D-Link

2025 | Business Class Networking

# NUCLIAS NETWORK CONTROLLER
# DNH-1000 User Manual

V 1.00

nuclias connect

# Table of Contents

# Introduction

Nuclias Connect is D-Link's centralized management solution for business networks. Nuclias Connect makes it easier to analyze, automate, configure, optimize, scale, and secure your network — delivering the convenience of an Enterprise-wide management solution, at an SMB price. Nuclias Connect gives you the financial and technical flexibility to expand from a medium-sized network to a larger one, while retaining a robust and centralized management system. And with its intuitive Graphical User Interface (GUI), a wealth of enhanced AP features, and a setup wizard that supports multiple languages, Nuclias Connect minimizes the hassle of deployment, configuration, and administration tasks.

The DNH-1000 Nuclias Network Controller is a hardware controller with pre-loaded Nuclias Connect software. It is designed to support small-to-middle business or enterprise environments by providing network administrators with the capability to manage D-Link DAP series access points and switches through a single platform. The Nuclias Network Controller can currently manage up to 500 devices per unit, with the potential to extend support to other Nuclias Connect products in future firmware updates.

# Product Overview

## Package Contents

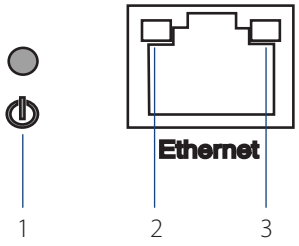
- DNH-1000 Nuclias Network Controller
- 12V/2A power adapter
- Quick start guide
- Foot pad(s)

## System Requirements

- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet Adapter
- Microsoft Edge, Safari 7, Firefox 28, or Google Chrome 33 and above (for configuration)

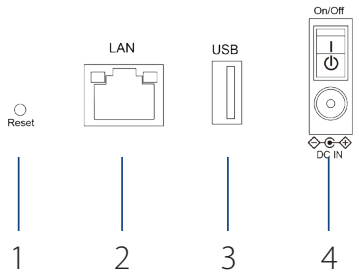
# Hardware Overview

## LED Indicators




| # | LED | Description |
|---|---|---|
| 1 | Power | Solid Green - Power on completed and NC management system boot-up ready.<br>Blinking Green (NORMAL) - The device and NC management system are under power-on process.<br>Blinking Green (FAST) - NC management system can't boot up. |
| 2 | Link Speed<br>(10/100/1000 Mbps) | Solid Amber - Port is operating at 10/100/1000 Mbps<br>Light Off - No Link. |
| 3 | Link Speed<br>(2500 Mbps) | Solid Green - Port is operating at 2500 Mbps<br>Light Off - No Link. |

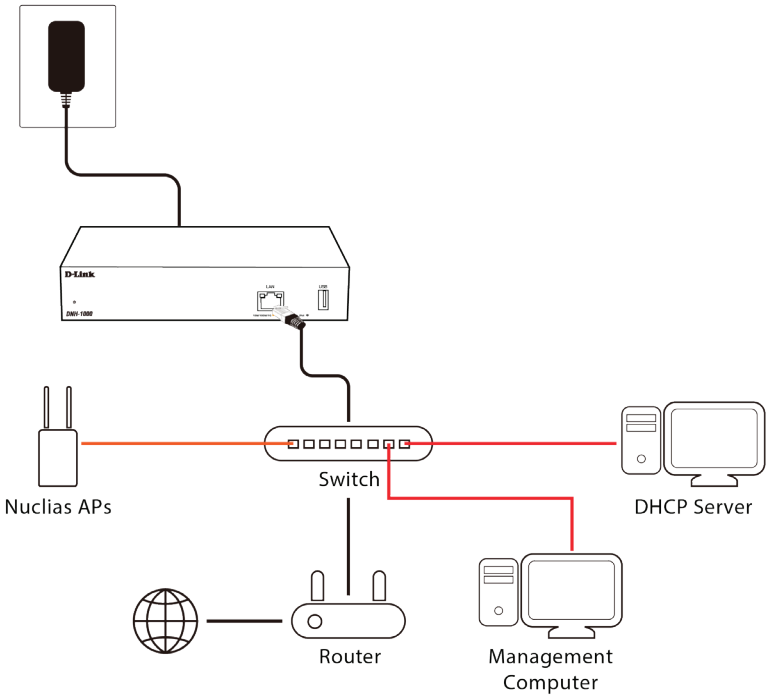
## Interface Connectors




| # | Connector | Description |
|---|---|---|
| 1 | Reset | Used for rebooting or resetting the device back to factory default settings. |
| 2 | Ethernet Port | Gigabit RJ-45 port for LAN connection. |
| 3 | USB Port | USB 3.0 Type A port (provides 5V/1A power for optional HDD connection). |
| 4 | Power Switch | Turn the power switch on/off. |

# Installation

## Connecting the Controller




To connect the DNH-1000, perform the following procedure:

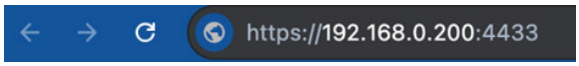
1. Install the DNH-1000 and access points/switches according to the instructions in their documentation. Access points by default will receive an IP address from the DHCP server.
2. Connect one end of an Ethernet LAN cable to port labeled as **Ethernet** on the front of the wireless controller. Connect the other end of the cable to an available RJ-45 port on a switch in the LAN network segment.
3. Plug one end of the AC power cord into the AC power connector on the back panel of the device. Plug the other end into an AC power source.

# Basic Configuration

## Launching Device Web GUI

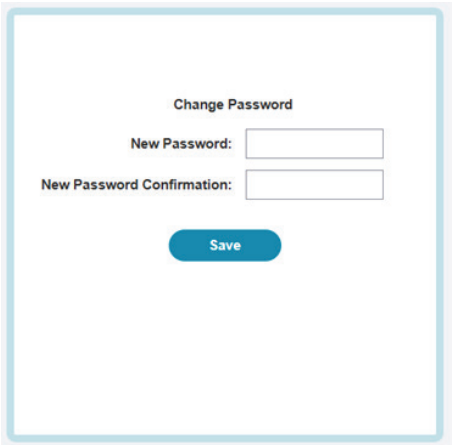
Open a web browser from the management computer and enter the **IP address** or **Domain Name** of the DNH-1000. The default IP address is https://192.168.0.200:4433.

**Note:** For initial configuration, the management computer and DNH-1000 must be in the same subnet.




The default user name and password of Device Web is 'admin'.

After the web browser opens and connects successfully to the server, a change-password prompt will appear. Updating 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 8 - 30 characters in length. By combining uppercase and lowercase characters, numbers and symbols, a strong password can be created.

**NOTE**: Do not include common words or names.

In the **New Password** field, enter the new password.

Enter the same password in the **New Password Confirmation** field to verify the entry.

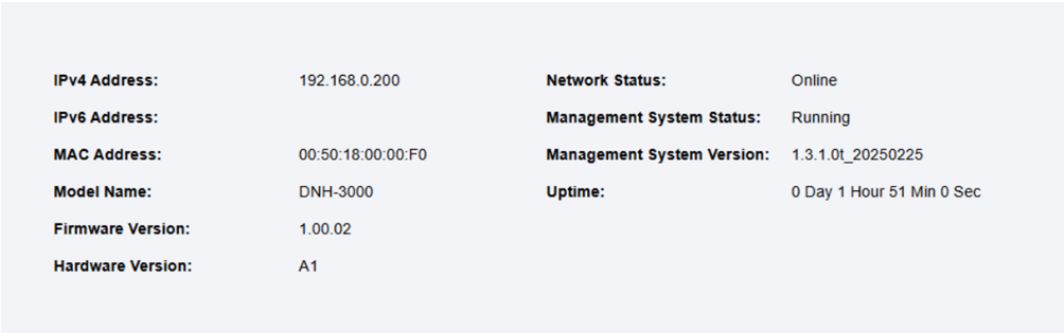
Click **Save** to complete the process.

# Device Web Configuration

## Home

Display the current information and status of the device.
Display Information as below:

- IP Address
- MAC Address
- Model Name
- Firmware Version
- Hardware Version
- Network Status (Online, Offline, Error)
- Management System Status (Running, Not Run)
- Management System Version
- Uptime



| | | | |
|---|---|---|---|
| **IPv4 Address:** | 192.168.0.200 | **Network Status:** | Online |
| **IPv6 Address:** | | **Management System Status:** | Running |
| **MAC Address:** | 00:50:18:00:00:F0 | **Management System Version:** | 1.3.1.0t_20250225 |
| **Model Name:** | DNH-3000 | **Uptime:** | 0 Day 1 Hour 51 Min 0 Sec |
| **Firmware Version:** | 1.00.02 | | |
| **Hardware Version:** | A1 | | |

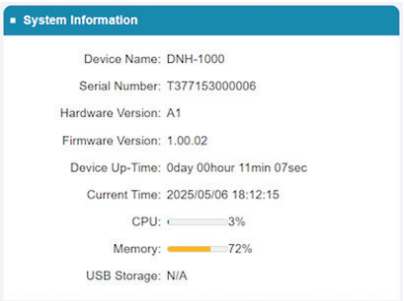
# Status

## Dashboard

The displayed sections include System Information, Network Interface Status, and System Information History.

System Information:

- Device Name
- Serial Number
- Hardware Version
- Firmware Version
- Device Up-Time
- Current Time
- CPU
- Memory
- USB Storage



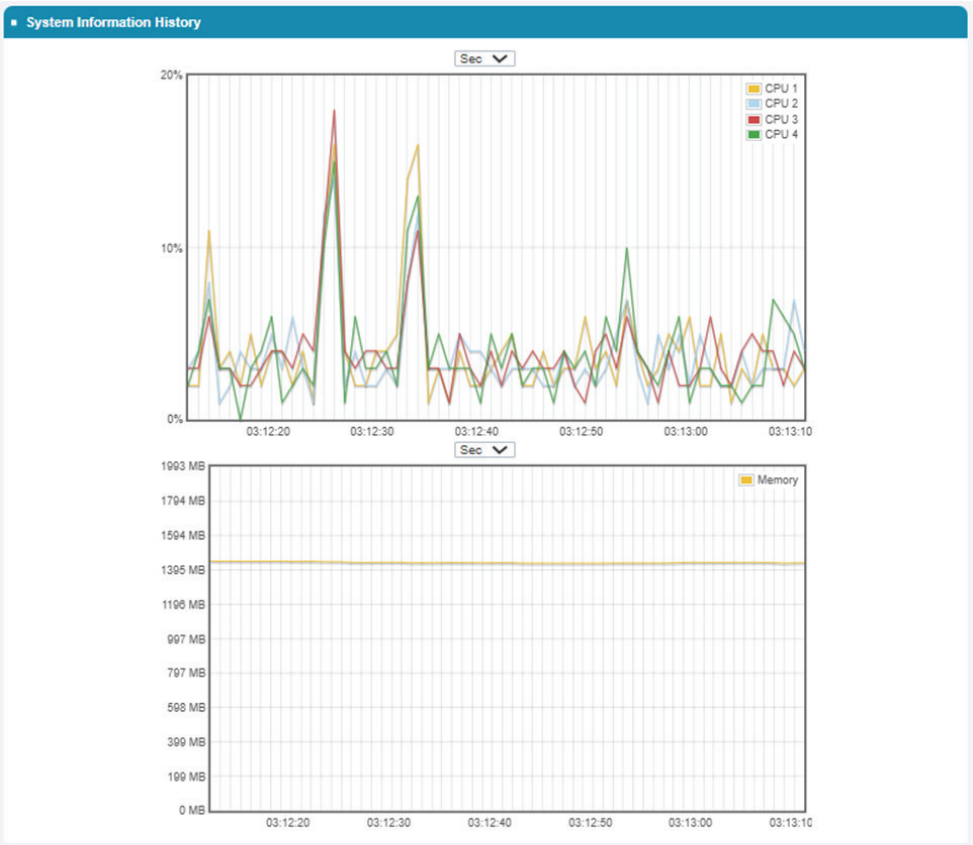

Network interface status information:

- Interface
- Upload Traffic
- Download Traffic
- Current Upload Traffic
- Current Download Traffic

**Network Interface Status**

| Interface | Upload Traffic | Download Traffic | Current Upload Traffic | Current Download Traffic |
|---|---|---|---|---|
| eth0 | 7 (MB) | 340 (MB) | 26 (KB) | 1 (KB) |

Display CPU usage graphics and memory consumption graphics of the system device.

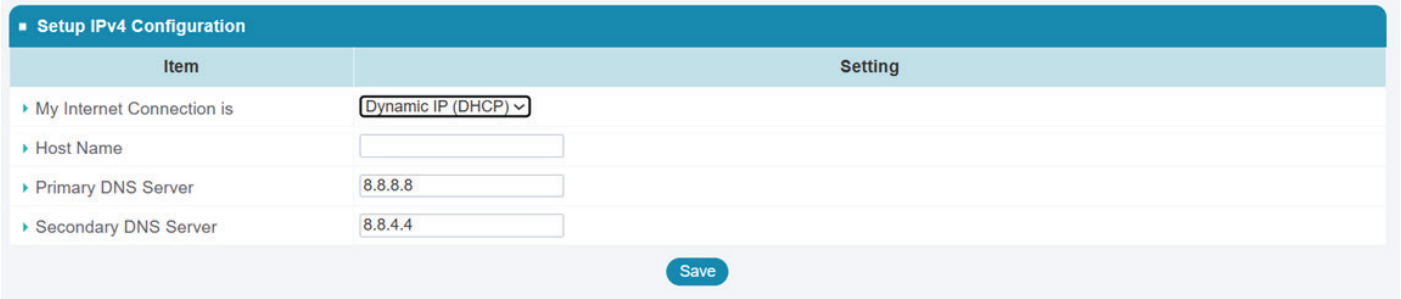


# Basic Network

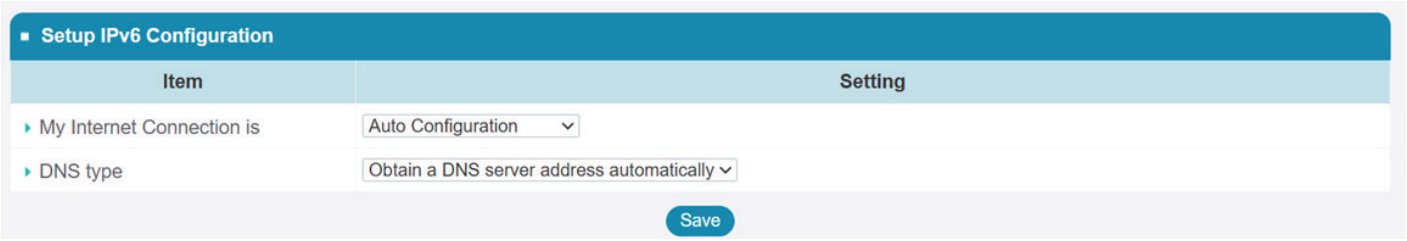
## LAN

Configure IPv4 and IPv6 settings.

Setup IPv4 Configuration




Setup IPv6 Configuration

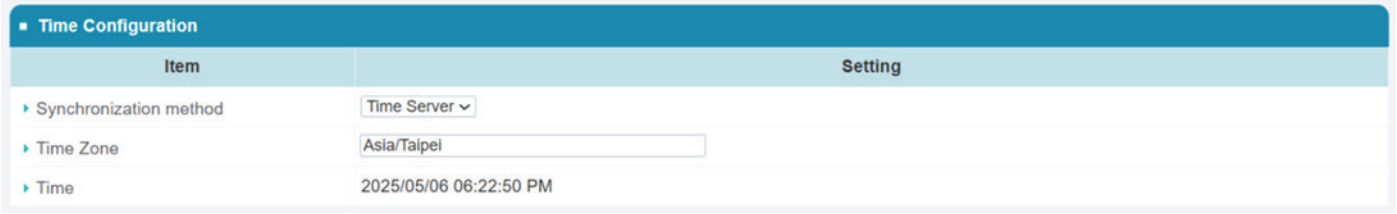


# System Settings

## Time

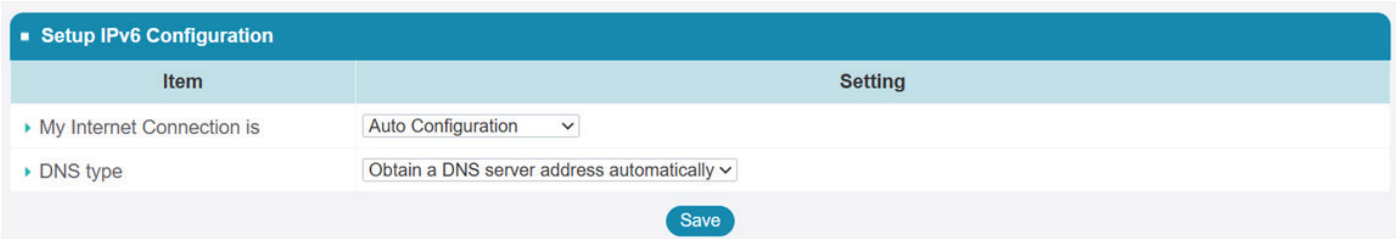
Time Configuration

Set the time server, time zone, and system time.




Auto Time Configuration

Set NTP Server - The time server is set to automatic by default, using Google's NTP server.



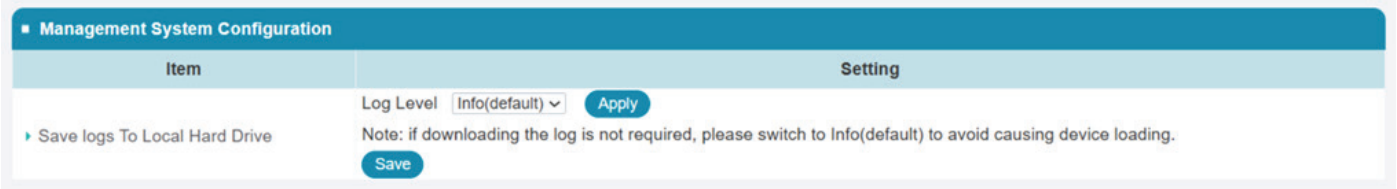
# System Admin

## Device System Configuration

The Device System Configuration includes options to save device settings to the local hard drive, load device settings from the local hard drive, and restore the device to factory default.


## Management System Configuration

Save the Management System log to the local hard drive. There are three options for the log level (Info, Debug, and Trace).




## Admin Password

The page for setting a new password.


## Reboot Configuration

This page is for rebooting the device.


## Shutdown Configuration

This page is for shutting down the device.

**Note**: Before turning off the power or removing the USB while it is inserted, be sure to perform this action to prevent unexpected data corruption.

# Upgrade

Device Firmware Upgrade

You can update new device firmware on this page.

**Device Firmware Upgrade**

| Item | Setting |
|---|---|
| FW Upgrade | FW Upgrade |
| Current Firmware Version | 1.00.02 |

Management System Upgrade

You can update new management system firmware on this page.

**Management System Upgrade**

| Item | Setting |
|---|---|
| FW Upgrade | Upgrade |
| Current Firmware Version | 1.3.1.0t_20250225 |

# Tools

Diagnostic Tools

This page allows you to perform ping and tracert tests.

**Diagnostic Tools**

| Item | Setting | |
|---|---|---|
| Ping Test | Host IP | 192.168.0.200 |
| | Outer Interface | All |
| | Ping | |
| Tracert Test | Host IP | 192.168.0.200 |
| | Outer Interface | All |
| | Protocol | UDP |
| | Tracert | |

Ping Test Results

The results of the ping test will be displayed on this page.

**Ping Test Results**

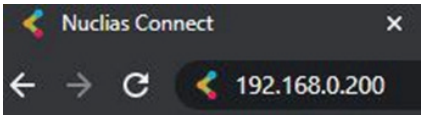
```
PING 192.168.0.200 (192.168.0.200) 56(84) bytes of data.
64 bytes from 192.168.0.200: icmp_seq=1 ttl=64 time=0.112 ms
64 bytes from 192.168.0.200: icmp_seq=2 ttl=64 time=0.112 ms
64 bytes from 192.168.0.200: icmp_seq=3 ttl=64 time=0.117 ms
64 bytes from 192.168.0.200: icmp_seq=4 ttl=64 time=0.107 ms

--- 192.168.0.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3064ms
rtt min/avg/max/mdev = 0.107/0.112/0.117/0.003 ms
```

# Basic Nuclias Connect Configuration

## Launching Nuclias Connect

The DNH-1000 comes preloaded with Nuclias Connect. Open a web browser from the management computer and enter the **IP address** or **Domain Name** of the DNH-1000. The default IP address is https://192.168.0.200.

**Note**: For initial configuration, the management computer and DNH-1000 must be in the same subnet.

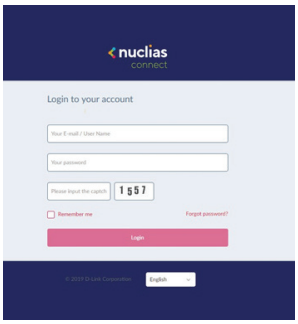



The default username and password of Nuclias Connect is 'admin'.

Enter the Captcha code as shown on screen.

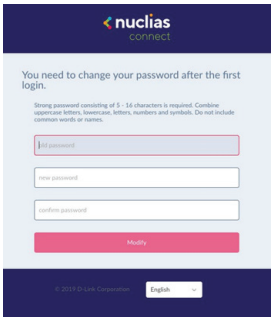
**Note**:

- The **Remember me** function can be selected to save the password entry for future use.
- The **Forgot password?** function allows you to reset your password in the event that you forget your current password. To use this function, the SMTP server and email address must be configured first.
- The interface supports multi-language options. By clicking the language drop-down menu, a different language can be selected.




After the web browser opens and connects successfully to the server, a change-password prompt will appear. Updating 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. By combining uppercase and lowercase characters, numbers and symbols a strong password can be created.




**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.

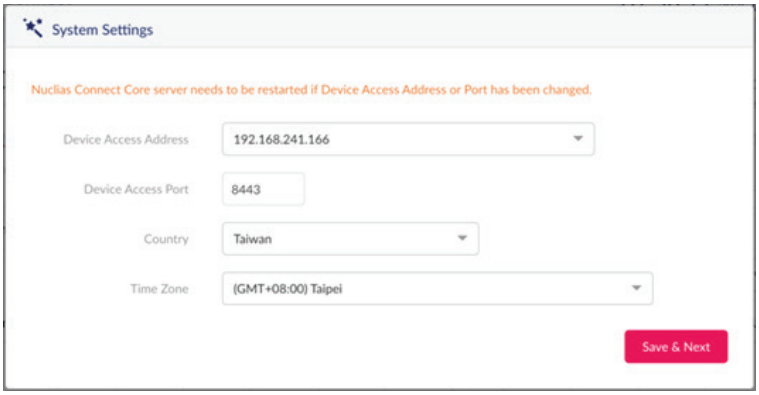
Click **Modify** to complete the process.

# Nuclias Connect Configuration

## Wizard

A wizard is available to guide you through first-time setup of the device. If at any time you wish to re-run the wizard, you can click on the icon on the top right to start the wizard.

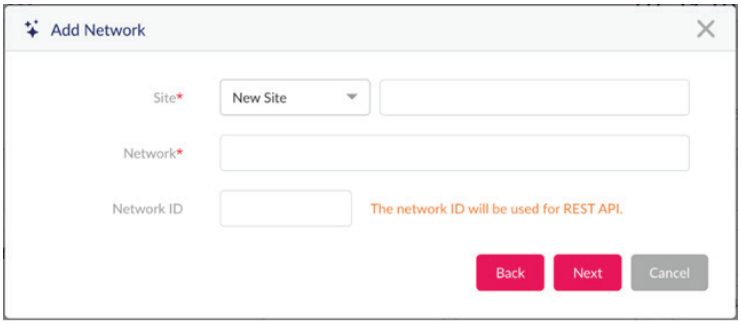
When wizard is activated, a string of settings prompt will appear.




In the **System Settings** window, configure the following:

| Parameter | Description |
|---|---|
| **Device Access Address** | Enter the Nuclias Connect 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 Connect server application's listen port number. The default value is 8443. For remote AP management behind a firewall or router, the inboud port must be opened. |
| **Country** | Select the designated country from the drop-down menu. |
| **Time Zone** | Select the geographic area from the drop-down menu. |

Once the system settings have been configured, click **Next** to continue. The **Add Network** page will appear:

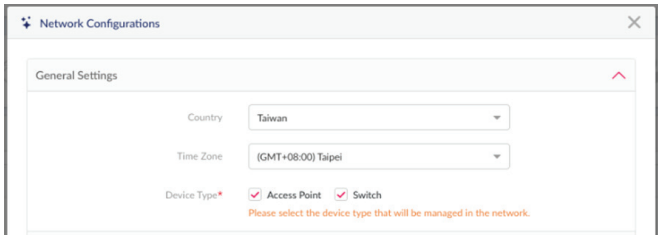


In the **Add Network** window, configure the following:

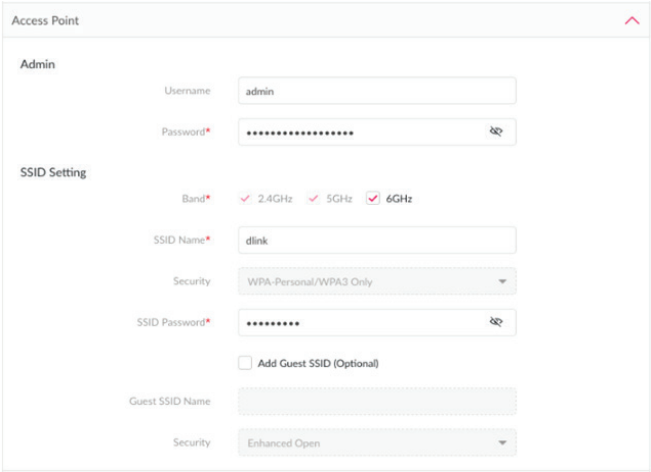
| Parameter | Description |
|---|---|
| **Site** | From the Site drop-down menu, select an existing site or new site and enter the name of the site in the field. |
| **Network Name** | Enter a name to identify the new network. |
| **Network ID** | The Network ID is an optional field. It will be used on REST API function. Leave it as blank if not using REST API. |

Once the network settings has been configured, click **Next** to continue or **Exit** to return to the previous step.

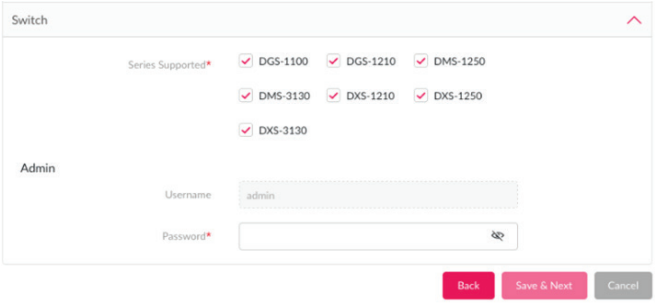
The **Network Configurations** page is displayed below. Under the **General Settings** tab, select a country, time zone, and the device type that will be managed in the network.




When **Acces Point** is selected, the following configuration will appear:

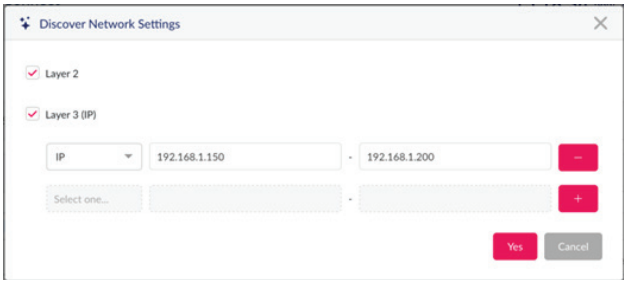



When **Switch** is selected as the device type, the following configuration will appear:



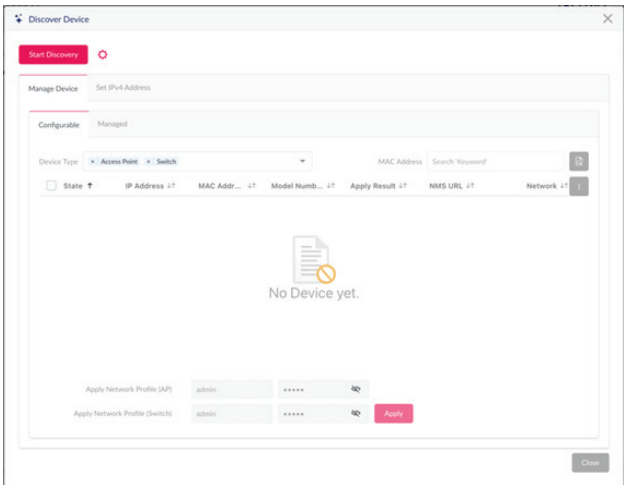
When the network configuration is defined, click **Save & Next** to continue, or click **Back** to return to the previous page.

The **Discover Device** page is displayed. Click ⚙ to 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 **Yes** to continue. Click **Cancel** to discontinue the **Device Network Settings** process.

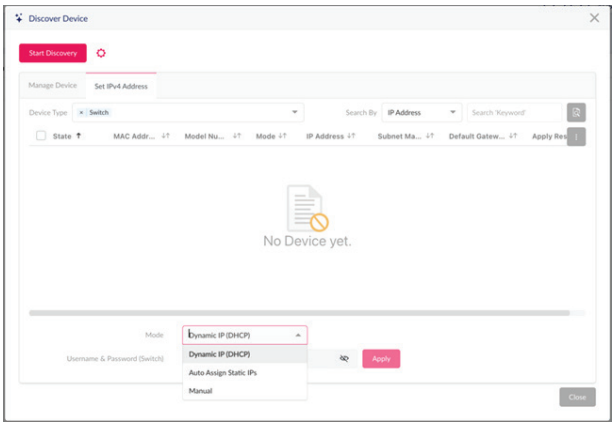



The **Start Discovery Page** is displayed. Click **Start Discovery** to search for all available unmanaged devices. If a device is found, select it and click **Apply** to import the network profile. Click on the **Managed** tab to select defined devices and add them to the network.

The **Set IPv4 Address** tab is used for configuring the correct IP address for switch devices, with the default IP set to 10.90.90.90.




The "Set IPv4 Address" has three modes: Dynamic IP (DHCP), Auto Assign Static IPs, and Manual.

