

# NUCLIAS CONNECT DNH-100 User Manual

V 1.00

# Table of Contents

- Introduction.....3**
- Product Overview.....3**
  - Package Contents.....3
  - System Requirements.....3
- Hardware Overview.....4**
  - LED Indicators.....4
  - Interface Connectors.....4
- Installation.....5**
  - Mounting.....5
  - Connecting the Controller.....6
- Basic Configuration.....7**
  - Launch Nuclias Connect.....7
- Nuclias Connect Configuration.....9**
  - Wizard.....9
  - Dashboard.....12
  - Monitor.....13
    - Access Point.....13
    - Wireless Client.....14
  - Configuration.....16
    - Create Profile.....16
    - Profile Settings.....19
    - Firmware Upgrade.....36
    - SSL Certificate.....37
    - Payment Gateway.....38
  - Report.....39
    - Peak Network Activity.....39
    - Most Active AP.....40
    - Hourly Network Activity.....41
    - Daily Network Activity.....42
  - Log.....43
    - SNMP Traps.....43
    - Syslogs.....44
    - System Event Log.....45
    - Device Log.....46
  - System.....47
    - Device Management.....47
    - User Management.....48
    - Settings.....50
    - About.....61
- Appendix.....62**
  - Nuclias Connect App.....62

## Introduction

Nuclias Connect is D-Link's centralized management solution for Small-to-Medium-Sized Business (SMB) 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 small network to a larger one (up to 1,000 APs), 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 11 languages, Nuclias Connect minimizes the hassle of deployment, configuration, and administration tasks.

The DNH-100 Nuclias Connect Hub is a hardware controller with pre-loaded Nuclias Connect software. It is designed to support small-to-medium business or enterprise environments by providing network administrators the capability to manage D-Link DAP series access points through one single platform. The Nuclias Connect Hub can currently manage up to one hundred APs per unit with the potential to extend to other Nuclias Connect products in future firmware updates.

## Product Overview

### Package Contents

### System Requirements

## Package Contents

- DNH-100 Nuclias Connect Hub
- Power Cord
- Rack Mount Kit
- Quick Start Guide
- 16 Gb MicroSD Card (Optional\*)

## System Requirements

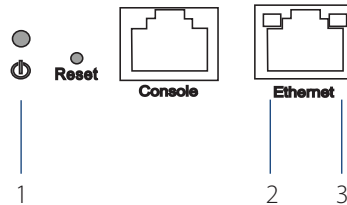
- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet Adapter
- Microsoft Edge, Safari 7, Firefox 28, or Google Chrome 33 and above (for configuration)

# Hardware Overview

## LED Indicators

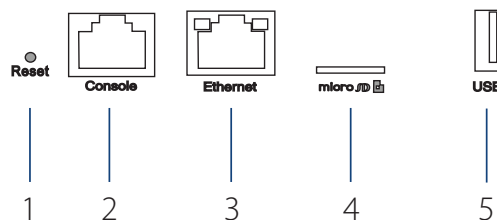
## Interface Connectors

### LED Indicators



#	LED	Description
1	Power	Solid Green - The device is powered on and ready for use, and it is in standalone mode. Blinking Green - The device is booting up. Solid Orange - The device is connected to Nuclias server and single sign-on is available for use. Solid Red - Device is unable to boot .
2	Link Speed (10/100 Mbps)	Solid Green - Port is operating at 10/100 Mbps Light Off - No Link.
3	Link Speed (1000 Mbps)	Solid Green - Port is operating at 1000 Mbps Light Off - No Link.

### Interface Connectors



#	Connector	Description
1	Reset	Used for rebooting or resetting the device back to factory default settings.
2	Console Port	RJ-45 port to connect the RJ-45 console cable for CLI management .
3	Ethernet Port	Gigabit RJ-45 port for LAN connection.
4	MicroSD Slot	MicroSD slot for MicroSD card <sup>1,2,3</sup> up to 32 Gb.
5	USB Port	USB 3.0 Type A port <sup>2</sup> (provides 5V/1A power for optional HDD connection).

<sup>1</sup> Due to EU regulations the 16 Gb MicroSD card is only included in the WW version.

<sup>2</sup> Only FAT32 format is supported.

<sup>3</sup> Do not remove the microSD card while the power is on as this may damage your card.

# Installation

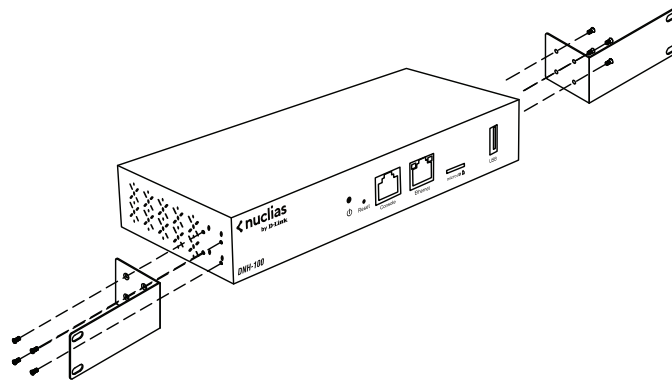
## Mounting

## Connecting the Controller

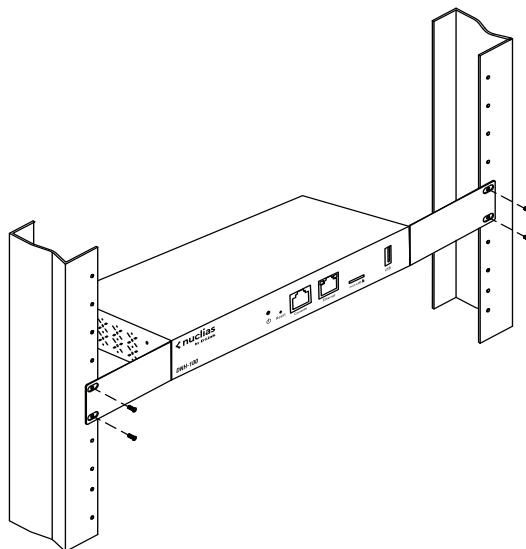
### Mounting

The DNH-100 can be mounted in an EIA standard size 19-inch rack, which can be placed in wiring closet with other equipment.

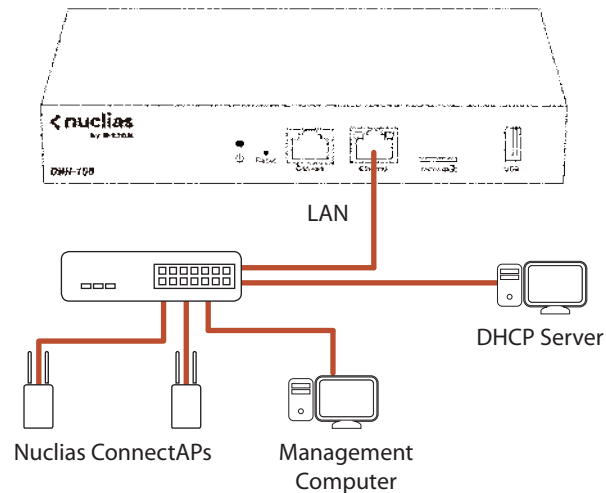
1. Attach the L-shaped mounting brackets to each side of the chassis as shown in Figure 3 and secure them with the screws provided.



2. Mount the device in the rack using a screwdriver and the supplied rack-mounting screws.



## Connecting the Controller



To connect the DNH-100, perform the following procedure:

1. Install the DNH-100 and access points 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.

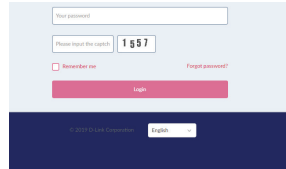
# Basic Configuration

## Launch Nuclias Connect

### Launch Nuclias Connect

The DNH-100 comes preloaded with Nuclias Connect. Open a web browser from the management computer and enter the **IP address** or **Domain Name** of the DNH-100. The default IP address is `https://192.168.0.200`.

**Note:** For initial configuration, the management computer and DNH-100 must be in the same subnet.

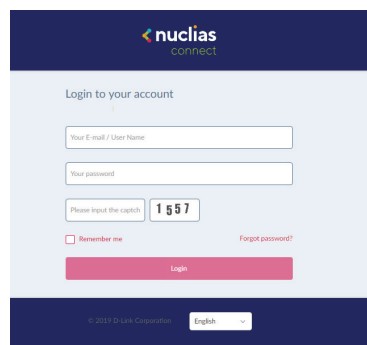


The default user name and password of Nuclias Connect is 'admin'.

Enter the Captcha code as shown on screen.

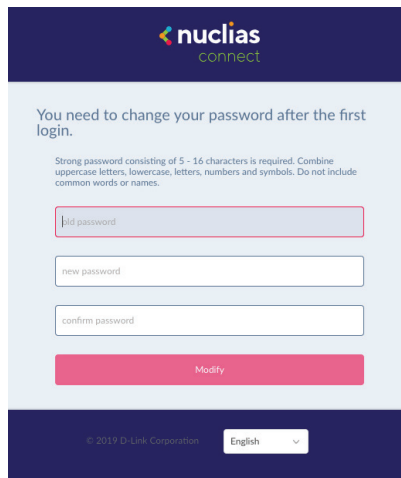
**NOTE:**

- The **Remember me** function can be selected to save the password entry for future use.
- The **Forgot password?** function provides an option to reset your password in the event that you've forgotten your current password. To use this function, the smtp server and email address must be configured first.
- The interface supports multilanguage 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 dialog will appear. A change in the default password is required after the first login.

When assigning a password, it is recommended to use a strong password. The new password is required to be 5 - 16 characters in length. By combining uppercase and lowercase characters, numbers and symbols a strong password can be created.



The screenshot shows a web interface for changing a password. At the top, the 'nuclias connect' logo is displayed. Below the logo, a message states: 'You need to change your password after the first login.' A sub-message provides password requirements: 'Strong password consisting of 5 - 16 characters is required. Combine uppercase letters, lowercase, letters, numbers and symbols. Do not include common words or names.' There are three input fields: 'old password', 'new password', and 'confirm password'. A red 'Modify' button is located below the input fields. At the bottom of the page, there is a copyright notice '© 2019 D-Link Corporation' and a language dropdown menu set to 'English'.

**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 to start the wizard.

In the **Lan Settings** section, the device connection parameters can be configured. These settings allow the management computer to connect to the device.

Parameter	Description
<b>Get Address From</b>	Click the drop-down menu to choose whether the DNH-100 will get an IP address from a DHCP server or to manually set a static IP address. By default it is set to Static IP Address. <b>Note:</b> DHCP server is not recommended.
<b>IP Address</b>	If the above is set to Static IP address, specify an IP address for the DNH-100.
<b>Subnet Mask</b>	Specify a subnet mask for the device.
<b>Gateway</b>	Specify a gateway mask for the device. (Optional)
<b>Primary DNS</b>	Specify a primary DNS for the device. (Optional)
<b>Secondary DNS</b>	Specify a secondary DNS for the device. (Optional)
<b>Synchronize Device Access Address</b>	Check to enable the synchronization of the device access address. If the device access address is different than the LAN IP address and you want to manage remote APs, this function needs to be disabled.

In the **Date and Time** section, parameters about the device time and date can be configured. It is recommended that an NTP server is used; log and schedule settings are depending on correct time and date configurations.

Parameter	Description
<b>Time Zone</b>	Click the drop-down menu to select the time zone.
<b>NTP</b>	Check to enable use of NTP server(s) to manage device's date and time.
<b>NTP Server 1</b>	Specify the NTP Server's address.
<b>NTP Server 2</b>	Specify the secondary NTP Server's address.

Click **Save** and the device will automatically restart. Re-login to continue with the wizard.

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

Parameter	Description
<b>Device Access Address</b>	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.
<b>Device Access Port</b>	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 inbound port must be opened.
<b>Web Access Port</b>	The web access ports as defined during the installation. The values are predefined.

Click **Next** to continue

The screenshot shows the 'System Settings' window with the following fields:

- Device Access Address: 192.168.0.200
- Device Access Port: 8443
- Web Access Port: 443
- Country: Afghanistan

A red 'Next' button is located at the bottom right of the window.

From the Site drop-down menu, selecting an existing site or select newSite 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. 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 first screenshot shows the 'Add Network' window with the following fields:

- Site: newSite
- Network Name: Network1

Buttons: Back, Next, Exit

The second screenshot shows the 'Network Configurations' window with the following sections:

- Wireless Settings:**
  - SSID Name: dflak
  - Security: WPA-Auto-Personal
  - SSID Password: [Redacted]
  - Add Guest SSID(Optional)
  - Guest SSID Name: [Redacted]
- Device Setting:**
  - Country: Afghanistan
  - Time Zone: (GMT+08:00) Taipei
  - Username: admin
  - New Password: [Redacted]

Buttons: Back, Next

The Discover Network Settings page will appear. Select the data link layer (layer 2 or layer 3) to define the type of network in which to find manageable access points. 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 screenshot shows the 'Discover Network Settings' window with the following options:

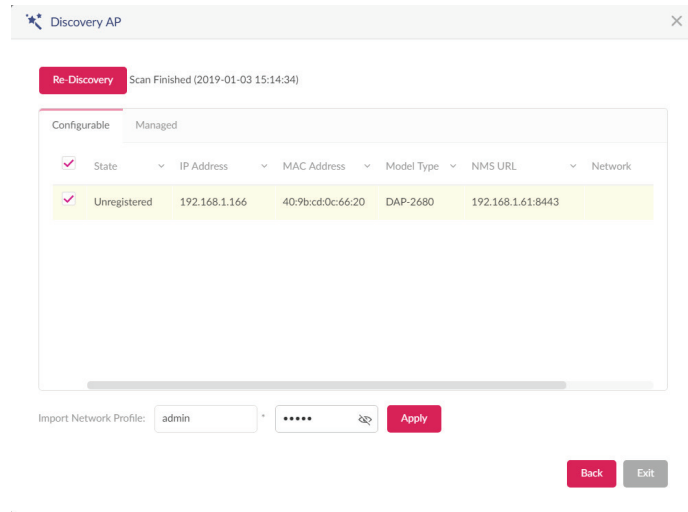
- Layer 2
- Layer 3 (IP)

Under Layer 3 (IP):

- IP: 192.168.1.150 - 192.168.1.200
- Pick one...: [Redacted]

Buttons: Next, Exit

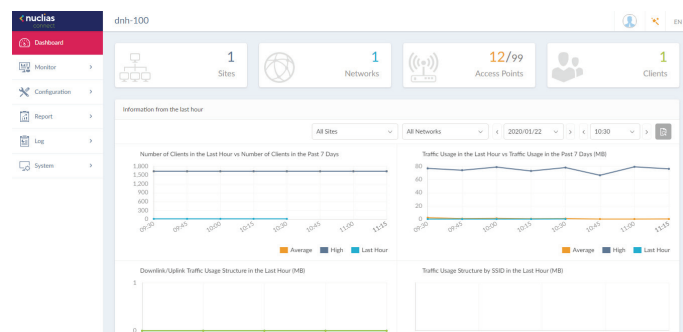
The Start Discovery Page will appear. Click **Start Discovery** to list all available unmanaged devices. If a device is found, select it and click **Apply** to import the network profile. Click on the Managed tab to select already defined devices and add them to this network.



