

NUCLIAS CONNECT DAP-2720 User Guide

V 1.00

Table of Contents

Nuclias Connect	4	Wireless Resource	26
Introduction	4	Multi-SSID.....	28
Nuclias Connect Key Features.....	5	VLAN.....	30
Package Contents.....	6	VLAN List.....	30
System Requirements.....	6	Port List.....	31
Hardware Overview.....	7	Add/Edit VLAN	32
LEDs.....	7	PVID Settings.....	33
Connections	7	Intrusion.....	34
Basic Installation	8	Schedule	35
Hardware Setup	8	Internal RADIUS Server.....	36
Configure the access point.....	8	ARP Spoofing Prevention	37
Setup Wizard.....	9	Bandwidth Optimization	38
Web User Interface	10	Captive Portal.....	40
Wireless	11	Authentication Settings-Web Redirection Only	40
Access Point Mode	11	Authentication Settings- Username/Password..	42
WDS with AP Mode.....	13	Authentication Settings- Passcode	44
WDS Mode	15	Authentication Settings- Remote RADIUS.....	47
Wireless Client Mode.....	17	Authentication Settings- LDAP.....	49
Wireless Security	18	Authentication Settings- POP3.....	51
Wired Equivalent Privacy (WEP)	18	Login Page Upload	53
Wi-Fi Protected Access (WPA / WPA2).....	19	MAC Bypass.....	54
LAN	21	DHCP Server	55
IPv6	22	Dynamic Pool Settings.....	55
Advanced Settings.....	23	Static Pool Setting	56
Performance	24	Current IP Mapping List.....	58
		Filters.....	59

Wireless MAC ACL.....	59	Country Setting	79
WLAN Partition	60	Nuclias Connect Settings.....	79
IP Filter Settings.....	61	Firmware and SSL Upload.....	80
Traffic Control.....	62	Configuration File Upload	81
Uplink/Downlink Setting	62	Time and Date Settings	82
QoS.....	63	Configuration and System.....	83
Traffic Manager.....	64	System Settings.....	84
Status	65	Help	85
Device Information	66	Technical Specifications	86
Client Information	67	Antenna Pattern	87
WDS Information Page	68	Power Usage.....	89
Channel Analyze	69		
Statistics.....	70		
Ethernet Traffic Statistics.....	70		
WLAN Traffic Statistics.....	71		
Log	72		
View Log.....	72		
Log Settings.....	73		
Maintenance Section	75		
Administration.....	76		
Limit Administrator	76		
System Name Settings.....	77		
Login Settings	77		
Console Settings	77		
SNMP Settings.....	78		
Ping Control Setting	78		
LED Settings.....	78		
DDP Setting	79		
Router Settings.....	79		

Nuclias Connect 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 of up to 1,000 Access Points (APs), while retaining a robust and centralized management system. 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.

Deployable on a Windows server (or Linux via Docker), PC, or Smartphone (via lite management app) the Nuclias Connect free-to-download software is capable of managing up to 1,000 APs without licensing charges, coupled with an inexpensive optional hardware controller (DNH-100 Nuclias Connect Hub) suitable for remote locations. Through software-based monitoring and remote management of all wireless Access Points (APs) on your network, Nuclias Connect offers tremendous flexibility compared to traditional hardware-based unified management systems. Configuration can be done remotely. Network traffic analytics are available at a glance (in whole or in part). Load Balancing, Airtime Fairness, and Localized Throttling are enabled.

Nuclias Connect supports multi-tenancy, so network administrators can grant localized management authority for local networks. In addition, because APs can support 8 SSIDs per radio (Total 24 SSIDs for DAP-2720), administrators have the option of using one SSID to create a guest network for visitors.

Nuclias Connect provides direct AP discovery and provisioning when it shares the same Layer-2/Layer-3 network with a given AP, allowing users to find APs and import profiles with minimum effort, which can be applied as needed to groups or individual APs for even more effective configuration.

Since Nuclias Connect's software operates transparently on the network, an AP can be deployed anywhere in an NAT environment. Admins can provide and manage a variety of distributed deployments, including settings and admin account configuration for each deployment.

Nuclias Connect allows for multiple user authentications while enabling specific access control configurations for each SSID, giving admins the option of configuring separate internal networks for different subnets, while enabling more advanced Value-Added Services, such as Captive Portal or Wi-Fi Hotspot.

Nuclias Connect Key Features

- Free-to-Download Management Software
- Searchable Event Log and Change Log
- License-Free Access Points
- Traffic Reporting & Analytics
- Authentication via Customizable Captive Portal, 802.1x and RADIUS Server, POP3, LDAP
- Remote Config. & Batch Config.
- Multilingual Support
- Intuitive Interface
- Multi-Tenant & Role-Based Administration
- Payment Gateway (PayPal) Integration and Front-Desk Ticket Management

For more information on how to use Nuclias Connect with the DAP-2720, please refer to the Nuclias Connect User Guide.

Package Contents

- DAP-2720 802.11ac Power over Ethernet (PoE) Access Point
- Mounting Brackets
- Ceiling Brackets
- Quick Setup Guide

Note: No PSU supplied. To power the units use a D-Link 802.3at PoE switch or the D-Link DPE-301GI PoE injector.

System Requirements

- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet Adapter
- Internet Explorer 11, Safari 7, Firefox 28, or Google Chrome 33 and above (for configuration)

Hardware Overview

LEDs



Connections



1	Power/Status	Solid Red	Indicates the access point has malfunctioned.
		Blinking Red	This LED will blink during boot-up.
		Solid Green	Indicates that the DAP-2720 is working properly.

2	Power Receptor	Connect the supplied power adapter. (*Note: no longer used, replaced by PoE)
3	LAN (PoE) Port	Connect to a Power over Ethernet (PoE) switch or router via an Ethernet cable.
4	Reset	Reset button for reset to factory default.

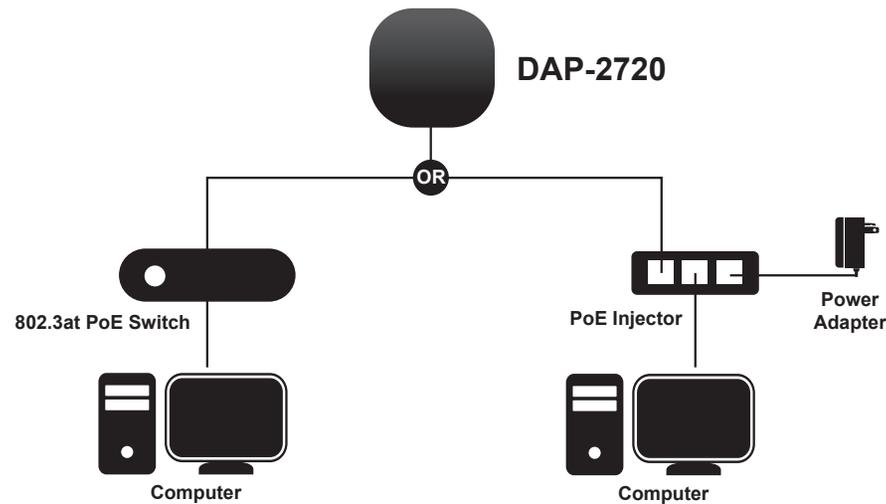
Basic Installation

Hardware Setup

To power on the DAP-2720, you can use ONE of the following methods:

1. Plug one end of your Ethernet cable into the LAN port of the DAP-2720, and the other end into a port on a 802.3at PoE switch.
2. Purchase a DPE-301GI PoE injector separately if you need to connect the access point without a 802.3at PoE Switch.

Configure the access point



To set up and manage the DAP-2720, use one of the following methods:

1. Connect the access point and your computer to the same PoE switch. Manage the access point from the computer.

Enter **dap2720.local** in the address field of your browser.

Log in to the Administration Web pages. The default login information is:

Username: **admin**

Password: **admin**

2. Connect the access point and your computer via DPE-301GI PoE injector. Manage the access point from the computer.

Enter **dap2720.local** in the address field of your browser.

Log in to the Administration Web pages. The default login information is:

Username: **admin**

Password: **admin**

Setup Wizard

The first login instance displays the System Settings window which requires a change in password. Additional settings include the System Time and System Country functions.

After logging in to the user interface, fill in the New Password and Confirm New Password fields.

In the System Time function, select **Using Network Time Protocol (NTP)** or **Manually** to define the system time. If required, click the Daylight Saving Offset drop-down menu and select the value (minutes).

- Setting NTP System Time: Before trying to configure NTP check, perform a ping test with the NTP server. In the NTP Server field, enter the NTP server to use. Then click the Time Zone drop-down menu and select the appropriate time zone.
- Setting System Time Manually: From the System Date drop-down menu, select the Year, Month, and Day along with the Hour and Minutes appropriate for the AP.
- Enable Daylight Saving: Click the radio button to enable the daylight savings time (DST) function. Set the DST start (24 hours) and end (24 hours) time by clicking on the drop-down menus and setting the Month, Week, Day, Hour, and Minute of the DST starting days.

Once the settings are configured, click **Update** button to accept the configuration and proceed to the main interface menu page.

PROVIDE SYSTEM SETTINGS ...

These settings apply to this access point.

New Password

Confirm New Password

System Time Using Network Time Protocol(NTP)
 Manually

System Date

System Time(24 HR) :

Enable Daylight Saving

DST Start(24 HR) in at

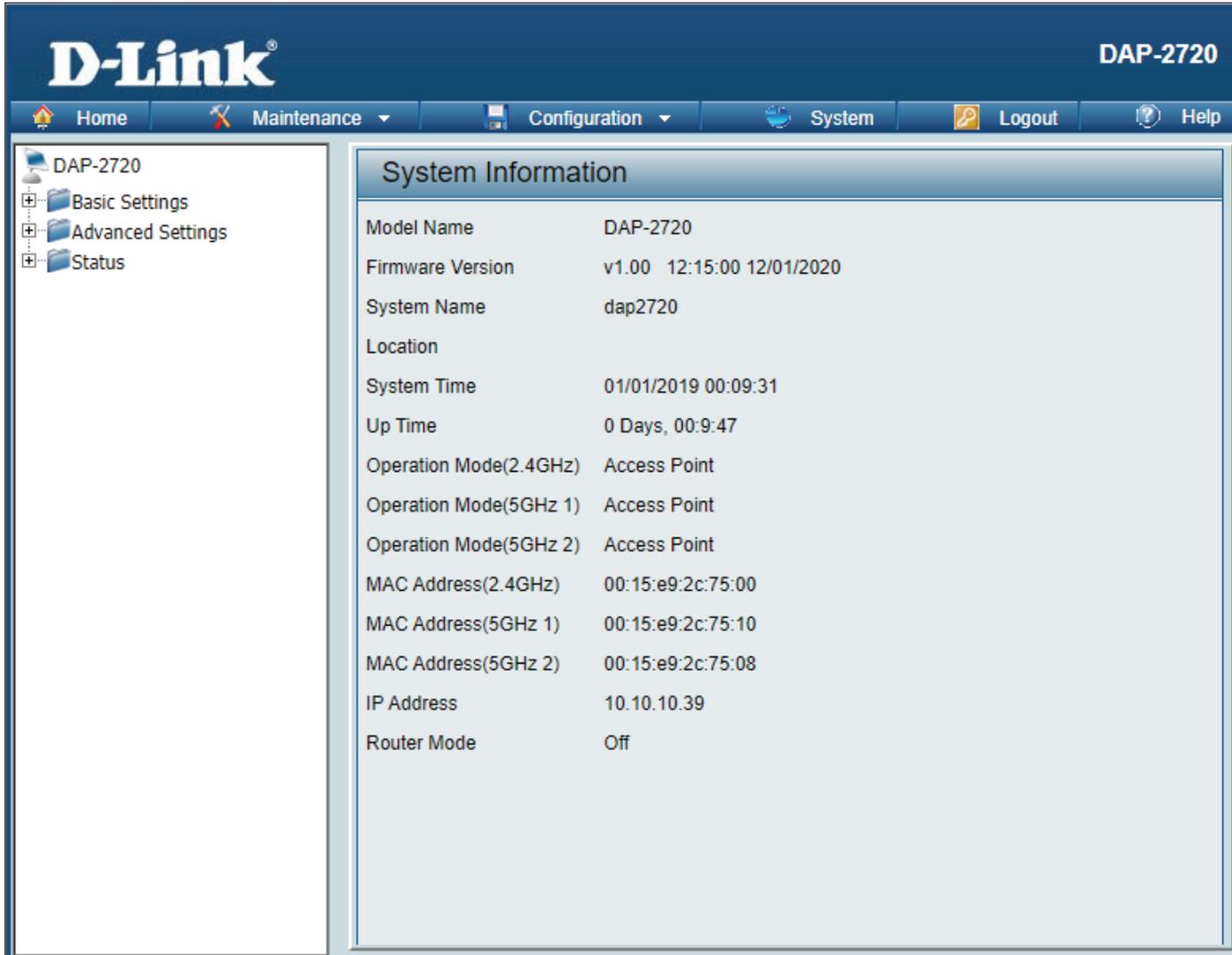
DST End(24 HR) in at

Daylight Offset(minutes)

System Country

Web User Interface

The DAP-2720 supports an elaborate web user interface where the user can configure and monitor the device. Launch a web browser, type **dap2720.local** in the address field and then press Enter to login. Most of the configurable settings are located in the left menu of the web GUI which contains sections called **Basic Settings**, **Advanced Settings** and **Status**.



The screenshot displays the D-Link DAP-2720 web user interface. The top navigation bar includes the D-Link logo, the device name "DAP-2720", and menu items: Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view with "DAP-2720" expanded, containing "Basic Settings", "Advanced Settings", and "Status". The main content area is titled "System Information" and lists the following details:

Model Name	DAP-2720
Firmware Version	v1.00 12:15:00 12/01/2020
System Name	dap2720
Location	
System Time	01/01/2019 00:09:31
Up Time	0 Days, 00:9:47
Operation Mode(2.4GHz)	Access Point
Operation Mode(5GHz 1)	Access Point
Operation Mode(5GHz 2)	Access Point
MAC Address(2.4GHz)	00:15:e9:2c:75:00
MAC Address(5GHz 1)	00:15:e9:2c:75:10
MAC Address(5GHz 2)	00:15:e9:2c:75:08
IP Address	10.10.10.39
Router Mode	Off

Wireless

On the wireless settings page, you can set up the basic wireless configuration for the access point. The user can choose from 4 different wireless modes:

Access Point - Used to create a wireless LAN

WDS with AP - Used to connect multiple wireless networks while still functioning as a wireless access point

WDS - Used to connect multiple wireless networks

Wireless Client - Used when the access point needs to act as a wireless network adapter for an Ethernet enabled device

Access Point Mode

Wireless Band: Select **2.4GHz or 5GHz 1 or 5GHz 2** from the drop-down menu.

Mode: Select **Access Point** from the drop-down menu.

Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. The SSID can be up to 32 characters and is case-sensitive.

SSID Visibility: Select **Enable** to broadcast the SSID across the network, thus making it visible to all network users. Select **Disable** to hide the SSID from the network.

Auto Channel Selection: This feature when enabled automatically selects the channel that provides the best wireless performance. The channel selection process only occurs when the AP is booting up. To manually select a channel, set this option to **Disable** and select a channel from the drop-down menu.



Channel: To change the channel, first toggle the *Auto Channel Selection* setting to **Disable**, and then use the drop-down menu to make the desired selection.

Note: *The wireless adapters will automatically scan and match the wireless settings.*

Channel Width: Allows you to select the channel width you would like to operate in 2.4GHz and 5GHz. Use the drop-down menu to choose **20 MHz** or **Auto 20/40 MHz** or **Auto 20/40/80 MHz**.

Authentication: Click the drop-down menu to select **Open System**, **Shared Key**, **WPA-Personal**, **WPA-Enterprise**, or **802.1X**.

- . Select **Open System** to communicate the key across the network (WEP).
- . Select **Shared Key** to limit communication to only those devices that share the same WEP settings. If multi-SSID is enabled, this option is not available.
- . Select **WPA-Personal** to secure your network using a password and dynamic key. No RADIUS server is required.
- . Select **WPA-Enterprise** to secure your network with the inclusion of a RADIUS server.
- . Select **802.1X** if your network is using port-based Network Access Control.

WDS with AP Mode

Wireless Band: Select **2.4GHz** or **5GHz 1** or **5GHz 2** from the drop-down menu.

Mode: WDS with AP mode is selected from the drop-down menu.

Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

SSID Visibility: Enable or Disable SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.

Auto Channel Selection: Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is not supported in WDS with AP mode. The channel selection process only occurs when the AP is booting up.