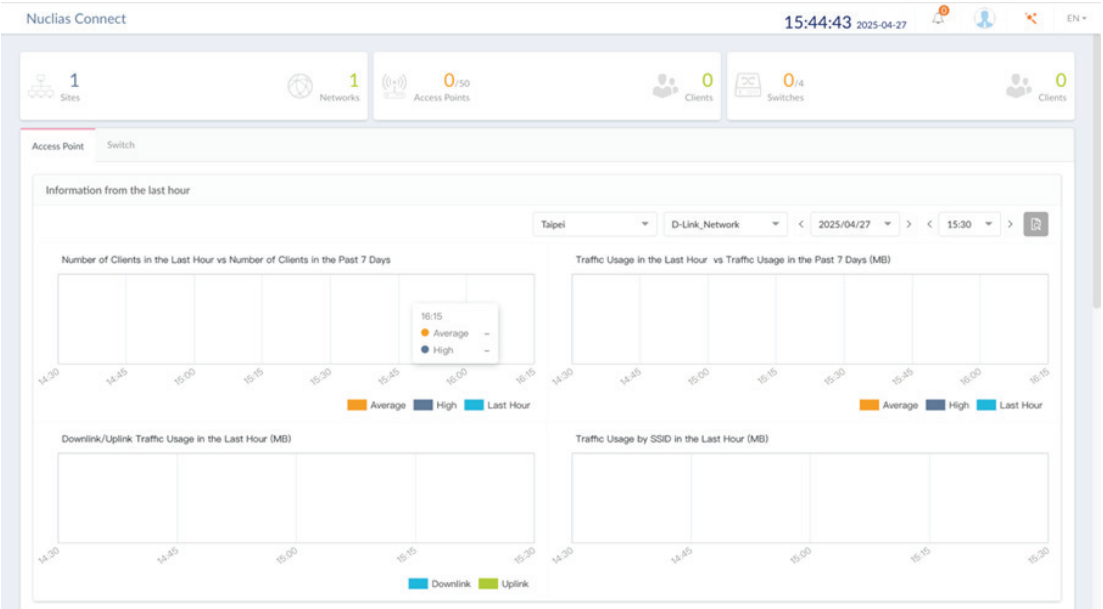


# Dashboard

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 | Description |
|---|---|
| **Information from Last Hour** | Displays log information for the number of clients, traffic usage, downlink/uplink traffic usage, and traffic usage by SSID. |
| **Channel Utilization** | Displays the utilization rate for both 2.4 and 5 GHz bandwidth. |
| **Last Events** | Displays a simplified log version of the latest events across all or selected sites. |

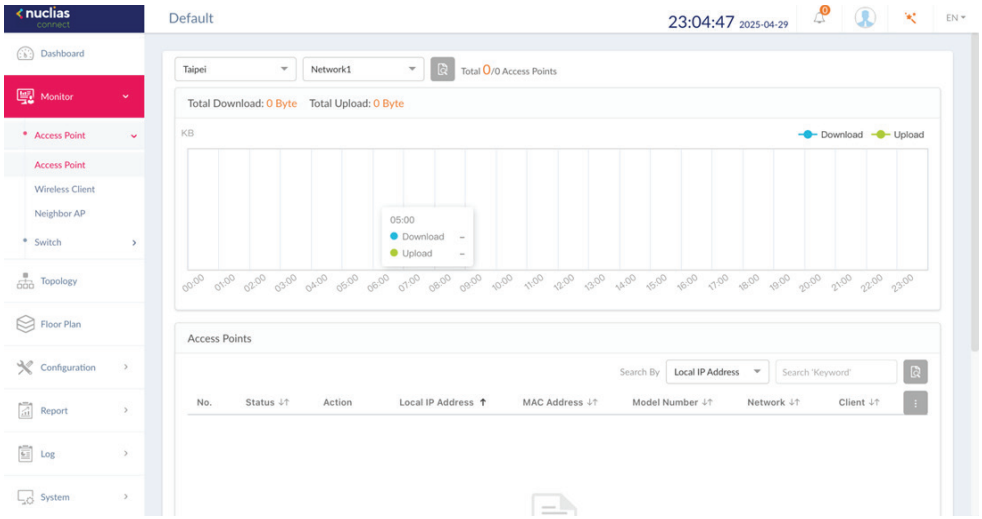
| Switch | Description |
|---|---|
| **Information from Last Hour** | Displays log information for Tx/Rx traffic usage and PoE USAGE. |
| **PoE Utilization** | Displays the utilization rate of switches across different sites and networks. |
| **Last Events** | Displays a simplified log version of the latest events across all or selected sites. |



# Monitor

## Access Point

Go to **Monitor** -- > **Access Point** 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.



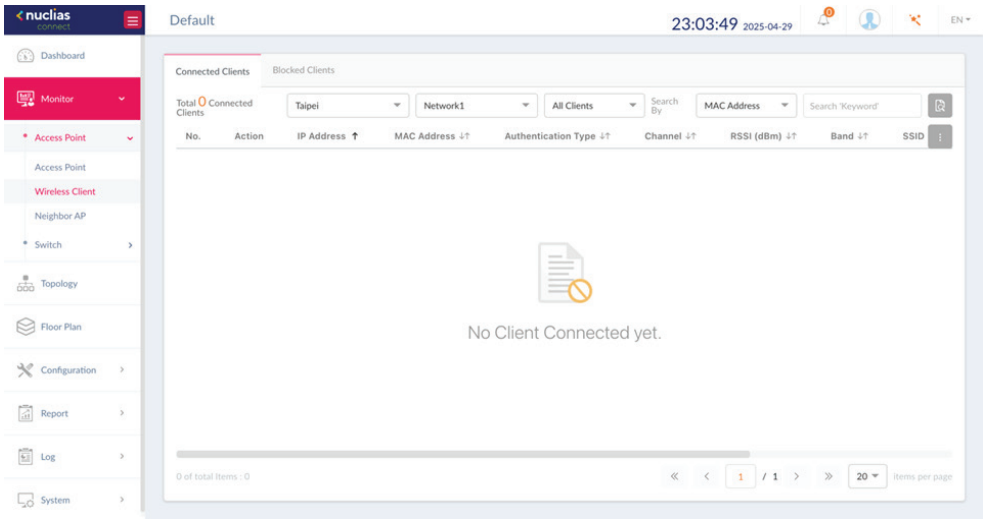

In the **Search By** drop-down field, select an attribute (**Local IP Address, Local IPv6 Address, NAT IP Address, MAC Address, Model Type, FW Version, Name, Location, Channel 2.4G, Channel 5G, Channel 6G, Power 2.4G, Power 5G, Power 6G**) to specify the search field or enter a keyword related to the target device in the Search field. Click to start the search. Any relevant devices meeting the search criteria will be listed.

## Wireless Client

### Connected Clients

Navigate to **Monitor > Access Point > Wireless Client**, the Connected Clients tab is displayed. A detail summary of all connected clients managed by the application can be viewed. Three filters can be applied to narrow the scope of connected clients: **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. Next, select a searching criteria (**Mac address, IP Address, User Authentication**). Any relevant devices meeting the search criteria will be listed.

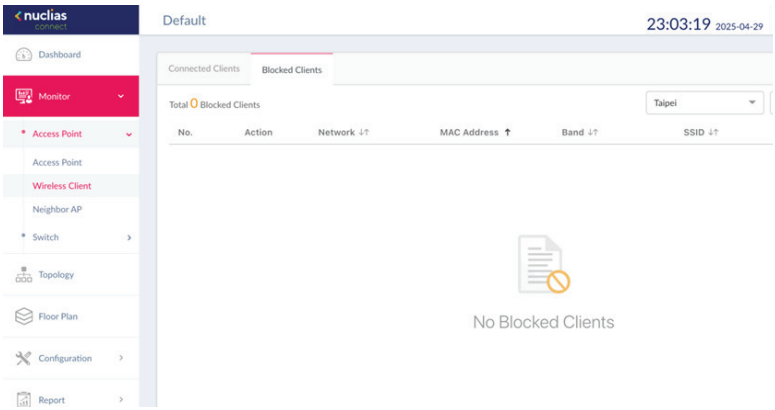


All wireless clients connected to the access points that are managed by this application are displayed. Information such as **Site**, **Network**, **IP Address**, **IPv6 Address**, **MAC Address**, **Auth. Type**, **OS** (only available on captive portal clients), **Upload**, **Download**, **Channel**,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

## Blocked Clients

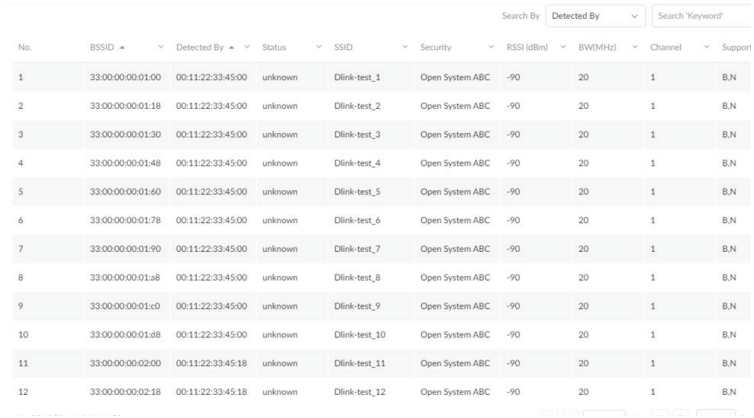
In the Wireless Client page, select the **Blocked Clients** tab. All blocked clients detected can be viewed here. Use the **Sites** and **Networks** drop-down menu to select a Site and Network. Click to start the search. Any relevant devices meeting the search criteria will be listed.

The summary contains the following information: **No.**, **Action**, **Network**, **MAC Address**, **Band**, **SSID**, and **Auth. Type**.




# Neighbor AP

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



| No. | BSSID | Detected By | Status | SSID | Security | RSSI (dBm) | BW(MHz) | Channel | Support |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 33:00:00:00:01:00 | 00:11:22:33:45:00 | unknown | Dlink-test_1 | Open System ABC | -90 | 20 | 1 | B,N |
| 2 | 33:00:00:00:01:18 | 00:11:22:33:45:00 | unknown | Dlink-test_2 | Open System ABC | -90 | 20 | 1 | B,N |
| 3 | 33:00:00:00:01:30 | 00:11:22:33:45:00 | unknown | Dlink-test_3 | Open System ABC | -90 | 20 | 1 | B,N |
| 4 | 33:00:00:00:01:48 | 00:11:22:33:45:00 | unknown | Dlink-test_4 | Open System ABC | -90 | 20 | 1 | B,N |
| 5 | 33:00:00:00:01:60 | 00:11:22:33:45:00 | unknown | Dlink-test_5 | Open System ABC | -90 | 20 | 1 | B,N |
| 6 | 33:00:00:00:01:78 | 00:11:22:33:45:00 | unknown | Dlink-test_6 | Open System ABC | -90 | 20 | 1 | B,N |
| 7 | 33:00:00:00:01:90 | 00:11:22:33:45:00 | unknown | Dlink-test_7 | Open System ABC | -90 | 20 | 1 | B,N |
| 8 | 33:00:00:00:01:a8 | 00:11:22:33:45:00 | unknown | Dlink-test_8 | Open System ABC | -90 | 20 | 1 | B,N |
| 9 | 33:00:00:00:01:c0 | 00:11:22:33:45:00 | unknown | Dlink-test_9 | Open System ABC | -90 | 20 | 1 | B,N |
| 10 | 33:00:00:00:01:d8 | 00:11:22:33:45:00 | unknown | Dlink-test_10 | Open System ABC | -90 | 20 | 1 | B,N |
| 11 | 33:00:00:00:02:00 | 00:11:22:33:45:18 | unknown | Dlink-test_11 | Open System ABC | -90 | 20 | 1 | B,N |
| 12 | 33:00:00:00:02:18 | 00:11:22:33:45:18 | unknown | Dlink-test_12 | Open System ABC | -90 | 20 | 1 | B,N |

| 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

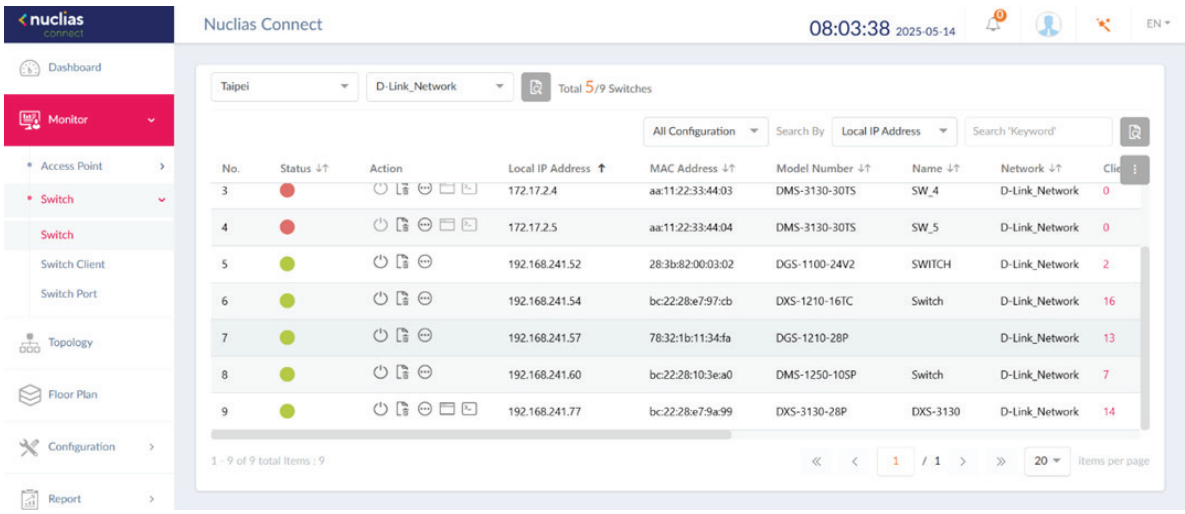
Go to **Monitor > Switch** and use the Site and Network filter to locate the device you'd like to monitor. On this page, you can view a summary of the devices managed by the application. The summary includes the following: **Status, Local IP Address, NAT IP Address, MAC Address, Model Type, FW Version, 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).<br>• Profile: Devices under profile mode share the same configurations in the profile.<br>• Standalone: Devices have their own configurations, and does not get affected by profile. |
| **Last Seen** | Displays the last connected time of the switch. |
| **Uptime** | The activating time of the switch after reboot. |

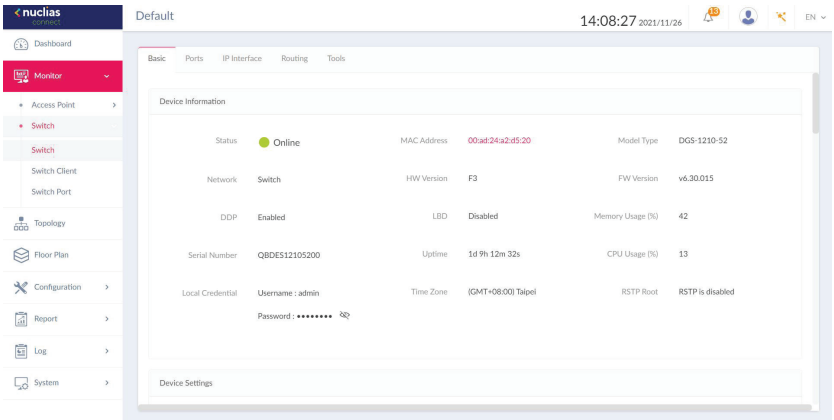


# Device Detail Page

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.

## Basic

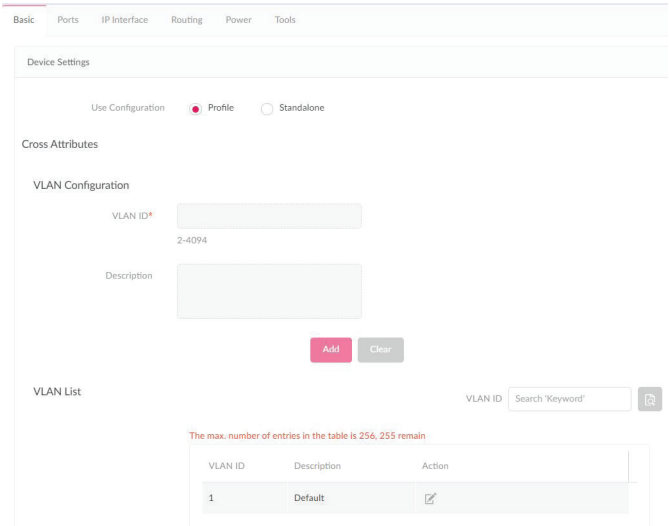
On the **Basic** tab, you can configure your device and view a summary of Device Information. The following information is displayed under the **Device Information** section: **Online Status, Network, DDP, Serial Number, Local Credential, MAC Address, HW Version, LBD, Uptime, Time Zone, Model Type, FW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

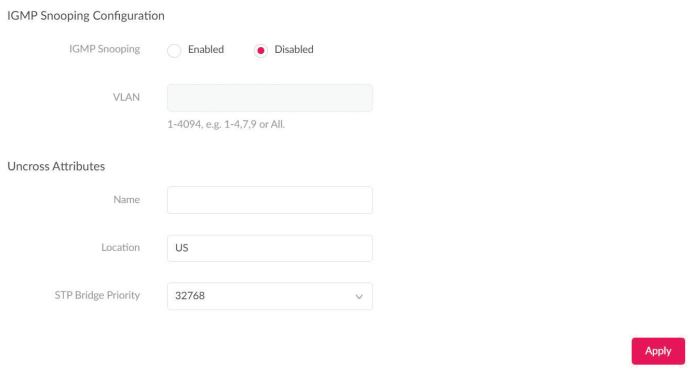
In the **Device Settings** section, select a use configuration (Profile or Standalone). If Profile is selected, the subsequent settings, such as VLAN and IGMP Snooping will be fixed. If Standalone is selected, the above-mentioned settings will be available for editing.

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.

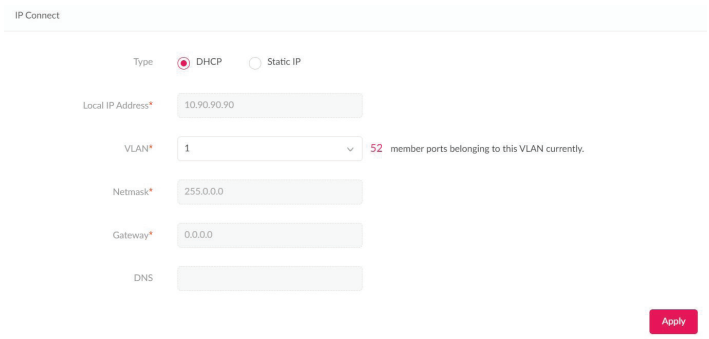


**IGMP Snooping** is disabled by default. When use configuration is set to **Standalone**, you can enable IGMP Snooping. Enter the VLAN to complete the process.

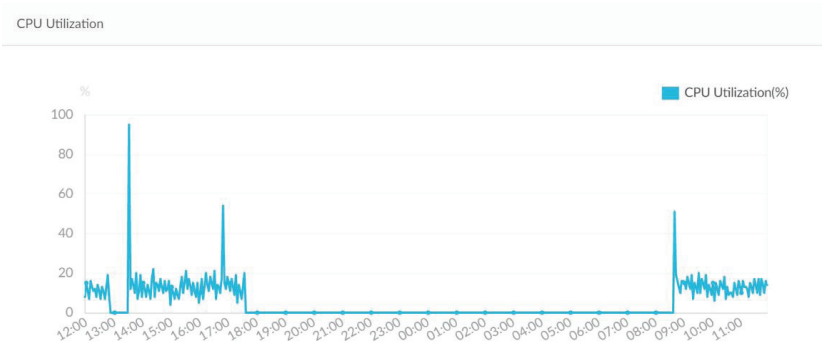
In the **Uncross Attributes** section, features that cannot be configured via profile will be listed here. Enter a name, location, and use the drop down menu to select a STP Bridge Priority. Click Apply to complete the settings.




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.

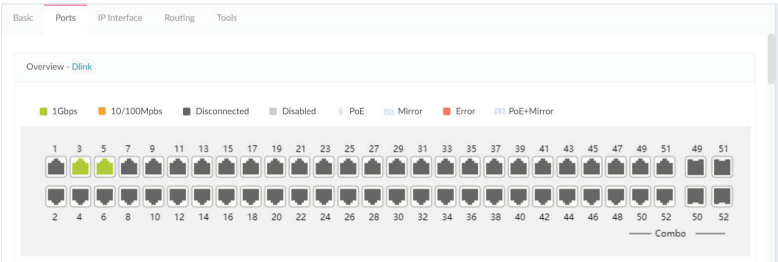



In the **CPU utilization** section, a CPU Utilization graph is displayed. On the Y axis shows the percentage of CPU utilization. On the X axis shows the time by hour.



## Ports

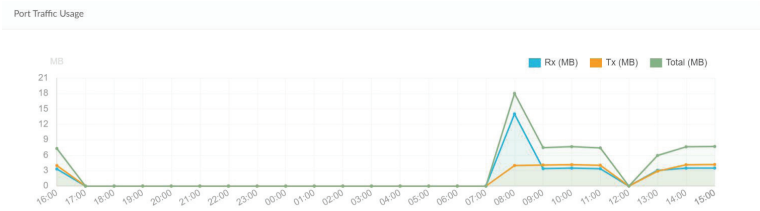
Under the **Ports** tab, a port status overview is presented. The graph displays a range of colors and icons to inform users of the status of each individual port. Clicking on the port icons will direct users to the **Port Detail** page of the specified port.




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

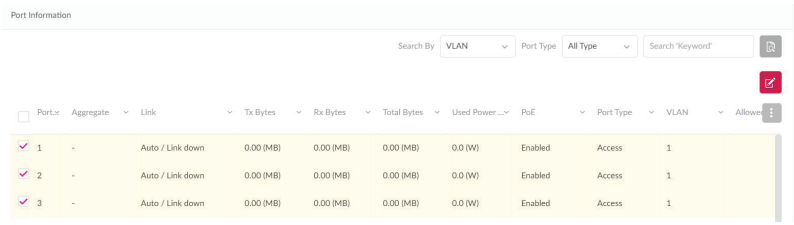
| Status | Description |
|---|---|
| **Green** | Connected to Gigabit Ethernet |
| **Orange** | Connected to 10/100Mbps Ethernet |
| **Dark Gray** | Port disconnected |
| **Light Gray** | Port disabled |
| | Powered by PoE |
| | Port mirrored |
| **Red** | Error detected |
| | PoE+Mirror |

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



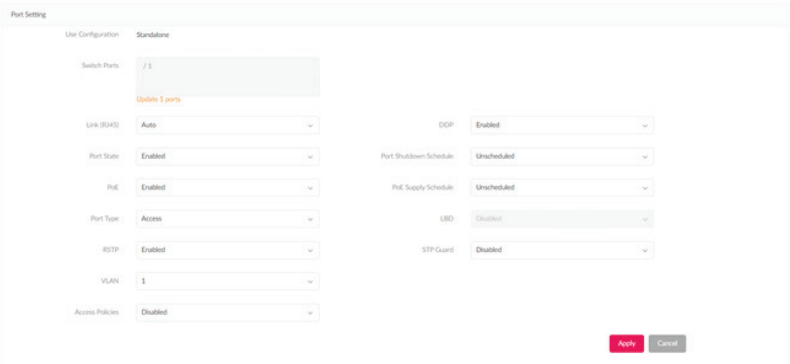

In the **Port Information** section, you can view a summary of all active and inactive ports. The summary includes information such as **port number, Aggregate link status, Tx/Rx/Total bytes, used power, PoE, Port type, VLAN, Allowed VLANs, Port State, PoE Supply Schedule, RSTP, LBD, DDP, Port Shutdown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

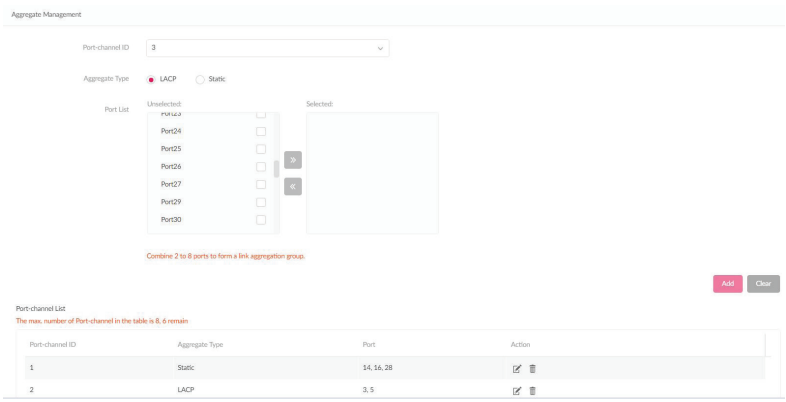
To make changes to a port or port group on the switch, first make sure the User Configuration is set to Standalone in the Device Settings section. Next, check the boxes next to the port(s) you'd like to change. Click to edit. Scroll down to access the Port Settings. Once the changes are made, click **Apply**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



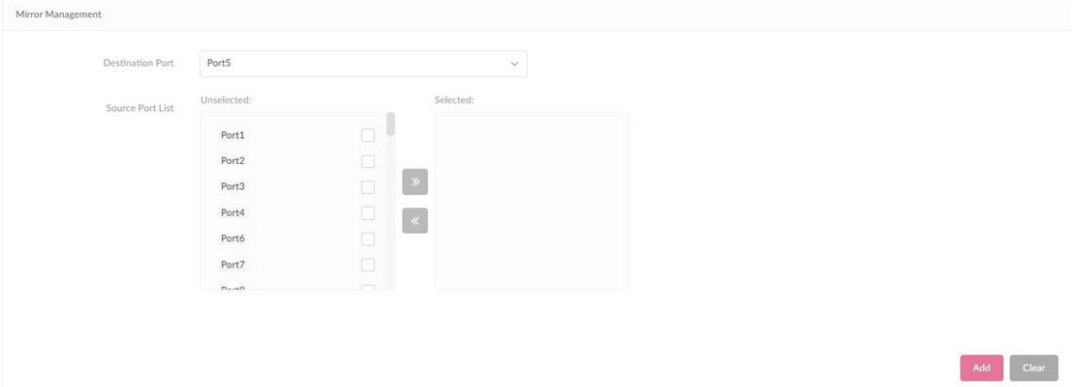

| Field | Description |
|---|---|
| **Port Shutdown Schedule** | Apply a time profile to the port shutdown function. The time profile is created in the time profile page. |
| **PoE Supply Schedule** | Apply a time profile to the PoE supply function. |
| **Port Type** | Type: Switch ports can be configured as one of the following two types.<br>(1) Trunk: Trunk port allows the selected port to accept/pass 802.1Q tagged traffic.<br>• Native VLAN: All untagged traffic will be placed on this VLAN. The range is 1-4094.<br>• Allowed VLANs: Only selected VLANs are able to traverse this link. The range is All/1-4094.<br>(2) Access: Access port places all traffic on its defined VLAN.<br>• Access VLAN: All traffic is placed on this VLAN. The range is 1-4094.<br>• Access policy: Apply a restriction policy to this port.<br>• Disabled: All Devices can access this port.<br>• Static MAC Whitelist: Only the devices with MAC addresses specified in this list can access this port.<br>• 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." When the total number of "Dynamic Whitelisted MACs" exceeds the value of "Dynamic Whitelist Size Limit," all subsequent MAC addresses will be denied access to this port. A table displaying dynamically learned MAC addresses is available.<br>• 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.

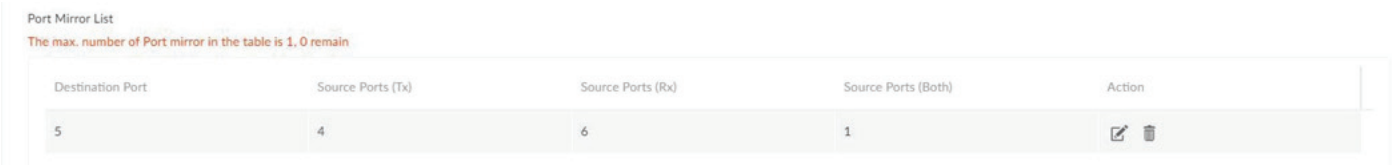
Under the Port-channel List, you'll see a summary list of link aggregation you have created. The summary shows the Port-channel ID, Aggregate Type and Port numbers. Beneath the Action field, click to edit, or to delete. Click **Apply** to save the changes.



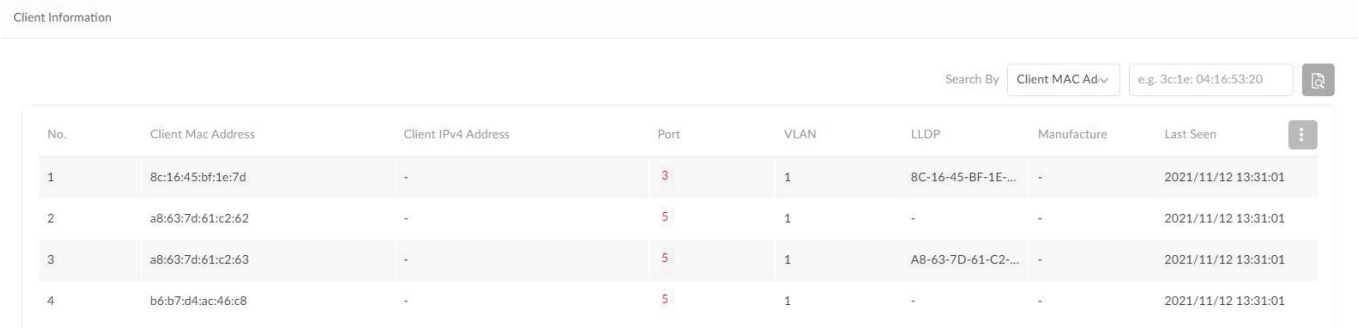
In the **Mirror Management** section, you can mirror the network packet on one switch port to another. First select a Destination Port using the drop-down menu. Next, from the Souce Port list, select the ports you'd like to mirror. Once selected, from the drop-down menu, pick the type of traffic to mirror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




Under the **Port Mirror** list, you'll see a 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.



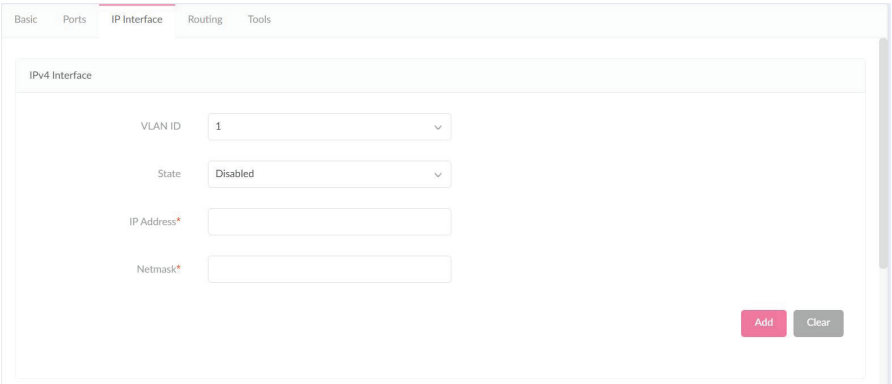

In the **Client Information** section, a summary of client information is displayed. Use the **Search By** drop-down menu to select a criteria to filter the search result. Click to start the search. The following information is displayed in the summary: **Number, Site, Network, Client MAC Address, Client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



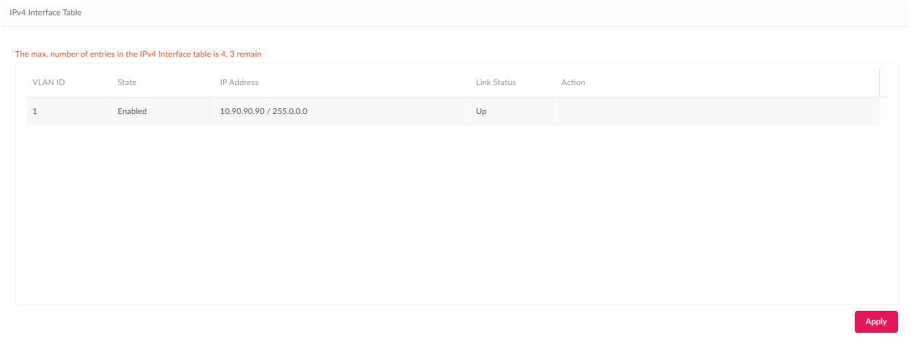

| Key Fields | Description |
|---|---|
| **Port** | Displays the port number of the switch to which the client is connected to. Click the Port number to be directed to port detail page |
| **LLDP** | Displays the LLDP information of neighbors. |
| **Manufacture** | Displays the Manufacture name of the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

## IP 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.



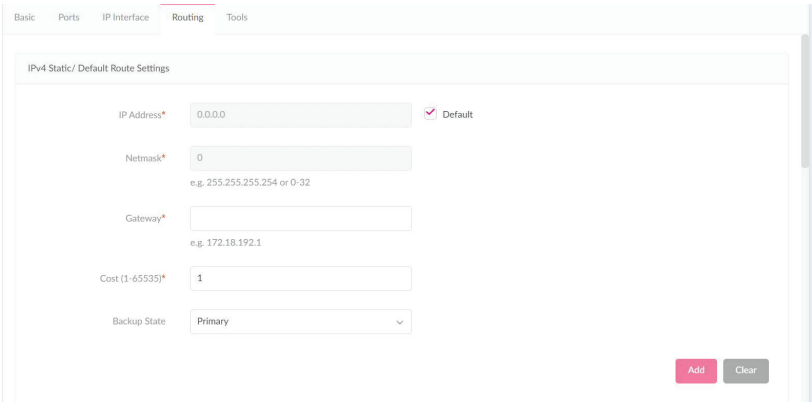

In the IPv4 Interface Table, a summary containing VLAN ID, State, IP Address, and Link Status is displayed. Beneath the Action field, click to edit, or to delete. Click **Apply** to save the changes.



