NUCLIAS CONNECT
DAP-2622 User Guide

V 1.03

nuclias connect

Table of Contents

Nuclias Connect 4
Introduction 4
Nuclias Connect Key Features 5
Package Contents 6
System Requirements 6

Hardware Overview 7
LEDs 7
Connections 7

Basic Installation 8
Hardware Setup 8
Method 1 - PoE with PoE Switch or Router 8
Method 2 - PoE without PoE Switch or Router 9

Setup Wizard 10

Web User Interface 11
Wireless 12
Access Point Mode 12
WDS with AP Mode 14
WDS Mode 16
Wireless Client Mode 18
Wireless Client Mode 19
Wireless Security 20
Wired Equivalent Privacy (WEP) 20
Wi-Fi Protected Access (WPA / WPA2) 21
LAN 23
IPv6 24
Advanced Settings 25
Performance 26
Wireless Resource Control 28
Multi-SSID 30
VLAN 32
VLAN List 32
Port List 33
Add/Edit VLAN 34
PVID Settings 35
Intrusion 36
Schedule 37
Internal RADIUS Server 38
ARP Spoofing Prevention 39
Bandwidth Optimization 40
Captive Portal 42
Authentication Settings - Web Redirection Only 42
Authentication Settings - Username/Password. 44
Authentication Settings - Passcode 46
Authentication Settings - Remote RADIUS 48
Authentication Settings - LDAP 50
Authentication Settings - POP3 52
Login Page Upload 54
MAC Bypass 55
DHCP Server 56
Dynamic Pool Settings 56
Static Pool Setting 57
Current IP Mapping List 58

Filters 59
Wireless MAC ACL 59
WLAN Partition 60
IP Filter Settings 61
Traffic Control 62
Uplink/Downlink Setting 62
QoS 63
Traffic Manager 64
Status 65
Device Information 66
Client Information 67
WDS Information Page 68
Stats Page 69
Ethernet Traffic Statistics 69
WLAN Traffic Statistics 70
Log 71
View Log 71
Log Settings 72
Maintenance Section 74
Administration 75
Limit Administrator 75
System Name Settings 76
Login Settings 76
Console Settings 76
Ping Control Setting 77
LED Settings 77
DDP Control Setting 78
Country Settings 78
Nuclias Connect Setting 78
Firmware and SSL Upload 79
Configuration File Upload 80
Time and Date Settings 81
Configuration and System 82
System Settings 83
Help 84

Technical Specifications 85

Antenna Pattern 86

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 (up to 1,000 APs), while retaining a robust and centralized management system. And with its intuitive Graphical User Interface (GUI), a wealth of enhanced AP features, and a setup wizard that supports 11 languages, Nuclias Connect minimizes the hassle of deployment, configuration, and administration.

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 Access Points (APs) without licensing charges, coupled with an inexpensive optional hardware controller (the 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 admins can grant localized management authority for local networks. In addition, because APs can support 8 SSIDs per radio (16 SSIDs per dual band APs), 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 & manage a variety of distributed deployments, including setting & 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, AD
- 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 DAP-2622, please refer to the Nuclias Connect User Guide.

Package Contents

- DAP-2622 Nuclias Connect AC1200 Wave 2 Wall-Plated Access Point
- Mounting Plate and Hardware

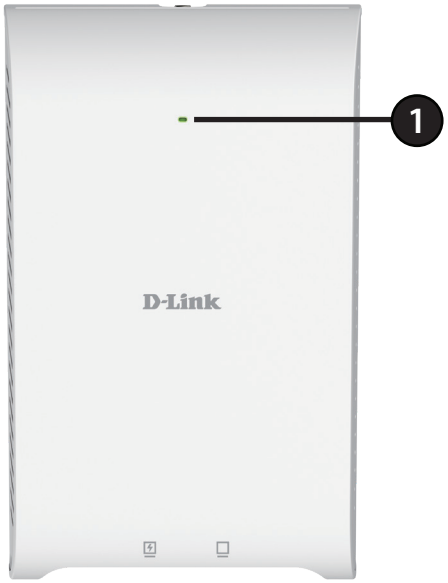
Note: No PSU supplied. To power the units use a D-Link 802.3at PoE switch or the D-Link DPE-301GI PoE injector.

System Requirements

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

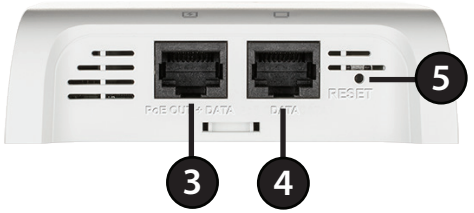
Hardware Overview

LEDs



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-2622 is working properly.

Connections

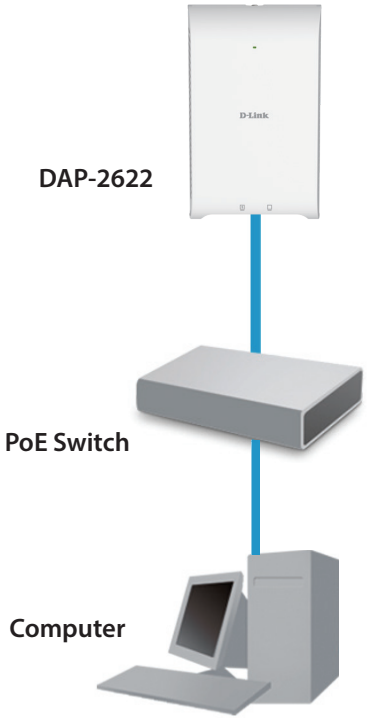


2	LAN (PoE) Port	Connect to a Power over Ethernet (PoE) switch or router via an Ethernet cable.
3	Lan (PoE Out) Port	Gigabit RJ-45 port for data and PSE out.
4	Ethernet LAN Port	Gigabit RJ-45 port for data.
5	Reset Button	Press and hold for five seconds to reset the access point to the factory default settings. Press and hold for ten seconds to reboot the access point.

Basic Installation
Hardware Setup

To power the access point, you can use one of the following 2 methods:

Method 1 - Use if you have a PoE switch or router
Method 2 - Use if you have a PoE injector and do not have a PoE-capable switch or router



Method 1 - PoE with PoE Switch or Router

Plug in one end of your Ethernet cable into the LAN port of the DAP-2622's back panel, and the other end into the port on a switch.

Configure the Access Point

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

2. Enter **dap2622.local** in the address field of your browser.

3. Log in to the Administration Web pages. The default login information is:
   Username: **admin**
   Password: **admin**

Method 2 - PoE without PoE Switch or Router

1. Connect one end of an Ethernet cable into the **Data In** port on the PoE base unit (not included) and the other end into one port on your switch, router, or computer.

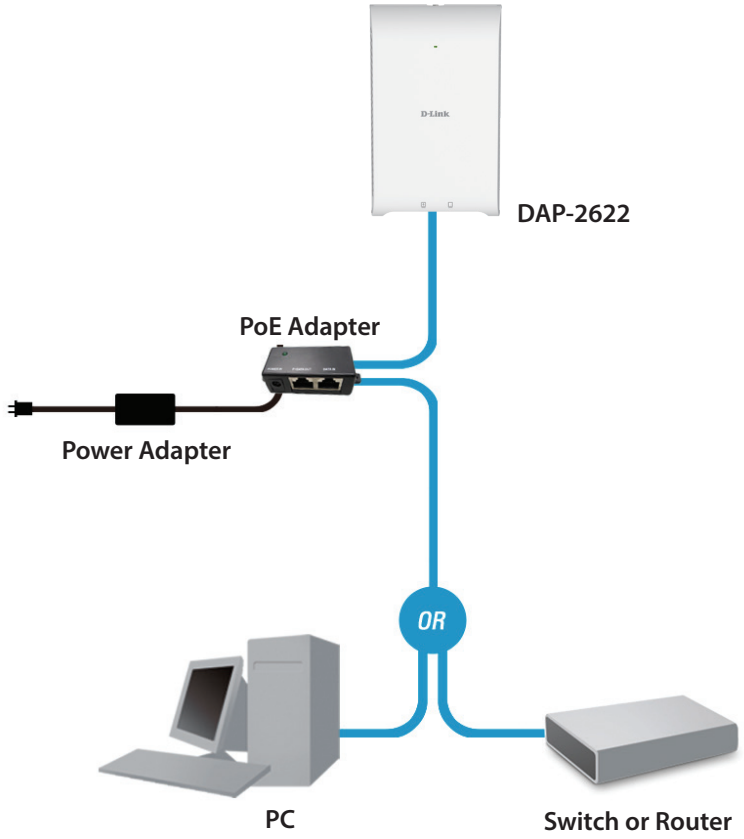
2. Connect one end of an Ethernet cable into the **P+Data Out** port on the PoE base unit and the other end into the LAN (PoE) port on the access point.

3. Use the supplied power adapter. Connect the power adapter to the **Power In** receptor on the PoE adapter.

4. Connect the power cable to the power adapter and then connect the other end into a power outlet.

5. Enter **dap2622.local** in the address field of your browser.

6. Log in to the Administration Web pages. The default login information is:
   Username: **admin**
   Password: **admin**



Setup Wizard

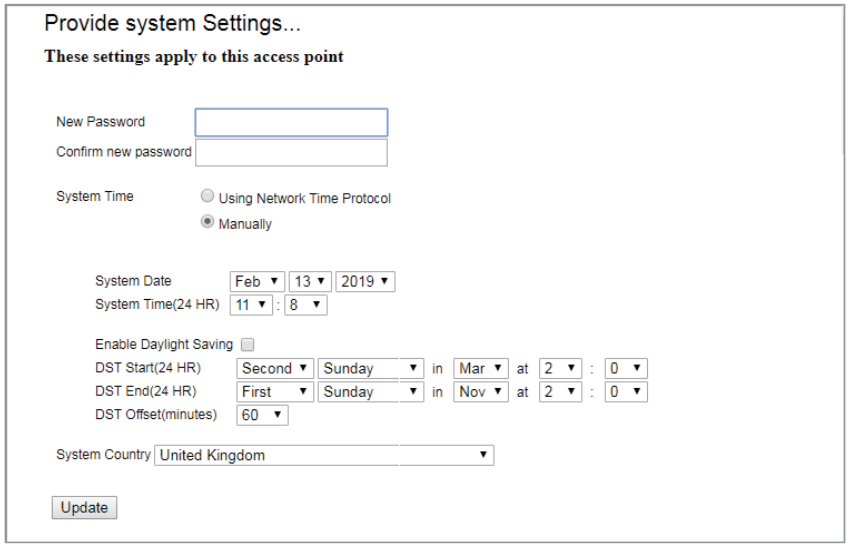
The first login instance displays the System Settings window which requires you to change the password used to access the web UI. Additional settings include the System Time and System Country functions.

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).

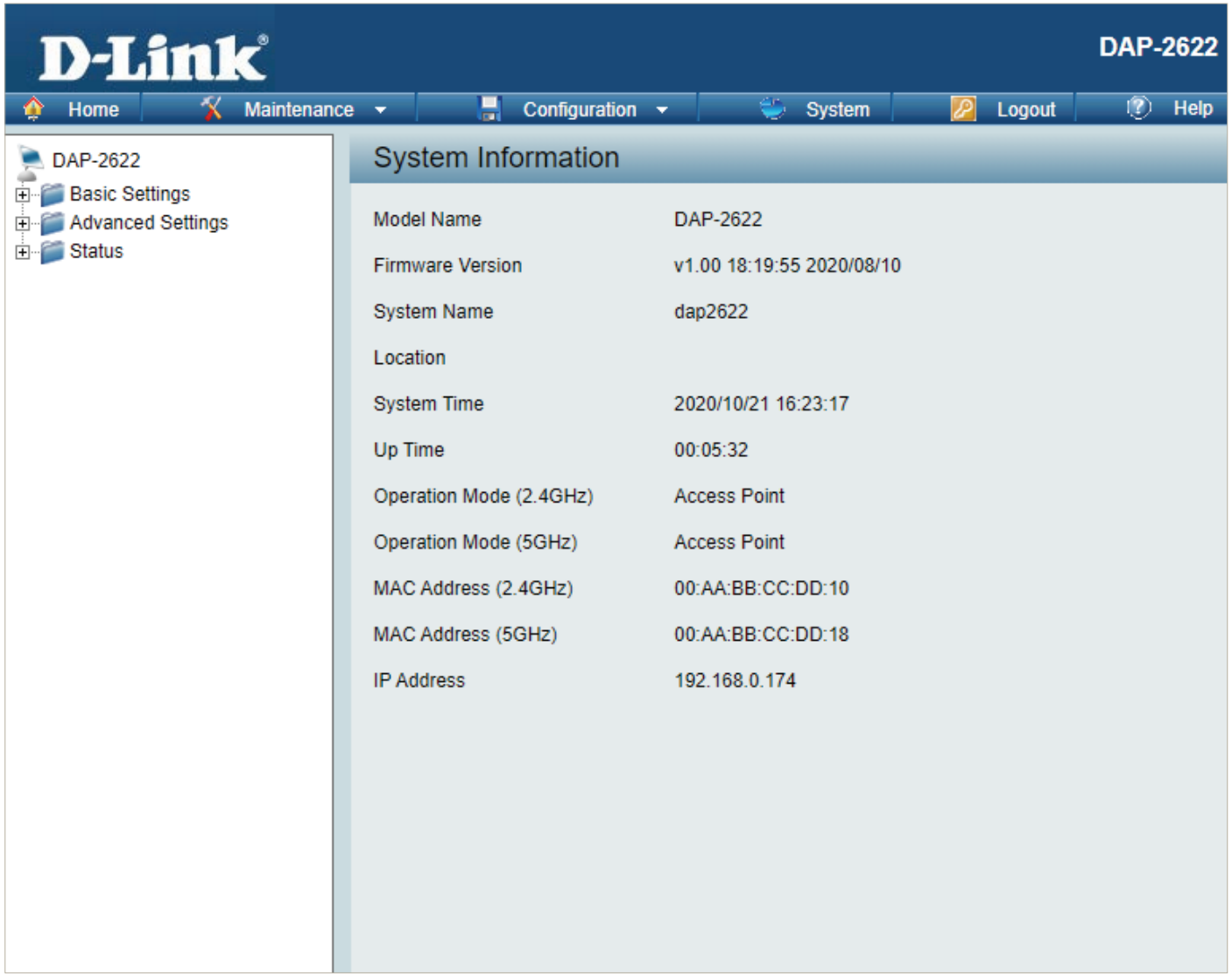
- **Setting NTP System Time**: Before trying to configure NTP, perform a ping test with the NTP server. In the NTP Server field, enter the NTP server to use. Then click the **Time Zone** drop-down menu and select the appropriate time zone.
- **Setting System Time Manually**: From the **System Date** 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 saving time (DST) function. Set the DST start and end time by clicking on the drop-down menus and setting the Month, Week, Day, Hour, and Minute of the DST starting days.
- **System Country**: Click the drop-down menu to select your country.

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



Web User Interface

The DAP-2622 supports an elaborate web user interface where the user can configure and monitor the device. Launch a web browser, type **dap2622.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**.



Wireless

On the wireless settings page, you can setup 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 either **2.4 GHz** or **5 GHz** from the drop-down menu.

Note: *2.4GHz and 5GHz bands should be configured individually with the following settings, each of which can have a different SSID, channel, authentication, etc.*

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: Click the drop-down menu to select **20 MHz, Auto 20/40 MHz** or **Auto 20/40/80 MHz**. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** allows you to connect to both 802.11n and 802.11b/g or 802.11a wireless devices on your network.

Authentication: Use the drop-down menu to choose **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 changes. 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.

Note: *The default Open System authentication allows wireless connection without requiring user authentication. It is highly recommended that you encrypt your network using one of the security methods other than the default setting.*

WDS with AP Mode

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

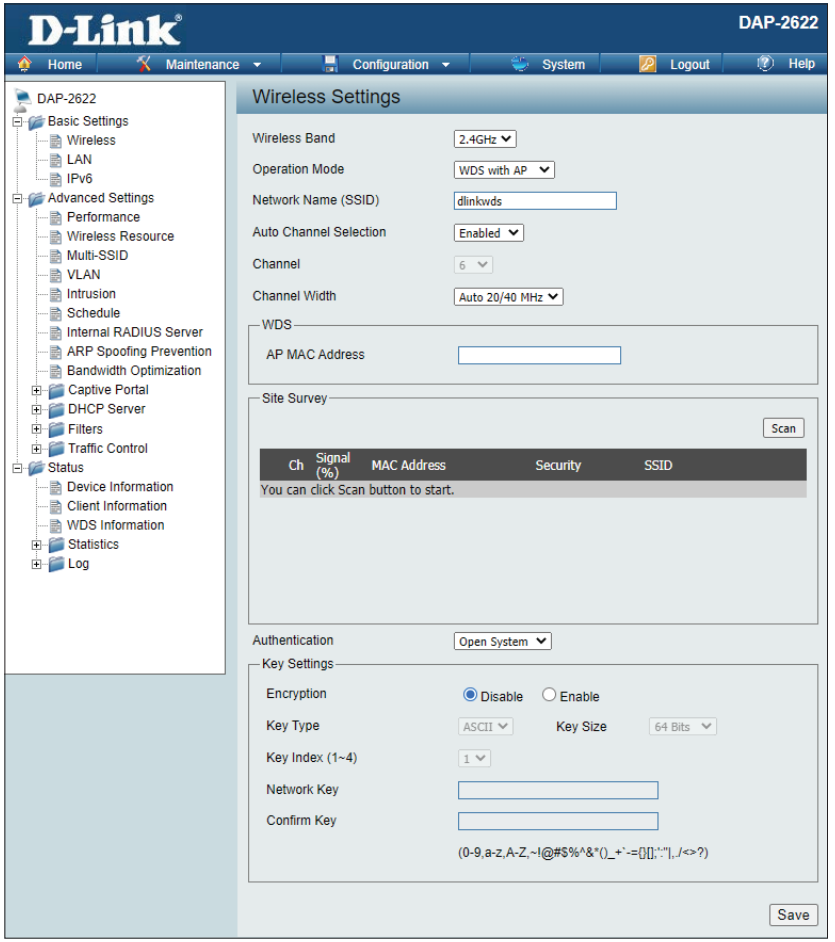
Operation Mode: **WDS with AP** mode is selected from the drop-down menu.

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.

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: Click the drop-down menu to select **20 MHz, Auto 20/40 MHz** or **Auto 20/40/80 MHz**. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** allows you to connect to both 802.11n and 802.11b/g or 802.11a wireless devices on your network.



AP MAC Address: Enter the MAC address of the AP on your network that will serve as a bridge 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 to.

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.