Channel: All devices on the network must share the same channel. To change the channel, use the drop-down menu to make the desired selection. (Note: The wireless adapters will automatically scan and match the wireless settings.)

Channel Width: Allows you to select the channel width you would like to operate in 2.4GHz and 5GHz. Use the drop-down menu to choose 20 MHz or Auto 20/40 MHz or Auto 20/40/80 MHz.

The screenshot shows the 'Wireless Settings' configuration interface. The 'Wireless Band' is set to '2.4GHz', 'Mode' is 'WDS with AP', and 'Network Name (SSID)' is 'dlink'. 'Auto Channel Selection' is 'Enable', 'Channel' is '6', and 'Channel Width' is '20 MHz'. The 'AP MAC Address' field is empty. The 'Site Survey' section has a 'Scan' button and a table with columns: CH, RSSI, BSSID, Security, and SSID. The 'Authentication' section is set to 'Open System'. The 'Key Settings' section has 'Encryption' set to 'Disable', 'Key Type' set to 'HEX', 'Key Index(1~4)' set to '1', and 'Key Size' set to '64 Bits'. There are input fields for 'Network Key' and 'Confirm Key' with a validation hint: '(0-9,a-z,A-Z,~!@#\$\$%^&*()_+`-={}|:~\|,./<>?)'. A 'Save' button is at the bottom right.

AP MAC Address: Enter the MAC addresses of the APs on your network that will serve as bridges to wirelessly connect multiple networks.

Site Survey: Click on the **Scan** button to search for available wireless networks, then click on the available network that you want to connect with.

Authentication: Use the drop-down menu to choose **Open System** or **WPA-Personal**.

- Select Open System to communicate the key across the network.
- Select WPA-Personal to secure your network using a password and dynamic key changes. No RADIUS server is required.

WDS Mode

Wireless Band: Select 2.4GHz or 5GHz 1 or 5GHz 2 from the drop-down menu.

Mode: WDS is selected from the drop-down menu.

Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

SSID Visibility: Enable or Disable SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.

Auto Channel Selection: Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is not supported in WDS mode.

Channel: All devices on the network must share the same channel. To change the channel, use the drop-down menu to make the desired selection.

Channel Width: Allows you to select the channel width you would like to operate in 2.4GHz and 5GHz. Use the drop-down menu to choose 20 MHz or Auto 20/40 MHz or Auto 20/40/80 MHz.

AP MAC Address: Enter the MAC addresses of the APs on your network that will serve as bridges to wirelessly connect multiple networks.

Wireless Settings

Wireless Band: 2.4GHz ▾
 Mode: WDS ▾
 Network Name (SSID): dlink
 Auto Channel Selection: Enable ▾
 Channel: 6 ▾
 Channel Width: Auto 20/40 MHz ▾
 AP MAC Address:

Site Survey

CH	RSSI	BSSID	Security	SSID
Scan				

Authentication: Open System ▾

Key Settings

Encryption: Disable Enable
 Key Type: HEX ▾ Key Size: 64 Bits ▾
 Key Index(1~4): 1 ▾
 Network Key:
 Confirm Key:
 (0-9,a-z,A-Z,~!@#%^&*()_+`-={}|:~\|,./<>?)

Save

Site Survey: Click on the **Scan** button to search for available wireless networks, then click on the available network that you want to connect with.

Authentication: Use the drop-down menu to choose **Open System** or **WPA-Personal**.

- Select Open System to communicate the key across the network.
- Select WPA-Personal to secure your network using a password and dynamic key changes. No RADIUS server is required.

Wireless Client Mode

Wireless Band: Select 2.4GHz or 5GHz 1 or 5GHz 2 from the drop-down menu.

Mode: Wireless Client is selected from the drop-down menu.

Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is dlink. The SSID can be easily changed to connect to an existing wireless network.

SSID Visibility: This option is unavailable in Wireless Client mode.

Auto Channel Selection: This option is unavailable in Wireless Client mode.

Channel: This option is unavailable in Wireless Client mode.

Channel Width: This option is unavailable in Wireless Client mode.

Site Survey: Click on the **Scan** button to search for available wireless networks, then click on the available network that you want to connect with.

Authentication: Use the drop-down menu to choose **Open System** or **WPA-Personal**.

- Select **Open System** to communicate the key across the network.
- Select **WPA-Personal** to secure your network using a password and dynamic key changes. No RADIUS server is required.

Wireless Settings

Wireless Band: 2.4GHz

Mode: Wireless Client

Network Name (SSID): dlink

SSID Visibility: Enable

Auto Channel Selection: Enable

Channel: 1

Channel Width: Auto 20/40 MHz

Site Survey

CH	Signal	BSSID	Security	SSID	
<input type="radio"/>	1	78%	00:21:91:84:DD:69	WEP	DAP-1522
<input type="radio"/>	1	100%	00:18:02:6D:B2:E0	OPEN	kay2553
<input type="radio"/>	1	100%	00:21:91:4F:7A:70	OPEN	dlink
<input type="radio"/>	1	62%	00:22:80:F8:4F:FF	OPEN	6666-P
<input type="radio"/>	2	64%	00:05:5D:35:20:64	OPEN	dlink
<input type="radio"/>	2	78%	00:18:84:A5:23:3D	OPEN	FON_Key

Authentication: Open System

Key Settings

Encryption: Disable Enable

Key Type: HEX Key Size: 64 Bits

Key Index(1~4): 1

Network Key:

Confirm Key:

Wireless MAC Clone

Enable:

MAC Source: Auto

MAC Address: : : : : : :

MAC Address

Wireless Security

Wireless security is a key concern for any wireless network installed. Unlike any other networking method wireless networks will broadcast its presence for anyone to connect to it. Today, wireless security has advanced to a level where it is virtually impenetrable. There are mainly two forms of wireless encryption and they are called Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP was the first security method developed. It is a low level encryption but better than no encryption. WPA is the newest encryption standard and with the advanced WPA2 standard wireless networks have finally reach a point where the security is strong enough to give users the peace of mind when installing wireless networks.

Wired Equivalent Privacy (WEP)

WEP Open System will send a request to the access point and if the key used matches the one configured on the access point, the access point will return a success message back to the wireless client. If the key does not match the one configured on the access point, the access point will deny the connection request from the wireless client.

Encryption: Use the radio button to disable or enable encryption.

Key Type: Select HEX** or ASCII*.

Key Size: Select 64 Bits or 128 Bits.

Key Index (1-4): Select the 1st through the 4th key to be the active key.

Key: Input up to four keys for encryption. You will select one of these keys in the Key Index drop-down menu.

**Hexadecimal (HEX) digits consist of the numbers 0-9 and the letters A-F.

*ASCII (American Standard Code for Information Interchange) is a code that represents English letters using numbers ranging from 0-127.

The screenshot shows the 'Wireless Settings' window. The 'Key Settings' section is expanded, showing the following configuration:

- Encryption: Enable
- Key Type: HEX
- Key Size: 64 Bits
- Key Index(1~4): 1
- Network Key: [Masked]
- Confirm Key: [Masked]

Wi-Fi Protected Access (WPA / WPA2)

The WPA protocol is based on the 802.11i standard. WPA offers two variations called WPA-Personal (PSK) and WPA-Enterprise (EAP). WPA-EAP requires the user to install a Radius Server on the network for authentication, while WPA-Personal does not. In comparison, WPA-PSK is seen as a weaker authentication variation than WPA-EAP. WPA-EAP is the highest level of wireless security a user can use for wireless today. WPA2 is an upgrade of WPA and solves security issues found in WPA. WPA2 also offers two variations called WPA2-Personal (PSK) and WPA2-Enterprise (EAP) similar to WPA.

WPA Mode: When **Authentication** setting is set to **WPA Personal**, click the drop-down menu to select one of the following: **Auto (WPA or WPA2)**, **WPA2 Only**, or **WPA Only**.

Auto (WPA or WPA2) allows the device to select either setting to match the client configuration.

Cipher Type: Click the drop-down menu to select the cipher type for the WPA setting, type: **Auto**, **AES**, or **TKIP**.

Group Key Update Interval: Enter the interval period in seconds in which the interval period is valid.

Encryption key: Select the method to define the cipher type encryption key: **Manual** or **Periodical Key Change**.
Manual: Enter the PassPhrase encryption key. The minimum and maximum number of characters is 8 to 63 ASCII characters and 64 characters in HEX. In the Confirm PassPhrase field enter the same key to confirm.

Periodical Key Change: Select the option to have each client negotiate a unique encryption key between the client and the access point.

Wireless Settings

Wireless Band: 2.4GHz

Mode: Access Point

Network Name (SSID): dlink

SSID Visibility: Enable

Auto Channel Selection: Enable

Channel: 6

Channel Width: 20 MHz

Authentication: WPA-Personal

PassPhrase Settings

WPA Mode: AUTO (WPA or WPA2)

Cipher Type: Auto Group Key Update Interval: 3600 (Sec)

Manual Periodical Key Change

Activated From: Sun : 00 : 00

Time Interval: 1 (1~168)hour(s)

PassPhrase:

Confirm PassPhrase:

notice: 8~63 in ASCII or 64 in Hex.
(0-9,a-z,A-Z,~!@#\$\$%^&*()_+`-={}|;'\:|,./<>?)

Save

WPA Mode: When WPA-Enterprise is selected, you must also select a WPA mode from the drop-down menu: AUTO (WPA or WPA2) or WPA2 Only.

Cipher Type: When WPA-Enterprise is selected, you must also select a cipher type from the drop-down menu: Auto, AES, or TKIP.

Group Key Update Interval: Select the interval during which the group key will be valid. 3600 is the recommended value as a lower interval may reduce data transfer rates.

Network Access Protection: Enable or disable Microsoft Network Access Protection.

RADIUS Server: Enter the IP address of the RADIUS server to be used in authenticate.

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the shared secret to be used between the radius server and the DAP to authenticate.

Accounting Mode: Click the drop-down menu to enable or disable the accounting mode.

Accounting Server: Enter the IP address of the accounting server.

Accounting Port: Enter the accounting port.

Accounting Secret: Enter the accounting secret.

The screenshot shows the 'Wireless Settings' configuration interface. The 'Authentication' is set to 'WPA-Enterprise'. Under 'RADIUS Server Settings', the 'WPA Mode' is 'AUTO (WPA or WPA2)', 'Cipher Type' is 'Auto', and 'Group Key Update Interval' is '3600 (Sec)'. The 'Network Access Protection' is set to 'Disable'. The 'RADIUS Server Mode' is set to 'External'. The 'Primary RADIUS Server Setting' includes fields for 'RADIUS Server', 'RADIUS Port' (1812), and 'RADIUS Secret'. The 'Backup RADIUS Server Setting (Optional)' also includes fields for 'RADIUS Server', 'RADIUS Port' (1812), and 'RADIUS Secret'. The 'Primary Accounting Server Setting' includes fields for 'Accounting Server', 'Accounting Port' (1813), and 'Accounting Secret'. The 'Backup Accounting Server Setting (Optional)' also includes fields for 'Accounting Server', 'Accounting Port' (1813), and 'Accounting Secret'. A 'Save' button is located at the bottom right of the configuration area.

LAN

LAN is short for Local Area Network. This is considered your internal network. These are the IP settings of the LAN interface for the DAP-2720. These settings may be referred to as private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

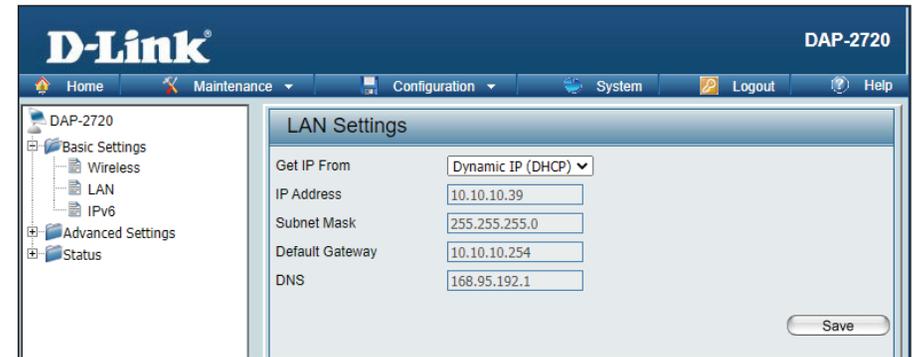
Get IP From: **Dynamic IP (DHCP)** is chosen here. Choose this option if you have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2720. When **Dynamic IP (DHCP)** is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

IP Address: Assign a static IP address that is within the IP address range of your network.

Subnet Mask: Enter the subnet mask. All devices in the network must share the same subnet mask.

Default Gateway: Enter the IP address of the gateway/router in your network.

DNS: Enter a DNS server IP address. This is usually the local IP address of your gateway/router.



IPv6

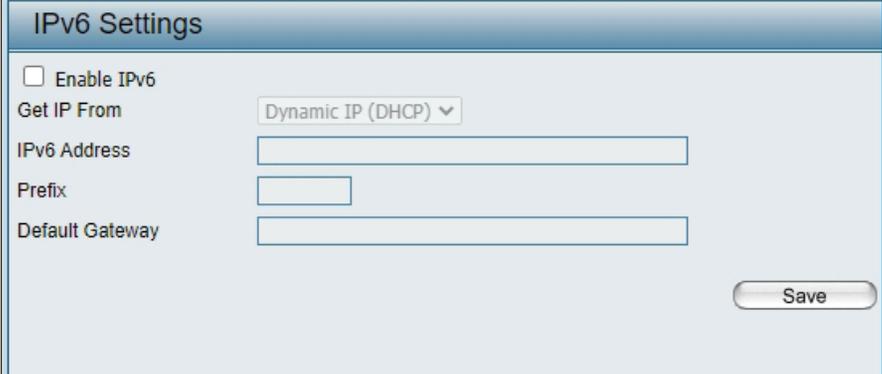
Enable IPv6: Check to enable IPv6

Get IP From: Dynamic IP is chosen here. Choose this option the DAP-2720 can get IPv6 address automatically or use Static to set IPv6 address manually. When **Auto** is selected, the other fields here will be grayed out.

IPv6 Address: Enter the LAN IPv6 address used here.

Prefix: Enter the LAN subnet prefix length value used here.

Default Gateway: Enter the LAN default gateway IPv6 address used here.

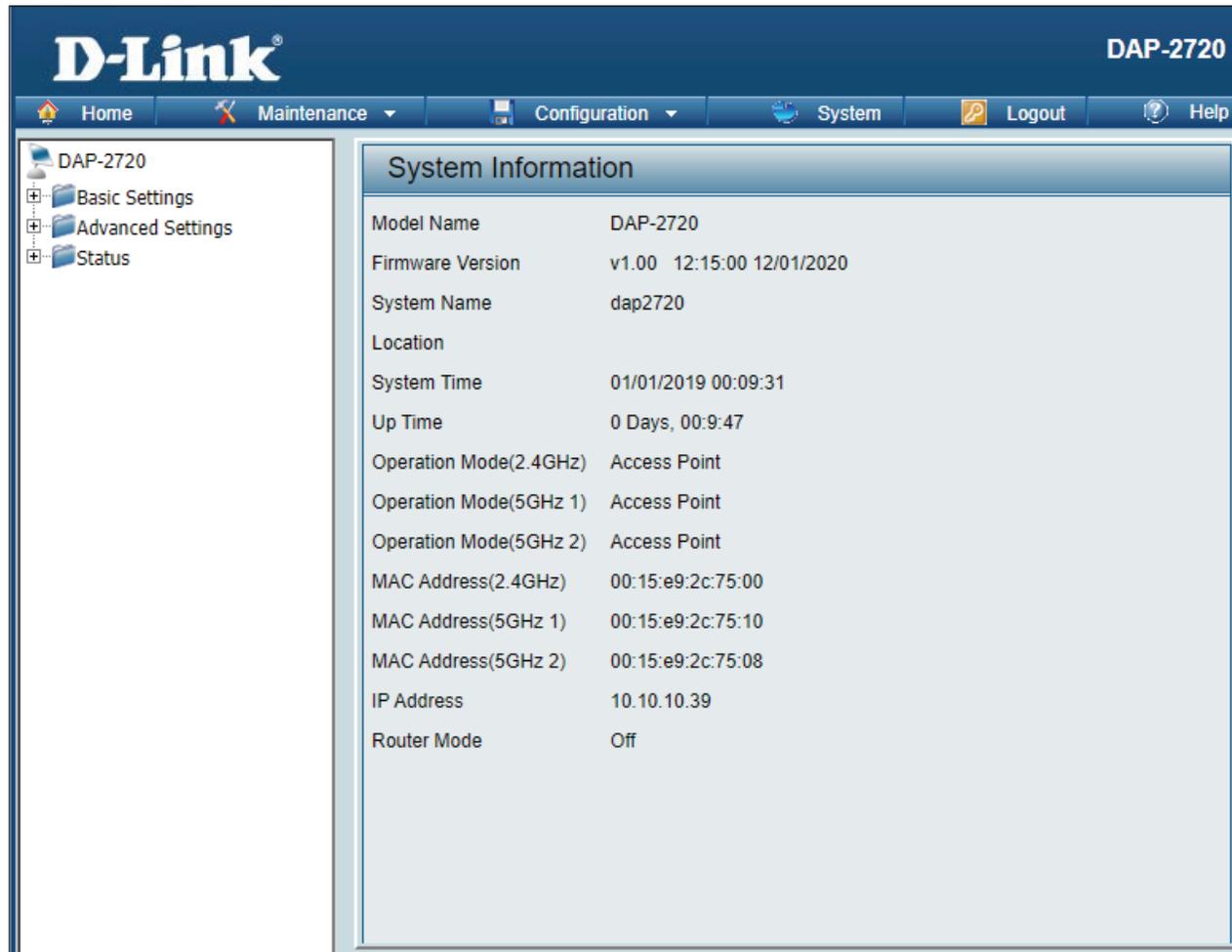


The screenshot shows a configuration window titled "IPv6 Settings". It contains the following elements:

- An unchecked checkbox labeled "Enable IPv6".
- A dropdown menu labeled "Get IP From" with "Dynamic IP (DHCP)" selected.
- A text input field labeled "IPv6 Address".
- A text input field labeled "Prefix".
- A text input field labeled "Default Gateway".
- A "Save" button in the bottom right corner.

