D-Link®
Building Networks for People

DAP-2230

Version 1.00

Wireless N

PoE Access Point

User Manual

Business Class Networking

Preface

D-Link reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes.

Manual Revisions

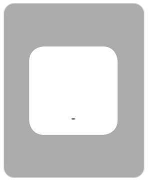
Revision	Date	Description
1.00	June 30, 2015	• Initial release for revision A1

Trademarks

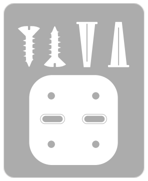
D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Table of Contents

Package Contents



DAP-2230 Wireless N PoE Access Point



Wall mounting bracket with mounting kit

12 V DC, 1 A Power Adapter (included with some models)

Quick Installation Guide

If any of the above items are missing, please contact your reseller.

Note: Using a power supply with a different voltage rating will cause damage and void the warranty for this product.

System Requirements

Network Requirements	• An Ethernet-based Network • IEEE 802.11n/g wireless clients (AP Mode) • IEEE 802.11n/g wireless network (AP Mode)
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Microsoft Internet Explorer® 7, Mozilla® Firefox® 12.0, Google® Chrome 20.0, or Safari® 4 or higher **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.

Introduction

The D-Link DAP-2230 Wireless N PoE Access Point is an 802.11n compliant device that delivers real world performance of up to 300 Mbps* while still maintaining backwards compatibility with slower 802.11g and 802.11b devices. The DAP-2230 increases productivity by allowing you to work faster and more efficiently. With the DAP-2230, bandwidth-intensive applications like graphics or multimedia will benefit significantly because large files are now able to move across the network more quickly. Create a secure wireless network to share photos, files, music, video, printers, and network storage outside of your normal internal networking environment. Built to withstand harsh environments, the DAP-2230 also excels in connecting separate networks that cannot be joined physically using a traditional medium. The built-in omni-directional 3 dBi antenna is designed to deliver high performance, ensuring that wireless coverage will cover even hard to reach locations. The DAP-2230 is an ideal solution for quickly creating and extending a wireless local area network (WLAN) in offices or other workplaces, hotels, resorts, trade shows, and special events.

The DAP-2230 features four different operation modes: Access Point, Wireless Distribution System (WDS), WDS with AP, and Wireless Client mode, allowing it to adapt to many situations. As a standard wireless Access Point (AP) the DAP-2230 can connect to a wide range of devices that are 802.11 n/g/b compliant. In WDS mode it can expand current wireless coverage without the need for a wired backbone link. As a wireless client it can connect to an existing AP, and expand the network physically with the built-in 10/100 Ethernet port.

The DAP-2230 supports 64/128-bit WEP data encryption and WPA/WPA2 security functions. In addition, it provides MAC Address Filtering to control user access, and the Disable SSID Broadcast function to limit unauthorized access to the internal network. Network administrators have multiple options for managing the DAP-2230, including Web (HTTP) or Secured Web (HTTPS). For advanced network management, administrators can use SNMP v1, v2c, v3 to configure and manage access points.

*Maximum wireless signal rate derived from IEEE Standard 802.11n and 802.11g specifications. Actual data throughput may vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead can lower actual data throughout rate.

Features

- **Faster Wireless Networking -** The DAP-2230 provides an up to 300 Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.

- **Compatible with IEEE802.11g Devices -** The DAP-2230 is still fully compatible with the 802.11g standards, so it can connect with existing 802.11g adapters.

- **Four different operation modes -** Capable of operating in one of four different operation modes to meet your wireless networking needs: Access Point, WDS with AP, WDS, and Wireless Client.

- **Power over Ethernet -** The DAP-2230 supports IEEE 802.3af PoE (Power over Ethernet) which enables it to be supplied with power over an Ethernet cable or IEEE 802.3af PoE switch.

- **Comprehensive Web-Interface -** Fine tune network settings using the DAP-2230's robust network-based configuration software.

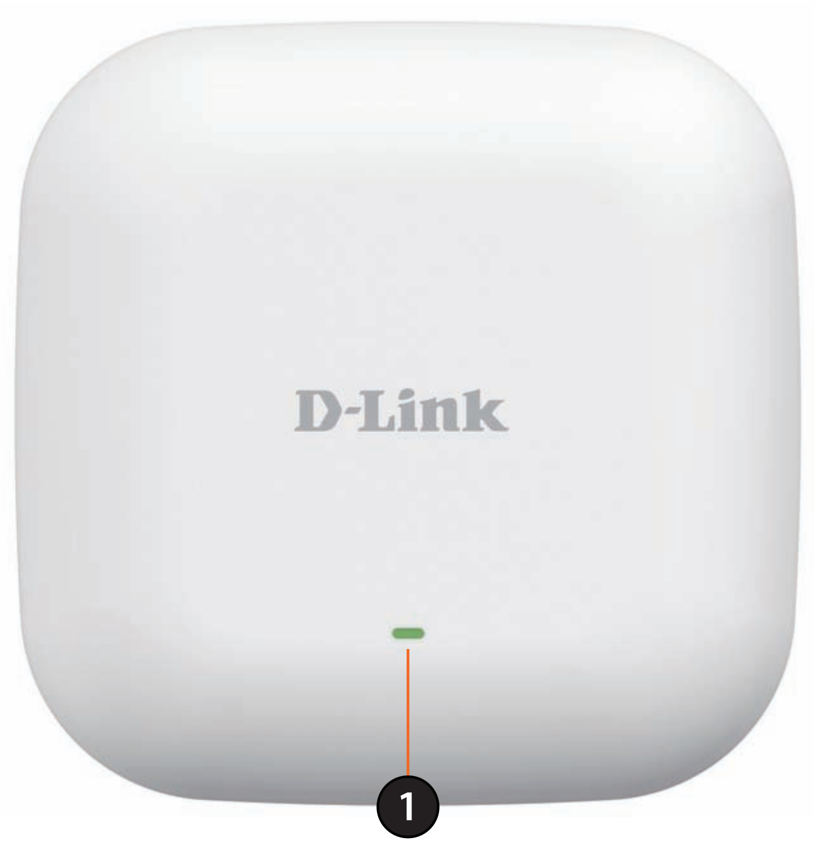
- **Central WiFiManager management software compatibility -** The real-time display of the network's topology and AP's information makes network configuration and management of multiple devices quick and simple.

- **SNMP for management -** The DAP-2230 supports SNMP v1, v2c, and v3 for better network management. Superior wireless AP manager software is bundled with the DAP-2230 for network configuration and firmware upgrade. Systems administrators can also set up the DAP-2230 easily with the Web-based configuration utility.

- **Convenient Installation -** The DAP-2230 features a wall mount in the rear for easy setup on walls.

Hardware Overview

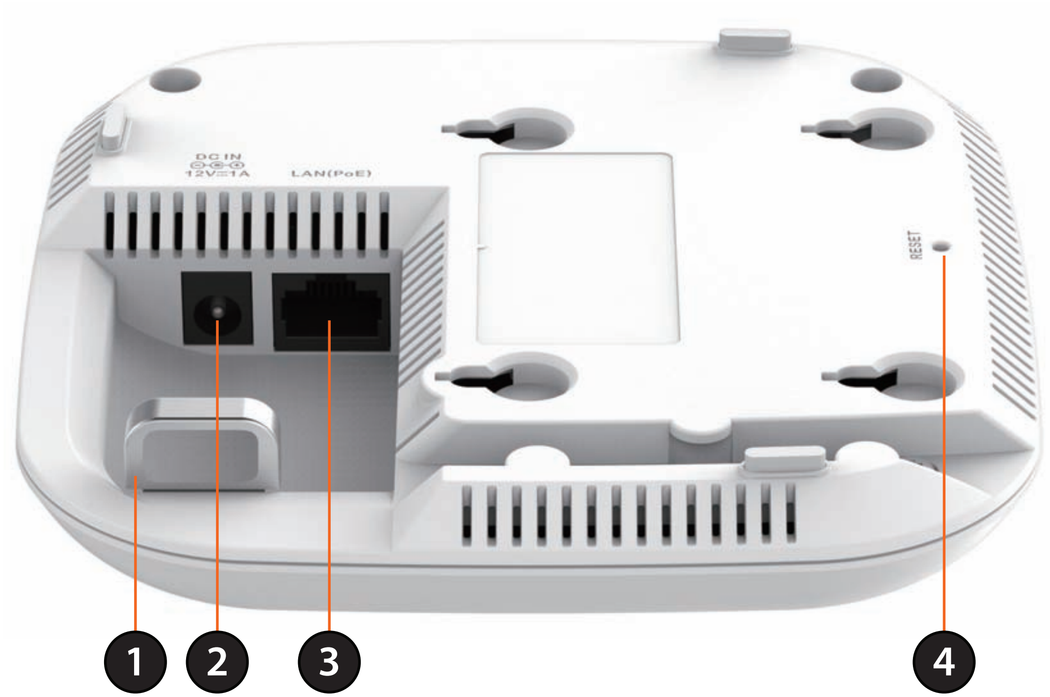
Top Panel



Power/Status LED		
1	Static Green	Ready/Working Properly
	Flashing Green	Transmitting/Receiving data
	Flashing Red	Malfunction during boot
	Solid Red	Boot failure

Hardware Overview

Bottom Panel



1	**Security Lock**	Physically secure your device with this lock.
2	**Power Connector**	Connector for a power adapter.
3	**10/100 LAN (PoE)Port**	Connect an Ethernet cable to this device and your network. Power may be supplied to this port via a LAN cable that is connected to a PoE injector or PoE switch.
4	**Reset Button**	Press and hold the reset button with a paperclip for at least 5 seconds to reset the device back to the factory default settings. The LED will turn on for 2 seconds and then begin the reboot process.

Physical Installation

Before You Begin

This chapter describes safety precautions and product information that you must know and check before installing this product.

Professional Installation Required

1. Please seek assistance from a professional installer who is well trained in RF installation and knowledgeable about local regulations.
2. This product is distributed through distributors and system installers with professional technicians and is not to be sold directly through retail stores.

