D-Link®

2025 | Business Class Networking

NUCLIAS HYPER
User Manual

V 1.00

nuclias hyper

Table of Contents

Product Overview

D-Link Nuclias Hyper is a versatile, convenient software solution for administrators to manage wireless devices throughout the network from a central point.

Recommended System Requirements

	Large Scale Install	Small Scale Install
Recommended Processor	Intel 12th i7 or later	Intel 12th i5 or later
Recommended RAM	32G	16G
Recommended Storage	4TB	1TB
Ethernet NIC	Gigabit Ethernet card	Gigabit Ethernet card
Monitor resolution	1080P	1080P
Platform	Windows Server 2019 (64bit)* Linux Ubuntu (22.04 or above)	Windows 11 Pro (64bit)* Linux Ubuntu (22.04 or above)
Browser for Nuclias Hyper mgt.	Edge, Chrome and Safari	Edge, Chrome and Safari

[1] Recommended uplink bandwidth: 20 Mbps for larger scale, 10 Mbps for smaller scale.

*Nuclias Hyper is a Linux-based version running on Docker, so it can run on Docker on Windows.

Software Installation

In the following section, we'll discuss the software that needs to be installed to successfully run the Nuclias Hyper application.

The following software applications must be installed in the following order:

- The **Nuclias Hyper Server** application. This is the main application that will be responsible for the day-to-day wireless network management and maintenance tasks.

Nuclias Hyper Server Installation

Linux OS Installation

Install Docker

Please execute the following command to install.

```
$ sudo apt update
$ sudo apt upgrade
$ sudo apt install curl
$ sudo apt install docker.io
$ docker -v <if install OK, will get version by this command>
```

Install Docker Compose

Compose is available for the Windows or 64-bit Linux operating systems.

Prerequisites

Docker Engine must be installed prior to the installation of Compose.

- On Windows OS, Docker Compose is included in the desktop installation.
- On Linux OS, the Docker software for your specific OS must first be installed. Once installed, continue with the Compose installation process.

Installing Compose on Linux

On Linux, the Docker Compose binary can be downloaded from the Compose repository release page found on GitHub. See the following instructions.
Check the latest Docker Compose from Github at https://github.com/docker/compose.

```
$ sudo curl -L "https://github.com/docker/compose/releases/download/v2.37.0/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose
```

NOTE: To install a different version of Compose, substitute the variable 2.37.0 with the preferred version of Compose.

Apply executable permissions to the aforementioned binary. See the following command:

```
$ sudo chmod +x /usr/local/bin/docker-compose
```

Once the installation is complete, verify it by checking its version number. See the following command to verify the version of the Compose binary.

```
$ sudo docker-compose -v
Docker Compose version v2.37.0
```

Tarball Installation Nuclias Hyper

Once the package is downloaded, make a note of its location for later use. In this example, the tar package (nuclias-hypert.tar.gz) is downloaded in an archived form (GZ) to the Home folder.
Once in the correct directory, use the ls command to view a list of available files in the directory.
To extract the package, type in the following command and the respective password for the user.

```
$ ~ tar zxvf nuclias_hyper.tar.gz
```

The command will extract the contents of the package. The following results will appear.

```
NucliasHyper/
NucliasHyper/init.sh
NucliasHyper/config/
NucliasHyper/config/nucliasConnectSystemconfig.json
NucliasHyper/config/nucliasHyperSystemconfig.json
NucliasHyper/config/nucliasConnectAppconfig.json
NucliasHyper/config/ssl.conf
NucliasHyper/docker-compose.yml
NucliasHyper/docker-entrypoint-initdb.d/
NucliasHyper/docker-entrypoint-initdb.d/template_config_view.sql
NucliasHyper/docker-entrypoint-initdb.d/sFlow_NicVendorMapping.sql
NucliasHyper/docker-entrypoint-initdb.d/01_schema.sql
NucliasHyper/docker-entrypoint-initdb.d/Base_CommonData.sql
NucliasHyper/docker-entrypoint-initdb.d/00_entrypoint-initdb.sql
NucliasHyper/docker-entrypoint-initdb.d/sFlow_mapping_DSCP.sql
NucliasHyper/docker-entrypoint-initdb.d/sFlow_mapping_application.sql
NucliasHyper/docker-entrypoint-initdb.d/...
NucliasHyper/images/
NucliasHyper/images/web.tar
NucliasHyper/images/postgredb.tar
NucliasHyper/images/NucliasHyper.tar
NucliasHyper/images/core.tar
NucliasHyper/README.md
```

The Nuclias Hyper package is now extracted and ready for installation.
Navigate to the directory containing the init.sh shell file and type in the following command to initialize the Nuclias Hyper package.

```
$ ~ cd NucliasHyper
~/NucliasHyper$ sudo ./init.sh
```

The binary is executed and the following results will appear.

########## Welcome use Nuclias Hyper ##########

--

--

--

(1/12)---- Uninstall the version ----

No version installation detected

(2/12)---- check Nuclias Hyper image ----

message: 1

start down Nuclias Hyper image

Nuclias Hyper image is existed

(3/12)---- check NMS image ----

message: 1

start down NMS image

NMS image is existed

(4/12)---- check core image ----

message: 1

start down core image

core image is existed

(5/12)---- check web image ----

message: 1

start down web image

web image is existed

(6/12)---- check old DB ----

message: 0

no such old postgreDB container

(7/12)---- check DB image ----

message: 1

start find PostgreSQL image

(8/12)---- check PostgreSQL port ----

message: 0

postgre_port 5432 is free

message: 0

postgre_port 5433 is free

(9/12)---- check hyper_port ----

message: 0

hyper_port is free

(10/12)---- check web_port ----

message: 0

web_port is free

```
(11/12)---- check core_port ----
message: 0
core_port is free
(12/12)---- check file and directory ----
check file finished
all check_job finished

The system will initial setup the database administrator account for Nuclias Connect, is this the first time to
setup an administrator account? [y/n]
y ← input “y”
User Name：xxxxx ← input your user name
Password：xxxxxxxx ← input your password
Confirm Password：xxxxxxxx ← input your password again
Please enter the host IP address. This IP will be used for NMS features such as Configuration Backup/Restore,
Firmware Upgrade, and Trap/Syslog host setup:
xxx.xxx.xxx.xxx ← input your host IP
WARN[0000] /home/dlink/NucliasHyper/docker-compose.yml: the attribute `version` is obsolete, it will be
ignored, please remove it to avoid potential confusion
[+] Running 7/7
 ✓ Volume "nucliashyper_POSTGRES_DATA"   Created            0.0s
 ✓ Volume "de008396"                     Created            0.0s
 ✓ Container postgresql                  Started            2.1s
 ✓ Container nms                         Started            2.9s
 ✓ Container nuclias_connect_core        S...               2.7s
 ✓ Container nuclias_connect_web         St...              3.5s
 ✓ Container nuclias_hyper               Started            3.7s
Nuclias Connect services are running...

-- commands list ----------------------
|                                      |
| start: docker-compose up -d          |
| stop:: docker-compose down           |
|                                      |

~ $ sudo docker-compose up -d
WARN[0003] /home/dlink/NucliasHyper/docker-compose.yml: the attribute `version` is obsolete, it will be
ignored, please remove it to avoid potential confusion
[+] Running 5/5
 ✓ Container postgresql              Running                 0.0s
 ✓ Container nuclias_connect_core    Runnin...               0.0s
 ✓ Container nms                     Running                 0.0s
 ✓ Container nuclias_hyper           Running                 0.0s
 ✓ Container nuclias_connect_web     Running                 0.0s
~$
```

Please confirm that all container items are successfully running.

As the initialization of the Nuclias Hyper software takes place, a prompt will appear requesting the database administrator account. If this is the first time using the database, you need to set a database administrator for the account.
Otherwise, skip this step and go to Verifying the Installed Software.

Windows OS Installation

It provides step-by-step instructions to install and configure WSL2, Ubuntu 24.04, Docker Desktop, and D-Link Nuclias Hyper on Windows 11.

1. Enable WSL2 on Windows

1. Open PowerShell as Administrator.
2. Run the following command:
   wsl –install
3. Restart your computer when prompted.

2. Install Ubuntu 24.04

Run the following command in PowerShell:
wsl --install -d Ubuntu-24.04
wsl –install –web-download -d Ubuntu-24.04
Once installed, launch Ubuntu and create a UNIX username and password.

3. Verify WSL Installation

Run the following command to check your WSL version:
wsl -l -v
If it shows VERSION 1, run: wsl --set-version Ubuntu-24.04 2

4. Install Docker Desktop

1. Download Docker Desktop from https://www.docker.com/products/docker-desktop/
2. Run the installer and ensure 'Use WSL 2 instead of Hyper-V' is selected.
3. Restart your computer after installation.

5. Configure Docker Desktop for WSL2

1. Open Docker Desktop > Settings > General > Enable 'Use the WSL 2 based engine'.
2. Go to Settings > Resources > WSL Integration > Enable 'Ubuntu-24.04'.

6. Install Nuclias Hyper

1. Download the Nuclias Hyper package (nuclias_hyper.tar.gz) to your Ubuntu home directory.
2. Extract the package: tar zxvf nuclias_hyper.tar.gz
3. Navigate to the extracted folder and start the installation:
cd NucliasHyper
sudo ./init.sh
4. install finish and then exec “sudo docker-compose up -d”
5. During setup, you will be asked to configure the admin account and host IP.
   Example URL: https://localhost:30003 or https://<your-IP>:30003

7. Verify Running Containers

Check active containers using:
sudo docker ps
Ensure containers for nuclias_hyper, nms, core, web, and postgresql are running.

8. Access Nuclias Hyper

Open your browser and go to: https://localhost:30003
Login using the admin credentials created during setup.

9. Initial Configuration

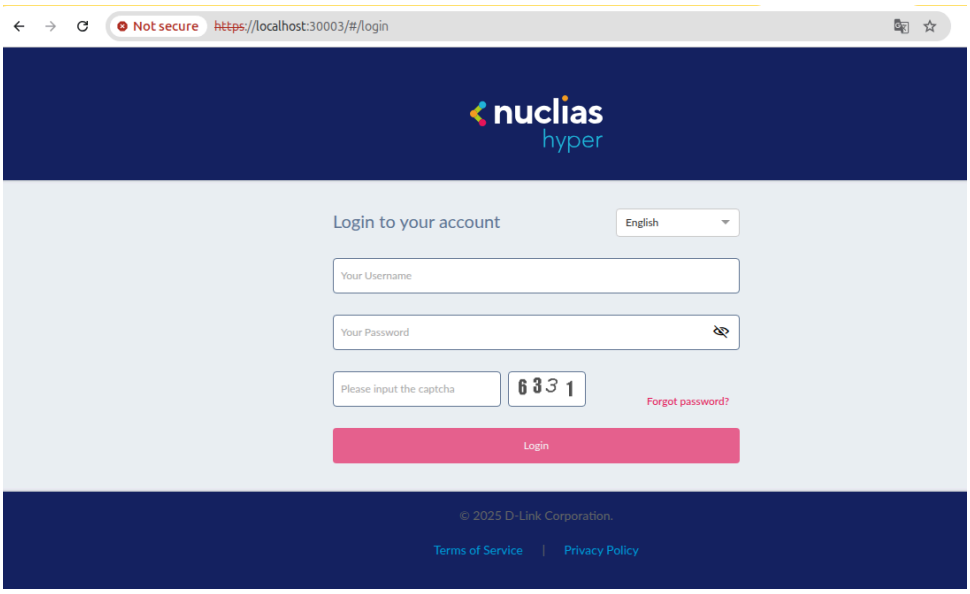
1. Complete the setup wizard.
2. Add network and access points for discovery.
3. Configure NMS for switch management.
4. Verify devices under Monitor > Access Point and Monitor > Switch.

10. Summary

You have successfully installed WSL2, Ubuntu 24.04, Docker Desktop, and Nuclias Hyper. Nuclias Hyper is now ready for network management via a web browser.

Launching Nuclias Hyper

With the core containers set up and the PostgreSQL profiles configured, Nuclias Hyper can be accessed through a web browser.
Open a browser on Ubuntu, and then access https://localhost:30003.



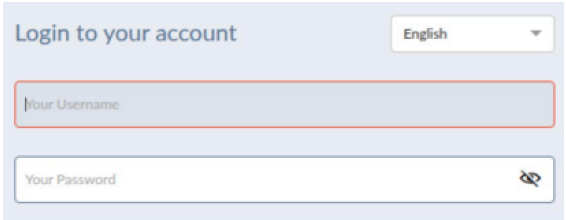
Alternatively, use any other host on the network and access https://[HOST IP]:30003.
You should now be able to access and use Nuclias Hyper.

Note: NC Part will use TCP Port 30001, NMS Part will use TCP 17300.

Enter the modified username and password in the respective fields. Enter the Captcha code as shown on screen.

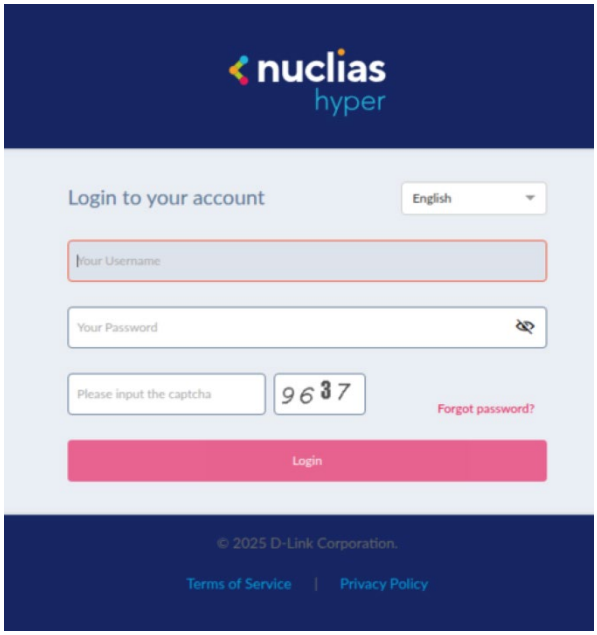
NOTE:

- The Forgot password function allows you to reset your password if the current password is lost.
- The interface supports multi-language options. Click the language drop-down menu to select a different language.



After the web browser opens and connects successfully to the server, a change-password dialog will appear. A change in the default password is required after the first login.

When assigning a password, it is recommended to use a strong password. The new password is required to be 5 - 16 characters in length. Mixing uppercase and lowercase characters along with numbers and symbols can help ensure stronger security.



NOTE: Do not include common words or names.

Enter the previous password in the **Old Password** field. In the **New Password** field enter the new password.
Enter the same password in the **Confirm Password** field to verify the entry.
Click Modify to complete the process.

Upon logging in, the System Settings page will appear. If the device-access address or port has been changed, the Nuclias Hyper Core server must be restarted. Complete the following settings page before continuing.

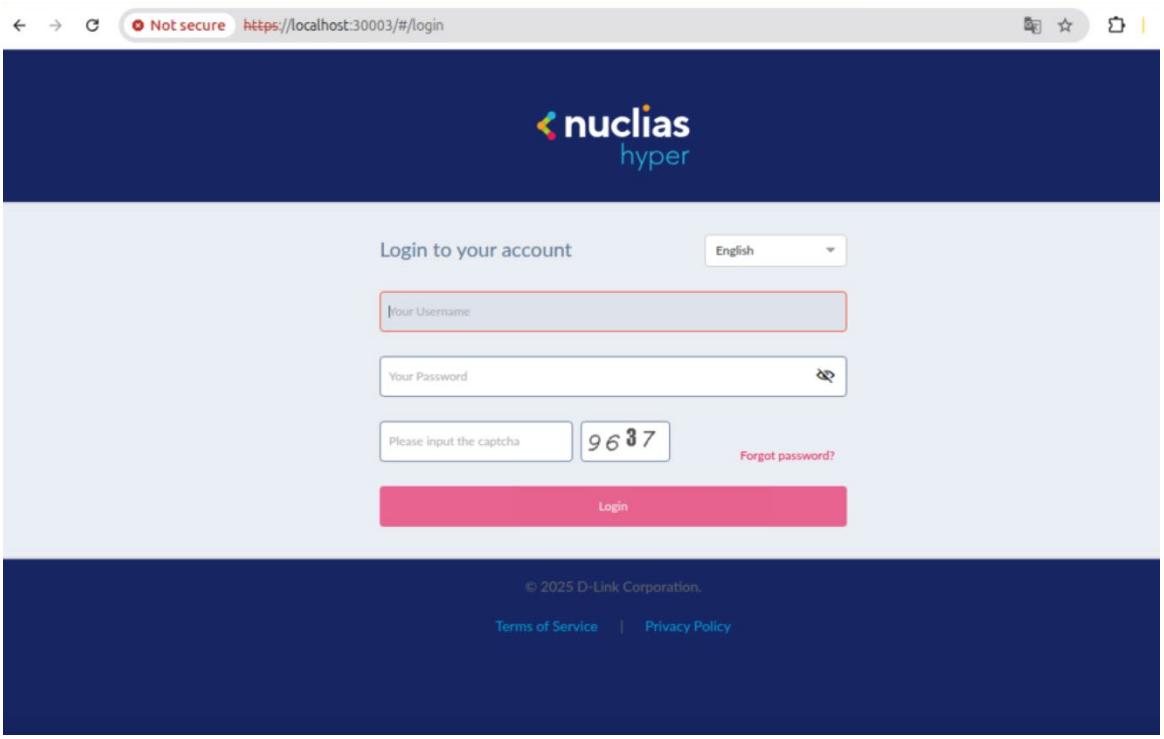
Nuclias Hyper Configuration

Nuclias Hyper uses a secure HTTPS connection to connect to the Nuclias Hyper Controller. By default, the application will open the default Web browser and connect to the localhost, which is the local means of connecting to the computer's own IP address.

Alternatively, from a remote computer, you can also connect to the Nuclias Hyper Server by entering the IP address of the computer that has the controller application installed on the web browser. Open the web browser on the remote computer (Internet Explorer or Google Chrome are recommended) and enter the IP address or domain name of the host computer in the address bar of the Web browser and press **ENTER** to open the Nuclias Hyper management interface.

The Nuclias login screen will appear once a connection to the server is established. Enter the login username, password and captcha requirement, if applicable. Click **Login** to enter Nuclias Hyper.

NOTE: By default, the username and password are "**admin**". Supported languages include English (default), Traditional Chinese, Simplified Chinese, Korean, Japanese, French, Spanish, German, Russian, Italian, and Turkish.

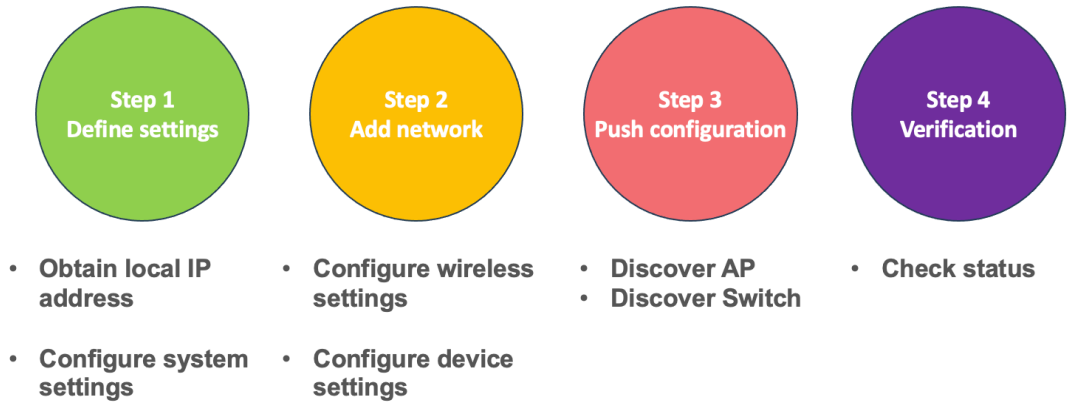


Introduction

This tutorial describes how to run the Nuclias Hyper Server application and create a scenario to display the first-time configuration via setup wizard.

After installing Nuclias Hyper in Linux operating system, we are going to follow the steps below:

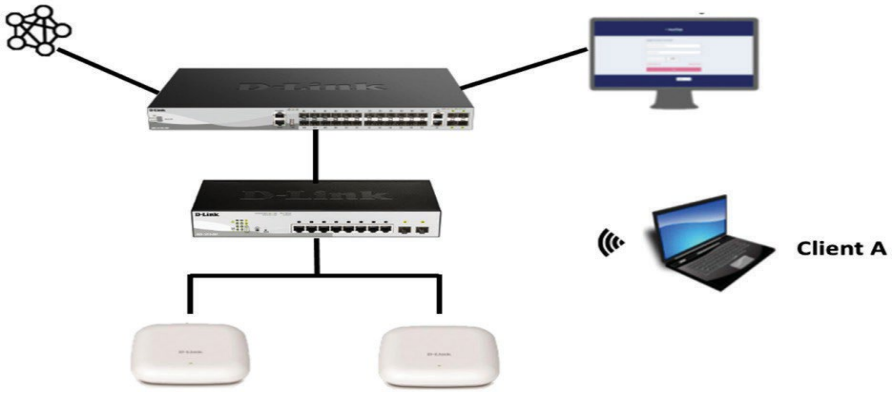
For Nuclias Connect



For NMS

Scenario

We were planning to establish a managed wireless network environment with the equipment below: Nuclias Hyper server, a managed Switch, a smart Switch and two wireless APs.

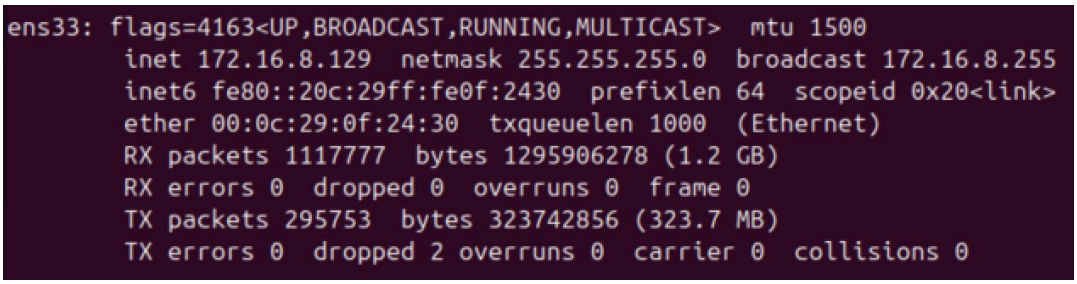


Initial configuration of Nuclias Connect

1. Define Nuclias Connect Settings

1.1 Obtain local IP address.

From the Desktop or Terminal, enter ifconfig to obtain local IP address from this server. In our lab facility, the IP is 172.16.8.129

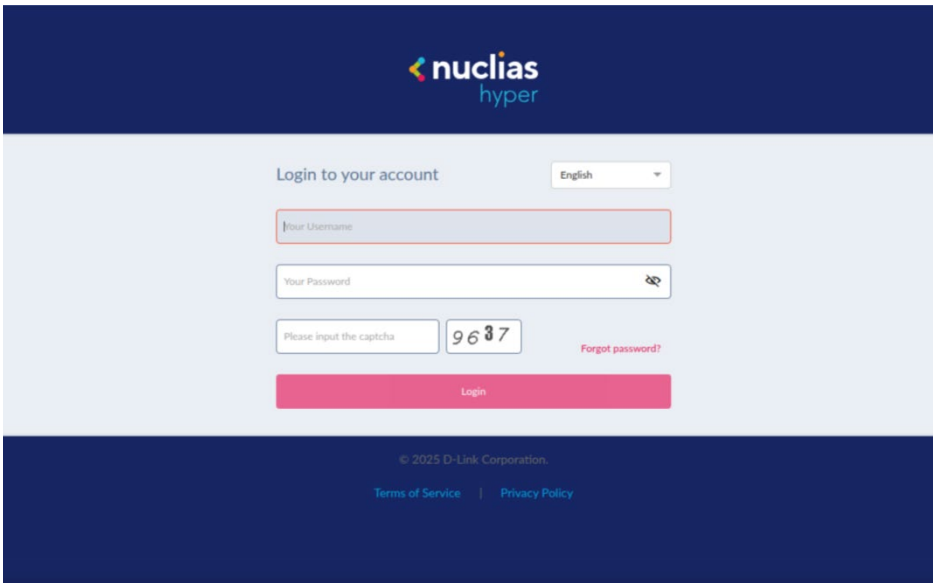


1.2 Launch a browser to Nuclias Hyper

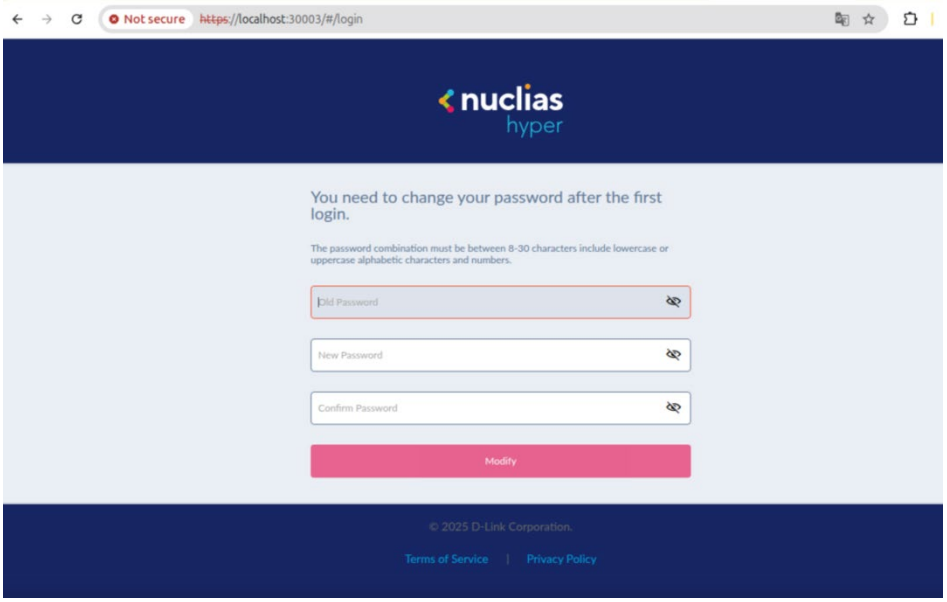
- After the installation is completed.
- Before you can manage Nuclias Hyper, the Docker service must be running first, if not, Please start the Docker service first.
- The Nuclias Hyper configurator interface is accessible through a browser window, please open your browser and enter the following URL: https://IP:30003

1.3 Login to Nuclias Hyper

- The Nuclias Hyper main login displayed as screen.
- The default username and password are admin.

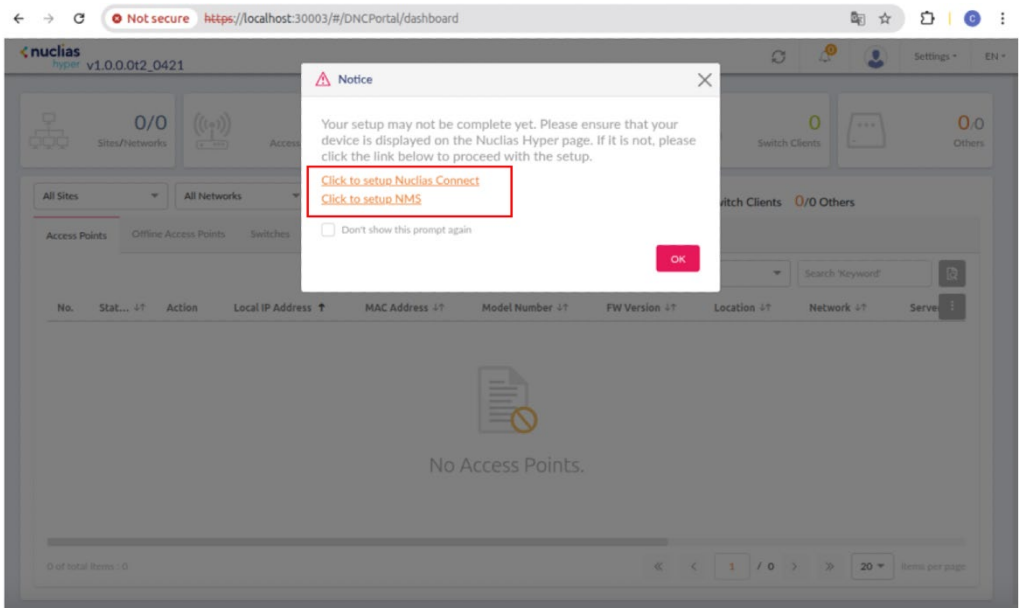


- You will be required to change your password after the initial login.
- Enter the current password, then enter your new password and its confirmation in the appropriate fields.



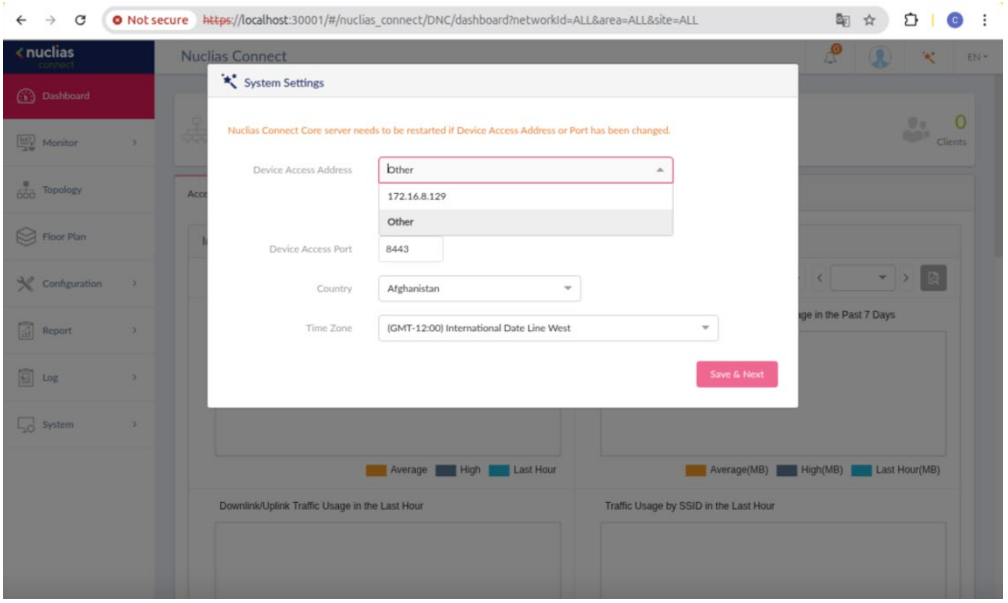
1.4 Go to Nuclias Connect

- Click the link to set up Nuclias Connect



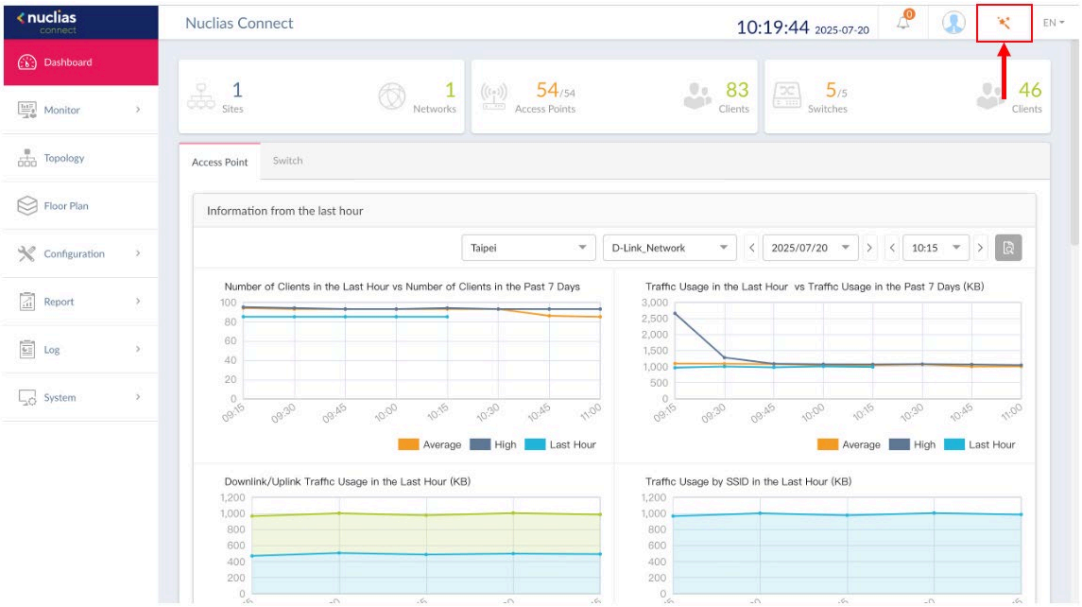
1.5 Setup Nuclias Connect Wizard

- If you are not currently managing any network, the Wizard will pop out automatically.



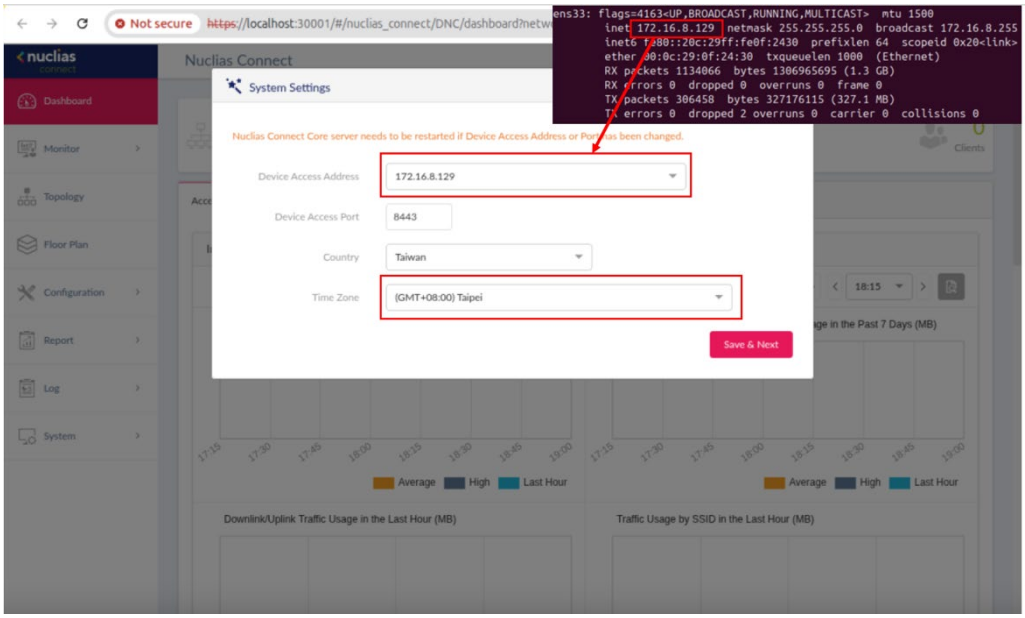
1.6 Reopen setup wizard

- Should you carelessly close the Wizard, you can reopen with a magic wand tool in the upper right corner.



1.7 Configure system settings

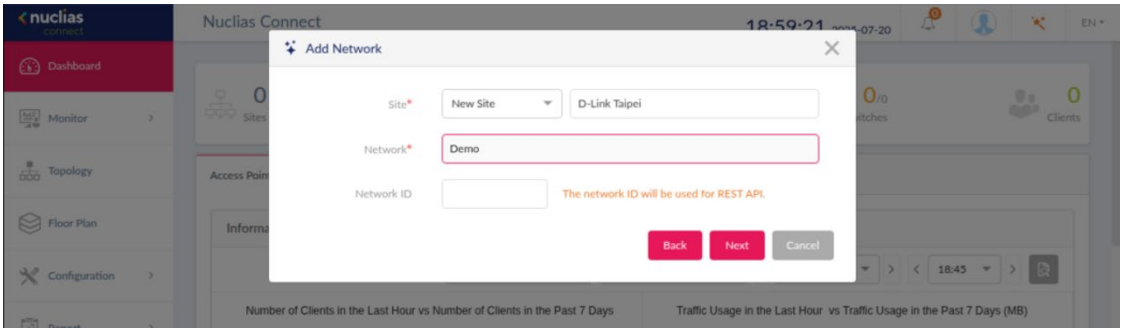
- Input the device address previously displayed in Command Prompt.
- Nuclias Connect Device Access Port:8443
- Time Zone: You must choose the place where the application is, otherwise, the log record will present incorrect time stamp.



2. Nuclias Connect Step 2 Add Network

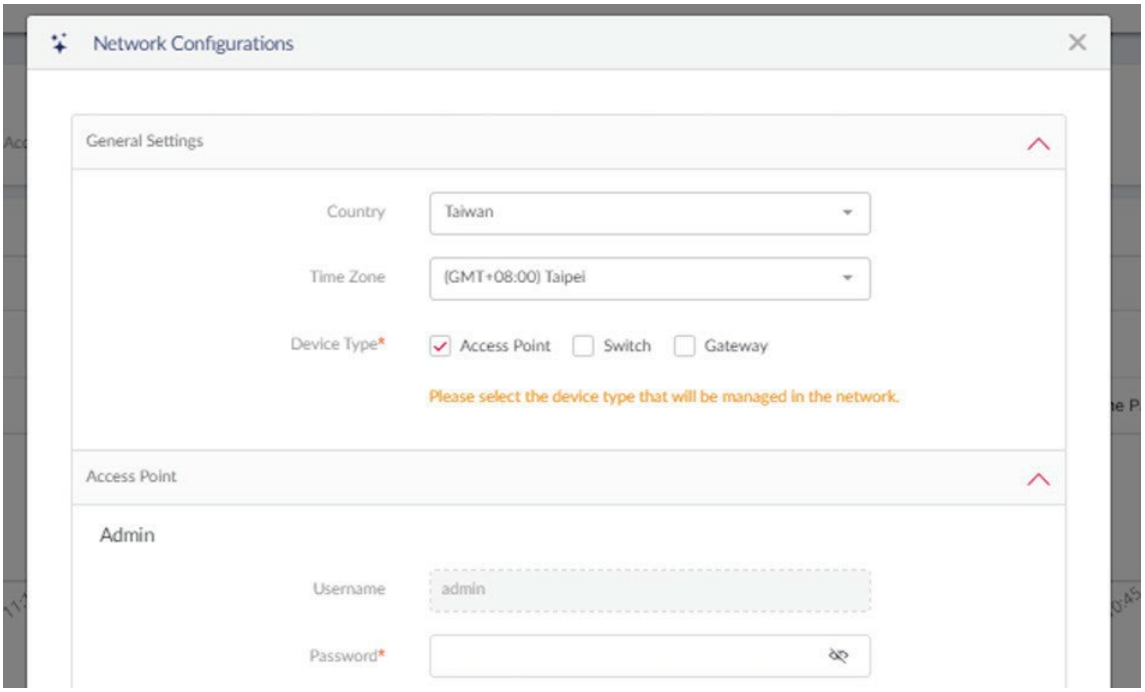
2.1 Choose Site

- To add the network, choose new Site or use an exist site.
- The network name is also the profile which configuration's you would like to push to APs.



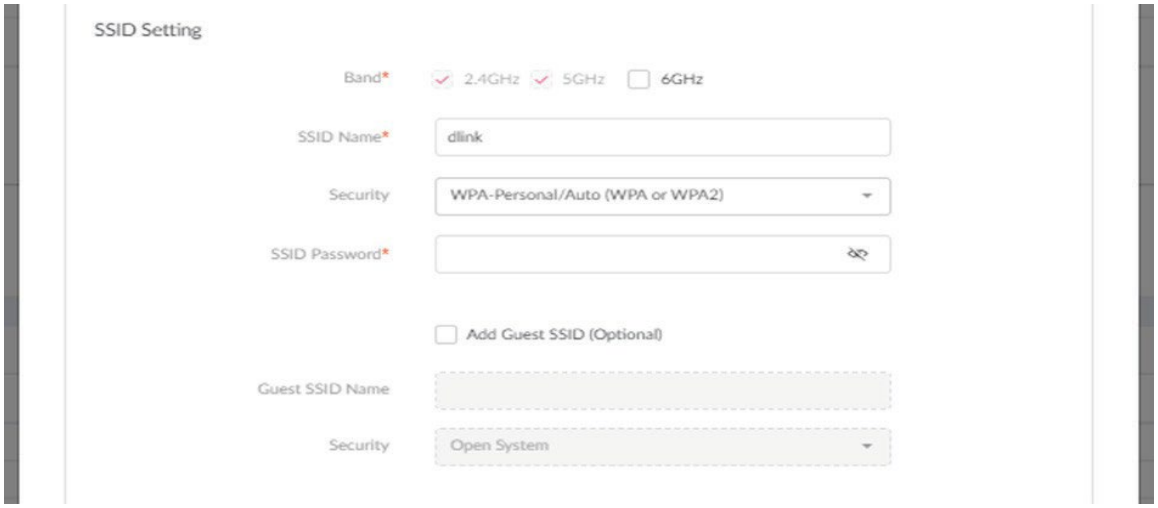
2.2 Configure General settings and AP account

- You should select relevant time based on the location of the APs.
- The username & password will be pushed into the APs in the next steps.



2.3 Configure wireless settings

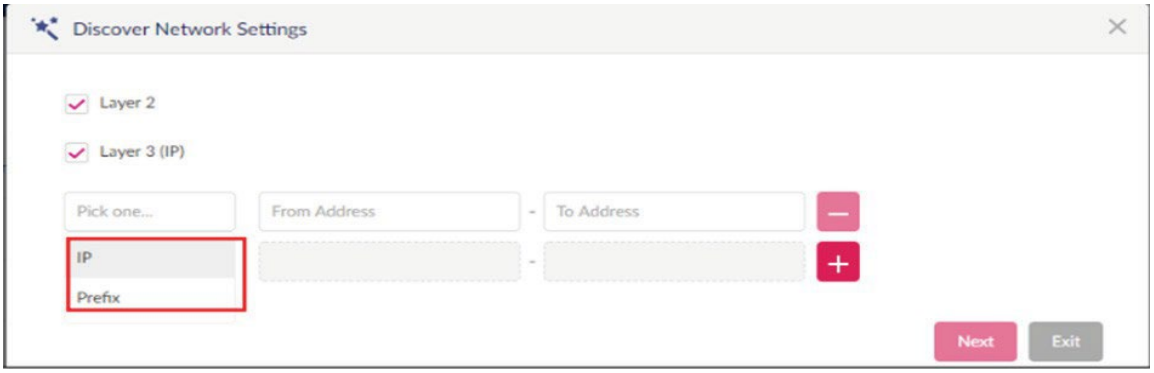
- SSID cannot contain some symbols.
- Security: Select Open System or WPA to determine if the password for the connection is opening or not.
- If you want to add guest SSID, click the checkbox, the status of security would be Open System as default.



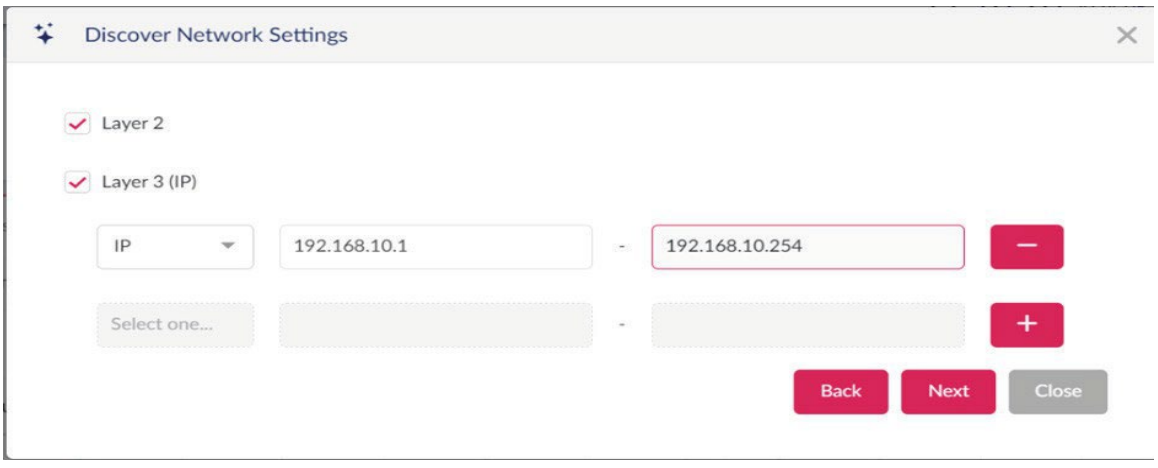
3. Nuclias Connect Step 3 Push Configuration

3.1 Discovery

- Select Layer 2 or Layer 3 (you also can choose both of them)
- There are two ways in layer 3 option if your network segment is quite complex, using prefix might let you focus on smaller discovery range.



- Our local ID is “192.168.10.66”
- We can search cross-domain IP to discover APs.



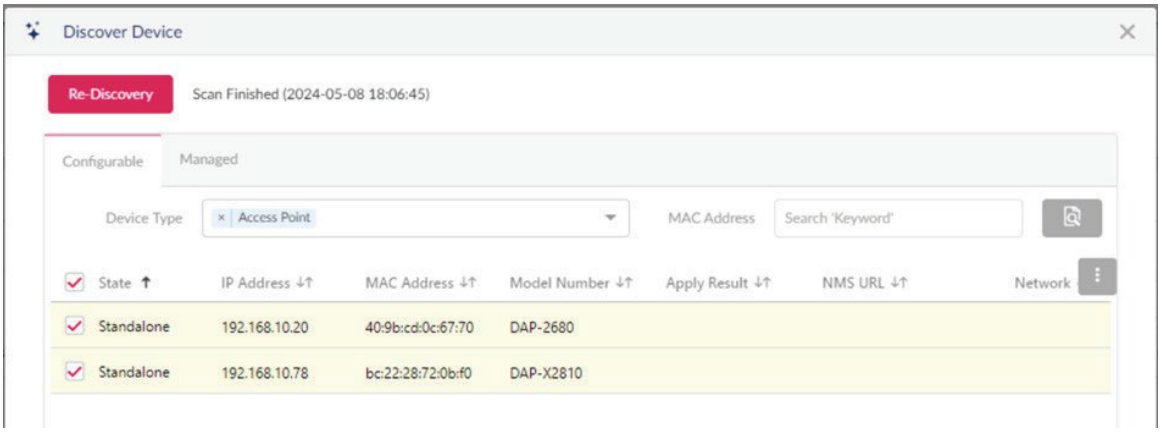
3.2 Type of AP status in management process

There are 5 types of state to know whether the AP is being managed.

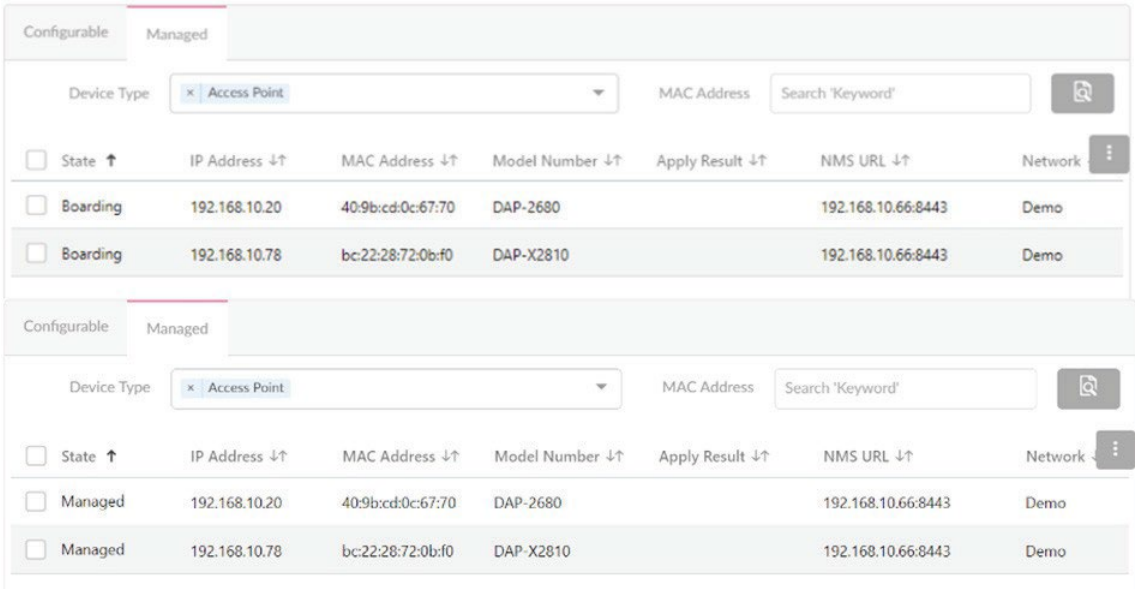
- Not managed (Standalone)
- Unregistered
- Boarding
- Managed
- Unmanaged

Types of AP status to know whether the AP is being managed (in DAP GUI)

The default ID & password is admin

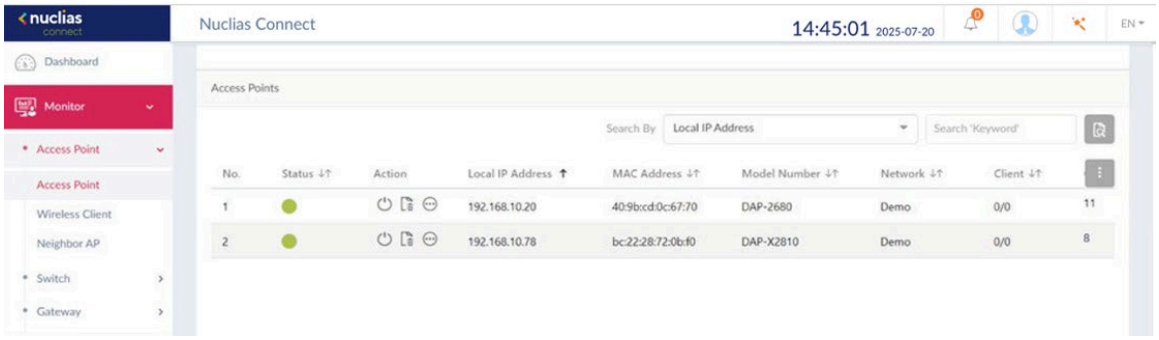


You may have to wait several minutes for the Connection to be done, the state will change from "Boarding" to "Managed."

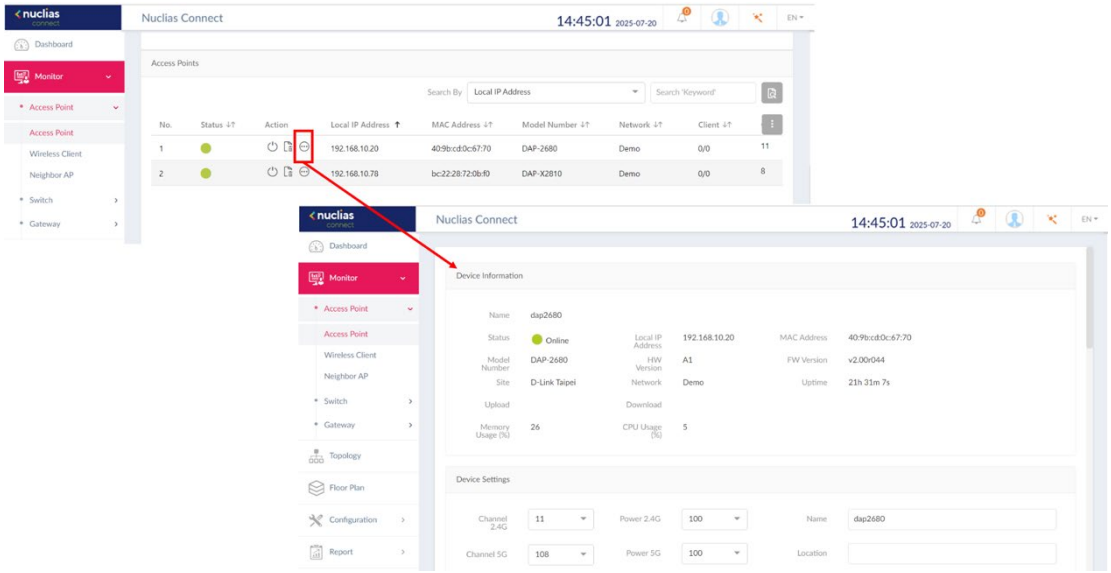


4. Nuclias Connect Step 4 Verification

The DAP device should be displayed in Nuclias Connect menu (Monitor > Access Point).



- Click action icon to open device detail page.



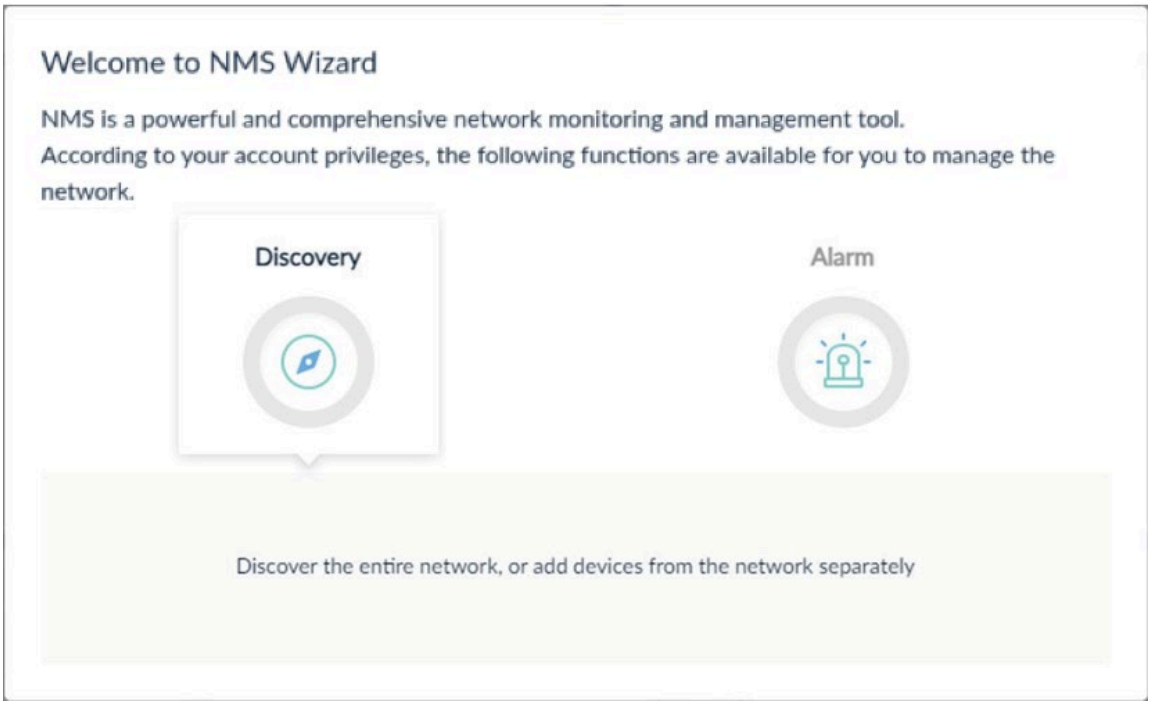
Initial configuration of NMS

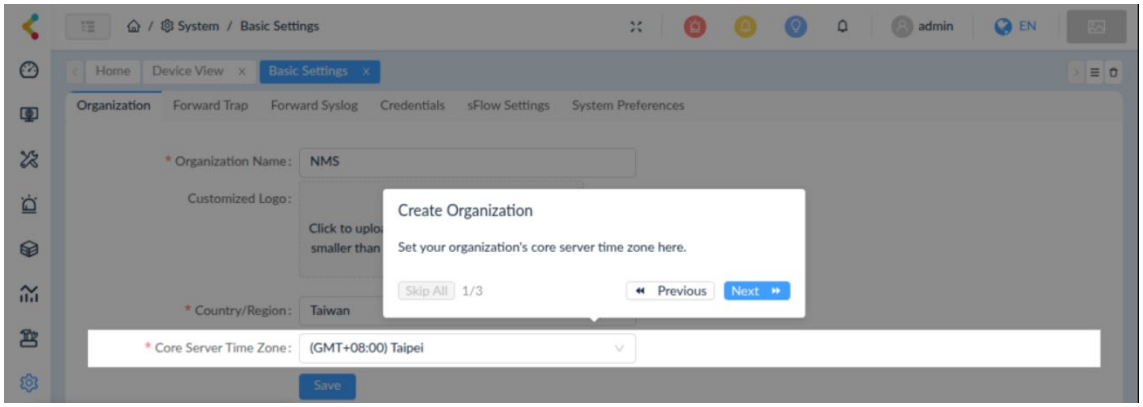
1. NMS Step 1 Preconfigured switches

Before initially configuring NMS, please pre-configure the IP of the switches you want to manage and enable SNMP, and even add routes to ensure network connectivity with the server/probe.

2. NMS Step 2 Create organization

When a Super Admin redirects into the NMS for the first time, a wizard will appear, please select Discovery to be guided through the Network Discovery process, which requires you to set up an organization first.

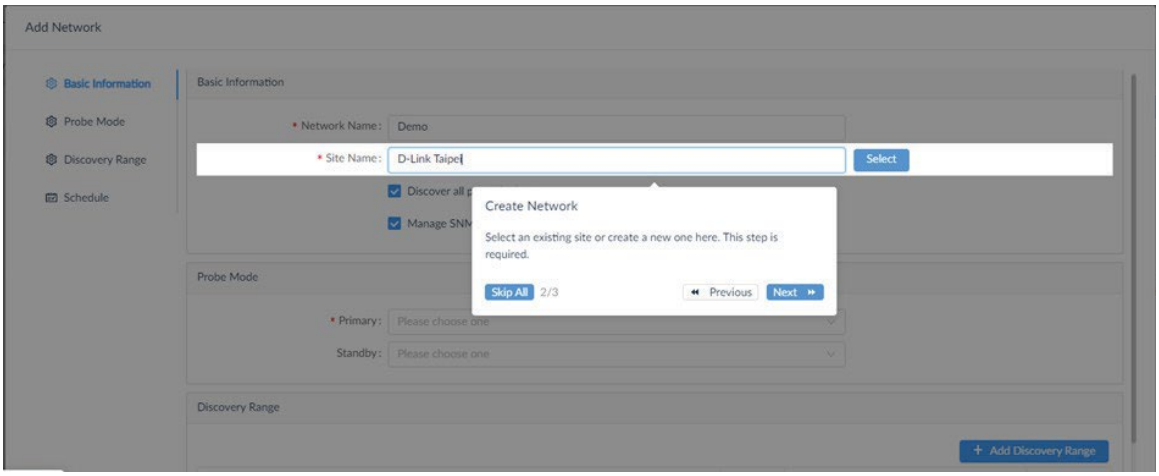




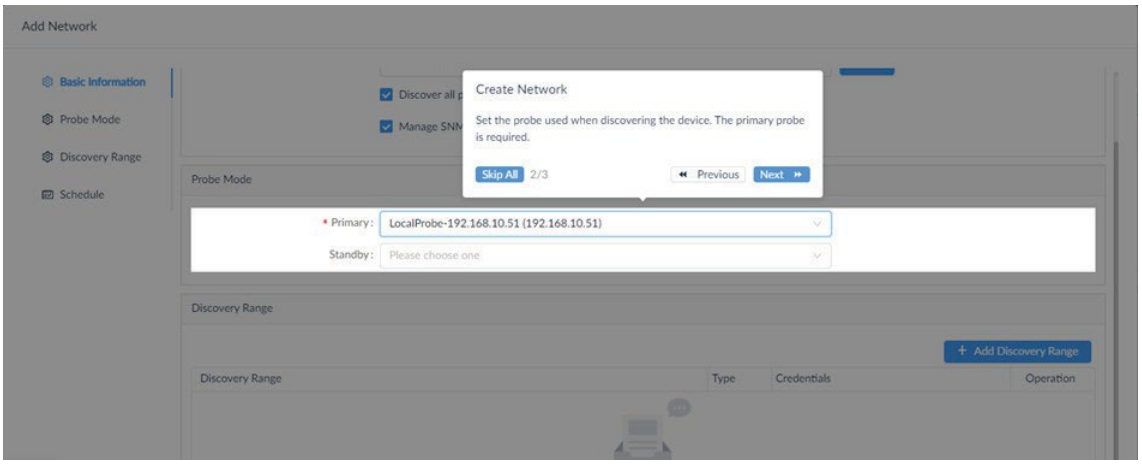
3. NMS Step 3 Add network

- Follow the wizard or go to Monitoring > Network Discovery.
- Click + Add Network.
- Enter the new network information for discovery

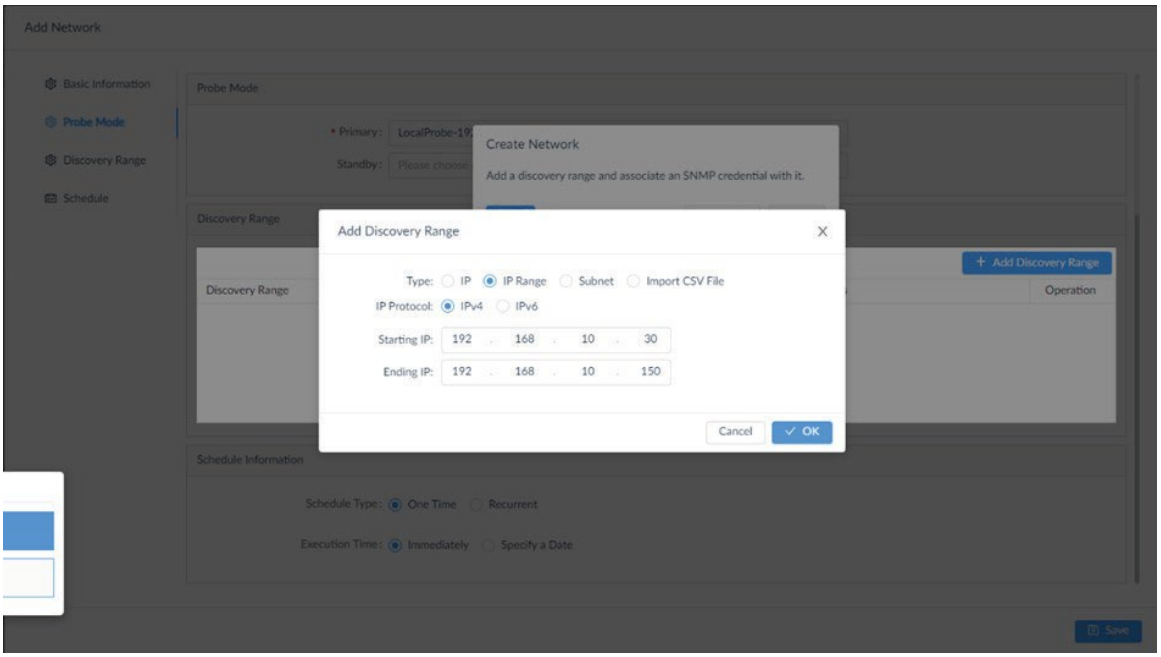
Note: Click the drop-down menu to select an existing site or click New to name this site.



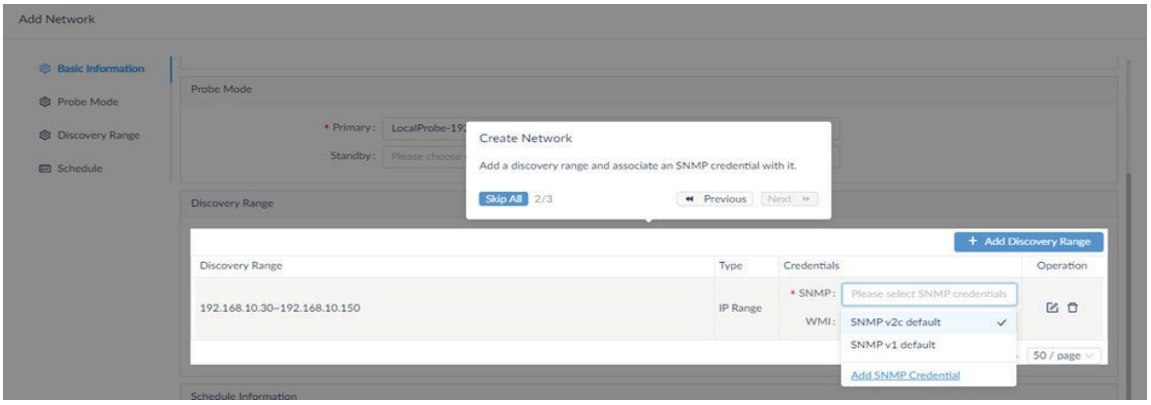
- Click the drop-down menu to select the primary probe.



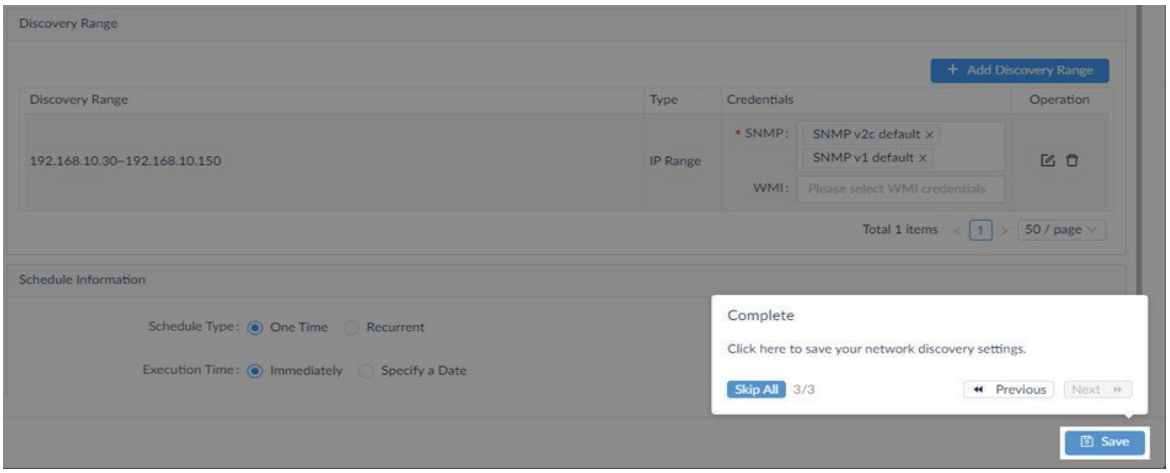
- Click the Add Discovery Range button to define a range for network search.



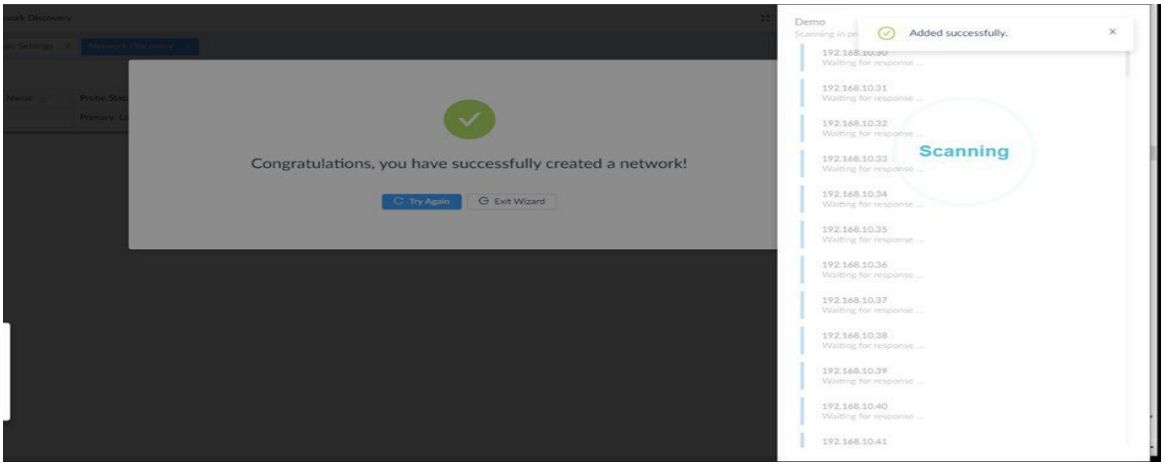
- Click the SNMP field and select the credential version for discovery. The available credentials are set via the Basic Settings menu.



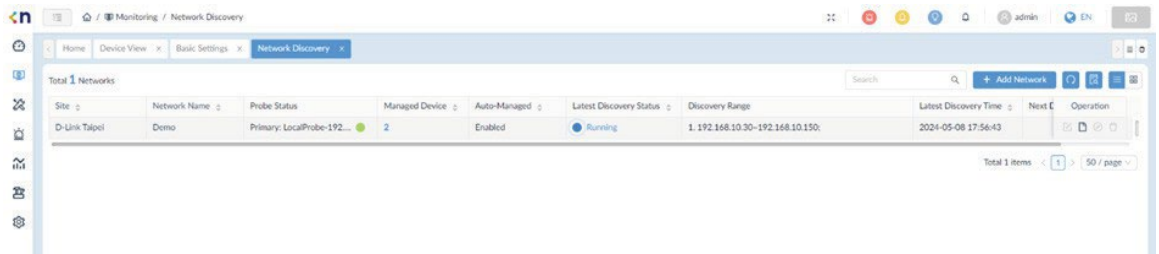
- Then select "One Time" and "Immediately" in the schedule information block to initiate the network discovery.



- Click "Save" to add the new network and execute the network discovery immediately. The Discovery Results page displays. The list of discovered devices will be shown.

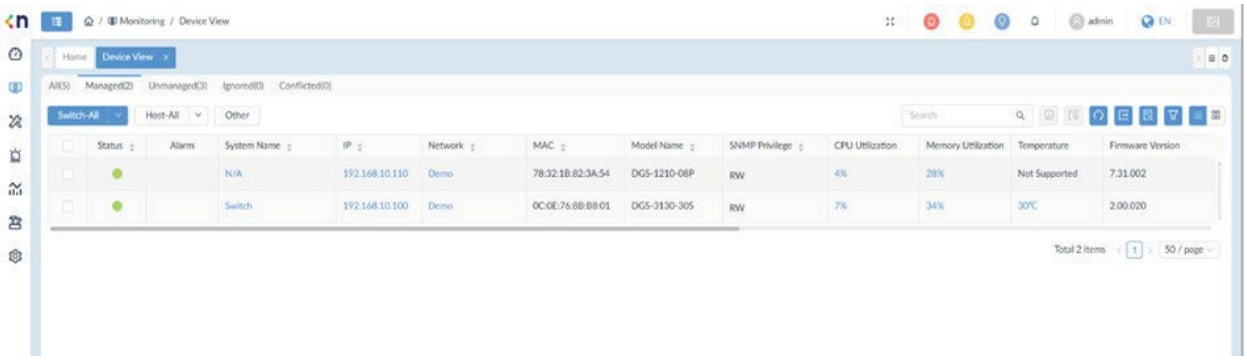


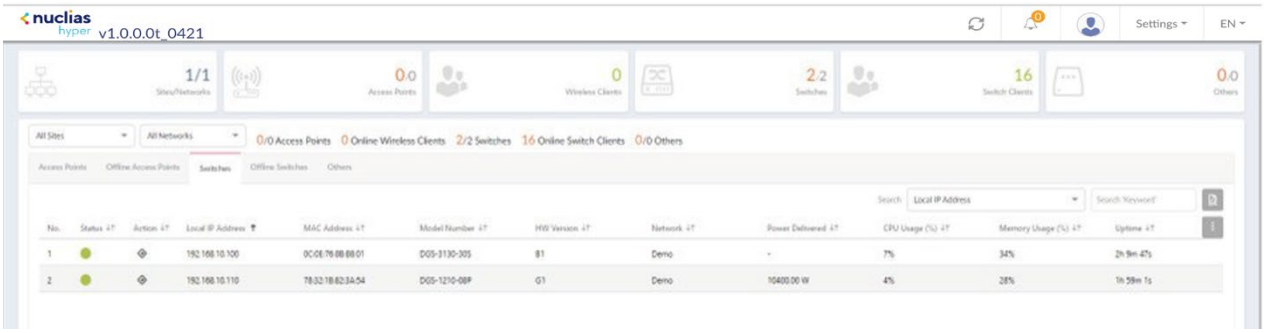
- You can click Exit Wizard to return to Network Discovery.



4. NMS Step 4 View managed switches

The Device View shows devices, which are categorized by managed/unmanaged, ignored, and conflicted. The default view is All. Managed devices are devices that can be communicated with the NMS system and have the required SNMP parameters. The managed switches would be listed both in NMS and Nuclias Hyper.

