Open-Vision Pro

Management Utility

User's Manual

Version 1.1

Sep, 2025

ORing Industrial Networking Corp.

3F.,NO.542-2, Jhong-Jheng Rd.Sindian

District, New Taipei City 23148 Taiwan,

R.O.C.

Tel: + 886 2 2218 1066

Fax: + 886 2 2218 1014

Website: www.oringnet.com

E-mail: support@oringnet.com

Table of Content

About Open Vision Pro

1.1 About the Open-Vision Pro

A Powerful management utilities are important for administrators to monitor and manage all devices on the local network. ORing is proud to launch Open-Vision pro, a powerful network management utility suite. Open-Vision pro provides a new operating interface and introduces a WEB-style management interface. You no longer need to install complex The suite can be used normally as long as there is a WEB Browser. Moreover, it further integrates the Cyber SIEM security detection function, allowing users to master security information to ensure the stability and reliability of the local network.

1.2 System environment

Minimum System Requirements

- Intel Core i5 (or above)
- VGA Monitor with 1024 x 768 resolution
- 4 GB RAM (recommended 8GB and above)
- Microsoft Edeg / Google Ghrome (64bit)

Supported Network Protocols

- SNMP v1/2
- SNMP v3
- LLDP
- ICMP ping

Operating System

- Windows 10
- Windows 11

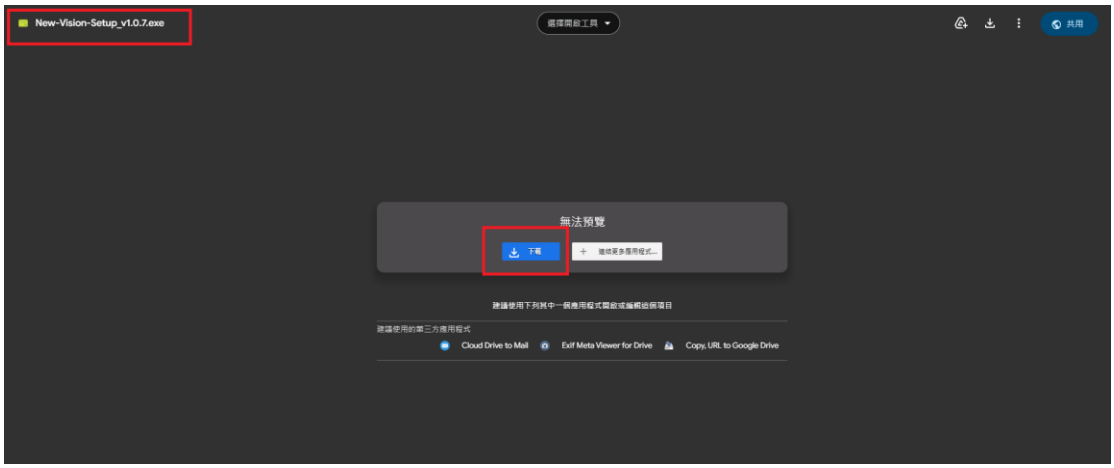
1.3 Install Open-Vision

Please see the following instruction to install New Vison Pro

Step 1

Download the latest setup file from website

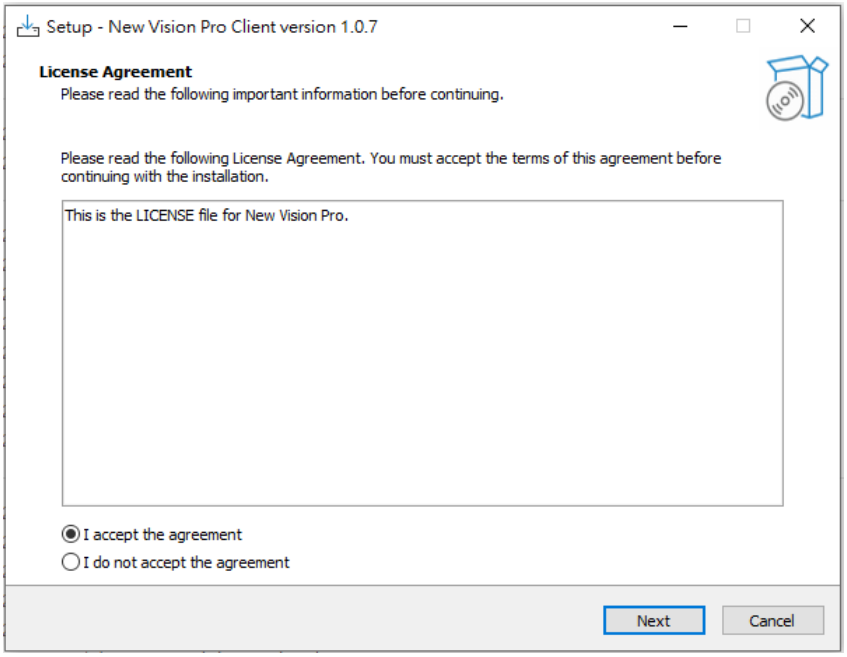
When the download is finished, open the folder where the file is located.



Step 2

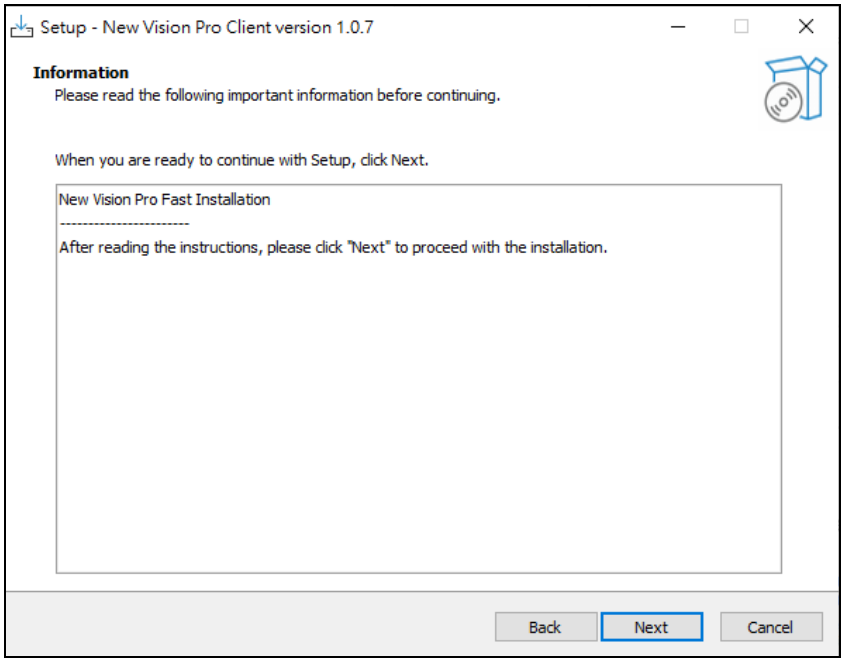
Execute the New-Vison-setup EXE file to start the installation.

Select **[I accept the agreement]** and click **[Next]** to continue.



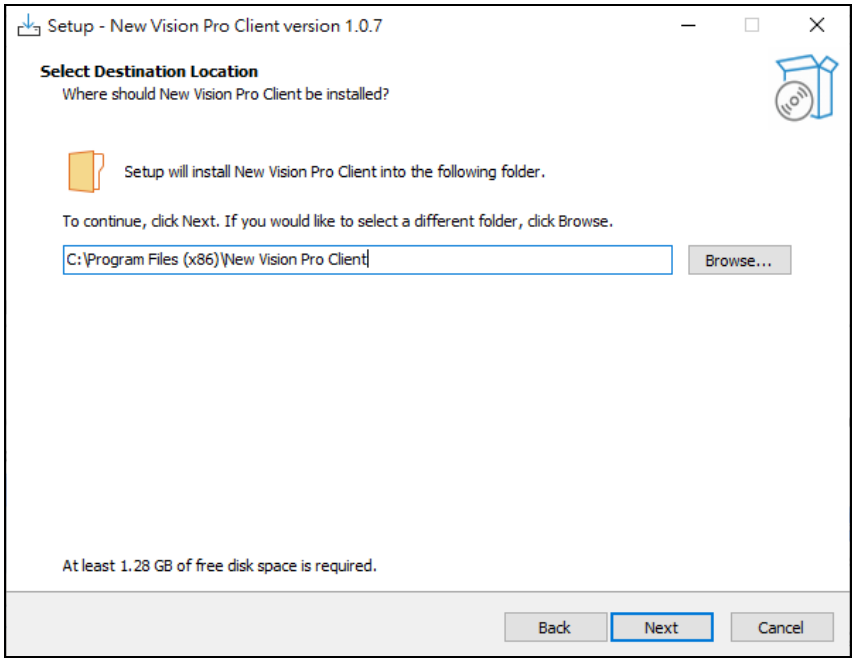
Step 3

Click **[Next]** to continue setup process.



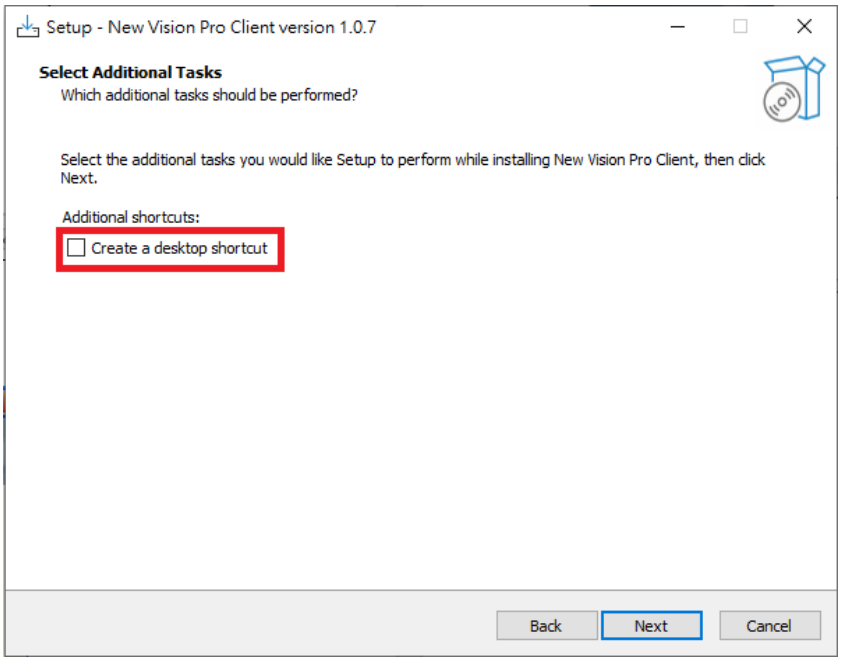
Step 4

Click on **[Next]** to install the Open-Vision on default directory. Click **[Browse]** to change the path of installation, then click on **[Next]** to continue.



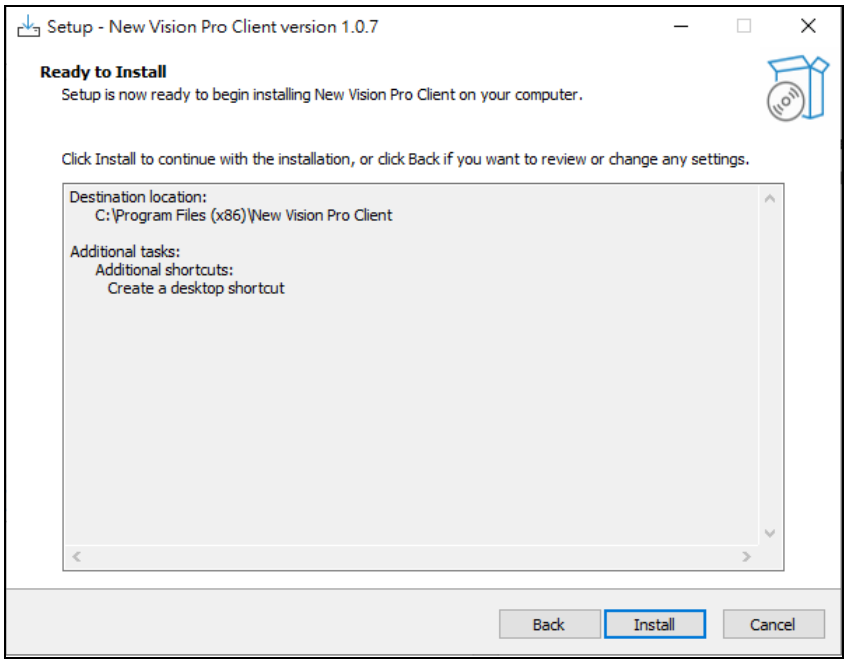
Step 5

Check the box if a desktop shortcut is preferred, then click **[Next]** to continue.



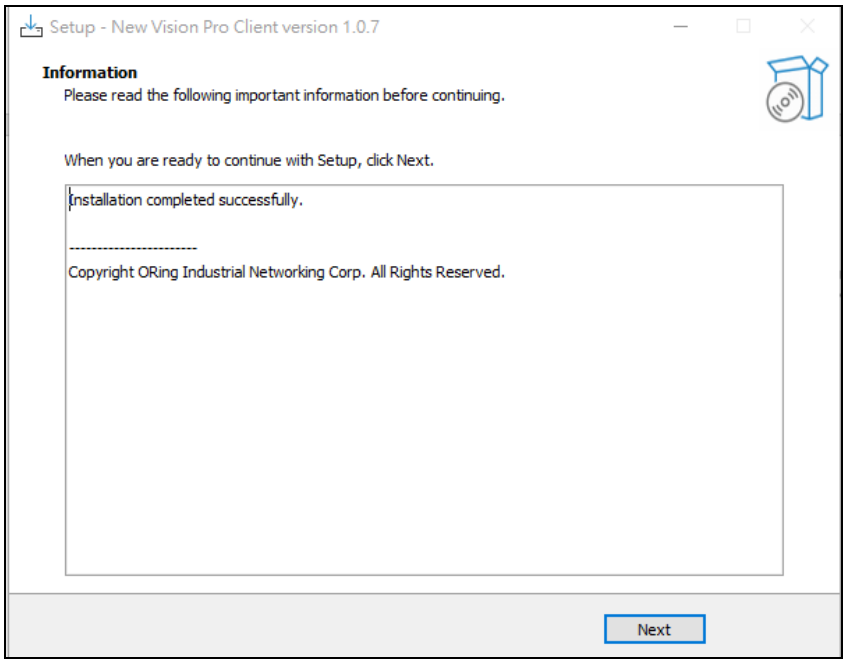
Step 6

Click on **[Install]** to start the installation.



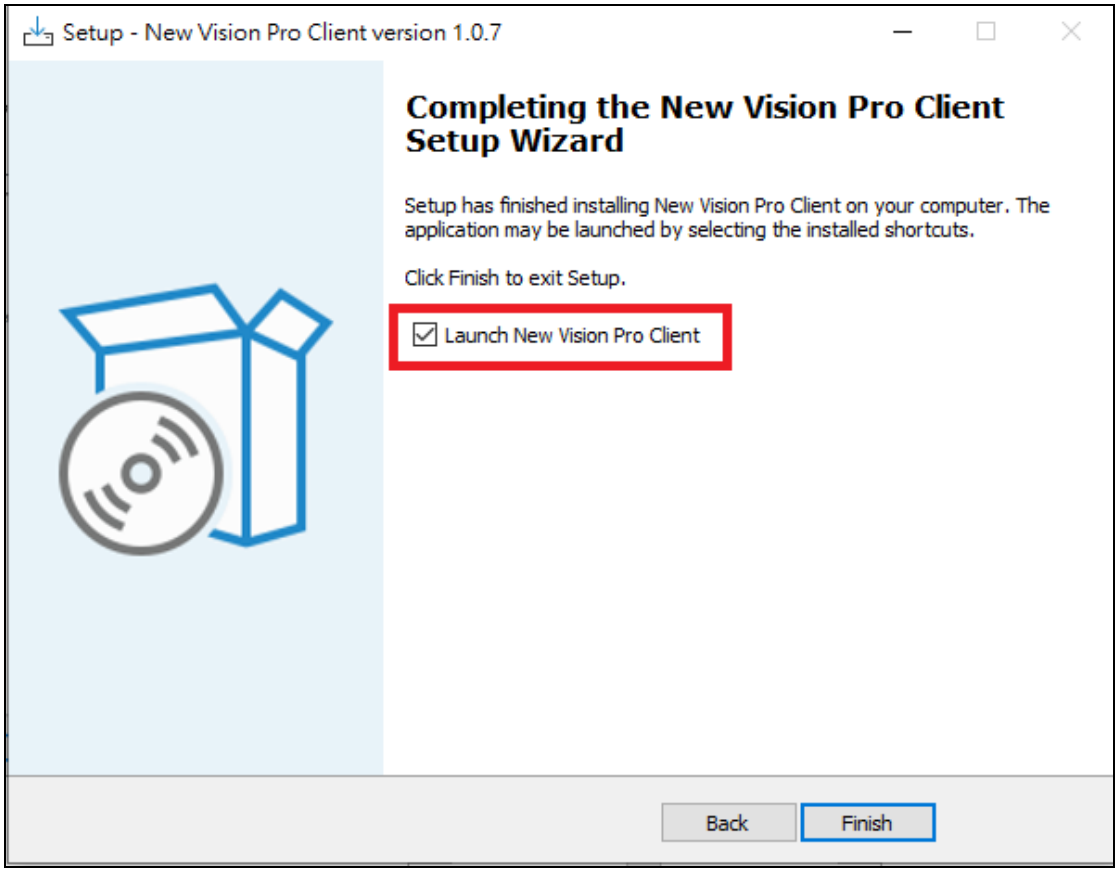
Step 7

After the installation is finished, please read the information and click **[Next]** to continue.



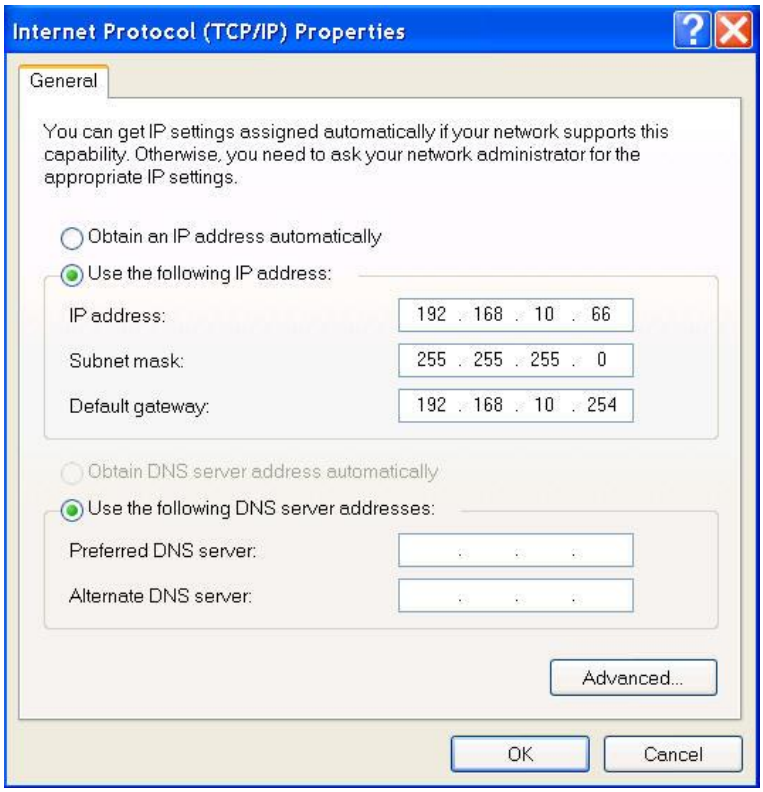
Step 8.

Check the box if launching New Vision Pro automatically after closing this window is preferred. Click **[Finish]** to close the Setup Wizard.



1.4 Configuring PC network interface card

Please set the PC's IP address and subnet mask as the switch you wish to connect.

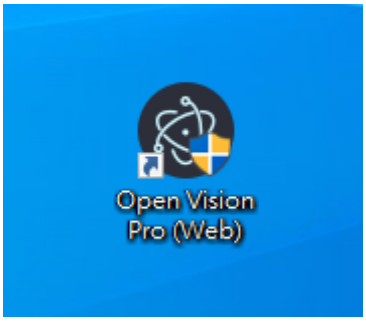


If there's two swich in different subnet, user will need to add in both subnets into the NIC.

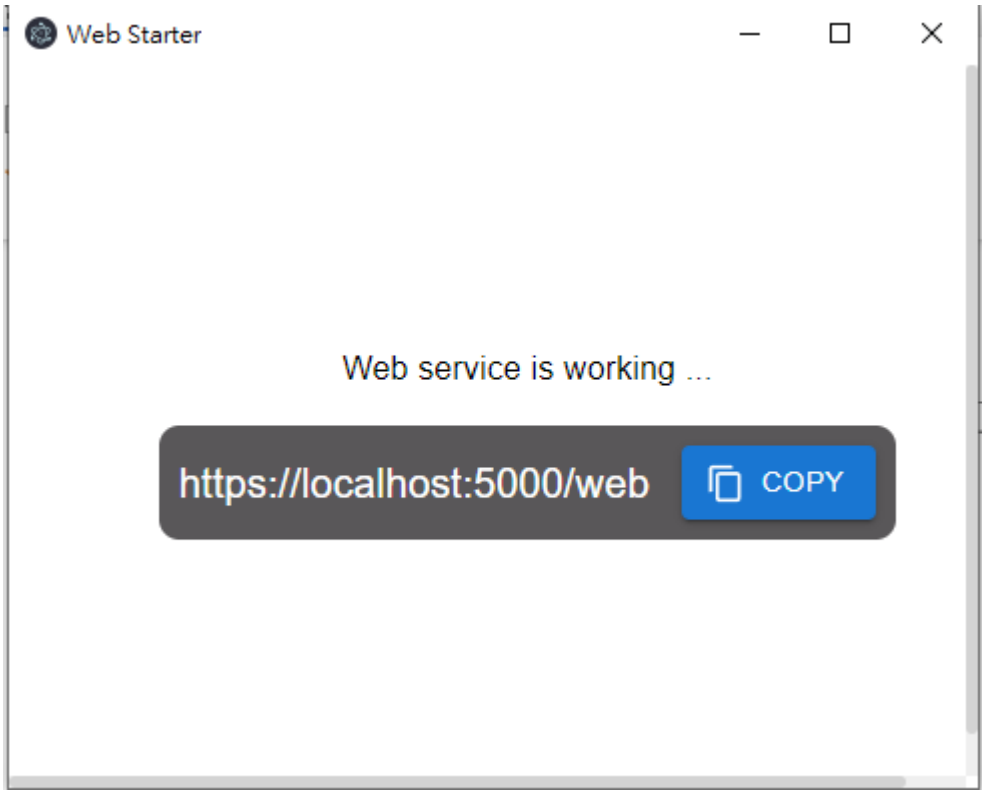
Main Function

2.1 Start OPEN VISION Pro

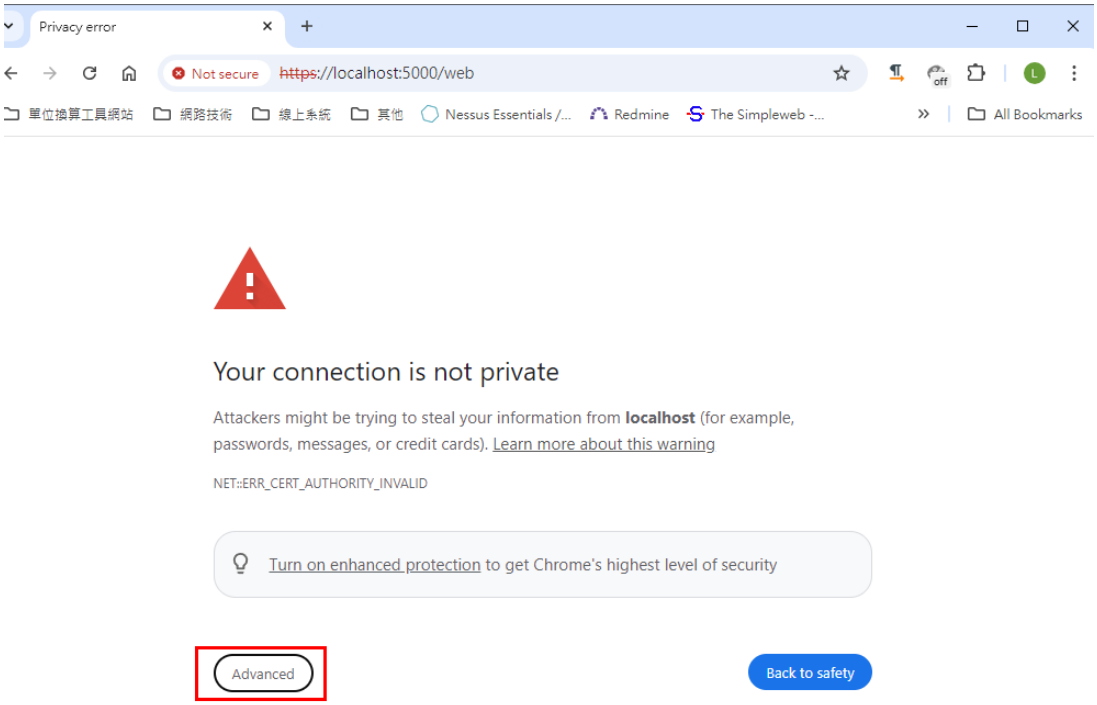
Please double click OPEN VISIO ICON



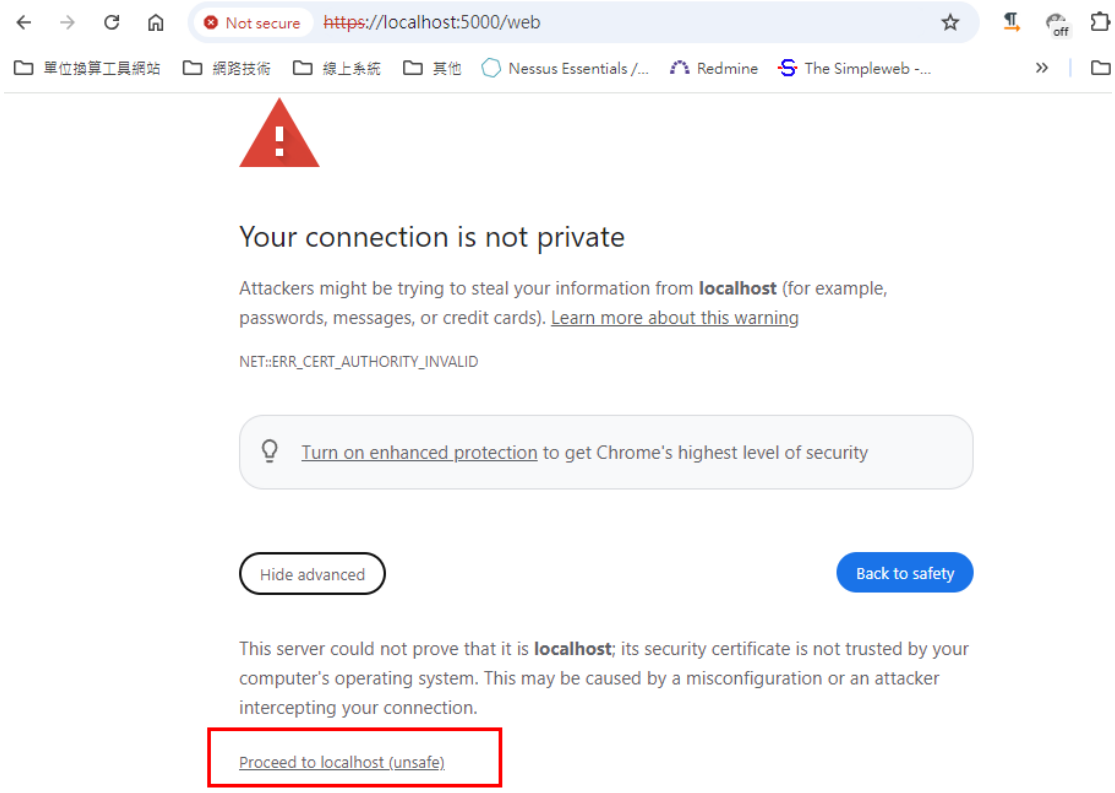
Wait few sec , open vison servcie will wokring . please copy the URL , paste to any Web browser. (use HTTPS)