Connect to your Network

To power the access point, you can use one of the following 3 methods:

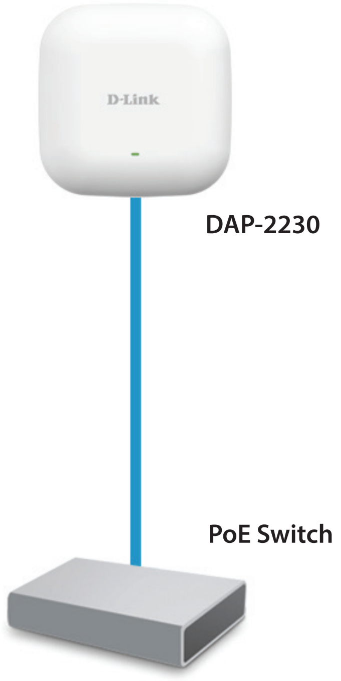
Method 1 - Powered by PoE Switch

Method 2 - Powered by PoE Injector

Method 3 - Powered by DC Adapter

Method 1 - Powered by PoE Switch

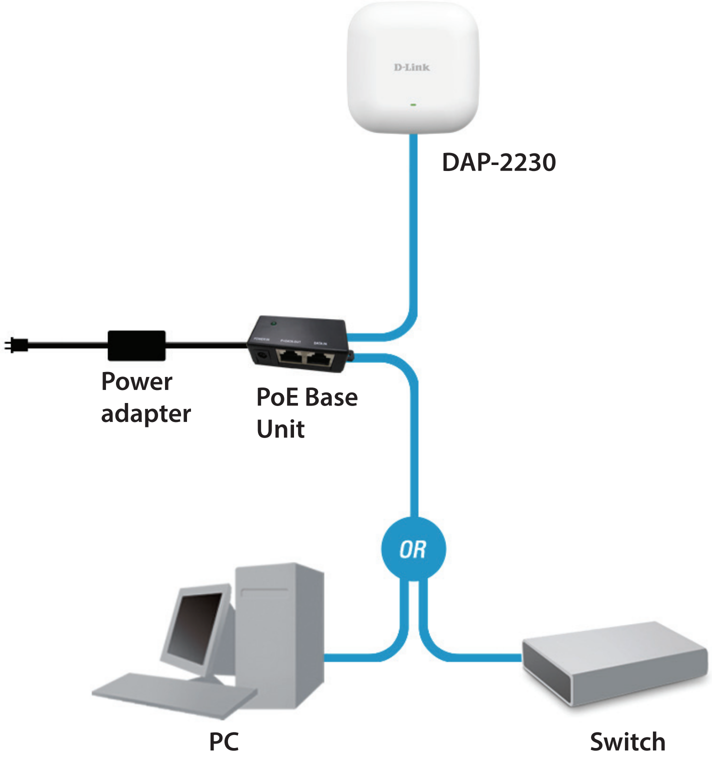
1. Connect one end of an Ethernet cable into the **LAN (PoE)** port on the DAP-2230 and then connect the other end to a PoE switch.



Method 2 - Powered by PoE Injector

If you wish to power the DAP-2230 without a PoE switch, we suggest you use a PoE injector, such as a DPE-101GI.

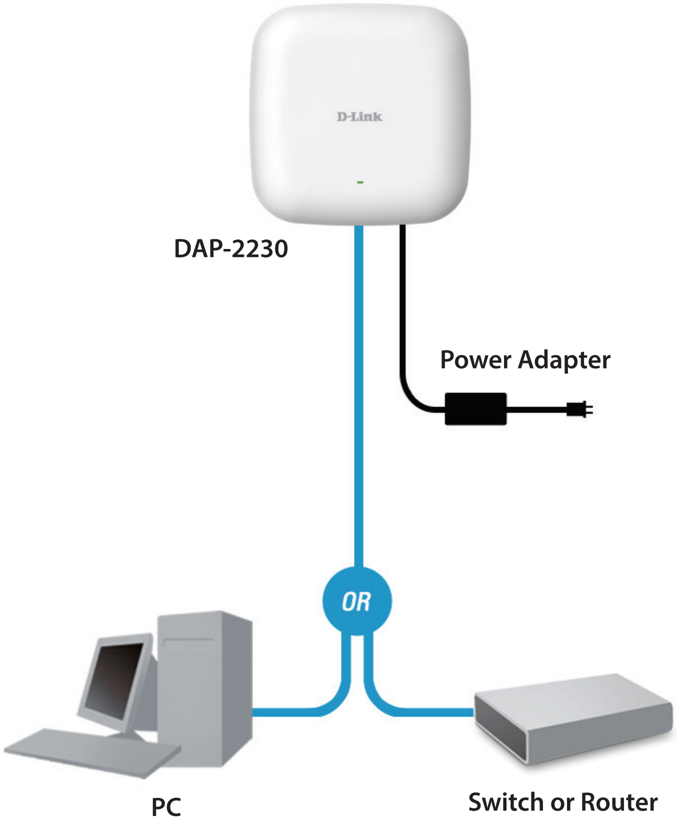
1. Connect one end of an Ethernet cable into the **DATA IN** port on the PoE injector and the other end into a port on a switch, router, or computer.
2. Connect one end of a different Ethernet cable into the **P+DATA OUT** port on the PoE injector and the other end into the **LAN (PoE)** port on the DAP-2230 access point.
3. Connect the supplied power adapter to the **POWER IN** connector on the PoE Injector.
4. Plug the power adapter into a power outlet.



Method 3 - DC Adapter

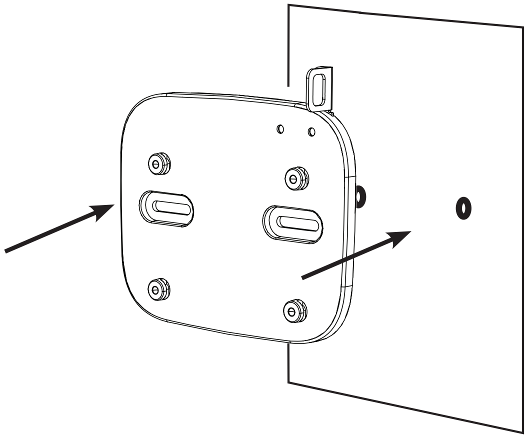
A power adapter is included with some DAP-2230 models.

1. Connect an Ethernet cable from your network device to the **LAN(PoE)** port on the DAP-2230.
2. Connect the supplied power adapter to the **DC IN** connector on the DAP-2230.
3. Plug the power adapter into a power outlet.

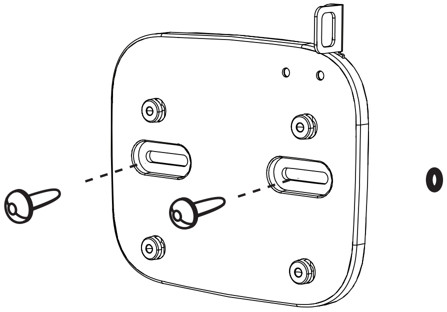


Mounting the AP

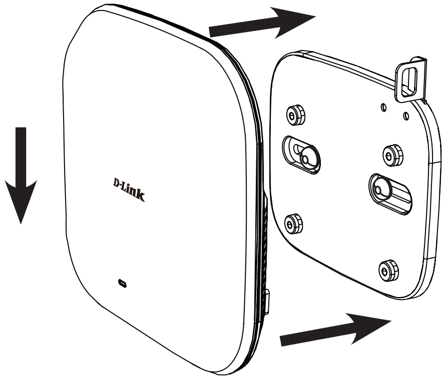
Place the mounting bracket on a wall or ceiling and mark holes where you will insert the screws with a marker. Drill holes in the marked points and insert the plastic wall anchors.



Use the supplied screws to attach the mounting plate to the wall.



Reattach the DAP-2230 to the mounting bracket.



Wireless Installation Considerations

The D-Link DAP-2230 Wireless N PoE Access Point lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

1. Keep the number of walls and ceilings between the D-Link access point and other network devices to a minimum. Each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters). Position your devices so that the number of walls or ceilings is minimized.

2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless access points, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.

4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

5. If you are using 2.4 Ghz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 Hz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

Four Operational Modes

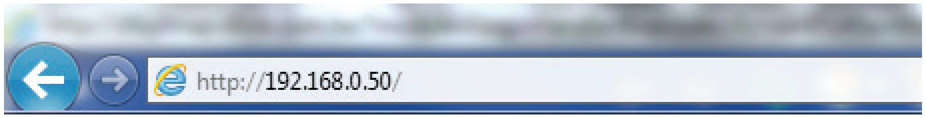
Operation Mode **(Only supports 1 mode at a time)**	**Function**
Access Point (AP)	Create a wireless LAN
WDS with AP	Wirelessly connect multiple networks while still functioning as a wireless AP
WDS	Wirelessly connect multiple networks
Wireless Client	AP acts as a wireless network adapter for your Ethernet-enabled device

Configuration

This section will show you how to configure your new D-Link Wireless N PoE Access Point using the web-based configuration utility.

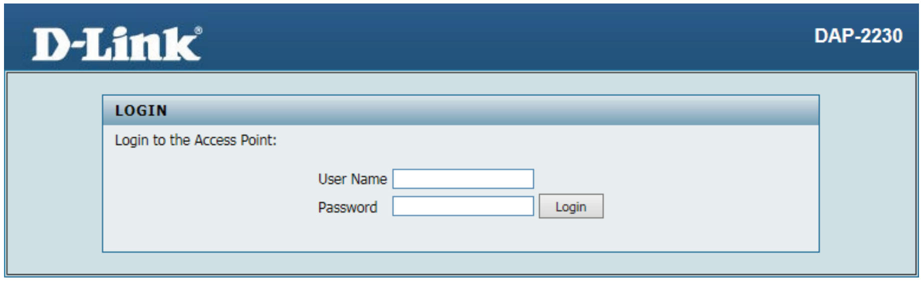
Web-based Configuration Utility

If you wish to change the default settings or optimise the performance of the DAP-2230, you may use the web-based configuration utility.



http://192.168.0.50/

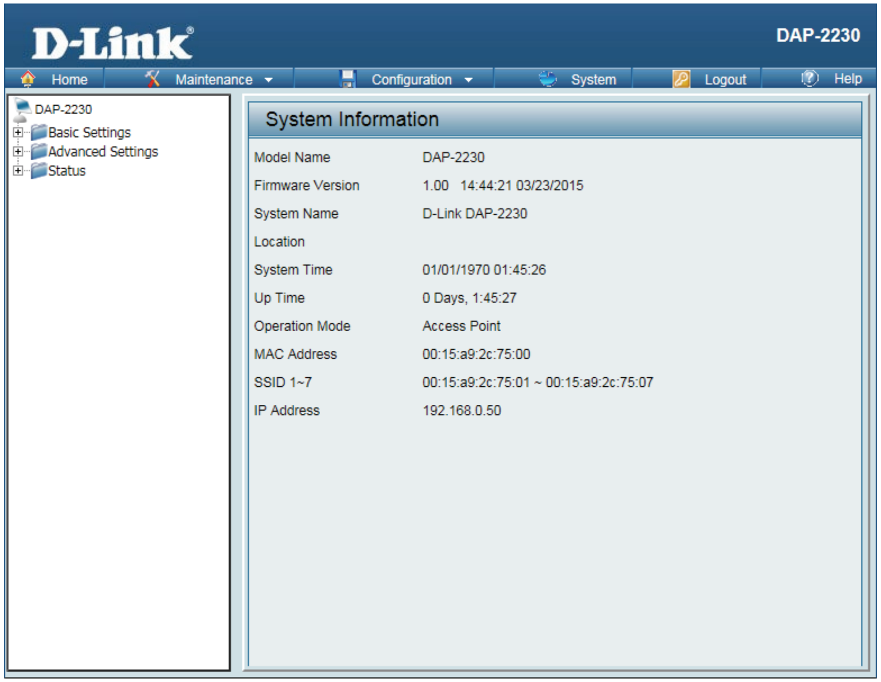
To access the configuration utility, open a web browser such as Internet Explorer and enter **http://192.168.0.50**



Type **admin** and then enter your password. Leave the password blank by default.