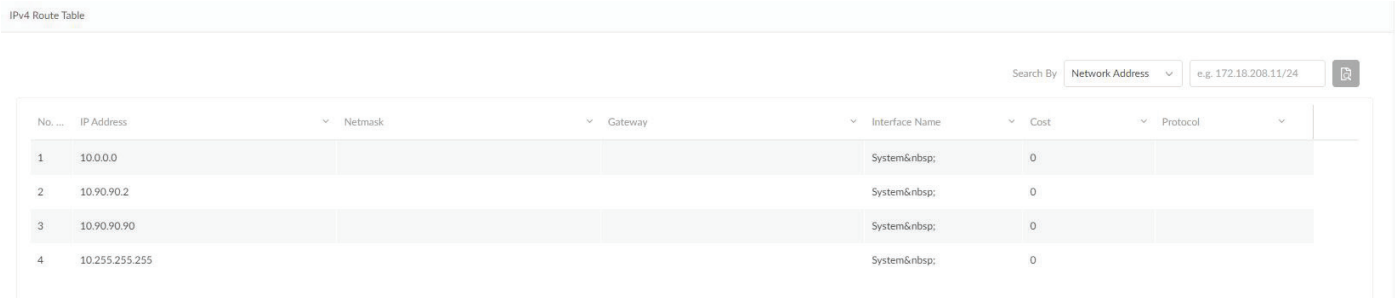
## Routing

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.



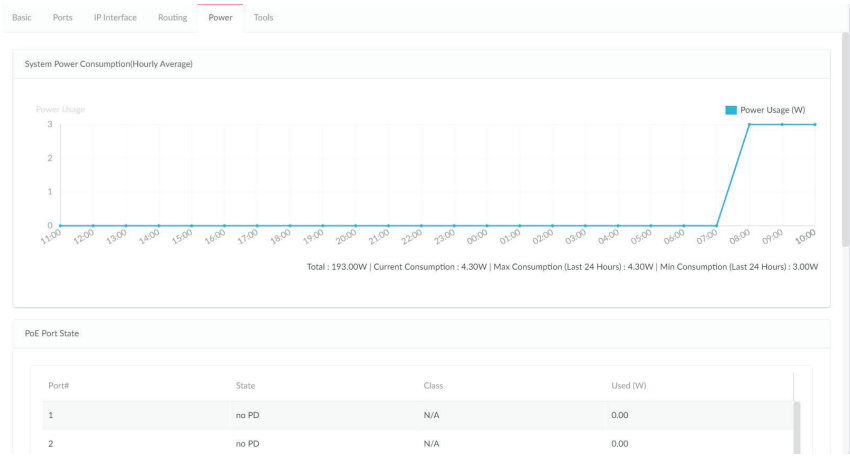

The IPv4 Route Table stores the routes information of the switch. Use the **Search By** drop-down menu to select a search criteria (**Network/IP Address**) to filter your search. Click to start the search. The following information is presented in the table: **Number, IP Address, Netmask, Gateway, Interface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




## Power

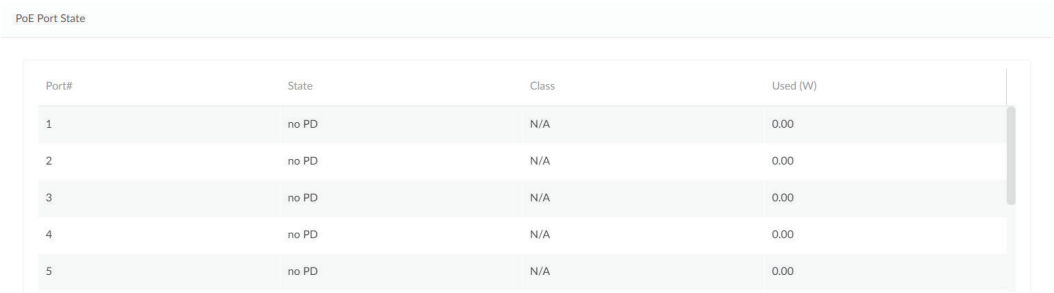
Under the **Power** tab, the **System Power Consumption** chart and **PoE Port State** summary is displayed. Note that the Power tab will only be available if your switch supports PoE.

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:

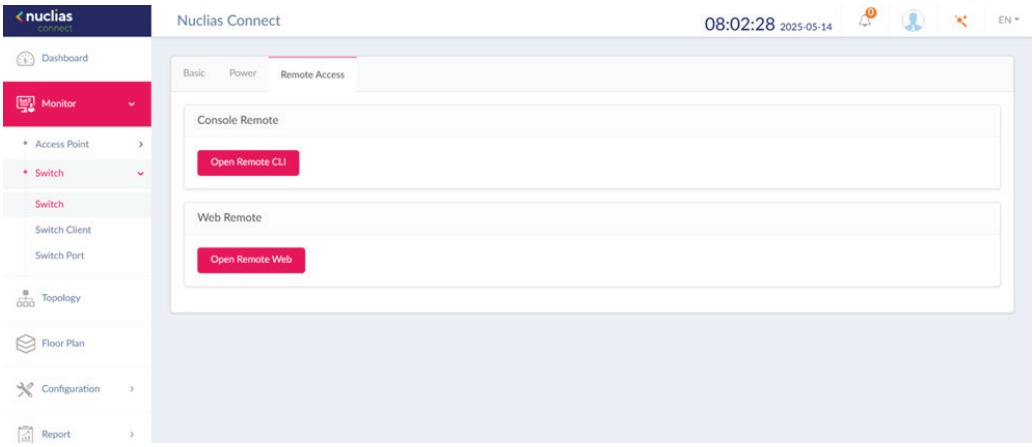
| Field | Description |
|---|---|
| **No.** | Port number |
| **State** | PoE port status |
| **Class** | The IEEE classification: N/A or a value from IEEE class 0 to 4 |
| **Used(W)** | The amount of power that is currently allocated to PoE ports in watts |

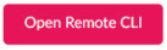



## Remote Access

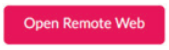
Under the Remote Access tab, you can use remote tunnel access technology to connect to the device. Note that the feature will only appear on managed switch devices.

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 

to jump to embedded UI terminal page.

Click 

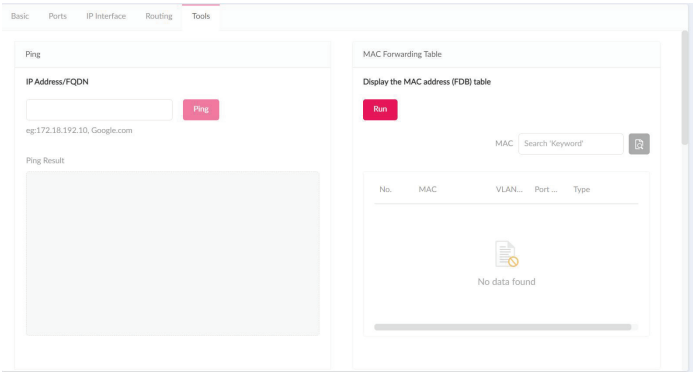
to open device web GUI .

## 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.

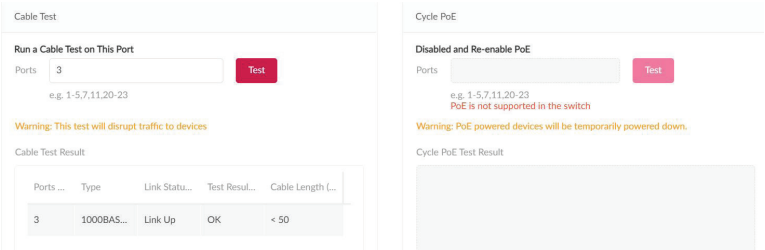
The **MAC Forwarding Table** shows a summary of **MAC addresses, VLAN, Port**, and **IP Address Type**. Press Run to begin the process. On the MAC search filed, enter a relevant keyword to help locate the MAC address.



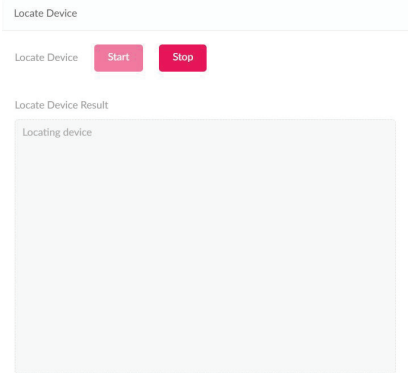

The **Cable Test** allows you to test the connectivity of one or multiple ports. Enter a number of port(s) and click Test to begin the process. The following information will be displayed: **Port number, Type, Link Status, Test Result**, and **Cable Length.** Under the Test Result field, 5 statuses can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

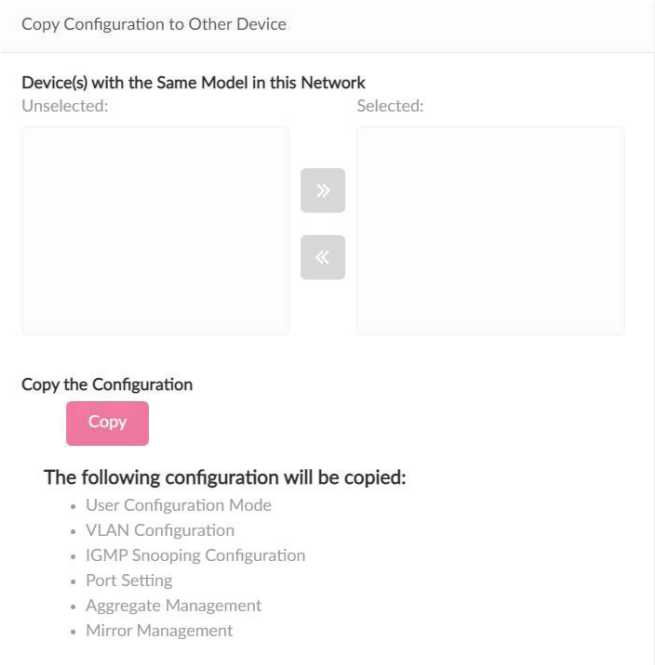



The **Locate Device** function can help identify unlabled switches by lighting up the LEDs on the switch. Click the Start button to light up the switch. All LEDs will light up in green for 5 minutes. Click the Stop button to stop the light immediately. If a device is located, a message "Locating device..." 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).

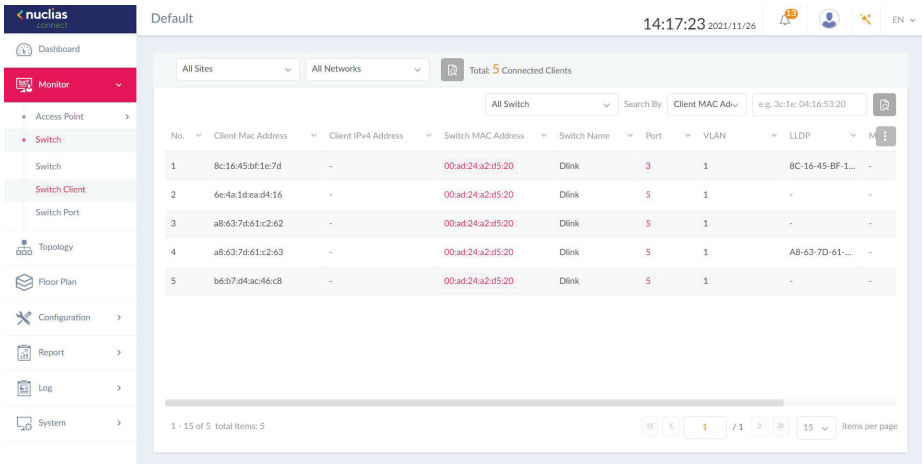
To copy the configuration, select the switch(es) in the network that will be copied. Click the **Copy** button to copy the configuration from your device to the selected device(s). A pop-up window will confirm once again. Click **Copy** to continue or **Cancel** to stop.



# 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 criteria (**Client MAC address, Client IPv4 Address, VLAN** and **Port**) and enter relevant keywords to narrow the search result.

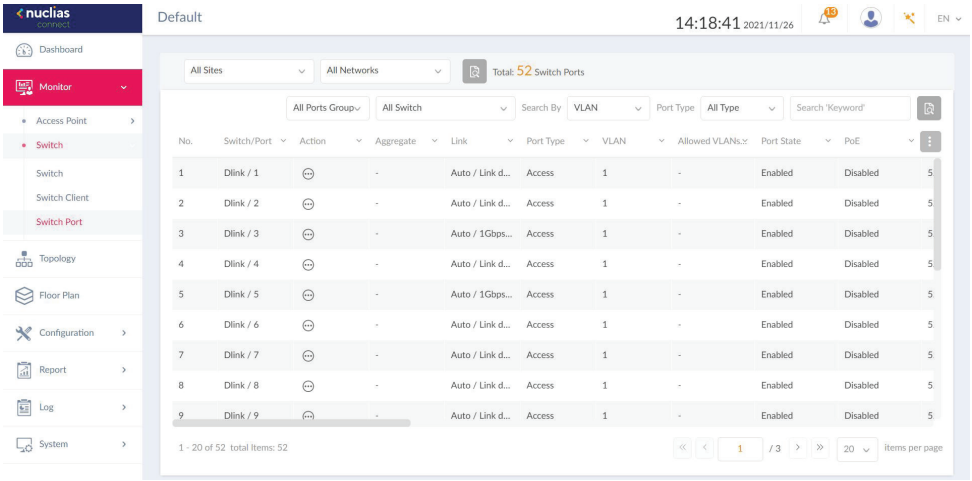



| Key Fields | Description |
|---|---|
| **Switch MAC Address** | Displays the MAC Address of the switch that the client is connected to. Click the MAC Address to be redirected to the switch detail page. |
| **Port** | Displays the port number of the D-Link switch that the client is connected to. Click 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.

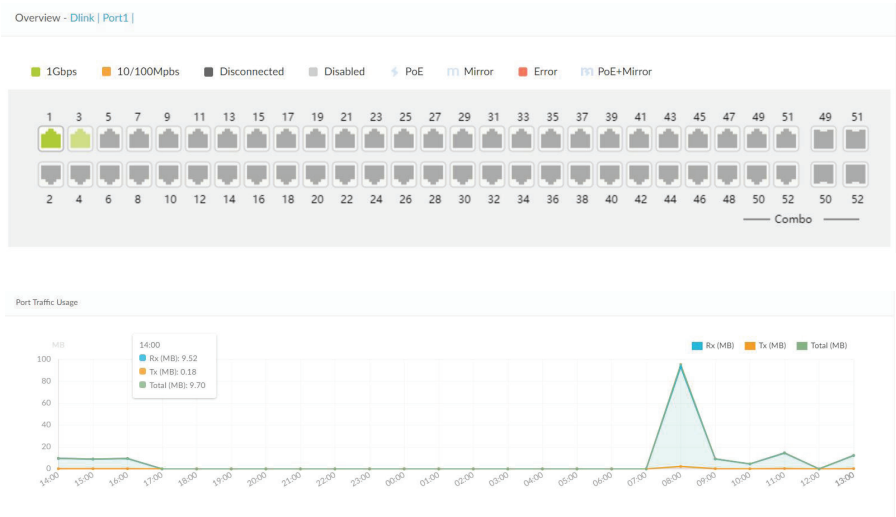
The following information is displayed: **Number, Switch/Port, Aggrregate, Link, Port Type, VLAN, Allowed VLANs, Port State, PoE, Ports, RSTP, LBD, DDP, Port Shutdown Schedule, PoE Supply Schedule, Access Policies, Mirror, LLDP, Port Name, Rx Broadcast Packets, Tx Boardcast Packets, Rx Multicast Packets,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

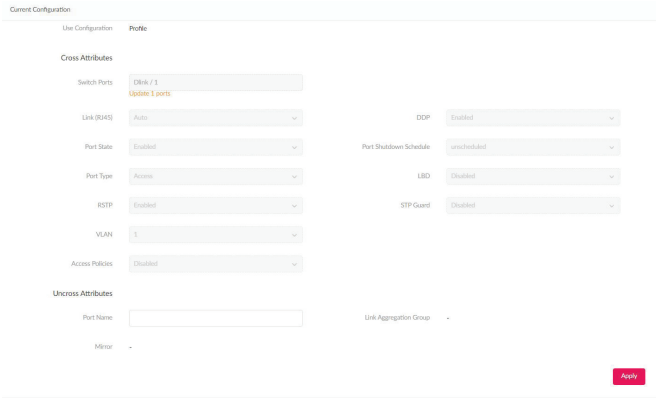


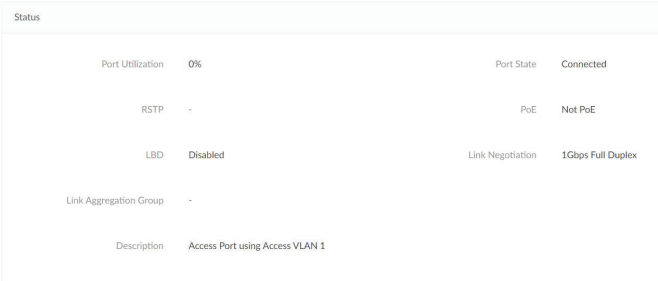

| Key Fields | Description |
|---|---|
| **Switch/ Port** | Displays the switch name and the port number. |
| **Aggregate** | Displays the link aggregation type (Static/LACP/-) of the port-channel group. |
| **Link** | Displays link configuration and link status of the port. |

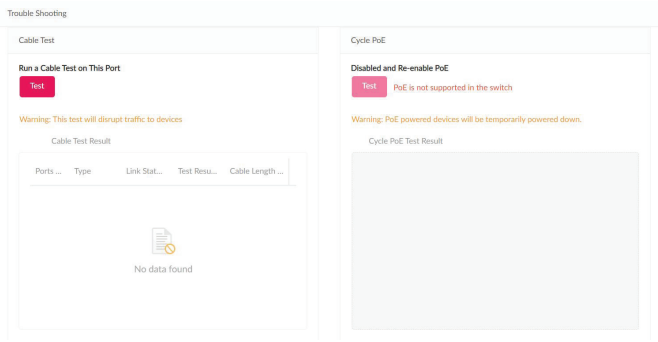
Under the **Action** field, click to go to the Port Detail page. You'll be directed to detail page for the specific port of the switch you have selected.

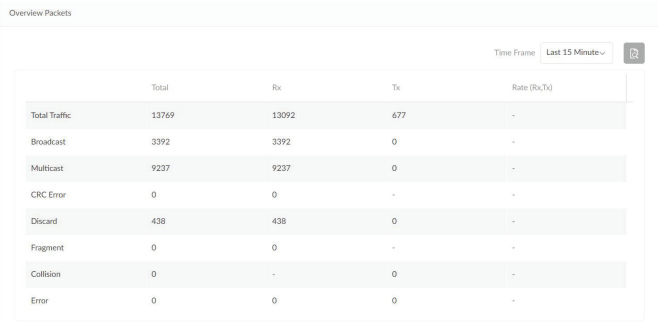
In the **Port Detail** page, you get an overview on the **Switch Port Connection Status, Port Traffic Usage, Current Configuration, Port Status, Testing Tools including Cable Test and Cycle PoE, Packet Overview** and **Client Information**.



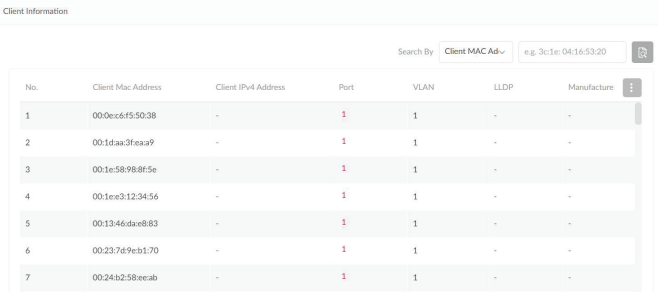



| | Total | Rx | Tx | Rate (Rx,Tx) |
|---|---|---|---|---|
| Total Traffic | 13769 | 13092 | 677 | - |
| Broadcast | 3392 | 3392 | 0 | - |
| Multicast | 9237 | 9237 | 0 | - |
| CRC Error | 0 | 0 | - | - |
| Discard | 438 | 438 | 0 | - |
| Fragment | 0 | 0 | - | - |
| Collision | 0 | - | 0 | - |
| Error | 0 | 0 | 0 | - |

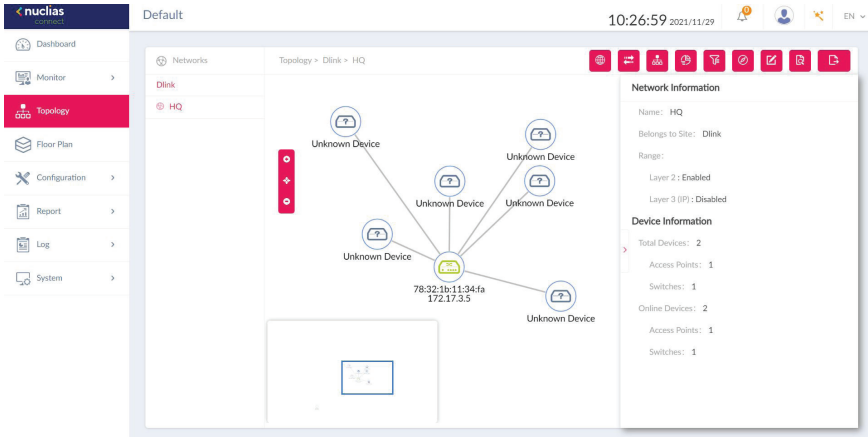



| No. | Client Mac Address | Client IPv4 Address | Port | VLAN | LLDP | Manufacture |
|---|---|---|---|---|---|---|
| 1 | 00:0e:c6:f5:50:38 | - | 1 | 1 | - | - |
| 2 | 00:1d:aa:3f:eaa9 | - | 1 | 1 | - | - |
| 3 | 00:1e:58:98:8f:5e | - | 1 | 1 | - | - |
| 4 | 00:1e:e3:12:34:56 | - | 1 | 1 | - | - |
| 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

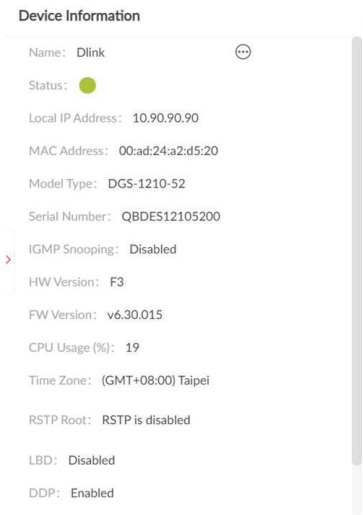
Under the **Topology** page, users can view the topological relations between switch devices and access points in a network. Press to zoom in, to zoom out, and to reset the topology. A basic network and device summary is displayed. The following information is included: Network name, Belonging Site,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

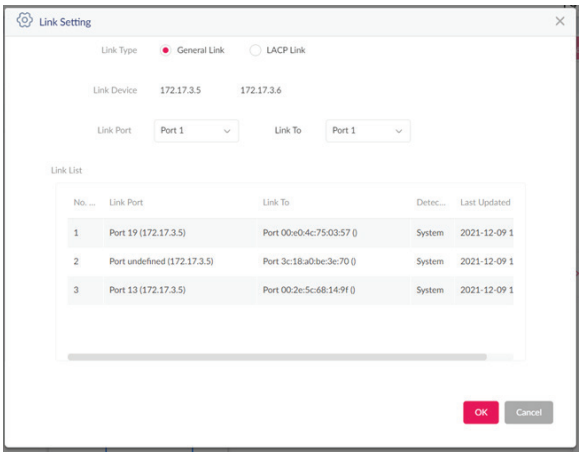
| Field | Description |
|---|---|
| **Name** | Displays the name to identify the switch on server. Click the name to be redirected to the device detail page.<br>Note that the AP name must be unique to the Site. |
| **Status** | Displays the connection status of the AP: Online, Offline or Unmanaged. Green 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 Detail**

| Field | 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.<br>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.<br>Display format:<br>• "Root is X/ root bridge priority: Y"<br>X represents device name (System name) of the root switch.<br>Y represents bridge priority of root switch.<br>• "RSTP is disabled"<br>- When RSTP is not enabled on the switch<br>- RSTP is enabled only on the switch, not the ports.<br>• "-"<br>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. |

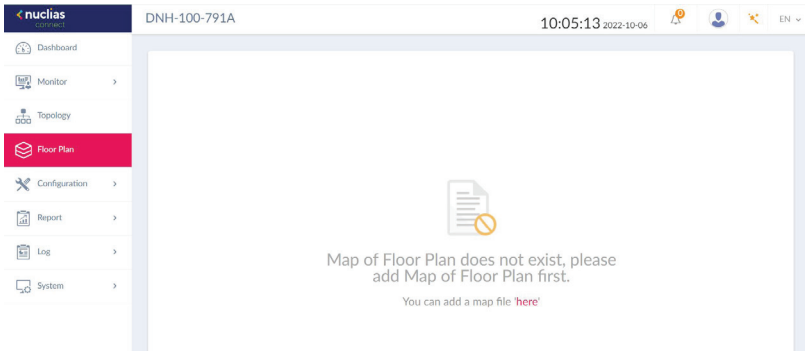
Users can also view relations between two devices by manually defining the link. Click to begin edit. Click on one of the a targeted device icon, then click another device icon to create a linkage. Once created, the Link Setting page is displayed. Below charts explain what each field entails.



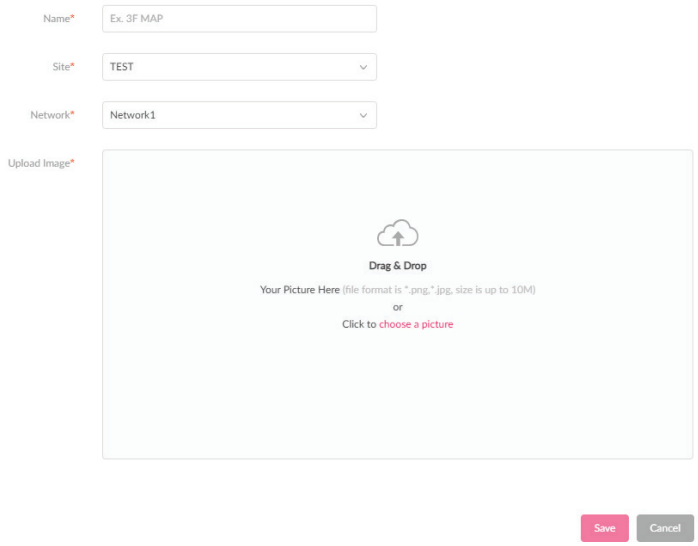

On the upper right corner, there are options available to modify and check basic information of switches and access points. Click to show Network and Device information. Click to change the background image of the topology. Click to configure the arrangement type (Star/Tree) and Central Device. Click 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 rediscovery the topology. Click to search for matching devices in the network, and finally, click to export the topology as a PDF file.

# Floor Plan

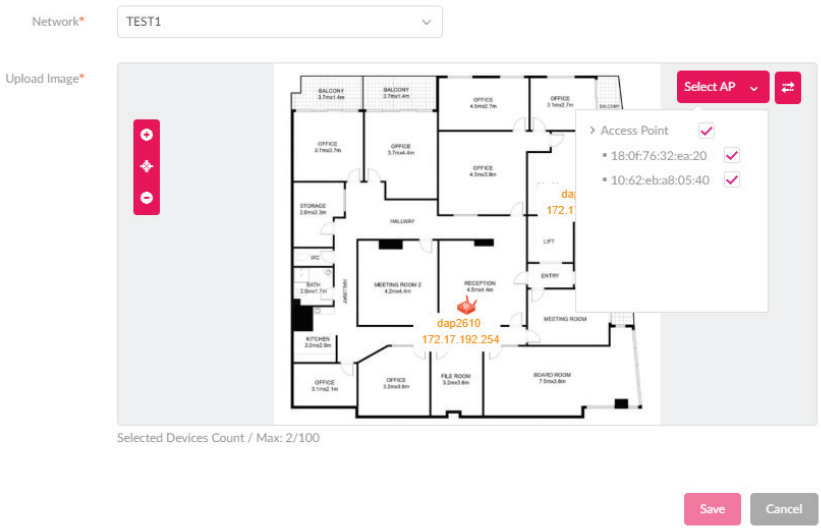
Floor plan is a drawing to scale, a bird's-eye view of the relationships between rooms, spaces, traffic patterns, and other physical features at one level of a structure. Click **Here** to add a new floor image, enter the name and select Site and Network.




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




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

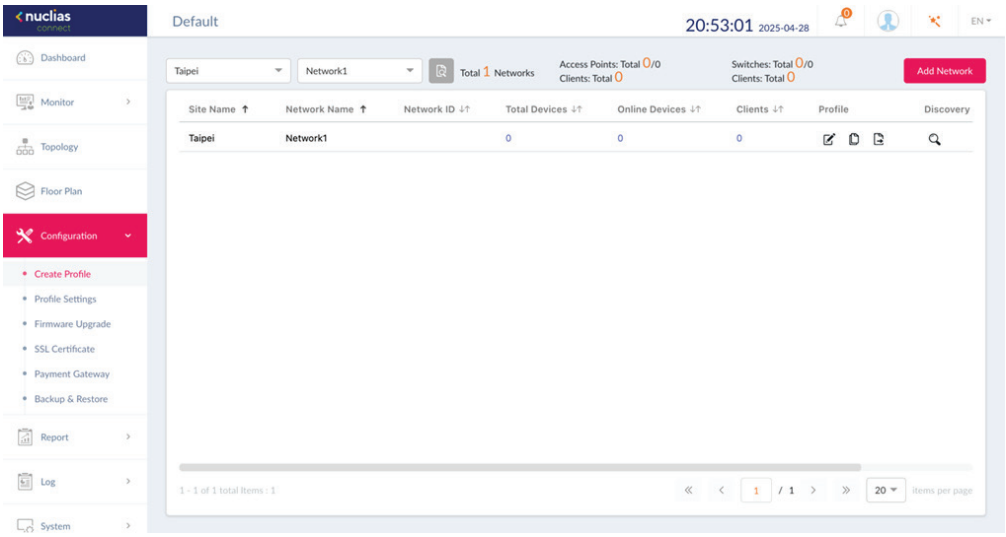



Connection status (Green: Online, Red: Offline) of the device as well as information such as name, model type, IP address, etc... can be seen when hovering the mouse over to the device icon.

