

NUCLIAS CONNECT DNH-100 User Manual

V 1.10

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
Floor Plan.....	17
Configuration.....	19
Create Profile.....	19
Profile Settings.....	22
Firmware Upgrade.....	40
SSL Certificate.....	41
Payment Gateway.....	42
Report.....	43
Peak Network Activity.....	43
Most Active AP.....	44
Hourly Network Activity.....	45
Daily Network Activity.....	46
Log.....	47
Device Syslog.....	47
System Event Log.....	48
Device Log.....	49
Audit Log.....	50
Alerts.....	51
System.....	52
Device Management.....	52
User Management.....	53
Settings.....	55
Resources.....	67
About.....	68
Appendix	69
Nuclias Connect App.....	69

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

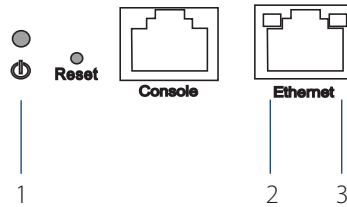
- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet Adapter
- Microsoft Edge, Safari 7, Firefox 28, or Google Chrome 33 and above (for configuration)

Hardware Overview

LED Indicators

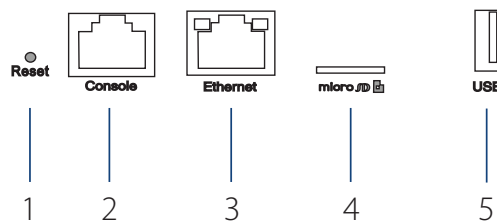
Interface Connectors

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 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 ^{1,2,3} up to 32 GB.
5	USB Port	USB 3.0 Type A port ² (provides 5V/1A power for optional HDD connection).

¹ Due to EU regulations the 16 GB MicroSD card is only included in the WW version.

² Only FAT32 format is supported.

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

Installation

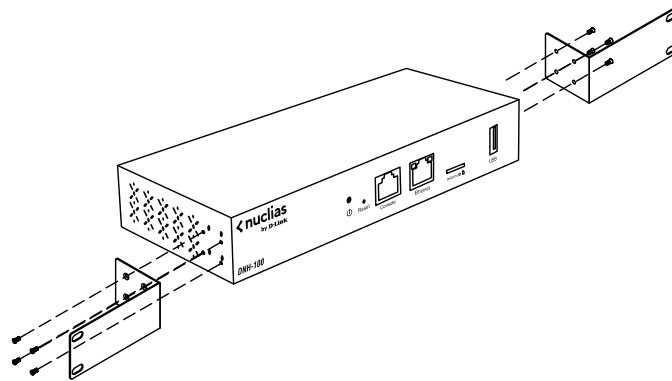
Mounting

Connecting the Controller

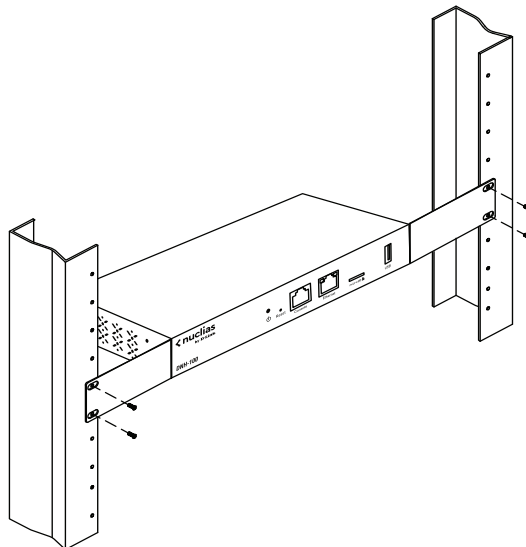
Mounting

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.



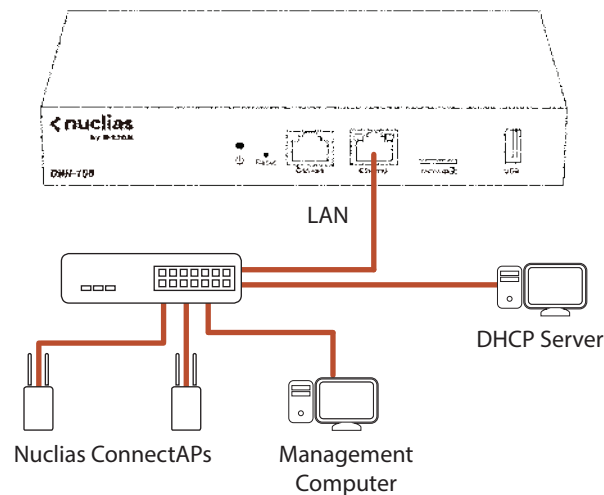
2. Mount the device in the rack using a screwdriver and the supplied rack-mounting screws.



Mounting

Connecting the Controller

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.

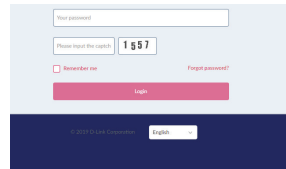
Basic Configuration

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.



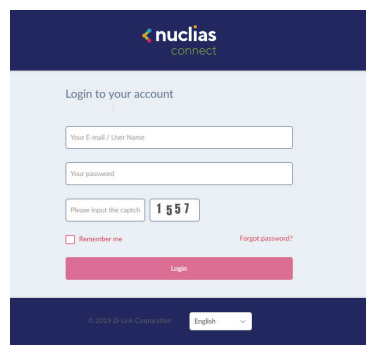
The screenshot shows a login form with the following elements: a text input for 'Your password', a captcha input with the code '1 5 5 7', a checkbox for 'Remember me', a link for 'Forgot password?', and a red 'Login' button. At the bottom, there is a footer with '© 2017 D-LAN Corporation' and a language dropdown menu set to 'English'.

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

Enter the Captcha code as shown on screen.

NOTE:

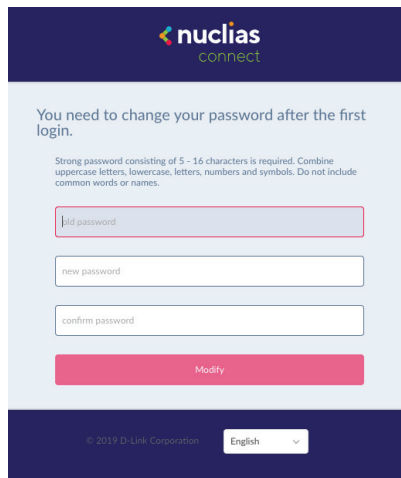
- The **Remember me** function can be selected to save the password entry for future use.
- The **Forgot password?** function provides an option to reset your password in the event that you've forgotten your current password. To use this function, the smtp server and email address must be configured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



The screenshot shows a login form with the following elements: a header with the 'nuclias connect' logo, a sub-header 'Login to your account', a text input for 'Your E-mail / User Name', a text input for 'Your password', a captcha input with the code '1 5 5 7', a checkbox for 'Remember me', a link for 'Forgot password?', and a red 'Login' button. At the bottom, there is a footer with '© 2017 D-LAN Corporation' and a language dropdown menu set to 'English'.

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, there is a dark blue header with the 'nuclias connect' logo. Below the header, the text reads: 'You need to change your password after the first login.' Underneath, a note states: '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 dark blue footer containing the 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
Get Address From	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. Note: DHCP server is not recommended.
IP Address	If the above is set to Static IP address, specify an IP address for the DNH-100.
Subnet Mask	Specify a subnet mask for the device.
Gateway	Specify a gateway mask for the device. (Optional)
Primary DNS	Specify a primary DNS for the device. (Optional)
Secondary DNS	Specify a secondary DNS for the device. (Optional)
Synchronize Device Access Address	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.

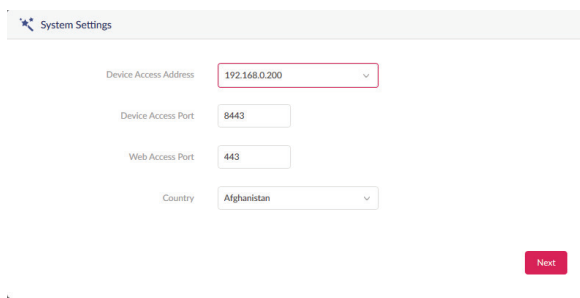
Parameter	Description
Time Zone	Click the drop-down menu to select the time zone.
NTP	Check to enable use of NTP server(s) to manage device's date and time.
NTP Server 1	Specify the NTP Server's address.
NTP Server 2	Specify the secondary NTP Server's address.

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

Click **Next** to continue

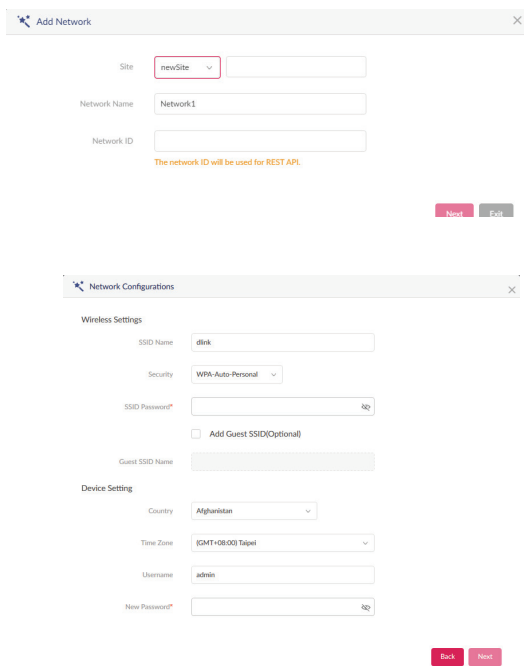


The screenshot shows the 'System Settings' window. It contains four input fields: 'Device Access Address' with a dropdown menu showing '192.168.0.200', 'Device Access Port' with a text box containing '8443', 'Web Access Port' with a text box containing '443', and 'Country' with a dropdown menu showing 'Afghanistan'. A red 'Next' button is located at the bottom right of the form.

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

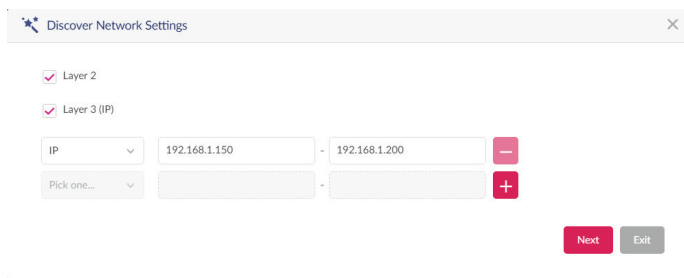
In the Network Name field, enter the name in which to identify the new network. The Network ID is an optional field. It will be used on REST API function, leave it as empty if not using REST API. Click **Next** to continue or **Exit** to return to the previous screen.

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



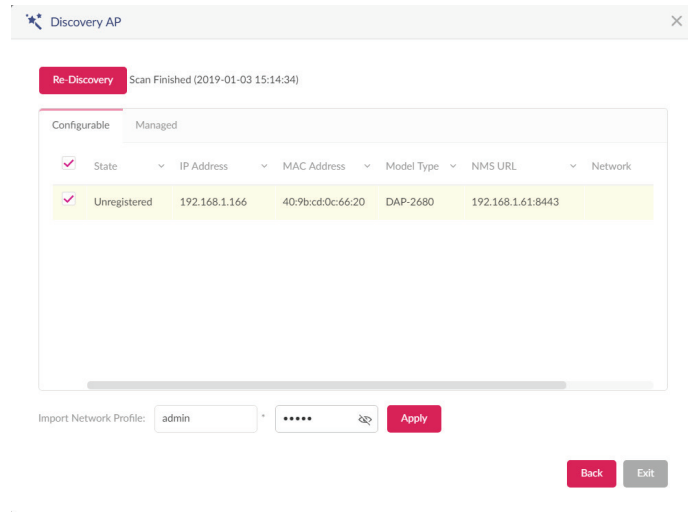
The screenshot shows two stacked forms. The top form is 'Add Network' with fields for 'Site' (dropdown with 'newSite'), 'Network Name' (text box with 'Network1'), and 'Network ID' (text box). A note below the Network ID field says 'The network ID will be used for REST API'. The bottom form is 'Network Configurations' with sections for 'Wireless Settings' (SSID Name: 'dlink', Security: 'WPA-Auto-Personal', SSID Password, Add Guest SSID checkbox, Guest SSID Name) and 'Device Setting' (Country: 'Afghanistan', Time Zone: 'GMT+08:00 Taipei', Username: 'admin', New Password). Both forms have 'Next' and 'Exit' buttons at the bottom right.

