NUCLIAS CONNECT DNH-100 User Manual





Table of Contents

Introduction	
Product Overview	
Package Contents	
System Requirements	
Hardware Overview	4
LED Indicators	4
Interface Connectors	4
Installation	5
Mounting	5
Connecting the Controller	6
Basic Configuration	
Launch Nuclias Connect	
Nuclias Connect Configuration	9
Wizard	
Dashboard	
Monitor	
Access Point	13
Wireless Client	
Configuration	
Create Profile	
Profile Settings	
Firmware Upgrade	
SSL Certificate	
Payment Gateway	
Report	
Peak Network Activity	
Most Active AP	
Hourly Network Activity	
Daily Network Activity	
Log SNMP Traps	
Sivier traps	
, .	
System Event Log	
Device Log System	
Device Management	
User Management	
Settings	
About	
Appendix Nuclias Connect App	
Huends connect App	02

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

Interface Connectors



#	Connector	Description
1	Reset	Used for rebooting or resetting the device back to
1	neset	factory default settings.
2	Console	RJ-45 port to connect the RJ-45 console cable for CLI
2	Port	management .
3	Ethernet	Gigabit RJ-45 port for LAN connection.
5	Port	Gigabit KJ-43 port for LAN connection.
4	MicroSD	MicroSD slot for MicroSD card ^{1,2,3} up to 32 Gb.
4	Slot	
5	USB Port	USB 3.0 Type A port ² (provides 5V/1A power for
5	USBFOIL	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 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.

< nuclias connec	
Login to your account	
Your E-mail / User Name	
Your password	
Please input the captch 1557	
Remember me	Forgot password?
Login	
© 2019 D-Link Corporation English	h v

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.

< nuclias connect	
You need to change your password after the first login. Strong password consisting of 5 - 16 characters is required. Combine uppercase letters, lowercase, letters, numbers and symbols. Do not include common words or names.	
Jild password	
new password	
confirm password	
Modify	
© 2019 D-Link Corporation English 🗸	ļ

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 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 differant 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 depanding 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 inboud port must be opened.
Web Access Port	The web access ports as defined during the installation. The values are predefined.

Click **Next** to continue

	192.168.0.200	~	
Device Access Port	8443		
Web Access Port	443		
Country	Afghanistan	~	

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

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

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

Site	ite v	
Network Name Netwo	ork1	
		Back Next Exit
* Network Configurations		
Wireless Settings		
SSID Name	dlink	
SSID Name Security	dlink WPA-Auto-Personal v	
	WPA-Auto-Personal v	
Security		
Security	WPA-Auto-Personal v	
Security SSID Password*	WPA-Auto-Personal v	
Security SSID Passwort ^e Guest SSID Name	WPA-Auto-Personal v	
Security SSID Passwort ^e Guest SSID Name Device Setting	WRk-Auto-Pennanal	
Security 550 Presence" Guest SSD Name Device Setting Coastly	WMA-Auto-Pensenal 40 40 Add Guest SSID(Optional)	
Security SSED Pressore" Gueret SSED Name Device Setting Country Tree Zone	WMA.Adub Personal Roy Roy Add Guest SSID(Optional) Addpumates KDMT-08.00 Taged	

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 ^H to add additional IP/prefix segments or **Next** to continue. Click **Exit** to discontinue the configuration process.

 Layer 2 					
 Layer 3 (II 	.»)				
IP	~	192.168.1.150	- 192.168.1.200		
Pick one	~			—	

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.

Config	urable	Manage	ed.						
~	State	~	IP Address	~	MAC Address ~	Model Type 🗸	NMS URL	~	Network
~	Unregi	stered	192.168.1.166		40:9b:cd:0c:66:20	DAP-2680	192.168.1.61:8443		

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

lonitor

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.

< nuclias	C	Default							Trial (23 d	ays), click to act	ivate 🔹	×
Dashboard		Usage										
별 Monitor	-	Code										
Access Point		All Sites		~ N	I Network:	• • R	Total: 0/15 Access	Points Total Down	load: 429.65 KB	Total Upload:	5.48 KB	
Wireless Client		Transf Orders	Access Points									
Configuration	>	KA	Accessforme							Download	d (KB) 🛛 🔶 Upla	ad (KB)
Report	5	250										
Log	,	150	Λ									
		100	()									
O System	2		$\backslash /$	1								
		50 0 15:00 1	×00 1700 1	200 19:00	20:00	0.00 22.00 23.00 30	9 ⁰ 01.9 ⁰ 07.9 ⁰ 031	²⁶ 04. ⁰⁶ 05. ⁰⁶ 0	60 ⁰ 01.00 08.00 0	900 1000 1	100 1200 130	0 1400
		15:00 15	Access Points	29:00	2000 7	0.00 [°] 200 [°] 20 ^{0°} 00	59 [°] 01.59 [°] 02.59 [°] 05.1				198 1298 139	
		15:00 15		Action	20/00	Local IP Address ~		Search By				0 1430 1430
		0 15 ⁰⁰ 1 Total 0 /15	Access Points					Search By	Local IP Address	v Search 1	Keyword	R
		0 15 ⁰⁰ 1 Total 0/15 No.	Access Points	Action	•	Local IP Address	MAC Address 🗠	Search By Model Type V	Local IP Address Network V	 Search 1 Client × 	Keyword Channel 2.4G	
		0 75 ⁰⁰ 75 Total 0/15 No. 1	Access Points	Action	0	Local IP Address v 172.17.134.68	MAC Address ~ 40.9bxxtb0:67:10	Search By Model Type v DAP-2680	Local IP Address Network × Network1	 Search 1 Client 0 	Keyword Channel 2.4G 11	R
		0 75 ⁰⁰ 5 Total 0/15 No. 1 2	Access Points Status ~	Action	0	Local IP Address × 172.17.134.68 172.17.134.71	MAC Address ~ 40.9bxxt0c:67:10 40.9bxxt0c:65:70	Search By Model Type V DAP-2680 DAP-2680	Local IP Address Network Vetwork1 UC0079	v Search 1 Client v 0	Keyword Channel 2.4G 11 11	R
		0 75500 5 Total 0/15 No. 1 2 3	Access Points Status ~	Action	0 0 0	Local IP Address ~ 172.17.134.68 172.17.134.71 192.168.0.4	MAC Address 40.9bcd.0c.67:10 40.9bcd.0c.65:70 40.9bcd.0c.67:20	Search By Model Type V DAP-2680 DAP-2680 DAP-2680	Local IP Address Network V Network1 UC0079 hithBith	 Search 1 Client O O O 	Keyword Channel 2.4G 11 11 11	R - : 1 5
		0 7500 V Total 0/15 1 2 3 4	Access Points Status ~	Action		Local IP Address V 172.17.134.68 172.17.134.71 192.168.0.4 192.168.0.6	MAC Address ~ ~ 40.9bcd.0c:67:10 40.9bcd.0c:67:20 40.9bcd.0c:67:20 00.87:03:55:3d:90	Search By Model Type * DAP-2690 DAP-2690 DAP-2690 DAP-2662	Local IP Address Network VC00079 Nhibih	 Search 1 Client 0 0 0 0 0 	Keywood Channel 2.4G 11 11 11 5	S 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2

The following figure represents a typical report. This report can be refined by selecting the a specific Site from the first dropdown 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.