Pelase click " Advanced"



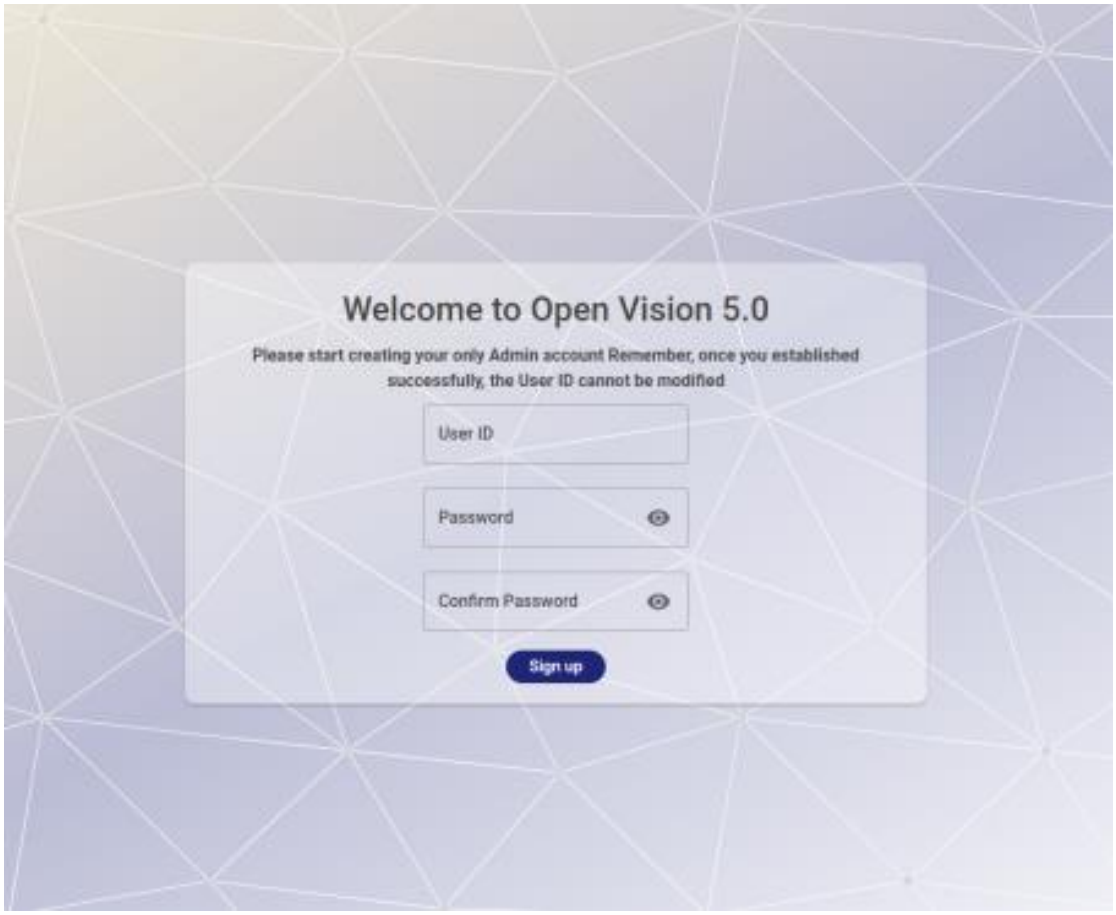
Next select " proceed to localhost(unsafe), start "OPEN VISON Pro "



2.2 Register

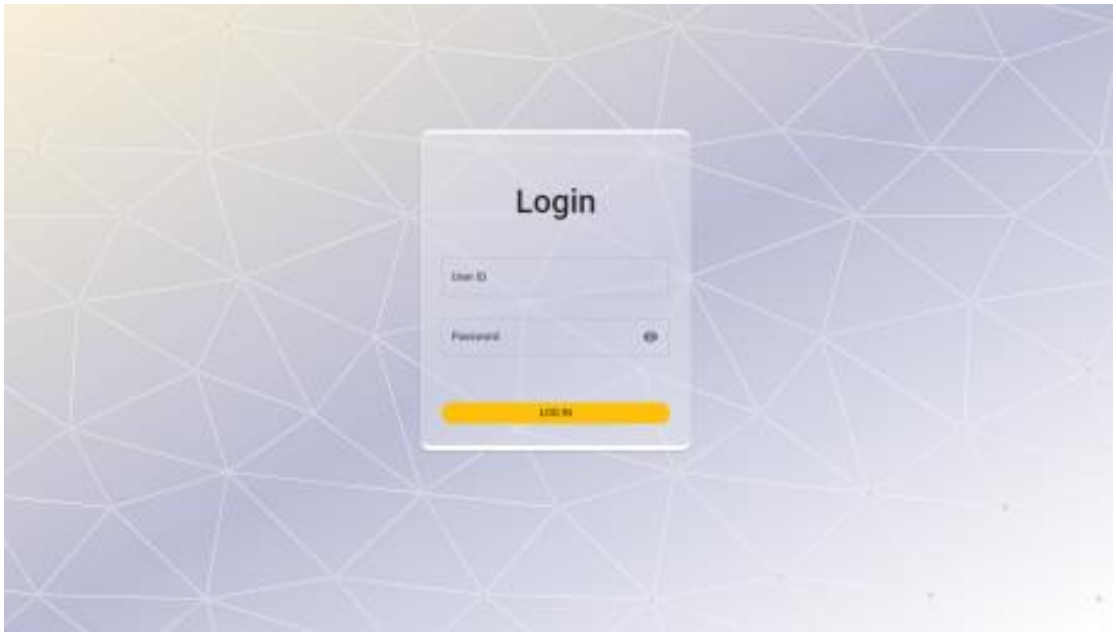
When logging in for the first time, the user must create a login account. The system wizard will guide you through this step..

Notes : Password must contain at least one uppercase letter [A-Z], one lowercase letter [a-z], one number[0-9], and one special character[@$!%#*^()?+=&_]

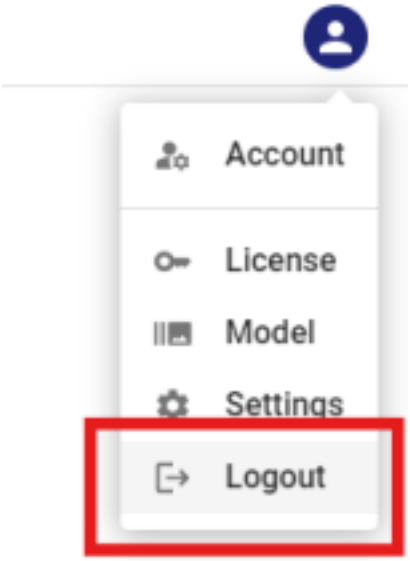


2.3 Login /Logout

After successful registration, You will first come to the pilot screen to start a new project or choose to start an old project.

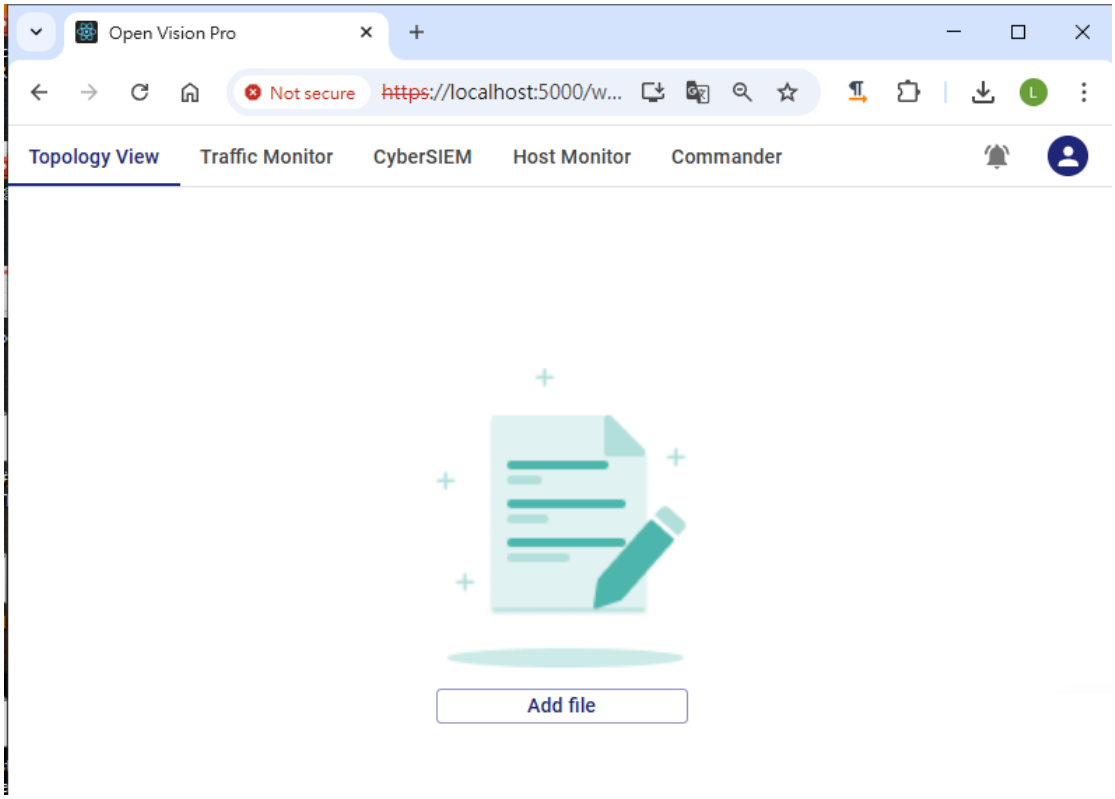


if want logout the account , can click below icon , logout option .



2.4 Dashboard

On the main screen of the dashboard, you can see three functions themedTabs: TopologyView, Host Monitor and CyberSIEM

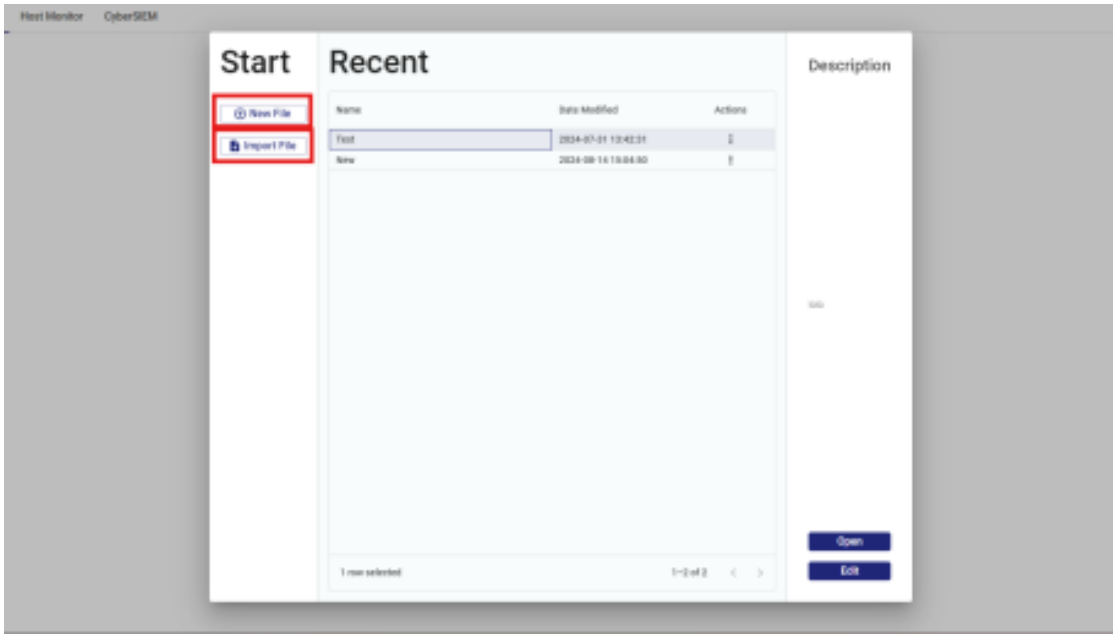


2.5 Topology View

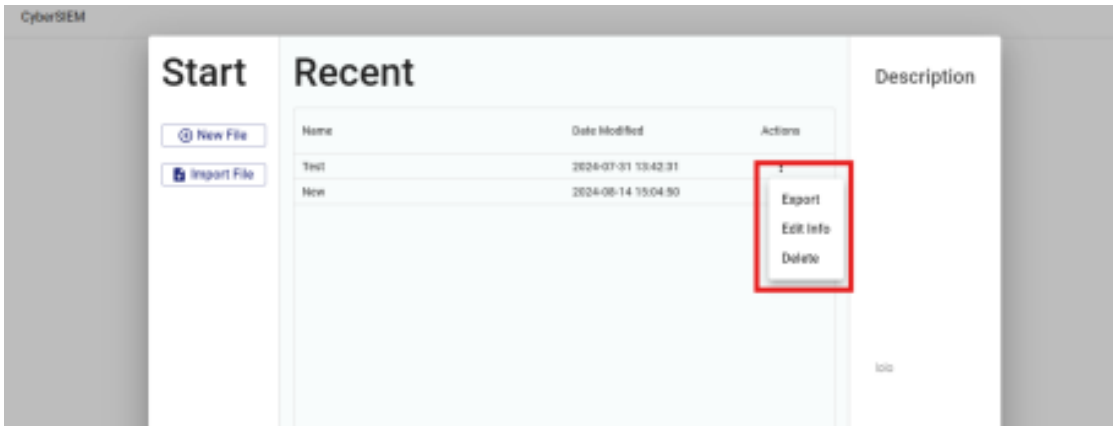
Open the project and import to create a new project, Topographic observations are all included in this function.itch.

Project Creation and Editing Process

ClickAdd file Open the project management interface as follows
Create new project& Import project(Red box mark)

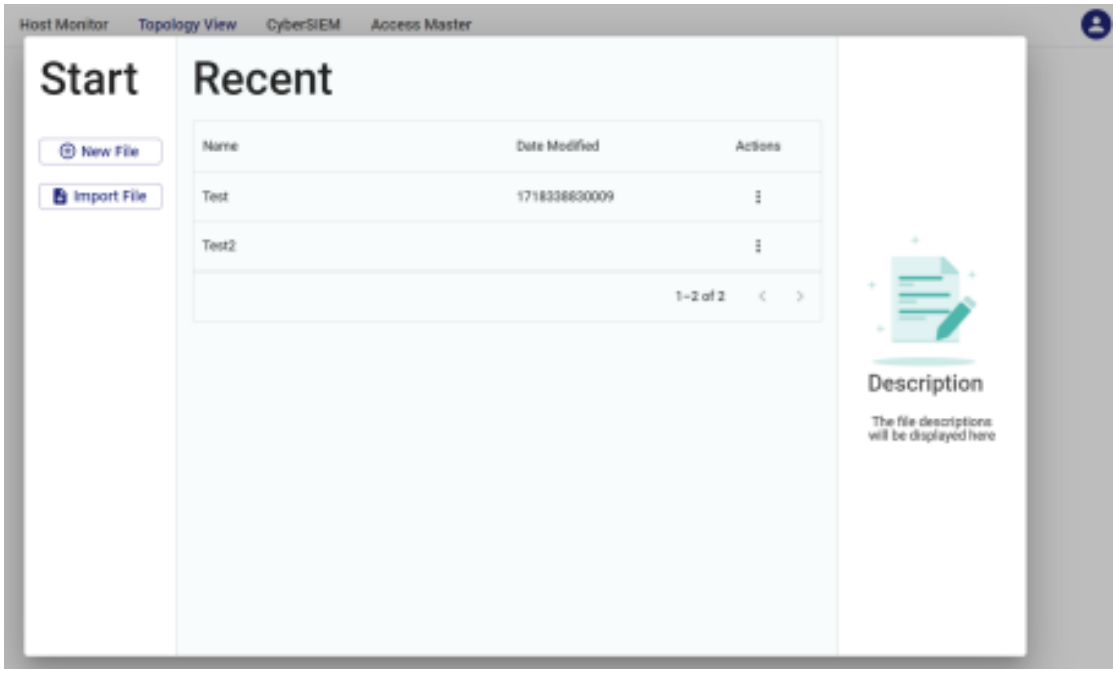


Export project, Edit project, Remove project

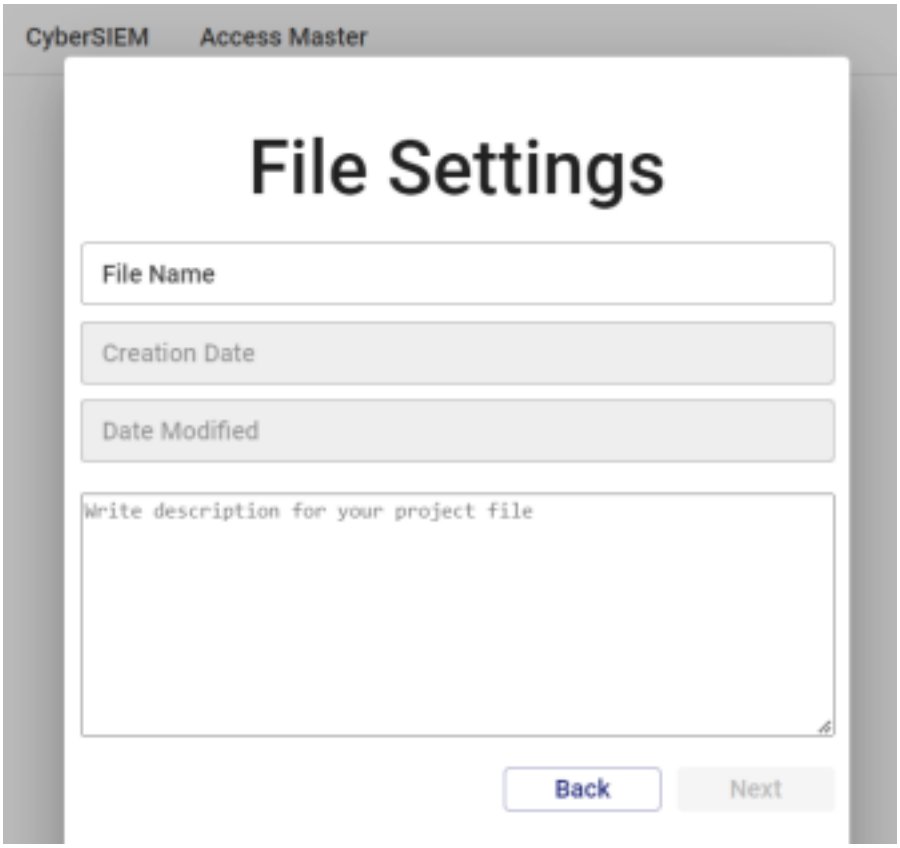


Create new project process

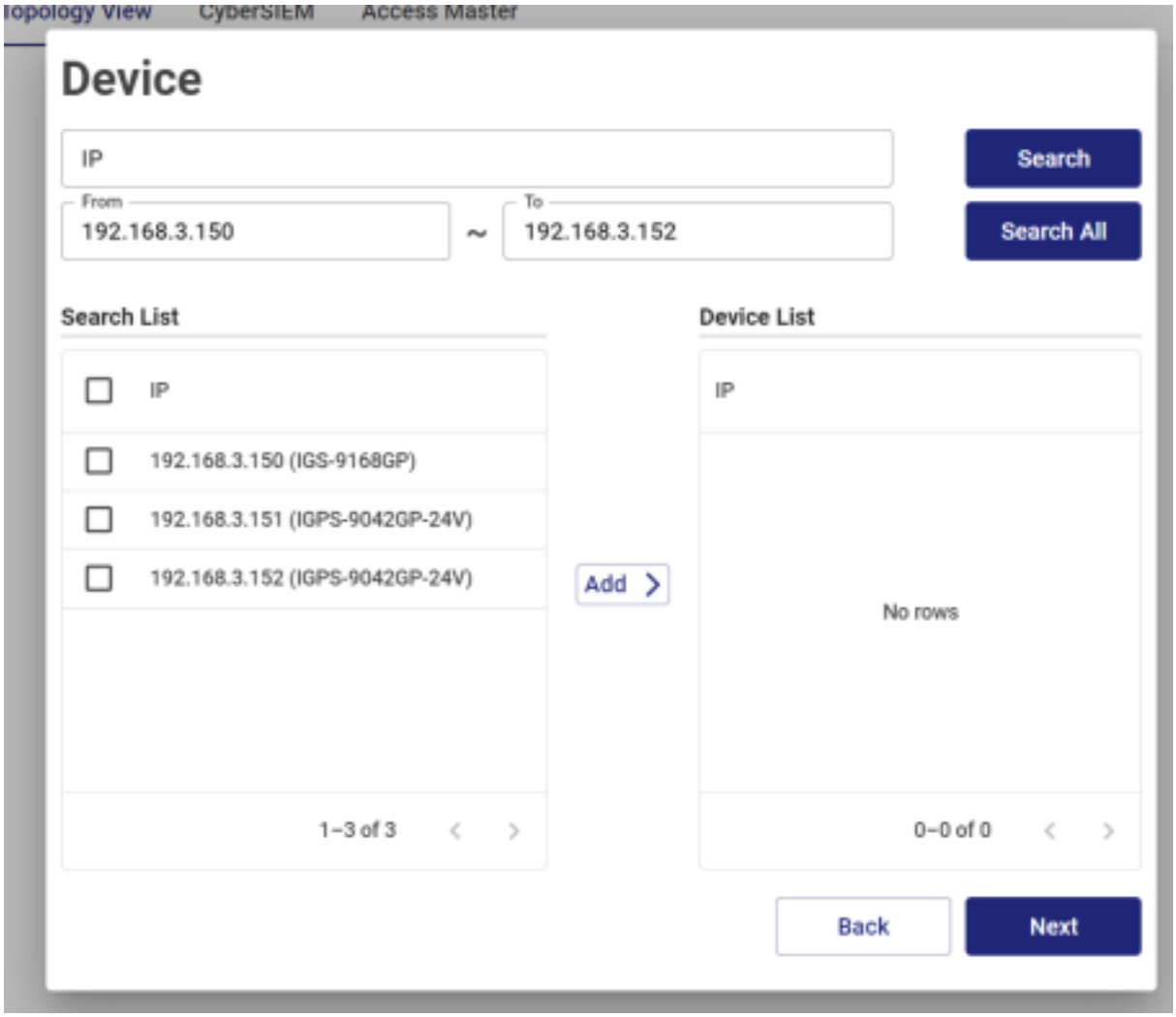
1. After completing the login process, Enter the navigation



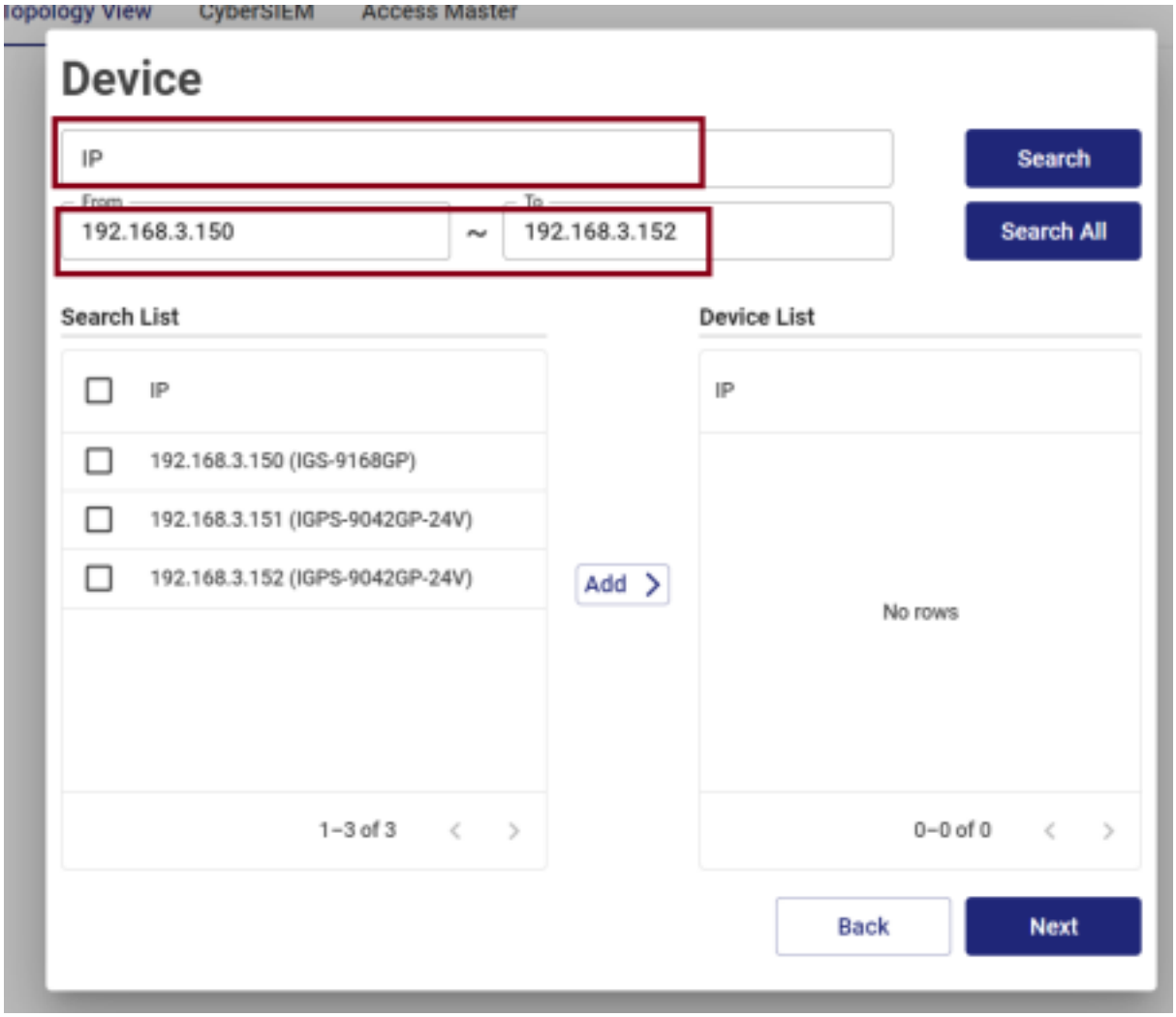
2. point New File to add a new project



3. After completing the description, point Next to set up the project environment, Device On the surface, it mainly provides user settings in the project.IP group