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. It has two checked radio buttons: 'Layer 2' and 'Layer 3 (IP)'. Below them are two rows of input fields. The first row has a dropdown for 'IP', a text box with '192.168.1.150', a text box with '192.168.1.200', and a minus sign button. The second row has a dropdown for 'Pick one...', an empty text box, another empty text box, and a plus sign button. 'Next' and 'Exit' buttons are at the bottom right.

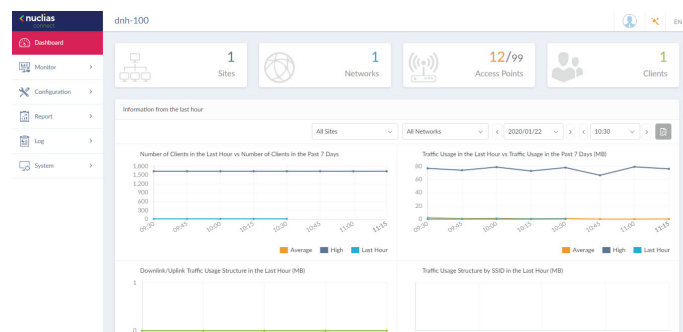
The Start Discovery Page will appear. Click **Start Discovery** to list all available unmanaged devices. If a device is found, select it and click **Apply** to import the network profile. Click on the Managed tab to select already defined devices and add them to this network.



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.

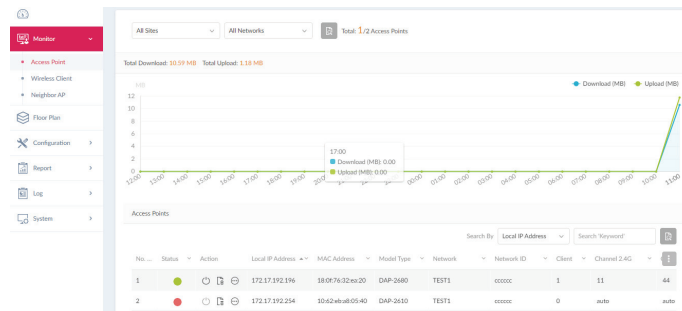
Block	Description
Sites	Displays the number of created profiles, also called sites.
Networks	Displays the total number of created networks.
Access Points	Displays the total number of available and online access points.
Clients	Displays the total number of wireless clients connected to the network.
Information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

No.	Action	IP Address	MAC Address	Auth Type	Channel	RSSI (dBm)	Band	SSID
1		169.254.225.82	54:9f:13:0e:1c:b7	Disabled	11	-61	2.4GHz	dlink

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

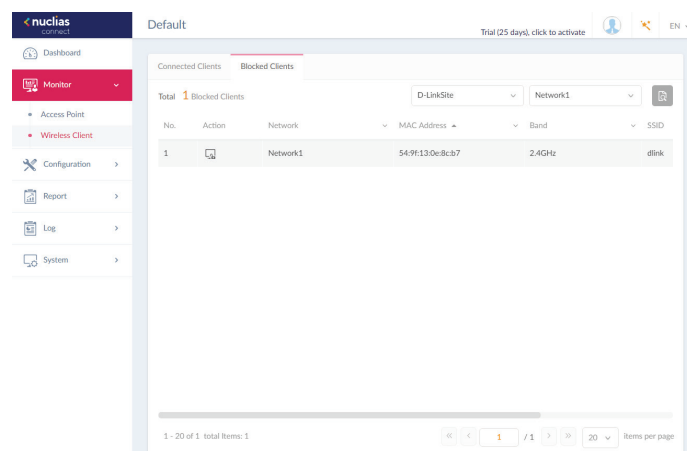
Click on **Blocked Clients**. In this frame, you can view a report of all blocked clients detected. This report can be generated by specifying **Site** and **Network** criteria.


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

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

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

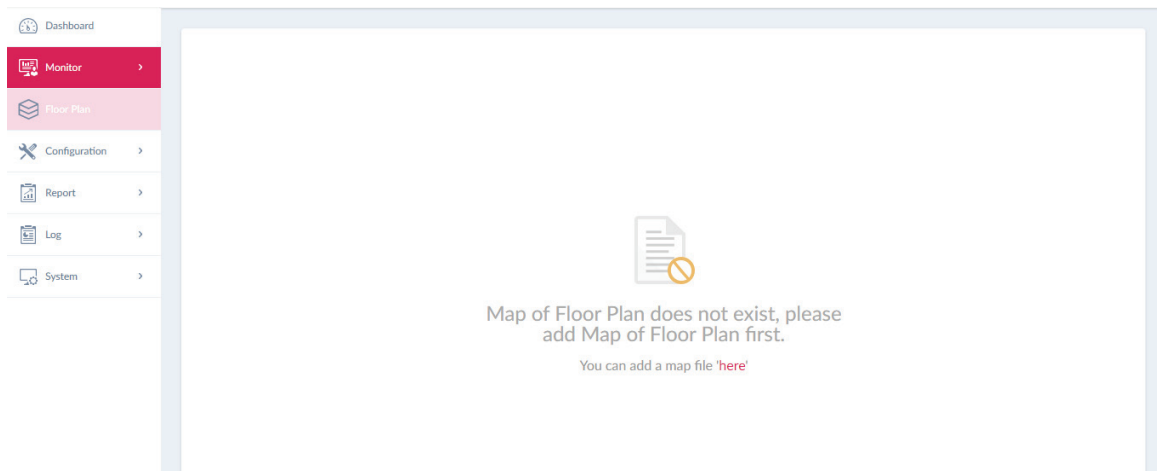
1 - 20 of 50 total items: 50

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

Nuclias

Floor Plan

Floor plan shows a birds'-eye view of the relationship between spaces and rooms, providing traffic patterns and other physical features of a structure on a single floor. Click **"Here"** to add a new floor image, enter the name and select Site and Network.




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

Name*

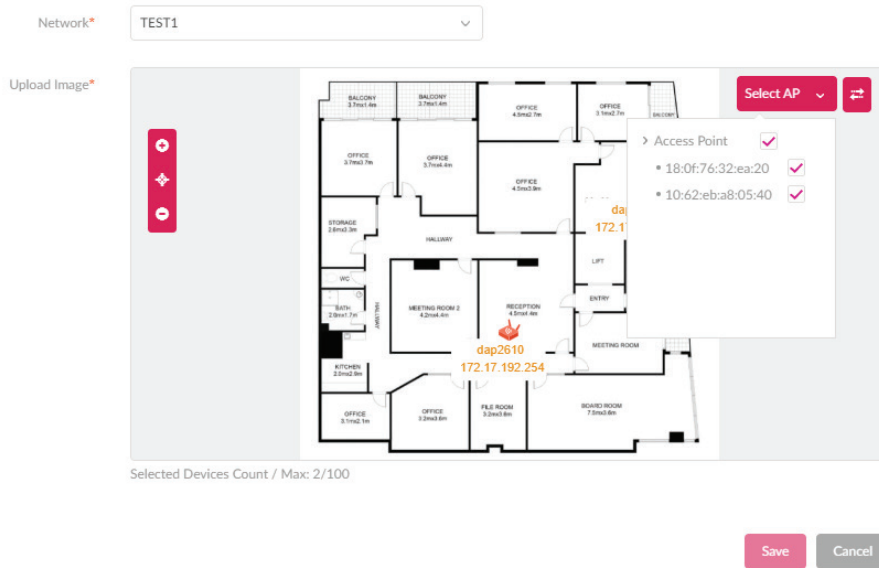
Site*

Network*

Upload Image*


Drag & Drop
Your Picture Here (file format is *.png,*.jpg, size is up to 10M)
or
Click to **choose a picture**

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

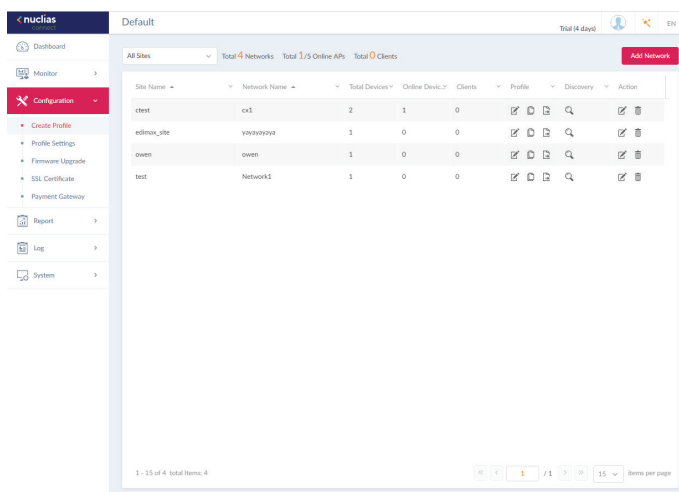


Connection status(Green: Online, Red: Offline) of the device as well as information such as name, model type, IP address, etc... can be seen when hovering the mouse over to the device icon.

Nuclias Configuration **Create Profile**

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

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. The Network ID is an optional field. It will be used on REST API function, leave it as empty if not using REST API. Click **Next** to continue or **Exit** to return to the previous screen.

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

The image shows two screenshots of a web configuration interface. The top screenshot is titled 'Add Network' and contains the following fields: 'Site' (a dropdown menu with 'newSite' selected and an adjacent empty text input), 'Network Name' (a text input containing 'Network1'), and 'Network ID' (an empty text input). Below the 'Network ID' field is a small orange note: 'The network ID will be used for REST API.' The bottom screenshot is titled 'Network Configurations' and is divided into two sections: 'Wireless Settings' and 'Device Setting'. Under 'Wireless Settings', there are fields for 'SSID Name' (containing 'dlink'), 'Security' (a dropdown menu with 'WPA-Auto-Personal' selected), 'SSID Password*' (an empty password field with a visibility icon), and a checkbox for 'Add Guest SSID(Optional)'. Below this is a 'Guest SSID Name' field. Under 'Device Setting', there are fields for 'Country' (a dropdown menu with 'Taiwan' selected), 'Time Zone' (a dropdown menu with '(GMT+08:00) Taipei' selected), 'Username' (containing 'admin'), and 'Password' (an empty password field with a visibility icon). At the bottom right of the 'Network Configurations' form are three buttons: 'Back' (red), 'Next' (pink), and 'Exit' (grey).

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.