Note: *It is highly recommended that you use WPA-Personal to encrypt your network.*

WDS Mode

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

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

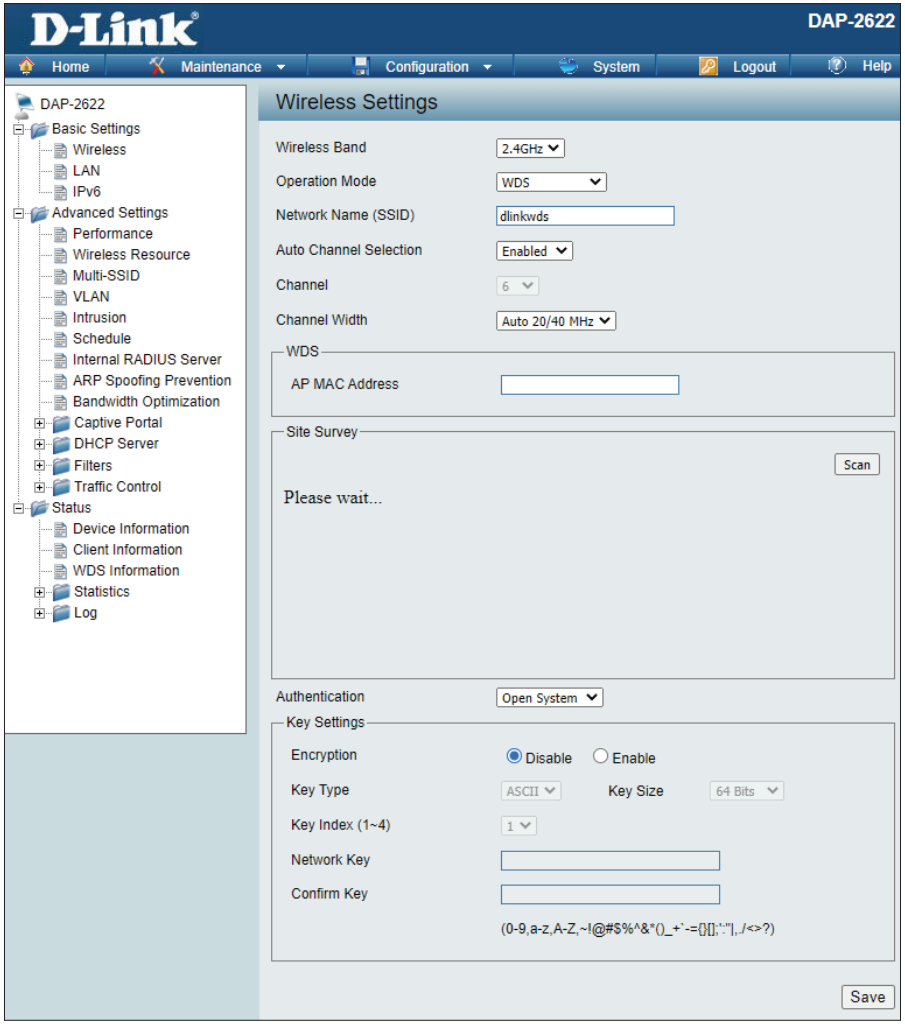
Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

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: Click the drop-down menu to select **20 MHz, Auto 20/40 MHz** or **Auto 20/40/80 MHz**. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** allows you to connect to both 802.11n and 802.11b/g or 802.11a wireless devices on your network.

AP MAC Address: Enter the MAC address of the AP on your network that will serve as a bridge 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.

Note: *It is highly recommended that you use WPA-Personal to encrypt your network.*

Wireless Client Mode

Wireless Band: Select either **2.4 GHz** or **5 GHz** 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.

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

Channel: The channel used will be displayed, and matches the AP that the DAP-2622 is connected to when set to Wireless Client mode.

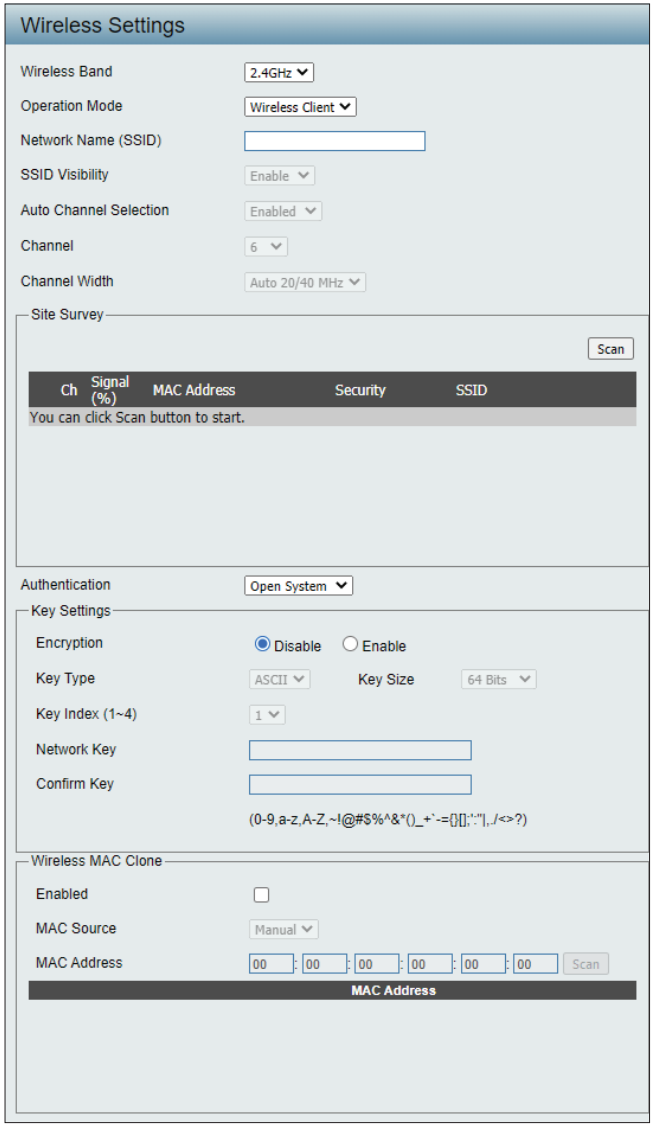
Channel Width: Click the drop-down menu to select **20 MHz, Auto 20/40 MHz** or **Auto 20/40/80 MHz**. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** allows you to connect to both 802.11n and 802.11b/g or 802.11a wireless devices on your network.

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: Will be explained in the next topic.

Check the box to enable the Wireless MAC Clone function.

Click the drop-down menu to select **Auto** or **Manual.**

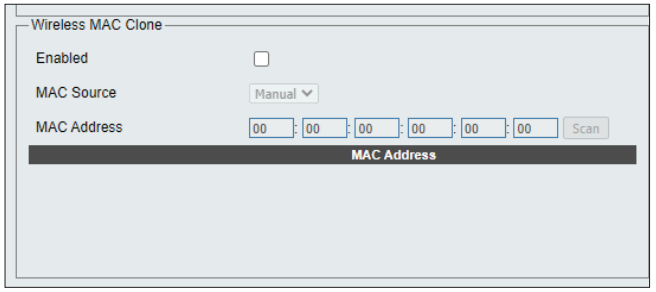


Wireless Client Mode

Enable: Check the box to enable the Wireless MAC Clone function.

MAC Source: Click the drop-down menu to select **Auto** or **Manual**.

MAC Address: When **MAC Source** is set to **Manual**, click **Scan** to find the MAC address to clone.



Wireless Security

There are mainly two forms of wireless encryption, 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 a newer encryption standard, and with the more advanced WPA2 standard wireless networks have finally reached a point where their security is strong enough to give users peace of mind.

Note: *The default Open System authentication allows wireless connection without requiring user authentication. It is highly recommended that you encrypt your network using one of the security methods other than the default setting.*

Wired Equivalent Privacy (WEP)

WEP provides two variations, called **Open System** and **Shared Key**.

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.

Shared Key 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 send a challenge to the client. The client will then again send a confirmation of the same key back to the access point where the access point will either return a success or a denial packet back to 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.

Wi-Fi Protected Access (WPA / WPA2)

WPA was created by the Wi-Fi Alliance to address the limitations and weaknesses found in WEP. This protocol is mainly based on the 802.11i standard. There are also two variations found in WPA called WPA-Personal (PSK) and WPA-Enterprise (EAP).

WPA-EAP requires the user to install a RADIUS server on the network for authentication.
WPA-Personal does not require the user to install a RADIUS server on the network.

WPA-PSK is a weaker form of authentication when compared with WPA-EAP, but WPA-PSK is far more secure than WEP.

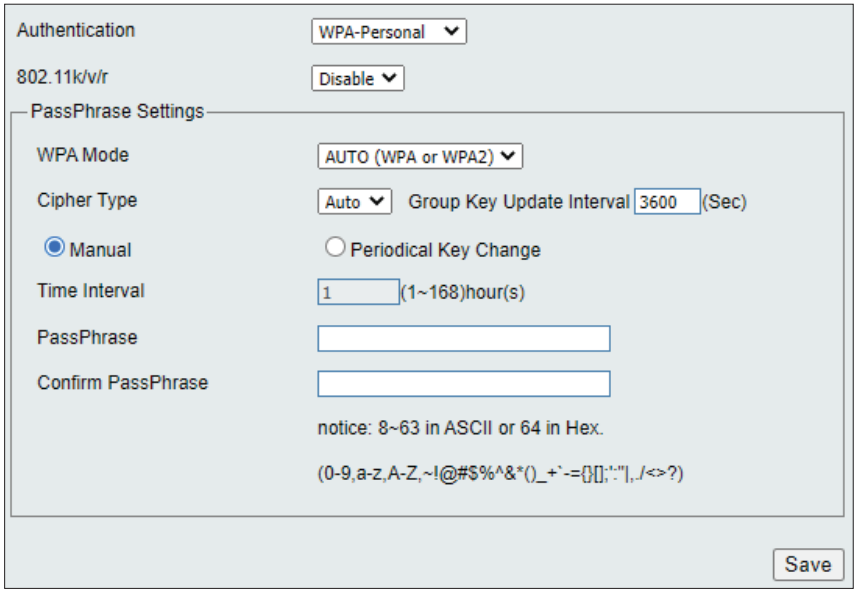
WPA2 is an upgraded form of WPA. WPA2 solves some security issues found in WPA. Similar to WPA, WPA2 has two variations, called WPA2-Personal (PSK) and WPA2-Enterprise (EAP).

WPA Mode: When **WPA-Personal** is selected, you must also select 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.

Cipher Type: When you select **WPA-Personal,** you must also select **AUTO**, **AES**, or **TKIP** from the pull-down menu.

Group Key Update: Select the interval during which the group key will be valid. The default value of **3600** is recommended.

PassPhrase: When you select **WPA-Personal**, please enter a passphrase in the corresponding field.



WPA Mode: When **WPA-Enterprise** is selected, you must also select 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.

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.

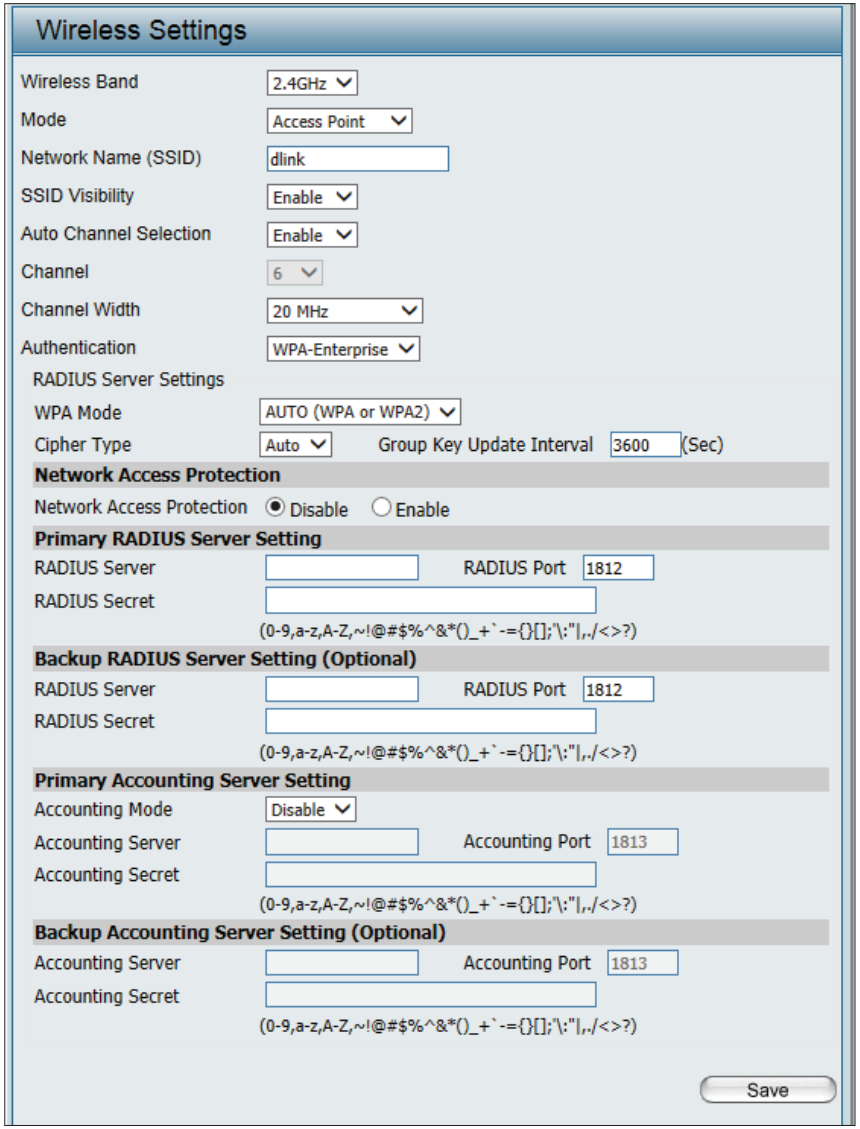
RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the RADIUS secret.

Account Server: Enter the IP address of the account server.

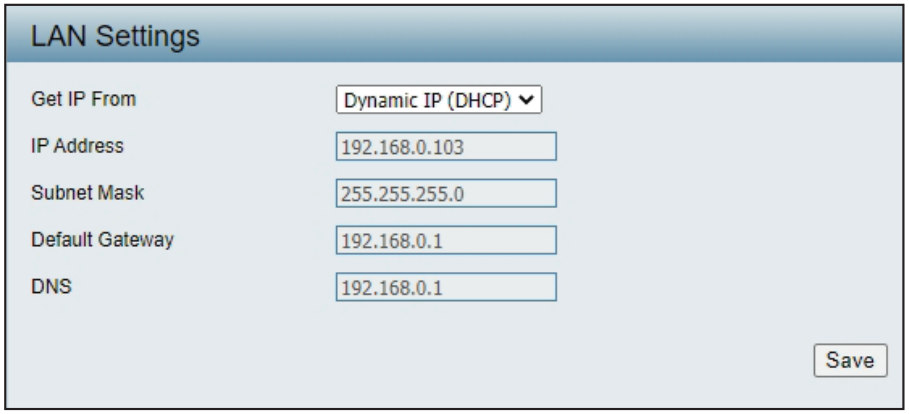
Account Port: Enter the account port.

Account Secret: Enter the account secret.



LAN

LAN is short for Local Area Network. This is your internal network. These are the IP settings of the LAN interface for the DAP-2622. 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: **Click the drop-down menu to select IP address setting mode.**

Static IP (Manual): Select this setting to assign a static IP address to the device.
Dynamic IP (DHCP): Select this setting to obtain an IP address from a DHCP server on the network.

IP Address: Enter the IP address to assign a static IP address.

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

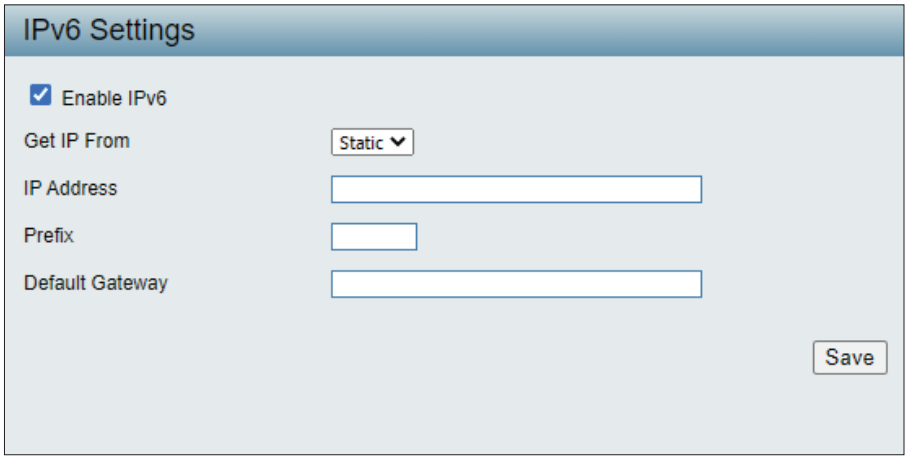
Enable IPv6: Check to enable IPv6.

Get IP From: Choose **Auto** to acquire IPv6 address automatically or use **Static** to set IPv6 address manually. When **Auto** is selected, the other fields here will be grayed out.

IP Address: Enter the LAN IPv6 address used here.

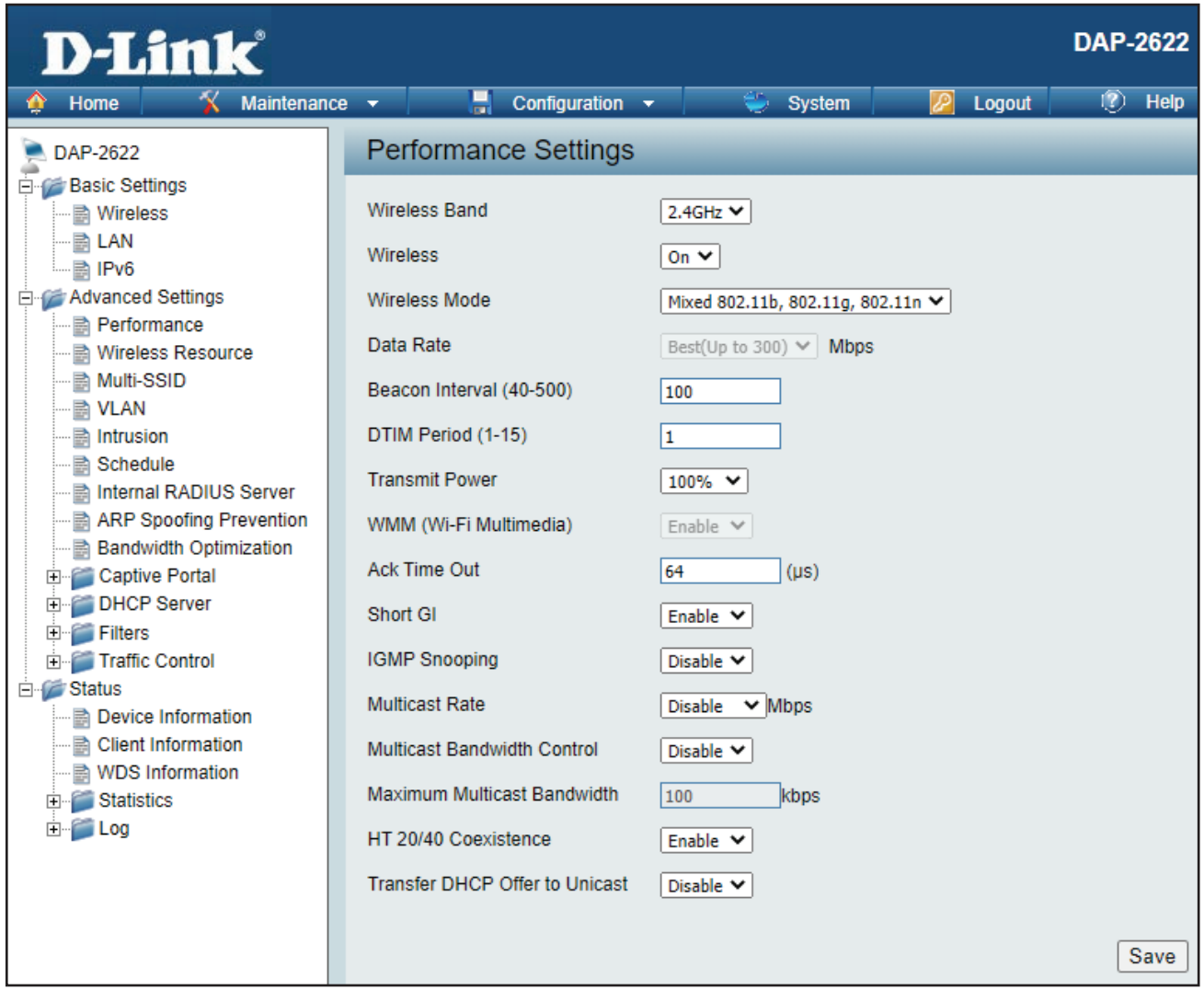
Prefix: Enter the LAN subnet prefix length value used here.