<nuclias< th=""><th></th><th>Default</th><th></th><th></th><th></th><th></th><th></th><th></th><th>Trial (25 day</th><th>s), clic</th><th>k to activate</th><th></th><th>×</th><th>EN</th></nuclias<>		Default							Trial (25 day	s), clic	k to activate		×	EN
Dashboard		Connecte	ed Clients	Blocked Clients										
Monitor	× .	Total 1	Connected Cl	ents										
Access Point		D-Link	Site	 Network1 	v v	All Clients	~	Search By	MAC Address	•	Search 'Ke	ryword'		R
Wireless Client Configuration	>	No.	Action	IP Address 🔺	 MAC Address 	 Auth Type 	Channel	~	RSSI (dBm)	~	Band	v	SSID	
_	>	1	G.	169.254.225.82	54:9f:13:0e:8c:b7	Disabled	11		-61		2.4GHz		dlink	
Log	•													
System	2													
		-												
		1 - 20 o	of 1 total Items	:1					< 1	/1	> >>	20 v	items p	er page

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

Aonitor

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.

<nuclias< th=""><th></th><th>Default</th><th>Trial (25 days), click to activate 🔍 EN</th></nuclias<>		Default	Trial (25 days), click to activate 🔍 EN
Dashboard		Connected Clients Blocked Clients	
Monitor	~	Total 1 Blocked Clients	D-LinkSite v Network1 v 🕃
Access Point Wireless Client		No. Action Network	 MAC Address Band SSID
Configuration	,	1 S Network1	54:9f:13:0e:8c:b7 2.4GHz dlink
Report	,		
Log	>		
System	>		
		1 - 20 of 1 total Items: 1	((1 /1)) 20 v Rems per page

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.

nuclias connect		Default									Trial (4 days)		×	EN
) Dashboard		All Sites	✓ Tot	al 4 Networks Total 1/5 0	Online AP	s Total O Clients							Add Netw	vork
Monitor	>	Site Name		Network Name		Total Denisor V	Online Devic.Y	Climate	Profile		Discovery	v . Au	tion	
Configuration	-	ctest		cx1		2	1	0	R. C		Q		1	
Create Profile		edimax site		yayayayaya		1	0	0	RC		q			
Profile Settings		owen		owen		1	0	0	RC		q		8	
Firmware Upgrade		test		Network1		1	0	0	RC		d d		8	
SSL Certificate Payment Gateway		054		PRELWOORLE			0	v	15 L	비년	4	Ľ		
Report	>													
log	2													
3 System	,													
		1 - 15 of 4 total Ite	me d							1.4			dame ner r	
		1 - 15 of 4 total Ite	10552 49						1	/1		5 V	items per p	balle

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 ${}^{\square}$	Copies existing profile to a designated site and network.
Export Network Profile 🗄	Exports selected profile to a file (*.dat) on a local directory.
Discovery ^Q	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. 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.

X Add Network			×
Site	newSite v		
Network Name	Network1		
			Next Exit
Network Configurations			×
Wireless Settings			
SSID Name	dlink		
Security	WPA-Auto-Personal v		
SSID Password*		96	
	Add Guest SSID(Optional)		
Guest SSID Name			
Device Setting			
Country	Taiwan v		
Time Zone	(GMT+08:00) Taipei	~	
Time Zone Username	(GMT+08:00) Taipei admin	~	
		~	

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 \blacksquare to add additional IP/prefix segments or **Next** to continue. Click **Exit** to discontinue the configuration process.

✓ Layer 2					
 Layer 3 (I 	P)				
IP	~	192.168.1.150	- 192.168.1.200		
Pick one	~		-	+	

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.

onfigu	rable	Manage	ed						
~	State	~	IP Address	~	MAC Address ~	Model Type 🗸	NMS URL	 ✓ Net 	twork
~	Unreg	istered	192.168.1.166		40:9b:cd: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.



SSID

Nuclias Configuration Profile Settings

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 (802.11 k/v/r) ⁴	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.
Кеу Туре	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 19 for further information.

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



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. Note: SLA Login (Click through) is currently only available for DAP-2662 and DAP-3666.
Idle Timeout (2~1440)	Enter the session timeout value.
Enable White List	Check the box to enable the white list function. This function is only available when Authentication Type is Username/Password .

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

Block	Description
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: Click Preview to preview the selected style. Click Upload Login File to upload a new style. Click is to delete the selected style. Click is to delete the selected style. Click is to delete the selected style. Click is to download the style template.

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

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

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

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

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

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

Click **Clear** to reset all settings.

VLAN

Nuclias Configuration Profile 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.

< nucl	ias nect		Default	Trial (4 daya)		×	EN S
🚯 Das	shboard						
Mor	nitor	>	C? Profile	Profile > ctest > cx1 > VLAN			-
		_	ctest				
× Con	nfiguration	*	@ ex1	VLAN Status Disabled V Save			
• Crea	ate Profile		SSID				
• Profi	ile Settings		VLAN	VLAN List Port List Add/Edit VLAN PVID Setting			
	nware Upgrade Certificate		Bandwidth Optimiz RF Optimization	VLAN VID 🗵 VLAN Name* Tag VLAN Ports * Untag VLAN Ports	~ Actio	in	
• Payn	ment Gateway		Schedule	1 default SSID7 (5G), SSID6 (5G), SSID5 (5G), SSID-	Ľ	8	
Rep	ort	>	Device Setting Performance				
E Log		•	WLAN Partition Wireless Resource				
Syst	tem	,	edimax_site				
			greet				
			owen				
			test				
				1-15ef1 total items 1 (1) (1) (15	v items	s per pag	<i>p</i>

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.

