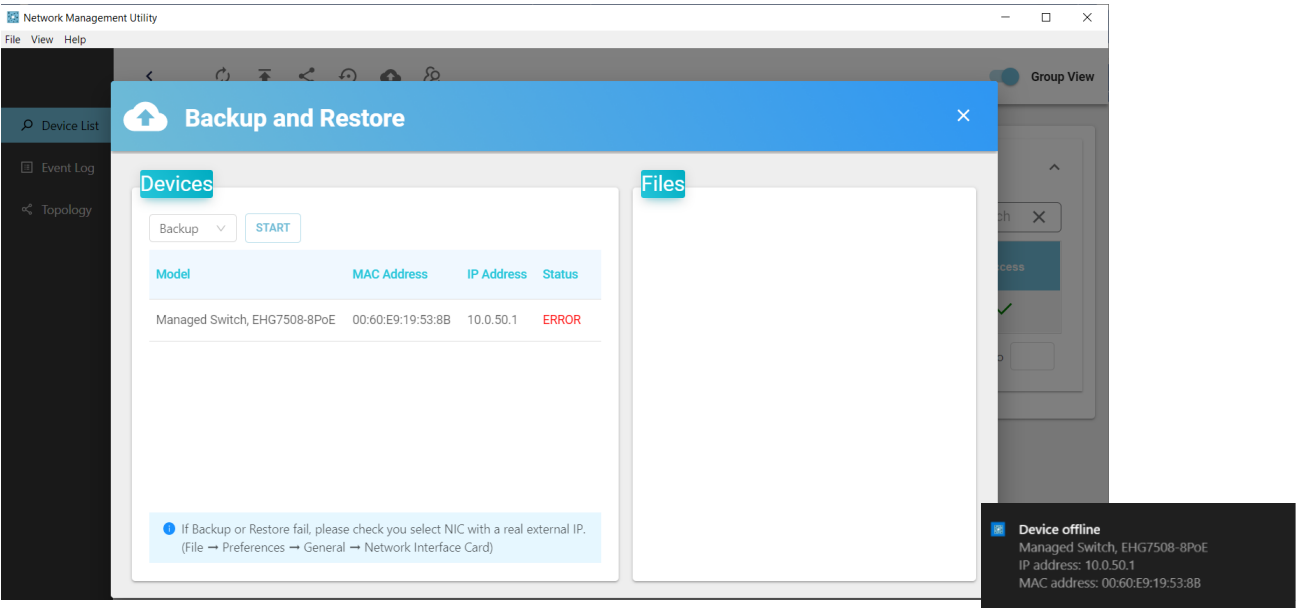

Figure 6.17 Backup Success

Figure 6.18 Backup Fail

Click on a device row in the left side of the Backup and Restore window to see the list of already backed up configuration files in the right side section, as shown in Figure 6.19. Click the red × at the end of each row to remove that backup configuration.
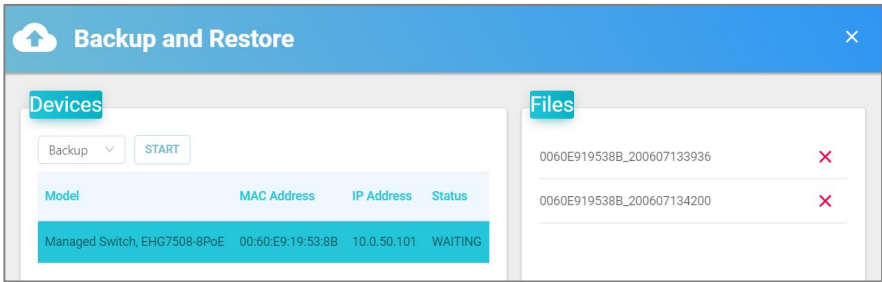

Figure 6.19 Configuration Files that are Already Backed Up

To restore a configuration, first, select the **Restore** option from the drop-down menu. Second, click on the row of the device to restore configurations for, and its list of configuration files will display on the right side of the window. Third, select the configuration file to restore. The Backup **Status** is will now be WAITING. Last, click the **START** button. Figure 6.20 shows the **Backup and Restore** window after successfully finishing the Restore process. A couple of beeps will sound from the device and the device will restarted. The user will see a notification box appear on the bottom right of the window showing that the device is going offline and online again. Same as for the Backup configuration process, if Restoration fails, check that your selected Network Interface Card (NIC) is the one with a real external IP address.
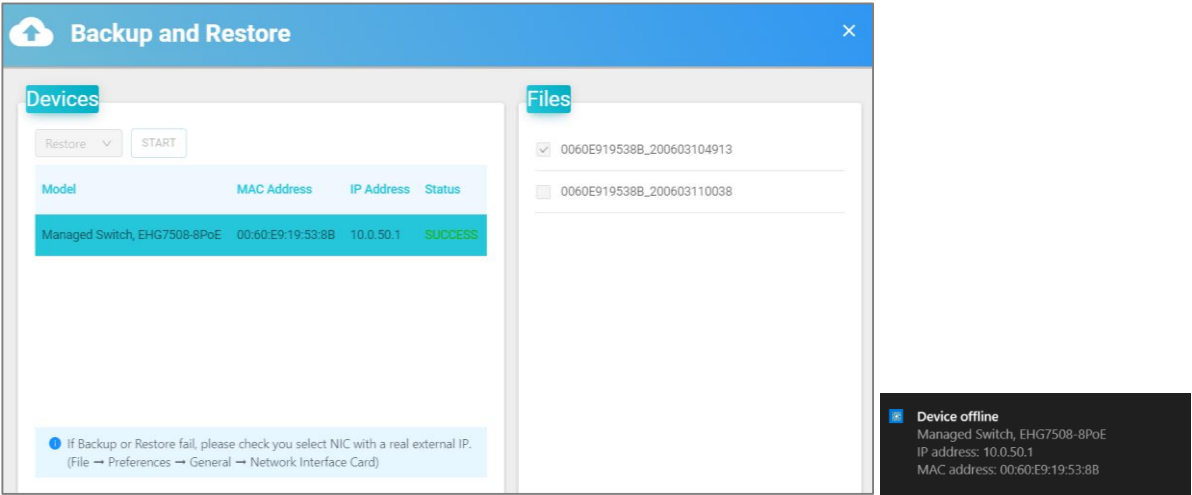
Figure 6.20 Sucessful Configuration File Restoration

ATOP Technologies, Inc.

www.**atoponline**.com

TAIWAN HEADQUARTERS and INTERNATIONAL SALES:

2F, No. 146, Sec. 1, Dongxing Rd.,
30261 Zhubei City, Hsinchu County
Taiwan, R.O.C.
Tel: +886-3-550-8137
Fax: +886-3-550-8131
sales@atop.com.tw

ATOP CHINA BRANCH:

3F, 75th, No. 1066 Building,
Qingzhou North Road,
Shanghai, China
Tel: +86-21-64956231