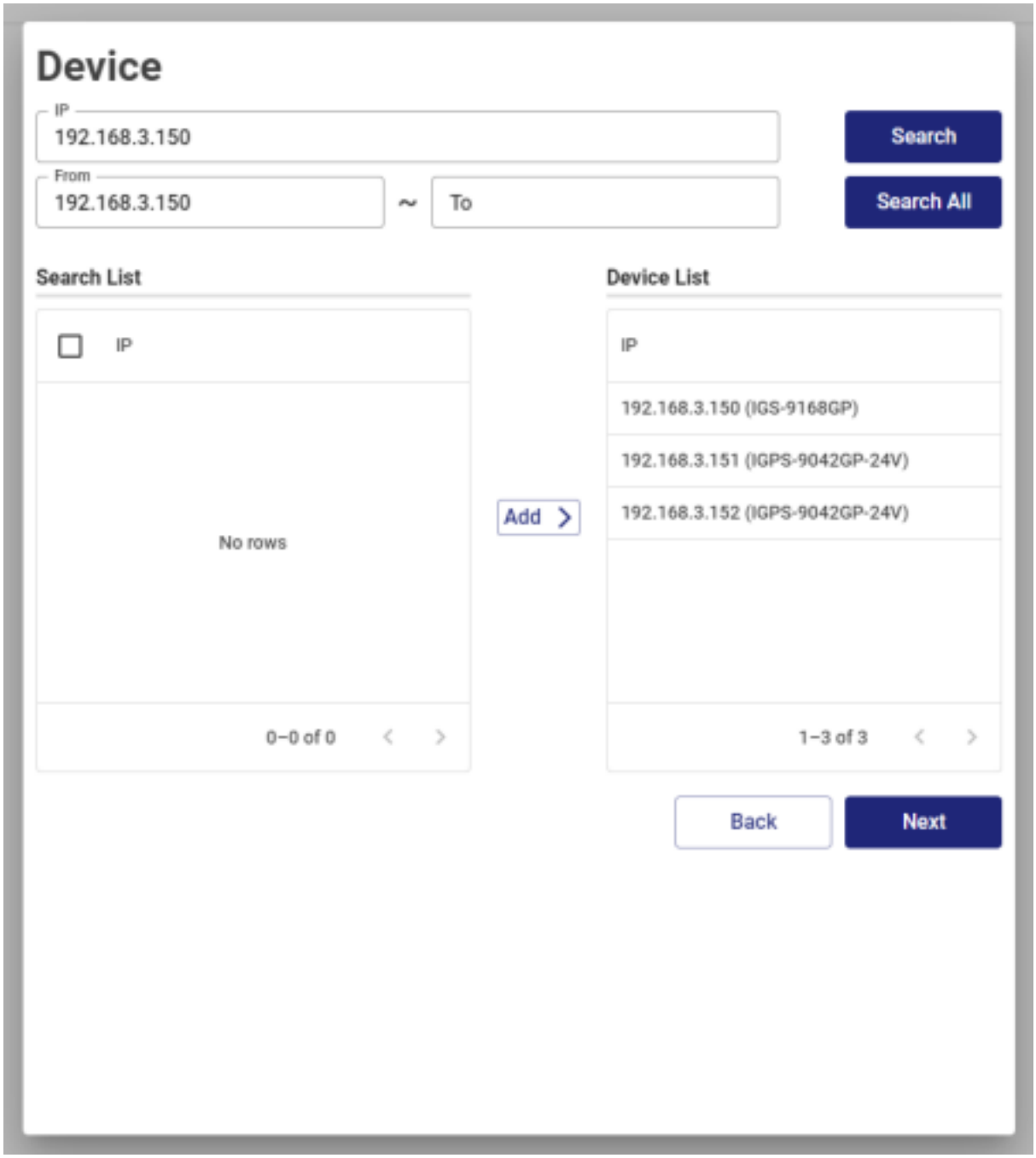


4. Device There are two retrieval modes, one is singleip, The other is range search



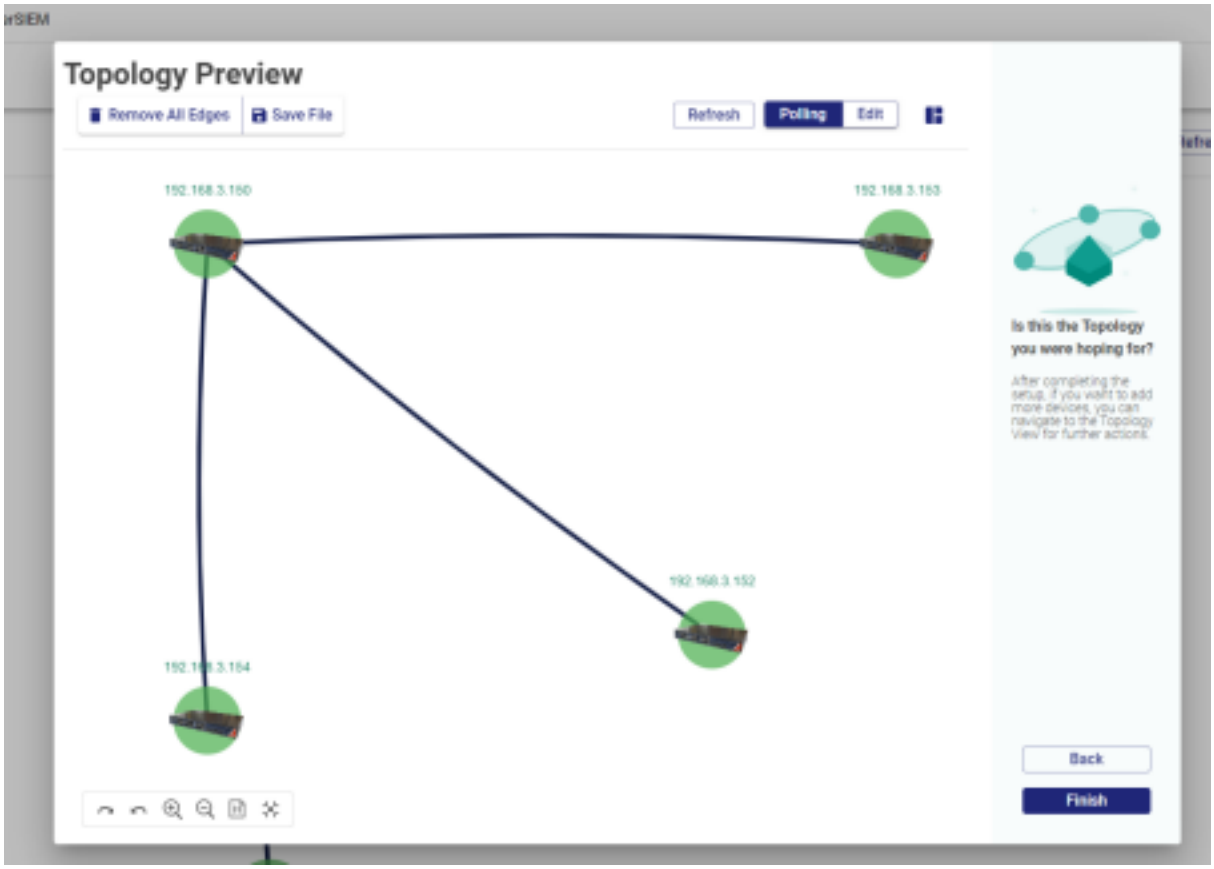
5. Search List Devices scanned according to settings for this current useIP, Device List Device to save settings for the projectIP,

Check the box you want to joinDevice List of devices and click onAdd to add device, When finished pressNext

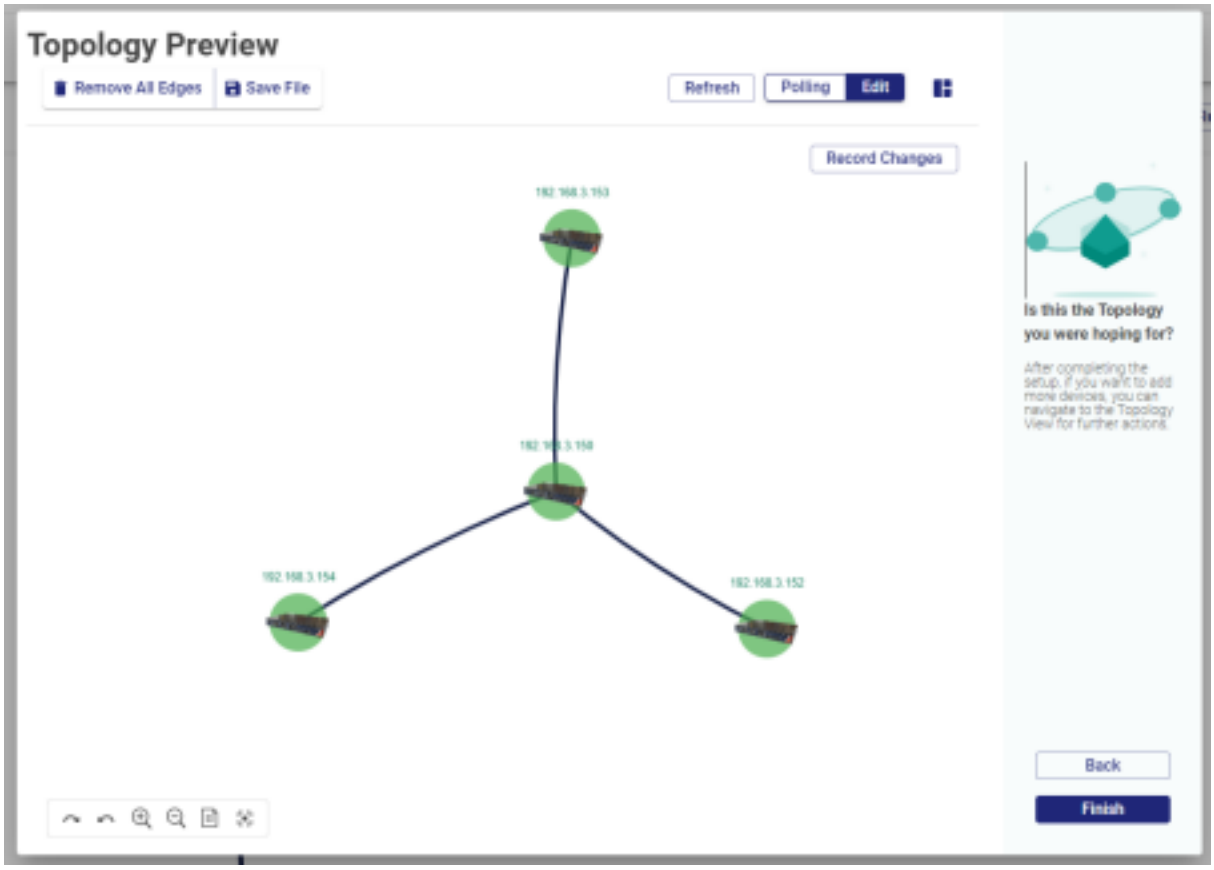


6. Enter Topology Preview screen, Tool field functions:

- Remove All Edges : Clear the line segment relationships of the current topology, Refers to the remaining device nodes
- Save File: Contains the relationship between equipment nodes and line segments of the current topology
- Refresh: Immediately refresh the topology information
- Polling / Edit : Switch to edit mode to manually adjust node coordinates(X.Y)
- Working mode switch: Deployment/ Collapse the device tree diagram on the left.
- Finish: After clicking, the current relationship between equipment and line segments will be saved first and then closed.



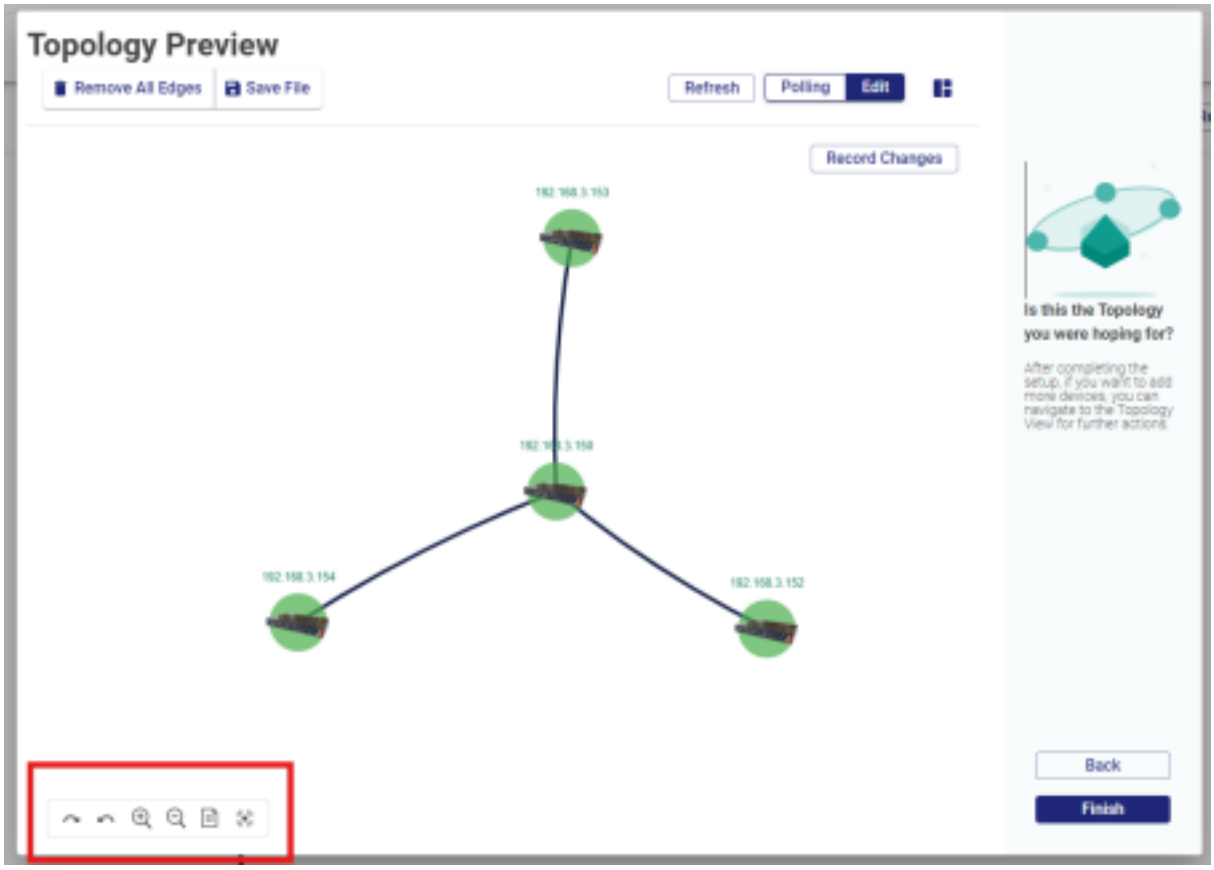
After dragging the device location, Remember to pressRecord Changes To record the currently changed topogram



Map Tools

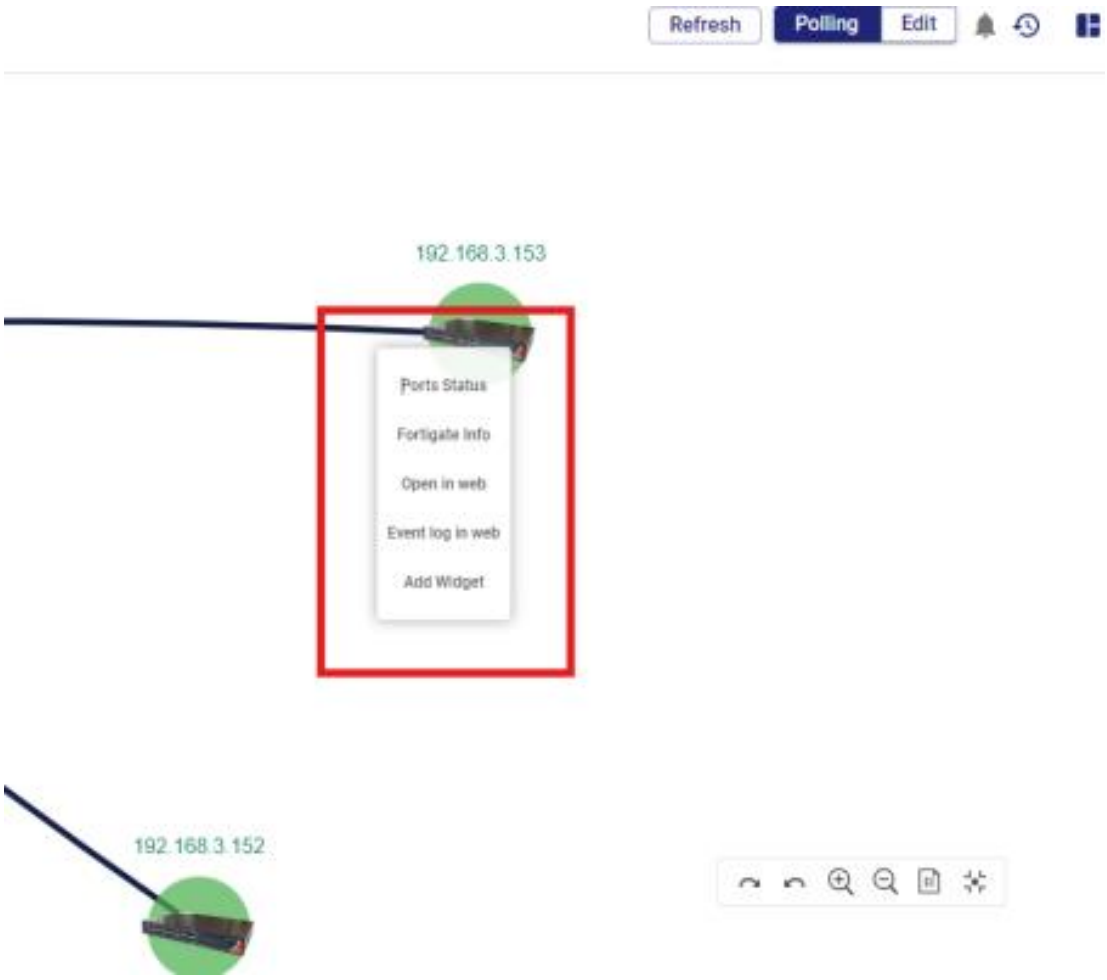
Map extension toolbar (from right to left in order as follows)

- Previous and back buttons: will perform operations based on the recorded XY coordinates when changing device nodes.
- Magnifying glass : ZOOM IN, ZOOM OUT
- Center alignment button : The screen will automatically align with the center node position of the topology
- Screen center button : will automatically focus the entire topography to the center of the canvas



Device(Node) – Device Menu

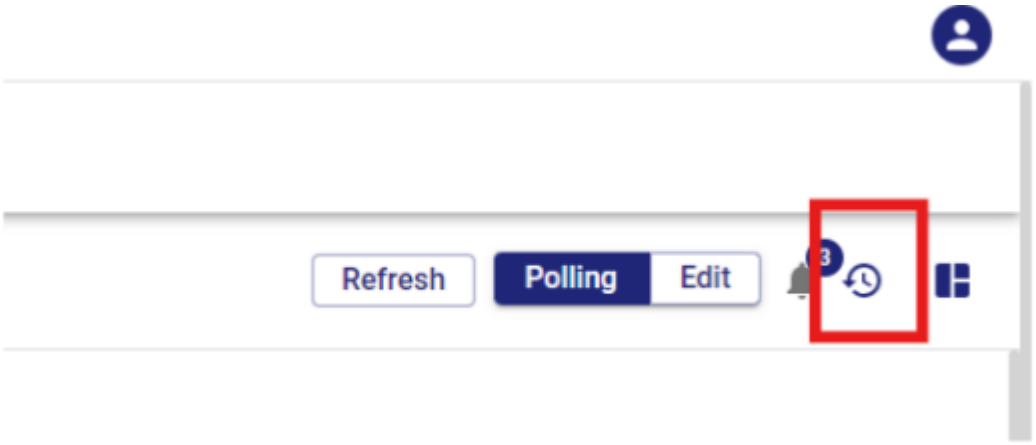
Right click on the extension device to see the option menu

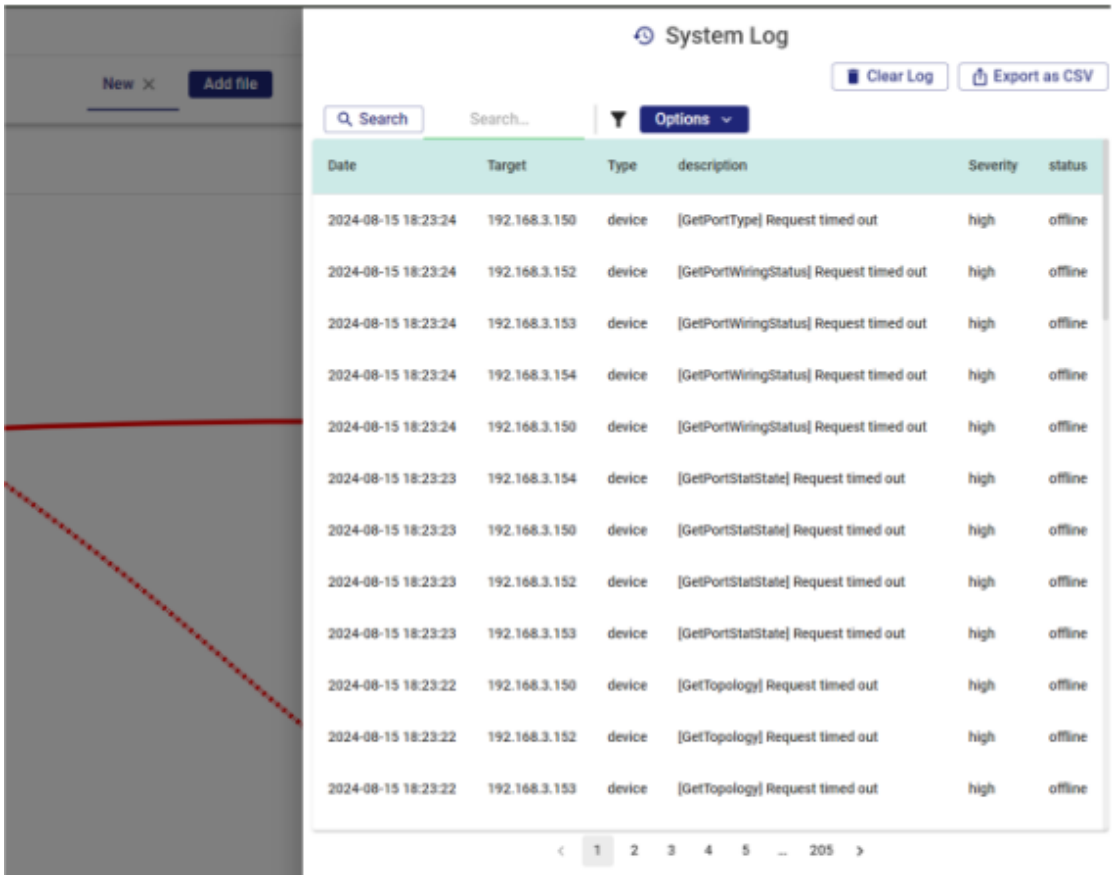


- Ports status: Jump to HostMonitor page
- Fortigate Info: Jump to CyberSIEM page
- Open in web: Open the login screen of the current device router
- Event log in web: Open the Event Log of the current device route
- Add Widget: Add device node

System log

After clicking, the system log form will pop up.

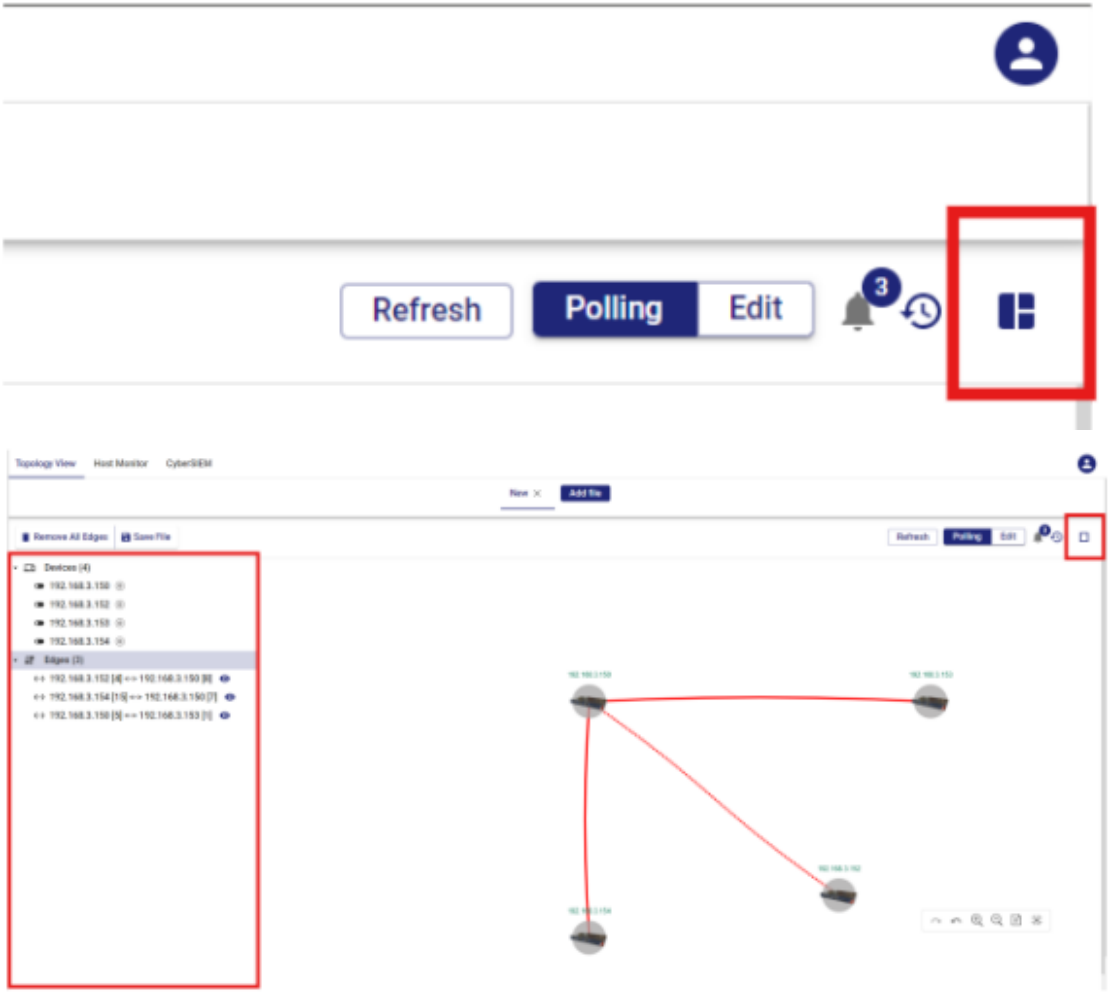




- Clear Log: Clear current log
- Export as CSV: Replace the current system log withcsv Format export

Working mode window switching

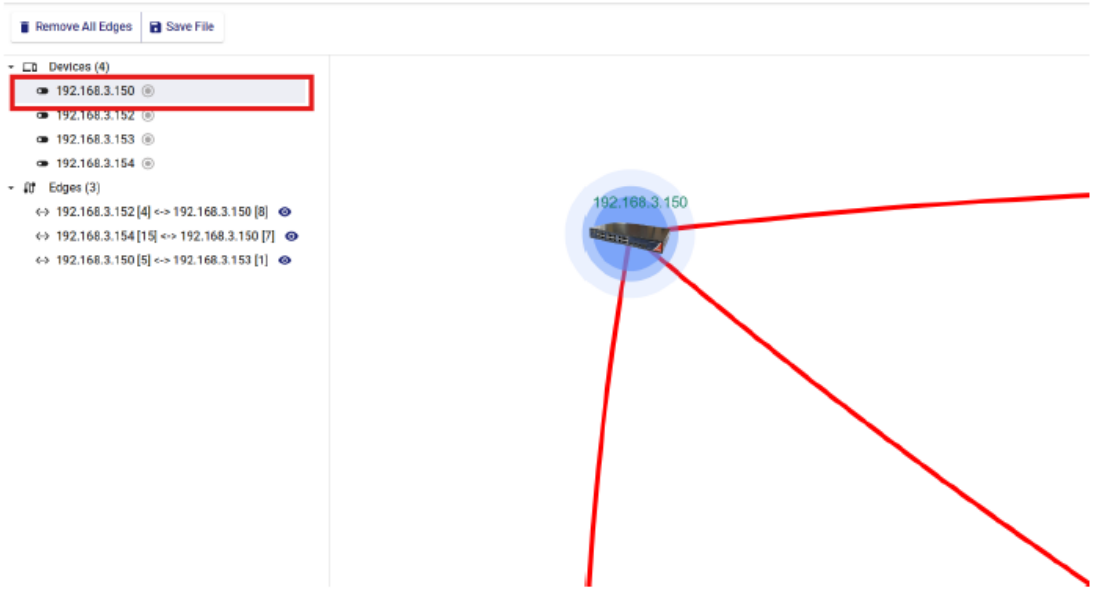
After clicking, the system log form will pop up.