If you get a Page Cannot be Displayed error, please refer to “Troubleshooting” on page 104 for assistance.

After successfully logging into the DAP-2230, the following screen will appear:



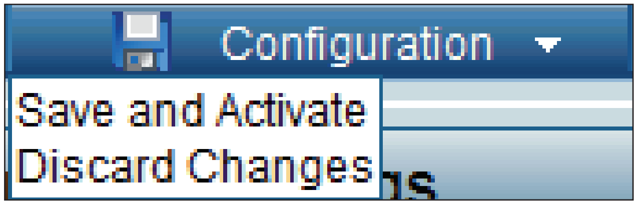
System Information

Model Name	DAP-2230
Firmware Version	1.00 14:44:21 03/23/2015
System Name	D-Link DAP-2230
Location	
System Time	01/01/1970 01:45:26
Up Time	0 Days, 1:45:27
Operation Mode	Access Point
MAC Address	00:15:a9:2c:75:00
SSID 1~7	00:15:a9:2c:75:01 ~ 00:15:a9:2c:75:07
IP Address	192.168.0.50

Save and Activate Settings

When making changes on most of the configuration screens in this section, use the Save button at the bottom of each screen to save (not activate) your configuration changes.

You may change settings to multiple pages before activating. Once you are finished, click the **Configuration** button located at the top of the page and then click **Save and Activate**.



Basic Settings

Wireless

Access Point mode

Wireless Band: Select **2.4 Ghz** from the drop-down menu.

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

The other three choices are **WDS with AP**, **WDS**, and **wireless Client**.

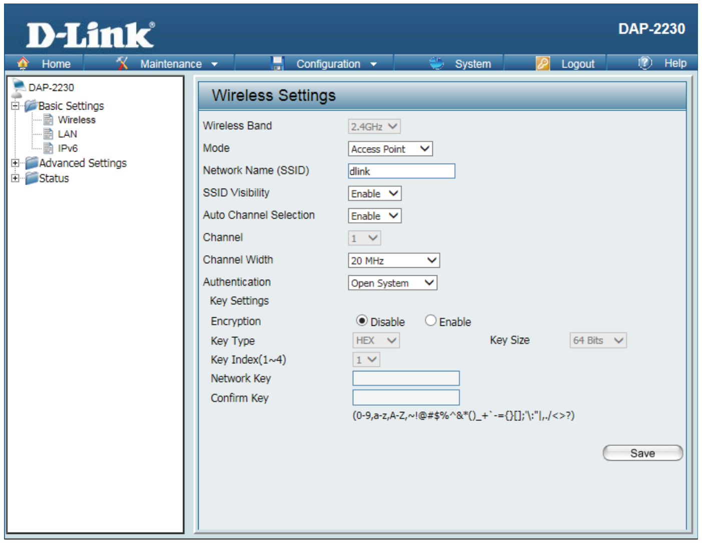
Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. The SSID can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

SSID Visibility: **Enable** or **Disable** SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users. This feature is enabled by default.

Auto Channel Selection: Enabling this feature automatically selects the channel that provides the best wireless performance. **Enable** is set by default. 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, 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.*



Wireless Settings

Wireless Band	2.4GHz
Mode	Access Point
Network Name (SSID)	dlink
SSID Visibility	Enable
Auto Channel Selection	Enable
Channel	1
Channel Width	20 MHz
Authentication	Open System
Key Settings	
Encryption	● Disable ○ Enable
Key Type	HEX
Key Size	64 Bits
Key Index(1~4)	1
Network Key	
Confirm Key	

(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)

Channel Width: Allows you to select the channel width you would like to operate in. 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 wireless devices on your network.

Authentication: Use the drop-down menu to choose **Open System**, **Shared Key**, **WPA-Personal**, **WPA-Enterprise**, or **802.11x**.

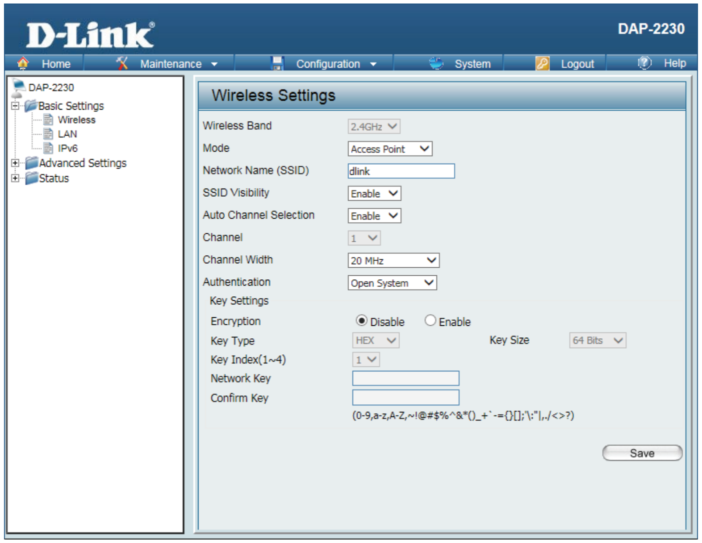
Select **Open System** to communicate the key across the network.

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 to secure your network using 802.1x authentication.



Wireless Settings

Wireless Band	2.4GHz
Mode	Access Point
Network Name (SSID)	dlink
SSID Visibility	Enable
Auto Channel Selection	Enable
Channel	1
Channel Width	20 MHz
Authentication	Open System
Key Settings	
Encryption	● Disable ○ Enable
Key Type	HEX
Key Size	64 Bits
Key Index(1~4)	1
Network Key	
Confirm Key	

(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)

WDS with AP mode

In WDS with AP mode, the DAP-2230 wirelessly connects multiple networks while still functioning as a wireless AP.

Wireless Band: Select **2.4 Ghz** from the drop-down menu.

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

The other three choices are **Access Point, WDS**, and **wireless Client**.

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

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

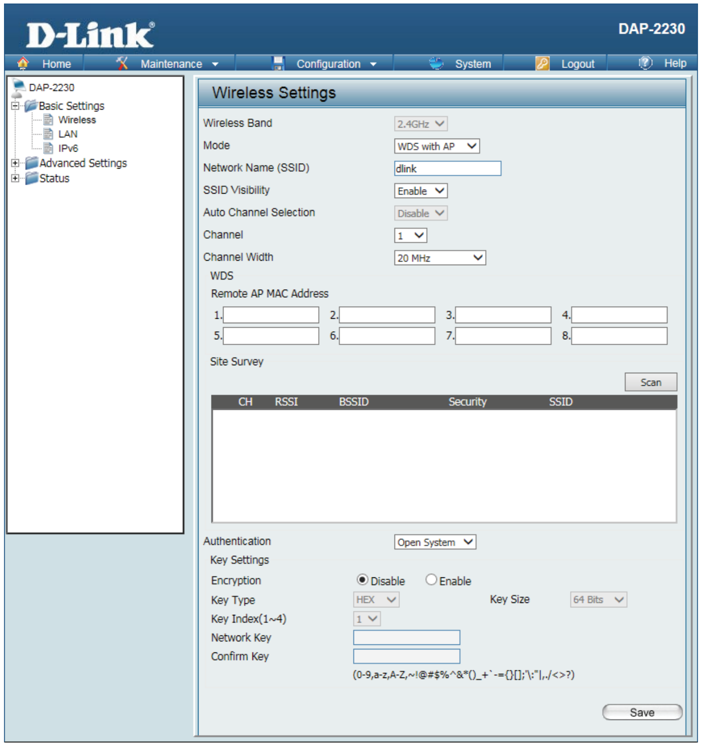
Auto Channel Selection: Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is not supported in WDS with AP mode. The channel selection process only occurs when the AP is booting up.

Channel: 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: Indicates whether the device is capable of 20 MHz operation only or both 20 MHz and 40 MHz operation.

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

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



Wireless Settings

Wireless Band: 2.4GHz

Mode: WDS with AP

Network Name (SSID): dlink

SSID Visibility: Enable

Auto Channel Selection: Disable

Channel: 1

Channel Width: 20 MHz

WDS

Remote AP MAC Address

1. 2. 3. 4.

5. 6. 7. 8.

Site Survey

CH	RSSI	BSSID	Security	SSID

Authentication: Open System

Key Settings

Encryption: ● Disable ○ Enable

Key Type: HEX Key Size: 64 Bits

Key Index(1~4): 1

Network Key

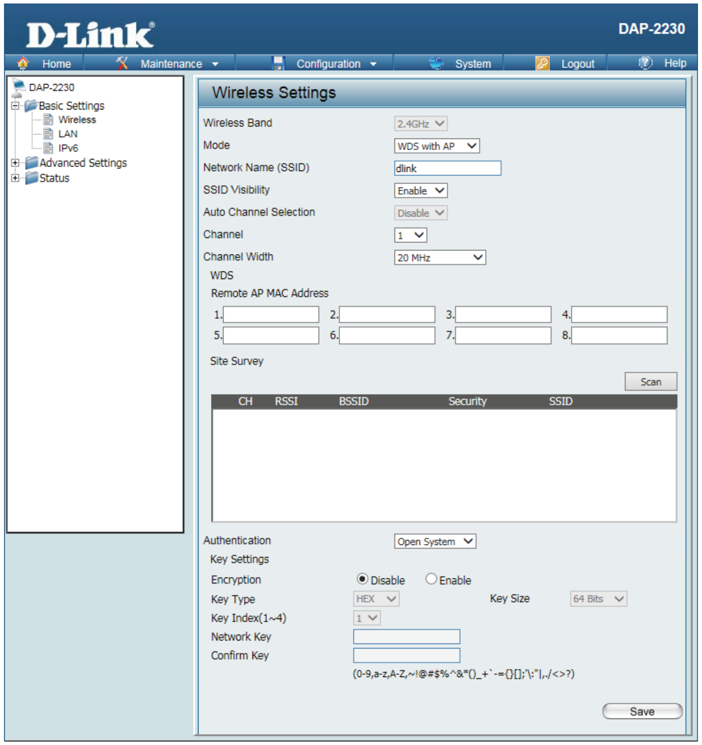
Confirm Key

(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)

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

Select **Open System** to communicate the key across the network.