# Configuration

## Create Profile

The **Create Profile** function allows for the creation of new sites and networks. Navigate to **Configuration** > **Create Profile,** click **Add Network** to create a new site and network. All available sites and networks will be listed in the Default page.



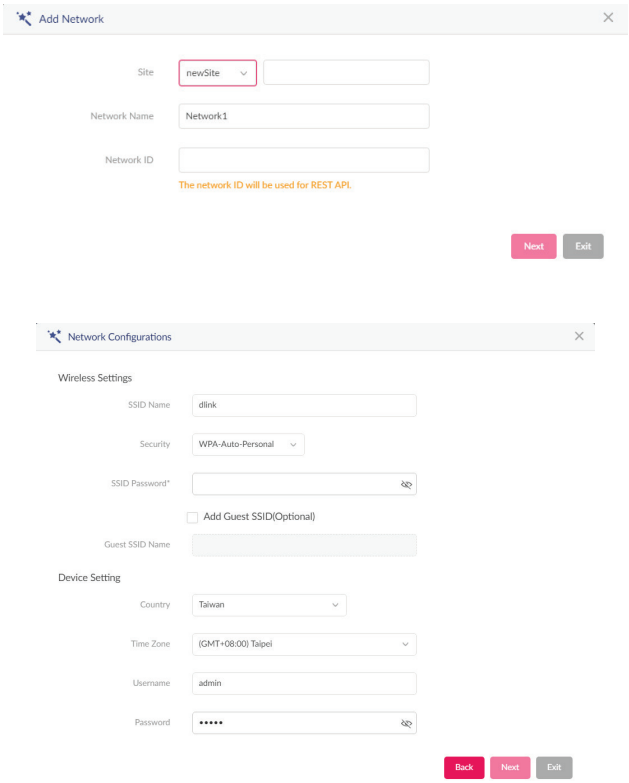

| Field | Description |
|---|---|
| **Edit Profile** | Opens site details page. Editing is available for selected site's security, access control, and user authentication settings. |
| **Copy Profile to this Network** | Copies existing profile to a designated site and network. |
| **Export Network Profile** | Exports 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 is defined, click **Next**. Click **Start Discovery** to find the results (Configurable and Managed devices) of the search. |
| **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** | Deletes the selected network configuration. |

## Add Network

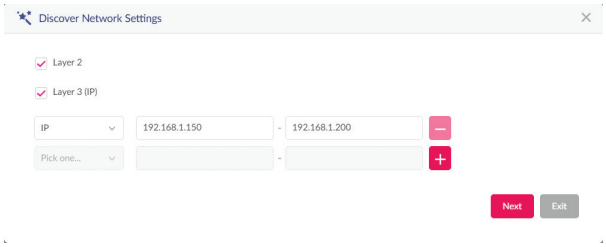
Click **Add Network** to create a new site and/or network. From the Site drop-down menu, selecting an existing site or select new Site and enter the name of the site in the empty field.

In the Network Name field, enter the name in which to identify the new network. The Network ID is an optional field. It will be used on REST API function, leave it as empty if not using REST API. Click **Next** to continue or **Exit** to return to the previous screen.

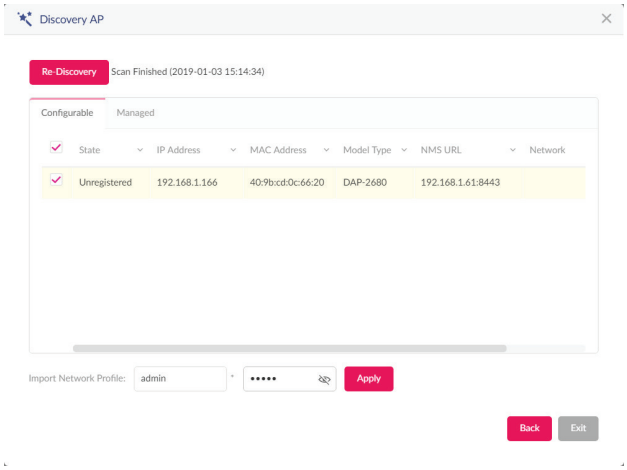
The **Network Configurations** page will appear. Enter the wireless and device settings to define the network configuration. Click **Next** to continue. To return to the previous page, click **Back** or click **Exit** to discontinue the configuration process. The Network ID field is optional and is used 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 list 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

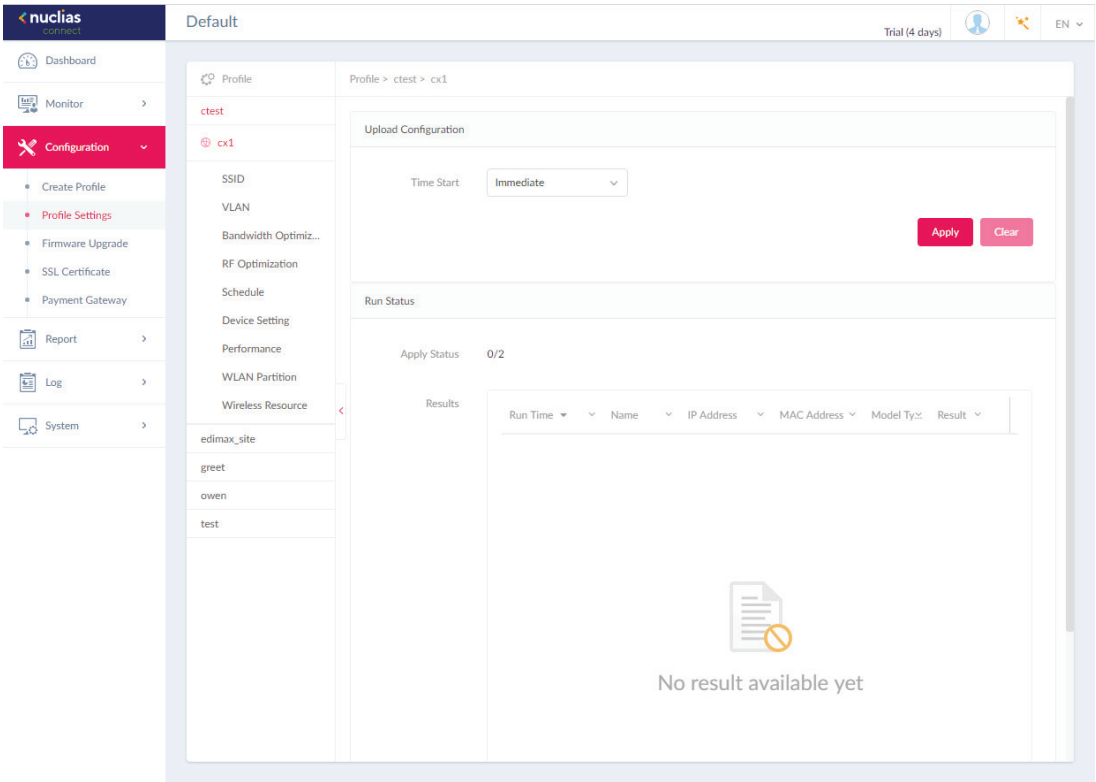
The **Profile Settings** function allows for the management of existing networks. Navigate to **Configuration > Profile Settings** to view existing sites. Select a site followed by a network to view all settings that are available for editing. site followed by a network to view all settings that are available for edit.

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 following screen will appear. The upload configuration function is available on the **Profile Settings > [Site] > [Network]** page.

For any updates to site or network configuration to take effect, the configuration must be uploaded to the access point/switch.




Under the **Upload Configuration** tab, click the **Time Start** drop-down menu and select the time **Immediate** or **Select Time** to set the time for uploading the configuration.

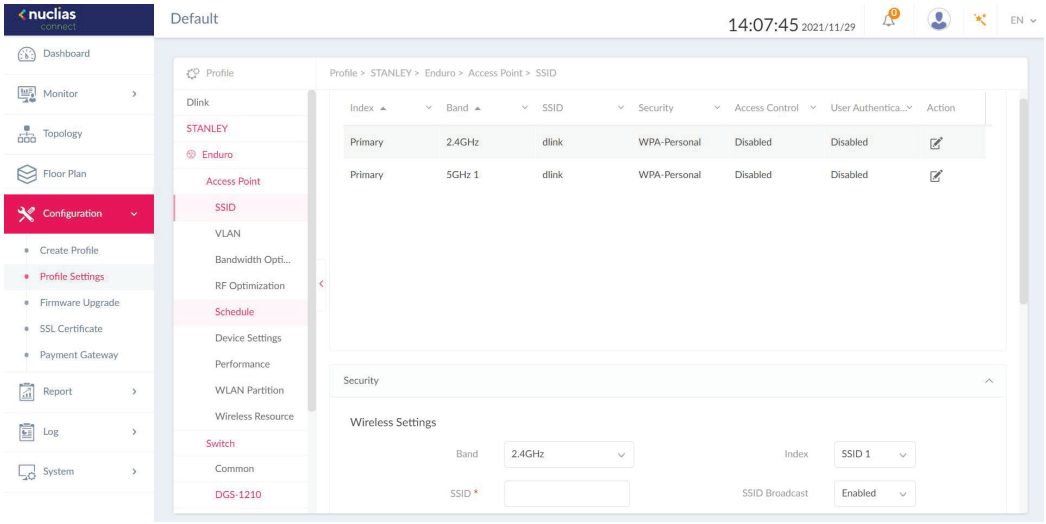
If Select Time is configured, set the day and time to upload the configuration. Once the Time Start is defined, click **Apply** to initiate the process.

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

# Access Point

## SSID

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. 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.**




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

| Wireless Settings | 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 the Nuclias Network Controller. For further information, see the 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 the Nuclias Network Controller. |
| **SSID Broadcast** | Click the drop-down menu to enable or disable the wireless SSID visibility. |
| **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). |
| **WMM (Wi-Fi Multimedia)** | Click the drop-down menu to enable or disable the Wi-Fi multimedia. |
| **Fast Roaming** | Click the drop-down menu to enable or disable fast roaming. This function is only available for compatible models and specific software version. |
| **Security Settings** | **Description** |
| **Encryption** | Click the drop-down menu to enable or disable WEP Open System encryption. The function is only available when **Security** is set as **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 Value** | Enter the open system WEP encryption key. |

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

| ACL Settings | Description |
|---|---|
| **Action** | Click the drop-down menu to select the action that will 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 the MAC address file, located on the local computer, that will be uploaded. Click **Upload** to update the MAC address list. Click **Download** to download the current MAC address list. |
| **IP Filter Settings** | **Description** |
| **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:

| Field | 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)** | Enter the session timeout value. |
| **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 whitelisted and click **Add** to add the address to the white list table. This function is only available when **Authentication Type** is **Username/Password**. |
| **Upload Whitelist File** | Click **Browser...** to select the white list file, located on the local computer, that will be uploaded. Click **Upload** to update the white list. Click **Download** to download the current white list. The function is only available when **Authentication Type** is **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**. |
| **Password** | Enter the password and click **Add**. Click **Clear** to clear the entered fields. This function is only available when **Authentication Type** is **Username/Password**. |
| **RADIUS Server** | Enter the RADIUS server's IP address. This function is only available when **Authentication Type** is **Remote RADIUS** or **MAC Address**. |
| **RADIUS Port** | Enter the RADIUS server's port number. This function is only available when **Authentication Type** is **Remote RADIUS** or **MAC Address**. |
| **RADIUS Secret** | Enter the RADIUS server's secret. This function is only available when **Authentication Type** is **Remote RADIUS** or **MAC Address**. |
| **Remote RADIUS Type** | Enter the RADIUS server's type. This function is only available when **Authentication Type** is **Remote RADIUS** or **MAC Address**. |
| **Server** | Enter the LDAP server's IP address. This function is only available when **Authentication Type** is **LDAP**. |
| **Port** | Enter the LDAP server's port number. This function is only available when **Authentication Type** is **LDAP**. |
| **Authentication Mode** | Click on the drop-down menu to select the authentication mode. This function is only available when **Authentication Type** is **LDAP**. |
| **Username** | Enter the administrator's username that will be able to access and search the LDAP database. This function is only available when **Authentication Type** is **LDAP**. |
| **Password** | Enter the administrator's password that will be able to access and search the LDAP database. This function is only available when **Authentication Type** is **LDAP**. |
| **Base DN** | Enter the base domain name of the LDAP database. This function is only available when **Authentication Type** is **LDAP**. |

| | |
|---|---|
| **Account Attribute** | Enter attribute for the account. This function is only available when **Authentication Type** is **LDAP**. |
| **Identity** | Enter the name of the administrator. This function is only available when **Authentication Type** is **LDAP**. |
| **Server** | Enter the POP3 server's IP address. This function is only available when **Authentication Type** is **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 **POP3**. |
| **Passcode List** | Display the configured front desk user accounts that have been assigned to this network and have already generated a passcode from the Web login page. This function is only available when **Authentication Type** is **Passcode**. |
| **External Captive Portal** | 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 **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. |
| **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.**<br>**Note:**<br>• Click **Preview** to preview the selected style.<br>• Click **Upload Login File** to upload a new style.<br>• Click to delete the selected style.<br>• Click to download the style template. |

In the **Hotspot 2.0** section, the following parameters can be configured:

Please note that Hotspot 2.0 is only available for compatible models and specific firmware version.[5]

| Block | Description |
|---|---|
| **Hotspot 2.0** | Click the drop-down menu to enable or disable hotspot 2.0. |
| **OSEN** | Enable OSU Server-only authenticated layer-2 Encryption Network (OSEN) to indicate that the hotspot uses a OSEN network type. |
| **Allow Cross Connection** | Choose enable to allow cross connection for clients. |
| **Manage P2P** | Choose enable to allow P2P. |
| **DGAF** | This option configures the Downstream Group Addressed Forwarding. Choose enable to allow AP to forward downstream groupaddressed frames. |
| **Proxy APR** | Choose enable to allow proxy ARP. |
| **L2TIF** | Choose enable to allow Layer 2 Traffic Inspection and Filtering. |
| **Interworking** | Choose enable to enable the interworking function. |
| **Access Network Type** | Choose from drop-down menue the access network type. |
| **Internet** | Choose to enable or disable Internet access for this network. |
| **ASRA** | Choose enable if the network has Additional Steps required for Access. |
| **ESR** | Choose enable to indicate that emergency services are reachable through this device. |
| **USEA** | Choose to enable or disable USEA. |
| **Venue Group** | Specify group venue belongs to. |
| **Venue Type** | Specify type of venue. |
| **Venue Name** | Specify name of venue. Choose from the drop down list a language used in the name. |
| **HESSID** | Specify a homogenous extended service set (ESS) ID that can be used to identify a specific service provider network. |
| **WAN Link Status** | Set information about the status of the Access Point's WAN connection from the drop-down menu. |
| **WAN Symmetric Link** | Specify state of the WAN link is symmetric (upload and download speeds are the same). |
| **WAN At Capacity** | Specify yes if the Access Point or the network is at its max capacity, or specify no if not. |
| **WAN Metrics DL Speed (kps)** | The downlink speed of the WAN connection set in kbps. If the downlink speed is not known, set to 0. |

| | |
|---|---|
| **WAN Metrics UL Speed (kps)** | The uplink speed of the WAN connection set in kbps. If the uplink speed is not known set to 0. |
| **Network Auth Type** | Choose from drop-down menu the network authentication type and specify the web-address. |
| **IP Address Type Availability** | Choose from drop-down menu the IP address version and type that the Hotspot Operator uses and that would be allocated and available to a mobile device after it authenticates to the network. Click Delete icon to delete it from the list. |
| **Domain Name** | List one or more domain names for the entity operating the AP. |
| **Roaming Consortium** | Add service providers or groups of roaming partners whose security credentials can be used to connect to a network. Click Delete icon to delete it from the list. |
| **Nai Realm** | Specify list of all NAI realms available through the BSS. Click subtract icon to delete it from the list. |
| **EAP Method** | Specify one or more EAP methods and its authentication ID and Parameter type. Click Delete icon to delete it from the list. |
| **RFC 4282** | Click on drop-down menue to enable or disable RFC 4282. |
| **3gpp Cellular Network** | Specify a list of the 3GPP cellular networks available through the AP. Spcify the MCC and MNC, then click Add icon. Click Delete icon to delete it from the list. |
| **Connection Capability** | Specify a list of common IP protocols (TCP, UDP, IPsec) and ports (21, 80, 443, 5060), specify its port number and the status of the IP protocol and click Add. Click Delete icon to delete it from the list. |
| **Operator Friendly Name** | Identifies the Hotspot venue operator and choose its language. |
| **OSU SSID** | Specify OSU SSID name. |
| **OSU Server URI** | Specify OSU Server URI. |
| **OSU Method** | Specify a list of OSU methods by choosing its language and then specifying a method by clicking Add. Click Delete icon to delete it from the list. |
| **OSU Config** | Choose from drop-down menu the OSU Configu. |
| **OSU Language Code** | Choose a language from the drop-down menu. |
| **OSU Friendly Name** | Choose a language from the drop-down menu and specify the OSU friendly name. |
| **OSU Nai** | Specify the OSU NAI. |
| **OSU Service Description** | Specify a service description for the OSU. |
| **OSU Icon Language Code** | Specify from drop-down menu the language of the icon. |
| **OSU Icon File Path** | Specify location of icon file. |
| **OSU Icon File Name** | Specify icon file name. |
| **OSU Icon Width** | Specify width of the icon, in pixels. |
| **OSU Icon Height** | Specify length of the icon, in pixels. |
| **OSU Icon Type** | Specifiy icon file type from the drop-down menu. |

5 As of the time of writing, only DAP-2662 and DAP-3666 support this function.

Click **Add** to save the values and update the screen.
Click **Clear** to reset all settings.

## VLAN

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

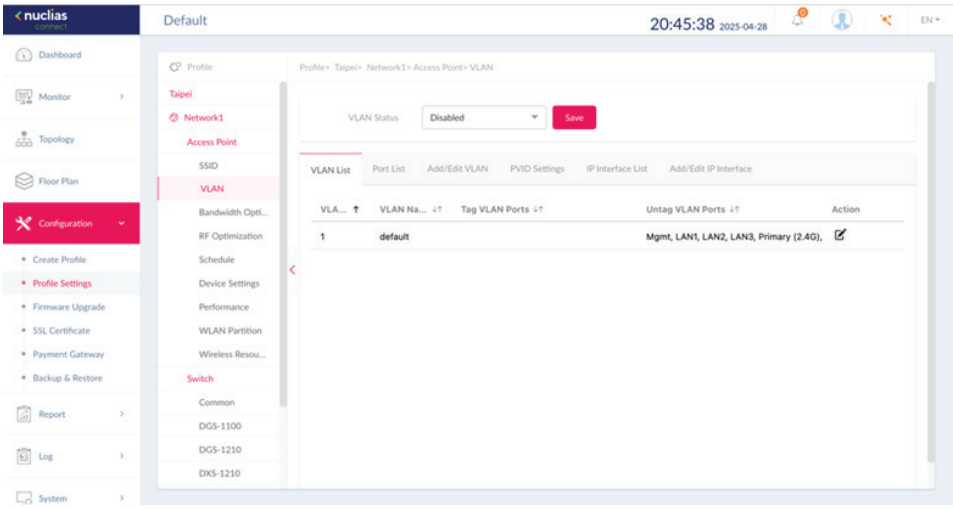
| Field | Description |
|---|---|
| **VLAN Status** | Click the drop-down menu to enable or disable VLANs. |

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 indicates the available 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, we can create a new VLAN and assign untagged ports in 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 client 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** for further information.

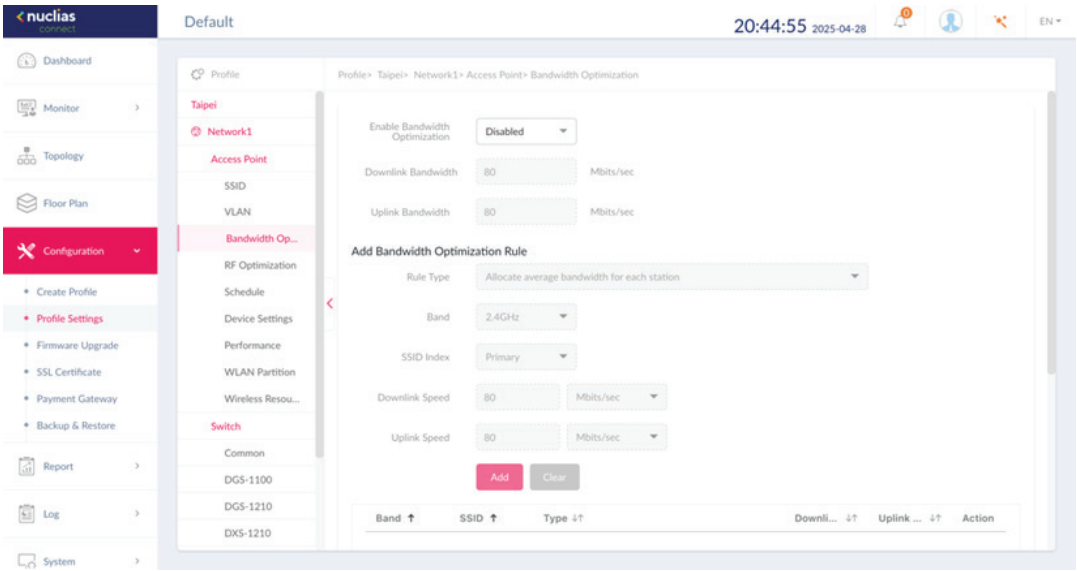
## Bandwidth Optimization

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

| Field | 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.<br>• Allocate an average BW for each station: Optimize bandwidth by averaging the allocated bandwidth for each client.<br>• Allocate a maximum BW for each station: Specify the maximum bandwidth for each connected client, while reserving available bandwidth for additional clients.<br>• 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.<br>• 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** for further information.



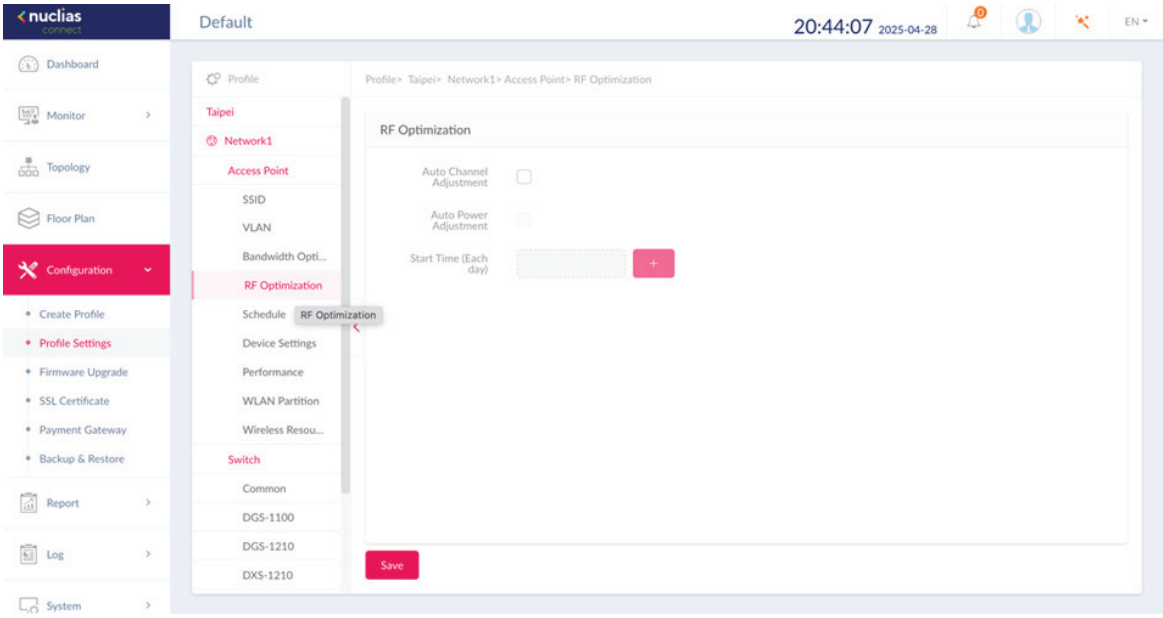
## RF Optimization

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** 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 existing settings.

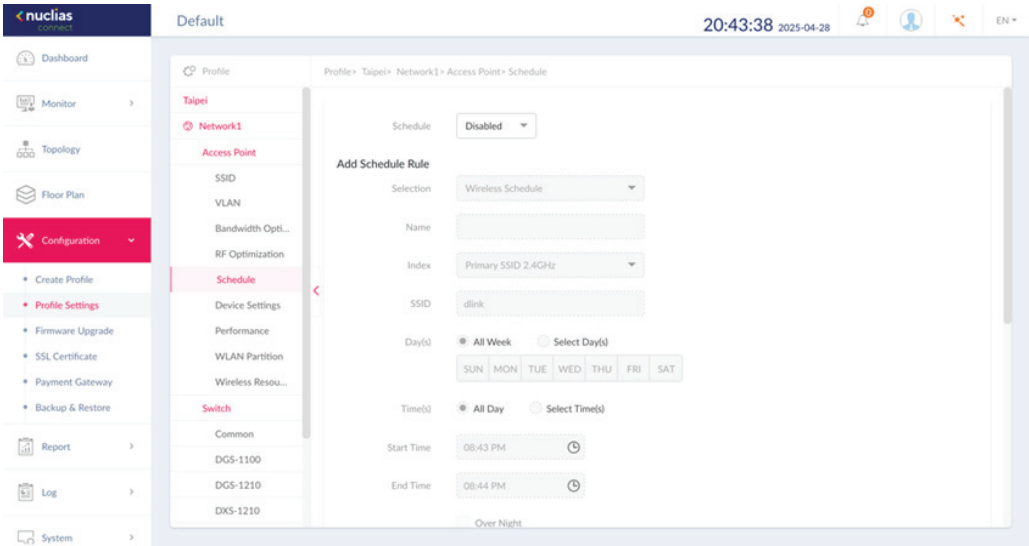
| Parameter | Description |
|---|---|
| **Wireless Schedule** | Click the drop-down menu to enable or disable the wireless schedule function. |
| **Name** | Enter the name of the schedule rule. |
| **Index** | Click the drop-down menu to select SSID on which the schedule setting is applied. |
| **SSID** | Display the SSID name. |
| **Day(s)** | Click the radio button to select the active days for the schedule.<br>• All Week: Enable the rule for the whole week.<br>• Select Day(s): Specifies particular day(s) to activate the rule. |
| **Time(s)** | Click the radio button to select the active times for the schedule.<br>• All Day: Enable the rule for the whole day.<br>• Select Time(s): Specifies a starting and ending time for the rule. |
| **Start Time** | Enter the hours and minutes of the day. This function is only available when **Time(s)** is **Select Time(s)**. |
| **End Time** | Enter the hours and minutes of the day. This function is only available when **Time(s)** is **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** for further information.



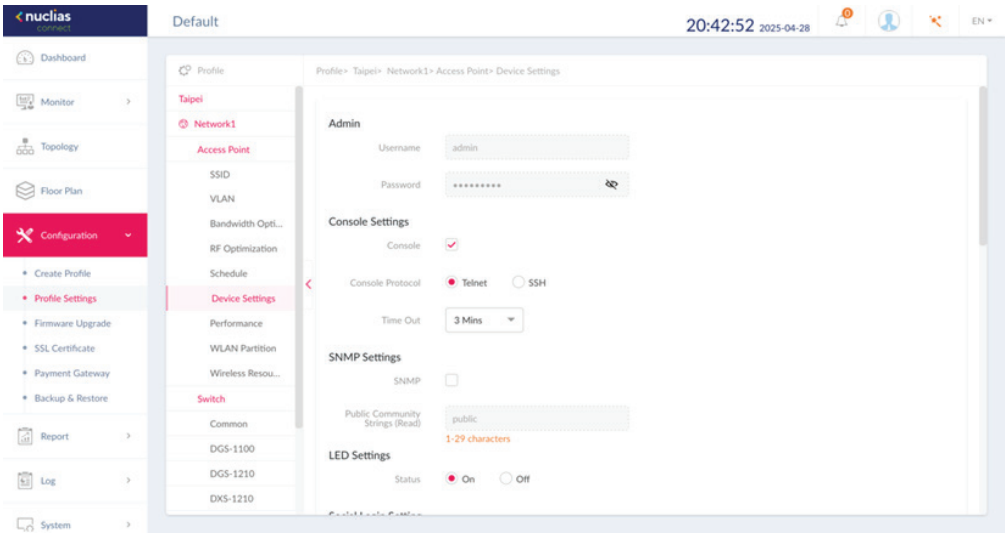
## Device Settings

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 on this page 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** for further information.



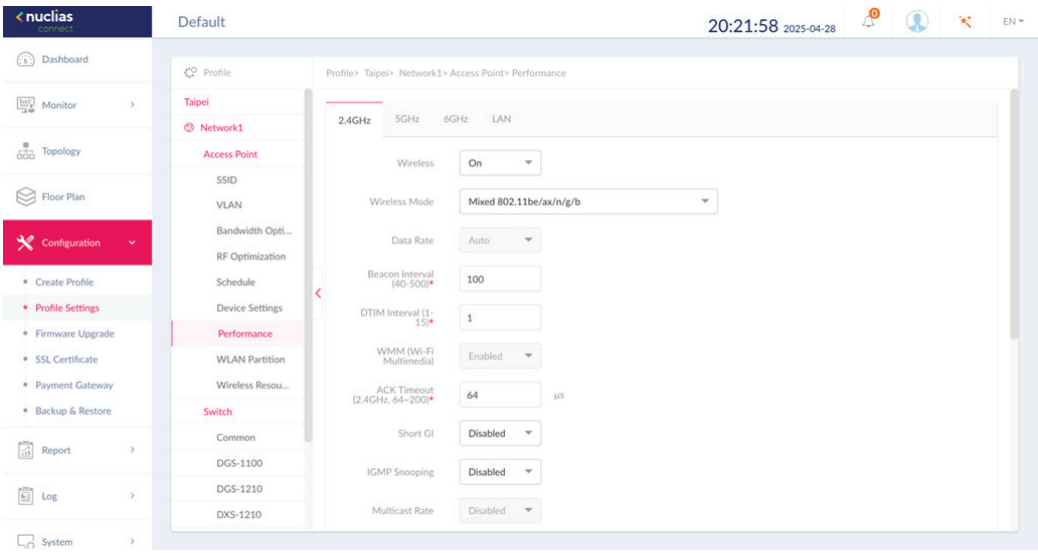
## Performance

The **Performance** 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] > Device Setting** 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 **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)** | Click the drop-down menu to enable or disable the Wi-Fi Multimedia (WMM) function. |
| **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** | Enter the maximum multicast bandwidth value. The default value is 100. The function is only available when **Multicast Bandwidth Control** is **Enabled**. |
| **HT20/40 Coexistence** | Click the drop-down menu to enable or disable the HT20/40 coexistence function. |
| **Change DHCPOFFER 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.