Devices (IP + Device status)

- Gray light signal : Device offline
- Green light : Device online

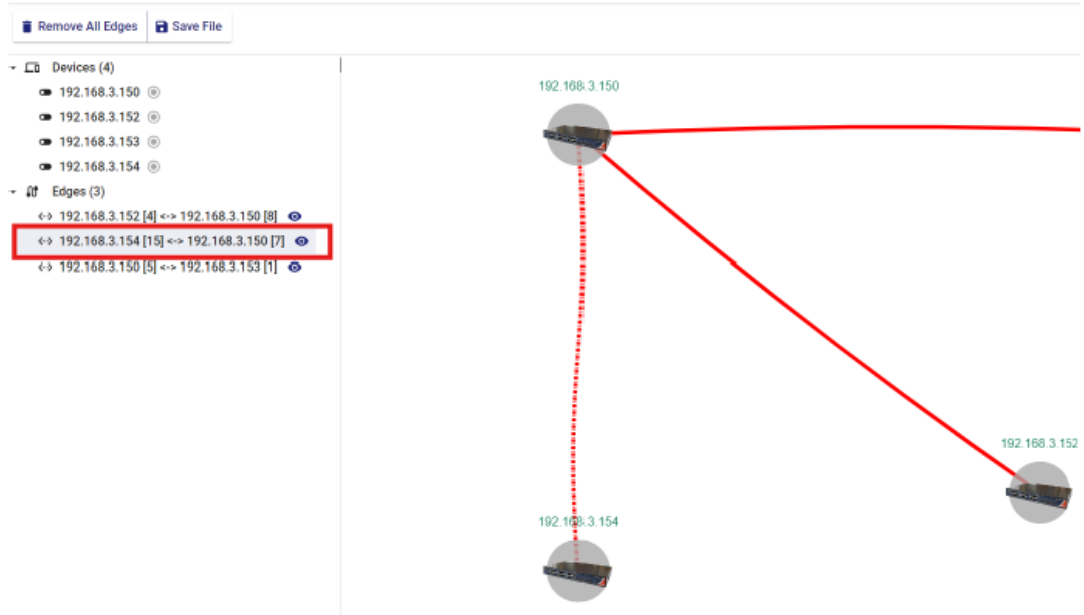
Click on the item and the device will show a fluctuating state in the map on the right.



Edges (A IP +[A Port] < - > B IP + [B Port])

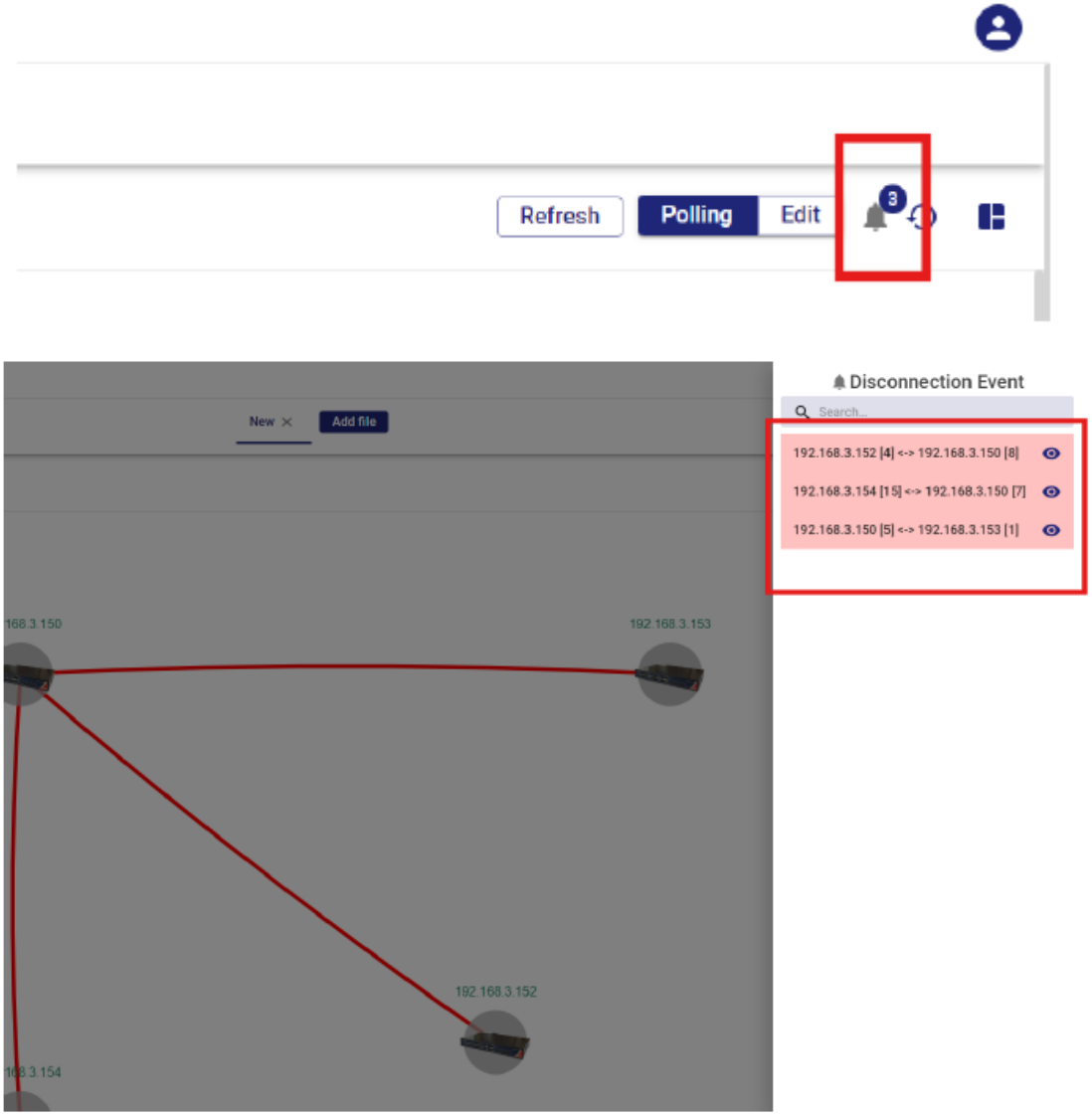
Click on the eye to view the historical events of the line segment

Click on the item and the line segment will appear in a flowing state in the map on the right.



Notification

Disconnection event notification, Abnormal traffic notifications will be displayed with a small bell here.

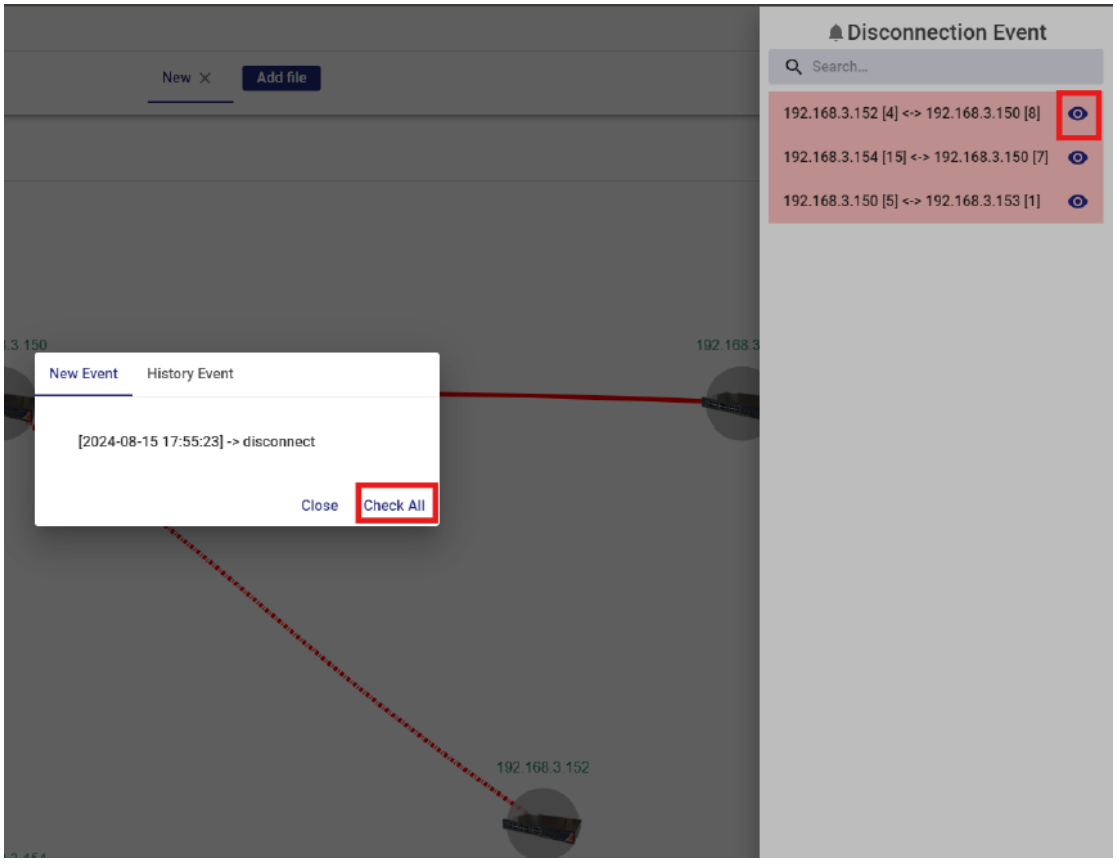


Notification – Detail

Item comes in two colors

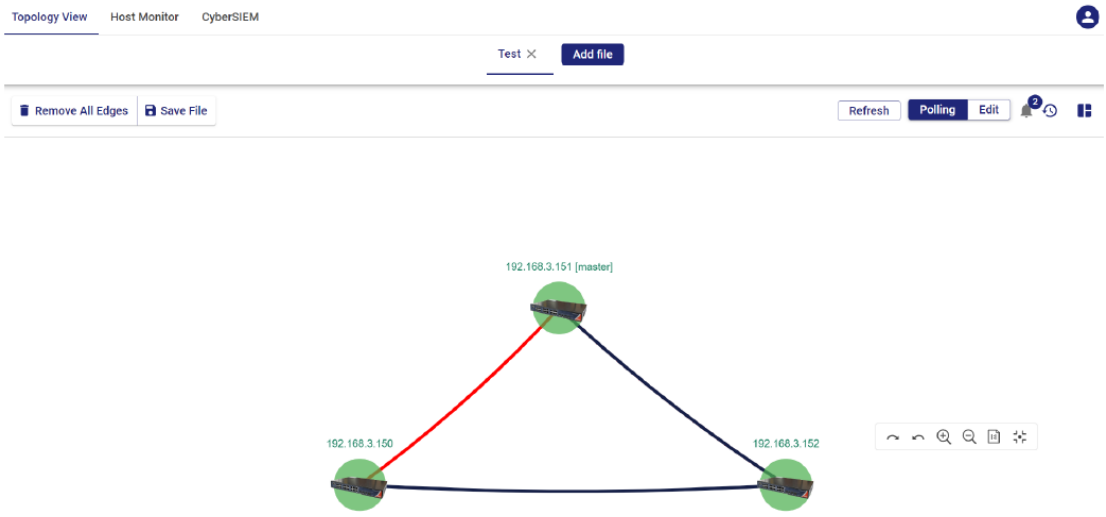
- Red : The current line segment is detected as disconnected
- Yellow : The connection has been disconnected before, and the connection has been restored. You need to clear and confirm the disconnection event.

Click the eye icon to view the event history for this connection

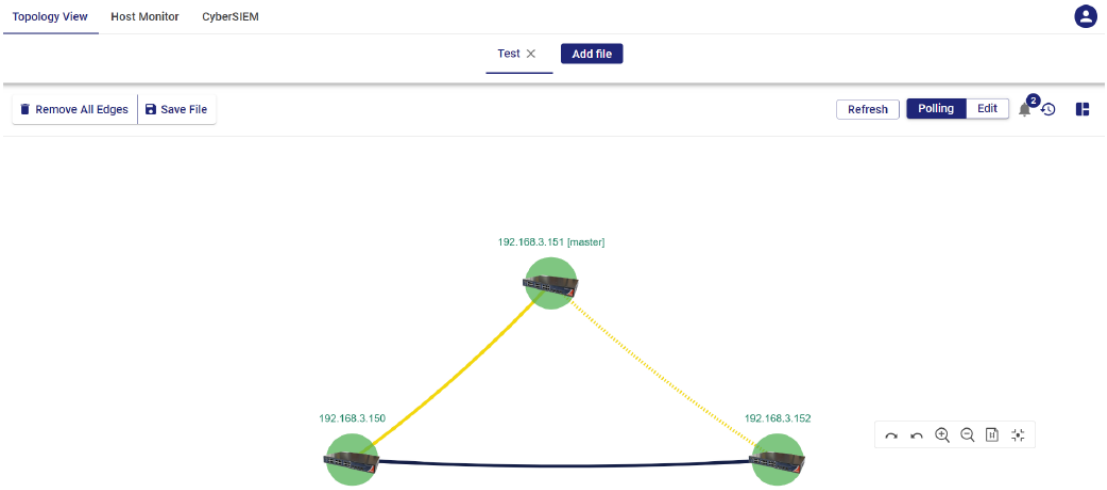


How to clear exception warnings for line segments?

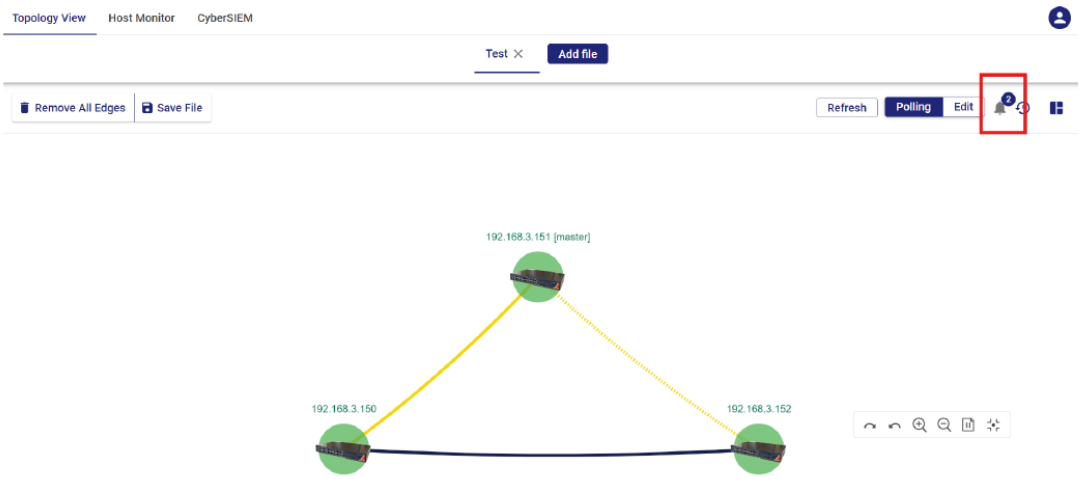
This is when a disconnection event is currently detected (the default disconnection warning will appear in red)



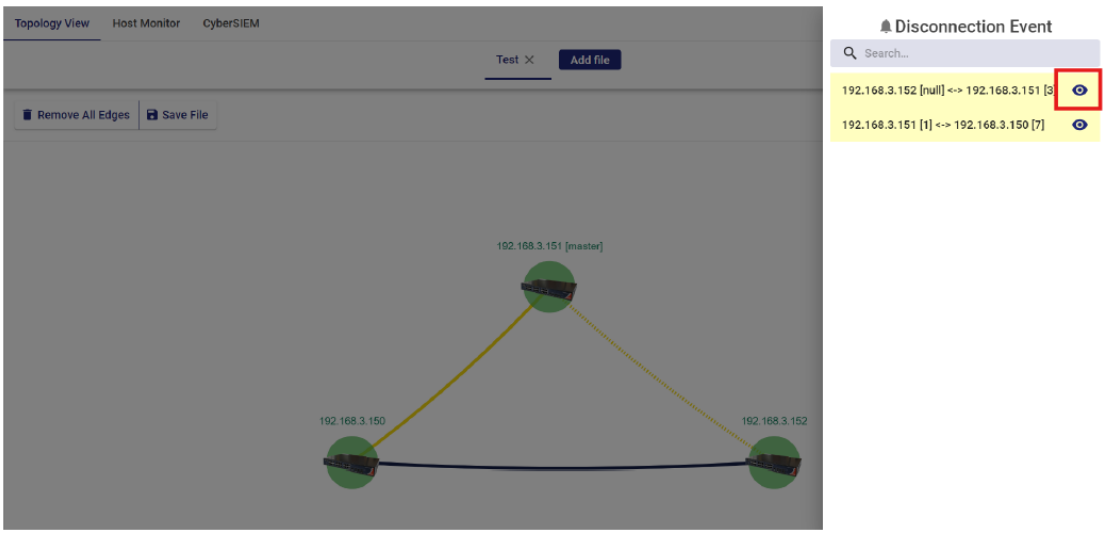
If the disconnection is restored, the backup line segment that has been disconnected or activated will be displayed in yellow by default.



Clicking the notification icon will expand the list of disconnection events. You need to confirm the abnormal line segment before you can change the line segment from yellow Color (Once disconnected and now restored) Return to the original normal line segment color (default is black)

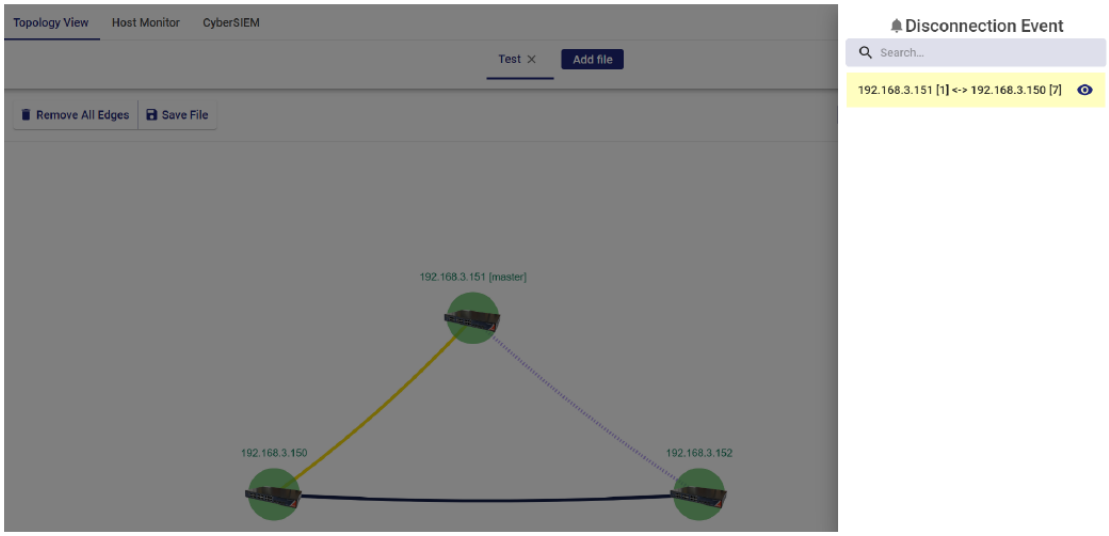


For abnormal line segments, click the check icon to confirm the disconnection event.



After opening, you can view the currently unconfirmed historical disconnection events. Click Check All to confirm.

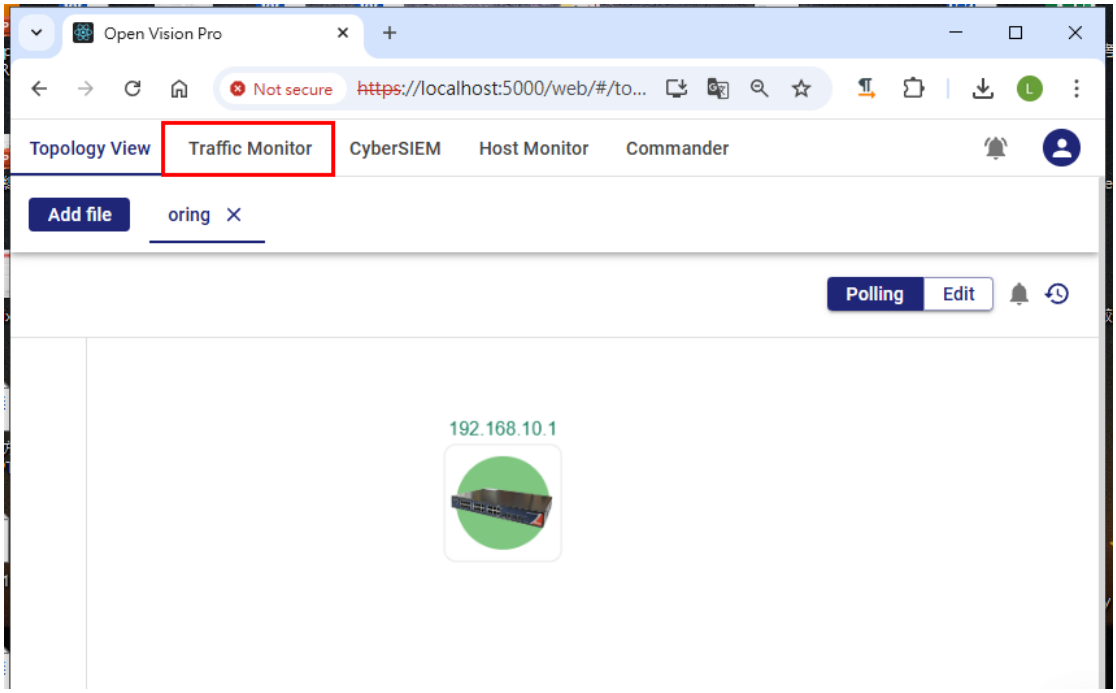
As long as the unconfirmed disconnection event of the line segment is cleared, the line segment will return to its normal color.



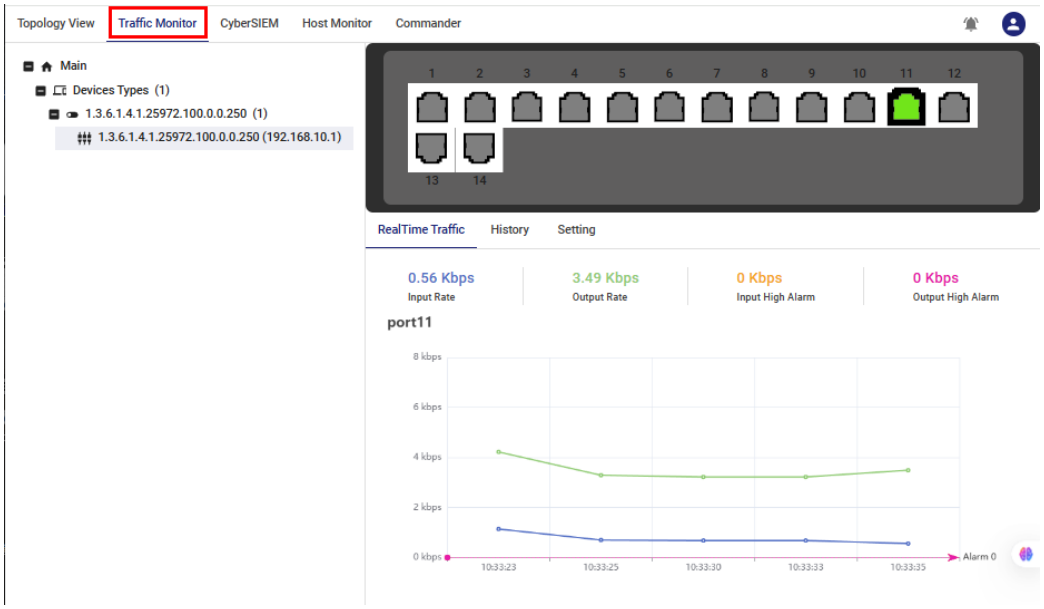
2.6 Traffic Monitor

Monitor the traffic status of scanned device ports

First open a project in Topology. Traffic Monitor will capture all devices bound to the opened project.

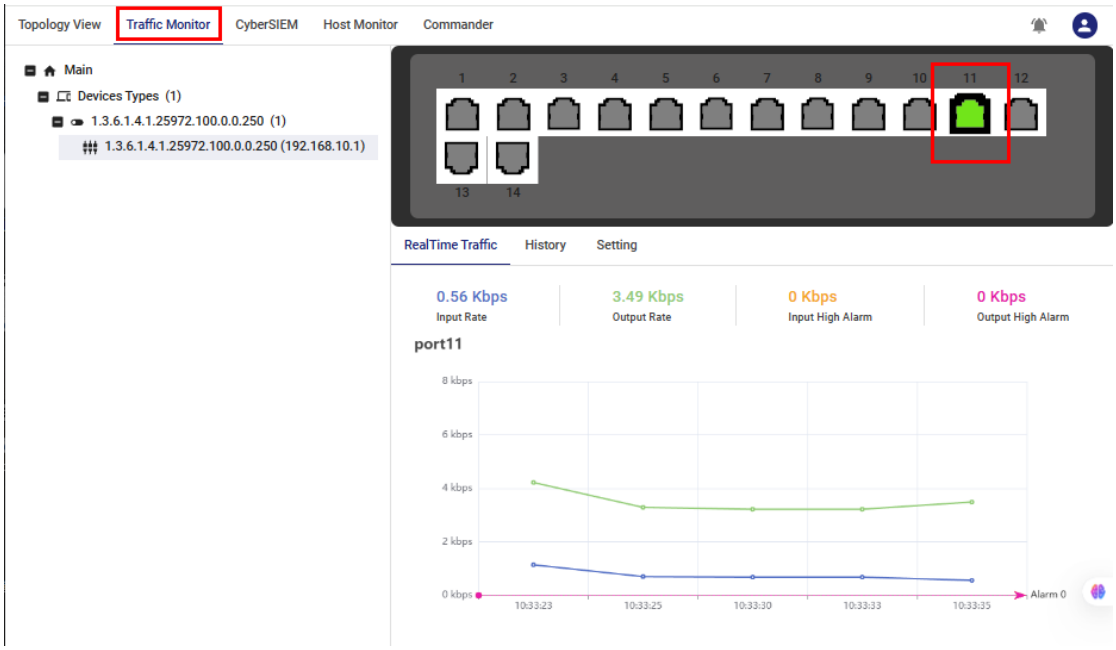


Switch to Traffic Monitor and you can see that the device just mapped has been captured and the port traffic is tracked.



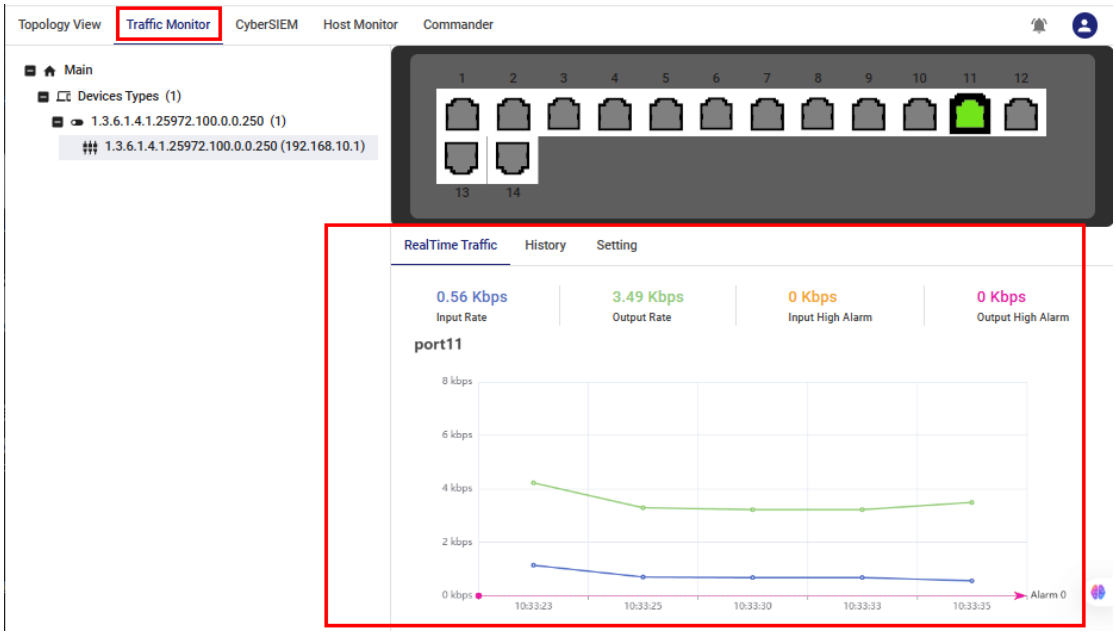
Port color and status

- Green: Connecting
- Gray: Not connected
- Red: Port is locked



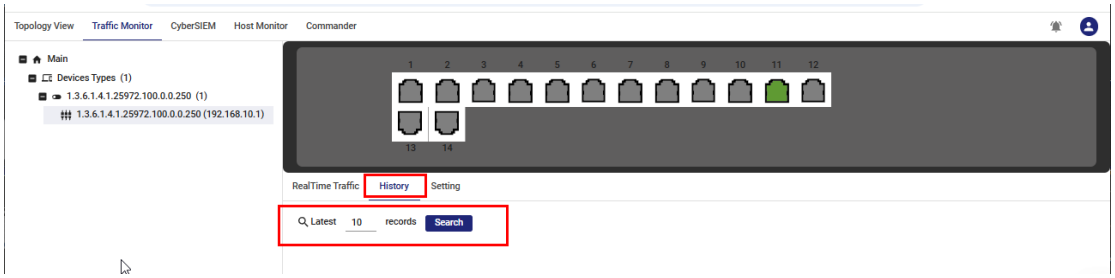
RealTime Traffic

Click on the specified port, and the (Realtime, History) information below will also be displayed based on the port. RealTime is that time flow presentation

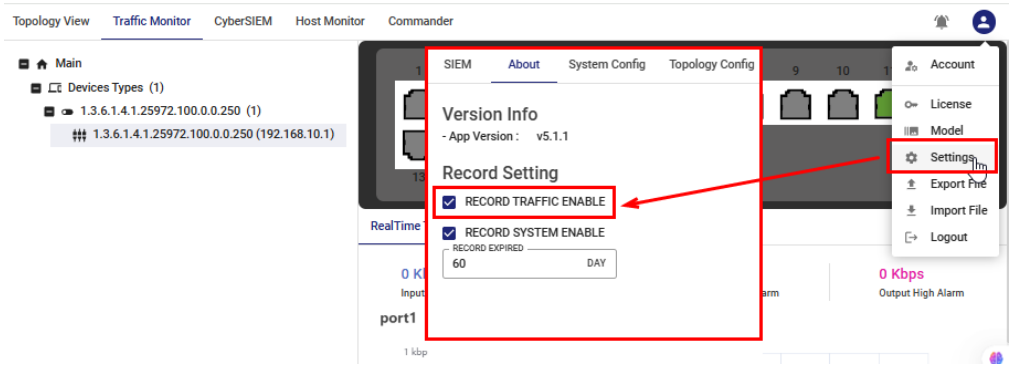


History

The History page can be used to query the traffic record history of the current specified port.