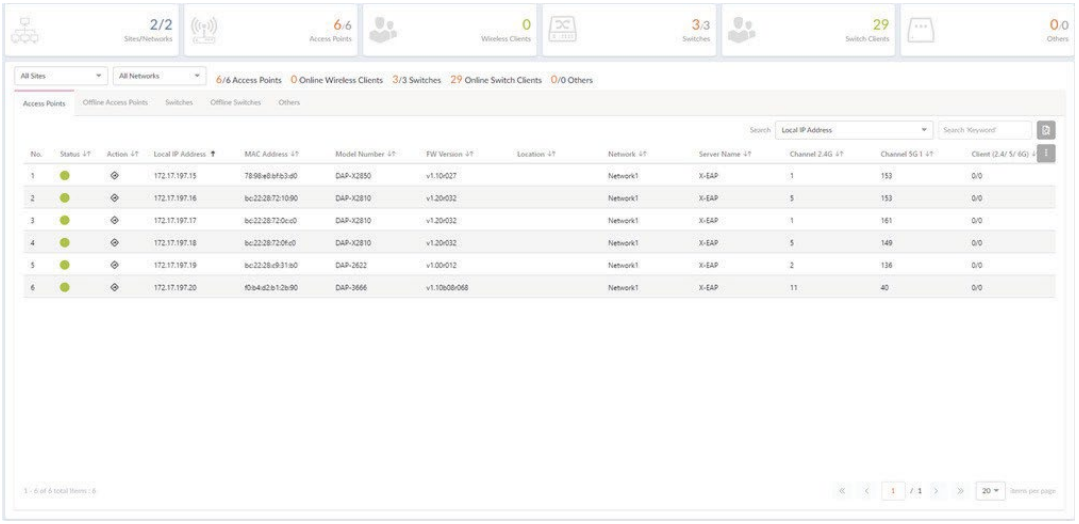




Nuclias Hyper

Dashboard

The device list page for access points and switches is displayed. It provides an overview of total sites, networks, available access points, switches and their clients devices that have enabled SNMP, and those that have been discovered by NMS. These are categorized as "Others."

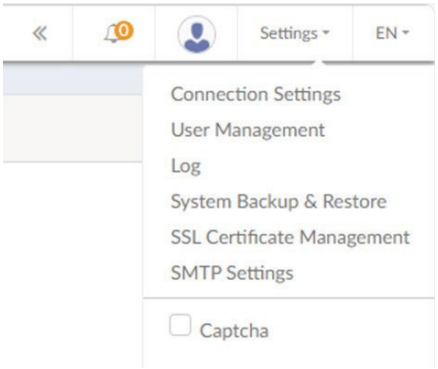


In Access Points field, it displays **No., Status, Action, Local IP Address, MAC Address, Model Number, FW Version, Location, Name, Network, Server Name, Upload, Download, Channel 24G, Channel 5G1, Channel 6G, Client Number, CPU Usage, Memory Usage and Uptime.** In the Search By drop-down field, select an attribute (Local IP Address, MAC Address, Model Number, FW Version, Name, Network, Server Name, Location, Channel 24G, Channel 5G1, Channel 6G) to specify the search field or enter a keyword related to the target device in the Search field. Click to start the process. Any relevant devices meeting the search criteria will be listed. -

In Switches field, it displays **No., Status, Action, Local IP Address, MAC Address, Model Number, FW version, Location, Name, Network, Server Name, Ports, Switch Client, Power Delivered, CPU Usage, Memory Usage and Uptime**. In the Search By drop-down field, select an attribute (Local IP Address, MAC Address, Model Number, FW Version, Name, Server Name, Ports) to specify the search field or enter a keyword related to the target device in the Search field. Click to start the process. Any relevant devices meeting the search criteria will be listed.

In Others field, it displays **No., Status, Action, Local IP Address, MAC Address, Model Number, Device Type, Name, Network, Server Name and Uptime.** In the Search By drop-down field, select an attribute (Local IP Address, MAC Address, Model Number, Name, Server Name, Device Type) to specify the search field or enter a keyword related to the target device in the Search field. Click to start the process. Any relevant devices meeting the search criteria will be listed.

In the upper right corner of the main screen there are alerts, settings menu and language menu. You can also enable or disable Captcha function here.



Connection Settings

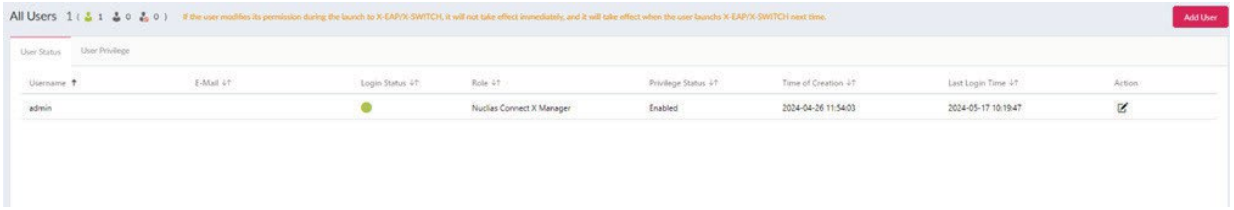
This page displays one Nuclias Connect and one NMS. You can click the redirect button in the action field to navigate to the Nuclias Connect or NMS GUI.

User Management

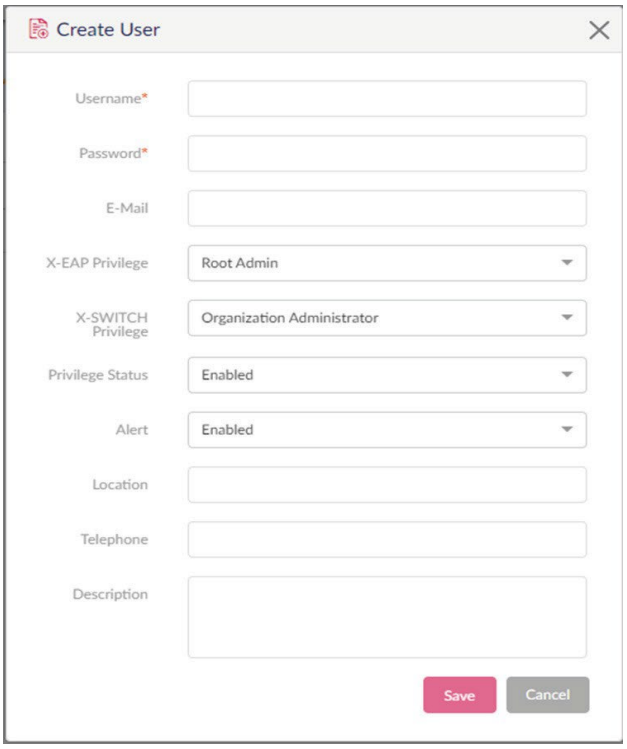
The User Status page allows administrators to view, edit, or delete the status of all registered user profiles. When the Login Status shows green, the user is logged in. When the Login Status shows red, the user is logged out.

To edit a user profile, click the edit button corresponding to the user. The username, password, email, privilege, privilege status, alert, location, telephone as well as the user description are available for editing. Note that the administrator account cannot be deleted or have its username and privilege settings modified.

Once the user settings are completed, click Save to confirm or Cancel to return to the previous menu.



To add a user to the selected network, click Add User to open the Create User page. In this page, enter the new user information. Fields marked with an asterisk (*) are required in order to complete the new entry. Once the information is filled in, click Create to save the new user profile. Alternatively, click Cancel to return to the previous screen without saving.



Nuclias Connect Privileges

Options	Descriptions
Root Admin	Manage all sites/networks on Nuclias Connect
Root User	View all sites/networks on Nuclias Connect
Local Admin	Manage your own network on Nuclias Connect
Local User	View your own network on Nuclias Connect
Front Desk Staff	Able to generate and manage passcodes on Nuclias Connect

NMS Privileges

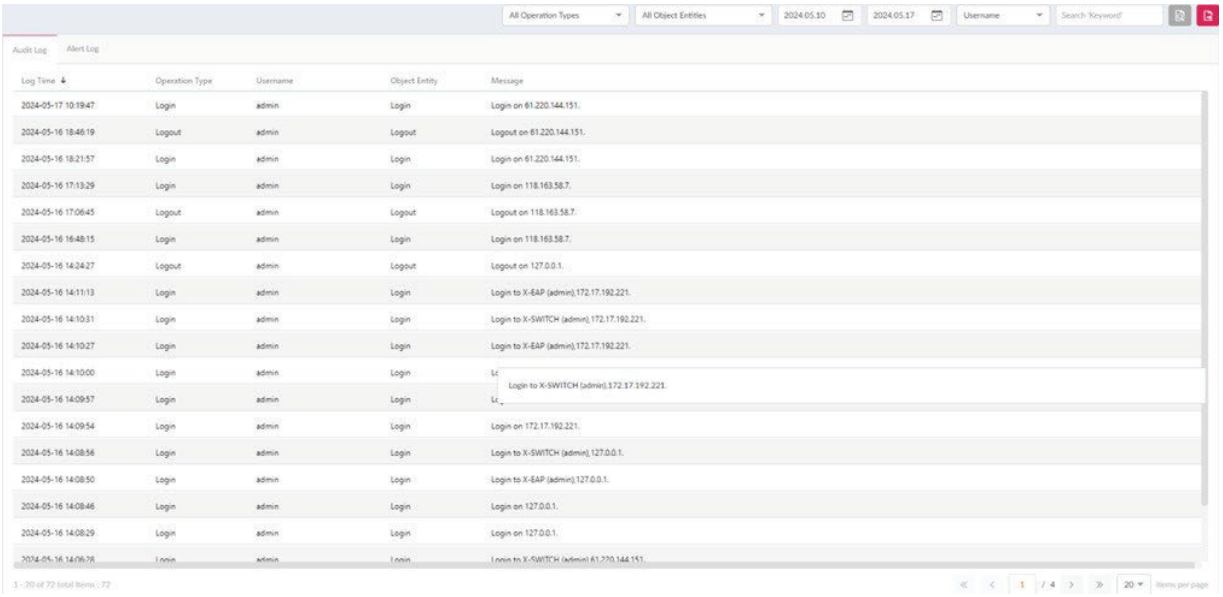
Options	Descriptions
Organization Administrator	The user can perform all administrative functions on NMS, including the management of users and security profiles within an organization
Site Administrator	The user can perform administrative functions within a site on NMS.
Network Administrator	The user can perform all administrative functions within a network on NMS.
Network Local User	View your own network on NMS

Log

Audit Log: This type of log records user activities that can be performed on an object entity such as profile and network creation or deletion.

To generate an Audit Log report, select the entries by Operation Type (operations that performed on the object entities) and Object Entity (i.e. objects associated with the functional tabs in the left pane), define the time period, and select Username or Message as the filtering criteria.

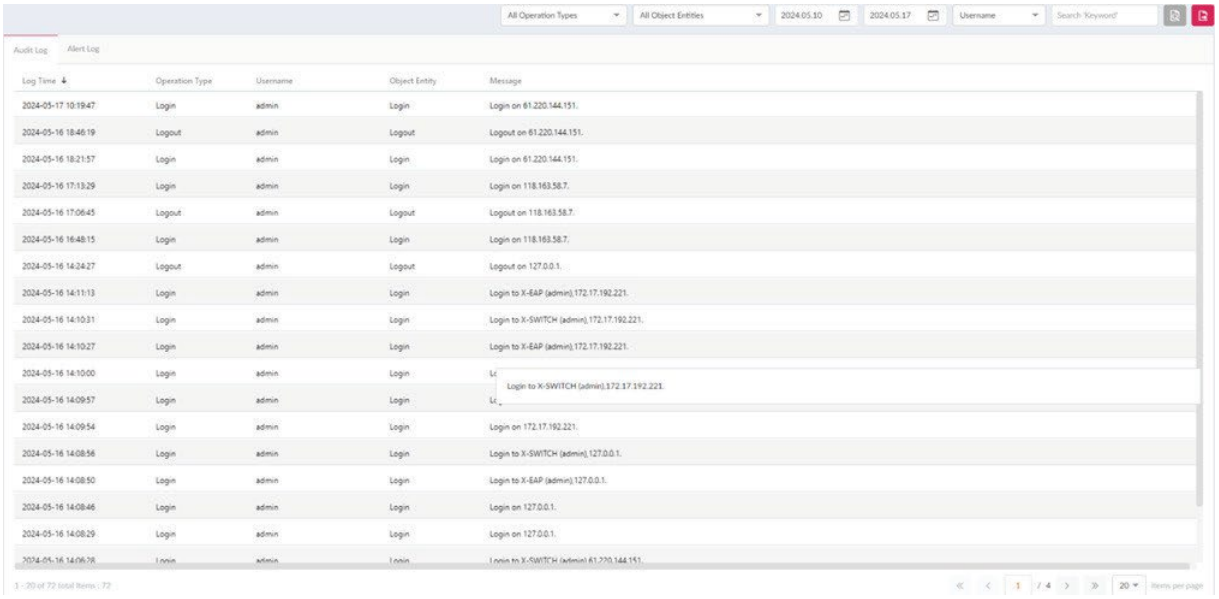
Then enter a keyword and click to display the search results. Once a report is generated, click to export it as a local Excel file. The file will be saved to your browser's download directory and will be named as follows: **Nuclias_Connect_log type_YYYY_MMDD_HHMMSS.**



Alert Log:

This type of log records alert events such as new firmware release, port linked or blocked, device online status.

To generate an alert report, select the alert events, define the time period, and select IP Address or Message as the filtering criteria. Then enter a keyword and click to display the search results. Once a report is generated, click to export it as a local Excel file. The file will be saved to your browser's download directory and will be named as follows: **Nuclias_Connect_log** type_YYYY_MMDD_HHMMSS.



System Backup & Restore

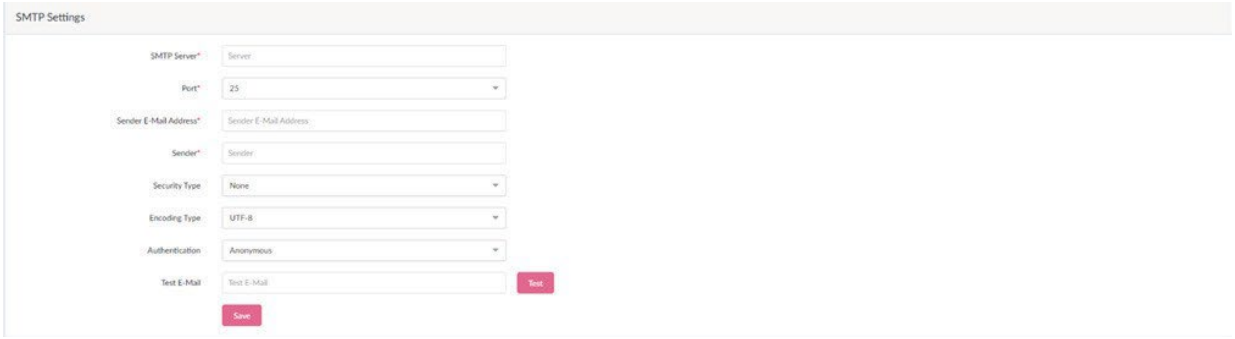
In the Backup Settings section, the database can be backed up, downloaded to a local hard drive, click "Backup Now" to back up the database file. In the Restore Settings section, database files can be restored from local hard drive.

SSL Certificate Management

The SSL Certificate function provides the means to install an SSL certificate for use on the network. To accomplish this task, an intermediate certificate is required. The intermediate certificate is used to establish the trust of the SSL certificate by binding it to the Certificate Authority's root certificate. To complete the certificate trust configuration, the SSL Certificate function requires the certificate file to be uploaded. Please restart Nuclias Hyper services in Nuclias Hyper Configurator to activate this function.

SMTP Settings

The SMTP tab displays customizable settings for the simple mail transfer protocol (SMTP). This is necessary in order to send emails on behalf of the system such as reset password validation emails. Navigate to System > Settings and click on the SMTP tab to display the function information.



Parameter	Description
SMTP Host	Enter the SMTP server's IP address or domain name.
Port	Enter the SMTP server's port number.
From Email Address	Enter the sender's email address.
From Name	Enter the sender's name.
Security Type	Click the drop-down menu to select the security type to be used in the e-mail system. The options include None or SSL.
Encoding Type	Click the drop-down menu to select the encoding type to match the supported e-mail client. The options include UTF-8 or ASC-II.
Authentication	Click the drop-down menu to select the authentication mechanism during login. The options include Anonymous or SMTP Authentication.
Test Email	Enter the recipient e-mail address to initiate a test e-mail through the SMTP configuration. Click Test to start the test function.

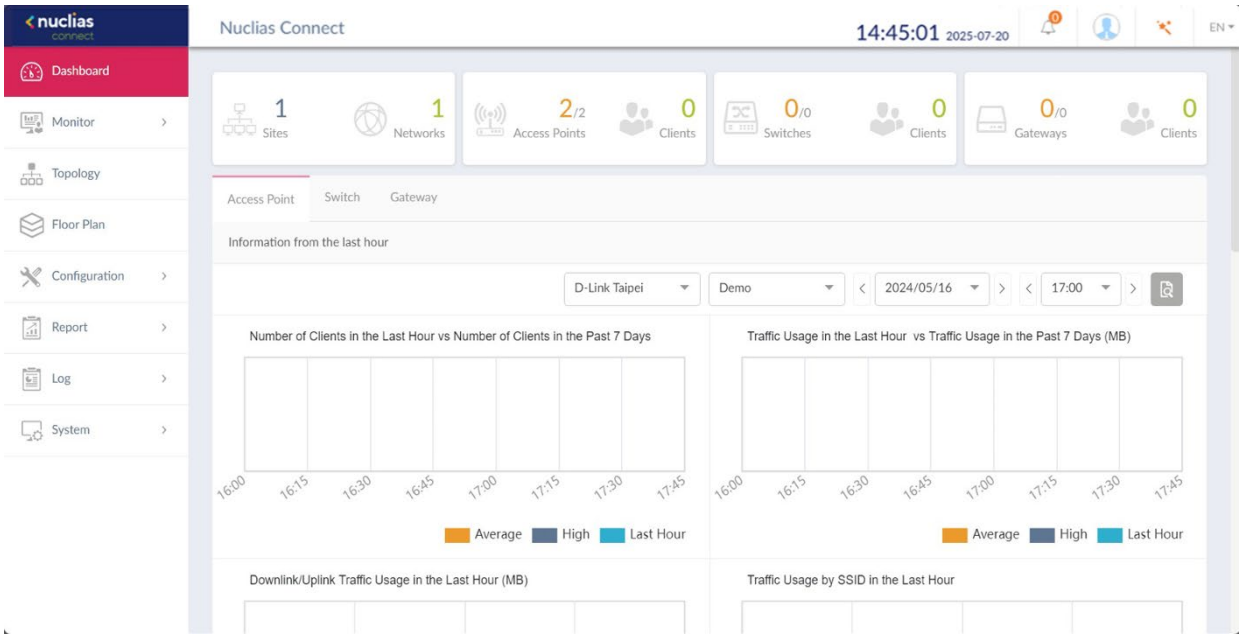
Nuclias Hyper / Nuclias Connect

Dashboard

After successfully logging into the server, the **Dashboard** page for Access Point and Switch is displayed. The dashboard provides an overview of total sites, created networks, available access points and its clients, and available switches and its clients

Access Point Field	Description
Information from the Last Hour	Displays the number of clients (Last hour vs Past 7 days), traffic (Last hour vs Past 7 days), last hour downlink/ uplink traffic, and last hour traffic by SSID.
Channel Utilization	Displays the utilization rate for both 2.4 and 5 GHz bandwidth.
Latest Events	Displays a simplified log of the latest events across all or selected sites.

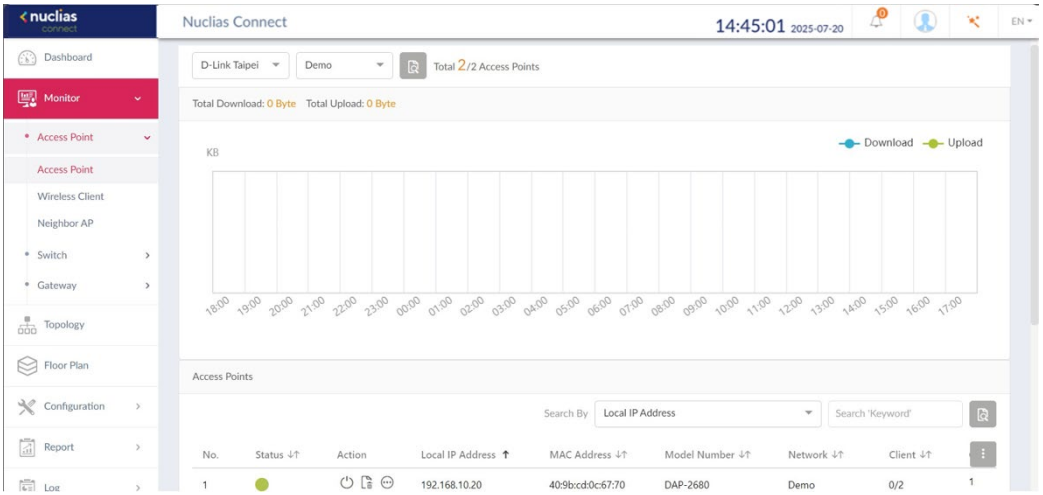
Switch Field	Description
Information from the Last Hour	Displays last hour Tx/Rx traffic usage and last hour PoE total power usage.
PoE Utilization	Displays the utilization rate of switches across different sites and networks.
Latest Events	Displays a simplified log of the latest events across all or selected sites.



Monitor

Access Point

Go to **Monitor** on the left panel to view data usage and total number of access points. On this page, you can view a summary of the data usage of all or selected number of wireless clients and networks managed by the application.



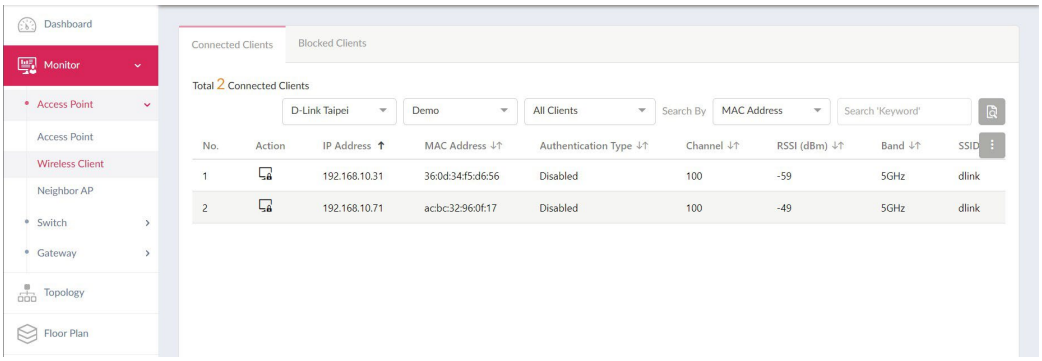
In the **Search By** drop-down field, select an attribute (**Local IP Address**, **Local IPv6 Address**, **NAT IP Address**, **MAC Address**, **Model Type**, **FW Version, Name, Location, Channel 2.4G, Channel 5G 1, Channel 5G 2 (Tri-Band**), **Power 2.4G, Power 5g 1, Power 5g 2 (Tri-Band))** to specify the search field or enter a keyword related to the target device in the Search field. Click to start the process. Any relevant devices meeting the search criteria will be listed.-

Access Point > Wireless Client > Connected Clients

Navigate to **Monitor > Access Point > Wireless Client** on the left panel, the **Connected Clients** tab is displayed. You can view a summary of all connected clients managed by the application.

Three filters are displayed: **Site**, **Network**, and **Clients**.

The following figure shows a typical summary. Use the filters to select a specific Site, network and client. Additionally, you can enter a keyword related to the target device in the Search field and click to start the process. Any relevant devices meeting the search criteria will be listed in the frame.

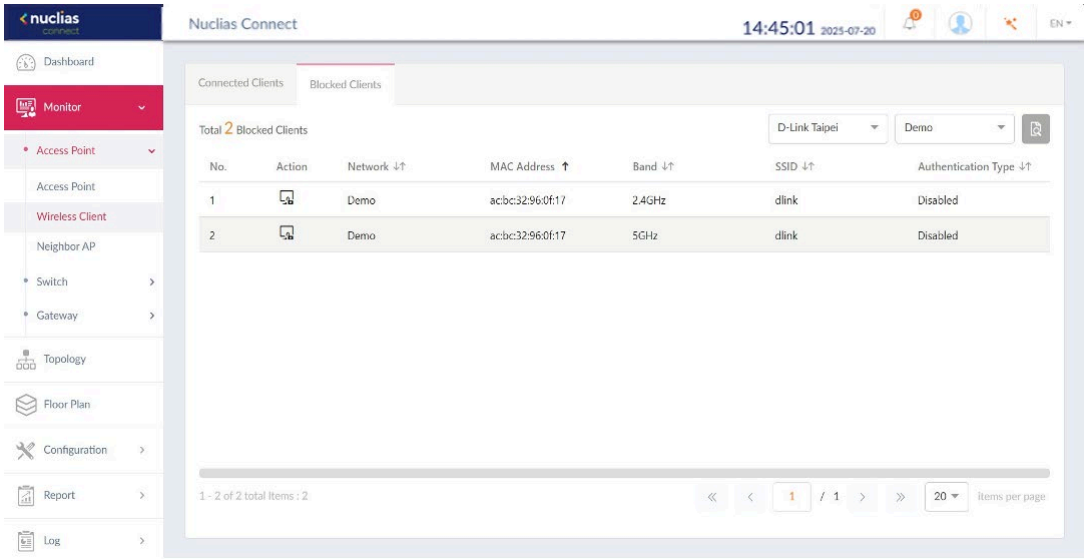


All wireless clients connected to the access points that are managed by this application are displayed. Information such as **Network**, **IP Address**, **IPv6 Address**, **MAC Address**, **Auth. Type**, **OS** (only available on captive portal clients), **Upload**, **Download**, **Channel**, **RSSI (dBm)**, **SNR (dB)**, **Band**, **SSID**, **AP MAC Address**, **Traffic Usage**, **Traffic Usage(%)**, **Last Seen**, and **Uptime** is displayed for each wireless client.

Access Point > Wireless Client > Blocked Clients

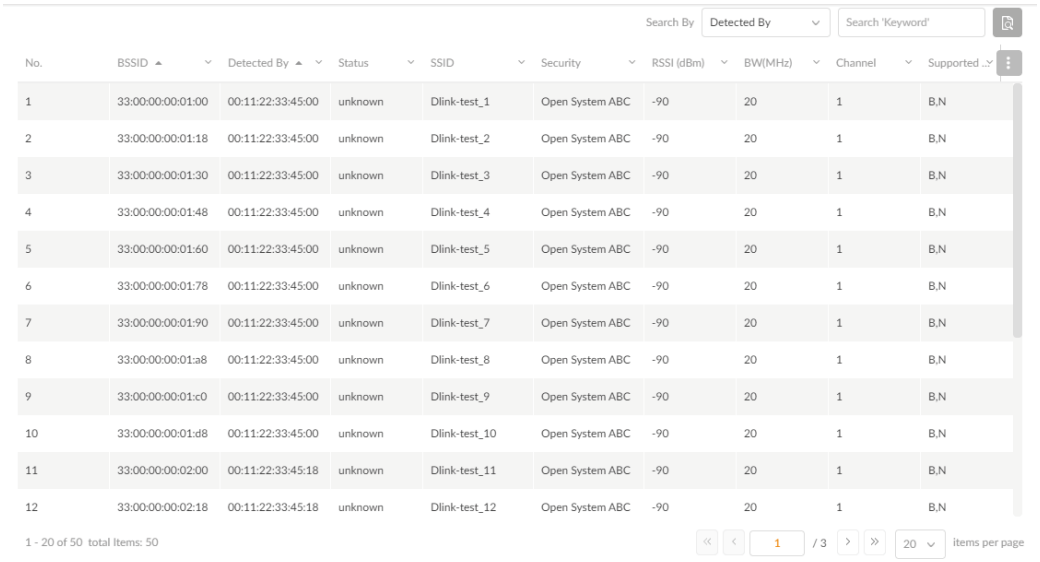
Navigate to **Monitor > Access Point > Wireless Client** on the left panel, then click the **Blocked Clients** tab. Use the **Sites** and **Networks** drop-down menu to select a Site and Network. Click to start the search. Any relevant devices meeting the search criteria will be listed.

The page lists the following information: **Blocked client count**, **Action**, **Network**, **MAC Address**, **Band**, **SSID**, and **Auth. Type**.



Access Point > Neighbor AP

Navigate to **Monitor > Access Point > Neighbor AP** on the left panel, the neighbor AP list is displayed. To enable this function, go to **Configuration > Profile Settings > Site>Network > Wireless Resource > Neighbor AP Detection** and click **Enabled**.



Field	Description
BSSID	Displays the MAC address of the AP's wireless interface.
Detected by	Displays the mac address of AP that the AP was scanning.
Status	Displays the status of AP (Unknown, Known, and Managed).
SSID	Displays the name of the wireless network.
Security	Displays the security status indicating whether encryption is used.
RSSI	Displays the RSSI that the AP was detecting.
BW(MHz)	Displays the channel width that the AP was using.
Channel	Displays the channel setting that the AP was detected on.
Supported Modes	Displays the list of modes that the AP was supported.

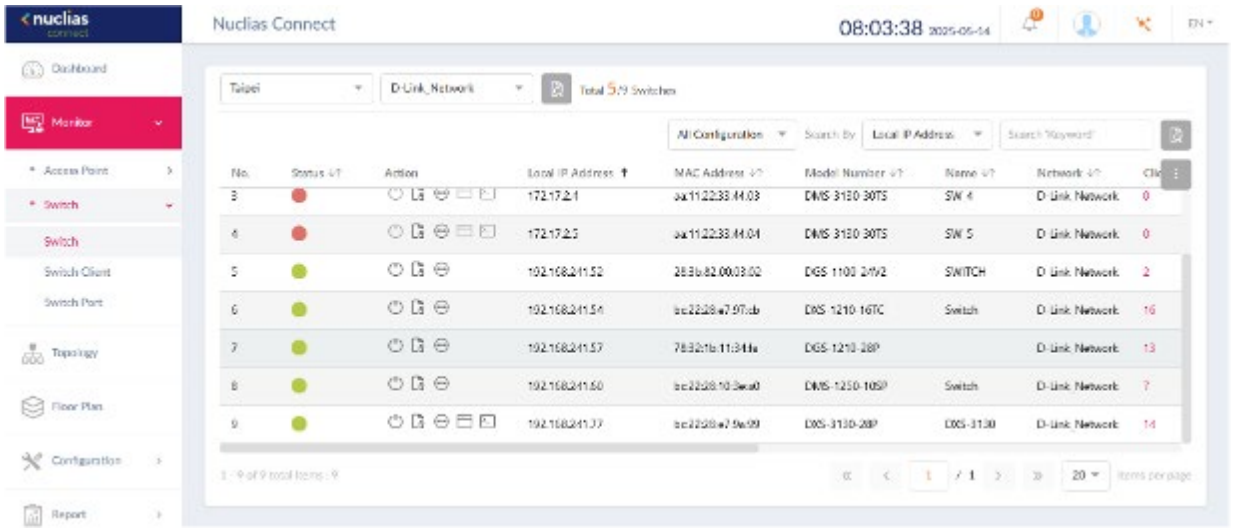
Switch

Go to **Monitor > Switch** and use the Site and Network filter to locate the device you'd like to monitor. On this page, you can view a summary of the devices managed by the application. The summary includes the following: **Status, Local IP Address, NAT IP Address, MAC Address, Model Type, FW Version, HW Version, Serial Number, Name, Location, Site, Network, Network ID, Clients**, **Power Budget, CPU Usage, Memory Usage, Ports, Use Configuration, Last Seen, Uptime** and **Power Delivered.**

Select a configuration type (**Profile, Standalone, All**) and attribute (**Local IP Address**, **MAC Address**, **Model Type**, **FW Version, Name, Ports)** to narrow down the search field or enter a keyword related to the target device in the Search field. Click to start the process. Any relevant devices meeting the search criteria will be listed.

Under the Action panel, click to restart your device. Click to move the device to Unmanaged. Click to enter the Device Detail Page. Click to open device remote web GUI (Only managed switch will appear). Click to open remote CLI embedded UI terminal (Only managed switch will appear).

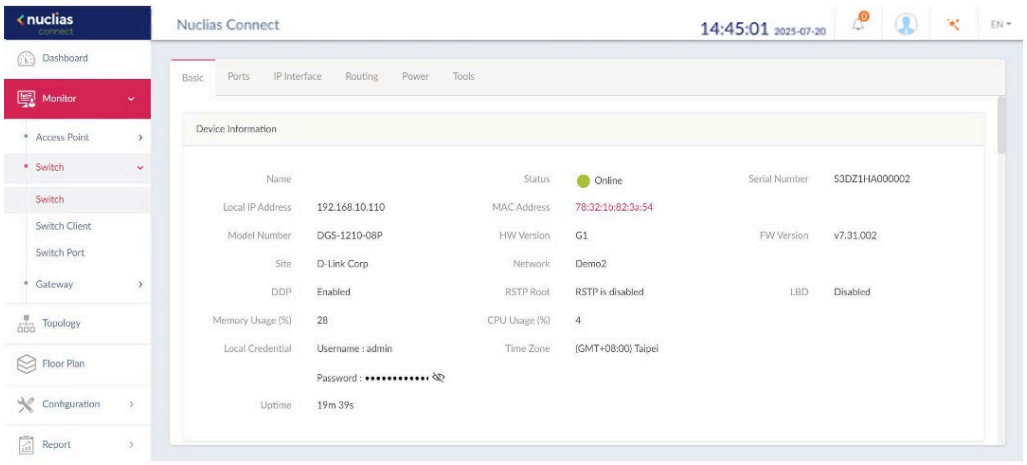
Key Fields	Description
Name	Displays user-defined name of the switch. Empty if no name is given. Click the column to revise or create a name. The max length of the name is 63 characters.
Location	Displays the location of the switch. Click the column to revise or create a name for the location. The max length for the location name is 32 characters.
Clients	Displays the total number of clients connecting to the switch. Click on the Clients number to be directed to the Switch Client page.
Ports	Displays the total number of ports on the switch. Click on the ports to be directed to the Switch Port page.
Use Configuration	Displays the configuration mode (Profile/ Standalone). • Profile: Devices under profile mode share the same configurations in the profile. • Standalone: Devices have their own configurations and do not get affected by profile.
Last Seen	Displays the last connected time of the switch.
Uptime	The activating time of the switch after reboot.



Basic

The device detail page displays comprehensive information of your switches and allows users to configure the ports, IP interface, route settings, and many more. Navigate to **Monitor > Switch** and click **Link to Device Detail Page** under Action.

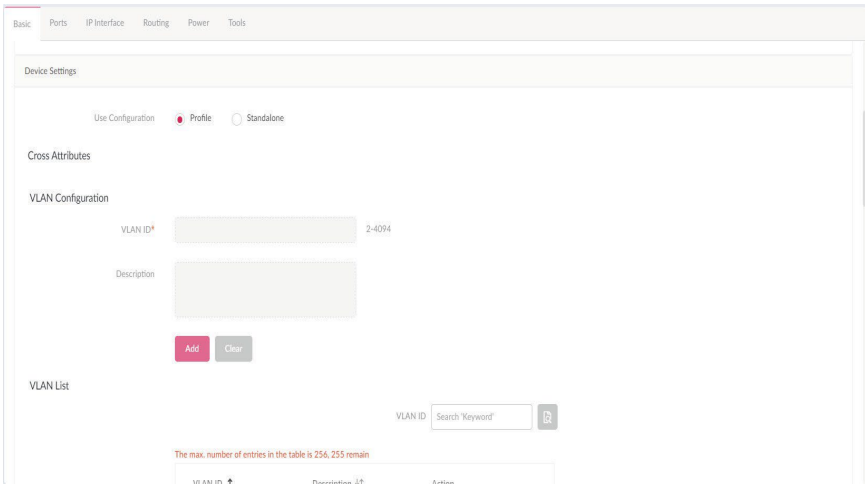
On the **Basic** tab, you can configure your device and view a summary of Device Information. The following information is displayed under the **Device Information** section: **Online Status, Network, DDP, Serial Number, Local Credential, MAC Address, HW Version, LBD, Uptime, Time Zone, Model Type, FW Version, Memory Usage, CPU Usage**, and **RSTP Root**.



Key Fields	Description
DDP	Displays the DDP (D-Link Discovery Protocol) settings of the switch.
Local Credential	Displays the username and password for local GUI/console.
LBD	Displays the LBD (Loopback Detection) settings of the switch.
RSTP Root	Displays the root bridge and its priority of the spanning tree.

In the **Device Settings** section, select a use configuration (Profile or Standalone). If Profile is selected, the subsequent settings, such as VLAN and IGMP Snooping will be fixed. If Standalone is selected, the above-mentioned settings will be available for editing.

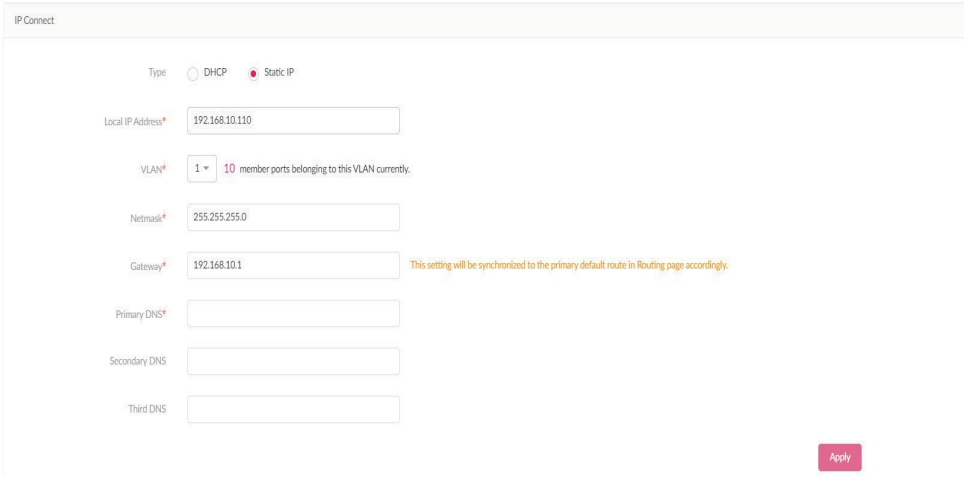
Under **VLAN Configuration**, you can set up a VLAN by entering a VLAN ID (2-4094) and a description for ease of identification. Click Add to create, or Clear to cancel. The created VLAN IDs will be displayed under the VLAN list. Enter a keyword in the search field and click to locate a VLAN ID. Click to edit the ID or click to delete it.



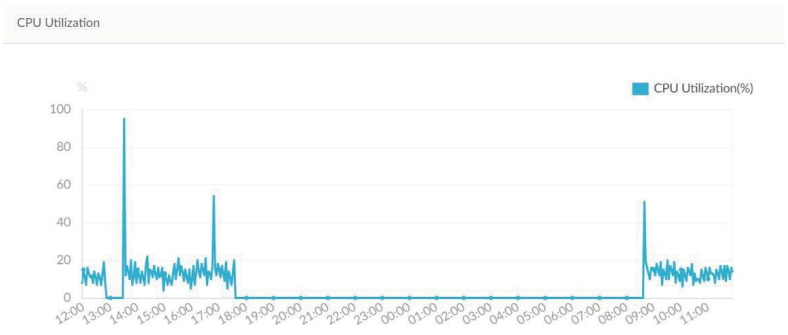
IGMP Snooping is disabled by default. When configuration is set to **Standalone**, you can enable IGMP Snooping. Enter the VLAN to complete the process.

In the **Uncross Attributes** section, features that cannot be configured via profile will be listed here. Enter a name, location, and use the drop down menu to select a STP Bridge Priority. Click Apply to complete the settings.

In the **IP Connect** section, you can deploy primary connections. Choose a type of IP (DHCP or Static IP), and enter a Local IP Address, VLAN (VLAN ID), Netmask, Gateway. If DHCP is selected, enter the DNS. If static IP is selected, enter a Primary DNS, Secondary DNS, Third DNS. Click **Apply** to complete the set up.



In the **CPU utilization** section, a CPU Utilization graph is displayed. On the Y axis shows the percentage of CPU utilization. On the X axis shows the time by hour.



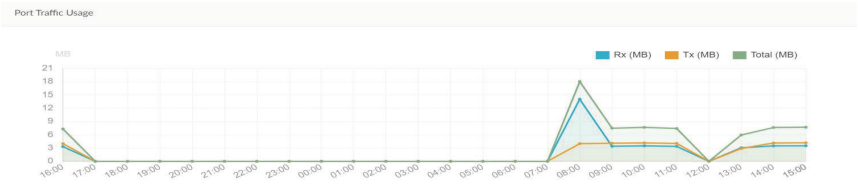
Ports

Under the Ports tab, a port status overview is presented. The graph displays a range of colors and icons to inform users of the status of each individual port. Clicking on the port icons will direct users to the **Port Detail** page of the specified port.

Here's a summary of all the statuses and what they represent:

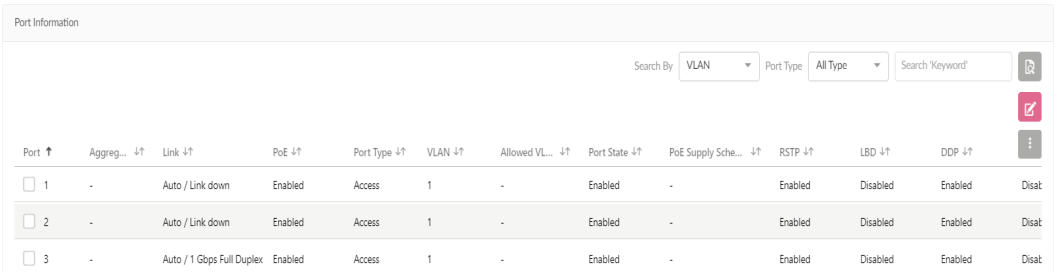
Status	Description
Green	Connected to Gigabit Ethernet
Orange	Connected to 10/100Mbps Ethernet
Dark Gray	Port disconnected
Light Gray	Port disabled
	Powered by PoE
	Port mirrored
Red	Error detected
	PoE+Mirror

In the **Port Traffic Usage** section, a graph indicating Rx and Tx usage based on time is presented.



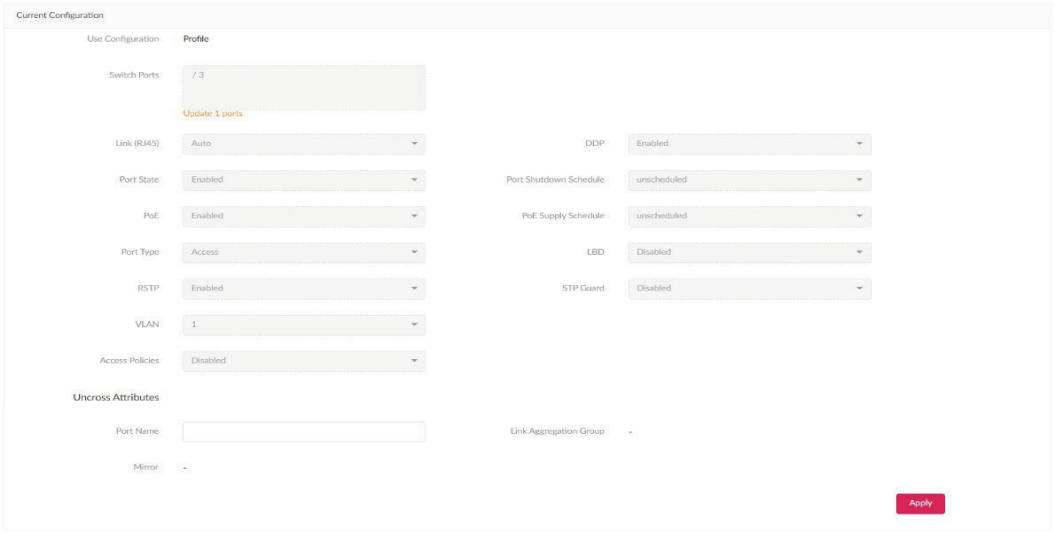
In the **Port Information** section, you can view a summary of all active and inactive ports. The summary includes information such as **port number, Aggregate link status, Tx/Rx/Total bytes, used power, PoE, Port type, VLAN, Allowed VLANs, Port State, PoE Supply Schedule, RSTP, LBD, DDP, Port Shutdown Schedule, Mirror, Access Policies, LLDP**, and **Port Name.**

Use the **Search By** drop down menu to select between VLAN and Port, and select a **Port Type** (Access, Trunk, or all) to narrow down the search or enter a keyword to locate a port.



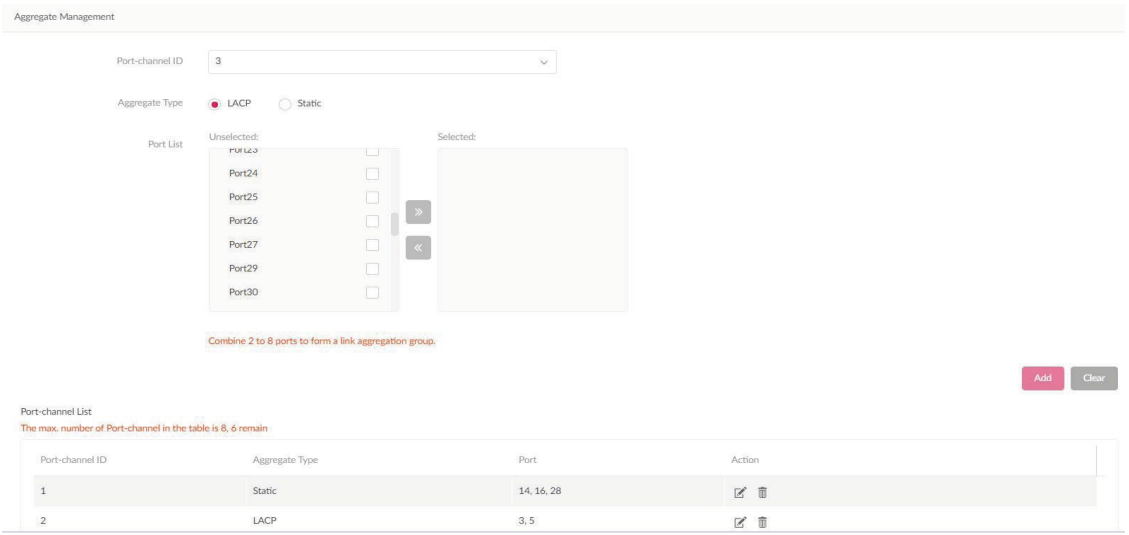
Key Fields	Description
Aggregate	Displays the port-channel ID and aggregate type (static/LACP).
VLAN	Displays the native VLAN ID of Trunk mode or the VLAN ID of Access mode. In addition, it also indicates the Voice VLAN ID when display.
Allowed VLANs	Displays the allowed VLAN ID when the Port Type belongs to Trunk.

To make changes to a port or port group on the switch, first make sure the User Configuration is set to Standalone in the Device Settings section. Next, check the boxes next to the port(s) you'd like to change. Click to edit. Scroll down to access the Port Settings. Once the changes are made, click **Apply** to update the changes.

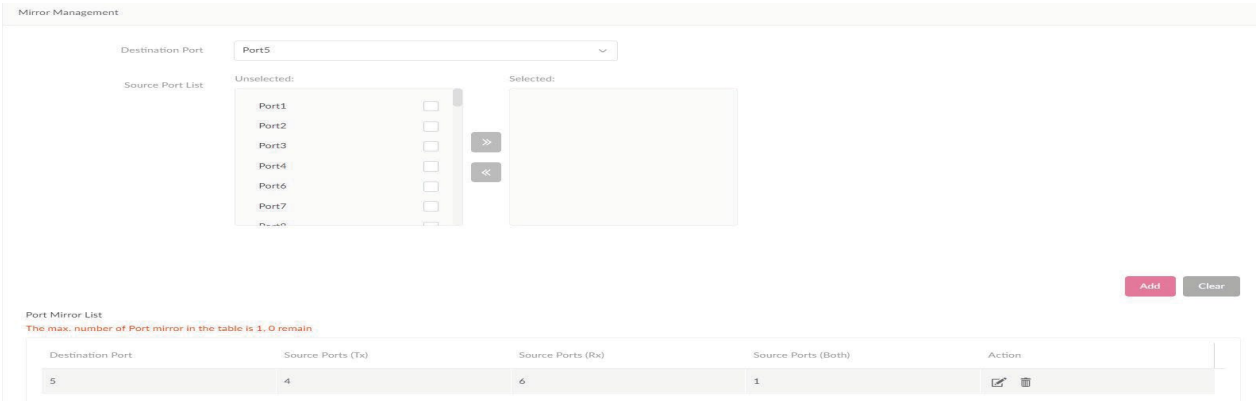


Key Fields	Description
Port Shutdown Schedule	Apply a time profile to the port shutdown function. The time profile is created in the time profile page.
PoE Supply Schedule	Apply a time profile to the PoE supply function.
Port Type	Type: Switch ports can be configured as one of the following two types. (1) Trunk: Trunk port allows the selected port to accept/pass 802.1Q tagged traffic. • Native VLAN: All untagged traffic will be placed on this VLAN. The range is 1-4094. • Allowed VLANs: Only selected VLANs are able to traverse this link. The range is All/1-4094. (2) Access: Access port places all traffic on its defined VLAN. • Access VLAN: All traffic is placed on this VLAN. The range is 1-4094. • Access policy: Apply a restriction policy to this port. • Disabled: All devices can access this port. • Static MAC Whitelist: Only the devices with MAC addresses specified in this list can access this port. • Port Security Delete-on-time Mode: All learned MAC addresses will be purged when an entry is aged out or when the user manually deletes these entries. Users can configure the number of dynamic learned entries via “Dynamic whitelist size limit”. When the total number of “Dynamic Whitelisted MACs” exceeds the value of “Dynamic Whitelist Size Limit”, all subsequent MAC address will be denied access to this port. A table displaying dynamically learned MAC address is available. • User defined access policy: Apply a policy name defined via Access Policy Page.

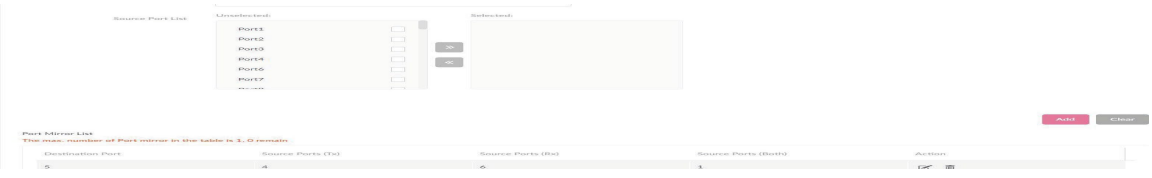
In the **Aggregate Management** section, you can combine a minimum of 2 to 8 network connections into a link aggregation group. From the Port-channel ID drop-down menu, select between 1 to 8. Next, select an aggregate type, **LACP** or **Static**. From the Port list, select 2 to 8 ports to form a link aggregation group. Click **Add** to form, or **Clear** to cancel.
Under the Port-channel List, you'll see a summary list of link aggregation you have created. The summary shows the Port-channel ID, Aggregate Type and Port numbers. Beneath the Action field, click to edit, or to delete. Click Apply to save the changes.



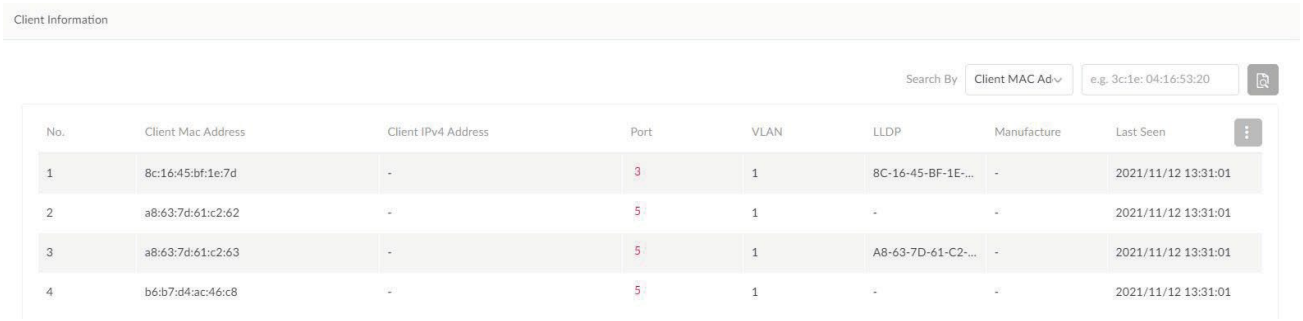
In the **Mirror Management** section, you can mirror the network packet on one switch port to another. First select a Destination Port using the drop-down menu. Next, from the Source Port list, select the ports you'd like to mirror. Once selected, from the drop-down menu, pick the type of traffic to mirror over (Rx, Tx, or Both). Click Add to create, or Clear to cancel.



Under the **Port Mirror** list, you'll see a summary of the ports you have mirrored. The summary displays the Destination Port, and Source Ports(Tx/Rx/Both). Beneath the Action field, click to edit, or to delete. Click Apply to save the changes.



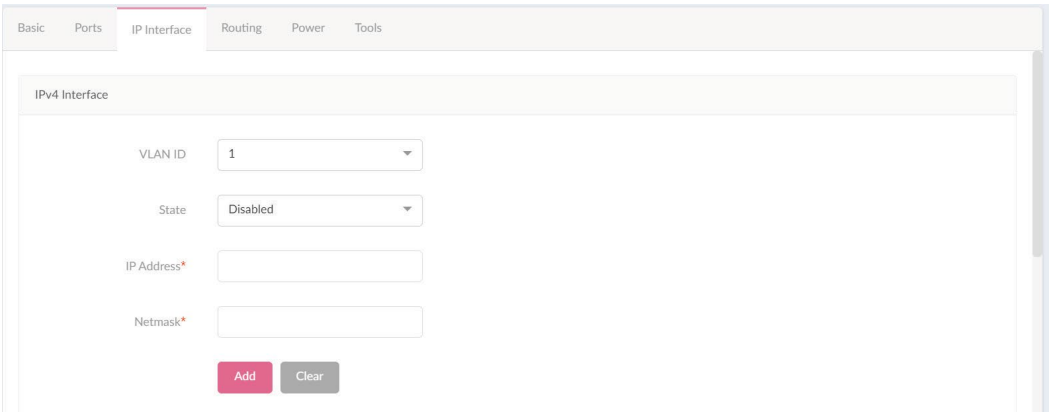
In the **Client Information** section, a summary of client information is displayed. Use the **Search By** drop-down menu to select a criteria to filter the search result. Click to start the search. The following information is displayed in the summary: **Number, Site, Network, Client MAC Address, Client IPv4 Address, Port, VLAN, LLDP, Manufacture**, and **Last Seen.**



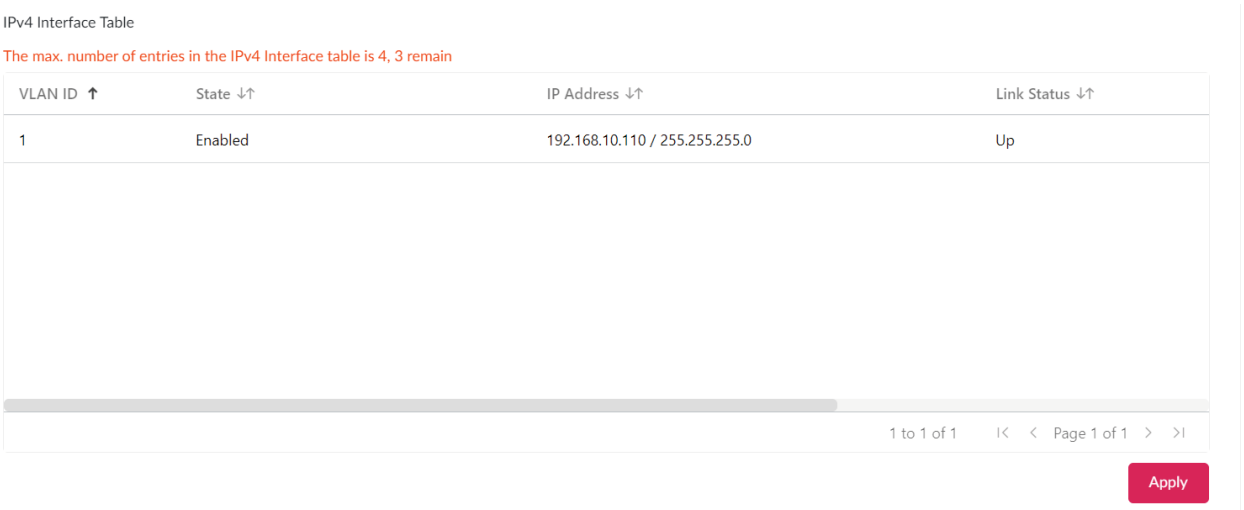
Key Fields	Description
Port	Displays the port number of the switch to which the client is connected to. Click the Port number to be directed to port detail page
LLDP	Displays the LLDP information of neighbors.
Manufacture	Displays the Manufacture name of the remote device via LLDP.
Last Seen	Displays the last time that the client was seen on the network.

Interface

Under the IP Interface tab, you can configure the IPv4 interface and view a summary of their statuses. To create an IPv4 interface, go to **IPv4 Interface**, select a **VLAN ID**, and choose to **Enable** or **Disable** the interface admin state. Enter an IPv4 **IP address** and **Netmask**. Click **Add** to apply the IP interface to a VLAN, or **Clear** to remove the entered values.



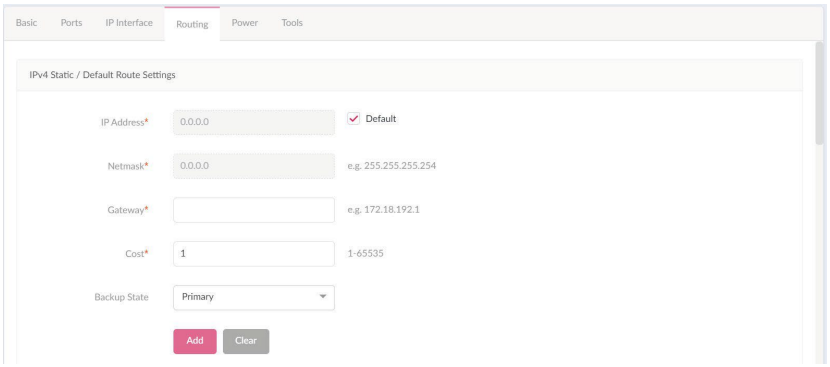
In the IPv4 Interface Table, a summary containing VLAN ID, State, IP Address, and Link Status are displayed. Beneath the Action field, click to edit, or to delete. Click Apply to save the changes.



Routing

In the Routing tab, you can set up static routing for IPv4 formatted addressing. Under the IPv4 Static/Default Route Settings section, enter an **IP address or use the Default route, Netmask, Gateway, Cost**, and **Backup State(Primary/Backup)**. Click **Add** to add the route settings, or **Clear** to clear the values entered.

In the **Static Route Table**, a summary of Static Route containing **Number, IP Address/Netmask, Gateway, Cost, Protocol, Backup**, and **Status** is displayed. Beneath the Action field, click **Delete** to delete the static route. Click **Apply** to apply the settings to the switch.



The IPv4 Route Table stores the routes information of the switch. Use the **Search By** drop-down menu to select a search criteria (**Network/IP Address**) to filter your search. Click to start the search. The following information is presented in the table: **Number, IP Address, Netmask, Gateway, Interface Name, Cost**, and **Protocol**.

IPv4 Route Table

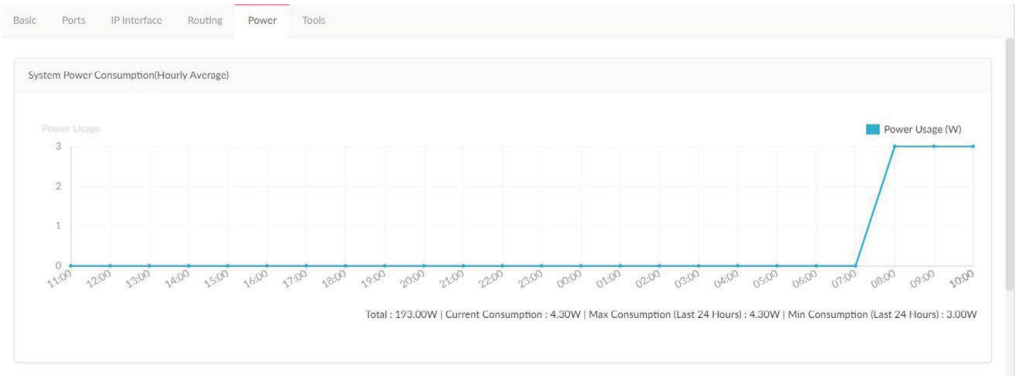
Search By: Network Address — e.g. 172.18.208.11/24

No.	IP Address	Netmask	Gateway	Interface Name	Cost	Protocol
1	0.0.0.0	0.0.0.0	192.168.10.1	System	1	static
2	192.168.10.0			System	0	
3	192.168.10.1			System	0	
4	192.168.10.110			System	0	
5	192.168.10.255			System	0	
6	192.168.10.92			System	0	

Power

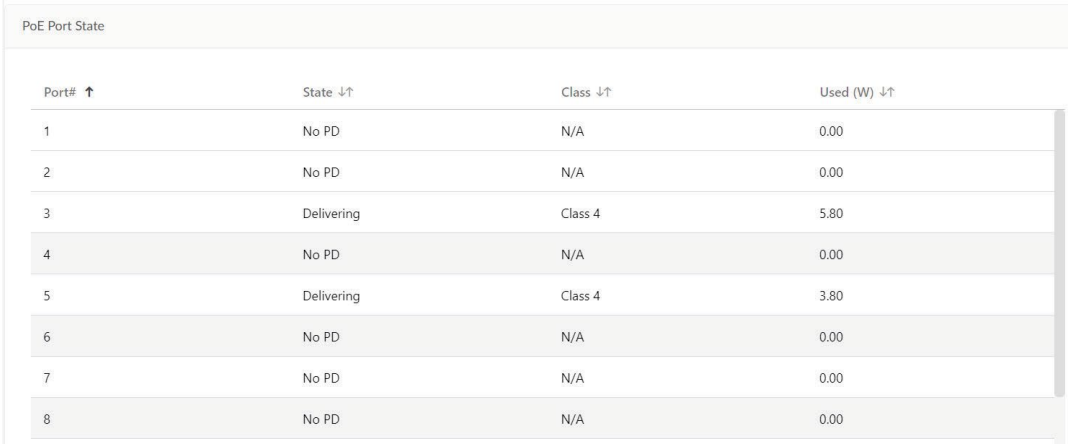
Under the Power tab, the **System Power Consumption** chart and **PoE Port State** summary are displayed. Note that the Power tab will only be available if your switch supports PoE.

The System Power Consumption chart shows your switch's power usage in watt by the hour, as well as the total, current, minimum, and maximum power consumption.



The PoE Port State summary shows the IEEE classification and the power consumption of each port on the switch. The following table describes each of the field in the summary:

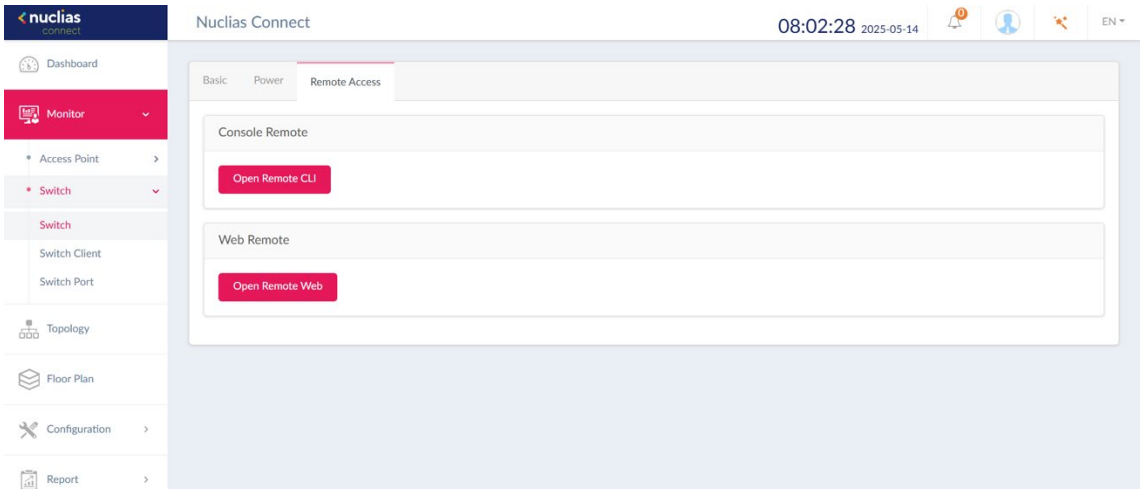
Field	Description
No.	Port number
State	PoE port status.
Class	The IEEE classification: N/A or a value from IEEE class 0 to 4.
Used(W)	The amount of power that is currently allocated to PoE ports in watts.



Remote Access

Under the Remote Access tab, you can use remote tunnel access technology to connect to the device. Note that the feature will only appear on managed switch devices.

Open Remote Web/CLI button unable to operate when user permissions are insufficient. When user permission is “Root User” or “Local User” or “Local Admin”, the button is shown as disabled



Click Open Remote CLI to jump to embedded UI terminal page

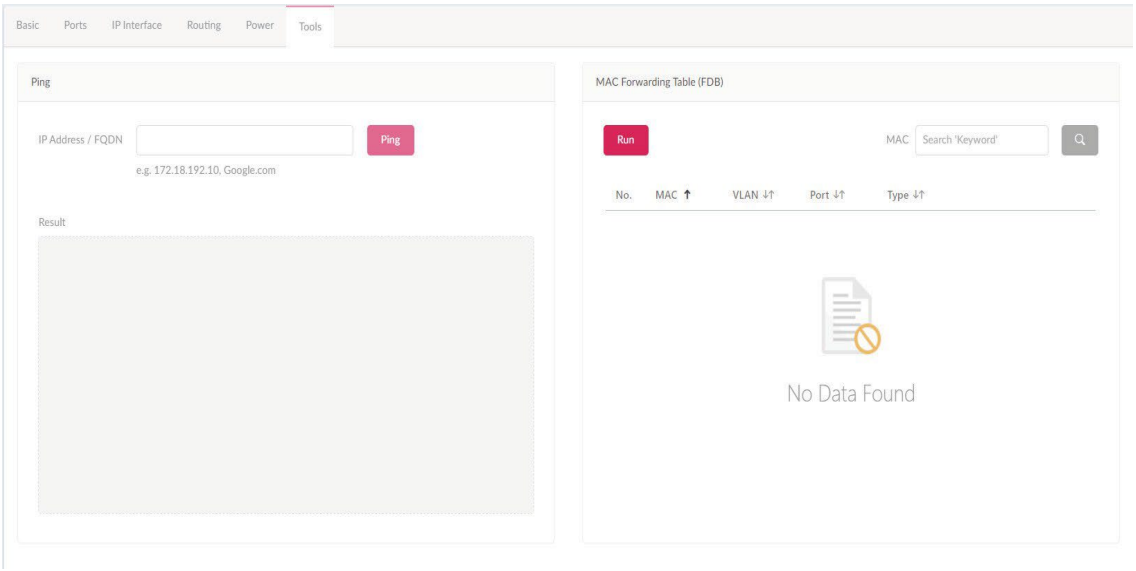
Click Open Remote Web to open device web GUI

Tools

Under the Tools tab, you're presented with the following tests to help troubleshooting: **Ping, Locate Device, Cable Test, Cycle PoE, MAC Forwarding Table**, and **Copy Configuration to Other Device**. Note that the tools are disabled when your devices are offline.

The **Ping Tool** can identify if a connection is working. Enter a host name or IP address and click **Ping** to perform the ping test. When the server received the ping signal, a summary of Ping Statistics including **Packet sent, received**, and **lost** is displayed. If no signal is received, the message "The device is unreachable" is displayed.

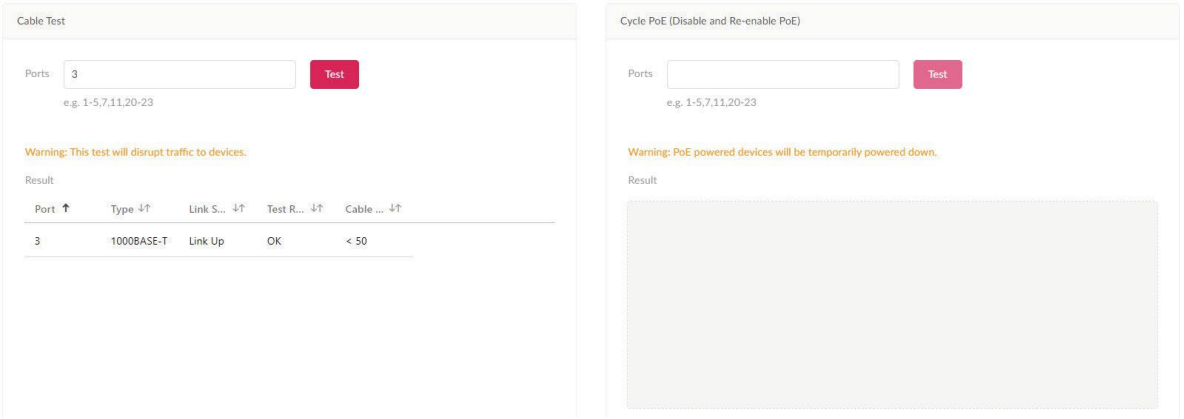
The **MAC Forwarding Table** shows a summary of **MAC addresses, VLAN, Port**, and **IP Address Type**. Press Run to begin the process. On the MAC search filed, enter a relevant keyword to help locate the MAC address.



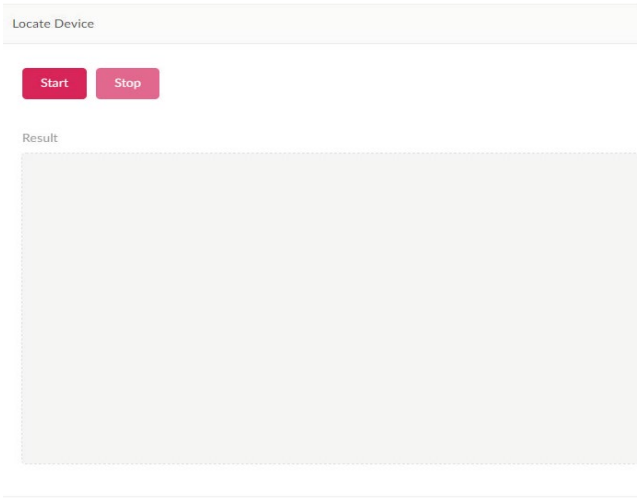
The **Cable Test** allows you to test the connectivity of one or multiple ports. Enter a number of port(s) and click Test to begin the process. The following information will be displayed: **Port number, Type, Link Status, Test Result**, and **Cable Length.** Under the Test Result field, 5 statuses can be displayed: **OK, Open, Short, Test failed** *and* **-.**

Note: The cable test will disrupt traffic to devices.

The **Cycle PoE** tool allows you to disable or enable PoE on specific ports. This tool can only be executed when PoE is enabled. Note that if the switch does not support PoE, this section will be disabled.

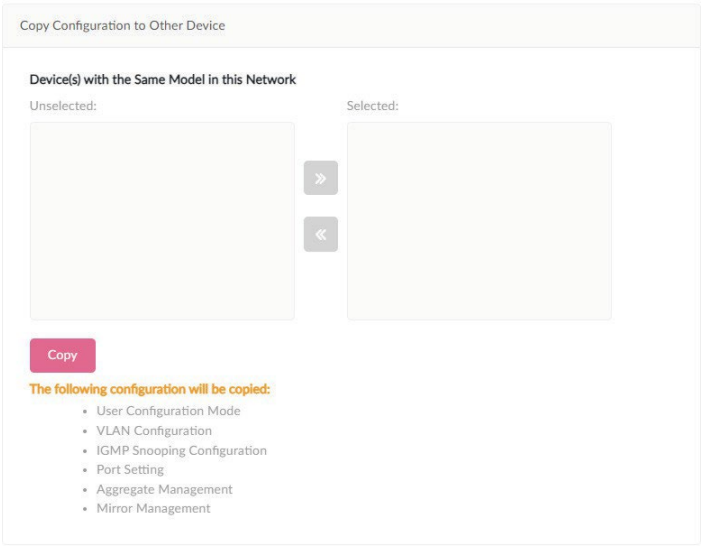


The **Locate Device** function can help identify unlabeled switches by lighting up the LEDs on the switch. Click the Start button to light up the switch. All LEDs will light up in green for 5 minutes. Click the Stop button to stop the light immediately. If a device is located, the message "Locating device..." will be displayed under the Locate Device Result field. If no devices can be located, a message "The device is unreachable" will be displayed. If the server receives failure message sent by the switch, a message "Locate device failed" will be displayed.