State	IP Address	MAC Address	Model Type	NMS URL	Network
Unregistered	192.168.1.166	40:9b:cdd:0c:66:20	DAP-2680	192.168.1.61:8443	

Nuclias Configuration Profile Settings

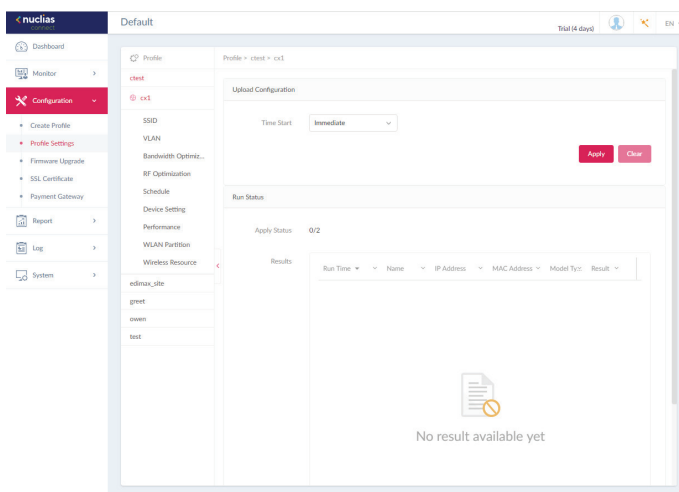
The **Profile Settings** function allows for the management of existing networks. Navigate to **Configuration > Profile Settings** to view existing sites. Select a site followed by an available network to view all settings that are available for editing: **SSID, VLAN, Bandwidth Optimization, RF Optimization,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



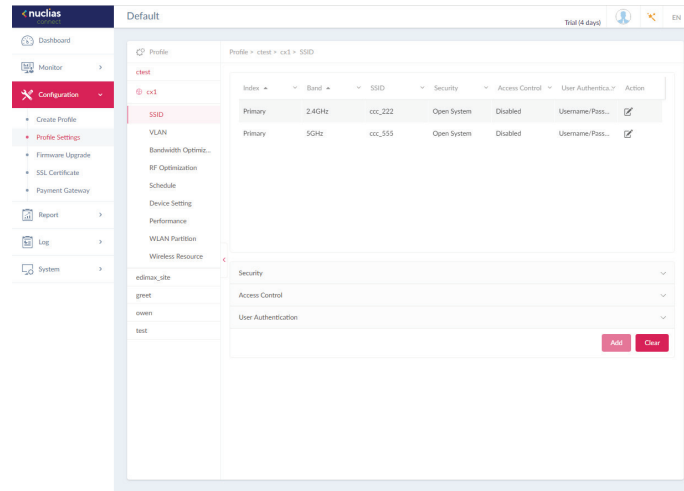
The SSID page displays the configurable parameters of a network's wireless settings. Navigate to **Configuration > Profile Settings > [Site] > [Network] > SSID** to view existing settings.

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

Block	Description
Band	Click the drop-down menu to select wireless frequency band.
Index	Click the drop-down menu to select SSID index (Parameters: Primary, SSID 1 to SSID 7). To create a new SSID, select the index parameter first.
SSID	Enter the wireless network name. The SSID must be the same across all frequencies. In addition, make sure the network name (SSID) on the selected access point is the same as the defined network name (SSID) on the Nuclias 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.
Character Set	Click the drop-down menu to select the character set to be used in the SSID encoding: UTF-8 or GB2312.
SSID Broadcast	Click the drop-down menu to enable or disable the wireless SSID visibility.
WMM (Wi-Fi Multimedia)	Click the drop-down menu to enable or disable the Wi-Fi multimedia.
Security	Click the drop-down menu to select the wireless security protocol: Open System (no pre-shared key required), WPA-Personal, WPA Enterprise (Radius server required), WPA2-Personal, WPA2-Enterprise (Radius server required), WPA-Auto-Personal, WPA-Auto-Enterprise (Radius server required).
Fast Roaming	Click the drop-down menu to enable or disable fast roaming. This function is only available for compatible models and specific software version.
Encryption	Click the drop-down menu to enable or disable WEP Open System encryption. The function is only available when Security is set as Open System .
Key Size	Click the drop-down menu to select the WEP key size.
Key Type	Click the drop-down menu to select the WEP key type.
Key Index	Click the drop-down menu to select the WEP key index.
Key Value	Enter the open system WEP encryption key.
Encryption Type	Click the drop-down menu to select the encryption type: Auto, AES, or TKIP.
Group Key Update Interval	Enter the WPA group key update interval value.
Passphrase	Enter the secret pass phrase used. The function is only available when Security is WPA-Personal , WPA2-Personal or WPA-Auto-Personal .
RADIUS Server	Enter the RADIUS server's IP address. The function is only available when Security is WPA-Enterprise , WPA2-Enterprise or WPA-Auto-Enterprise .

Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 22 for further information.

Nuclias Configuration Profile Settings SSID



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



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

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

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

Block	Description
Authentication Type	Click the drop-down menu to select the authentication type applied to the wireless client. (Web redirection only. User name/Password, Remote Radius, LDAP, POP3, Passcode, External Captive Portal, MAC address, Click through and Social Login)
Idle Timeout (2~1440)	Enter the session timeout value.

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

Block	Description
Identity	Enter the name of the administrator. This function is only available when Authentication Type is LDAP .
Server	Enter the POP3 server's IP address. This function is only available when Authentication Type is POP3 .
Port	Enter the POP3 server's port number. This function is only available when Authentication Type is POP3 .
Connection Type	Click the drop-down menu to select the connection type. This function is only available when Authentication Type is POP3 .
Passcode List	Display the configured front desk user accounts that have been assigned to this network and have already generated a passcode from the Web login page. This function is only available when Authentication Type is Passcode .
External Captive Portal	Click the drop-down menu to select HTTP or HTTPS. After selecting, enter the URL of the website. This function is only available when Authentication Type is External Captive Portal .
Web Redirection	Check the box to enable the website redirection function.
Website	Click the drop-down menu to select HTTP or HTTPS. After selecting, enter the URL of the website.
Choose Template	Click the drop-down menu to select the used login style. This function is only not available when Authentication Type is Web Redirection Only . Note: <ul style="list-style-type: none"> Click Preview to preview the selected style. Click Upload Login File to upload a new style. Click  to delete the selected style. Click  to download the style template.

In the **Hotspot 2.0** section, the following parameters can be configured: Please note that Hotspot 2.0 is only available for compatible models and specific firmware version.⁵

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

⁵ Currently only DAP-2662 and DAP-3666 supports this function.

ASRA	Choose enable if the network has Additional Steps required for Access.
ESR	Choose enable to indicate that emergency services are reachable through this device.
USEA	Choose to enable or disable USEA.
Venue Group	Specify group venue belongs to.
Venue Type	Specify type of venue.
Venue Name	Specify name of venue. Choose from the drop down list a language used in the name.
HESSID	Specify a homogenous extended service set (ESS) ID that can be used to identify a specific service provider network.
WAN Link Status	Set information about the status of the Access Point's WAN connection from the drop-down menu.
WAN Symmetric Link	Specify state of the WAN link is symmetric (upload and download speeds are the same).
WAN At Capacity	Specify yes if the Access Point or the network is at its max capacity, or specify no if not.
WAN Metrics DL Speed (kps)	The downlink speed of the WAN connection set in kbps. If the downlink speed is not known, set to 0.
WAN Metrics UL Speed (kps)	The uplink speed of the WAN connection set in kbps. If the uplink speed is not known set to 0.
Network Auth Type	Choose from drop-down menu the network authentication type and specify the web-address.
IP Address Type Availability	Choose from drop-down menu the IP address version and type that the Hotspot Operator uses and that would be allocated and available to a mobile device after it authenticates to the network. Click Delete icon to delete it from the list.
Domain Name	List one or more domain names for the entity operating the AP.
Roaming Consortium	Add service providers or groups of roaming partners whose security credentials can be used to connect to a network. Click Delete icon to delete it from the list.
Nai Realm	Specify list of all NAI realms available through the BSS. Click subtract icon to delete it from the list.
EAP Method	Specify one or more EAP methods and its authentication ID and Parameter type. Click Delete icon to delete it from the list.
RFC 4282	Click on drop-down menu to enable or disable RFC 4282.
3gpp Cellular Network	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.
Connection Capability	Specify a list of common IP protocols (TCP, UDP, IPsec) and ports (21, 80, 443, 5060), specify its port number and the status of the IP protocol and click Add. Click Delete icon to delete it from the list.
Operator Friendly Name	Identifies the Hotspot venue operator and choose its language.
OSU SSID	Specify OSU SSID name.
OSU Server URI	Specify OSU Server URI
OSU Method	Specify a list of OSU methods by choosing its language and then specifying a method by clicking Add. Click Delete icon to delete it from the list.
OSU Config	Choose from drop-down menu the OSU Configu.
OSU Language Code	Choose a language from the drop-down menu.

OSU Friendly Name	Choose a language from the drop-down menu and specify the OSU friendly name.
OSU Nai	Specify the OSU NAI.
OSU Service Description	Specify a service description for the OSU.
OSU Icon Language Code	Specify from drop-down menu the language of the icon.
OSU Icon File Path	Specify location of icon file.
OSU Icon File Name	Specify icon file name.
OSU Icon Width	Specify width of the icon, in pixels.
OSU Icon Height	Specify length of the icon, in pixels.
OSU Icon Type	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.


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

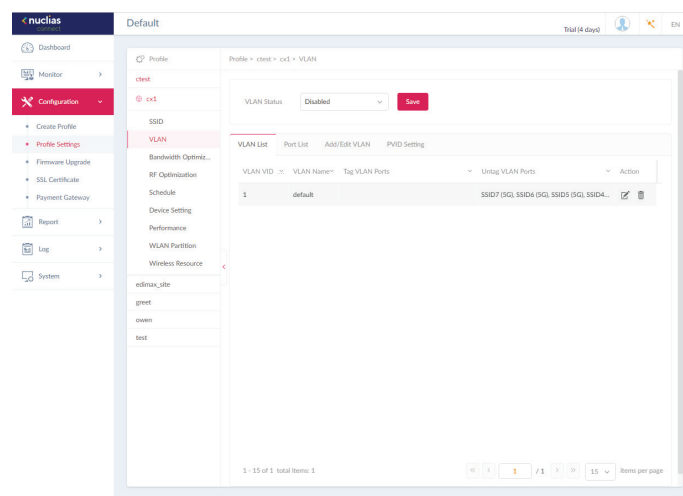
Block	Description
VLAN Status	Click the drop-down menu to enable or disable VLANs.

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

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

Click  to modify an existing VLAN.

Click  to remove an existing VLAN.



In the **Port List** tab, a list of port assignments 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.

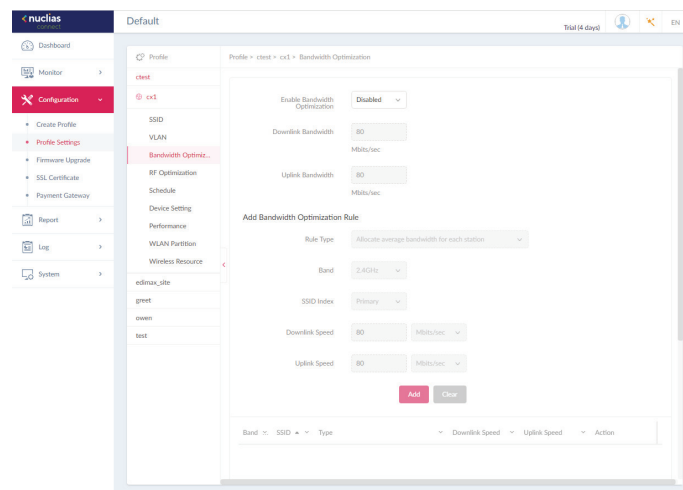
Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 22 for further information.

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
Enable Bandwidth Optimization	Click the drop-down menu to enable or disable the bandwidth optimization function.
Downlink Bandwidth	Enter the total downlink bandwidth speed for the access points in the network.
Uplink Bandwidth	Enter the total uplink bandwidth speed for the access points in the network.
Rule Type	Click the drop-down menu to select the rule type. <ul style="list-style-type: none"> • Allocate an average BW for each station: Optimize bandwidth by averaging the allocated bandwidth for each client. • Allocate a maximum BW for each station: Specify the maximum bandwidth for each connected client, while reserving available bandwidth for additional clients. • Allocate a different BW for 11a/b/g/n station: The weight of 802.11b/g/n and 802.11a/n clients are 10%/20%/70% and 20%/80%. The AP will distribute different bandwidth for 802.11a/b/g/n clients. • Allocate a specific BW for SSID: All clients share the assigned bandwidth.
Band	Click the drop-down menu to select the wireless frequency band used in the rule.
SSID Index	Click the drop-down menu to select the SSID used in the rule.
Downlink Speed	Enter the downlink speed assigned to either each station or the specified SSID.
Uplink Speed	Enter the uplink speed assigned to either each station or the specified SSID.
Add	Click Add to add the rule into the Bandwidth Optimization Rules.
Clear	Click Clear to clear the entered rule.