Advanced Settings

In the Advanced Settings Section the user can configure advanced settings concerning Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, Captive Portal, DHCP Server, Filters and Traffic Control. The following pages will explain settings found in the Advanced Settings section in more detail.



The screenshot displays the D-Link DAP-2720 web interface. The top navigation bar includes Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view with DAP-2720, Basic Settings, Advanced Settings, and Status. The main content area is titled "System Information" and contains the following details:

Model Name	DAP-2720
Firmware Version	v1.00 12:15:00 12/01/2020
System Name	dap2720
Location	
System Time	01/01/2019 00:09:31
Up Time	0 Days, 00:9:47
Operation Mode(2.4GHz)	Access Point
Operation Mode(5GHz 1)	Access Point
Operation Mode(5GHz 2)	Access Point
MAC Address(2.4GHz)	00:15:e9:2c:75:00
MAC Address(5GHz 1)	00:15:e9:2c:75:10
MAC Address(5GHz 2)	00:15:e9:2c:75:08
IP Address	10.10.10.39
Router Mode	Off

Performance

On the Performance Settings page the users can configure more advanced settings concerning the wireless signal and hosting.

Wireless Band: Select 2.4GHz or 5GHz 1 or 5GHz 2.

Wireless: Use the drop-down menu to turn the wireless function On or Off.

Wireless Mode: The different combination of clients that can be supported include Mixed 802.11n, 802.11g and 802.11b, Mixed 802.11g and 802.11b and 802.11n Only in the 2.4 GHz band and Mixed 802.11ac, Mixed 802.11n, 802.11a, 802.11a only, and 802.11n Only in the 5 GHz band. Please note that when backwards compatibility is enabled for legacy (802.11a/g/b) clients, degradation of 802.11n wireless performance is expected.

Data Rate*: Indicate the base transfer rate of wireless adapters on the wireless LAN. The AP will adjust the base transfer rate depending on the base rate of the connected device. If there are obstacles or interference, the AP will step down the rate. This option is enabled in Mixed 802.11g and 802.11b mode (for 2.4 GHz) and 802.11a only mode (for 5 GHz). The choices available are Best (Up to 54), 54, 48, 36, 24, 18, 12, 9, 6 for 5 GHz and Best (Up to 54), 54, 48, 36, 24, 18, 12, 9, 6, 11, 5.5, 2 or 1 for 2.4 GHz.

Beacon Interval (40-500): Beacons are packets sent by an access point to synchronize a wireless network. Specify a value in milliseconds. The default (100) is recommended. Setting a higher beacon interval can help to save the power of wireless clients, while setting a lower one can help a wireless client connect to an access point faster.

DTM Interval (1-15): Select a Delivery Traffic Indication Message setting between 1 and 15. 1 is the default setting. DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

Performance Settings	
Wireless band	2.4GHz
Wireless	On
Wireless Mode	Mixed 802.11n, 802.11g and 802.11b
Data Rate	Best(Up to 600) (Mbps)
Beacon Interval (40-500)	100
DTIM Interval (1-15)	1
Transmit Power	100%
WMM (Wi-Fi Multimedia)	Enable
Ack Time Out (2.4GHz, 48-200)	48 (us)
Short GI	Enable
IGMP Snooping	Disable
Multicast Rate	Disable (Mbps)
Multicast Bandwidth Control	Disable
Maximum Multicast Bandwidth	100 kbps
HT20/40 Coexistence	Enable
Transfer DHCP Offer to Unicast	Enable

Save

Transmit Power: This setting determines the power level of the wireless transmission. Transmitting power can be adjusted to eliminate overlapping of wireless area coverage between two access points where interference is a major concern. For example, if wireless coverage is intended for half of the area, then select 50% as the option. Use the drop-down menu to select 100%, 50%, 25%, or 12.5%.

WMM (Wi-Fi Multimedia): WMM stands for Wi-Fi Multimedia. Enabling this feature will improve the user experience for audio and video applications over a Wi-Fi network.

Ack Time Out (2.4 GHZ, 48~200): To effectively optimize throughput over long distance links enter a value for Acknowledgement Time Out between 25 and 200 microseconds for 5 GHz or from 48 to 200 microseconds for 2.4 GHz in the field provided.

Short GI: Select Enable or Disable. Enabling a short guard interval can increase throughput. However, be aware that it can also increase the error rate in some installations due to increased sensitivity to radio-frequency installations.

IGMP Snooping: Select Enable or Disable. Internet Group Management Protocol allows the AP to recognize IGMP queries and reports sent between routers and an IGMP host (wireless STA). When IGMP snooping is enabled, the AP will forward multicast packets to an IGMP host based on IGMP messages passing through the AP.

Multicast Rate : Select the multicast rate to adjust multicast packet data rates.

Multicast Bandwidth Control : Adjust the multicast packet data rate here. The multicast rate is supported in AP mode, (2.4 GHZ and 5 GHZ) and WDS with AP mode, including Multi-SSIDs.

Maximum Multicast Bandwidth : Set the multicast packets' maximum bandwidth pass through rate from the Ethernet interface to the Access Point.

HT20/40 Coexistence : Enable this option to reduce interference from other wireless networks in your area. If the channel width is operating at 40 MHz and there is another wireless network's channel overlapping and causing interference, the Access Point will automatically change to 20 MHz.

Transfer DHCP Offer to Unicast : Enable to transfer the DHCP Offer to Unicast from LAN to WLAN. It is suggested to enable this function if stations number is larger than 30.

Wireless Resource

The Wireless Resource Control window is used to configure the wireless connection settings so that the device can detect the better wireless connection in your environment.

Airtime Fairness: Click the drop-down menu to enable or disable the airtime fairness function.

Band Steering: Click the drop-down menu to enable the band steering function. When the wireless clients support both 2.4GHz and 5GHz and the 2.4GHz signal is not strong enough, the device will use 5GHz as higher priority.

Wireless Band: Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz 1 or 5GHz 2.

Connection Limit: Click the drop-down menu to enable or disable the connection limit function. The option is for load balancing. This determines whether to limit the number of users accessing this device. The exact number is entered in the User Limit field below. This feature allows the user to share the wireless network traffic and the client using multiple APs. If this function is enabled and when the number of users exceeds this value, or the network utilization of this AP exceeds the percentage that has been specified, the DAP-2720 will not allow clients to associate with the AP.

User Limit (0 - 64): This function is only available when Connection Limit is enabled. Set the maximum amount of users that are allowed access (0 - 64 users) to the device using the specified wireless band.



The screenshot shows the 'Wireless Resource Control' configuration window. It contains the following settings:

Setting	Value
Airtime Fairness	Disable
Band Steering	Disable
Wireless band	5GHz
Connection Limit	Disable
User Limit (0 - 64)	20
11n/ac Preferred	Disable
Network Utilization	100%
Aging out	Disable
RSSI Threshold	100%
Data Rate Threshold	54
ACL RSSI	Disable
ACL RSSI Threshold	60%

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

-
- 11n Preferred:** This function is only available when Connection Limit is enabled. Use the drop-down menu to enable the 11n Preferred function. The wireless clients with 802.11n protocol will have higher priority to connect to the device.
- Network Utilization:** Click the drop-down menu to set the maximum utilization of this access point for service. The DAP-2720 will not allow any new clients to associate with the AP if the utilization exceeds the value the user specifies. When this network utilization threshold is reached, the device will pause for one minute to allow network congestion to dissipate.
- Aging out:** Use the drop-down menu to select the criteria for disconnecting the wireless clients.
- RSSI Threshold:** When **Aging out** is **RSSI**, click the drop-down menu to select the percentage of RSSI. When the RSSI of wireless clients is lower than the specified percentage, the device disconnects the wireless clients. The function is only available when **Aging out** is **RSSI**.
- Data Rate Threshold:** When **Aging out** is **Data Rate**, click the drop-down menu to select the threshold of data rate. When the data rate of wireless clients is lower than the specified number, the device disconnects the wireless clients. The function is only available when **Aging out** is **Data Rate**.
- ACL RSSI:** Click the drop-down menu to enable the ACL RSSI function. When enabled, the device denies the connection request from the wireless clients with the RSSI lower than the specified threshold below.
- ACL RSSI Threshold:** Click the drop-down menu to set the ACL RSSI Threshold.
- Save:** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

Multi-SSID

The device supports up to four multiple Service Set Identifiers. You can set the Primary SSID in the Basic > Wireless section. The SSID's factory default setting is dlink. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

Enable Multi-SSID: Check to enable support for multiple SSIDs.

Enable Priority: Check to enable the Priority function.

Band: Select **2.4GHz** or **5GHz 1** or **5GHz 2**.

Index: You can select up to seven multi-SSIDs. With the Primary SSID, you have a total of eight multi-SSIDs per radio.

SSID: Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

SSID Visibility: Enable or Disable SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.

The Multi-SSID security can be Open System, WPA-Personal, or WPA-Enterprise. For a detailed description of the Open System parameters please go to pages 19. For a detailed description of the WPA-Personal parameters please go to page 20. For a detailed description of the WPA-Enterprise parameters please go to page 21.

Priority: Select the priority level of the SSID selected.

WMM (Wi-Fi Multimedia): WMM stands for Wi-Fi Multimedia. Enabling this feature will improve the user experience for audio and video applications over a Wi-Fi network.

Index	SSID	Band	Encryption	Delete
Primary SSID	dlink	2.4 GHz	None	

Encryption: When you select Open System, toggle between Enable and Disable. If Enable is selected, the Key Type, Key Size, Key Index (1~4), Key, and Confirm Keys must also be configured.

Key Type: Select HEX or ASCII.

Key Size: Select 64-bit or 128-bit.

Key Index (1-4): Select from the 1st to 4th key to be set as the active key.

Key: Input up to four keys for encryption. You will select one of these keys in the Key Index drop-down menu.

WPA Mode: When you select either WPA-Personal or WPA-Enterprise, you must also choose a WPA mode from the drop-down menu: AUTO (WPA or WPA2), WPA2 Only, or WPA Only. WPA and WPA2 use different algorithms. AUTO (WPA or WPA2) allows you to use both WPA and WPA2. In addition, you must configure Cipher Type, and Group Key Update Interval.

Cipher Type: Select Auto, AES, or TKIP from the drop-down menu.

Group Key Update Interval: Select the interval during which the group key will be valid. The default value of 1800 seconds is recommended.

Pass Phrase: When you select WPA-Personal, please enter a Pass Phrase in the corresponding field.

Confirm Pass Phrase: When you select WPA-Personal, please re-enter the Pass Phrase entered in the previous item in the corresponding field.

RADIUS Server: When you select WPA-Enterprise, enter the IP address of the RADIUS server. In addition, you must configure RADIUS Port and RADIUS Secret.

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the RADIUS secret.

Accounting Mode: Click the drop-down menu to enable or disable the accounting mode.

Accounting Server: Enter the IP address of the accounting server.

VLAN

VLAN List

The DAP-2720 supports VLANs. VLANs can be created with a Name and VID. Mgmt (TCP stack), LAN, Primary/Multiple SSID, and WDS connection can be assigned to VLANs as they are physical ports. Any packet which enters the DAP-2720 without a VLAN tag will have a VLAN tag inserted with a PVID. The VLAN List tab displays the current VLANs.

VLAN Status: Use the radio button to toggle to Enable. Next, go to the Add/Edit VLAN tab to add or modify an item on the VLAN List tab.

VLAN Mode: The current VLAN mode is displayed.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

VID: Displays the VID of the VLAN.

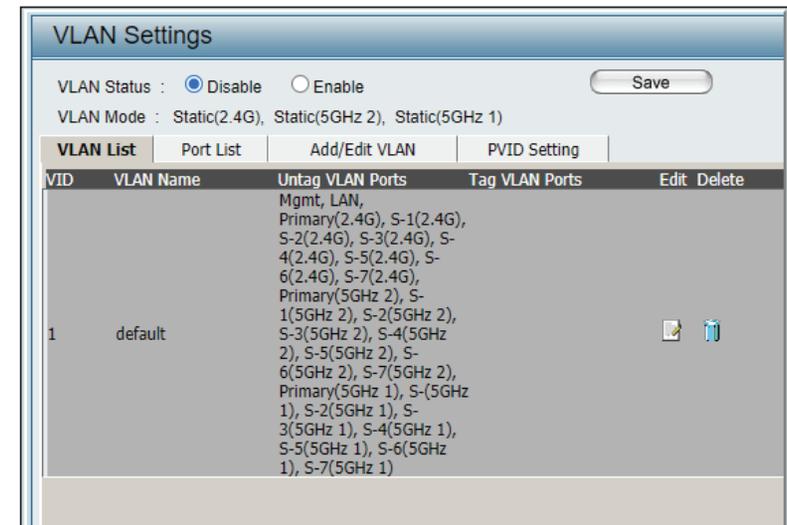
VLAN Name: Displays the name of the VLAN.

Untag VLAN Ports Displays the untagged ports.

Tag VLAN Ports: Displays the tagged ports.

Edit: Click the icon to edit the current VLAN.

Delete: Click the icon to delete the current VLAN.



Port List

The Port List tab displays the current ports. If you want to configure the guest and internal networks on a Virtual LAN (VLAN), the switch and DHCP server you are using must also support VLANs. As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE 802.1Q standard.

VLAN Status: Use the radio button to toggle to Enable. Next, go to the Add/Edit VLAN tab to add or modify an item on the VLAN List tab.

VLAN Mode: Displays the current VLAN mode.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

Port Name: The name of the port is displayed in this column.

Tag VID: The Tagged VID is displayed in this column.

Untag VID: The Untagged VID is displayed in this column.

PVID: The Port VLAN Identifier is displayed in this column.

Port Name	Tag VID	Untag VID	PVID
Mgmt	1	1	1
LAN	1	1	1
Primary(2.4G)	1	1	1
Primary(5GHz 2)	1	1	1
Primary(5GHz 1)	1	1	1
S-1(2.4G)	1	1	1
S-2(2.4G)	1	1	1
S-3(2.4G)	1	1	1
S-4(2.4G)	1	1	1
S-5(2.4G)	1	1	1
S-6(2.4G)	1	1	1
S-7(2.4G)	1	1	1
S-1(5GHz 2)	1	1	1
S-2(5GHz 2)	1	1	1
S-3(5GHz 2)	1	1	1
S-4(5GHz 2)	1	1	1
S-5(5GHz 2)	1	1	1
S-6(5GHz 2)	1	1	1
S-7(5GHz 2)	1	1	1

Add/Edit VLAN

The Add/Edit VLAN tab is used to configure VLANs. Once you have made the desired changes, click the Save button to let your changes take effect.

VLAN Status: Use the radio button to toggle to Enable.

VLAN Mode: Displays the current VLAN mode.

VLAN ID: Provide a number between 1 and 4094 for the Internal VLAN.