# Dashboard

After successfully logging into the server, the **Dashboard** page will appear. A summary of information of all connected access points and wireless clients is available on this page.

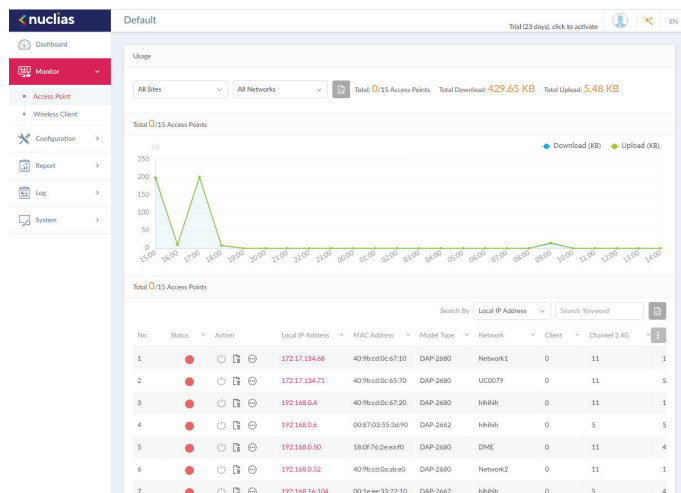
Block	Description
<b>Sites</b>	Displays the number of created profiles, also called sites.
<b>Networks</b>	Displays the total number of created networks.
<b>Access Points</b>	Displays the total number of available and online access points.
<b>Clients</b>	Displays the total number of wireless clients connected to the network.
<b>Information from the Last Hour</b>	Displays log information for the number of clients, traffic usage, downlink/uplink traffic usage, and traffic usage by SSID.
<b>Channel Utilization</b>	Displays the utilization rate for both 2.4 and 5 GHz bandwidth.
<b>Last Events</b>	Displays a shortened log version of the latest events across all or selected sites.



Nuclias Monitor Access Point

After clicking on **Monitor** -- > **Access Points** in the menu, the Usage and Total Access Points frames will appear. On this frame, you can view a report of all or a selected number wireless clients and networks managed by the application.

Three reports can be generated using **Site**, **Network**, or **Local IP** address.



The following figure represents a typical report. This report can be refined by selecting the a specific Site from the first drop-down menu, and then selecting the network in the second drop-down menu.

Block	Description
Usage	Displays a report listing the RX (kB) / TX (kB) usage for the specified site and network.
Total X Access Points	Displays a report listing all detected wireless clients.

In the **Search By** drop-down field, select an attribute (**Local IP Address**, **Local IPv6 Address**, **NAT IP Address**, **MAC Address**, **Model Type**, or **FW Version**) to specify the search function or enter a keyword related to the target device in the Search field.

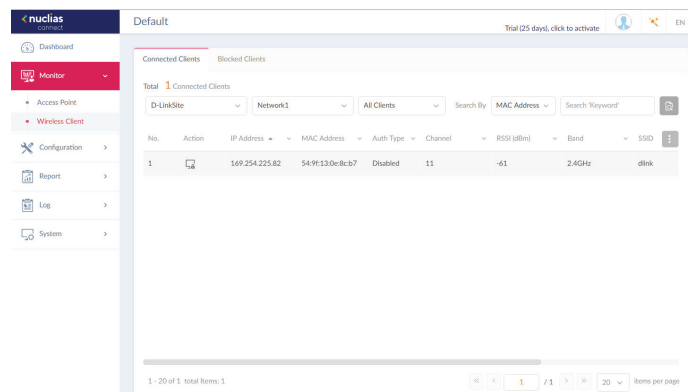
Click to start the process. Any relevant devices meeting the search criteria will be listed in the frame.

**Nuclias** **Monitor** **Wireless Client** **Connected Clients**

After clicking on **Wireless Clients** in the menu the Connected Clients frame will show by default. In this frame, you can view a report of all connected clients managed by the application.


Three association reports can be generated by **Site**, **Network**, and **Clients**.

The following figure represents a typical report. This report can be refined by selecting a specific Site from the first drop-down menu, and then selecting a network and client.



This page shows a report that was generated by connected wireless clients. This report can be refined by selecting the date and time **From** and **To**, and then selecting the **Type**, either **By MAC Address** or **By Alias**, and also additionally entering **Key Words** in the text box provided.

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

In the Search field, enter a keyword related to the target device and click  to start the process. Any relevant devices meeting the search criteria will be listed in the frame.

## Nuclias

## Monitor


## Wireless Client

## Blocked Clients

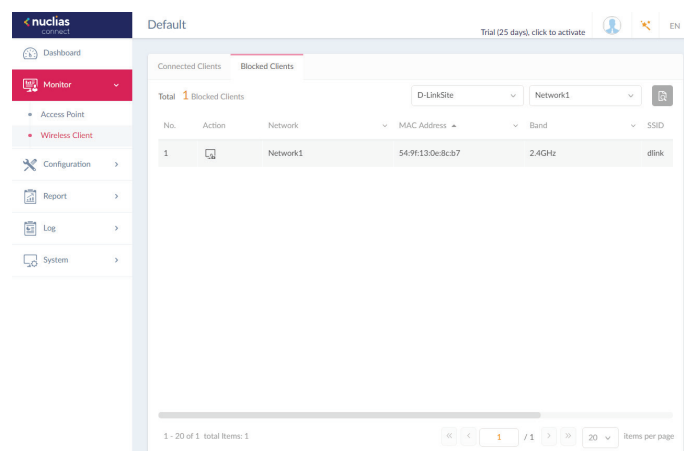
Click on **Blocked Clients**. In this frame, you can view a report of all blocked clients detected. This report can be generated by specifying **Site** and **Network** criteria.


The following figure represents a typical report. This report can be refined by selecting a specific Site from the first drop-down menu, and also then selecting the network.

In this report a list of blocked wireless client connections are displayed.

In the Search field, click the drop-down menu and select a Site then select a Network. Click  to start the process. Any relevant devices meeting the search criteria will be listed in the frame.

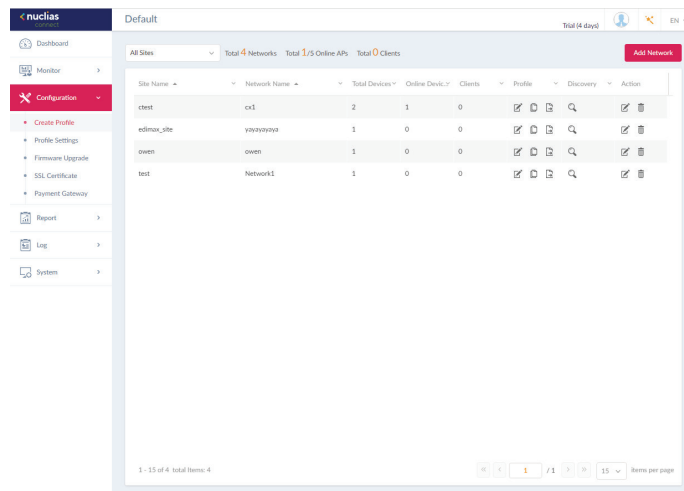
The report lists the following information: **No.**, **Action**, **Network**, **MAC Address**, **Band**, **SSID**, and **Auth. Type**.









No.	Action	Network	MAC Address	Band	SSID
1		Network1	54-9E-13-0e-Bc-b7	2.4GHz	dlink

The Create Profile function allows for the creation of new sites and networks.

After clicking on **Configuration > Create Profile** the Default frame displays listing all available sites and networks, see the following screen for further information.



Block	Description
<b>Edit Profile</b> 	Opens site details page, editing is available for selected site's security, access control, and user authentication settings.
<b>Copy Profile to this Network</b> 	Copies existing profile to a designated site and network.
<b>Export Network Profile</b> 	Exports selected profile to a file (*.dat) on a local directory.
<b>Discovery</b> 	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 <b>Next</b> . Click <b>Start Discovery</b> to find the results (Configurable and Managed devices) of the search.
<b>Edit Network</b> 	Opens the Edit Network page. From this page, you can edit network settings or migrate to a new or existing site.
<b>Delete Network</b> 	Deletes the selected network configuration.



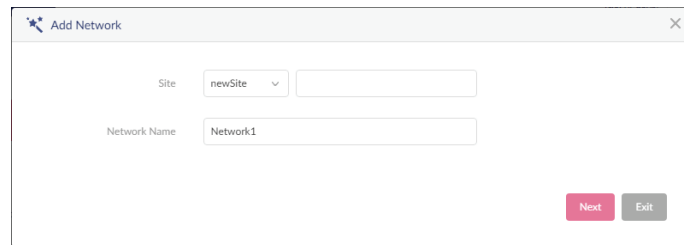
# Nuclias Configuration Create Profile **Add Network**

Click **Add Network** to create a new site and/or network.

From the Site drop-down menu, selecting an existing site or select newSite and enter the name of the site in the empty field.

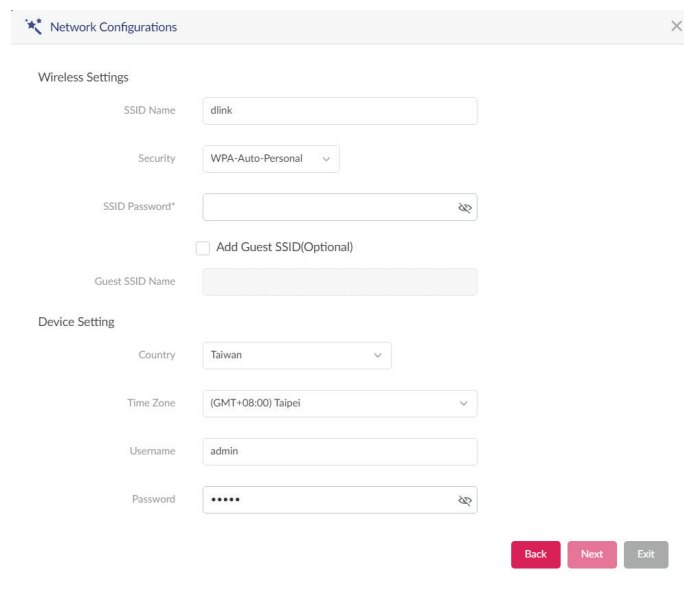
In the Network Name field, enter the name in which to identify the new network. Click **Next** to continue or **Exit** to return to the previous screen.

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 'Add Network' dialog box contains the following fields and controls:

- Site:** A dropdown menu with 'newSite' selected and an adjacent empty text input field.
- Network Name:** A text input field containing 'Network1'.
- Buttons:** 'Next' (pink) and 'Exit' (grey) buttons located at the bottom right.

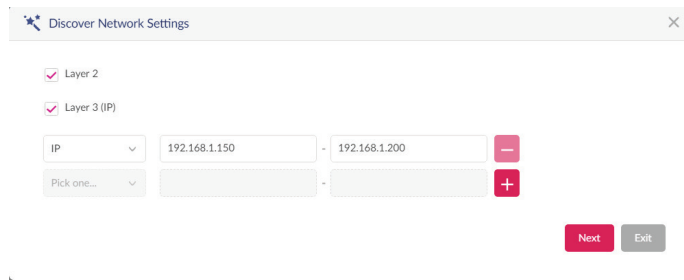


The 'Network Configurations' dialog box is divided into two sections:

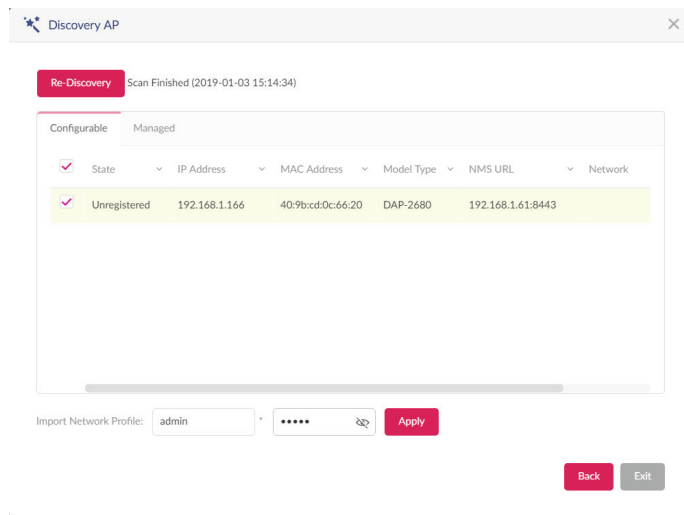
- Wireless Settings:**
  - SSID Name:** Text input field with 'dlink' entered.
  - Security:** Dropdown menu with 'WPA-Auto-Personal' selected.
  - SSID Password\*:** Password input field with a visibility icon.
  - Add Guest SSID(Optional):** An unchecked checkbox.
  - Guest SSID Name:** A disabled text input field.
- Device Setting:**
  - Country:** Dropdown menu with 'Taiwan' selected.
  - Time Zone:** Dropdown menu with '(GMT+08:00) Taipei' selected.
  - Username:** Text input field with 'admin' entered.
  - Password:** Password input field with four dots and a visibility icon.
- Buttons:** 'Back' (pink), 'Next' (pink), and 'Exit' (grey) buttons located at the bottom right.

**Nuclias Configuration Create Profile Add Network**

The Discover Network Settings page will appear. Select the data link layer (layer 2 or layer 3) to define the type of network in which to find manageable access points. 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 will appear. 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 already defined devices and add them to this network.