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. 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.

nuclias	Default			Trial (4 days) 🙁 E
Dashboard	₹2 Profile	Profile > ctest > cx1 > Bandwidth Opt	imization	
A Monitor	ctest			
🕻 Configuration 🗸	@ cx1	Enable Bandwidth Optimization	Disabled v	
Create Profile	SSID	Downlink Bandwidth	80	
Profile Settings	VLAN	Downlink Bandwidth	80 Mbits/sec	
Firmware Upgrade	Bandwidth Optimiz		Multij sec	
SSL Certificate	RF Optimization	Uplink Bandwidth	80	
Payment Gateway	Schedule Device Setting		Mbits/sec	
Report >	Performance	Add Bandwidth Optimization	Rule	
log >	WLAN Partition	Rule Type	Allocate average bandwidth for each station	
System >	Wireless Resource	< Band		
O alorent	edimax_site			
	greet	SSID Index		
	owen test	Downlink Speed	80 Mbits/sec v	
		Uplink Speed	80 Mbits/sec v	
			Add Clear	
		Band X. SSID + Y Type	 Downlink Speed 	~ Uplink Speed ~ Action

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.

<nuclias< th=""><th>Default</th><th>Trial (4 days)</th><th>💘 🛛 EN 👻</th></nuclias<>	Default	Trial (4 days)	💘 🛛 EN 👻
Dashboard	C Profile	Profile > ctest > cx1 > RF Optimization	
Monitor >	ctest		
🗙 Configuration 👒	@ ext	RF Optimization	
Configuration C	 cit SSD VLM Bandwidth Oppintz. BF Oppinzation Schools Device Setting Performance WAAR Purchises Workess Resource edinaus, alter genet exemit text 	Adjut Freuence: 6 v 9 Hunt	Sive

Nuclias Configuration Profile Settings Schedule

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

Parameter	Description
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.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.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 *I* to modify the desired rule.

Click 💼 to delete the desired rule.

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



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.



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

Click Save to save the values and update the screen.



Nuclias Configuration Profile Settings WLAN Partition

2.4GHz/5GHz

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

Parameter	Description
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.

<nuclias< th=""><th>Default</th><th></th><th></th><th></th><th></th><th>Trial (4 days)</th><th>R ×</th><th>EN v</th></nuclias<>	Default					Trial (4 days)	R ×	EN v
Dashboard	C Profile	Profile > ctest > cx1 > V	VLAN Partition					
Monitor >	ctest							
🗙 Configuration 🕞	@ ex1	2.4GHz 5GHz						
Create Profile Profile Settings	SSID VLAN	Link Integrity	Disabled					
Firmware Upgrade SSL Certificate	Bandwidth Optimiz RF Optimization Schedule	Ethernet to WLAN Access	nnection	~				
Payment Gateway Report >	Device Setting Performance	Primary SSID Multi-SSID 1	EnabledEnabled	 Disabled Disabled 	Guest Mode			
E Log >	WLAN Partition Wireless Resource	Multi-SSID 2	Enabled	Olisabled	Guest Mode			
Go System →	edimax_site	Multi-SSID 3	Enabled	O Disabled	Guest Mode			
	greet	Multi-SSID 4	Enabled	O Disabled	Guest Mode			
	test	Multi-SSID 5	Enabled	O Disabled	Guest Mode			
		Multi-SSID 6	Enabled	O Disabled	Guest Mode			
		Multi-SSID 7	Enabled	O Disabled	Guest Mode			
							Sa	we

Nuclias Configuration Profile Settings Wireless Resource 2.4GHz/5GHz

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

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

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

< nuclias	Default			Trial (4 days)) 🗙 🖻
Dashboard	© Profile	Profile > ctest > cx1 > Wireless Resou	rce		
Configuration v	ctest @ cx1	2.4GHz 5GHz Airtime Fair	ness Band Steering		
Create Profile Profile Settings Firmware Upgrade	SSID VLAN Bandwidth Optimiz	ACL RSSI Threshold			
SSL Certificate Payment Gateway	RF Optimization Schedule	Aging Out			
Report >	Device Setting Performance	RSSI Threshold Data Rate			
E Log >	WLAN Partition Wireless Resource	Connection Limit			
	edimax_site greet	User Limit (0-64)	20 Enabled v		
	test	Network Utilization			
					Save
					_

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.



Nuclias Configuration Profile Settings Wireless Resource Band Steering

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

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

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

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



Nuclias

Configuration

Firmware Upgrade

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

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

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

Click **Apply** to save the above configuration settings. Click **Clear** to delete the defined settings.

<nuclias< th=""><th>Default</th><th></th><th>Trial (4 days) 🔍 K EN 🖲</th></nuclias<>	Default		Trial (4 days) 🔍 K EN 🖲
Dashboard	Firmware Upgrade	Firmware Upgrade > ctest > cx1	
Monitor >	ctest		
X Configuration -	@ ext	Upload firmware files for each model	
Create Profile	edimax_site	Model Name / HW Version 12. FW Version In Firmware File	
 Profile Settlings 	greet		
Firmware Upgrade	owen	DAP-2610/A1	Change
SSL Certificate	test	DAP-2680/N/A	Charge
 Payment Gateway 			
Payment Gateway			
Report >			
Log >			
Go System		¢	
		Time Start, lenvelide v	Apply Case
		Run Status	

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.

Aun Satus	
Apply Soutan Q/Q	
Reside hin Time + v Name + 10 Address + 144C Address + Model Type + Bault	
No result available yet	
Configuration

SSL Certificate

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

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

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.

< nuclias	Default			Trial (4 days)		×	EN v
Dashboard		SSL Certificate > ctest > cx1					
Monitor >	ctest						
🗙 Configuration 🗸	@ cx1	Update SSL certificate					
Create Profile	edimax_site	Upload Certificate Fro	om File	Cerrtificate File.PEM			
 Profile Settlings 	greet						
 Firmware Upgrade 	owen						
SSL Certificate	test	Upload Key Fro	om File	Key File.XML			
Payment Gateway					_	_	
Report >					Upload		
Log >		Run Status					
Go System →		¢ Apply Status	0/0				
		Results	Run Ti	me 👻 🕆 Name 🕆 IP Address 🕆 MAC Address 🗸 Model Tyy, Result	×		
				No result available vet			

Configuration

Payment Gateway

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

Navigate to **Configuration > Payment Gateway**.