The **Copy Configuration** function allows you to copy **Configuration Mode, VLAN Configuration, IGMP Snooping, Port Settings, Aggregate Management**, and **Mirror Management** settings from your device to other device(s) in the network. (Note that the two device needs to be the same model.)

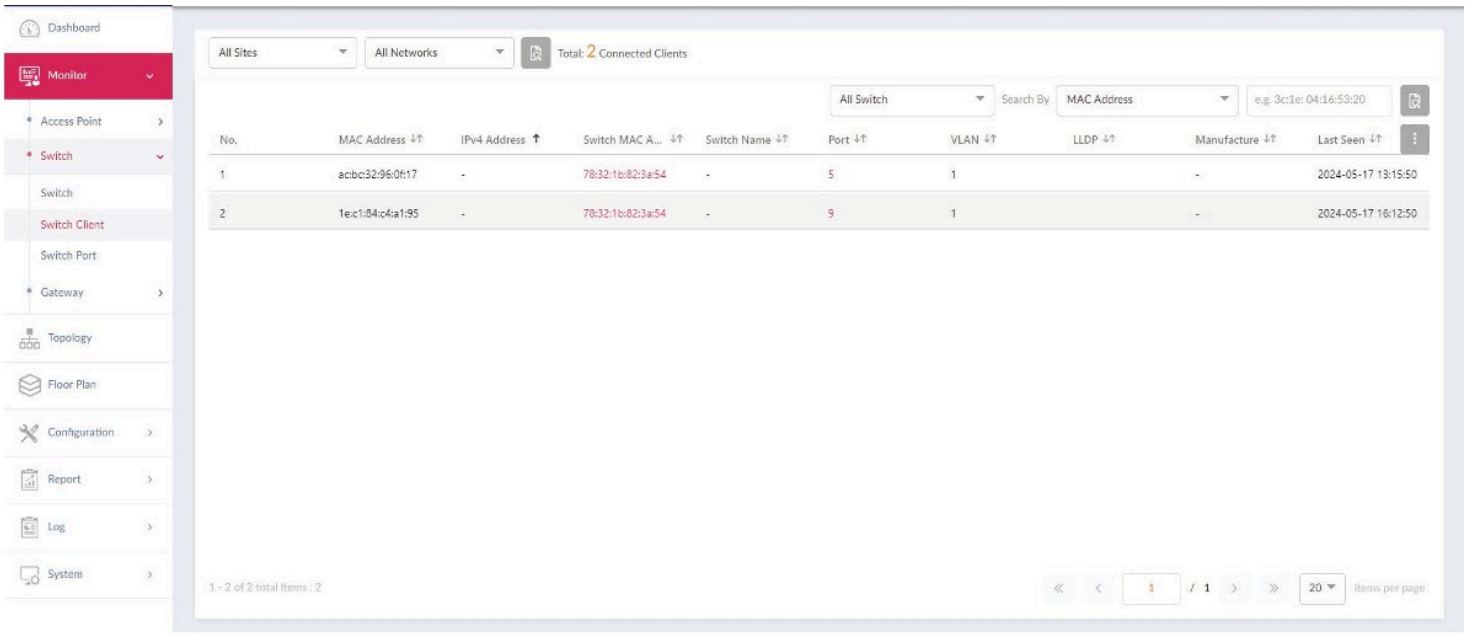
To copy the configuration, select the switch(es) in the network that will be copied. Click the **Copy** button to copy the configuration from your device to the selected device(s). A pop-up window will confirm once again. Click Copy to continue or Cancel to stop.



Switch Client

The Switch Client page displays a cumulative list of all the active client devices that are connected to the switch network. The following information is displayed: **Number, Client MAC Address, Client IPv4 Address, Switch MAC Address, Switch Name, Port, VLAN, LLDP, Manufacturer**, and **Last Seen**.

Use the **Site and Network** drop-down menu to filter the information and click to start the search. Likewise, you can use the **Switch** and **Search By** drop-down menu to select a criterion (**Client MAC address, Client IPv4 Address, VLAN** and **Port**) and enter relevant keywords to narrow the search result.

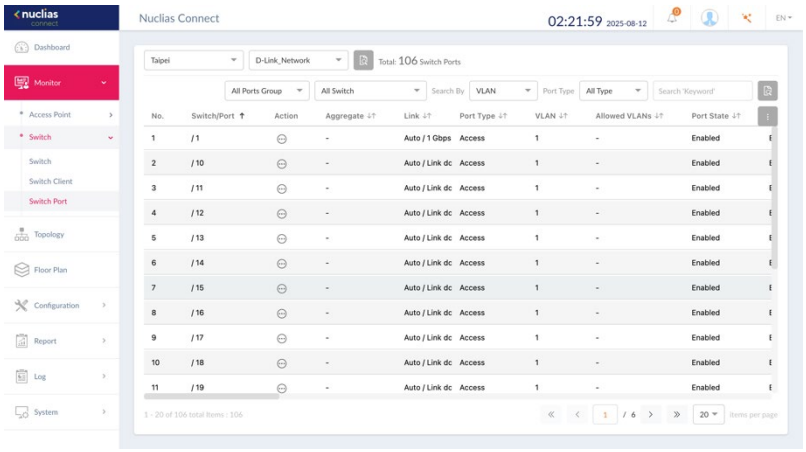


Key Fields	Description
Switch MAC Address	Displays the MAC Address of the switch that the client is connected to. Click the MAC Address to be redirected to the switch detail page.
Port	Displays the port number of the D-Link switch that the client is connected to. Click the port number, it will be directed to per port page.

Switch Port

Under the Switch Port section, you can view the statuses of all the switch ports from all sites and networks. Use the Sites and Networks drop-down menu to filter the search. Click to start the search. Subsequently, use the Ports Group and Switch drop-down menu to filter the search, and select **VLAN/Port** and **Access/Trunk/All** from the **Search By** and **Port Type** drop down menu respectively. Under the Search column, enter a relevant keyword to narrow the search. Click to start the search.

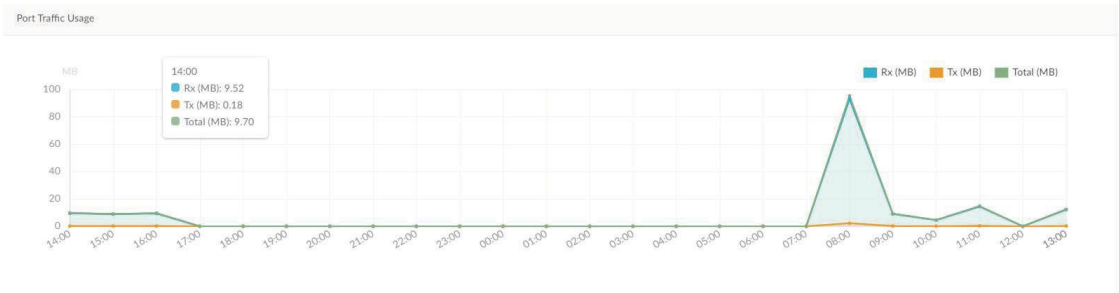
The following information is displayed: Number, Switch/Port, Aggregate, Link, Port Type, VLAN, Allowed VLANs, Port State, PoE, Ports, RSTP, LBD, DDP, Port Shutdown Schedule, PoE Supply Schedule, Access Policies, Mirror, LLDP, Port Name, Rx Broadcast Packets, Tx Broadcast Packets, Rx Multicast Packets, Tx Multicast Packets, Rx Bytes, Tx Bytes, Rx Packets, Tx Packets, and Total Bytes.

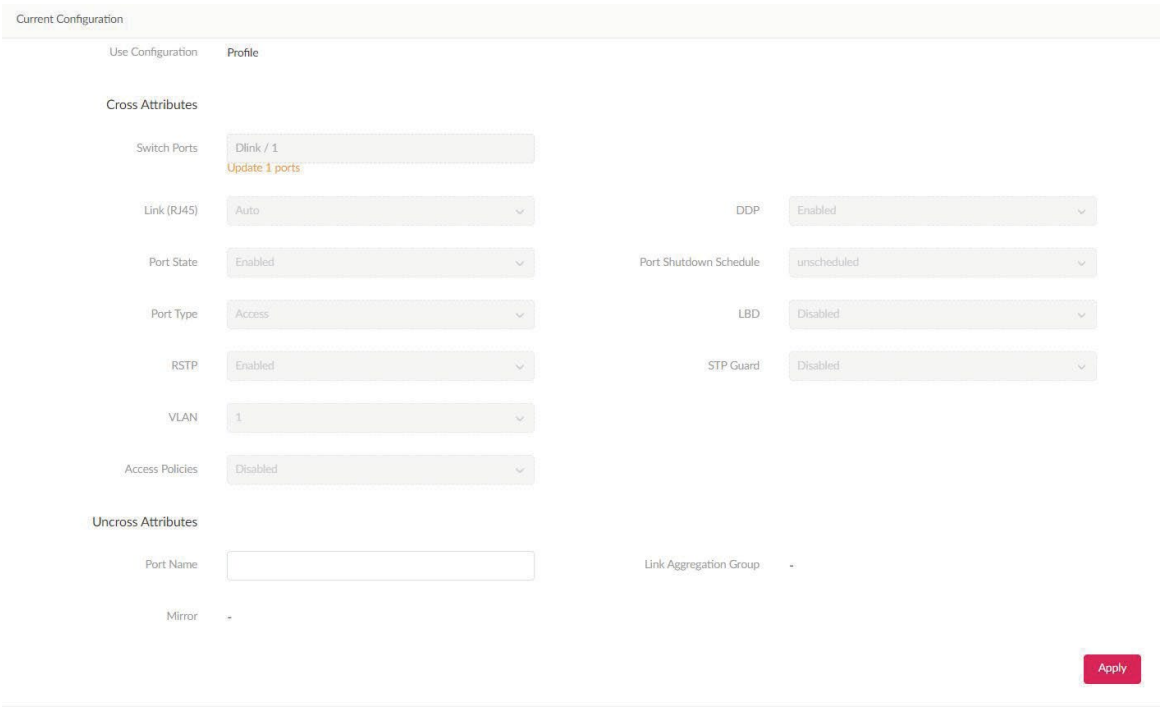


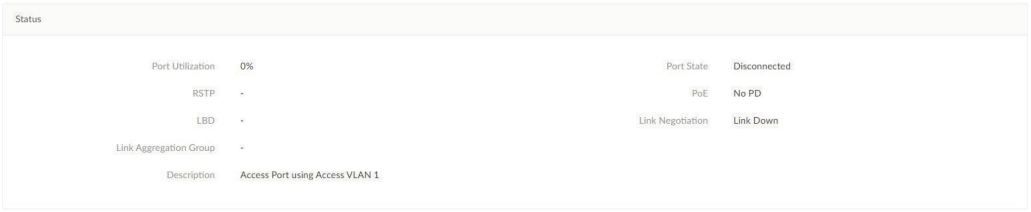
Key Fields	Description
Switch/ Port	Displays the switch name and the port number.
Aggregate	Displays the link aggregation type (Static/LACP/-) of the port-channel group.
Link	Displays link configuration and link status of the port.

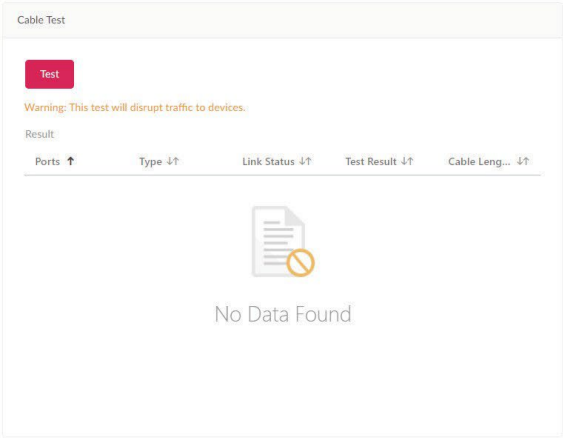
Under the **Action** field, click to go to the Port Detail page. You'll be directed to detail page for the specific port of the switch you have selected.

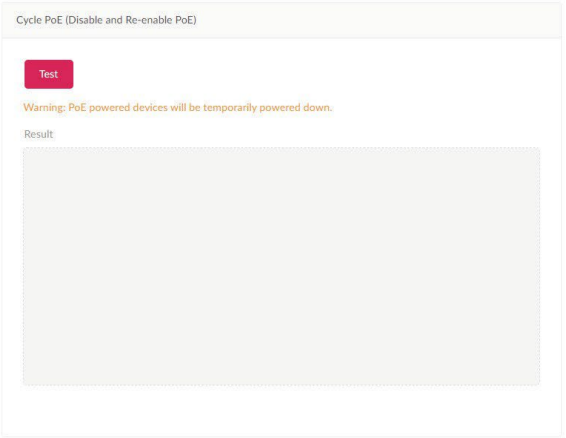
In the Port Detail page, you get an overview of the Switch Port Connection Status, Port Traffic Usage, Current Configuration, Port Status, Testing Tools including Cable Test and Cycle PoE, Packet Overview and Client Information.




Current Configuration
Use Configuration
Profile
Cross Attributes
Switch Ports
Dlink / 1
Update 1 ports
Link (RJ45)
Auto
DDP
Enabled
Port State
Enabled
Port Shutdown Schedule
unscheduled
Port Type
Access
LBD
Disabled
RSTP
Enabled
STP Guard
Disabled
VLAN
1
Access Policies
Disabled
Uncross Attributes
Port Name
Link Aggregation Group
-
Mirror
-
Apply


Status
Port Utilization
0%
Port State
Disconnected
RSTP
-
PoE
No PD
LBD
-
Link Negotiation
Link Down
Link Aggregation Group
-
Description
Access Port using Access VLAN 1


Cable Test
Test
Warning: This test will disrupt traffic to devices.
Result
Ports
Type
Link Status
Test Result
Cable Leng...
No Data Found


Cycle PoE (Disable and Re-enable PoE)
Test
Warning: PoE powered devices will be temporarily powered down.
Result

Overview Packets

Time Frame Last 15 Minutes

	Total	Rx	Tx	Rate (Rx,Tx)
Broadcast	0	0	0	-
CRC Error	0	0	0	-
Collision	0	0	0	-
Discard	0	0	0	-
Error	0	0	0	-
Fragment	0	0	0	-
Multicast	0	0	0	-
Total Traffic	0	0	0	-

Client Information

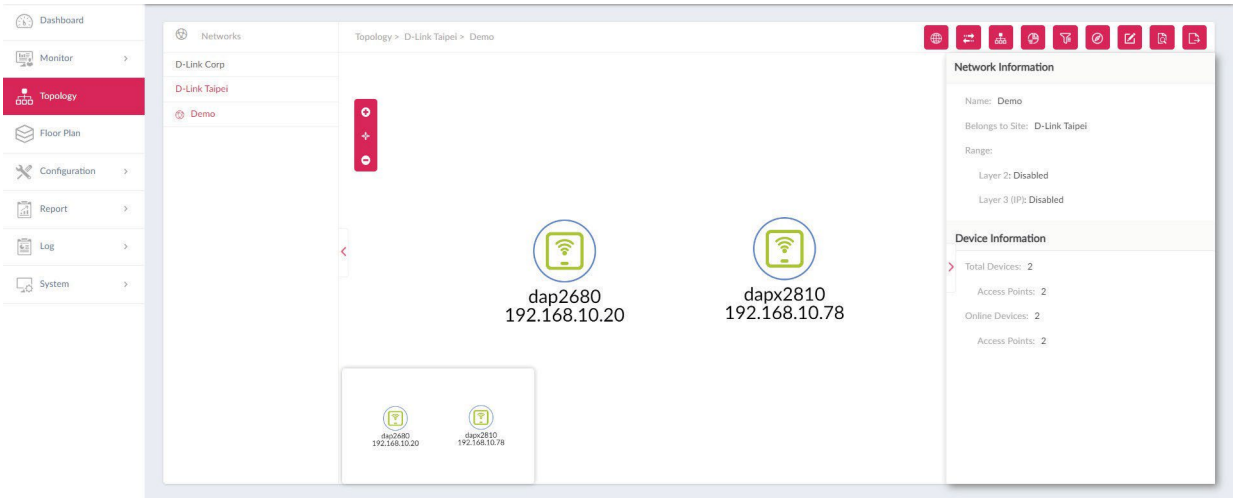
Search By Client MAC Ad e.g. 3c:1e: 04:16:53:20

No.	Client Mac Address	Client IPv4 Address	Port	VLAN	LLDP	Manufacture
1	00:0e:c6:f5:50:38	-	1	1	-	-
2	00:1d:aa:3f:ea:a9	-	1	1	-	-
3	00:1e:58:98:8f:5e	-	1	1	-	-
4	00:1e:e3:12:34:56	-	1	1	-	-
5	00:13:46:da:e8:83	-	1	1	-	-
6	00:23:7d:9e:b1:70	-	1	1	-	-
7	00:24:b2:58:ee:ab	-	1	1	-	-

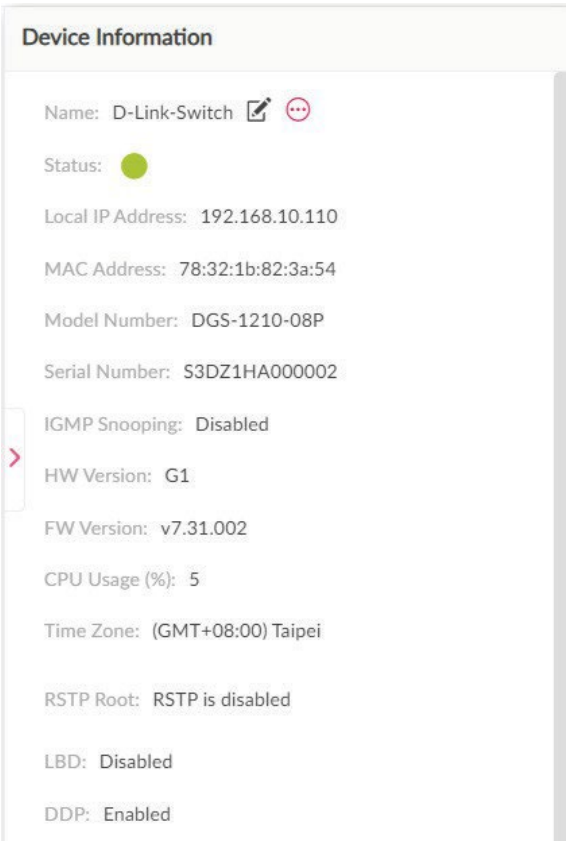
Topology

Under the Topology page, users can view the topological relations between switch devices and access points in a network. Press to zoom in, to zoom out, and to reset the topology. A basic network and device summary is displayed. The following information is included: Network name, Belonging Site, Range, Total Device/Switch, Online Device/Switch.

Select an access point or switch from the site and network. The Device and Link information will be displayed on the right side. Clicking on the green device icon will reveal detailed device information. Clicking on the link will reveal the Link information.

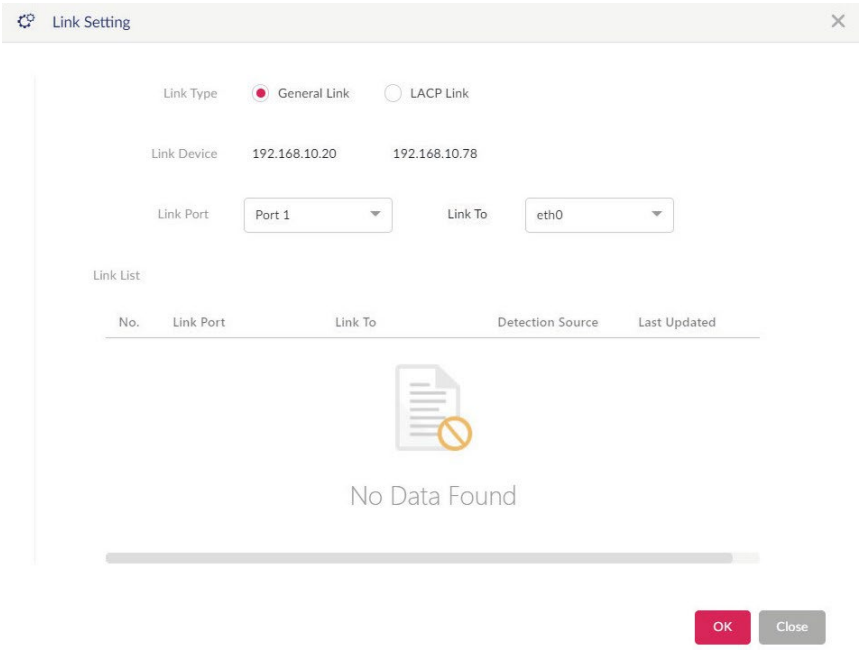


AP Device Detail Field	Description
Name	Displays the name to identify the switch on server. Click the name to be redirected to the device detail page. Note that the AP name must be unique to the Site.
Status	Displays the connection status of the AP: Online, Offline or Unmanaged. Green indicates online, red indicates offline.
Local IP Address	Displays the IP address.
MAC Address	Displays the system MAC address of the device.
Model Type	Displays the model type of the device.
Hardware Version	Displays the hardware version of the device. **FW version** Displays the Firmware version
CPU Usage (%)	Displays the CPU Usage of the device. **Memory Usage (%)** Displays the memory usage of the device. **Upload** Displays the upload traffic of the device.
Download	Displays the download traffic of the device.
Uptime	Display the activating time of the AP since after last start or reboot.
Location	Displays the location of the device.



Switch Device Field	Detail Description
Name	Displays the switch name on the server. Click the name to be directed to the device detail page. Note that the switch name must be unique to the Site.
Status	Displays the connection status of the switch: Online or offline. Green indicates online, red indicates offline and is unreachable by the server.
IP Address	Displays the IPv4 address. Note: User configured IPv4 address is displayed when the device is unknown.
MAC Address	Displays the system MAC address of the switch.
Model Type	Displays the model type of the switch.
Serial Number	Displays the serial number of the switch.
IGMP Snooping	Displays the state of IGMP snooping.
RSTP Root	Displays the root bridge and its spanning tree priority. Display format. • "Root is X/ root bridge priority: Y" X represents device name (System name) of the root switch. Y represents bridge priority of root switch. • "RSTP is disabled" - When RSTP is not enabled on the switch - RSTP is enabled only on the switch, not the ports. • "-" When the switch is offline or doesn't relay the information.
DDP	Display the DDP setting of the switch.
LBD	Display the LBD setting of the switch.
IGMP Snooping	Displays the state of IGMP snooping.
Hardware Version	Displays the hardware version of the switch.
CPU Usage (%)	Displays the CPU Usage of the switch.
FW Version	Displays the Firmware version of the switch.
Time zone	Displays the time zone which the device belongs to.
Uptime	Display the activating time of the switch after the last start or reboot.
Location	Displays the location of the switch.

Users can also view relations between two devices by manually defining the link. Click to begin editing. Click on one of the targeted device icons, then click another device icon to create a linkage. Once created, the Link Setting page is displayed.
Below charts explain what each field entails.



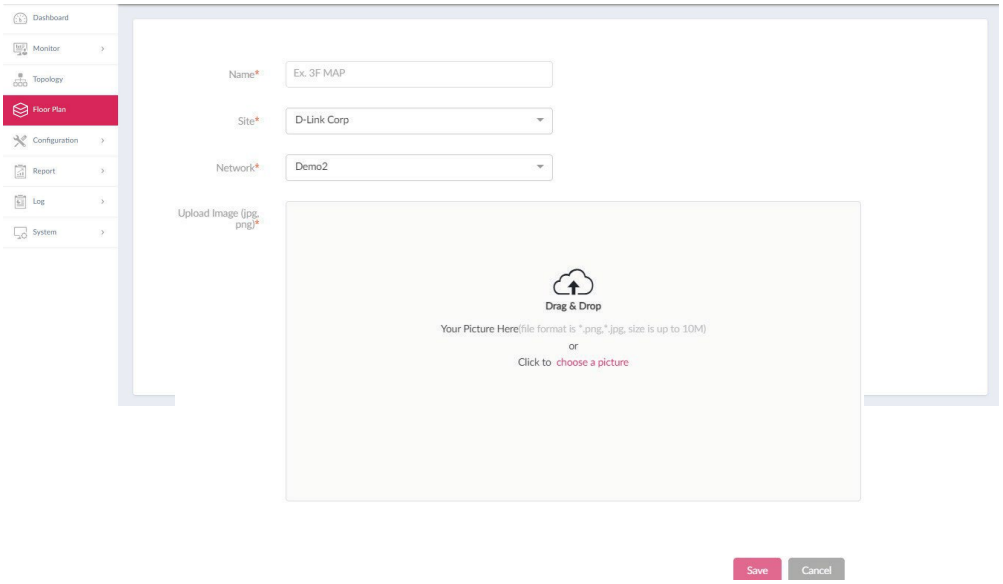
On the upper right corner, there are options available to modify and check basic information of the switches and access points.

Click to show Network and Device information. Click to change the background image of the topology. Click to configure the arrangement type (Star/Tree) and Central Device. Click to view the Topological Legend, or the meaning of symbols and colors used on the topology. Click to set the display content for node information (IP Address or Name). Click to rediscover the topology. Click to search for matching devices in the network, and finally, click to export the topology as a PDF file.

Floor Plan

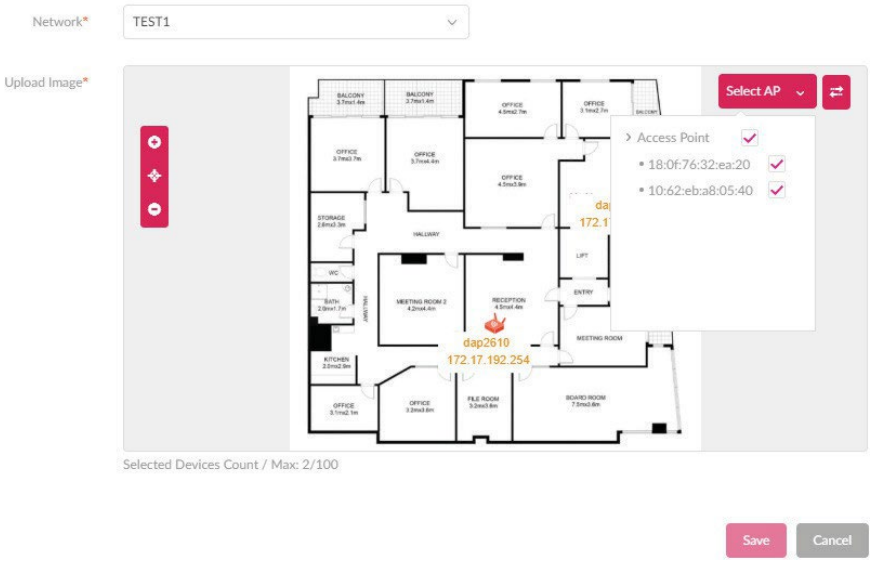
Floor plan is a drawing to scale, a bird's-eye view of the relationships between rooms, spaces, traffic patterns, and other physical features at one level of a structure.

Click "here" to add a new floor image, enter a name and select Site and Network.



Click "choose a picture" to upload the image, then click "Save".

Click **Select AP** to choose devices, move devices to the correct position and save it.

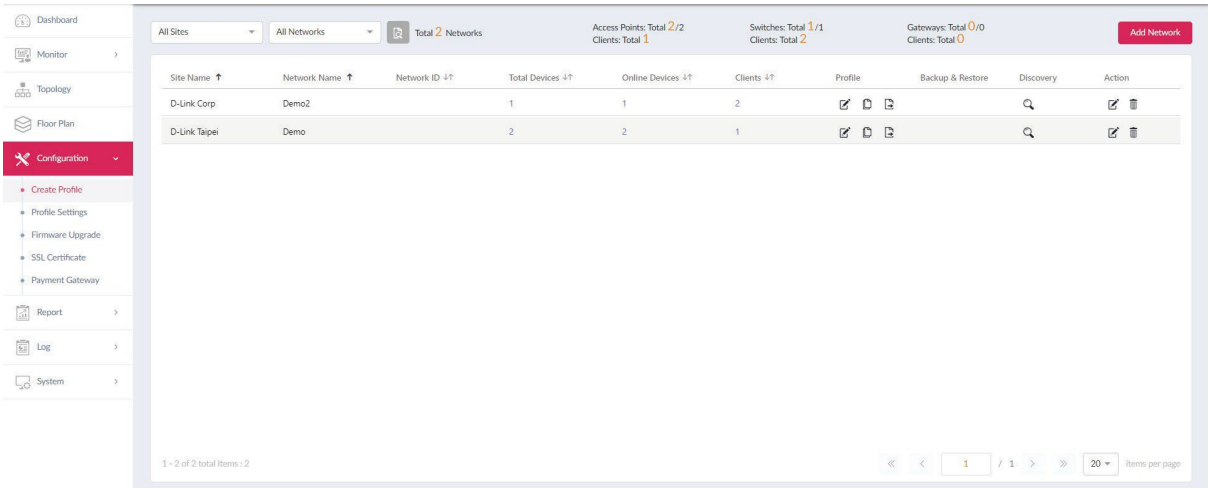


Configuration

Create Profile

Navigate to **Configuration > Create Profile,** click **Add Network** to create a new site and network. All available sites and networks are listed on the Default page. See the following for further information.

Field	Description
Edit Profile	Opens Profile Settings page of the selected site. The security, access control, user authentication settings , many more are available.
Copy Profile to this Network	Copy existing profile to a designated site and network.
Export Network Profile	Export selected profile to a file (*.dat) on a local directory
Discovery	Opens the Discovery Network Settings page. From this page, you can search for devices located on L2 protocol layer or specific IP addresses / Prefix subnet IPs. Once the criteria are defined, click Next. Click Start Discovery to find begin the search (Configurable and Managed devices).
Edit Network	Opens the Edit Network page. From this page, you can edit network settings or migrate to a new or existing site.
Delete Network	Delete the selected network configuration.



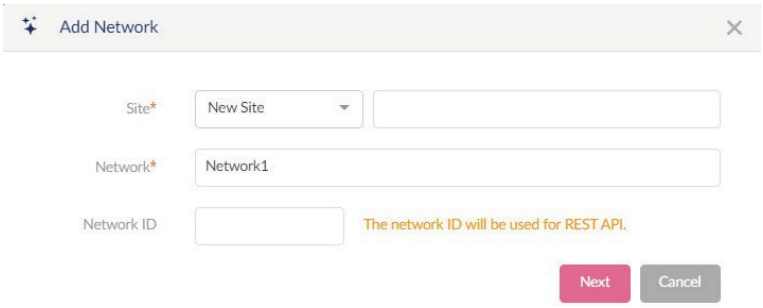
Add Network

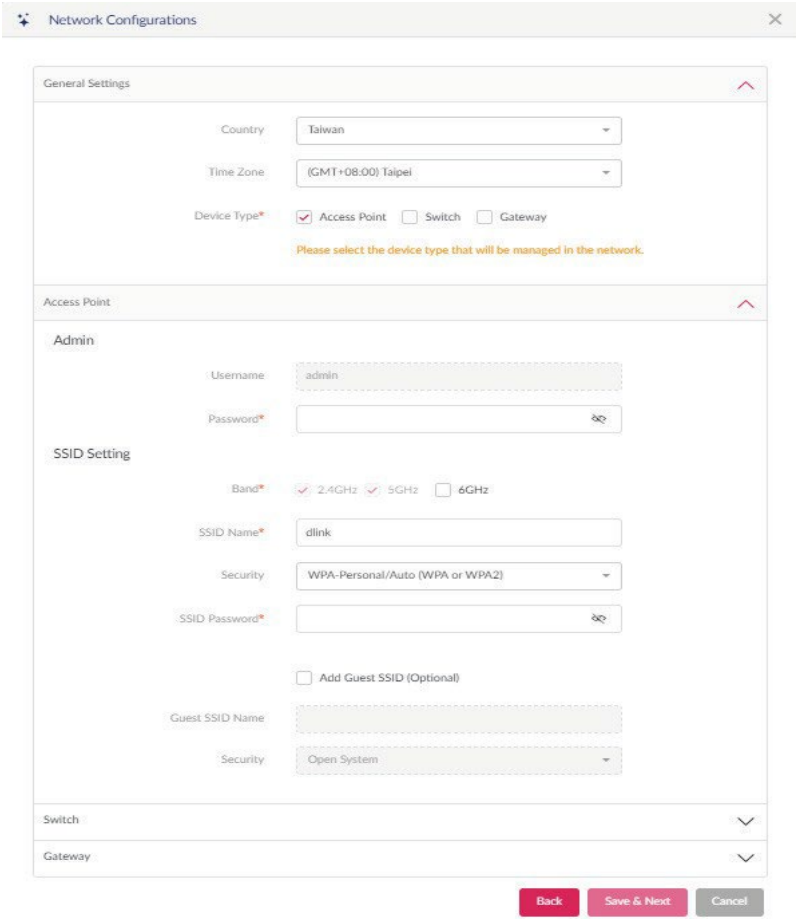
From the Create Profile link, click on **Add Network** to create a new network.

The Add Network page is displayed. From the Site drop-down menu, select an existing site or a new Site and enter the name of the site in the empty field.

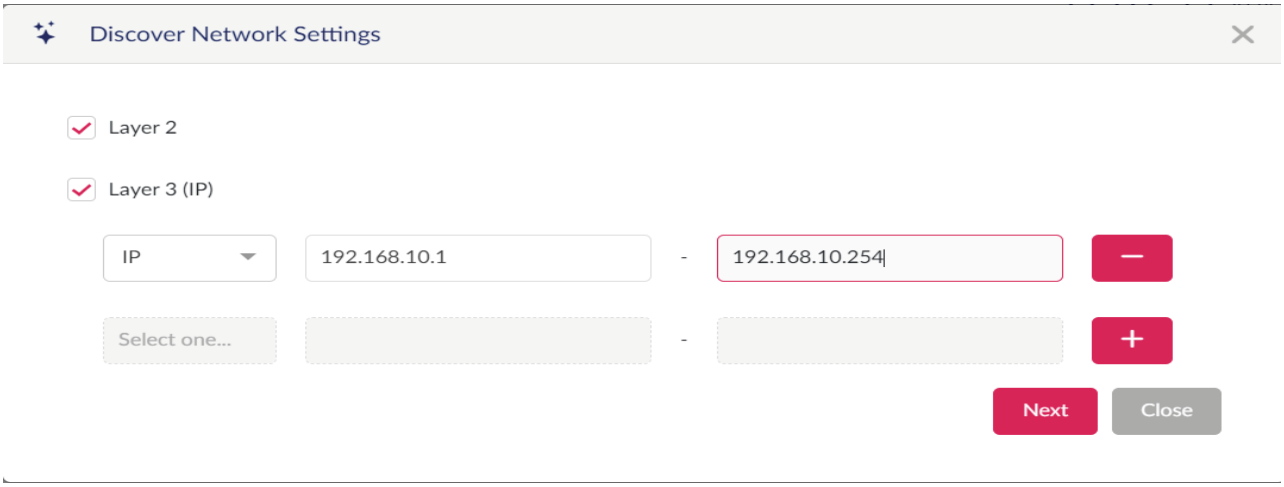
In the Network Name field, enter the name to identify the new network. Click **Next** to continue or **Exit** to return to the previous screen.

The Network Configurations page will appear. Enter the wireless and device settings to define the network configuration. Click **Next** to continue. To return to the previous page, click **Back** or click **Exit** to discontinue the configuration process. The Network ID field is optional and is used for REST API function. Leave it as empty if you're not intended to use REST API.

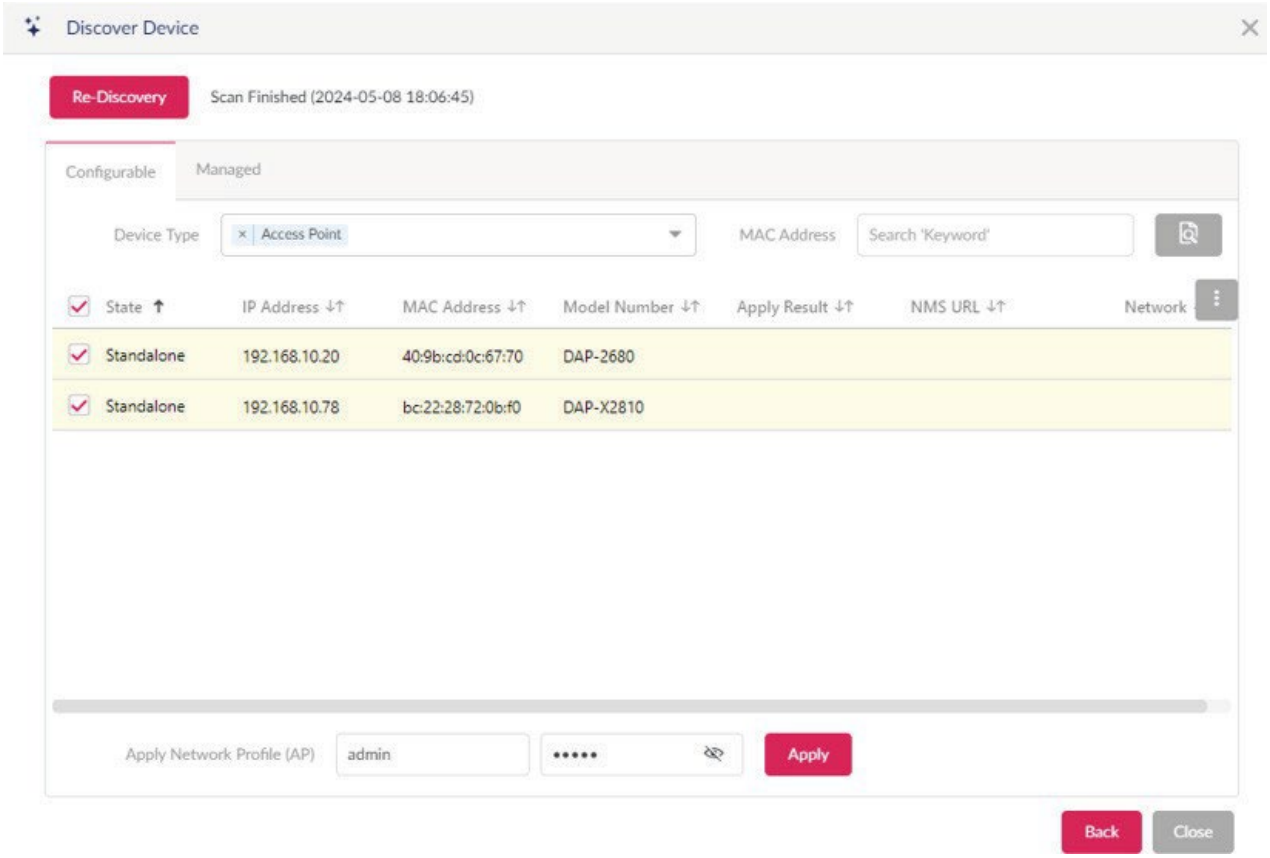




The Discover Network Settings page is displayed. Select the data link layer (layer 2 or layer 3) to define the type of network to run on. If Layer 3 is selected, click the drop-down menu to define either an IP or a prefix segmentation. Click + to add additional IP/prefix segments or **Next** to continue. Click **Exit** to discontinue the configuration process.



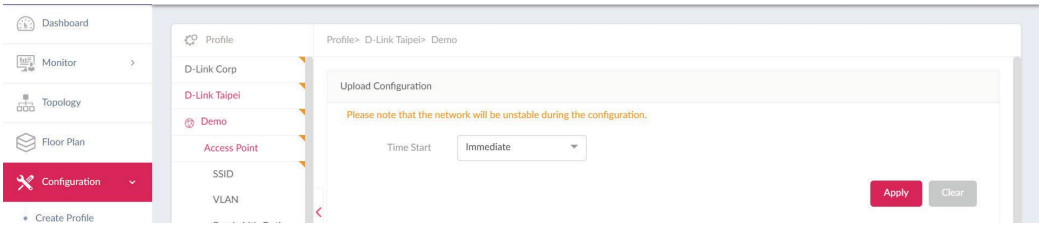
The Start Discovery Page is displayed. Click **Start Discovery** to search for all available unmanaged devices. If a device is found, select it and click **Apply** to import the network profile. Click on the Managed tab to select defined devices and add them to the network.



Profile Settings

The Profile Settings function allows for the management of existing networks. Navigate to **Configuration > Profile Settings** to view existing sites. Select a site followed by a network to view all settings that are available for editing. For Access Points, the below options are displayed: **SSID**, **VLAN**, **Bandwidth Optimization**, **RF Optimization**, **Schedule**, **Device Setting**, **Performance**, **WLAN Partition**, and **Wireless Resources**. For Switches, the following options are displayed: Common settings (**RADIUS Server** and **Time Profile**) and **Switch series** (**Basic**, **IPv4 ACL**, **Access Policy**, **Port Setting**, and **SNTP**.)

Once a network is selected, the Upload Configuration and Run Status will become available for both switches and access points.



For the configuration to take effect, it must be uploaded to the access point/switch. Under the **Upload Configuration** tab, click the **Time Start** drop-down menu and select **Immediate** or **Select Time** to set the time for uploading the configuration.

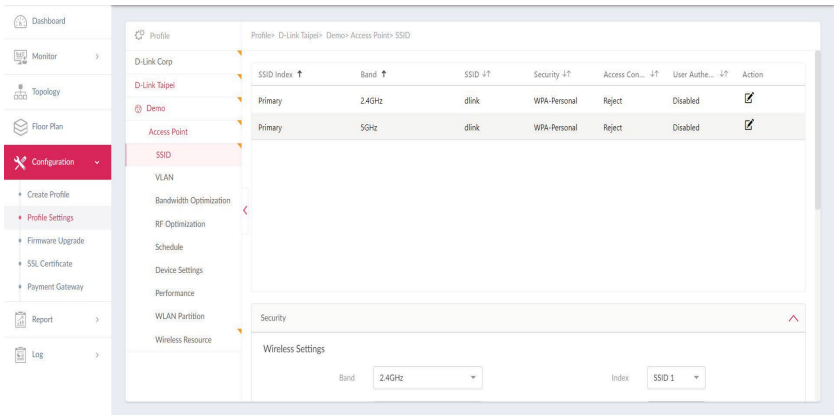
If Select Time is selected, set the day and time to upload the configuration. Once the Time Start is defined, click **Apply** to initiate the process.

Under the **Run Status** window, the status of the upload configuration is reported. Once an update is complete, the results will be displayed in the **Results** window.

SSID

If the device type of the profile chosen is an Access Point, the following options are displayed: **SSID, VLAN, Bandwidth Optimization, RF Optimization, Schedule, Device Settings, Performance, WLAN Partition**, and **Wireless Resource**.

The SSID page displays the configurable parameters of a network's wireless settings. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Access Point > SSID** to view existing settings.



In the **Security** section, the following parameters can be configured:

Field	Description
Band	Click the drop-down menu to select wireless frequency band.
Index	Click the drop-down menu to select SSID index (Parameters: Primary, SSID 1 to SSID 7). To create a new SSID, select the index parameter first.
SSID	Enter the wireless network name. The SSID must be the same across all frequencies. In addition, make sure the network name (SSID) on the selected access point is the same as the defined network name (SSID) on Nuclias Connect X. For further information, go to Access Point Basic > Wireless Settings and Advanced Settings > DHCP Server > Dynamic Pool Settings, to ensure the Domain Name field reflects the defined network name (SSID) on Nuclias Connect X.
Character Set	Click the drop-down menu to select the character set to be used in the SSID encoding: UTF-8 or GB2312.
SSID Broadcast	Click the drop-down menu to enable or disable the wireless SSID visibility.
WMM (Wi-Fi Multimedia)	Click the drop-down menu to enable or disable the Wi-Fi multimedia.
Security	Click the drop-down menu to select the wireless security protocol: Open System (no pre-shared key required), WPA-Personal, WPA Enterprise (Radius server required), WPA2-Personal, WPA2-Enterprise (Radius server required), WPA-Auto-Personal, WPA-Auto-Enterprise (Radius server required).
Fast Roaming	Select Enabled to enable Fast Roaming function on AP. (Applicable only to APs that support this function.)
Encryption	Click the drop-down menu to enable or disable WEP Open System encryption. The function is only available when Security is set to Open System.
Key Size	Click the drop-down menu to select the WEP key size.
Key Type	Click the drop-down menu to select the WEP key type.
Key Index	Click the drop-down menu to select the WEP key index.
Key Value	Enter the open system WEP encryption key.

In the **Access Control** section, the following parameters can be configured:

Block	Description
Action	Click the drop-down menu to select the action that will be applied to the clients.
MAC Address	Enter the MAC address of the clients that will be allowed or denied access and click **Add**.
Upload MAC Address List	Click **Browser...** to select an MAC address file located on the local computer. Click **Upload** to update the MAC address list. Click **Download** to download the current MAC address list.
Action	Click on the drop-down menu to enable or disable the IP filter function.
IP Address	Enter the IP address.
Subnet Mask	Enter the subnet mask.

In the **User Authentication** section, the following parameters can be configured:

Block	Description
Authentication Type	Click the drop-down menu to select the authentication type applied to the wireless client. (Web redirection only, User name/Password, Remote Radius, LDAP, POP3, Passcode, External Captive Portal, MAC address, Click through and Social Login)
Idle Timeout (2~1440) **Session timeout**	Idle Timeout (2~1440) Define how long wireless clients can use network without re-login.
Allow	Define how many times wireless client can re-login per day (The start time is 0:00)
Interval	Define how long wireless clients can log in after session timeout
Enable White List	Check the box to enable the white list function. This function is only available when **Authentication Type** is Username/Password.
MAC Address	Enter the MAC address of the network device that will be whitelisted and click Add to add the address to the white list table. This function is only available when **Authentication Type** is set to **Username/Password**.
Upload Whitelist File	Click **Browser...** to select a white list file, located on the local computer. Click **Upload** to update the white list. Click Download to download the current white list. The function is only available when **Authentication Type** is set to **Username/Password.**
IPIF Status	Click the drop-down menu to enable or disable the use of the IP interface.
VLAN Group	Enter the VLAN group name.
Get IP Address From	Click the drop-down menu to select the IP address configuration setting.
IP Address	Enter the IP address of the IP interface.
Subnet Mask	Enter the subnet mask of the IP interface.
Gateway	Enter the gateway of the IP interface.
DNS	Enter the preferred DNS address of the IP interface.
Username	Enter the username. The function is only available when **Authentication Type** is set as **Username/Password**.

Block	Description
Password	Enter the password and click Add. Click Clear to clear the entered fields. This function is only available when Authentication Type is set to Username/Password.
RADIUS Server	Enter the RADIUS server's IP address. This function is only available when Authentication Type is set to Remote RADIUS or MAC Address.
RADIUS Port	Enter the RADIUS server's port number. This function is only available when Authentication Type is set to Remote RADIUS or MAC Address.
RADIUS Secret	Enter the RADIUS server's secret. This function is only available when Authentication Type is set to Remote RADIUS or MAC Address
Remote RADIUS Type	Enter the RADIUS server's type. This function is only available when Authentication Type is set to Remote RADIUS or MAC Address.
Server	Enter the LDAP server's IP address. This function is only available when Authentication Type is set to LDAP.
Port	Enter the LDAP server's port number. This function is only available when Authentication Type is set to LDAP.
Authentication Mode	Click on the drop-down menu to select the authentication mode. This function is only available when Authentication Type is set to LDAP.
Username	Enter the administrator's username to access and search for the LDAP database. This function is only available when Authentication Type is set to LDAP.
Password	Enter the administrator's password to access and search for the LDAP database. This function is only available when Authentication Type is set to LDAP.
Base DN	Enter the base domain name of the LDAP database. This function is only available when Authentication Type is set to LDAP.
Account Attribute	Enter attribute for the account. This function is only available when Authentication Type is set to LDAP.
Identity	Enter the name of the administrator. This function is only available when Authentication Type is set to LDAP.
Server	Enter the POP3 server's IP address. This function is only available when Authentication Type is set to POP3.
Port	Enter the POP3 server's port number. This function is only available when Authentication Type is POP3.
Connection Type	Click the drop-down menu to select the connection type. This function is only available when Authentication Type is set to POP3.
Passcode List	Display the configured front desk user accounts that have been assigned to this network and have generated a passcode from the Web login page.
Account Server Status	Click the drop-down menu to select HTTP or HTTPS. After selecting, enter the URL of the website. This function is only available when Authentication Type is set to External Captive Portal.
Web Redirection	Check the box to enable the website redirection function.
Website	Click the drop-down menu to select HTTP or HTTPS. After selecting, enter the URL of the website.

Block	Description
Choose Template	Click the drop-down menu to select the used login style. This function is only not available when **Authentication Type** is set to **Web Redirection Only**. • Click **Preview** to preview the selected style. • Click **Upload Login File** to upload a new style. • Click to delete the selected style. • Click to download the style template.

Click **Save** to save the values and update the screen.

Click **Reset** to reset all settings.

Click **Cancel** to restore default value.

Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 65 for further information.

VLAN

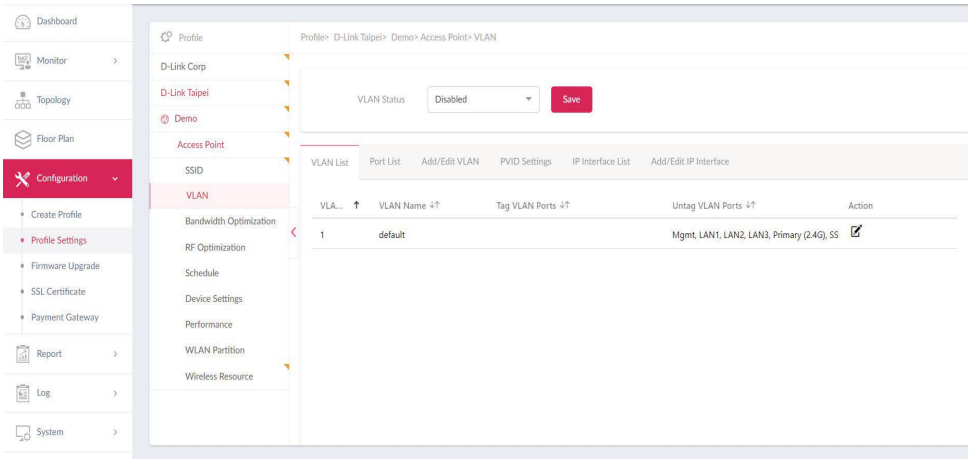
The VLAN page will show the configurable settings of a network's virtual LAN subnetwork settings. Navigate to **Configuration > Profile Settings > [Site] > [Network] > VLAN** to view existing settings.

Block	Description
VLAN Status	Click the drop-down menu to enable or disable VLANs.

Click **Save** to save the values and update the screen.

The **VLAN List** tab will show a list of all created VLANs.

Click to modify an existing VLAN.
Click to remove an existing VLAN.



In the **Port List** tab, a list of port assignments is displayed. The list shows the tagged and untagged ports available on the access points in the network.

In the columns next to the Port Name entries, the Tag/Untag ID columns indicate if the port is a tagged member (Tag VID) or an untagged member (Untag VID) of the VLAN. In the last column, the port VLAN ID shows the connected virtual LAN segment.

In the **Add/Edit VLAN** tab, you can create a new VLAN and assign untagged ports to that VLAN. Click the Modify icon in the VLAN List tab to modify an existing VLAN.

In the **PVID Setting** tab, you can view and configure the Port VLAN Identifier (PVID) settings for access points and wireless clients in this network.

In the **IP Interface List** tab, you can view a summary of IP Interface. The following information is listed: VLAN VID, VLAN Name, Get IP Address From, and IP Address. Under the action field, click to revise, or click to delete.

In the **Add/Edit IP Interface** tab, you can add or edit IP interface. The following fields are presented: VLAN VID, Get IP Address From, IP Address, Subnet Mask, Gateway, and DNS. Click **Save** to save your changes.

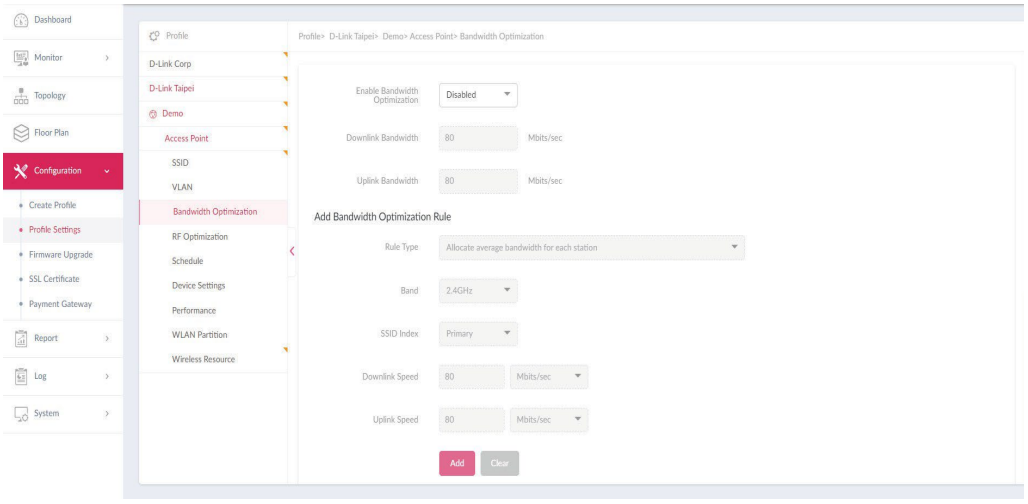
Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 65 for further information.

Bandwidth Optimization

The Bandwidth Optimization page displays configurable settings to optimize available bandwidth. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Bandwidth Optimization** to view existing settings.

Block	Description
Enable Bandwidth Optimization	Click the drop-down menu to enable or disable the bandwidth optimization function.
Downlink Bandwidth	Enter the total downlink bandwidth speed for the access points in the network.
Uplink Bandwidth	Enter the total uplink bandwidth speed for the access points in the network.
Rule Type	Click the drop-down menu to select the rule type. • Allocate an average BW for each station: Optimize bandwidth by averaging the allocated bandwidth for each client. • Allocate a maximum BW for each station: Specify the maximum bandwidth for each connected client, while reserving available bandwidth for additional clients. • Allocate a different BW for 11a/b/g/n station: The weight of 802.11b/g/n and 802.11a/n clients are 10%/20%/70% and 20%/80%. The AP will distribute different bandwidth for 802.11a/b/g/n clients. • Allocate a specific BW for SSID: All clients share the assigned bandwidth.
Band	Click the drop-down menu to select the wireless frequency band used in the rule.
SSID Index	Click the drop-down menu to select the SSID used in the rule.
Downlink Speed	Enter the downlink speed assigned to either each station or the specified SSID.
Uplink Speed	Enter the uplink speed assigned to either each station or the specified SSID.
Add	Click **Add** to add the rule into the Bandwidth Optimization Rules.
Clear	Click **Clear** to clear the entered rule.

Click **Save** to save the values and update the screen.



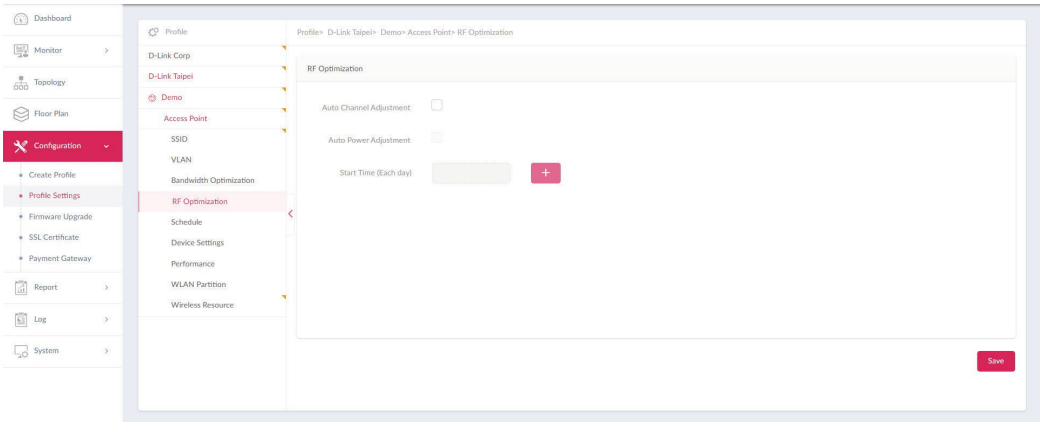
Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 65 for further information.

RF Optimization

The RF Optimization page displays the configurable Radio Frequency (RF) settings used on the access points of the wireless network. Navigate to **Configuration > Profile Settings > [Site] > [Network] > RF Optimization** to view existing settings.

Block	Description
Adjust Frequency	Click the drop-down menu to set the rate in hours at which the RF frequency is adjusted.
Auto Channel Adjustment	Click the **Auto RF Optimize** radio button to enable the function to automatically adjust the channel of the client to avoid RF interference.
Auto Power Adjustment	Available if Auto Channel Adjustment is enabled. Click the radio button to enable the feature to automatically adjust AP radio power to optimize coverage when interference is present.

Click **Save** to save the values and update the screen.



Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 65 for further information.

Schedule

Under the Schedule page, you can configure a schedule to keep the SSID active within a specified time. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Schedule** to view settings.

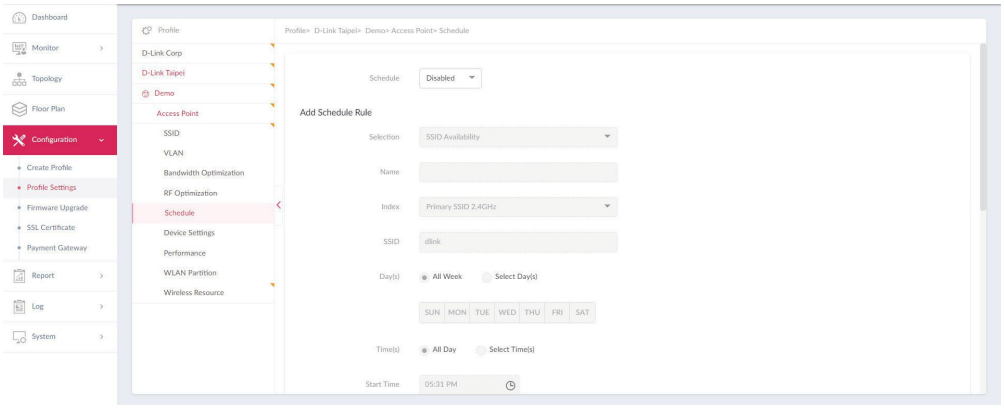
Parameter	Description
Wireless Schedule	Click the drop-down menu to enable or disable the wireless schedule function.
Name	Enter the name of the schedule rule.
Index	Click the drop-down menu to select SSID to which the schedule setting is applied.
SSID	Display the SSID name.
Day(s)	Click the radio button to select the active days for the schedule. • All Week: Enable the rule for the whole week. • Select Day(s): Specify particular day(s) to activate the rule.
Time(s)	Click the radio button to select the active times for the schedule. • All Day: Enable the rule for the whole day. • Select Time(s): Specify a start and end time for the rule.
Start Time	Enter the hours and minutes of the day. This function is only available when **Time(s)** is set as **Select Time(s)**.
End Time	Enter the hours and minutes of the day. This function is only available when **Time(s)** is set as **Select Time(s)**.
Over Night	Check the box to enable activity overnight.
Add	Click **Add** to add the rule into the schedule.
Clear	Click **Clear** to clear the entered rule.

Click to modify the desired rule.

Click to delete the desired rule.

Click **Save** to save the values and update the screen.

Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 68 for further information.



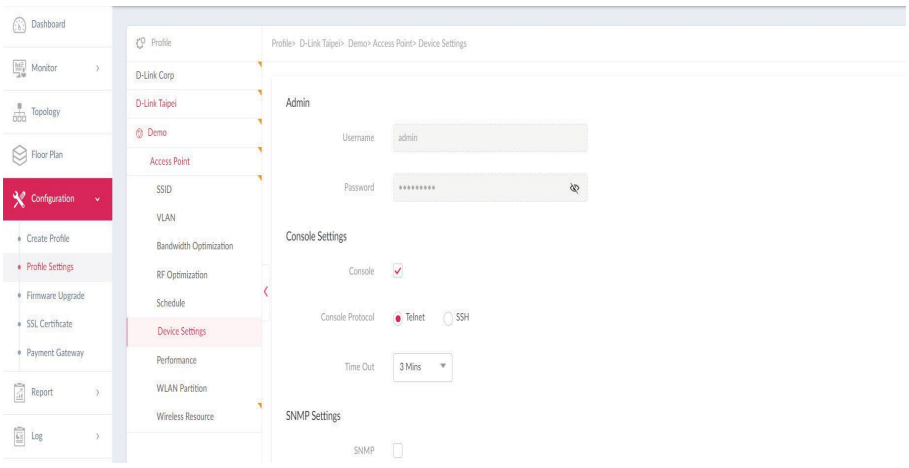
Device Settings

The Device Settings page allows you to view and configure the login and accessibility settings for access points in this network. Advanced wireless settings can be configured for both the 2.4GHz and 5GHz frequency bands. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Device Setting** to view existing settings.

Parameter	Description
Username	Enter the administrative username that is used to access the configuration settings for all access points in the network.
Password	Enter the administrative password that is used to access the configuration settings for to all access points in the network.
Enable	Check the box to enable the console function.
Console Protocol	Click the radio button to select the console protocol that is applied to all access points in the network.
Time Out	Click the drop-down menu to select the active console session time out value.
Enable NTP Server	Check the box to enable the Network Time Protocol (NTP) server function.
NTP Server	Enter the IP address or domain name of the NTP server.
Select Country	Click the drop-down menu to select the country region of APs in the network.
Time Zone	Click the drop-down menu to select the time zone.
Enable Daylight Saving	Check the box to enable the daylight saving function.
DST Start (24HR)	Click the drop-down menu to designate the start date and time for Daylight Saving Time (DST).
DST End (24HR)	Click the drop-down menu to designate the end date and time for Daylight Saving Time (DST).
DST Offset (minutes)	Click the drop-down menu to select DST Offset time.
External Syslog Server	Enter the IP address or domain name of the external syslog server.

Click **Save** to save the values and update the screen.

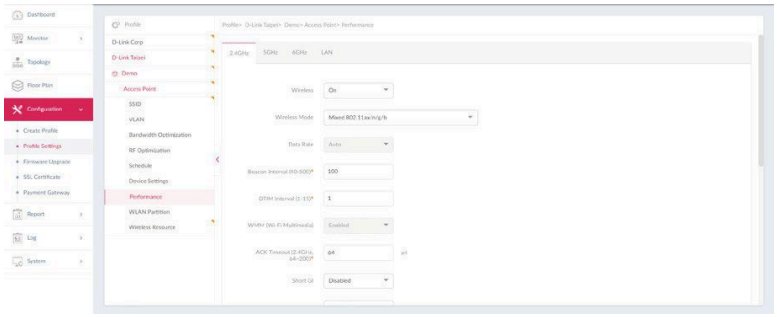
Once the settings are updated, the configuration must be uploaded to the related access points. See “Profile Settings” on page 65 for further information.



The Schedule page allows you to configure the wireless performance for access points on your network. Additionally, advanced wireless settings can be configured on the page for both the 2.4GHz and 5GHz frequency bands. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Access Point > Device Settings** to view existing settings. Click the 2.4GHz or 5GHz tab to view existing settings.

Parameter	Description
Wireless	Click the drop-down menu to turn on or off the wireless band for the network.
Wireless Mode	Click the drop-down menu to select the wireless mode used in the network.
Data Rate	Click the drop-down menu to select the wireless data rate. The function is only available when **Wireless Mode** is set as **Mixed 802.11g and 802.11b (2.4GHz)** or **802.11a Only (5GHz)**.
Beacon Interval	Enter the beacon interval value. The default value is 100.
DTIM Interval (1-15)	Enter the DTIM interval value. The default value is 1.
WMM (Wi-Fi Multimedia)	Enter the LDAP server's IP address. This function is only available when Authentication Type is set to LDAP.
ACK Timeout	Enter the ACK timeout value. The default value is 48.
Short GI	Click the drop-down menu to enable or disable the short GI function.
IGMP Snooping	Click the drop-down menu to enable or disable the IGMP snooping function
Multicast Rate	Click the drop-down menu to select the multicast rate value.
Multicast Bandwidth Control	Click the drop-down menu to enable or disable the multicast bandwidth control function.
Maximum Multicast Bandwidth	Click the drop-down menu to enable or disable the multicast bandwidth control function.
HT20/40 Coexistence	Click the drop-down menu to enable or disable the HT20/40 coexistence function.
Change DHCP Offers from Multicast to Unicast	Click the drop-down menu to allow or deny the transfer of DHCP offers to unicast function.
RTS Length (256-2346)	Enter the RTS length value. The default value is 2346.
Fragment Length (256-2346)	Enter the fragment length value. The default value is 2346.
Channel Width	Click the drop-down menu to select the channel width used by the network.

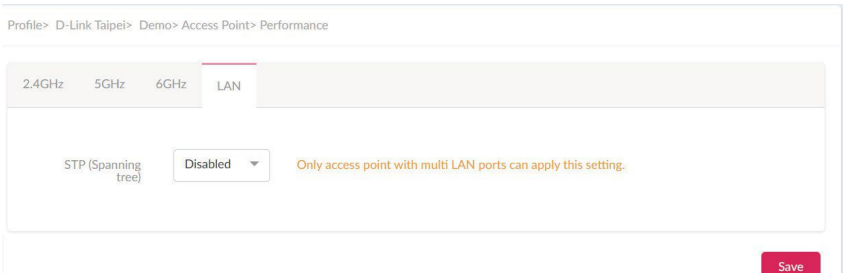
Click **Save** to save the values and update the screen.



Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 68 for further information

Performance > LAN

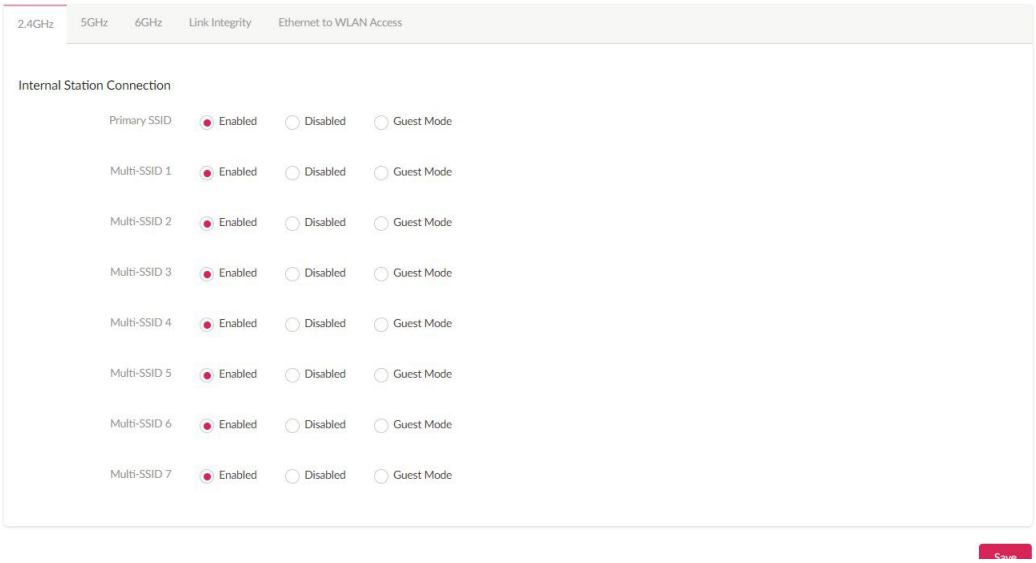
Under the **LAN** tab, users can enable or disable **STP** (Spanning tree). STP can help ensure that no loops are created when you have redundant paths in your network. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Access Point > Performance > LAN.** Note that only access points with multi LAN ports can apply this setting.



Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 65 for further information.

WLAN Partition > 2.4GHz / 5GHz / 6GHz

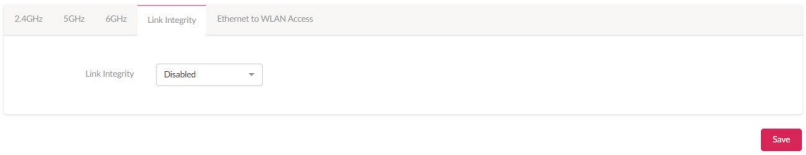
The WLAN Partition page displays the wireless partitioning settings that allow you to enable/disable associated wireless clients from communicating with each other. Additionally, advanced wireless settings can be configured on the page for both the 2.4GHz and 5GHz frequency bands. Navigate to **Configuration > Profile Settings > [Site] > [Network] > WLAN Partition**. Click the 2.4GHz or 5GHz tab to view existing settings. Click **Save** to save the values and update the screen.



Once the settings are updated, the configuration must be uploaded to the related access points. See “Profile Settings” on page 65 for further information.

WLAN Partition > Link Integrity

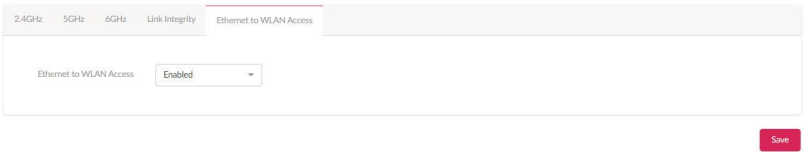
The Link Integrity feature disassociates wireless segments from the AP when the LAN and AP are disconnected. Click the drop-down menu to enable or disable the wireless link integrity function.



Click **Save** to save the changes. Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 65 for further information.

WLAN Partition > Ethernet to WLAN Access

The Ethernet to WLAN Access feature allows Ethernet to send and receive data from associated wireless devices. Click the drop-down menu to enable or disable Ethernet to WLAN Access.



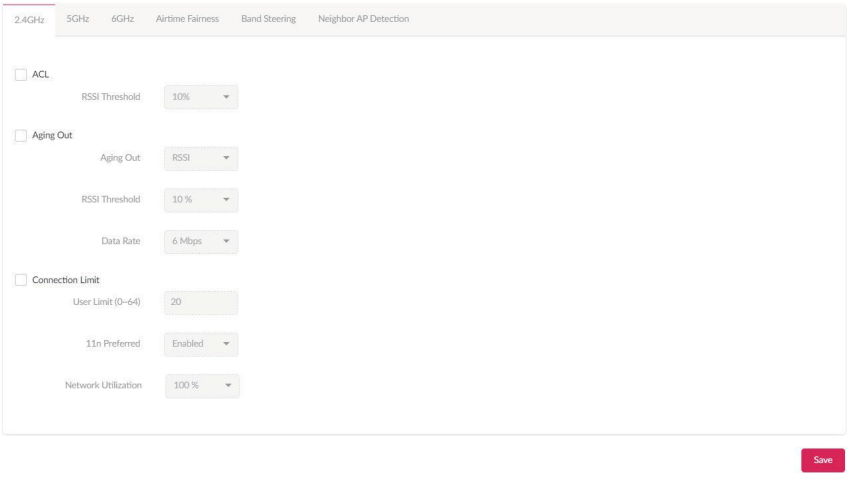
Click **Save** to save the changes. Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 65 for further information.

Wireless Resource

The Wireless Resource function in Nuclias Hyper helps provide real-time RF management of the wireless network. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Wireless Resource**. Click the 2.4GHz or 5GHz tab to view existing settings.

Parameter	Description
ACL RSSI Threshold	Check the box to enable ACL RSSI threshold function and click the drop-down menu to select the ACL RSSI threshold percentage.
Aging Out	Click to enable the Aging Out function. From the menu, select a criteria to disconnect wireless clients. Available options are RSSI and Data Rate.
RSSI Threshold	When **RSSI** is selected in the Aging out drop-down menu, select a value between 10% to 100%. This parameter sets the minimum RRSI for wireless clients to respond to a probe. If the determined value is lower than the specified percentage, the wireless client is disconnected.
Data Rate	Click the drop-down menu to select the data rate connection limit. The function is only available when the **Aging Out** policy is set to **Data Rate**.
Connection Limit	Click the radio button to enable or disable the function. Connection limit is designed to provide load balancing. This policy allows user access management on the wireless network. The exact number is entered in the User Limit field below. If this function is enabled and the number of users exceeds this value, or the network utilization exceeds the specified percentage, the policy will not allow further client association.
User Limit (0~64)	Enter the user connection limit. The default value is 20.
11n Preferred	Click the drop-down menu to enable or disable the preferred use of 802.11n.
Network Utilization	Click the drop-down menu to select the network utilization percentage.

Click **Save** to save the values and update the screen.



Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 65 for further information.