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



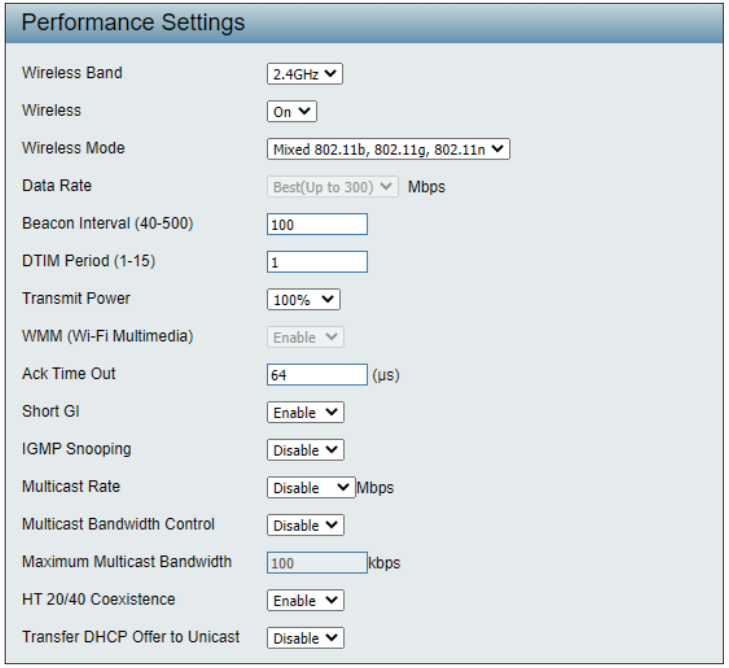
Advanced Settings

In the **Advanced Settings** section, the user can configure advanced settings concerning Performance, Multiple SSID, VLAN, Security, Quality of Service, AP Array, Web Redirection, DHCP Server, Filters and Scheduling. The following pages will explain settings found in this section in more detail.



Performance

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



Wireless Band: Select either **2.4GHz** or **5GHz**.

Wireless: Use the drop-down menu to turn the wireless function on or off.

Wireless Mode: Click the drop-down menu to select the wireless mode. 2.4GHz band supports**: Mixed 802.11b, 802.11g, 802.11n; Mixed 802.11b, 802.11g**; and **802.11n Only**. 5GHz band supports: **Mixed 802.11n, 802.11a; 802.11a Only; 802.11n Only**; and **Mixed 802.11ac**.

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*: When **Wireless Mode** is set to **Mixed 802.11b, 802.11g** (for 2.4GHz) and **802.11a Only** (for 5GHz), click the drop-down menu to 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 derate the transfer rate.

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.

DTIM 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.

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 your Wi-Fi network.

Ack Time Out (2.4 GHZ, 64~200): To effectively optimize throughput over long-distance links, enter a value for Acknowledgement Time Out between 25 and 200 microseconds for 5 GHz, or 64 to 200 microseconds for 2.4 GHz.

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: 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.

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

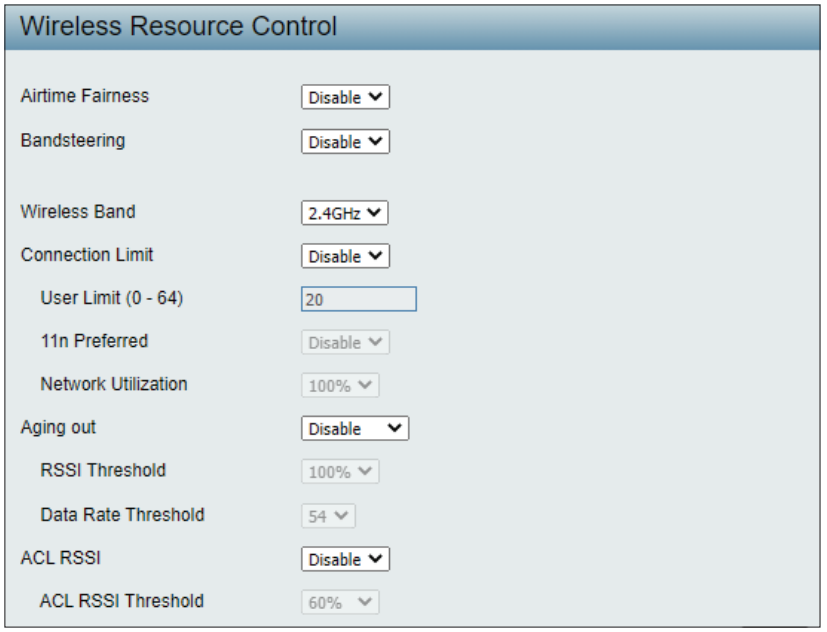
Maximum Multicast Bandwidth: Set the multicast packets maximum bandwidth passthrough rate from the Ethernet interface to the access point.

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. Enable this function if the number of stations on your network is larger than 30.

Wireless Resource Control

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.



Band Steering: Use the drop-down menu to **Enable** the 5G Preferred function. When the wireless clients support both 2.4GHz and 5GHz and the 2.4GHz signal is not strong enough, the device will use 5G as the higher priority.

Wireless band: Select **2.4GHz** or **5GHz**.

Connection Limit: Select **Enable** or **Disable**. This is an option 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-2622 will not allow clients to associate with the AP.

User Limit: Set the maximum amount of users that are allowed access (zero to 64 users) to the device using the specified wireless band. The default setting is **20**.

11n Preferred: 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: Set the maximum utilization of this access point for service. The DAP-2622 will not allow any new clients to associate with the AP if the utilization exceeds the value the user specifies. Select a utilization percentage between **100%, 80%, 60%, 40%, 20%**, and **0%**. 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 of disconnecting the wireless clients. Available options are **RSSI** and **Data Rate**.

RSSI Threshold: When **RSSI** is selected in the **Aging out** drop-down menu, select the percentage of RSSI here. When the RSSI of wireless clients is lower than the specified percentage, the device disconnects the wireless clients.

Data Rate Threshold: When **Data Rate** is selected in the **Aging out** drop-down menu, select the threshold of the data rate here. When the data rate of wireless clients is lower than the specified number, the device disconnects the wireless clients.

ACL RSSI: Use the drop-down menu to **Enable** the 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: Set the ACL RSSI Threshold.

Multi-SSID

The device supports up to eight multiple Service Set Identifiers per radio. 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.

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

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.

Security: 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 page 20. For a detailed description of the WPA-Personal parameters please go to page 21. For a detailed description of the WPA-Enterprise parameters please go to page 22.

Note: *It is highly recommended that you encrypt your network for all SSIDs in Multi-SSID configuration.*

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.

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** 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.

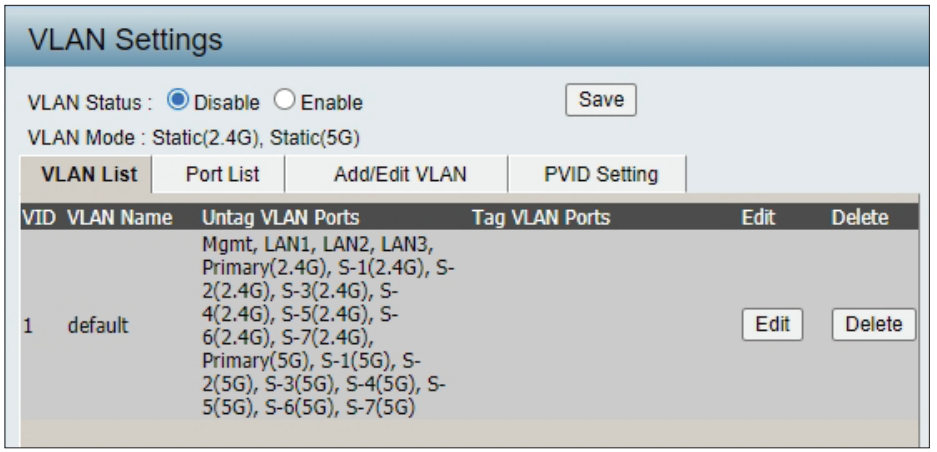
RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the RADIUS secret.

VLAN

VLAN List

The DAP-2622 supports VLANs. VLANs can be created with a name and VID. Mgmt (TCP stack), LAN, primary/multiple SSID, and WDS connections can be assigned to VLANs as they are physical ports. Any packet which enters the DAP-2622 without a VLAN tag will have a VLAN tag inserted with a PVID. The **VLAN List** tab displays the current VLANs.



VLAN Status: Click the radio button to enable or disable VLAN status. Next, go to the **Add/Edit VLAN** tab to add or modify an item on the VLAN List tab.

VLAN Status: Displays the current VLAN status.

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 **Edit** to edit the current VLAN.

Delete: Click **Delete** 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 Click the radio button to enable or disable VLAN status. 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.

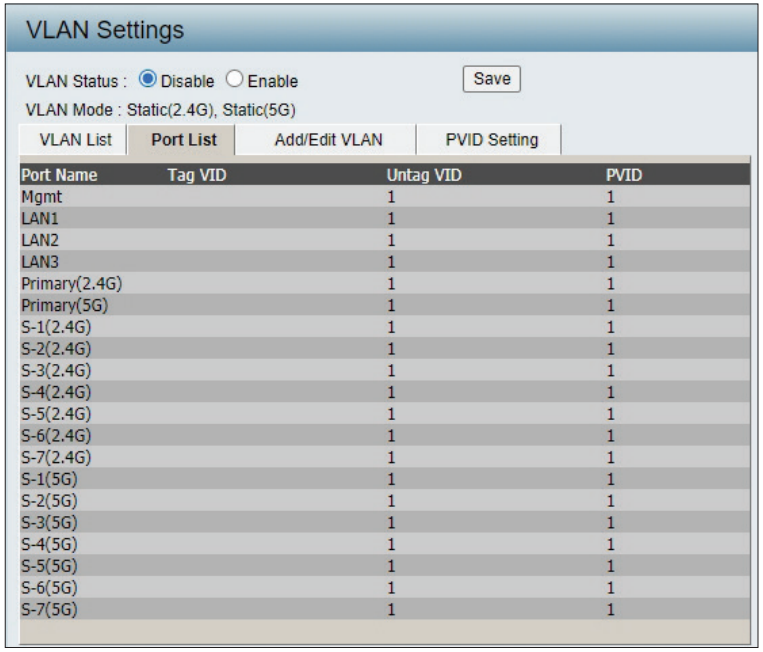
Save Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

Port Name Displays the name of the port.

Tag VID Displays the tagged VID of the port.

Untag VID Displays the untagged VID of the port.

PVID Displays the PVID of the port.



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.

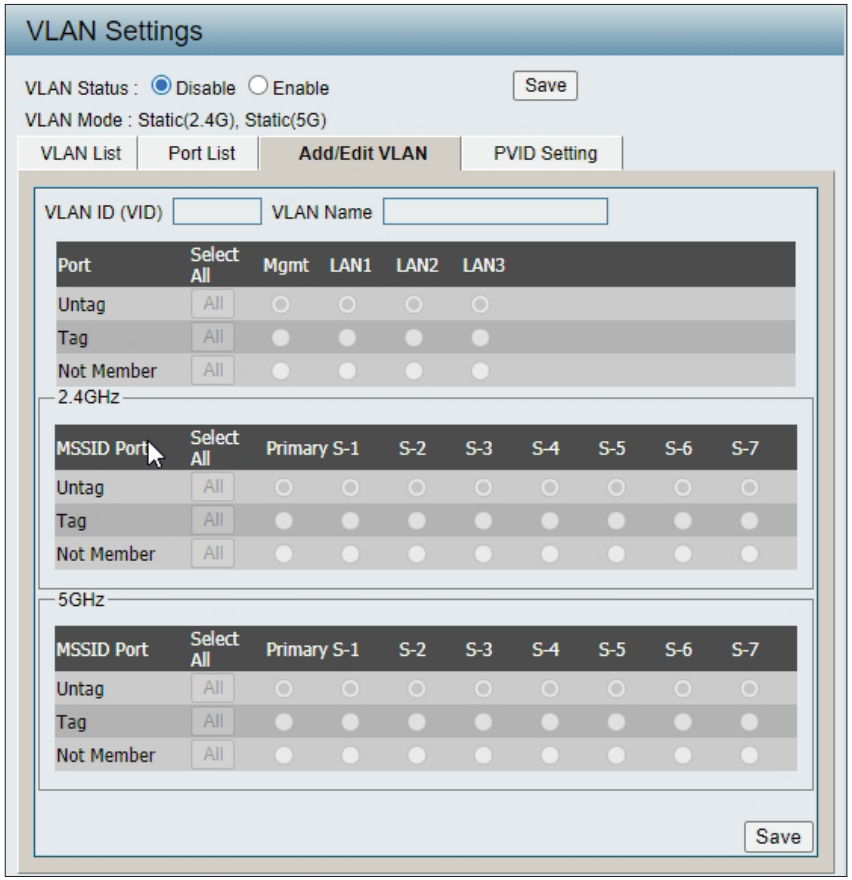
VLAN Status: Click the radio button to enable or disable VLAN status. By default this feature is disabled.

VLAN Mode: Displays the current VLAN mode.

VLAN ID: Enter a value (1-4094) for the Internal VLAN.

VLAN Name: Enter the VLAN name to add or modify.

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

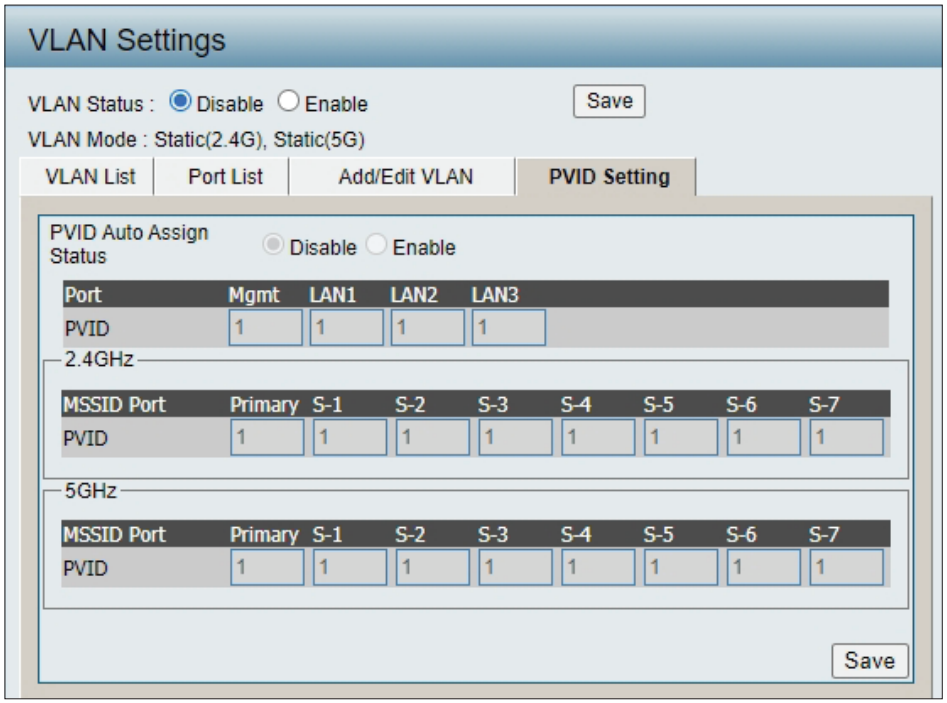


From the Port fields, select the radio button to set Untag/Tag/Not Member settings to the Mgmt (management) and LAN ports. The port configuration functions are also available for the defined 2.4GHz and 5GHz ports.

Untagged ports are used for connecting to client devices, such as a computer host. While tagged ports are designated for VLAN trunk links.

PVID Settings

The **PVID Settings** 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: Click the radio button to enable or disable VLAN status. By default this feature is disabled.

VLAN Mode: Displays the current VLAN mode.

PVID Auto Assign Status: Click the radio button to enable or disable PVID auto assign status.

For each untagged port, set the PVID of the port to its assigned VLAN ID. For example, if ports 1, 2, 3, 4, and 5 are untagged members of VLAN 10, ports 1, 2, 3, 4, and 5 would be configured with a PVID of 10.

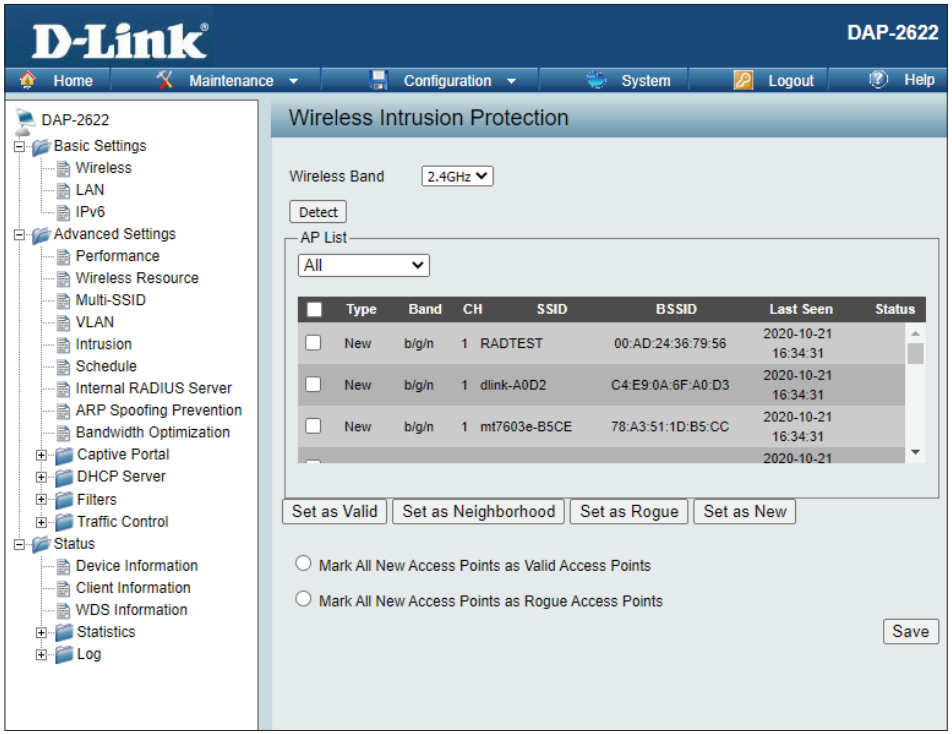
For better system consistency, the following are recommended:

- set MSSID ports S1 and S2 to 16 and 17, respectively
- set switch port trunk native VLAN 1 for trunk port 1

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

Intrusion

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



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

Detect Click **Detect** to initiate a scan of the network.

AP List Click the drop-down menu to select **All**, **Valid**, **Neighborhood**, **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.
- Neighborhood: 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 with out 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**.

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.