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

< nuclias	Default						Trial (23 days), click to activate	×	EN V
Dashboard									
Monitor >	Payment Settings								
🗙 Configuration 🔷 👻	PayPal Currency*	USD	~						
Create Profile Profile Settings	PayPal Client ID*	AXcoX8i6QBVym/	4G217xRocmRD9	GoZCWqCq9T3dKh9c					
 Firmware Upgrade SSL Certificate 	PayPal Secret*		••••••	•••••					
Payment Gateway	Options*	Duration	1	Minute(s)		Cost	1		
Report >		Duration	1	Hour(s)	•	Cost	1		
E Log >		Duration	1	Day(s)		Cost	1 –		
System >		Duration		Pick one		Cost	+		
								Save	

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.



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 \mathbb{Z} or \mathbb{T} . 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.



Report

Hourly Network Activity

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

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



Report

Daily Network Activity

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.

< nuclias	Default				Trial	(23 days), click to act	tivate (D	K D
Dashboard	Daily Stats in Wireless Network	All Sites v	All Networks	2018.12.15	鎆	2018.12.24	鎆	R	8
Configuration	Daily Traffic Usage vs Unique O	lients							
Report Peak Network Activity Most Active AP Hourly Network Activity	Traffic Usage (KB) 4,000,000 3,000,000 2,000,000		\triangleright	Traffic Use	ige (KB)	Unique Clients		Unique Cli 1 1 9	8
Daily Network Activity Log >	1,000,000 0 2018/121/5	SOLANDAS DOLANDA SO	2012018 2012019 201	anana zotanana	-718/12/	22 2018/12/23	01802224	6	
System >	20181	Jong, Jong, 30,	a. 20181, 201	2018/	2018	20181	20791		

Nuclias	Log	SNMP Traps
---------	-----	------------

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

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

nuclias	Default			Trial (23 days), click to ac	tivate 🔱 🔀 I
) Dashboard	All SNMP Versions v All Generic Typ	w ∨ 2018.12.18	2018.12.25	IP Address v	Search 'Keyword'
Monitor >	R 🕒				
Configuration >	Receive Time ~ Time of Trap	 Name 	 IP Address SNMP Version 	 Trap Type 	 Trap Details
Report >	2018-12-25 09: 1970-01-01 15:04:33	dap2610	192.168.100.161 V1	enterpriseSpecific	["TrapOID: 1.3.6.1.4
log ~	2018-12-25 09: 1970-01-01 15:04:30	dap2610	192.168.100.161 V1	enterpriseSpecific	["TrapOID: 1.3.6.1.4
SNMP Traps	2018-12-25 09: 1970-01-01 15:04:30	dap2610	192.168.100.161 V1	enterpriseSpecific	["TrapOID: 1.3.6.1.4
Syslogs	2018-12-25 09: 1970-01-01 15:04:29	dap2610	192.168.100.161 V1	enterpriseSpecific	['TrapOID: 1.3.6.1.4
System Event Log	2018-12-25 09: 1970-01-01 15:04:29	dap2610	192.168.100.161 V1	enterpriseSpecific	["TrapOID: 1.3.6.1.4
Device Log	2018-12-25 09: 1970-01-01 15:04:29	dap2610	192.168.100.161 V1	enterpriseSpecific	['TrapOID: 1.3.6.1.4
System >	2018-12-25 09: 1970-01-01 15:04:16	dap2610	192.168.100.161 V1	enterpriseSpecific	["TrapOID: 1.3.6.1.4
	2018-12-25 09: 1970-01-01 14:51:36	dap2610	192.168.100.161 V1	enterpriseSpecific	['TrapOID: 1.3.6.1.4
	2018-12-25 09: 1970-01-01 14:51:36	dap2610	192.168.100.161 V1	enterpriseSpecific	["TrapOID: 1.3.6.1.4
	2018-12-25 09 1970-01-01 14:51:36	dap2610	192.168.100.161 V1	enterpriseSpecific	['TrapOID: 1.3.6.1.4
	2018-12-25 09: 1970-01-01 14:51:35	dap2610	192.168.100.161 V1	enterpriseSpecific	["TrapOID: 1.3.6.1.4
	2018-12-25 09: 1970-01-01 14:51:35	dap2610	192.168.100.161 V1	enterpriseSpecific	['TrapOID: 1.3.6.1.4
	2018-12-25 04: 1970-01-01 10:26:25	dap2610	192.168.100.161 V1	enterpriseSpecific	("TrapOID: 1.3.6.1.4
	2018-12-25 04: 1970-01-01 10:26:20	dap2610	192.168.100.161 V1	enterpriseSpecific	["TrapOID: 1.3.6.1.4
	1 - 50 of 1205 total items: 1205			< 1 /25 >	≫ 50 v items per pag



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

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

Dashboard		AI	Severity		AI	Facility		v 20	18.12.18		龠	2018.12.2	25	69	IP Address	v	Search 'P	leyword"		
Monitor	>	R	B																	
Configuration	>	S	rslog	Captive P	ortal Log															
Report	>		Receive T	ine .	Log	lime	~	Name	~	IP Addre	55 ×	Facility	~	Severity ~	Directive Ser.	Mess	age		~	
	*		2018-12-	25 09:14	2001	-01-01 1	5:04	dap2610	D	192.168	100	kernel mes	sages	Notice		Jan 01	15:04:33 1	92.168.100.	161	
SNMP Traps			2018-12-	25 09:14	2001	-01-01 1	5:04	dap2610	D	192.168	100	kernel mes	sages	Notice		Jan 01	15:04:30 1	92.168.100	161	
Syslogs			2018-12-	25 09:14	2001	-01-01 1	5:04	dap2610	0	192.168	100	kernel mes	sages	Notice		Jan 01	15:04:30 1	92.168.100.	161	
System Event Log Device Log			2018-12-	25 09:14	2001	-01-01 1	5:04	dap2610	0	192.168	100	kernel mes	sages	Notice		Jan 01	15:04:29 1	92.168.100.	161	
System	,		2018-12-	25 09:14	2001	-01-01 1	5:04	dap2610	0	192.168	100	kernel mes	sages	Notice		Jan 01	15:04:29 1	92.168.100.	161	
system	,		2018-12-	25 09:14	2001	-01-01 1	5:04	dap2610	0	192.168	100	kernel mes	sages	Notice		Jan 01	15:04:29 1	92.168.100	161	
			2018-12-	25 09:14	2001	-01-01 1	5:04	dap2610	D	192.168	100	kernel mes	sages	Informati		Jan 01	15:04:16 1	92.168.100	161	
			2018-12-	25 09:01	2001	-01-01 14	4:51	dap2610	D	192.168	100	kernel mes	sages	Notice		Jan 01	14:51:36 1	92.168.100	161	
			2018-12-	25 09:01	2001	-01-01 14	4:51	dap2610	D	192.168	100	kernel mes	sages	Notice		Jan 01	14:51:36 1	92.168.100.	161	
			2018-12-	25 09:01	2001	-01-01 14	4:51	dap2610	0	192.168	100	kernel mes	sages	Notice		Jan 01	14:51:36 1	92.168.100.	161	
			2018-12-	25 09:01	2001	-01-01 14	4:51	dap2610	0	192.168	100	kernel mes	sages	Notice		Jan 01	14:51:35 1	92.168.100.	161	
			2018-12-	25 09:01	2001	-01-01 14	4:51	dap2610	0	192.168	100	kernel mes	sages	Notice		Jan 01	14:51:35 1	92.168.100.	161	
			2018-12-	25 04:36	2001	-01-01 10	0.26	dap2610	D	192.168	100	kernel mes	sages	Notice		Jan 01	10:26:25 1	92.168.100	161	
				1778 total													> >>	50 ~	items per	