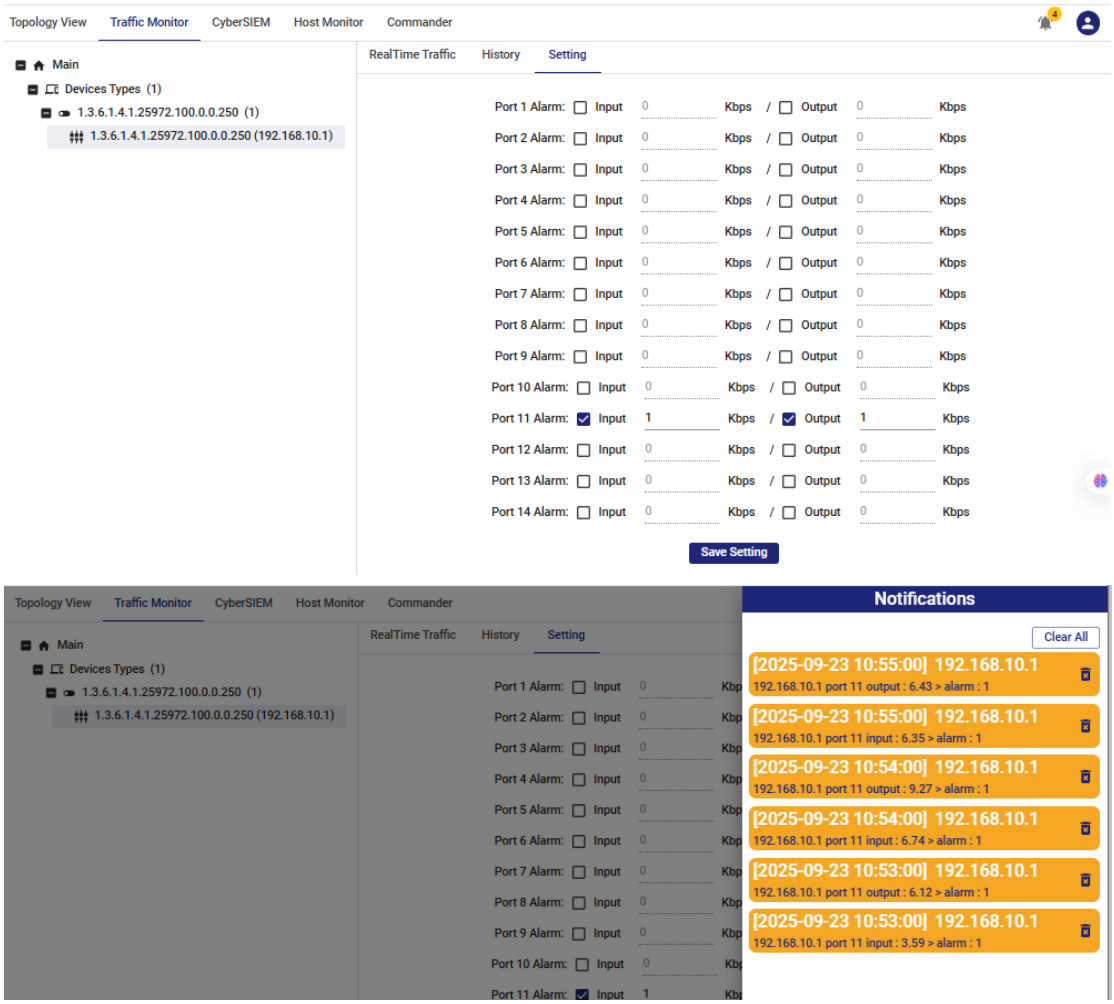


Notes: if want get history log , need enable "Record Traffic " first .

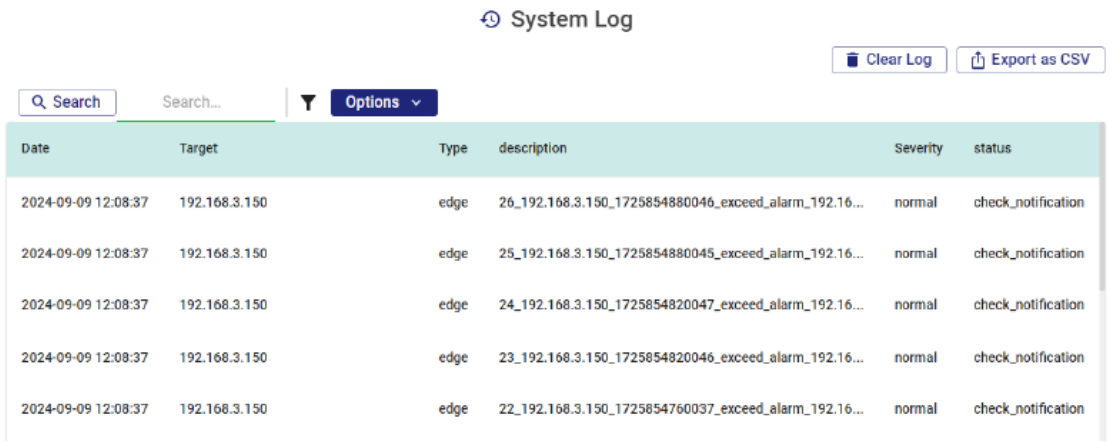


Setting (alarm)

This page can setting traffic alarm value , if traffic flow over this value Open vision will sent alarm log



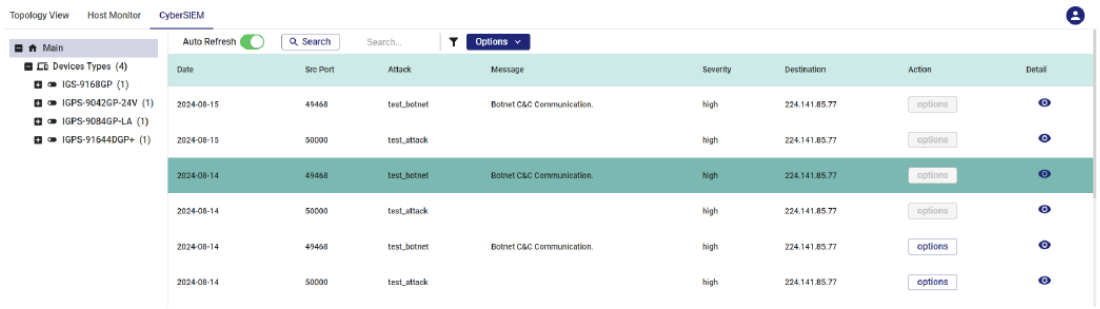
Confirmed events will be recorded in System Log



.

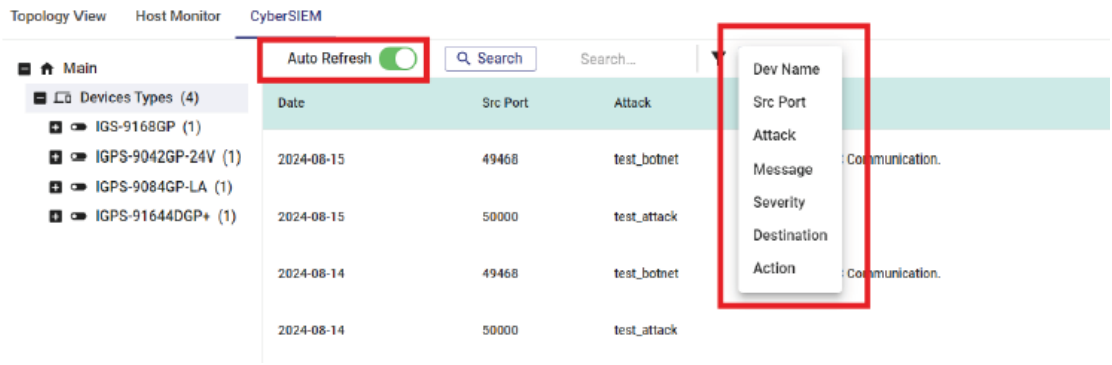
2.7 CyberSIEM

Provide information security-related system records, queries, and operations that match designated equipment



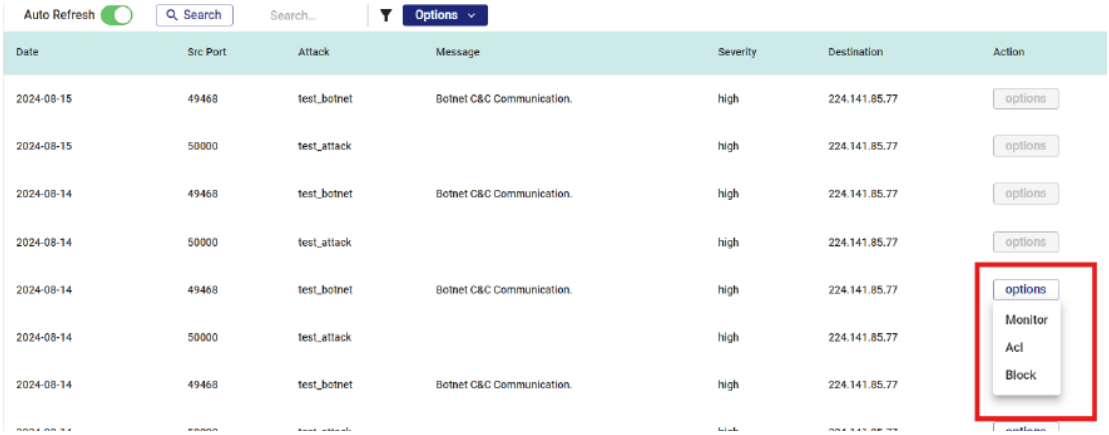
Search Tool bar

- Auto Refresh : When enabled, the form can be refreshed automatically at regular intervals.
- Option : Provides various query parameters



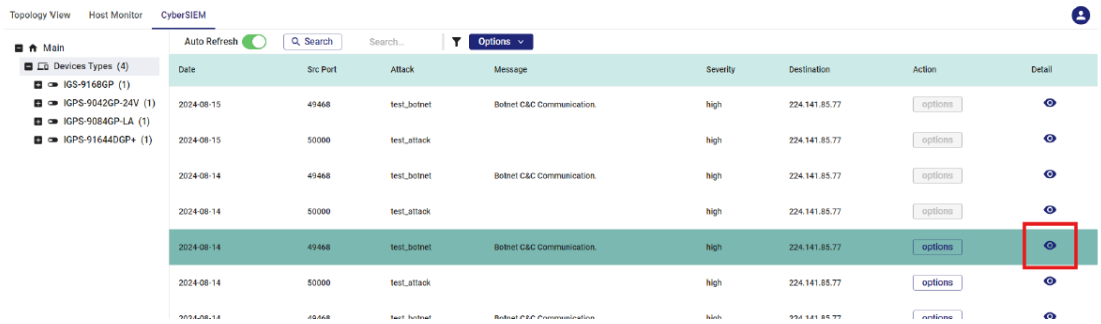
Action Menu

- ACL: blacklist settings
- Monitor: monitor
- Block: Lock port



Detail status

Click the Detail eye icon to view detailed information about the security alert project



Detail info as below :

2.8 Host Monitor

The Host Monitor function polls the corresponding IP address using ICMP pings at regular intervals to monitor whether the device is online or offline. When the device status changes, relevant information is generated and recorded.

Monitor Panel Description:

The Monitor screen is the main function of the Host Monitor function to perform tests on specific IP addresses. Through the Monitor screen, you can add IP addresses and use the Host Monitor function to monitor the status of specific IP addresses. The total number of tests sent and the number of failures will be recorded.

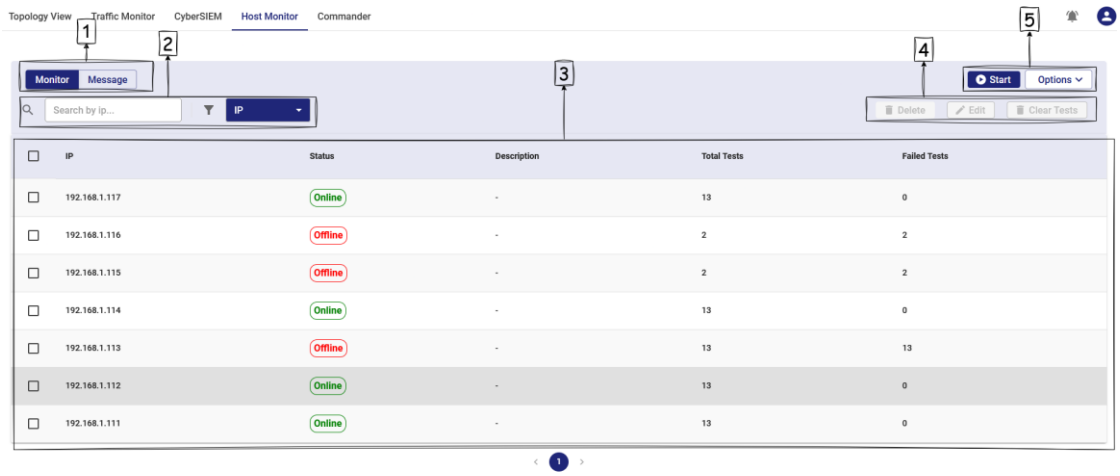


Figure 1 Monitor function panel

Above Figure 1 shows the main panel of Monitor. The following functional description will explain the functions of the above panels to analyze the functions and uses of each block:

1. Function switch button

The switch button can switch between the Host panel and the Message panel. The Host panel is mainly responsible for executing the test function and displaying information such as the status and results of the test IP. The Message panel is mainly used to display event notifications, that is, the information panel for recording logs.

2. Content search function

The search function allows you to search for specific content by using keywords in a specified field.

3. Test and related content display block

This area mainly displays the test IP and its binding information, and displays the test results and IP device status and other related information.

4. Function panel block

This block is mainly a function button block. There are buttons to clear test results or devices, as well as a "Description function" to edit the device IP.

5. Action execution related blocks

This block is mainly used for execution of kinetic energy related blocks, such as the execution of test action buttons, adding new equipment or modifying test settings, etc.

Message Screen Description

The Message screen is mainly used to record messages. When a specific event occurs in the Monitor function, the Message screen will record the event, which is also the Log recording function. Users can freely export and import event records.

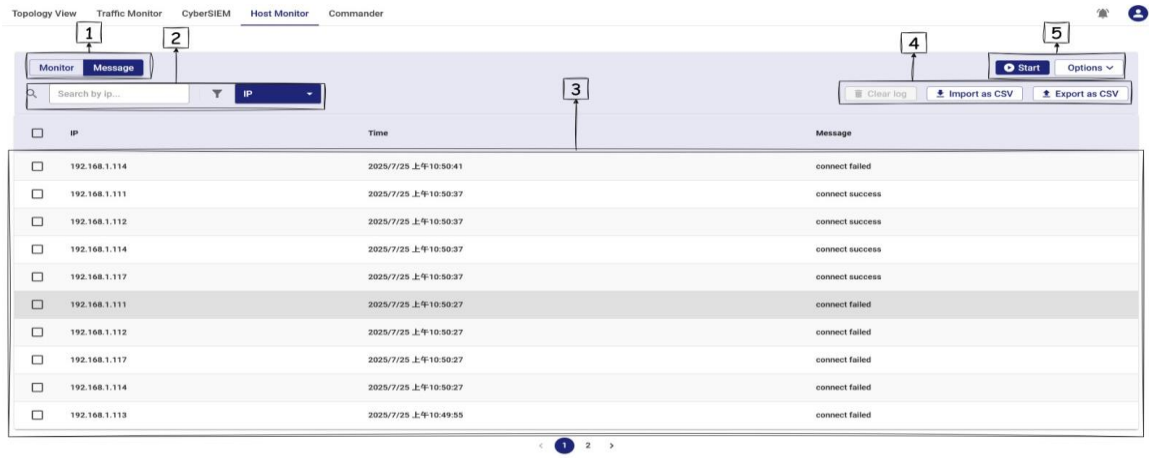


Figure 2 Message panel description

1. Panel switch button

This function button is mainly used to switch the display screen, allowing users to freely switch the display screen between Monitor and Message.

2. Search function

You can specify the field you want to search through the button at the back. After selecting it, enter the content you want to search in the input field in front. The system will search for the data in the corresponding field according to the input content and filter it to display.

3. Event display screen block

This block is mainly used to display the recorded event information. The message content is divided into three items: the IP address of the event, the time when the event occurred, and the event content.

4. Function button block

The main function buttons are mainly concentrated in this block, including the clear event button, the export event log function, and the import event log function.

5. Action execution function

This block is mainly used in the Monitor panel and has no direct connection with the Message panel.

Monitor search function

To use the Monitor search function, you must first select the field you wish to search. Currently, the available fields are IP, Status, and Description(as below picture box 1). Once selected, enter your search terms in the search box(as below picture box 2). The information below will filter to only those matching results.

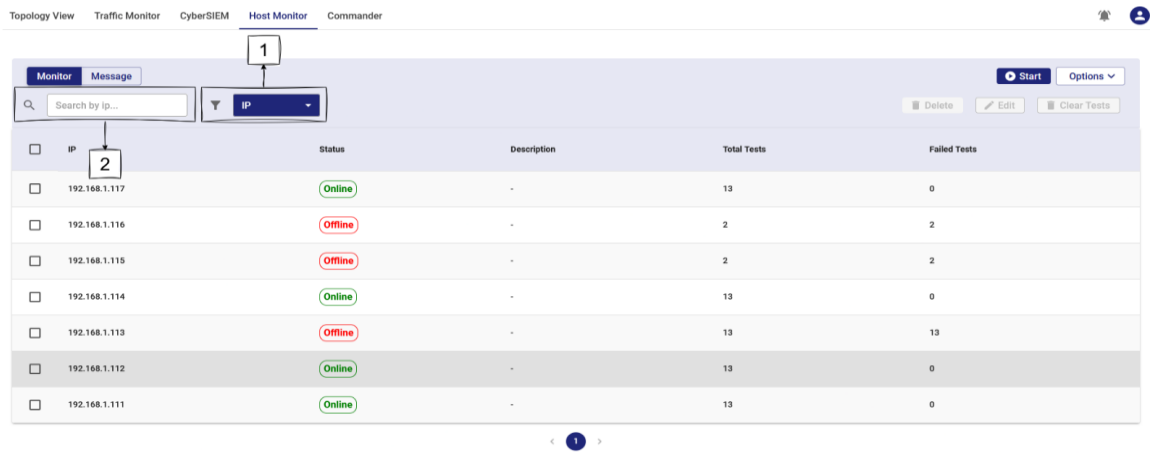


Figure 3 Monitor search function

Monitor information display panel

The Monitor information display consists of five columns. The first column is the IP field, which displays the IP address of the device being tracked. The second column is the Status field, which displays the status of the corresponding IP address. The current status is Online and Offline. The third column is the Description field, which is used to display user-added notes. The fourth column is the Total Tests field, which records the total number of tests reached. The last column is the Failed Tests field, which displays the total number of test failures for this IP address group.

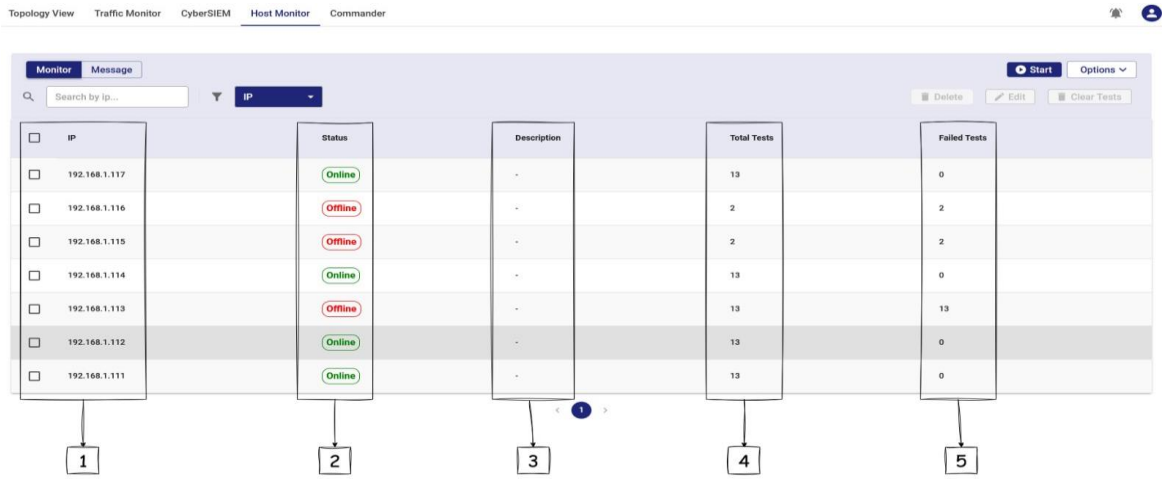


Figure 4 Information displayed in the Monitor panel

Number	Field Name	Description
1	IP	Monitored IP, all device IPs included in the monitoring content will be listed here
2	Status	Status bar, mainly displays the status of Online status and Offline status
3	Description	The description field can be filled in by the user
4	Total Tests	Displays the total number of tests
5	Failed Tests	Record the total number of test failures

Monitor function button block

There are three function buttons in the function block. The first button is the Delete button, which is used to delete the selected device IP. The second button is the Edit button, which is used to edit the Description content of the selected device. The third button is the Clear Tests button, which is used to clear the test results of the selected device.

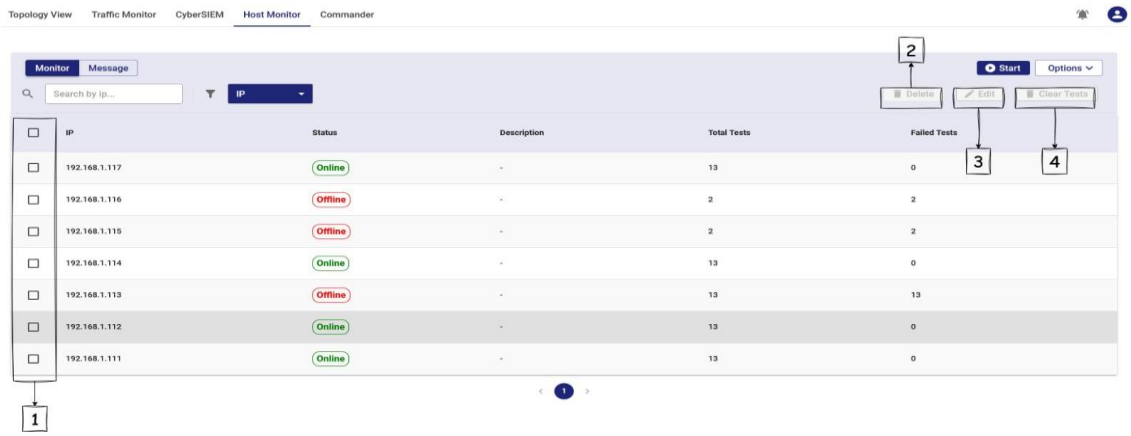


Figure 5 Function button block description

Number	Description
1	Check the device IP to be executed. You can check one or more devices to coordinate with subsequent actions.
2	Delete button, click it to delete the selected IP
3	Edit button, click it to edit the Description of the selected device
4	Clear test button, click it to clear the test results and failure records of the selected device

Monitor action execution block

This section primarily focuses on action-related functions. The Start button on the left initiates monitoring. Once started, it periodically performs an ICMP ping test on a specified IP address. Clicking it again stops the test or reaches a specified stop condition. Stopping the test does not clear the previous test results.

Under the Options button are three functions: adding a device, clearing the test history and restarting the test, and Host Monitor settings.

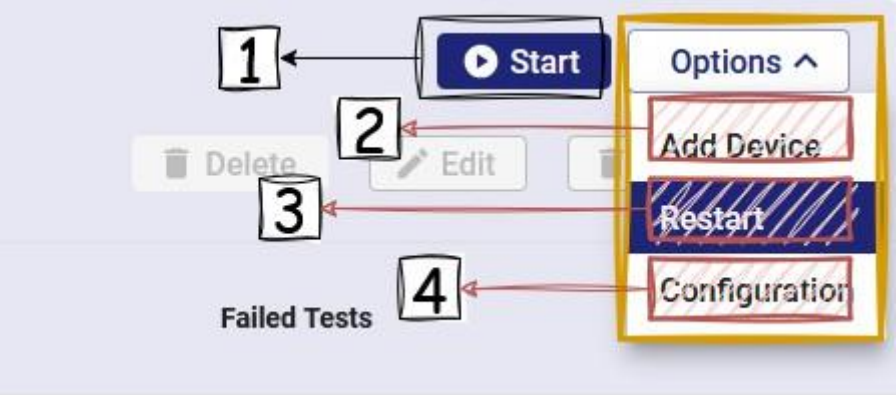


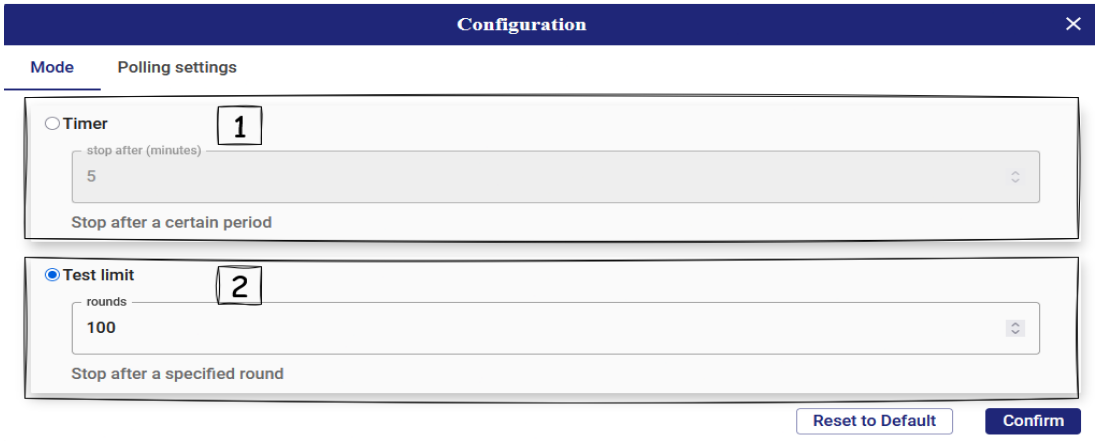
Figure 6 Host Monitor action button description

Number	Description
1	Start execution button, click the button to start the monitoring test function
2	Add device button, click it to add device IP through the interface
3	Retest button, click to clear all
4	Set button, click it to set up Host Monitor

Host Monitor Settings

The Host Monitor function settings can be divided into two parts. The first part is the Mode setting, which mainly sets the polling scheme. The other part is the Polling settings, which sets the parameters related to polling.