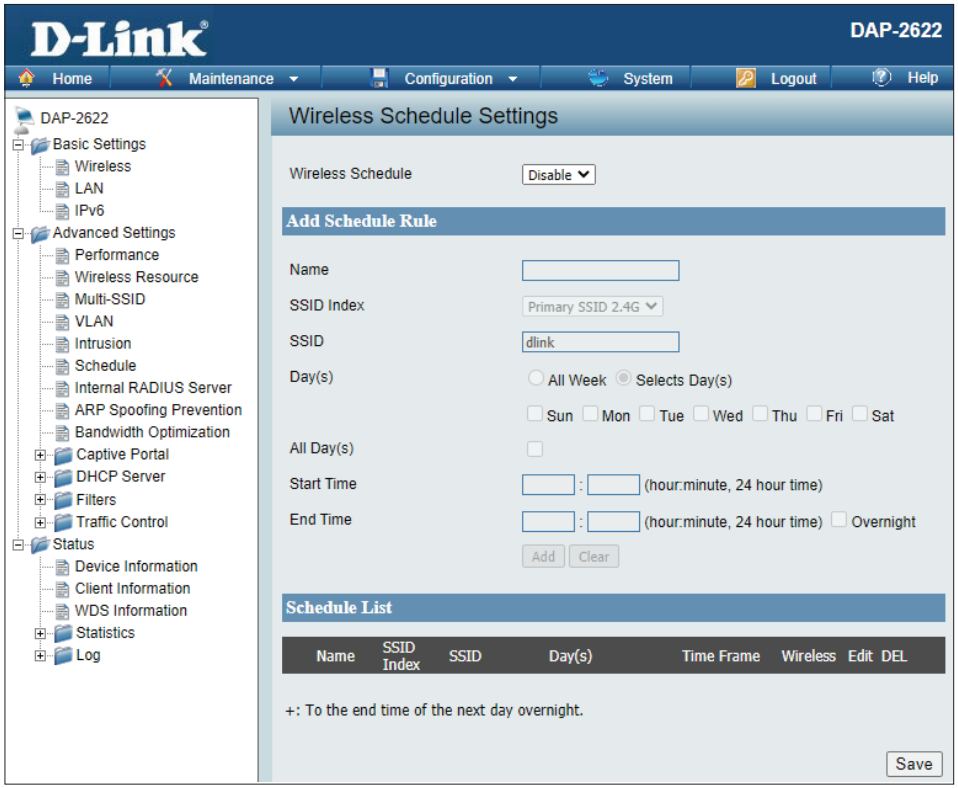
SSID: This read-only field indicates the current SSID in use. To create a new SSID, go to the **Wireless Settings** window (**Basic Settings** > **Wireless**).

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.



Internal RADIUS Server

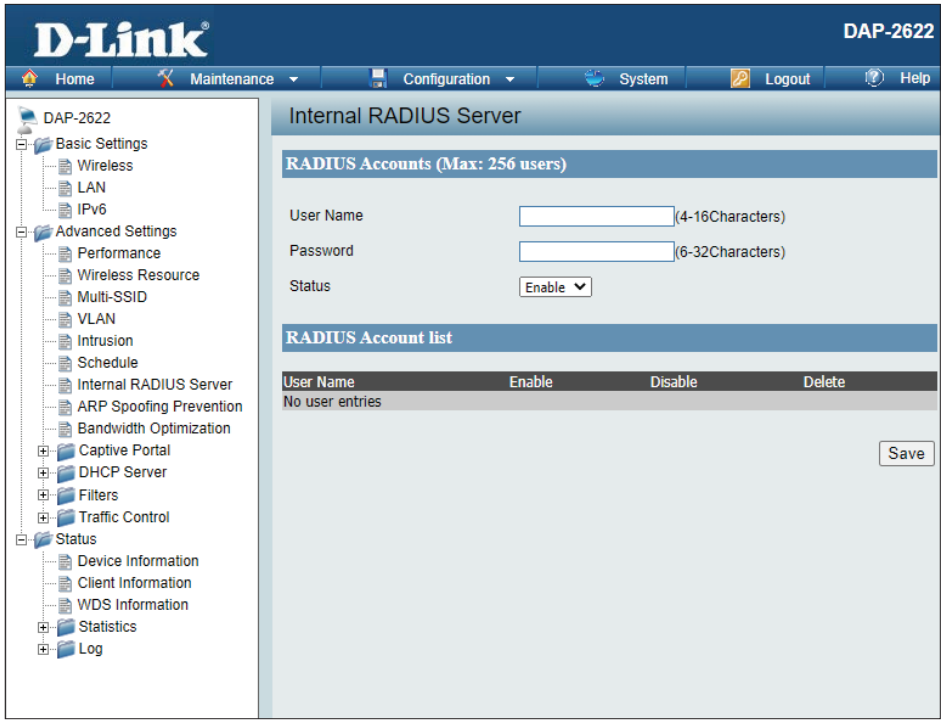
The DAP-2622 features a built-in RADIUS server. Once you have finished adding a RADIUS account, click the **Save** button to let your changes take effect. The newly-created account will appear in the **RADIUS Account List**. The radio buttons allow the user to enable or disable the RADIUS account. Click the icon in the delete column to remove the RADIUS account. We suggest you limit the number of accounts to 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 to 64 characters.

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

RADIUS Account List: Displays the list of users.



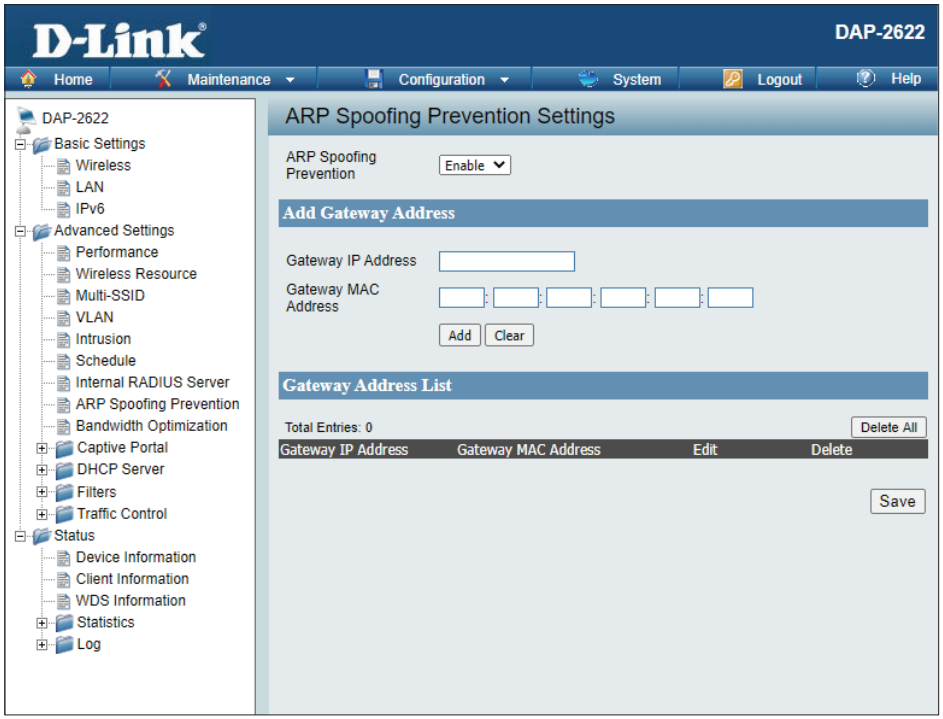
ARP Spoofing Prevention

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

ARP Spoofing Prevention: This check box allows you to enable the ARP spoofing prevention function.

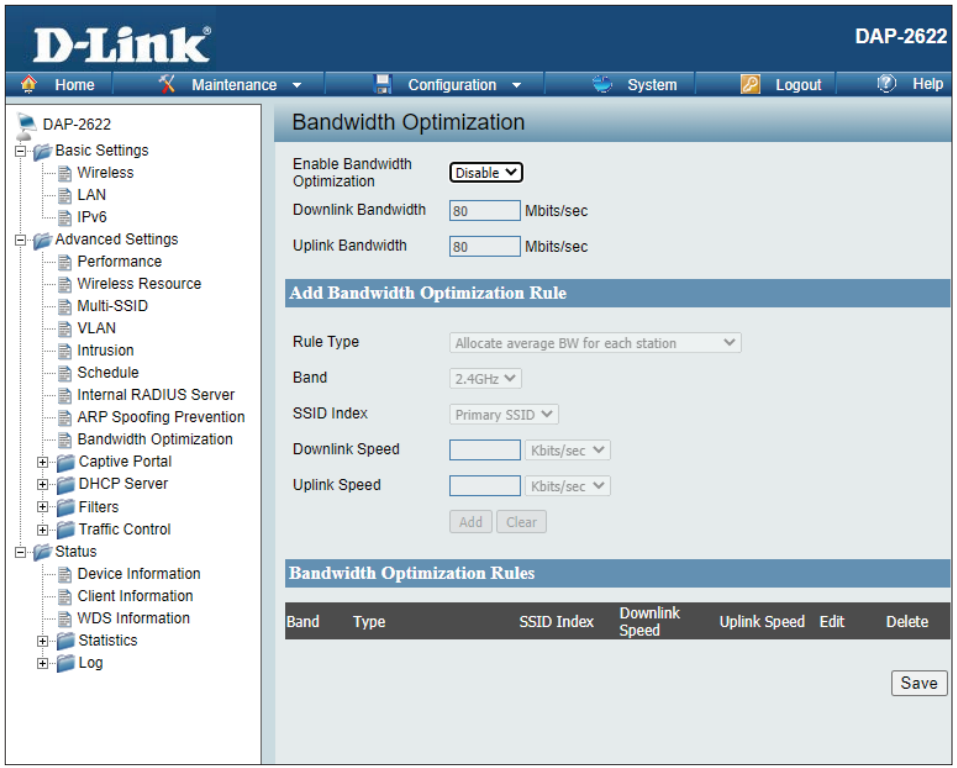
Gateway IP Address: Enter a gateway IP address.

Gateway MAC Address: Enter a gateway MAC address.



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.

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 **Allocte specific BW for SSID**. The rules are described below.

Allocate average BW for each station: The 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 the 11b/g/n and 11a/n clients are 10%/20%/70% and 20%/80%. The AP will distribute different bandwidth for 11a/b/g/n clients.

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

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.

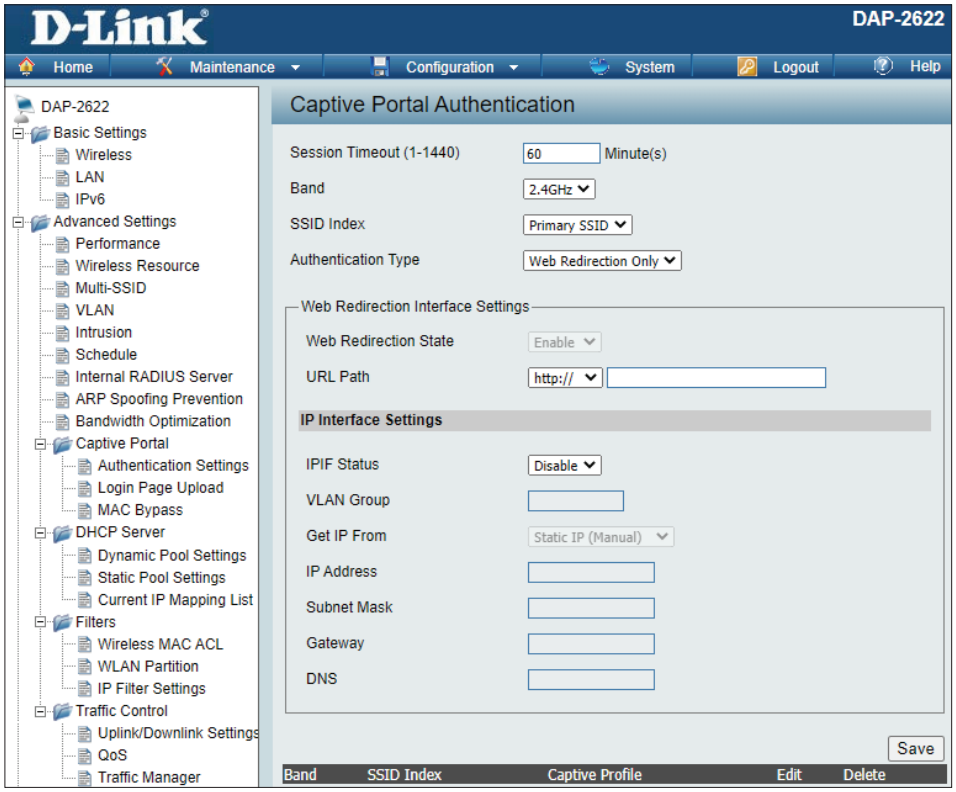
Delete: Click to delete the gateway entry.

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, user 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**.

SSID Index: Select the SSID for this authentication.

Authentication Type: Select the captive portal encryption type here. The 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: Default setting is **Enable** when 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.

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-2622. 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.

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, you can view and configure the Captive Portal settings. After selecting **Username/Password** as the authentication type, you 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**.

SSID Index: Select the SSID for this authentication.

Authentication Type: Select the captive portal encryption type here. The 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: 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-2622. 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.

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, user can view and configure the Captive Portal settings. After selecting **Passcode** as the authentication type, we 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**.

SSID Index : Select the SSID for this authentication.

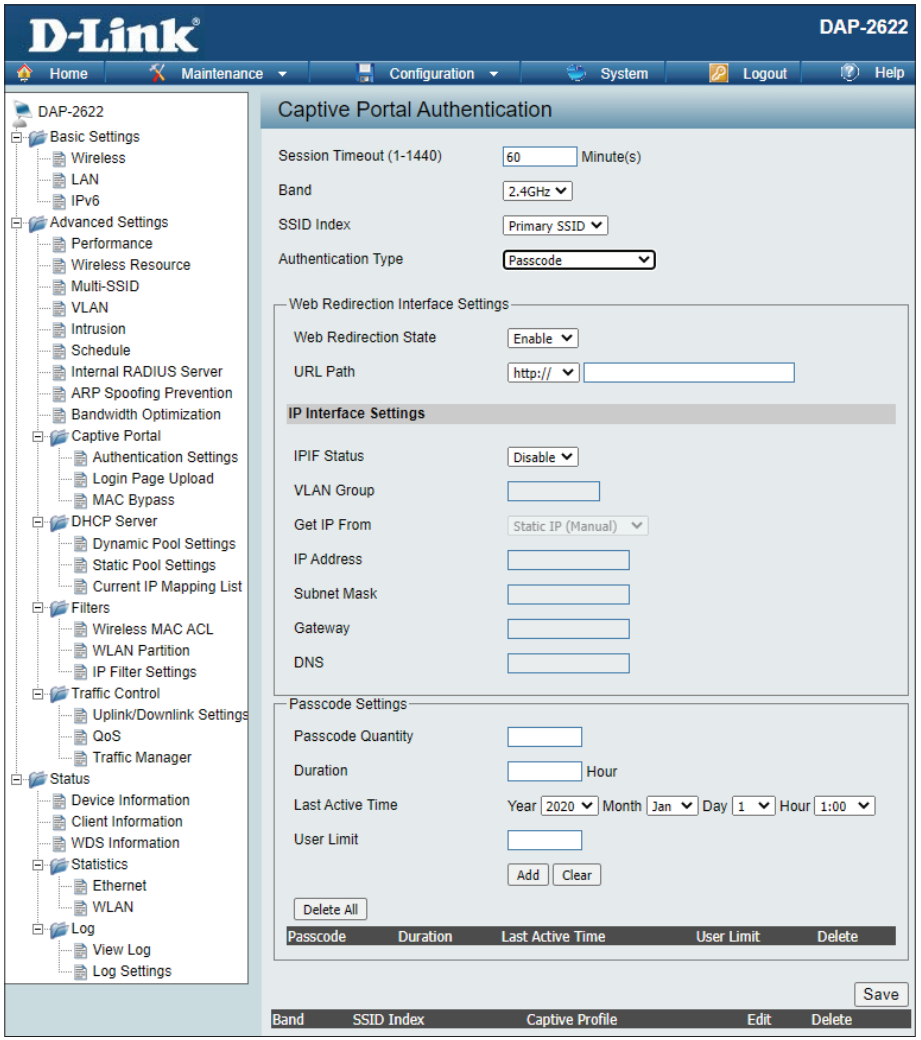
Authentication Type : Select the captive portal encryption type here. Options to choose from are **Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP** and **POP3**. In this section we'll discuss the **Passcode** option.

Web Redirection State : 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-2622. 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 is selected.

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 tickets that will be used here.

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

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.

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, you can view and configure the Captive Portal settings. After selecting **Remote RADIUS** as the authentication type, we 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**.

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.

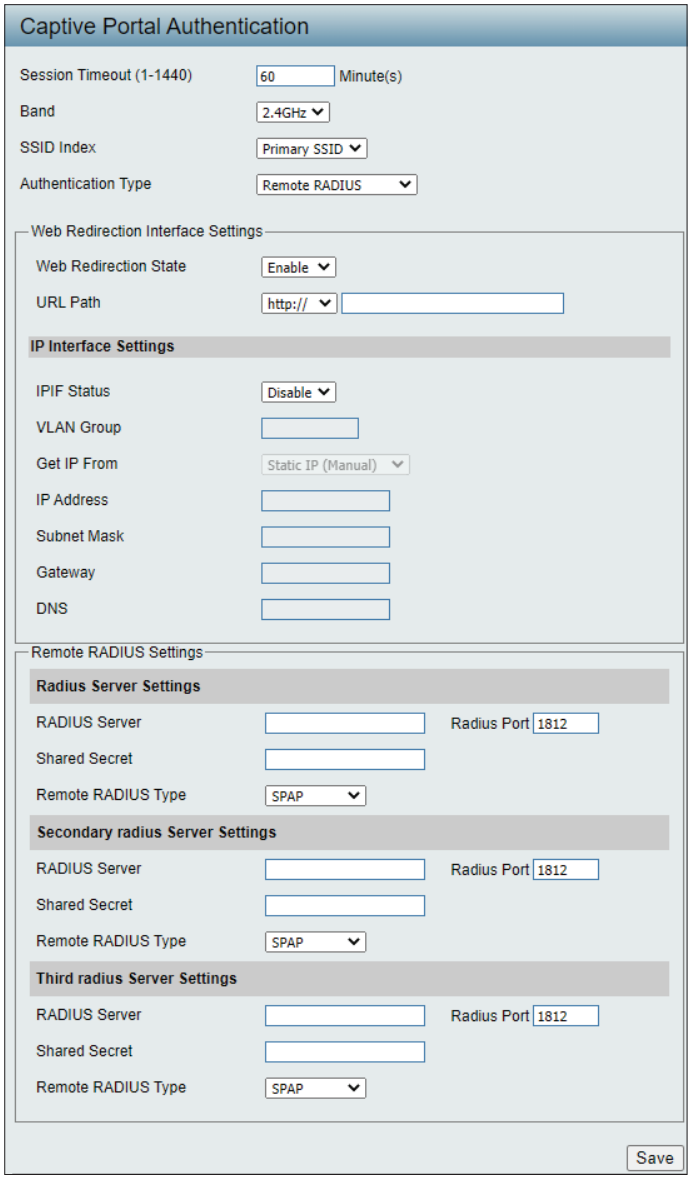
Web Redirection State: Select **Enable** to enable the website redirection feature.

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-2622. 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.

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, user can view and configure the Captive Portal settings. After selecting **LDAP** as the authentication type, we 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**.

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.

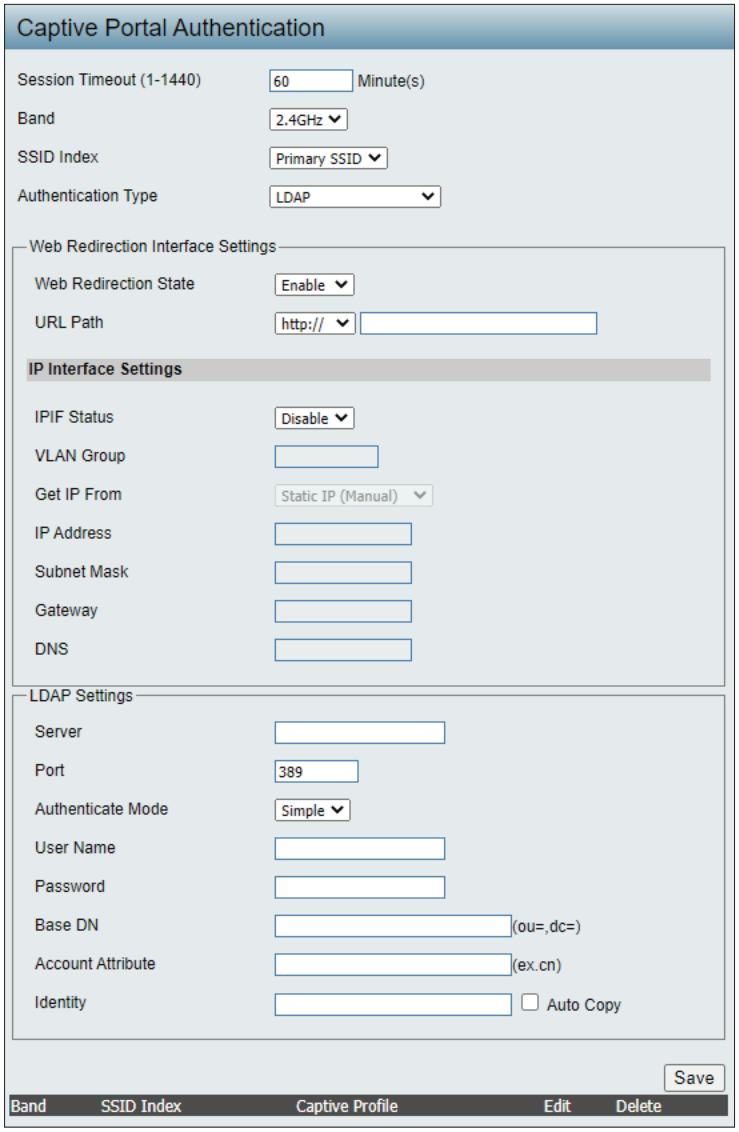
Web Redirection State: Select **Enable** to enable the website redirection feature.