Nuclias	Log	System Event Log
---------	-----	------------------

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

To generate a System Event Log report, select the event severity and define the period of time to report. Click the drop-down menu to choose either IP address or Message as report criteria. Fill in the keyword field and click 📷 to view the generated report.

< nuclias	Default					Trial (23 days), click to activate	EN
Dashboard		All Event Type 🗸 🗸	2018.12.18	m 2018.12	.25 mm	IP Address v Search 'Keyword'	B
Monitor	Loz Time	 Event Type 	 Network 	· IP Address ·	MAC Address?	Messare	
Configuration	> 2018-12-25 1	3:48:45 Invalid HTTP Mess	age			Reject an unknown message. JSON format error: SyntaxError: Unex.	
Report	2018-12-25 1	3:47:54 Invalid HTTP Mess	age			Reject an unknown message. JSON format error: SyntaxError: Unex.	
🗐 Log	2018-12-25 1	3:46:50 Invalid HTTP Mess	age			Reject an unknown message. JSON format error: SyntaxError: Unex.	
 SNMP Traps 	2018-12-25 0	19:14:40 Invalid HTTP Mess	age oxtest	192.168.100	00:26:10:12:	Reject an invalid message 'Client Disassociate' due to 'sta'loApRxDa.	
 Syslogs 	2018-12-25 0	19:14:40 Invalid HTTP Mess	age oxtest	192.168.100	00:26:10:12:	Reject an invalid message 'Client Disassociate' due to 'staToApRxDa.	-
System Event Log Device Log	2018-12-25 0	19:14:39 Invalid HTTP Mess	age oxtest	192.168.100	00:26:10:12:	Reject an invalid message 'Client Disassociate' due to "staToApRxDa.	-
_	2018-12-25 0	9:14:39 Invalid HTTP Mess	age cxtest	192.168.100	00:26:10:12:	Reject an invalid message 'Client Disassociate' due to 'staToApRxDa.	
System	2018-12-25 0	19:14:39 Invalid HTTP Mess	age oxtest	192.168.100	00:26:10:12:	Reject an invalid message 'Client Disassociate' due to 'staToApRxDa.	
	2018-12-25 0			192.168.100	00:26:10:12:	Reject an invalid message 'Client Disassociate' due to "staToApRxDa.	
	2018-12-25 0			192.168.100	00:26:10:12:	Reject an invalid message 'Client Disassociate' due to "sta'lloApRxDa.	
	2018-12-25 0			192.168.100	00:26:10:12:	Reject an invalid message 'Client Disassociate' due to "staToApRxDa.	
	2018-12-25 0			192.168.100	00:26:10:12:	Reject an invalid message 'Client Disassociate' due to 'staToApRxDa. Reject an invalid message 'Client Disassociate' due to 'staToApRxDa.	
	2018-12-25 0			192.168.100	00.26:10.12:	Reject an invalid message 'Client Disassociate' due to "staToApRxDa.	
	2018-12-24 2					Reject an unknown message. JSON format error: SyntaxError: Unex.	
	2018-12-24 2					Reject an unknown message. JSON format error: SyntaxError: Unex.	
	1 - 50 of 179	total items: 179				< 1 /4 > > 50 v items per	r page

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.

Log

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.

nuclias		Default						Trial (23 days), click to activate	8	× P
Dashboard		All Operation Ty	ipe i	2018.12.18	m	2018.12.25 💼	IP Address	✓ Search 'Keywor	ď	R G
Monitor	>	Log Time ~	Name	 IP Address 	MAC Address	Operation Type	< Result	 Log Details 		.
Configuration	>	2018-12-25 04:36:39	dap2610	192.168.100	00:26:10:12:	. Channel or IP Address C.		Channel. 2.4 GHz: 11, Cha	nnel. 5 GHz: 4	8
Report	•	2018-12-25 04:36:29	dap2610	192.168.100	00:26:10:12:	. Channel or IP Address C.		Channel. 2.4 GHz: 1, Chan	nel. 5 GHz: 48	
a Log	•	2018-12-25 02:12:47	dap2610	192.168.100	00:26:10:12:	. Channel or IP Address C.		Channel. 2.4 GHz: 11, Cha	nnel. 5 GHz: 4	8
SNMP Traps		2018-12-25 02:12:37	dap2610	192.168.100	00:26:10:12:	. Channel or IP Address C.		Channel. 2.4 GHz: 1, Chan	nel. 5 GHz: 48	
Syslogs		2018-12-25 02:03:15	dap2610	192.168.100	00:26:10:12.	. Channel or IP Address C.		Channel. 2.4 GHz: 11, Cha	nnel. 5 GHz: 4	8
System Event Log Device Log		2018-12-25 02:03:05	dap2610	192.168.100	00:26:10:12:	. Channel or IP Address C.		Channel. 2.4 GHz: 11, Cha	nnel. 5 GHz: 3	6
	,	2018-12-25 01:47:38	dap2610	192.168.100	00:26:10:12:	. Channel or IP Address C.		Channel. 2.4 GHz: 11, Cha	nnel. 5 GHz: 4	6
O System		2018-12-25 01:47:28	dap2610	192.168.100	00:26:10:12:	Channel or IP Address C.		Channel. 2.4 GHz: 11, Cha	nnel. 5 GHz: 3	6
		2018-12-25 01:44:31	dap2610	192.168.100	00:26:10:12:	. Channel or IP Address C.		Channel. 2.4 GHz: 6, Chan	nel. 5 GHz: 15	3
		2018-12-25 01:25:40	dap2610	192.168.100	00:26:10:12:	. Channel or IP Address C.		Channel. 2.4 GHz: 11. Cha	nnel. 5 GHz: 1	61
		2018-12-25 01:25:30	dap2610	192.168.100	00:26:10:12:	Channel or IP Address C.		Channel. 2.4 GHz: 1, Chan	nel. 5 GHz: 14	9
		2018-12-25 00:33:27	dap2610	192.168.100	00:26:10:12	. Channel or IP Address C.		Channel. 2.4 GHz: 6, Chan	nel. 5 GHz: 14	9
		2018-12-25 00:17:28	dap2610	192.168.100	00:26:10:12:	. Channel or IP Address C.		Channel. 2.4 GHz: 11, Cha	nnel. 5 GHz: 1	49
		2018-12-25 00:17:18	dap2610	192.168.100	00:26:10:12:	. Channel or IP Address C.		Channel. 2.4 GHz: 1, Chan	nel. 5 GHz: 15	3
		2018-12-24 21:22:50	dap2610	192.168.100	00:26:10:12:	Synchronize Device Se	Success	Configuration		
		2018-12-24 21:14:21	dap2610	192.168.100	00:26:10:12:	. Register Device	Success	otest		
		1 - 50 of 406 total Item	5: 406					1 /9 > »	so v iter	tis per page