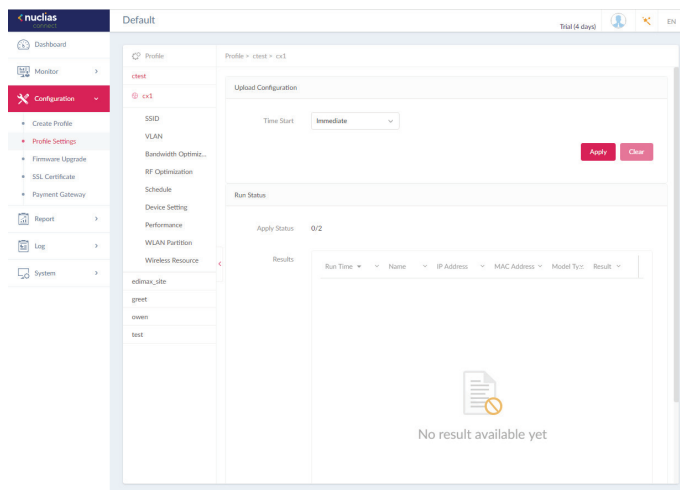
The **Profile Settings** function allows for the management of existing networks. Navigate to **Configuration > Profile Settings** to view existing sites. Select a site followed by an available network to view all settings that are available for editing: **SSID, VLAN, Bandwidth Optimization, RF Optimization, Schedule, Device Setting, Performance, WLAN Partition, and Wireless Resources**.

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. Under the **Upload Configuration** frame, click the **Time Start** drop-down menu and select the time (Immediate or Select Time) to update the configuration to the access point.

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

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



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

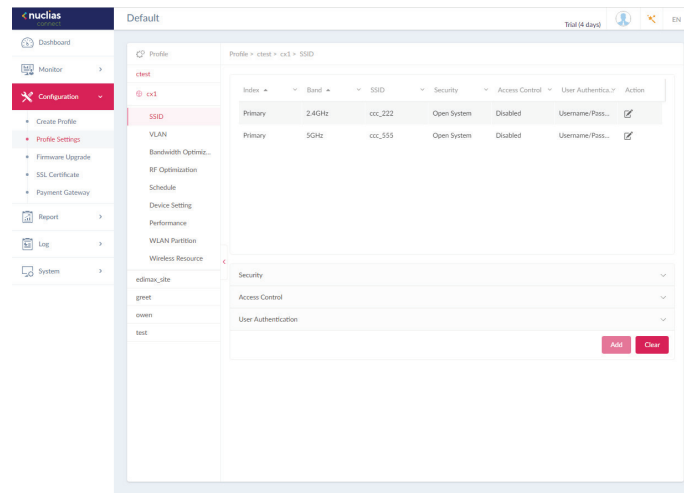
In the **Security** section, the following parameters can be configured:

Block	Description
<b>Band</b>	Click the drop-down menu to select wireless frequency band.
<b>Index</b>	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.
<b>SSID</b>	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 Connect. 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 Connect.
<b>Character Set</b>	Click the drop-down menu to select the character set to be used in the SSID encoding: UTF-8 or GB2312.
<b>SSID Broadcast</b>	Click the drop-down menu to enable or disable the wireless SSID visibility.
<b>WMM (Wi-Fi Multimedia)</b>	Click the drop-down menu to enable or disable the Wi-Fi multimedia.
<b>Security</b>	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).
<b>Fast Roaming (802.11 k/v/r)<sup>4</sup></b>	Click the drop-down menu to enable or disable fast roaming. This function is only available for compatible models and specific software version.
<b>Encryption</b>	Click the drop-down menu to enable or disable WEP Open System encryption. The function is only available when <b>Security</b> is set as <b>Open System</b> .
<b>Key Size</b>	Click the drop-down menu to select the WEP key size.
<b>Key Type</b>	Click the drop-down menu to select the WEP key type.
<b>Key Index</b>	Click the drop-down menu to select the WEP key index.
<b>Key Value</b>	Enter the open system WEP encryption key.
<b>Encryption Type</b>	Click the drop-down menu to select the encryption type: Auto, AES, or TKIP.
<b>Group Key Update Interval</b>	Enter the WPA group key update interval value.
<b>Passphrase</b>	Enter the secret pass phrase used. The function is only available when <b>Security</b> is <b>WPA-Personal</b> , <b>WPA2-Personal</b> or <b>WPA-Auto-Personal</b> .
<b>RADIUS Server</b>	Enter the RADIUS server's IP address. The function is only available when <b>Security</b> is <b>WPA-Enterprise</b> , <b>WPA2-Enterprise</b> or <b>WPA-Auto-Enterprise</b> .

Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 19 for further information.

<sup>4</sup> Currently only DAP-2662 and DAP-3666 supports this function.

Nuclias Configuration Profile Settings SSID



Block	Description
<b>Port</b>	Enter the RADIUS server's port number. The function is only available when <b>Security</b> is <b>WPA-Enterprise</b> , <b>WPA2-Enterprise</b> or <b>WPA-Auto-Enterprise</b> .
<b>RADIUS Secret</b>	Enter the RADIUS server's secret pass phrase. The function is only available when <b>Security</b> is <b>WPA-Enterprise</b> , <b>WPA2-Enterprise</b> or <b>WPA-Auto-Enterprise</b> .



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

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

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

Block	Description
<b>Authentication Type</b>	Click the drop-down menu to select the authentication type applied to the wireless client. <b>Note:</b> SLA Login (Click through) is currently only available for DAP-2662 and DAP-3666.
<b>Idle Timeout (2~1440)</b>	Enter the session timeout value.
<b>Enable White List</b>	Check the box to enable the white list function. This function is only available when <b>Authentication Type</b> is <b>Username/Password</b> .

Block	Description
<b>MAC Address</b>	Enter the MAC address of the network device that will be whitelisted and click <b>Add</b> to add the address to the white list table. This function is only available when <b>Authentication Type</b> is <b>Username/Password</b> .
<b>Upload Whitelist File</b>	Click <b>Browser...</b> to select the white list file, located on the local computer, that will be uploaded. Click <b>Upload</b> to update the white list. Click <b>Download</b> to download the current white list. The function is only available when <b>Authentication Type</b> is <b>Username/Password</b> .
<b>IPIF Status</b>	Click the drop-down menu to enable or disable the use of the IP interface.
<b>VLAN Group</b>	Enter the VLAN group name.
<b>Get IP Address From</b>	Click the drop-down menu to select the IP address configuration setting.
<b>IP Address</b>	Enter the IP address of the IP interface.
<b>Subnet Mask</b>	Enter the subnet mask of the IP interface.
<b>Gateway</b>	Enter the gateway of the IP interface.
<b>DNS</b>	Enter the preferred DNS address of the IP interface.
<b>Username</b>	Enter the username. The function is only available when <b>Authentication Type</b> is set as <b>Username/Password</b> .
<b>Password</b>	Enter the password and click <b>Add</b> . Click <b>Clear</b> to clear the entered fields. This function is only available when <b>Authentication Type</b> is <b>Username/Password</b> .
<b>RADIUS Server</b>	Enter the RADIUS server's IP address. This function is only available when <b>Authentication Type</b> is <b>Remote RADIUS</b> or <b>MAC Address</b> .
<b>RADIUS Port</b>	Enter the RADIUS server's port number. This function is only available when <b>Authentication Type</b> is <b>Remote RADIUS</b> or <b>MAC Address</b> .
<b>RADIUS Secret</b>	Enter the RADIUS server's secret. This function is only available when <b>Authentication Type</b> is <b>Remote RADIUS</b> or <b>MAC Address</b> .
<b>Remote RADIUS Type</b>	Enter the RADIUS server's type. This function is only available when <b>Authentication Type</b> is <b>Remote RADIUS</b> or <b>MAC Address</b> .
<b>Server</b>	Enter the LDAP server's IP address. This function is only available when <b>Authentication Type</b> is <b>LDAP</b> .
<b>Port</b>	Enter the LDAP server's port number. This function is only available when <b>Authentication Type</b> is <b>LDAP</b> .
<b>Authentication Mode</b>	Click on the drop-down menu to select the authentication mode. This function is only available when <b>Authentication Type</b> is <b>LDAP</b> .
<b>Username</b>	Enter the administrator's username that will be able to access and search the LDAP database. This function is only available when <b>Authentication Type</b> is <b>LDAP</b> .
<b>Password</b>	Enter the administrator's password that will be able to access and search the LDAP database. This function is only available when <b>Authentication Type</b> is <b>LDAP</b> .
<b>Base DN</b>	Enter the base domain name of the LDAP database. This function is only available when <b>Authentication Type</b> is <b>LDAP</b> .
<b>Account Attribute</b>	Enter attribute for the account. This function is only available when <b>Authentication Type</b> is <b>LDAP</b> .
<b>Identity</b>	Enter the name of the administrator. This function is only available when <b>Authentication Type</b> is <b>LDAP</b> .

Block	Description
<b>Server</b>	Enter the POP3 server's IP address. This function is only available when <b>Authentication Type</b> is <b>POP3</b> .
<b>Port</b>	Enter the POP3 server's port number. This function is only available when <b>Authentication Type</b> is <b>POP3</b> .
<b>Connection Type</b>	Click the drop-down menu to select the connection type. This function is only available when <b>Authentication Type</b> is <b>POP3</b> .
<b>Passcode List</b>	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 <b>Authentication Type</b> is <b>Passcode</b> .
<b>External Captive Portal</b>	Click the drop-down menu to select HTTP or HTTPS. After selecting, enter the URL of the website. This function is only available when <b>Authentication Type</b> is <b>External Captive Portal</b> .
<b>Web Redirection</b>	Check the box to enable the website redirection function.
<b>Website</b>	Click the drop-down menu to select HTTP or HTTPS. After selecting, enter the URL of the website.
<b>Choose Template</b>	Click the drop-down menu to select the used login style. This function is only not available when <b>Authentication Type</b> is <b>Web Redirection Only</b> . <b>Note:</b> <ul style="list-style-type: none"> <li>Click <b>Preview</b> to preview the selected style.</li> <li>Click <b>Upload Login File</b> to upload a new style.</li> <li>Click  to delete the selected style.</li> <li>Click  to download the style template.</li> </ul>

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.<sup>5</sup>

Block	Description
<b>Hotspot 2.0</b>	Click the drop-down menu to enable or disable hotspot 2.0.
<b>OSEN</b>	Enable OSU Server-only authenticated layer-2 Encryption Network (OSEN) to indicate that the hotspot uses a OSEN network type.
<b>Allow Cross Connection</b>	Choose enable to allow cross connection for clients.
<b>Manage P2P</b>	Choose enable to allow P2P.
<b>DGAF</b>	This option configures the Downstream Group Addressed Forwarding. Choose enable to allow AP to forward downstream groupaddressed frames.
<b>Proxy APR</b>	Choose enable to allow proxy ARP.
<b>L2TIF</b>	Choose enable to allow Layer 2 Traffic Inspection and Filtering.
<b>Interworking</b>	Choose enable to enable the interworking function.
<b>Access Network Type</b>	Choose from drop-down menue the access network type.
<b>Internet</b>	Choose to enable or disable Internet access for this network.
<b>ASRA</b>	Choose enable if the network has Additional Steps required for Access.

<sup>5</sup> Currently only DAP-2662 and DAP-3666 supports this function.

<b>ESR</b>	Choose enable to indicate that emergency services are reachable through this device.
<b>USEA</b>	Choose to enable or disable USEA.
<b>Venue Group</b>	Specify group venue belongs to.
<b>Venue Type</b>	Specify type of venue.
<b>Venue Name</b>	Specify name of venue. Choose from the drop down list a language used in the name.
<b>HESSID</b>	Specify a homogenous extended service set (ESS) ID that can be used to identify a specific service provider network.
<b>WAN Link Status</b>	Set information about the status of the Access Point's WAN connection from the drop-down menu.
<b>WAN Symmetric Link</b>	Specify state of the WAN link is symmetric (upload and download speeds are the same).
<b>WAN At Capacity</b>	Specify yes if the Access Point or the network is at its max capacity, or specify no if not.
<b>WAN Metrics DL Speed (kps)</b>	The downlink speed of the WAN connection set in kbps. If the downlink speed is not known, set to 0.
<b>WAN Metrics UL Speed (kps)</b>	The uplink speed of the WAN connection set in kbps. If the uplink speed is not known set to 0.
<b>Network Auth Type</b>	Choose from drop-down menu the network authentication type and specify the web-address.
<b>IP Address Type Availability</b>	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.
<b>Domain Name</b>	List one or more domain names for the entity operating the AP.
<b>Roaming Consortium</b>	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.
<b>Nai Realm</b>	Specify list of all NAI realms available through the BSS. Click subtract icon to delete it from the list.
<b>EAP Method</b>	Specify one or more EAP methods and its authentication ID and Parameter type. Click Delete icon to delete it from the list.
<b>RFC 4282</b>	Click on drop-down menu to enable or disable RFC 4282.
<b>3gpp Cellular Network</b>	Specify a list of the 3GPP cellular networks available through the AP. Specify the MCC and MNC, then click Add icon. Click Delete icon to delete it from the list.
<b>Connection Capability</b>	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.
<b>Operator Friendly Name</b>	Identifies the Hotspot venue operator and choose its language.
<b>OSU SSID</b>	Specify OSU SSID name.
<b>OSU Server URI</b>	Specify OSU Server URI
<b>OSU Method</b>	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.
<b>OSU Config</b>	Choose from drop-down menu the OSU Configu.
<b>OSU Language Code</b>	Choose a language from the drop-down menu.
<b>OSU Friendly Name</b>	Choose a language from the drop-down menu and specify the OSU friendly name.
<b>OSU Nai</b>	Specify the OSU NAI.



---

<b>OSU Service Description</b>	Specify a service description for the OSU.
<b>OSU Icon Language Code</b>	Specify from drop-down menu the language of the icon.
<b>OSU Icon File Path</b>	Specify location of icon file.
<b>OSU Icon File Name</b>	Specify icon file name.
<b>OSU Icon Width</b>	Specify width of the icon, in pixels.
<b>OSU Icon Height</b>	Specify length of the icon, in pixels.
<b>OSU Icon Type</b>	Specify icon file type from the drop-down menu.

---

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

Click **Clear** to reset all settings.

Nuclias Configuration Profile Settings **VLAN**

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

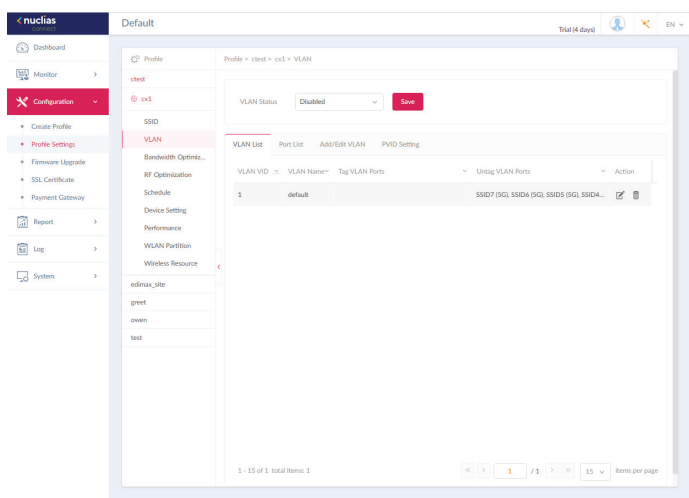
Block	Description
<b>VLAN Status</b>	Click the drop-down menu to enable or disable VLANs.