- **2.4GHz / 5GHz / 6GHz**




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

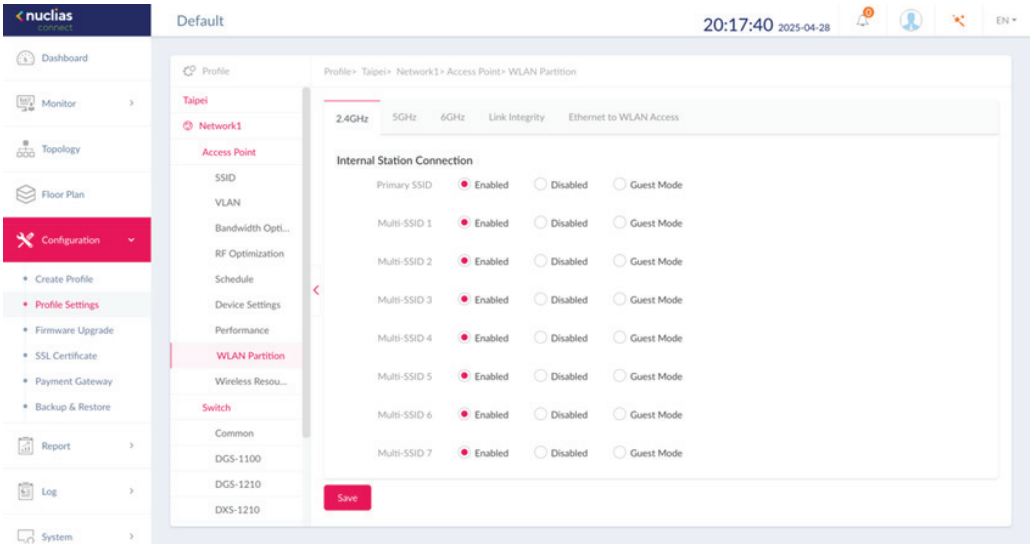
- **LAN**

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 point 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** for further information.

## WLAN Partition

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 for further information.

- **Link Integrity**

  The Link Integrity feature disassociates wireless segments from the AP when the LAN and AP is 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** for further information.

- **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.

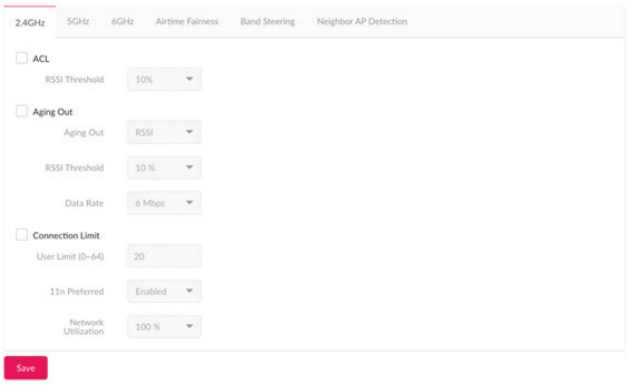

  Click **Save** to save the changes. Once the settings are updated, the configuration must be uploaded to the access points. See **Profile Settings** for further information.

## Wireless Resource

The **Wireless Resource** function in Nuclias Network Controller 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** | Use the drop-down menu to select criteria to disconnect wireless clients. Available options are RSSI and Data Rate. |
| **Aging Out** | Click the drop-down menu to select the aging out mode |
| **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 a 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 when 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** for further information.

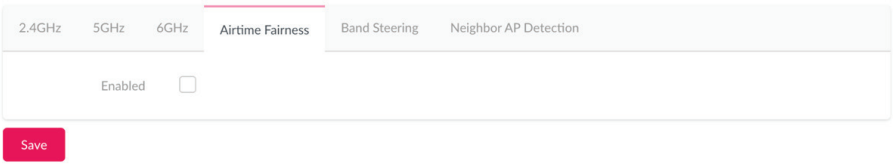
- **Airtime Fairness**

  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 WiFi speed can be slow from either long physical distances, 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 setting.

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

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



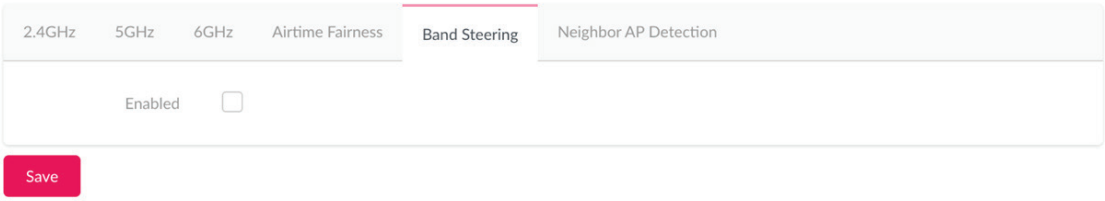

Once the settings are updated, the configuration must be uploaded to the related access points. See **Profile Settings** for further information.

- **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 those clients who support 2.4GHz only.

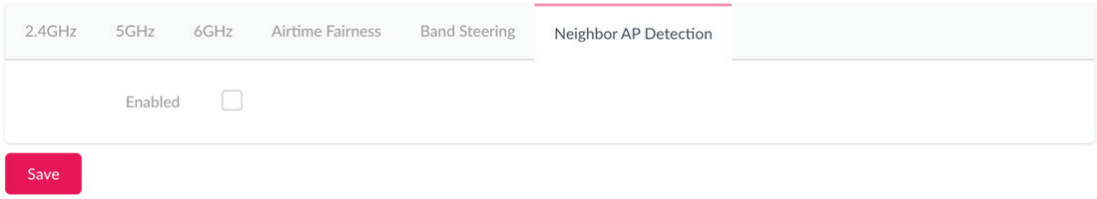
  Navigate to **Configuration > Profile Settings > [Site] > [Network] > Wireless Resource**. Click on the **Band Steering** tab to view the existing setting.

  Check the box to enable or disable the wireless band steering function.
  Click **Save** to save the values and update the screen.




- **Neighbor AP Detection**

  Users can view neighbor information on a specified AP radio to determine the AP location and neighbor relationship, help locating rogue APs and plan the WLAN.
  Check "**Enabled**" to enable detection and go to **Monitor>Neighbor AP** to review AP list.



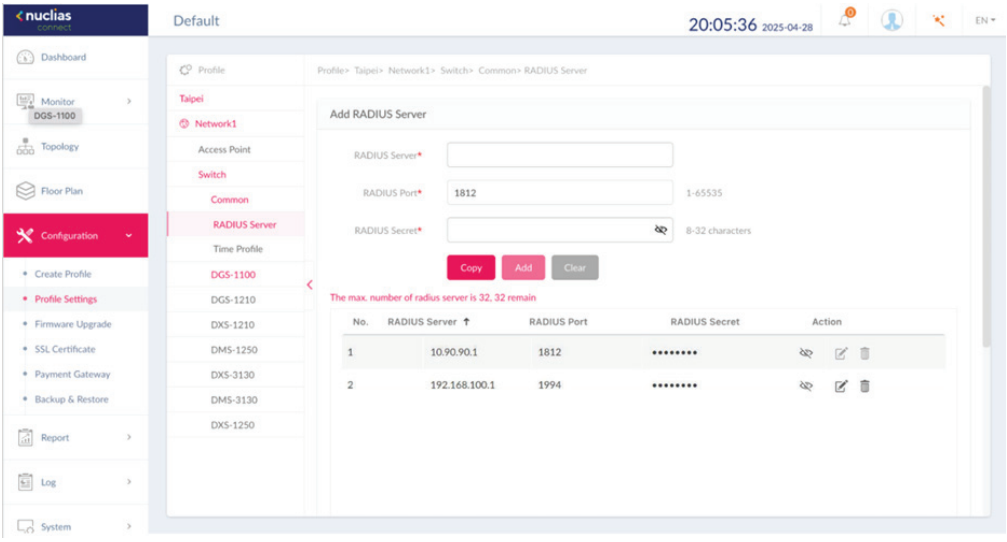
# Switch

## Common

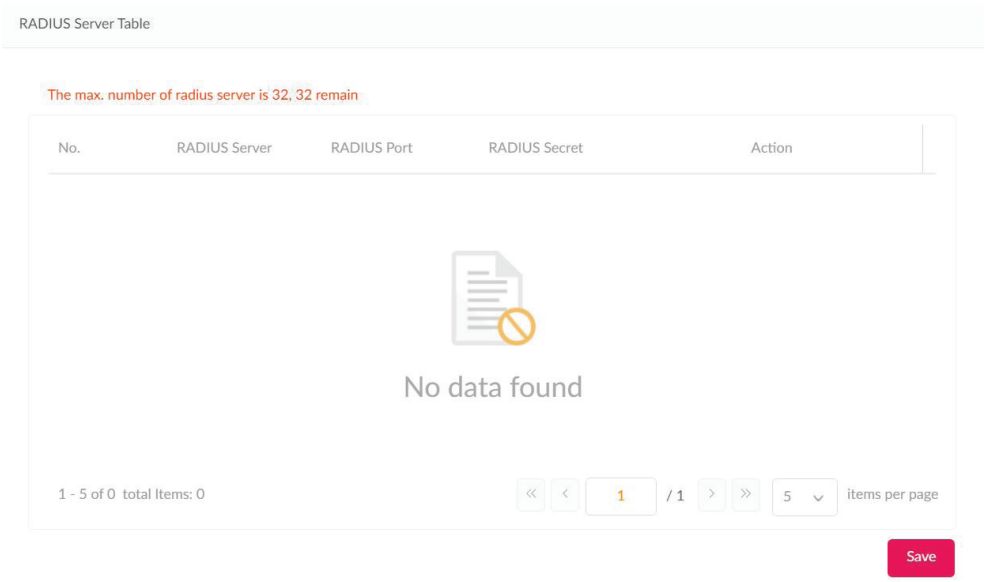
- **RADIUS Server**

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 re mote 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 other network. Once completed, click **Add** to add a new RADIUS server, or **Clear** to remove the entries.



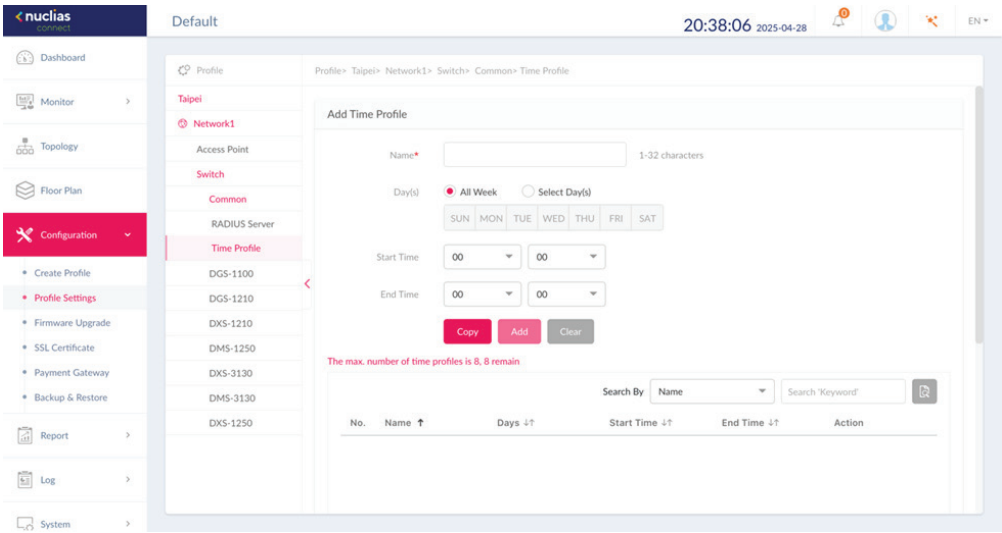

In the **RADIUS Server Table** below, a summary of all the RADIUS Servers details including the **number, RADIUS server, port** and **secret** is displayed. Under the Action field, click to edit the RADIUS server. Click to delete the selected RADIUS server. Click **Save** when completed.



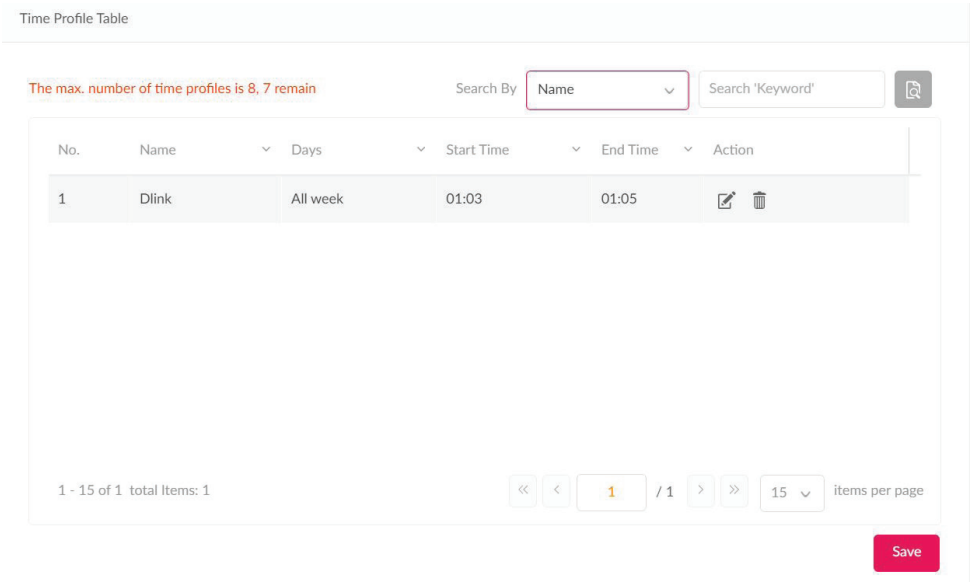
- **Time Profile**

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 other 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.



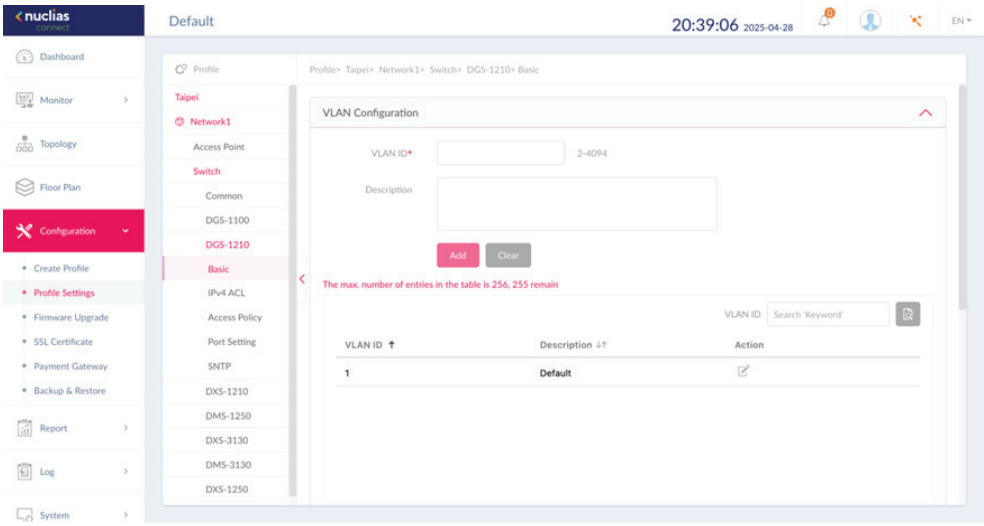
## Basic

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.

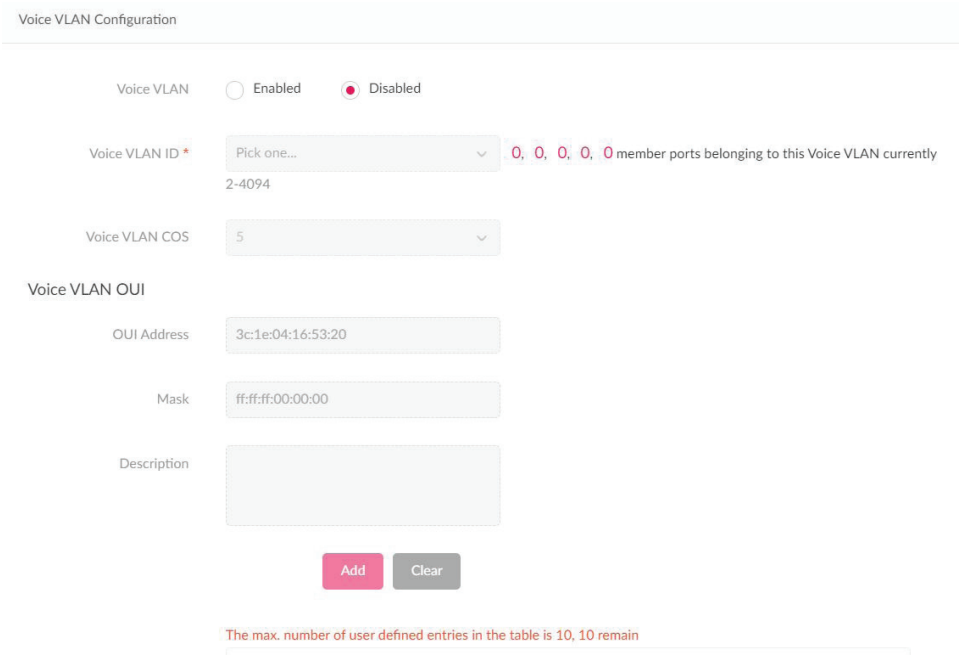
In the VLAN List section, a summary of VLAN is dispalyed. Enter keyword in the VLAN ID search field to locate a VLAN. Click to start the search. Under the Action field, click to edit a VLAN. Click to delete a VLAN. Click **Save** when complete.



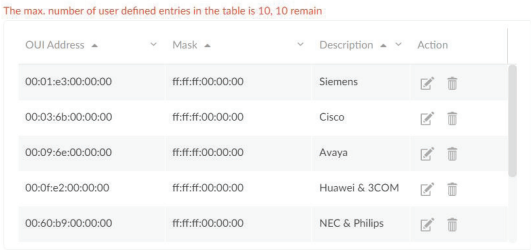

### Voice VLAN Configuration

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 entires can be entered.

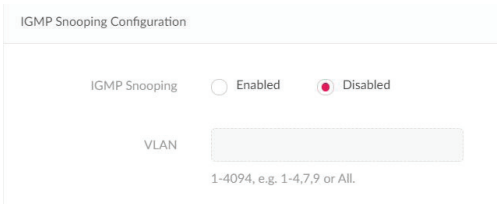


When Voice VLAN is enabled, a default Voice VLAN OUI list is displayed in the summary list below. These entries cannot be edited nor deleted.



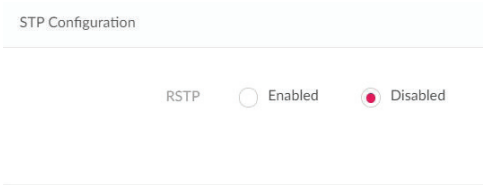

**IGMP Snooping Configuration**

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.



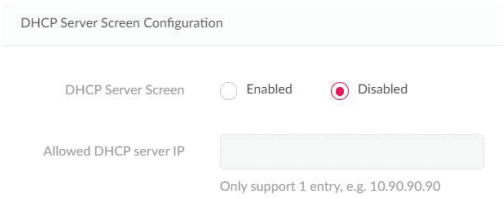

**STP Configuration**

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.



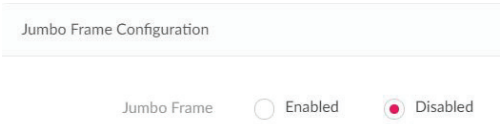

**DHCP Server Screen Configuration**

DHCP (Dynamic Host Configuration Protocol) server screening provides a 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.



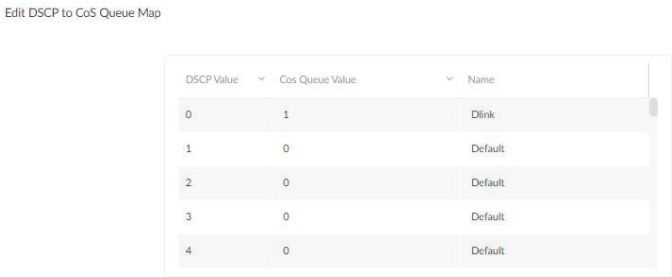

**Jumbo Frame Configuration**

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**.

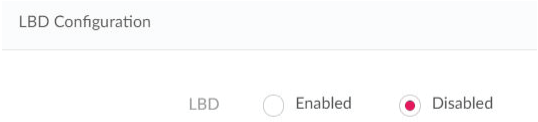


**Quality of Service**
The **QoS** feature can prioritize certain types of data with the use of differentiated services model. The priorities are marked in each packet using Differentiated Services Code Point (DSCP) for traffic classification. To set the DSCP to CoS (Class of Service) queue, choose a 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.

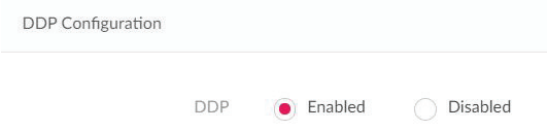



**LBD Configuration**
The Loopback Detection (LBD) feature can detect loops occurring on one or across different ports. In the LBD field, click **Enabled** to turn on the feature. It is disabled by default.

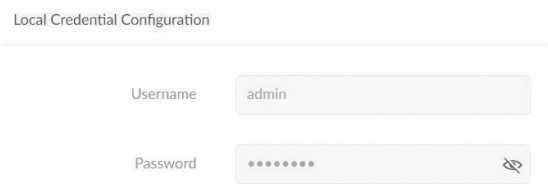



**DDP Configuration**
The D-Link Discovery Protocol (DDP) is a communication protocol defined by D-Link. When enabled, your device will become discoverable and can be managed by the DNC server. Features from DNA (D-Link Network Assistant) like IP settings, firmware upgrade, reboot and reset function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



## IPv4 ACL

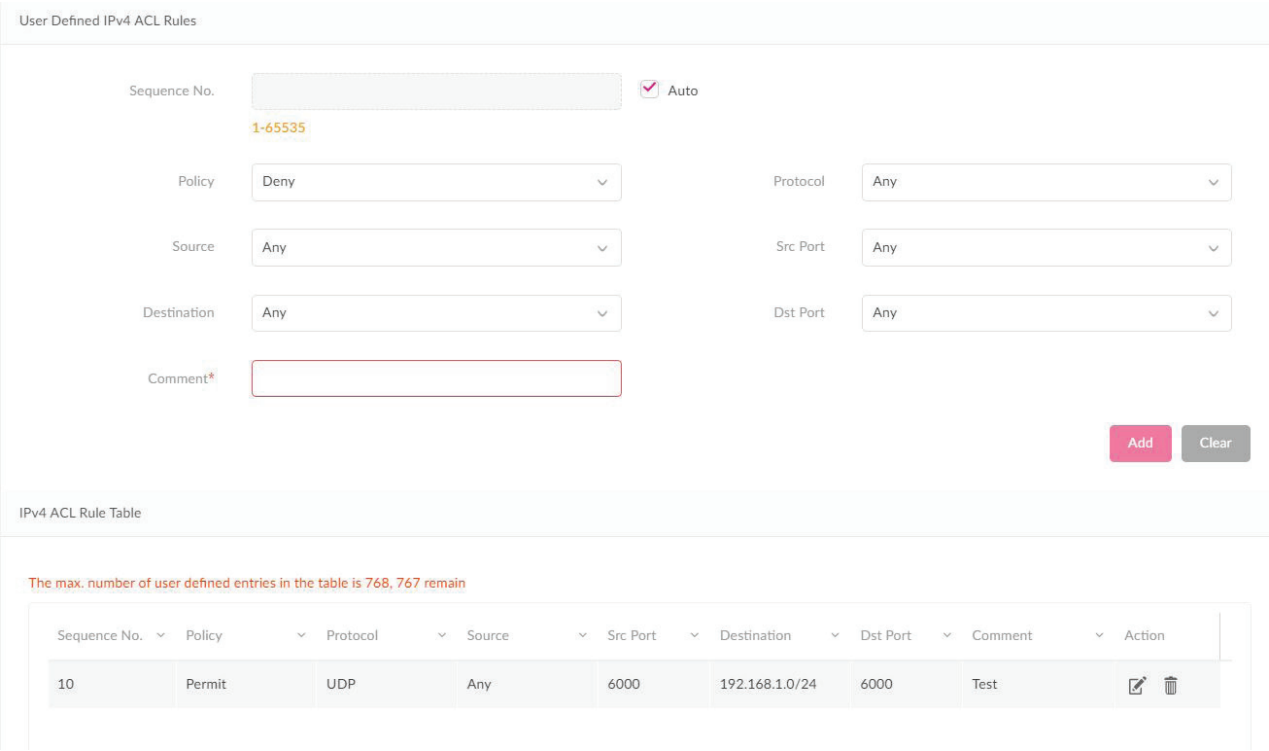
The **IPv4 ACL** (Access Control List) feature for the switch can help improve network performance and security by blocking selected traffic. Navigate to **Configuration** > **Profile Settings** > **Site** > **Network** > **Switch** > **Your Device** > **IPv4 ACL** to configure the settings.

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

| Field | Description |
|---|---|
| **Sequence No.** | Set the sequence number from 1 to 65535, or select **Auto** to auto-assign the sequence number. |
| **Policy** | Select to permit or deny what traffic goes through the switch. |
| **Source** | Enter the source IP address. When the Protocol is set to **Any**, all traffic destination 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 from 0 to 65535. When the Src Port is set to **Any,** all traffic sources will be evaluated. |
| **Dst Port** | Specify the number of the destination port from 0 to 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.

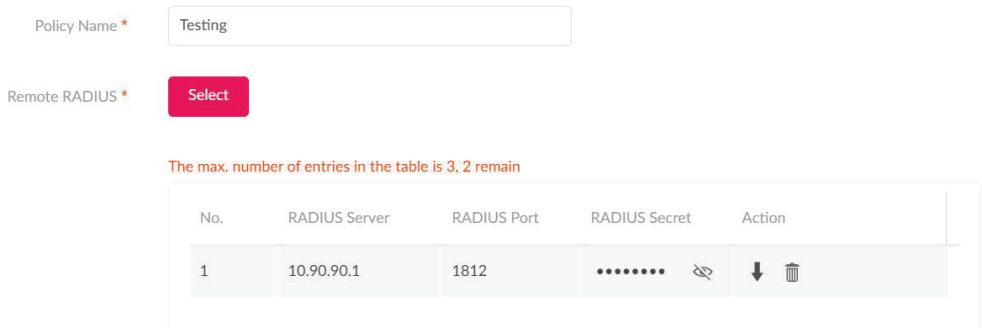


## Access Policy

D-Link switches support 802.1X authentication, MAC authentication and port security to prevent unauthorized client 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.

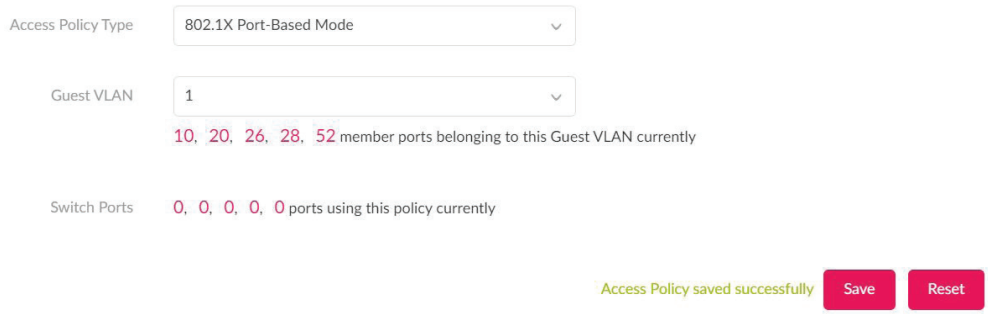
Once the RADIUS Servers is selected, a summary of the RADIUS servers will be listed in the table. In the **Action** field, click to move the entry up, click to move the entry down. Click to delete the entry.




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.



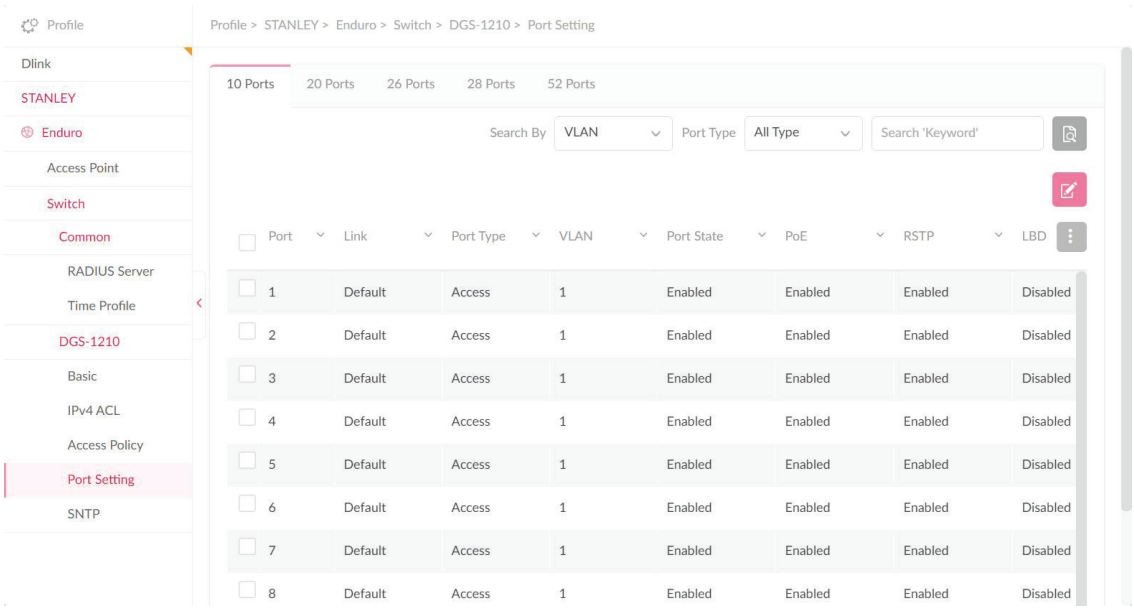
## Port Setting

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.

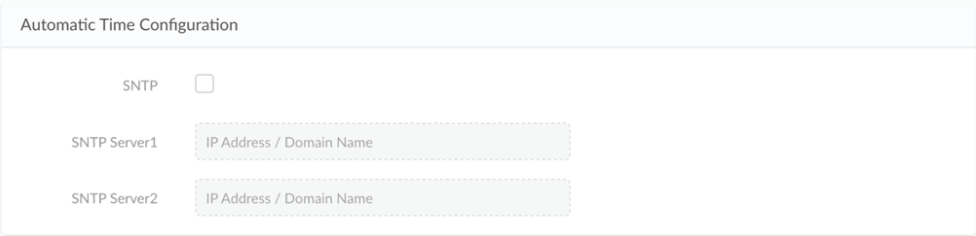


## SNTP

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.