System

Device Management

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

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.

< nuclias	Default Trial (4 days)	🐌 🔫 en v
C Dashboard	Retroots Manged Unmanged	e to Unmanaged
Configuration	ort ort Sutus v Local P Address v NAT P Address v MAC Address v Model Type v HW Westor v edmou,dze pref v 192.164.100.190 17/2217.182 Oct.5xe/3c/7500 DAP-2660 NA	FW Version
Log System Device Management User Management	eeee 192.244/300.396 377.222.77.1492 00.224/0.324570 0.44-2410 A1 test	v2.00
 Settings About 	¢	
	1-9042 total frame 2	v 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; o indicates a logged in state, while o 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 \mathbb{Z} . The username, password, email, priviledge, priviledge 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.

nuclias		Default								Trial (23 days),	click to	activate	ж	E
) Dashboard		All Users Tot	al Users 12 (🕹 3 🚜 S	4 0)								Add	User
Monitor	>	User Status	User Privilege											
Configuration	>	Username	✓ Email			Login Status 🗸	Role ~	Privilege Status	÷	Time of Creation	× 1	ast Login Time	~	Acti
Report	•	admin				•	Root admin	Enable		2018-12-18 12:04:25	2	018-12-25 15:25:37		
log		alpha				•	Root admin	Enable		2018-12-18 12:10:52	2	018-12-25 01:54:43		Ľ
System	•	edimax to ed				•	Root admin	Enable		2018-12-18 12:11:38	2	018-12-24 15:16:48		Ľ
Device Manageme	ent	test				٠	Root admin	Enable		2018-12-18 12:12:01	2	018-12-25 15:22:02		Ľ
User Management	t	novatest				•	Root admin	Enable		2018-12-18 12:12:23	2	018-12-24 15:25:41		Ľ
Settings		frontdesk				٠	Front des	Enable		2018-12-18 12:12:43	2	018-12-19 09:02:50		Ľ
About		fdesk				•	Front des	Enable		2018-12-18 13:34:35				Ľ
		2682-ft				٠	Front des	Enable		2018-12-19 10:09:10	2	018-12-19 14:31:25		Ľ
		1 - 10 of 12 ti	stal Items: 12								2)	» 10 v ite	ms per	page
											- C)			

User Privilege

Nuclias System User Management

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.

<nuclias< th=""><th>Default</th><th>Trial (4 days)</th><th>٩</th><th>× D</th><th>4 4</th></nuclias<>	Default	Trial (4 days)	٩	× D	4 4
Dashboard	All Users Total Users 8 (🌡 2 : 🌡 6 : 👗 0)			Add User	ľ
Monitor >	User Status User Privilege				1
X Configuration >	ctest Unauthorized Users Authorised Users				
Report >	edmax_site				
Log >	greet				
	test				
System ~	«				
Device Management	_				
User Management Settings					
About					

System

Settings

General

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 depanding 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.		

System

Settings

General

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

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

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.

C Deshboard	General Connection SMTP	Rackup Firmson Upgrafe System Operation Single-Sign-On (550)
Monitor >		1
X Configuration	Customized Setting	
Report >	Device Name	ph-100
E log >	Logo	
🕞 System 🗸 🗸		
Device Management		Drag & Drop Lago File Hars, or Drevour
User Management Settings		The lags lie must be in FMG or JPG image file formut
 Most 	Login Captcha	Enabled v
		Kee
		_
	LAN Settings	
	Get IP Address From	Startic IP Address (manual) ~
	17 Address*	192168.0.300 %.deet Mod* 255255.255.0
	Gateway	
	Primary DNS	Secondary DNS
		C Synchroniae Davies Access Address
		See .
	Date And Time	
	Time Zone	15MT) Greenwich Moon Time : Dublin, Editiourgh, Lidoon, Landon 🔍
		У нти У
	NTP Server 1	ngdullikuon
	NTP Server 2	P address/Comain name
		2009.135 📺 Capy New Computers Time
		05.20 AM
		Sour -
	Consule Setting	
	Consele	V twice
	Consist Protocol	Telect • 55H
	Timeout	5Mini v
		See
	Device Setting	
	Live Packet Interval	1Mn v
		See

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 inboud 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.

(1) × IN -

System

Settings

SMTP

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

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

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.

Cnuclias	dnh-100		(1) × IN -
Deskboard	Council Committee 1977	Backup / Firmware Upgrade System Operation Single Sign On (33C)	
Monitor >	Canada Connection 3MTP	Backup Periwari Uggade Syntem Operation Single Sign Ch (SSU)	
X Configuration	Customized Setting		
Report >	SMTP Host*	Hoat	
E log >	Port*	Pick one	
🖓 System 🗸 🗸	From Email Address'		
Device Management	From Name*		
User Management Settings			
+ About	Security Type	None v	
	Encoding Type	utria v	
	Authentication	Aeanymaus 🗸 🗸	
	Test Email	Text Eval Text	
		See	

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:

Auto Backup	Disabled	~	Recommend to use external syslog server to backup syslog if you want to keep syslog
External Syslog Server	IP address/Domain na		

Parameter	Description
Auto Backup	Click on drop-down list to enable or disable auto backup.
External Sylog 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.

My Hard Disk USB storage	
20190116_configuration.tar	
	 20170115_comparation.tar

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
То	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.

T Delete	\times
All Backup Files	
Delete Cancel	
	-

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.