VLAN Name: Enter the VLAN to add or modify.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

VLAN Settings

VLAN Status : Disable Enable Save

VLAN Mode : Static(2.4G), Static(5GHz 2), Static(5GHz 1)

VLAN List |
 Port List |
 Add/Edit VLAN |
 PVID Setting

VLAN ID (VID) VLAN Name

Port	Select All	Mgmt	LAN
Untag	All	<input type="radio"/>	<input type="radio"/>
Tag	All	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input type="radio"/>	<input type="radio"/>

2.4GHz

MSSID Port	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	<input type="radio"/>							
Tag	All	<input type="radio"/>							
Not Member	All	<input type="radio"/>							

5GHz 2

MSSID Port	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	<input type="radio"/>							
Tag	All	<input type="radio"/>							
Not Member	All	<input type="radio"/>							

5GHz 1

MSSID Port	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	<input type="radio"/>							
Tag	All	<input type="radio"/>							
Not Member	All	<input type="radio"/>							

PVID Settings

The PVID Setting tab is used to enable/disable the Port VLAN Identifier Auto Assign Status as well as to configure various types of PVID settings. Click the Save button to let your changes take effect.

VLAN Status: Use the radio button to toggle between Enable and Disable.

VLAN Mode: Displays the current VLAN mode.

PVID Auto Assign Status: Use the radio button to toggle PVID auto assign status to Enable.

VLAN Settings

VLAN Status : Disable Enable Save

VLAN Mode : Static(2.4G), Static(5GHz 2), Static(5GHz 1)

VLAN List | Port List | Add/Edit VLAN | **PVID Setting**

PVID Auto Assign Status Disable Enable

Port	Mgmt	LAN
PVID	1	1

2.4GHz

MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
PVID	1	1	1	1	1	1	1	1

5GHz 2

MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
PVID	1	1	1	1	1	1	1	1

5GHz 1

MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
PVID	1	1	1	1	1	1	1	1

Save

Intrusion

The Wireless Intrusion Protection window is used to set APs as All, Valid, Neighborhood, Rogue, and New. Click the Save button to let your changes take effect.

Wireless Band: Select 2.4GHz or 5GHz 1 or 5GHz 2.

AP List: Click the drop-down menu to select **All**, **Valid**, **Neighbor**, **Rogue**, and **New**.

The following is a definition of the listed AP categories:

- **Valid:** An AP which is authenticated to the network with encryption is classified as valid.
- **Neighbor:** A detected AP with a weak signal strength is classified as a suspect neighbor.
- **Rogue:** An AP that has been installed on the secure network without explicit authorization.
- **New:** An alternative category.

From the AP List select a detected AP and click **Set as Valid**, **Set as Neighborhood**, **Set as Rogue**, or **Set as New** to manually define the category type for the AP. Alternatively, click the radio button to mark all new access points as valid or rogue.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

Wireless Intrusion Protection

Wireless Band: 2.4GHz ▼

Detect

AP List

All ▼

Type	Band	CH	SSID	BSSID	Last Seen	Status

Set as Valid Set as Neighborhood Set as Rogue Set as New

Mark All New Access Points as Valid Access Points

Mark All New Access Points as Rogue Access Points

Save

Schedule

The Wireless Schedule Settings window is used to add and modify scheduling rules on the device. Click the Save button to let your changes take effect.

Wireless Schedule: Use the drop-down menu to enable the device's scheduling feature.

Name: Enter a name for the new scheduling rule in the field provided.

Index: Use the drop-down menu to select the desired SSID.

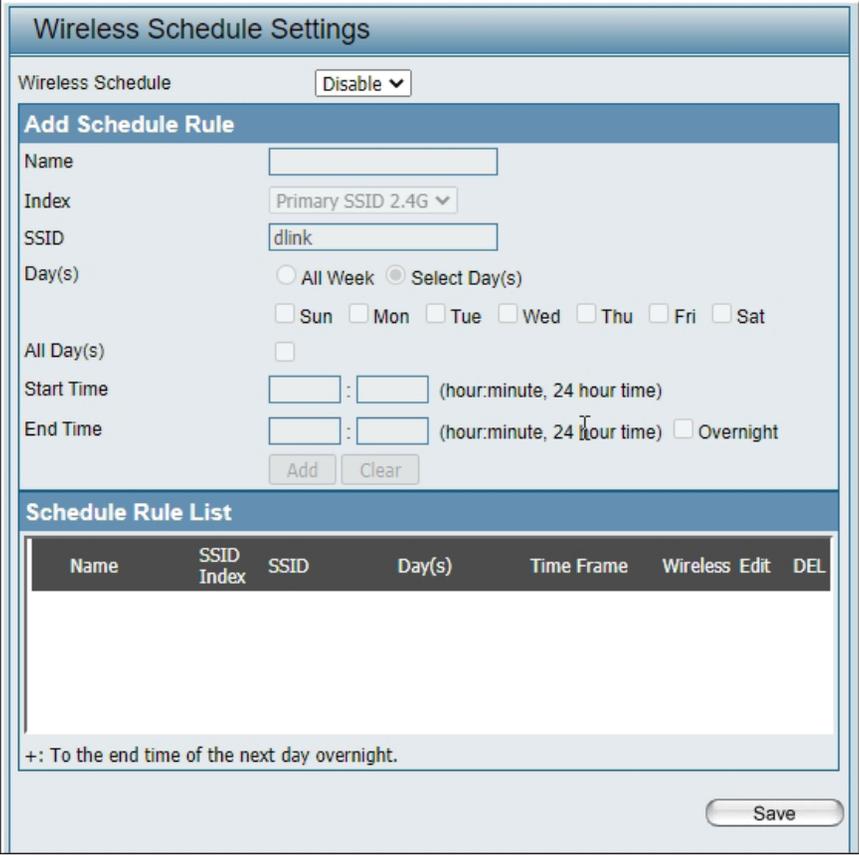
SSID: This read-only field indicates the current SSID in use. To create a new SSID, go to the Wireless Settings window (Basic Settings > **Wireless**).

Day(s): Toggle the radio button between All Week and Select Day(s). If the second option is selected, check the specific days you want the rule to be effective on.

All Day(s): Check this box to have your settings apply 24 hours a day.

Start Time: Enter the beginning hour and minute, using a 24-hour clock.

End Time: Enter the ending hour and minute, using a 24-hour clock.



Wireless Schedule Settings

Wireless Schedule Disable ▾

Add Schedule Rule

Name

Index Primary SSID 2.4G ▾

SSID dlink

Day(s) All Week Select Day(s)

Sun Mon Tue Wed Thu Fri Sat

All Day(s)

Start Time : (hour:minute, 24 hour time)

End Time : (hour:minute, 24 hour time) Overnight

Schedule Rule List

Name	SSID Index	SSID	Day(s)	Time Frame	Wireless Edit	DEL
+: To the end time of the next day overnight.						

Internal RADIUS Server

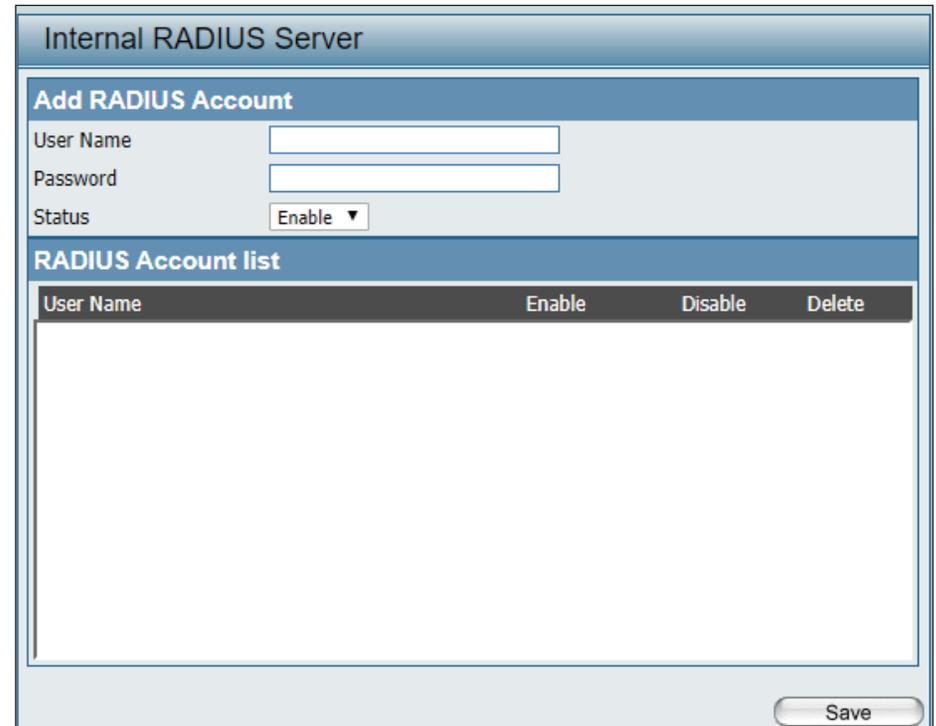
The DAP-2720 features a built-in RADIUS server. Once you have finished adding a RADIUS account, click the Save button to let your changes take effect. The newly-created account will appear in this RADIUS Account List. The radio buttons allow the user to enable or disable the RADIUS account. Click the icon in the delete column to remove the RADIUS account. We suggest you limit the number of accounts below 30.

User Name: Enter a name to authenticate user access to the internal RADIUS server.

Password: Enter a password to authenticate user access to the internal RADIUS server. The length of your password should be 8~64.

Status: Toggle the drop-down menu between Enable and Disable.

RADIUS Account List: Displays the list of users.



The screenshot shows the 'Internal RADIUS Server' configuration window. It is divided into two main sections: 'Add RADIUS Account' and 'RADIUS Account list'. The 'Add RADIUS Account' section contains three input fields: 'User Name' (a text box), 'Password' (a text box), and 'Status' (a dropdown menu currently set to 'Enable'). The 'RADIUS Account list' section is a table with a header row containing 'User Name', 'Enable', 'Disable', and 'Delete'. The table body is currently empty. A 'Save' button is located at the bottom right of the window.

User Name	Enable	Disable	Delete
-----------	--------	---------	--------

ARP Spoofing Prevention

The ARP Spoofing Prevention feature allows users to add IP/MAC address mapping to prevent ARP spoofing attacks.

ARP Spoofing Prevention: This drop-down allows you to enable the ARP spoofing prevention function.

Add: Click to create a defined rule.

Clear: Click to clear a defined rule.

Gateway IP Address: Enter a gateway IP address.

Gateway MAC Address: Enter a gateway MAC address.

Delete All: Click to delete all gateway entries.

Edit: Click to edit the selected gateway entry.

Delete: Click to delete the gateway entry.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

ARP Spoofing Prevention Settings

ARP Spoofing Prevention ▾

Add Gateway Address

Gateway IP Address

Gateway MAC Address : : : : :

Gateway Address List

Total Entries: 0

Gateway IP Address	Gateway MAC Address	Edit	Delete
<input type="button" value="Save"/>			

Bandwidth Optimization

The Bandwidth Optimization window allows the user to manage the bandwidth of the device and arrange the bandwidth for various wireless clients. When the Bandwidth Optimization rule is finished, click the **Add** button. To discard the Add Bandwidth Optimization Rule settings, click the **Clear** button. Click the **Save** button to let your changes take effect.

Enable Bandwidth Optimization: Use the drop-down menu to Enable the Bandwidth Optimization function.

Downlink Bandwidth: Enter the downlink bandwidth of the device in Mbits per second.

Uplink Bandwidth: Enter the uplink bandwidth of the device in Mbits per second.

Allocate average BW for each station: AP will distribute average bandwidth for each client.

Allocate maximum BW for each station: Specify the maximum bandwidth for each connected client. Reserve certain bandwidth for future clients.

Allocate different BW for a/b/g/n stations: The weight of 11b/g/n and 11a/n client are 10%/20%/70% and 20%/80%. AP will distribute different bandwidth for 11a/b/g/n clients.

Allocate specific BW for SSID: All clients share the total bandwidth.

Rule Type: Use the drop-down menu to select the type that is applied to the rule. Available options are: **Allocate average BW for each station**, **Allocate maximum BW for each station**, **Allocate different BW for 1a/b/g/n stations**, and **Allocate specific BW for SSID**.

Bandwidth Optimization

Enable Bandwidth Optimization

Downlink Bandwidth Mbits/sec

Uplink Bandwidth Mbits/sec

Add Bandwidth Optimization Rule

Rule Type

Band

SSID Index

Downlink Speed Kbits/sec

Uplink Speed Kbits/sec

Bandwidth Optimization Rules

Band	Type	SSID Index	Downlink Speed	Uplink Speed	Edit	Del
------	------	------------	----------------	--------------	------	-----

Band: Use the drop-down menu to toggle the wireless band between 2.4GHz and 5GHz.

SSID Index: Use the drop-down menu to select the SSID for the specified wireless band.

Downlink Speed: Enter the limitation of the downloading speed in either Kbits/sec or Mbits/sec for the rule.

Uplink Speed: Enter the limitation of the uploading speed in either Kbits/sec or Mbits/sec for the rule.

Add: Click to create a defined rule.

Clear: Click to remove the settings from the menu interface.

Edit: Click to edit the selected gateway entry.

Delete: Click to delete the gateway entry.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate.**

Captive Portal

Authentication Settings-Web Redirection Only

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, users can view and configure the Captive Portal settings. After selecting Web Redirection Only as the Authentication Type, we can configure the redirection website URL that will be applied to each wireless client in this network.

Session timeout(1-1440): Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band: Select 2.4GHz or 5GHz 1 or 5GHz 2.

SSID Index: Select the SSID for this Authentication.

Authentication Type: Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Web Redirection option.

Web Redirection State: The default setting is Enable when you select **Web Redirection Only**.

URL Path: Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.

IPIF Status: Select to **Enable** or **Disable** the Captive Portal with its IP interface feature here.

VLAN Group: Enter the VLAN Group ID here.

Captive Portal Authentication

Session Timeout (1-1440) Minute(s)

Band

SSID Index

Authentication Type

Band	SSID Index	Captive Profile	Edit	Delete

Get IP From: Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2720. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

IP Address: Assign a static IP address that is within the IP address range of your network.

Subnet Mask: Enter the subnet mask. All devices in the network must share the same subnet mask.

Gateway: Enter the IP address of the gateway/router in your network.

DNS: Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

Edit: Click to edit the selected entry.

Delete: Click to delete the entry.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

Authentication Settings- Username/Password

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, users can view and configure the Captive Portal settings. After selecting Username/Password as the Authentication Type, we can configure the Username/Password authentication that will be applied to each wireless client in this network.

Session timeout(1-1440): Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band: Select 2.4GHz or 5GHz 1 or 5GHz 2.

SSID Index: Select the SSID for this Authentication.

Authentication Type: Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Username/Password option.

Web Redirection State: Disable is default setting. Select Enable to enable the website redirection feature.

URL Path: Select whether to use HTTP or HTTPS. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.

IPIF Status: Select to Enable or Disable the Captive Portal with its IP interface feature here.

VLAN Group: Enter the VLAN Group ID here.

Captive Portal Authentication

Session Timeout (1-1440) Minute(s)

Band

SSID Index

Authentication Type

Web Redirection Interface Settings

Web Redirection State

URL Path

IP Interface Settings

IPIF Status

VLAN Group

Get IP From

IP Address

Subnet Mask

Gateway

DNS

Username/Password Settings

Username

Password

Username	Edit	Delete

Band	SSID Index	Captive Profile	Edit	Delete

Get IP From: Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2720. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

IP Address: Assign a static IP address that is within the IP address range of your network.

Subnet Mask: Enter the subnet mask. All devices in the network must share the same subnet mask.

Gateway: Enter the IP address of the gateway/router in your network.

DNS: Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

Username: Enter the username for the new account here.

Password: Enter the password for the new account here.

Add: Click to create a defined rule.

Clear: Click to remove the settings from the menu interface.

Edit: Click to edit the selected gateway entry.

Delete: Click to delete the gateway entry.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

Authentication Settings- Passcode

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, users can view and configure the Captive Portal settings. After selecting Passcode as the Authentication Type, you can configure the Passcode authentication that will be applied to each wireless client in this network.

Session timeout(1-1440): Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band: Select 2.4GHz or 5GHz 1 or 5GHz 2.

SSID Index: Select the SSID for this Authentication.

Authentication Type: Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Passcode option.

Web Redirection State: The default setting is Disable. Select Enable to enable the website redirection feature.

URL Path: Select whether to use HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.

IPIF Status: Select to Enable or Disable the Captive Portal with its IP interface feature here.

VLAN Group: Enter the VLAN Group ID here.

Captive Portal Authentication

Session Timeout (1-1440) Minute(s)

Band

SSID Index

Authentication Type

Web Redirection Interface Settings

Web Redirection State

URL Path

IP Interface Settings

IPIF Status

VLAN Group

Get IP From

IP Address

Subnet Mask

Gateway

DNS

Passcode Settings

Passcode Quantity

Duration Hour

Last Active Time Year Month Day Hour

User Limit

Passcode	Duration	Last Active Time	User Limit	Delete

Get IP From: Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2720. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

IP Address: Assign a static IP address that is within the IP address range of your network.