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



Wireless Settings

Wireless Band	2.4GHz
Mode	WDS with AP
Network Name (SSID)	dlink
SSID Visibility	Enable
Auto Channel Selection	Disable
Channel	1
Channel Width	20 MHz

WDS

Remote AP MAC Address

1. 2. 3. 4.
5. 6. 7. 8.

Site Survey

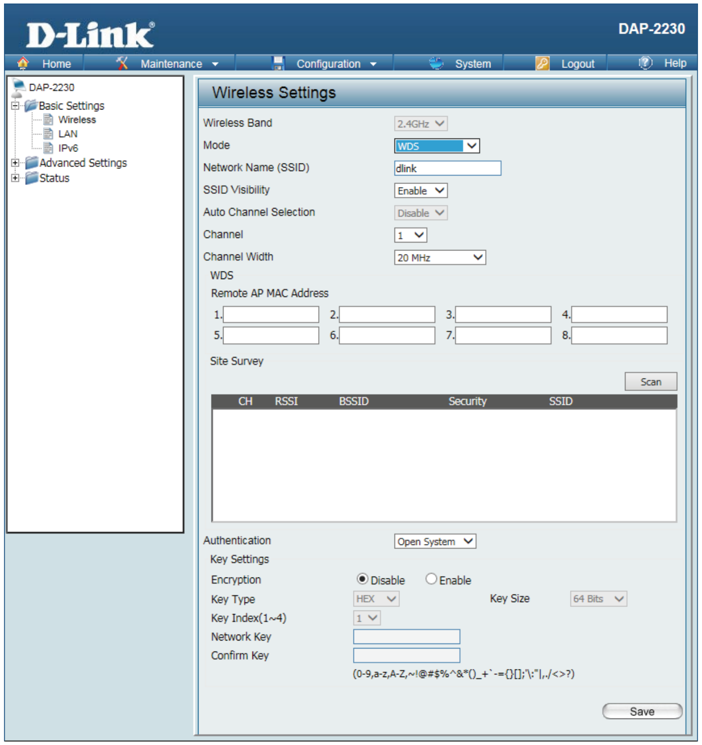
CH	RSSI	BSSID	Security	SSID

Authentication	Open System		
Key Settings			
Encryption	● Disable ○ Enable		
Key Type	HEX	Key Size	64 Bits
Key Index(1~4)	1		
Network Key			
Confirm Key			

(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)

WDS mode

In WDS mode, the DAP-2230 wirelessly connects multiple networks, without functioning as a wireless AP.



Wireless Settings

Wireless Band: 2.4GHz

Mode: WDS

Network Name (SSID): dlink

SSID Visibility: Enable

Auto Channel Selection: Disable

Channel: 1

Channel Width: 20 MHz

WDS

Remote AP MAC Address

1. 2. 3. 4.
5. 6. 7. 8.

Site Survey

CH	RSSI	BSSID	Security	SSID

Authentication: Open System

Key Settings

Encryption: ● Disable ○ Enable

Key Type: HEX   Key Size: 64 Bits

Key Index(1~4): 1

Network Key

Confirm Key

(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)

Wireless Band: Select **2.4 Ghz** from the drop-down menu.

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

The other three choices are **Access Point, WDS with AP**, and **wireless Client**.

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

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

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

Channel: 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: Indicates whether the device is capable of 20 MHz operation only or both 20 MHz and 40 MHz operation.

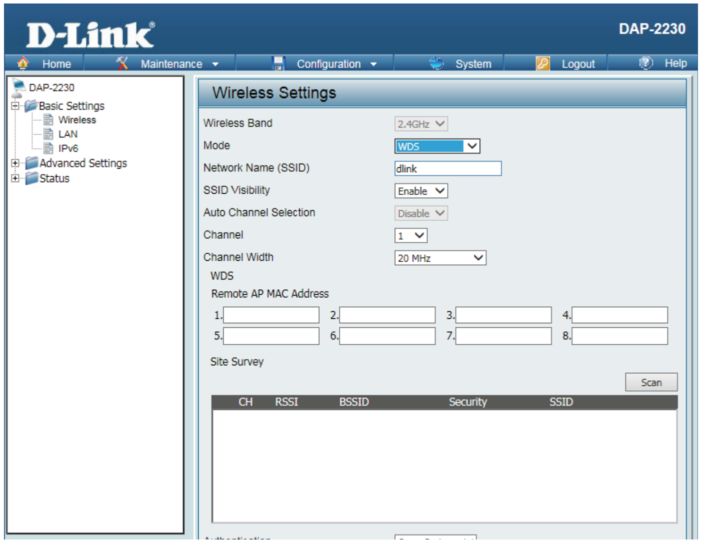
Remote AP MAC Address: Enter the MAC addresses of the APs on your network that will serve as bridges to wirelessly connect multiple networks.

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

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

Select **Open System** to communicate the key across the network.

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



Wireless Settings

Wireless Band	2.4GHz
Mode	WDS
Network Name (SSID)	dlink
SSID Visibility	Enable
Auto Channel Selection	Disable
Channel	1
Channel Width	20 MHz

WDS

Remote AP MAC Address

1. 2. 3. 4.
5. 6. 7. 8.

Site Survey

CH	RSSI	BSSID	Security	SSID

Wireless Client mode

Wireless Band: Select **2.4 Ghz** from the drop-down menu.

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

The other three choices are **Access Point, WDS with AP**, and **WDS**.

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

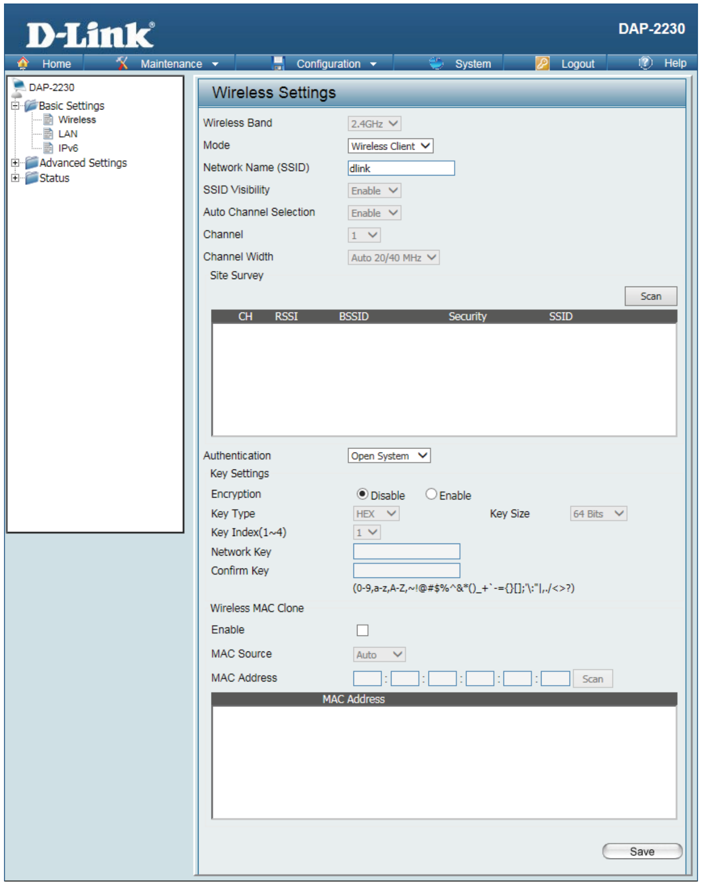
SSID Visibility: **Enable** or **Disable** SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users. Disabling SSID is not supported in Wireless Client mode.

Auto Channel Selection: Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is automatically enabled in Wireless Client mode. The channel selection process only occurs when the AP is booting up.

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: Indicates whether the device is capable of 20 MHz operation only or both 20 MHz and 40 MHz operation.

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



Wireless Settings

Wireless Band: 2.4GHz
Mode: Wireless Client
Network Name (SSID): dlink
SSID Visibility: Enable
Auto Channel Selection: Enable
Channel: 1
Channel Width: Auto 20/40 MHz
Site Survey

Authentication: Open System
Key Settings
Encryption: ● Disable ○ Enable
Key Type: HEX   Key Size: 64 Bits
Key Index(1~4): 1
Network Key:
Confirm Key:
(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)

Wireless MAC Clone
Enable: □
MAC Source: Auto
MAC Address: _ : _ : _ : _ : _ : _

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

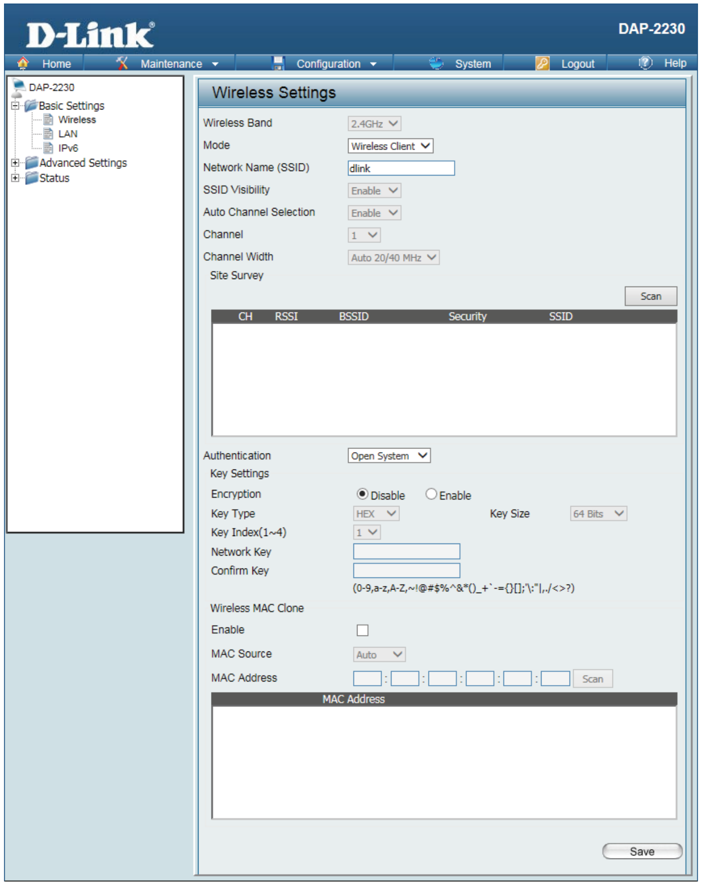
Select **Open System** to communicate the key across the network.