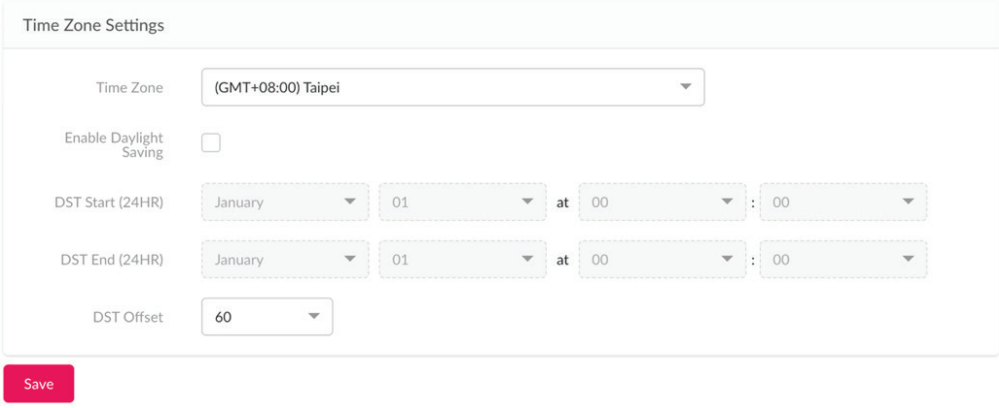
Under the SNTP tab, you can configure **Automatic Time Configuration** and **Time Zone Settings**.

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 saving 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

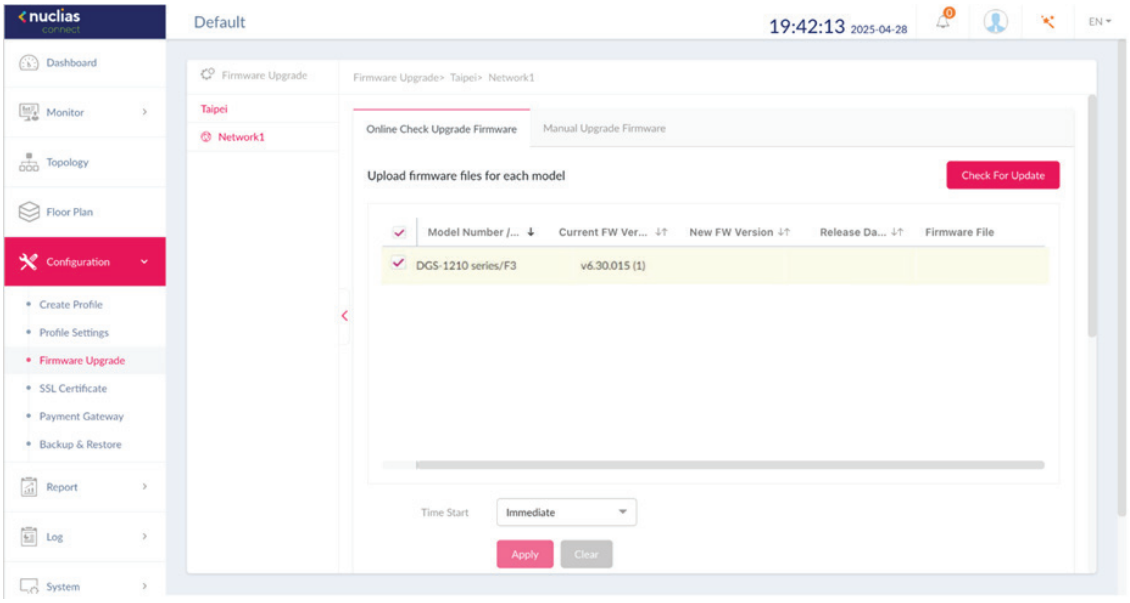
The **Firmware Upgrade** function allows users to perform a firmware upgrade. For online update, please confirm your device is online. For manual upgrade, please visit D-Link website of your region to see if newer firmware available.

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

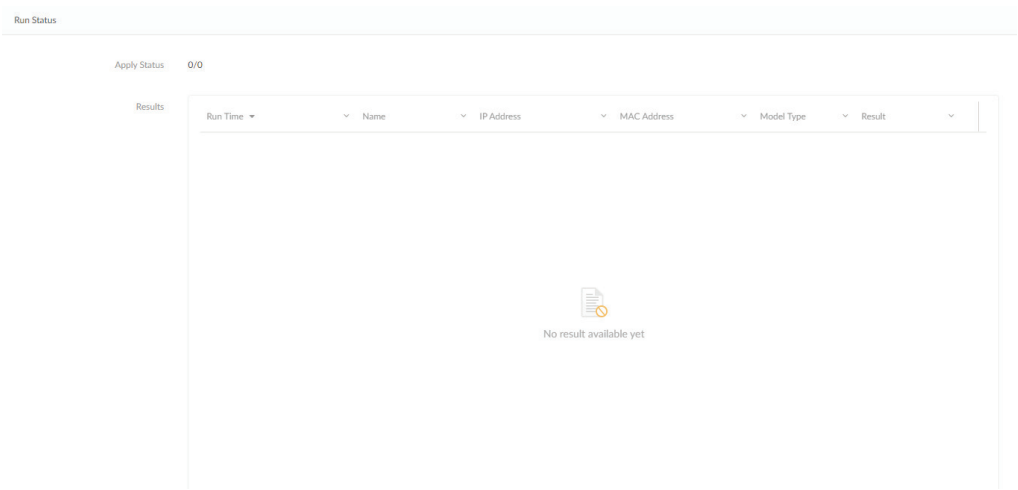
| Block | Description |
|---|---|
| **Online Check Upgrade Firmware** | Click to configure online upgrade. |
| **Check For Update** | Click to check if newer firmware is available on online server. |
| **Manual Upgrade Firmware** | Click to configure manual upgrade. |
| **Change** | Click to select a 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 result 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**.



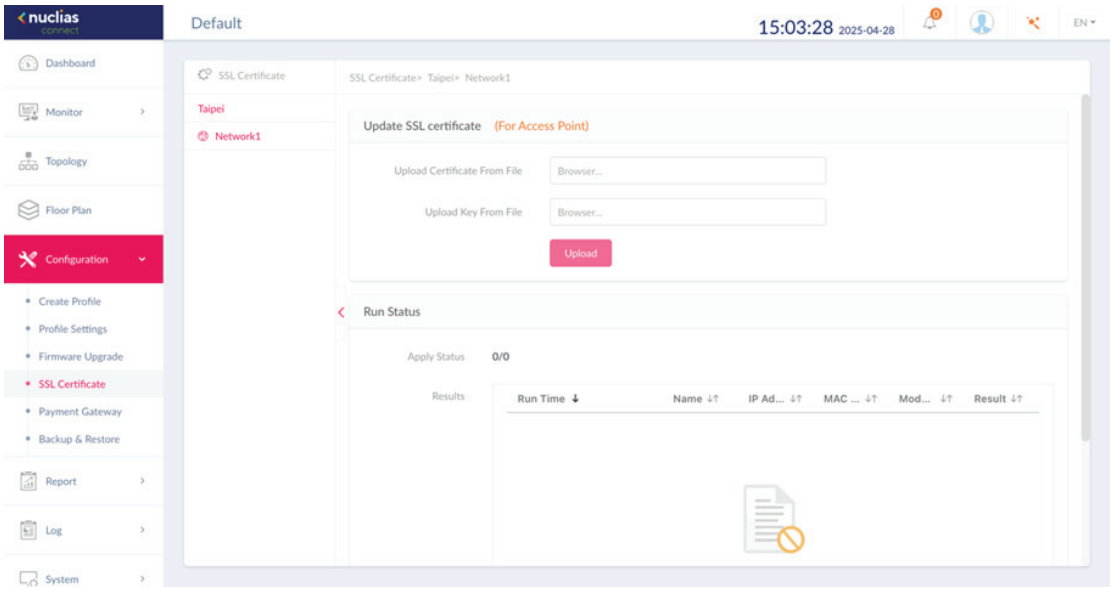
# SSL Certificate

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. Please reboot your APs after you uploaded certificate.

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

| Options | Description |
|---|---|
| **Upload Certificate From File** | Click **Browser...** to select the SSL certificate file located on the drive that will be uploaded. |
| **Upload Key From File** | Click **Browser...** to select the SSL key file located on the local drive that will be uploaded. |

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



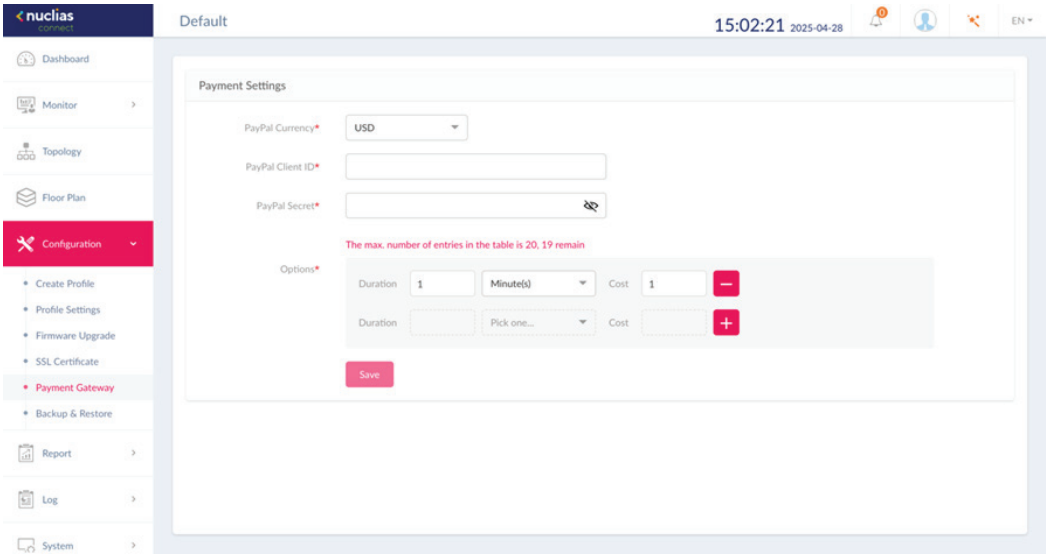
# Payment Gateway

The **Payment Gateway** function 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.



# Backup & Restore

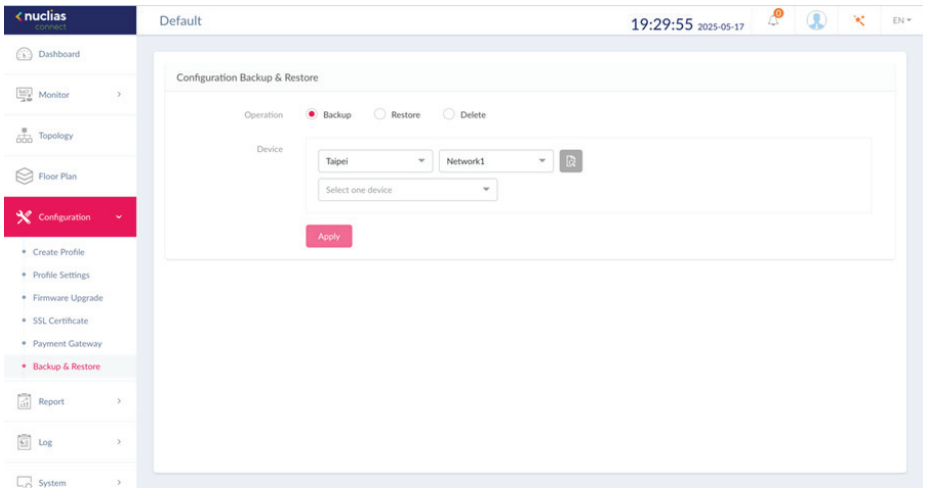
The **Backup & Restore** function allows users to back up and restore the device configuration. This feature currently only supports managed switch series.

## Backup

Navigate to **Configuration > Backup & Restore**.

Select **Backup**.

Select a device from the network of a site to perform a configuration backup.

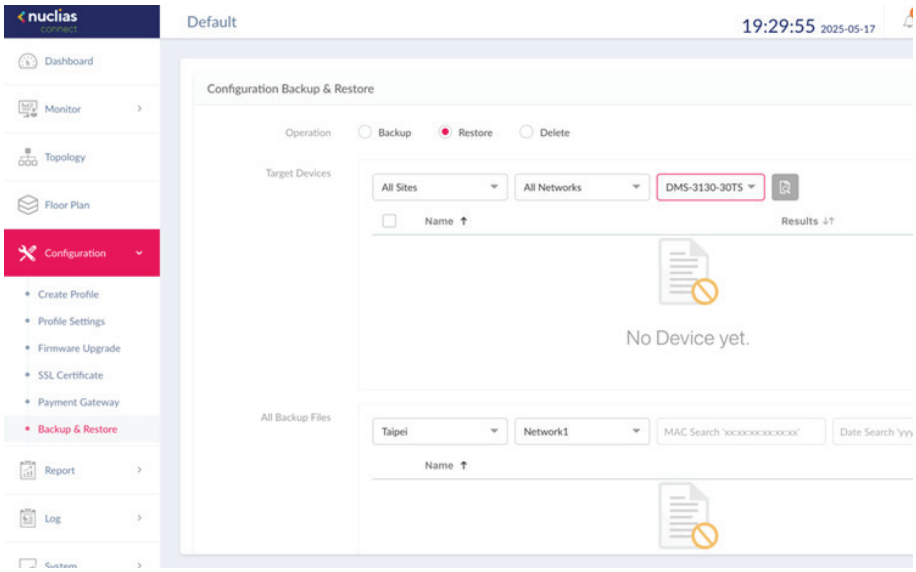



## Restore

Navigate to **Configuration > Backup & Restore**.

Select **Restore**.

In the **All Backup Files** field, select the file to be used for restoration, and in the **Target Devices** field, choose the device(s) to be restored, which can be one or multiple.



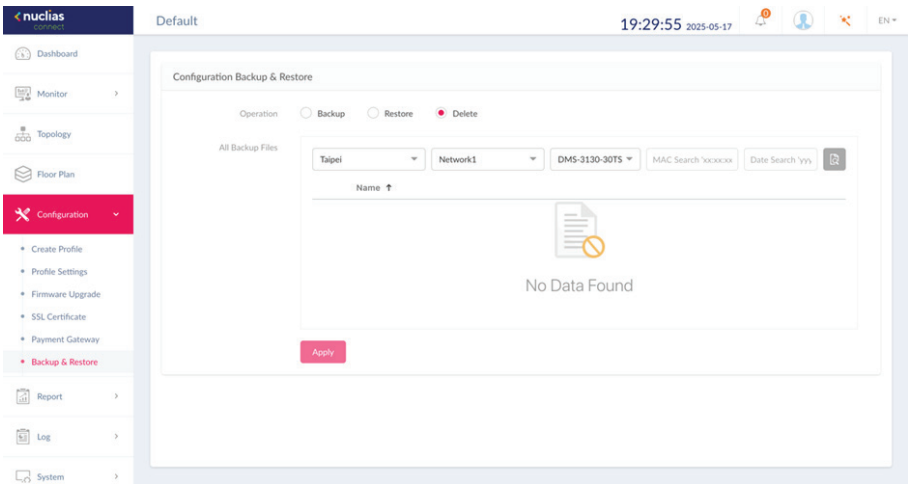

**Note**: Restore typically excludes network configuration parameters (IP address/VLAN/Gateway/DNS), unless the option **Restore includes network configuration parameters (IP address/VLAN/Gateway/DNS)** is selected.

## Delete

Navigate to **Configuration > Backup & Restore**.

Select **Delete**.

In the **All Backup Files** field, the selected file will be deleted.



# Report

## Access Point

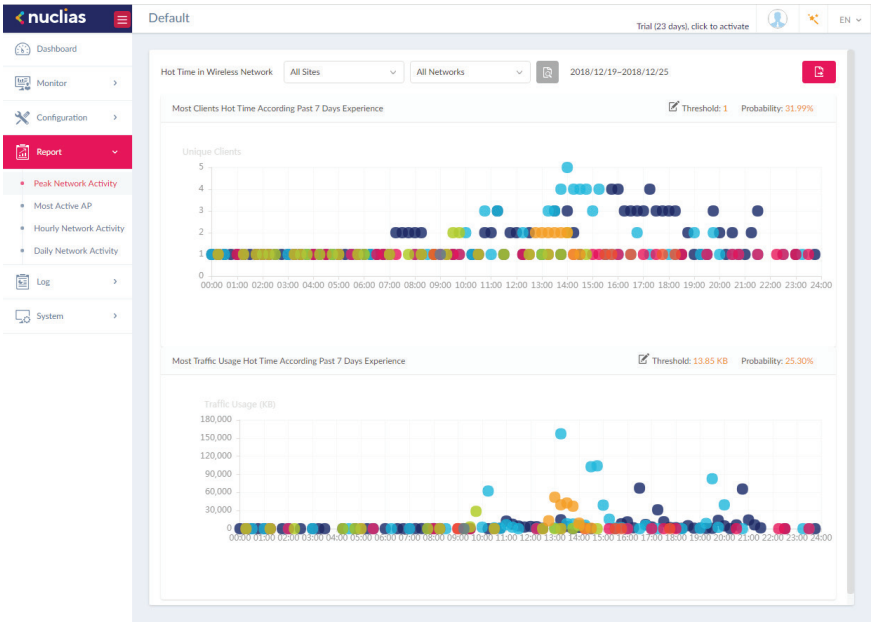
### Peak Network Activity

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.



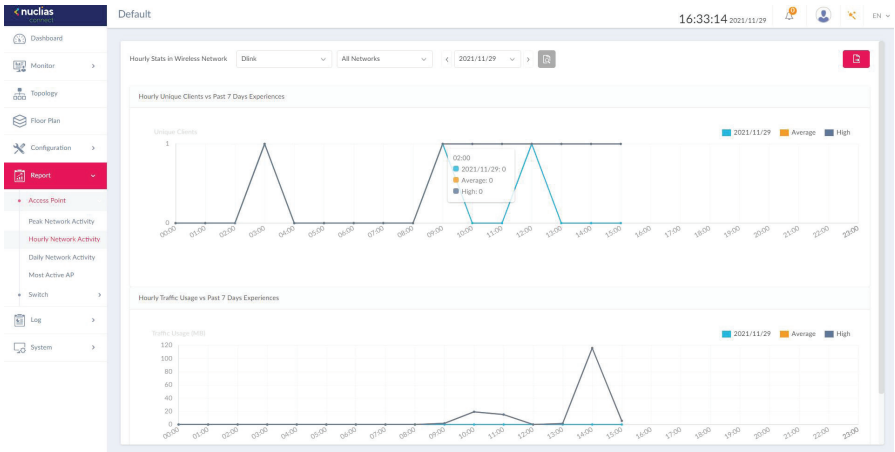
# Hourly Network Activity

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 > 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.



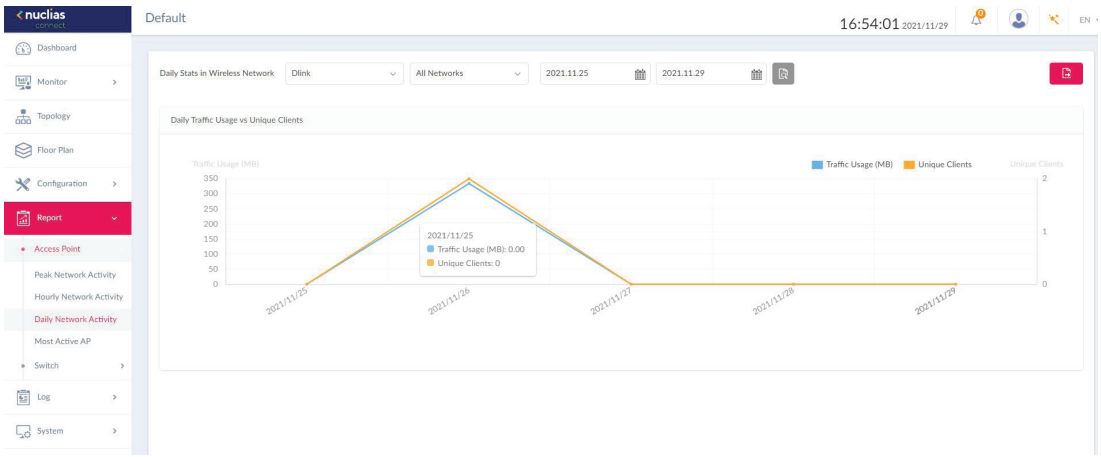
# Daily Network Activity

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 > 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.

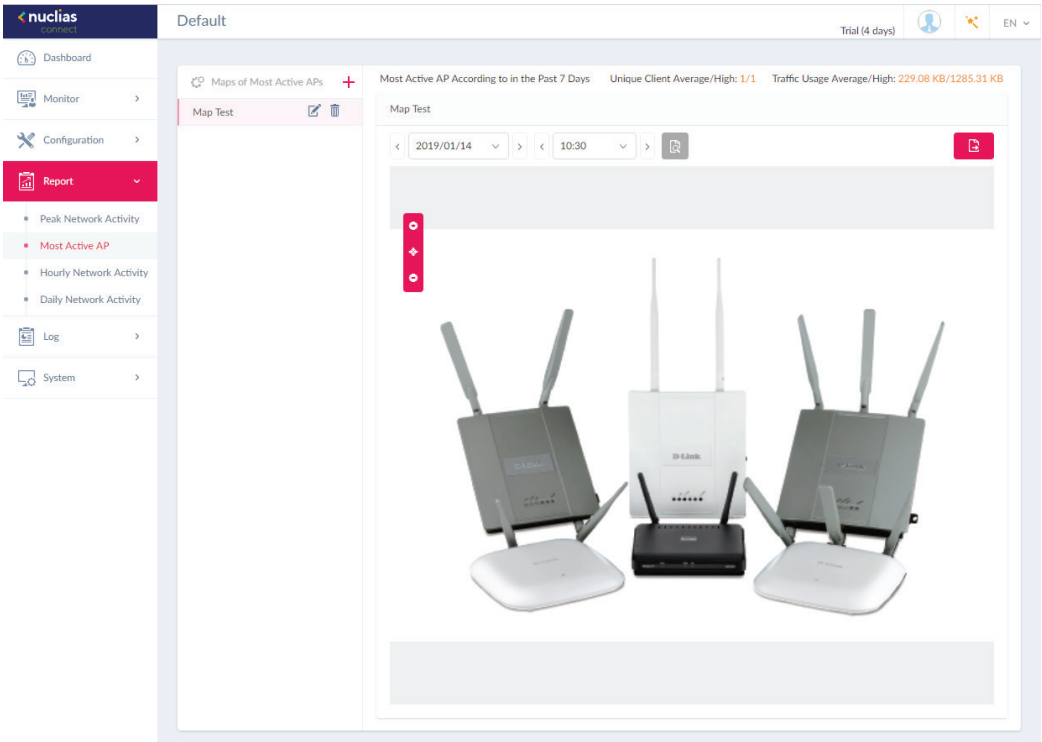


# Most Active AP

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 name 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 the image.

To view a network AP active map report, select the date and time then click to view the report.
Once a report has been generated, click to save the report to a local PDF file.



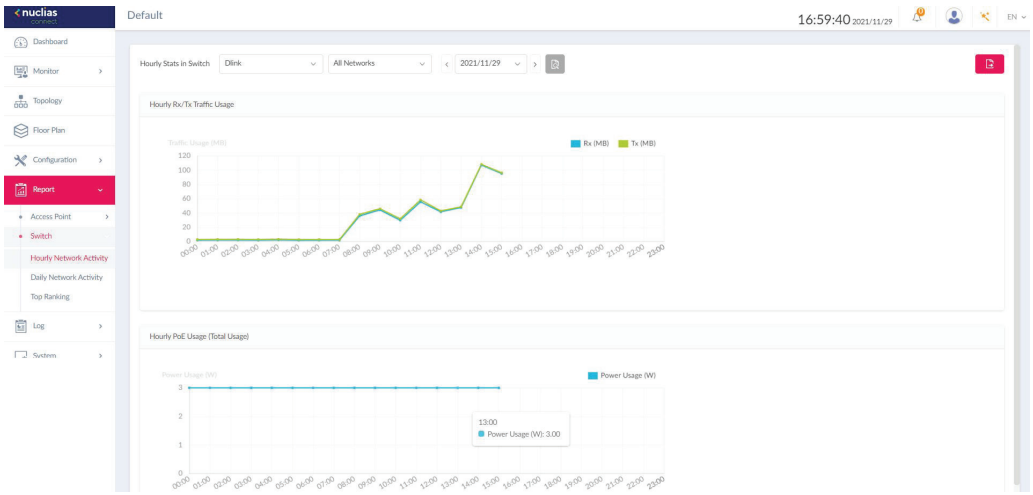
# Switch

## 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.

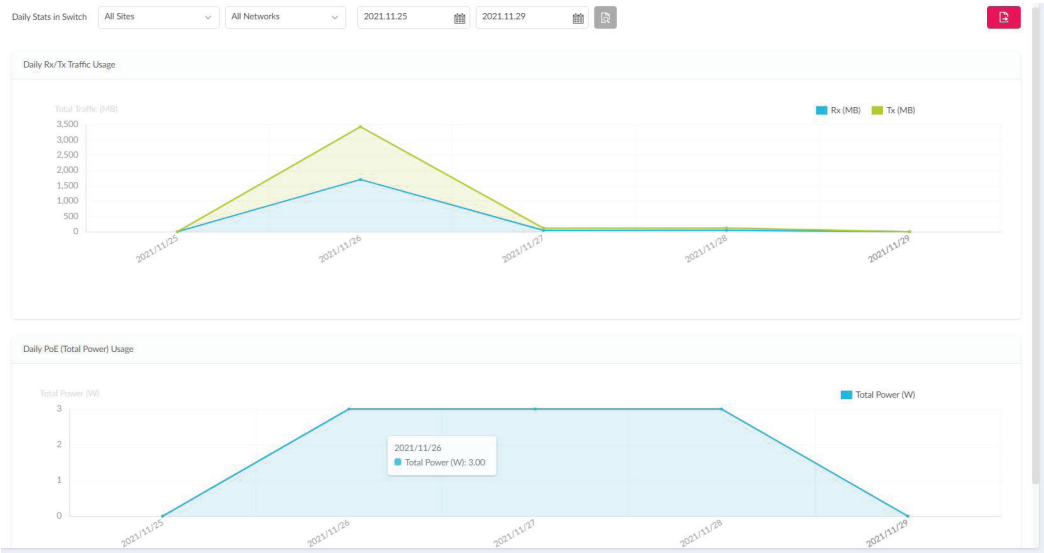


# Daily Network Activity

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.



# 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.

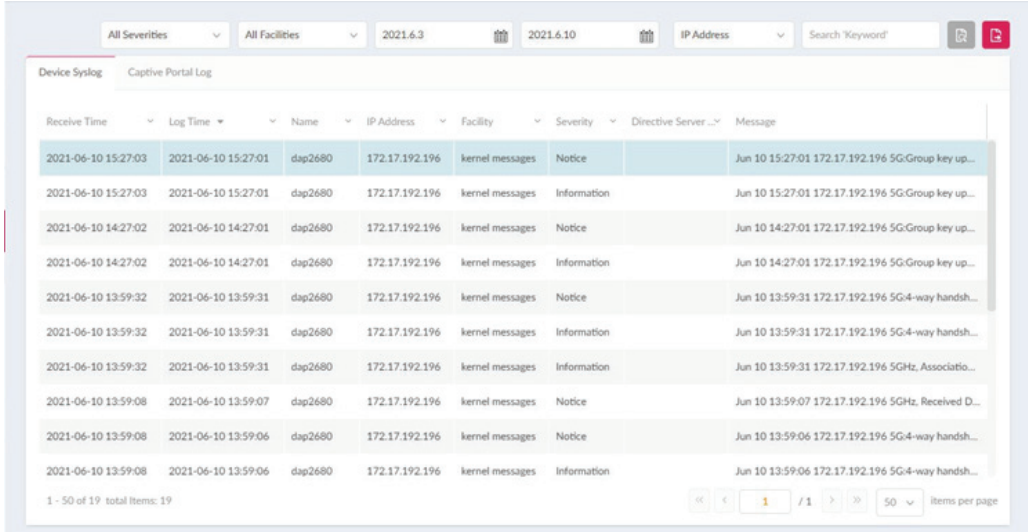
# Log

## Device Syslog

The **Device 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 > Device 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 has been generated, click to save the report to a local PDF file.

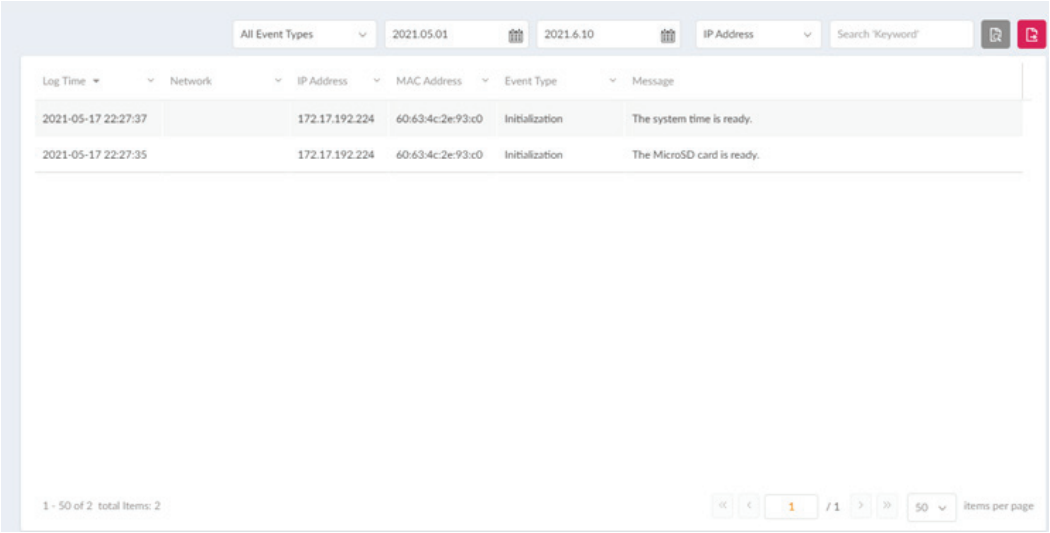


# System Event Log

The **System Event Log** function allows administrators to view alerts that may require attention and necessary action to continue smooth operation and to 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 choose either IP address or Message as report criteria. Fill in the keyword field and click to view the generated report.

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



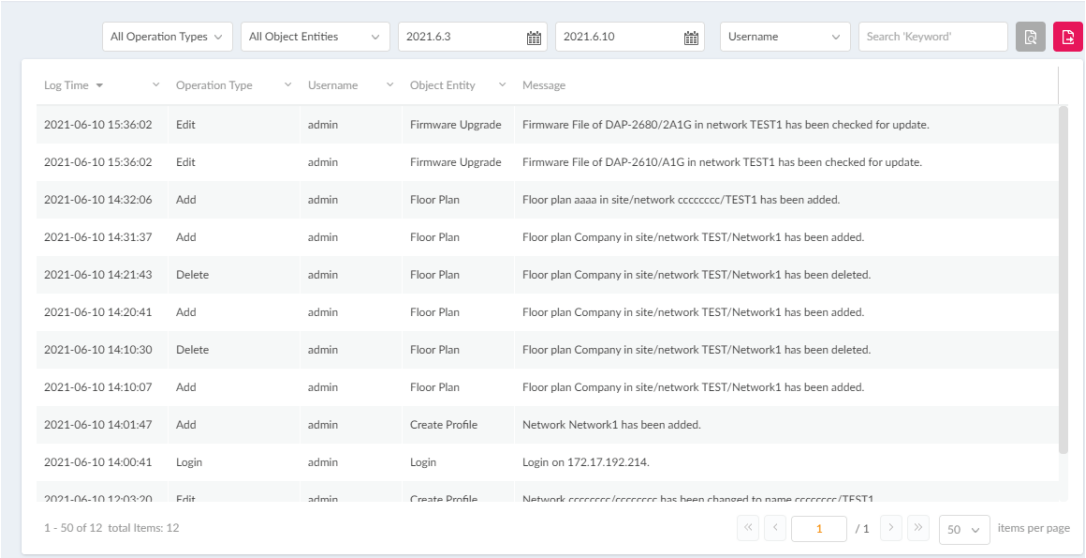
# Device Log

The **Device Log** function allows administrators to view alert messages from an AP's embedded memory. The system and network messages includes 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.