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 will appear. 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 will 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 will show the connected virtual LAN segment.

In the **Add/Edit VLAN** tab, we can create a new VLAN and assign untagged ports in that VLAN. After clicking the Modify icon in the VLAN List tab, you will be re-directed to this 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.

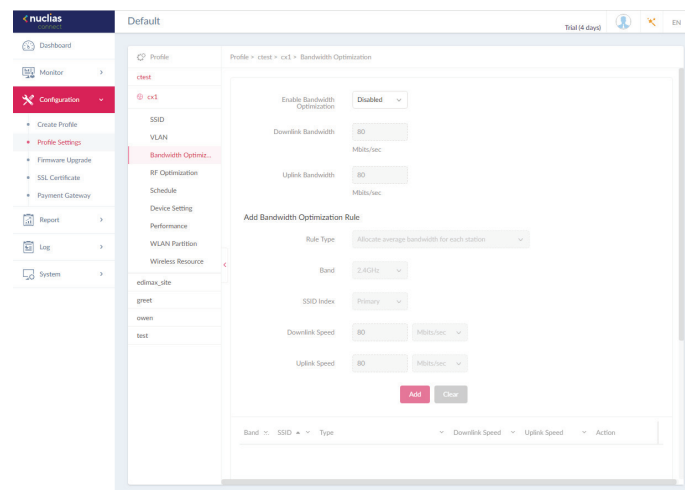
Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 19 for further information.

## Nuclias Configuration Profile Settings **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.

Block	Description
<b>Enable Bandwidth Optimization</b>	Click the drop-down menu to enable or disable the bandwidth optimization function.
<b>Downlink Bandwidth</b>	Enter the total downlink bandwidth speed for the access points in the network.
<b>Uplink Bandwidth</b>	Enter the total uplink bandwidth speed for the access points in the network.
<b>Rule Type</b>	Click the drop-down menu to select the rule type. <ul style="list-style-type: none"> <li>Allocate an average BW for each station: Optimize bandwidth by averaging the allocated bandwidth for each client.</li> <li>Allocate a maximum BW for each station: Specify the maximum bandwidth for each connected client, while reserving available bandwidth for additional clients.</li> <li>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.</li> <li>Allocate a specific BW for SSID: All clients share the assigned bandwidth.</li> </ul>
<b>Band</b>	Click the drop-down menu to select the wireless frequency band used in the rule.
<b>SSID Index</b>	Click the drop-down menu to select the SSID used in the rule.
<b>Downlink Speed</b>	Enter the downlink speed assigned to either each station or the specified SSID.
<b>Uplink Speed</b>	Enter the uplink speed assigned to either each station or the specified SSID.
<b>Add</b>	Click <b>Add</b> to add the rule into the Bandwidth Optimization Rules.
<b>Clear</b>	Click <b>Clear</b> to clear the entered rule.

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



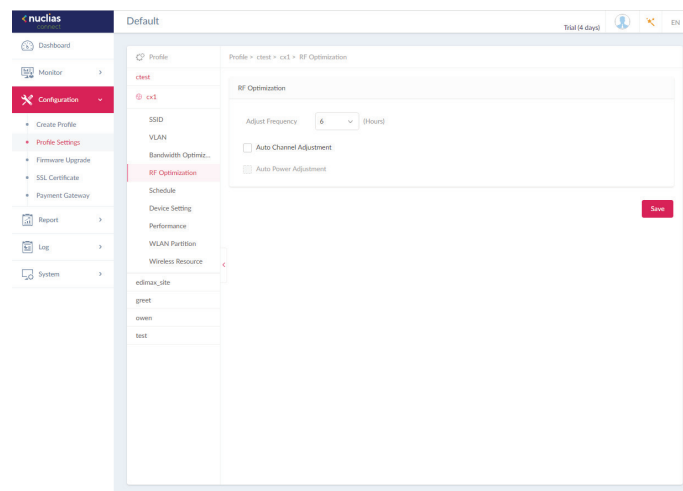
Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 19 for further information.

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

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



Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 19 for further information.

Nuclias Configuration Profile Settings **Schedule**

The Schedule page displays the wireless schedule settings describing how to specify a schedule for your network. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Schedule** to view existing settings.

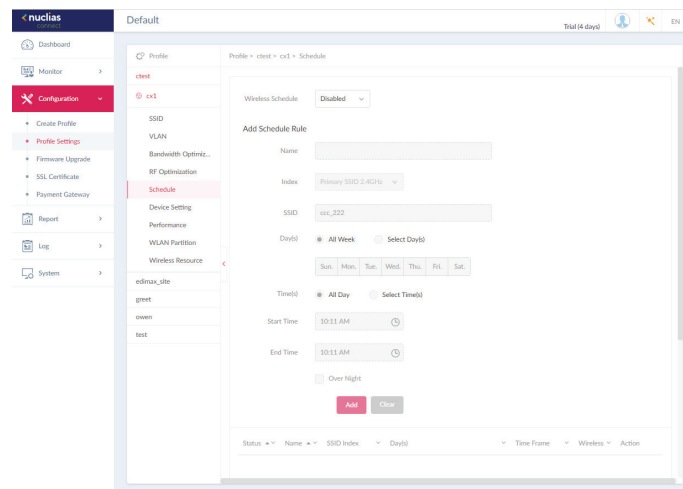
Parameter	Description
<b>Wireless Schedule</b>	Click the drop-down menu to enable or disable the wireless schedule function.
<b>Name</b>	Enter the name of the schedule rule.
<b>Index</b>	Click the drop-down menu to select SSID on which the schedule setting is applied.
<b>SSID</b>	Display the SSID name.
<b>Day(s)</b>	Click the radio button to select the active days for the schedule. <ul style="list-style-type: none"> <li>All Week: Enable the rule for the whole week.</li> <li>Select Day(s): Specifies particular day(s) to activate the rule.</li> </ul>
<b>Time(s)</b>	Click the radio button to select the active times for the schedule. <ul style="list-style-type: none"> <li>All Day: Enable the rule for the whole day.</li> <li>Select Time(s): Specifies a starting and ending time for the rule.</li> </ul>
<b>Start Time</b>	Enter the hours and minutes of the day. This function is only available when <b>Time(s)</b> is <b>Select Time(s)</b> .
<b>End Time</b>	Enter the hours and minutes of the day. This function is only available when <b>Time(s)</b> is <b>Select Time(s)</b> .
<b>Over Night</b>	Check the box to enable activity overnight.
<b>Add</b>	Click <b>Add</b> to add the rule into the schedule.
<b>Clear</b>	Click <b>Clear</b> to clear the entered rule.

Click  to modify the desired rule.

Click  to delete the desired rule.

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

Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 19 for further information.



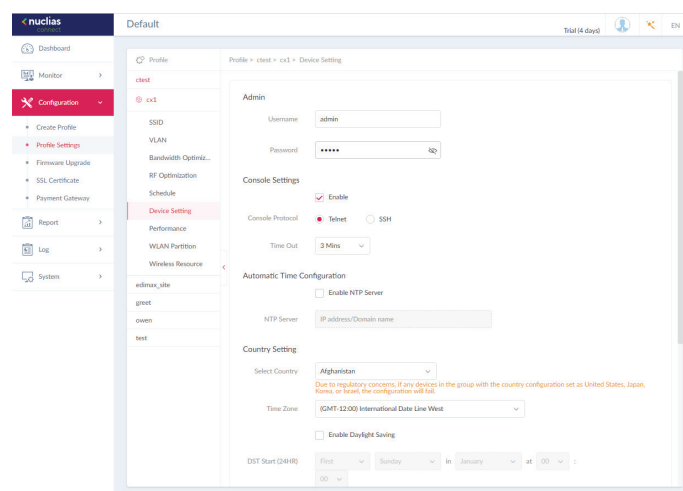
# Nuclias Configuration Profile Settings **Device Setting**

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

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

Once the settings are updated, the configuration must be uploaded to the related access points. See "Profile Settings" on page 19 for further information.

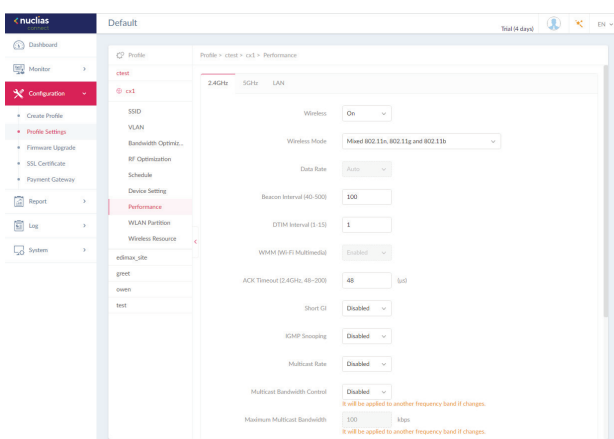


## Nuclias Configuration Profile Settings **Performance 2.4GHz/5GHz**

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

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



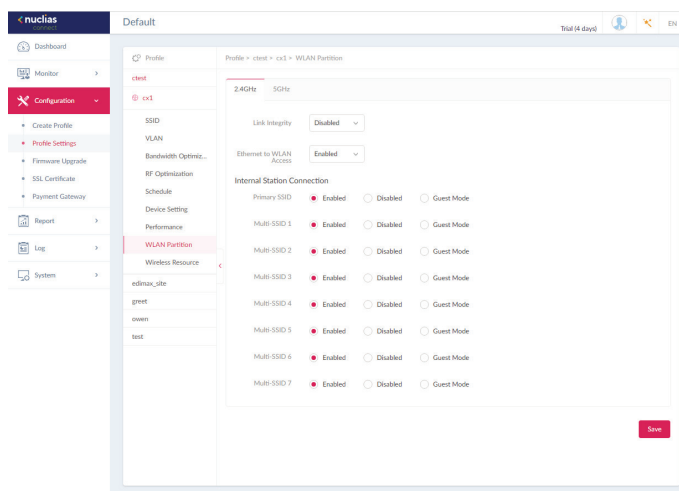
Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 19 for further information.

Nuclias Configuration Profile Settings WLAN Partition  
**2.4GHz/5GHz**

The WLAN Partition page displays the wireless partitioning settings that allows 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.

Parameter	Description
<b>Link Integrity</b>	Click the drop-down menu to enable or disable the wireless link integrity function.
<b>Ethernet to WLAN Access</b>	Click the drop-down menu to enable or disable Ethernet to WLAN access function.
<b>Internal Station Connection</b>	Click the radio button to enable or disable the membership of the SSID to the WLAN partition. Select <b>Guest Mode</b> to allow this SSID to have access to this WLAN partition as a guest.

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



Once the settings are updated, the configuration must be uploaded to the related access points. See “Profile Settings” on page 19 for further information.



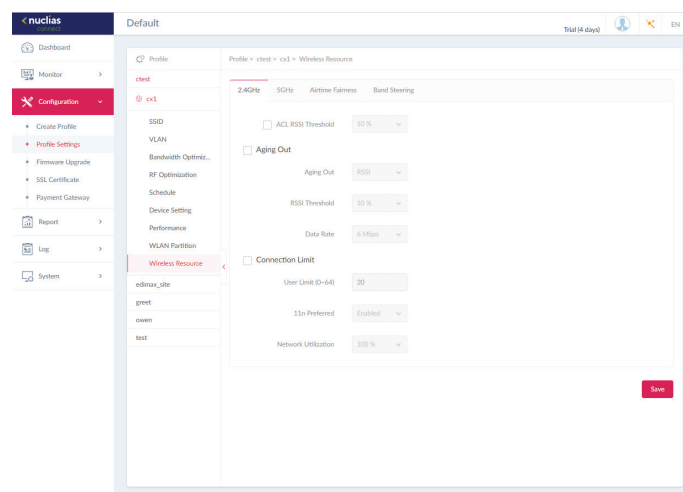
# Nuclias Configuration Profile Settings Wireless Resource

## 2.4GHz/5GHz

The Wireless Resource function in Nuclias Connect helps provides 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
<b>ACL RSSI Threshold</b>	Check the box to enable ACL RSSI threshold function and click the drop-down menu to select the ACL RSSI threshold percentage.
<b>Aging Out</b>	Use the drop-down menu to select criteria to disconnect wireless clients. Available options are RSSI and Data Rate.
<b>Aging Out</b>	Click the drop-down menu to select the aging out mode
<b>RSSI Threshold</b>	When <b>RSSI</b> is selected in the Aging out drop-down menu, select a value between 10% to 100%. This parameter sets the minimum RSSI for a wireless clients to respond to a probe. If the determined value is lower than the specified percentage, the wireless client is disconnected.
<b>Data Rate</b>	Click the drop-down menu to select the data rate connection limit. The function is only available when the <b>Aging Out</b> policy is set to <b>Data Rate</b> .
<b>Connection Limit</b>	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.
<b>User Limit (0~64)</b>	Enter the user connection limit. The default value is 20.
<b>11n Preferred</b>	Click the drop-down menu to enable or disable the preferred use of 802.11n.
<b>Network Utilization</b>	Click the drop-down menu to select the network utilization percentage.

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



Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 19 for further information.

# Nuclias Configuration Profile Settings Wireless Resource

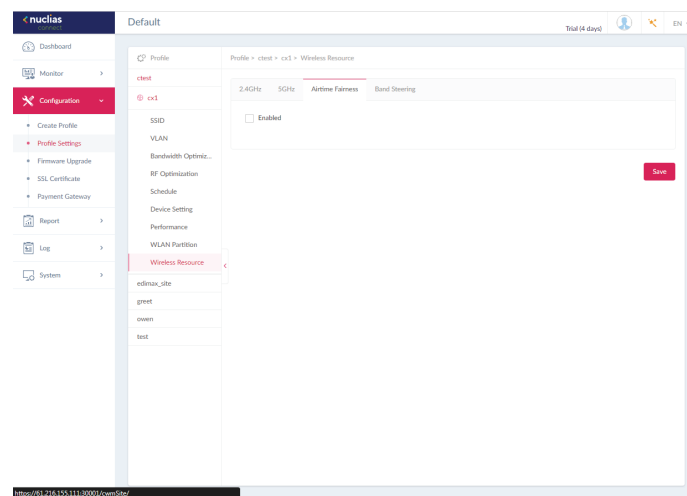
## Airtime Fairness

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

Note: Devices identified as having slow 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" on page 19 for further information.