Picture 7 shows the Configuration settings Mode in Host Monitor. There are currently two modes. The first is Timer Mode, which uses the timer as the primary mode. The user enters the desired test time and the test will stop when the timer expires. The second is Test Count Mode, in which Host Monitor will test the specified number of times and stop when the specified number of times is reached.



Picture 7 Host Monitor Configuration settings Mode

Number	Description
1	Timer test mode, a mode based on test time, will stop testing when the test time reaches the set time
2	Test limit mode, which is based on the number of tests. When the number of tests reaches the specified number, the test will stop.

Another setting in Host Monitor's Configuration is Polling settings. Polling settings are mainly responsible for setting various parameters of ICMP Ping, including the interval time for each Ping and the timeout time for each Ping.

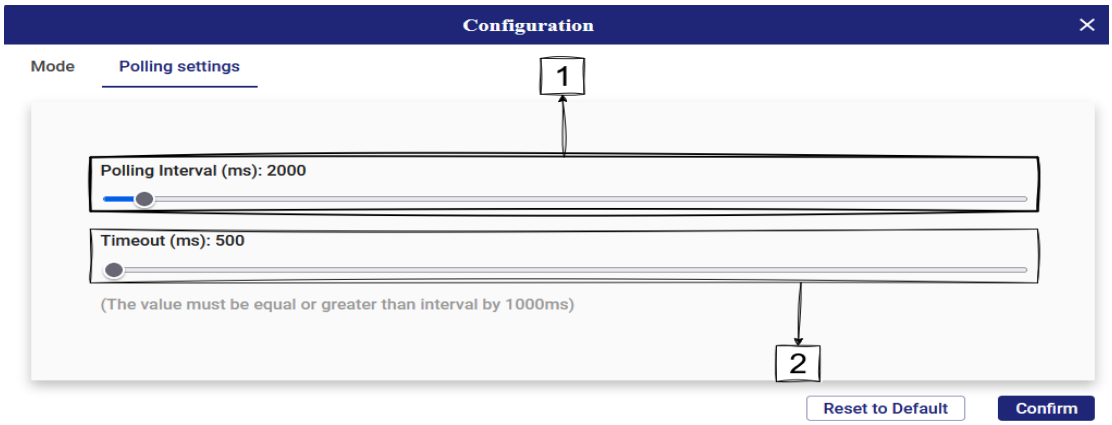


Figure 8 Configuration Polling settings screen

Number	Description
1	Polling Interval setting is used to set the time interval between each polling, and the setting unit is milliseconds (ms)
2	The Timeout setting is used to set the timeout limit for each poll. If the waiting time exceeds this value, the poll will be considered a failure. The setting unit is milliseconds.

Host Monitor New Device Interface Description

Host Monitor has its own device management interface. You can use the Add Device function to add device IP addresses to Host Monitor. This basic usage is similar to adding devices in the Topology function.

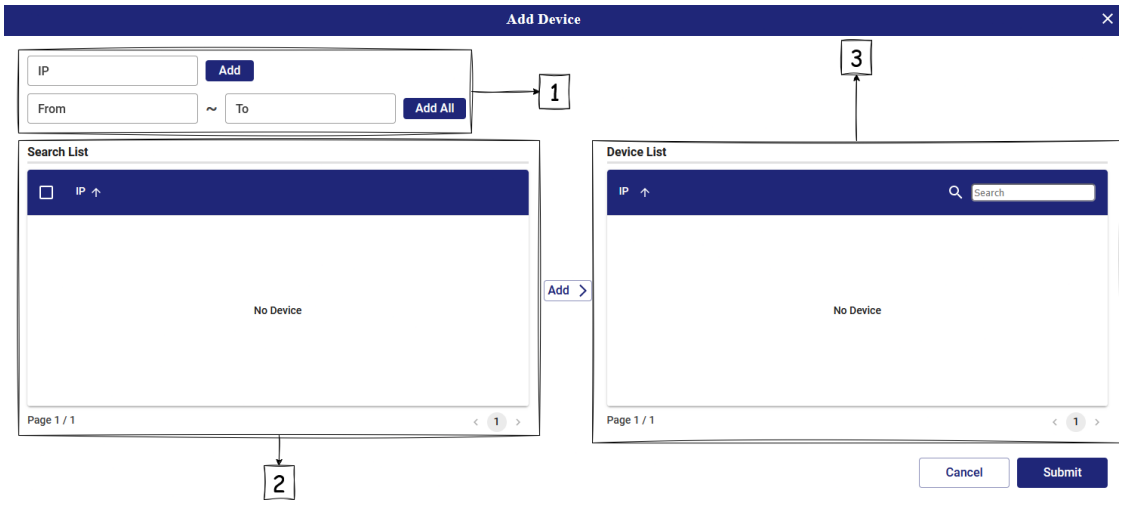


Figure 9 Add Device User Interface

Number	Description
1	The IP field block is responsible for inputting IP functions, providing single IP input or IP range input
2	Search List block, responsible for displaying the list of IP addresses to be added to the test
3	The Device List block is responsible for formally determining the list of devices to be included in the Host Monitor test function

The Add Device function works by first entering the device IP address you want to add in the IP settings area. You can add multiple IP addresses by specifying a range or a single IP address. The results will be displayed in the Search List area. Then, in the Search List area, select the devices you want to add to the test list. Once selected, click the Add button to move the selected IP addresses to the Device List screen. After confirming that the IP address you want to test is correct, click the Submit button to officially add the test IP to Host Monitor.

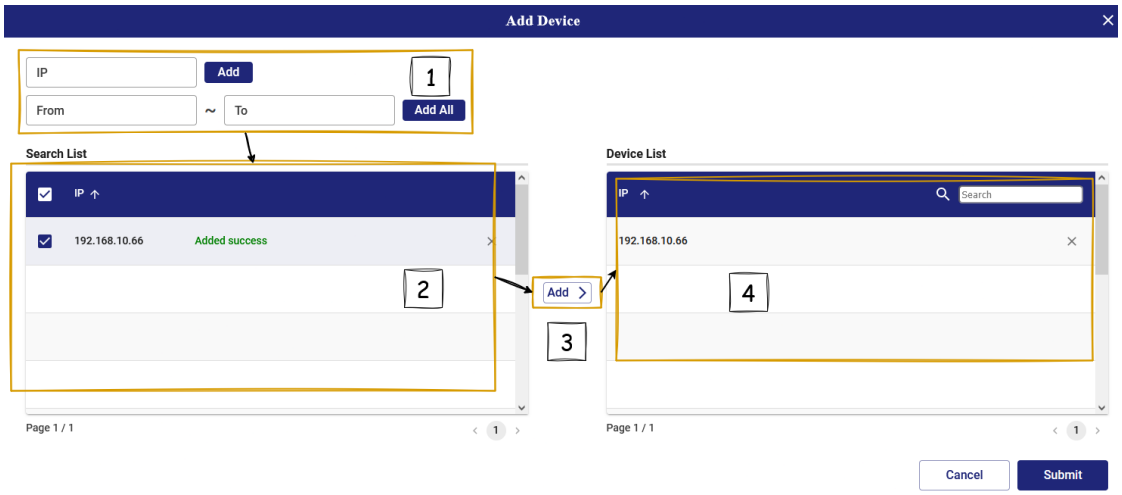


Figure 10 Add Device operation process

Number	Description
1	Enter the device you want to search for. You can add it to the list by entering a single IP or entering the IP range you want to search for.
2	The search list contains the IP addresses added in the previous step. In this step, select the IP addresses you wish to add to Host Monitor.
3	Click the Add button to copy the devices selected in the search list to the device list.
4	The IP address in the device list is the one you'll be adding to Host Monitor. Once you've confirmed everything is correct, click Submit to add the IP address to Host Monitor.

2.9 Commander

The primary function of Commander is to perform firmware upgrade and configuration backup/restore operations for ORing standard devices (currently limited to S12/K12 and 3000 series models).Commander supports both single-device and multi-device operations, and can simultaneously execute these actions on devices of different or identical models.

Commander Interface Overview

The device list displayed in Commander is mainly composed of devices included in the **Topology File**.

Therefore, before using Commander, make sure that the devices already exist in a Topology File. Devices can be stored in the same file or across different files, but Commander cannot read from unopened files.

If a device to be managed by Commander is not yet present in an existing Topology File, the user must first create a Topology File and add the target device(s). After that, when entering the Commander interface, all devices from the selected Topology File will be shown.

Commander provides two display modes:

1. **OID-based view**
2. **System Name-based view**

The display mode can be switched using the toggle button at the top of the interface. When switched to **System Name mode**, users can filter devices by selecting a specific system name or by entering keywords in the **search bar**.

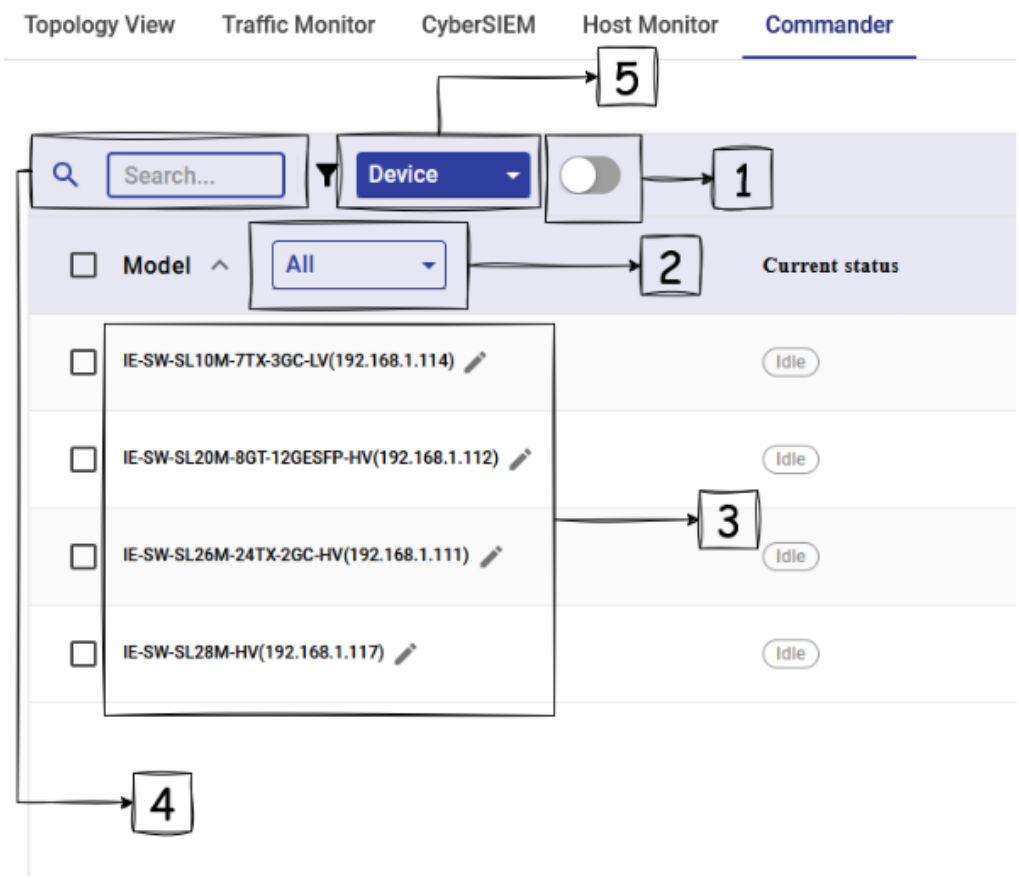


Figure 1: Commander Interface Overview

Number	Description
1	Toggle button: Switches between OID-based and System Name-based device lists.
2	Model filter button: Available only in System Name view. Used to filter and display devices of a specific model.
3	Device list area: Displays all selectable devices.
4	Search bar: Allows entering keywords for quick device search.
5	Search field selector: Defines which column to search against.

Before executing any Commander actions, device-related settings must be configured.

- **Individual device settings** can be modified via the edit button next to each device.
- **Batch settings** can be applied using the **Apply Settings** button at the top.

⚠ Note: The **Apply Settings** option can only be used on multiple devices if they are of the **same model**. If different models are selected simultaneously, this function will be disabled.

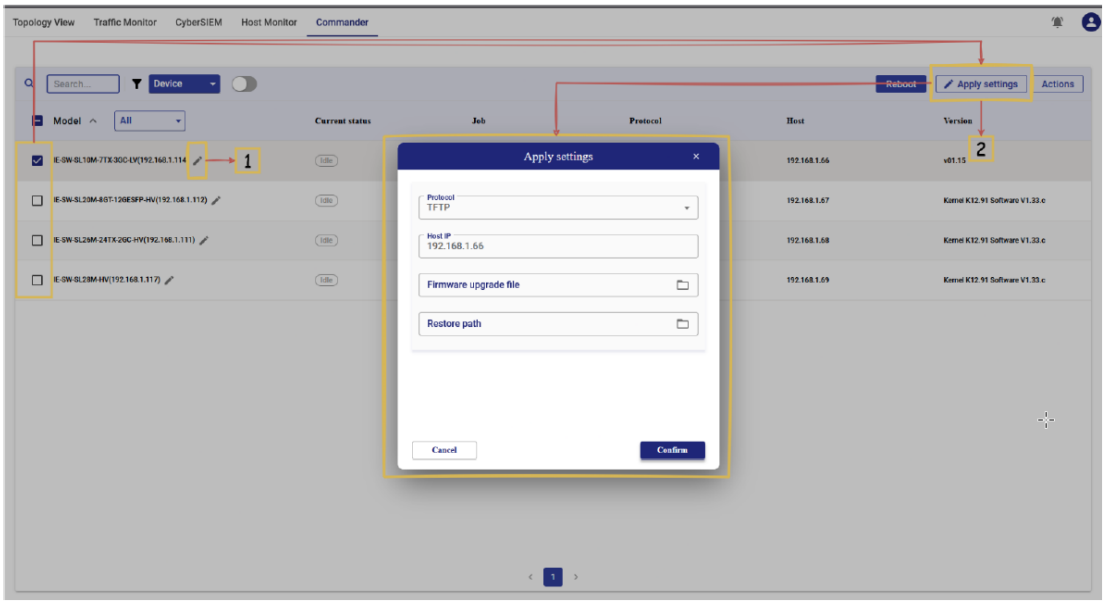


Figure 2: Commander Settings Overview

Number	Description
1	Individual setting button: Configure settings for a single device.
2	Apply Settings button: Allows batch configuration of multiple devices (only available if all selected devices are the same model).

Firmware Upgrade Function

To use the **Firmware Upgrade** function, the following parameters must be configured:

- Transmission protocol
- Host server IP address
- Firmware file

Currently (version **5.1.1**), Commander only supports **TFTP** as the transmission protocol, Therefore:

1. Select **TFTP** as the protocol.
2. Enter the **TFTP server IP address**.
3. Choose the firmware file to be uploaded.

Since Open Vision Pro does not include a built-in TFTP service, users must **set up an external TFTP server**

Once the settings are completed, clicking **Action** → **Firmware Upgrade** will show a confirmation dialog. Two display modes are available:

- **Simplified View**: Displays only basic information, with tooltips providing extra details.
- **Detailed View**: Displays all relevant information.

After verifying correctness, click **Confirm** to execute.

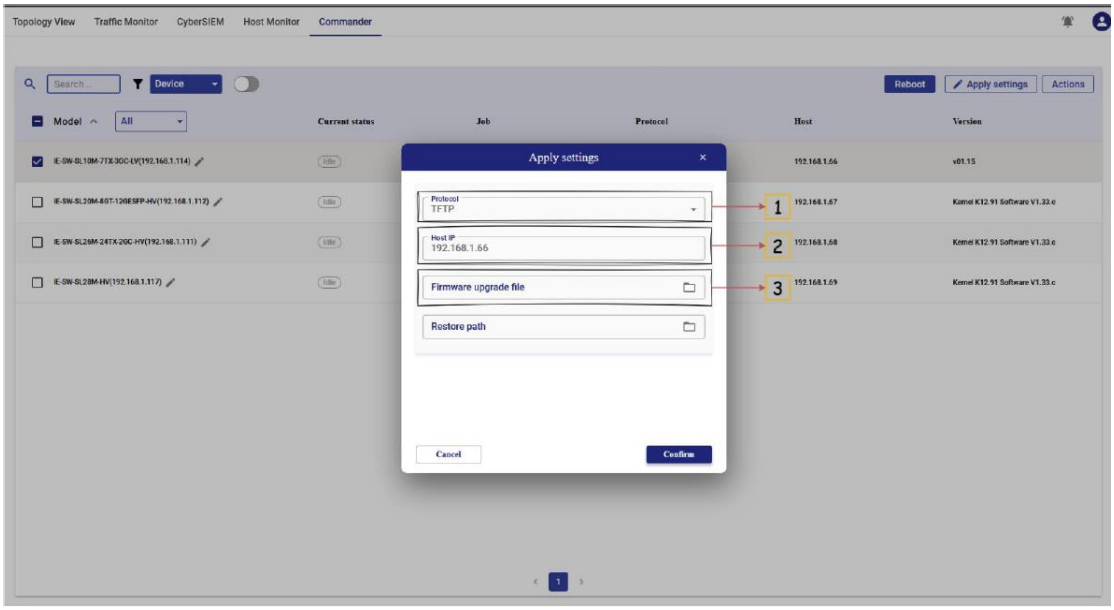


Figure 3: Firmware Upgrade Setting Screen

Number	Description
1	Transmission protocol (only TFTP supported)
2	TFTP server IP
3	Firmware file selection

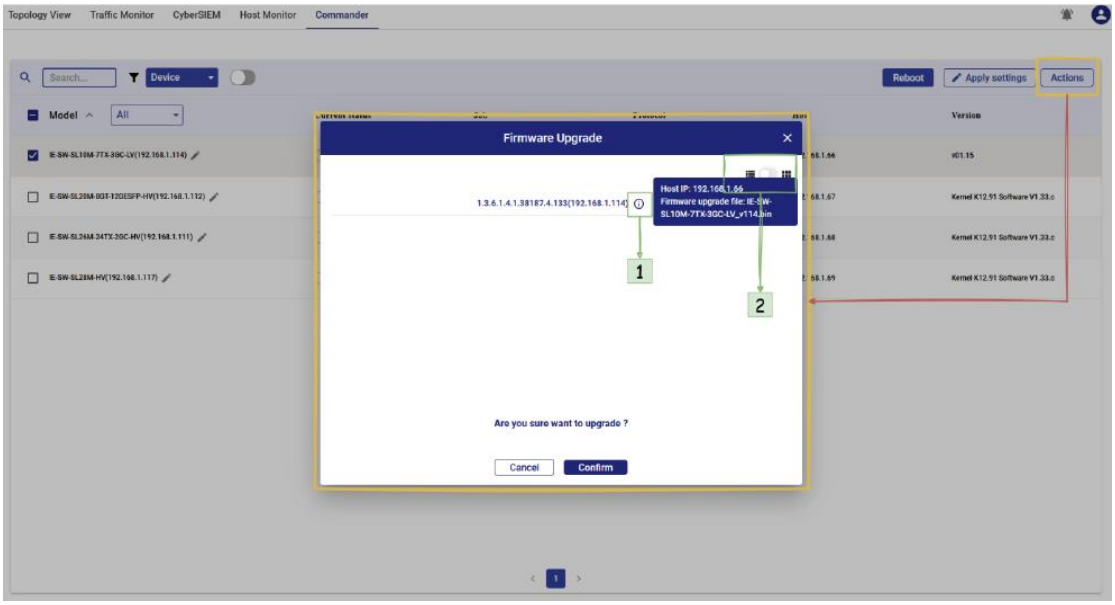


Figure 4: Firmware Upgrade – Simplified Info Panel

Number	Description
1	Info tooltip: Hover to display additional device details.
2	Panel toggle button: Switch between simplified and detailed views.

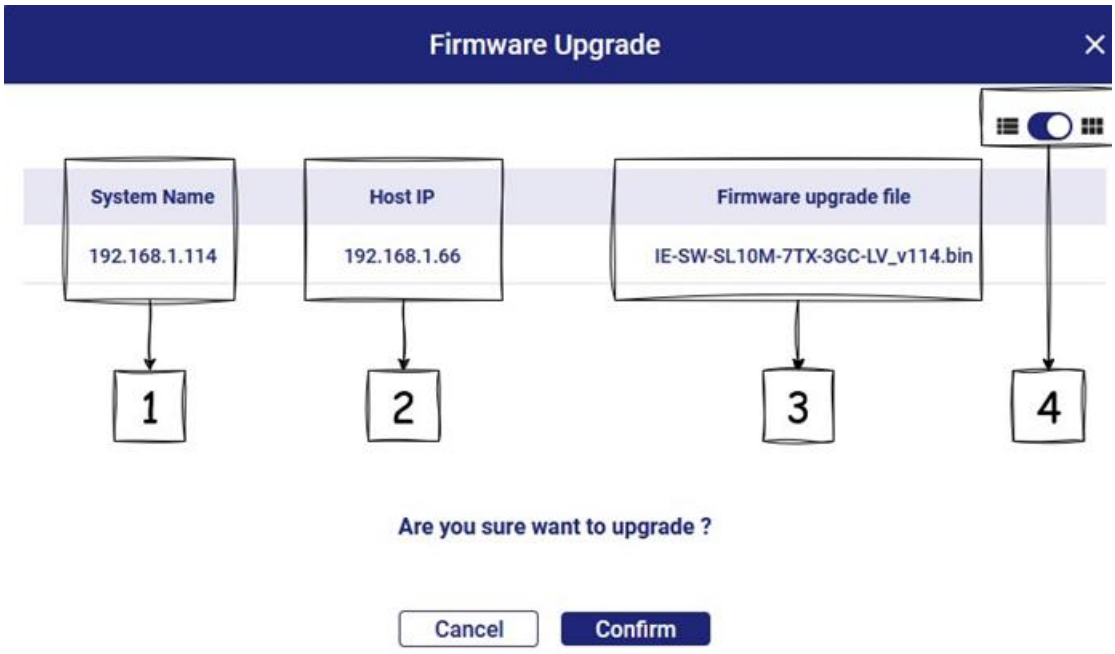


Figure 5: Firmware Upgrade – Detailed Info Panel

Number	Description
1	Device IP
2	Server IP(TFTP)
3	Firmware file
4	Panel toggle button

Execution states include:

Status	States
Pending	Waiting in queue
Running	Currently executing
Success	Completed successfully
Failed	Execution failed

⚠ After completion, devices must be **rebooted** to finalize the firmware update. Selected devices can be rebooted via the **Reboot** button.

Configuration Backup Function

To use the Configuration Backup function, configure the following:

- Transmission protocol (currently only TFTP)
- Host server IP address

⚠ File name does not need to be specified manually. Commander automatically generates the backup file name as: systemName_ip_time.cfg

where systemName is the device's system name, ip is the device's IP, and time is the timestamp. As with firmware upgrade, users must set up an e**xternal TFTP server.**

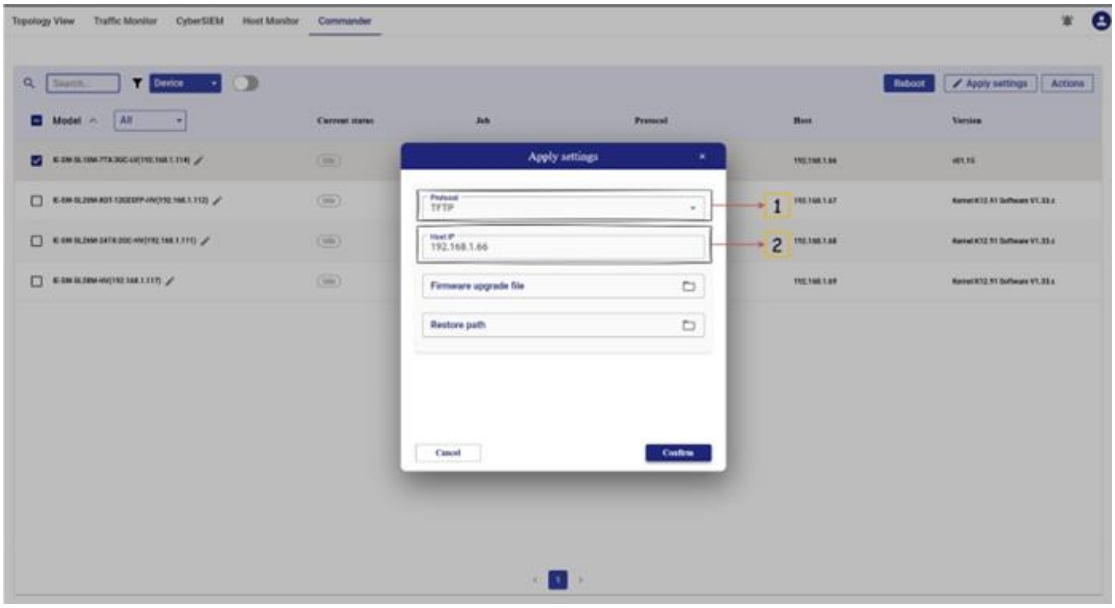


Figure 6: Configuration Backup Setting Screen

Number	Description
1	Transmission protocol (TFTP only)
2	TFTP server IP

Before execution, Commander displays a confirmation panel with both **simplified** and **detailed** views.

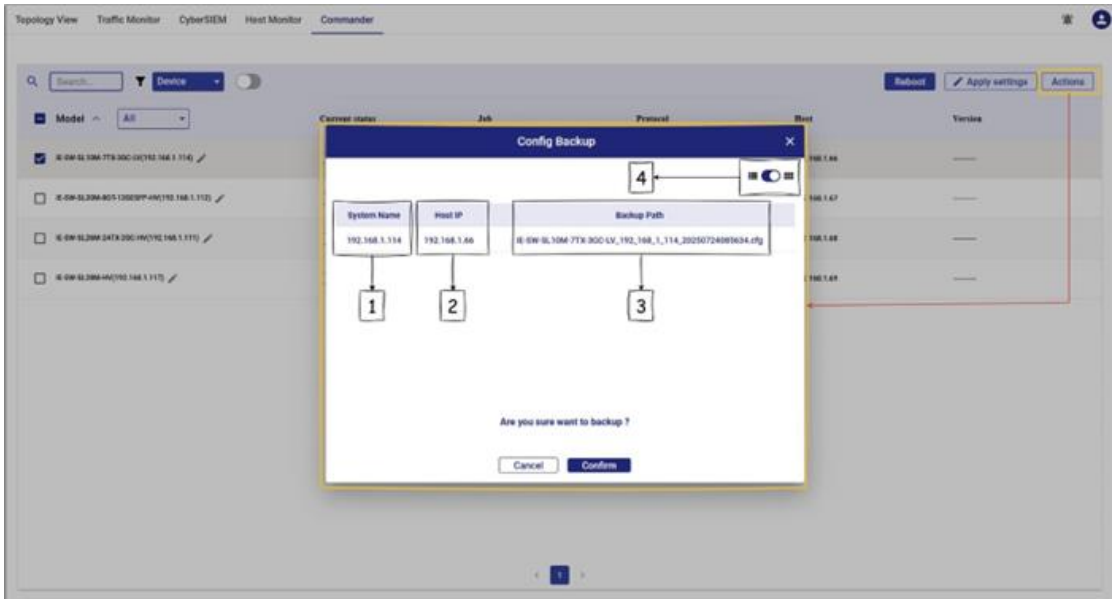


Figure 7: Backup Detailed Confirmation View

Number	Description
1	Device IP
2	Server IP
3	Backup file name
4	Panel toggle button

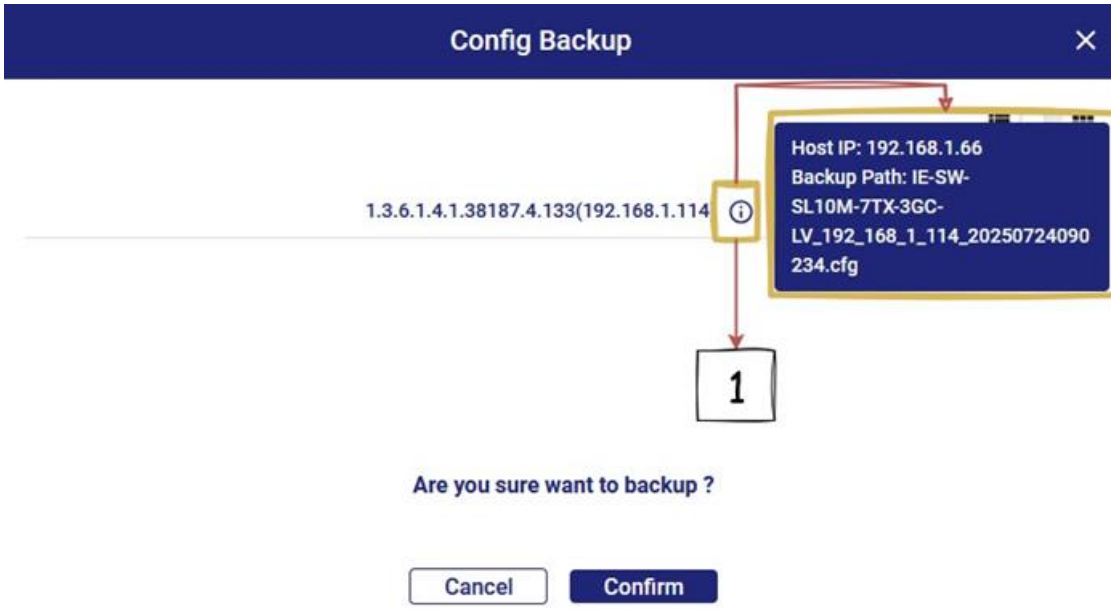


Figure 8: Backup Simplified Confirmation View

Execution states are the same as firmware upgrade (Pending, Running, Success, Failed).