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-2622. 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 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.

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, user can view and configure the Captive Portal settings. After selecting **POP3** as the Authentication Type, we 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**.

SSID Index: Select the SSID for this authentication.

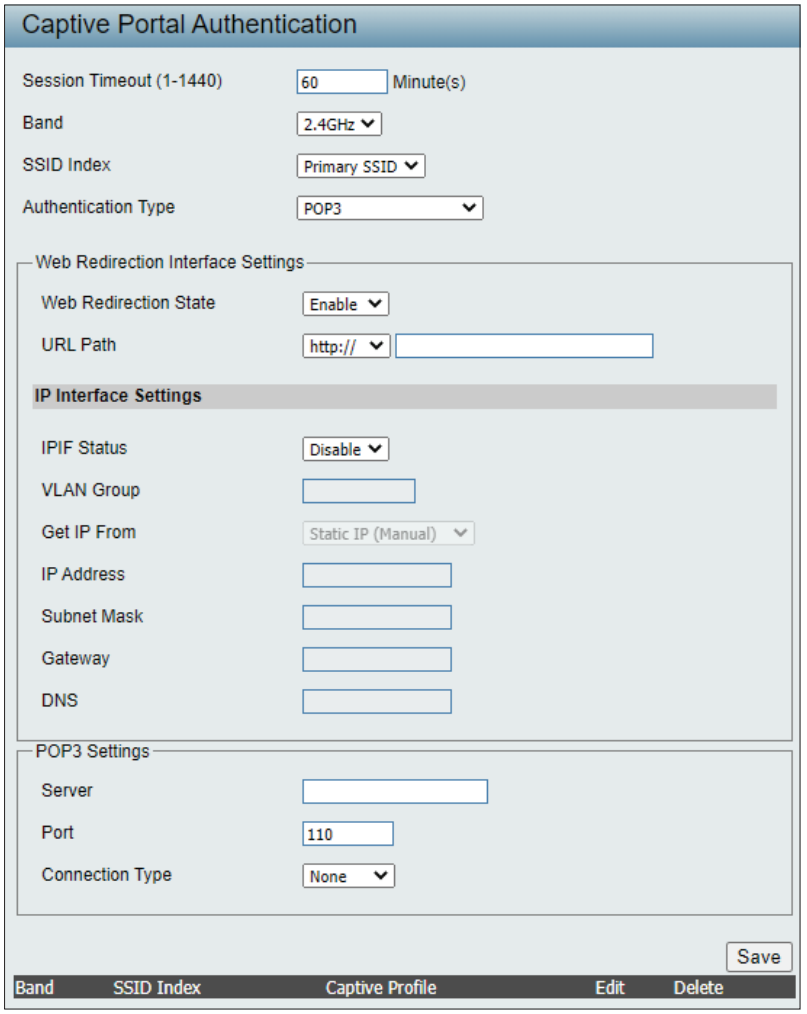
Authentication Type: Select the captive portal encryption type here. Options to choose from are **Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP** and **POP3**. In this section we'll discuss the POP3 option.

Web Redirection State: 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-2622. 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: Enter the POP server's port number here.

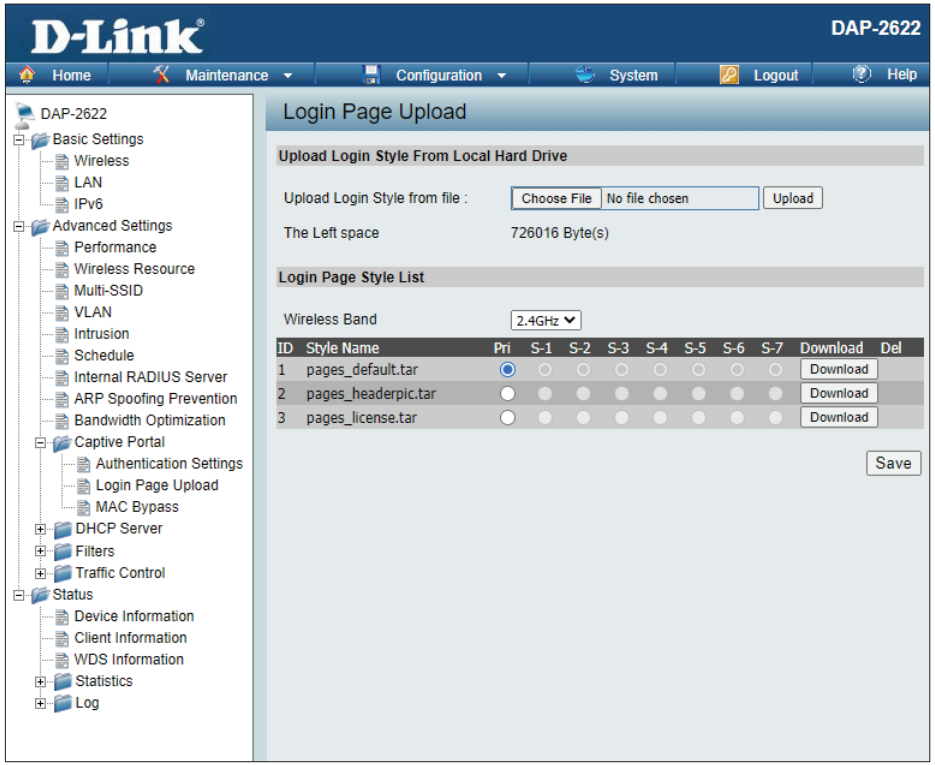
Connection Type: Select the connection type here. Options to choose from are **None** and **SSL/TLS**.

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 file: In this field, the path to the login style file that will be uploaded will be 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. Click the **Del** button to delete the template file.



MAC Bypass

The DAP-2622 features a wireless MAC Bypass feature that may be configured here. Once you are finished with these settings, click the **Save** button.

Wireless Band: Select the wireless band for the MAC Bypass feature.

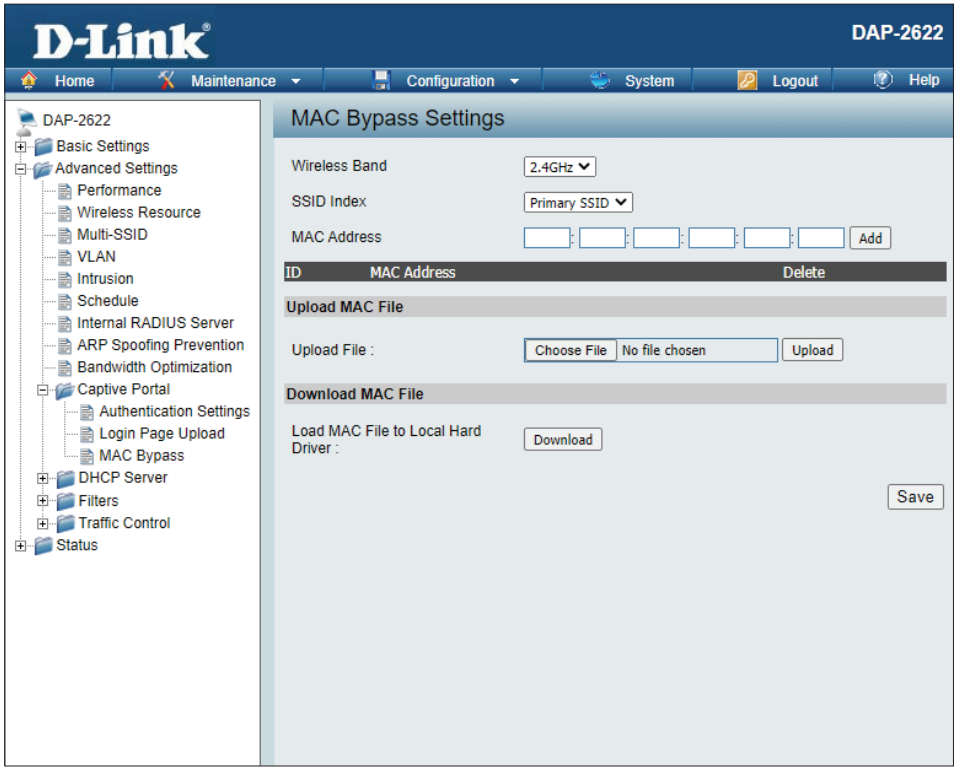
SSID Index: Select the SSID for the MAC Bypass feature.

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**.

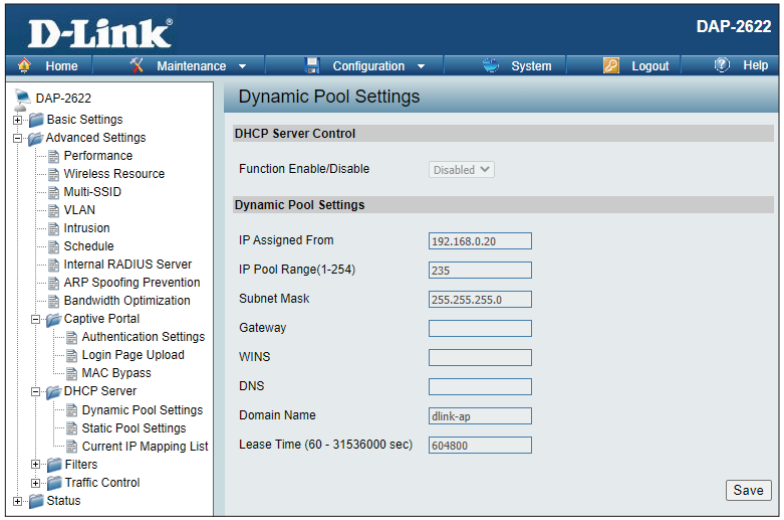
Load MAC File to Local Hard Driver: To download MAC bypass list file, click **Download** to save the MAC bypass list.



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 required, the DAP-2622 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-2622 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.

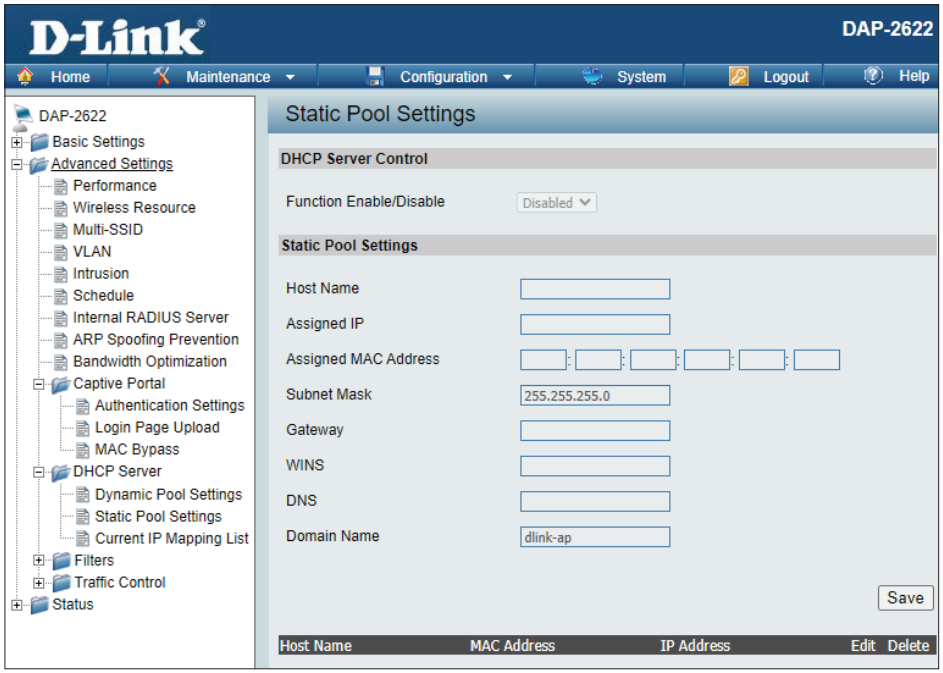
DNS: Enter the IP address of the Domain Name System (DNS) server. The DNS server translates domain names such as **www.dlink.com** into IP addresses.

Domain Name: Enter the domain name of the network, if applicable.

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

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-2622 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.

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.

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.

Current IP Mapping List

This window displays information about the currently assigned 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 that 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.

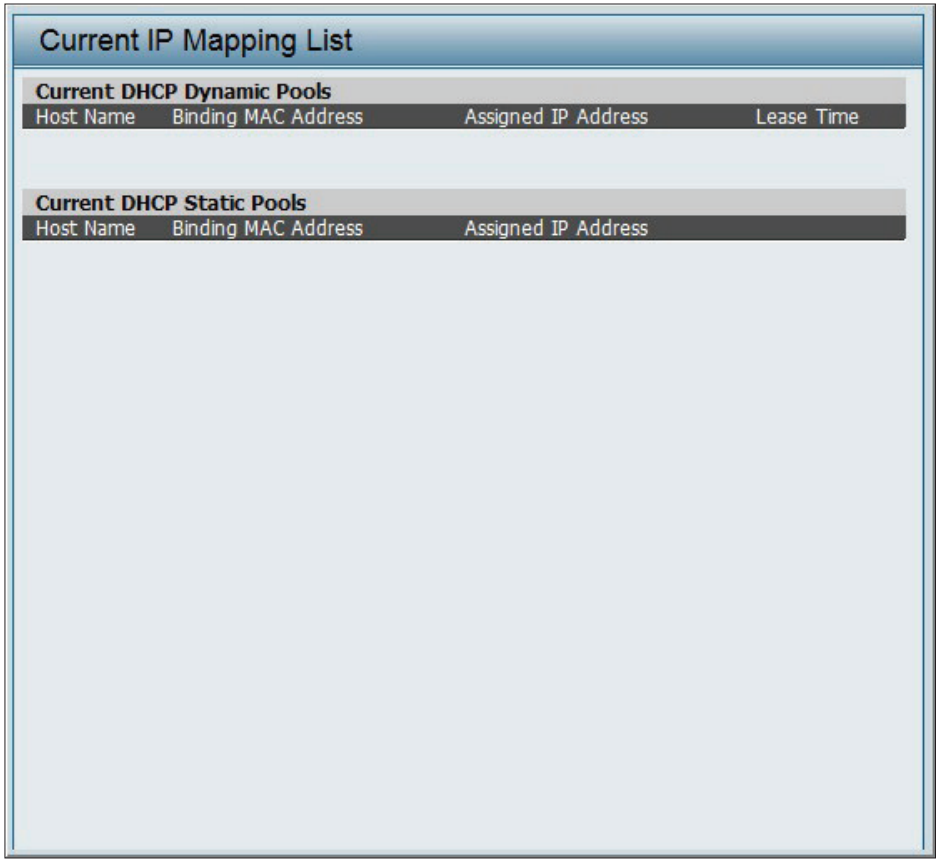
Current DHCP Static Pools: These are the IP address pools of the DHCP server assigned through the static pool settings.

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.

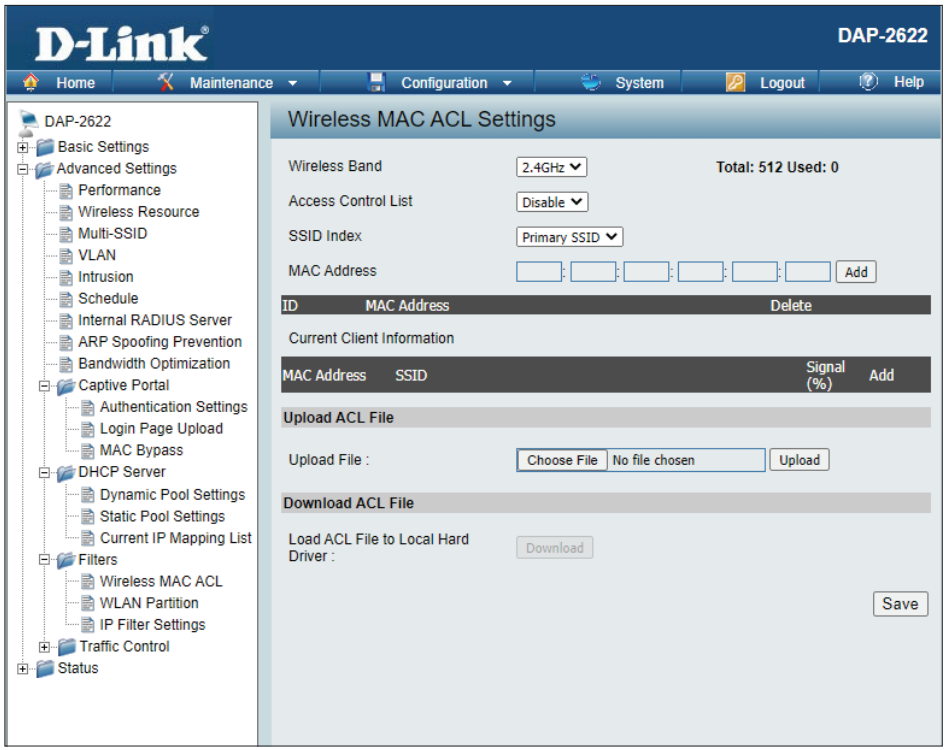
Assigned IP Address: The current corresponding DHCP-assigned static IP address of the device.



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.

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 a ACL list file, click **Browse...** and navigate to the ACL list file saved on the computer, and then click **Upload.**

Load ACL File to Hard Drive: To download ACL list file, click **Download** and to save the ACL list.

WLAN Partition

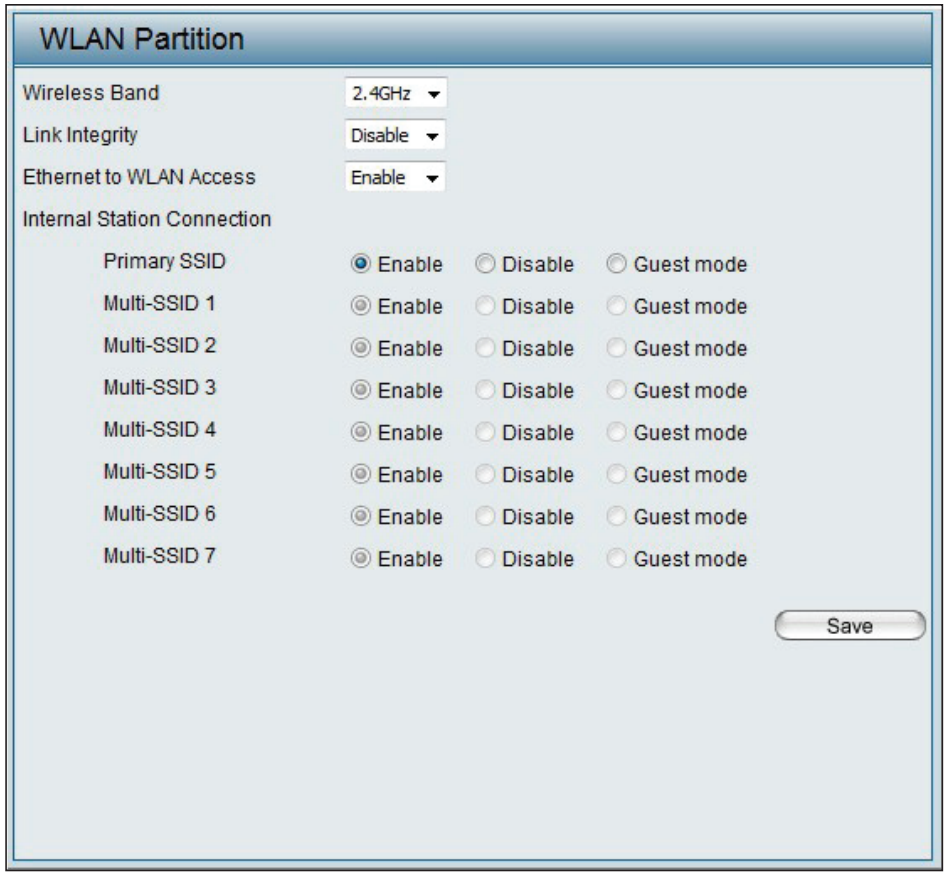
This page allows the user to configure a WLAN Partition.