# Nuclias Configuration Profile Settings Wireless Resource

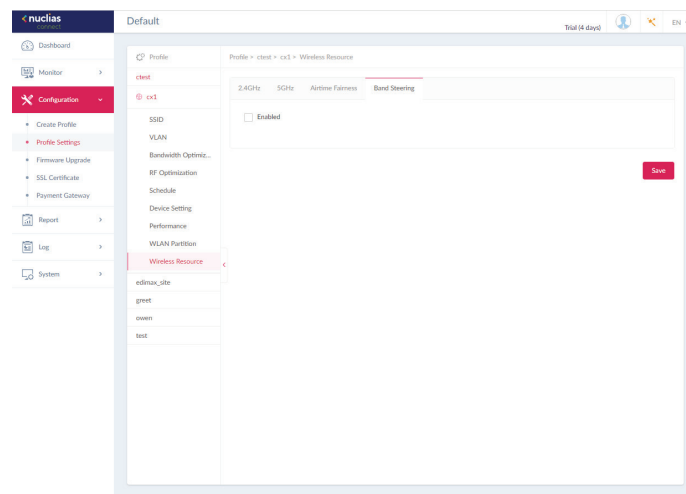
## Band Steering

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



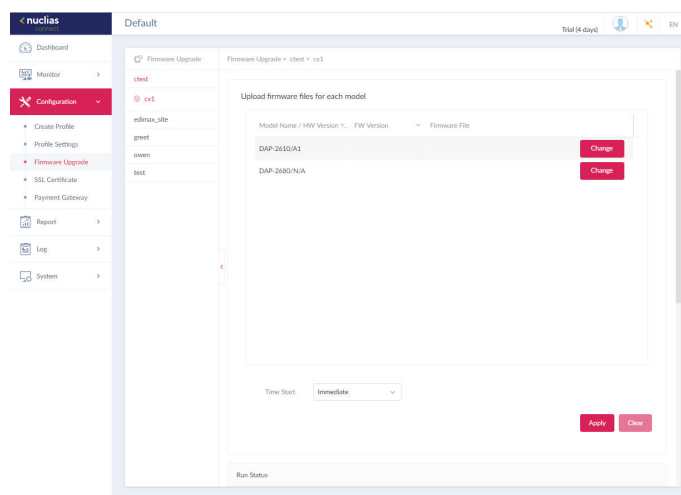
The Firmware Upgrade function allows users to perform a firmware upgrade. This is a useful feature that prevents future bugs and allows for new features to be added your device. Please go to your local D-Link website to see if there is a newer version firmware available.

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

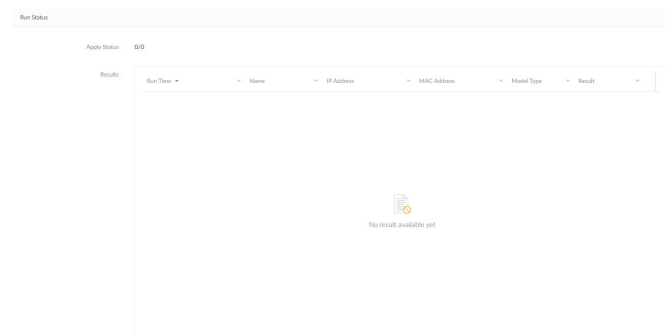
Block	Description
<b>Change</b>	Click to select a firmware file to upload. Files are model specific.
<b>Time Start</b>	Click the drop-down menu to select a specific time or to update immediately.

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 bottom of this page. The results can be sorted by Run Time, Name, IP Address, MAC Address, Model Type and Result.

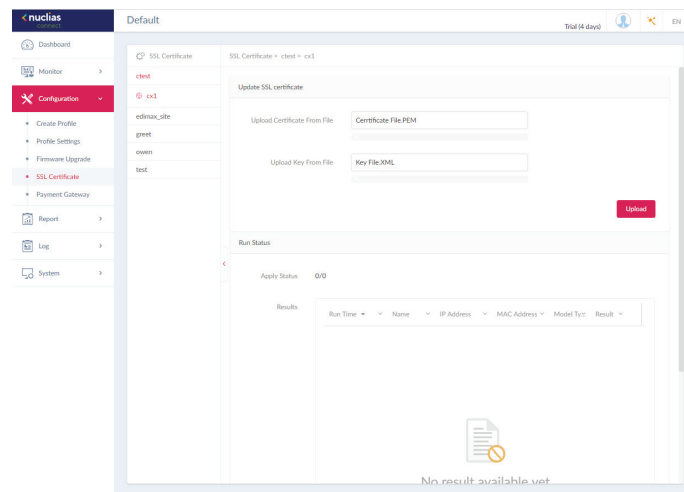


The SSL Certificate function provides the means to install an SSL certificate for use on the network. To accomplish this task an intermediate certificate is required. The intermediate certificate is used to establish the trust of the SSL certificate by binding it to the Certificate Authority's root certificate.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

Block	Description
<b>Upload Certificate From File</b>	Click <b>Browser...</b> to select the SSL certificate file located on the drive that will be uploaded.
<b>Upload Key From File</b>	Click <b>Browser...</b> 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 below area.

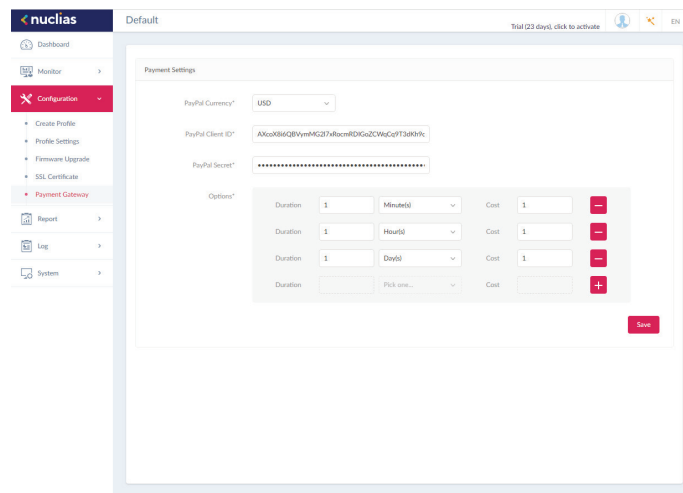


The payment gateway is a function that allows e-commerce services within the network. The Payment Gateway page will show payment settings and options necessary to enable payment services.

Navigate to **Configuration > Payment Gateway**.

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

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




## Nuclias

## Report

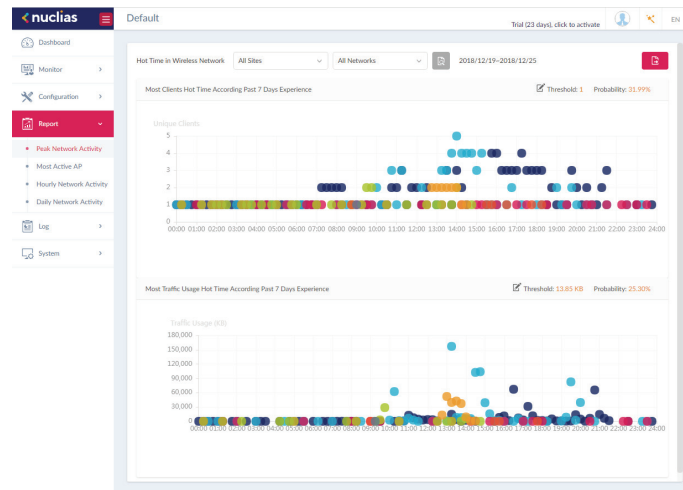
## Peak Network Activity

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 > 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.






## Nuclias

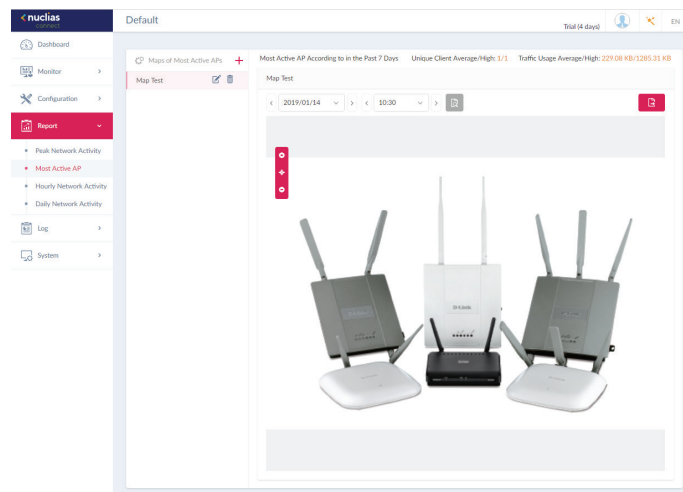
## Report

## 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.






## Nuclias

## Report

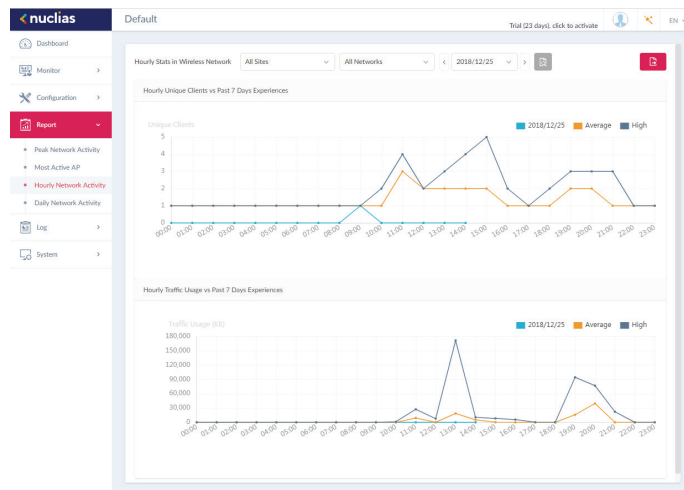
## Hourly Network Activity

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

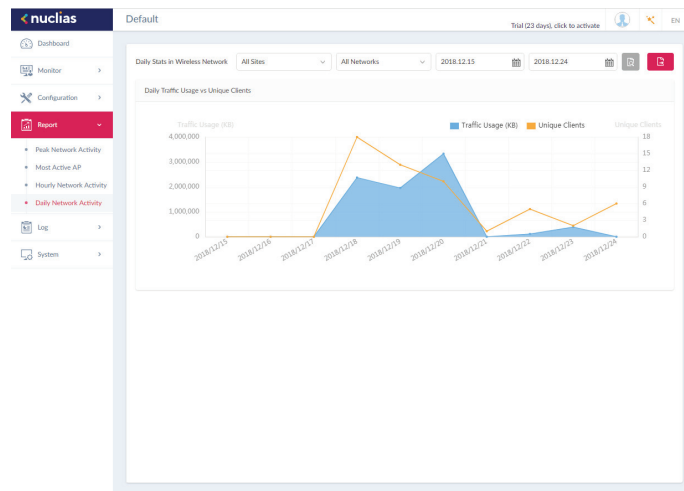


The Daily Network Activity function allows administrators to monitor daily wireless traffic on the network. Wireless activity is displayed according to unique clients and daily traffic usage.


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.

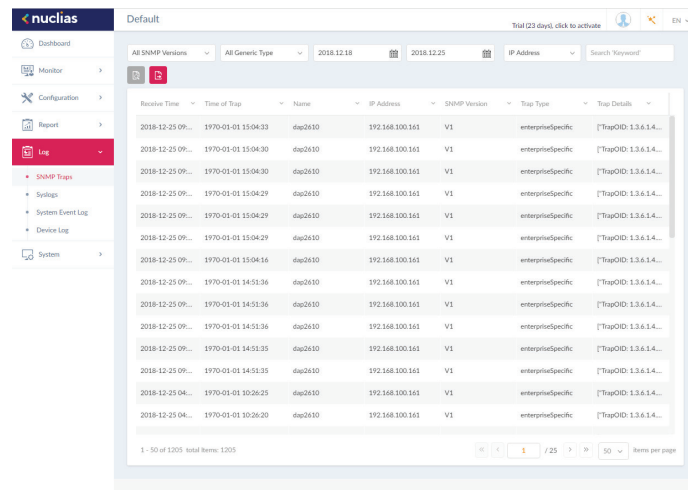
Once a report has been generated, click  to save the report to a local PDF file.



The SNMP Traps function allows administrators to view alert messages when events concerning network devices occur. Navigate to **Log > SNMP Traps** to generate and view the report.

To start a trap report, select the SNMP version, the event type and define the period of time to report. Click the drop-down menu to choose either IP address or Trap Details as report criteria. Fill in the keyword field and click  to view the defined report.