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



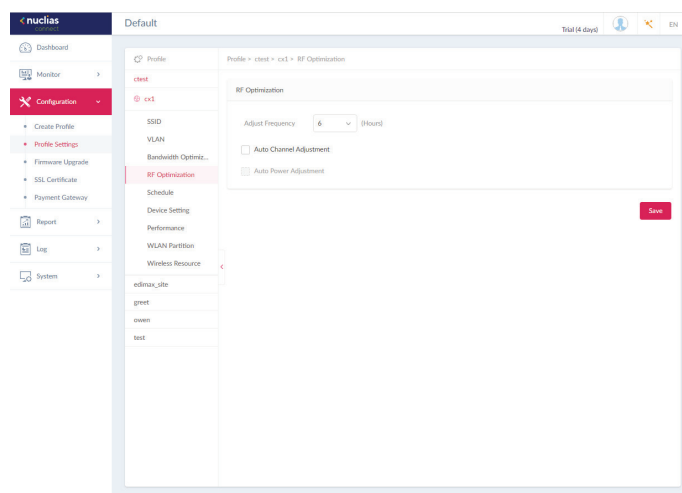
Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 22 for further information.

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

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



Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 22 for further information.

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.

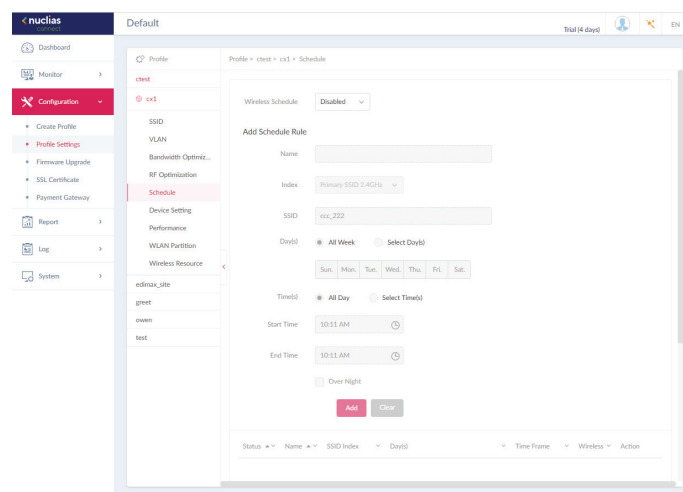
Parameter	Description
Wireless Schedule	Click the drop-down menu to enable or disable the wireless schedule function.
Name	Enter the name of the schedule rule.
Index	Click the drop-down menu to select SSID on which the schedule setting is applied.
SSID	Display the SSID name.
Day(s)	Click the radio button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

Click  to modify the desired rule.

Click  to delete the desired rule.

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

Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 22 for further information.



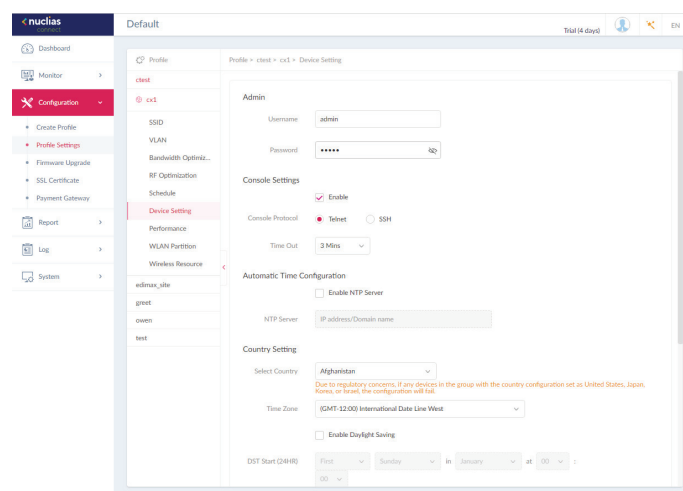
Nuclias Configuration Profile Settings **Device Setting**

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

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

Once the settings are updated, the configuration must be uploaded to the related access points. See "Profile Settings" on page 22 for further information.

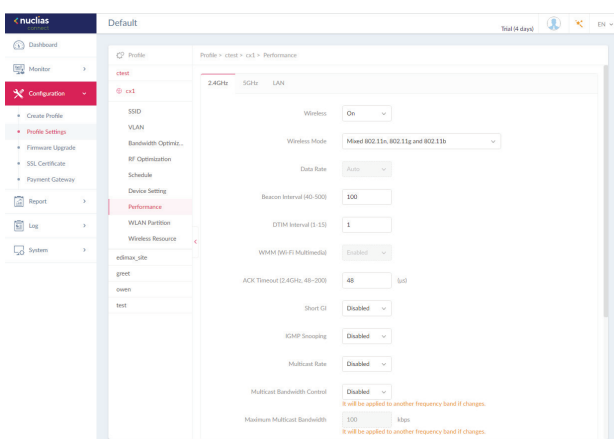


Nuclias Configuration Profile Settings **Performance 2.4GHz/5GHz**

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

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



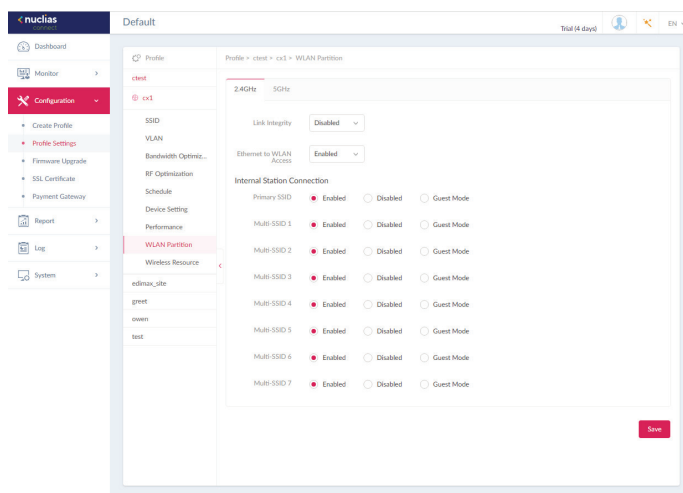
Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 22 for further information.

Nuclias Configuration Profile Settings WLAN Partition
2.4GHz/5GHz-1/5GHz-2

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

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



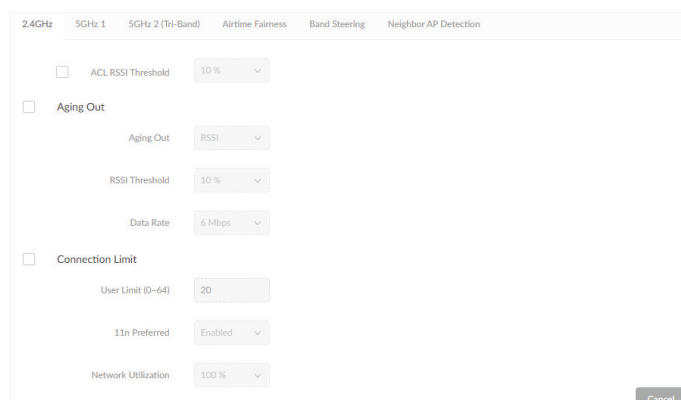
Once the settings are updated, the configuration must be uploaded to the related access points. See "Profile Settings" on page 22 for further information.

Nuclias Configuration Profile Settings Wireless Resource
2.4GHz/5GHz-1/5GHz-2

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

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



Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 22 for further information.

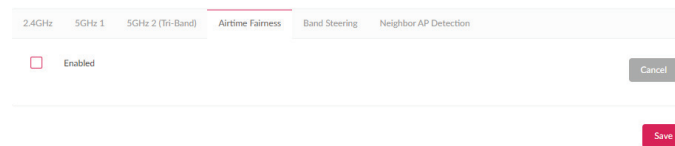
Nuclias Configuration Profile Settings Wireless Resource**Airtime Fairness**

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.



The screenshot shows a configuration interface for 'Airtime Fairness'. At the top, there is a horizontal menu with tabs: '2.4GHz', '5GHz 1', '5GHz 2 (Tri-Band)', 'Airtime Fairness', 'Band Steering', and 'Neighbor AP Detection'. The 'Airtime Fairness' tab is currently selected. Below the menu, there is a checkbox labeled 'Enabled' which is currently unchecked. To the right of the checkbox is a 'Cancel' button. Below the checkbox area is a 'Save' button.

Once the settings are updated, the configuration must be uploaded to the related access points. See "Profile Settings" on page 22 for further information.

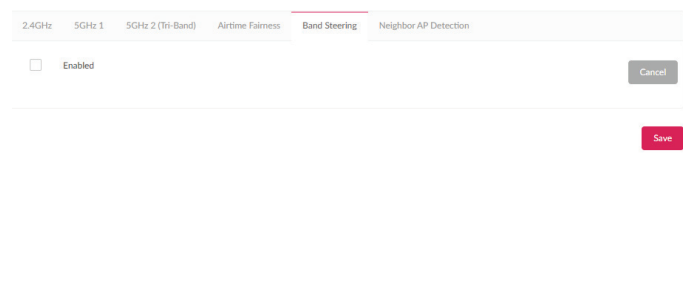
Band Steering

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

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

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

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

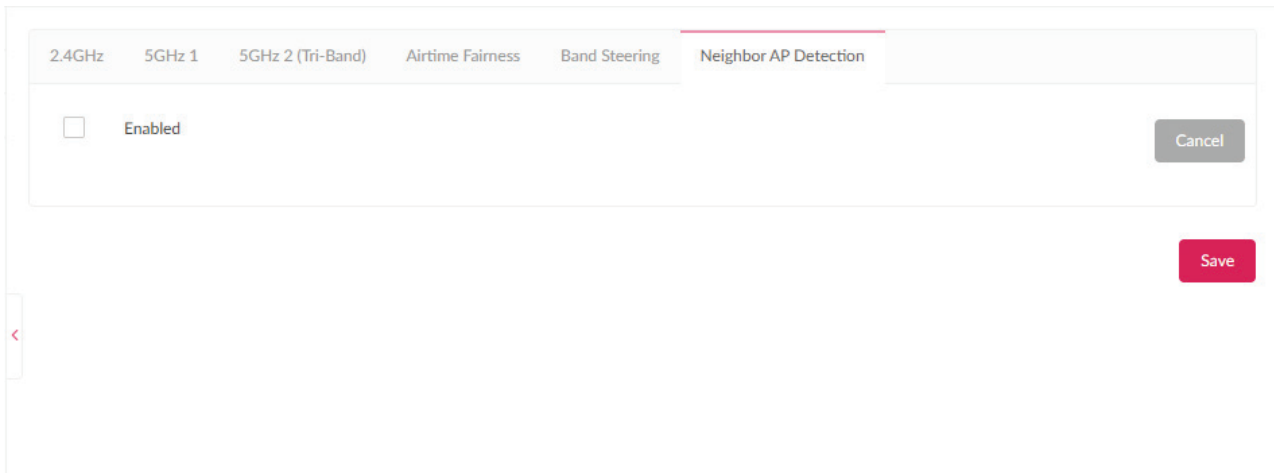


The screenshot shows a configuration interface with a horizontal tab bar at the top. The tabs are: 2.4GHz, 5GHz 1, 5GHz 2 (Tri-Band), Airtime Fairness, Band Steering (which is the active tab), and Neighbor AP Detection. Below the tabs, there is a checkbox labeled "Enabled" which is currently unchecked. To the right of the checkbox is a grey "Cancel" button. At the bottom right of the form area is a red "Save" button.

Neighbor AP Detection

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

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



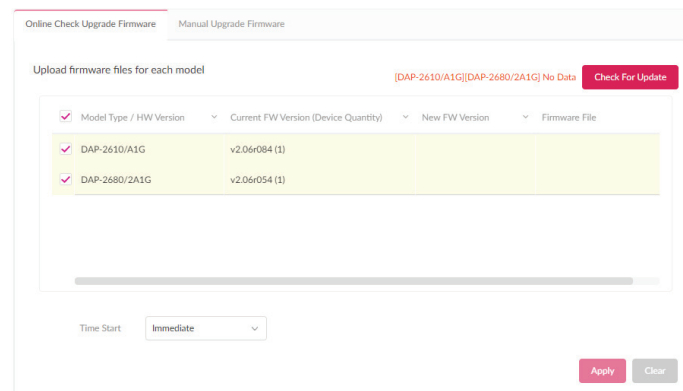
The Firmware Upgrade function allows users to perform a firmware upgrade. This is a useful feature that prevents future bugs and allows for new features to be added your device. For online updates, please confirm your controller is online. For manual upgrade, please go to your local D-Link website to see if there's new firmware available.