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 over the Ethernet interface.

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.



IP Filter Settings

Enter the IP address or network address that will be used in the IP filter rule (or example, 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.

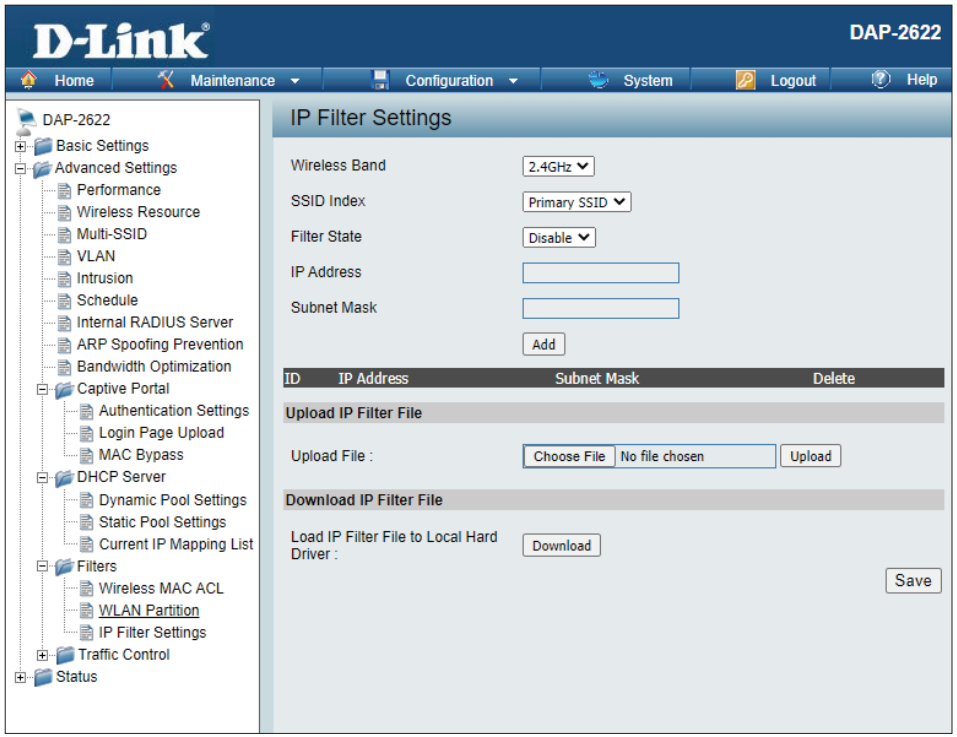
Wireless Band : Select **2.4GHz** or **5GHz**.

IP Address: Enter the IP address or network address.

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

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

Download IP Filter File: To download an IP Filter list file, click **Download** .



Traffic Control

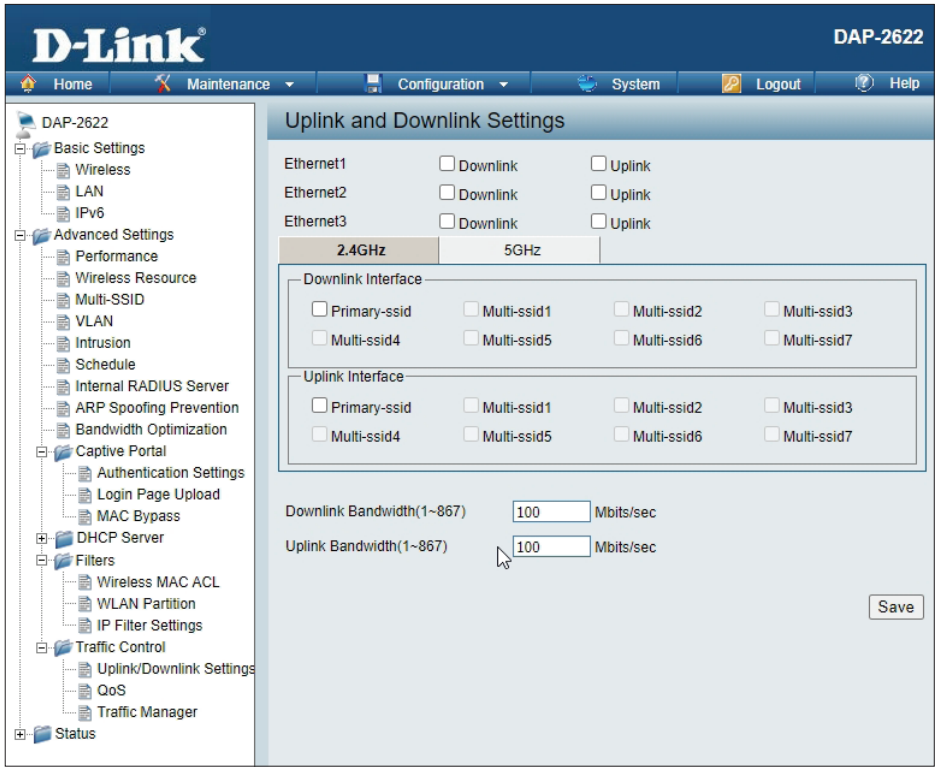
Uplink/Downlink Setting

The **Uplink/Downlink Settings** page allow you to customize the Ethernet, 2.4 GHz and 5 GHz downlink and uplink interfaces by 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.

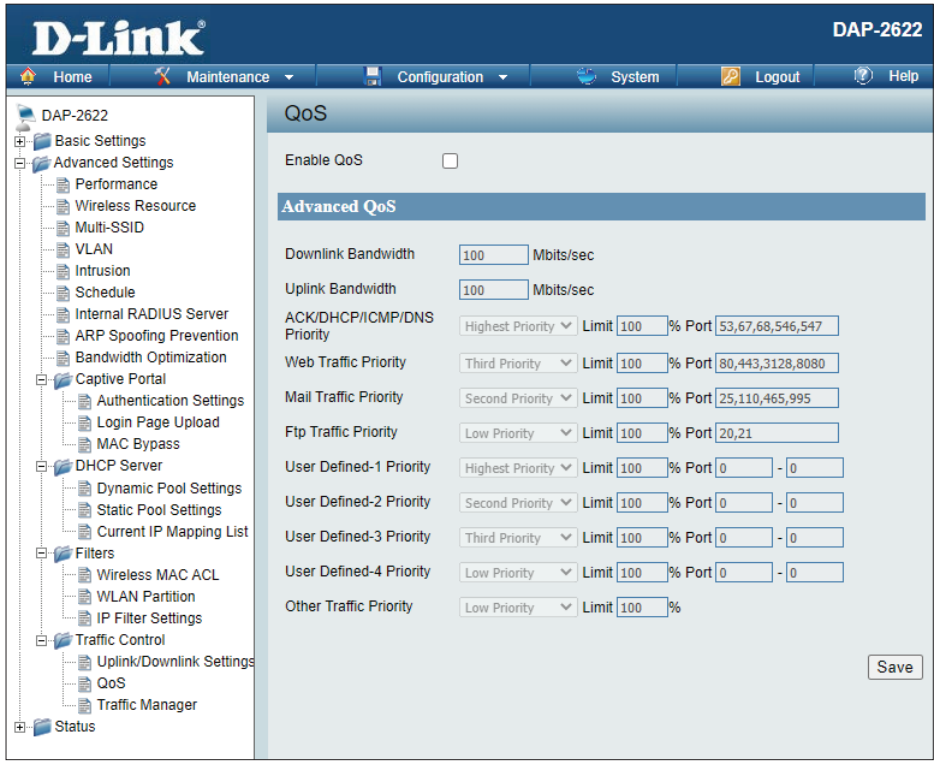
Uplink Bandwidth: The uplink bandwidth in Mbits per second.

Ethernet: Check the box to specify the Downlink or Uplink settings.



QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications. The DAP-2622 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 for the various kinds of traffic listed below (e.g. web, mail, FTP, etc). Click the **Save** button when you are finished.

Downlink Bandwidth Enter the downlink bandwidth in Mbits per second. This value is entered in the **Uplink/ Downlink Settings** window.

Uplink Bandwidth Enter the uplink bandwidth in Mbits per second. This value is entered in the **Uplink/ Downlink Settings** 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.

Mail 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**.

Traffic Manager

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

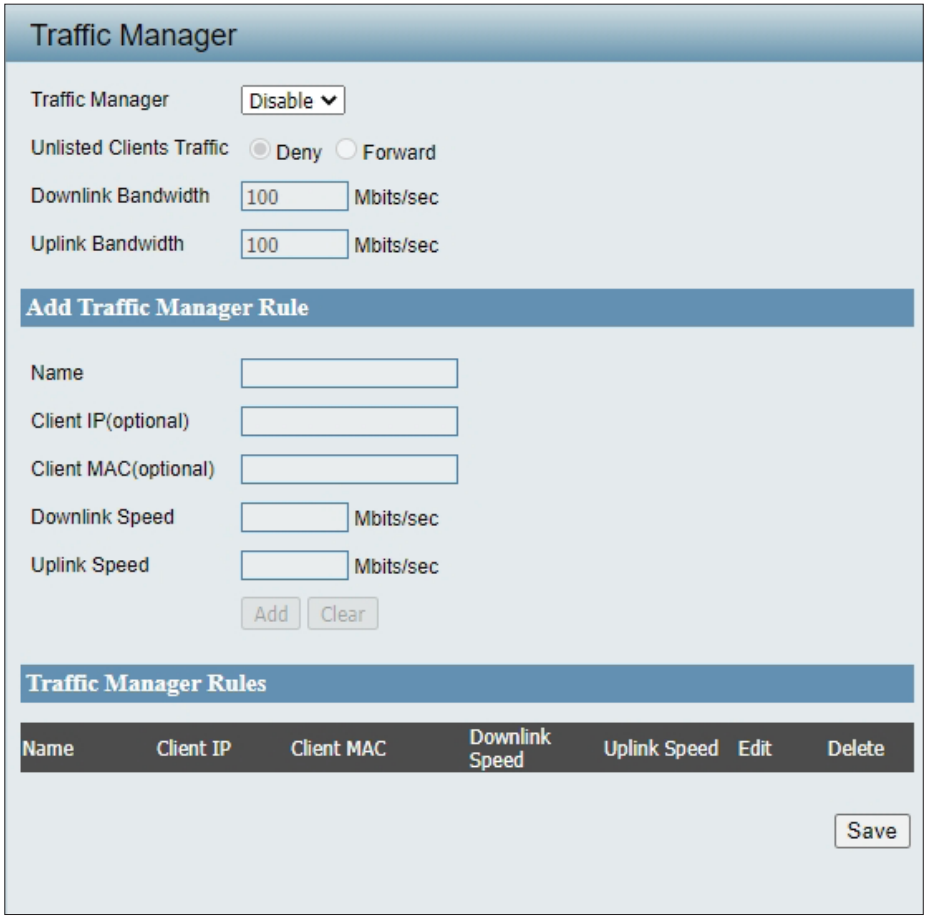
Traffic Manager: Use the drop-down menu to **Enable** the traffic manager feature.

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 Settings** window.

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

Add Traffic Manager Rule: Enter a name to designate the traffic management rule. Designate an IP/MAC address to apply the rule to and specify the downlink/uplink speed for the client.



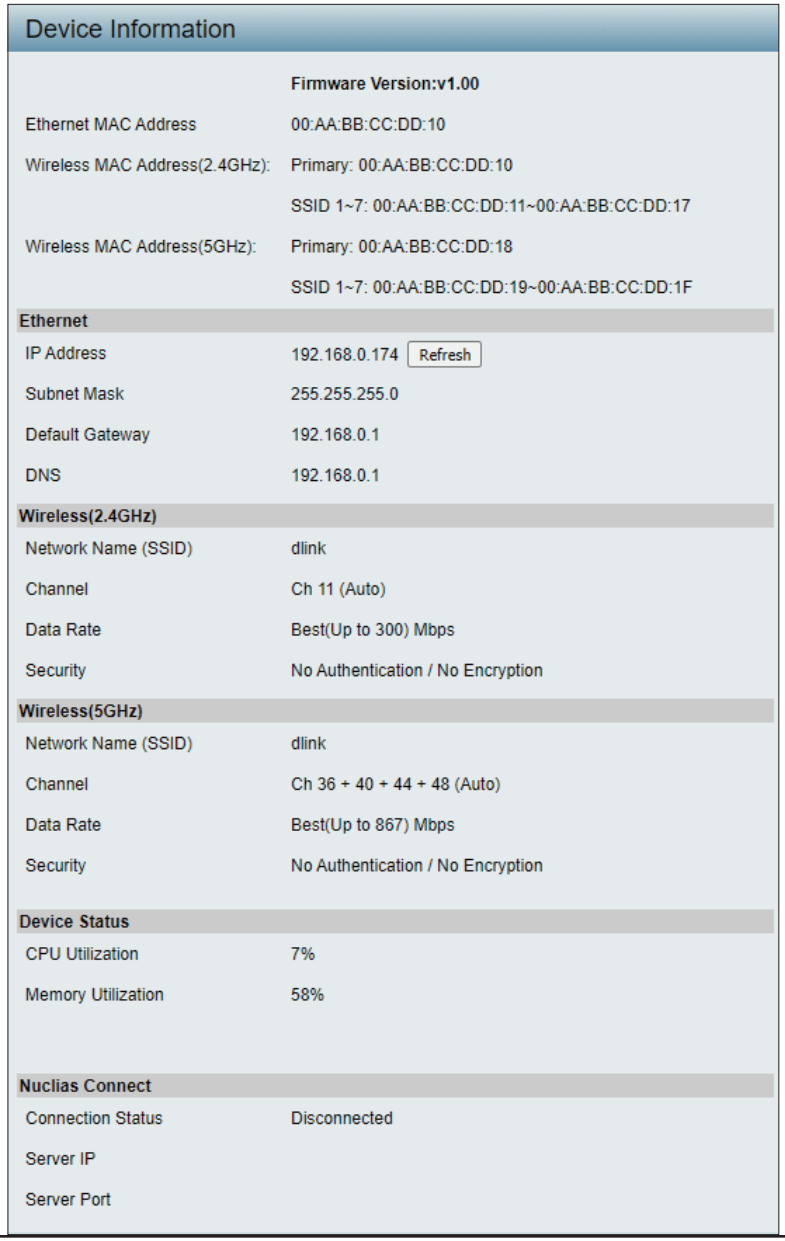
Status

In the **Status Section** screen, 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 Status section in more detail.

Device Information

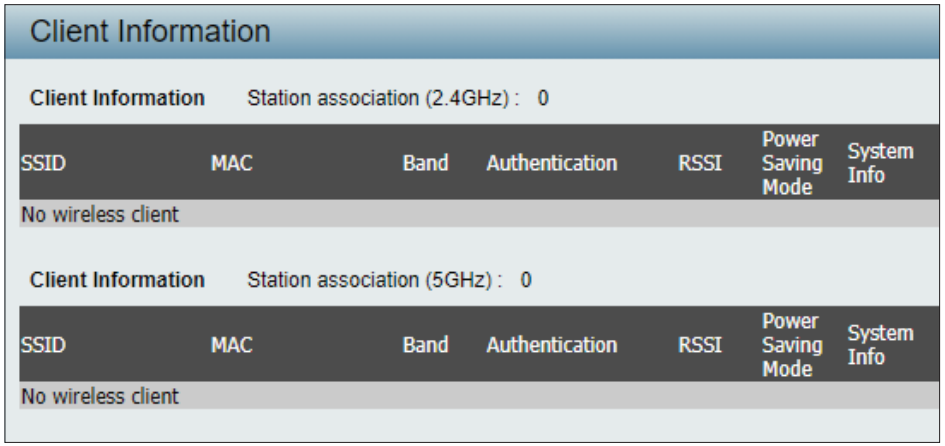
This page displays information like the current firmware version and Ethernet and wireless parameters, as well as the information regarding CPU and memory utilization.

Device Information: This read-only window displays the configuration settings of the DAP-2622, including the firmware version and the device's MAC address.



Client Information

This page displays information for associated clients, such as their SSID, MAC, band, authentication method, signal strength, and power saving mode.



Client Information: This window displays the wireless client information for clients currently connected to the DAP-2622.

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 client's information for the network.

WDS Information Page

This page displays the access point's SSID, MAC, band, authentication method, signal strength, and status.

WDS Information: This window displays the Wireless Distribution System information for clients currently connected to the DAP-2622.

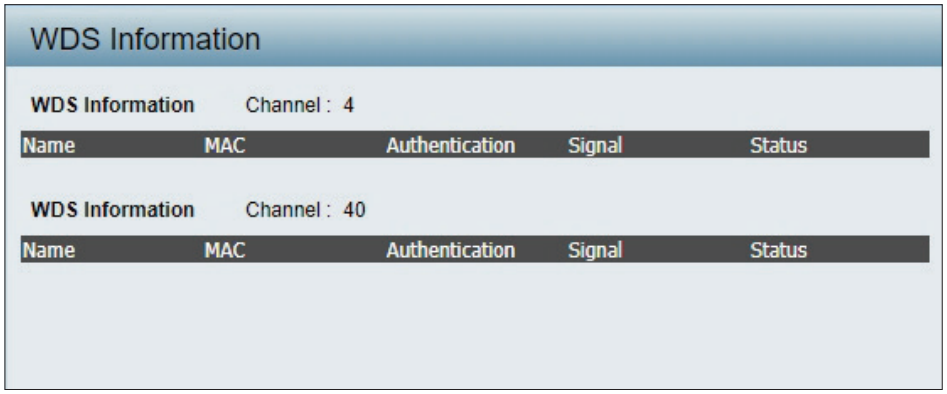
Name: Displays the SSID of the client.

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.