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

Wireless Mac Clone Enable: Check to enable clone MAC. This feature will allow you to change the MAC address of the access point to the MAC address of a client.

MAC Source: Select the MAC source from the drop-down menu.

MAC Address: Enter the MAC address that you would like to assign to the access point.



Wireless Settings

Wireless Band	2.4GHz		
Mode	Wireless Client		
Network Name (SSID)	dlink		
SSID Visibility	Enable		
Auto Channel Selection	Enable		
Channel	1		
Channel Width	Auto 20/40 MHz		
Site Survey			

CH	RSSI	BSSID	Security	SSID

Authentication	Open System		
Key Settings			
Encryption	● Disable ○ Enable		
Key Type	HEX	Key Size	64 Bits
Key Index(1~4)	1		
Network Key			
Confirm Key			
	(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)		
Wireless MAC Clone			
Enable	□		
MAC Source	Auto		
MAC Address	: : : : :		

MAC Address

Authentication Types

Each of the wireless modes on the DAP-2230 support different types of wireless encryption security standards. Not every mode supports all types of encryption.

Open System/Shared Key Authentication

All wireless modes on the DAP-2230 support Open System/Shared Key Authentication.

Encryption Use the radio button to disable or enable encryption.

Key Type: Select **HEX*** or **ASCII****.

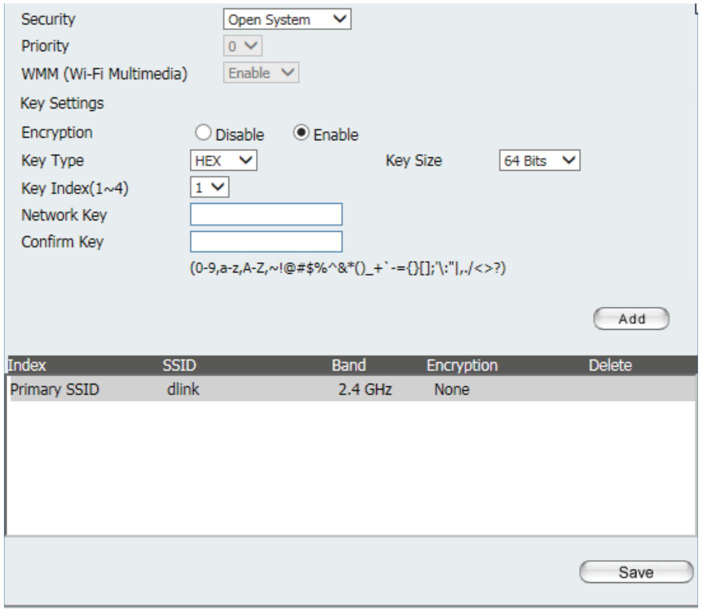
Key Size: Select **64 Bits** or **128 Bits**.

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.*

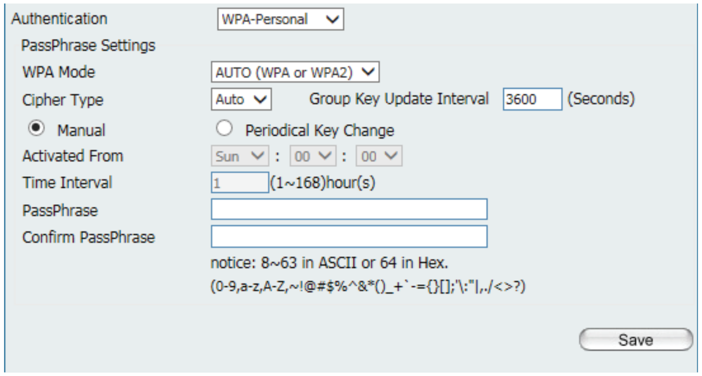


Security: Open System
Priority: 0
WMM (Wi-Fi Multimedia): Enable
Key Settings
Encryption: ○ Disable ● Enable
Key Type: HEX Key Size: 64 Bits
Key Index(1~4): 1
Network Key:
Confirm Key:
(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)

Index	SSID	Band	Encryption	Delete
Primary SSID	dlink	2.4 GHz	None	

WPA/WPA2-Personal Authentication

WPA/WPA2 Personal Authentication can be enabled for **Access Point**, **WDS with AP**, **WDS**, and **Wireless Client** modes.



Authentication: WPA-Personal

PassPhrase Settings

WPA Mode: AUTO (WPA or WPA2)

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

● Manual   ○ Periodical Key Change

Activated From: Sun : 00 : 00

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

PassPhrase:

Confirm PassPhrase:

notice: 8~63 in ASCII or 64 in Hex.

(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)

WPA Mode: When **WPA-Personal** is selected for Authentication type, 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 drop-down menu.

Group Key Update: Select the interval during which the group key will be valid. The default value of **3600** is recommended.
Select **Manual** to enter your key (PassPhrase).
You can select **Periodical Key Change** to have the access point automatically change your PassPhrase.

Periodical Key Change: Enter the Activate From time and the time in hours to change the key.

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

Confirm PassPhrase: Type the passphrase again to guard against typos.

WPA/WPA2-Enterprise Authentication

WPA/WPA2 Enterprise Authentication can only be enabled for **Access Point** mode.

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**.

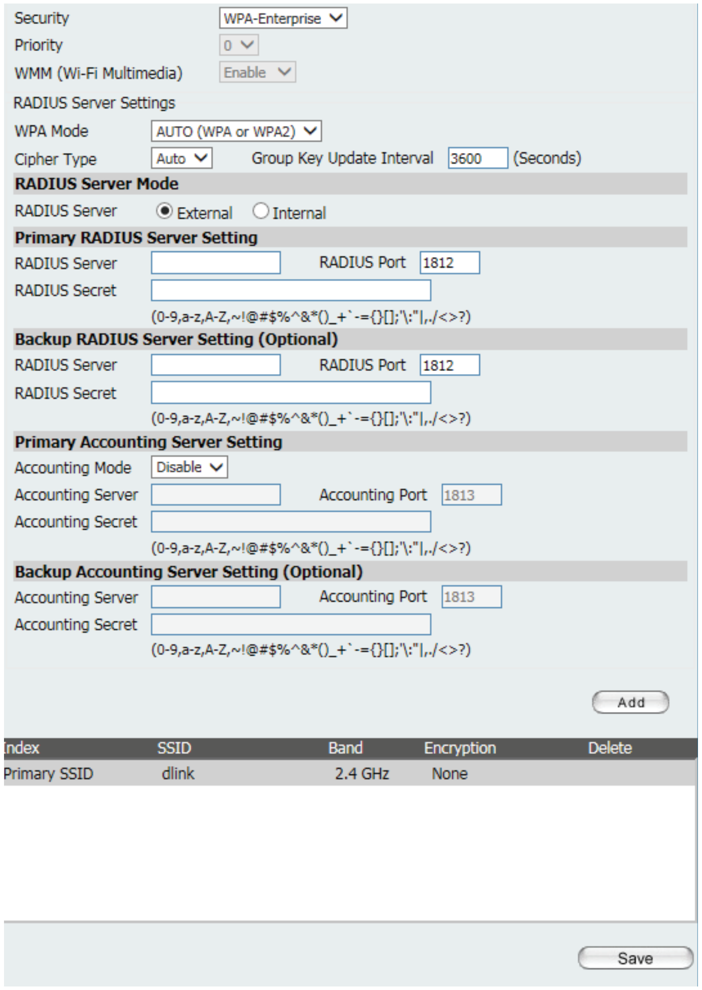
Group Key Update Interval: Select the interval during which the group key will be valid. The recommended value is **3600.** A lower interval may reduce data transfer rates.

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.



```
Security                    WPA-Enterprise
Priority                    0
WMM (Wi-Fi Multimedia)      Enable
RADIUS Server Settings
WPA Mode                    AUTO (WPA or WPA2)
Cipher Type                 Auto        Group Key Update Interval 3600 (Seconds)
RADIUS Server Mode
RADIUS Server               ● External  ○ Internal
Primary RADIUS Server Setting
RADIUS Server                           RADIUS Port 1812
RADIUS Secret
                            (0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)
Backup RADIUS Server Setting (Optional)
RADIUS Server                           RADIUS Port 1812
RADIUS Secret
                            (0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)
Primary Accounting Server Setting
Accounting Mode             Disable
Accounting Server                       Accounting Port 1813
Accounting Secret
                            (0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)
Backup Accounting Server Setting (Optional)
Accounting Server                       Accounting Port 1813
Accounting Secret
                            (0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)
```

Index	SSID	Band	Encryption	Delete
Primary SSID	dlink	2.4 GHz	None	

802.1x Authentication

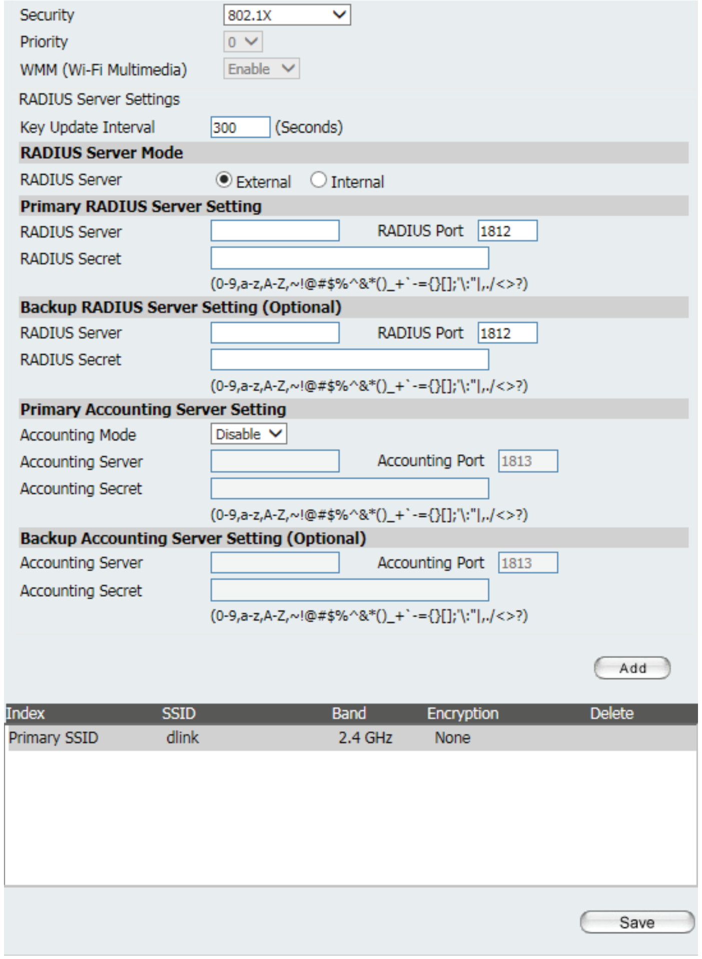
802.1x Authentication can only be enabled for **Access Point** mode.