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

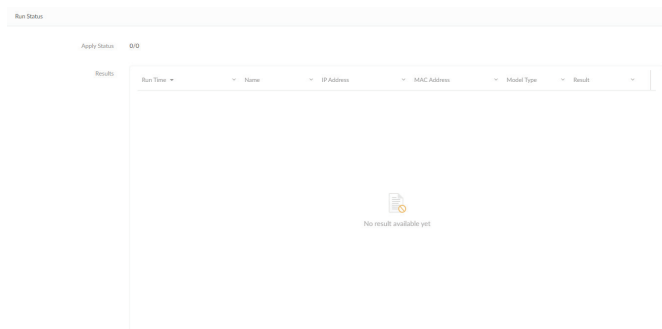
Block	Description
Change(Manual Firmware Upgrade)	Click to select a firmware file to upload. Files are model specific.
Check For Update(Check Upgrade Firmware Online)	Click to check if there's new firmware available on online server.
Time Start	Click the drop-down menu to select a specific time or to 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.

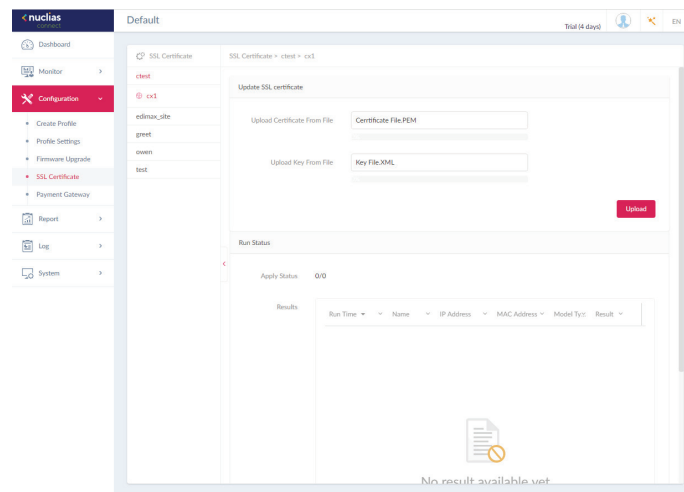


The SSL Certificate function provides the means to install an SSL certificate for use on the network. To accomplish this task an intermediate certificate is required. The intermediate certificate is used to establish the trust of the SSL certificate by binding it to the Certificate Authority's root certificate. 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
Upload Certificate From File	Click Browser... to select the SSL certificate file located on the drive that will be uploaded.
Upload Key From File	Click Browser... to select the SSL key file located on the local drive that will be uploaded.

Click **Upload** to initiate the file upload. The upload status and result will appear in the 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
PayPal Currency	Click the drop-down menu to select the currency code for the Paypal account.
PayPal Client ID	Enter the username for the Paypal account.
PayPal Secret	Enter the password for the Paypal account.
Options	Enter the duration time in minutes, hours, or days as well as the associated cost for the entry. Click + to enter the option.

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

The screenshot shows the Nuclias Configuration interface for the Payment Gateway. The left sidebar contains navigation options: Dashboard, Monitor, Configuration (selected), Create Profile, Profile Settings, Firmware Upgrade, SSL Certificate, Payment Gateway (highlighted), Report, Log, and System. The main content area is titled 'Payment Settings' and includes the following fields:

- PayPal Currency:** A dropdown menu set to 'USD'.
- PayPal Client ID:** A text input field containing 'AKcoK8i8QBvymMG2fYh8cmRDGozV6cQpT3d8N9c'.
- PayPal Secret:** A text input field with masked characters (dots).
- Options:** A table with four rows for adding, editing, or deleting options. Each row has a 'Duration' field (with a dropdown menu), a 'Cost' field (with a numeric input), and a red button with a minus sign (-) for removal. The last row has a red button with a plus sign (+) for adding a new option.

A red 'Save' button is located at the bottom right of the settings area.


Nuclias

Report

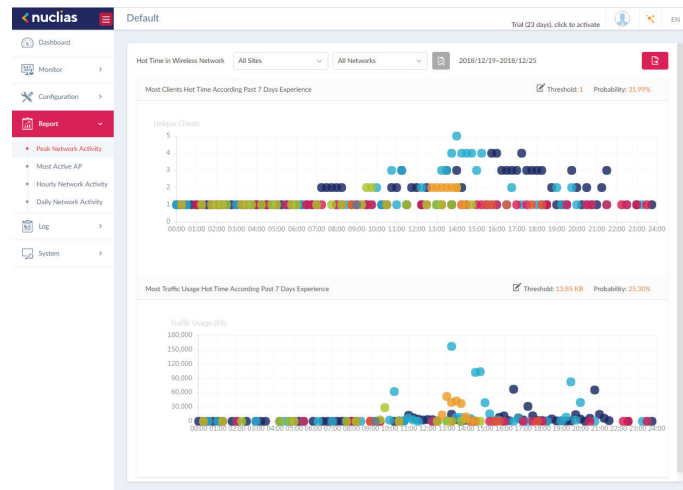
Peak Network Activity

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

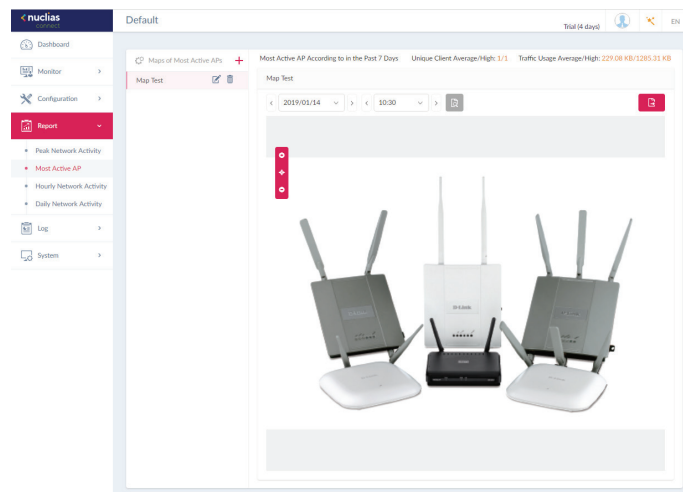
Report

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.

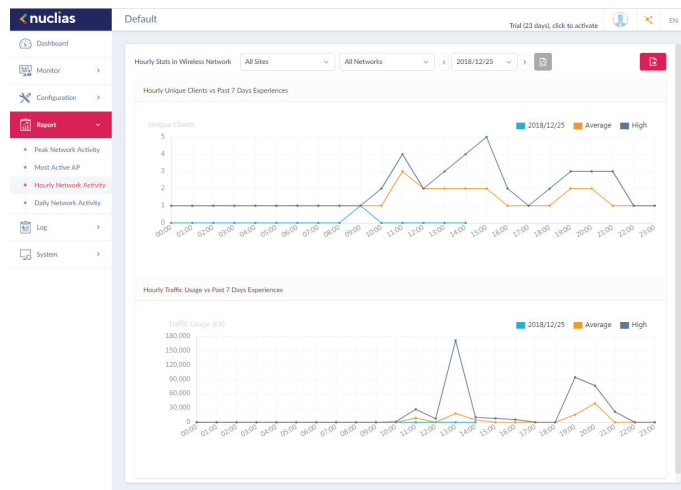


The Hourly Network Activity function allows administrators to monitor wireless traffic on the network. Wireless activity for all or specific sites and networks is displayed according to unique clients and traffic usage as reported by the hour.

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.

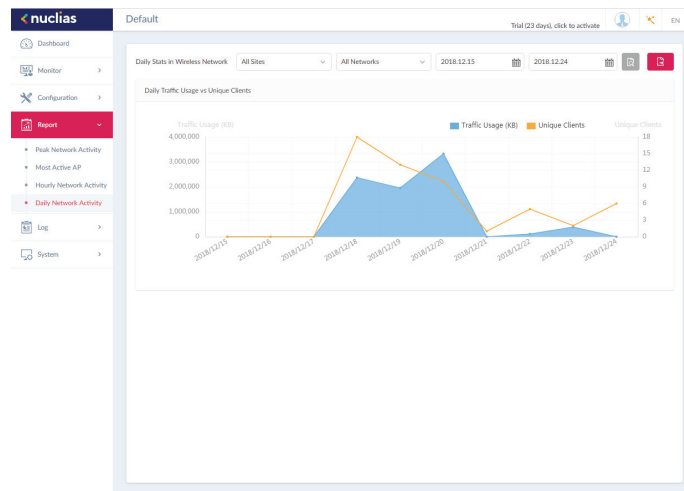


The Daily Network Activity function allows administrators to monitor daily wireless traffic on the network. Wireless activity is displayed according to unique clients and daily traffic usage.


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.

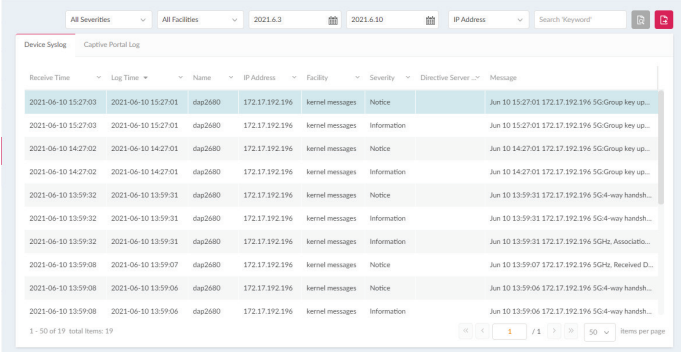
Once a report has been generated, click  to save the report to a local PDF file.



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

To start a syslog report, select the event severity, facility system, and define the period of time to report. Click the drop-down menu to 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 screenshot shows the 'Device Syslog' interface with a table of log entries. The table has columns for Receive Time, Log Time, Name, IP Address, Facility, Severity, Directive Server, and Message. The entries are filtered by 'All Severities', 'All Facilities', and the date range '2021.6.3' to '2021.6.10'. The search criteria is set to 'IP Address' with the keyword '172.17.192.196'. The table contains 19 entries, with the first one highlighted in blue. The interface also includes a search bar, a search icon, and a download icon.

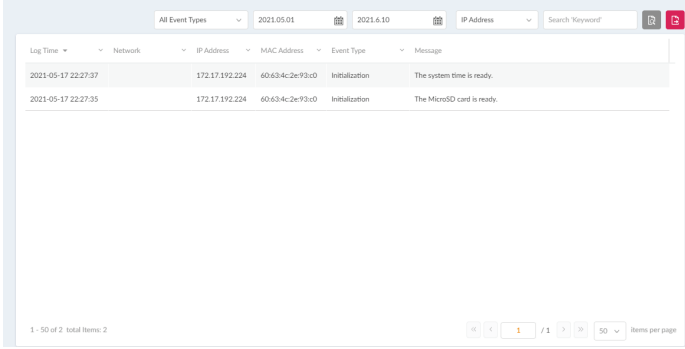
Receive Time	Log Time	Name	IP Address	Facility	Severity	Directive Server	Message
2021-06-10 15:27:03	2021-06-10 15:27:01	dsap2680	172.17.192.196	kernel messages	Notice	Jun 10 15:27:01 172.17.192.196 SG-Group key up...	
2021-06-10 15:27:03	2021-06-10 15:27:01	dsap2680	172.17.192.196	kernel messages	Information	Jun 10 15:27:01 172.17.192.196 SG-Group key up...	
2021-06-10 14:27:02	2021-06-10 14:27:01	dsap2680	172.17.192.196	kernel messages	Notice	Jun 10 14:27:01 172.17.192.196 SG-Group key up...	
2021-06-10 14:27:02	2021-06-10 14:27:01	dsap2680	172.17.192.196	kernel messages	Information	Jun 10 14:27:01 172.17.192.196 SG-Group key up...	
2021-06-10 13:59:32	2021-06-10 13:59:31	dsap2680	172.17.192.196	kernel messages	Notice	Jun 10 13:59:31 172.17.192.196 SG-4-way handsh...	
2021-06-10 13:59:32	2021-06-10 13:59:31	dsap2680	172.17.192.196	kernel messages	Information	Jun 10 13:59:31 172.17.192.196 SG-4-way handsh...	
2021-06-10 13:59:32	2021-06-10 13:59:31	dsap2680	172.17.192.196	kernel messages	Information	Jun 10 13:59:31 172.17.192.196 SG-Chc_Associa...	
2021-06-10 13:59:08	2021-06-10 13:59:07	dsap2680	172.17.192.196	kernel messages	Notice	Jun 10 13:59:07 172.17.192.196 SG-Chc_Received D...	
2021-06-10 13:59:08	2021-06-10 13:59:06	dsap2680	172.17.192.196	kernel messages	Notice	Jun 10 13:59:06 172.17.192.196 SG-4-way handsh...	
2021-06-10 13:59:08	2021-06-10 13:59:06	dsap2680	172.17.192.196	kernel messages	Information	Jun 10 13:59:06 172.17.192.196 SG-4-way handsh...	