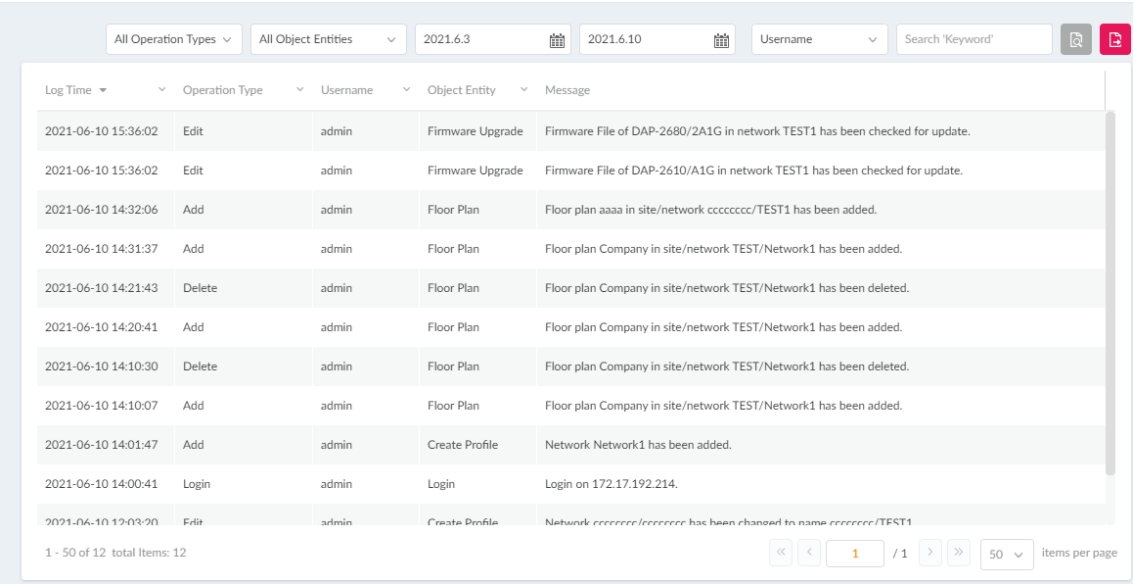
To start a Device Log, select the operation type and define the period of time to report. Click the drop-down menu to choose either IP address or Log Details as report criteria. Fill in the keyword field and click to view the generated report.

Once a report has been 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.



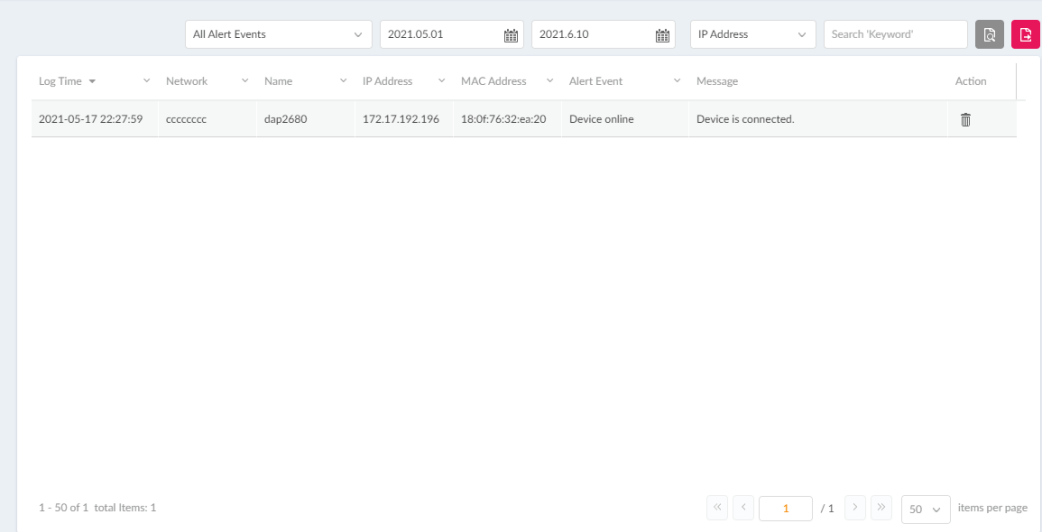

| Log Time | Operation Type | Username | Object Entity | Message |
|---|---|---|---|---|
| 2021-06-10 15:36:02 | Edit | admin | Firmware Upgrade | Firmware File of DAP-2680/2A1G in network TEST1 has been checked for update. |
| 2021-06-10 15:36:02 | Edit | admin | Firmware Upgrade | Firmware File of DAP-2610/A1G in network TEST1 has been checked for update. |
| 2021-06-10 14:32:06 | Add | admin | Floor Plan | Floor plan aaaa in site/network cccccccc/TEST1 has been added. |
| 2021-06-10 14:31:37 | Add | admin | Floor Plan | Floor plan Company in site/network TEST/Network1 has been added. |
| 2021-06-10 14:21:43 | Delete | admin | Floor Plan | Floor plan Company in site/network TEST/Network1 has been deleted. |
| 2021-06-10 14:20:41 | Add | admin | Floor Plan | Floor plan Company in site/network TEST/Network1 has been added. |
| 2021-06-10 14:10:30 | Delete | admin | Floor Plan | Floor plan Company in site/network TEST/Network1 has been deleted. |
| 2021-06-10 14:10:07 | Add | admin | Floor Plan | Floor plan Company in site/network TEST/Network1 has been added. |
| 2021-06-10 14:01:47 | Add | admin | Create Profile | Network Network1 has been added. |
| 2021-06-10 14:00:41 | Login | admin | Login | Login on 172.17.192.214. |
| 2021-06-10 12:03:20 | Edit | admin | Create Profile | Network cccccccc/cccccccc has been changed to name cccccccc/TEST1 |

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

# Alerts

This type of log records events activities for alert, e.g. new firmware release, port linked or blocked, and device online or offline.




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

# System

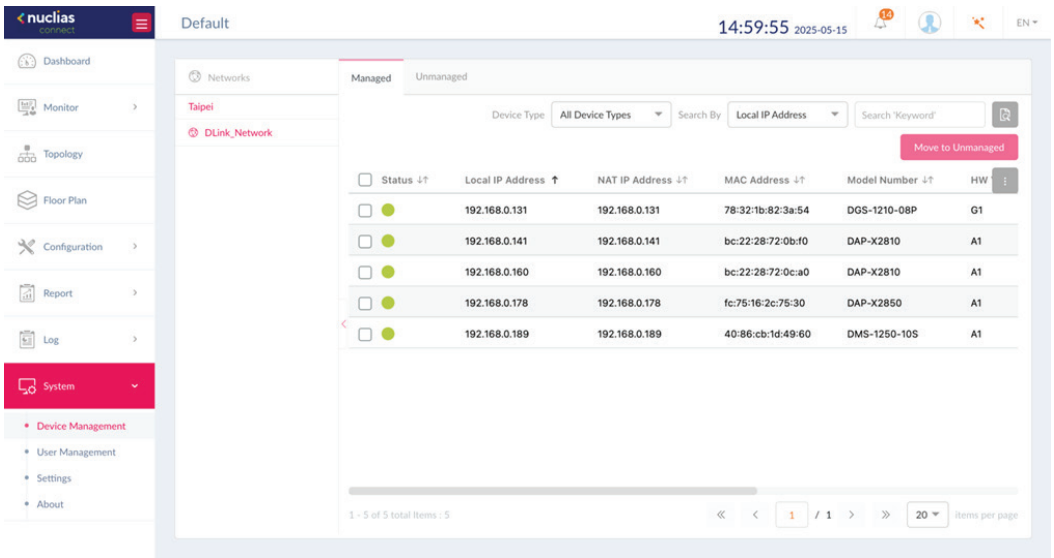
## Device Management

The **Device Management** function allows user to view list of all devices on the network both managed and unmanaged devices. Navigate to **Log** > **Device** Log to view the relevant information.

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 to 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.



# User Management

## User Status

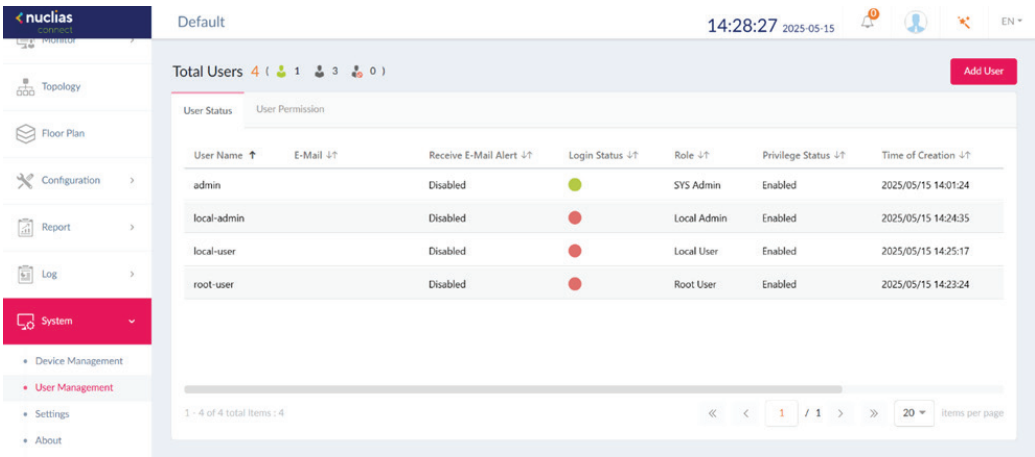
The **User Status** function allows administrators to view the current status of all registered user profiles, edit or delete the profile. When the Login Status shows green ●, the user is logged in. When the Login Status shows red ●, the user is logged out. Navigate to **System > User Management** to view the relevant information.

To edit a user profile, click the edit button corresponding to the user. The username, password, email, privilege, privilege status, location, contact number as well as the user description are available for edit. 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.

The following is a list of available user profiles and a description of their function.

| Options | Description |
|---|---|
| **Admin** | This is the operator account and cannot be deleted. |
| **Root admin** | Manage all sites/networks on this server. |
| **Local admin** | Manage your own network. |
| **Root user** | View all sites/networks on this server. |
| **Local user** | View your own network. |
| **Front desk user** | Able to generate and manage passcodes. |

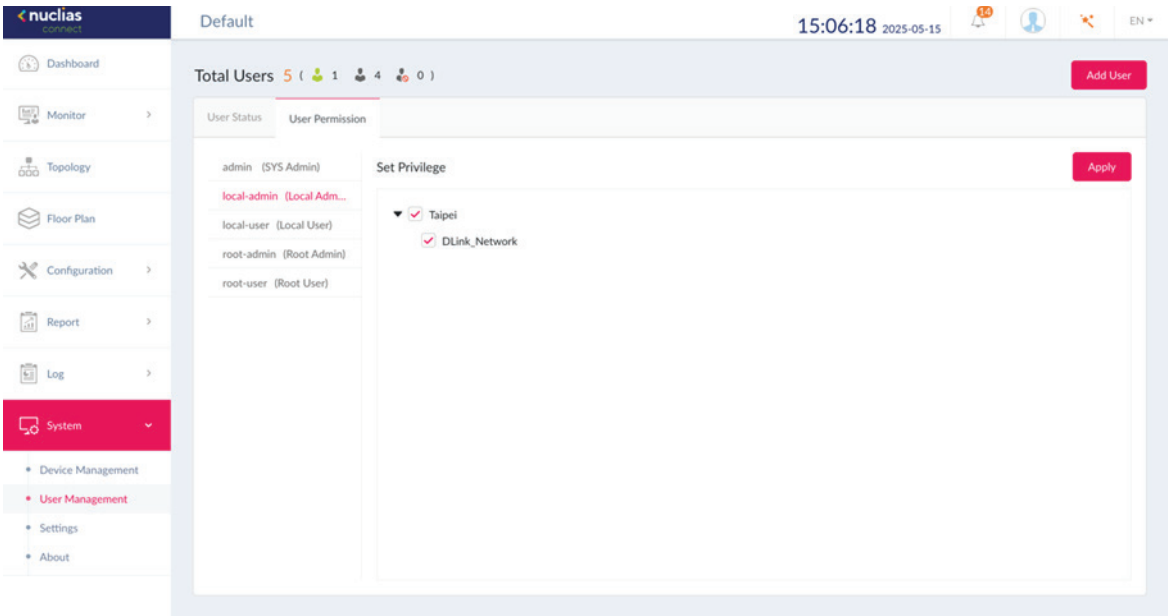


# User Permission

The **User Permission** function allows administrators to add, view, and authorize/unauthorize users on a selected network. Navigate to **System > User Management** and click on the **User Permission** tab to display the relevant information.

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 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.

To authorize or unauthorize an existing user, select an available site and then the target network. Click the **Apply** button to save the set privileges. The same process is used to unauthorize users.



# Settings

## General

The **Settings** page displays General, Connection, SMTP, Backup & Restore, REST API, Single-Sign-On (SSO) information, Alerts, FOTA, Client Description and Remote Access.

The **General** tab displays customizable system settings, which includes adding a logo and enabling the captcha feature. Device time and date and live packet interval settings are also available.

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

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

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

| Parameter | Description |
|---|---|
| **Country** | Click the drop-down menu to select the country. |
| **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. |
| **Timeout of Firmware Update** | Set the time, with a range from 3 minutes to 30 minutes. |

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

In the **Clear Saved Data in Database** section, there are two options to select: one is **Report** and the other is **Log**.

Click **Clear** to delete the data.

# 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:

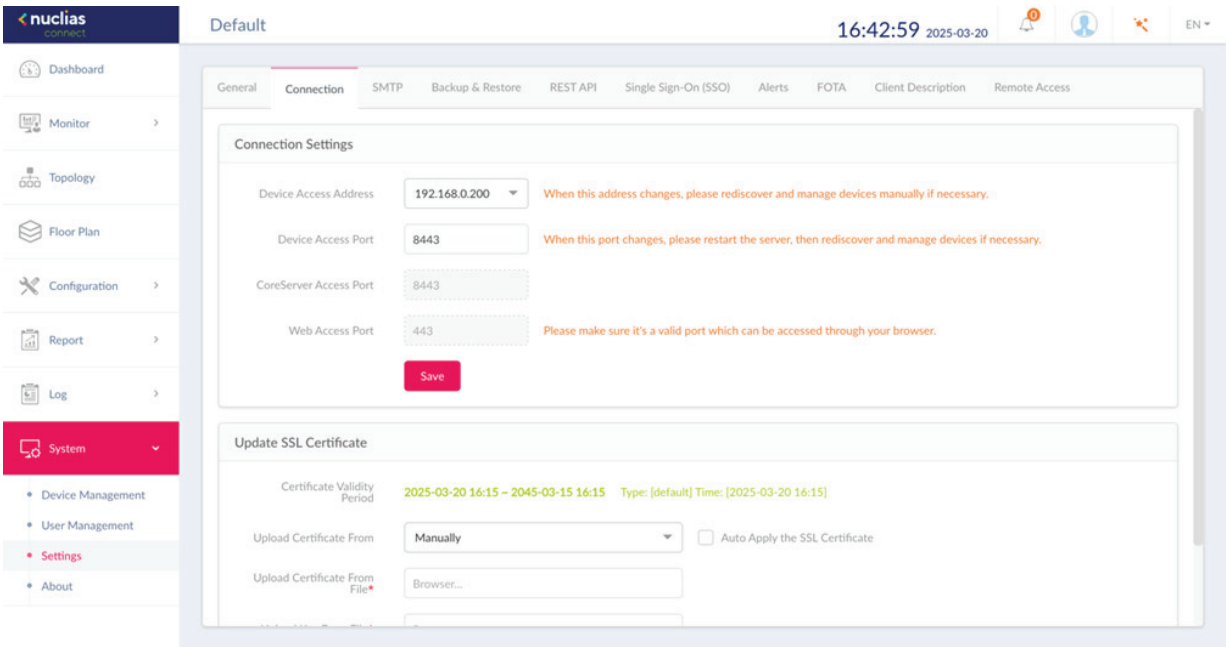
| Parameter | Description |
|---|---|
| **Device Access Address** | Enter the Nuclias Network Controller Server application's IP address. To manage remote APs, the IP address must be a public IP address; IP mapping is required for instances behind a firewall or router. |
| **Device Access Port** | Enter the Nuclias Network Controller 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. |
| **Core Server Access Port** | The core server access port, as defined during the install, has a default value of 8443 and cannot be modified. |
| **Web Access Port** | The web access ports, as defined during the installation, has a default value of 443 and connot be modified. |

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

In the **Update SSL Certificate** section, the following parameters can be configured:

| Parameter | Description |
|---|---|
| **Upload Certificte From** | Click the drop-down menu to select either **Manually** or **Certbot Automatically**. |
| **Upload Certificate From File** | Click **Browser...** to select the SSL certificate file located on the local drive that will be uploaded. |
| **Upload Key From File** | Click **Browser...** to select the SSL key file located on the local drive, that will be uploaded. |

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



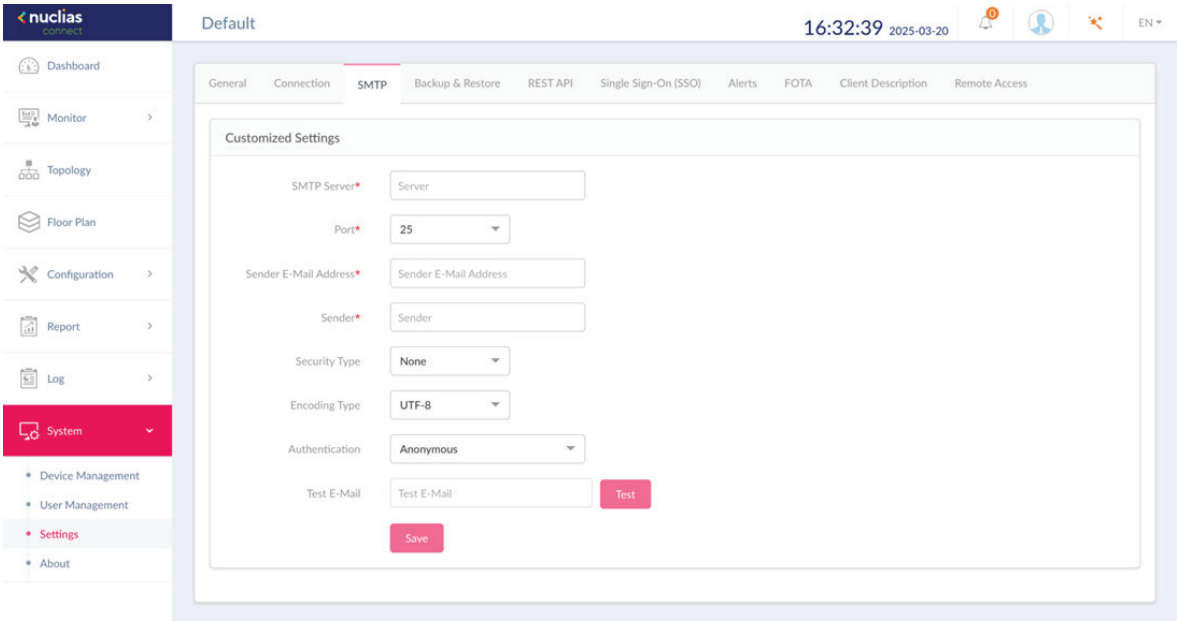
# SMTP

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.

| Parameter | Description |
|---|---|
| **SMTP Server** | Enter the SMTP server's IP address or domain name. |
| **Port** | Enter the SMTP server's port number. |
| **Sender E-Mail Address** | Enter the sender's email address. |
| **Sender** | 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 logging supported by the e-mail server. The options include Anonymous or SMTP Authentication. |
| **Test E-Mail** | 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.

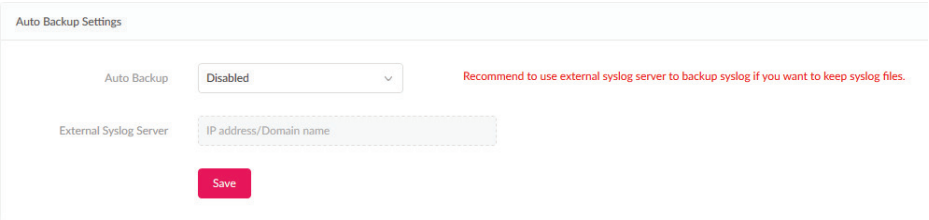


# Backup & Restore

The **Backup & Restore** tab displays customizable settings for backing up configuration settings or logs.

Navigate to **System > Settings** and click on the **Backup & Restore** tab to configure the settings.

In the **Auto Log Backup Settings** section, parameters regarding auto backup can be configured:

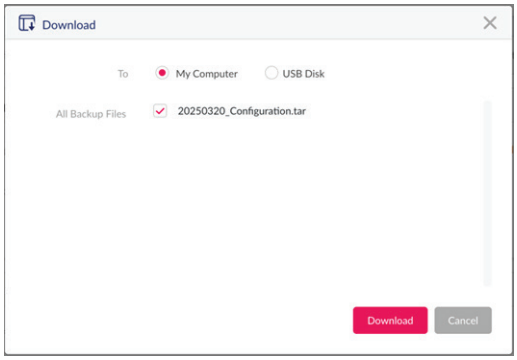



| Parameter | Description |
|---|---|
| **Auto Backup** | Click on drop-down list to enable or disable auto backup. |
| **External Syslog Server** | Enter the external syslog's IP address or domain name. |

In the **Backup Settings** section, device configuration and logs can be backed up, and downloaded to a local hard drive or USB, or deleted:

Click Backup Now to backup the configuration file or log files.

Click to download the backup file to either the management computer's hard drive or a USB drive.




Specify the following parameters from the pop-up window, then click **Download** to download the file or **Cancel** to exit from the operation.

| Parameter | Description |
|---|---|
| **To** | Choose either My Computer or USB Disk to download your backup file to. |
| **All Backup Files** | A list of all backup files that are available to be downloaded will be displayed. Select the radio button of the file you want to download. |

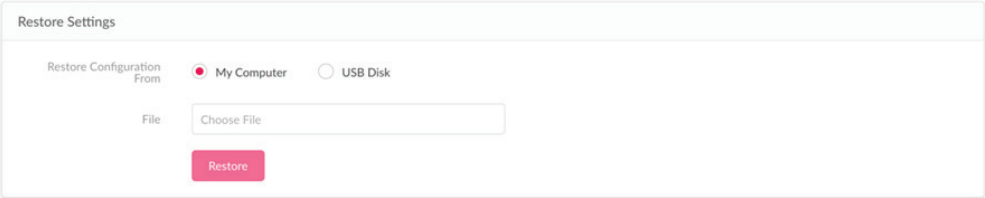
Click to delete the backup configuration files or log files that are stored on the device.

Select which files from the pop-up window you want to delete, then click **Delete** to confirm your action or **Cancel** to exit from the operation.

In the **Restore Settings** section, device configuration can be restored from local hard drive or USB storage.

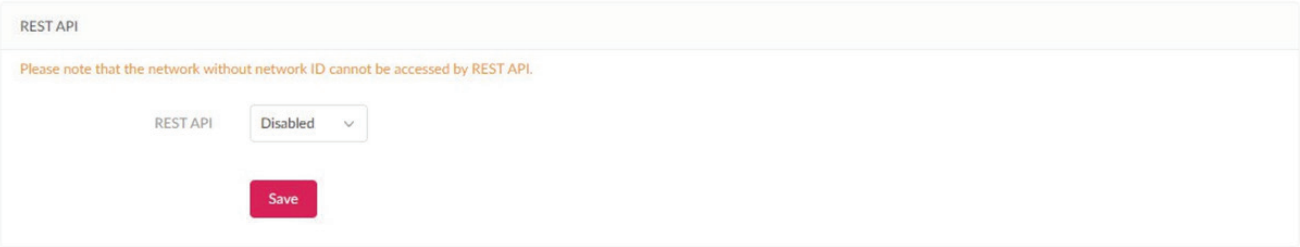
Specify the following parameters, then click **Restore**.

| Parameter | Description |
|---|---|
| **Restore Configuration From** | Choose either My Computer or USB Disk to upload your configuration file. |
| **File** | Click **Choose File** to select your configuration file's location. |



# 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.



# Single-Sign-On (SSO)

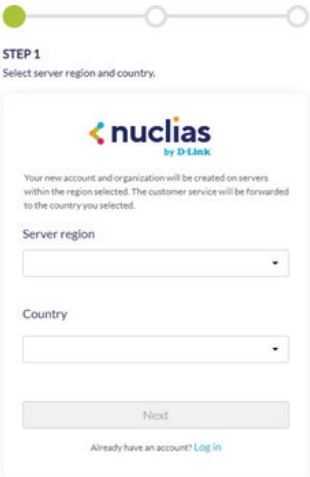
The **Single-Sign-On** tab allows you to use a Nuclias Account to access Nuclias Cloud and the Nuclias Connect portal.

If you do not already have a Nuclias account, you can click **Create Account**, in which a separate window will open to allow you to create one.

There are three steps in the registration process.

Step 1: Select server region and country.

The account is created on the servers within the selected region and the selected country. Your account data will be stored in the regional server based on your selected region and country.



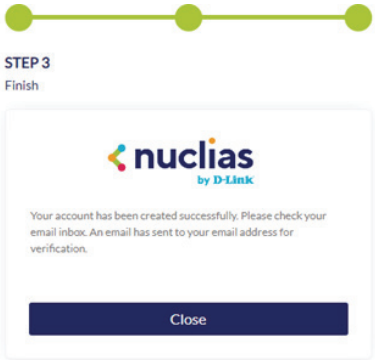

Step 2: Create organization and site.

Once the region and country have been entered, you now have to enter your Email, Name, Password, Organization name, and address. Enter the required information and agree to the Terms of Use and Privacy agreement to enable the account creation button.

Click **Create Account** to continue.

Step 3: Finish registration.

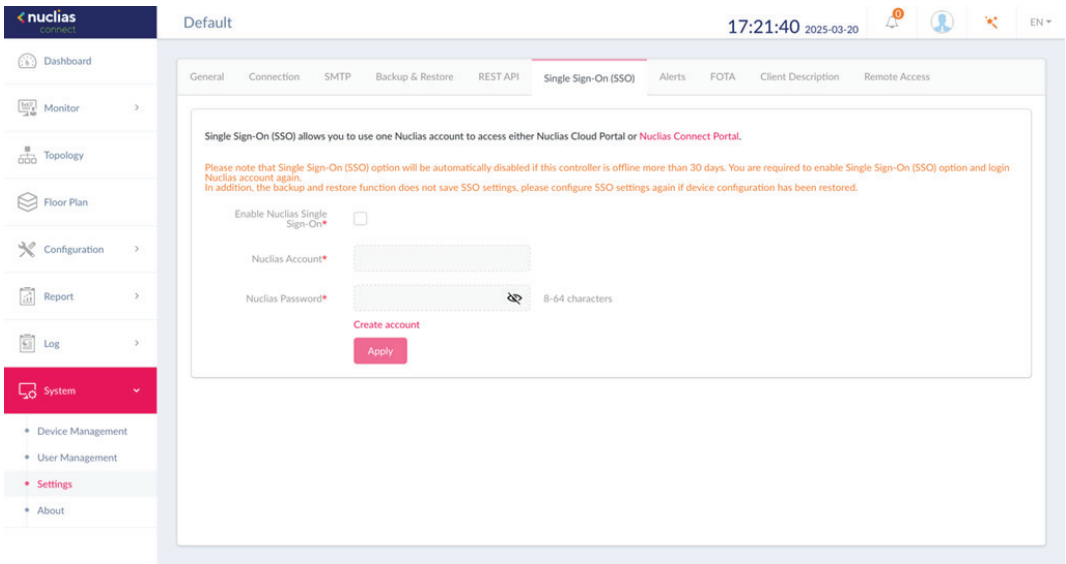
Click **Close** to complete the process. The registered account is now available for use. The verification information will be delivered to the registered email of the account.




Your Nuclias account must be validated before use. You will receive an email from verify@nuclias.com with a verification link included. Please click on the verification link to activate your Nuclias account.

Once finished, specify the following parameters on the **Single-Sign-On** page and then click **Apply**.

| Parameter | Description |
|---|---|
| **Enable Single Sign-on** | Check to enable single sign-on. |
| **Nuclias Account** | Enter your Nuclias Account username. |
| **Nuclias Password** | Enter your Nuclias Account password. |



The Nuclias Connect Portal provides you with a easy way to view and connect to your Nuclias Network Controller.

Requirements for use include:

- A Nuclias account
- DNH-1000 device(s) with single sign-on enabled

The portal can be found at: https://connect.nuclias.com/

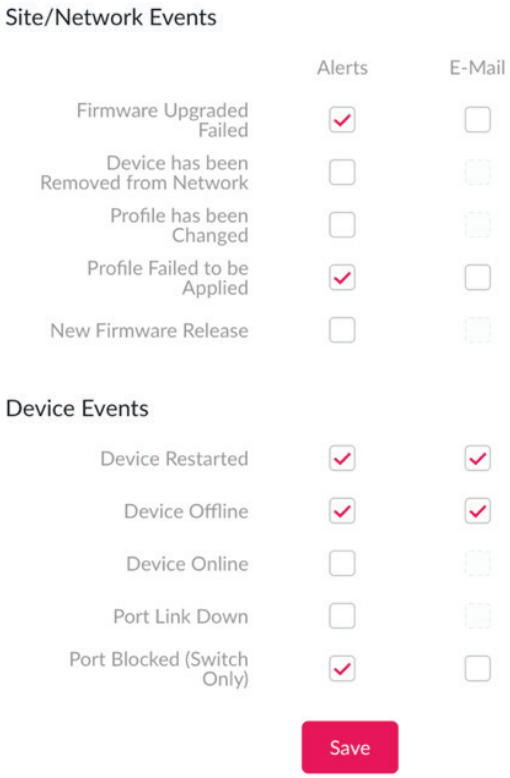

The Portal provides the following information:

| Parameter | Description |
|---|---|
| **Number** | Number of the DNH-1000 on the list. |
| **Status** | Displays whether or not the Nuclias Connect portal can link to that DNH-1000. |
| **Name** | Name of the Nuclias Network Controller You can change this name by clicking on it then typing on the available text box. |
| **Host** | Displays both the device IP address and its public IP address. |
| **Sites** | Number of sites managed by that DNH-1000. |
| **Networks** | Number of networks managed by that DNH-1000. |
| **Devices** | Number of devices managed by that DNH-1000. |
| **Clients** | Number of clients connected to devices managed by that DNH-1000. |
| **Version** | Firmware version number of that DNH-1000. |
| **Actions** | Click **Launch** to open the DNH-1000 Nuclias Connect interface. Please note that IP mapping is required for instances behind a firewall or router. Click **Forget** to unlink this DNH-1000 from the Nuclias Connect portal. (**Forget** is only available when that device is offline.) |

# Alerts

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

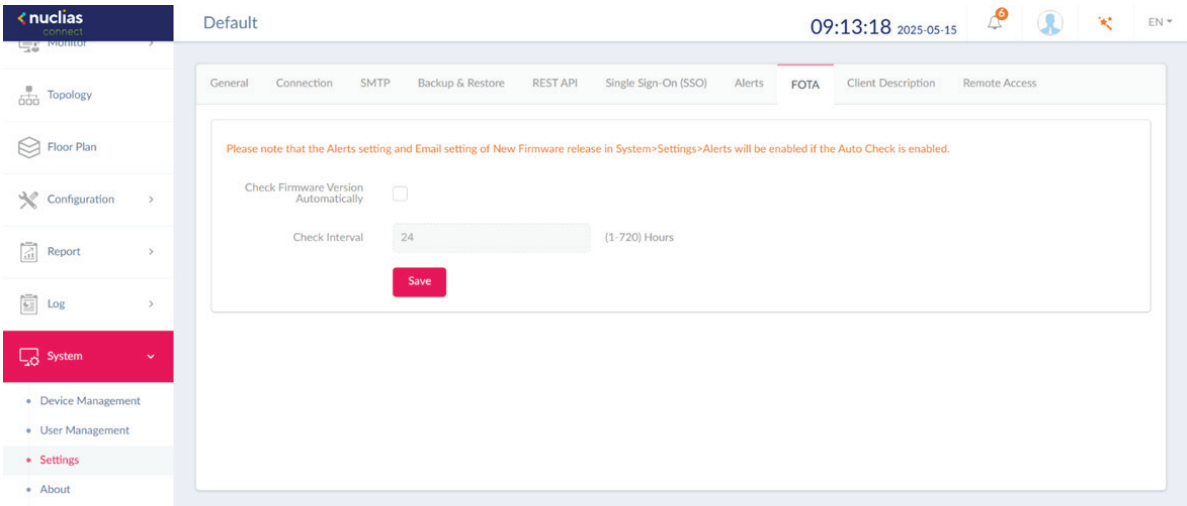
Check the **Email** box to receive Email notification of specific events. Go to **System>Settings>User Management** to edit the user and select **Receive Email Alert** to allow user to receive alert email from Nuclias Connect. Click **Save** to save the values and update the screen.