Key Update Interval: Select the interval during which the group key will be valid (**300** is the recommended value). A lower interval may reduce data transfer rates.

RADIUS Server: Enter the IP address of the RADIUS server.

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the RADIUS secret.



Security: 802.1X

Priority: 0

WMM (Wi-Fi Multimedia): Enable

RADIUS Server Settings

Key Update Interval: 300 (Seconds)

RADIUS Server Mode

RADIUS Server: ● External ○ Internal

Primary RADIUS Server Setting

RADIUS Server: RADIUS Port: 1812

RADIUS Secret:

(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)

Backup RADIUS Server Setting (Optional)

RADIUS Server: RADIUS Port: 1812

RADIUS Secret:

(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)

Primary Accounting Server Setting

Accounting Mode: Disable

Accounting Server: Accounting Port: 1813

Accounting Secret:

(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)

Backup Accounting Server Setting (Optional)

Accounting Server: Accounting Port: 1813

Accounting Secret:

(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)

Index	SSID	Band	Encryption	Delete
Primary SSID	dlink	2.4 GHz	None	

LAN

LAN is short for Local Area Network. This is considered your internal network. These are the IP settings of the LAN interface for the DAP-2230. 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.

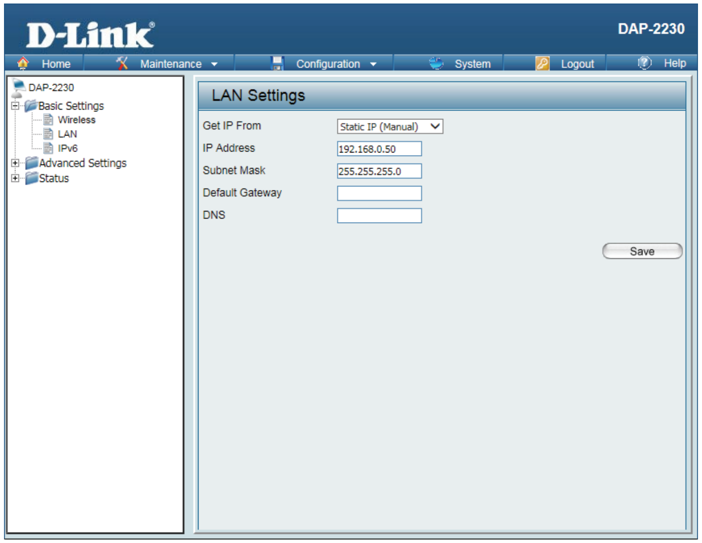
Get IP From: **Static IP (Manual)** is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2230. When **Dynamic IP (DHCP)** is selected, the other fields here will be grayed out. Please allow about two minutes for the DHCP client to be functional once this selection is made.

IP Address: The default IP address is 192.168.0.50. Assign a static IP address that is within the IP address range of your network.

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

Default Gateway: Enter the IP address of the gateway in your network. If there is a gateway in your network, please enter an IP address within the range of your network.

DNS: Enter the DNS IP address used here.



LAN Settings

Get IP From: Static IP (Manual)

IP Address: 192.168.0.50

Subnet Mask: 255.255.255.0

Default Gateway:

DNS:

IPv6

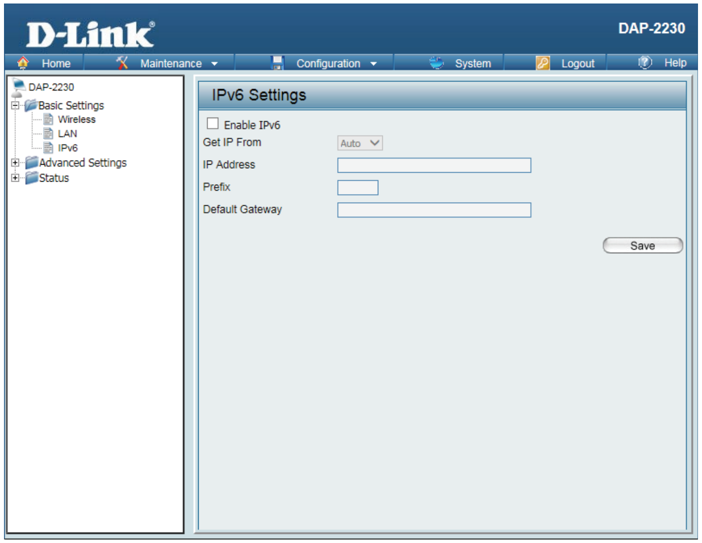
Enable IPv6: Check to enable the IPv6.

Get IP From: **Auto** is the default option. The DAP-2230 will get an 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.



IPv6 Settings

□ Enable IPv6

Get IP From: Auto

IP Address

Prefix

Default Gateway

Save

Advanced Settings

Performance

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

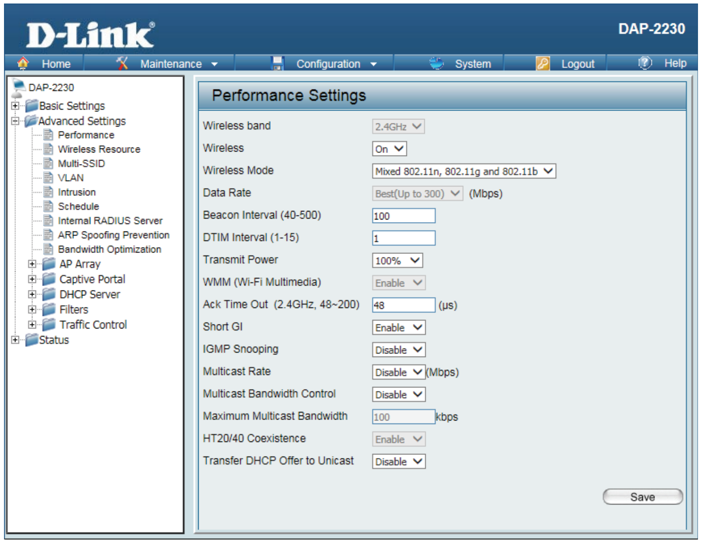
Wireless Mode: The different combination of clients that can be supported include **Mixed 802.11n, 802.11g and 802.11b**, **Mixed 802.11g and 802.11b** and **802.11n Only**. Please note that when backwards compatibility is enabled for legacy (802.11g/b) clients, degradation of 802.11n wireless performance is expected.

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

Beacon Interval (25-500): Beacons are packets sent by an access point to synchronize a wireless network. Specify a value in milliseconds. The default (**100**) is recommended. Setting a higher beacon interval can help to save the power of wireless clients, while setting a lower one can help a wireless client connect to an access point faster.

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

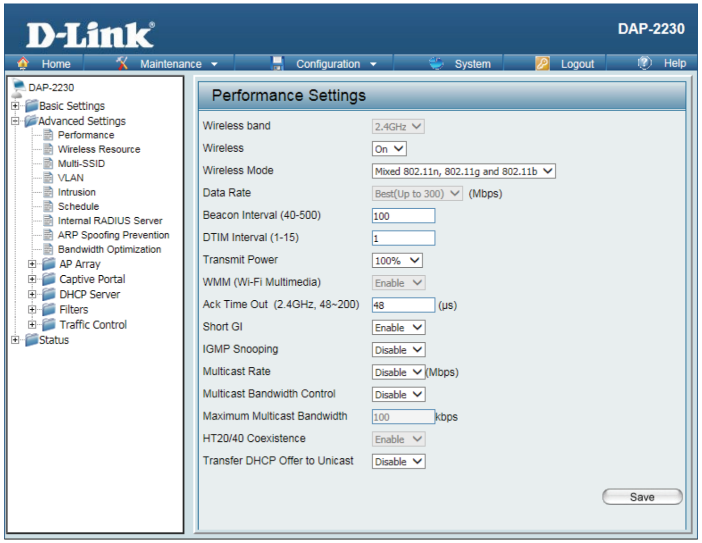
Transmit Power: This setting determines the power level of the wireless transmission. Transmitting power can be adjusted to eliminate overlapping of wireless area coverage between two access points where interference is a major concern. For example, if wireless coverage is intended for half of the area,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



Performance Settings

Wireless band	2.4GHz
Wireless	On
Wireless Mode	Mixed 802.11n, 802.11g and 802.11b
Data Rate	Best(Up to 300) (Mbps)
Beacon Interval (40-500)	100
DTIM Interval (1-15)	1
Transmit Power	100%
WMM (Wi-Fi Multimedia)	Enable
Ack Time Out (2.4GHz, 48~200)	48 (µs)
Short GI	Enable
IGMP Snooping	Disable
Multicast Rate	Disable (Mbps)
Multicast Bandwidth Control	Disable
Maximum Multicast Bandwidth	100 kbps
HT20/40 Coexistence	Enable
Transfer DHCP Offer to Unicast	Disable

*Maximum wireless signal rate derived from IEEE Standard 802.11n and 802.11g specifications. Actual data throughput may vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead can lower actual data throughout rate.