1 - 50 of 19 total items: 19

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.



The screenshot displays the System Event Log interface. At the top, there are filters for 'All Event Types', a date range from '2021.05.01' to '2021.6.10', and a dropdown menu set to 'IP Address'. A search bar labeled 'Search Keyword' is also present. Below the filters is a table with the following columns: Log Time, Network, IP Address, MAC Address, Event Type, and Message. Two log entries are visible:

Log Time	Network	IP Address	MAC Address	Event Type	Message
2021-05-17 22:27:37		172.17.192.224	60:63:4c:2e:93:c0	Initialization	The system time is ready.
2021-05-17 22:27:35		172.17.192.224	60:63:4c:2e:93:c0	Initialization	The MicroSD card is ready.

At the bottom of the table, there is a pagination control showing '1 - 50 of 2 total items: 2' and a 'Items per page' dropdown menu set to '50'.


Nuclias

Log

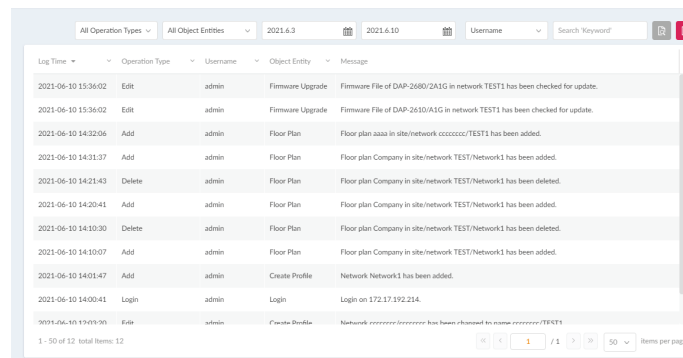
Device Log

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	Operation Type	Username	Object Entity	Message
2021-06-10 15:36:02	Edit	admin	Firmware Upgrade	Firmware File of DAP-2680/2A1G in network TEST1 has been checked for update.
2021-06-10 15:36:02	Edit	admin	Firmware Upgrade	Firmware File of DAP-2610/A1G in network TEST1 has been checked for update.
2021-06-10 14:32:06	Add	admin	Floor Plan	Floor plan aaaa in site/network ccccccc/TEST1 has been added.
2021-06-10 14:31:37	Add	admin	Floor Plan	Floor plan Company in site/network TEST/Network1 has been added.
2021-06-10 14:21:43	Delete	admin	Floor Plan	Floor plan Company in site/network TEST/Network1 has been deleted.
2021-06-10 14:20:41	Add	admin	Floor Plan	Floor plan Company in site/network TEST/Network1 has been added.
2021-06-10 14:10:30	Delete	admin	Floor Plan	Floor plan Company in site/network TEST/Network1 has been deleted.
2021-06-10 14:10:07	Add	admin	Floor Plan	Floor plan Company in site/network TEST/Network1 has been added.
2021-06-10 14:01:47	Add	admin	Create Profile	Network Network1 has been added.
2021-06-10 14:00:41	Login	admin	Login	Login on 172.17.192.214.
2021-06-10 13:49:36	Edit	admin	Create Profile	Network ccccccc/cccccc has been changed to name ccccccc/TEST1

1 - 50 of 12 total items: 12

Nuclias Log Audit Log

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

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

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

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

Nuclias

Log

Alerts

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

Log Time	Network	Name	IP Address	MAC Address	Alert Event	Message	Action
2021-05-17 22:27:59	ccccc	dap2680	172.17.192.196	18:0f:76:32:ea:20	Device online	Device is connected.	

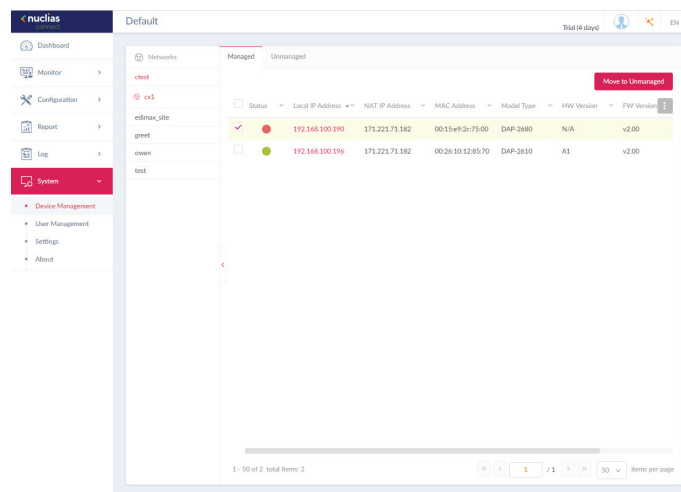
To generate an Alert report, select the alert events, define the time period, and select IP Address or Message as the filtering criteria. Then enter a keyword and click to display the search results. Once a report has been generated, click to export it as a local Excel file. The file will be saved in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

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 below represents the data shown in the interface.


Status	Local IP Address	NAT IP Address	MAC Address	Model Type	HW Version	FW Version
<input checked="" type="checkbox"/>	192.168.100.190	173.223.71.182	00:15:e9:2c:75:00	DAP-2680	N/A	v2.00
<input type="checkbox"/>	192.168.100.196	173.223.71.182	00:26:10:32:85:70	DAP-2680	A1	v2.00

At the bottom of the table, there is a pagination control showing '1 - 50 of 2 total items' and '50 items per page'.

Nuclias System User Management **User Status**

The User Status function allows administrators to view the current status of all registered user profiles, edit or delete the profile. 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.

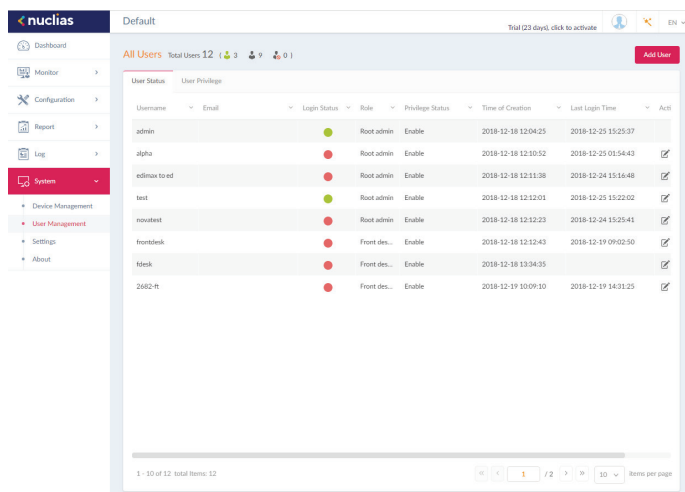
Navigate to **System > User Management** to view the relevant information.

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.

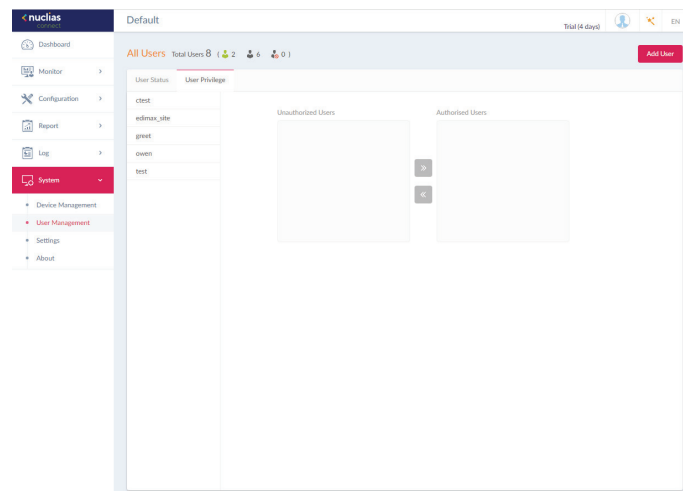
- Admin: This is operator account and can not be deleted.
- Root admin: Can manage all sites/networks on this server.
- Local admin: Can manage his own network.
- Root user: Can view all sites/networks on this server.
- Local user: Can view his own network
- Front desk user: Can generate and manage passcodes.



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
Device Name	Enter a description to set the device name.
Logo	Click Browser to select a file to be used as the interface logo. A local file can be selected by using the browse function or by dragging and dropping a file into the frame. Supported file types include PNG or JPG images.
Login Captcha	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
Get Address From	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. Note: DHCP server is not recommended.
IP Address	If the above is set to Static IP address, specify an IP address for the DNH-100.
Subnet Mask	Specify a subnet mask for the device.
Gateway	Specify a gateway mask for the device. (Optional)
Primary DNS	Specify a primary DNS for the device. (Optional)
Secondary DNS	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
Time Zone	Click the drop-down menu to select the time zone.
NTP	Check to enable use of NTP server(s) to manage device's date and time.
NTP Server 1	Specify the NTP Server's address.
NTP Server 2	Specify the secondary NTP Server's address.
Copy Your Computer's Time	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.

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

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

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

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

The screenshot displays the configuration interface for the Nuclias Connect device. The left sidebar shows the navigation menu with 'Settings' highlighted. The main content area is divided into several sections:

- Customized Setting:** Includes fields for Device Name (DNH-100), Login (with a 'Drag & Drop Login File Here, or Upload' button), Login Protocol (Telnet), and Login Control (Enabled).
- LAN Settings:** Includes fields for WAN IP Address From (Static IP Address Manual), 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 Time Zone (GMT+08:00:00: Asia/Shanghai), NTP (checked), NTP Server 1 (ntp.aliyun.com), and NTP Server 2 (IP Address/Domain name). A 'Copy Real Computer's Time' button is present.
- Console Setting:** Includes a checked 'Console' checkbox, 'Console Protocol' (SSH), and 'Timeout' (5 Min).
- Device Setting:** Includes 'Live Packet Interval' (5 Min).

Each section has a '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:

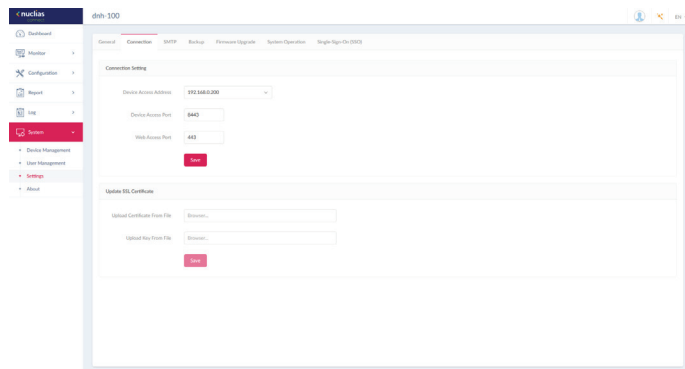
Parameter	Description
Device Access Address	Enter the Nuclias Connect Server application’s IP address. To manage remote APs, the IP address must be a public IP address; IP mapping is required for instances behind a firewall or router.
Device Access Port	Enter the Nuclias Connect server application’s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

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

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

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

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

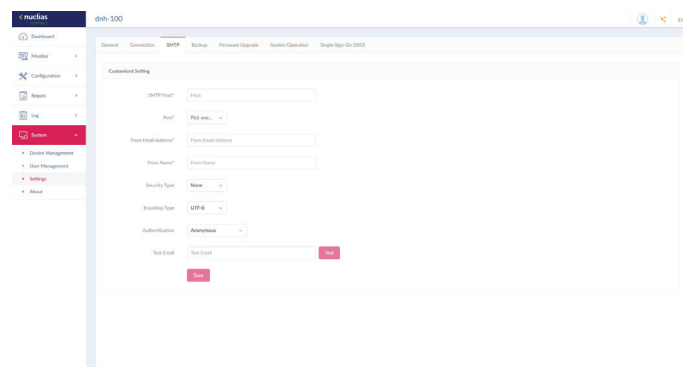


The SMTP tab displays customizable settings for the simple mail transfer protocol (SMTP). This is necessary in order to send emails on behalf of the system such as reset password validation emails.