Upload Configuration From	My Hard Disk USB storage	
File	Choose File	

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.

https://192.168.0.200/pr

System Settings

Firmware Upgrade

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.

Market > Market Market Market Market<	Weaking > Veaking >	General Connection SMTP Backup Fermover Uggende System Operation Single Signe On (SSO) ation > Uggende May Hard Diak > b Uggende Firmover Uggende Single Signe On (SSO) b Uggende Firmover Uggende Single Signe On (SSO) b Uggende Firmover Uggende Single Signe On (SSO)	General Connection MPP Backage Premove Uggade System Operation Sigle-Sign-Op (SOC) Monter >	Connection SetTP Booking Connection Connect	Model Connection MM Pile Bakkap Permaner Departe System Operation Sigle-Sign-On (SO)	<pre><nuclias connect<="" pre=""></nuclias></pre>	dnh-100	٩
Wather > Kather > Kather > Rapet > Part 2	Weaking > Veaking >	ation J Ation My Hard Disk J Bowwer J B	Mather Mather Configuration Report Depart Mather Mat	Q Mantar Q Mantar Q Mantar Q Mantar Q Mantar Papert	Montary >	Dashboard	General Conservice SMTP Barline Emmanal Journale Service Service Service Service (SST)	
Rpot It It It State Oxfore Oxfore Decke Maragement Username Oxfore State State Abad It	Report > Report > Bug > Porte Port	> File > File > File > File > File > File > Paraseed > File > File	Repot It top It top It top Poster Management Uber Management Uber Management Vor Management Abad Filmsare File Path and file rame	Pepert Pepert Pepert Peret	Rpart > Rpart > Bayer FRe Bayer FRe Porte Port Dorker Management Uor Management Dorker Management Dorker Management Senings Abard	Monitor >		
log Setter Bit of Setter • Decker Management Username • Decker Management Password • Decker Management Password • Settige Password • Abad Firmware File	Instant Instant Instant Instant Instant Instant Instant Unername Instant Unername Instant Instant Setting Instant Instant Setting Instant Instant	File Bowesc Port Data Port Data Suggement Datasende Parasend Data Parasende Data	Ing FR Browser Ing FR Browser Prefer FR Part 21 Browser Browser Prefer Username Part Ver Management Password AQ Setting Firmware File Path and file rame	Ing Pice System PFP Server Device Management Domanne Over Management Password Setting Abud	Ing Ing	X Configuration	Upload Firmware From My Hard Disk v	
System Fird Server: Fird Server: 21 Device Management Username 1 Vasc Maagement About Ressourd About Firmsure File Path and file name	FTP Server Port 21 Device Muagement Username 21 Var Mangement Rep 1 Abart Fernare File Rath and file name	Imponent Post 21 aggment Decrame Imponent Pressure Repression Imponent Firmware File Path and file name	System FPI Server Part 21 Deske Mangament Username 21 Userkand Password 20 Serings Firmware File Path and file name	System FTP Server Fort 21 Deske Management Utername Deske Management Passwerd App Settlegs App	System FITP Server Fut 21 Device Management Username 22 Var Management About Ressord About Firmware File Path and file name	Report >	File Browser	
Johan Usernane Decke Management Usernane User Management Password Setting Password Abod Firmsore File	Sprine V Derice Management Vermanne User Management Permont Setting About Finance Fize Puth and file name	Imagement Ucersame agement Pathword Termsame File Path and file mather	Optime Username Deske Management Username User Management Password Setting Password About Pinname File	System Versame Device Management Versame Settegs Passwerf lie Abut Firmware File	Josham Jumman Decke Management Jumman Uber Management Passwort Settings About	🖬 log >	FTP Server Port 21	
Decker Management User Management Settings About Firmware File Path and the name	Device Management Vere Management Vere Management Vere Management Settings About Fermaner File Public and file name	Augment Password Age Firmware File Path and file name	Decke Mangement User Mangement Sentage About Firmsore File Path and file rame	Device Management Personer User Management Personer Setting About About Firmmore File Path and file name	Deckor Management Voor Management Voor Management Password Pas	System ~		
Settings About Firmware File Path and file name	Settings About Firmware File Puth and file name	Fremoure File Path and file name	Setting Abod Firmware File Path and file name	Settings Openational Openational	Settings About Firmware File Path and file name		Username	
							Password &	
Apply						About		
	Andr						Andr	

System Operation Settings **Nuclias** System

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



to Reboot the DNH-100 immediately.

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

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

< nuclias	dnh-100	×	EN ~
() Dashboard	General Connection SMTP Backup Firmware Upgrade System Operation Single-Sign-On (SSO)		
Monitor >	ocicia coneccon ante pocup reinnae oggiae apoen operation ange agron (200)		
X Configuration	Rebot the Device Rebot		
Report >	Restore the Factory Default Restore Except IP address		
i log >	Format MicroSD card Format		
🗔 System 👻	Found Wickold Cald		
Device Management			
User Management			
 Settings 			
About			

Nuclias System Settings Single-Sign-On (SSO)

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

If you do not already have a Nuclias account, you can click on **Create acount** 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 reginoal server based on your selected region and country.

TEP 1	
elect server i	region and country.
within the	ccount and organization will be created on servers region selected. The customer service will be forwarde try you selected.
Serverre	egion
	-
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.

< ni	
novascriptor@gmail.com	
D-Link	
	¢
	C
D-Link Test	
Taiwan	
Asia/Taipei(UTC+08:00, 0	067)
No.1 Street Name, City N	ame, State, Country, ZIP

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.			

۲	onnect		dnh-100 (8	<	EN v
6	Dashboard		General Connection SMTP Backup Firmware Upgrade System Operation Single-Sign-Cn (SSO)			
	Monitor	>	онтва салескал энт р Балар глипае оррае зулял органол зарездуги (200			
×	Configuration	>	Single-Sign-On allows you to use one Nuclias account to access either Nuclias Cloud or Nuclias Connect portal :			
3	Report	>	Exable single sign on			
	Log	>	Nuclas Account*			
50	System	×	Nuclas Passoord* The length is between 8-64			
	Device Manageme					
	User Management Settings		Create account			
	About		Apply			

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: <u>https://connect.nuclias.com/</u>

	ASHBOARI								
						Type :	All 👻	Status : All	Q Search
#	Status	Name	Host	Sites	Networks	Devices	Clients	Version	Actions
1		dnh-100	172.17.5.225,61.220.144.151	1	1	0/0	0	1.0.0.10	C 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 About

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.