Performance Settings

Wireless band	2.4GHz
Wireless	On
Wireless Mode	Mixed 802.11n, 802.11g and 802.11b
Data Rate	Best(Up to 300) (Mbps)
Beacon Interval (40-500)	100
DTIM Interval (1-15)	1
Transmit Power	100%
WMM (Wi-Fi Multimedia)	Enable
Ack Time Out (2.4GHz, 48~200)	48 (µs)
Short GI	Enable
IGMP Snooping	Disable
Multicast Rate	Disable (Mbps)
Multicast Bandwidth Control	Disable
Maximum Multicast Bandwidth	100 kbps
HT20/40 Coexistence	Enable
Transfer DHCP Offer to Unicast	Disable

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

Ack Time Out (2.4 GHZ, 64~200): To effectively optimize throughput over long distance links, enter a value for Acknowledgement Time Out from **64** to **200** microseconds in the 2.4 GHz in the field provided.

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

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

Multicast Rate: Select the multicast rate for 2.4G band.

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.

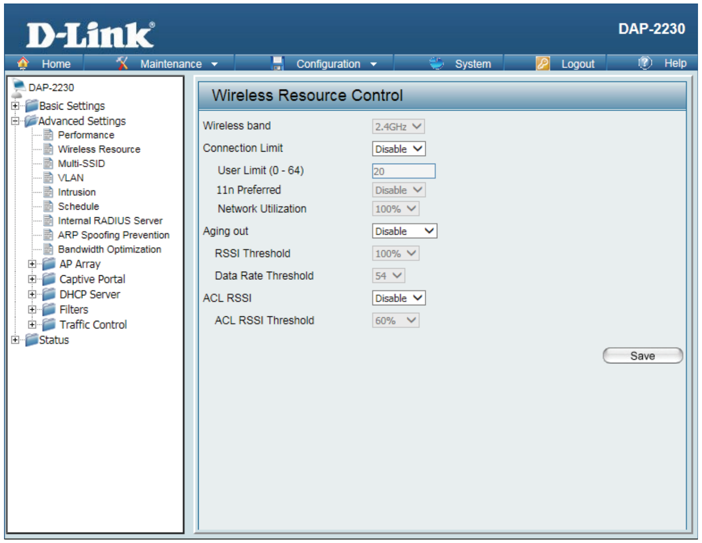
Maximum Multicast Bandwidth : Set the multicast packets maximum bandwidth pass through rate from the Ethernet interface to the Access Point.

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

Transfer DHCP Offer to Unicast : Enable to transfer the DHCP Offer to Unicast from LAN to WLAN, it is recommended to enable this function if the number of stations is larger than 30.

Wireless Resource Control

The Wireless Resource Control window is used to configure the wireless connection settings so that devices can detect and connect to the Access Point with the strongest signal.



Wireless Resource Control

Wireless band	2.4GHz
Connection Limit	Disable
User Limit (0 - 64)	20
11n Preferred	Disable
Network Utilization	100%
Aging out	Disable
RSSI Threshold	100%
Data Rate Threshold	54
ACL RSSI	Disable
ACL RSSI Threshold	60%

Wireless band: Select **2.4 Ghz**.

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-2230 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. The DAP-2230 will not allow any new clients to associate with the AP if the utilization exceeds the specified value. Select a utilization percentage between 100%, 80%, 60%, 40%, 20%, or 0%. When this network utilization threshold is reached, the device will pause for one minute to allow network congestion to dissipate.

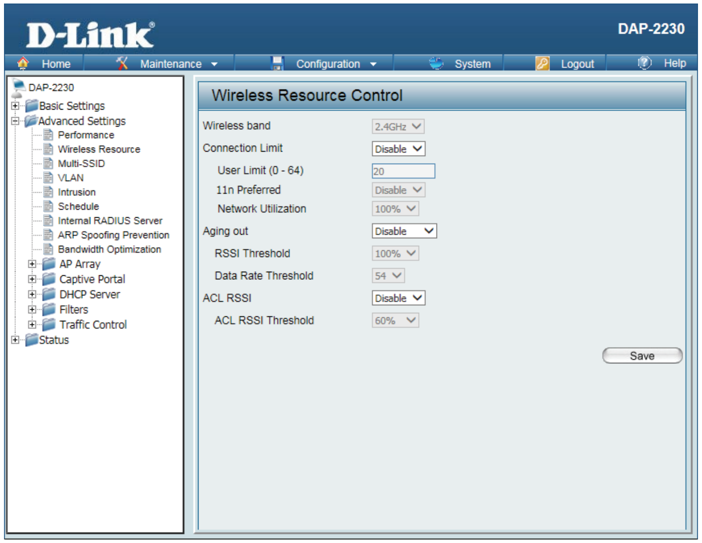
Aging out: Use the drop-down menu to select the criteria of disconnecting the wireless clients. Available options are **RSSI** and **Data Rate**.

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 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.

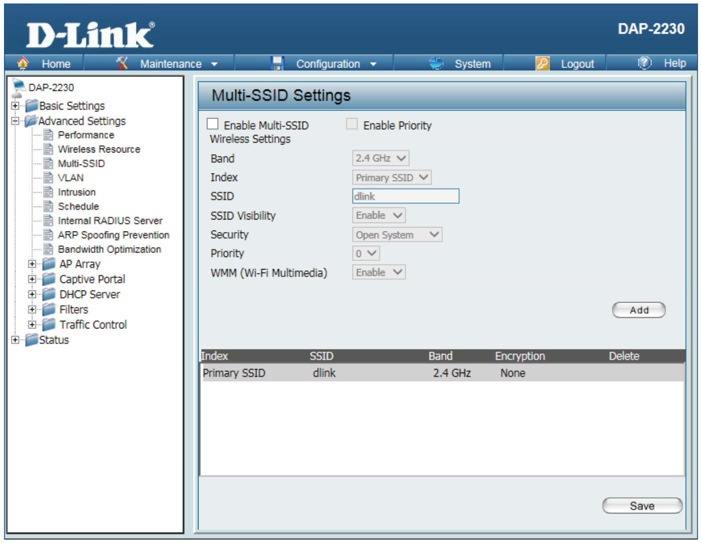


Wireless Resource Control

Wireless band	2.4GHz
Connection Limit	Disable
User Limit (0 - 64)	20
11n Preferred	Disable
Network Utilization	100%
Aging out	Disable
RSSI Threshold	100%
Data Rate Threshold	54
ACL RSSI	Disable
ACL RSSI Threshold	60%

Multi-SSID

The device supports up to four multiple Service Set Identifiers. In the **Basic** > **Wireless** section, you can set the Primary SSID. 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.



Multi-SSID Settings

☐ Enable Multi-SSID ☐ Enable Priority

Wireless Settings

Band: 2.4 GHz
Index: Primary SSID
SSID: dlink
SSID Visibility: Enable
Security: Open System
Priority: 0
WMM (Wi-Fi Multimedia): Enable

Index	SSID	Band	Encryption	Delete
Primary SSID	dlink	2.4 GHz	None	

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

Band: This read-only value is the current band setting.

Index: You can select up to three multi-SSIDs. With the Primary SSID, you have a total of four multi-SSIDs.

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**, **WPA-Enterprise, or 802.1x**. For a detailed description of the Open System parameters, please go to page 26. For a detailed description of the WPA-Personal parameters, please go to page 27. For a detailed description of the WPA-Enterprise parameters, please go to page 28. For a detailed description of the 802.1x parameters, please go to page 29.

Priority: Check the **Enable Priority** box at the top of this window to enable. Select the priority from the drop-down menu.

WMM (Wi-Fi Multimedia): Select **Enable** or **Disable**.

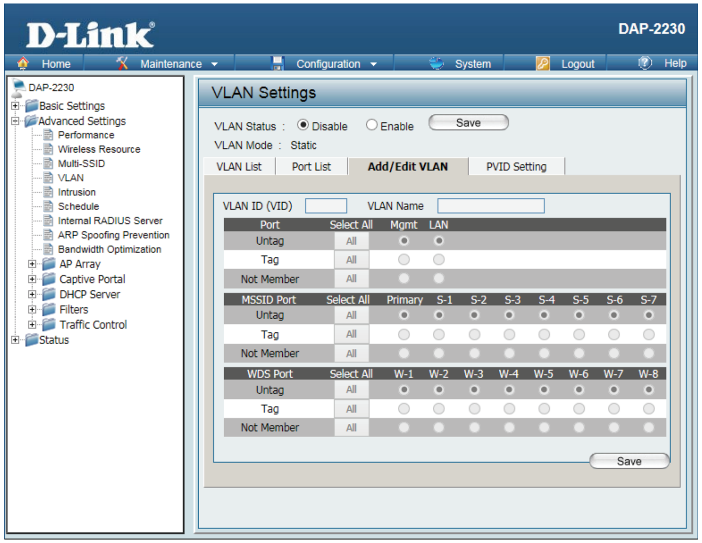
VLAN

VLAN List

The DAP-2230 supports VLANs. VLANs can be created with a Name and VID. Mgmt (TCP stack), LAN, Primary Multiple SSID, and WDS connection can be assigned to VLANs as they are physical ports. Any packet which enters the DAP-2230 without a VLAN tag will have a VLAN tag inserted with a PVID.

The VLAN List tab displays the current VLANs.

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



VLAN Settings

VLAN Status : ● Disable ○ Enable

VLAN Mode : Static

VLAN ID (VID) ▭ VLAN Name ▭

Port	Select All	Mgmt	LAN
Untag	All	●	●
Tag	All	○	○
Not Member	All	○	○

MSSID Port	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	●	●	●	●	●	●	●	●
Tag	All	○	○	○	○	○	○	○	○
Not Member	All	○	○	○	○	○	○	○	○

WDS Port	Select All	W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
Untag	All	●	●	●	●	●	●	●	●
Tag	All	○	○	○	○	○	○	○	○
Not Member	All	○	○	○	○	○	○	○	○

Port List

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

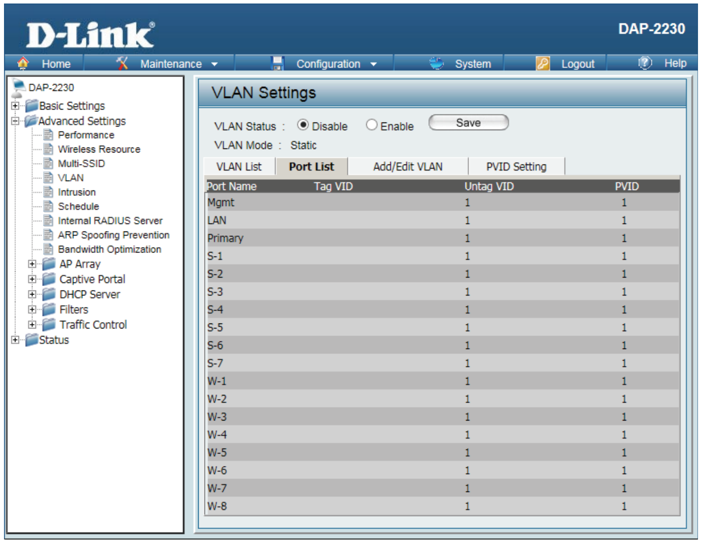
VLAN Status: Use the radio button to toggle to Enable. Next, go to the **Add/Edit VLAN** tab to add or modify an item on the **VLAN List** tab.