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



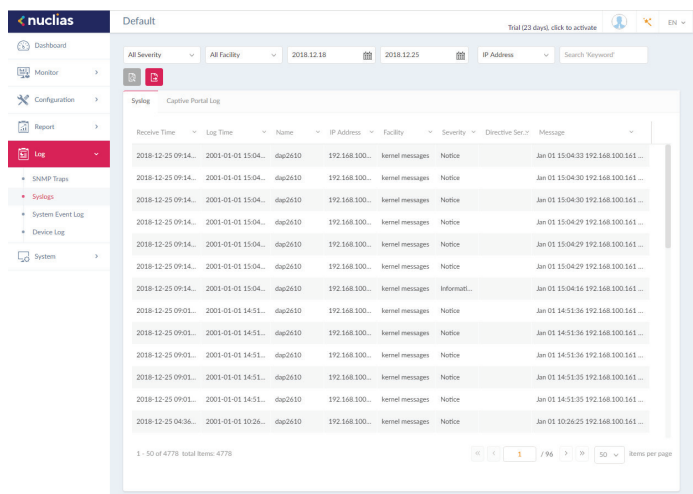
Receive Time	Time of Trap	Name	IP Address	SNMP Version	Trap Type	Trap Details
2018-12-25 09:...	1970-01-01 15:04:33	dap2610	192.168.100.161	V1	enterpriseSpecific	[TrapOID: 1.3.6.1.4...
2018-12-25 09:...	1970-01-01 15:04:30	dap2610	192.168.100.161	V1	enterpriseSpecific	[TrapOID: 1.3.6.1.4...
2018-12-25 09:...	1970-01-01 15:04:30	dap2610	192.168.100.161	V1	enterpriseSpecific	[TrapOID: 1.3.6.1.4...
2018-12-25 09:...	1970-01-01 15:04:29	dap2610	192.168.100.161	V1	enterpriseSpecific	[TrapOID: 1.3.6.1.4...
2018-12-25 09:...	1970-01-01 15:04:29	dap2610	192.168.100.161	V1	enterpriseSpecific	[TrapOID: 1.3.6.1.4...
2018-12-25 09:...	1970-01-01 15:04:29	dap2610	192.168.100.161	V1	enterpriseSpecific	[TrapOID: 1.3.6.1.4...
2018-12-25 09:...	1970-01-01 15:04:16	dap2610	192.168.100.161	V1	enterpriseSpecific	[TrapOID: 1.3.6.1.4...
2018-12-25 09:...	1970-01-01 14:55:36	dap2610	192.168.100.161	V1	enterpriseSpecific	[TrapOID: 1.3.6.1.4...
2018-12-25 09:...	1970-01-01 14:55:36	dap2610	192.168.100.161	V1	enterpriseSpecific	[TrapOID: 1.3.6.1.4...
2018-12-25 09:...	1970-01-01 14:55:36	dap2610	192.168.100.161	V1	enterpriseSpecific	[TrapOID: 1.3.6.1.4...
2018-12-25 09:...	1970-01-01 14:55:35	dap2610	192.168.100.161	V1	enterpriseSpecific	[TrapOID: 1.3.6.1.4...
2018-12-25 04:...	1970-01-01 10:26:25	dap2610	192.168.100.161	V1	enterpriseSpecific	[TrapOID: 1.3.6.1.4...
2018-12-25 04:...	1970-01-01 10:26:20	dap2610	192.168.100.161	V1	enterpriseSpecific	[TrapOID: 1.3.6.1.4...

Nuclias Log Syslogs Syslog


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

To start a syslog report, select the event severity, facility system, and define the period of time to report. Click the drop-down menu to choose either IP address or Message as report criteria. Fill in the keyword field and click  to view the generated report.

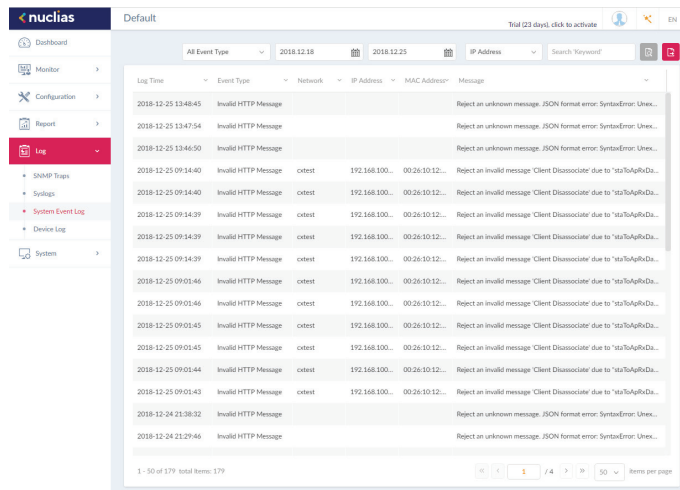
Once a report has been generated, click  to save the report to a local PDF file.



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.




Nuclias

Log

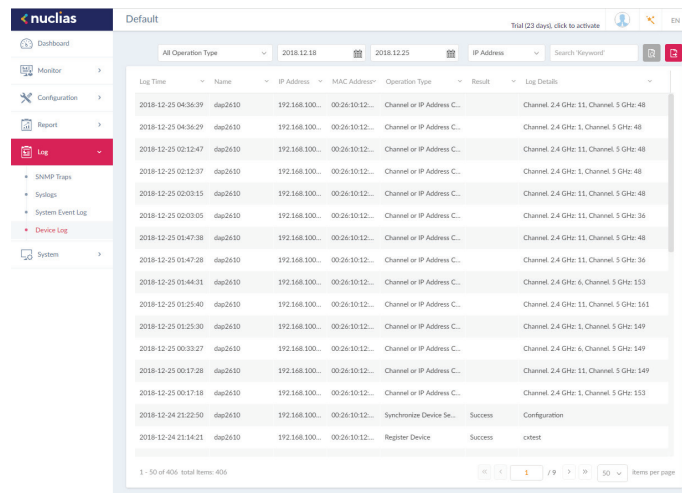
Device Log

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.



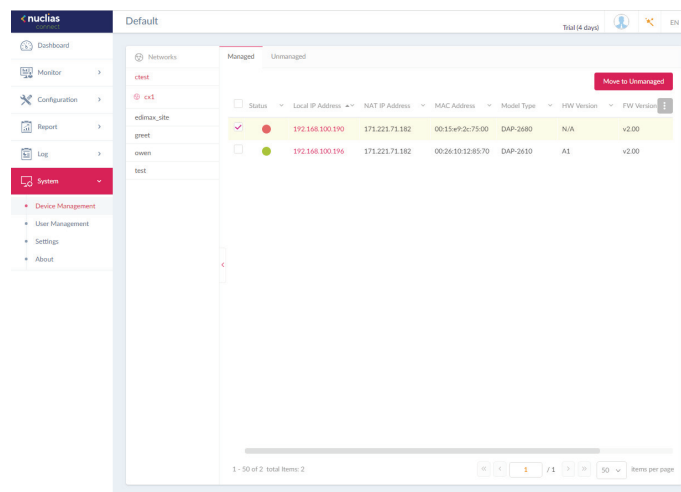
Log Time	Name	IP Address	MAC Address	Operation Type	Result	Log Details
2018-12-25 04:36:29	dap2650	192.168.100...	00:26:10:12...	Channel or IP Address C...		Channel 2.4 GHz: 11, Channel 5 GHz: 48
2018-12-25 02:12:47	dap2650	192.168.100...	00:26:10:12...	Channel or IP Address C...		Channel 2.4 GHz: 11, Channel 5 GHz: 48
2018-12-25 02:12:37	dap2650	192.168.100...	00:26:10:12...	Channel or IP Address C...		Channel 2.4 GHz: 11, Channel 5 GHz: 48
2018-12-25 02:03:15	dap2650	192.168.100...	00:26:10:12...	Channel or IP Address C...		Channel 2.4 GHz: 11, Channel 5 GHz: 48
2018-12-25 02:03:05	dap2650	192.168.100...	00:26:10:12...	Channel or IP Address C...		Channel 2.4 GHz: 11, Channel 5 GHz: 36
2018-12-25 01:47:38	dap2650	192.168.100...	00:26:10:12...	Channel or IP Address C...		Channel 2.4 GHz: 11, Channel 5 GHz: 48
2018-12-25 01:47:28	dap2650	192.168.100...	00:26:10:12...	Channel or IP Address C...		Channel 2.4 GHz: 11, Channel 5 GHz: 36
2018-12-25 01:44:31	dap2650	192.168.100...	00:26:10:12...	Channel or IP Address C...		Channel 2.4 GHz: 6, Channel 5 GHz: 153
2018-12-25 01:25:40	dap2650	192.168.100...	00:26:10:12...	Channel or IP Address C...		Channel 2.4 GHz: 11, Channel 5 GHz: 161
2018-12-25 01:25:30	dap2650	192.168.100...	00:26:10:12...	Channel or IP Address C...		Channel 2.4 GHz: 1, Channel 5 GHz: 149
2018-12-25 00:32:27	dap2650	192.168.100...	00:26:10:12...	Channel or IP Address C...		Channel 2.4 GHz: 6, Channel 5 GHz: 149
2018-12-25 00:17:28	dap2650	192.168.100...	00:26:10:12...	Channel or IP Address C...		Channel 2.4 GHz: 11, Channel 5 GHz: 149
2018-12-25 00:17:18	dap2650	192.168.100...	00:26:10:12...	Channel or IP Address C...		Channel 2.4 GHz: 1, Channel 5 GHz: 153
2018-12-24 21:22:50	dap2650	192.168.100...	00:26:10:12...	Synchronize Device Se...	Success	Configuration
2018-12-24 21:14:21	dap2650	192.168.100...	00:26:10:12...	Register Device	Success	extest

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.

Click on the relevant tab to view either managed or unmanaged devices.

On the upper right hand corner of each tab is a button that you can use to move devices to Unmanaged, and vice versa. Next to the Move button in the unmanaged tab, the Delete button the Delete button that can be used to delete a device on the network.

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 criteria by which you can add to the list to view.




The screenshot displays the Nuclias Device Management interface. The left sidebar shows the navigation menu with 'System' selected. The main content area is titled 'Default' and shows a list of devices under the 'Managed' tab. The table has columns for Status, Local IP Address, NAT IP Address, MAC Address, Model Type, HW Version, and FW Version. There are two rows of device data.

Status	Local IP Address	NAT IP Address	MAC Address	Model Type	HW Version	FW Version
✓	192.168.100.190	173.223.71.182	00:15:e9:2c:75:00	DAP-2680	N/A	v2.00
●	192.168.100.196	173.223.71.182	00:26:10:32:85:70	DAP-2680	A1	v2.00

The User Status function allows administrators to view the current status of all registered user profiles, edit or delete the profile. From the page, the Login Status displays the login state of the user; ● indicates a logged in state, while ● indicates the user is logged off.

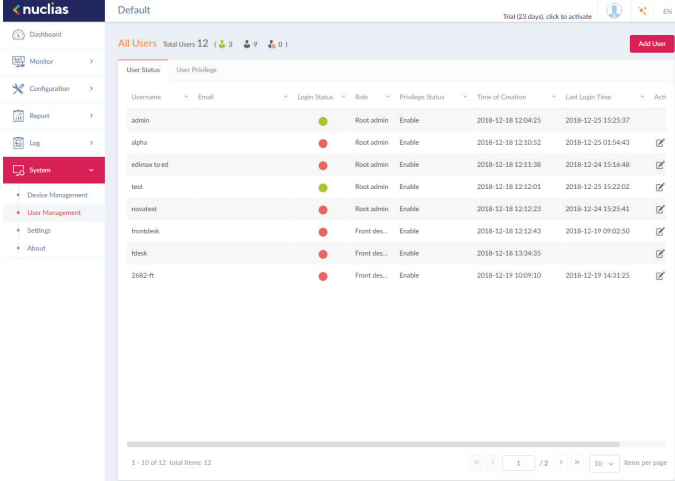
Navigate to **System > User Management** to view the relevant information.








To edit a user profile, select a user and click . The username, password, email, privilege, privilege status, location, contact number as well as the user description are editable from the modifications page. As a note, the administrator account cannot be deleted or have its username and privilege settings modified.

Once you have finished editing user settings, 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.

- Admin: This is operator account and can not be deleted.
- Root admin: Can manage all sites/networks on this server.
- Local admin: Can manage his own network.
- Root user: Can view all sites/networks on this server.
- Local user: Can view his own network
- Front desk user: Can generate and manage passcodes.



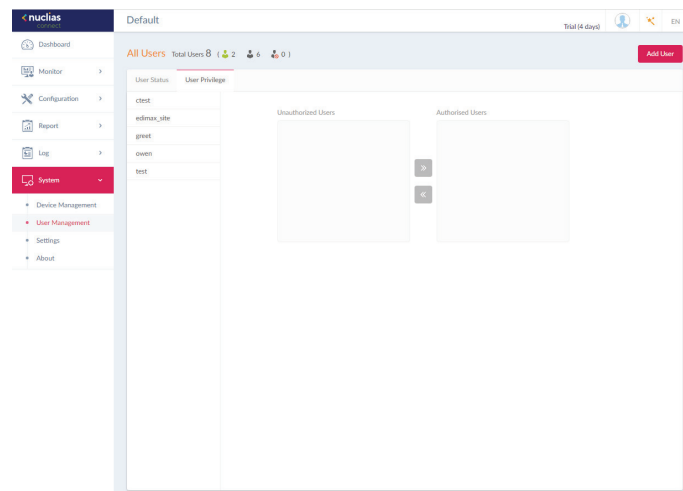
Username	Email	Login Status	Role	Privilege Status	Time of Creation	Last Login Time	Act
admin		●	Root admin	Enable	2018-12-18 12:04:25	2018-12-25 15:25:37	
alpha		●	Root admin	Enable	2018-12-18 12:10:52	2018-12-25 01:54:43	
edimax to ed		●	Root admin	Enable	2018-12-18 12:11:38	2018-12-24 15:16:48	
test		●	Root admin	Enable	2018-12-18 12:12:01	2018-12-25 15:22:02	
nowtest		●	Root admin	Enable	2018-12-18 12:12:23	2018-12-24 15:25:41	
frontdesk		●	Front des...	Enable	2018-12-18 12:12:43	2018-12-19 09:02:50	
fsdesk		●	Front des...	Enable	2018-12-18 13:34:35		
2682-ft		●	Front des...	Enable	2018-12-19 10:09:10	2018-12-19 14:31:25	



The User Privilege function allows administrators to add, view, and authorize/unauthorize users on a selected network. Navigate to **System > User Management** and click on the **User Privilege** 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, click an available site and then the target network. The available users for the network are displayed on the ensuing screen. From the Unauthorized Users column, click the radio box of the target user. Once a user is selected, click **>>** to move to the respective column to authorize the user. The same process is used to unauthorize a user.



The **Settings** page displays General, Connection, SMTP, Backup, Firmware Upgrade, System Operation and Single-Sign-On (SSO) information. 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
<b>Device Name</b>	Enter a description to set the device name.
<b>Logo</b>	Click <b>Browser</b> 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.
<b>Login Captcha</b>	Click the drop-down menu to enable or disable the login Captcha function.

In the **Lan Settings** section, the device connection parameters can be configured. These settings allow the management computer to connect to the device.

Parameter	Description
<b>Get Address From</b>	Click the drop-down menu to choose whether the DNH-100 will get an IP address from a DHCP server or to manually set a static IP address. By default it is set to Static IP Address. <b>Note:</b> DHCP server is not recommended.
<b>IP Address</b>	If the above is set to Static IP address, specify an IP address for the DNH-100.
<b>Subnet Mask</b>	Specify a subnet mask for the device.
<b>Gateway</b>	Specify a gateway mask for the device. (Optional)
<b>Primary DNS</b>	Specify a primary DNS for the device. (Optional)
<b>Secondary DNS</b>	Specify a secondary DNS for the device. (Optional)

In the **Date and Time** section, parameters about the device time and date can be configured. It is recommended that an NTP server is used; log and schedule settings are depending on correct time and date configurations.