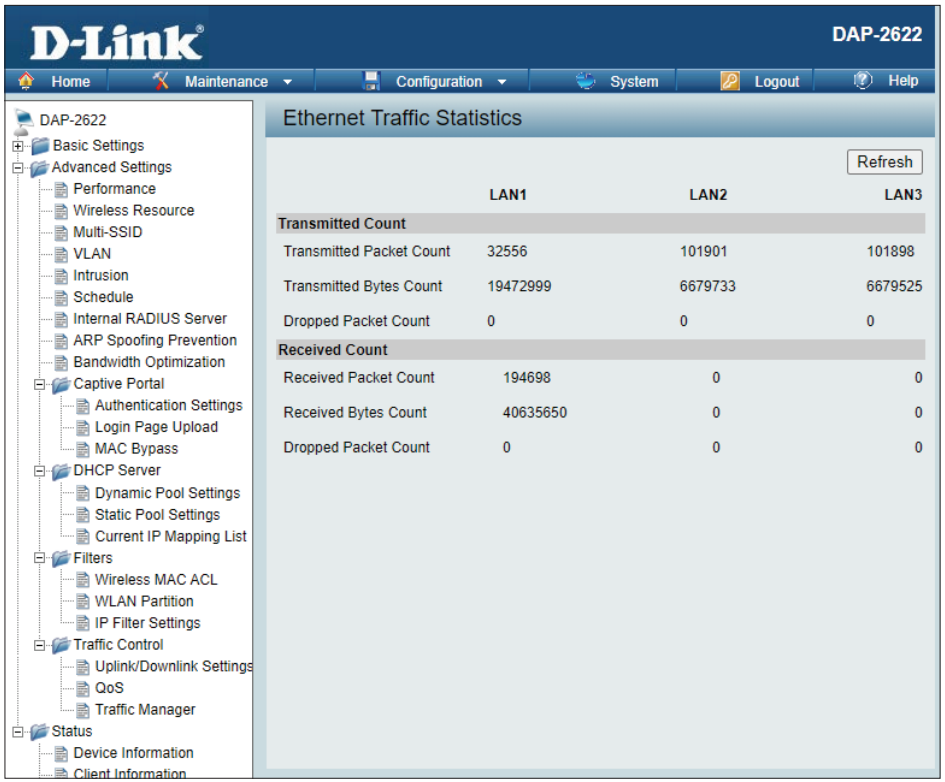


Stats Page

Ethernet Traffic Statistics

Displays wired interface network traffic information.

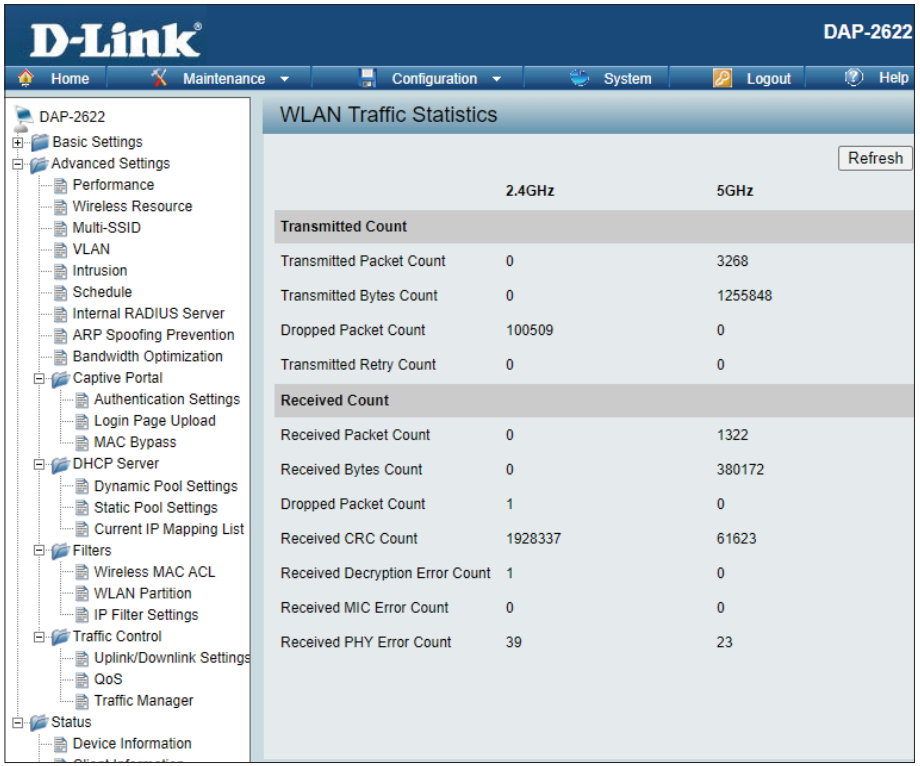
Ethernet Traffic Statistics: This page displays transmitted and received statistics for packets and bytes.



WLAN Traffic Statistics

Displays throughput, transmitted frame, received frame, and WEP frame 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.

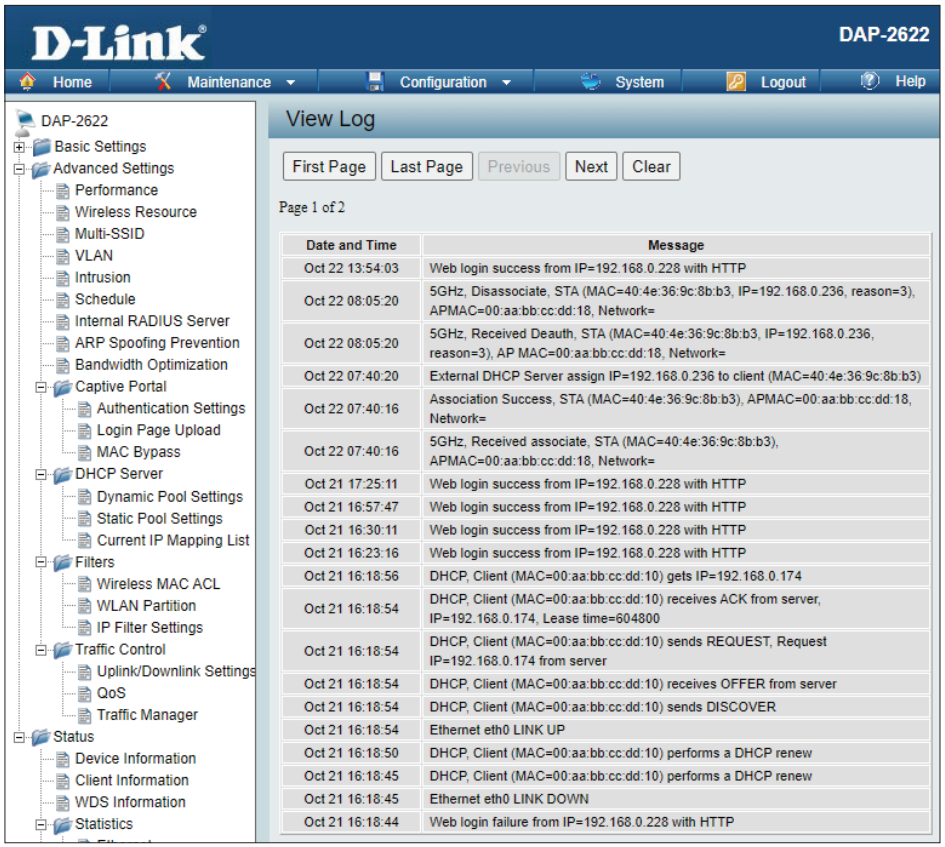


Log

View Log

The AP's embedded memory holds logs here. The log information includes but is not limited to the following items: upgrading firmware, clients associating and disassociating with AP, and logins to the web UI. The page holds up to 500 logs.

View Log: The AP's embedded memory displays system and network messages, including a timestamp and message type.



Log Settings

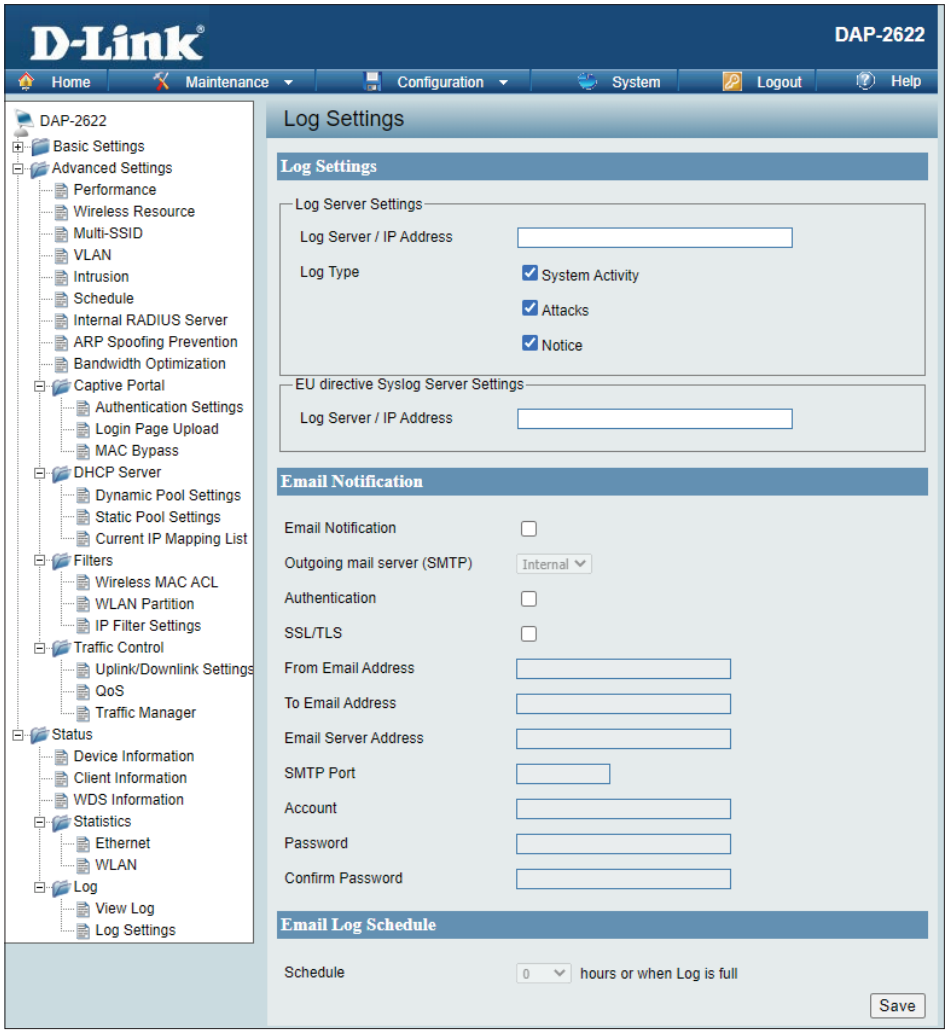
Enter the log server's IP address to send the log to that server. Check or uncheck **System Activity, Wireless Activity**, or **Notice** to specify what kind of log type you want.

Log Server/IP Address: Enter the IP address of the server you would like to send the DAP-2622 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**.

E-mail Notification: The DAP-2622 supports Simple Mail Transfer Protocol for log scheduling and periodical key changing. It does not support Gmail SMTP port 465. Please set to Gmail SMTP port 25 or 587.

E-mail Log Schedule: Use the drop-down menu to set the e-mail schedule.



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 of the account you would like to send the log.

To Email Address Enter the email address of the account you would like to send the log.

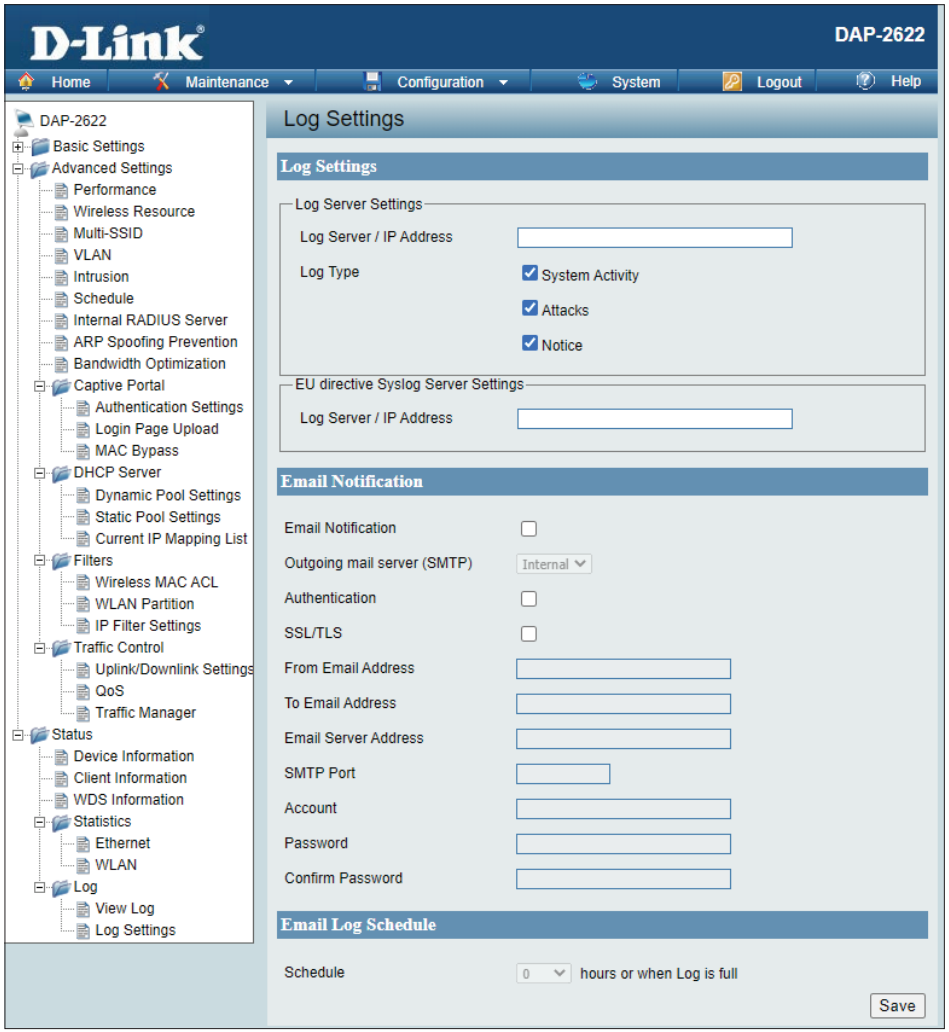
Email Server Address Enter the IP address of the server you would like to send the log.

SMTP Port Enter the SMTP port of the email server.

Account Enter the user name of the of the listed email address.

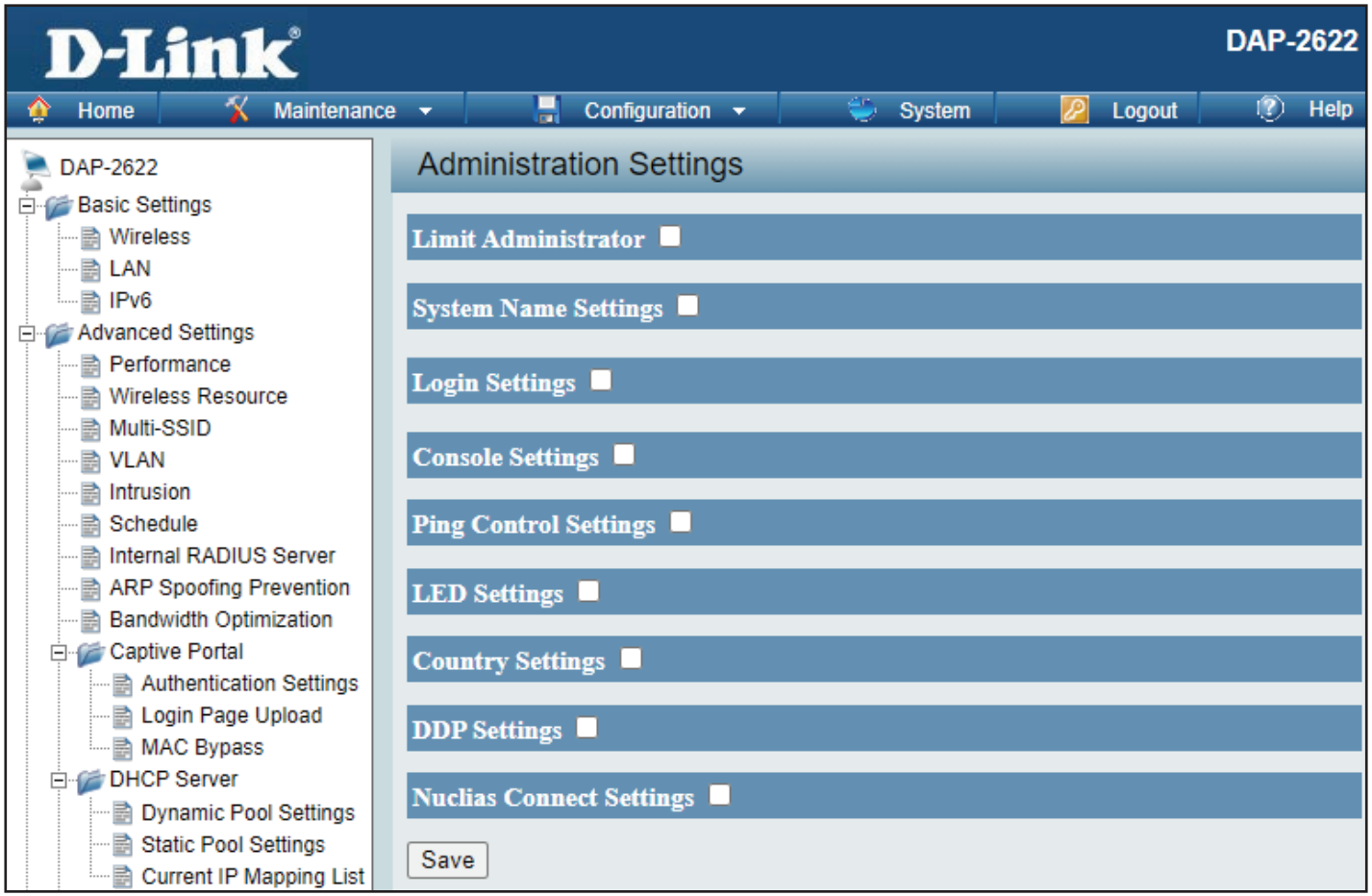
Password Enter the password set for the email notification.

Confirm Password Retype the password entry to confirm the password.



Maintenance Section

In the **Maintenance** section, you can configure miscellaneous settings for the DAP-2622. The following pages will explain settings found in this section in more detail.



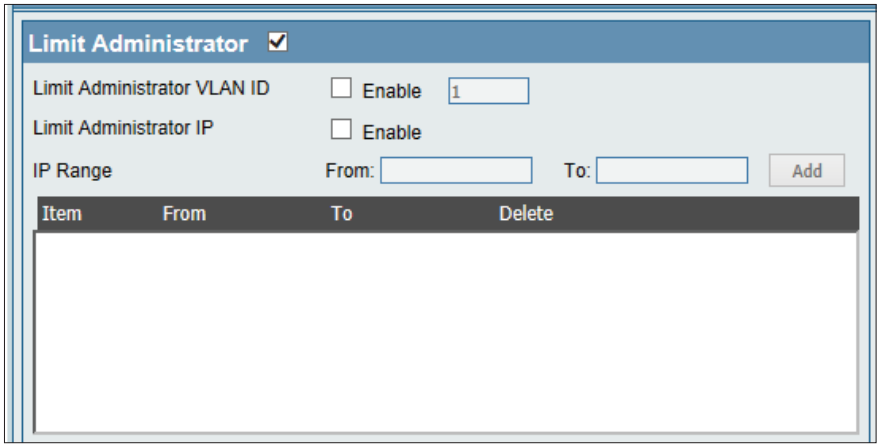
Administration

Limit Administrator

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

Limit Administrator IP: Check to limit the range of IPs that the administrator will be allowed to log in from.

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

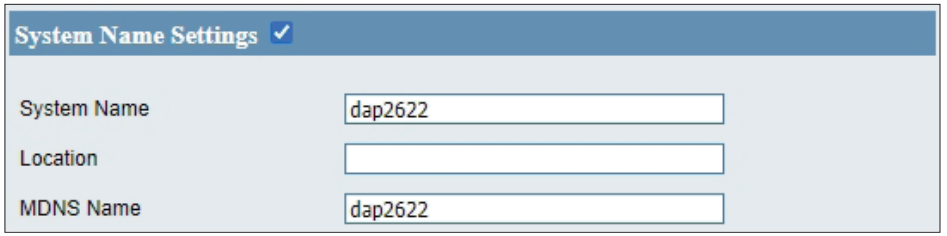


System Name Settings

System Name: The name of the device. The default name is **dap2622**.

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

MDNS Name: The MDNS name of the device. The default name is **dap2622**.