Subnet Mask: Enter the subnet mask. All devices in the network must share the same subnet mask.

Gateway: Enter the IP address of the gateway/router in your network.

DNS: Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

Passcode Quantity: Enter the number of ticket that will be used here.

Duration: Enter the duration value, in hours, for this passcode.

Last Active Day: Select the last active date for this passcode here. Year, Month and Day selections can be made.

User Limit: Enter the maximum amount of users that can use this passcode at the same time

Add: Click to create a defined rule.

Clear: Click to remove the settings from the menu interface.

Delete All: Click to delete all passcode setting entries

Edit: Click to edit the selected entry.

Delete: Click to delete the entry.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate.**

Authentication Settings- Remote RADIUS

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, users can view and configure the Captive Portal settings. After selecting Remote RADIUS as the Authentication Type, you can configure the Remote RADIUS authentication that will be applied to each wireless client in this network.

Session timeout(1-1440): Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band: Select 2.4GHz or 5GHz 1 or 5GHz 2.

SSID Index: Select the SSID for this Authentication.

Authentication Type: Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Remote RADIUS option.

Web Redirection State: The default setting is Disable. Select Enable to enable the website redirection feature.

URL Path: Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.

IPIF Status: Select to Enable or Disable the Captive Portal with its IP interface feature here.

VLAN Group: Enter the VLAN Group ID here.

Captive Portal Authentication

Session Timeout (1-1440) Minute(s)

Band

SSID Index

Authentication Type

Web Redirection Interface Settings

Web Redirection State

URL Path

IP Interface Settings

IPIF Status

VLAN Group

Get IP From

IP Address

Subnet Mask

Gateway

DNS

Remote RADIUS Settings

Radius Server Settings

Radius Server Radius Port

Radius Secret

Remote RADIUS Type

Secondary radius Server Settings

Radius Server Radius Port

Radius Secret

Remote RADIUS Type

Third radius Server Settings

Radius Server Radius Port

Radius Secret

Remote RADIUS Type

Band	SSID Index	Captive Profile	Edit	Delete

Get IP From: Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2720. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

IP Address: Assign a static IP address that is within the IP address range of your network.

Subnet Mask: Enter the subnet mask. All devices in the network must share the same subnet mask.

Gateway: Enter the IP address of the gateway/router in your network.

DNS: Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

Radius Server: Enter the RADIUS server's IP address here

Radius Port: Enter the RADIUS server's port number here

Radius Port: Enter the RADIUS server's shared secret here

Remote Radius Type: Select the remote RADIUS server type here. Currently, only SPAP will be used.

Edit: Click to edit the selected entry.

Delete: Click to delete the entry.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate.**

Authentication Settings- LDAP

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, users can view and configure the Captive Portal settings. After selecting LDAP as the Authentication Type, you can configure the LDAP authentication that will be applied to each wireless client in this network.

Session timeout(1-1440): Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band: Select 2.4GHz or 5GHz 1 or 5GHz 2.

SSID Index: Select the SSID for this Authentication.

Authentication Type: Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the LDAP option.

Web Redirection State: The default setting is Disable. Select Enable to enable the website redirection feature.

URL Path: Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.

IPIF Status: Select to Enable or Disable the Captive Portal with its IP interface feature here.

VLAN Group: Enter the VLAN Group ID here.

Get IP From: Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2720. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

Captive Portal Authentication

Session Timeout (1-1440) Minute(s)

Band

SSID Index

Authentication Type

Web Redirection Interface Settings

Web Redirection State

URL Path

IP Interface Settings

IPIF Status

VLAN Group

Get IP From

IP Address

Subnet Mask

Gateway

DNS

LDAP Settings

Server

Port

Authenticate Mode

Username

Password

Base DN (ou=,dc=)

Account Attribute (ex.cn)

Identity Auto Copy

Band	SSID Index	Captive Profile	Edit	Delete

IP Address: Assign a static IP address that is within the IP address range of your network.

Subnet Mask: Enter the subnet mask. All devices in the network must share the same subnet mask.

Gateway: Enter the IP address of the gateway/router in your network.

DNS: Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

Server: Enter the LDAP server's IP address or domain name here.

Port: Enter the LDAP server's port number here.

Authenticate Mode: Select the authentication mode here. Options to choose from are Simple and TLS.

Username: Enter the LDAP server account's username here.

Password: Enter the LDAP server account's password here.

Base DN: Enter the administrator's domain name here

Account Attribute: Enter the LDAP account attribute string here. This string will be used to search for clients.

Identity: Enter the identity's full path string here. Alternatively, select the Auto Copy checkbox to automatically add the generic full path of the web page in the identity field.

Edit: Click to edit the selected entry.

Delete: Click to delete the entry.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

Authentication Settings- POP3

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, users can view and configure the Captive Portal settings. After selecting POP3 as the Authentication Type, you can configure the POP3 authentication that will be applied to each wireless client in this network.

Session timeout(1-1440): Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band: Select 2.4GHz or 5GHz 1 or 5GHz 2.

SSID Index: Select the SSID for this Authentication.

Authentication Type: Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the POP3 option.

Web Redirection State: The default setting is Disable. Select Enable to enable the website redirection feature.

URL Path: Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.

IPIF Status: Select to Enable or Disable the Captive Portal with its IP interface feature here.

VLAN Group: Enter the VLAN Group ID here.

Captive Portal Authentication

Session Timeout (1-1440) Minute(s)

Band

SSID Index

Authentication Type

Web Redirection Interface Settings

Web Redirection State

URL Path

IP Interface Settings

IPIF Status

VLAN Group

Get IP From

IP Address

Subnet Mask

Gateway

DNS

POP3 Settings

Server

Port

Connection Type

Band	SSID Index	Captive Profile	Edit	Delete

Get IP From: Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2720. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

IP Address: Assign a static IP address that is within the IP address range of your network.

Subnet Mask: Enter the subnet mask. All devices in the network must share the same subnet mask.

Gateway: Enter the IP address of the gateway/router in your network.

DNS: Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

Server: Enter the POP3 server's IP address or domain name here.

Port: Port: Enter the POP server's port number here.

Connection Type: Select the connection type here. Options to choose from are None and SSL/TLS.

Edit: Click to edit the selected entry.

Delete: Click to delete the entry.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate.**

Login Page Upload

In this window, users can upload a custom login web page that will be used by the captive portal feature. Click the **Browse** button to navigate to the login style located on the managing computer and then click the **Upload** button to initiate the upload.

Upload Login Style From Local Hard Drive: In this field the path to the login style file that will be uploaded is displayed. Alternatively, the path can be manually entered here.

Login Page Style List : Select the wireless band and login style that will be used in each SSID here. Click the download button to download the template file for the login page and click the delete button to delete the template file.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

Login Page Upload

Upload Login Style From Local Hard Drive

Upload Login Style from file :

The Left space 457216 Byte(s)

Login Page Style List

Wireless Band 2.4GHz ▼

ID	Style Name	Pri	S-1	S-2	S-3	S-4	S-5	S-6	S-7	Download	Del
1	pages_default.tar	<input checked="" type="radio"/>	<input type="button" value="Download"/>	<input type="button" value="Del"/>							
2	pages_headerpic.tar	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="button" value="Download"/>	<input type="button" value="Del"/>
3	pages_license.tar	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="button" value="Download"/>	<input type="button" value="Del"/>

MAC Bypass

The DAP-2720 features a wireless MAC Bypass. Once finished editing these settings, click the **Save** button to let the changes take effect.

Wireless Band: Select the wireless band for MAC Bypass.

SSID Index: Select the SSID for MAC Bypass.

MAC Address: Enter each MAC address that you wish to include in your bypass list, and click Add.

MAC Address List: When a MAC address is entered, it appears in this list.
Highlight a MAC address and click the Delete icon to remove it from this list.

Upload File: To upload a MAC bypass list file, click Browse and navigate to the MAC bypass list file saved on the computer, and then click Upload.

Load MAC File to Local Hard Driver: To download MAC bypass list file, click Download and to save the MAC bypass list.

Save: Click to save the updated configuration.
To make the updates permanent, click Configuration > **Save and Activate**.

The screenshot shows the 'MAC Bypass Settings' web interface. At the top, there are three configuration fields: 'Wireless Band' set to '2.4GHz', 'SSID Index' set to 'Primary SSID', and 'MAC Address' with six empty boxes and an 'Add' button. Below these is a table with three columns: 'ID', 'MAC Address', and 'Delete'. The table is currently empty. Underneath the table, there are two sections: 'Upload MAC File' with a 'Choose File' button, 'No file chosen' text, and an 'Upload' button; and 'Download MAC File' with a 'Download' button. At the bottom right of the interface is a 'Save' button.

DHCP Server

Dynamic Pool Settings

The DHCP address pool defines the range of the IP address that can be assigned to stations in the network. A Dynamic Pool allows wireless stations to receive an available IP with lease time control. If needed or required in the network, the DAP-2720 is capable of acting as a DHCP server.

Function Enable/Disable: Dynamic Host Configuration Protocol (DHCP) assigns dynamic IP addresses to devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses. Select Enable to allow the DAP-2720 to function as a DHCP server.

IP Assigned From: Input the first IP address available for assignment on your network.

IP Pool Range(1-254): Enter the number of IP addresses available for assignment. IP addresses are increments of the IP address specified in the "IP Assigned From" field.

Subnet Mask: All devices in the network must have the same subnet mask to communicate. Enter the subnet mask for the network here.

Gateway: Enter the IP address of the gateway on the network.

WINS: Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer that has a dynamically assigned IP address.

DNS: Enter the IP address of the Domain Name System (DNS) server. The DNS server translates domain names such as www.dlink.com into IP addresses.

Domain Name: Enter the domain name of the network, if applicable. (An example of a domain name is: www.dlink.com.)

Lease Time: The lease time is the period of time before the DHCP server will assign new IP addresses.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

Dynamic Pool Settings	
DHCP Server Control	
Function Enable/Disable	Disable ▼
Dynamic Pool Settings	
IP Assigned From	192.168.0.20
IP Pool Range(1-254)	235
Subnet Mask	255.255.255.0
Gateway	192.168.0.50
WINS	192.168.0.50
DNS	192.168.0.50
Domain Name	dlink-ap
Lease Time (60 - 31536000 sec)	604800
Save	

Static Pool Setting

The DHCP address pool defines the range of IP addresses that can be assigned to stations on the network. A static pool allows specific wireless stations to receive a fixed IP without time control.

Function Enable/Disable: Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to wireless devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign IP addresses. Select Enable to allow the DAP-2720 to function as a DHCP server.

Assigned IP: Use the Static Pool Settings to assign the same IP address to a device every time you start up. The IP addresses assigned in the Static Pool list must NOT be in the same IP range as the Dynamic Pool. After you have assigned a static IP address to a device via its MAC address, click Apply; the device will appear in the Assigned Static Pool at the bottom of the screen. You can edit or delete the device in this list.

Assigned MAC Address: Enter the MAC address of the device requesting association here.

Subnet Mask: Define the subnet mask of the IP address specified in the "IP Assigned From" field.

Static Pool Settings

DHCP Server Control

Function Enable/Disable: Enable

Static Pool Setting

Host Name:

Assigned IP:

Assigned MAC Address: : : : : :

Subnet Mask: 255.255.255.0

Gateway:

WINS:

DNS:

Domain Name: dlink-ap

Save

Host Name	MAC Address	IP Address	Edit	Delete

Gateway: Specify the Gateway address for the wireless network.

WINS: Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.

DNS: Enter the DNS server address for your wireless network.

Domain Name: Specify the domain name for the network.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate.**

Current IP Mapping List

This window displays information about the current assigned DHCP dynamic and static IP address pools. This information is available when you enable the DHCP server on the AP and assign dynamic and static IP address pools.

Current DHCP Dynamic Profile: These are IP address pools the DHCP server has assigned using the dynamic pool setting.

Binding MAC Address: The MAC address of a device on the network that is assigned an IP address from the DHCP dynamic pool.

Assigned IP Address: The current corresponding DHCP-assigned IP address of the device.

Lease Time: The length of time that the dynamic IP address will be valid.

Current DHCP Static Pools: These are the IP address pools of the DHCP server assigned through the static pool settings.

Binding MAC Address: The MAC address of a device on the network that is within the DHCP static IP address pool.

Assigned IP Address: The current corresponding DHCP-assigned static IP address of the device.

Binding MAC Address: The MAC address of a device on the network that is assigned an IP address from the DHCP dynamic pool.

Assigned IP Address: The current corresponding DHCP-assigned static IP address of the device.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

Current IP Mapping List			
Current DHCP Dynamic Pools			
Host Name	Binding MAC Address	Assigned IP Address	Lease Time
Current DHCP Static Pools			
Host Name	Binding MAC Address	Assigned IP Address	

Filters

Wireless MAC ACL

This page allows the user to configure Wireless MAC ACL settings for access control.

Wireless Band: Displays the current wireless band rate.

Access Control List: Select **Disable** to disable the filters function.

Select **Accept** to accept only those devices with MAC addresses in the Access Control List. All other devices not on the list will be rejected.

Select **Reject** to reject the devices with MAC addresses on the Access Control List. All other devices not on the list will be accepted.

SSID Index: Click the drop-down menu to select the SSID for the specified wireless band.

MAC Address: Enter each MAC address that you wish to include in your filter list, and click **Apply**.

MAC Address List: When you enter a MAC address, it appears in this list. Highlight a MAC address and click Delete to remove it from this list.

Current Client Information: This table displays information about all the current connected stations.

Upload File: To upload an ACL list file, click Browse and navigate to the ACL list file saved on the computer, and then click Upload.

Load MAC File to Local

Hard Driver: To download the ACL list, click Download and to save the ACL list.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

Wireless MAC ACL Settings

Wireless Band: 2.4GHz Total : 512 Used : 0

Access Control List: Disable

SSID Index: Primary SSID

MAC Address: [] : [] : [] : [] : [] : [] Add

ID	MAC Address	Delete

Current Client Information

MAC Address	SSID	Band	Authentication	Signal	Add

Upload ACL File

Upload File : Choose File No file chosen Upload

Download ACL File

Load ACL File to Local Hard Driver : Download

Save

WLAN Partition

This page allows the user to configure a WLAN Partition.

Wireless Band: Displays the current wireless band.

Link Integrity: Select **Enable** or **Disable**. If the Ethernet connection between the LAN and the AP is disconnected, enabling this feature will cause the wireless segment associated with the AP to be disassociated from the AP.

Ethernet WLAN Access: The default is Enable. When disabled, all data from the Ethernet to associated wireless devices will be blocked. Wireless devices can still send data to the Ethernet.

Internal Station Connection: The default value is Enable, which allows stations to intercommunicate by connecting to a target AP. When disabled, wireless stations cannot exchange data on the same Multi-SSID. In Guest mode, wireless stations cannot exchange data with any station on your network.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

WLAN Partition

Wireless Band 2.4GHz ▾

Link Integrity Disable ▾

Ethernet to WLAN Access Enable ▾

Internal Station Connection

Primary SSID	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	<input type="radio"/> Guest mode
Multi-SSID 1	<input type="radio"/> Enable	<input type="radio"/> Disable	<input type="radio"/> Guest mode
Multi-SSID 2	<input type="radio"/> Enable	<input type="radio"/> Disable	<input type="radio"/> Guest mode
Multi-SSID 3	<input type="radio"/> Enable	<input type="radio"/> Disable	<input type="radio"/> Guest mode
Multi-SSID 4	<input type="radio"/> Enable	<input type="radio"/> Disable	<input type="radio"/> Guest mode
Multi-SSID 5	<input type="radio"/> Enable	<input type="radio"/> Disable	<input type="radio"/> Guest mode
Multi-SSID 6	<input type="radio"/> Enable	<input type="radio"/> Disable	<input type="radio"/> Guest mode
Multi-SSID 7	<input type="radio"/> Enable	<input type="radio"/> Disable	<input type="radio"/> Guest mode

IP Filter Settings

Enter the IP address or network address that will be used in the IP filter rule (e.g. an IP address like 192.168.70.66 or a network address like 192.168.70.0). This IP address or network will be inaccessible to wireless clients in this network.

Wireless Band: Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz 1 or 5GHz 2.

SSID Index: Click the drop-down menu to select the SSID for the IP filter.

Filter State: Click the drop-down menu to enable or disable the filter state. By default this feature is disabled.

IP Address: Enter the IP address or network address.

Subnet Mask: Enter the subnet mask of the IP address or networks address.

IP Address List: When an IP address is entered, it appears in the list. Highlight an IP address and click **Delete** icon to remove it from the list.