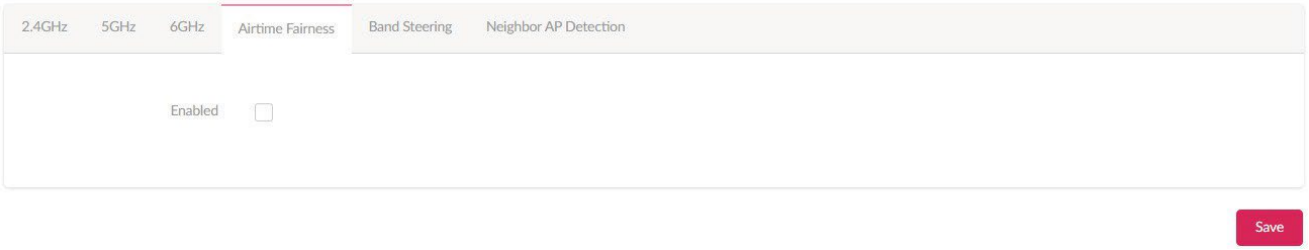
Wireless Resource > Airtime Fairness

Airtime Fairness allows you to boost overall network performance. This function sacrifices network time from the slowest devices to boost overall performance of the network.

Note: Devices identified as having slow Wi-Fi speed may be attributed to long connection distance, weak signal strength or older legacy hardware. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Wireless Resource**. Click the **Airtime Fairness** tab to view the existing settings.

Check the box to enable or disable the airtime fairness function.

Click **Save** to save the values and update the screen.



Once the settings are updated, the configuration must be uploaded to the related access points. See “Profile Settings” on page 65 for further information.

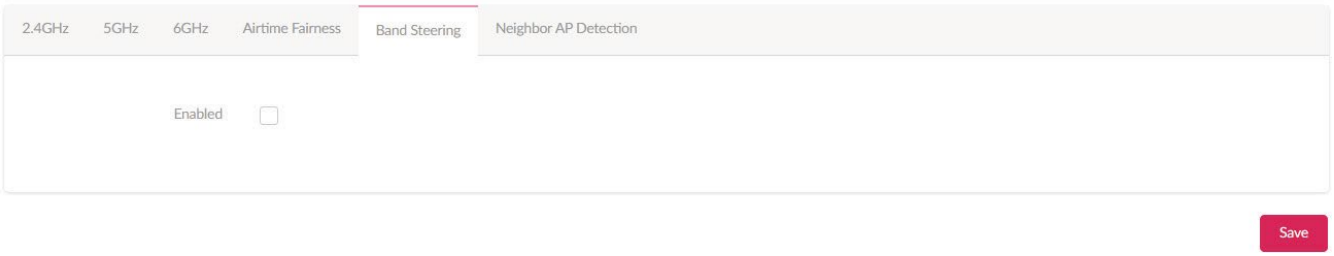
Wireless Resource > Band Steering

Band Steering allows dual-band-capable clients to connect to the less crowded 5GHz network and leave the 2.4GHz network available for clients that support 2.4GHz only.

Navigate to **Configuration > Profile Settings > [Site] > [Network] > Wireless Resource**. Click on the **Band Steering** tab to view the existing setting.

Check the box to enable or disable the wireless band steering function.

Click **Save** to save the values and update the screen.



Once the settings are updated, the configuration must be uploaded to the related access points. See “Profile Settings” on page 65 for further information.

Wireless Resource > Neighbor AP Detection

Users can view neighbor information on a specified AP radio to determine the AP location and neighbor relationship, helping locate rogue APs and plan the WLAN.

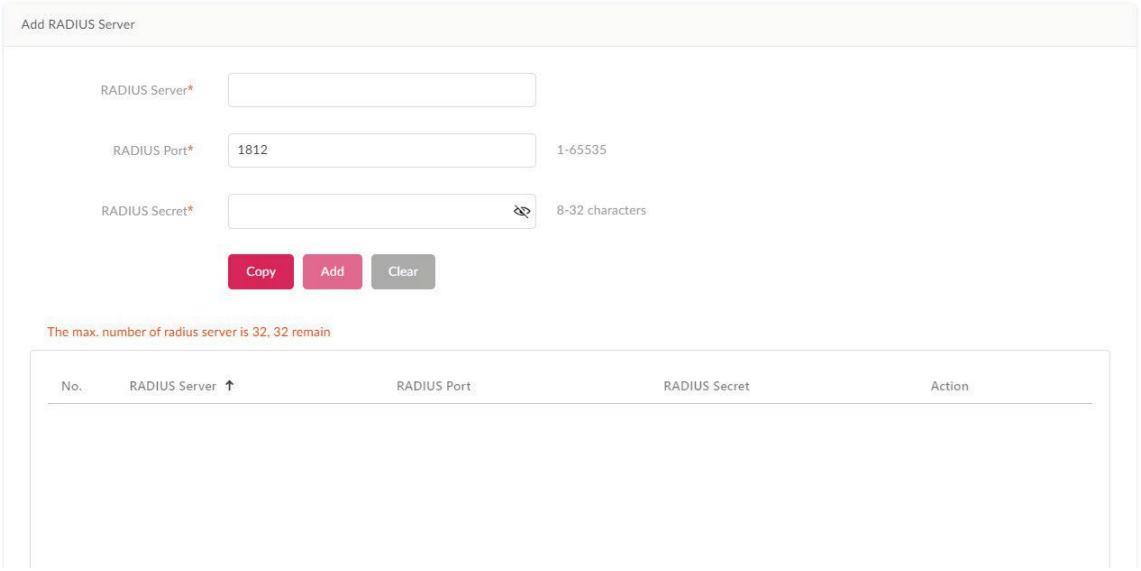
Check "Enabled" to enable detection and go to Monitor>Neighbor AP to review AP list.

Once the settings are updated, the configuration must be uploaded to the related access points. See "Profile Settings" on page 68 for further information.

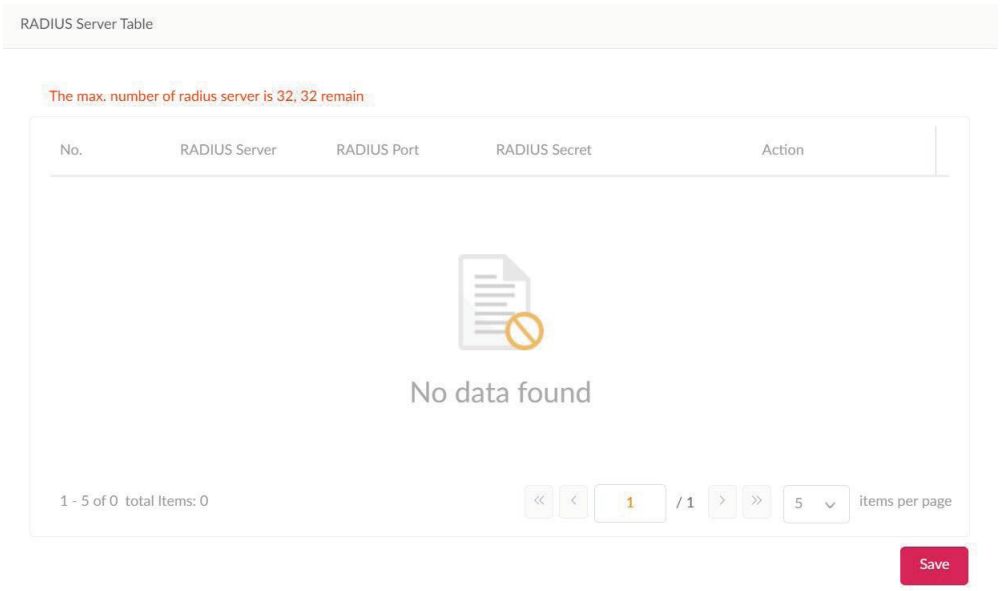
Switch > Common > RADIUS Server

In the RADIUS Server page, you can forward access requests from your switches to one or more specified remote RADIUS servers. Navigate to **Configuration > Profile Settings >Switch > Common > RADIUS Server** to set up remote RADIUS server for all switches in the network.

To add a RADIUS server, enter the RADIUS authentication server, the UDP port and the secret used to communicate with the server. Alternatively, click **Copy** to copy RADIUS server from another network. Once completed, click **Add** to add a new RADIUS server, or **Clear** to remove the entries.



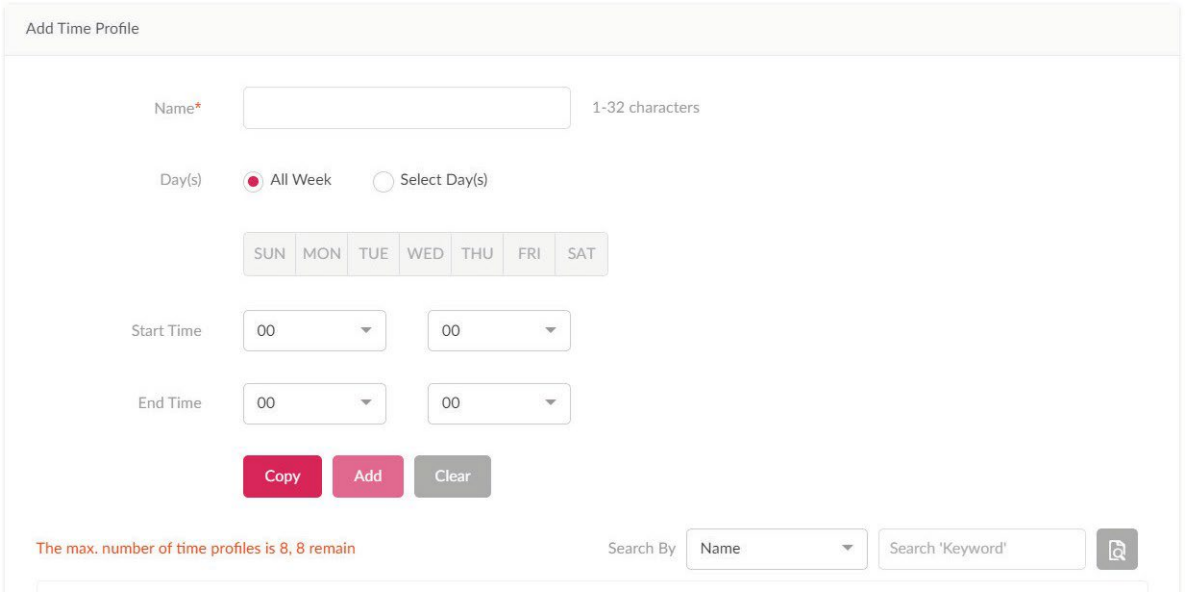
In the **RADIUS Server Table** below, a summary of all the RADIUS Servers details including the **number, RADIUS server, port** and **secret** is displayed. Under the Action field, click to edit the RADIUS server. Click to delete the selected RADIUS server. Click **Save** when completed.



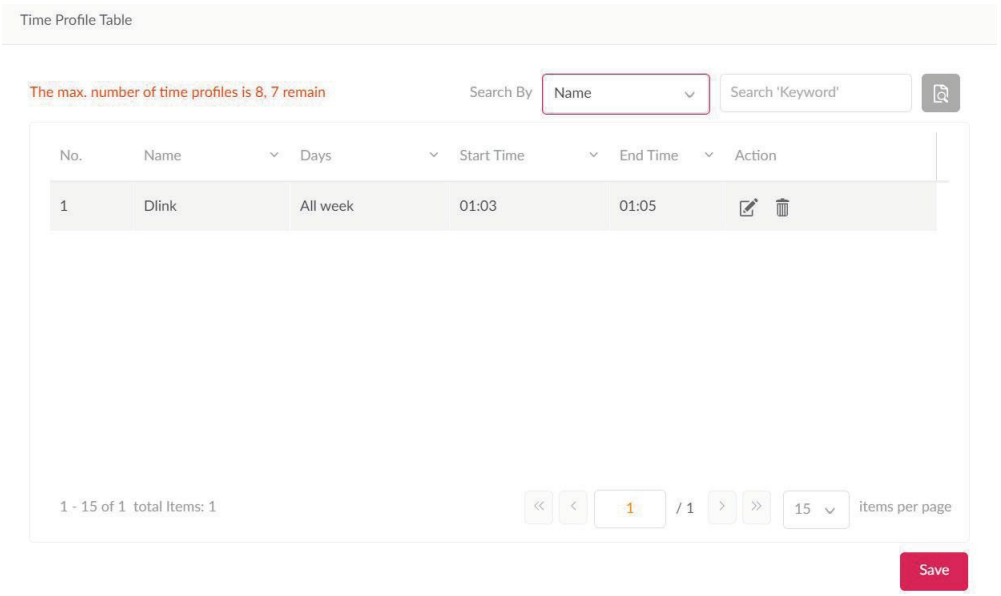
Switch > Common > Time Profile

Under the Time Profile page, users can set up time profile for all the switches in the network. Navigate to **Configuration > Profile Settings > Switch > Common > Time Profile** to set up the time profile.

In the **Add Time Profile** page, enter a name for the profile. Select the work days for the switch. Next, enter the **Start** and **End** time using the drop-down menu. Alternatively, click **Copy** to copy the time profile from another network. Once the time is set, click **Add** to add a schedule, or **Clear** to remove all values.



In the Time Profile Table, a summary of the time profile, including the name, days, start/end time is displayed. Use the drop-down menu to filter the time profiles by either **Name** or **Days**. Enter a relevant keyword to narrow the search. Click to start the search. Under the Action field, click to edit the time profile. Click to delete the time profile. Click **Save** when completed.



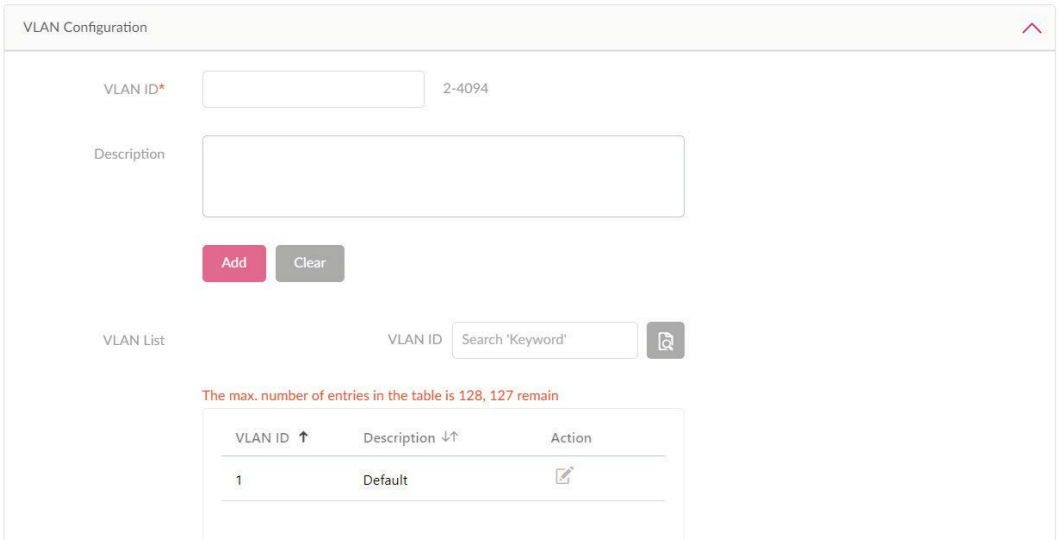
Switch > Basic

Under the **Basic** tab, users can configure global switch settings such as VLAN, IGMP Snooping, Quality of service and more. Navigate to **Configuration > Profile Settings > Switch > Your Device > Basic** to configure the switch. Below describes the functionality of each configuration options.

VLAN Configuration

In this section, users can add, edit, or delete a VLAN. Enter a VLAN ID in the VLAN ID field, the range of 2 to 4094. Next, enter a description for the VLAN. Once complete, click Add to add a VLAN, or Clear to clear the entry.

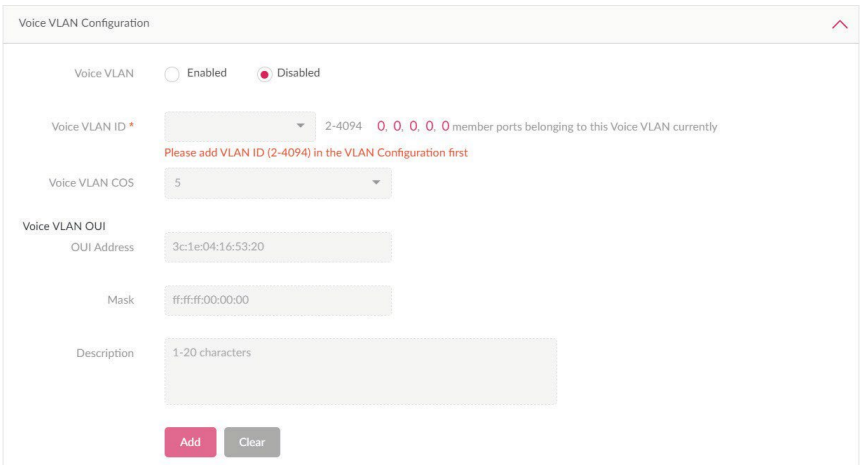
In the VLAN List section, a summary of VLAN is displayed. Enter keyword in the VLAN ID search field to locate a VLAN. Click to start the search. Under the Action field, click to edit a VLAN. Click to delete a VLAN. Click **Save** when complete.



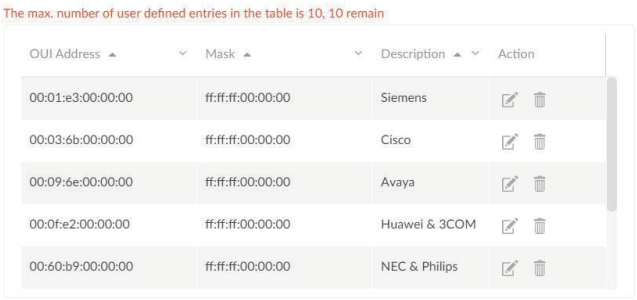
Voice VLAN Configuration

In this section, users can view and configure global Voice VLAN settings and Voice VLAN OUI(Organizationally Unique Identifier). In the Voice VLAN field, select Enabled or Disabled. If Enabled, select Voice VLAN ID and Voice VLAN COS from the drop-down menu. On the right side of Voice VLAN ID field, users can view the number of member ports belonging to the voice VLAN. Click the numbers to be directed to the Port Setting page.

In the Voice VLAN OUI section, Voice VLAN is disabled. When enabled, users can add self-defined OUI for the voice VLAN. To do so, enter a description for ease of identification. Click **Add** to add a new Voice VLAN, or **Clear** to remove entered values. Up to 10 entries can be entered.



When Voice VLAN is enabled, a default Voice VLAN OUI list is displayed in the summary list below. These entries cannot be edited or deleted.

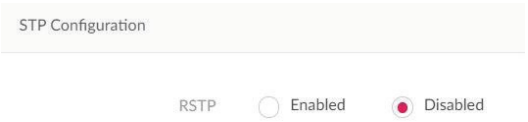


IGMP Snooping Configuration

IGMP snooping allows switches to be aware of multicasting groups and forward network traffic accordingly. In this section, users can enable or disable the IGMP Snooping function. When enabled, enter the VLAN ID of the VLAN. The max number of VLANs is 256.

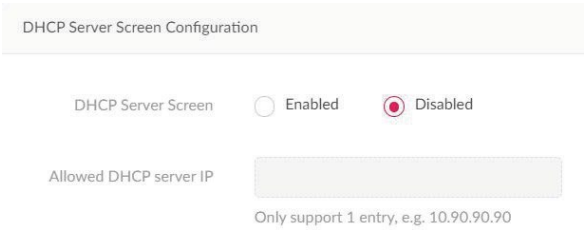
STP Configuration

RSTP (Rapid Spanning Tree Protocol) can ensure a loop-free topology and speedy convergence time. In this section, users can enable or disable RSTP on all switches in the network.



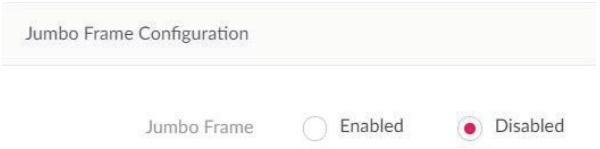
DHCP Server Screen Configuration

DHCP (Dynamic Host Configuration Protocol) server screening provides higher security by filtering illegal DHCP server packets. Select **Enabled** to turn on DHCP Server Screening. When **Enabled** is selected, enter the **Allowed DHCP Server IP** in the field.



Jumbo Frame Configuration

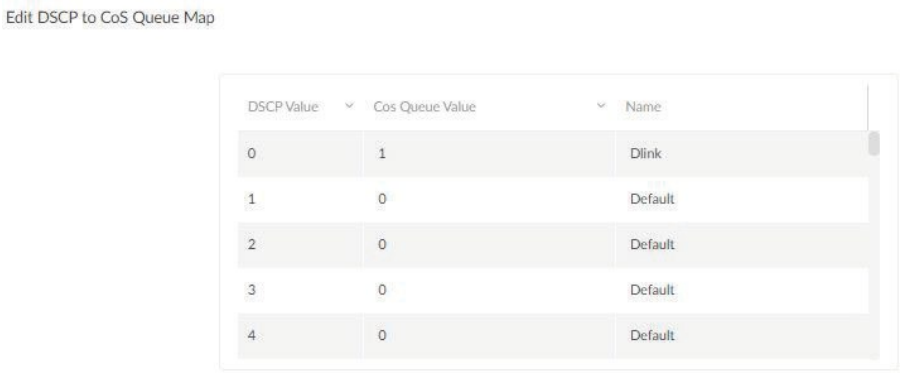
Jumbo frames are Ethernet frames with massive payload. They are used to reduce frame overload, increase system throughput and reduce CPU utilization. In the Jumbo Frame field, select **Enabled** or **Disabled**.



Quality of Service

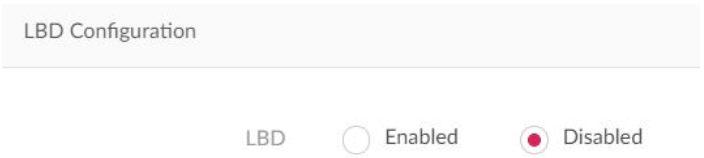
The QoS feature can prioritize certain types of data with the use of differentiated services models. The priorities are marked in each packet using Differentiated Services Code Point (DSCP) for traffic classification. To set the DSCP to CoS (Class of Service) queue, choose a value from the drop-down menu and set a name for it.

Note: One DSCP value can only be mapped to one CoS queue value.



LBD Configuration

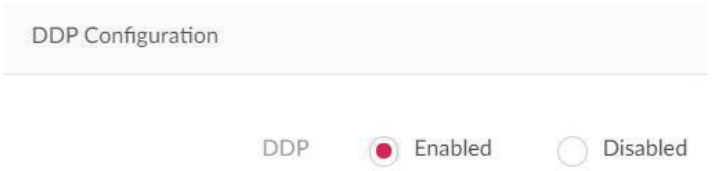
The Loopback Detection (LBD) feature can detect loops occurring on one or across different ports. In the LBD field, click **Enabled** to turn on the feature. It is disabled by default.



DDP Configuration

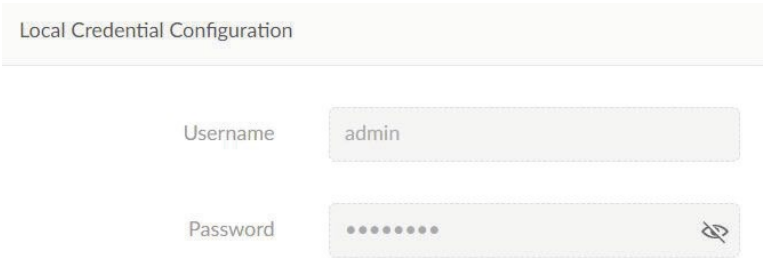
The D-Link Discovery Protocol (DDP) is a communication protocol defined by D-Link. When enabled, your device will become discoverable and can be managed by the DNC server. Features from DNA (D-Link Network Assistant) like IP settings, firmware upgrade, reboot and reset function will also be supported.

In the DDP field, click **Enabled** to turn on, or **Disabled** to turn off this feature. It is enabled by default.



Local Credential Configuration

The username and password of your device is listed here.



Switch > IPv4 ACL

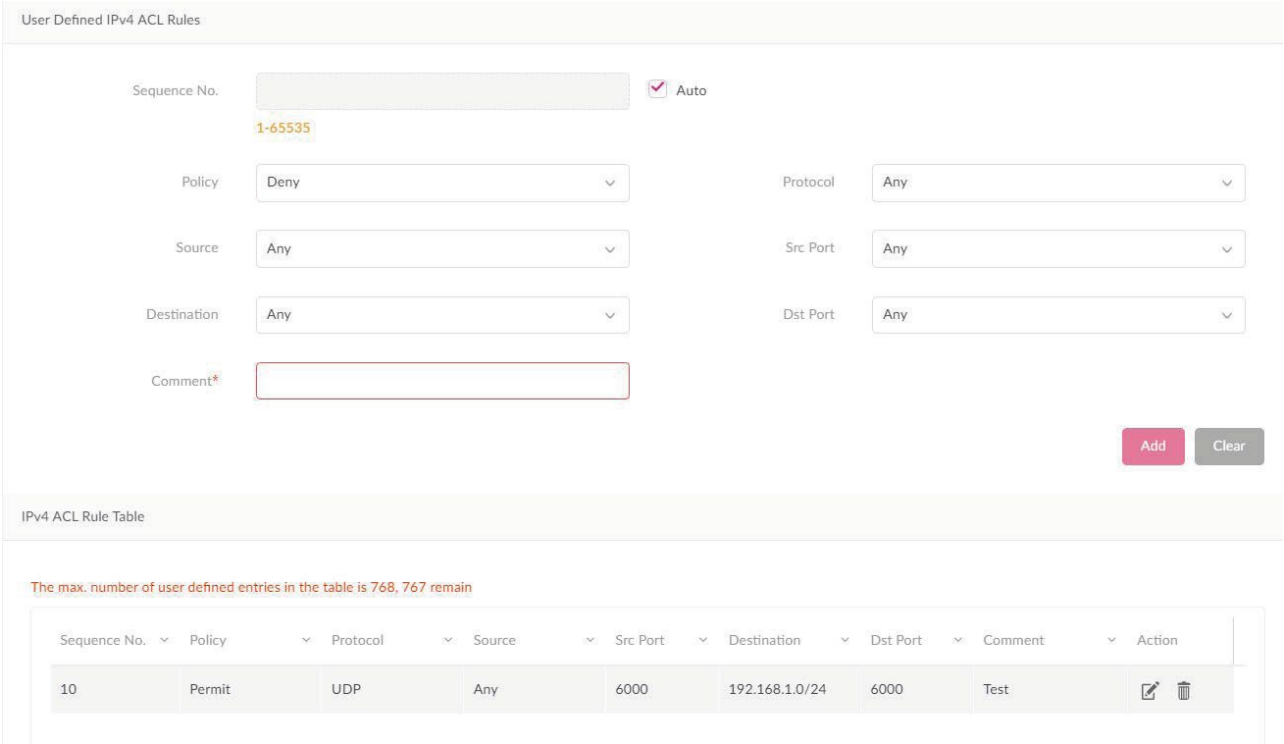
The IPv4 ACL (Access Control List) feature for the switch can help improve network performance and security by blocking selected traffic. Navigate to **Configuration > Profile Settings > Site > Network > Switch > Your Device > IPv4 ACL** to configure the settings.

In the User defined IPv4 ACL Rules section, the following fields are presented:

Field	Description
Sequence No.	Set the sequence number. The range is 1-65535. Select **Auto** to auto-assign the sequence number
Polic	Select to permit or deny what traffic goes through the switch.
Sourc	Enter the source IP address. When the Protocol is set to **Any**, all traffic destinations will be evaluated.
Destination	Enter the destination IP address. When the destination is set to **Any**, all traffic destination will be evaluated.
Comment	Enter a description for the rule.
Protocol	Select between **TCP, UDP**, or **Any**.
Src Port	Specify the number of the source port. The valid value is 0-65535. When the Src Port is set to **Any,** all traffic sources will be evaluated.
Dst Port	Specify the number of the destination port. The valid value is 0-65535. When the Dst Port is set to **Any,** all traffic sources will be evaluated.

Once complete, click **Add** to add the rule, or **Clear** to clear all values.

In the **IPv4 ACL Rule Table** section, a summary of all IPv4 ACL Rule is displayed. Under the Action field, click **Edit** to edit the ACL rule; Click **Delete** to delete the ACL rule. Click **Save** to save the changes.

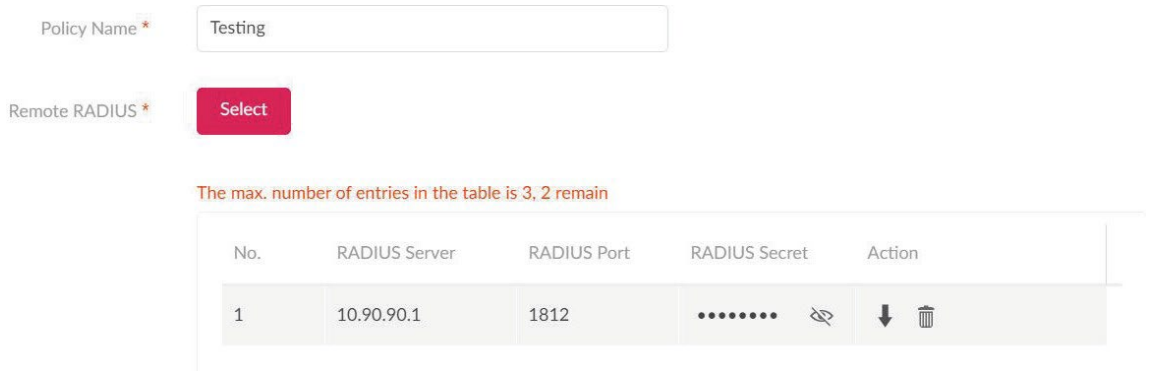


Switch > Access Policy

D-Link switches support 802.1X authentication, MAC authentication and port security to prevent unauthorized clients from accessing the network. Navigate to **Configuration > Profile Setting > Site > Network > Switch > Your Device > Access Policy** to configure the settings.

In the **Policy Name** field, enter a name for the policy. In the **Remote RADIUS Server** section, specify up to 3 RADIUS Servers for the switches to forward access requests. Authentication requests will be processed by each of the RADIUS servers in the order that they are submitted. Click **Select** to select existing RADIUS servers created via the RADIUS Server page. A pop window will be presented to confirm your selection. Click **OK** to confirm or **Cancel** to close the window.

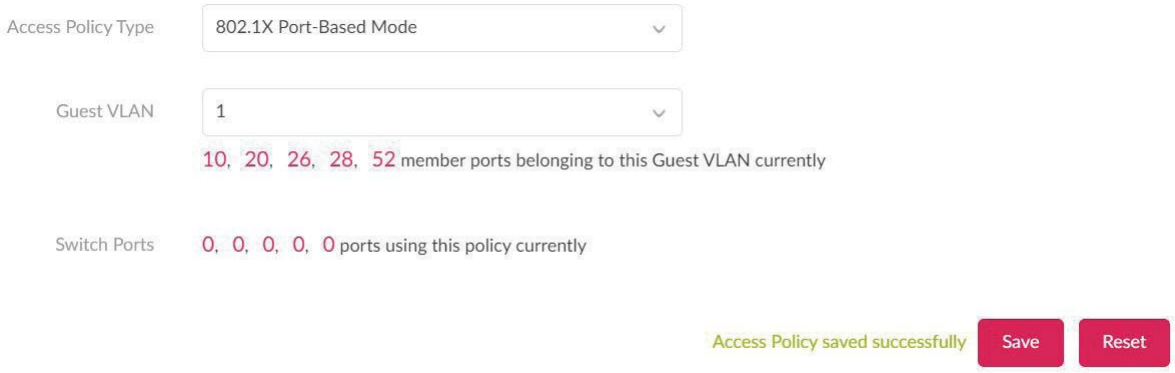
Once the RADIUS Servers are selected, a summary of the RADIUS servers will be listed in the table. In the **Action** field, click to move the entry up, click to move the entry down. Click to delete the entry.



In the **Access Policy Type** field, select 802.1x Port Based. This will allow only one user to be authenticated per port by a remote RADIUS server.

In the Guest VLAN field, specify a guest VLAN ID or disable it from the drop-down menu. The VLAN ID range is 1 to 4094. One switch only supports one Guest VLAN. When a VLAN ID is selected, the member port information will be presented. Click the number to be directed to the Port Settings page

In the Switch Ports field, the number of switch ports that's applying to the policy is listed. Click the numbers to be directed to the Port Settings page.



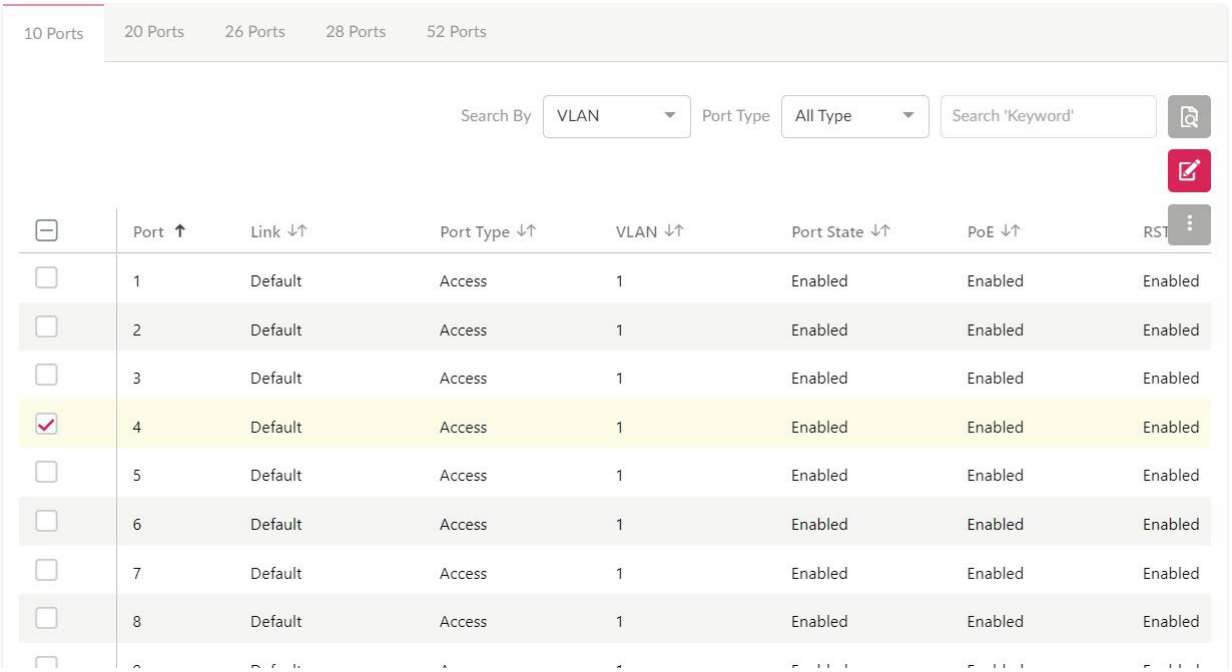
Switch > Point Setting

Navigate to **Configuration > Profile Settings > Network > Switch > Your Switch > Port Setting**, a summary of each of the switch port groups is displayed. Note that the number of port groups depends on the switch series.

To filter the search, from the **Search By** drop down menu, select **VLAN/Port/Access Policy,** and select Port Type **Access/ Trunk/All**. Under the Search column, enter a relevant keyword to narrow the search. Click to start the search. The summary includes information such as **Port number, Link, Port type, VLAN, Allowed VLAN, Port State, PoE, RSTP, LBD, DDP, Port Shutdown Schedule, PoE Supply Schedule**, and **Access Policies.**

Note that under the Link field, the value is **Default** (System default value) and cannot be modified in Profile Configuration. Links can only be modified in Standalone mode via Monitor > Switch > Switch Port, or Monitor > Device Detail page > Ports.

To make changes to a port or port group, select the port(s) and click to make the desired changes. Scroll down to view the Port Setting table. Once complete, click **Save** to save the changes.



Switch > SNTP

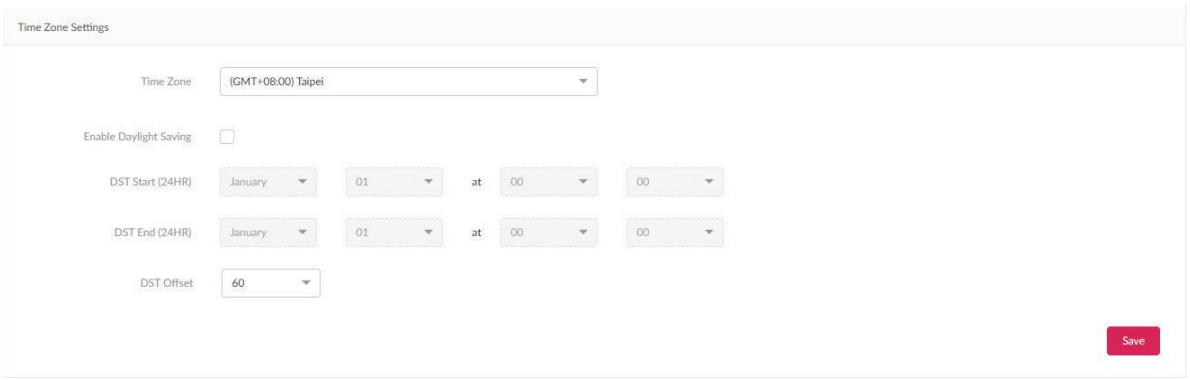
The SNTP (Simple Network Time Protocol) function allows the switch to synchronize clocks on a network. Navigate to **Configuration > Profile Settings > Site > Network > Switch > Your Switch > SNTP** to configuration the settings.

Under the SNTP tab, you can configure **Automatic Time Configuration** and **Time Zone Settings**.

In the Automatic Time Configuration section, click **Enable SNTP Server** to enable or disable it.
Once enabled, specify the IPv4 address or domain name of the primary SNTP server from which the system time is retrieved in the **SNTP Server 1** field, and the secondary SNTP server in the **SNTP Server 2** field.

In the Time Zone Settings section, users can configure time zones and daylight savings for SNTP. From the **Time Zone** field, select your local time zone. Click **Enable Daylight Saving** to enable or disable daylight saving.

In the **DST Start (24HR)** field, enter the month, date, and time in which DST will start at. In the **DST End (24HR)** field, enter the month, date, and time in which DST will end at. In the **DST Offset** field, specify the amount of time that will constitute the local DST offset - 30, 60, 90, or 120 minutes. The default is 60 min. Click **Save** when complete.



Firmware Upgrade

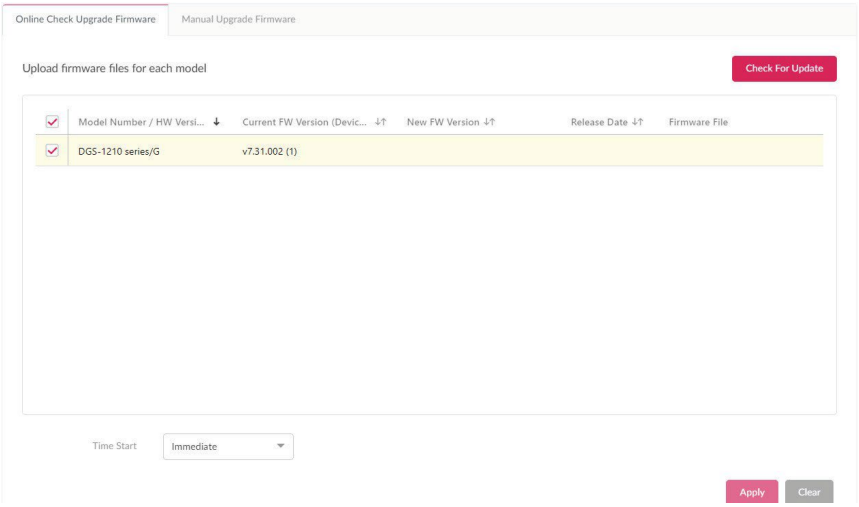
The Firmware Upgrade function allows users to perform a firmware upgrade. For online update, please confirm your device is online. For manual upgrade, please visit D-Link website of your region to see if newer firmware is available.

Navigate to Configuration > Firmware Upgrade > [Site] > [Network].

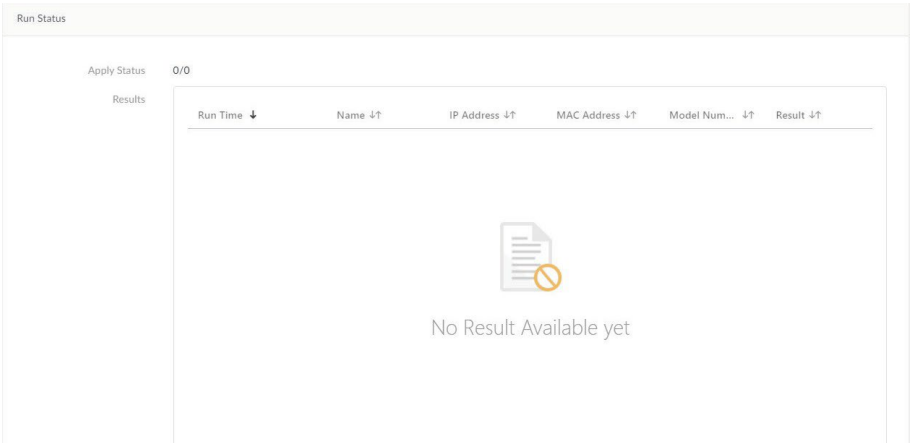
Block	Description
Online Check Upgrade Firmware	Click to configure online upgrade.
Check For Update	Click to check if newer firmware is available on online server.
Manual Upgrade Firmware	Click to configure manual upgrade.
Change	Click to select a firmware file to upload. Files are model specific.
Time Start	Click the drop-down menu to select a specific time or update immediately.

Click **Apply** to save the above configuration settings.

Click **Clear** to delete the defined settings.



The firmware upgrade status and results can be seen at the **Run Status** section. The results can be sorted by **Run Time, Name, IP Address, MAC Address, Model Type and Result**.



SSL Certificate

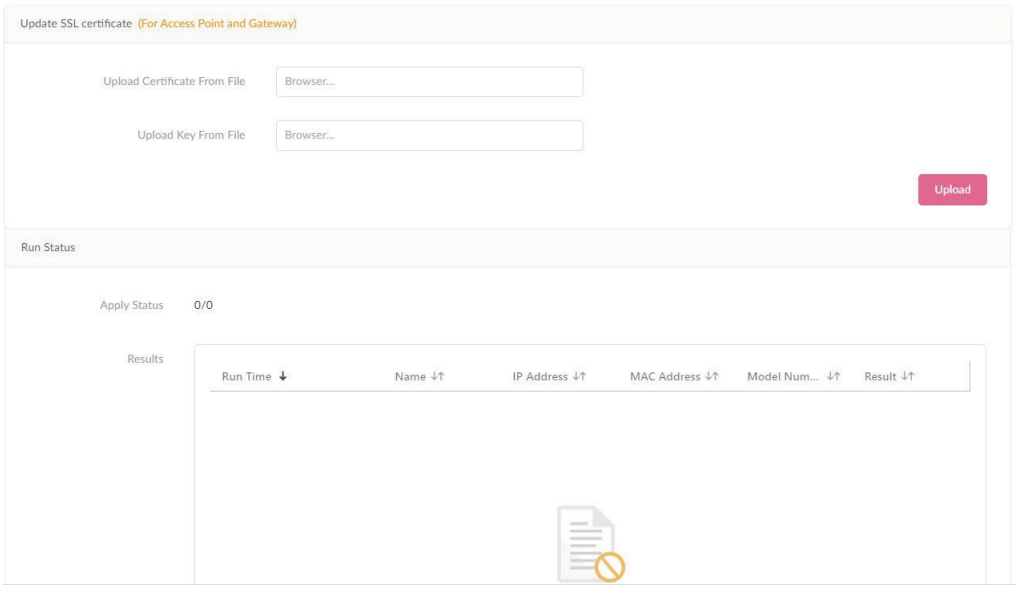
The SSL Certificate function provides the means to install an SSL certificate for use on the network. To accomplish this task, an intermediate certificate is required. The intermediate certificate is used to establish the trust of the SSL certificate by binding it to the Certificate Authority's root certificate. To complete the certificate trust configuration, the SSL Certificate function requires the certificate file to be uploaded.

In the **Update SSL certificate** section, the following parameters can be configured.

Note that this setting is only applicable to Access Points.

Options	Description
Upload Certificate From File	Click **Browser...** to select the SSL certificate file located on the drive to upload.
Upload Key From File	Click **Browser...** to select the SSL key file located on the local drive to upload.

Click **Upload** to initiate the file upload. The upload status and result will appear in the below area.



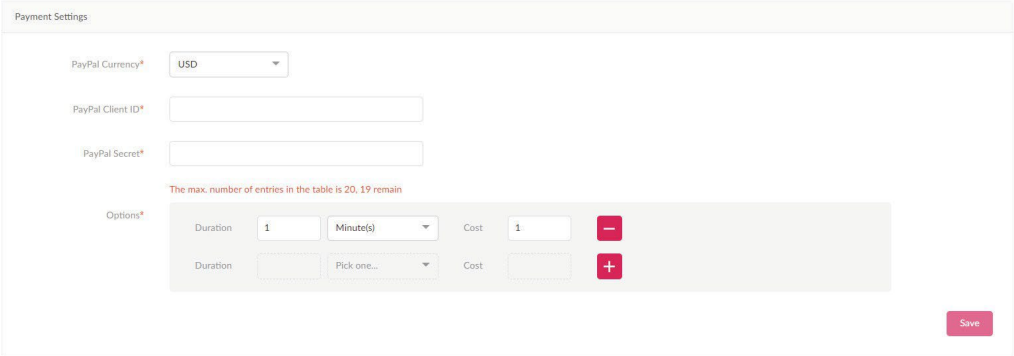
Payment Gateway

The payment gateway is a function that allows e-commerce services within the network. The Payment Gateway page will show payment settings and options necessary to enable payment services.

Navigate to **Configuration > Payment Gateway**.

Parameter	Description
PayPal Currency	Click the drop-down menu to select the currency code for the PayPal account.
PayPal Client ID	Enter the username for the PayPal account.
PayPal Secret	Enter the password for the PayPal account.
Options	Enter the duration time in minutes, hours, or days as well as the associated cost for the entry. Click + to enter the option.

Click **Save** to save the values and update the screen.



Report

Access Point

Access Point > Peak Network Activity

The Peak Network Activity function allows administrators to monitor wireless traffic on the network. Wireless activity for all or specific sites and networks can be displayed according to unique clients and traffic usage.
Navigate to Report > Access Point > Peak Network Activity to view the information.

To view a network activity report, select the site and network from the corresponding drop-down menu and click to view the report.
Once a report has been generated, click to save the report to a local PDF file.

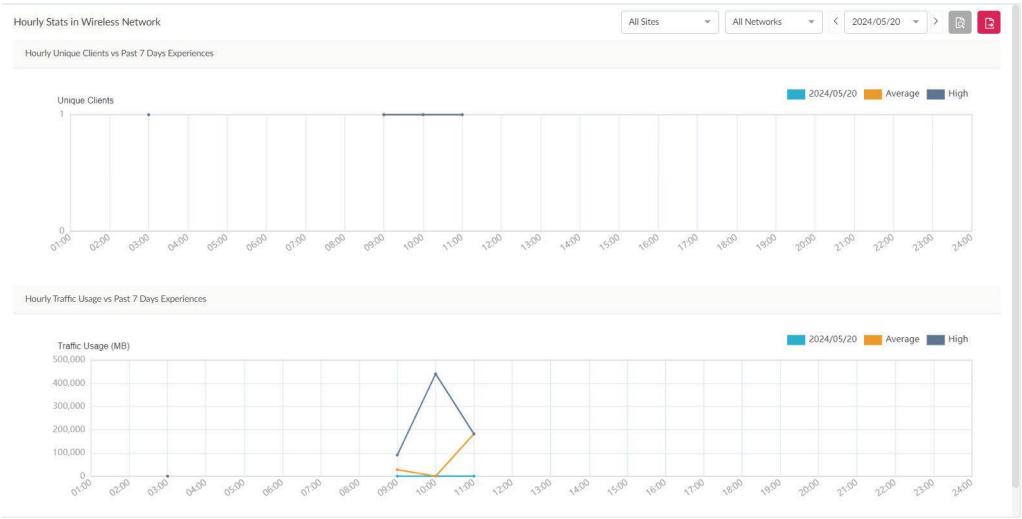
Access Point > Hourly Network Activity

The Hourly Network Activity function allows administrators to monitor wireless traffic on the network. Wireless activity for all or specific sites and networks is displayed according to unique clients and traffic usage as reported by the hour.

Navigate to **Report > Access Point > Hourly Network Activity** to view the report.

To start a daily report, select the site and network from the corresponding drop-down menu and click to view the report.

Once a report is generated, click to save the report to a local PDF file.



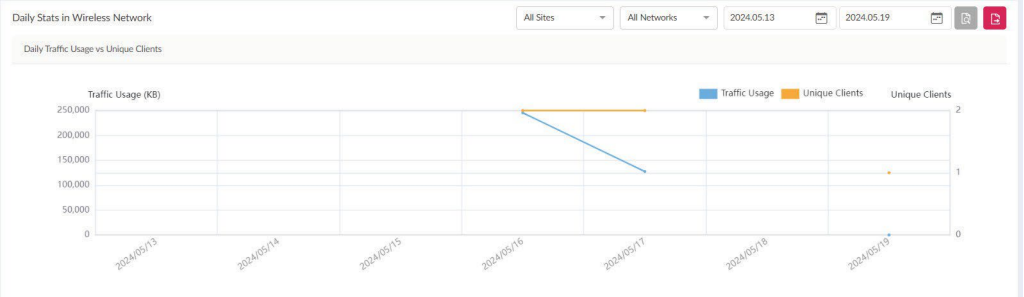
Access Point > Daily Network Activity

The Daily Network Activity function allows administrators to monitor daily wireless traffic on the network. Wireless activity for unique clients and traffic usage is displayed according to unique clients and traffic usage as reported by the day.

Navigate to **Report > Access Point > Daily Network Activity** to generate and view the report.

To display a specific client's traffic usage, select a site, network, and define the starting and ending dates of the search. Once the search parameters are defined, click to view the report.

Once a report is generated, click to save the report to a local PDF file.



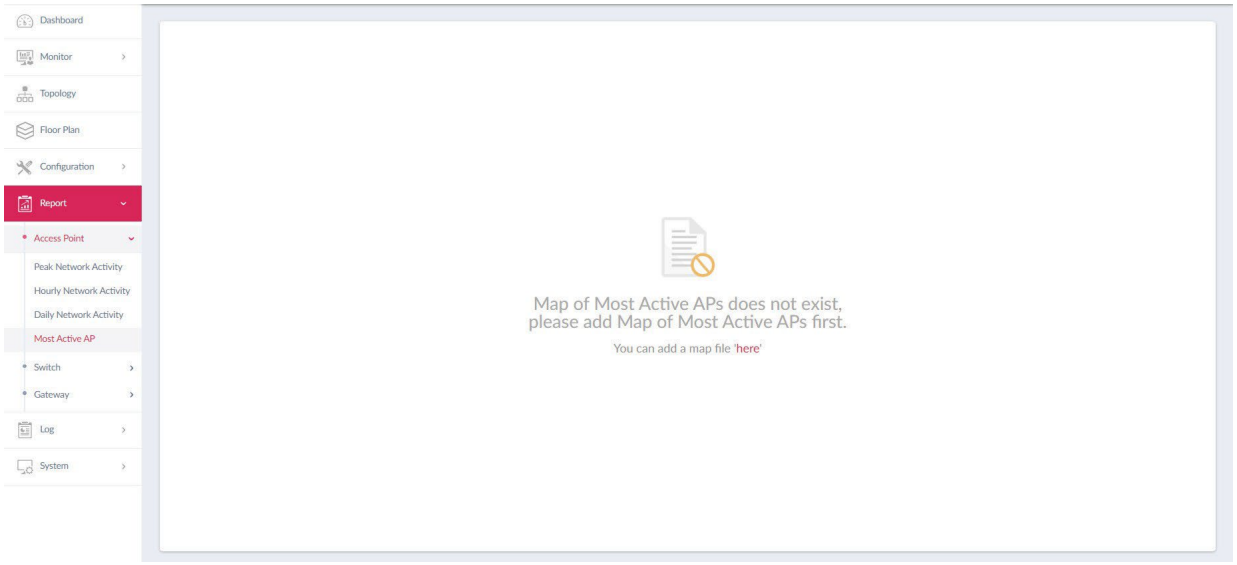
Access Point > Most Activity AP

To view a specific client's traffic usage, select a client from the most active APs column. Available maps can be edited or deleted by clicking or . In the **Edit Map of Most Active APs** page, enter the name of the map and click the **Select AP** drop-down menu to select an AP from a list of available APs. Once defined, click **Save** to complete the process.

To add a new map, click to open the **Create Map of Most Active APs**. Enter the map name in the name field. Customize the map by dragging and dropping an image (supported file formats: *.png,*.jpg; max. size: 10M) or browsing a local folder to select an image.

To view a network AP active map report, select the date and time, and click to view the report.

Once a report has been generated, click to save the report to a local PDF file.



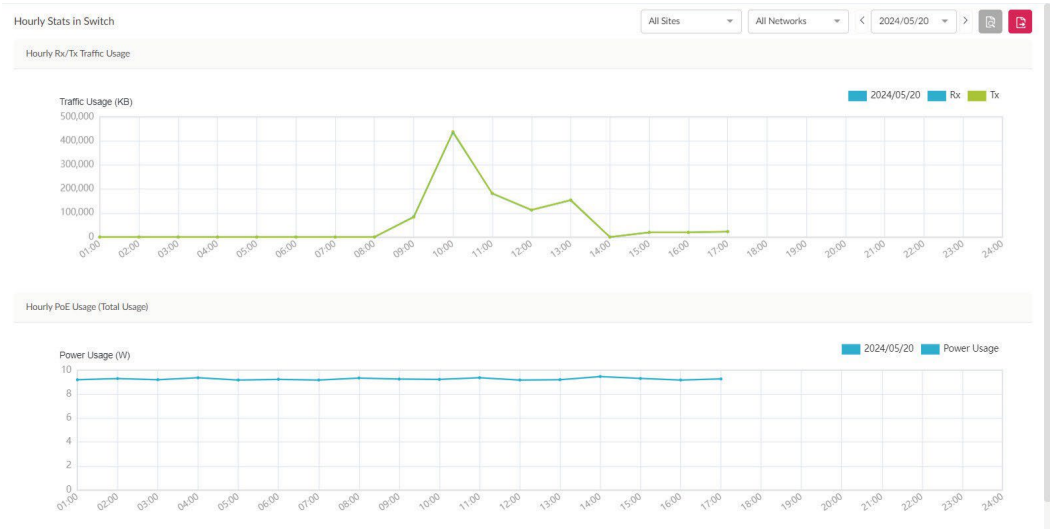
Switch

Switch > Hourly Network Activity

The Hourly Network Activity function allows administrators to monitor daily traffic and power usage on the network. Traffic usage and PoE Usage is reported by the hour. Navigate to **Report > Switch > Hourly Network Activity** to generate and view the report.

To display clients' traffic usage and PoE usage, select a site, network, and define the starting and ending dates of the search. Once the search parameters are defined, click to view the report.

Once a report is generated, click to save the report to a local PDF file.



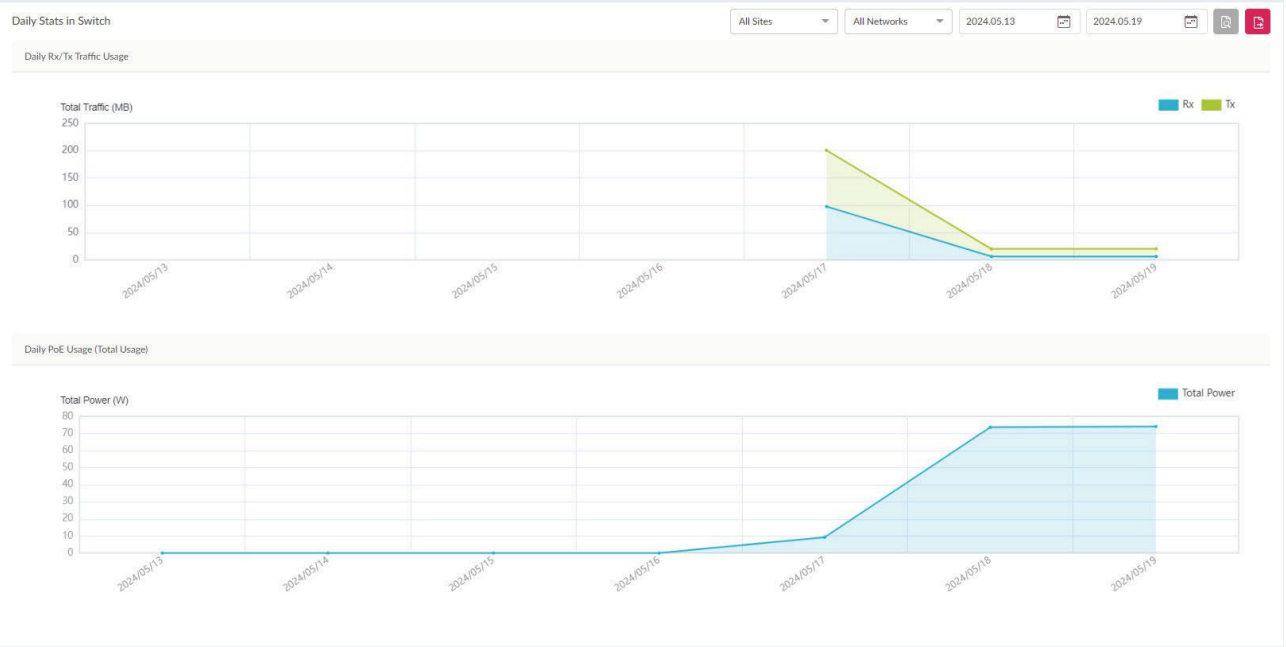
Switch > Daily Network Activity

The Daily Network Activity function allows administrators to monitor daily traffic and power usage on the network.

Navigate to **Report > Switch > Daily Network Activity** to generate and view the report.

To display clients' traffic usage and PoE usage, select a site, network, and define the starting and ending dates of the search. Once the search parameters are defined, click to view the report.

Once a report is generated, click to save the report to a local PDF file.



Switch > Top Ranking

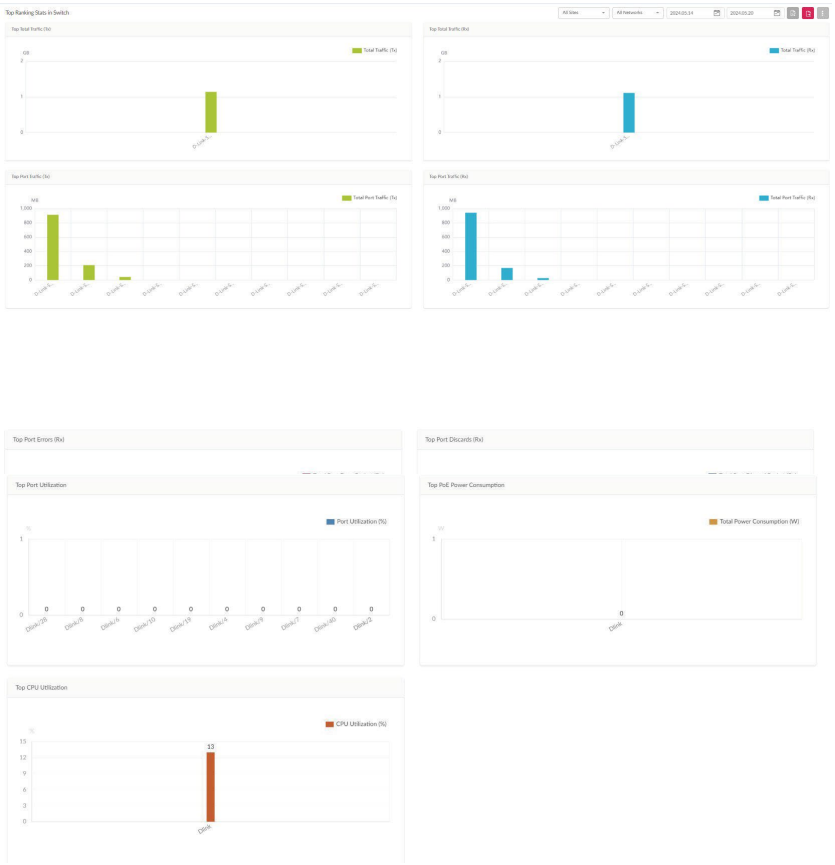
The Top Ranking report allows administrators to view a range of switch traffic reports sorted by top 10 rankings on the site and network.

The following ranking reports are available: Top Total Traffic (Tx), Top Total Traffic (Rx), Top Port Traffic (Tx), Top Port Traffic (Rx), Top Port Errors (Tx), Top Port Discards (Rx), Top Port Multicast (Rx), Top Port Broadcast (Rx), Top Port Utilization, Top PoE Power Consumption, and Top CPU Utilization.

Navigate to **Report > Top Ranking** to view the report.

To filter the top ranking report, select the site and network from the corresponding drop-down menu and click to view the report.

Once a report is generated, click to save the report to a local PDF file.



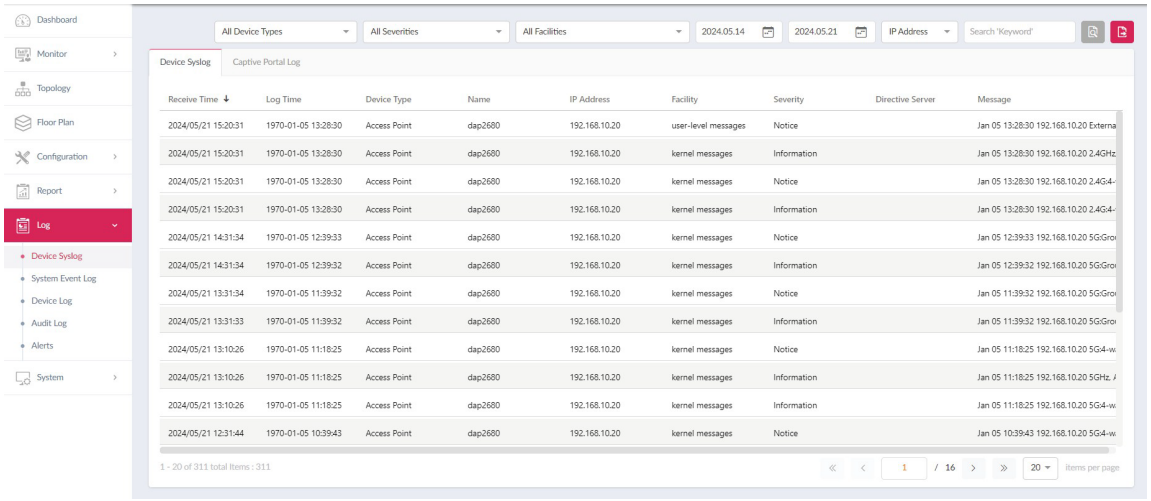
Log

Syslog

The Syslog function allows administrators to view alert messages for events concerning system logs. Log messages for the system and captive portals can be viewed here. Navigate to **Log > Syslog** to view the relevant information.

To start a syslog report, select the event severity, facility system, and define the period of time to report. Click the drop-down menu to define the type of search criteria to view, IP Address or Trap Details. Fill in the keyword field and click to view the generated report.

Once a report is generated, click to save the report to a local PDF file.

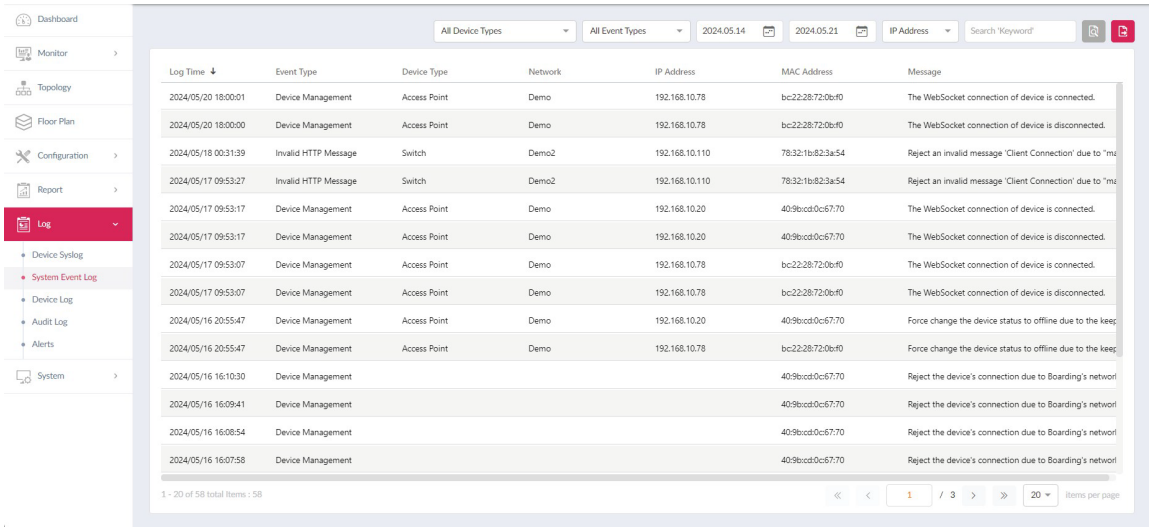


System Event Log

The System Event Log function allows administrators to view alerts that may require attention and necessary action to continue operation and prevent failures. Navigate to **Log > System Event Log** to view the relevant information.

To generate a System Event Log report, select the event severity and define the period of time to report. Click the drop-down menu to define the type of search criteria to view, IP Address or Trap Details. Fill in the keyword field and click to view the generated report.

Once a report is generated, click to save the report to a local PDF file.

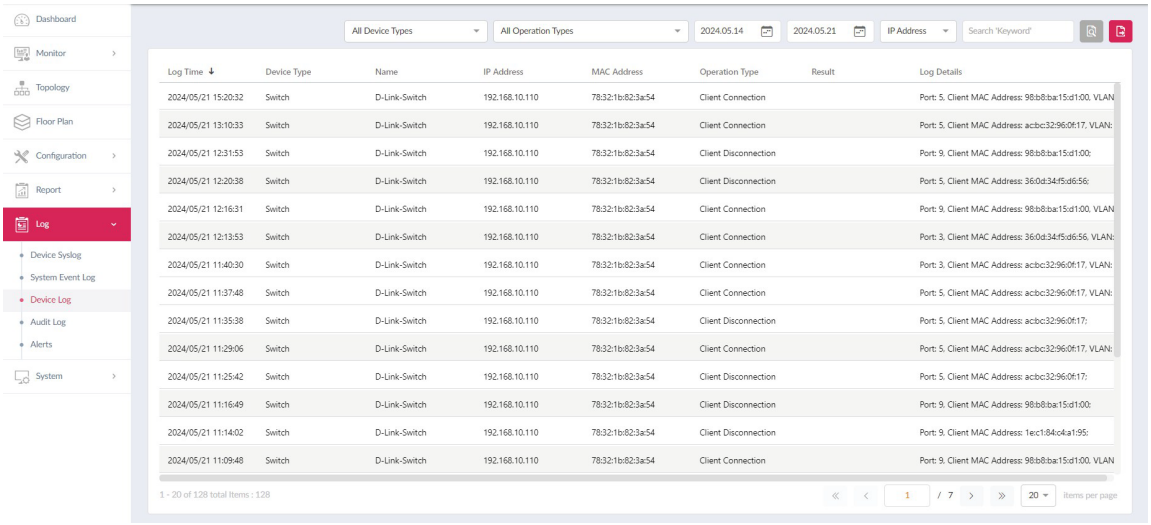


Device Log

The Device Log function allows administrators to view alert messages from a device's embedded memory. The system and network messages include a time stamp and message type. The log information includes but is not limited to the following items: Synchronize device settings, upgrading firmware, upload configuration, and blocking clients.

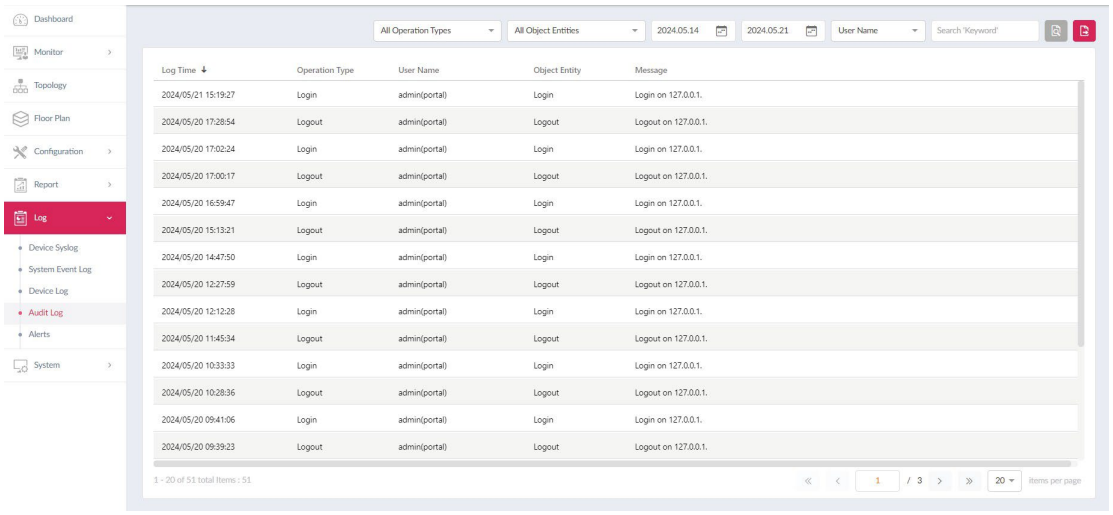
Navigate to **Log > Device Log** to display the function information.

To start a Device Log, select the operation type and define the period of time to report. Click the drop-down menu to define the type of search criteria to view, IP address or Trap Details. Fill in the keyword field and click to view the generated report. Once a report is generated, click to save the report to a local PDF file.



Audit Log

This type of log records user activities that can be performed on an object entity such as profile and network creation or deletion.

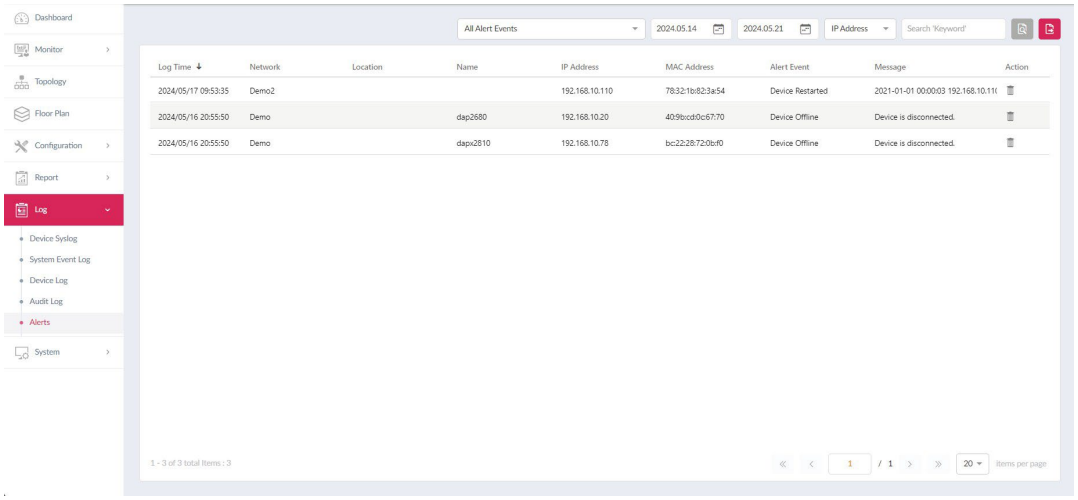


To generate an Audit Log report, select the entries by Operation Type (operations that performed on the object entities) and Object Entity (i.e. objects associated with the functional tabs in the left pane), define the time period, and select Username or Message as the filtering criteria. Then enter a keyword and click to display the search results.

Once a report is generated, click to export it as a local Excel file. The file will be saved to your browser's download directory and will be named as follows: Nuclias_Connect_log type_YYYY_MMDD_HHMMSS.

Alerts

This type of log records alert events such as new firmware release, port linked or blocked, device online status.



To generate an Alert report, select the alert events, define the time period, and select IP Address or Message as the filtering criteria. Then enter a keyword and click to display the search results. Once a report is generated, click to export it as a local Excel file. The file will be saved to your browser's download directory and will be named as follows: Nuclias_Connect_log type_YYYY_MMDD_HHMMSS.