Configuration Restore Function

To use the **Configuration Restore** function, configure the following:

- Transmission protocol (currently only TFTP)
- Host server IP address
- Configuration file to restore

As with the other functions, users must prepare an **external TFTP server.**

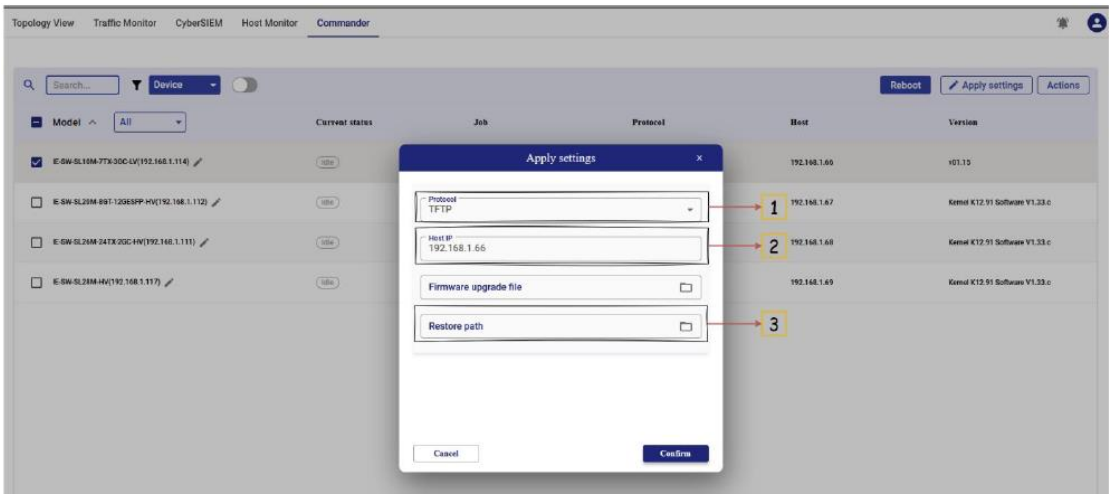


Figure 9: Configuration Restore Setting Screen

Number	Description
1	Transmission protocol (TFTP only)
2	TFTP server IP
3	Configuration file to restore

Before execution, Commander displays a confirmation screen with both simplified and detailed views.

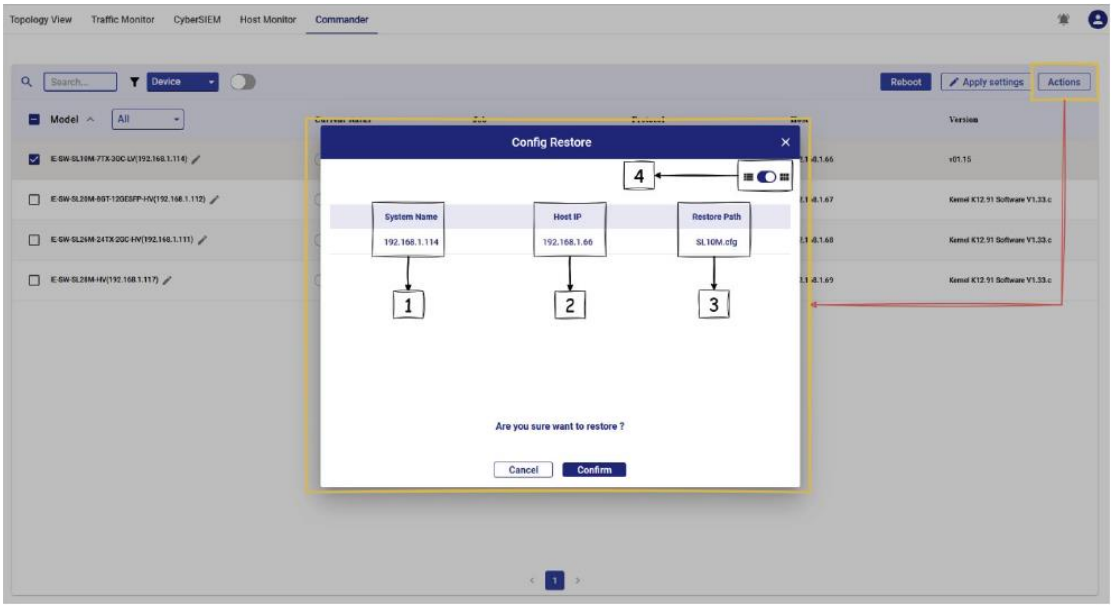


Figure 10: Restore Detailed Confirmation View

Number	Description
1	Device IP
2	Server IP(TFTP)
3	Configuration file name
4	Panel toggle button

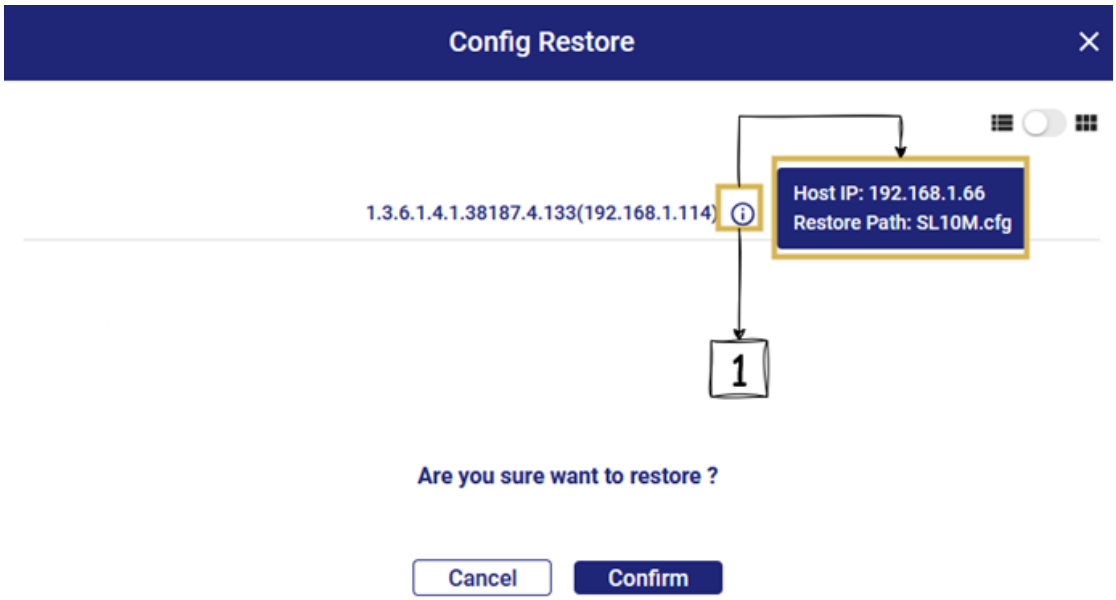


Figure 11: Restore Simplified View

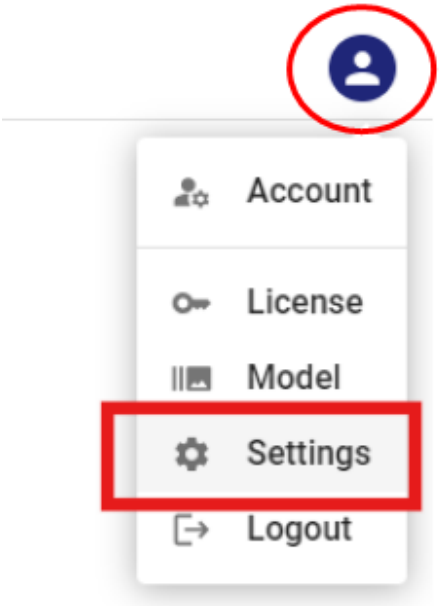
Execution states: Pending, Running, Success, Failed.

⚠ After restoration, devices must be rebooted for the configuration to take effect. Selected devices can be **rebooted** via the Reboot button.

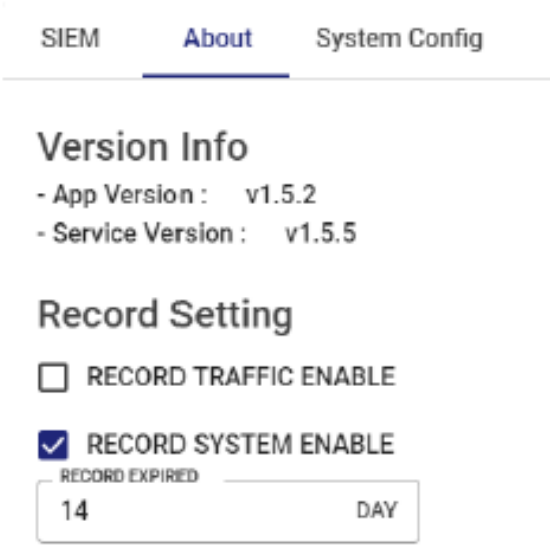
System Configuration

3.1 System Setting

System settings mainly include: System Config, About and SIEM Page
Open the system settings window, as shown below

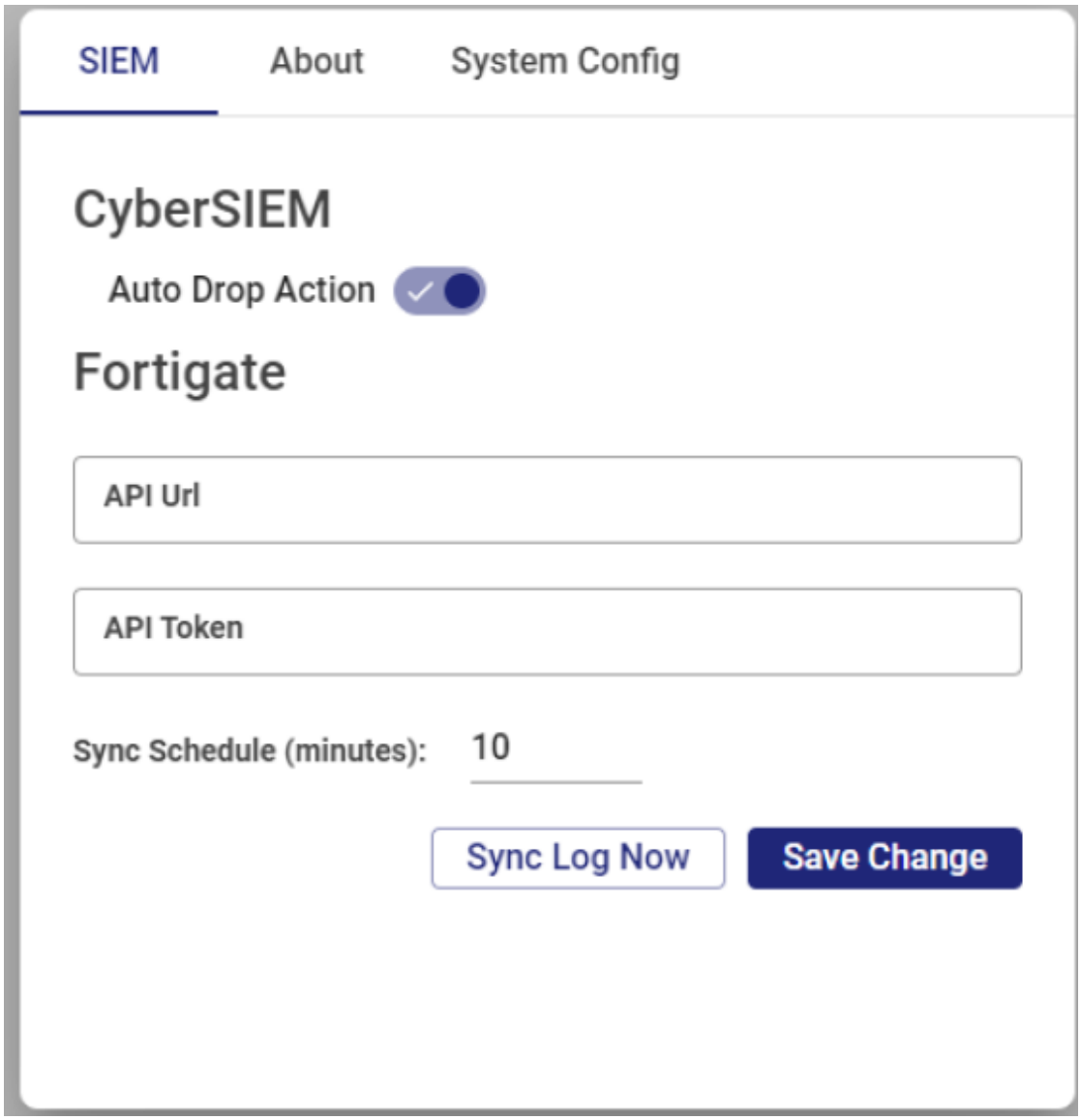


Setting interface :



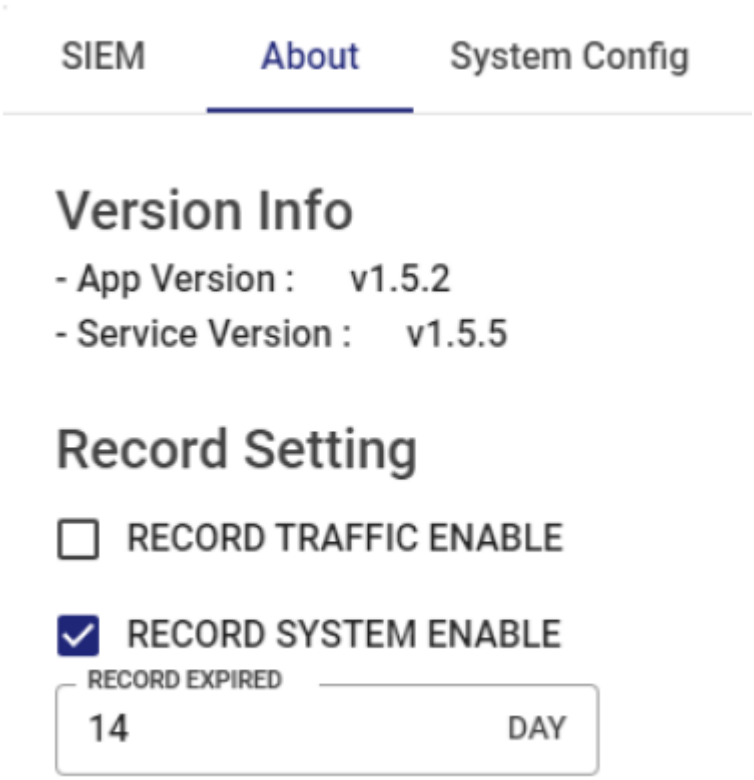
SIEM

- **Auto Drop Action :** After being notified of an abnormal attack, the system will automatically lock the abnormal port.
- **API Url :** Enter the Fortigate device address
- **API Token :** Enter the key for Fortigate device connection
- **Sync Schedule (minutes) :** Set the synchronization interval
- **Sync Log Now :** Perform data synchronization refresh immediately



About

- **Version Info :** Contains APP and service version information
- **RECORD TRAFFIC ENABLE:** When turned on, it can actively monitor and record traffic information.
- **RECORD SYSTEM ENABLE :** After turning it on, you can record system information and choose the number of days to keep the log.



System config(Polling, SNMP)

- **Auto Polling:**

Provides adjustable topography scan interval

Provides settings for the number of Retry times when a single point scan is abnormal.

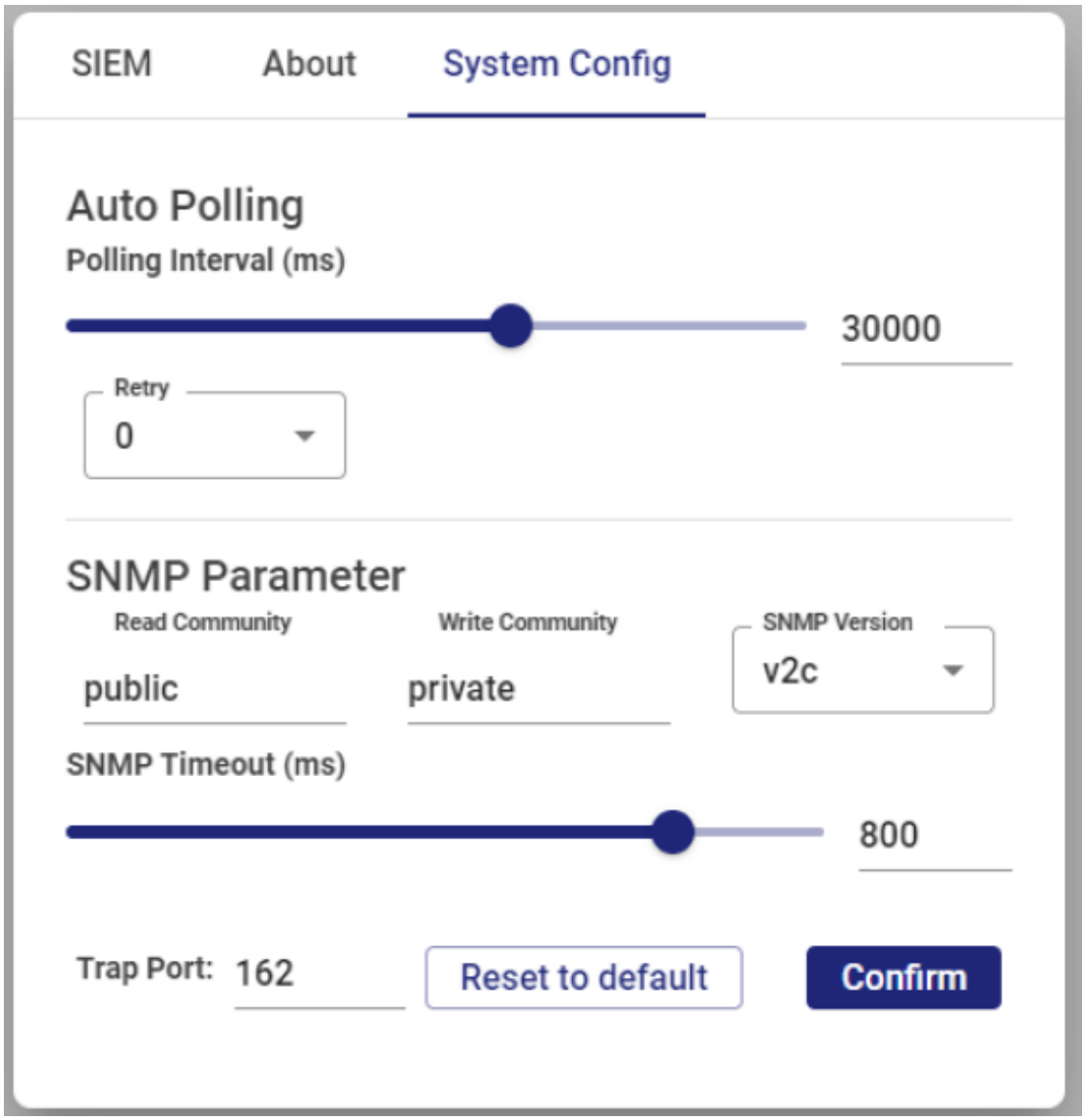
- **SNMP Parameter:**

Provides basic SNMP v1/2 configuration interface

Adjustable SNMP Timeout

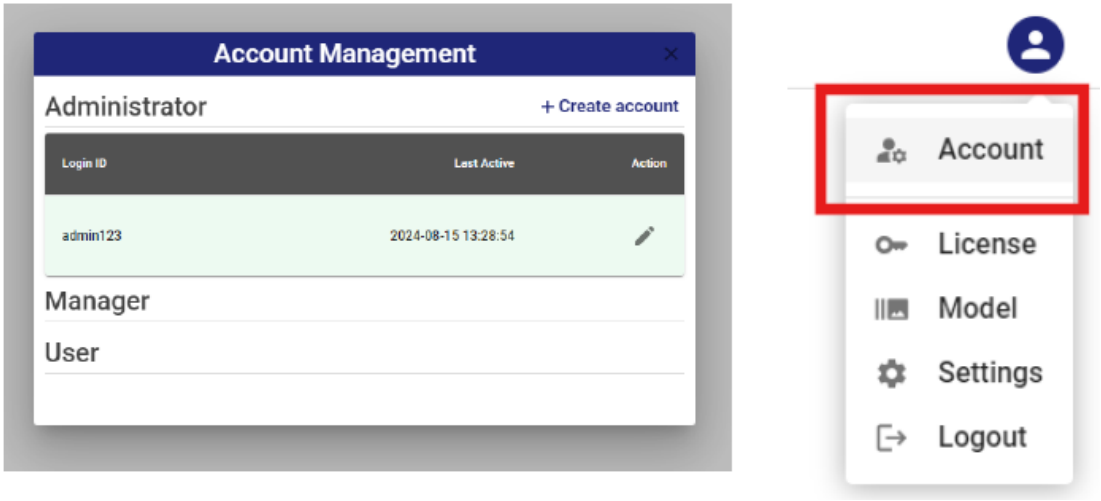
Trap port can be changed

Reset to default: Restore SNMP initial settings with one click



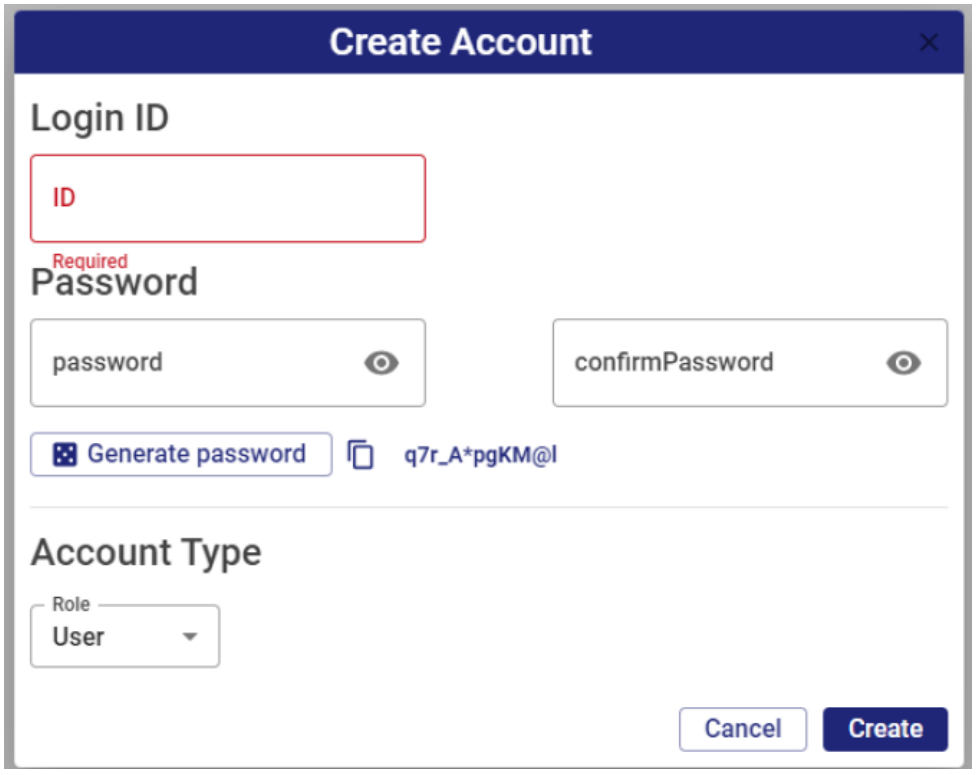
3.2 Account Manager

Administrators are allowed to create multiple user accounts. The accounts are divided into three levels: Admin/Manager/User. The details are as follows:



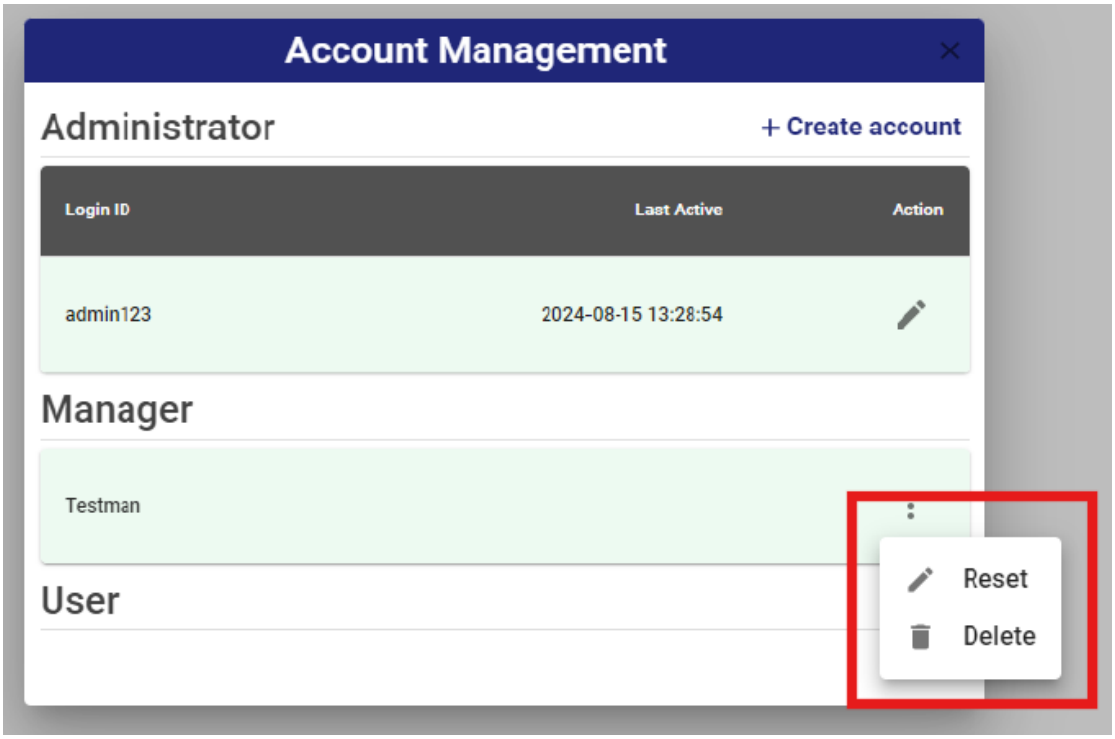
Create Account

Only the Administrator with the highest authority can create Manager and user accounts

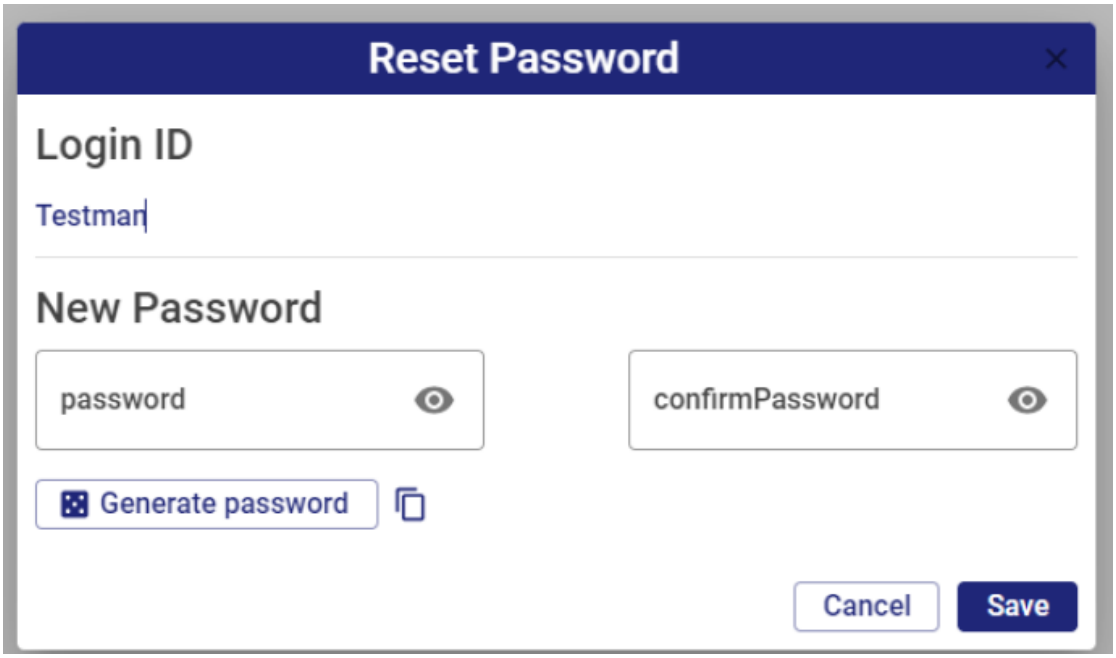


Edit account

Click the options icon on the right side of the account you just created. You will see the delete and reset buttons.