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

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

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



Nuclias

System

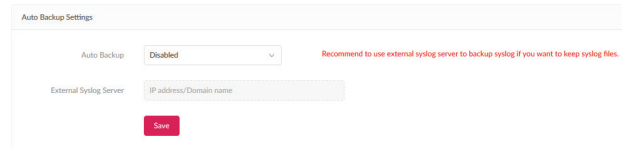
Settings

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:

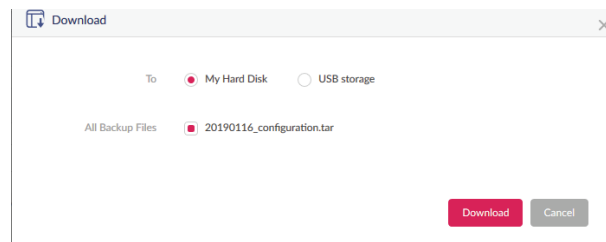


Parameter	Description
Auto Backup	Click on drop-down list to enable or disable auto backup.
External Syslog Server	Enter the external syslog's ip address or domain name.

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


Click  to backup the configuration file or log files.

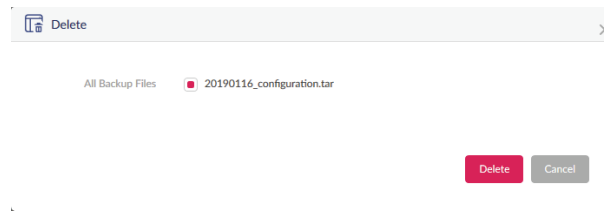
Click  to download the backup file to either the management computer's hard drive or a USB drive.



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

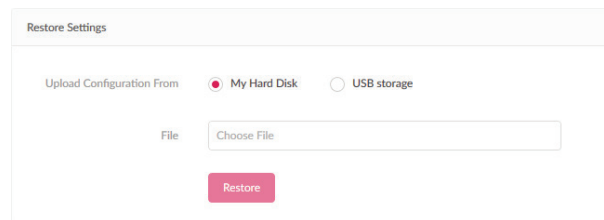
Parameter	Description
To	Choose either My Hard Disk or USB Storage to download your backup file to.
All Backup Files	A list of all backup files that are available to be downloaded will be displayed. Select the radio button of the file you want to download.

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



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

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



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

Parameter	Description
Upload Configuration From	Choose either My Hard Disk or USB Storage to upload your configuration file.
File	Click on Choose File 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
Upload Firmware From	Choose either My Hard Disk, USB Storage or FTP Server to upload your firmware file.
File	Click on Choose File to select your configuration file's location. (Only available if My Hard Disk or USB Storage is chosen.)
FTP Server	Specify IP address or domain name of FTP server.
Port	Specify port number of FTP server.
Username	Specify username.
Password	Specify password.
Firmware File	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, Device Management, User Management, Settings, and About. The main content area has tabs for General, Connection, SMTP, Backup, Firmware Upgrade, System Operation, and Single-Sign-On (SSO). The Firmware Upgrade tab is active, displaying the following configuration 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)

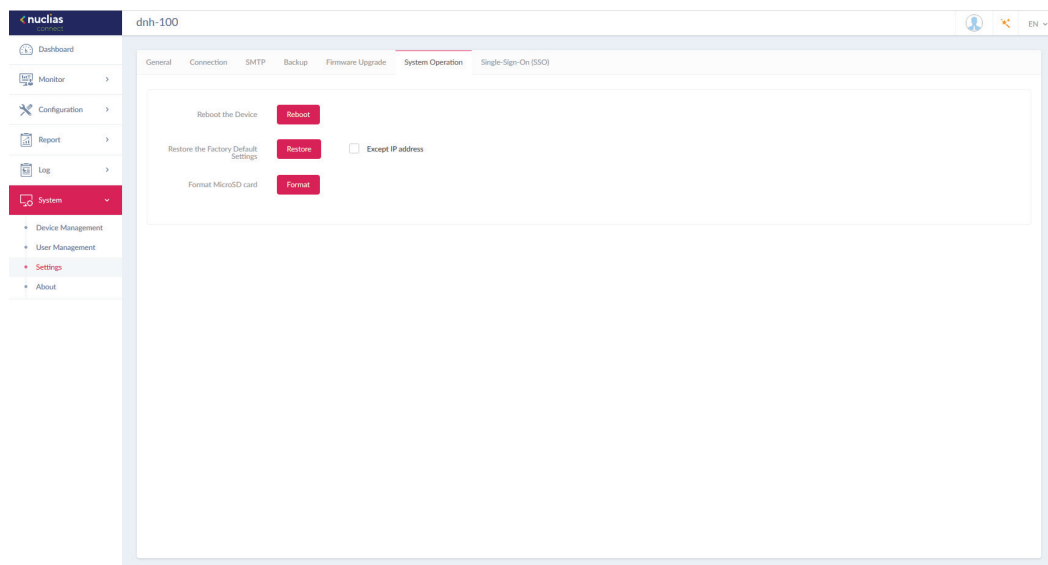
An Apply button is located at the bottom of the form.

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.



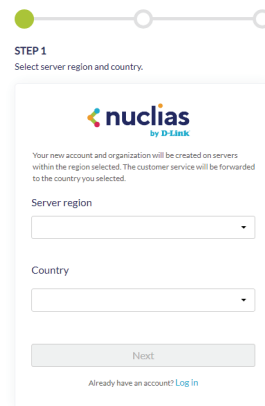
The **Single-Sign-On** tab allows you to use a Nuclias Account to access Nuclias Cloud and the Nuclias Connect portal.

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

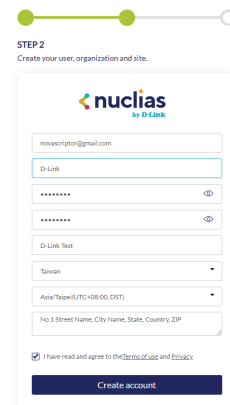
Next

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)

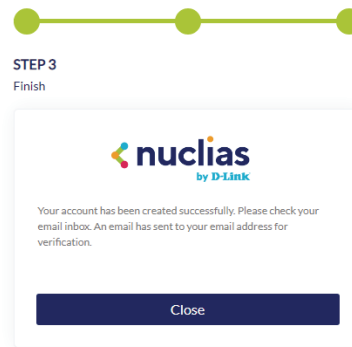
No.1 Street Name, City Name, State, Country, ZIP

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

Create account

Step 3: Finish the registration.

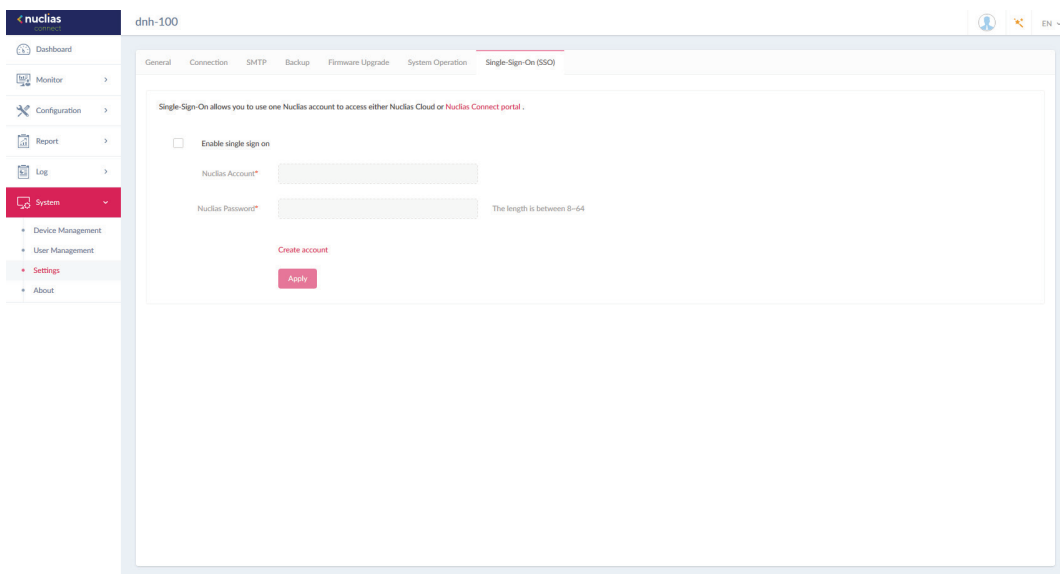
Click Close to complete the process. The registered account is now available for use. The verification information will be delivered to the registered email of the account.



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



The Nuclias Connect Portal provides you with a easy way to view and connect to 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 screenshot shows the Nuclias Connect Dashboard. At the top, there is a navigation bar with the Nuclias Connect logo, a user profile for 'Esther Lei', and a language dropdown set to 'English'. Below the navigation bar is a 'DASHBOARD' header. A search bar is present with filters for 'Type: All' and 'Status: All'. The main content is a table with the following columns: #, Status, Name, Host, Sites, Networks, Devices, Clients, Version, and Actions. There is one row of data with the following values: # 1, Status (green dot), Name dnh-100, Host 172.17.5.225,61.230.144.131, Sites 1, Networks 1, Devices 0/0, Clients 0, Version 1.0.0.10, and Actions (LAUNCH, FORGET). At the bottom right of the table, there are pagination controls: 'Previous', '1', 'Next', and '10'.

#	Status	Name	Host	Sites	Networks	Devices	Clients	Version	Actions
1	●	dnh-100	172.17.5.225,61.230.144.131	1	1	0/0	0	1.0.0.10	LAUNCH FORGET

The Portal provides the following information:

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

Nuclias System Settings **REST API**

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

REST API

Please note that the network without network ID cannot be accessed by REST API.

REST API

Save

Nuclias System Settings **Alerts**

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

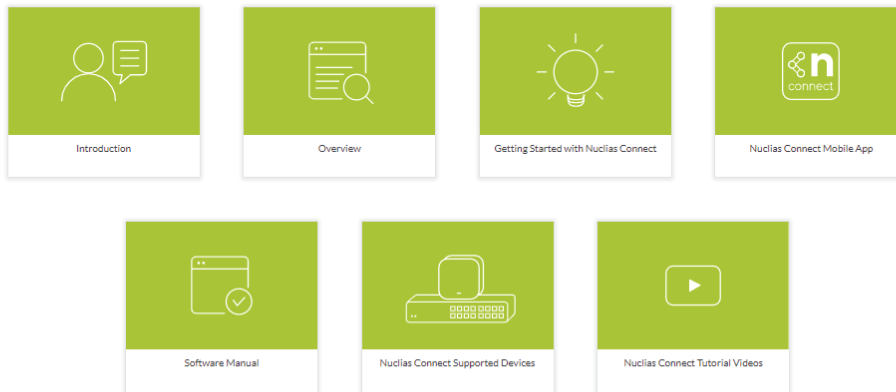
Check the Email box to receive Email notification of specific events. Go to **System>Settings>User Management** to edit the user and select "Receive Email Alert" to allow user to receive alert email from Nuclias Connect. Click **Save** to save the values and update the screen.