٩n	uclias	dnh-100		٩	×	EN ~
۵	Dashboard	System Information Model List				
	Monitor >					
×	Configuration >	Device Name :	dmb-100			
-		Firmware Version :	1007			
	Report >	Hardware Version :	LA L			
		Nuclias Connect Version :	1008			
5	Log	DDPv5 Client Version :	1006			
53		IP mode :				
			192.168.0.200			
	Device Management		255.255.255.0			
	User Management	Gateway :				
		DNS1 :				
1	Settings	DNS2 :				
	About	MAC Address :	ECAD:0:C12ECD			
			17.8G / 642.2M			
		MicroSD usage :				
		USB usage :	n/a			
		NTP :	Evabled, rdp1.dlink.com (The Time settings of this DNH-100 can not be detected correctly. Please ensure you have the correct network settings.)			
			2019-01-15 05:31:22			
		Timezone :	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London			
		Up Time :	13 days, 17 hours, 31 minutes			

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

<nuclias< th=""><th></th><th>dnh-100</th><th></th><th></th><th></th><th></th></nuclias<>		dnh-100				
Dashboard		System Information Model	1 let			
Monitor	,					Update Online
X Configuration	>	Model Type 🔺	 Band Type 	 HW Version 	~ Description	Chemic China
Report	>	DAP-2680	dual	A	Wireless AC1750 Wave 2 Dual-Band PoE Access Point	
Log	,					
System	Ų.					
Device Management User Management Settings About	t					
		1 - 20 of 1 total Beens: 1				(a) (x) (1) (x) (a) (2) (x) (green for both

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** (B) icon to export the network profile to your computer.

Central WiFiManager	Default	🕵 🔀 EN -
Dashboard	All SRes V Total 1. Networks Total 0/10 Online APs Total O Cliners	Add Network
Monitor >	Site Name * v Network Name * v Total Devices v Ortine Devices v Clients v Profie v Discovery v	Action ~
🗙 Configuration 🕞		R. D
Create Profile		
 Profile Settings 		
Firmware Upgrade SSL Certificate		
 Payment Gateway 		
Report >		
G System →		
	1-15 of 1 Total Rems 1	15 v items per page

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.

CWM Core server needs to be restarted If Device Access Address or Port has been changed. Device Access Address Device Access Port B443
Device Access Port 8443
CWM Web server needs to be restarted if Web Access Address or Port has been changed.
Web Access Address other v
Web Access Port 30001.
Save

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.

中華電信 4G 9:27 AM थ 64% ■⊃ く Quick Setup	
Constraints Constrain	The Provision file was not found or this device.
toropy, please go to the Nucleas Connect and follow the legs there to get a suitable AP Provision profile.	Download profile
	Cancel

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.

-ml中華電信 4G	9:27 AM Quick Setup	0 64% 🔳)
•	-0	0
STEP 1: Please select an A	P Provision Profile to pus	a to suitable
Access Points.		
Provision File	nuclias connect_tes	t_Network132 >
storage, please gr	suitable AP provision prot to the Nuclias Connect a a suitable AP Provision p	and follow the



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

Ca	ncel	Select AP Provision file	Done
1	nucli	as connect_test_Network132	

The process will continue and the App wil 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 ($^{\oplus}$) to create a new IP range entry. Tap remove (\bigcirc) 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.

-ml中華電信 4/	3 9:2 Quick	^{B AM} Setup	،	64% 💶 🤇
-		_		-0
STEP 2:				
Discover sta wireless net	ndalone Access P vorks	oints in	L2/L3	
L2				
L3				õ
🤣 From	192.168.1.50	to	192.168.1.20	0 0
	④ Add an	IP Ra	inge	

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.

all中華電信	♀ 9:49 AM	0 61% 🔳
	Quick Setup	5
		-
STEP 3		
Check th the Acce	e settings for each Access Point below th ss Points you want to push the provision	nen select file to.
Discover	ed AP List	•
	Access Point Login	
O DA	Access Fork Login	166 >:10
	Password	
	Apply To All Selected Access Points	
		1
	Cancel	J.
	Push Provision File	

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.

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	t 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.

山中華電信 🗢	9:49 AM	0 61% 🗖
<	Quick Setup	5
•	-	
STEP 3:		
	is for each Access Point b s you want to push the pro	
Discovered AP Lis	st	۵ ک
DAP-2662		192.168.1.166
v1.00		1:ca:cc:99:10

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.

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.

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



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



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

Standalone Access Point

Discover 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.

00

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.

2



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.

all 中華電台	19	9:48 AM	ŭ	61% 💷
	Push Access Point Configuration			3
	Ali	Standalone Access Point	Managed Access	
Discover	red AP List		\oslash	
	P-2662	00	192.168.1.1 (taatcatoo:99	
	Access	Point Login 192	2.168.1.166 xcaxcc:99:10	
			۲	
		Apply		
		Cancel		
		Push Configuration		

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.

I中華電信 중 Cancel	9:48 AM DAP-2680	o 61% Done	
IP Info	Wireless	Client	
Model Name		DAP-2680	
MAC	00:aa:ca:cc:99:10		
DHCP Mode		0	
IP Address	192.168.1.166 >		
Subnet Mask	3	255.255.255.0 >	
Default Gateway		192.168.1.1 >	
DNS		0.0.0.0 >	

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, 80211g and 802.11b; Mixed 802.11g, 802.11b; 802.11n Only.			
Radio 5G Mode	Tap to select a specific 5G radio mode: Mixed 802.11n, 80211a; 802.11a Only; 802.11n; Mixed 802.11ac.			
Country Code	Displays the assigned country designation for the 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.			

না। হ Cancel	4:27 РМ DAP-2680	99% —
IP Info	Wireless	Client
DAP-2680		192.168.1.166 40:9b:cd:0c:66:20
2.4G SSID		
SSID-1		
SSID Name		dlink
Security		Open System
SSID-2		\bigcirc
SSID-3		\bigcirc
5G SSID		
SSID-1		
SSID Name		dlinkiii
Security		Open System
SSID-2		\bigcirc

ul ô		4:27 PM	99% 🥅
	Cancel	DAP-2680	
	IP Info	Wireless	Client
	SSID-1		
	SSID Name		dlinkiii
	Security		Open System
	SSID-2		\bigcirc
	SSID-3		\bigcirc
	Wireless Information		
	Radio Band		2.4G \ 5G
	Radio 2.4G Mod	e Mixed 802.11n,	802.11g and 8
	Radio 5G Mode		Mixed 802.11ac
	Country Code		United States
	Copy & Save Config	uration	
	Apply Configura	tion	>
	Save Configurat	ion	>