System

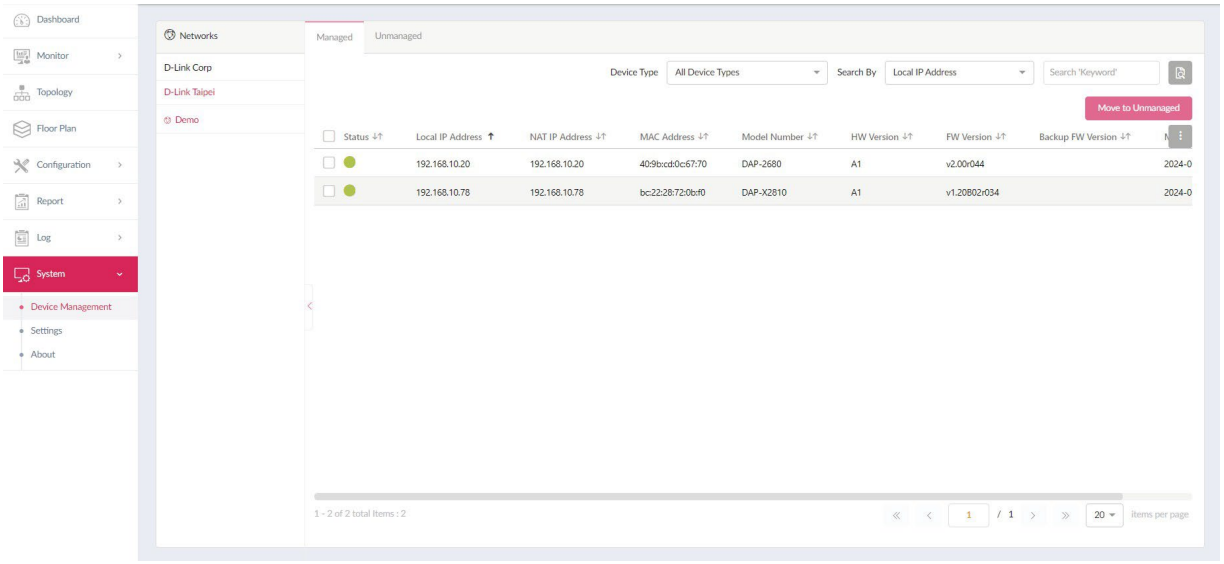
Device Management

Navigate to **System > Device Management** to view both managed and unmanaged devices on the network. To view more detailed information about the device, navigate to **Log > Device Log**.

First select the site and network, then click on the respective tab to view either managed or unmanaged devices.

The **Move to...** button on the upper right corner of each tab allows you to move devices between Managed and Unmanaged. When a device is moved to Unmanaged, you'll have the option to remove the device from the network by clicking the Delete button.

The list of devices can be sorted by the following criteria: Status, Local IP Address, NAT IP address, MAC Address, Model Type, HW Version, FW Version, Managed Time, Backup FW Version. The Menu button contains more fields to which you can add to the list to view.



Settings

Settings > General

The Settings page displays General, Connection, SMTP, Backup, REST API, Single Sign-On (SSO), Alerts, and FOTA information.

Under the General tab, there are options to customize system settings, which include adding a logo and enabling the captcha feature. Device time and date and live packet interval settings are also available.

Navigate to **System > Settings** to configure your device settings.

In the **Customized Settings** section, the following parameters can be configured:

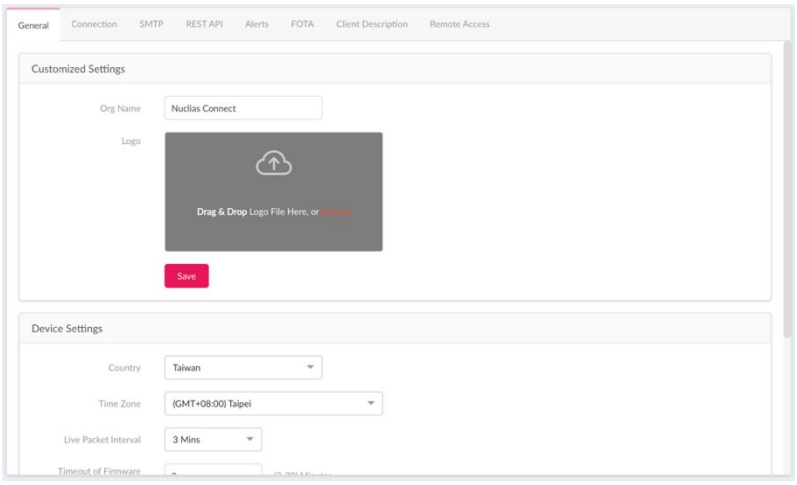
Parameter	Description
Org Name	Enter a description to set the organization name.
Logo	Click **Browser** to select a file to be used as the interface logo. A local file can be selected by using the browsing function or by dragging and dropping a file into the frame. Supported file types include PNG or JPG images.
Login Captcha	Click the drop-down menu to enable or disable the login Captcha function.

Click **Save** to save the settings.

In the **Device Settings** section, the following parameters can be configured:

Parameter	Description
Country	Click the drop-down menu to select the country region of the switches/APs in the network.
Time Zone	Click the drop-down menu to select the time zone.
Live Packet Interval	Click the drop-down menu to select the live packet interval time.

Click **Save** to save the values and update the screen.



Settings > Connection

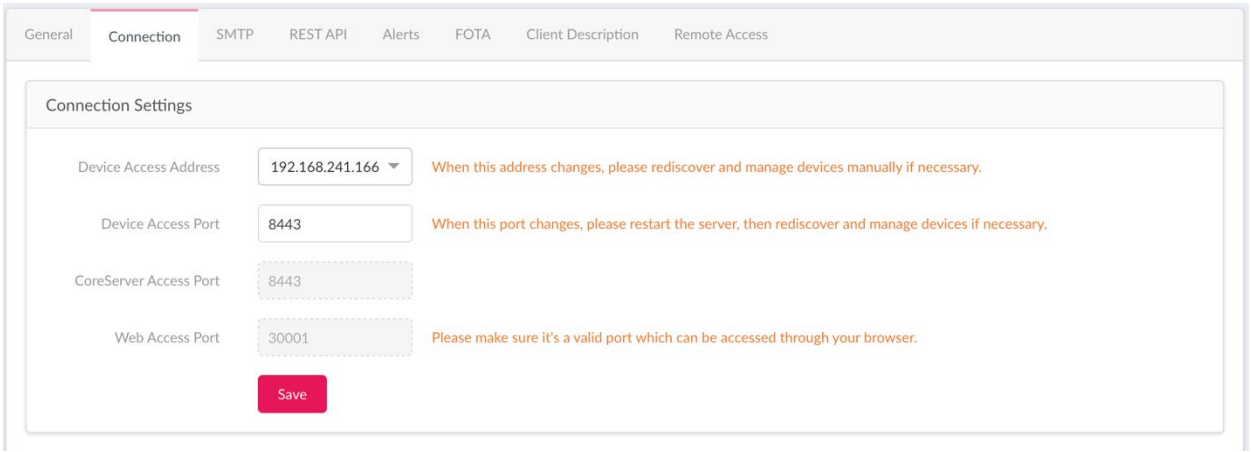
The Connection tab displays device access address, port, and SSL certificate settings.

Navigate to System > Settings and click the Connection tab to display the relevant information.

In the Connection Setting section, the following parameters can be configured:

Parameter	Description
Device Access Address	Enter the Nuclias Hyper Server application's IP address. To manage remote APs, the IP address must be a public IP address; IP mapping is required for instances behind a firewall or router.
Device Access Port	Enter the Nuclias Hyper server application's listen port number. The default value is 8443. For remote AP management behind a firewall or router, the inbound port must be opened.
CoreServer Access Port	Enter the server application's service port number. The default value is 8443.
Web Access Port	The web access ports as defined during the installation. The values are predefined.

Click **Save** to save the values and update the screen.



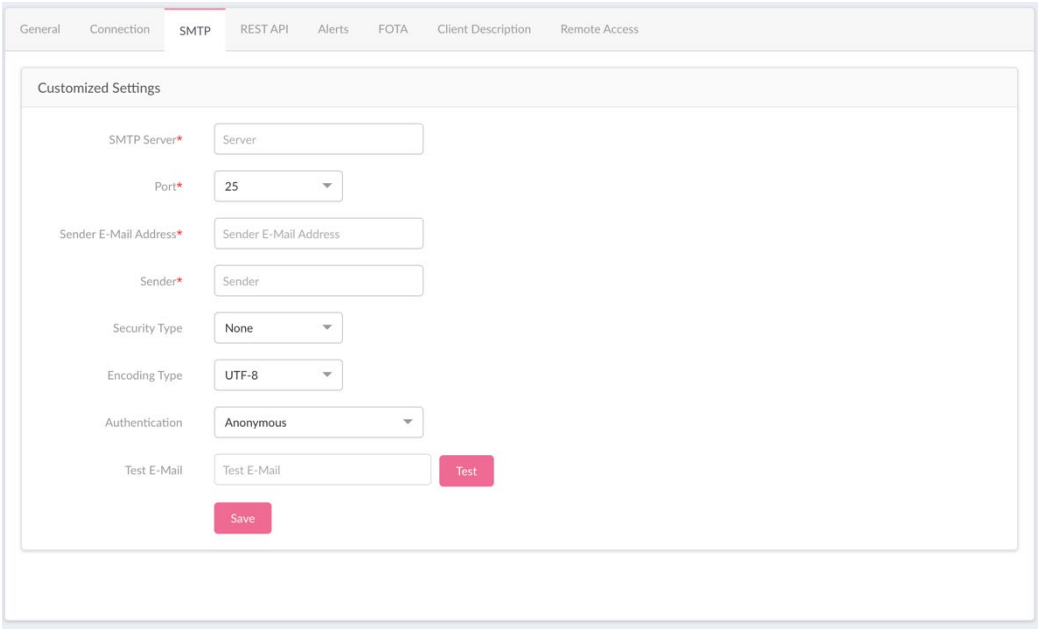
Settings > SMTP

The SMTP tab displays customizable settings for the simple mail transfer protocol (SMTP). This is necessary in order to send emails on behalf of the system such as reset password validation emails.

Navigate to **System > Settings** and click on the **SMTP** tab to display the function information.

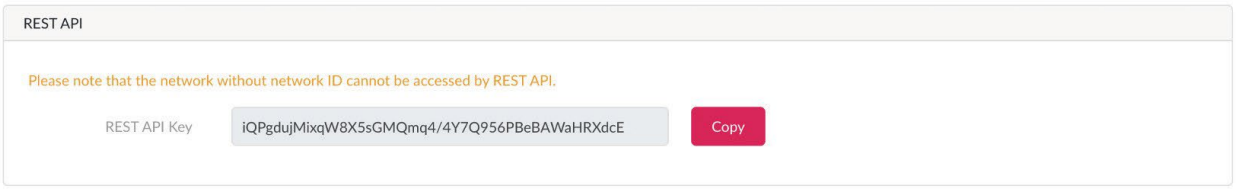
Parameter	Description
SMTP Host	Enter the SMTP server's IP address or domain name.
Port	Enter the SMTP server's port number.
From Email Address	Enter the sender's email address.
From Name	Enter the sender's name.
Security Type	Click the drop-down menu to select the security type to be used in the e-mail system. The options include None or SSL.
Encoding Type	Click the drop-down menu to select the encoding type to match the supported e-mail client. The options include UTF-8 or ASC-II.
Authentication	Click the drop-down menu to select the authentication mechanism during login. The options include Anonymous or SMTP Authentication.
Test Email	Enter the recipient e-mail address to initiate a test e-mail through the SMTP configuration. Click **Test** to start the test function.

Click **Save** to save the values and update the screen.



Settings > REST API

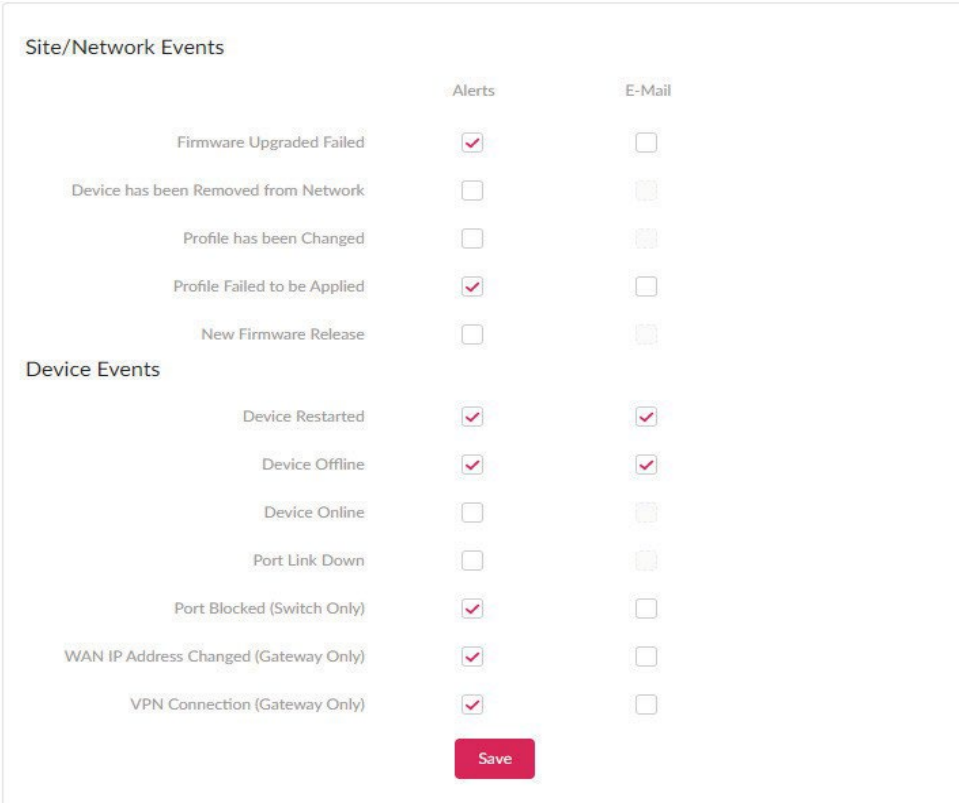
REST API is a software interface that allows two applications to communicate with each other over the internet and through devices. Enable it to allow Nuclias Connect communicate with third-party application through REST API.



Settings > Alerts

The Alerts tab allows you to configure the alert event types. Check the types of events that should generate an alert. To view generated alerts, go to **Log** > **Alerts** to view alerts.

To receive Email alerts, check the Email box next to the Events, and go to **System**>**Settings**>**User Management**, edit the user and select "Receive Email Alert" to allow users to receive email alerts from Nuclias Connect.

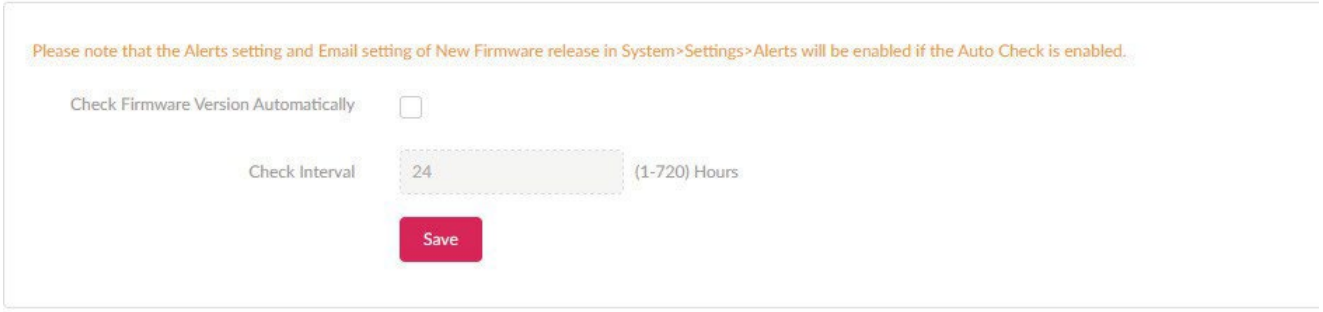


Click **Save** to save the values and update the screen.

Settings > FOTA

The FOTA (Firmware Over-The-Air) feature enables users to wirelessly upgrade to the latest firmware. Click the box to enable automatic firmware check. Once Auto Check is enabled, you can then set a check interval between 1-720 hours.

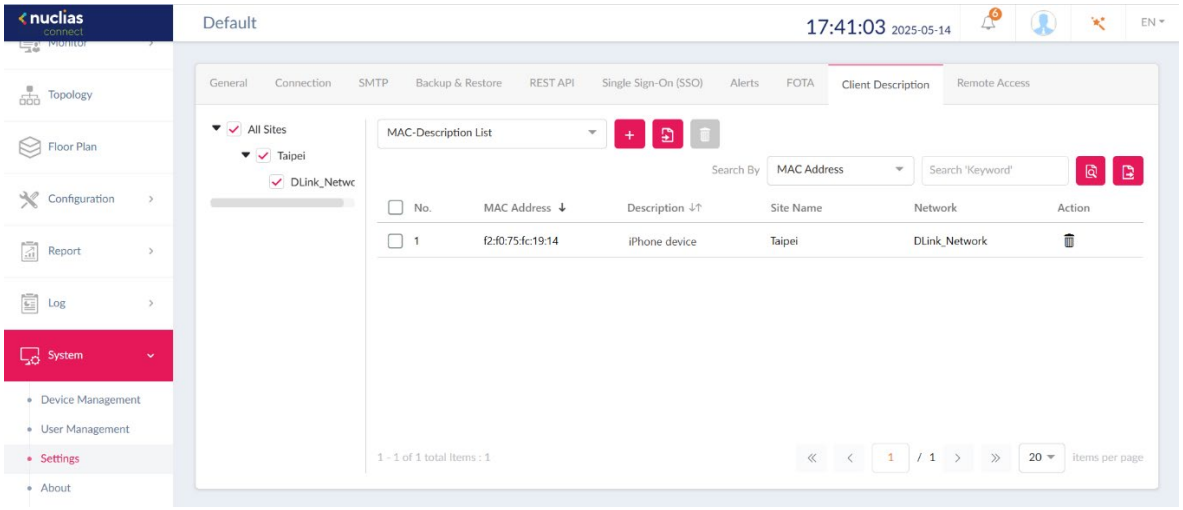
Note that when Auto Check is enabled, the Alert and Email settings will also be enabled.



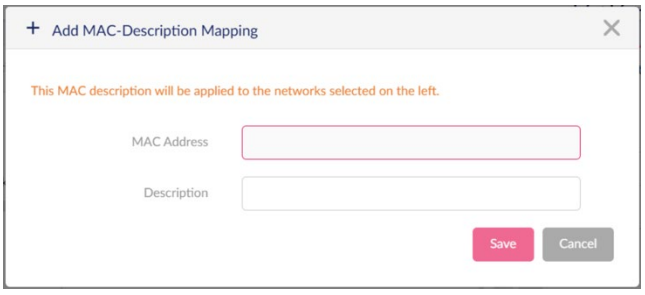
Settings > Client Description

The Client Description tab show client device description list

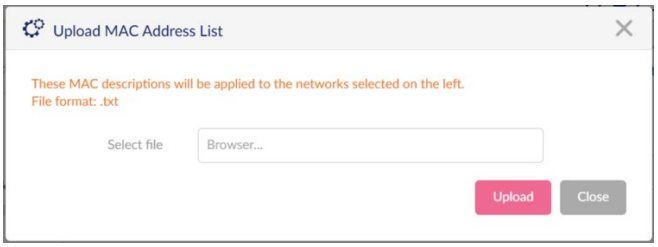
Administrator can enter client description manually.
Non-administrators can only view, not edit.



Click + to add MAC description mapping



Click next to the + to upload MAC address list and format is txt file



Click to delete the selected item

Click next to the to export client description list CSV file

Settings > Remote Access

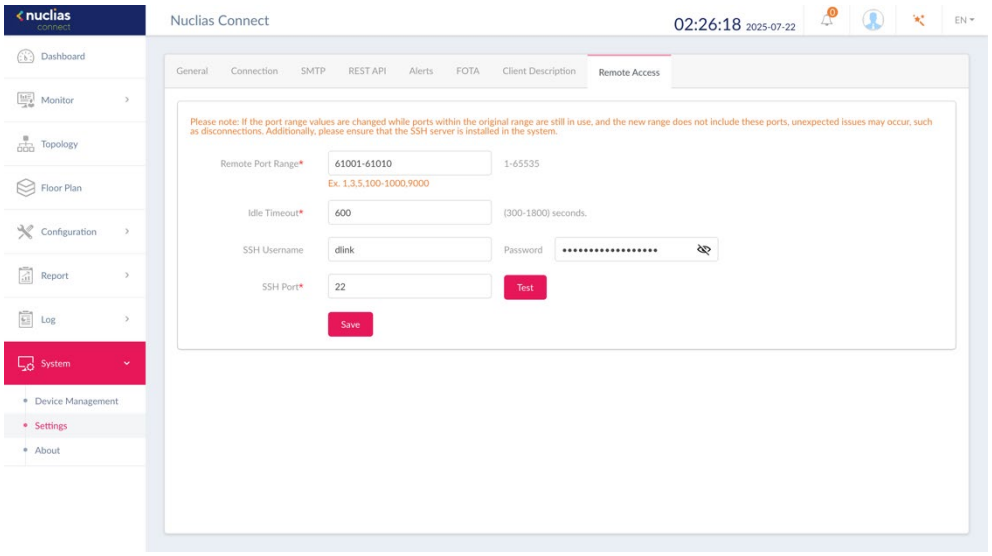
The Remote Access tab allows you to configure the remote access setting

Remote Port Range specifies the range of ports that the server's Remote CLI and Remote Web can use. The default range is 61001–61010. You can set a value, multiple values, or a range. The Port Range is from 1 to 65535.

Idle timeout default is 600s, range 300s~1800s, the adjustment of the Idle Timeout will only affect newly established tunnels, and existing tunnels will not be affected.

In the SSH Username & Password fields, enter the admin username and password of the computer where Nuclias Hyper is installed.

Note: Unable to operate when user permissions are insufficient. When user permission is “Root User” or “Local User” or “Local Admin”, the page items are shown as disabled



Note: When the Remote Access function is unavailable in the DNC environment, please check the following items.

1. Please first confirm whether the SSH service is installed.
2. Modify the following configuration.

Software name: **sshd**
Configuration file path: **/etc/ssh/sshd_config**

A. **Modification**: Remove the # symbol from the line

```
shell

#GatewayPort yes
```

so it becomes:

```
shell

GatewayPorts yes
```

B. **Restart sshd command**:

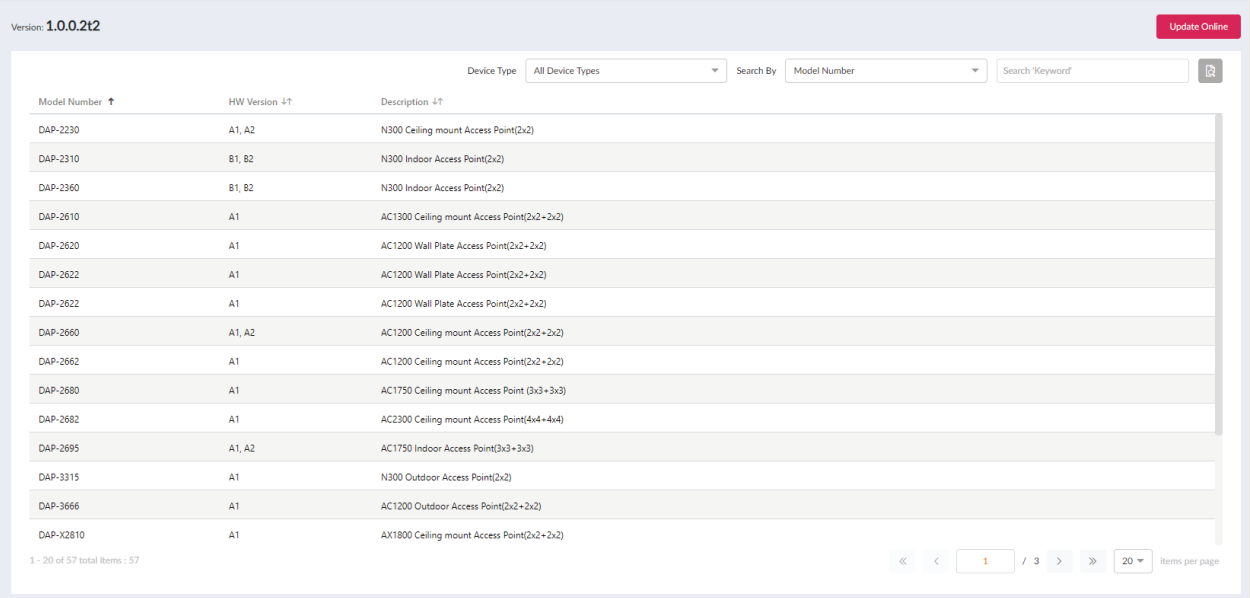
```
shell

sudo systemctl restart sshd
```

About

The **About** page displays a list of supported switches and access points.
Navigate to **System > About** to view the information.

The list can be updated by clicking **Update Online**. If an update is available, new supported device will also be displayed.

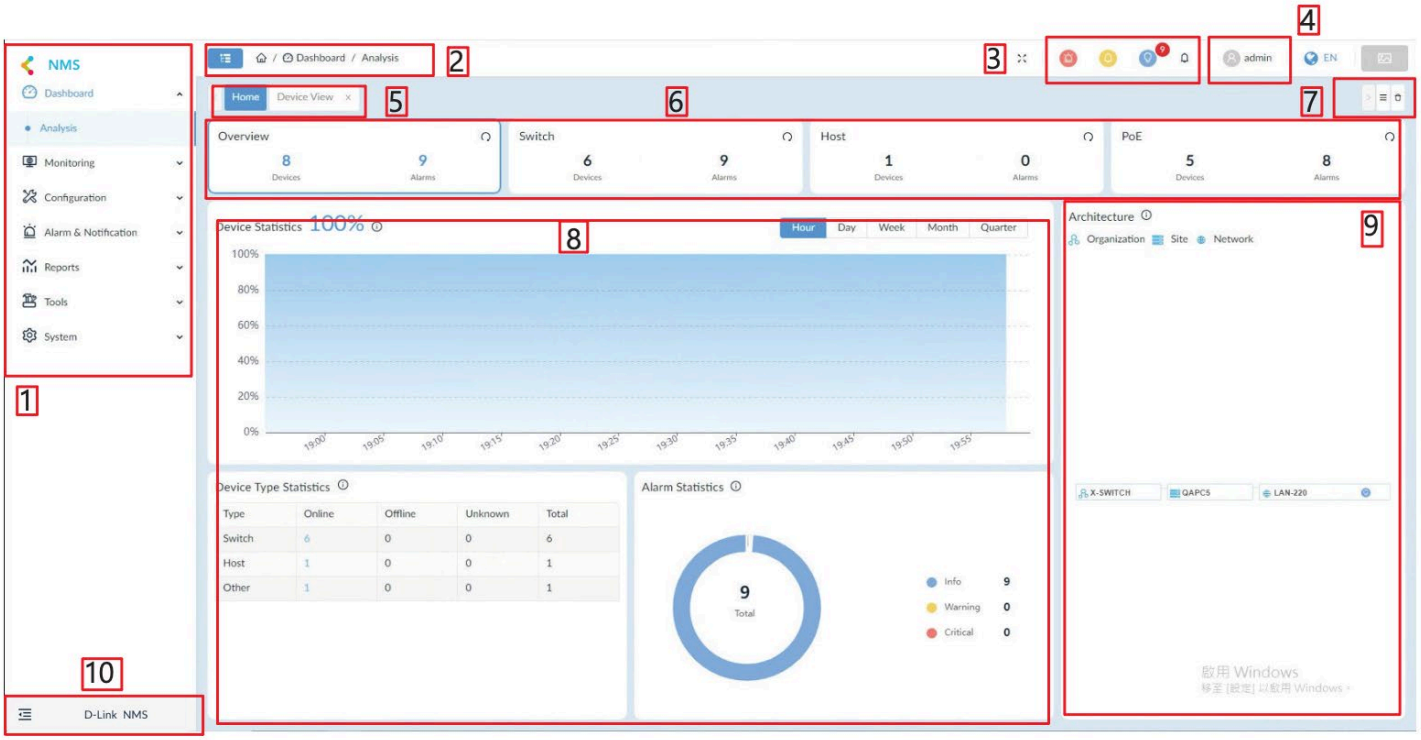


Nuclias Hyper / NMS

Overview

Dashboard

The NMS Dashboard features and functionality can be accessed through the menus and toolbar of the web interface. The availability of the tools is determined by a user's role.



Web Dashboard Annotations			
1	Main Menu	2	Title Bar
3	Annunciators	4	User profile and Wizard
5	Menu Tab	6	Widget Menu
7	Tab Selector	8	Widget Information
9	Architecture Diagram	10	Collapse / Expand Sidebar

Common Features

There are several features that are common on the NMS dashboard regardless of the user privilege.

- Menus are used to access tools and configurations.
- Sort and Filter functions help you refine table data.
- Configuration menus help you access features that are available on a configuration page, which can be accessed through toolbar buttons.
- Help menus can be opened by clicking ⓘ to obtain additional information relevant to the displayed page.
- Toolbars give quick access to the functions or pages of corresponding menu options.
- Annunciators offer visual notification of system state or alarms.

Menus and Toolbar

The following section describes the menu and toolbar options available through the NMS dashboard. The menu items are listed along with the corresponding submenus and description.

Note: Menu and toolbar options vary depending on the user role and device type.

Item	Description
Basic Settings	Organization • Configures the organization's name, country, time zone, etc. • Upload the organization logo in PNG or JPG file format (less than 2MB file size) Forward Trap • Configures the trap receiver to send incoming device trap messages Forward Syslog • Configures the system log receiver to send device syslog messages Credentials • Configures the SNMP protocol types, community name and related parameters • Configures Windows WMI (Windows Management Instrumentation) and SSH/Telnet communication credentials System Preferences • Configures the table display settings and theme of NMS
Scheduling	Configures the "Recurrent Schedule" and "Time-range Schedule" Recurrent Schedule List • Allows users to configure recurrent schedules with customized frequency and duration Time-range Schedule List • Allows users to configure
Server Management	• Monitors the status of NMS Core Server, Web Server and Probe • Checks the real-time report of server's status, which includes the utilization of CPU, memory, hard drive, and the network traffic
NMS Log	NMS features three types of logs: User Operation Log, System Log, and Device Maintenance Log User Operation Log: • Records user operational activity via web interface System Log: • Keeps the records of NMS's running status of servers and probes Device Maintenance Log: • Keeps configuration activity logs for devices
About Page	• The About page keeps the following information: • Product Name • Software version • The latest update time • The number of supported and used nodes • System uptime information

Dashboard

Item	Description
Analysis	By default, there are four tabs representing major topics or device types in the analysis page: • Overview • Switch • Host • PoE Provides an overview of alarm statistics, online/offline status of the devices, CPU/memory utilization, performance report, device health, etc. The information varies according to device type

Monitoring

Item	Description
Network Discovery	Configures network discovery parameters, which include: • Basic Information: the name of the network and site to discover. • Probe Mode: Choose the primary and secondary probe • Discovery Range: Define the range that may include a single IPv4/v6 address, an IPv4/v6 address range, an IPv4/v6 subnet, or import of IP ranges from a file • Schedule: Define the discovery schedule that may include one-time discovery or recurrent discovery Displays discovery jobs' running status and related information
Device View	• Includes 5 categories: All, Managed, Unmanaged, Ignored and Conflicted • Displays a summary and detailed information of the devices • Detailed information can be accessed via the "System Name" link, which also allows login to a device using different protocols
Interface View	List of devices' network connection properties, which includes: • System/Model Name • Device's IP address • Interface and MAC address information • VLAN information • Update time information Each of the above can be searched to find a specific device
Topology Map	• Displays connections between devices for the entire network, site or organization • Displays the online/offline status of devices • Displays link information of devices • PNG or JPG format files can be uploaded as the topology's background image • Supports Star, Tree, Circular and Grid topology layout • Zoom in and out the topology map • Supports customized topologies
Device Group	• Allows users to create device groups to simplify management tasks

Configuration

Item	Description
Batch Configuration	Allows simultaneous configuration of multiple devices' parameters at the same time Two sub-features: • Quick Configuration: a template for each function to apply the settings to multiple devices • Advanced Configuration: a profile for a specific type of device. The profile contains configurations of multiple features. Users can apply the profile to multiple devices of the same type/model.
Task Management	Lists all created tasks to show the execution result with messages indicating a success or failure. It includes both Current and Historical Tasks. If a failure occurs, it will also state the reason for failure.
Firmware Management	• Management of devices' firmware centrally • Schedule-based updates of device firmware
Configuration Management	• Management of device configuration • Backup or restore of multiple device configuration files at the same time • Schedule-based backup or restore • Supports file baselining

Alarms & Notifications

Item	Description
Alarms	Displays all alarm information collected from network devices. The alarms include Active Alarms • Lists all unacknowledged network alarms Historical Alarms • Lists all acknowledged network alarms
Trap & Syslog	Displays the trap and system log receiving from devices. The trap log's information contains: • Time received • Device system name • Device IP address • SNMP version • Generic type • Trap description • Original message of the trap The syslog information contains: • Time received • System name of device generating the log • Device IP address • Syslog severity levels • Syslog messages • The associated alarm for the syslog • The site and network of the device
Trap & Syslog Editor	• Edits OID description for a specific trap OID • Edits syslog description with matched keywords
Monitor & Alarm Set tings	Monitor Settings • Configure the monitor status and interval for data collection Alarm Settings • Configure alarm rules to generate alarms with threshold values • Configure the CLI commands for devices and NMS servers to execute when the alarm is triggered • Define the alarm properties for customized monitors and alarms
Notification Center	Allow users to set the notification method when alarms are triggered: Web Scrolling Message, Email, and Execute script.

Reports

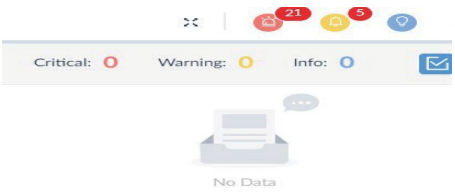
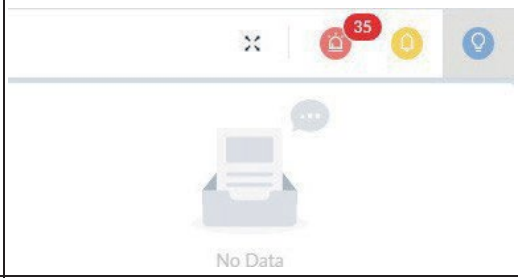
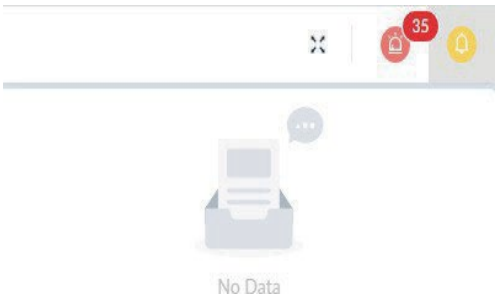
Item	Description
General Reports	Each report type has distinctive configurable parameters such as data source and data collection time interval. When reports are generated, they can be exported immediately or upgraded to Scheduled Report. The following types of reports are available: • Device Reports • Device Health • Trap • Syslog • Device Top N • Wired Interface Reports • Wired Traffic • Wired Throughput Top N • Advanced Reports • Inventory
Scheduled Reports	Reports can be a one-time report or recurrent report.

Tools

Item	Description
ICMP Ping	Checks device operation status and network performance
SNMP Test	Checks device SNMP capabilities using SNMPv1, SNMPv2c or SNMPv3
Trace Route	• Checks the route and measures transmit delay of packets across the network • Terminal interface for users to connect with the device
Command Line Inter- face (CLI)	Terminal interface for users to connect with the device

Annunciator

The Annunciator is typically located at the top right of the application webpage to notify users of the system status. The following are the different types of alarms displayed via the annunciator:

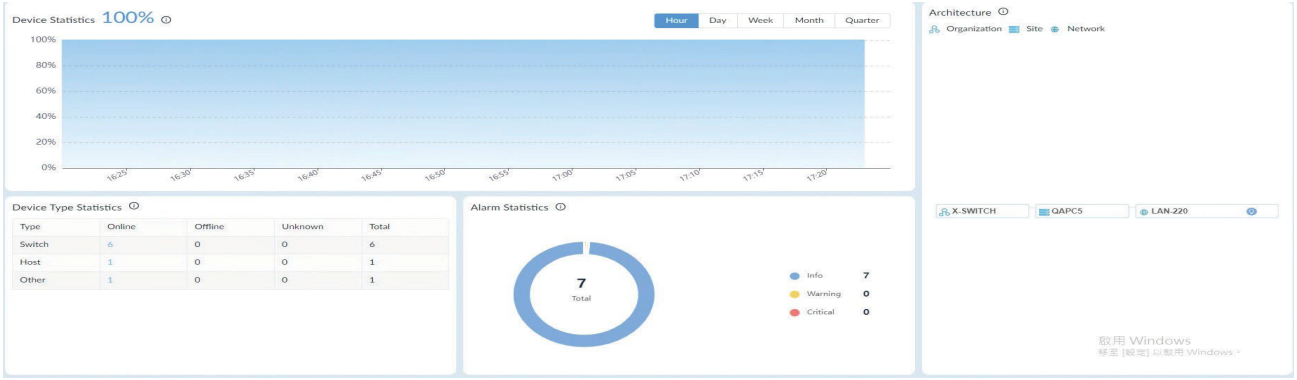
Item	Description	Icon
Notifications	Defined events to send notifications when an alarm is triggered	
Info Alarm	Information regarding system function re- quiring further attention to maintain proper system operation or to avoid unintended result.	
Warning Alarm	Information regarding system errors or faults that may affect system operation.	
Critical Alarm	Information regarding system errors or faults and requiring immediate attention and remediation to prevent further damage.	

User Menu

Item	Description
Wizard	• Discovery: discover the network and add devices to the network • Alarm: customize related network alarms and notifications
Network Discovery Records	Displays the record of the discovered networks

Workspace

The NMS workspace starts with a standard configuration displaying the available system and network information. Through the interface, you can quickly obtain the corresponding settings of the information displayed on the dashboard.



The workspace is designed for complete visibility and control of the entire network.

To view specific information, click on the link of the content.

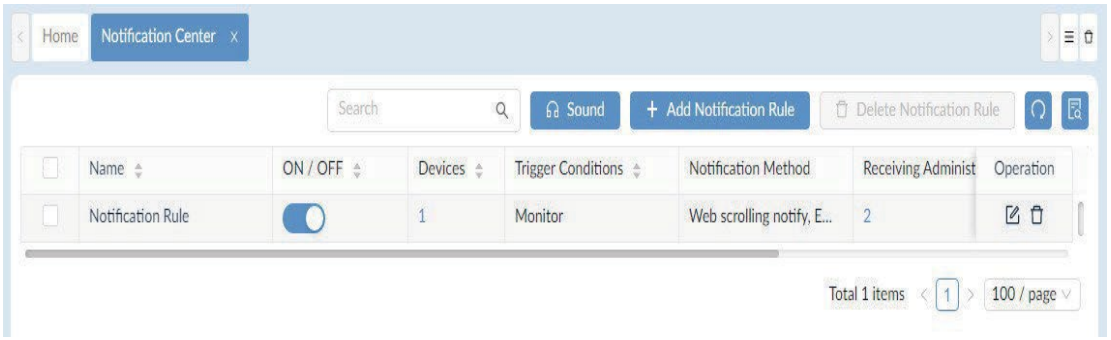
Configuration the Notification Center

Notifications are messages that the notification display of the NMS application. It provides you with timely information that requires your attention. The notifications can be easily accessed from the display at the top right of the NMS web application. The Notification Rule is generated according to monitoring conditions with the triggered alarm level. Only an Organization-privileged Administrator or a Super Administrator can configure notification settings.

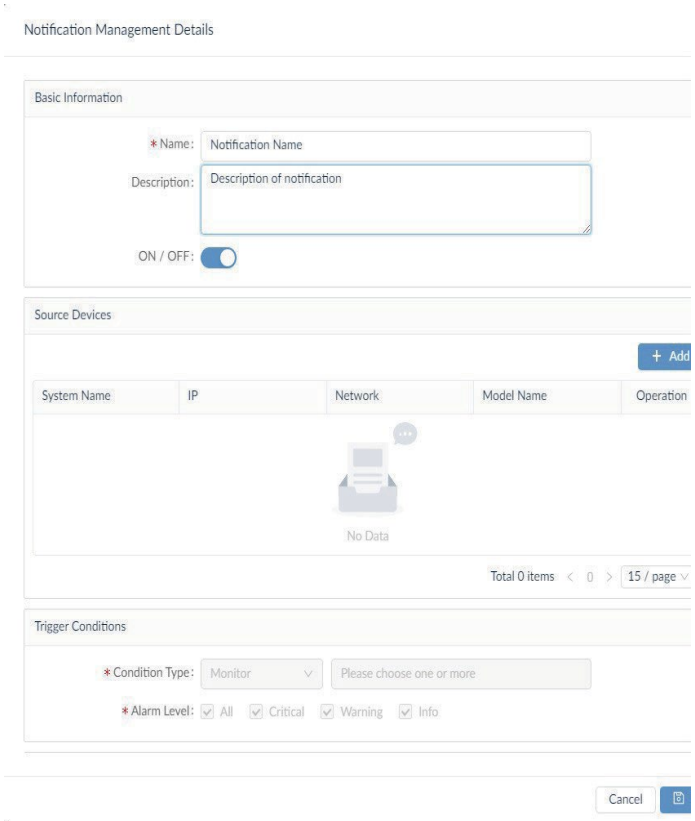
1. Click the **Alarm & Notification > Notification Center**.

The Notification Center page displays.

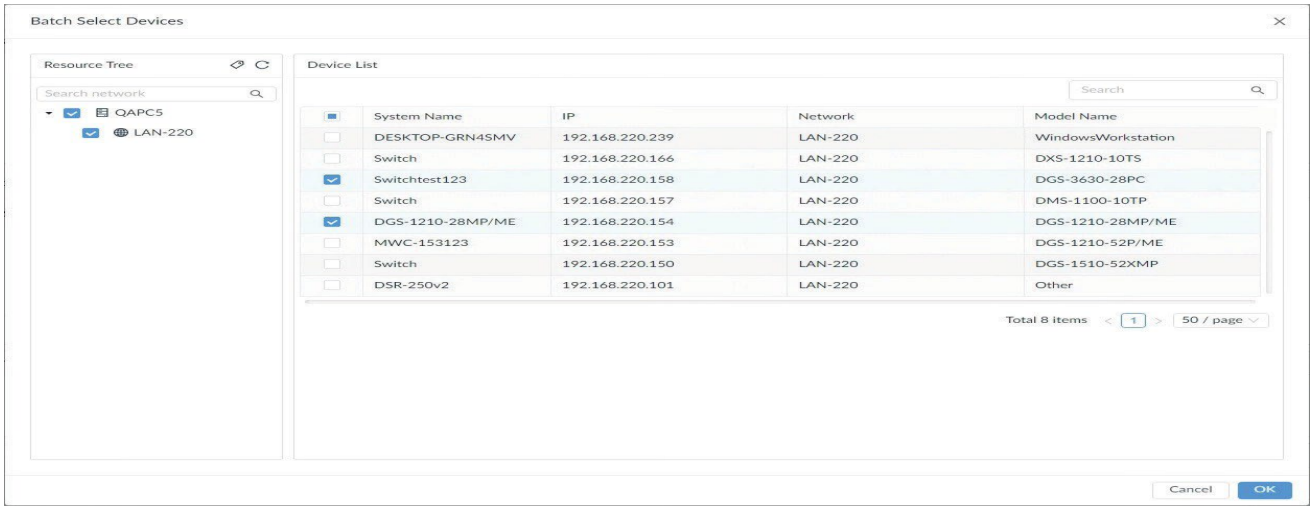
2. Click + Add Notification Rule.



3. Click the **ON/OFF** button to enable or disable the rule.

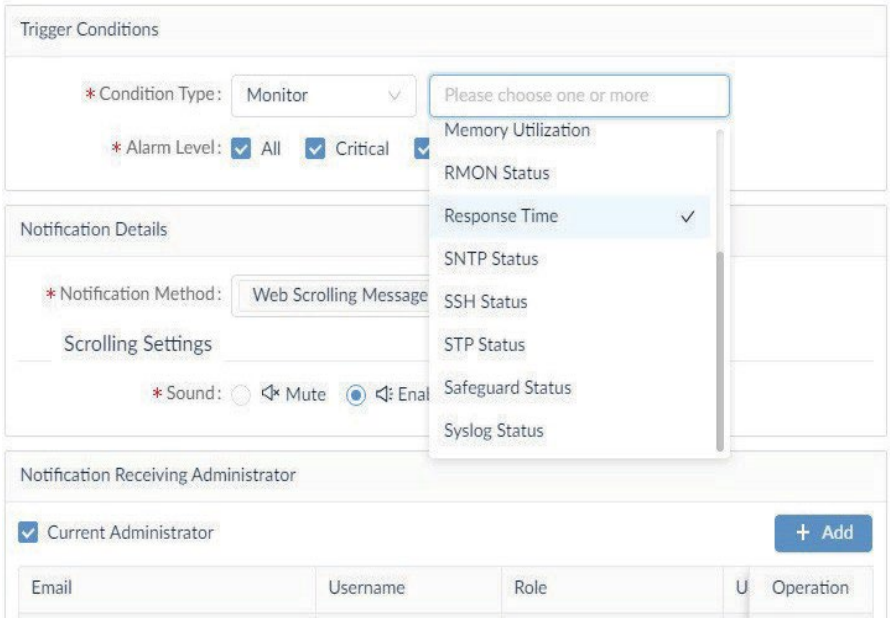


4. In Source Devices, click **Add** to select target devices. The Batch Select Devices page displays.
5. From the Device List, select the device(s) to which the notification rule will be applied.



6. Click **OK** to accept the device selection and return to the previous menu.

7. Under Trigger Conditions, click the Condition Type drop-down menu to define a condition that generates notifications.



The following table displays available options for trigger conditions:

Item	Description	
Condition Type		
Monitor	The availability of monitoring conditions varies depending on the selected device model.	
	• CPU Utilization • DHCP Server Status • Device Common Information • Fan • HTTP Status • LACP • LLDP • Memory Utilization • Private Port	• Response Time • SNTP Status • SSH Status • STP Status • Safeguard Status • Syslog Status • Telnet Status • Trap Status
Trap	Select Trap as the condition type for notification so that alarms triggered by the trap alarm rules will also generate notifications. To configure trap alarm rules, go to **Alarm & Notification > Monitor & Alarm Settings > Alarm Settings**, from the Type pane, select the **Trap** category.	
Syslog	Select Syslog as the condition type for notification so that alarms triggered by the syslog alarm rules will also generate notifications. To configure syslog alarm rules, go to **Alarm & Notification > Monitor & Alarm Settings > Alarm Settings**, from the Type pane, **select Syslog**.	
Wired Traffic	Select Wired Traffic as the condition type for notification so that alarms triggered by wired traffic alarm rules will also generate notifications. To configure wired traffic alarm rules, go to **Alarm & Notification > Monitor & Alarm Settings > Alarm Settings**, from the Type pane, select **Monitor > Wired Traffic**.	
Alarm Level	Select the level of severity that will activate the notification: All: all severity levels will activate the notification. Or select one of the following alarm levels: Critical: error information indicating failure or malfunction. Warning: error information that may cause future problems Info: information-only alarm level **Note** that there must be an alarm rule with the corresponding severity level for the notification to take effect.	

8. Under Notification Details, select the method to deliver the notification.

Item	Description
Notification Method	Configure the respective settings for each of the following notification methos.
Web Scrolling Message	Select whether to enable the sound: Mute or Enable Voice.
Execute Script	• In the Command Line, enter a script to automate a task or modify device properties or status on the source devices (Itself) or devices other than the source devices (Other Devices) when a notification is generated. • For Other Devices, select the devices to run the script. To execute a script, you need to provide credentials to log in to the system remotely. • The Acknowledge Alarm after Script Execution parameter can be used to terminate the repetitive execution of the script. For each execution of the script, the alarm will be automatically acknowledged. Enter the total Number of Repetitions (1-100) and Cycle Time (5-1440) minutes. The automatic script execution will stop when the maximum number of repetitions have been reached in the defined cycle time.

9. Under the Notification Suspension Period, click Add to select a pre-defined schedule. Or click Add Schedule to add a new schedule. The schedule prohibits delivery of notifications at the specified time range of a designated weekday or weekdays for the effective duration of dates.

10. Click **Save** to accept the notification rule or Cancel to return to the previous screen.

Network Discovery and Device

Before you can manage your network, you must let the application find the devices on your network.

This chapter covers the following topics:
- Network Discovery
- Manage Wired Devices on a Network
- Manage Device Groups
- SNMP Configuration
- Manage Networks with Batch Configuration

Network Discovery

NMS is designed to utilize probes to connect network devices. Probes run as a background process, discovering devices, polling devices for statistics, and forwarding data to the NMS server if devices are on other networks behind a firewall or in an NAT environment.

NMS probes are not limited to D-Link products and will communicate with any network device that sup- ports standard reporting protocols based on SNMP.

Deploying probes on servers for each network segment helps preserve bandwidth, as data is collected by the probe before being forwarded to the NMS server to be compiled and analyzed. This reduces network overhead by reducing the number of open connections and the need to have all the devices communicating directly with the server. Separating network devices into groups also simplifies management.

Probes are also responsible for executing commands received from the application's administrator on devices that are connected to the probe. Examples of this would be scheduling a reboot, managing event logs, or making changes to device configuration.

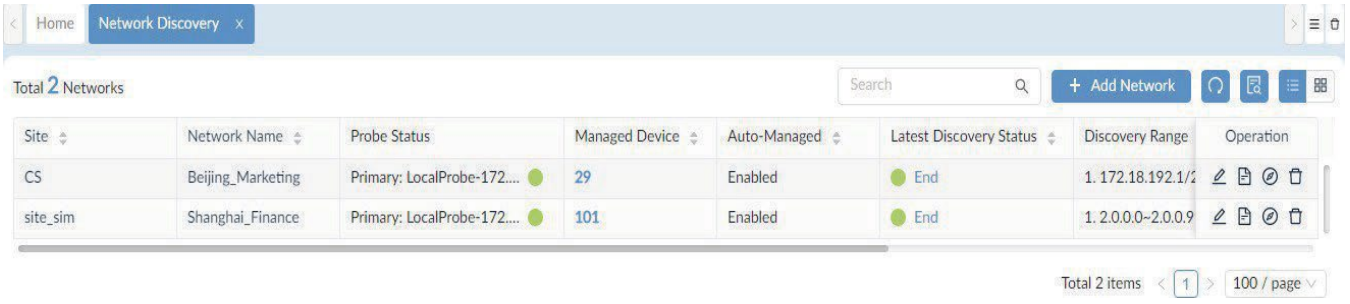
With network and device discovery, NMS can discover wired devices such as switches, no matter if they are D-Link devices or third-party devices supporting standard SNMP MIBs.
Network Discovery allows an administrator to monitor and manage active networks configured with the NMS server. Each network is displayed in the Architecture pane of the Dashboard. The number of managed devices is also displayed, along with device statistics, alarm statistics and an overview for all discovered devices.

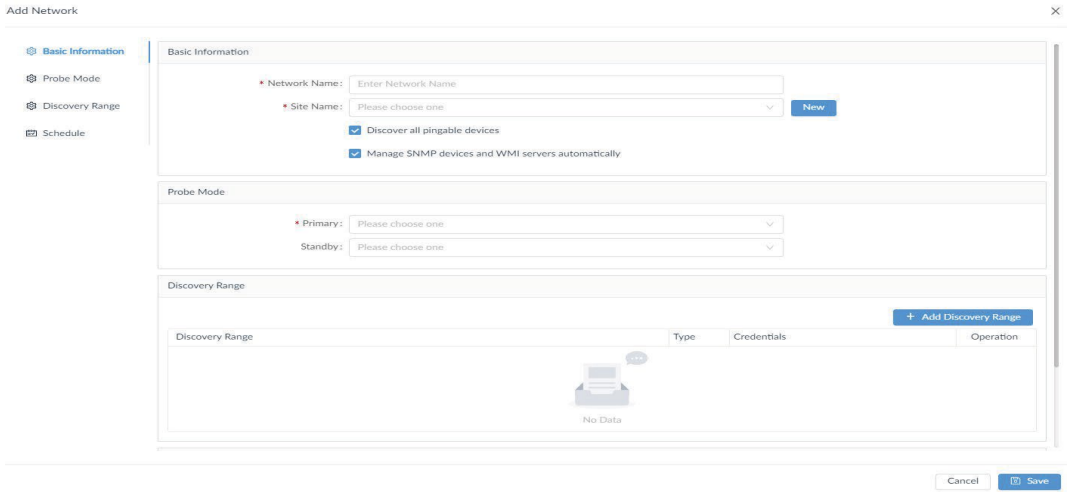
Add Network for Discovery

The application is accessible through a browser. Before logging in to the application, make sure that the NMS application is installed on a server with a static IP address.

NOTE: When a Super Admin redirects to the NMS application for the first time with the default username/password, a wizard will appear, please select Discovery to be guided through the Network Discovery process, which requires you to set up country first.

To add a network:
Go to Monitoring > Network Discovery.
1. Click + **Add Network**.





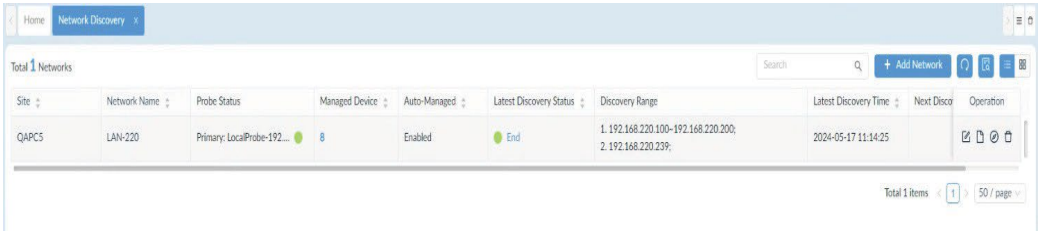
2. Enter the new network information for discovery:

Item	Description
Basic Information	
Network Name	Enter a text string to name the new network.
Site Name	Click the drop-down menu to select an existing site or click New to name this site.
Discover all pingable devices	Enable or disable the function to discover all devices that respond to the ping command automatically. The default is enabled.
Manage SNMP devices and WMI servers automatically	Enable or disable the automatic management of all SNMP or WMI de vices. If it is not selected, all detected devices via SNMP will be placed under the **Unmanaged** category. The default is enabled.
Probe Mode	
Primary	Click the drop-down menu to select the primary probe. **NOTE:** If a probe is identified as primary, it cannot be designated as a standby probe.
Standby	Click the drop-down menu to select the standby probe. The Standby probe is a backup probe in case the primary probe fails.
Discovery Range	
Add Discovery Range	Click the **Add Discovery Rang**e button to define a range for network search.
Discovery Range	List of the configured range settings. See "**Add a Discovery Range**" below for further information.
SNMP Credentials	Click the SNMP field and select the credential version for discovery: **SNMP v3, SNMP v2c, SNMP v1**, or **Add SNMP Credential**. The available credentials are set via the Basic Settings menu (go to System > **Basic Settings** and click the Credentials tab; refer to **Set Up Credentials**.) If you would like to add a new SNMP credential, click **Add SNMP Credential**.
WMI Credentials	Click the WMI field and select the credential for discovery or click **Add WMI Credential**. The available credentials are set via the Basic Settings menu (go to **System** > **Basic Setting**s and click the **Credentials** tab; refer to **Set Up Credentials**.) If you would like to add a new WMI credential, click **Add WMI Credential**.
Edit	Click the **Edit** button to modify the discovery range.
Delete	Click the **Delete** button to remove the discovery range.
Schedule Information	
Schedule Type	• One Time: Select this option to specify a date and time or immediately to initiate the network discovery. • Recurrent: Select this option to specify the frequency and effective time frame to initiate network discovery.
Cancel	Click **Cancel** to return to the previous page.
Save	Click **Save** to add the new network.

Add a Discovery Range

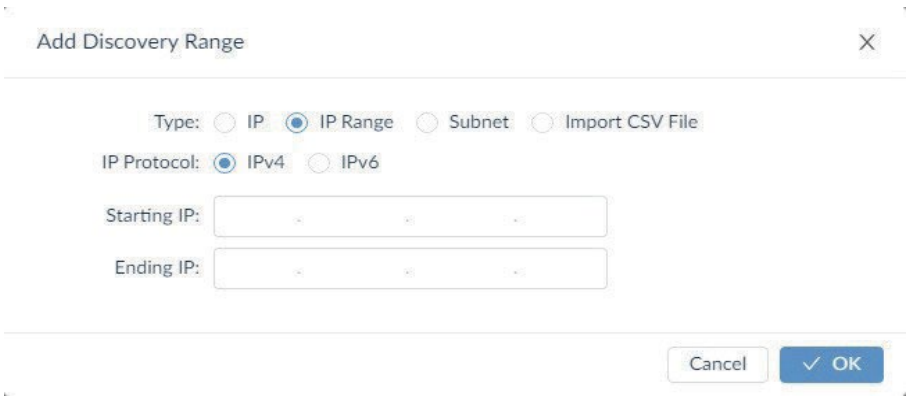
To add a discovery range:
Go to Monitoring > Network Discovery.

1. The Network Discovery information displays.



2. Click + **Add Network** to add a new network. To add a discovery range under an existing network, select a network and click Edit.

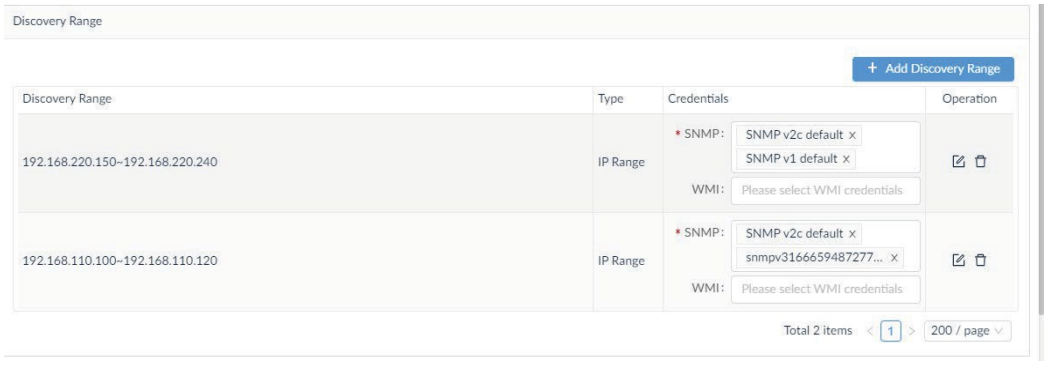
3. Select **Probe Mode** and click **Add Discovery Range** or **Edit Discovery Range**. The Add Discovery Range or **Edit Discovery Range** screen displays.



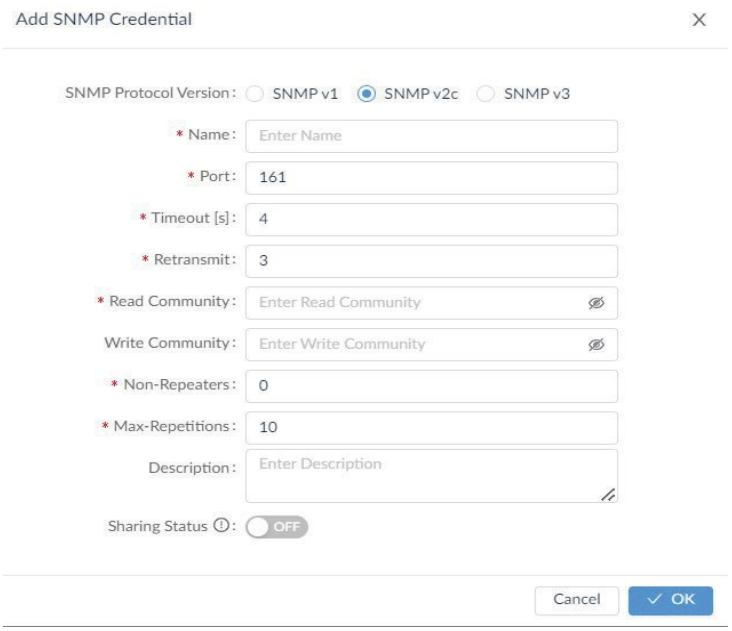
Item	Description
Type	Click to select the coverage range: IP, IP Range, Subnet, Import CSV File.
IP Protocol	Enter a single IP address as the discovery range. Select either IPv4 or IPv6 IP protocol.
IP Range	Enter the starting IP and ending IP addresses to define the range. • Use Starting IP to express the start of the discovery range. • Use Ending IP to express the end of the discovery range.
Subnet	Enter the subnet address in CIDR notation (e.g. 172.17.2.0/24 for IPv4 addressing or 2001:db8:ab-cd:0012::0/64 for IPv6 addressing) to define the discovery range. Select IPv4 or IPv6 to specify the IP protocol.
Import CSV File	Click **Select File** to select a pre-configured file. The following shows how the data should be recorded in the CSV file: 1. The import file extension must be ".csv". 2. Each line must contain no more than one discovery rule. 3. Use a comma "," to separate the parameters for each discovery rule: 4. The order of SNMP v2 parameters is: Discover IP, SNMP Version, Read-Only Community, RW Community. 5. The order of SNMP v3 parameters is: Discover IP, SNMP Version, Username, Mode, Auth Algorithm, Auth Password, Private Algorithm, Private Password. 6. Parameters can be set to the following values: • Security Level: authNoPriv, noAuthNoPriv, Auth. • Auth Protocol: MD5, SHA • Privacy Protocol: AES, DES. 7. The "Discovery IP" can be a single IP, an IP range, or a subnet. 8. Use "Start IP - End IP" to express the IP range. The starting IP expression cannot be greater than the ending IP expression. 9. Use "IP/subnet mask" to express a subnet. 10. The "Import CSV File" method only supports discovery of SNMP V1/V2/V3 devices. The acceptable "SNMP Version" values are "V1, v1, V2, v2, V3, v3". 11. The number of IP addresses defined in the CSV file must not exceed 5,000. 12. The file size must not exceed 1 MB. **Sample rules:** 192.168.1.10,v2,public,private 192.168.1.15-192.168.1.17,v2,public,private 192.168.2.0/24,v2,public,private 192.168.1.1,V3,user,noAuthNo-Priv 192.168.1.1-192.168.1.17,V3,user,AuthNoPriv,SHA,password 192.168.1.0/24,v3,user,authPriv,MD5,password,AES,password
Cancel	Click **Cancel** to return to the previous page.
OK	Click **OK** to add the new range.

4. Under the Discovery Range section, select an existing range and click the Credentials field.

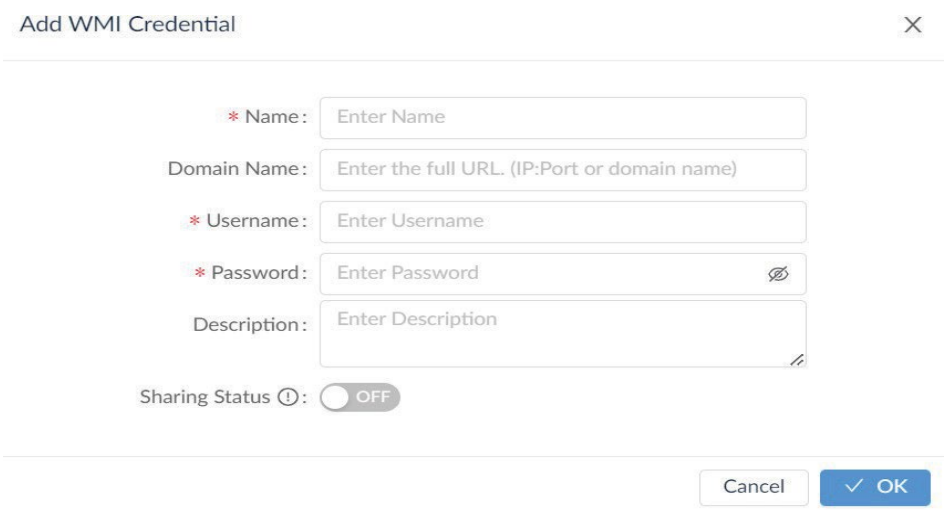
5. Click Add SNMP Credential or Add WMI Credential to define a new SNMP or WMI credential or select a pre-defined credential.



If Add SNMP Credential is selected, the **Add SNMP** Credential page displays.



If Add WMI Credential is selected, the **Add WMI Credential** page displays.

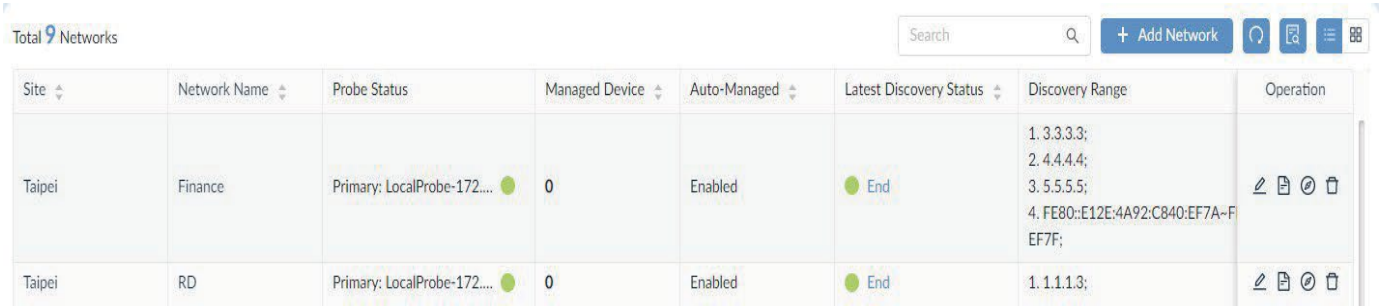


Note the added entry will be listed in the Credentials tab (go to **System > Basic Settings**).

Execute Network Discovery

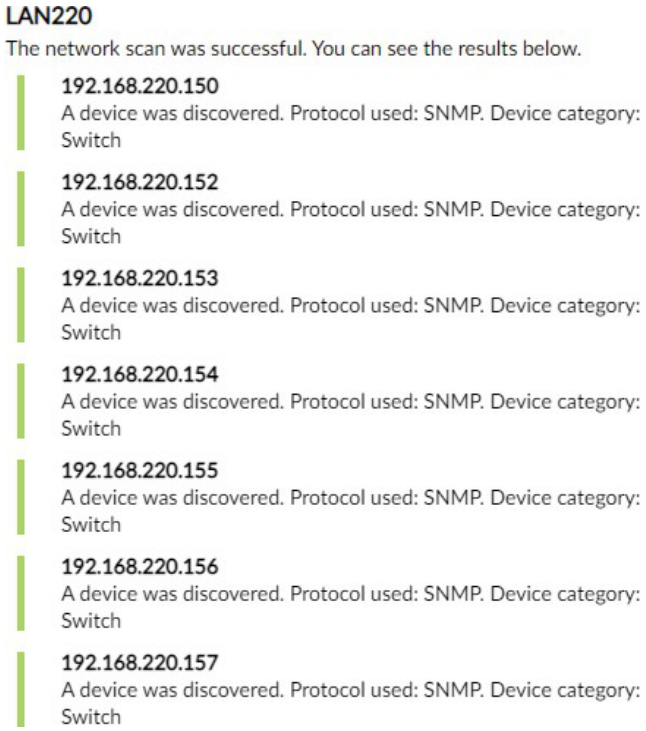
The NMS provides quick discovery of devices in a defined network.

To execute a discovery job:
Go to Monitoring > Network Discovery.
1. Select an existing network profile and click **Discover** to start detecting devices in the network.



The Latest Discovery Status field displays the discovery result.

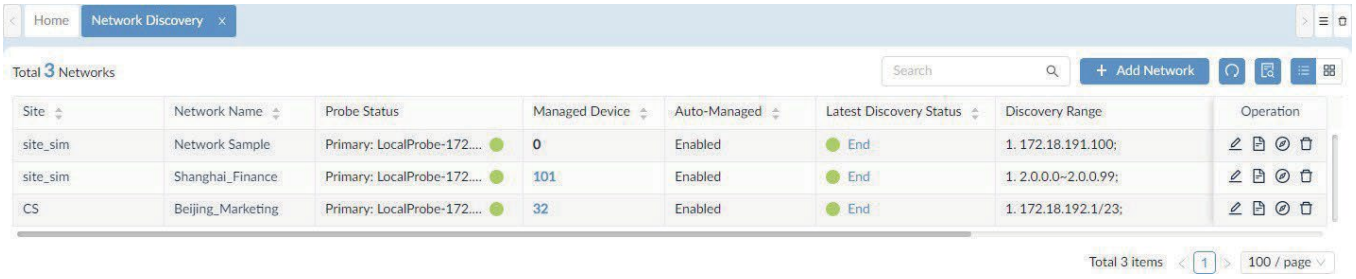
For example, it displays Running when the discovery is in progress
The Discovery Results page displays. The list of discovered devices will be shown.



Modify or Delete a Network Discovery Profile

If you delete a network discovery profile from the network list, the system deletes the profile along with the device information.

1. Go to Monitoring > Network Discovery. The Network Discovery information displays.



2. You can obtain more information about the network discovery profile by clicking **Network Information** It also provides detailed information about probes.

Select a network discovery profile and click **Delete** to delete the selected network or Edit to modify the network settings. A confirmation page displays for deletion; click OK to delete the profile or Cancel to return to the previous menu. To edit a discovered network, fill in the information on the Edit Network page. For detailed instructions, refer to the about Add Network
for Discovery.

Manage Wired Network Devices

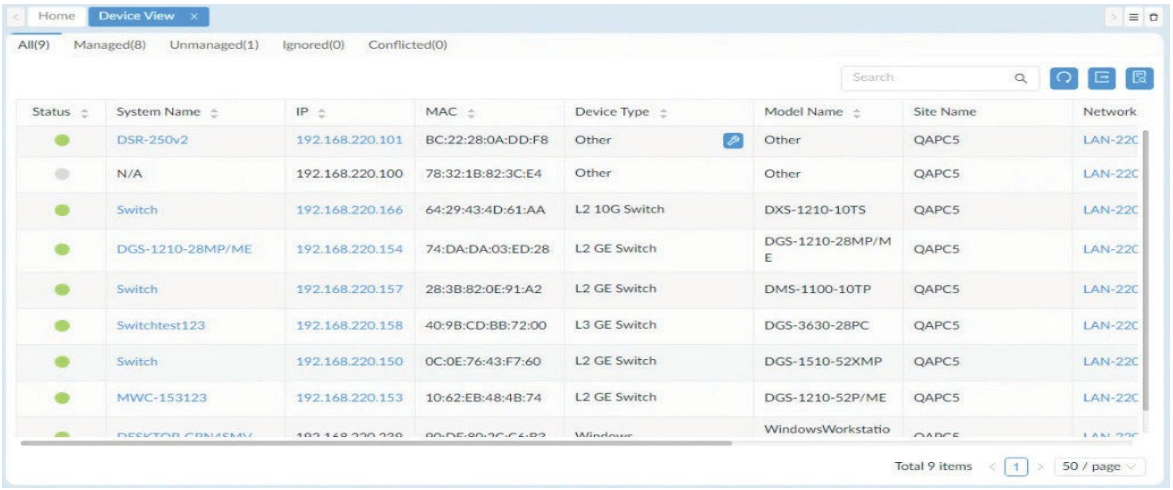
NMS is designed to help you manage your fleet of devices centrally. This section covers the following tasks that you can perform on devices:

- View Device Information
- Modify Device Information
- Ping or Reboot Device
- View and Export Interface List

View Device Information

The Device View shows devices, which are categorized by managed/unmanaged, ignored, and conflicted. The default view is All. For each device category, device information such as status, system name, IP, and MAC address is displayed. For more detailed information, click on the system name link to display the device's detail page.