Parameter	Description
<b>Time Zone</b>	Click the drop-down menu to select the time zone.
<b>NTP</b>	Check to enable use of NTP server(s) to manage device's date and time.
<b>NTP Server 1</b>	Specify the NTP Server's address.
<b>NTP Server 2</b>	Specify the secondary NTP Server's address.
<b>Copy Your Computer's Time</b>	Click to copy your management computer's time to use here or manually set the time in the text boxes to the left of this button.

## Nuclias

## System

## Settings

## General

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

In the **Console Setting** section, parameters about a console connection to the DNH-100 can be configured:

Parameter	Description
<b>Console</b>	Check to enable management through the console port.
<b>Console Protocol</b>	Choose whether to use Telnet or SSH
<b>Timeout</b>	Click the drop-down menu to select timeout time (in min).

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

Parameter	Description
<b>Live Packet Interval</b>	Click the drop-down menu to select the live packet interval time.

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

The screenshot displays the configuration page for a device, with the 'Settings' menu item highlighted in the left sidebar. The main content area is divided into several sections:

- Customized Setting:** Includes fields for 'Device Name' (set to 'DNH-100'), a 'Login' button with a warning icon, and a 'Login Control' dropdown set to 'Enable'.
- LAN Settings:** Includes fields for 'Static IP Address (Optional)', 'IP Address' (192.168.0.200), 'Subnet Mask' (255.255.255.0), 'Gateway', 'Primary DNS', and 'Secondary DNS'. A checkbox for 'Synchronize Device Access Address' is checked.
- Date And Time:** Includes a 'Time Zone' dropdown (GMT+08:00:00: Asia/Shanghai), a checked 'NTP' checkbox, and fields for 'NTP Server 1' (ntp.aliyun.com) and 'NTP Server 2' (IP address/Domain name).
- Console Setting:** Includes a checked 'Enable' checkbox, radio buttons for 'Serial' and 'SSH', and a 'Timeout' dropdown set to '5 Min'.
- Device Setting:** Includes a 'Live Packet Interval' dropdown set to '5 Min'.

Each section has a red 'Save' button at the bottom.

Nuclias System Settings **Connection**

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

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

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

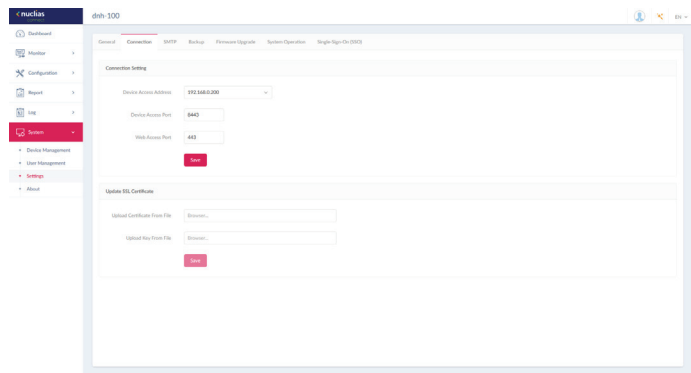
Parameter	Description
<b>Device Access Address</b>	Enter the Nuclias Connect Server application’s IP address. To manage remote APs, the IP address must be a public IP address; IP mapping is required for instances behind a firewall or router.
<b>Device Access Port</b>	Enter the Nuclias Connect server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

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

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

Parameter	Description
<b>Upload Certificate From File</b>	Click <b>Browser...</b> to select the SSL certificate file located on the local drive that will be uploaded.
<b>Upload Key From File</b>	Click <b>Browser...</b> 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.

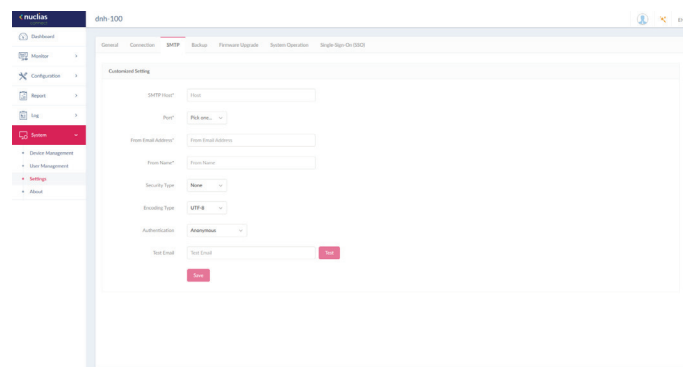


The SMTP tab displays customizable settings for the simple mail transfer protocol (SMTP). This is necessary in order to send emails on behalf of the system such as reset password validation emails.

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

Parameter	Description
<b>SMTP Host</b>	Enter the SMTP server's IP address or domain name.
<b>Port</b>	Enter the SMTP server's port number.
<b>From Email Address</b>	Enter the sender's email address.
<b>From Name</b>	Enter the sender's name.
<b>Security Type</b>	Click the drop-down menu to select the security type to be used in the e-mail system. The options include None or SSL.
<b>Encoding Type</b>	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.
<b>Authentication</b>	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.
<b>Test Email</b>	Enter the recipient e-mail address to initiate a test e-mail through the SMTP configuration. Click <b>Test</b> to start the test function.

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



Nuclias

System

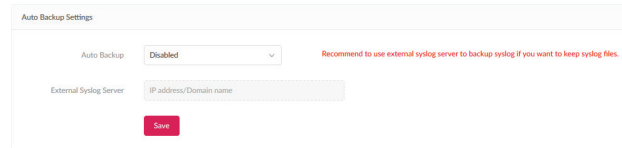
Settings

Backup

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


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


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

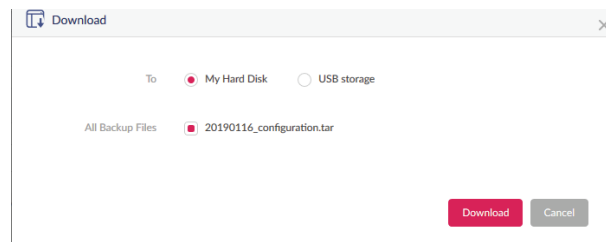


Parameter	Description
<b>Auto Backup</b>	Click on drop-down list to enable or disable auto backup.
<b>External Syslog Server</b>	Enter the external syslog's ip address or domain name.

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


Click  to backup the configuration file or log files.

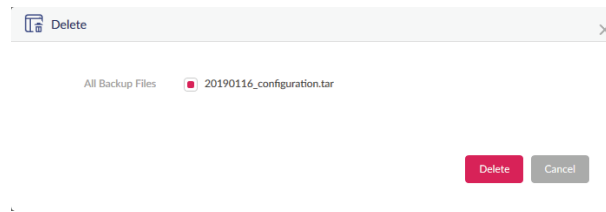
Click  to download the backup file to either the management computer's hard drive or a USB drive.



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

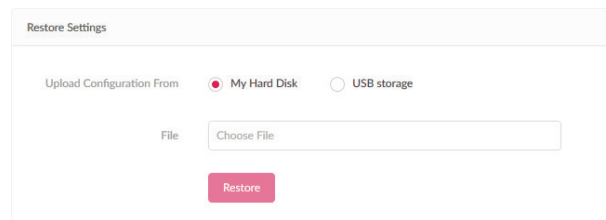
Parameter	Description
<b>To</b>	Choose either My Hard Disk or USB Storage to download your backup file to.
<b>All Backup Files</b>	A list of all backup files that are available to be downloaded will be displayed. Select the radio button of the file you want to download.

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
<b>Upload Configuration From</b>	Choose either My Hard Disk or USB Storage to upload your configuration file.
<b>File</b>	Click on <b>Choose File</b> to select your configuration file's location.

The **Firmware Upgrade** tab displays customizable settings to upgrade the firmware of the DNH-100.

Specify the following parameters and then click **Apply**.

Parameter	Description
<b>Upload Firmware From</b>	Choose either My Hard Disk, USB Storage or FTP Server to upload your firmware file.
<b>File</b>	Click on <b>Choose File</b> to select your configuration file's location. (Only available if My Hard Disk or USB Storage is chosen.)
<b>FTP Server</b>	Specify IP address or domain name of FTP server.
<b>Port</b>	Specify port number of FTP server.
<b>Username</b>	Specify username.
<b>Password</b>	Specify password.
<b>Firmware File</b>	Specify the path and filename on the FTP server where the firmware file is located.

The screenshot shows the Nuclias Connect web interface for a DNH-100 device. The left sidebar contains navigation options: Dashboard, Monitor, Configuration, Report, Log, System (highlighted), Device Management, User Management, Settings, and About. The main content area has tabs for General, Connection, SMTP, Backup, Firmware Upgrade (selected), System Operation, and Single-Sign-On (SSO). The Firmware Upgrade form includes the following fields:

- Upload Firmware From: My Hard Disk (dropdown menu)
- File: Browser... (text input)
- FTP Server: (text input)
- Port: 21 (text input)
- Username: (text input)
- Password: (text input with eye icon)
- Firmware File: Path and file name (text input)

An Apply button is located at the bottom of the form.

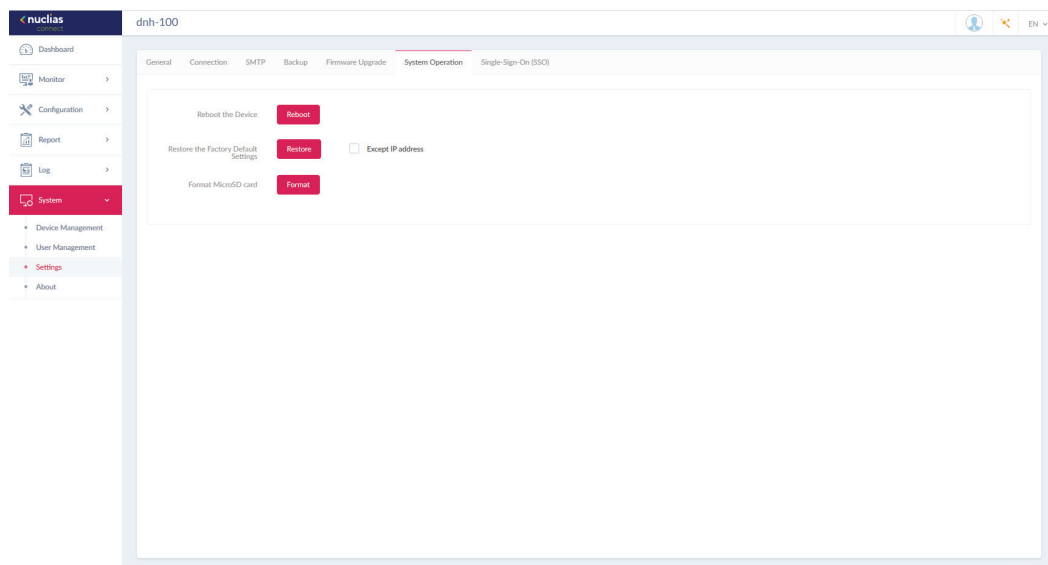


The **System Operation** tab allows you the option to reboot, restore to factory default settings, or format the MicroSD card in the DNH-100.

Click **Reboot** to Reboot the DNH-100 immediately.

Click **Restore** to restore the DNH-100 to factory default settings. If **Except IP address** is checked, then the device IP address will remain the same.

Click **Format** to format the MicroSD card. Please be aware that you will lose all information on the MicroSD card once you proceed.



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 on **Create account** where a browser window will open to a link where you can create one.

There are three steps in the registration process.

Step 1: Selecting 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 1  
Select server region and country.

**nuclias**  
by D-Link

Your new account and organization will be created on servers within the region selected. The customer service will be forwarded to the country you selected.

Server region

Country

Next

Already have an account? [Log In](#)

Step 2: Create organization and site.

Once the region and country have been entered, you will see the the user, organization, and site page. 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 2  
Create your user, organization and site.

**nuclias**  
by D-Link

D-Link

D-Link Test

Taiwan

Asia/Taipei (UTC+08:00, DST)

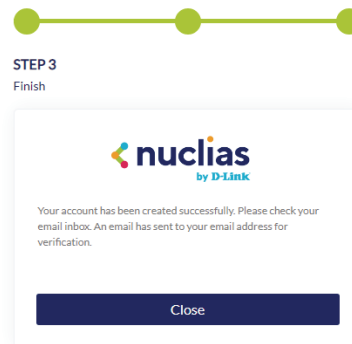
No.1 Street Name, City Name, State, Country, ZIP

I have read and agree to the [Terms of use](#) and [Privacy](#)

Create account

Step 3: Finish the registration.

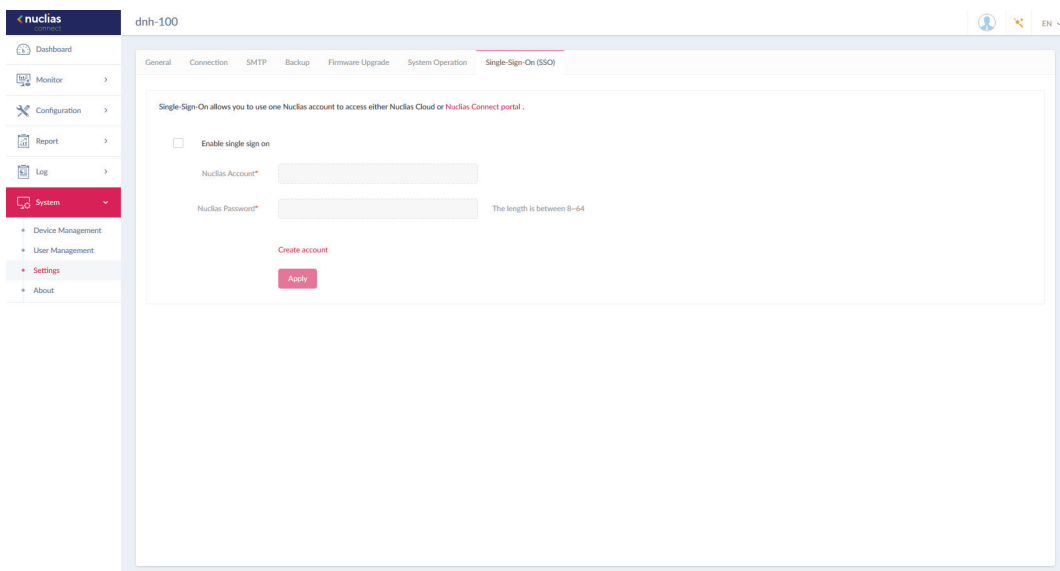
Click Close to complete the process. The registered account is now available for use. The verification information will be delivered to the registered email of the account.



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
<b>Enable single sign on</b>	Check to enable single-sign-on.
<b>Nuclias Account</b>	Enter your Nuclias Account username.
<b>Nuclias Password</b>	Enter your Nuclias Account password.