Upload IP Filter File: To upload the IP filter list file, click **Choose File** and navigate to the IP filter list file saved on the computer, and then click **Upload**.

Download IP Filter File: To download the IP Filter list file, click **Download** and to save the IP filter list.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

The screenshot shows the 'IP Filter Settings' web interface. It features a form with the following fields and controls:

- Wireless Band:** A dropdown menu set to '5GHz'.
- SSID Index:** A dropdown menu set to 'Primary SSID'.
- Filter State:** A dropdown menu set to 'Disable'.
- IP Address:** An empty text input field.
- Subnet Mask:** An empty text input field.
- Add:** A button to add a new filter rule.

Below the form is a table with the following columns: ID, IP Address, Subnet Mask, and Delete. The table is currently empty.

At the bottom of the interface, there are two sections for file management:

- Upload IP Filter File:** Includes a file selection button labeled 'Choose File' (which shows 'No file chosen') and an 'Upload' button.
- Download IP Filter File:** Includes a 'Download' button.

A 'Save' button is located at the bottom right of the interface.

Traffic Control

Uplink/Downlink Setting

The uplink/downlink setting allows users to customize the downlink and uplink interfaces including specifying downlink/uplink bandwidth rates in Mbits per second. These values are also used in the QoS and Traffic Manager windows. Once the desired uplink and downlink settings are finished, click the **Save** button to let your changes take effect.

Downlink Bandwidth: The downlink bandwidth in Mbits per second.

Uplink Bandwidth: The uplink bandwidth in Mbits per second.

Click to save the updated configuration.

Save: To make the updates permanent, click Configuration > **Save and Activate**.

The screenshot shows the 'Uplink and Downlink Setting' configuration window. At the top, there are radio buttons for 'Ethernet', 'Downlink', and 'Uplink'. Below this, there are three tabs: '2.4GHz', '5GHz 1', and '5GHz 2'. The '2.4GHz' tab is selected. The window is divided into two main sections: 'Downlink Interface' and 'Uplink Interface'. Each section contains a grid of checkboxes for 'Primary-ssid' and 'Multi-ssid1' through 'Multi-ssid7'. At the bottom of the window, there are two input fields: 'Downlink Bandwidth(1~867)' with a value of '100' and 'Uplink Bandwidth(1~867)' with a value of '100', both labeled 'Mbits/sec'. A 'Save' button is located at the bottom right of the window.

QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications. The DAP-2720 supports four priority levels. Once the desired QoS settings are finished, click the **Save** button to let your changes take effect.

Enable QoS: Check this box to allow QoS to prioritize traffic. Use the drop-down menus to select the four levels of priority. Click the Save button when you are finished.

Downlink Bandwidth: The downlink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

Uplink Bandwidth: The uplink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

ACK/DHCP/ICMP/DNS Priority: Click the drop-down menu to select the level of priority for the selected rule.

Web Traffic Priority: Click the drop-down menu to select the level of priority for the selected rule.

FTP Traffic Priority: Click the drop-down menu to select the level of priority for the selected rule.

User Defined-1/2/3/4 Priority: Click the drop-down menu to select the level of priority for the selected rule.

Other Traffic Priority: Click the drop-down menu to select the level of priority for the selected rule.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

The screenshot shows the QoS configuration interface. At the top, there is a title bar 'QoS' and an 'Enable QoS' checkbox. Below this is the 'Advanced QoS' section. It contains several rows of configuration options:

Category	Priority	Limit	% Port
Downlink Bandwidth		100	Mbits/sec
Uplink Bandwidth		100	Mbits/sec
ACK/DHCP/ICMP/DNS Priority	Highest Priority	100	53,67,68,546,547
Mail Traffic Priority	Second Priority	100	25,110,465,995
Web Traffic Priority	Third Priority	100	80,443,3128,8080
Ftp Traffic Priority	Low Priority	100	20,21
User Defined-1 Priority	Highest Priority	100	0 - 0
User Defined-2 Priority	Second Priority	100	0 - 0
User Defined-3 Priority	Third Priority	100	0 - 0
User Defined-4 Priority	Low Priority	100	0 - 0
Other Traffic Priority	Low Priority	100	%

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

Traffic Manager

The traffic manager feature allows users to create traffic management rules that specify how to deal with listed client traffic and specify downlink/ uplink speeds for new traffic manager rules. Click the **Save** button to let your changes take effect.

Traffic Manager: Use the drop-down menu to **Enable** the traffic manager feature.

Unlisted Client Traffic: Select **Deny** or **Forward** to determine how to deal with unlisted client traffic.

Downlink Bandwidth: The downlink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

Uplink Bandwidth: The uplink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

Name: Enter the name of the traffic manager rule.

Client IP (optional): Enter the client IP address of the traffic manager rule.

Client MAC (optional): Enter the client MAC address of the traffic manager rule.

Downlink Speed: Enter the downlink speed in Mbits per second.

Uplink Speed: Enter the uplink speed in Mbits per second.

Save: Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

Traffic Manager

Traffic Manager

Unlisted Clients Traffic Deny Forward

Downlink Bandwidth Mbits/sec

Uplink Bandwidth Mbits/sec

Add Traffic Manager Rule

Name

Client IP (optional)

Client MAC (optional)

Downlink Speed Mbits/sec

Uplink Speed Mbits/sec

Traffic Manager Rules

Name	Client IP	Client MAC	Downlink Speed	Uplink Speed	Edit	Del
<input type="button" value="Save"/>						

Status

In the Status Section the user can monitor and view the configuration settings of the access point. Here the user can also view statistics about client information, WDS information and more. The following pages will explain settings found in the Status section in more detail.

The screenshot displays the D-Link DAP-2720 web interface. The top navigation bar includes Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view with the following items: DAP-2720, Basic Settings, Advanced Settings, Status, Device Information, Client Information, WDS Information, Channel Analyze, Statistics, and Log. The main content area is titled "Device Information" and contains the following data:

Device Information	
Firmware Version:v1.00	
Ethernet MAC Address:	00:15:e9:2c:75:00
Wireless MAC Address(2.4GHz):	Primary: 00:15:e9:2c:75:00 SSID 1~7: 00:15:e9:2c:75:01 ~ 00:15:e9:2c:75:07
Wireless MAC Address(5GHz 1):	Primary: 00:15:e9:2c:75:10 SSID 1~7: 00:15:e9:2c:75:11 ~ 00:15:e9:2c:75:17
Wireless MAC Address(5GHz 2):	Primary: 00:15:e9:2c:75:08 SSID 1~7: 00:15:e9:2c:75:09 ~ 00:15:e9:2c:75:0f
Ethernet	
IP Address	10.10.10.39
Subnet Mask	255.255.255.0
Gateway	10.10.10.254
DNS	168.95.192.1 168.95.1.1
Wireless (2.4GHz)	
Network Name (SSID)	dlink
Channel	
Data Rate	Auto
Security	None
Wireless (5GHz 1)	
Network Name (SSID)	dlink
Channel	
Data Rate	Auto
Security	None
Wireless (5GHz 2)	
Network Name (SSID)	dlink
Channel	
Data Rate	Auto
Security	None
Device Status	
CPU Utilization	0%
Memory Utilization	20%
Nuclias Connect	
Connection Status	Disconnect
Server IP/PORT	
Group ID	

Device Information

This page displays information like firmware version, Ethernet and wireless parameters, as well as the information regarding CPU and memory utilization.

Device Information: This read-only window displays the configuration settings of the DAP-2720, including the firmware version and the device's MAC address.

Device Information	
Firmware Version:v1.00	
Ethernet MAC Address:	00:15:e9:2c:75:00
Wireless MAC Address(2.4GHz):	Primary: 00:15:e9:2c:75:00 SSID 1~7: 00:15:e9:2c:75:01 ~ 00:15:e9:2c:75:07
Wireless MAC Address(5GHz 1):	Primary: 00:15:e9:2c:75:10 SSID 1~7: 00:15:e9:2c:75:11 ~ 00:15:e9:2c:75:17
Wireless MAC Address(5GHz 2):	Primary: 00:15:e9:2c:75:08 SSID 1~7: 00:15:e9:2c:75:09 ~ 00:15:e9:2c:75:0f
Ethernet	
IP Address	10.10.10.39
Subnet Mask	255.255.255.0
Gateway	10.10.10.254
DNS	168.95.192.1 168.95.1.1
Wireless (2.4GHz)	
Network Name (SSID)	dlink
Channel	
Data Rate	Auto
Security	None
Wireless (5GHz 1)	
Network Name (SSID)	dlink
Channel	
Data Rate	Auto
Security	None
Wireless (5GHz 2)	
Network Name (SSID)	dlink
Channel	
Data Rate	Auto
Security	None
Device Status	
CPU Utilization	0%
Memory Utilization	20%
Nuclias Connect	
Connection Status	Disconnect
Server IP/PORT	
Group ID	

Client Information

This page displays the associated client's SSID, MAC, band, authentication method, signal strength, and power saving mode for the DAP-2720 network.

Client Information: This window displays the wireless client information for clients currently connected to the DAP-2720.

SSID: Displays the SSID of the client.

MAC: Displays the MAC address of the client.

Band: Displays the wireless band that the client is connected to.

Authentication: Displays the type of authentication being used.

RSSI: Displays the client's signal strength.

Power Saving Mode: Displays the status of the power-saving feature.

System Info: Displays the associated clients' OS information for the network.

Client Information							
Client Information		Station association(2.4GHz) : 0					
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode	System Info	
Client Information		Station association(5GHz 1) : 0					
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode	System Info	
Client Information		Station association(5GHz 2) : 0					
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode	System Info	

WDS Information Page

This page displays the access point's SSID, MAC, band, authentication method, signal strength, and status for the DAP-2720's Wireless Distribution System network.

WDS Information: This window displays the Wireless Distribution System information for clients currently connected to the DAP-2720.

Name: Displays the SSID of the client.

MAC: Displays the MAC address of the client.

Authentication: Displays the type of authentication being used.

Signal: Displays the client's signal strength.

Status: Displays the status of the power saving feature.

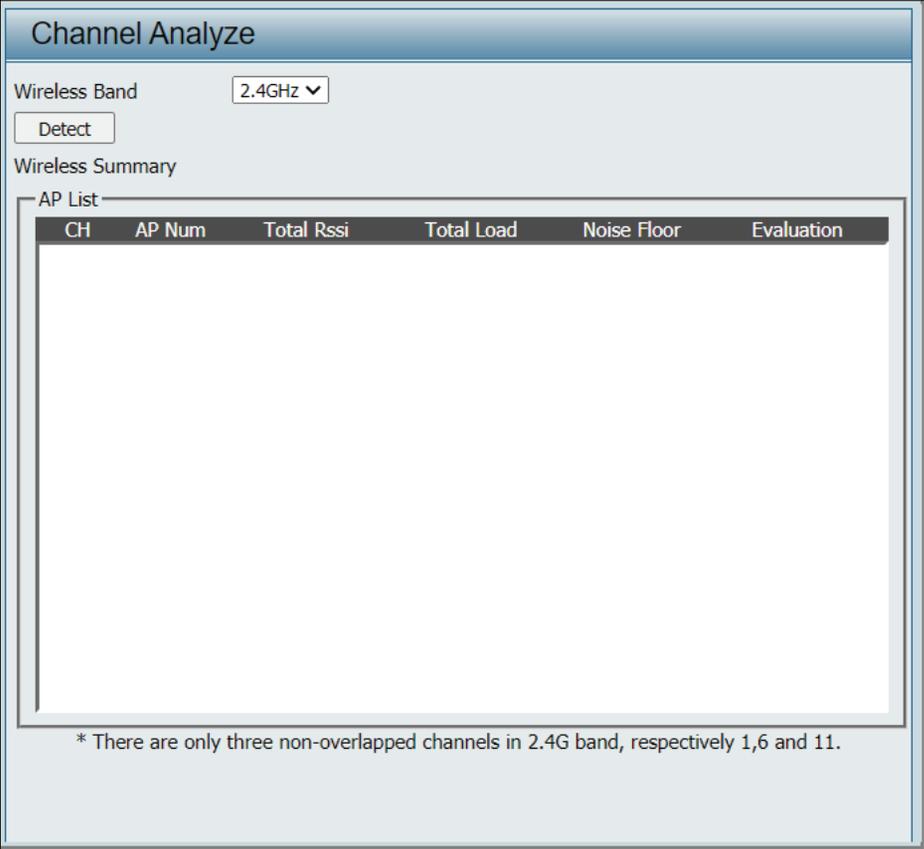
WDS Information				
WDS Information		Channel : (2.407 GHz)		
Name	MAC	Authentication	Signal	Status
WDS Information		Channel : (5 GHz 1)		
Name	MAC	Authentication	Signal	Status
WDS Information		Channel : (5 GHz 2)		
Name	MAC	Authentication	Signal	Status

Channel Analyze

Wireless Band: Select 2.4Ghz or 5GHz 1 or 5GHz 2.

Detect: Click the Detect button to scan.

AP List: This will list the transmitting channels and quality.



Channel Analyze

Wireless Band 2.4GHz ▾

Wireless Summary

AP List

CH	AP Num	Total Rssi	Total Load	Noise Floor	Evaluation
----	--------	------------	------------	-------------	------------

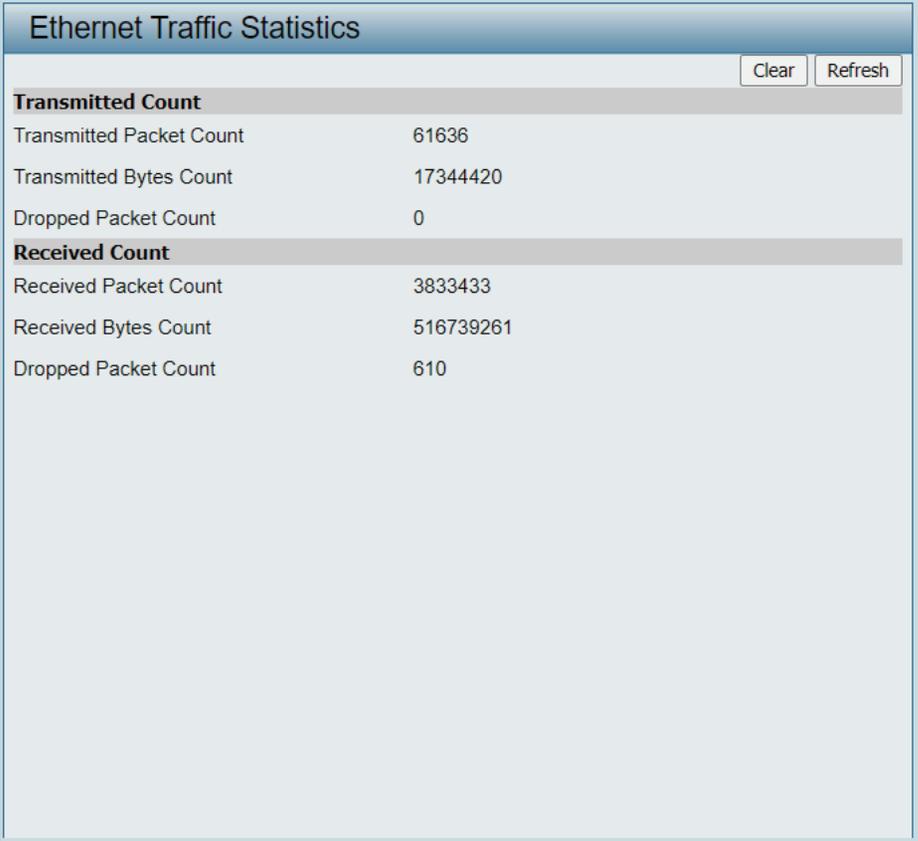
* There are only three non-overlapped channels in 2.4G band, respectively 1,6 and 11.

Statistics

Ethernet Traffic Statistics

Displays wired interface network traffic information.

Ethernet Traffic Statistics: This page displays transmitted and received count statistics for packets and bytes.



The screenshot shows a web interface titled "Ethernet Traffic Statistics". At the top right of the interface are two buttons: "Clear" and "Refresh". The data is organized into two sections: "Transmitted Count" and "Received Count". Each section contains three rows of data: "Transmitted Packet Count", "Transmitted Bytes Count", and "Dropped Packet Count".

Transmitted Count	
Transmitted Packet Count	61636
Transmitted Bytes Count	17344420
Dropped Packet Count	0

Received Count	
Received Packet Count	3833433
Received Bytes Count	516739261
Dropped Packet Count	610

WLAN Traffic Statistics

Displays throughput, transmitted frame, received frame, and error information for the AP network.

WLAN Traffic Statistics: This page displays wireless network statistics for data throughput, transmitted and received frames, and frame errors.