1. Go to **Monitoring > Device View**. The Device View information page displays.



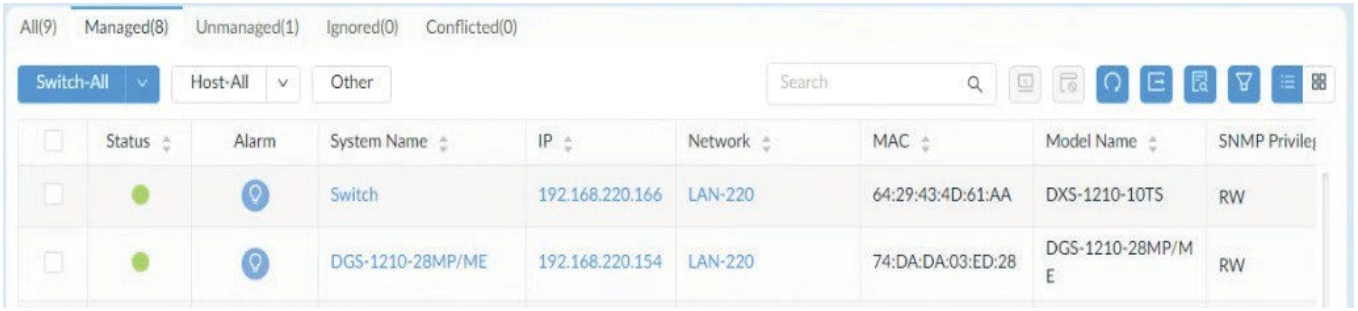
The following table describes the properties of the devices:

Item	Description
Management Type	All, Managed, Unmanaged, Ignored, and Conflicted. Managed: Displays all devices managed by the NMS server. Unmanaged: Displays all unmanaged devices. There are several reasons that a device is classified as Unmanaged: - Not being able to communicate with SNMP or WMI. - Lack of required system parameters such as SOID. - Exceeding the number of supported nodes. Ignored: Devices that are excluded from discovery. Conflicted: Devices that have an IP address conflict.
Status	Online (Green), Offline (Red), Unknown (Grey).
System Name	A unique name that identifies the device.
IP	The IP address of the device.
MAC	The MAC address of the device.
Device type	The type of the device, e.g., L2/L3 switch, access point, or workstation.
Model Name	The device's model name.
Site Name	The defined network site of the device.
Network	The defined network of the device.
Vendor	Displays the vendor's name of the device.
Discovered Time	Displays the latest discovered time of the device.

You can click on a column to sort the list by the column name; click it again to reverse the order. You can also configure the column headers with Column Selector  .

View Managed Device Information

Managed devices are devices that can be communicated with the NMS system and have the required SNMP parameters.
1. Go to **Monitoring > Device View**.
2. Select the **Managed** tab to view all the discovered devices that are managed by NMS. The drop-down menu at the top of the table allows you to refine the list with device type.



Item	Description
All	Displays all detected devices.
Managed	Displays all devices managed by the NMS server. Switch-All: click the drop-down menu to list All, sFlow, or PoE-capable switch devices. Host-All: click the drop-down menu to list All, Process, or Software-hosting devices. Other: click to list devices that do not belong to any of the above device categories.
Toolbar Function	
Search	Enter a keyword and select the matching property for search .
Unmanage	 Click to classify the selected device as unmanaged under the Managed category.
Manage	 Click to classify the selected device as managed under the Unmanaged category.
Ignore	 Click to classify the selected device as ignored. This device will be excluded from discovery. You can ignore a device under either Managed or Unmanaged category.
Refresh	 Click to refresh the list information.
Export	 Click to export the discovered device list to a CSV file. Up to 5000 entries can be included in a single export job.
Advanced query	 Select the criteria to filter the list.
Columns Selector	 Click to customize column headers. The available column properties vary depending on the device type. **Default:** Status, Alarm, System Name, Network, IP, MAC, Uptime, Vendor, CPU Utilization, Memory Utilization, Firmware Version, Hardware Version, Model Name, Temperature, Device Type, Serial Number, Discovered Time, SNMP Privilege. **Other:** Device Category, Site Name, PoE Status, sFlow Status, Stack Info, Current Activated License, Activated / Total Licenses, Port Count, Latest Discovered Time, Trap Status, DHCP Status, Total Flash, Syslog Status, Attached on Probe, SNTP / NTP Status, SSH Status, Spanning Tree, LLDP Status, LACP Status, RMON Status, Safeguard Engine Status, FDB MAC. Click **All** to select or deselect all the categories. Click **Apply** to save the selection.
View List	 Click to view the list either in a list format or a graphical representation.

To view the details of a device, click the device's **System Name** link.

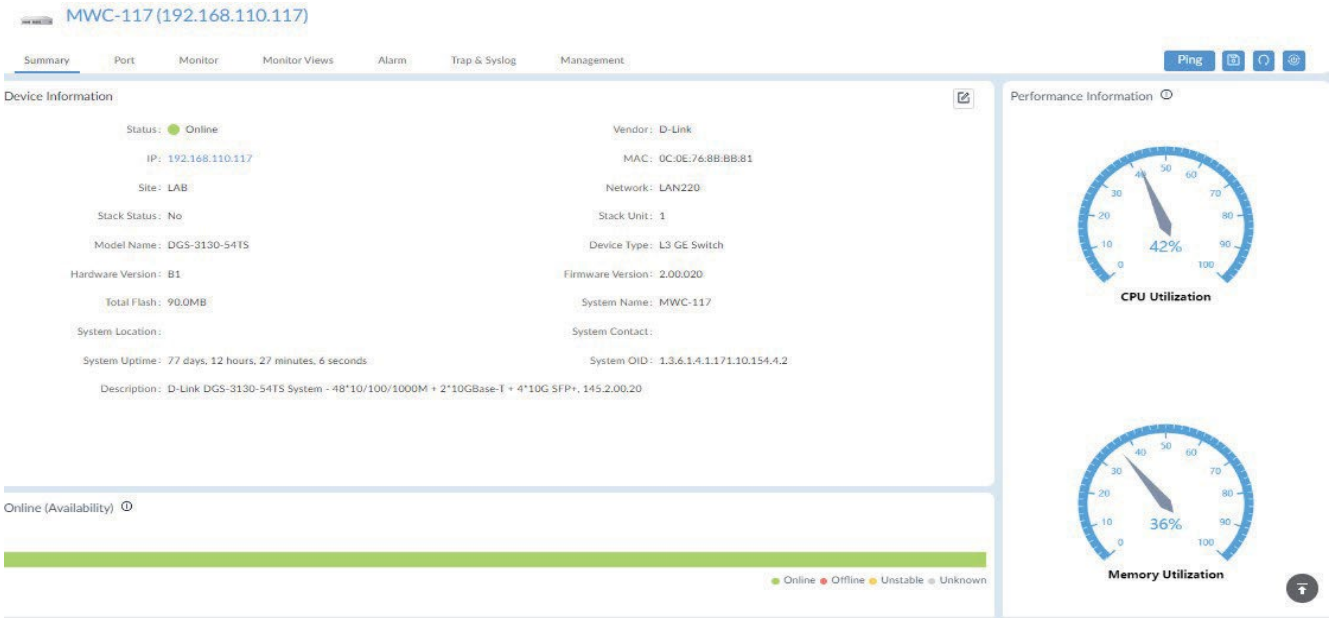
Modify Device Information

Device information can be modified for managed devices. You can modify device information such as system name, system location, system contact, and other properties depending on the device type.

To modify a device's information:

1. Log in to the Dashboard, see "0".
2. Click **Monitoring** and select **Device View.** The **Device View** information displays.
3. From the category menu select the **Managed tab**.
4. Select a device and click the **System Name**.

The device's detailed information page displays.



5. From the Device Summary page, click the edit button.
6. Click on a field to edit its property.
7. Click Save to update the device information.

Note: The device information also provides other tabs for additional information such as alarms and resource monitoring.

The following table describes the information available through the Device Information page.

Item	Description
Summary	
Device Information	Displays an overview of the device information. You can click **Edit** to modify the following: System Name, System Location, and System Contact. If a switch supports stacking and it has been enabled and configured as the Primary Master, the stack status can be obtained by hovering over the "view" button. The information for the stacked units includes the unit ID, model name, stack priority, and MAC address as well as firmware version (note that switches assigned with stacking roles as Slave and Backup Master will display Offline status). The Port and Monitor tab will incorporate the information on all the stacked units (refer to the below Port and Monitor status description). Click **Save** to accept the updates or **Cancel** to continue without saving.
Performance Information	Displays charts for the device's CPU and memory usage.
Online (Availability)	Displays the online status of the equipment in the past 24 hours.
SNMP Protocol Credentials	Set the SNMP settings for the device. Refer to Set Up SNMP Credentials in. Click Reset to discard any setting updates. Click Test to test the settings to verify if they are correct. Click Save to accept the settings.
SSH/Telnet Credentials	Enter security settings for SSH or Telnet connection. Refer to Set Up SNMP Credentials in.
Additional Information	Click Edit Additional Information to include further device details: Purchase Date, Keeper, Warranty Expiration, Service Vendor, Service Contact, and Description.
LACP Working Status	Provides Link Aggregation Control Protocol (LACP) data if LACP is enabled.
Hardware Health	Provides a tabular view of the operational status of the device's fan, power supply, and temperature.
Port	Click to display the Port List overview page. The following information categories are available: Monitor, Comparison, and Alarm Settings. The Monitor and Alarm settings can be set on a per-port basis. You can enable or disable the monitoring status and configure alarm settings using the on/off switch. Or you can go to the **Alarm & Notification > Monitor & Alarm Settings** and select the **Wired Traffic** category on the Monitor Settings tab and the **Alarm Settings** tab. The **Monitor Settings** can be used to select the ports to be monitored whereas the Alarm Settings allows you to set alarm rules based on Rx/Tx traffic, error rate, discard rate and bandwidth utilization. The **Admin Status** switch allows you to enable or disable each port. If a switch supports stacking and it has been enabled and configured as the Primary Master, the ports of the stacked units will be displayed. Hover the button to display the information on the selected port, including the unit Rx/Tx rate, port type, bandwidth, and PoE information. **Note:** The connectivity information of the device is only available for managed devices which can send SNMP data to the NMS server with a unique and identifiable SOID.
Monitor	Click to view a graphical presentation of the CPU and memory utilization, response time, etc. The information can be shown by Hour, Day, Week, Month, or Quarter (3 months retention period). **Monitoring Settings:** click to enable/disable a specific measurement to monitor. The following categories are available: 802.1Q VLAN, Base Info, CPU Utilization, Device Common Information, DHCP Server Status, HTTP Status, LACP, LLDP, Memory Utilization, Power Status, Private Port, RMON Status, Response Time, SNTP Status, SSH Status, STP Status, Temperature, Syslog Status, Telnet Status, Trap Status, Safeguard Status, Syslog Status, and sFlow Profile. Note that the available monitor categories depend on the device's capability. Go to **Alarm & Notification > Monitor & Alarm Settings** for monitoring status control. Once you have added a customized monitoring function to the device, a **Customized Monitor** tab will appear next to the default System Monitor tab. If a switch supports stacking and it has been enabled and configured as the Primary Master, the ports of the stacked units will be displayed. Hover the button to display the information on the selected port, including the unit Rx/Tx rate, port type, bandwidth, and PoE information.

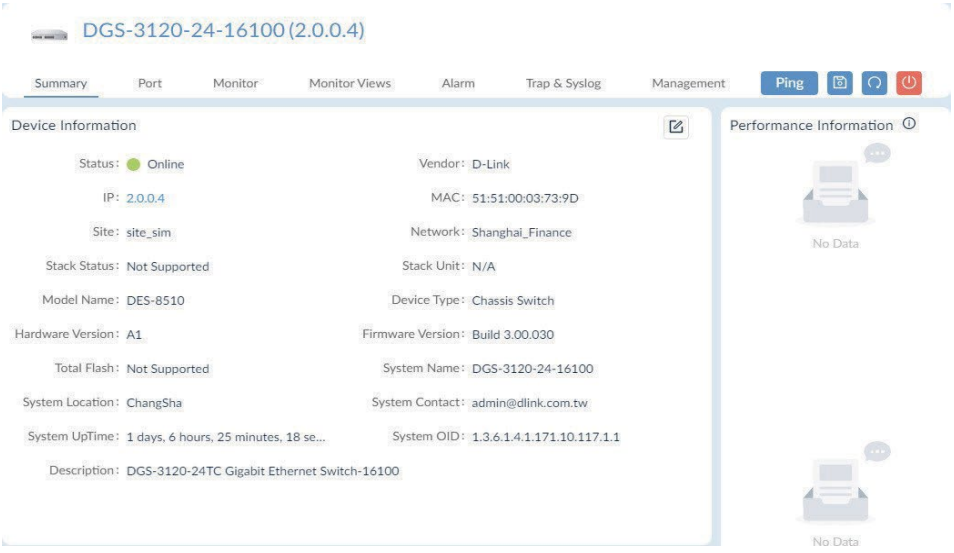
Item	Description
Monitor Views	Click to view monitoring information in a topological format: Rack View and System as well as Customized topology. Click the topology name link or go to Monitoring > Topology Map to access the topology map view. (Refer to View and Manage Network Topology for more information.)
Alarm	Click to view the active or historical (either automatically resolved by automatic script or manually resolved with admin acknowledgement) alarm events. Click Alarm Settings to turn on or off specific alarm rule listed by monitor category as in **Alarm & Notification > Monitor & Alarm Settings > Alarm Settings**. The **Trap** and **Syslog** tabs list alarms configured under the Trap and Syslog category.
Trap & Syslog	Click to view the trap messages and system logs. Go to **Alarm & Notification > Trap & Syslog** to access the Trap & Syslog page to view all trap events and system logs. (Refer to View Traps and Syslog for more information.)
Management	Click to view and configure device service settings and manage firmware and configuration files. It also provides links to **Task Management** in **Configuration**. Note that the available configuration categories depend on the device's supported features. To view all supported configuration features, click the **More Settings tab**. (Go to **Configuration > Batch Configuration > Quick Configuration** and **Advanced Configuration** to view available settings for both **Quick Configuration** and **Advanced Configuration** categories.) You can also create tasks to be executed immediately by clicking "+ **Create Task**" from this menu (refer to Create Tasks for Batch Configuration).
PoE	If a switch supports PoE and the PoE monitoring has been enabled, the PoE utilization status will be displayed. The PoE Power Supply Summary displays the total power supply in the defined timespan: Hour, Day, Week, Month, and Quarter. You can view the PoE supply status by port and configure PoE schedules if the device supports time-based PoE. The schedules can last for a specific period and can
Ping	Click Ping at the upper right to display the ICMP ping menu.
Save	Click Save to Device at the upper right to save the updated settings to the device.
Refresh	Click Refresh from Device at the upper right to synchronize the device and panel information.
Reboot	Click Reboot at the upper right to reboot the device.

Ping or Reboot Device

You can ping or reboot a network device. The device must be online to perform these tasks.

1. Go to **Monitoring > Device View**. The **Device View** information displays.

2. Select a device from the list and click its **System Name**. The **Device Information** page displays.



3. From the toolbar at the top right, perform one of the following actions:

- Ping the device: click Ping to initiate a ping command on the device. For ping, you can specify the supported parameters such as the number of times and packet size to send the ping request.
- Save to Devices: Click to save the updated information to the device.
- Refresh the information: click Refresh to update the information with the device.
- Reboot the device: click Reboot to restart the device.

View and Export an Interface List

View and Export an Interface List

You can view the interfaces (or ports) of device(s) managed by the application and export the table to a tabular formatted (.csv) file. The export list only lists the information on managed devices.

1. Go to **Monitoring > Interface View**. The Interface View information page displays.

The following device interface information is displayed:

Item	**Description**
System Name	The link redirects to the Device Information page.
Model Name	Device model name
IP	Device IP address
Network	The network of the device
Interface Index	The number of the port of the device.
Interface Name	The name of the port of the device.
Interface MAC	The MAC address of the port.
Connected MAC	The MAC address of connected port of the other device.
Connected Interface Name	The Interface Name of the connected port of the other device.
VLAN ID	The VLAN ID to which the port belongs.
VLAN Name	The VLAN name to which the port belongs.
VLAN Type	The configured VLAN type of the port.
VLAN Port Status	The status of the VLAN port: tagged or untagged.
Update Time	The last time that the information synced with the device.

2. Click **Export** to start the export job. The exported file will be saved in the default download folder of your browser.

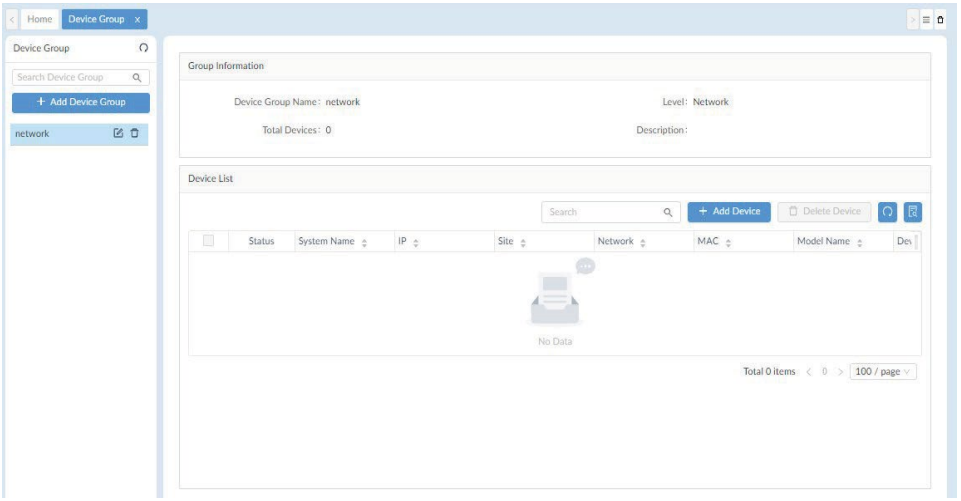
Manage Device Groups

Device groups are designed to simplify the organization of the network devices. It can be used for applying target devices in Batch Configuration and Firmware Management. Once a device is discovered, it can be added to a group. Groups can be created across sites or networks within an organization. After a device group is created, you can perform maintenance operations such as firmware upgrade on the devices of the group.

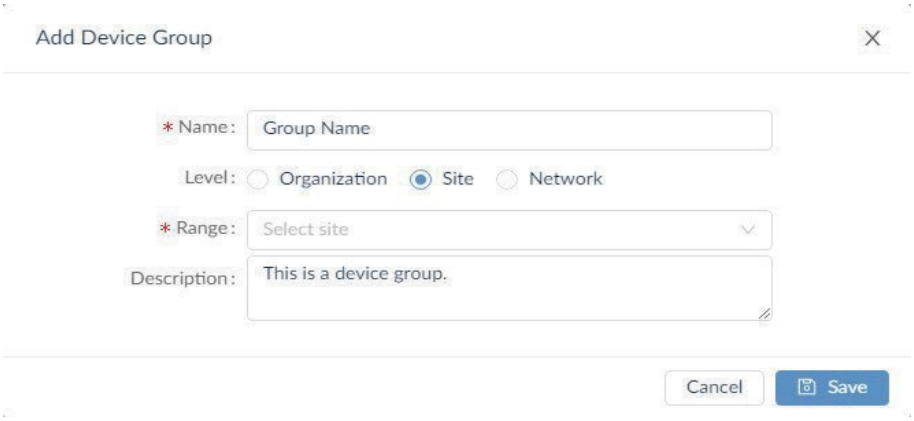
Add a Device Group

To add a device group:

1. Go to Monitoring > Device Group to open the device group page.



2. Click +Add Device Group from the left list pane.



The Add Device Group page displays.

Enter the group information:

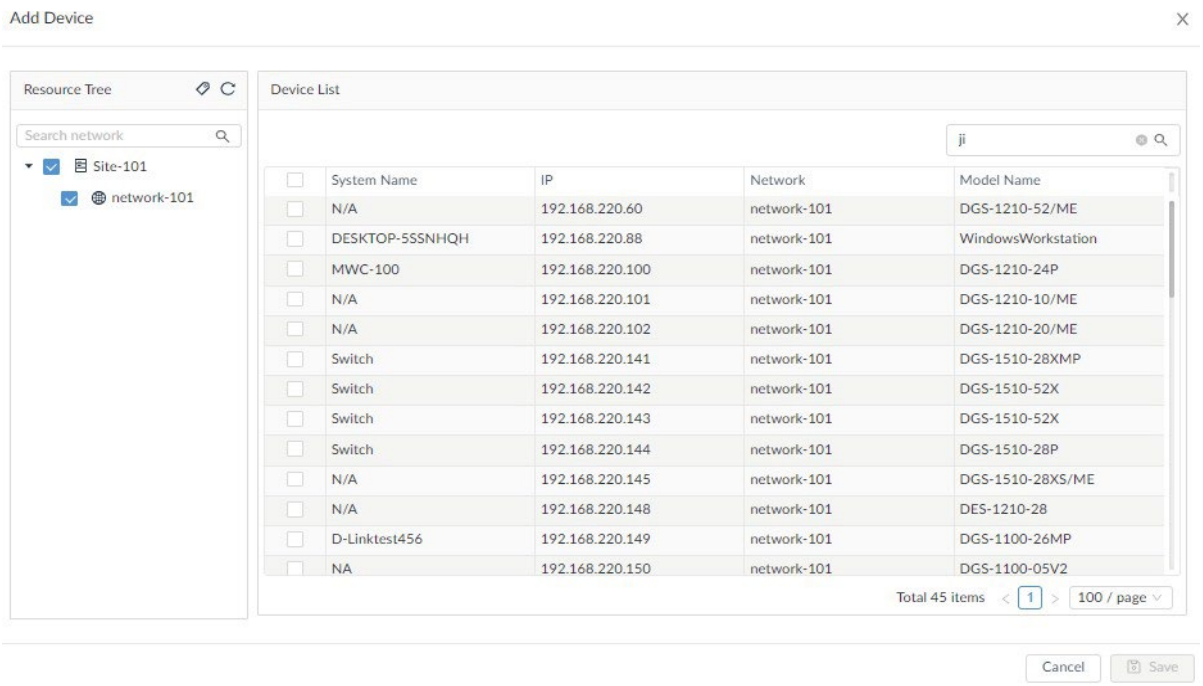
Item	Description
Name	Enter a name for the group.
Level	Click to select the group level (default: Organization). **Organization:** Select an organization to add all discovered devices in the organization. **Site:** Click the Range drop-down menu to select a site to add devices in the designated site. **Network:** Click the Range drop-down menu to select a network to add devices to the designated network.
Description	Enter a short description for easy identification.

3. Click **Save** to create the group.

The **Group Information** page will be shown on the right side.

4. Click + **Add Device**. The Add Device page displays. From the Resource Tree pane, select the site and network to find the desired devices.

5. From the entries in the Device List, select a device to be included in the selected group. Or enter an IP address or a model name to find the desired devices.

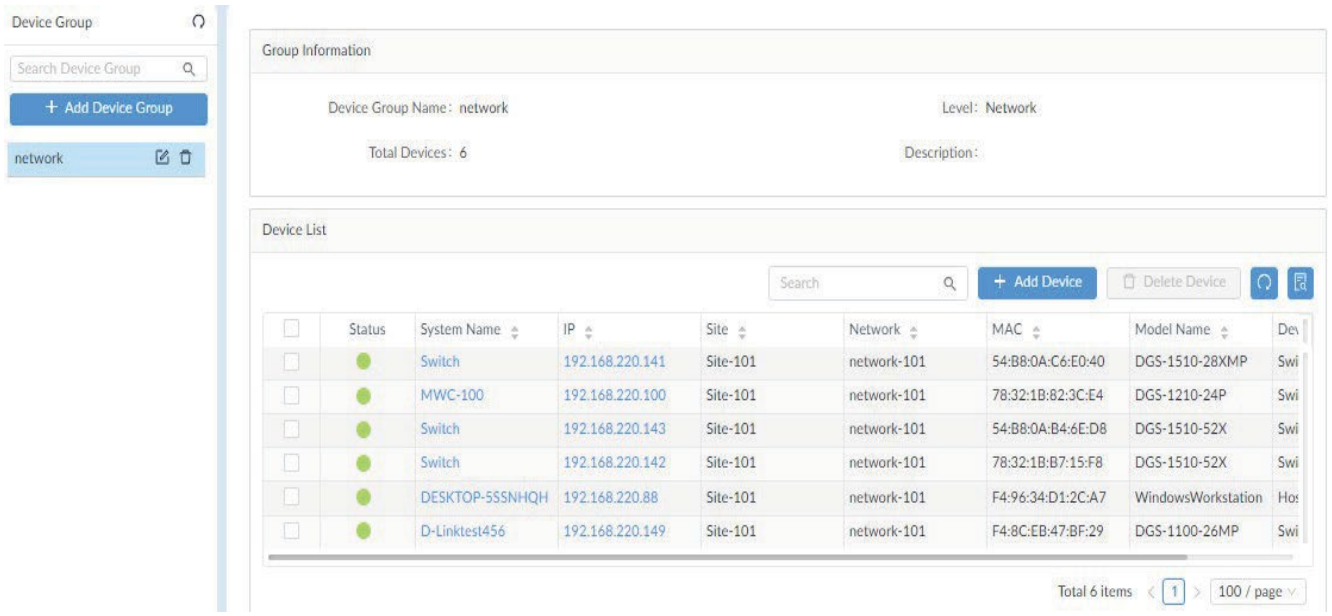


6. Click Save to add the devices to the group.

Edit or Remove a Device Group

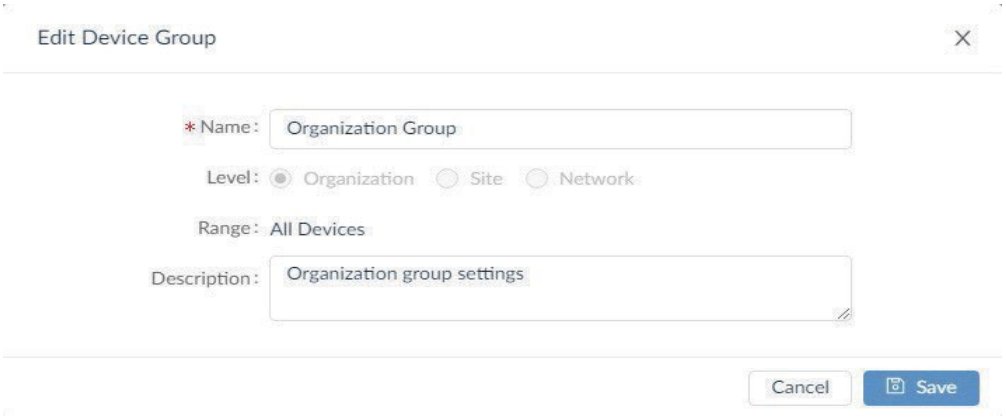
1. Go to **Monitoring > Device Group**.

2. The Device Group page displays.



3. Select an existing device group and perform the following:

- **Edit:** click to edit the device group name and description.
- **Delete:** click to remove the device group.



Remove a Device from a Group

1. Go to **Monitoring > Device Group**. The **Device Group** page displays.
2. Select a Group from the Device Group pane.

The Device List page displays the devices in the group.

3. Select a device and click **Delete Device** to remove it.
4. A confirmation message appears. Click **Yes** to remove the device from the group or **No** to cancel the deletion.

SNMP Configuration

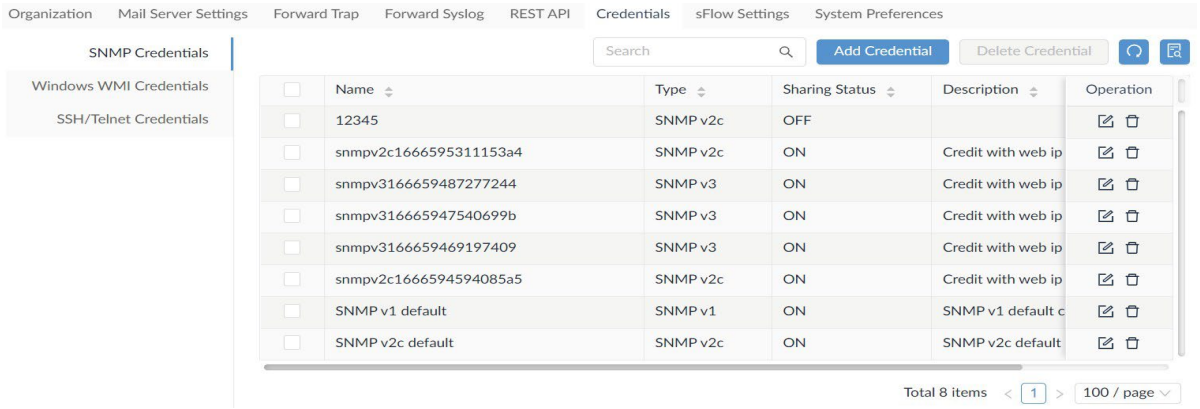
Network discovery and the device information is accomplished via Simple Network Management Protocol (SNMP). It allows X- SWITCH application to monitor certain parameters of the devices. In addition, an alarm can be triggered when certain types of traps are sent from devices.

Configure SNMP Credentials

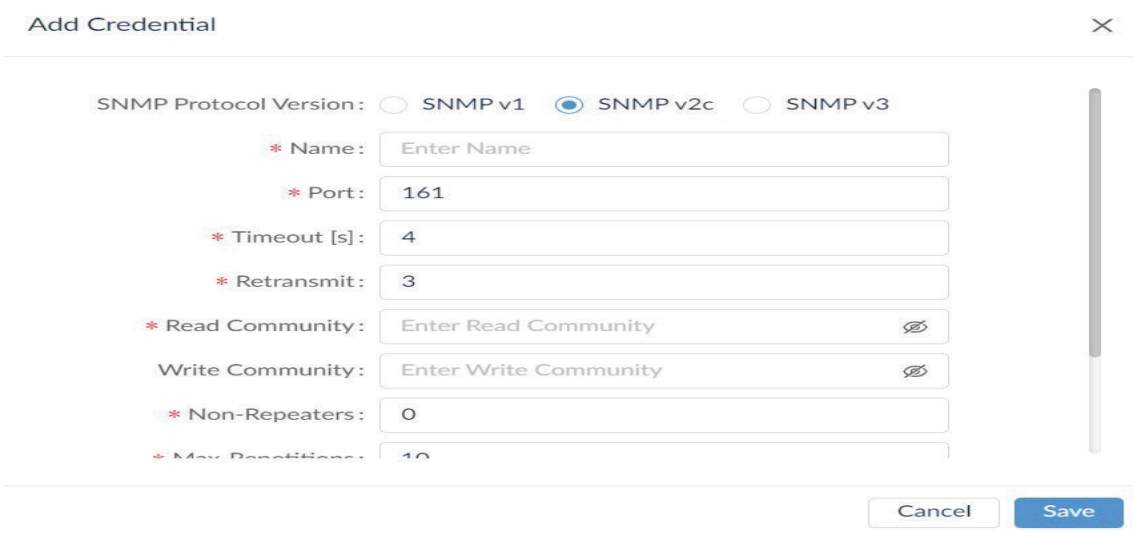
Devices can be polled individually for network discovery and monitoring. The required SNMP settings should be configured in SNMP credentials list.

To access the configuration page:
Go to System > Basic Settings > Credentials.

1. The SNMP Credentials page displays:



2. Click **Add Credential** to add SNMP credentials for devices within the network:



Test SNMP

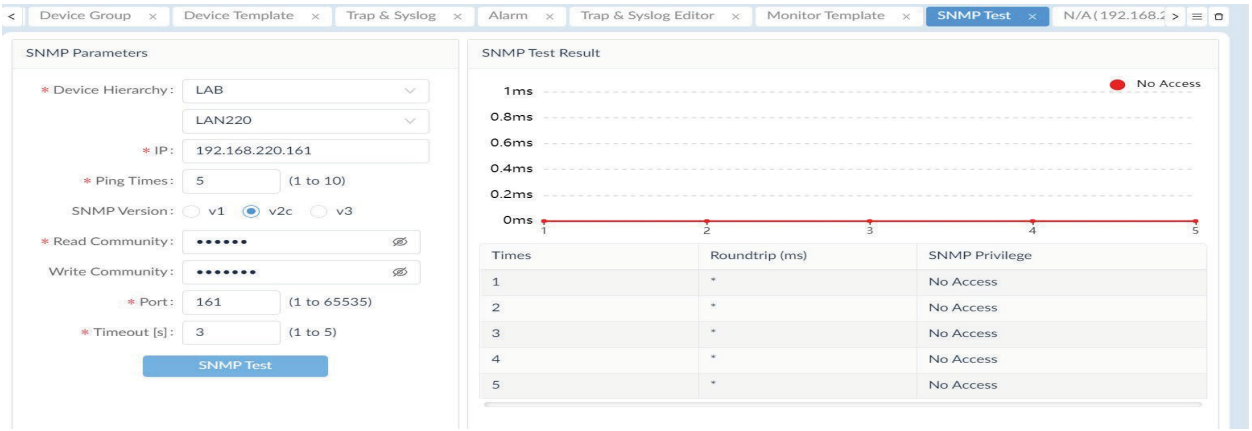
SNMP functionality can be tested on various platforms using compatible tools. The NMS provides a convenient SNMP tool to test SNMP access to SNMP agents.

To use this tool:

1. Go to **Tools > SNMP Test**.

2. Enter the SNMP Parameters in the left pane to access the device agent. The verified SNMP parameters can be maintained in the above Credentials list.

3. The test result should be displayed on the right pane.



View Traps and Generate Alarms for Traps

Traps can be viewed from the NMS application and forwarded from the NMS server to a configured destination. Alerts can also be triggered when a specific trap has been sent.

To enable traps on a device:

1. Go to **Monitoring > Device View**.
2. Select a device to open the **Device Information** page. Then click the **Management** tab and enable **Trap** Status to set the trap server.
3. You can then obtain trap information on the Trap& Syslog tab of the Device Information page or by going to **Alarm & Notification > Trap & Syslog.**

To manage traps:

1. Go to **Alarm & Notification > Trap & Syslog** to view all trap events.
2. You can also define a trap OID by adding an OID description in the Trap & Syslog Editor menu below.

Refer to **View Traps** and **Syslog** and **Trap Editor.**

To set an alarm with a specific trap:

1. Go to **Alarm & Notification > Monitor & Alarm Settings.** Then click the **Alarm Settings** tab.

Scroll down to the Trap section for traps that are available for triggering an alarm. Then click Add to add an alarm rule to define a trigger condition with the specified trap OID or binding values for a variable.
For detailed instructions, refer to Alarm Settings.

To forward traps:
1. Go to **System > Basic Settings**. Then click the Forward Trap tab.
2. Click **Add Destination Host** to add a destination to send the traps.

Manage Networks with Batch Configuration

The NMS allows for batch configuration of devices across networks using a pre-configured schedule. To start with, a configuration template must be selected. There are system-built templates. The templates are designed to cater for two different configuration types – quick configuration for a single configuration category or advanced configuration for multiple configuration categories when setting batch configuration.

Batch Configuration

To apply batch configuration to devices:

Go to Configuration > Batch Configuration.

1. Select either **Quick Configuration** or **Advanced Configuration** tab according to the type of the configuration template.

For Advanced Configuration, click **Add Profile** at the top right.

1. Enter a name and description for the profile, select the device model in the **Device Hierarchy** field, then select configuration categories for the device model in the **Configuration Feature List**. Note that you can select multiple categories for a profile.

2. Click **Next** to continue configuring configuration items of selected categories.

3. Click **Save** to create the configuration profile.

For **Quick Configuration,** select a configuration category in the left pane. Then create a task to apply the configuration changes (see below Create Tasks for Batch Configuration).

For more detailed instructions, refer to Create Configuration and Profiles.

Create Tasks for Batch Configuration

For Quick Configuration, select a configuration category in the left pane, then enter the following information:

Task Information	
Task Name	Enter the name for the task.
Task Description	Enter a brief description to identify the task.
Configuration Information	
Status/Input	Apply the configuration changes for the task. For custom category, the options depend on the design of the template and selected protocol.
Target Devices	
Add Devices	Click to add the device(s) for configuration. Note that only devices that support this function can be selected. For custom configuration categories, you need to associate the configuration template to the device template first (go to Templates > Device Template).
Schedule Information	
Schedule Type	• **One Time:** Select this option to specify a date and time or immediately to initiate the task. • **Recurrent:** Select this option to specify the frequency and effective time frame to initiate the task. Refer to Scheduling for more information.

Click Add Task at the upper right to save the task.

You can click **Task Management**  to open the **Task Management page**.

For Advanced Configuration, select a profile in the list, then click **Create Task** + under **Operation**.

Enter the following information:

Task Information	
Task Name	Enter a name for the task.
Task Description	Enter a brief description to identify the task.
Target Devices	
Add Devices	Click to add the device(s) for configuration. The Batch Select Devices screen opens. Select the desired devices or use the Search function to find devices.
Schedule Information	
Schedule Type	• **One Time:** Select this option to specify a date and time or immediately to initiate the task. • **Recurrent:** Select this option to specify the frequency and effective time frame to initiate the task. Refer to Scheduling for more information.

Click **Save** to create the new task and return to the previous menu.
You can click **Task Management** to open the **Task Management** page. Refer to Current Tasks for details about tasks.

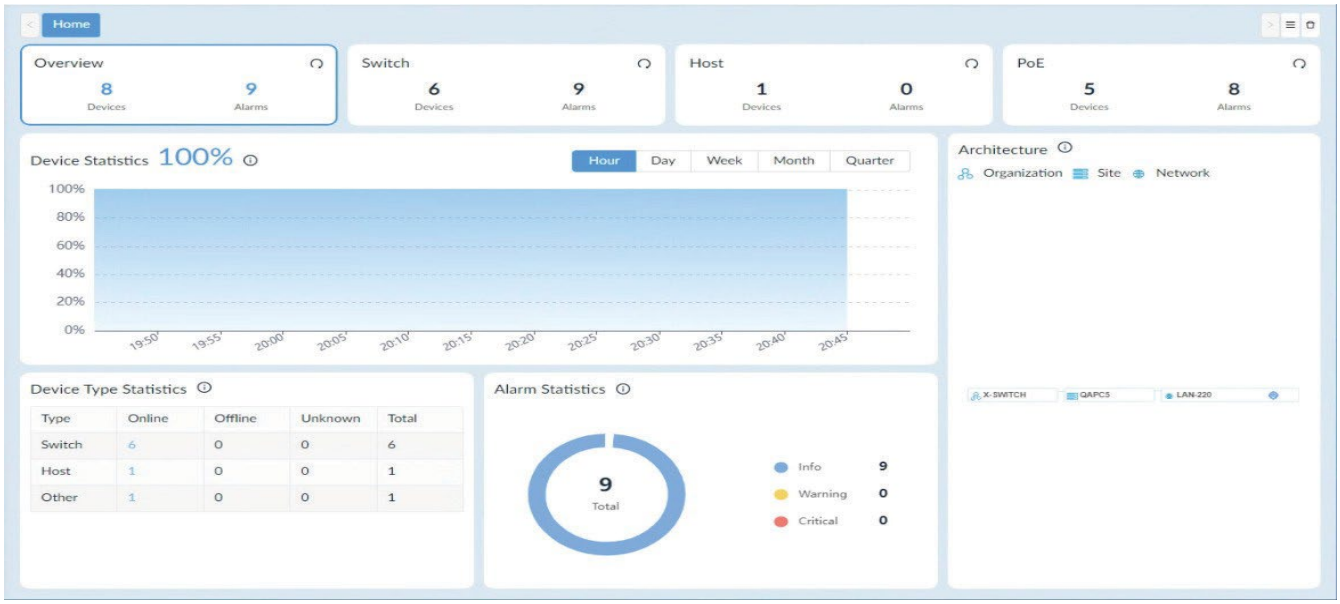
Monitoring and Reporting

You can monitor your network through the Dashboard to obtain real-time statistics.

View the Default Dashboard

The default dashboard provides information related to the distribution and management of the resources in the managed networks. The information can be used to assess, utilize, and centrally manage your networks.

To view the Overview dashboard, go to **Dashboard > Analysis**. The Overview dashboard will be displayed.



By default, the overview displays the following widgets. To refresh data, click Refresh at the upper right.

Widget	Description
Device Statistics	The percentage of managed devices that are online.
Architecture	The NMS network architecture diagram.
Device Type Statistics	The operating status of different types of managed devices.
Alarm Statistics	The distribution of alarm severity for managed devices.

You can click on any number or icon on the charts or graphs to be directed to the configuration page.

Switch Dashboard

From the Dashboard, click the Switch tab. The Switch Dashboard displays the following widgets. To refresh data, click **Refresh** at the upper right.

Widget	Description
Alarm Statistics	The distribution of alarm severity for managed switches.
Running Status	The online status of managed switches.
Temperature Statistics	The distribution of managed switches based on the specified temperature range: 40, 60, 80, or 90 ℃.
Top 10 Wired Throughput (Rx / Tx)	The top 10 managed switches that currently send and receive the most traffic.
Top 10 Memory Utilization	The top 10 managed switches with the highest current memory utilization.
Top 10 CPU Utilization	The top 10 managed switches with the highest CPU utilization.
Top 10 Response Times	The top 10 managed switches with the longest response time according to a specified time frame: current, last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.

Host Dashboard

From the Dashboard, click the Host tab. The Host Dashboard displays the following widgets. To refresh data, click **Refresh** at the upper right.

Widget	Description
Alarm Statistics	The distribution of alarm severity for all hosts.
Running Status	The online status of host devices.
Top 10 CPU Utilization	Display the top 10 hosts with the highest CPU utilization.
Top 10 Memory Utilization	Displays the top 10 hosts with the highest memory utilization in the specified time frame: current, last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.
Top 10 Most Installed Applications	Display the top 10 most installed applications on the hosts in the network.
Top 10 Volumes with Most Disk Usage	Display the top 10 volumes with the most disk usage in the network.
Top 10 Response Times	Display the top 10 hosts with the longest response time in the specified time frame: current, last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.
Top 10 Volumes with Least Disk Usage	Display the top 10 volumes with the least disk usage in the network.

PoE Dashboard

From the Dashboard, click the PoE details panel. The PoE panel displays the following widgets. To refresh data, click Refresh at the upper right.

Widget	Description
Alarm Statistics	The distribution of alarm severity of the managed PoE devices.
Running Status	online status of the managed PSE devices.
Top 10 PSEs by Current PD Count	The top 10 PSE devices with respect to the number of powered devices.
Top 10 Ports by Current Flow	The top 10 PoE device ports with the highest data flow.
Top 10 Ports by Power Output	The top 10 PoE ports with the highest power consumption.
Top 10 PSEs by Power Output	The top 10 PSE devices with the highest power output.
Top 10 Response Times	The top 10 PoE devices with the longest response time in the specified time frame: current, last hour, last 24 hours, last 7 days, last 30 days, or last 90 days.

View and Export Reports

The system provides a method to view information regarding the performance and resource utilization on the network.

The following reports are available:
• General Reports
• Scheduled Reports

The period for statistics generation is based on the scheduled retention period. To view and export reports:
1. Go to **Reports > General Reports**.
2. Select the report type from the General Reports pane.

Report Category	Category	Event
General Reports	Device Reports	Device Health Reports
		Trap Reports
		Syslog Reports
		Device Top N Reports
	Wired Interface Reports	Wired Traffic Reports
		Wired Throughput Top N Reports
	Advanced Reports	Inventory Reports
Scheduled Reports	One Time	
	Recurrent	

3. From Reports, click General Reports. The default Device Health Reports page displays.

You will need to configure the settings if a report does not display any data. Refer to the below section for more information.

4. Click the **Export** drop-down menu at the top right and select the type of file format for download: PDF, Excel, or CSV. The report file is downloaded to the default download folder of your browser.

View Report Settings

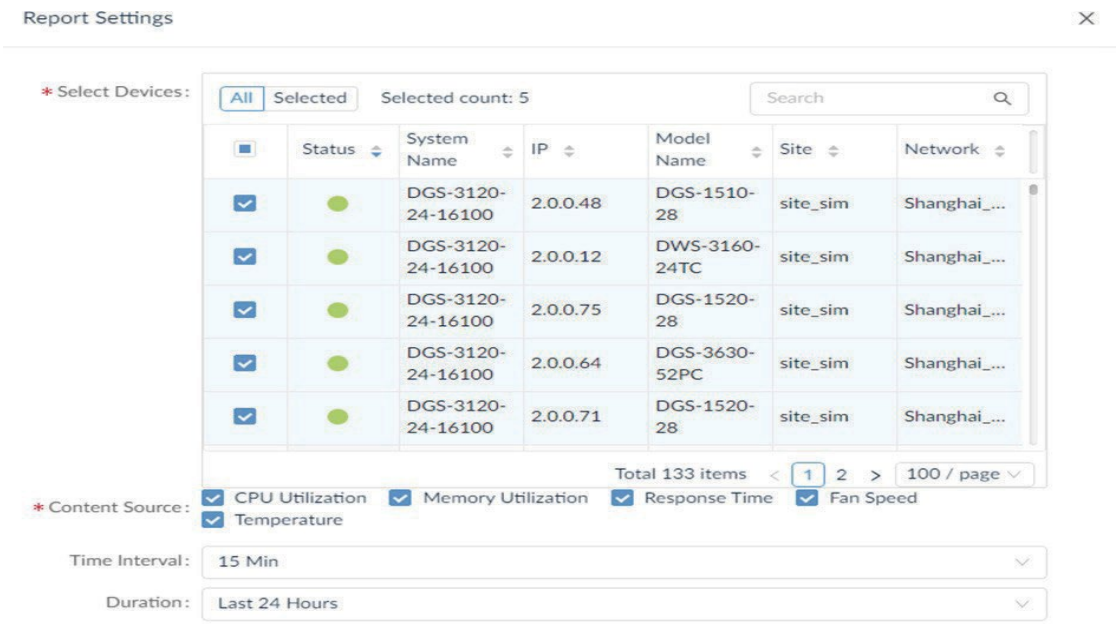
1. From Reports, click General Reports.

The default Device Health Reports page displays.

The toolbar displays available functions:

Item	Description
Show All	Display all information.
Show Chart Only	Display available information in chart format.
Show Table Only	Display available information in tabular format.
Upgrade to Scheduled Reports	Designate the current report as Scheduled Report.
Refresh	Re-synchronize the report information.
Export	Save the information to a file.
Report Settings	Configure the settings for the current report type.

1. Click Report Settings . The Report Settings page displays.



Available report setting options:

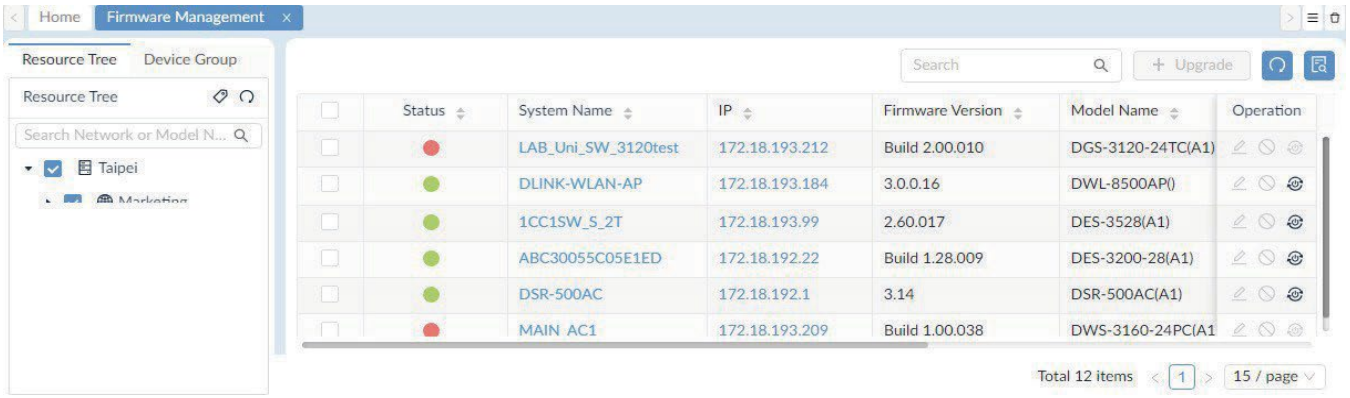
Item	**Description**
Select Devices	Click the slide bar to view All or only the Selected devices. To select a device, click a specific device.
Search	Enter a keyword to search for a device by System Name, IP, Model Name, Site, or Network.
Content Source	Click the report type: CPU Utilization, Memory Utilization, Response Time, Fan Speed, or Temperature.
Time Interval	Click to set the interval time to define the display interval for the report: Configured minimum interval, 15 min., 2 Hour, 8 Hour, 1 Day.
Duration	Click to select the duration for each report: Last 24 Hours, Today, Yesterday, Customized. If you select Customized, enter the Start and End Time.
Reset	Click to reset the report settings to the default settings.
Save	Click Save to create the report.
Note: The report settings vary depending on the report type.	

View Firmware Version

You can view the firmware version for all discovered D-Link devices.

To view the firmware version:

1. Go to **Configuration > Firmware Management**.
The Firmware Management page displays.



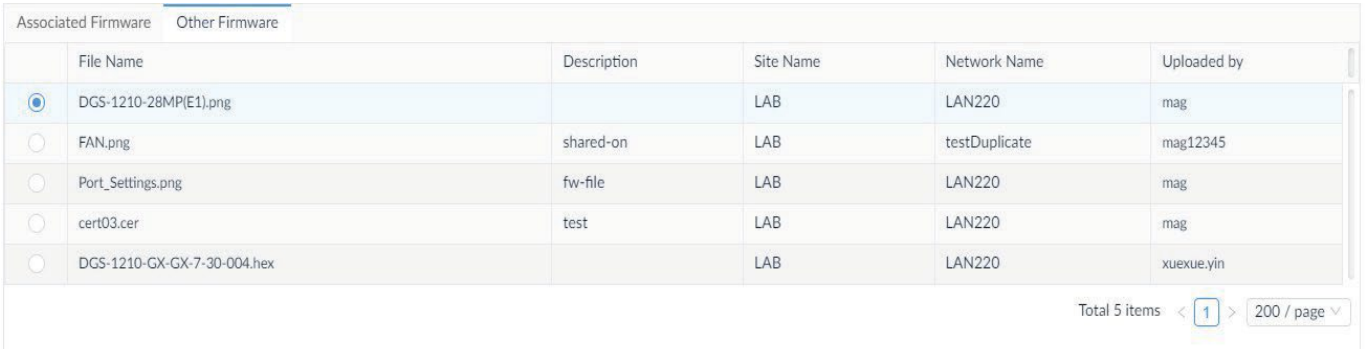
To upgrade firmware for devices”
2. Select devices for firmware upgrade.

NOTE: If multiple devices are selected, make sure that correct firmware is selected for update for each model.

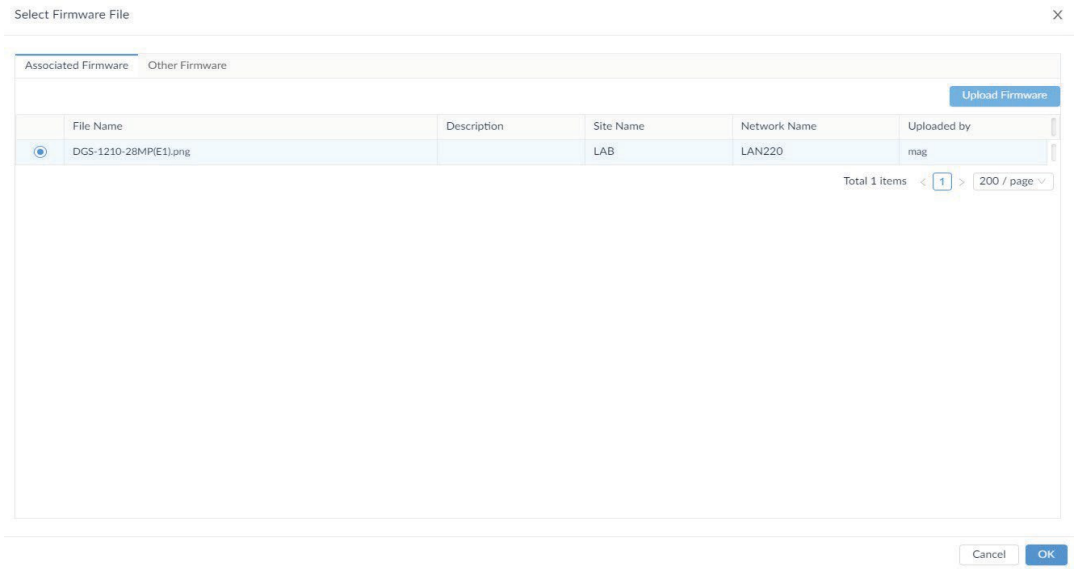
3. Click Upgrade to display Firmware Upgrade page.
4. Under Firmware File, click Select Firmware File to view available firmware sources.

NOTE: Make sure that you confirm the firmware version and its compatibility with the device before proceeding.

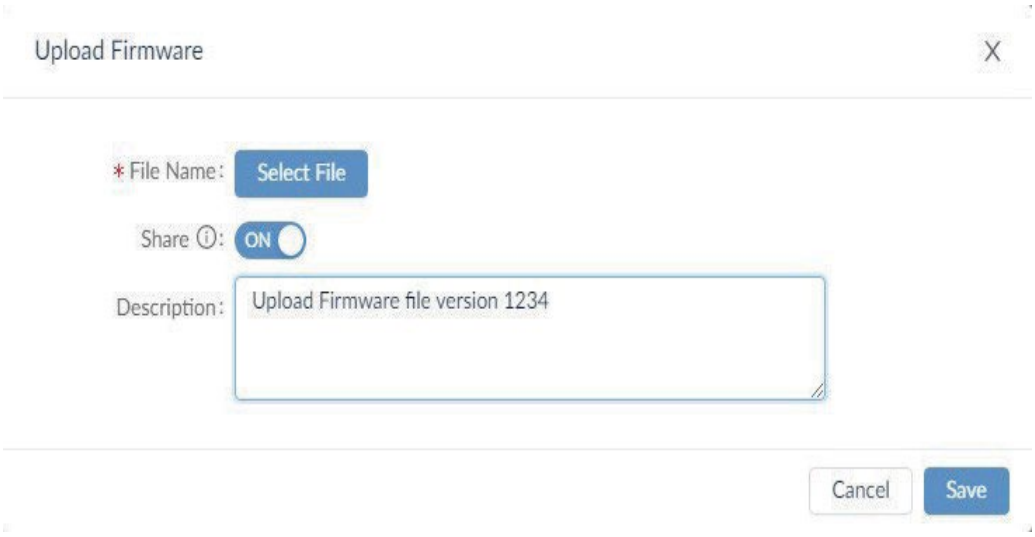
5. On the **Other Firmware** tab, select the appropriate file and click **OK** to continue. These firmware files have been uploaded to the NMS server.



6. Alternatively, select the Associate Firmware tab to view firmware that was uploaded specifically for this device model or to upload firmware from a local directory, then click Upload Firmware.



7. The Upload Firmware page appears. The Share slide bar can be used to enable or disable sharing this firmware file with other networks besides the device's current network. After selecting the firmware, click Save to upload the file selection or Cancel to delete the upload.



8. From the Firmware Upgrade page, set the Schedule under Schedule Information:

- Schedule Type: One Time
- Execution Time:
  - Immediately: start the firmware updating once the upload file is saved.
  - Specify a Date: click the **Date** drop-down menu to select a date and time.

Click **OK** to set the date.

9. From Reboot Type, click **Reboot by NMS** to enable a restart of the device through the NMS application. By de- fault, the Reboot by NMS option is disabled. A reboot is generally required for the new firmware to take effect.

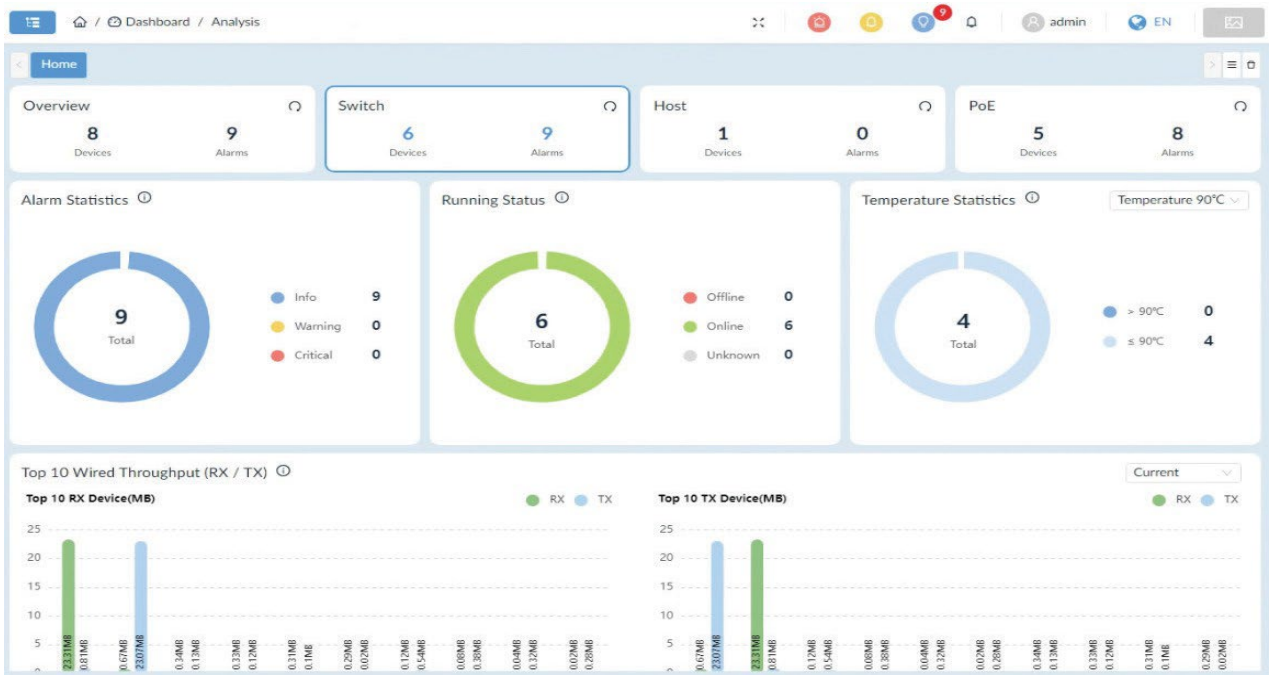
10. Click **Save** to confirm the new upgrade job. Click **Cancel** to return to the previous menu.

View NMS Notifications

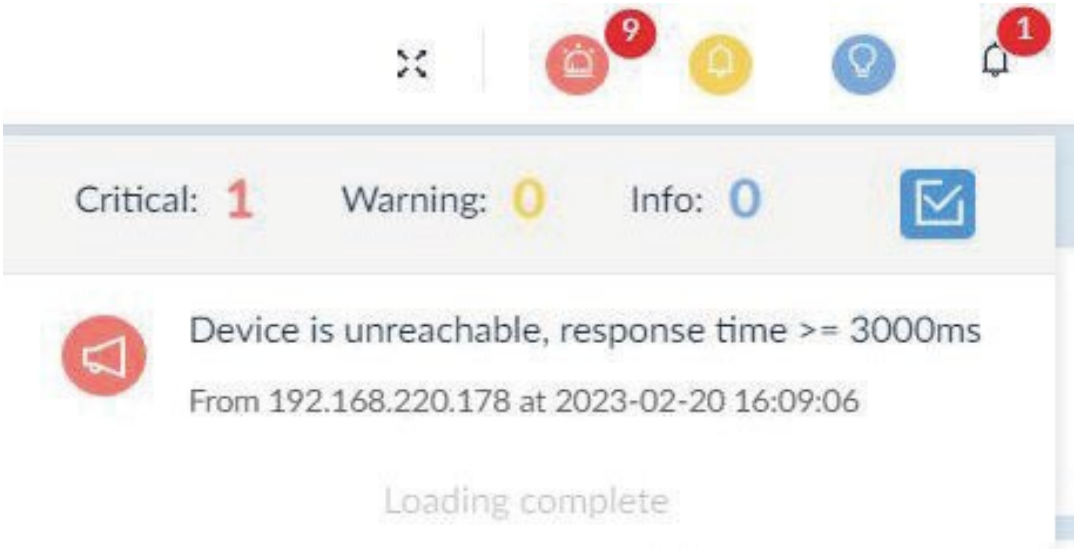
NMS provides notifications via the NMS web application. You can configure the notification rules for events that required immediate attention. For more information, refer to Configure the Notification Center.

To view notifications:

1. Go to the Dashboard, see the session of Launching NMS Web GUI".



2. On the right side of the toolbar, click the Notification icon .The Notification message page displays.



To clear the list, click . (Note that no historical records will be kept.). Click on a notification entry to open the Alarm Details page to obtain the alarms pertinent to this notification. You can view the notification rules from the Notification Center (go to **Alarm & Notification > Notification Center**).

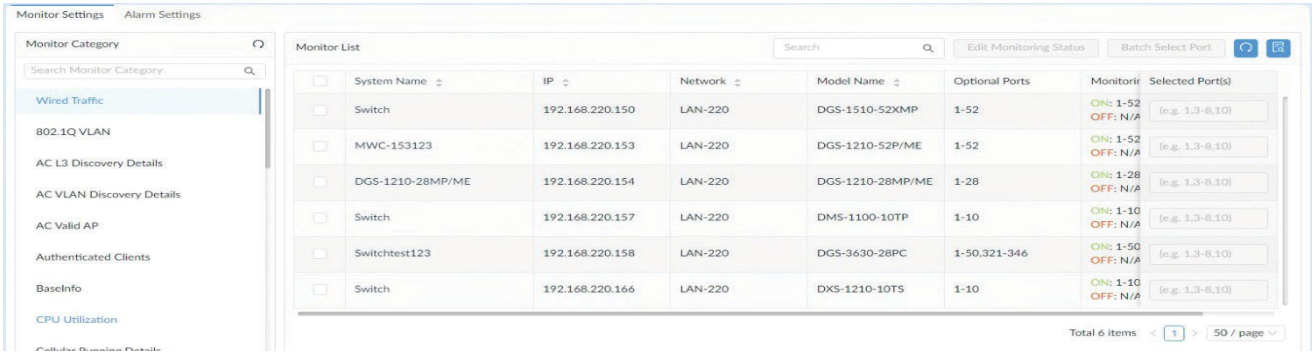
Monitor Networks

The NMS allows for efficient monitoring of devices with system default monitor functions.

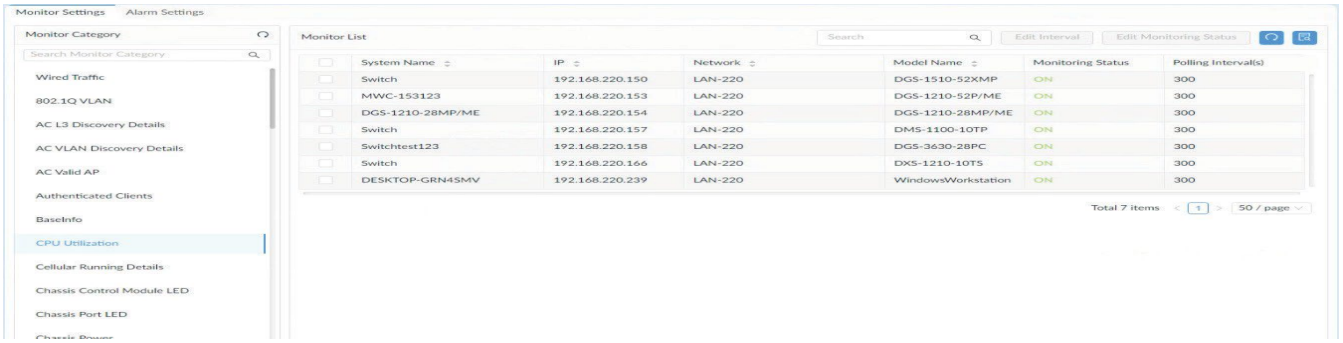
Configure Monitor Settings

You can configure monitoring settings such as monitoring status and polling interval.

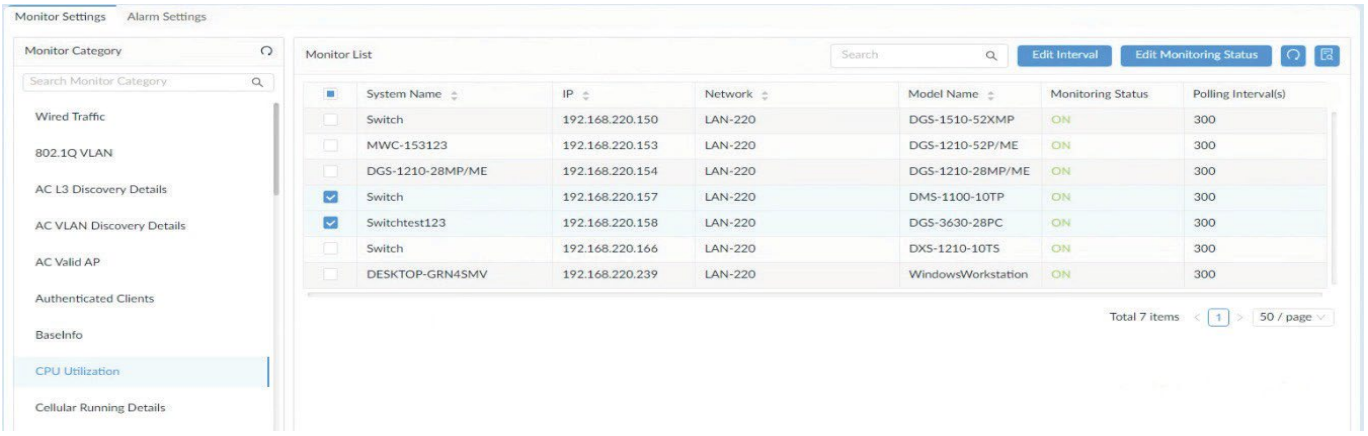
1. Go to **Alarm & Notification > Monitor & Alarm Settings**. Then Select the **Monitor Settings** tab.



2. Select the monitor category from the left pane. The devices that have been associated with monitoring templates in this category will be displayed.



3. Select the devices for configuration and the **Edit** Interval and **Edit Monitoring** Status button will be activated.



You can also enable or disable a monitor function on a per-device basis; go to the **Monitoring > Device View** and select the Device Information page by clicking the **System Name** link of the selected device. Then click the **Monitor** tab to access the **Monitoring Settings** button (refer to Modify Device Information).

Create Alarm Rules

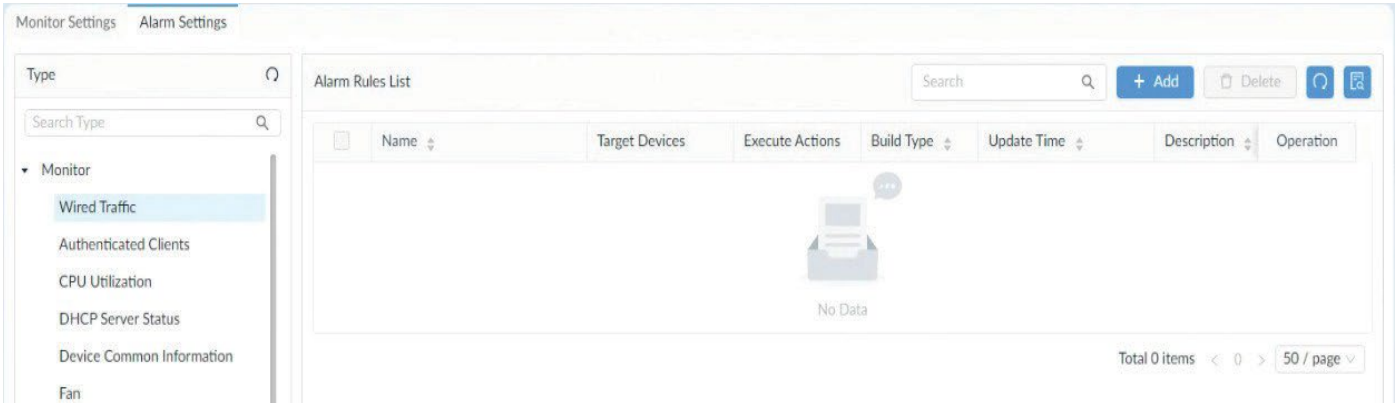
Alarms can be generated to be displayed in the Annunciator to notify users if a configured condition for alarms has been raised. Refer to Annunciator.

To add an alarm rule:

1. Go to **Alarm & Notification > Monitor & Alarm Settings**. Then select the Alarm Settings tab.

2. From the left pane, select a monitoring condition for configuration.

3. Click **+Add** to configure a rule.



The **Add Alarm Rule** page displays.

Different rules require different configurations. However, the following general settings are presented for all alarm rule types:

- Set profile information: enter a name and description for the alarm rule.
- Set alarm generation conditions: set the threshold value for different levels of severity of the alarm: Info, Warning, and Critical.
- Set alarm release conditions: set the threshold value for clearing the alarm.
- Add Inhibition Schedule Settings: select a pre-defined schedule. Or click **Add Schedule** to add a new schedule. The schedule prohibits delivery of alarms at the specified time range of a designated weekday or weekdays for the effective duration of dates.
- Select target devices: add devices for configuration.
- Set Action: execute a designated script. The script can be executed on designated device(s) other than the device configured as the alarm source or on selected NMS servers. Click the respective Device Command or Server Command tab. For executing commands on device(s), configure the credentials and method for logging in to the devices.

4. Click **Next** or **OK** to continue the rule configuration.

5. Click **Save** to create the rule and exit the screen.

Configuration and Firmware

The NMS makes it easy to save and restore device configurations. It also allows schedule-based firmware upgrade and configuration changes.

The following topics are covered:

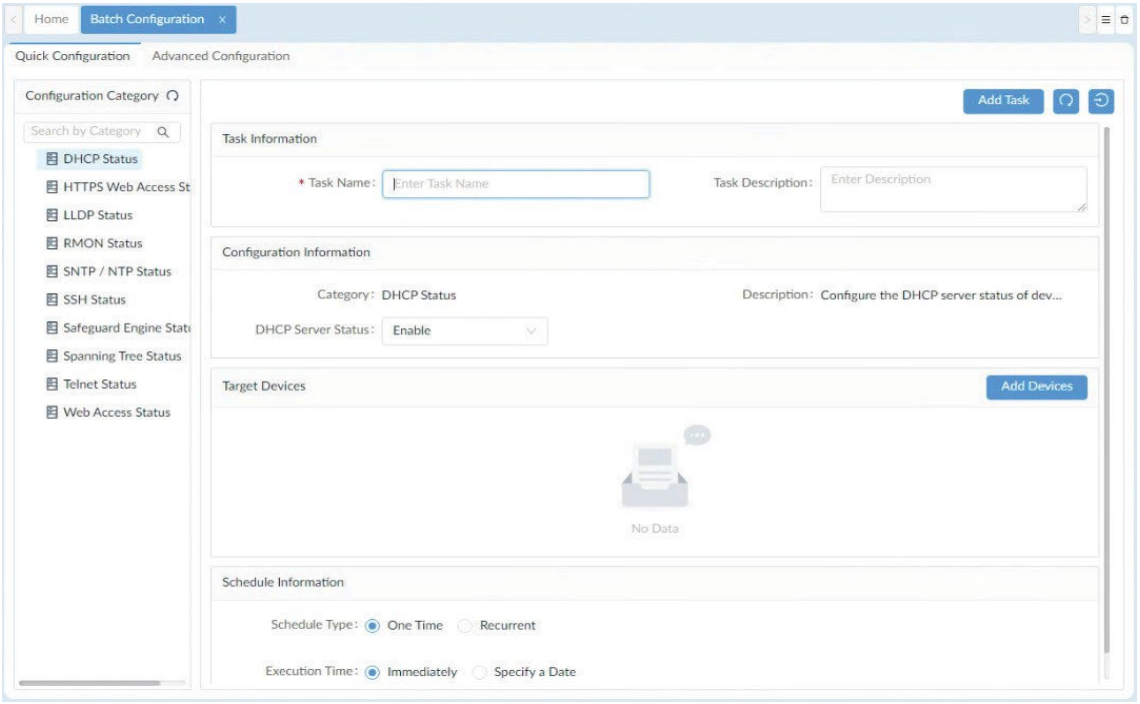
- Create Configuration
- Manage Tasks
- Upgrade Firmware
- Back Up and Restore Device Configuration
- Import Configuration and Firmware Files

Create Configuration and Profiles

You can apply specific configurations to designated devices on the network with quick or advanced batch operations.

Add a Configuration Task

1. Go to **Configuration > Batch Configuration**. The Batch Configuration page displays.



2. From the Configuration Category, select a category or enter a keyword in the search field to search for a desired configuration category. The system default configuration categories are explained below:

Item	Description
DHCP Status	Select to set the DHCP Status configuration task
HTTPS Web Access Status	Select to set the HTTPS Web Access Status configuration task
LLDP Status	Select to set the Link Layer Discovery Protocol Status configuration task
SNTP/NTP	Select to set the SNTP (Simple Network Time Protocol) or NTP (Network Time Protocol) status configuration task.
RMON Status	Select to set the RMON alarm status configuration task
SSH Status	Select to set the SSH Status configuration task
Safeguard Engine Status	Select to set the Safeguard Engine Status configuration task
Spanning Tree Status	Select to set Spanning Tree Status configuration task
Telnet Status	Select to set the Telnet Status configuration task.
Web Access Status	Select to set the Web Access Status configuration task
Note: The above listed are system-built categories and it also displays customized categories of the Quick Configuration type.	