Site/Network Events	Alerts	Email
Firmware Upgraded Failed	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device Has Been Removed From Network	<input type="checkbox"/>	<input type="checkbox"/>
Profile Has Been Changed	<input type="checkbox"/>	<input type="checkbox"/>
Profile Failed To Be Applied	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Device Events	Alerts	Email
Device Restarted	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Offline	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Online	<input type="checkbox"/>	<input type="checkbox"/>
Port Link Down	<input type="checkbox"/>	<input type="checkbox"/>
Port Blocked	<input checked="" type="checkbox"/>	<input type="checkbox"/>

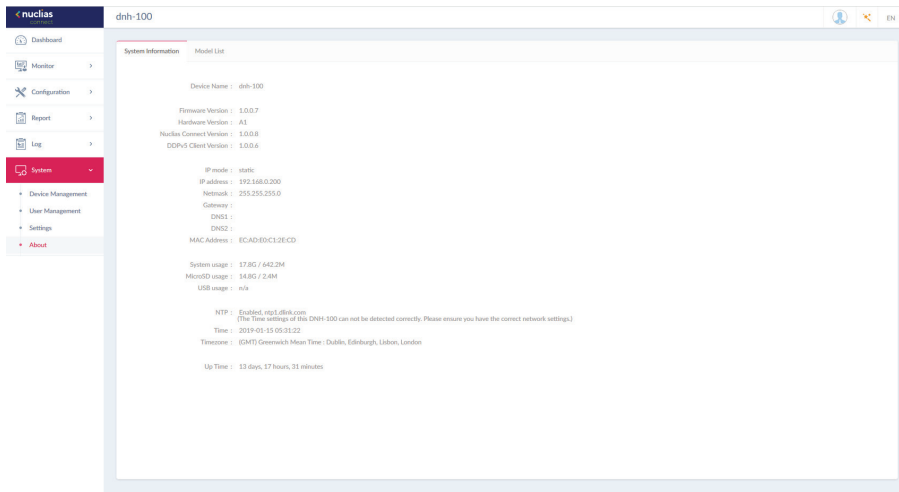
Save

The Resource page allows you to browse the online documents for quick setup, implementation guidelines, and troubleshooting tips.

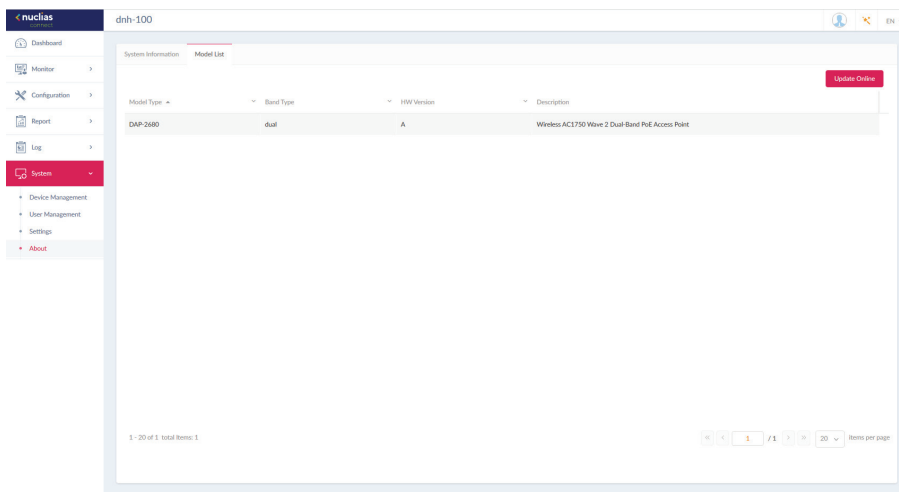


The About page displays system information about the DNH-100 and a list of supported access points.

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

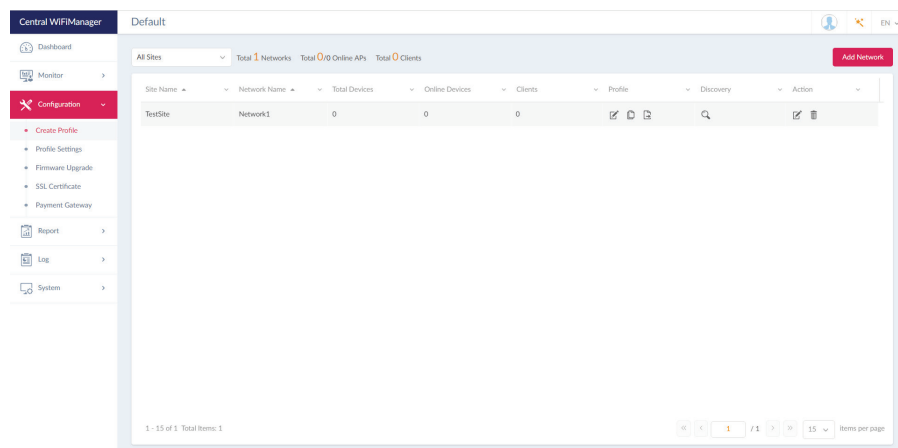
Nuclias Connect App

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.

The screenshot shows the 'Connection Setting' form. It contains the following fields:

- Device Access Address:** A dropdown menu with the value '192.168.1.61'.
- Device Access Port:** A text input field with the value '8443'.
- Web Access Address:** A dropdown menu with the value 'other' and an empty text input field below it.
- Web Access Port:** A text input field with the value '30001'.

A red 'Save' button is located at the bottom of the form. A note at the top of the form states: 'CWM Core server needs to be restarted if Device Access Address or Port has been changed.' and another note below it states: 'CWM Web server needs to be restarted if Web Access Address or Port has been changed.'

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:

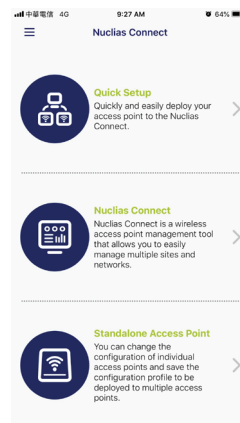
- Before attempting to import a network profile, ensure that you have access to the Nuclias Connect controller.

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.

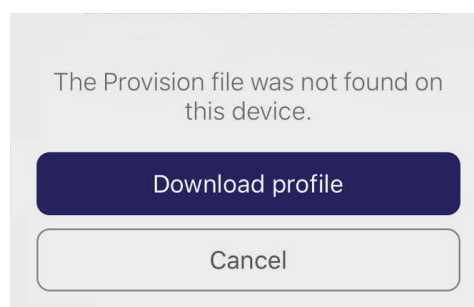
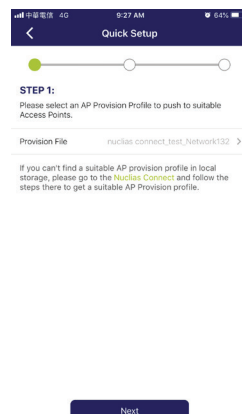


The next step is to select an AP provision profile. The profile is used to push to the selected DAPs. Tap **Quick Setup** to begin the deployment of a standalone DAP to the Nuclias Connect server.

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.

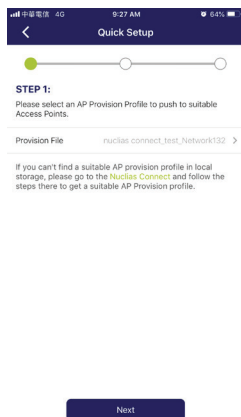
Tap **Download profile** in order to specify a connection to the Nuclias Connect controller.



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.



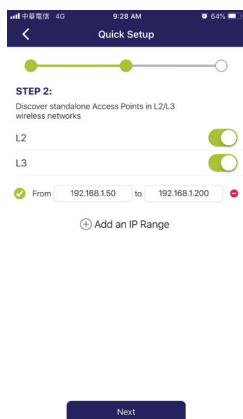
The process will continue and the App will return to the previous screen. From the Step 1 page, tap **Next** to continue.

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.

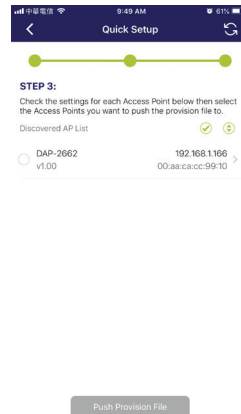


Nuclias Connect App

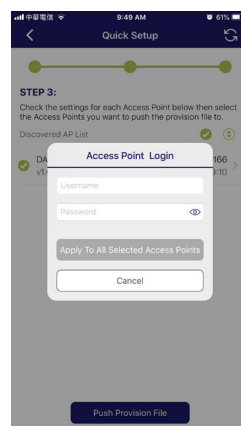
After the scanning the network range, the Step 3 page will list any detected access points.

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.

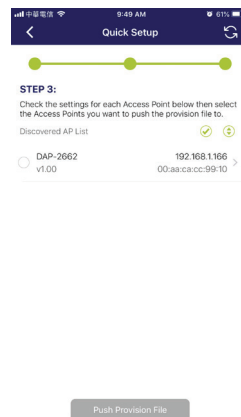
Parameter	Description
Cancel	Tap to discard any changes and continue the process.
Done	Tap to accept any changes and continue the process.
Model Name	Displays the model name for the listed DAP device.
MAC	Displays the MAC address of the listed DAP device.

Nuclias Connect App

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

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.

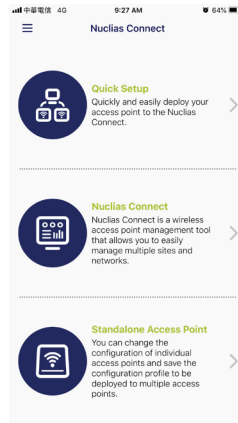


Nuclias Connect App

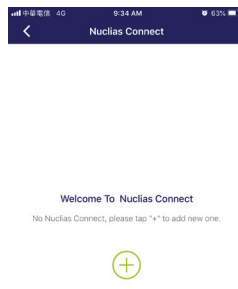
Nuclias Connect

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.



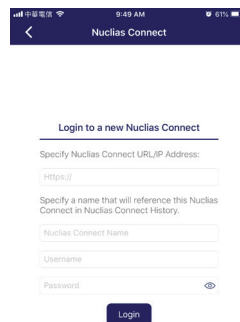
The following page lists the information required to log in to a designated Nuclias Connect controller. Enter the required information in each field.

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

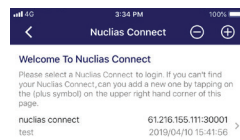
Nuclias Connect App

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

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



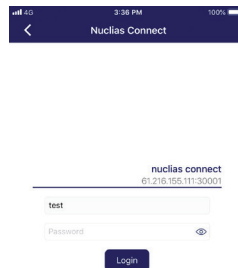
After a successful login, the pairing will be added to the listing and will be available for future login selection.



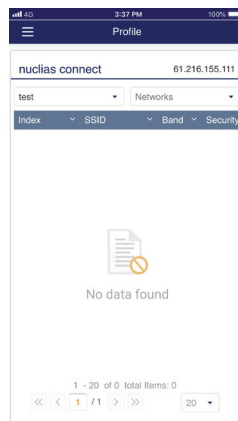
Tap on a **Nuclias Connect** server from the list.

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

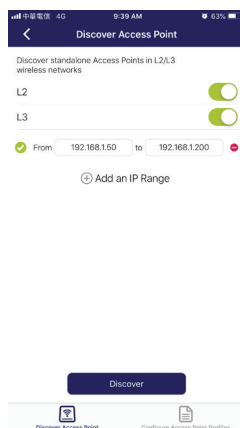
Discover DAPs

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.



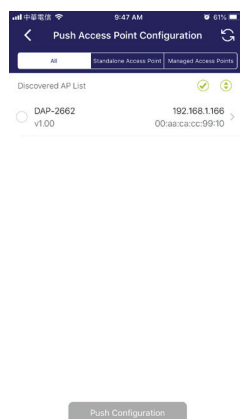
Once the range is defined, tap **Next** to initiate the discovery process.

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.

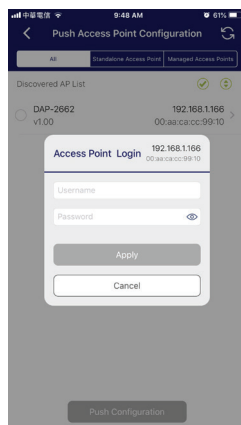
Tap the radio button next to the DAP to select it. The selected local provision file will be pushed to the selected DAP.

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



Nuclias Connect App

The Wireless settings menu is listed in the following figure.

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