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

Requirements for use include:

- A Nuclias account
- DNH-100 device(s) with single-sign-on enabled

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

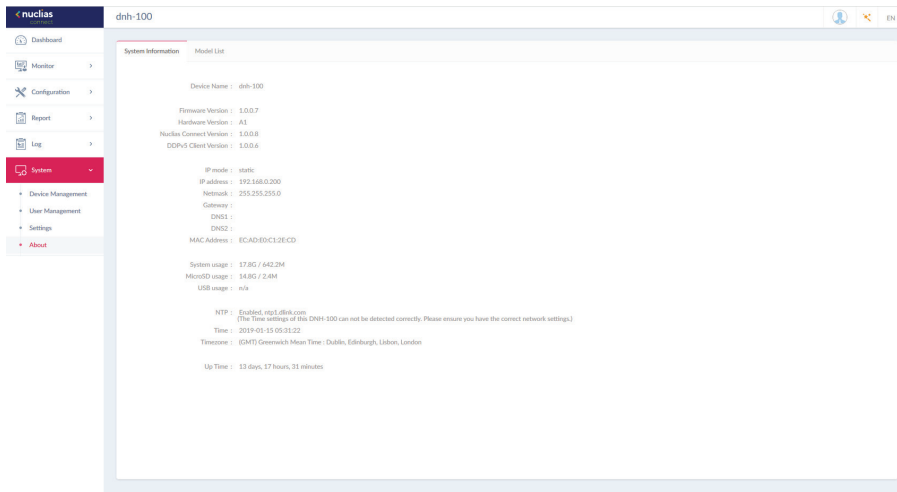


The Portal provides the following information:

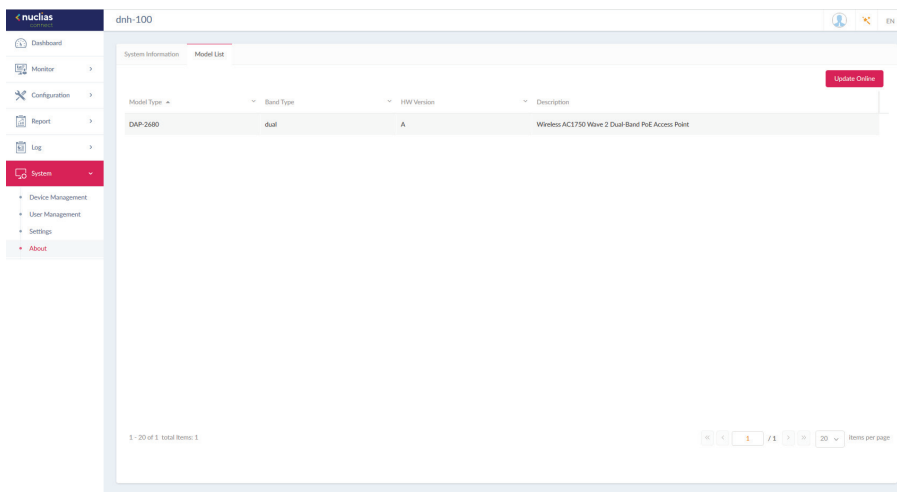
Parameter	Description
<b>Number</b>	Number of the DNH-100 on the list.
<b>Status</b>	Displays whether or not the Nuclias Connect portal can link to that DNH-100.
<b>Name</b>	Name of the Nuclias Connect Hub. You can change this name by clicking on it then typing on the available text box.
<b>Host</b>	Displays both the device IP address and its public IP address.
<b>Sites</b>	Number of sites managed by that DNH-100.
<b>Networks</b>	Number of networks managed by that DNH-100.
<b>Devices</b>	Number of devices managed by that DNH-100.
<b>Clients</b>	Number of clients connected to devices managed by that DNH-100.
<b>Version</b>	Firmware version number of that DNH-100.
<b>Actions</b>	Click <b>Launch</b> to open the DNH-100 Nuclias Connect interface. Please note that IP mapping is required for instances behind a firewall or router. Click <b>Forget</b> to unlink this DNH-100 from the Nuclias Connect portal. ( <b>Forget</b> is only available when that device is offline.)

The About page displays system information about the DNH-100 and a list of supported access points.

Navigate to **System > About**. By default you will see the System Information tab where information about the DNH-100 will be displayed.



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



# Appendix

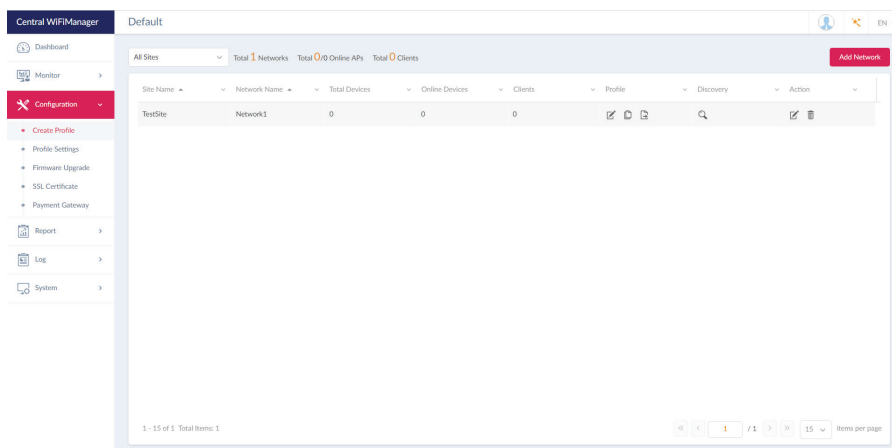
## Nuclias Connect App

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.

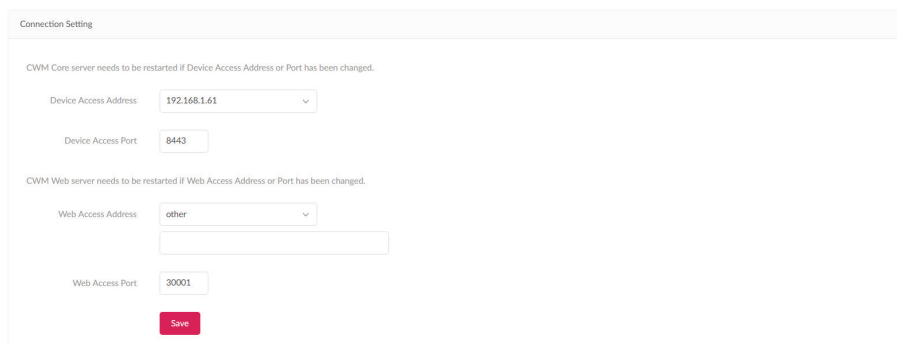
This section provides information on exporting the required network profiles from the Nuclias server for managing connected DAPs. Additional information explaining the functionality of the Nuclias Connect App is also included.

### 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 Nuclias Connect’s IP address, go to **System > Settings > Connection** and check the **Device Access Address** field.



# Nuclias Connect App

## Discover and Configure APs Using the Nuclias Connect 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 the 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.

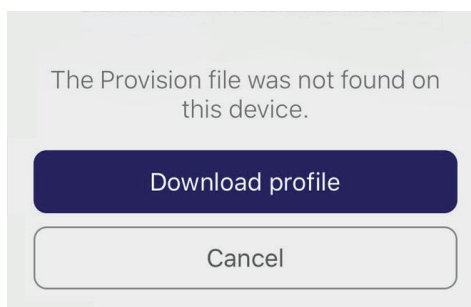
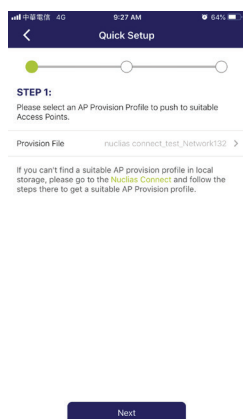


The next step is to select an AP provision profile. The profile is used to push to the selected DAPs. Tap **Quick Setup** to begin the deployment of a standalone DAP to the Nuclias Connect server.

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.

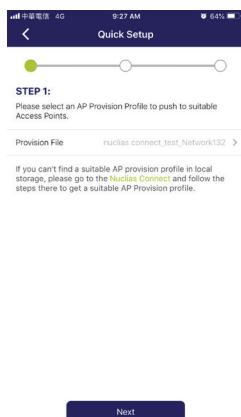
Tap **Download profile** in order to specify a connection to the Nuclias Connect controller.



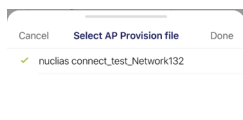
# Nuclias Connect App

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.



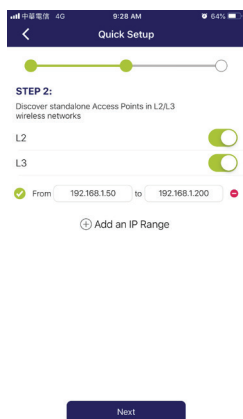
The process will continue and the App will return to the previous screen. From the Step 1 page, tap **Next** to continue.

From this page, you can discover standalone DAPs 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 (+) 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.



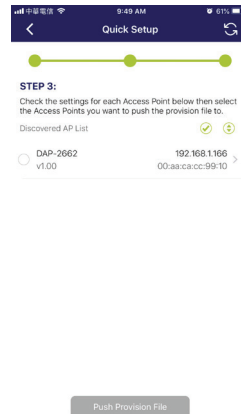


## Nuclias Connect App

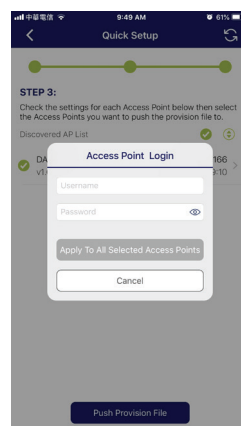
After the scanning the network range, the Step 3 page will list any detected access points.

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

Tap **Push Provision File** to continue.



The DAP 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 DAP.



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.

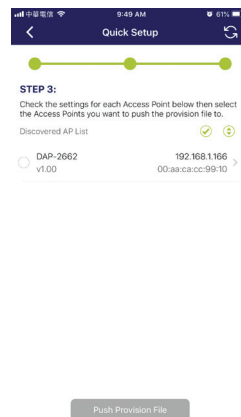
Parameter	Description
<b>Cancel</b>	Tap to discard any changes and continue the process.
<b>Done</b>	Tap to accept any changes and continue the process.
<b>Model Name</b>	Displays the model name for the listed DAP device.
<b>MAC</b>	Displays the MAC address of the listed DAP device.

## Nuclias Connect App

Parameter	Description
<b>DHCP Mode</b>	Tap to enable or disable the DHCP mode function. When enabled, the DAP establishes dynamic IP address settings with any authorized client connections.
<b>IP Address</b>	Tap to designate an IP gateway setting.
<b>Subnet Mask</b>	Tap to designate a subnet mask.
<b>Default Gateway</b>	Tap to designate a default gateway setting.
<b>DNS</b>	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 App

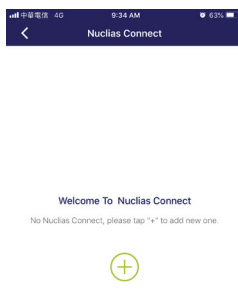
## **Nuclias Connect**

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.



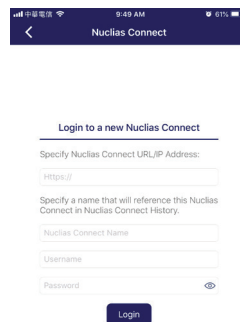
The following page lists the information required to log in to a designated Nuclias Connect controller. Enter the required information in each field.

Parameter	Description
<b>Specify NucliasConnect URL/IP Address</b>	Enter the secure URL/IP address of the Nuclias Connect server to pair with the App.
<b>Specify a reference name</b>	Enter a specific name to easily identify the paired Nuclias Connect server.

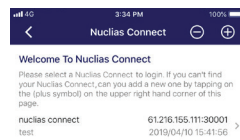
## Nuclias Connect App

Parameter	Description
<b>User name</b>	Enter a user name with the authority to access the Nuclias Connect controller.
<b>Password</b>	Enter the password for the referenced user name with the authority to access the Nuclias Connect server.
<b>Login</b>	Tap Login to initiate the login process.

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



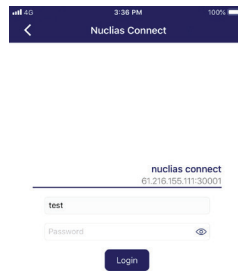
After a successful login, the pairing will be added to the listing and will be available for future login selection.



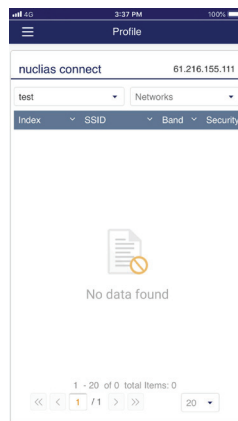
Tap on a **Nuclias Connect** server from the list.

## Nuclias Connect App

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.

# Nuclias Connect App

## Standalone Access Point

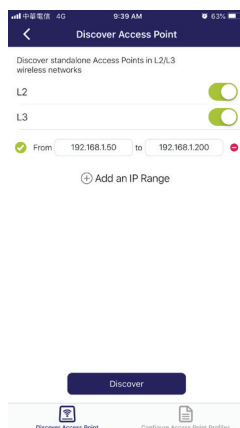
### Discover DAPs

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

From this page, you can discover standalone DAPs 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.



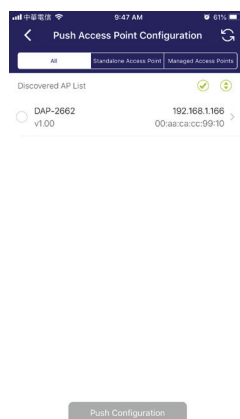
Once the range is defined, tap **Next** to initiate the discovery process.

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.

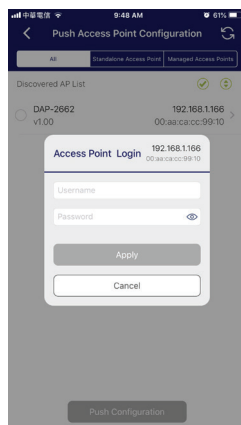
Tap the radio button next to the DAP to select it. The selected local provision file will be pushed to the selected DAP.

Tap **Push Provision File** to continue.



# Nuclias Connect App

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 DAP. Tap **Apply** to continue.



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

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



# Nuclias Connect App

The Wireless settings menu is listed in the following figure.

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