3. Complete the fields as explained below:

Task Information	
Task Name	Enter the name to define the task.
Task Description	Enter a brief description to identify the task.
Add Task	Click to create the defined task.
Refresh	Click to refresh the task.
Configuration Information	
Status/Input	Apply the configuration changes for the job. For customized category, the options depend on the design of the template and selected protocol.
Target Devices	
Add	Click to add the device(s) for configuration. Note that only devices that support this function can be selected. For customized configuration categories, you need to associate the configuration template to the device template first.
Note: You can select multiple devices across different networks. To confine the configuration to only devices under the same network for better security, use the below Configuration Profile method.	
Schedule Information	
Schedule Type	• **One Time:** Select this option to specify a date and time or immediately to initiate the network discovery. • **Recurrent:** Select this option to specify the frequency and effective time frame to initiate network discovery.

You can click **Task Management**  to open the Task Management page

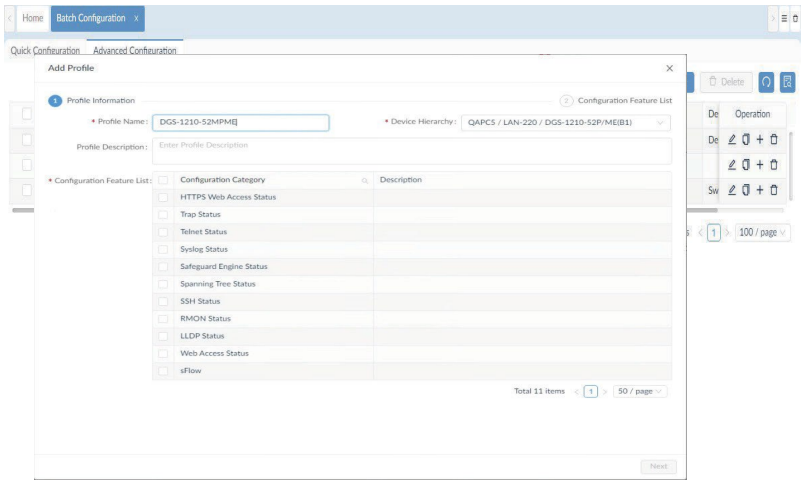
Add a Configuration Profile

Configuration profiles are designed to allow multiple configuration categories for rapid network deployment. Unlike the above quick configuration, it can accommodate different categories of the Advanced Configuration type in a profile. Once a profile is defined, you can apply it to multiple devices in a network.

Go to Configuration > Batch Configuration.

1. Select the **Advanced Configuration** tab.

The Advanced Configuration page displays.



2. Click Add Profile to display the Add Profile page.

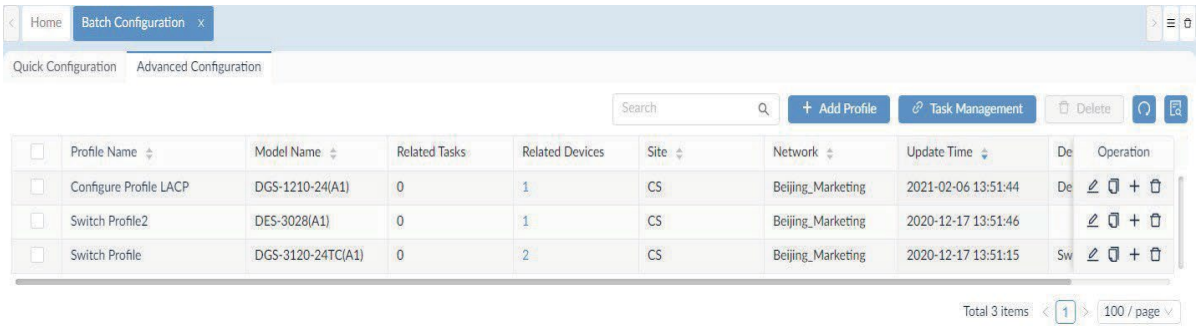
3. Enter the following information to define the profile:

Profile Name	Enter a name to define the profile.
Device Hierarchy	Click the drop-down menu to select a device. Note that here you only need to specify a model to apply the configuration to. You can select devices of the designated model when creating tasks. Refer to the below **Apply a Profile to Devices with Task**.
Profile Description	Enter a brief description to identify the profile.
Configuration Feature List	Select categories for the profile: • DHCP Status • HTTPS Web Access Status • LLDP Status • RMON Status • SNTP/NTP Status • SSH Status • Trap Status • Syslog Status • Safeguard Engine Status • Spanning Tree Status • Telnet Status • Web Access Status
Note: The available configuration category depends on the features supported. Unlike the Quick Configuration page described above, it allows you to select categories of the Advanced Configuration type.	

4. Click **Next** to continue and configure the selected features.

5. Click **Save** after configuring the features for each category. Click Previous to return to the previous screen.

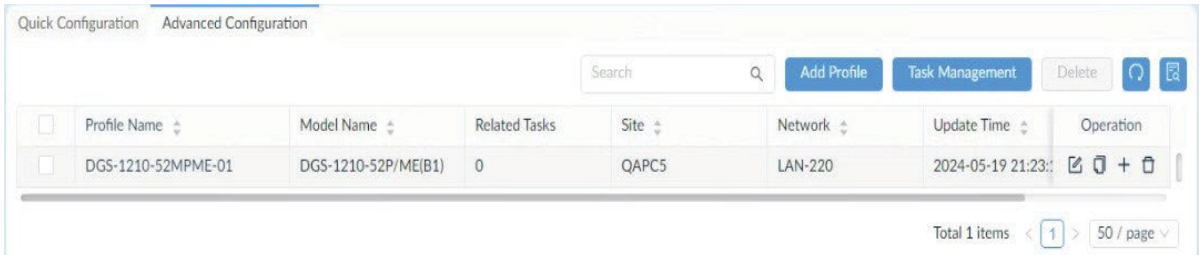
After a configuration profile is created, you can modify or delete it with the options under the Operation column.



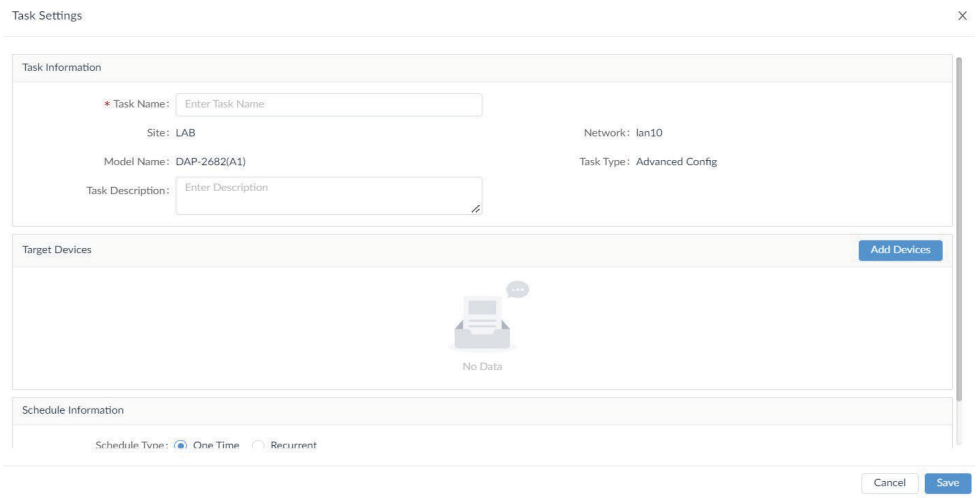
Item	Description
Edit	Modify the configuration profile settings.
Share	Copy the profile to configure devices of the same model on other networks.
Create Task	Create a task for the profile to perform the configuration on selected devices according to a set schedule. Refer to the following section for detailed instructions.
Delete	Remove the profile from the list.

Apply a Profile to Devices with Task

1. Go to **Configuration > Batch Configuration**.
2. Select **Advanced Configuration**.
3. Select a profile, then click + (Create Task) from the Operation column on the right to apply the profile to devices by creating a task.



The Task Settings page displays.



4. Enter the following information:

Task Information	
Task Name	Enter a name to define the task.
Task Description	Enter a brief description to identify the task.
Target Devices	
Add Devices	Click to add the device(s) for configuration. The Batch Select Devices screen displays. Select the desired devices or use the Search function to find devices.
Note: You can only select devices of the same model under the designated network. To apply the configuration profile to other networks, use the Share function under Operation. You can also create device groups with devices across networks in advance and select the desired group from the Device Group tab. (Refer to Manage Device Groups.)	
Schedule Information	
Schedule Type	• **One Time:** Select this option to specify a date and time or immediately to execute the task. • **Recurrent:** Select this option to specify the frequency and effective duration to execute the task. Refer to Scheduling for more information.

5. Click Save to create the new task and return to the previous menu.

You can click **Task Management** to open the **Task Management** page. Refer to Current Tasks for details about tasks.

Manage Tasks

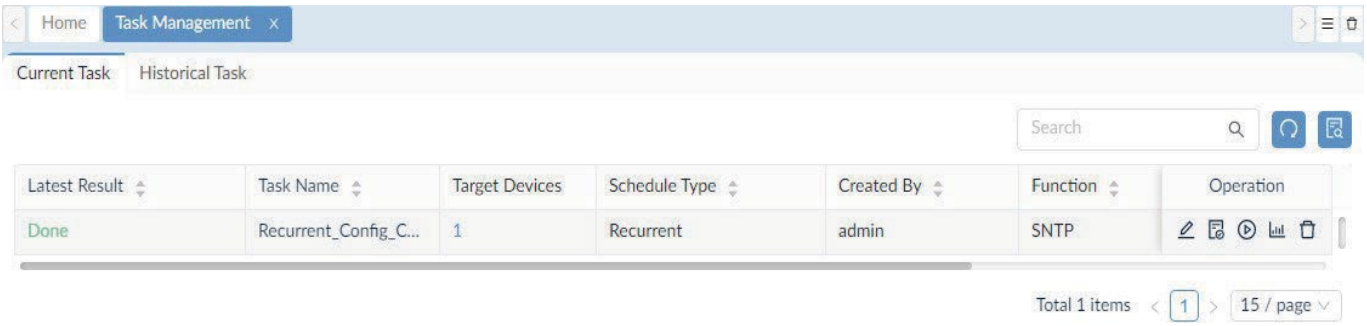
The Task Management function lets you manage current and previously performed tasks. Tasks initiated in the system can be edited, deleted, and restarted. You can also view the task execution record.

Current Tasks

Current tasks are tasks that are scheduled to be performed in the

future. To view current tasks:

1. Go to **Configuration > Task Management**. Then select the Current Task tab.



The following table displays the properties of the tasks and the functions that you can perform on them:

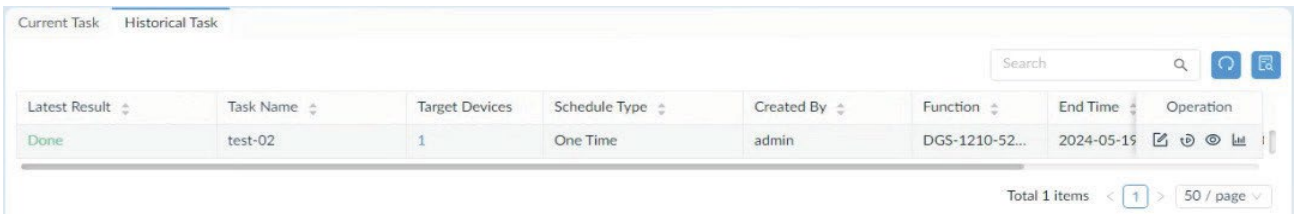
Item	**Description**
Task Name	Displays the defined name of the task.
Target Devices	Displays the number of devices that the task will be applied to.
Schedule Type	The configured schedule type: one-time or recurrent.
Created By	Displays the name of the task creator.
Function	Displays the featured functions or configuration profile name to be executed with the task.
Time Created	Displays the creation date of the task.
Next Execution Time	Displays the next scheduled start of the task.
Operation	
Edit Configuration	Click to edit the defined configuration.
Edit Task	Click to modify the task settings.
Restart/Pause Task	Click to activate/deactivate the task.
Show Task Record	Click to display the event timeline of the task, listed in chronological order.
Delete Task	Click to delete the task. You need to pause the task first for deletion.

Historical Tasks

Historical Tasks are tasks that have been performed in the past.

To view historical tasks:

Go to **Configuration > Task Management**. Then select the Historical Task tab.



Item	Description
Latest Result	Displays the results of the task: Partially done, Done, or Failed. Click on the link to open the result details page.
Task Name	Displays the defined name of the task.
Target Devices	Displays the number of devices that the task will be applied to.
Schedule Type	The configured schedule information
Created By	Displays the name of the task creator.
Function	Displays the featured functions or configuration profiles to be executed with the task.
End Time	Displays the finishing time of the task.
Time Created	Displays the creation date of the task.
Operation	
Edit Configuration	Click to edit the corresponding configuration file.
Re-execute Task	Click to modify the task and reschedule the task to be performed again. It will appear in the above Current Task tab for future execution dates.
Review Task	Obtain task details including name and type, target devices and task scheduling.
Show Task Record	Click to display the event timeline of the task, listed in chronological order.

Schedule a Firmware Upgrade

Scheduling a firmware upgrade task requires uploading firmware files first in File Management (refer to **Configuration > File Management**).

To configure a firmware upgrade task:

Go to Configuration > Firmware Management.

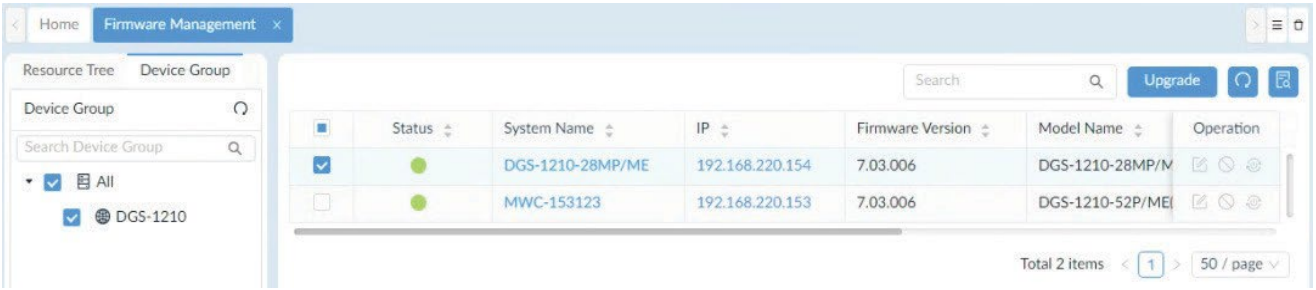
1. In the Resource Tree pane, select the desired device model under the designated site(s) and network(s) for the upgrade task. Or enter a keyword in the Search field to locate the target network or model name. You can select the Device Group tab if you have created device groups for designated devices.

2. From the discovered or listed devices, select device(s) for firmware upgrade.

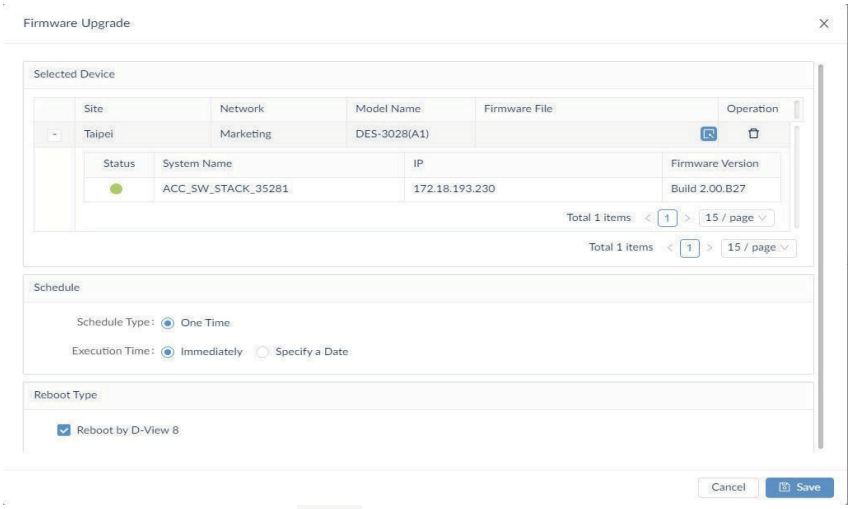
Device firmware information will be displayed:

Item	**Description**
Status	Displays the online/offline status of the device.
System Name	Displays the system name of the device.
IP	Displays the IP address of the device.
Firmware Version	Displays the device's firmware version.
Model Name	Displays the model name of the device.
Upgrade Result	Displays the result of the last firmware upgrade or the scheduled firmware upgrade.
Site/Network	Displays the site and network where the device resides.
Operation	
Edit	Click to modify the firmware upgrade task. You may need to stop the firmware upgrade task first to edit it.
Stop	Click to stop the task.
Reboot Device	Click to reboot the device after the firmware upgrade.

3. Click **Upgrade** in the upper right corner to configure the task.

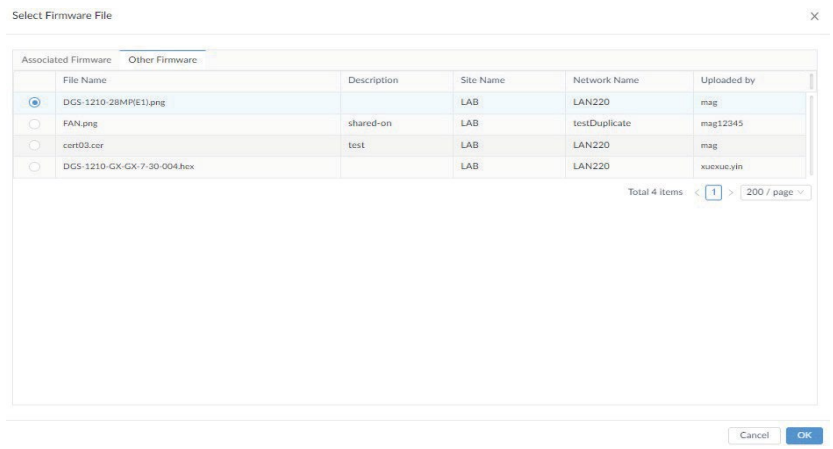


4. The **Firmware Upgrade** page displays.



5. Click Select **Firmware File** to select a firmware file for the specified devices.

6. The Select Firmware File page displays. Select the Associated Firmware tab to upload firmware from your local file system. Or select a firmware file stored in the server from the Other Firmware tab.



7. Configure the following:

Item	Description
Selected Device	Displays the device(s) selected for the task. You can click Delete to remove the selected devices.
Schedule Information	
Schedule Type	Firmware upgrade is a one-time event.
Execution Time	Define the execution time, immediately or a specific date and time.
Reboot Type	Click to enable or disable (default) device reboot after firmware upgrade. A reboot is typically required for the new firmware to take effect.

8. Click **Save** to create the firmware upgrade task. Click **Cancel** to return to the previous screen.

The **Upgrade Result** column will record the results of the firmware upgrade task.

Back Up and Restore Device Configuration

The NMS provides backup function to maintain configuration files on the server.

Add or Modify a Backup Profile

Regular system backup can be accomplished automatically through backup profiles.

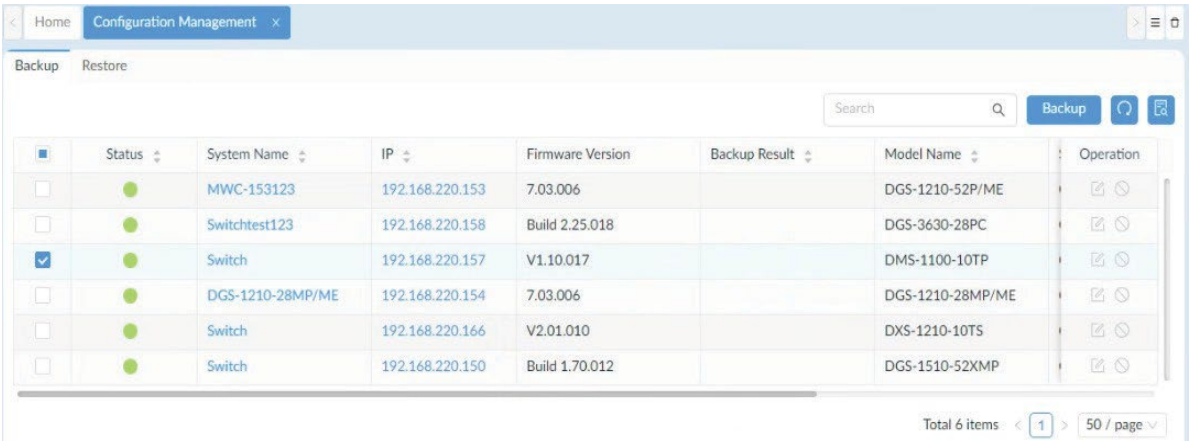
Go to Configuration > Configuration Management.

1. Select devices for backup.

Available devices with device information are displayed:

Item	Description
Status	Displays the online/offline status of the device.
System Name	Displays the system name of the device.
IP	Displays the IP address of the device.
Firmware Version	Displays the device's firmware version.
Model Name	Displays the model name of the device.
Backup Result	Displays the result of the last configuration backup or the scheduled backup.
Site/Network	Displays the site and network where the device resides.
Operation	
Edit	Click to modify the backup task. You may need to stop the backup task first to modify it.
Stop	Click to stop the task.

2. Click Backup to configure the task.



The **Backup** page displays.

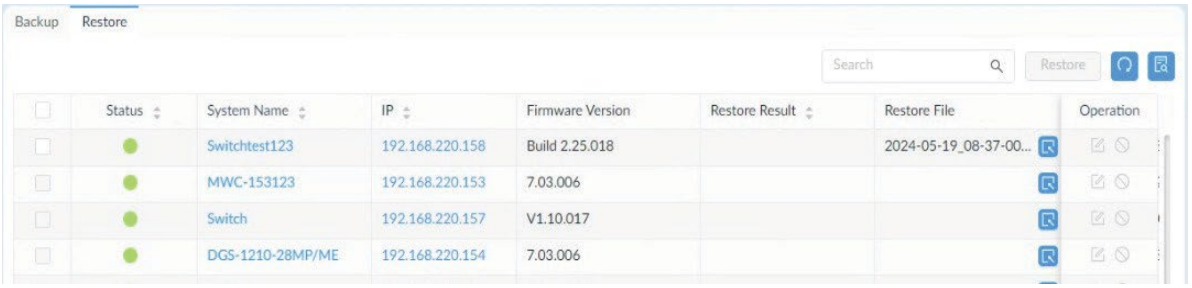
Restore Device Configurations

Device configuration settings can be restored through a defined backup task with an assigned configuration file.

To restore a device configuration:

1. Go to Configuration > Configuration Management.

2. Click the Restore tab to view the defined restore tasks.



3. Select a device with a pre-defined baseline file or the most recent backup version and click Restore to configure the task.

NOTE: Files that will be used for restoration can be selected by clicking the Select button under the **Restore File** column. You can also upload additional configuration files and assign a baseline file on the **Select Restoration File** page.

In the Select Restoration File page, you can perform the following on restoration files:
• Upload file
• Download file
• Set as baseline configuration

4. On the Restore page, under Schedule Information, select the scheduling method to perform the task:

- Schedule Type: Click to define the frequency of the task, a single event or recurring task. For a recurring task, specify a pre-defined schedule or add a new schedule by specifying the repetition frequency (daily, weekly, monthly, or discrete dates) and effective duration. Refer to Scheduling for more information.
- Execution Time: For a single event, define the execution, immediately or a specific date and time.

5. Click Save to create the restore task. Click Cancel to return to the previous screen.

6. You can also edit or stop a restore task. Under Operation, click Edit or Stop on the right.

The task is created and the restore task will be recorded in the Restore Result column along with other information such as system name, IP address, firmware version, and device model as well as device category.

Alarm and Notification

Alerts and notifications can be sent automatically when an upper or a lower threshold has been reached. If the threshold is exceeded, an alarm will be generated. You can set alarm notifications to be received by email, web scrolling notification, or as a script to be executed on selected devices.

The section covers the following topics:

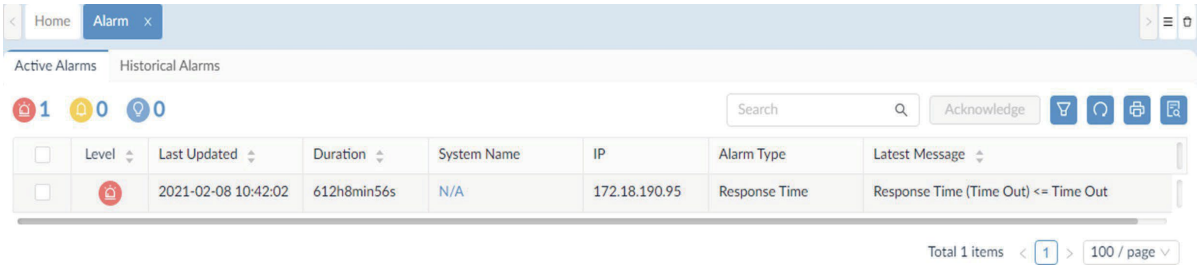
- View Alarms
- View Traps and Syslog
- Trap Editor
- Syslog Editor
- Monitor and Alarms
- View and Manage Notifications

View Alarms

Alarms for all devices can be viewed centrally from the NMS application interface.

Go to Alarm & Notification > Alarm.

1. You can view both active and historical alarms.



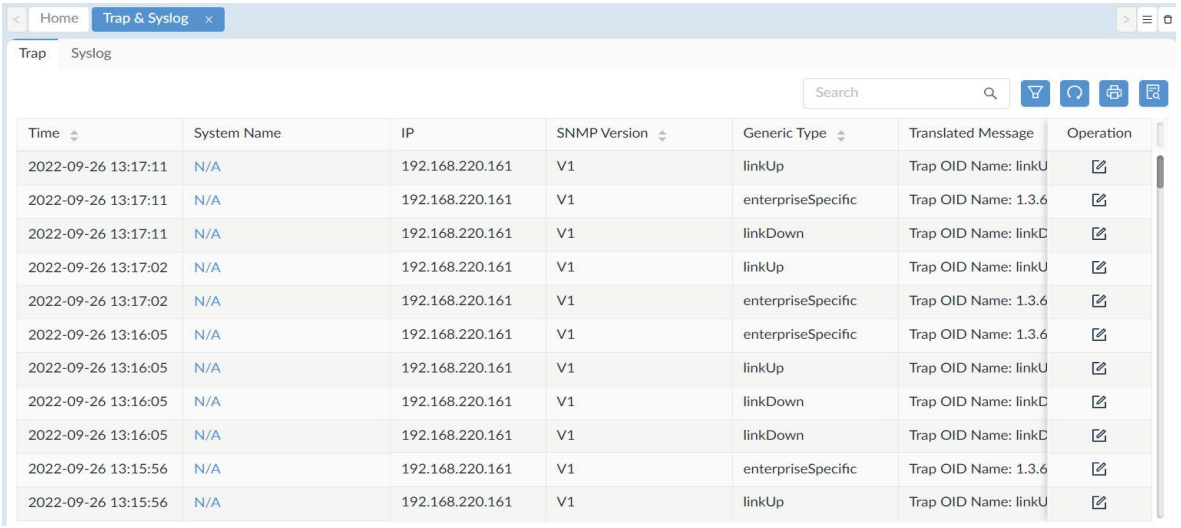
Item	Description
Active Alarms	Displays a list of the currently active alarm events.
Historical Alarms	Displays a list of alarm events already been acknowledged or been stopped.
Critical	Indicates a critical (highest) severity level for the alarm (red).
Warning	Indicates a warning (middle) severity level for the alarm (yellow).
Info	Indicates an informative (lowest) level for the alarm (blue).
Search	Enter a keyword to filter the list by System Name, IP, or Latest Message.
Acknowledge	Select an alarm event and click Acknowledge to move the alarm entry to Historical Alarms. Note that this will not disable the alarm setting.
Column Selector	Click to add or remove columns from the list. The following column properties are available: Level, Last Updated, Duration, System Name, IP, Alarm Type, and Latest Message.
Refresh	Click to refresh the table listing.
Export	Click to export the list as a CSV file. Up to 10,000 entries can be downloaded in one export job.
Advanced Query	Click to perform an advanced search job. Select the criteria to filter the table listing. Click Search to start the search.

View Traps and Syslog

The Trap & Syslog list displays the device trap events and syslog messages with the time. For trap events, the SNMP version, the original trap messages and the translated messages will be recorded. For syslog, messages will be assigned with a severity label. You can also send traps and logs to a remote logging server (go to **System > Basic Settings > Forward Trap** and **System > Basic Settings > Forward Syslog** to configure a remote trap and syslog server respectively). Both Trap and Syslog page allows you to refresh the list and export the records as a CSV file.

Note: You need to configure the NMS as Trap Server and Syslog Server for the managed devices so that logs and traps can be collected by the system (go to Monitoring > Device View and select the System Name link of a device to open its Device Information page. Then click the Management tab to find the Trap and Syslog status switch.) From the Device Information page, you can also view trap events and syslog messages generated from the selected device by clicking the Trap & Syslog tab.

To view device's logs, follow these steps:



You can perform the following operations on the Trap or Syslog list:

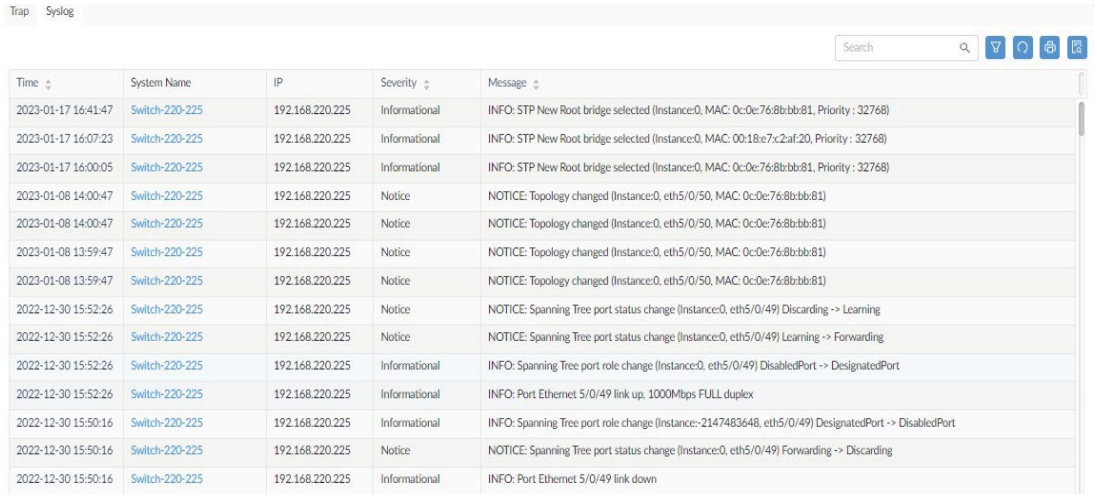
Item	Description
Search	Enter a keyword to filter the Trap or Syslog Editor list.
Edit	For SNMP traps, you can modify their OID description as well as the value description of a binding variable (refer to the below section).
Advanced Query	Select the criteria to filter the events or logs.
Refresh	Click to refresh the table listing.
Export	Export the table in CSV file format.

The translated message is based on the message from the original trap events. You can modify the translation between a trap OID and OID description as well as the translation between binding variable value and value description for OIDs with binding variables by clicking **Edit** under **Operation**.

Note the modification here will also be saved on the **Trap Editor** page (go to **Alarm & Notification > Trap & Syslog Editor > Trap Editor**.)

You can also configure alarm rules based on selected trap events with matched trap OID or binding values. Refer to Monitor and Alarms for more information.

Click the **Syslog** tab to view syslog list.



The syslog contains the following severity levels from the highest to the lowest.

Severity	**Description**
Emergency	Indicates that the device is failing to operate normally.
Alert	Indicates that immediate investigation is needed.
Critical	Indicates that the device is in critical condition.
Error	Indicates that an error has been found on the device.
Warning	Indicates a warning condition of the device's operation.
Notice	Indicates a normal but significant condition that needs an operator's attention.
Informational	Indicates a specific condition that is not erroneous but needs to be recorded for reference or troubleshooting purposes.
Debug	Indicates messages for debugging purposes.

You can easily spot a particular log message when interpreting syslog reports by setting a syslog description with associated syslog keywords. Refer to the Syslog Editor and Reports for more information.

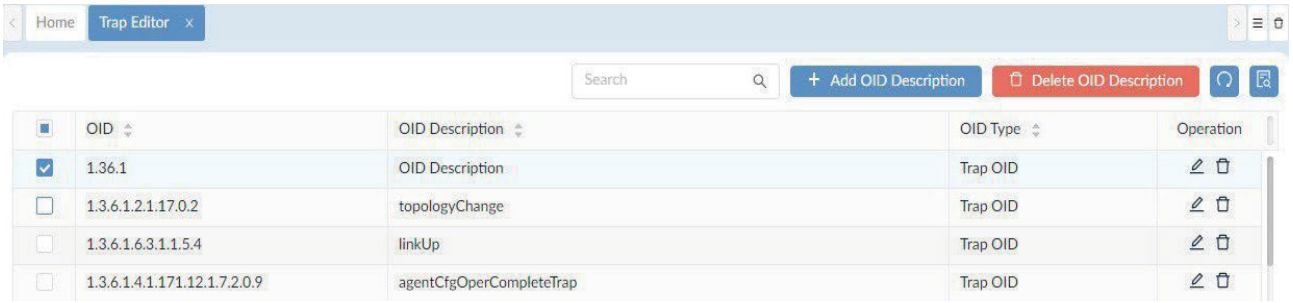
Trap Editor

Traps can alert you to possible errors of the managed devices while syslog records problems of device operation. You can define object identifiers (OIDs) of a trap to help determine the nature of a problem. To view trap messages of all managed devices, go to **Alarm & Notification >Trap & Syslog > Trap**.

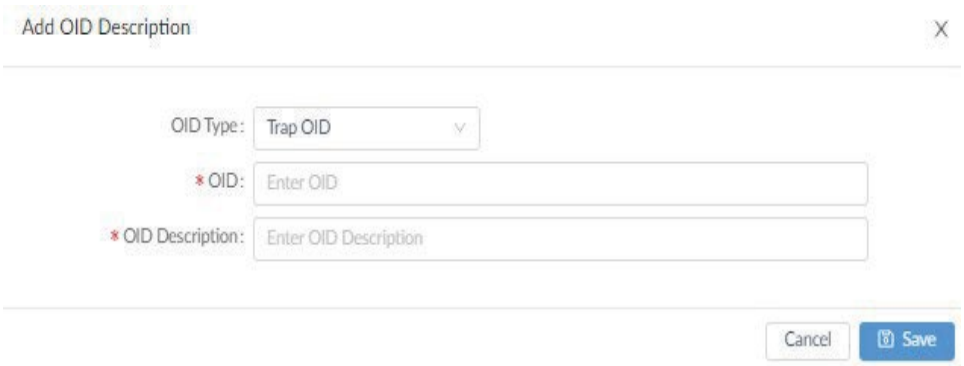
To add an OID description entry:

1. Go to Alarm & Notification > Trap & Syslog Editor.

2. Click the Trap Editor tab. You can add a trap OID or a binding variable OID type.



To add a trap or binding variable OID, click **Add OID Description**. Then enter an OID with a description for both types of OID. For binding variable OIDs, enter variable values with matching descriptions. The entry determines how a trap should be interpreted.



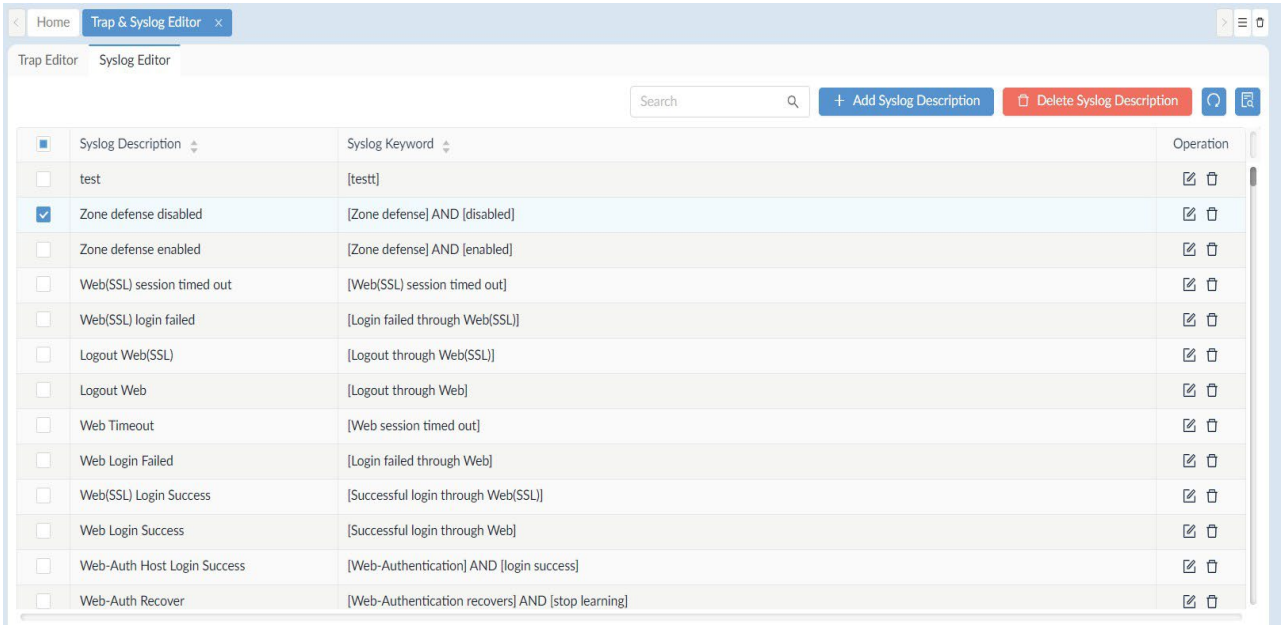
To edit an entry, select it and click Edit . The translated message in the Trap list should reflect the changes. You can generate trap reports using the provided report template and the OID description will be the highlighted text to signify trap events. Refer to Add a Report for more information.

Syslog Editor

The syslog is used to log device data. It allows you to analyze and help troubleshoot problems in time. Furthermore, you can add a syslog description to help you visualize particular log messages. To generate a Syslog report with the effect provided by Syslog Editor, go to **Reports > General Reports** and select the **Syslog** category under **Device Reports**. To view logs of all managed devices, go to Alarm & Notification >Trap & Syslog > Syslog.

To obtain the types of syslog messages:

1. Go to **Alarm & Notification > Trap & Syslog Editor**.



2. Click the **Syslog Editor** tab. You can perform the following operations on the list of Syslog Description:

Item	Description
Search	Enter a keyword to search for a log description entry using syslog description or syslog keyword.
Add Syslog Description	Add a syslog description representing selected log keywords to be displayed as highlight text to signify a condition or operation from log messages.
Delete Syslog Description	Click to delete a syslog description entry.
Refresh	Click to refresh the table listing.
Advanced Query	Click to perform advanced search. Enter the criteria to filter the table.
Edit	Click Edit to modify a syslog description.
Delete	Click to delete a syslog description.

You can also configure alarm rules based on the severity of Syslog. In addition, you can set the system to alert you that certain types of messages with matching content have been logged. Refer to Monitor and Alarms for more information.

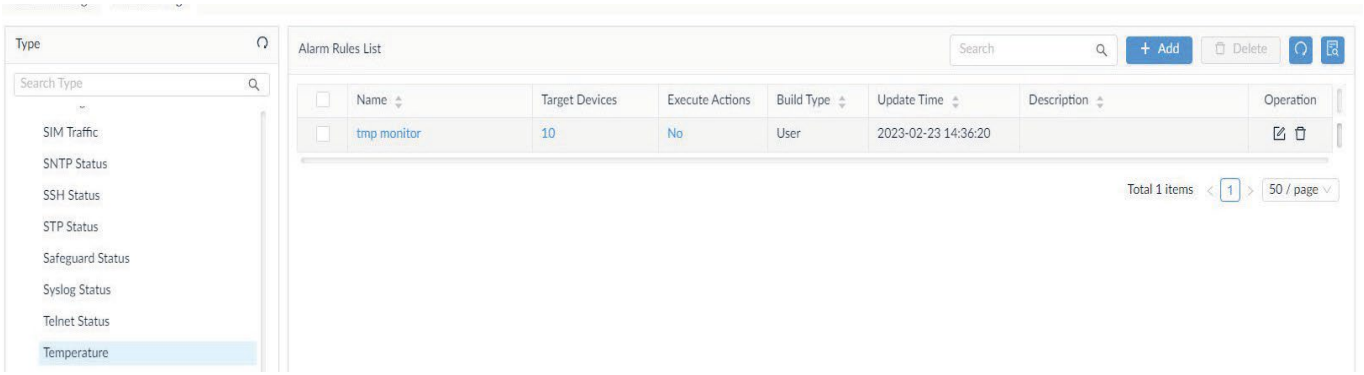
Monitor and Alarms
Alarm Settings

You can manage monitor and alarm settings and configure conditions to trigger alarms. Alarms can be triggered by CPU or memory utilization and a wide range of system metrics. They can be configured by users or by the system as the defaults.

To view all configured alarms:

1. Go to **Alarm & Notification** > **Monitor & Alarm** Settings.

2. Click the **Alarm Settings** tab.



The following system-built categories of device status can be configured for an alarm:

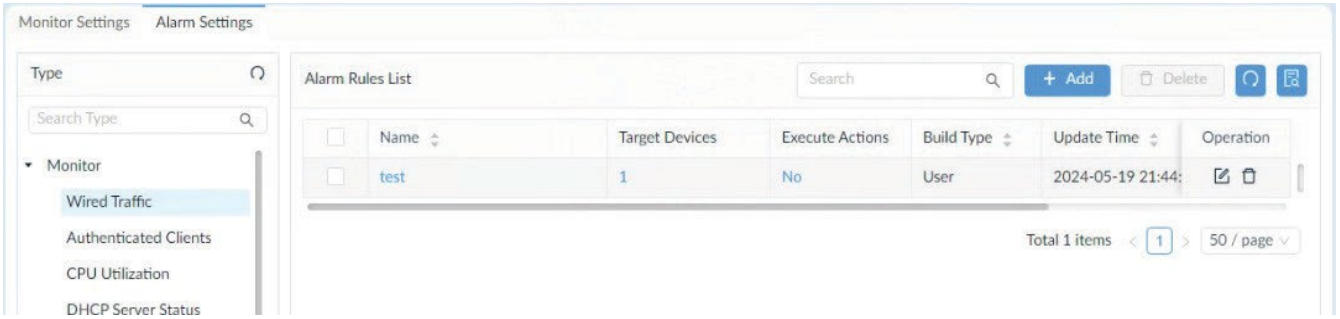
Category	Item	Description
Monitor	Wired Traffic	Alert based on Rx/Tx traffic, error rate, discard rate, and bandwidth utilization
	Authenticated Clients	Alert based on Rx/Tx speed of authenticated client sand client number
	CPU Utilization	Alert based on CPU utilization
	DHCP Server Status	Alert based on DHCP status
	Device Common Information	Alert based on firmware version, hardware version, MAC address, serial number, or total flash capacity.
	Fan	Alert based on fan status or speed
	HTTP Status	Alert based on HTTP status or port number.
	HTTPS Status	Alert based on HTTPS status
	Installed Apps	Alert based on the number of installed apps.
	LACP	Alert based on LACP state
	LLDP	Alert based on LLDP status
	Managed AP WLAN Traffic (packet)	Alert based on WLAN Rx or Tx traffic
	Memory Utilization	Alert based on memory utilization
	Power Status	Alert based on power status
	Private Port	Alert based on the port details of D-Link switches using the private MIB.
	RMON Status	Alert based on RMON status
	Response Time	Alert based on response time (a system-default alarm)
	Running Software	Alert based on the software running on hosts
	SIM Traffic	Alert based on the upload and download traffic on the SIM card
	SNTP Status	Alert based on the SNTP status
	SSH Status	Alert based on the SSH version, status, maximum authentication failed attempts, session key rekeying times, maximum session, connection timeout, or port number
	STP Status	Alert based on STP status
	Safeguard Status	Alert based on Safeguard status
	Syslog Status	Alert based on Syslog status
	Telnet Status	Alert based on telnet status and port
	Temperature	Alert based on the temperature indicators and measurements
	Trap Status	Alert based on the trap status

Category	Item	Description
Trap	Cold Start	Alert based on a device coldStart trap
	Warm Start	Alert based on a device warmStart trap
	Link Down	Alert based on a port linkDown trap
	Link Up	Alert based on a linkUp trap
	Authentication Failure	Alert based on an SNMP authentication failure trap
	EGP Neighbor Loss	Alert based on an EGP Neighbor Loss trap
	Enterprise Specific	Alert based on an enterprise-specific trap
Syslog	Syslog	Alert based on a syslog message with matching content

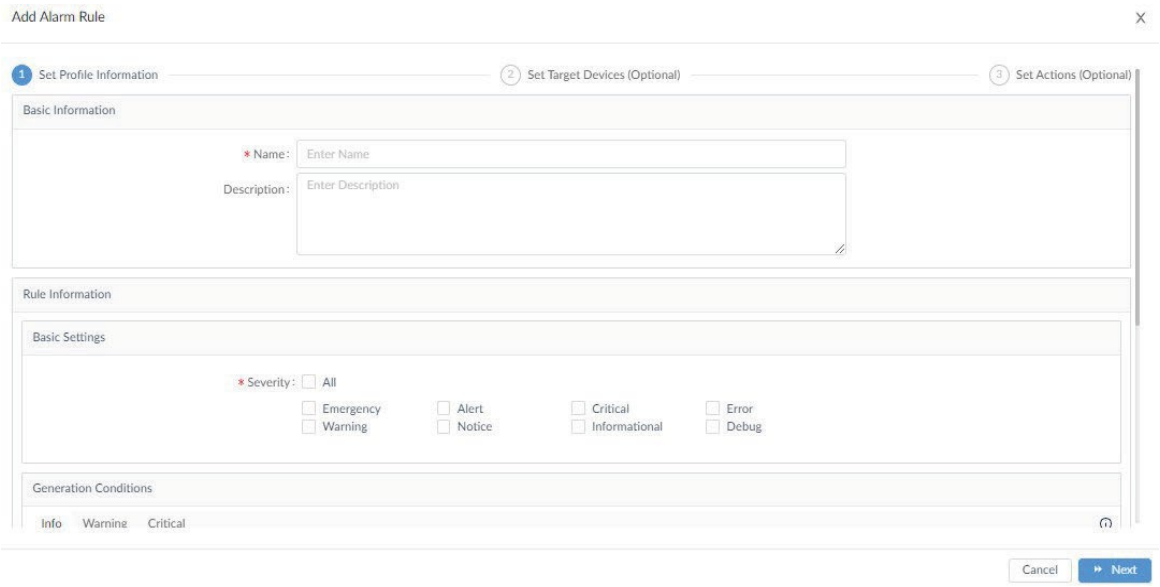
From the Alarm Settings menu, you can set rules for different monitor categories or traffic and message types such as Trap, Syslog.

To add an alarm rule:

1. Go to **Alarm & Notification > Monitor & Alarm Settings**. Then select the **Alarm Settings** tab.
2. From the left pane, select a system-defined monitor category (or a customized monitor category) for configuration.
3. Click +**Add** to configure a rule.



The Add Alarm Rule page displays.



Different rules require different configurations that may involve traffic rate or utilization percentage as well as traffic direction. The following general settings are presented for all alarm rule types:

- Set profile information: enter a name and description for the alarm rule.
- Set alarm generation conditions: set the threshold value for different levels of severity for the alarm: Info, Warning, and Critical. The parameters for settings the threshold value depend on the monitored condition types.
- Set alarm release conditions: set the threshold value for clearing the alarm.
- Set target device/source: set the devices and device interfaces (for the **Wired Traffic** monitoring condition) to be monitored.
- Set alarm criteria (only applicable to the sFlow alarm category): set criteria (e.g. application, DSCP value, IP address, or protocol) along with sFlow interfaces and direction to be monitored.
- Add Inhibition Schedule Settings: select a pre-defined schedule or click **Add Schedule** to add a new schedule. The Schedule prohibits delivery of alarms at the specified time range of a designated weekday or weekdays for the effective duration of dates.
- Set Actions (optional): execute a script. The script can be executed on designated device(s) other than the device configured as the alarm source or on the selected NMS servers. Click **Add actions** at the upper right and click the respective Device or Server Command tab. To execute commands on device(s), configure the credentials and method for logging in to the devices.

Click **Next** or **OK** to continue the rule configuration. Then click **Save** to create the rule and exit the screen.

Note: After an alarm has been configured for the selected devices, you can activate the alarm on a per-device or per-port basis (for the **Wired Traffic** monitoring condition) . Go to **Monitoring > Device View** and click the **System Name** link to go to the **Device Information** page. Then select the **Port** or **Alarm** tab to access the port list or alarm settings page. For Port list, you can turn on or off the Alarm Switch for each port. For Alarm settings, turn on or off a specific alarm type.

Monitor Settings

Network monitoring is performed through the Monitor and Alarm settings menu. You can select a specific monitor category to view available configuration settings.

To obtain monitoring conditions:

Go to Alarm & Notification > Monitor & Alarm Settings.

1. Click the **Monitor Settings** tab.

2. Click a **Monitor Category** to view all monitoring settings in that category.

To edit a monitoring condition:

Select a device or multiple devices and adjust the monitoring interval by clicking **Edit Interval**. Depending on the monitored condition, you may edit monitor status or port numbers if they are applicable.

To apply ports settings:

Select a device or multiple devices, click **Batch Select Port** and enter the port range (e.g. 1,3-8,10), and click **Apply**. Then click **Edit Monitoring Status** to enable or disable monitoring on the designated ports.

To stop monitoring:

Select a device or multiple devices and adjust the monitoring status by clicking **Edit Monitoring Status**. Then click **ON** or **OFF** to enable or disable monitoring.

Note: Stopping a monitoring condition will cause the associated alarms to be disabled automatically.

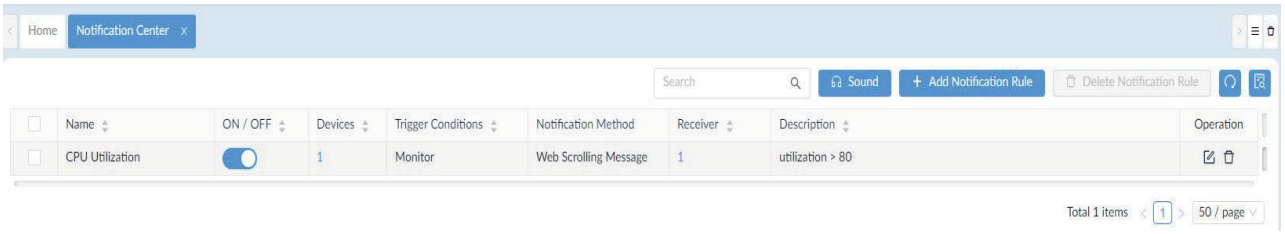
Manage Notifications

The Notification Center displays the notification rules. It allows you to configure rules of trigger conditions and notification recipients and set schedules for notification activation.

To set a notification rule:

Go to Alarm & Notification > Notification Center.

The Notification Center page displays.

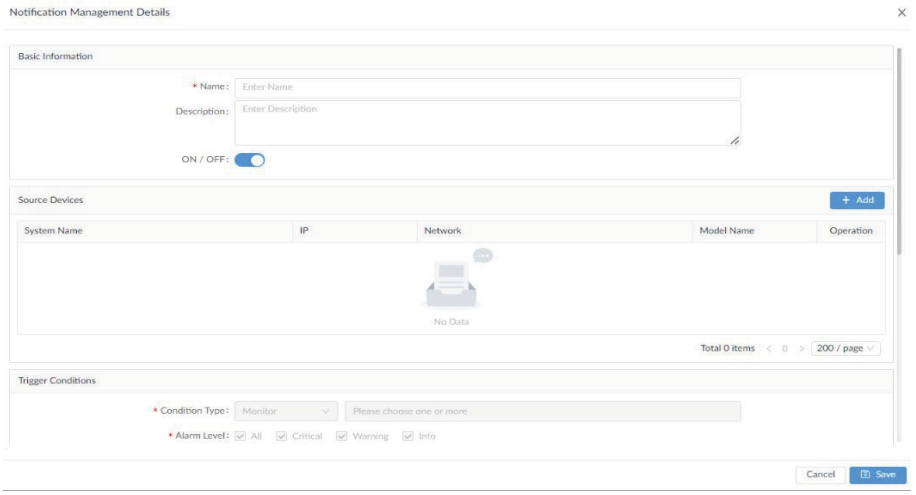


The list contains the following information on rules and display control:

Item	Description
Search	Enter a keyword to search for a specific notification name.
Sound	Click to customize a ringtone to sound when a notification is triggered. Different alarm levels can be configured with different built-in ringtones.
Add Notification Rule	Click to define a notification rule.
Delete Notification Rule	Click to remove the notification rule.
Refresh	Click to refresh the table.
Advanced Query	Click to configure an advanced search job. Select the criteria to filter the list: Name, On/Off status, Trigger Conditions, or Notification Method.
Name	The name of the notification rule.
On/OFF	Enable or disable the notification.
Devices	The number of devices to which the rule applies.
Trigger Conditions	The monitored condition type (i.e. monitor, trap, syslog, or wired traffic) to trigger a notification.
Notification Method	The method of notification for the rule (i.e. web scrolling message or execute script).
Description	A description of the rule.

1. Click + **Add Notification Rule** to configure a new rule.

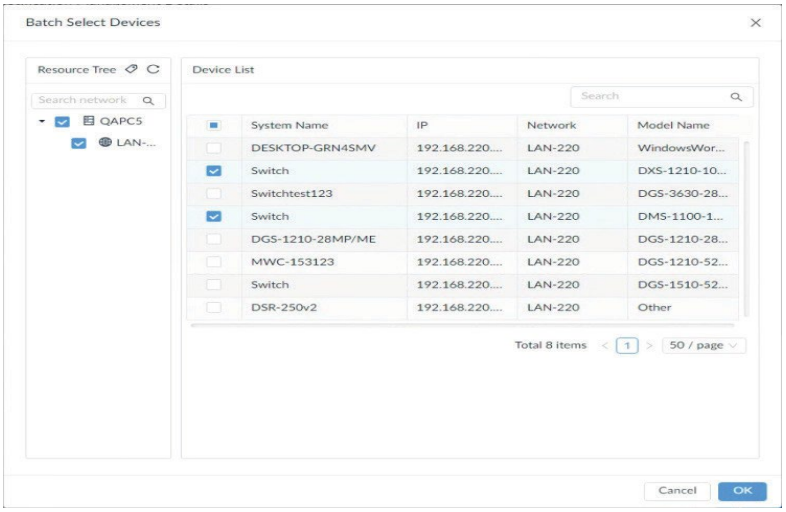
The Notification Management Details page displays.



2. Under Basic Information, enter a name and description to define the rule.

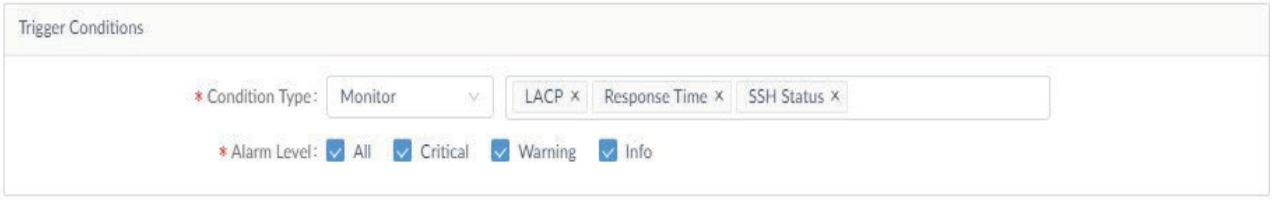
3. Click **ON/OFF** switch to enable or disable the rule.

4. In Source Devices, click **Add** to select target devices. The Batch Select Devices page displays.



5. Click **OK** to confirm the selection and return to the previous screen.

6. Under the Trigger Conditions, click the **Condition Type** drop-down menu to select a trigger condition type.



Item	Description
Condition Type	
Monitor	The monitor categories vary depending on the selected device model. • CPU Utilization • DHCP Server Status • Device Common Information • Fan • HTTP Status • LACP • LLDP • Memory Utilization • Power Status • Private Port • RMON Status • Response Time • SNTP Status • SSH Status • STP Status • Safeguard Status • Syslog Status • Telnet Status • Temperature • Trap Status • Authenticated Clients
Trap	Select the corresponding severity level to generate a notification for the configured alarms based on Trap: • All: all severity level of alarms will generate a notification. • Critical: critical level of alarms will generate a notification. • Warning: warning level of alarms will generate a notification. • Info: informational level of alarms will generate a notification.
Syslog	Select the corresponding severity level to generate a notification for configured alarms based on Syslog: • All: all severity level of alarms will generate a notification. • Critical: critical level of alarms will generate a notification. • Warning: warning level of alarms will generate a notification. • Info: informational level of alarms will generate a notification.
Wired Traffic	Select the corresponding severity level to generate a notification for configured alarms based on Wired Traffic: • All: all severity level of alarms will generate a notification. • Critical: critical level of alarms will generate a notification. • Warning: warning level of alarms will generate a notification. • Info: informational level of alarms will generate a notification. For Wired Traffic, select the ports that will be monitored for notification rules. Note that the monitored ports must also be the ports configured in the corresponding alarm rules for the notification to take effect. Note that there must be an alarm set with the corresponding severity level for the notification to take effect.

7. Under Notification Details, select the Notification Method.

Item	Description
Notification Method	
Web Scrolling Message	Notifications will appear as toast messages when you are logged in to the NMS web application. Select the Screen Scrolling Setting for the alert: Mute sound or Enable Voice.
Execute script	In the Command Line, enter the script to execute. **Notes:** 1. Lines begin with a '#' will be considered as comments and will not be considered as commands. 2. Use '%' before and after the word to label it as a variable. Example: %IP%. 3. The variables' value can be set in the 'Device Attribute' table. 4. Each line must contain no more than one CLI command. 5. Avoid endless CLI commands to prevent deadlock operation. Example: ping 10.0.0.1. 6. Avoid CLI commands that may require special inputs to exit to prevent deadlock operation. Example: show ports. Sample script: config ssh authmode password enable config ssh server contimeout 120 enable SSH Sample script with variables: config fdb aging_time %TimeoutSeconds% Sample comments: # this is a comment You can choose to execute a script for the source devices (Itself) or devices other than the source devices (Other Devices) when a notification is generated. To execute a script, config the username and password and protocol to log in to the selected devices to which the script will apply. The **Acknowledge Alarm after Script Execution** parameter can be used to terminate the repetitive execution of the script. For each execution of the script, the alarm will be automatically acknowledged. Enter the total Number of Repetitions (1-100) and Cycle Time (5-1440) minutes. The automatic script execution will stop when the maximum number of repetitions has been reached in the defined cycle time.

8. Under **Notification Suspension Period**, click **Add Schedule** to add a new schedule or select a pre-defined schedule whereby notification rule will be inactive. You can add a schedule for a specified time range of a designated weekday or weekdays for the effective duration of dates.

9. Click **Save** to accept the notification rule. Click **Cancel** to return to the previous screen.

After a notification rule is created, you can edit or delete it with the edit and delete functions under **Operation**.

Network Architecture

You can view network architecture through hierarchical maps. The following topics are covered in this section:

- View and Manage Network Topology
- Create a Topology View

Note: Please configure the managed devices to enable LLDP globally in advance to allow NMS to obtain physical topology information on all devices.

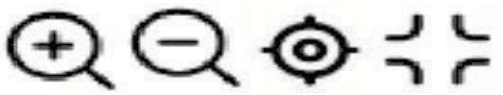
View and Manage Network Topology

Locating devices within the network can be accomplished through a hierarchical map. Additional information such as device information and status and related performance statistics can also be obtained from the map.

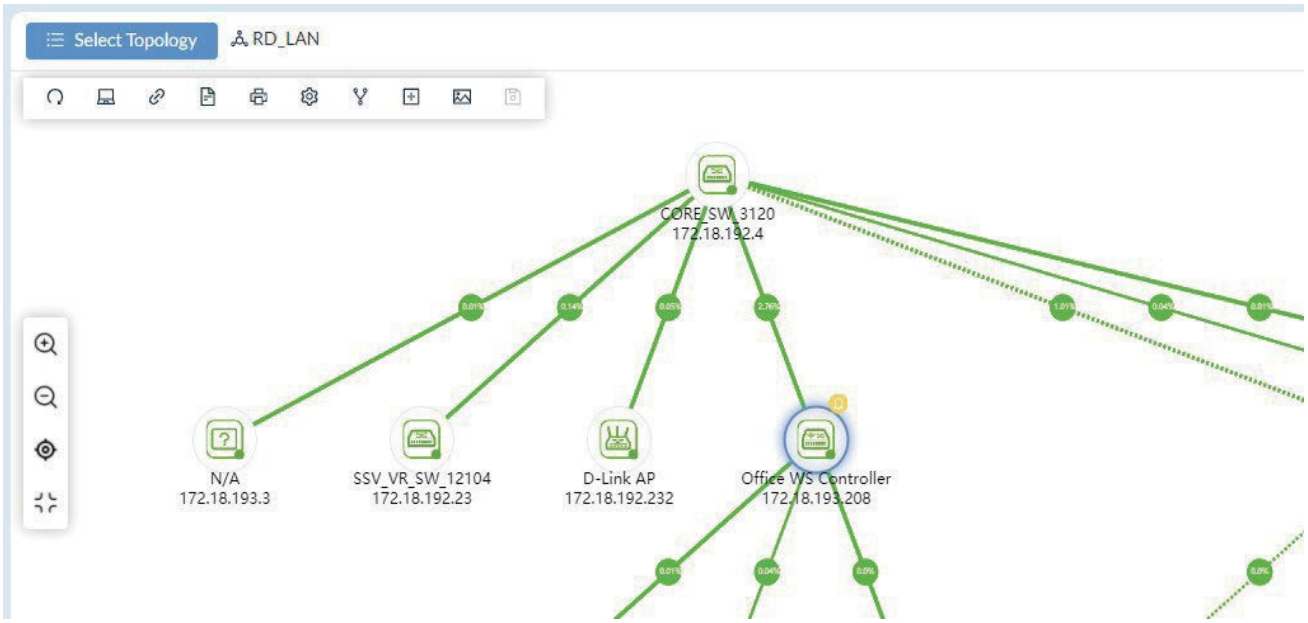
1. Go to **Monitoring > Topology Map**.

2. Click **Select Topology** to select the network diagram. The System Topology is built automatically whereas the Customized Topology is created by users.

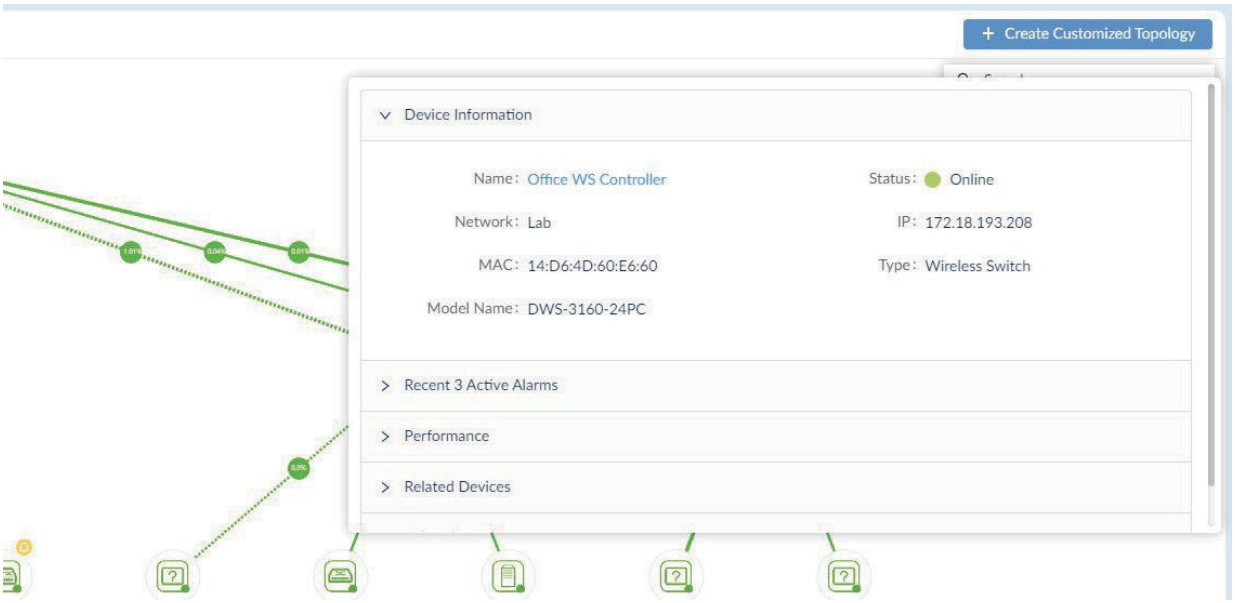
The Topology Map page displays.

Item	Description
Select Topology	Click to open the System Topology or Customized Topology library. Or you can use the Search function to search available maps by entering a keyword.
Create Customized Topology	Create a customized diagram with respect to organization, site, or network.
Toolbar	 Refresh: Refresh the screen display. Device List: Displays the Device View menu for the selected topology. Link List: Displays the Connection View page with the connecting interfaces. Network Overview: (1) Displays the distribution of the devices with respect to model, device type and status. (2) Displays the distribution of the devices with respect to bandwidth and status. Export: Save the map as a PNG file to your local drive. Topology Settings: Change the current topology's information settings and layout style. Also select the information to be displayed alongside the devices. Rediscover: Scan the devices on the map to update the link information. Display Settings/Current Topology Setting: Control what should be displayed for the nodes and links on the map. Control the topology layout and central device. Link Edit: Enable or disable the link editing function. Enable this option and right-click on a link on the map to edit or delete it. Or you can right-click on a node to delete it. Disable this option to create link lines on the map. Add Background: Add a background image to the map. Save: Save the current topology map.
Search	Click to search specific devices.
Control Bar	 The following is a description of the control bar icons from left to right. Zoom in Zoom out Focus on central node Zoom fit
Help	Help menu provides the following operation guidance: Topological Legend: the state/status, device type, and bandwidth representation explanation Link Operation: select a link to edit or delete Batch Select Nodes: select multiple nodes

3. From the Topology Map, select a device. When selected, the device will be highlighted.



4. Click on a device to display the device's information page in Link Edit mode ( ).



5. The Information page provides the following information:

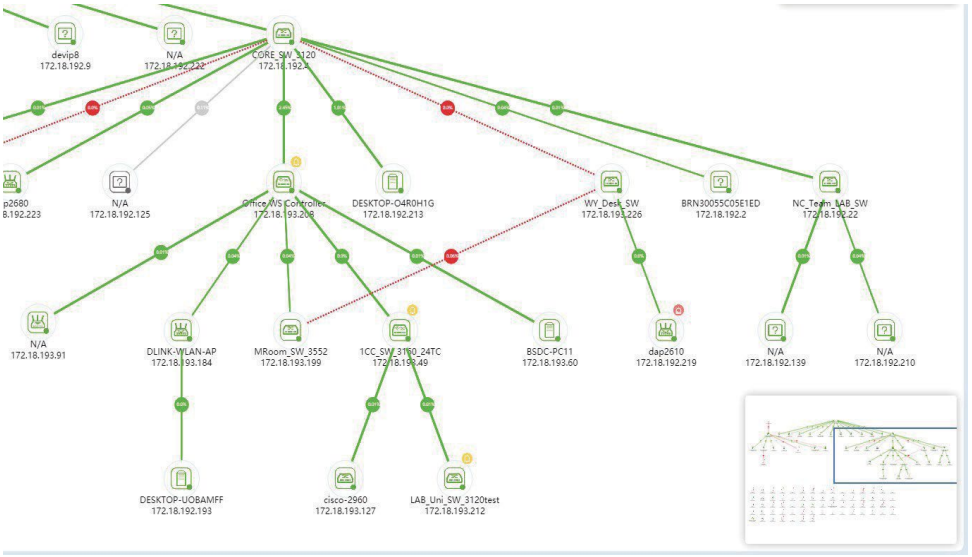
- Device Information: Name, Status, Network, IP Address, MAC Address, Type of the device, and Model Name.
- Recent 3 Active Alarms
- Performance: CPU utilization, availability, and memory utilization
- Related Devices: Connected devices' information
- Related Topology: Other topology from connected devices
- To modify device information, click the Device Name link to open the Device Information page.

6. To view details for a link, click on a link to display the Link Information page in Link Edit mode ( ).

7. The Information page provides the following:

- Link Information: devices that establish the link with link type and number of links
- Link Port: linked ports of the device, bandwidth, utilization and Rx/Tx rate
- Link Alarm: alarms generated for this link activity
- To edit a link, right-click on a link and click Edit Link. You can modify the type of link (Normal, LACP, or logical) and the ports of the link. Normal link uses wires and cables for physical data flow whereas logical link shows data flow regardless of the physical connections among the devices in the network. For LACP link, check the Device Information page for LACP support and configuration.

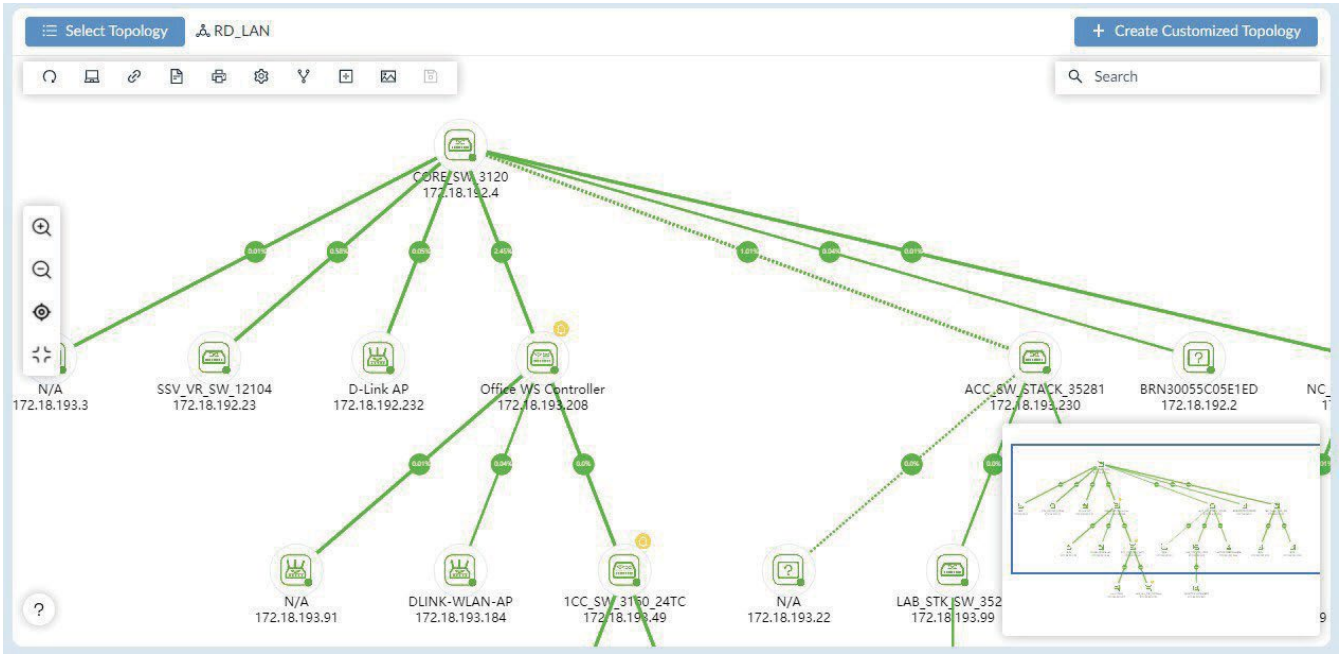
8. You can also use the navigation window at the lower right to focus an area on the map.



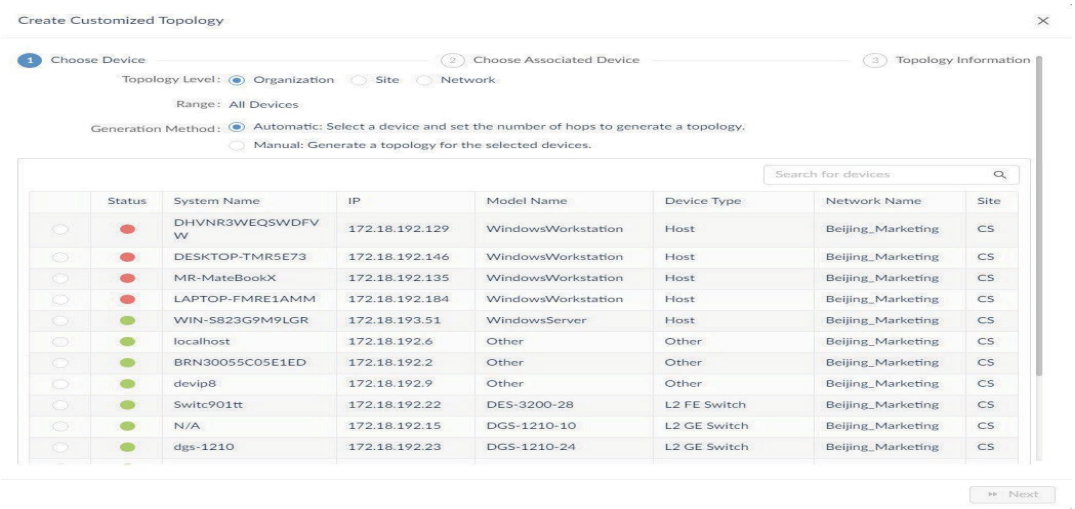
Create a Topology View

In addition to system-built topologies, you can create your own topology within a network hierarchy.