# FOTA

The FOTA (Firmware Over-The-Air) feature enables users to wireless 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 and 720 hours.

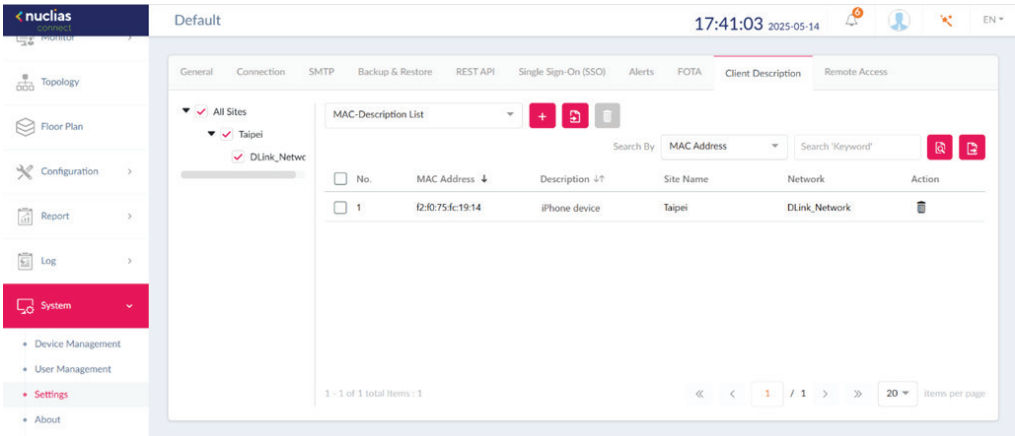
**Note**: When **Auto Check** is enabled, the **Alert** and **Email** settings will also be enabled.



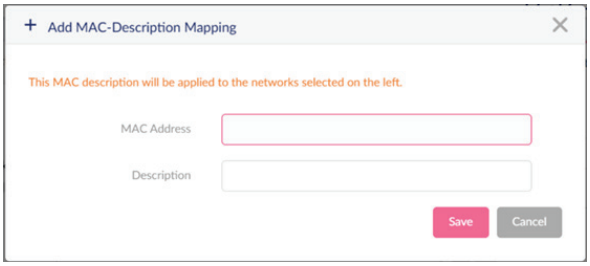
# Client Description

The **Client Description** tab show client device description list.

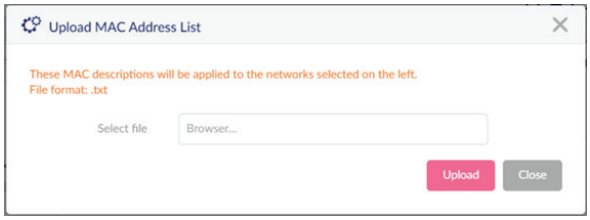
Administrator can enter client description manually.
Non-administrators can only view, not edit.




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  to export client description list CSV file.

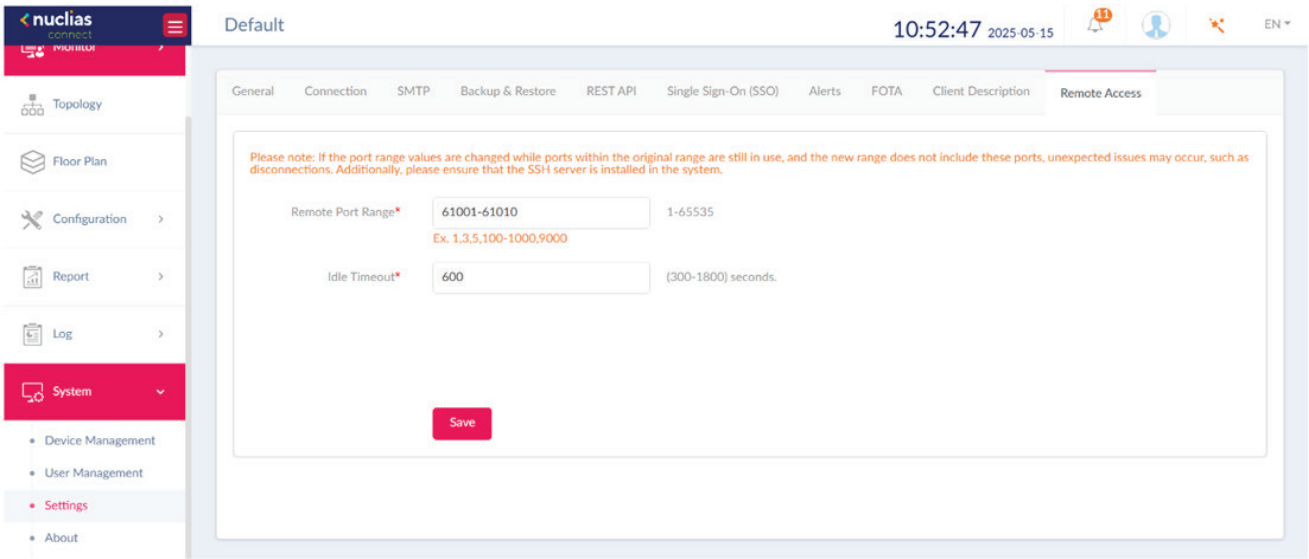
# Remote Access

The **Remote Access** tab allows you to configure the remote access settings.

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

Idle timeout default is 600 seconds and the range is from 300 to 1,800 seconds. The adjustment of the **Idle Timeout** will only affect newly established tunnels, and existing tunnels will not be affected.

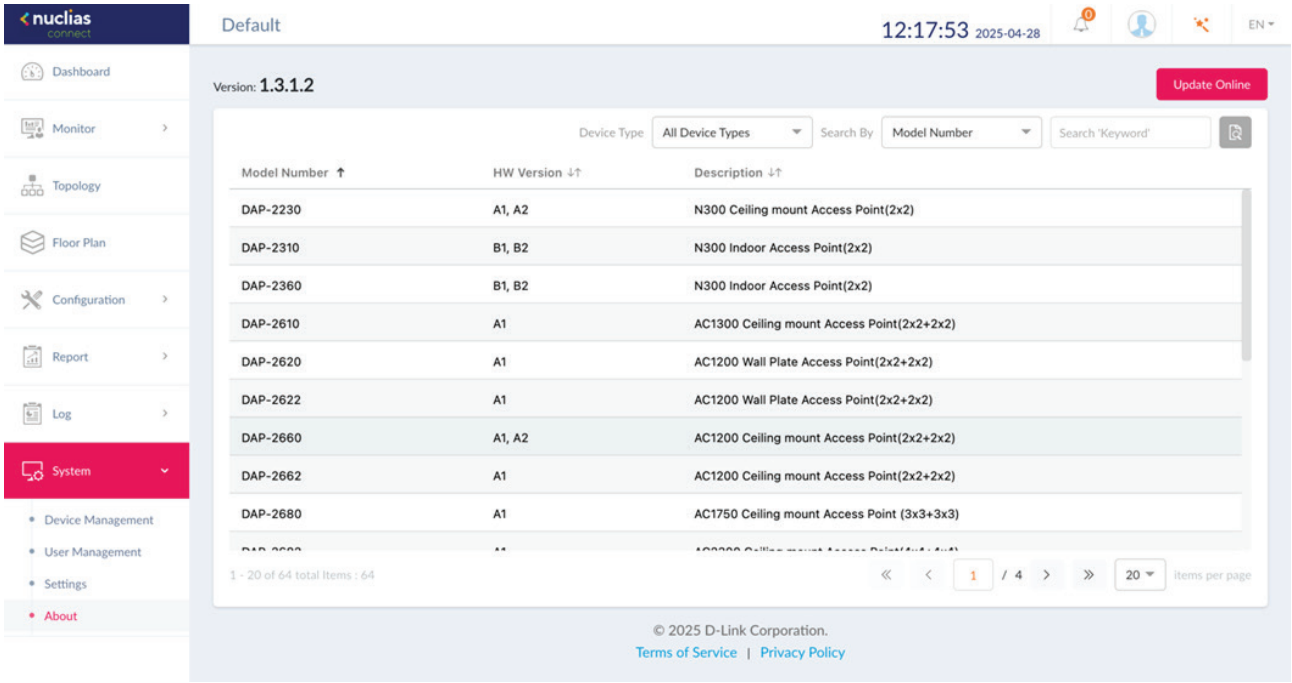
**Note**: Unable to operate when user permissions are insufficient. When user permission is **Root User** or **Local User** or **Local Admin**, the page items are shown as disabled.



# About

The **About** page displays system version number and a list of supported models.
Navigate to **System > About** to view the info.

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



# Appendix

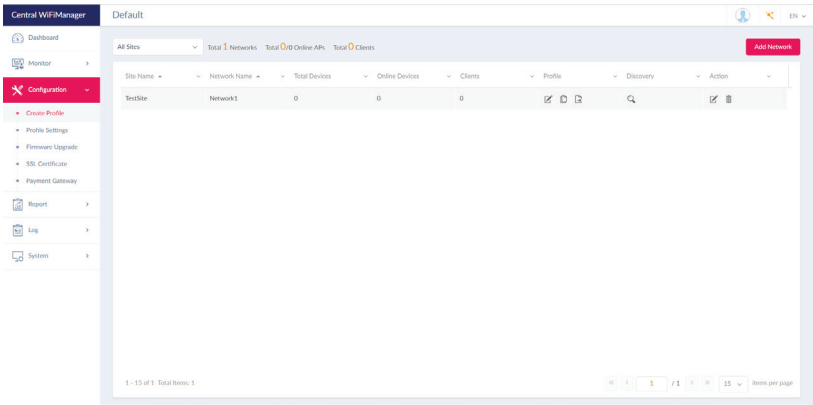
## Nuclias Connect App

Through the use of the **Nuclias Connect App**, users can manage sites and network remotely and easily by accessing the tool through a smart device.

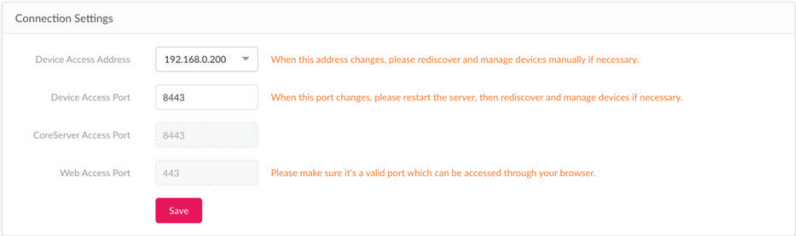
This section provides information on exporting the required network profiles from the Nuclias server for managing connected DAPs. Additional information explaining the functionality of the **Nuclias Connect App** is also included.

### Export Network Profiles

To add new access points to Nuclias Connect, you must first export the required network profile from Nuclias. The network profile contains the authentication key and the IP address of the controller. Select **Configuration** and then click the **Export** ( ) icon to export the network profile to your computer.




When access points are located on a public network and you are accessing **Nuclias Connect** remotely, you must ensure that **Nuclias Connect** uses a public IP address or domain name. To verify the **Nuclias Connect** IP address, go to **System > Settings > Connection** and check the **Device Access Address** field.




### Discover and Configure APs Using the Nuclias Network Controller App

The **Nuclias Connect App** is a wireless access management tool that provides the means to easily manage single or multiple sites and networks from your smartphone or tablet. With the **Nuclias Connect App**, you can quickly deploy standalone DAPs to Nuclias Connect, scan a network for D-Link access points or configure individual DAPs.

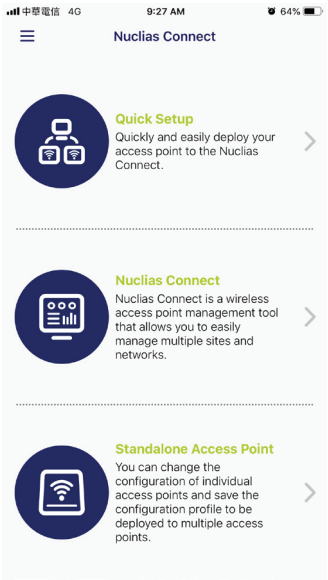
**NOTE:** Before attempting to import a network profile, ensure that you have access to the **Nuclias Connect** controller.

The **Nuclias Connect App** is available for both iOS and Android smart devices. The following functions are available:

- Quick Setup: Quickly and easily deploy your standalone DAP to the **Nuclias Connect** controller.
- **Nuclias Connect**: Manage your current sites and networks through **Nuclias Connect**.
- Standalone Access Point: You can change the configuration of individual DAPs and save the configuration profile to be deployed to multiple DAPs.

***Quick Setup***

After opening the **Nuclias Connect App**, the following window will appear (iOS). Tap on **Quick Setup** to start the setup process.

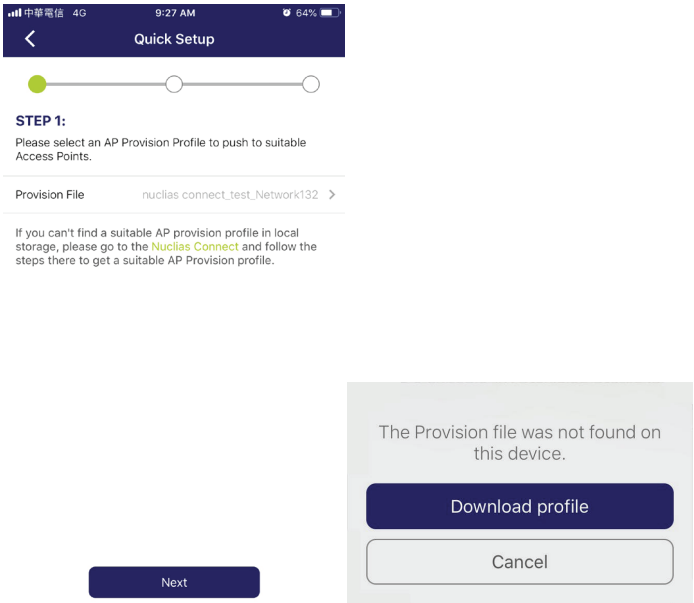



The next step is to select an AP provision profile. The profile is used to push to the selected DAPs. Tap **Quick Setup** to begin the deployment of a standalone DAP to the **Nuclias Connect** server.

In the below example the Provision File entry shown is **None**.

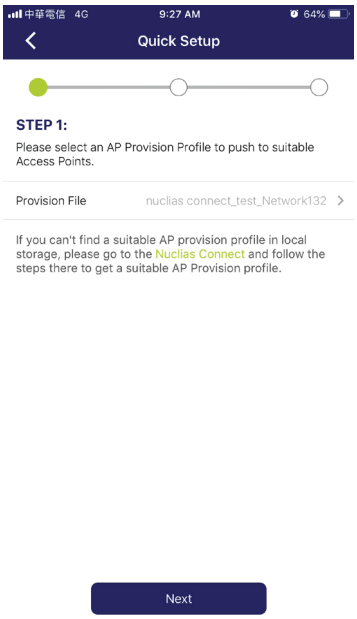
Tap **Provision File** to display a list of available local profiles. If no locally stored profile exists, a pop-up page will appear with further instructions on how to download a profile.

Tap **Download profile** in order to specify a connection to the **Nuclias Connect** controller.

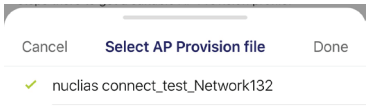



Once a **Nuclias Connect** controller connection is established, you will see it listed next to the field Provision File.

Tap **Provision File** to select a local AP provision profile. In the following figure, the entry **Nuclias_connect_test_Network132** is available.




After the Select AP Provision file window appears, select an available provision file from local storage and tap **Done** to continue.



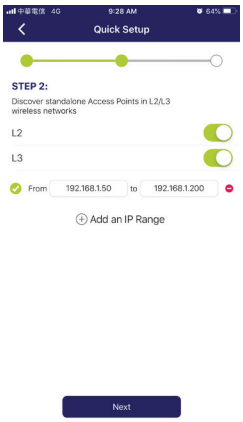

The process will continue and the App will return to the previous screen. From the Step 1 page, tap **Next** to continue.

From this page, you can discover standalone APs connected to the L2/L3 wireless network.

Tap the button on the L2 field to enable discovery on the L2 network.

Tap the button on the L3 field to enable discovery on the L3 network. Then enter an IP range in the provided From and To fields. Tap **Add an IP Range** ( ⊕ ) to create a new IP range entry. Tap remove ( ⊖ ) to delete any defined range entries.

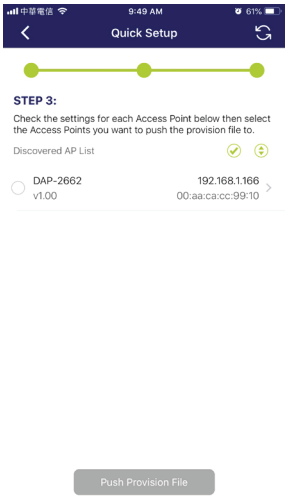
In the IP range fields, specify the starting and ending IP addresses. Once the range is defined, tap **Next** to initiate the discovery process.



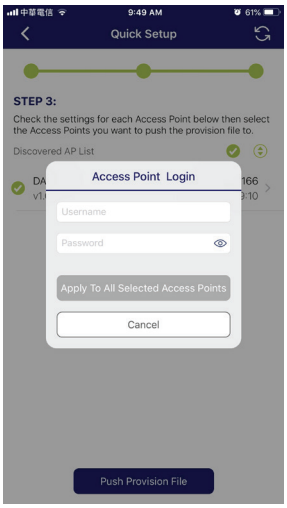
After the scanning the network range, the Step 3 page will list any detected access points.

Tap the radio button next to the AP to select it. The local provision file that you previously selected will be pushed to the selected AP.

Tap **Push Provision File** to continue.




The AP login pop-up window displays. The listed IP and MAC address are shown at the top of the window. Confirm the selection and enter the user name and password with authorization to access the selected AP.

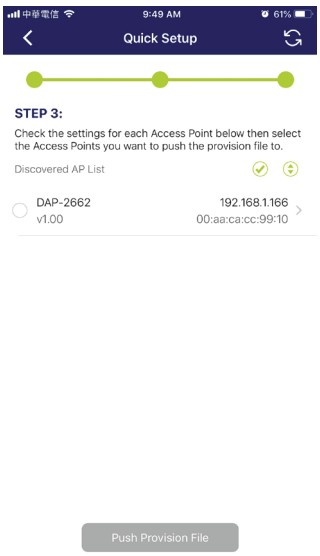



Tap **Apply** to continue the login process. The Modify IP Information page will appear. Any listed information can be modified; see the following figure for further information.

| Parameter | Description |
|---|---|
| **Cancel** | Tap to discard any changes and continue the process. |
| **Done** | Tap to accept any changes and continue the process. |
| **Model Name** | Displays the model name for the listed DAP device. |
| **MAC** | Displays the MAC address of the listed DAP device. |
| **DHCP Mode** | Tap to enable or disable the DHCP mode function. When enabled, the DAP establishes dynamic IP address settings with any authorized client connections. |
| **IP Address** | Tap to designate an IP gateway setting. |
| **Subnet Mask** | Tap to designate a subnet mask. |
| **Default Gateway** | Tap to designate a default gateway. |
| **DNS** | Tap to designate a DNS setting. |

Tap **Done** or **Cancel** to continue the process. The provision file will be pushed to the selected DAP device (s). The App will return to the Step 3 page and will display the status of the **Push** function. The discovered DAPs lists the state of the push function with either a successful or failed state. See the following figure for further details.

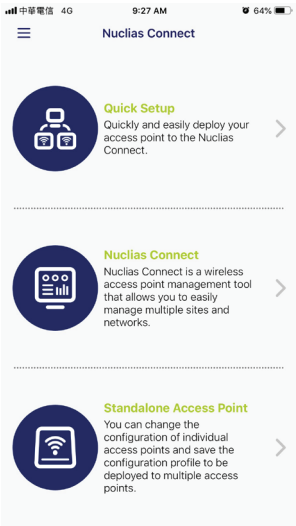
Tap **Finish** to complete the process. In the event of a failed process, tap **Push Provision File** to attempt the function a second time.



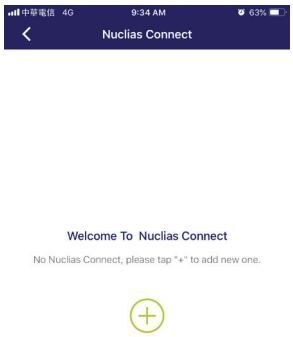

## Nuclias Connect

Nuclias Connect is a wireless access point management tool capable of managing your sites and networks.

Tap **Nuclias Connect** to connect to a **Nuclias Connect** server.



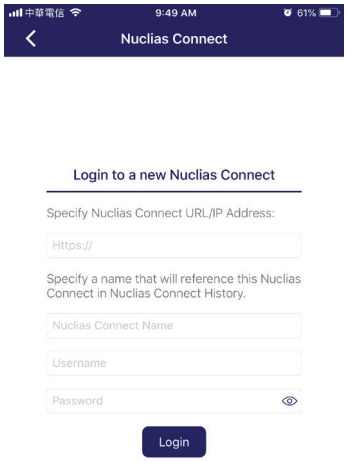
If no previous **Nuclias Connect** controller was paired it will ask you to create a new **Nuclias Connect** pairing. Tap the add (⊕) button to start the process.



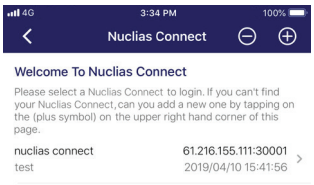

The following page lists the information required to log in to a designated Nuclias Connect controller. Enter the required information in each field.

| Parameter | Description |
|---|---|
| **Specify Nuclias Connect URL/IP Address** | Enter the secure URL/IP address of the Nuclias Network Controller server to pair with the App. |
| **Specify a Reference Name** | Enter a specific name to easily identify the paired Nuclias Network Controller server. |
| **User Name** | Enter a user name with the authority to access the Nuclias Network Controller controller. |
| **Password** | Enter the password for the referenced user name with the authority to access the Nuclias Connect server. |
| **Login** | Tap Login to initiate the login process. |

Tap on **Login** to initiate the login process.

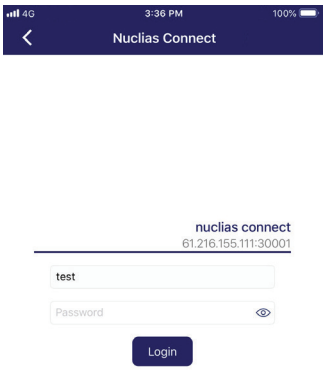


After a successful login, the pairing will be added to the listing and will be available for future login selection.

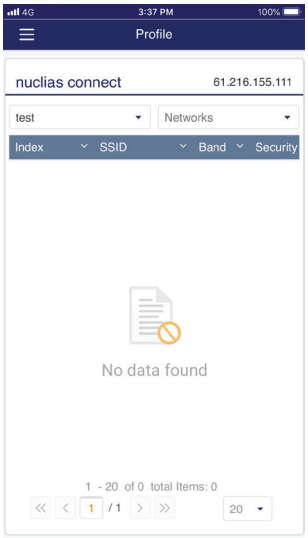



Tap on a **Nuclias Connect** server from the list.

The username page will appear.
Enter the username and password with authority to access the selected **Nuclias Connect** server.
Tap **Login** to initiate the login process.




After the login process is authenticated, the dashboard will appear. The **Nuclias Connect** dashboard will list any currently defined sites, networks, access points, and clients.




The **Nuclias Connect App** is now paired to the **Nuclias Connect** server. Through the use of the app, profiles can be downloaded to the local device, after which it can be pushed to supported access points.

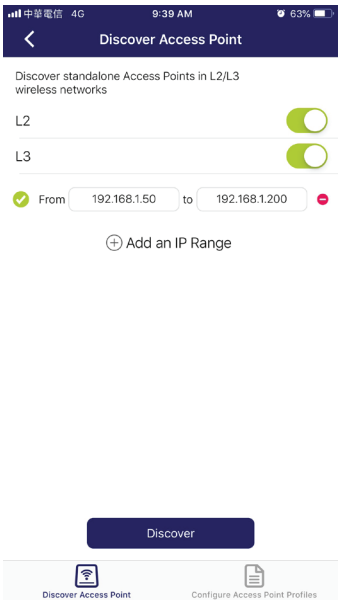
***Standalone Access Point***

**Discover APs**

The Discover AP function allows you to discover any access points in a L2/L3 wireless network.

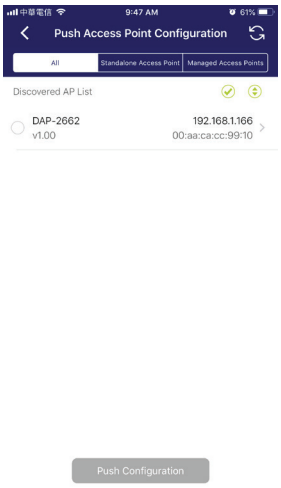
From this page, you can discover standalone APs connected to the L2/L3 wireless network.
Tap to enable discovery on the L2 network.

Tap to enable discovery on the L2 network. Then enter an IP range in the provided From and To fields. Tap add (⊕) to create a new IP range entry. Tap remove (⊖) to delete any defined range entries.

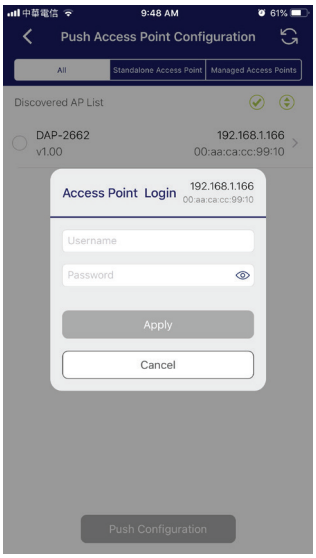



Once the range is defined, tap **Next** to initiate the discovery process.
Alternatively, tap **Configure Access Point Profiles** from the bottom of the page to add or delete any local profiles. See Configure Access Point Profiles.

After the scanning the network range, the Step 3 page will list any detected access points.
Tap the radio button next to the AP to select it. The selected local provision file will be pushed to the selected AP.
Tap **Push Provision File** to continue.

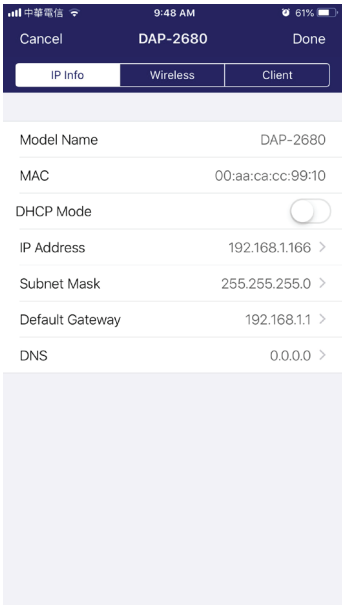


The DAP login pop-up window will appear. The IP and MAC address are shown at the top of the window. Confirm the selection and enter the user name and password with authorization to access the selected AP. Tap **Apply** to continue.




Once a successful login is established, the AP interface menu will appear. The IP information, Wireless, and Client menus will be listed as follows.

| Parameter | Description |
|---|---|
| **Cancel** | Tap to discard any changes and continue the process. |
| **Model Name** | Displays the model name for the listed DAP device. |
| **MAC** | Displays the MAC address of the listed DAP device. |
| **DHCP Mode** | Tap to enable or disable the DHCP mode function. When enabled, the DAP establishes dynamic IP address settings with any authorized client connections. |
| **IP Address** | Tap to designate an IP gateway setting. |
| **Subnet Mask** | Tap to designate a subnet mask. |
| **Default Gateway** | Tap to designate a default gateway setting. |
| **DNS** | Tap to designate a DNS setting. |



The Wireless settings menu is listed in the table below.

| Parameter | Description |
|---|---|
| **Cancel** | Tap to discard any changes and continue the process. |
| **DAP** | Displays the model name and IP address of the AP device. |
| **2.4G SSID** | |
| **SSID-#** | Tap the slide button to enable or disable the SSID. The # character indicates the identifying number of the SSID. |
| **SSID Name** | Tap to change the current name of the SSID. |
| **Security** | Tap to select a specific security protocol: Open System (default), WPA-Personal, or WPA-Enterprise. |
| **5G SSID** | |
| **SSID-#** | Tap the slide button to enable or disable the SSID. The # character indicates the identifying number of the SSID. |
| **SSID Name** | Tap to change the current name of the SSID. |
| **Security** | Tap to select a specific security protocol: Open System (default), WPA-Personal, or WPA-Enterprise. |
| **Wireless Information** | |
| **Radio Band** | Tap to select a specific radio band: Off, 2.4G, 5G, or 2.4G / 5G. |
| **Radio 2.4G Mode** | Tap to select a specific 2.4G radio mode: Mixed 802.11n, 80211g and 802.11b; Mixed 802.11g, 802.11b; 802.11n Only. |
| **Radio 5G Mode** | Tap to select a specific 5G radio mode: Mixed 802.11n, 80211a; 802.11a Only; 802.11n; Mixed 802.11ac. |
| **Country Code** | Displays the assigned country designation for the AP. |
| **Copy & Save Configuration** | |
| **Apply Configuration** | Tap to select an alternate discovered AP device to push the current configuration. |
| **Save Configuration** | Tap to name and archive the current configuration profile. |