WLAN Traffic Statistics			
	2.4GHz	5GHz 1	5GHz 2
Transmitted Count			
Transmitted Packet Count	0	0	0
Transmitted Bytes Count	0	0	0
Dropped Packet Count	0	0	0
Transmitted Retry Count	0	0	0
Received Count			
Received Packet Count	0	0	0
Received Bytes Count	0	0	0
Dropped Packet Count	0	0	0
Received CRC Count	0	0	0
Received Decryption Error Count	0	0	0
Received MIC Error Count	0	0	0
Received PHY Error Count	0	0	0

Log

View Log

The AP's embedded memory holds logs here. The log information includes but is not limited to the following items: cold start AP, upgrading firmware, client association with APs, and web login. The web page holds up to 500 logs.

View Log: The AP's embedded memory displays system and network messages including a time stamp and message type. The log information includes but is not limited to the following items: cold start AP, upgrading firmware, client association with APs, and web login. The web page holds up to 500 logs.

View Log				
<input type="button" value="First Page"/>	<input type="button" value="Last Page"/>	<input type="button" value="Previous"/>	<input type="button" value="Next"/>	<input type="button" value="Clear"/>
Page 1 of 14				
Time	Priority	Message		
Jun 3 10:39:01	[SYSACT]	Web login success from 172.17.6.10		
Jun 3 10:26:56	[SYSACT]	Web login success from 172.17.6.10		
Jun 3 10:15:37	[SYSACT]	Web login success from 172.17.6.10		
Jun 3 09:55:05	[Wireless]	External DHCP Server assign IP 172.17.6.88 TO Mac :8c:16:45:5d:8c:9e		
Jun 3 09:51:42	[Wireless]	External DHCP Server assign IP 172.17.6.120 TO Mac :c:54:e1:ad:76:b4:95		
Jun 3 09:43:47	[Wireless]	External DHCP Server assign IP 172.17.6.129 TO Mac :ec:f4:bb:20:56:1a		
Jun 3 09:41:05	[Wireless]	External DHCP Server assign IP 172.17.6.69 TO Mac :94:c6:91:b2:50:53		
Jun 3 09:38:37	[Wireless]	External DHCP Server assign IP 172.17.6.80 TO Mac :54:e1:ad:7b:16:a3		
Jun 3 09:35:43	[Wireless]	External DHCP Server assign IP 172.17.6.95 TO Mac :54:e1:ad:a1:c2:f1		
Jun 3 09:31:35	[Wireless]	External DHCP Server assign IP 172.17.6.17 TO Mac :50:7b:9d:01:b1:e8		
Jun 3 09:21:35	[Wireless]	External DHCP Server assign IP 172.17.6.22 TO Mac :04:0e:3c:41:2f:00		
Jun 3 09:18:59	[Wireless]	External DHCP Server assign IP 172.17.6.18 TO Mac :44:37:e6:52:6e:85		
Jun 3 09:12:14	[Wireless]	External DHCP Server assign IP 172.17.6.121 TO Mac :8c:16:45:5d:90:d8		
Jun 3 09:09:53	[Wireless]	External DHCP Server assign IP 172.17.6.14 TO Mac :64:00:6a:6e:a2:b2		
Jun 3 09:09:40	[Wireless]	External DHCP Server assign IP 172.17.6.74 TO Mac :54:e1:ad:98:b6:e4		
Jun 3 09:08:41	[Wireless]	External DHCP Server assign IP 172.17.6.57 TO Mac :28:d2:44:cb:8b:d7		
Jun 3 08:58:34	[Wireless]	External DHCP Server assign IP 172.17.6.97 TO Mac :94:c6:91:8c:c0:8e		
Jun 3 08:54:16	[Wireless]	External DHCP Server assign IP 172.17.6.13 TO Mac :94:c6:91:07:e6:e7		

Log Settings

Enter the log server's IP address to send the log to that server. Check or uncheck System Activity, Wireless Activity, or Notice to specify what kind of log type you want it to log.

Log Server/IP Address: Enter the IP address of the server you would like to send the DAP-2720 log to.

Log Type: Check the box for the type of activity you want to log. There are three types: System Activity, Wireless Activity, and Notice.

EU directive Syslog Server Settings: Enter the IP address of the syslog server you would like to send the DAP-2720 log to.

E-mail Notification: Support Simple Mail Transfer Protocol for log schedule and periodical change key. It can not support Gmail SMTP port 465. Please set to Gmail SMTP port 25 or 587.

Log Settings

Log Settings

Log Server Settings

Log Server / IP Address

Log Type System Activity
 Wireless Activity
 Notice

EU directive Syslog Server Settings

Log Server / IP Address

Email Notification

Email Notification Enable

Outgoing mail server (SMTP)

Authentication Enable

SSL/TLS Enable

From Email Address

To Email Address

Email Server Address

SMTP Port

User Name

Password

Confirm Password

Email Log Schedule

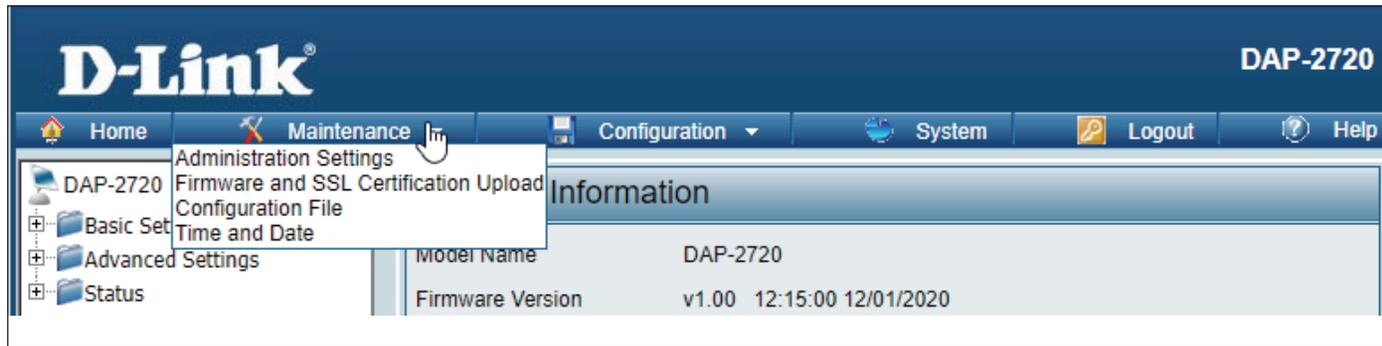
Schedule hours or when Log is full

Save

- Outgoing Mail Server (SMTP):** Click the drop-down menu to select the SMTP server type; options include: Internal, Gmail, Hotmail.
- Authentication:** Check the box to enable the authentication of the email notification.
- SSL/TLS:** Check the box to enable the SSL/TLS function.
- From Email Address:** Enter the email address.
- To Email Address:** Enter the email address.
- Email Server Address:** Enter the email server address.
- SMTP Port:** Enter the SMTP port.
- User Name:** Enter the name of the new user entry.
- Password:** Enter the password set for the email notification.
- Confirm Password:** Retype the password entry to confirm the password.
- E-mail Log Schedule:** Use the drop-down menu to set the email log schedule.
- Save:** Click to save the updated configuration. To make the updates permanent, click Configuration > **Save and Activate**.

Maintenance Section

In the Status Section the user can monitor and view configuration settings of the access point. Here the user can also view statistics about client information, WDS information and more. The following pages will explain settings found in the maintenance section in more detail.



Administration

Limit Administrator

Check one or more of the eight main categories to display the various hidden administrator parameters and settings displayed on the next five pages. Each of the eight main categories display various hidden administrator parameters and settings.

Limit Administrator VLAN ID: Check the box provided and the ID: enter the specific VLAN ID that the administrator will be allowed to log in from.

Limit Administrator IP: Check to enable the Limit Administrator IP address.

IP Range: Enter the IP address range that the administrator will be allowed to log in from and then click the Add button.

The screenshot shows the 'Administration Settings' interface. The 'Limit Administrator' section is active, indicated by a checkmark. It contains the following fields and controls:

- Limit Administrator VLAN ID:** A checkbox labeled 'Enable' is checked. Next to it is a text input field containing the number '1'.
- Limit Administrator IP:** A checkbox labeled 'Enable' is unchecked.
- IP Range:** Two text input fields labeled 'From:' and 'To:' are present. Below them is a button labeled 'Add'.

Below these fields is a table with the following columns: 'Item', 'From', 'To', and 'Delete'. The table is currently empty.

At the bottom of the page, there is a 'Save' button. Above the table, there are several expandable sections, each with a minus sign icon:

- System Name Settings
- Login Settings
- Console Settings
- SNMP Settings
- Ping Control Setting
- LED Settings
- DDP Control Setting
- Router Setting
- Country Settings
- Nuclias Connect Setting

System Name Settings

System Name: The name of the device. The default name is D-Link DAP-2720.

Location: The physical location of the device, e.g. 72nd Floor, D-Link HQ.

MDNS Name : The MDNS name of the device. The default MDNS name is dap2720

System Name Settings <input checked="" type="checkbox"/>	
System Name	<input type="text" value="dap2720"/>
Location	<input type="text"/>
MDNS Name	<input type="text" value="dap2720"/>

Login Settings

Login Name: Enter a user name. The default is **admin**.

New Password: When changing your password, enter the new password here. The password is case-sensitive. "A" is a different character than "a." The length should be between 0 and 12 characters.

Confirm Password: Enter the new password a second time for confirmation purposes.

Login Settings <input checked="" type="checkbox"/>	
Login Name	<input type="text" value="admin"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/> <input type="checkbox"/> Apply New Password

Console Settings

Status: Status is enabled by default. Uncheck the box to disable the console.

Console Protocol: Select the type of protocol you would like to use, Telnet or SSH.

Time-out: Set to 1 Min, 3 Mins, 5 Mins, 10 Mins, 15 Mins or Never.

Console Settings <input checked="" type="checkbox"/>	
Status	<input checked="" type="checkbox"/> Enable
Console Protocol	<input checked="" type="radio"/> Telnet <input type="radio"/> SSH
Timeout	<input type="text" value="3 Mins"/>

SNMP Settings

Status: Check the box to enable the SNMP functions. This is disabled by default.

Public Community String: Enter the public SNMP community string.

Private Community String: Enter the private SNMP community string.

Trap Status: Check the box to enable the Trap function. This is disabled by default.

Trap Server IP: Enter the Trap sever IP address.

Ping Control Setting

Status: Status is enabled by default. Uncheck the box to disable ping control.

LED Settings

LED Status: Select the LED on/off you would like to use.

DDP Setting

Status: Status is enabled by default. Uncheck the box to disable DDP control.

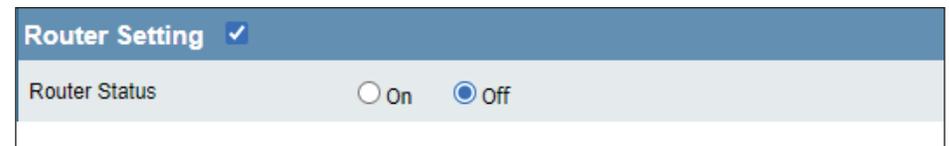


DDP Control Setting

Status Enable

Router Settings

Router Status: Select on/off for the Router Mode.

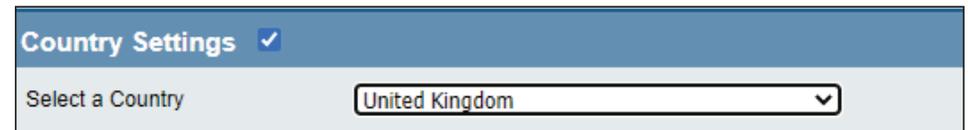


Router Setting

Router Status On Off

Country Setting

Select a Country: Choose from drop down list country where device is located.



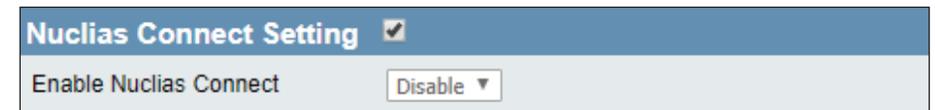
Country Settings

Select a Country

Nuclias Connect Settings

The Nuclias Connect section is used to create a set of APs on the Internet to be organized into a single group in order to increase ease of management. Nuclias Connect and AP Array are mutually exclusive functions.

Enable Nuclias Connect: Click the drop-down menu to enable or disable Nuclias Connect.



Nuclias Connect Setting

Enable Nuclias Connect

Note: To save the new configuration settings to the firmware, click **Configuration > Save and Activate**, otherwise click **Discard Changes** to delete any setting change.

Firmware and SSL Upload

This page allows the user to perform a firmware upgrade. This upgrades the software running on the hardware used by the access point. This is a useful feature that prevents future bugs and allows for new features to be added to this product. Please go to your local D-Link website to see if there is a newer version firmware available.

Firmware and SSL Certification Upload: You can upload files to the access point.

Upload Firmware from Local Hard Drive: The current firmware version is displayed above the file location field. After the latest firmware is downloaded, click on the "Choose File" button to locate the new firmware. Once the file is selected, click on the "Open" and "Upload" buttons to begin updating the firmware. Please don't turn the power off while upgrading.

Language Pack Upgrade : After you have downloaded a language pack to your local drive, click "Choose File." Select the language pack and click "Open" and "Upload" to complete the upgrade.

Upload SSL Certification from Local Hard Drive: After you have downloaded a SSL certification to your local drive, click "Choose File." Select the certification and click "Open" and "Upload" to complete the upgrade.

The screenshot shows a web interface titled "Firmware and SSL Certification Upload". It contains three main sections:

- Update Firmware From Local Hard Drive:** Displays "Firmware Version v1.00" and includes a label "Upload Firmware From File :", a "Choose File" button, a "No file chosen" text, and an "Upload" button.
- Language Pack Upgrade:** Includes a label "Upload :", a "Choose File" button, a "No file chosen" text, and an "Upload" button.
- Update SSL Certification From Local Hard Drive:** Includes a label "Upload Certificate From File :", a "Choose File" button, a "No file chosen" text, and an "Upload" button.

At the bottom, there is another label "Upload Key From File :" with a "Choose File" button, a "No file chosen" text, and an "Upload" button.

Configuration File Upload

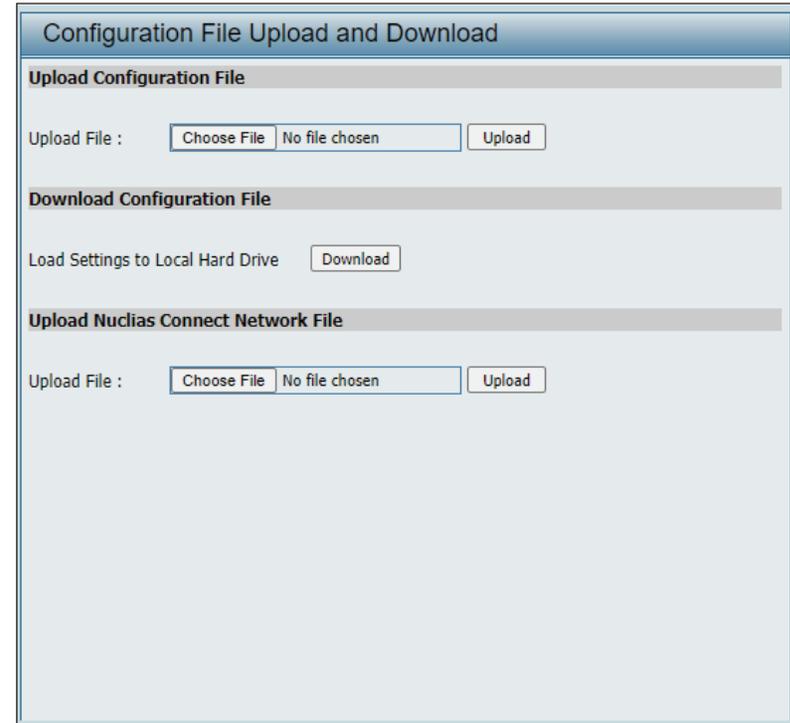
This page allows the user to back up and recover the current configuration of the access point in case of a unit failure.

Configuration File Upload and Download: You can upload and download configuration files of the access point.

Upload Configuration File: Browse to the saved configuration file you have in your local drive and click "Open" and "Upload" to update the configuration.

Download Configuration File: Click "Download" to save the current configuration file to your local disk. Note that if you save one configuration file with the administrator's password now, after resetting your DAP-2720 and then updating to this saved configuration file, the password will be gone.

Upload Nuclias Connect Network File: Browse to the saved Nuclias Connect Network file you have in your local drive and click "Open" and "Upload" to upload the CWM file .