Clicking Reset will pop up the Reset Password form. After resetting, press SAVE.



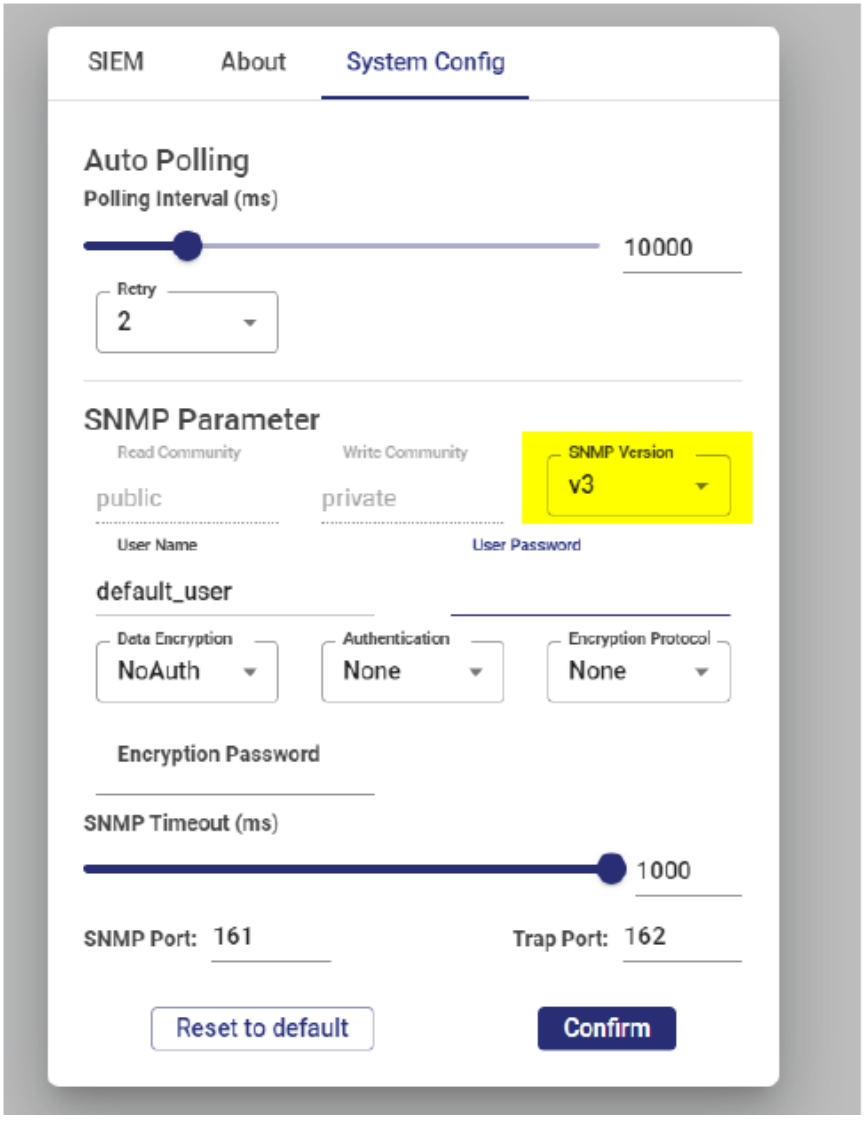
About Account Type

	Admin	Manager	User
Create / remove account	Y	N	N
System setting	Y	Y	N
backup config file	Y	Y	Y
Upload config file	Y	Y	N
Project view	Y	Y	Y

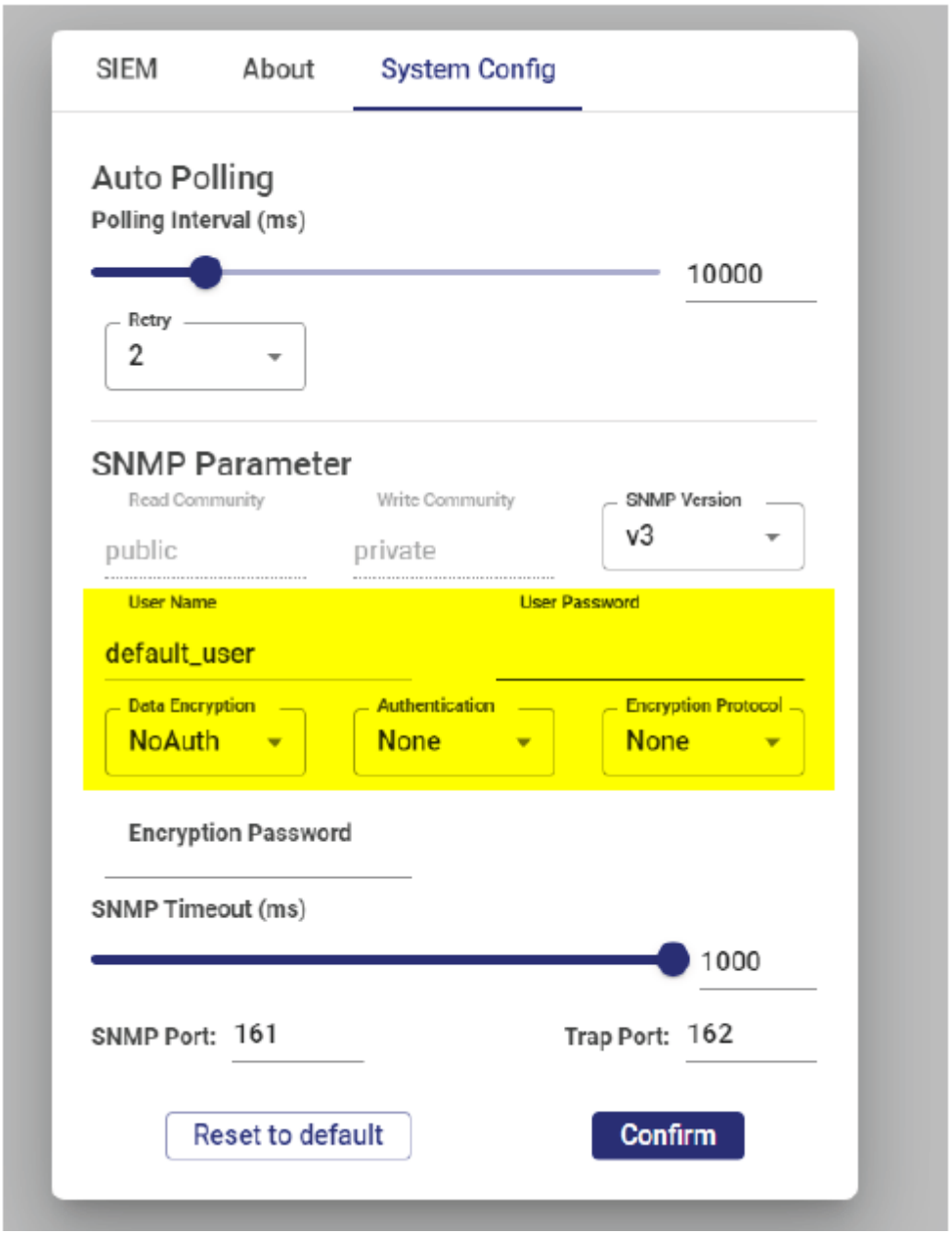
3.3 SNMP V3

OPEN VISION PRO uses SNMP V2c by default for communication between the software and the device. At the same time, SNMP VISION PRO also supports the higher specification SNMP V3 protocol. You can follow the instructions below to enable SNMP V3.

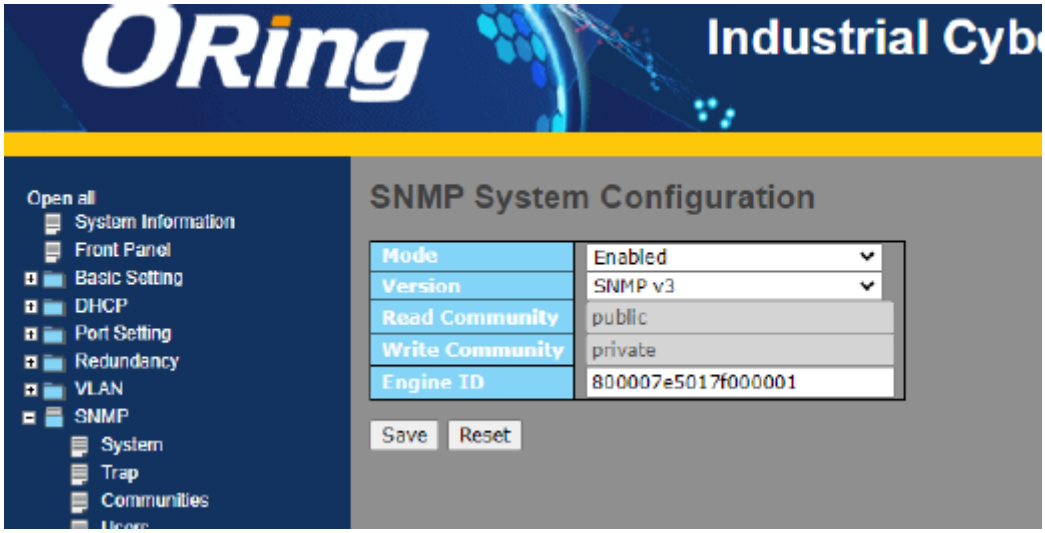
First setting version to V3

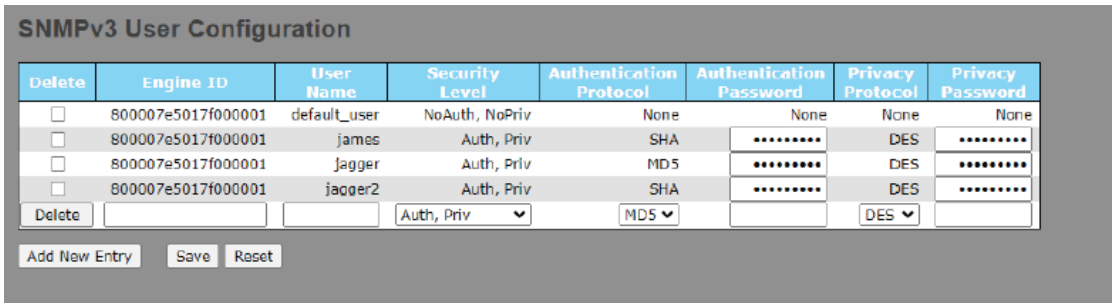


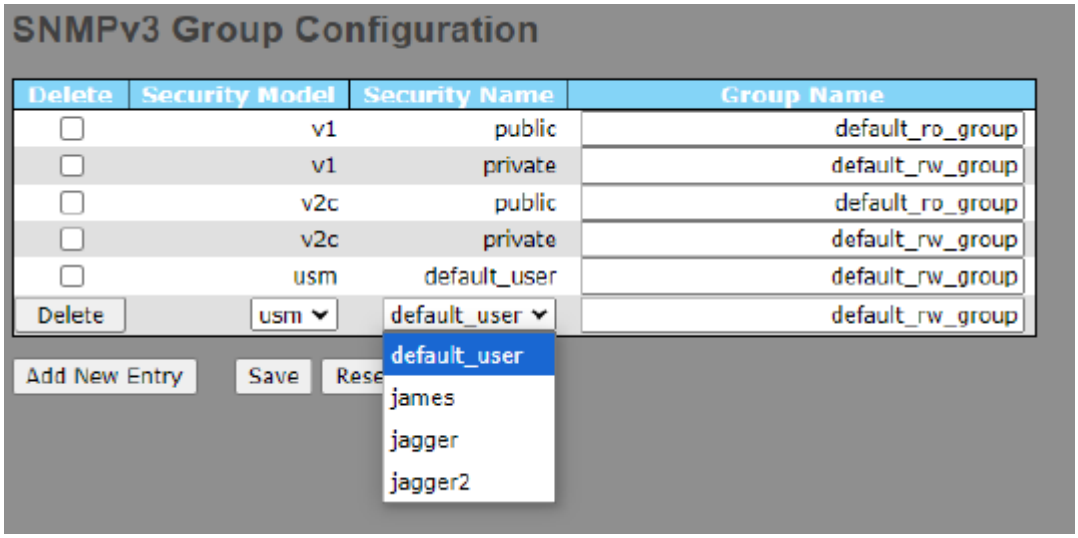
Define SNMP V3, User name / password and Encryption Protocol .



The managed device also needs to enable SNMP V3 and import the same configuration.





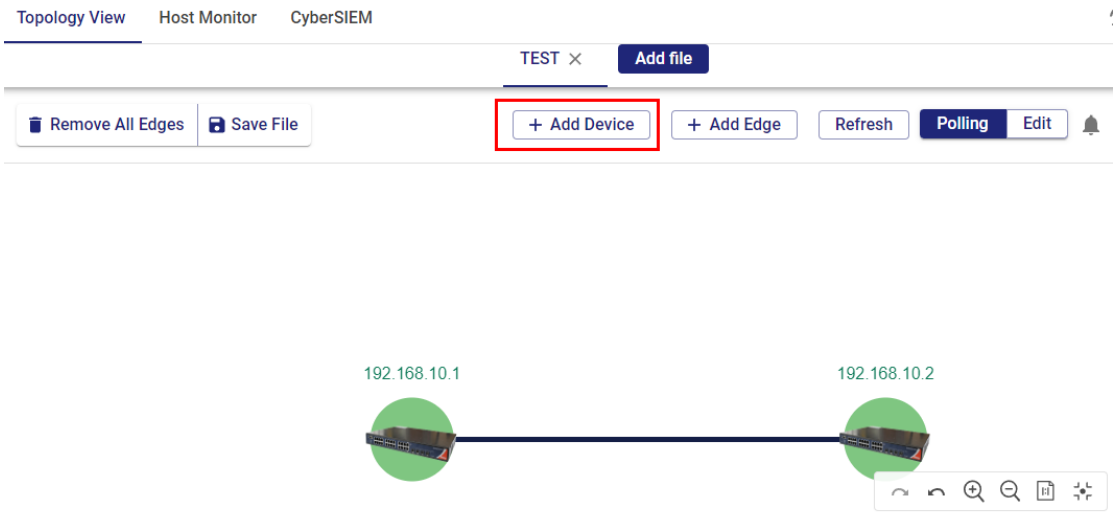


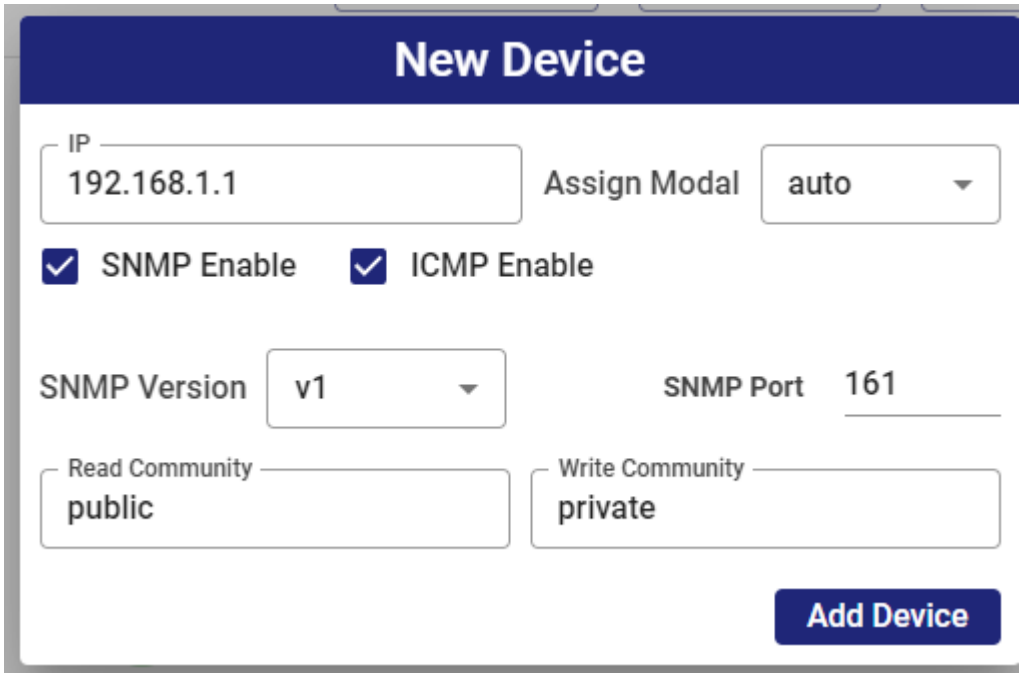
3.4 Adding new equipment to current project

OPEN VISION Pro supports adding new equipment to existing projects, making project planning more flexible. The detailed settings are as follows:

Add Device

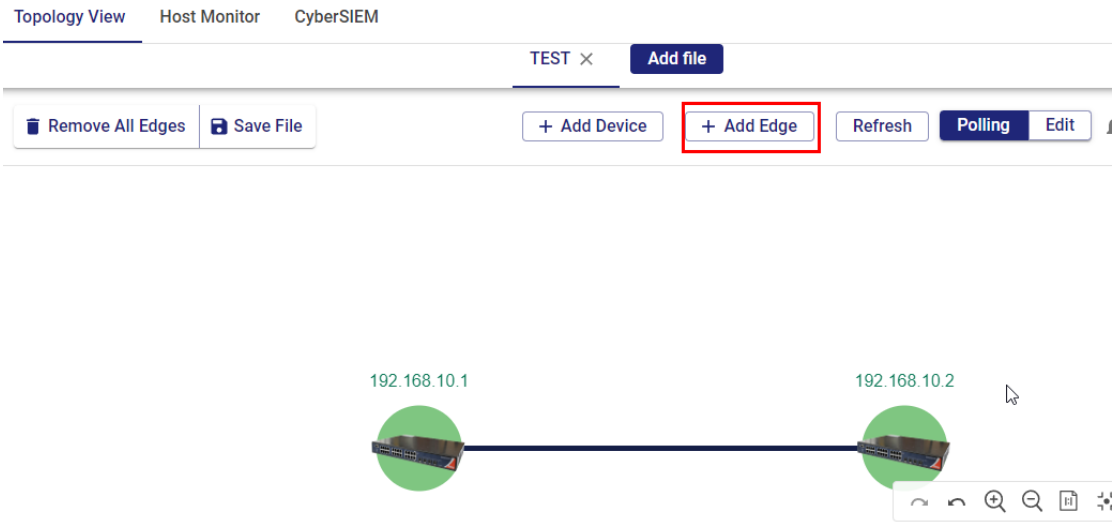
Allows users to add a single device

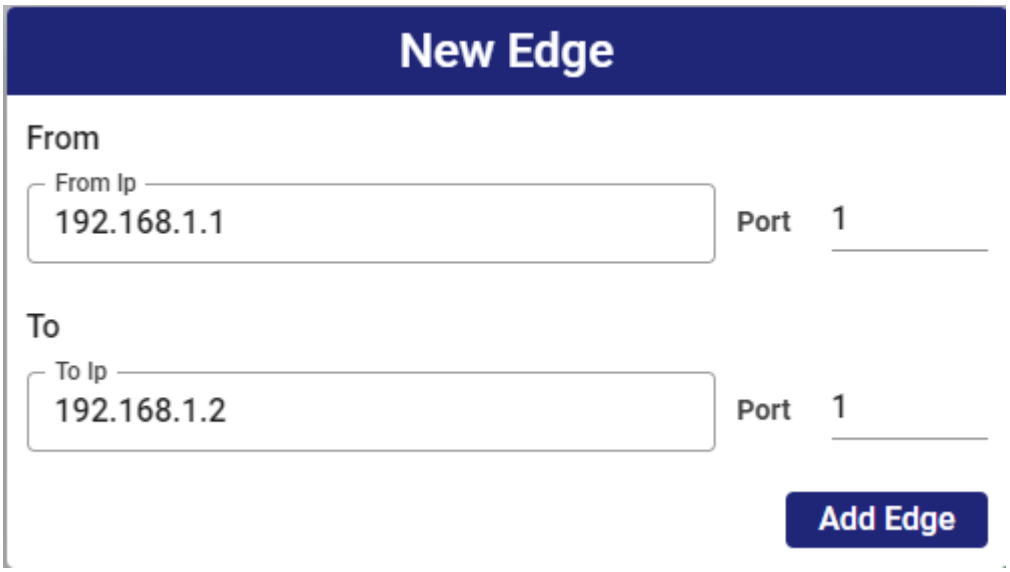




Add Edge

Allow users to add new connections

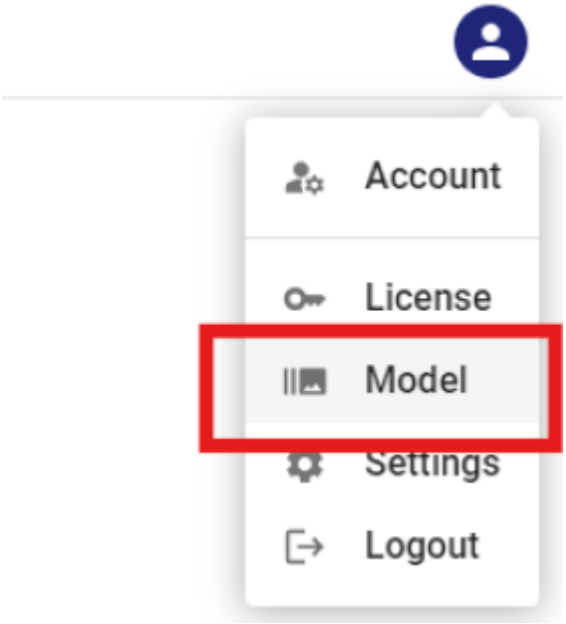




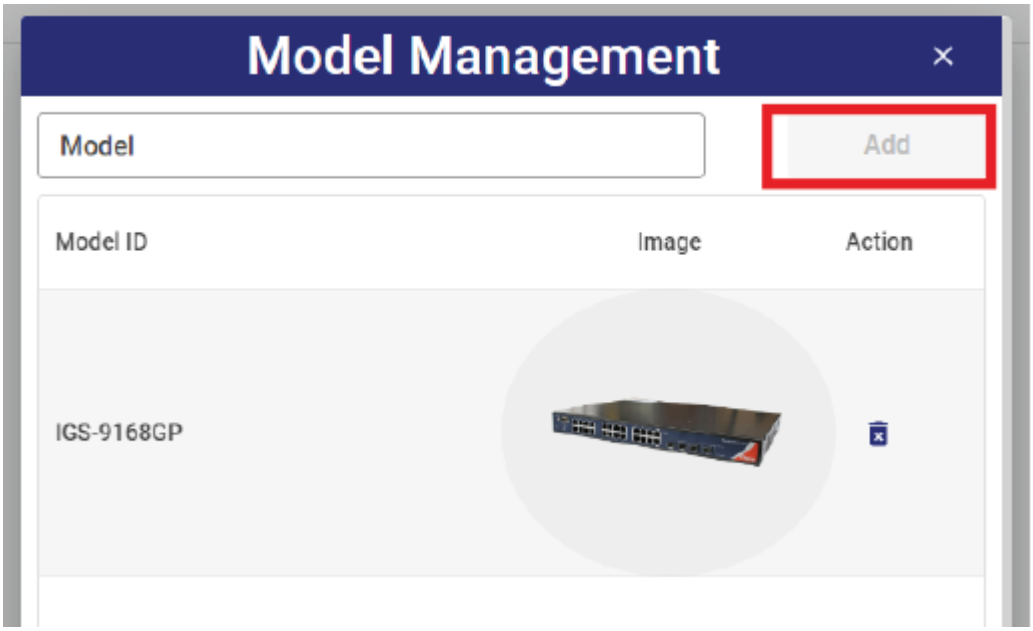
3.5 Model Manager

Allow users, devices that already exist in the project, detail setting as below .

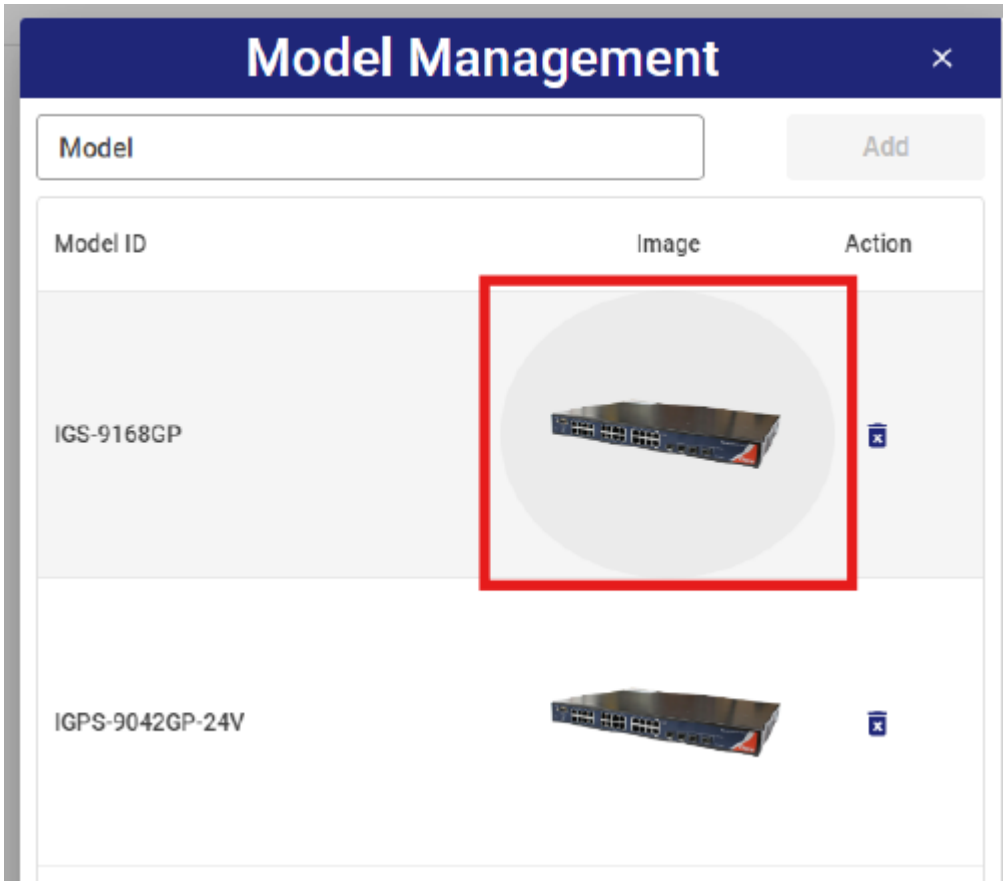
Click on the avatar in the upper right corner of the home screen > Settings



Enter the model name you want to add and click Add to add a new item.



Confirm the model project you just added in the list and click the Image icon to change the image.



You can also click the trash can on the right to delete the item