1. Go to **Monitoring > Topology Map**. The Topology Map page displays.



2. Click **Create Customized Topology** at the upper right. The Create Customized Topology page displays.



3. Select the Topology Level to choose devices from: Organization, Site, or Network.

4. Select the method to generate the diagram.

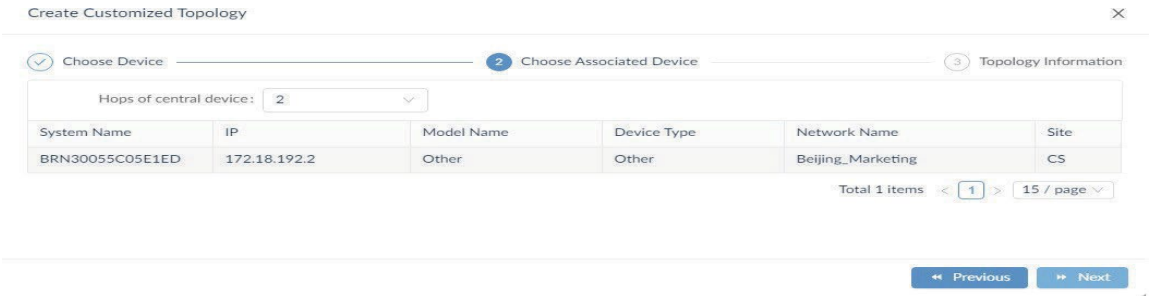
Automatic (default): select a device and set the number of hops to generate the topology.

Manual: generate a topology for the selected devices.

5. For manual, select device(s) to be included in the topology architecture. Or you can search for specific device(s) by entering a keyword in the search field.

6. Click **Next** to proceed.

The Choose Associated Device page displays if you select Automatic.



7. Click the **Hops of central device** drop-down menu to define the number of hops or devices (2 to 10) of a single link from the central de vice down to add additional devices in the diagram. This is only available if the Automatic method is selected above.

8. Click **Next** to continue or click **Previous** to return to the previous menu. The **Topology Information** page displays.

9. In the Name field, enter a name for the topology map.

10. In the Description field, enter a description to identify the map.

11. In **Data source of links**, select either **Synchronization with system** or **User-defined** to specify whether the data will be dynamically updated with the system. The user-defined type will not update dynamically with the system when there is any topological change with the nodes and links in the system.

12. Select the type of layout for the map: Star, Tree, Circular, or Grid.

13. Enable or disable sharing of the topology with other administrators so they may also view or modify it.

14. Enable or disable the **Auto** button to control the selection mode of the central device for display as the central device in the topology. ON indicates the system will specify the central device automatically. (The system will select the device having the greatest number of links as the central device.) If OFF is selected, choose a central device manually.

15. Select a central device if you disable the above Auto option.

16. Click **Save** to create the topology map. Click **Previous** to return to the previous menu.

You can modify the information of a customized topology or delete a customized topology. Click Select Topology at the upper left, select Customized Topology, select the desired topology, then click Edit or Delete .

Reports

Reports are available as either built-in templates or customized ones. They can be generated once only or repeatedly according to a recurrence pattern.

Generate Scheduled Reports

Scheduled reports can be generated through existing report templates. You can also create time-based reports to designate a date and time for a recurrent schedule.

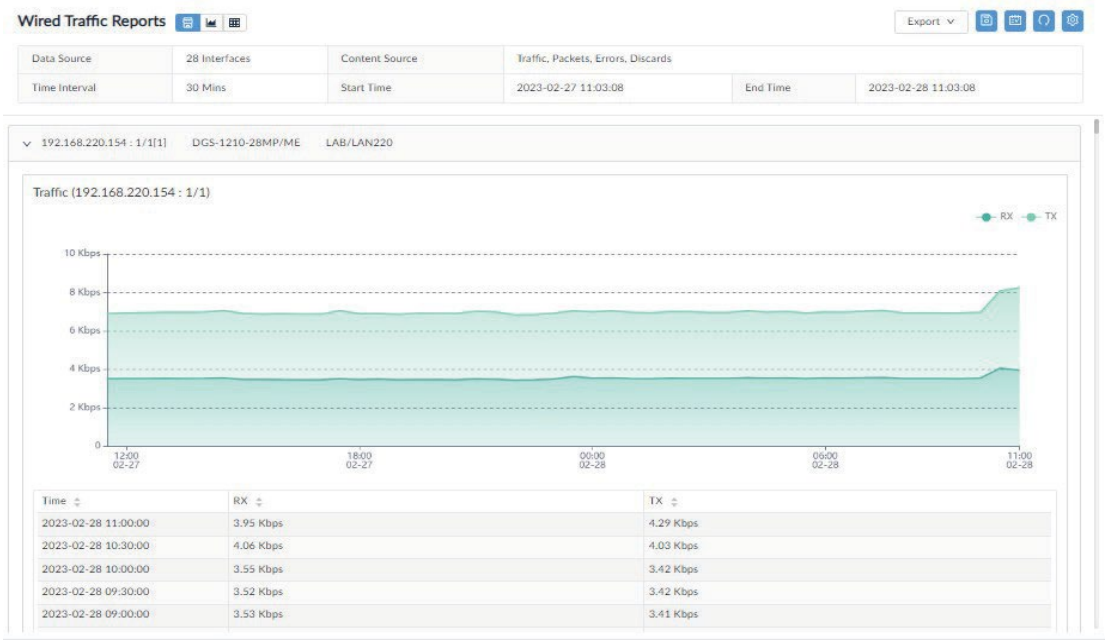
To generate a scheduled report:

1. Go to **Reports > General Reports** to display the General Reports page.

In order to create a scheduled report, an existing report must be present. See the below **Add a Report** section for further information.

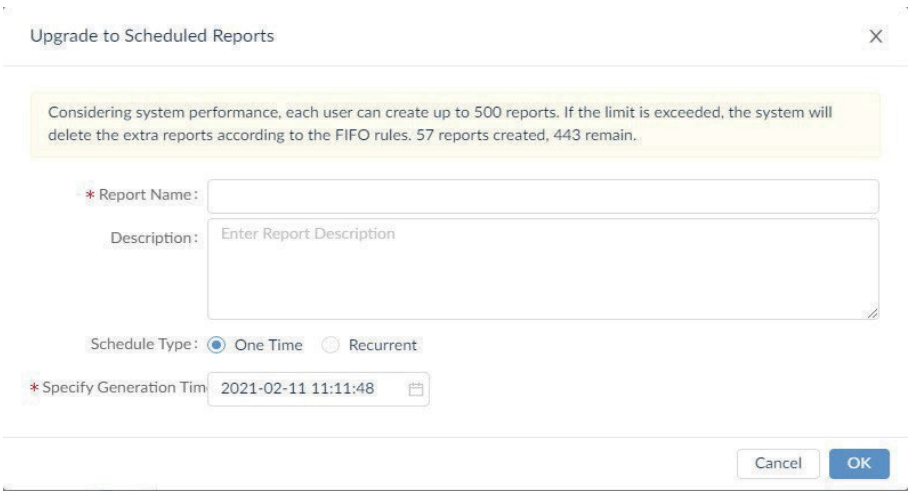
2. Select a specific category from the reports list: Device Reports, Wired Interface Reports or Advanced Reports.

The example below uses Wired Traffic category for demonstration.



3. At the top right, click **Upgrade** to Scheduled Reports.

The Upgrade to Scheduled Reports page displays.



NOTE: A maximum of 500 reports per user can be created to maintain optimal system performance. When the maximum is reached, older reports will be deleted.

4. Enter the required information:

- Report Name: enter a name for the report
- Description: enter a description to identify the report
- Schedule Type: select the scheduling method for the report, One Time or Recurrent.

For recurrent schedule, select a pre-defined schedule from the Schedule list or click Add Schedule to define a new schedule by selecting the frequency and effective duration to create reports:

Specific Days: Executes the report task a single time or multiple times for a single day at a specified date(s)/time(s). Choose times for a day and specify dates.

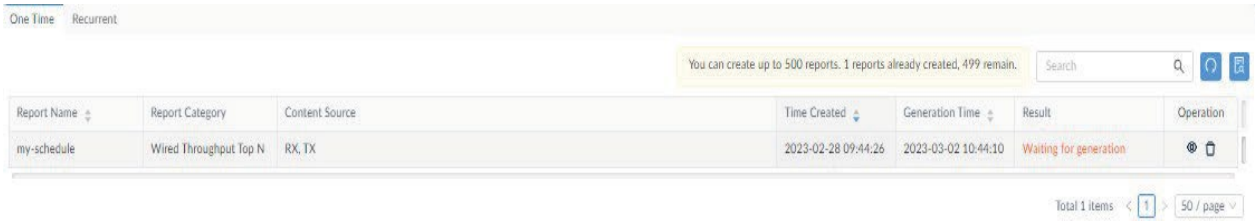
Daily: Executes the report task at a specified time or different times of the day. Choose daily interval between executions: 1 to execute the task every day, 2 to execute the task every other day, and so on.

Weekly: Executes the report task at a specified time or different times of a designated weekday or weekdays. Choose weekly interval between executions: 1 to execute the task on the specified weekday every week, 2 to execute the job every other week, and so on.

Monthly: Executes the report task at a specified time or different times on designated day or days of the month. Specify a month or months: Jan to Dec and the days of the month.

5. Click **OK** to configure the scheduled report or click **Cancel** to return to the previous menu.

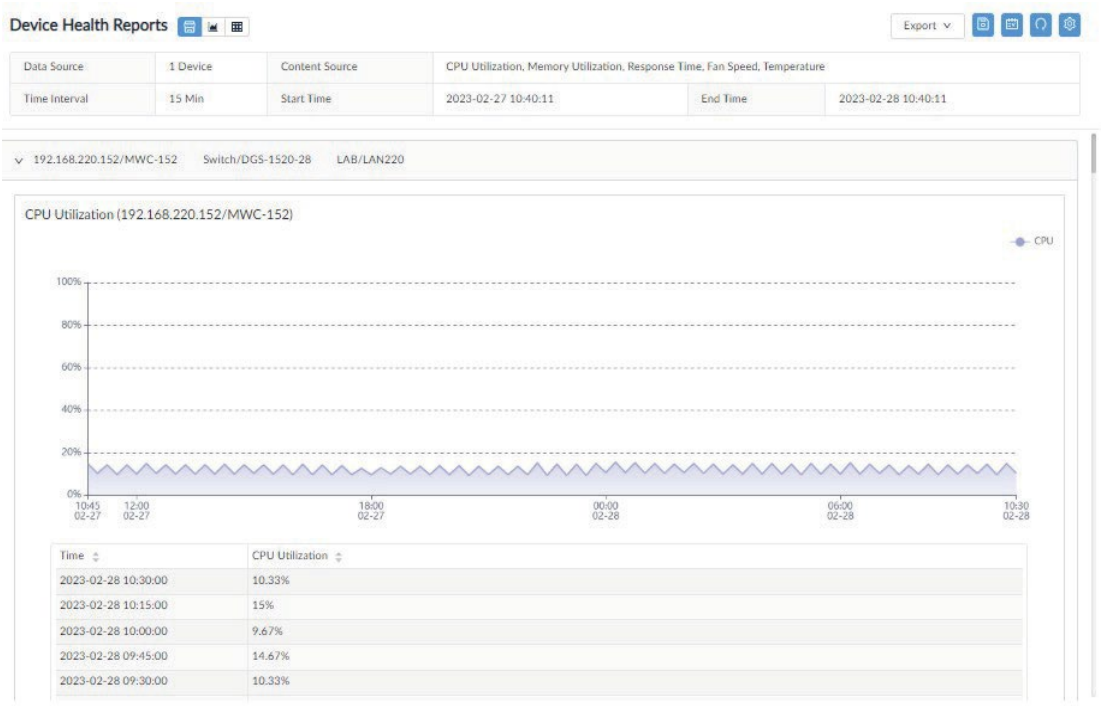
Select **Scheduled Reports** under the Reports menu to view the added report. If the report is defined as One Time, it will be listed under the **One Time** tab. If it is recurrent, click the **Recurrent** tab to view the report.



Manage Report Templates

The NMS provides built-in report templates for the supported devices to accommodate a variety of monitoring and reporting cases.

The following table shows the menu of the default templates along with the types of reports available.



Report	Type	Category
General Reports	Device Reports	Device Health: CPU Utilization, Memory, Utilization, Response Time, Fan Speed, and Temperature. Trap: trap event reports Syslog: syslog message reports Device Top N: shows the top 10 device statistics of the selected devices with respect to the following performance indicators: CPU Utilization, Memory Utilization, Response Time, Tx/Rx traffic, Trap and Syslog messages.
	Wired Interface Reports	Wired Traffic: shows statistics of Rx and Tx traffic for all interfaces of the selected devices.
		Wired Throughput Top N: shows the Rx/Tx traffic statistics of the top 10 device ports of the selected devices
	Advanced Reports	Inventory: shows the distribution of the selected devices with respect to device category and model.
Scheduled Reports	One Time Reports	An automatic report generated at a specified time.
	Recurrent Reports	An automatic report generated repeatedly at specified times.

The following demonstrates how to generate a Syslog report using the template provided:

1. Click **HERE** on the page to configure a new report.

2. Select devices from the device list. Note that the managed devices must have NMS configured as a Syslog Server for NMS to collect logs (go to **Monitoring > Device View** and select the **System Name** link to open the Device Information page. Then click the **Management** tab to find the Trap and Syslog status switch).

3. Configure duration by clicking the drop-down menu to determine the timespan of the report: last hour, last 6/12/24 hours, today, yesterday, last 7 days, this week, last week, last 30 days, this month, last month, or customized. For customized, select the Start/End date and time.

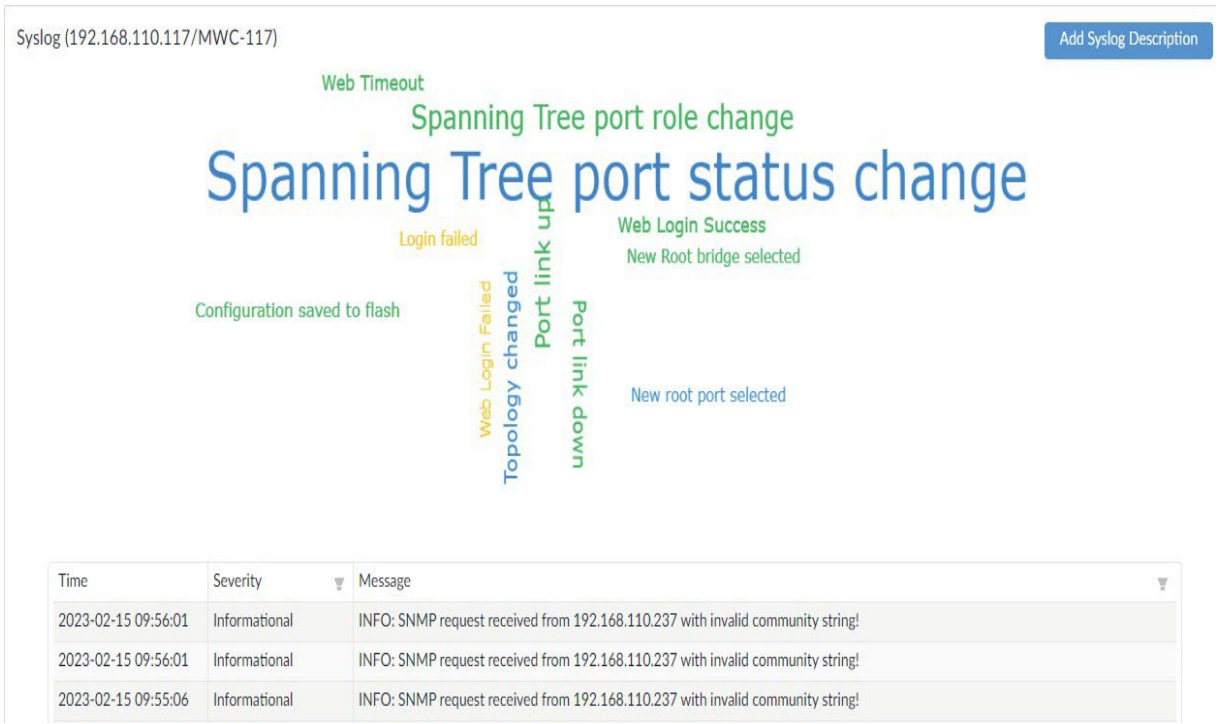
4. Click **Save** to display the generated report. Or click Reset to clear setting entered.

5. The buttons next to **Syslog Reports** control the representation of the report: show chart or table or both.

6. The **Add Syslog Description** button at the top right can be configured to represent a selected syslog message using descriptive text in the chart along with the number of occurrence and severity level. Hoover over a defined syslog description to display related information.

7. To add a syslog description, click **Add Syslog Description**. Enter a description that will be displayed as highlight text associated with matching keywords of the logs to signify a particular logged event. Then click **Save**. The new description entry will also be listed in **Alarm & Notification > Trap & Syslog Editor > Syslog Editor**.

8. The following shows the display of the syslog report using Syslog Description. Note that the larger the text, the higher the occurrence of the defined system log.



The Trap report also displays highlight text of OID description to signify trap events.
Refer to Trap Editor for more information.

Add a Report

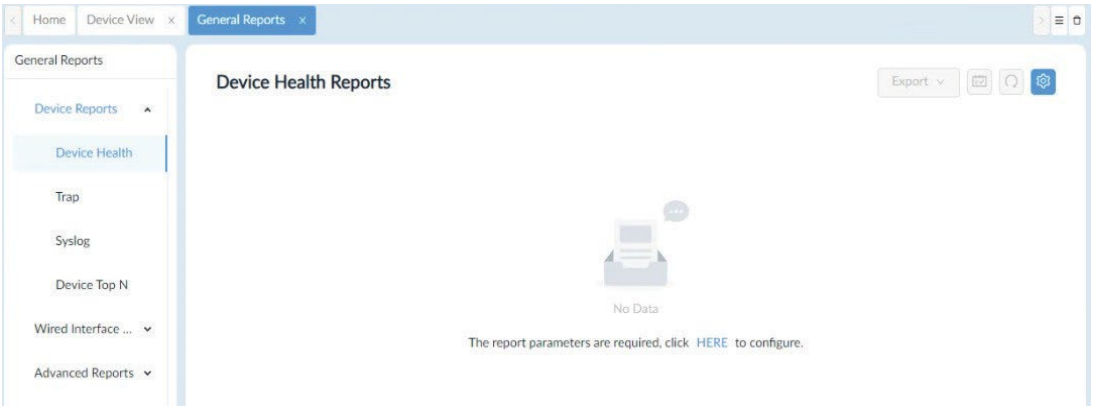
There are numerous templates for different reporting and summary purposes. By selecting a template, you can easily generate reports to help you maintain an effective network.

To select a report template or modify an existing one:

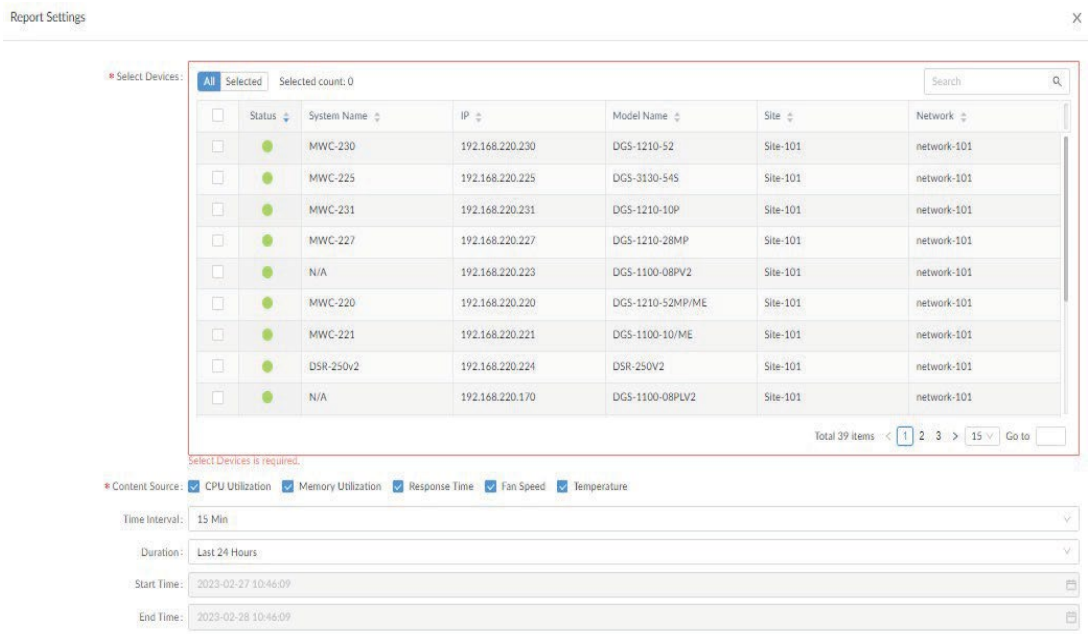
1. Go to **Reports > General Reports** to display the General Reports page.

2. Select a specific category from the reports list.

The following demonstration uses the Device Health Reports.



3. Click **HERE** to configure report settings.

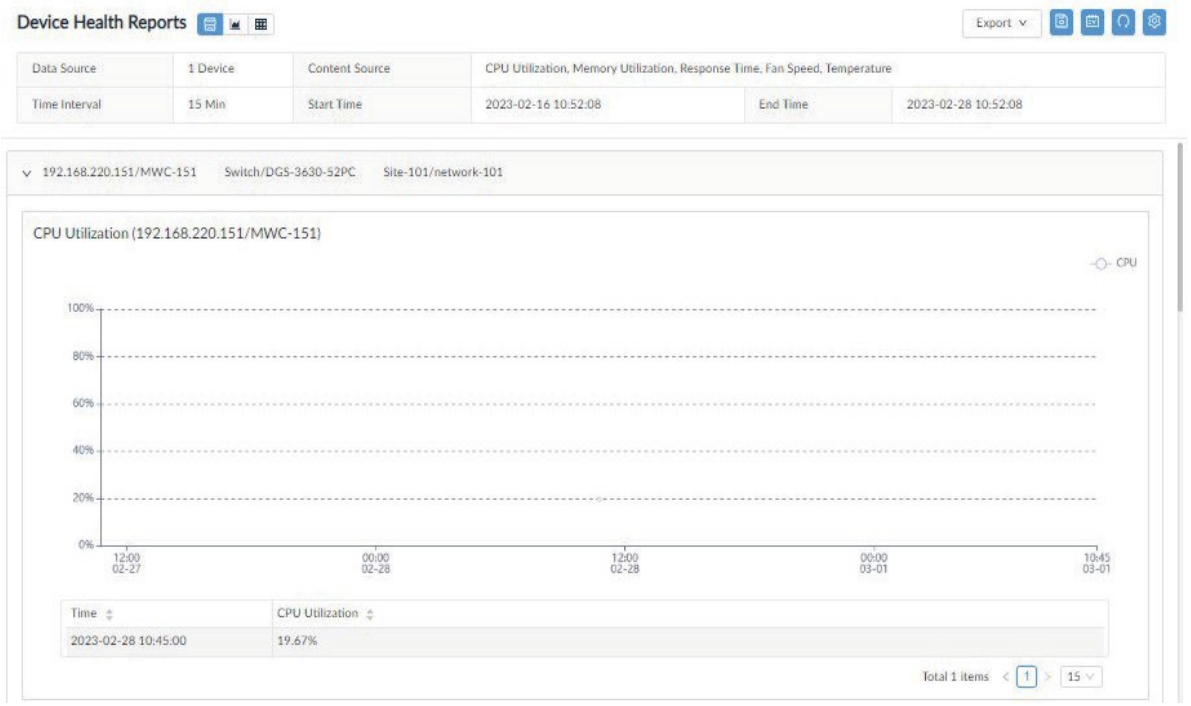


The Report Settings page displays.

4. Configure the following:

Item	Description
Select Devices	Scroll through the list to select devices or use the Search field to filter the list by System Name, IP, Model Name, Site or Network. Up to 15 devices can be selected for a single report in this category.
Content Source	Click to select the type of report data: CPU Utilization, Memory Utilization, Response Time, Fan Speed, or Temperature.
Time Interval	Select the interval for the data: 15 min, 2 hours, 8 hours, or 1 day
Duration	Click the drop-down menu to determine the timespan of the report: last hour, last 6/12/24 hours, today, yesterday, last 7 days, this week, last week, last 30 days, this month, last month, or customized.
Start Time	Set the starting date if customized duration is selected.
End Time	Set the ending date if customized duration is selected.
Note: The configurable settings vary depending on the type of report.	

5. Click **Save** to create the report or click **Reset** to clear settings entered.



You can then view the report data in the default format, chart, or table by using the control buttons 

Modify a Report

A report can be removed without deleting the template. However, the data generated by the report is deleted. We recommend that you save the reports using the Export function before deleting them.

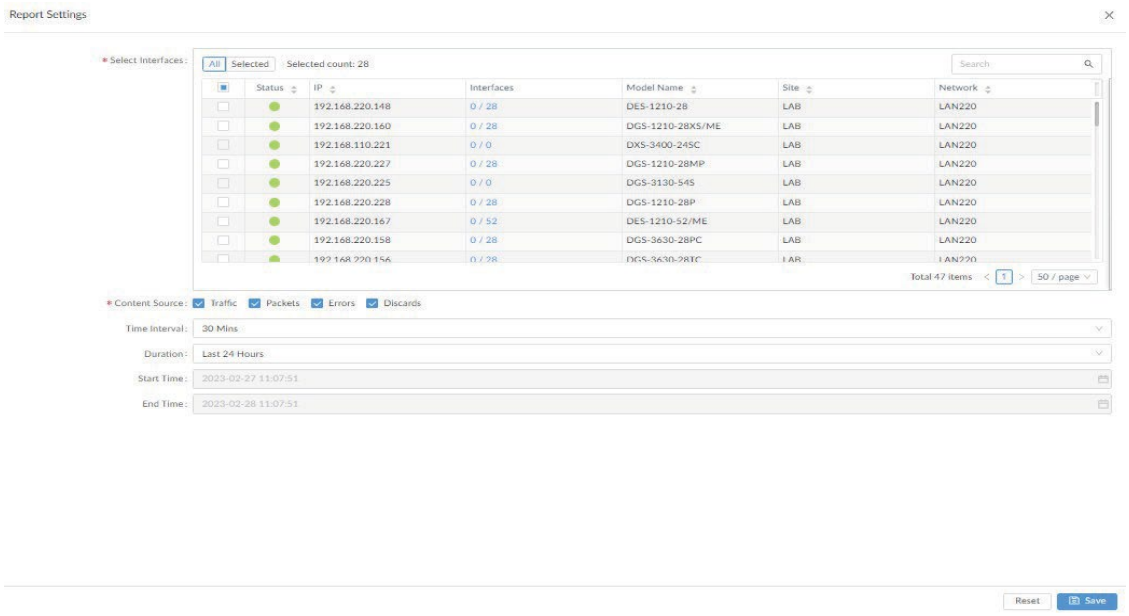
To delete or modify an existing report:

1. Go to **Reports > General Reports** to display the General Reports page.

2. Select a specific category from the reports list: Device Reports, Wired Interface Reports or Advanced Reports.

3. For demonstration, the Device Health category is selected and the existing report is also displayed.

4. Click **Report Settings** at the top right. The Report Setting page displays.



5. To modify the current report, re-configure the settings and click Save.

6. To clear all settings, click **Reset**. The report and the data will be removed from the General Reports page.

View and Remove Reports

All reports can be viewed for the period they are retained. Reports can also be removed.

To remove a Scheduled Report:

1. Click **Scheduled Reports** to view the list of scheduled reports.

2. Select the One Time or Recurrent tab.

3. Under **Operation,** click the **View report** or **Delete this report** to view or remove the report.

System Settings

You can configure global settings to be used for system-wide management and communication in the following areas:

- Organization
- Forward Trap
- Forward Syslog
- SNMP/WMI/Telnet Credentials
- System Preferences

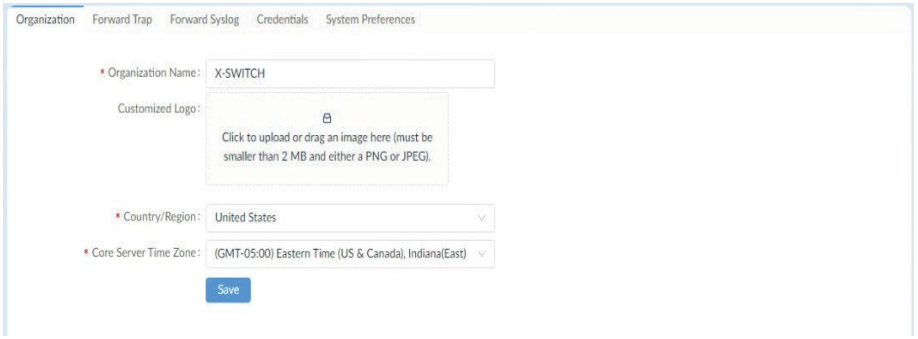
Configure Global Settings

Set Up Organization

The organization information is located under the Basic Settings menu. You can define the time zone, location, and name in the basic settings. The Organization information is required for Network Discovery and subsequent display of network architecture.

To set up organization information:

Go to System > Basic Settings.



1. Define the following information:

Item	Description
Organization Name	Enter the name to define the organization.
Customized Logo	Select an image to upload, which must be less than 2 MB in JPEG or PNG format.
Country/Region	Select the location of the organization.
Time Zone	Select the time zone corresponding to the specified location.

2. Click **Save**.

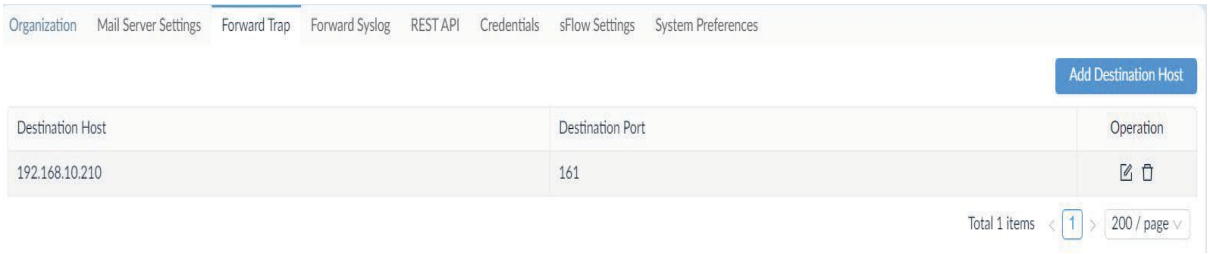
Set Up Forward Trap

X-SWITCH provides SNMP trap forwarding with the Forward Trap function. The function allows you to forward traps to a specified server destination.

To configure Forward Trap:

1. Go to **System > Basic Settings**.

2. Click the **Forward Trap** tab to display the Forward Trap page.

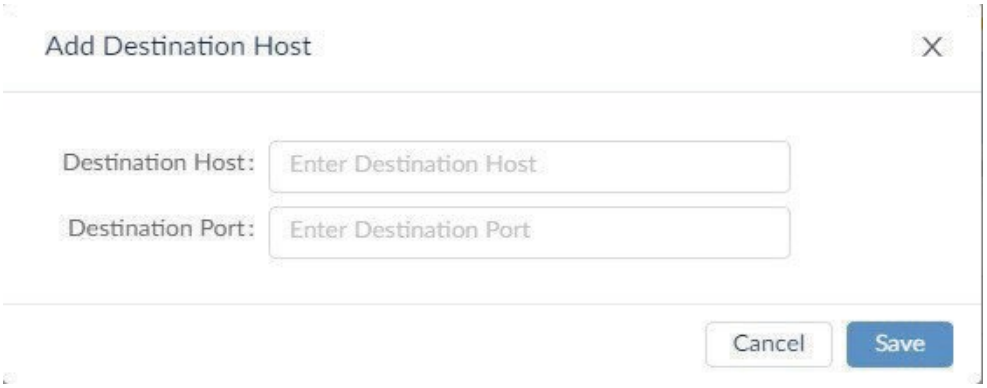


3. Click **Add** Destination Host. Then enter the destination host (IPv4 or IPv6 address) and port to define the trap destination.

4. Click **Save**.

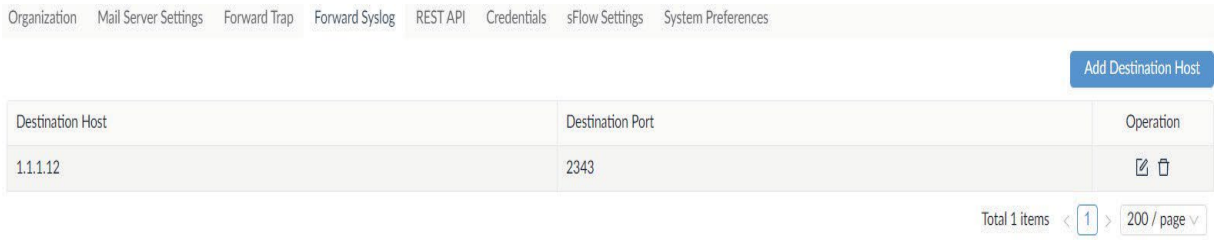
Set Up Forward Syslog

You can configure the system to send syslog messages to an external syslog server.
To configure Forward Syslog:



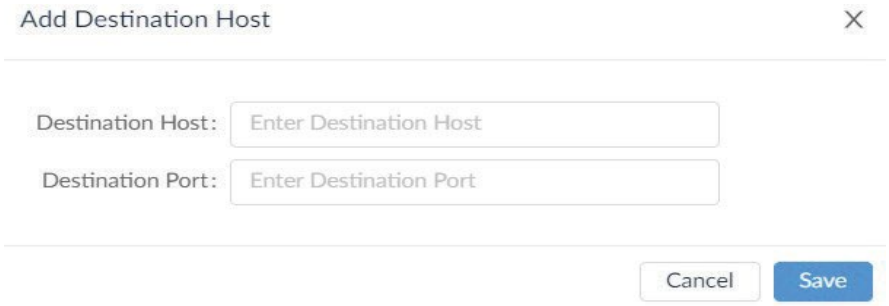
1. Go to **System > Basic Settings**.

2. Click the **Forward Syslog** tab to display the Forward Syslog page.



3. Click **Add** Destination Host. Then enter the destination host (IPv4 or IPv6 address) and port to define the syslog destination.

4. Click **Save**.



Set Up Credentials

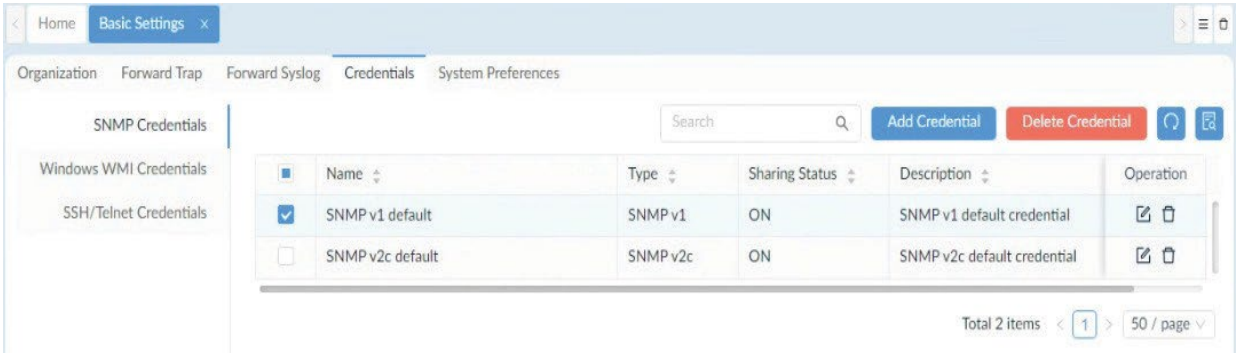
Set Up SNMP Credentials

The SNMP credentials manage access to SNMP-compatible devices. Storing the credentials is useful for when the system is scanning network devices in Network Discovery (go to **Monitoring > Network Discovery**). Refer to Network Discovery for more information about Network Discovery.

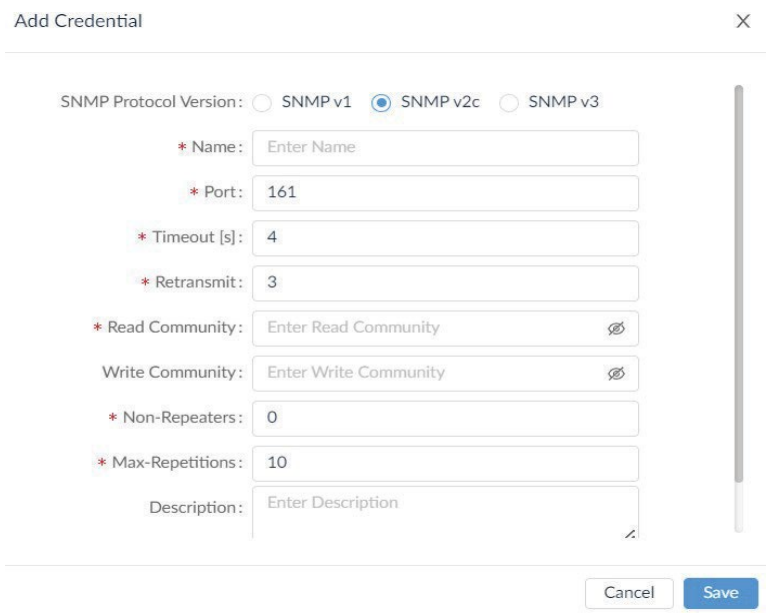
To configure SNMP credentials:

1. Go to **System > Basic Settings** to display the Organization page.

2. Click the **Credentials** tab and select **SNMP Credentials** from the left pane.



3. Click **Add Credential**.



4. Select the SNMP version of the credential: SNMP v1, SNMP v2c, or SNMP v3. By default, NMS uses SNMP v2c.

For SNMP v1:
- Enter a name and port for SNMP.
- Enter the timeout period in seconds (default: 4).
- Enter the number of retries (default: 3)
- Enter the read credential string (default: public).
- Enter the write credential string (default: private).
- Enter a description to help identify the profile (optional).
- Enable or disable **Sharing Status** to let other administrators with authorized role to view and edit this SNMP setting.

For SNMP v2c:
- Enter a name and port for SNMP.
- Enter the timeout period in seconds (default: 4).
- Enter the number of retires (default: 3)
- Enter the read credential string.
- Enter the write credential string.
- Enter the number of objects that can return in a single get-next instance (default: 0).
- Enter the number of Get Next operations to be performed on each variable (default: 10).
- Enter a description to help identify the profile (optional).
- Enable or disable **Sharing Status** to let other administrators with authorized role to view and edit this SNMP setting.

For SNMPv3:
- Enter a name and port for SNMP.
- Enter the timeout period in seconds (default: 4).
- Enter the number of retries (default: 3)
- Enter the number of objects that can return in a single get-next instance (default: 0).
- Enter the number of Get Next operations to be performed on each variable (default: 10).
- Enter the Context Name (optional), which is used as the identifier for a named subset of the object instances.
- Select the Security Level:
  - authPriv: authentication and privacy (default).
  - authNoPriv: authentication, no privacy.
  - noAuthNoPriv: no authentication, no privacy.
- Select the Auth Protocol if authentication is used:
  - MD5 (MD5 message-digest algorithm): produces a 128-bit hash value to authenticate users.
  - SHA (Secure Hash Algorithm): produces a 160-bit has value to authenticate users.
- Enter the Authentication Password to be used with the Authentication Protocol.
- Select the Privacy Protocol if privacy is used:
  - DES (Data Encryption Standard) or AES (Advanced Encryption Standard) for data encryption.
- Enter the Privacy Password to be used with the Privacy Protocol.
- Enter a description to help identify the profile (optional).

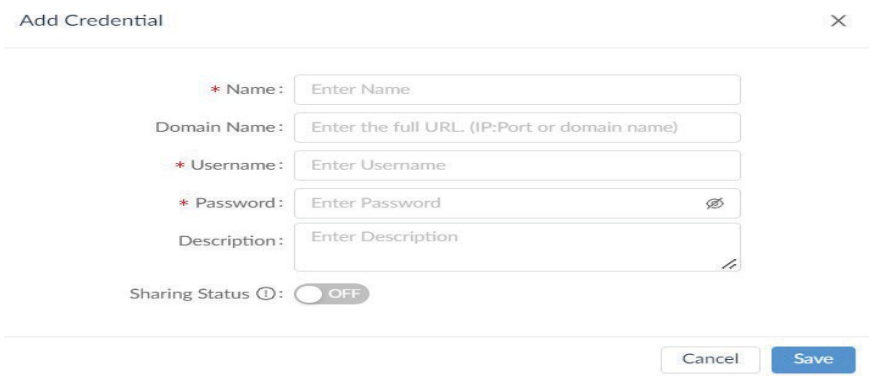
6. Enable or disable **Sharing Status** to share the credentials with other administrators with authorized roles.

7. Click **Save**.

Set Up Windows WMI Credentials

Windows Management Instrumentation (WMI) is used in Microsoft Windows systems to help retrieve information on a remote system and it requires appropriate permissions. Storing the credentials is useful when discovering network devices in Network Discovery (go to **Monitoring > Network Discovery**).

Enter the following to add a WMI credential profile:



Name: Enter a name for this profile.

Domain Name: Enter the windows domain name.

Username: Enter the username with the Windows system administrator privilege or a user account with permissions to access WMI data.

Password: Enter a password for the above user account.

Description: Enter a description to help identify this profile.

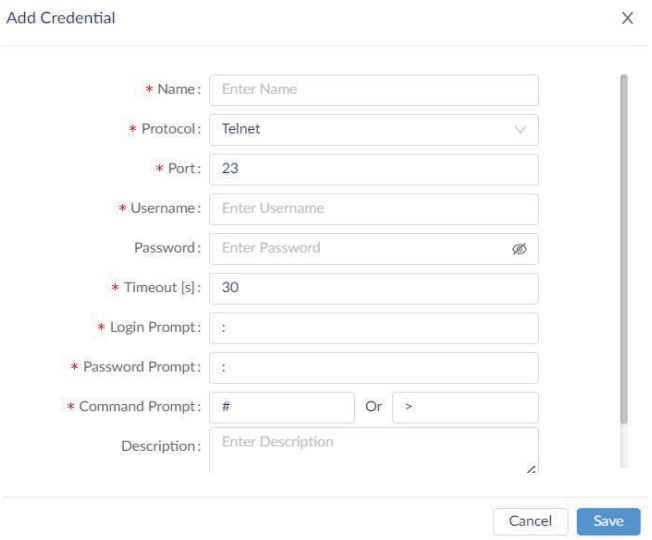
Sharing Status: Select whether other administrators with authorized roles in the organization can view or modify this profile.

Set Up SSH/Telnet Credentials

SSH and Telnet allows remote administration of an NMS server and it requires configuration of communication port and access privileges.

Note: This function is not applicable in this release and will be fixed in the future release.

Enter the following to add an SSH/Telnet credential profile:



Name: Enter a name for the profile.

Protocol: select the communication protocol for remote management: SSH or Telnet.

Port: select the associate port for the above protocol.

Username/Password: Enter the username and password that will be required to access the server.

Timeout: enter the session timeout value.

Login Prompt: enter the prompt to be displayed for login.

Password Prompt: enter the prompt to be displayed at the command line for entering password.

Command Prompt: Enter the prompt to be displayed at the command line for entering command.

Description: Enter a description to identify this profile.

Sharing Status: Select whether other administrators with authorized role in your organization can view or modify this profile.

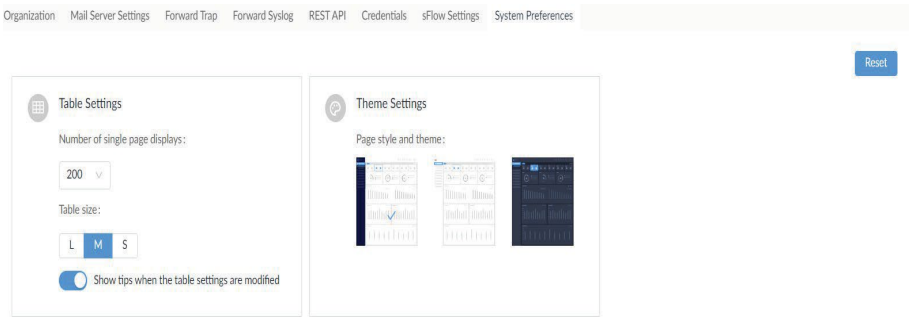
Set Up System Preferences

Theme settings for the overall layout of the interface are configured through System Preferences. You can configure Table and Theme settings to set specific page styles.

To configure System Preferences:

1. Go to **System > Basic Settings**.

2. Click the **System Preferences** tab to display the System Preferences page.

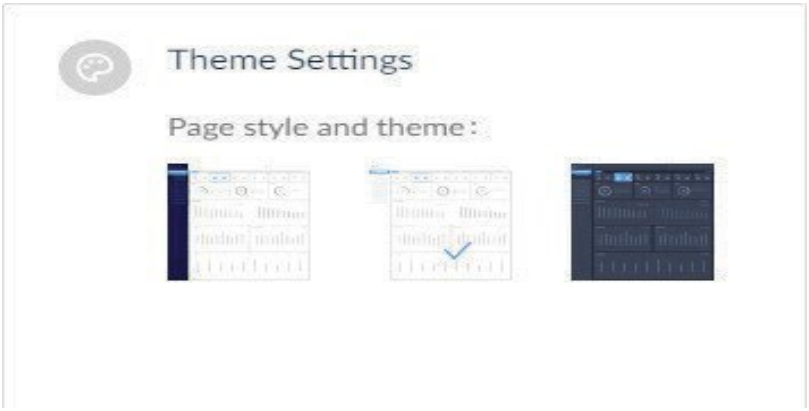


3. Click the drop-down menu to select the number of single page display (rows) for all tables in NMS 50 (default), 100, or 200.

4. From the table size selector, set the size for all the tables in NMS: Large, Middle (default), or Small.

5. Enable the option: Show tips when the table settings are modified so that users will be notified of table setting changes via toast messages.

In **Theme Settings**, select a defined theme to apply to the interface. You can select a dark or light background or dark side pane with light background.



To reset to the original settings, click the **Reset** button. All table and theme settings will be restored to the default.

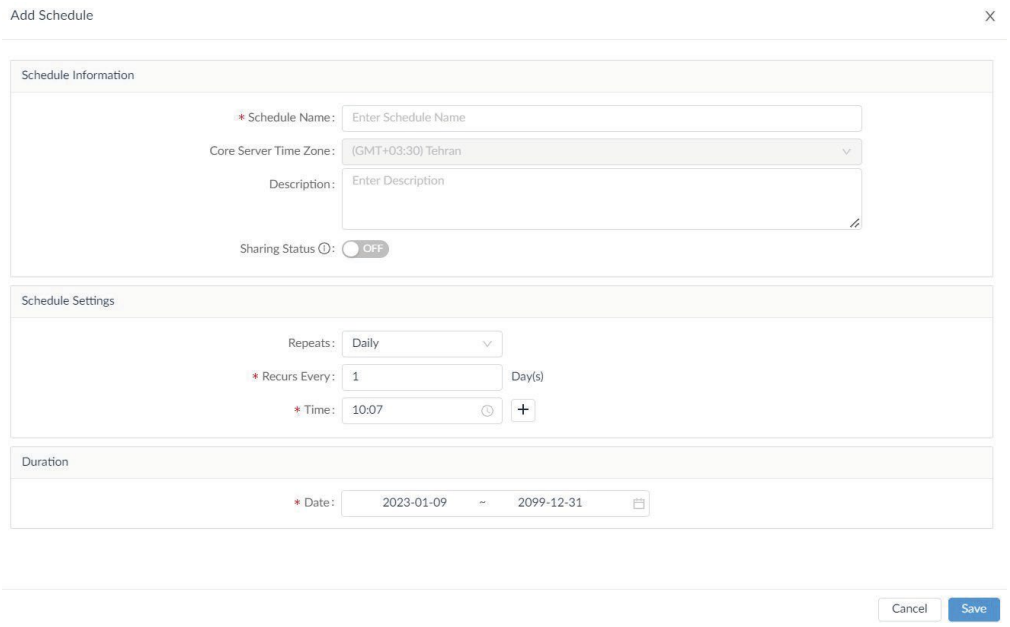
Scheduling

The scheduling function helps automate several functions periodically according to a defined recurrent frequency in the designated time span.

There are two types of scheduling options: Recurrent and Time-Range. The recurrent schedule can be assigned to network discovery, tasks, configuration backup and restore, and scheduled reports, whereas the time-range schedule can be assigned to alarm settings and notification rules.

To set a recurrent schedule:

1. Go to **System > Scheduling** and select the Recurrent Schedule List tab.



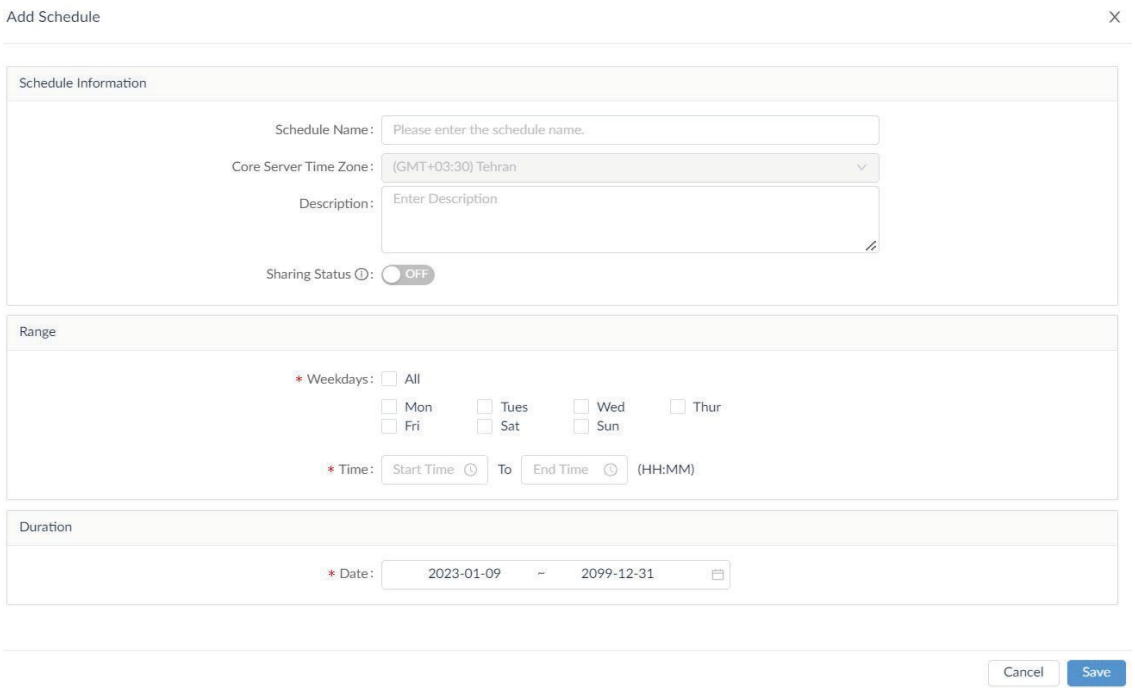
2. Click **Add Schedule** at the upper right. Then enter the following information:

Item	**Description**
Schedule Information	
Schedule Name	Enter a name for the schedule.
Core Server Time Zone	Select the time zone. (It can already be set in the Organization tab.)
Sharing Status	Enter a brief description for the schedule.
Schedule Settings	
Repeats	Select the frequency: Daily, Weekly, Monthly, or Specific Days.
Recurs Every	Specific Days: Schedule a single time or multiple times at a specified date(s)/time(s). Selecting multiple times will enable execution of the same task at different times for each date. Daily: Schedule a specified time of the day. Then choose daily interval between executions: 1 to execute the task every day, 2 to execute the task every other day, and so on. Weekly: Schedule a specified time of a designated weekday or weekdays. Then choose weekly interval between executions: 1 to execute the task every week, 2 to execute the job every other week, and so on. Monthly: Schedule a specified time on day(s) of the selected month(s): specify a month or months: Jan to Dec and the days of the month. Specific Days: Schedule a specified time and date(s).
Time	Select the time (24-hour clock): hh:mm for the schedule. Selecting multiple times will enable execution of the same task at different times of the same day.
Duration	Select the start and end dates to designate the effective time span.

To set a time-range schedule:

1. Go to **System > Scheduling** and select the **Time Range Schedule** List tab.

2. Click **Add Schedule** at the upper right. Then enter the following information:



Item	Description
Schedule Information	
Schedule Name	Enter a name for the schedule.
Core Server Time Zone	Select the time zone. (It can already be set in the Organization tab.)
Description	Enter a brief description for the schedule.
Sharing Status	Enable sharing to let other administrators with the authorized role to modify or view this schedule.
Range	
Weekdays	Select all weekdays or a specific weekday(s).
Time (range)	Select the start and end time (24-hour clock): hh:mm for the schedule.
Duration	Select the start and end dates to designate the effective time span.

View NMS Logs

The NMS Log page displays different types of logs. The User Operation Log tab displays logs related to management operations and tasks performed by users. The System Log displays logs related to activities related to system services and probe agents. The Device Maintenance Log displays logs related to operations performed by users on the managed devices. Logs can be used to analyze device health and troubleshoot network connectivity as well as exam network security. Note that the NMS logs are different from the device syslog, which are logs generated by managed devices (go to **Alarm & Notification > Trap & Syslog**).

Note: You can only view logs pertaining to the activities under your authorized level of network hierarchy.

To view user operation logs, go to **System > NMS Log**. Click the User **Operation Log** tab. The log entries contain the following information:

Item	**Description**
Log Time	The timestamp of the user activity.
Terminal Type	The device and interface used to connect with the NMS server.
User	Username
Operation Object	The object/menu category that the user operated on.
Detail	The detailed activity of the operation.

To view system logs, go to **System > NMS Log**. Click the **System Log** tab. The log entries contain the following information:

Item	Description
Log Time	The timestamp of the system activity.
Log Type	A brief description of server activity.
Server	The affected server and IP address.
Detail	The detailed information about the server activity.

To view device maintenance logs, go to **System > NMS Log**. Click the **Device Maintenance Log** tab. The log entries contain the following information:

Item	**Description**
Log Time	The timestamp of the device operation activity.
Result	The result of the device operation.
Configuration Type	The configuration category of the operation.
Function	The detailed information of the configuration.
System Name	The system name of the device.
Model Name	The model name of the device.
IP	The IP address of the device.
User	The username of the operator.
Site	The network site of the device.
Network	The network of the device.

You can filter these logs by time or activity. To create a filter, click **Advanced Query** at the top right. It allows you to specify the activity with timestamp of the log, function, configuration type, system name, IP address, username, etc. After the displayed records are refined according to the desired criteria, you can export it as a csv file.

Tools

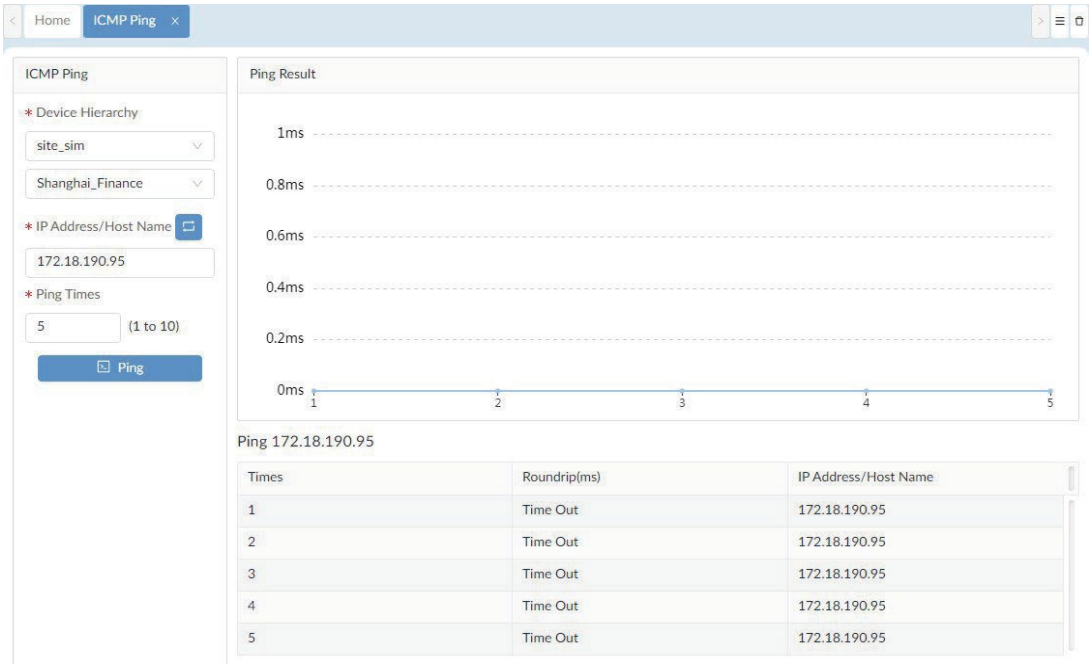
The NMS has added management effectiveness of your network by offering convenient tools. These tools help trouble- shoot network bottlenecks by providing transmission data and responses from nodes where the packets pass.

Perform an ICMP Ping

You can use Ping to diagnose the connectivity between two network devices.

To test a device with the Ping command:

1. Go to **Tools > ICMP Ping** to display the ICMP Ping page.



2. In the ICMP Ping pane, enter the following information to initiate a ping test:

- Device Hierarchy: click the drop-down menu to select site and network.
- Enter the destination host.
- Enter the number of times (1 to 10) to perform the ping test. The default is 5.
- Enter the packet size (in bytes) for the echo request messages. The default is 32.

3. Click **Ping** to initiate the test.

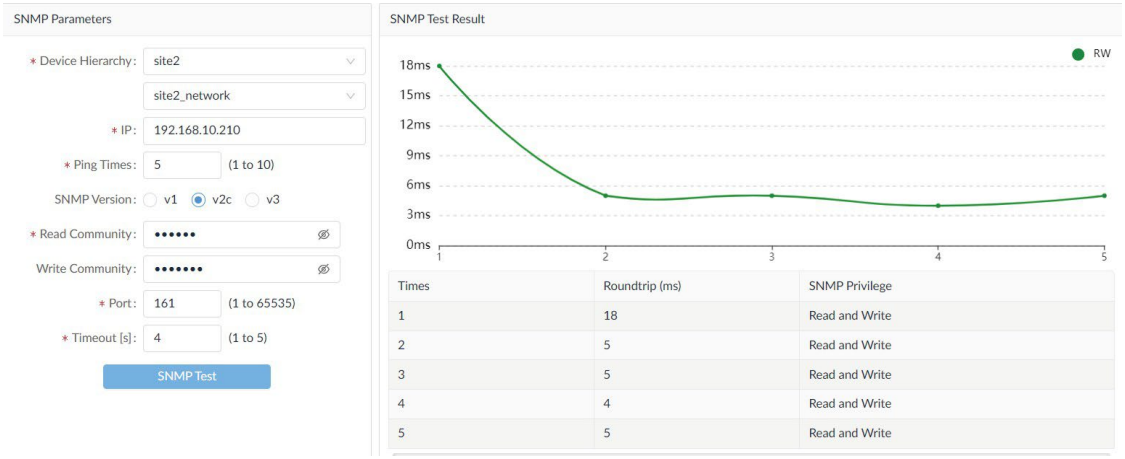
The Ping Result will be displayed on the right:

Perform an SNMP Test

SNMP lets administrators monitor discovered devices, allowing them to solve network problems and identify system health issues. For SNMP Version 1 (SNMPv1), SNMP Version 2c (SNMPv2c) test, you need to specify an SNMP community string. For SNMP Version 3 (SNMPv3), you need to specify username and authentication and encryption (or privacy) settings.

To test a device with SNMP communication:

1. Go to **Tools > SNMP Test** to display the SNMP Parameters page.

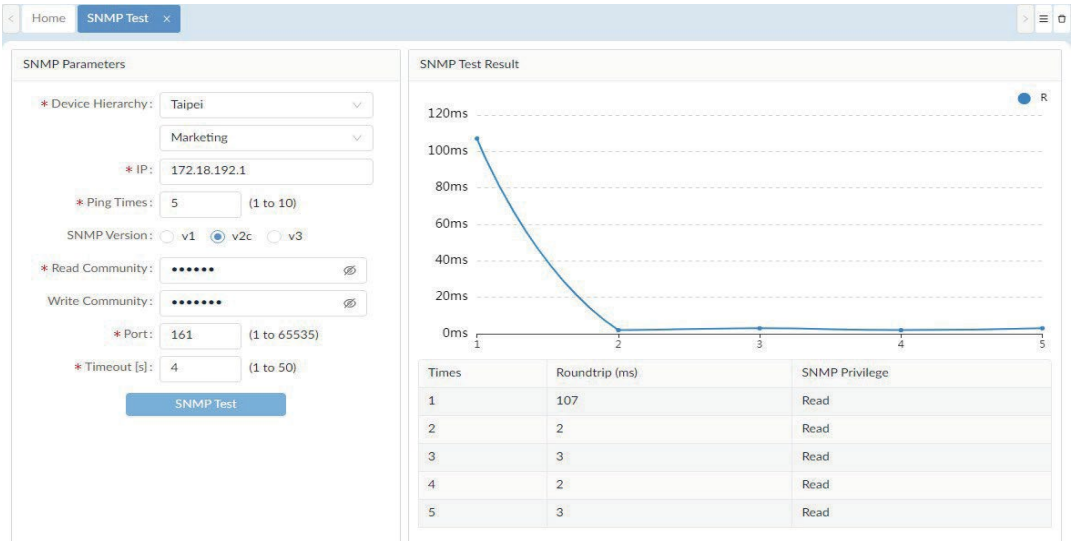


2. From the SNMP Parameters column, enter the following information to initiate an SNMP trap test:

Item	**Description**
Device Hierarchy	Click the drop-down menu to select the site and network of the device for SNMP test.
IP	Enter the device's IP address.
Ping Times	Enter the number of times (1 to 10) to perform the ping test.
SNMP Version	Select the SNMP version: v1, v2c, or v3.
Non-Repeaters (for v3 only)	Enter the number of objects that can be returned in a single get-next instance.
Max-Repetitions (for v3 only)	Enter the number of Get Next operations to be performed on each variable.
Username (for v3 only)	Enter the username for SNMP v3 requirement.
Context Name (for v3 only)	Enter the context name for SNMP v3 if it is used. It defines a named subset of the object instances in the MIB with access control.
Security Level (for v3 only)	Select whether authentication and privacy will be required and select the method accordingly. If authentication is used, enter the appropriate authentication parameters: protocol (MD5 or SHA) and password. If privacy is used, enter the appropriate privacy parameters (DES or AES) and password.
Read Community (for v1 and v2c only)	Specify the read community string.
Write Community (for v1 and v2c only)	Specify the write community string.
Port	Enter the Port number of the target device (1 to 65535, default: 161).
Timeout(s)	Enter the timeout (1 to 5, default: 4) value in seconds.
SNMP Test	Click SNMP Test to initiate the test.

3. Click **SNMP Test** to initiate the test.

The SNMP Test Result will be displayed:

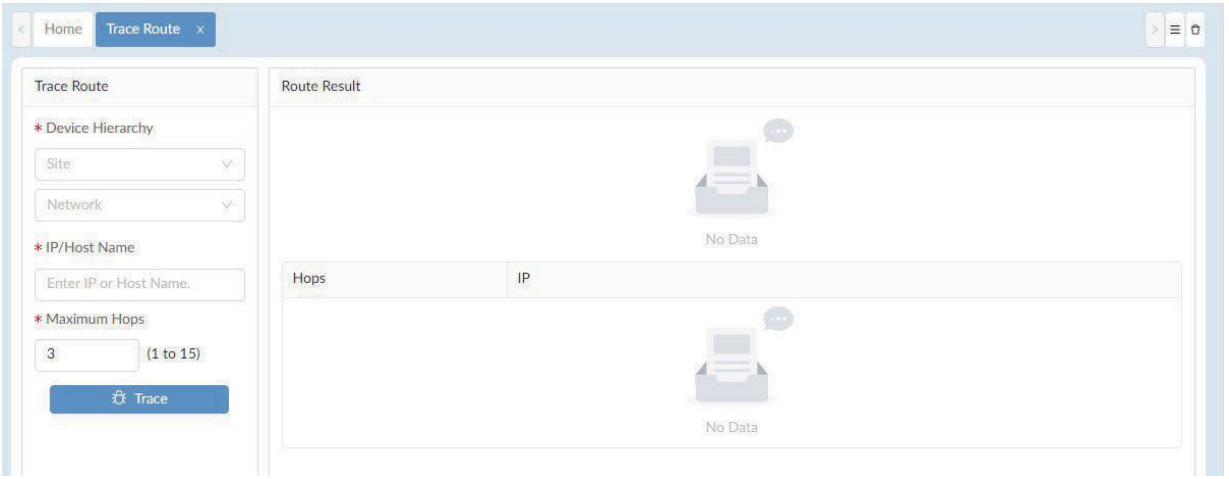


Perform a Trace Route Test

Trace route test diagnoses the path from one device to another.

To test a device by sending a trace route request:

1. Go to **Tools >Trace Route** to display the Trace Route page.

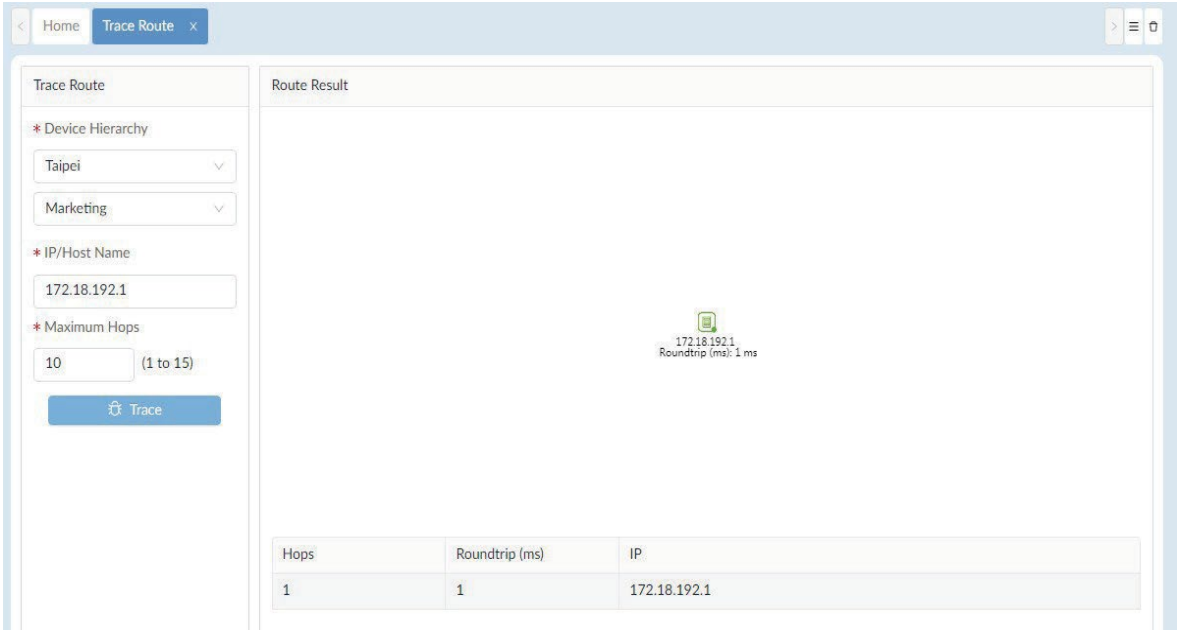


2. In the Trace Route pane, enter the following information to initiate a trace route test:

- Device Hierarchy: click the drop-down menu to select site and network.
- Enter the destination host.
- Enter the maximum number of routers that a trace route packet can pass (1 to 15).

3. Click **Trace** to initiate the test.

4. The Route Result displays as follows:



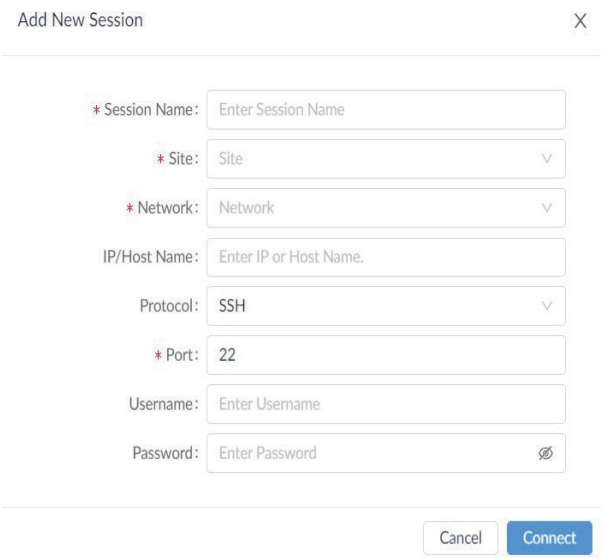
Configure Network Management from CLI

The NMS interface is designed with access through command line interface for network configuration and management. To add a new session:

1. Go to **Tools > CLI** to display the Session List page.

2. In the Session List pane, click **Add New Session**.

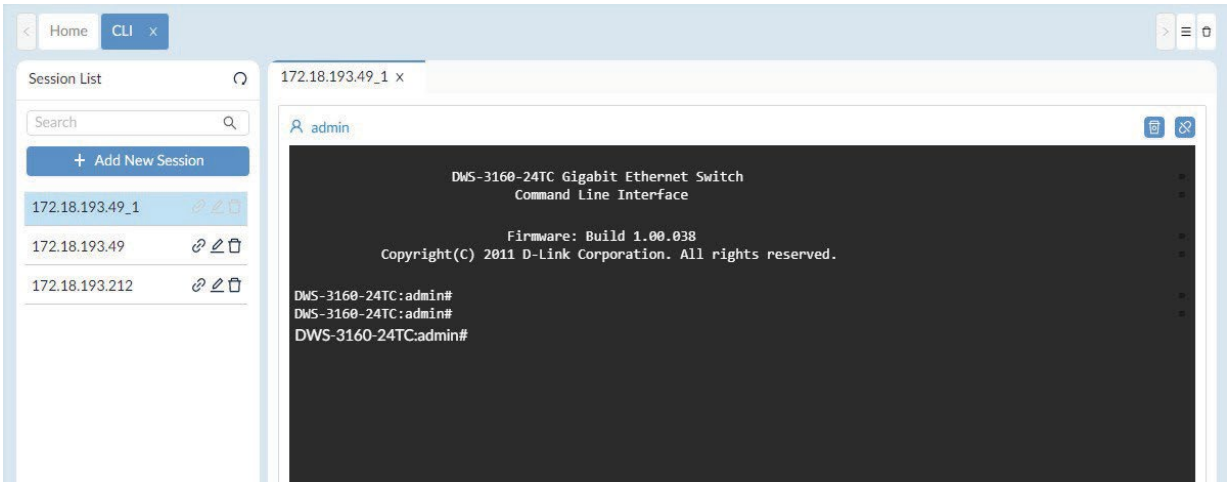
3. The **Add** New Session page displays.



4. Enter the following information to configure a CLI connection:

Item	Description
Session Name	Enter a name to define the CLI connection.
Site	Click the drop-down menu to select the desired site.
Network	Click the drop-down menu to select the desired network.
IP/Host Name	Enter the IP address or host name of the device to connect to.
Protocol	Click the drop-down menu to select the access protocol (SSH/Telnet).
Port	Enter the port number for the respective service (Telnet or SSH).
Username	Enter a username with authority to access the device.
Password	Enter the password of the user account.
Cancel	Click to Cancel the session entry.
Connect	Click Connect to start the session.

5. Click **Connect** to start the connection. Click Cancel to cancel the connection request. The CLI Connection will be listed in the Session and open in the connection pane.



6. For each connection setting, you can modify or remove it from the connection list, click on the available options.

- Connect: initiate a connection
- Edit: modify the settings
- Delete: remove the entry from the list