The screenshot shows a web interface titled "Configuration File Upload and Download". It is divided into three main sections:

- Upload Configuration File:** This section contains a label "Upload File:" followed by a text input field with the placeholder "Choose File" and "No file chosen", and an "Upload" button.
- Download Configuration File:** This section contains a label "Load Settings to Local Hard Drive" followed by a "Download" button.
- Upload Nuclias Connect Network File:** This section contains a label "Upload File:" followed by a text input field with the placeholder "Choose File" and "No file chosen", and an "Upload" button.

Time and Date Settings

Enter the NTP server IP, choose the time zone, and enable or disable daylight saving time.

Current Time: Displays the current time and date settings.

Enable NTP Server: Check to enable the AP to get system time from an NTP server from the Internet.

NTP Server: Enter the NTP server IP address.

Time Zone: Use the drop-down menu to select your correct Time Zone.

Enable Daylight Saving: Check the box to enable Daylight Saving Time.

Set the Date and Time Manually: A user can either manually set the time for the AP here, or click the Copy Your Computer's Time Settings button to copy the time from the computer in use (Make sure that the computer's time is set correctly).

Time and Date Settings

Time Configuration

Current Time 01/03/2019 00:15:17

Automatic Time Configuration

Enable NTP

NTP Server

Time Zone (GMT+08:00) Kuala Lumpur, Singapore

Set the Date and Time Manually

Date And Time Year 2021 Month Jun Day 3

Hour 10 Minute 10 Second 14

Copy Your Computer's Time Settings

Daylight Configuration

Enable Daylight Saving

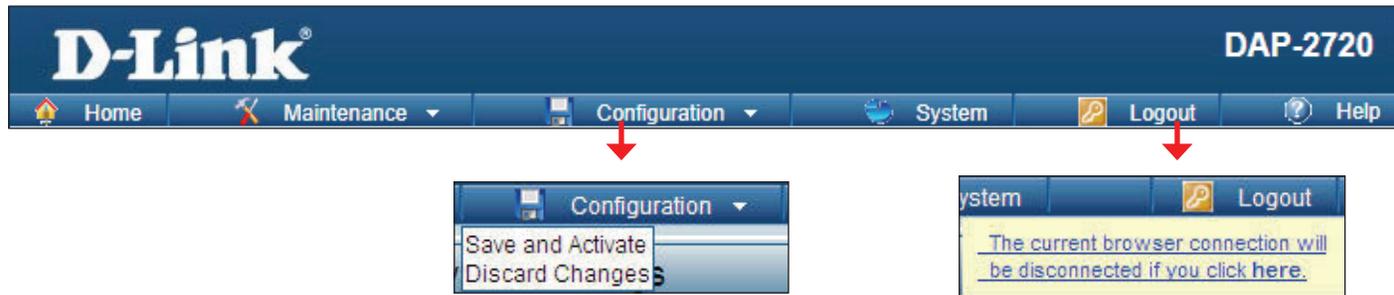
Daylight Saving Offset 15

	Month	Week	Day	Hour	Minute
Daylight Saving Dates DST Start	Jan	1st	Sun	12 am	0
DST End	Jan	1st	Sun	12 am	0

Save

Configuration and System

These are the remaining options to choose from in the top menu. **Configuration** allows the user to save and activate or discard the configurations. **System** allows the user to restart the unit, perform a factory reset or clear the language pack settings. **Logout** allows the user to safely log out from the access point's web configuration. **Help** allows the user to read more about the given options to configure without the need to consult the manual. The following pages will explain settings found in the configuration and system section in more detail.



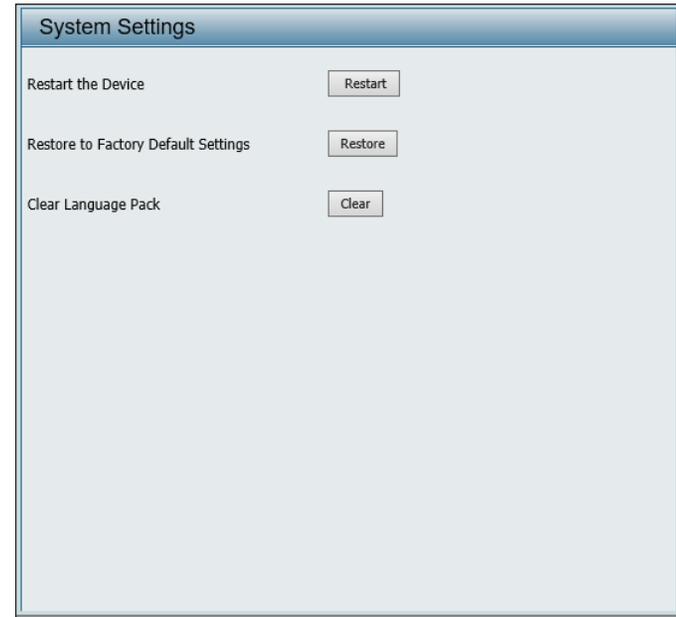
System Settings

On this page the user can restart the unit, perform a factory reset of the access point or clear the added language pack.

Restart the Device: Click Restart to restart the DAP-2720.

Restore to Factory Default Settings: Click Restore to restore the DAP-2720 back to factory default settings.

Clear Language Pack: Click to clear the current language pack.



Help

The help page is useful to view a brief description of a function available on the access point in case the manual is not present.

Help: Scroll down the Help page for topics and explanations.

Basic Settings

Wireless Settings

Allow you to change the wireless settings to fit an existing wireless network or to customize your wireless network.

Wireless Band
Operating frequency band. Choose 2.4GHz for visibility to legacy devices and for longer range. Choose 5GHz for least interference; interference can hurt performance. This AP will operate one band at a time.

Application
This option allows the user to choose for indoor or outdoor mode at the 5G Band.

Mode
Select a function mode to configure your wireless network. Function modes include AP, WDS (Wireless Distribution System) with AP, WDS and Wireless Client. Function modes are designed to support various wireless network topology and applications.

Network Name (SSID)
Also known as the Service Set Identifier, this is the name designated for a specific wireless local area network (WLAN). The factory default setting is "dlink". The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

SSID Visibility
Indicate whether or not the SSID of your wireless network will be broadcasted. The default value of SSID Visibility is set to "Enable," which allow wireless clients to detect the wireless network. By changing this setting to "Disable," wireless clients can no longer detect the wireless network and can only connect if they have the correct SSID entered.

Auto Channel Selection
If you check Auto Channel Scan, everytime when AP is booting up, the AP will automatically find the best channel to use. This is enabled by default.

Channel
Indicate the channel setting for the DAP-2553. By default, the AP is set to Auto Channel Scan. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

Channel Width
Allows you to select the channel width you would like to operate in. Select 20MHz if you are not using any 802.11n wireless clients. Auto 20/40MHz allows you to use both 802.11n and non-802.11n wireless devices in your network.

Authentication

Technical Specifications

Standards

- IEEE 802.11ac
- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.11a
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3at
- IEEE 802.3x

Network Management

- Web Browser interface (HTTP, Secure HTTP (HTTPS))
- NuLias Connect
- SNMP Support
- Command Line Interface (Telnet, Secure SSH Telnet)

Security

- WPA™ Personal/Enterprise
- WPA2™ Personal/Enterprise
- WEP™ 64-/128-bit

Wireless Frequency Range

- 2.4 to 2.4835 GHz and 5.15 to 5.85 GHz

Operating Voltage

- 12V/2.5A or 802.3at PoE

Antenna Type

- Six Internal Antennas (2x3dBi@2.4GHz & 2x3dBi@5-1GHz & 2x3dBi@5-2GHz)

LEDs

- Power/Status

Temperature

- Operating: 0°C to 40°C
- Storing: -20°C to 65°C

Humidity

- Operating: 10%~90% (non-condensing)
- Storing: 5%~95% (non-condensing)

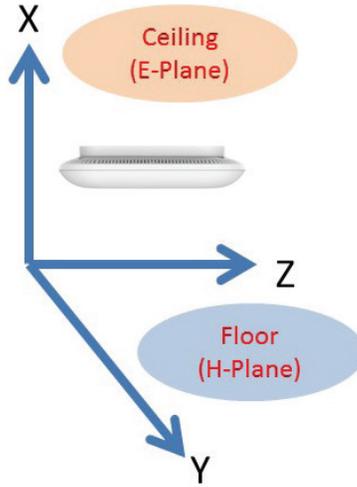
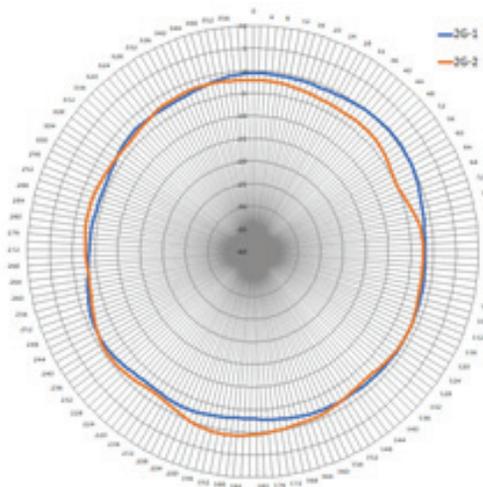
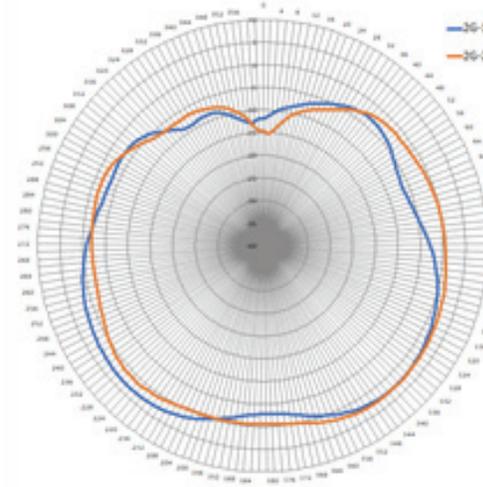
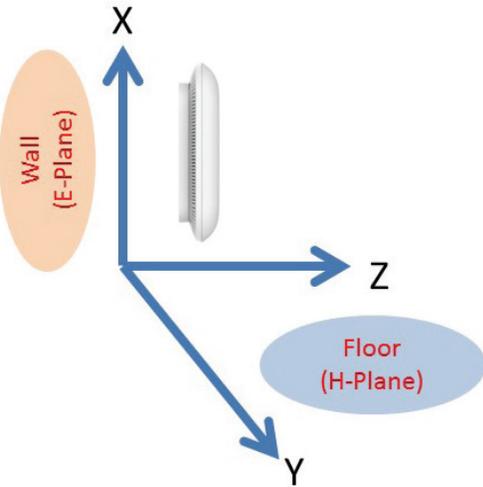
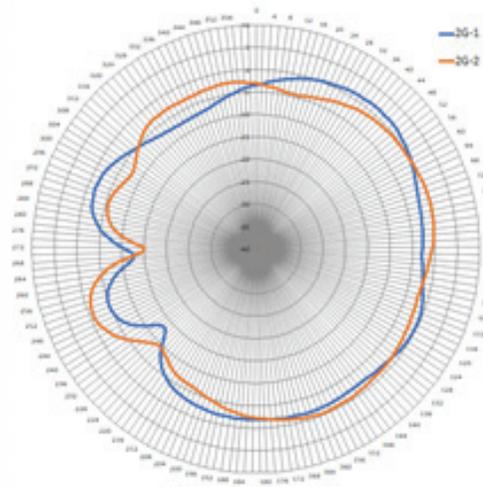
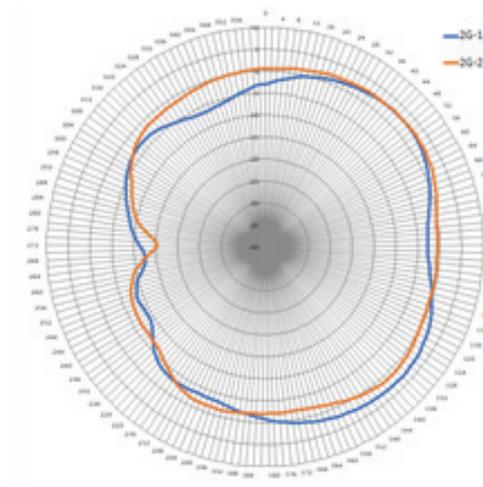
Certifications

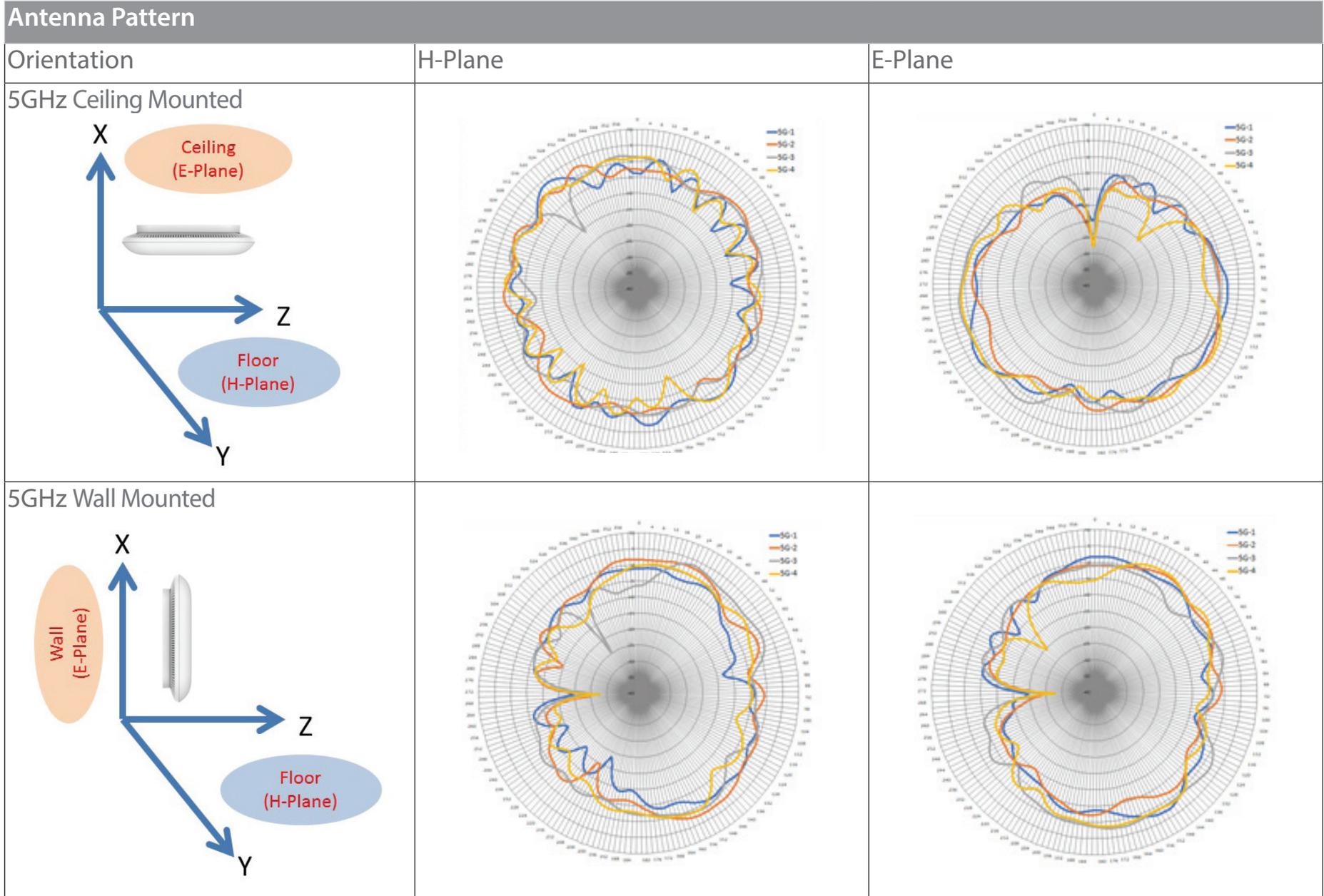
- FCC Class B
- CE
- UL
- RCM

Dimensions

- L = 212.4 mm (8.36 in)
- W = 212.4 mm (8.36 in)
- H = 47.7 mm (1.88 in)

Antenna Pattern

Antenna Pattern		
Orientation	H-Plane	E-Plane
<p>2.4GHz Ceiling Mounted</p> 		
<p>2.4GHz Wall Mounted</p> 		



Power Usage

This device is an Energy Related Product (ErP) with High Network Availability (HiNA), and automatically switches to a power-saving Network Standby mode within 1 minute of no packets being transmitted.

Network Standby: 5.065 watts