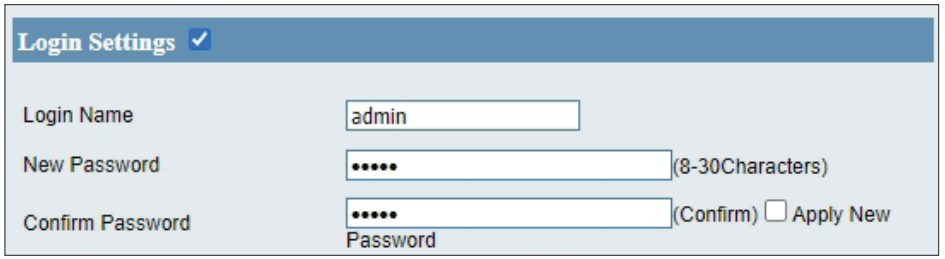


Login Settings

Login Name: Enter a username for the web UI. The default is **admin**.

New Password: When changing your password, enter the new password here. The password is case-sensitive. The length should be between 8 and 30 characters.

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

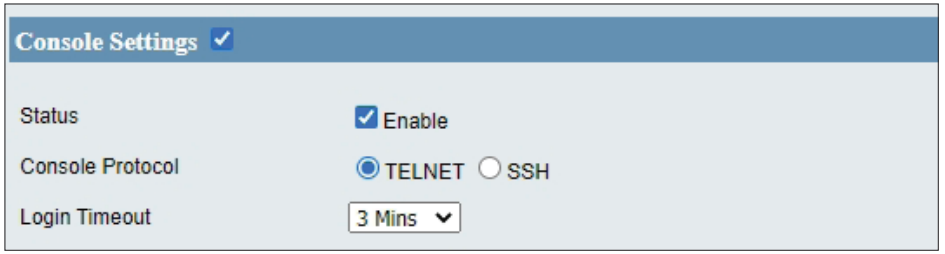


Console Settings

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

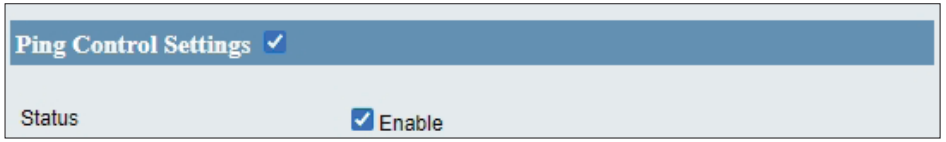
Console Protocol: Select the type of protocol you would like to use, Telnet or SSH.

Timeout: Set to **1 Min, 3 Mins, 5 Mins, 10 Mins, 15 Mins** or **Never**.



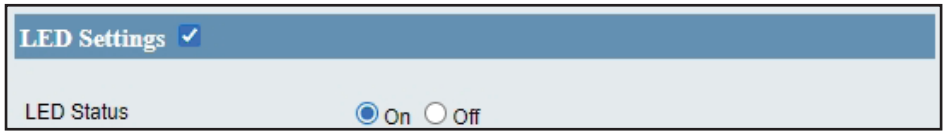
Ping Control Setting

Status: Check the box to enable Ping control. Ping works by sending ICMP "echo request" packets to the target host and listening for a response.



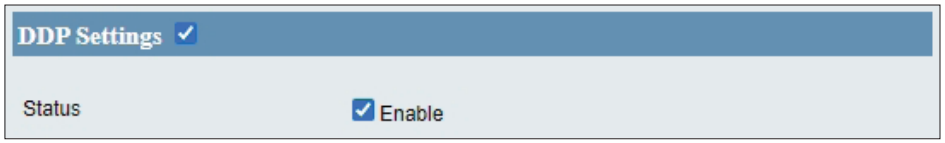
LED Settings

LED Status: Click **On** or **Off** to enable or disable the LED status display.



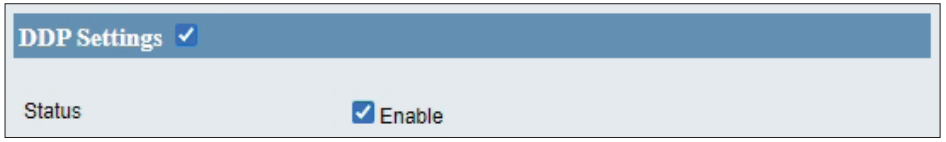
DDP Control Setting

Status: Check the box to enable the DDP control. This is enabled by default.



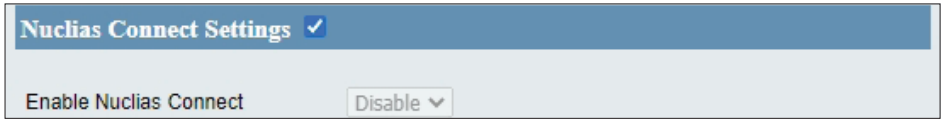
Country Settings

Select a Country: Select the country your network is located in from the drop-down menu.



Nuclias Connect Setting

Enable Nuclias Connect: Check this box to configure the DAP-2622 with Nuclias Connect.



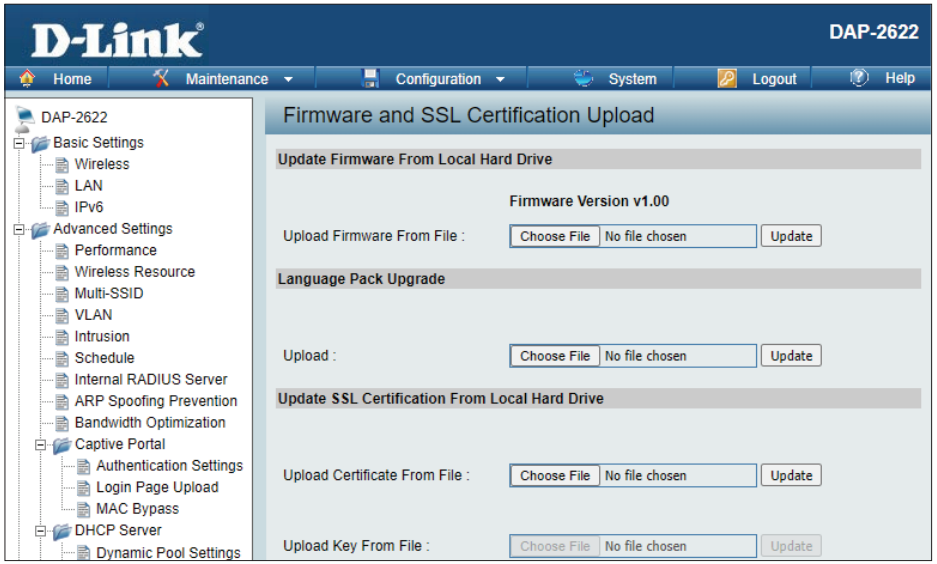
Firmware and SSL Upload

This page allows the user to perform a firmware upgrade. A firmware upgrade is a function that upgrade the running software 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.

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 **Upload** button to begin updating the firmware. Don't turn the power off while upgrading.

Language Pack Upgrade: Select a file with a language pack to upload to the access point.

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 **Upload** to complete the upgrade.



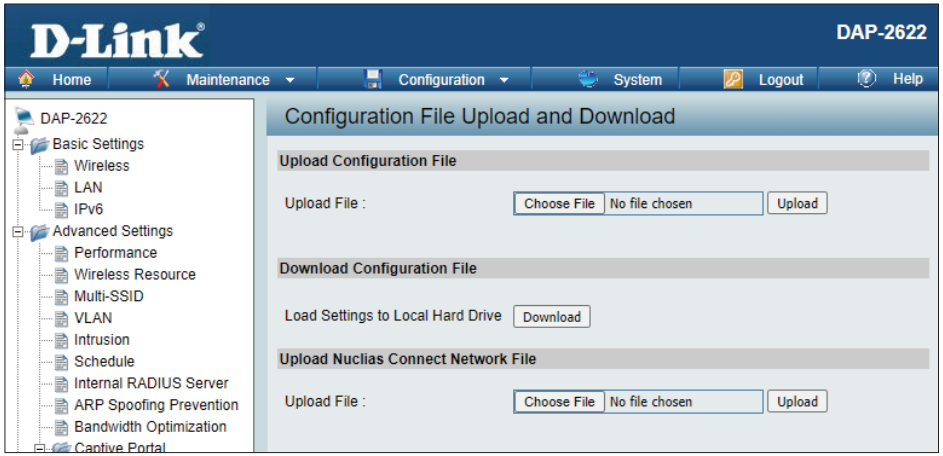
Configuration File Upload

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

Upload Configuration File: Browse to the saved configuration file you have in your local drive and click **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-2622 and then updating to this saved configuration file, the password will be gone.

Upload Nuclias Connect Network File: Browse to a Nuclias Connect configuration file and click **Upload** to upload it to the access point.



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.

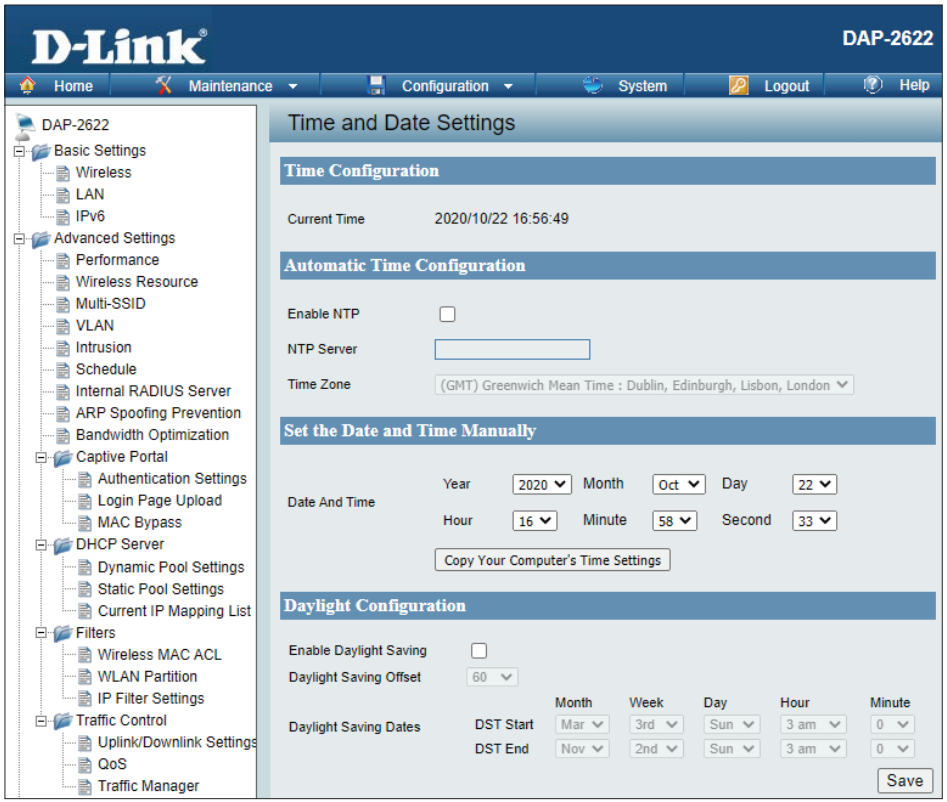
NTP Server: Enter the NTP server IP address.

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

Set the Date and Time Manually: You 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.)

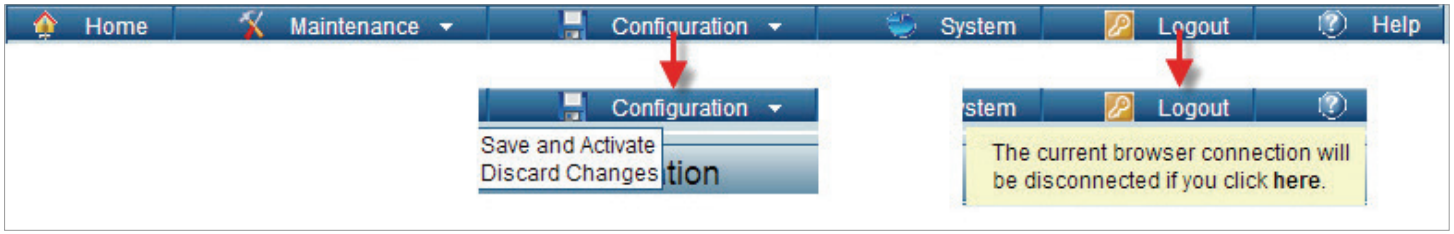
Enable Daylight Saving: Check the box to enable Daylight Saving Time.

Daylight Saving Dates: Use the drop-down menu to select the correct Daylight Saving offset.



Configuration and System

These options are the remaining option to choose from in the top menu. Configuration allows the user to save and activate or discard the current 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.



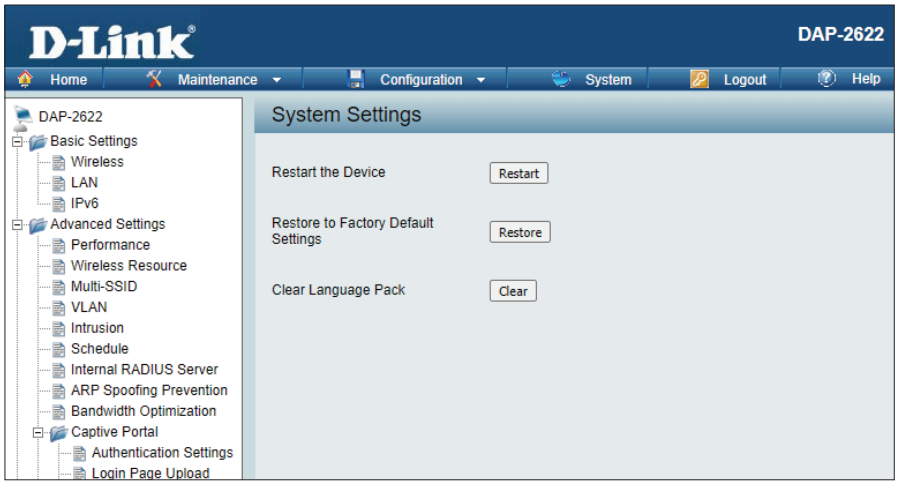
System Settings

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-2622.

Restore to Factory Default Settings: Click **Restore** to restore the DAP-2622 back to factory default settings.

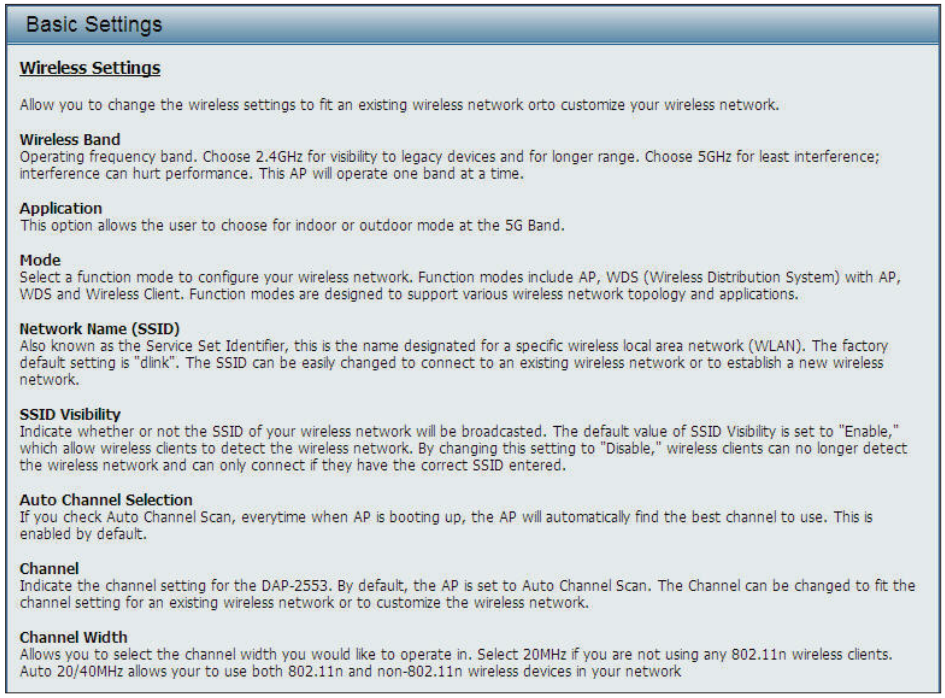
Clear Language Pack: Click to clear the current language pack.



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 orto 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 your to use both 802.11n and non-802.11n wireless devices in your network

Technical Specifications

Standards
- IEEE 802.11ac
- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.11b
- IEEE 802.11a
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3az
- IEEE 802.3at

Network Management
- Web Browser interface (HTTP, Secure HTTP (HTTPS))
- D-Link Nuclias Connect

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
- 802.3at PoE

Antenna Type
- 2 internal

LEDs
- Power/Status

Max. Power Consumption
- 9.5 W, 21.5 W (including PoE output)

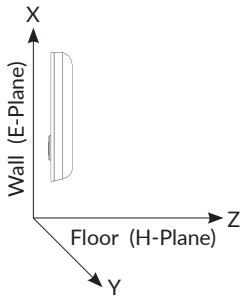
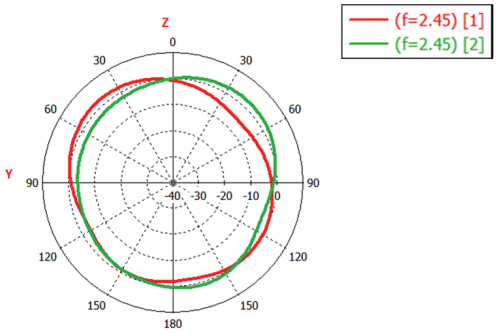
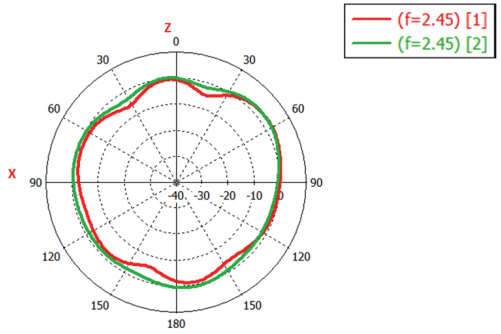
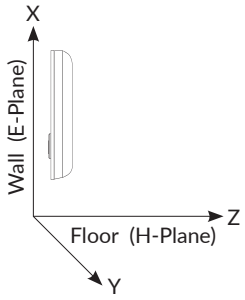
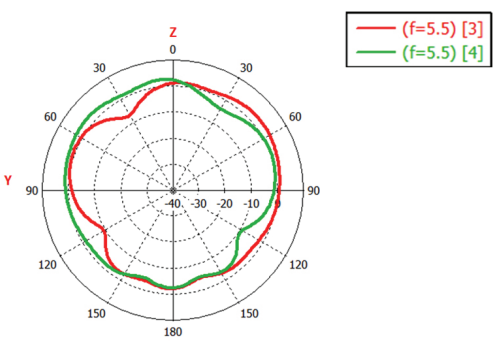
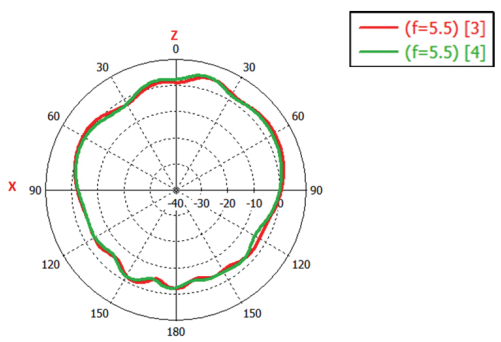
Temperature
- Operating: 0˚C to 40˚C
- Storing: -20˚C to 65˚C

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

Certifications
- CE
- FCC

Dimensions
- L = 154.1 mm (6 in)
- W = 95 mm (3.7 in)
- H = 27.4 mm (1 in)

Antenna Pattern

Orientation	H-Plane	E-Plane
2.4 GHz Wall Mounted	 	
5 GHz Wall Mounted