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

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

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

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



VLAN Settings

VLAN Status : ● Disable ○ Enable

VLAN Mode : Static

Port Name	Tag VID	Untag VID	PVID
Mgmt		1	1
LAN		1	1
Primary		1	1
S-1		1	1
S-2		1	1
S-3		1	1
S-4		1	1
S-5		1	1
S-6		1	1
S-7		1	1
W-1		1	1
W-2		1	1
W-3		1	1
W-4		1	1
W-5		1	1
W-6		1	1
W-7		1	1
W-8		1	1

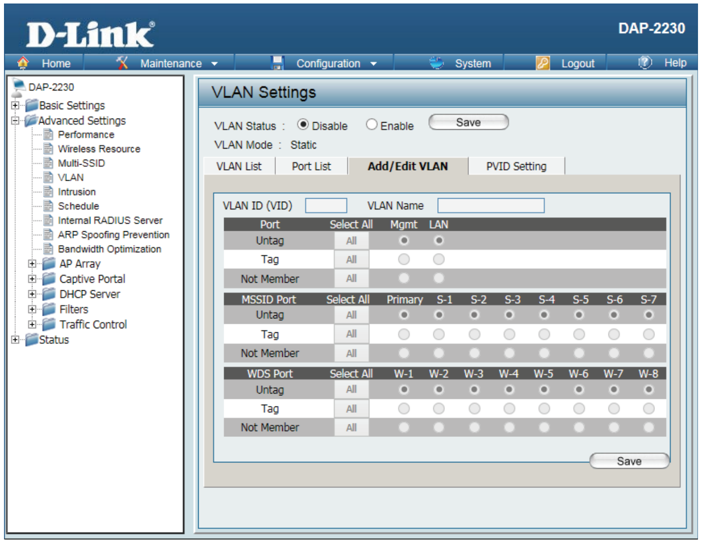
Add/Edit VLAN

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

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

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

VLAN Name: Enter the VLAN to add or modify.



VLAN Settings

VLAN Status : ● Disable ○ Enable

VLAN Mode : Static

VLAN ID (VID) ____ VLAN Name ____

Port	Select All	Mgmt	LAN
Untag	All	●	●
Tag	All	○	○
Not Member	All	○	○

MSSID Port	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	●	●	●	●	●	●	●	●
Tag	All	○	○	○	○	○	○	○	○
Not Member	All	○	○	○	○	○	○	○	○

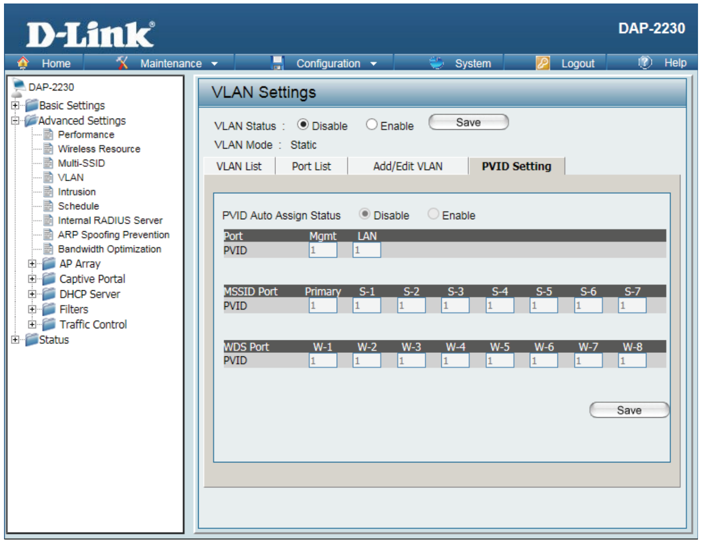
WDS Port	Select All	W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
Untag	All	●	●	●	●	●	●	●	●
Tag	All	○	○	○	○	○	○	○	○
Not Member	All	○	○	○	○	○	○	○	○

PVID Setting

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

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

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



VLAN Settings

VLAN Status : ● Disable ○ Enable

VLAN Mode : Static

PVID Auto Assign Status ● Disable ○ Enable

Port	Mgmt	LAN
PVID	1	1

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

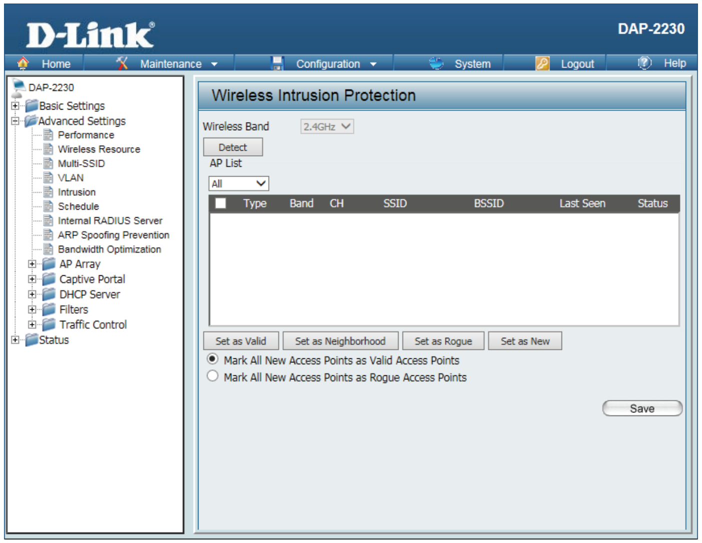
WDS Port	W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
PVID	1	1	1	1	1	1	1	1

Intrusion

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

AP List: The choices include **All**, **Valid**, **Neighbor**, **Rogue**, and **New**.

Detect: Click this button to initiate a scan of the network.



Wireless Intrusion Protection

Wireless Band: 2.4GHz

AP List: All

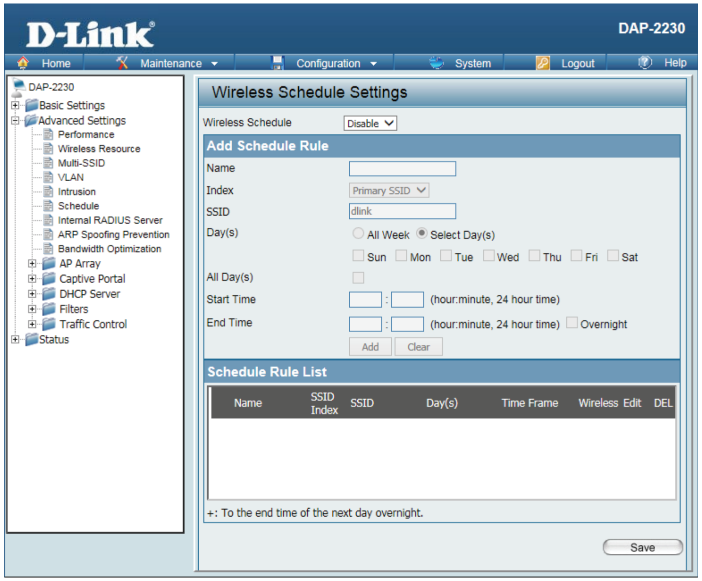
□	Type	Band	CH	SSID	BSSID	Last Seen	Status

● Mark All New Access Points as Valid Access Points

○ Mark All New Access Points as Rogue Access Points

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 Settings

Wireless Schedule: Disable

Add Schedule Rule

Name:

Index: Primary SSID

SSID: dlink

Day(s): ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

All Day(s): □

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

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

Schedule Rule List

Name	SSID Index	SSID	Day(s)	Time Frame	Wireless	Edit	DEL

+: To the end time of the next day overnight.

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: Select the SSID the schedule will apply to from the drop-down menu.

SSID: Enter the name of your wireless network (SSID).

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 to apply the rule to.

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

Start Time: Enter the start time for your rule. If you selected **All Day**, this option will be greyed out.

End Time: Enter the end time for your rule.

Add: Click to add the rule to the list.

Schedule Rule List: This section will display the list of created schedules.

Save: Click the **Save** button to save your created rules.

Internal RADIUS Server

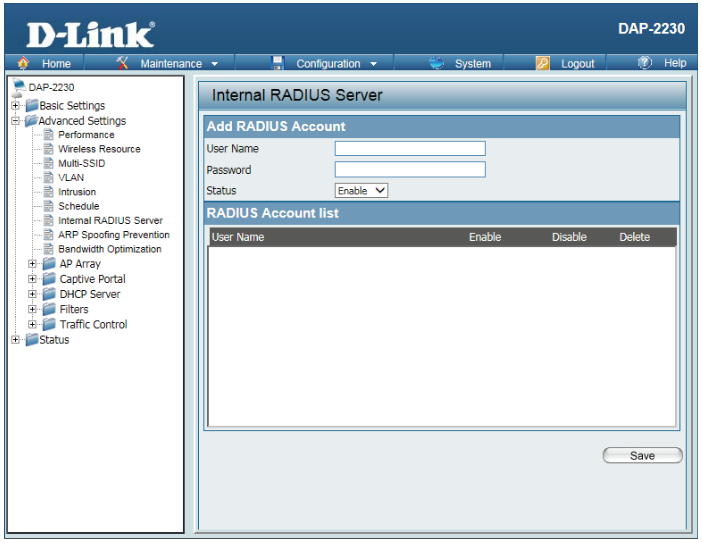
The DAP-2230 features a built-in RADIUS server. Once you have finished adding a RADIUS account, click the **Save** button to have your changes take effect. The newly-created account will appear in this RADIUS Account List. The radio buttons allow the user to enable or disable the RADIUS account. Click the icon in the delete column to remove the RADIUS account. We suggest you limit the number of accounts to under 30.

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

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

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

RADIUS Account List: Displays the list of users.



Internal RADIUS Server

Add RADIUS Account

User Name

Password

Status: Enable

RADIUS Account list

User Name	Enable	Disable	Delete

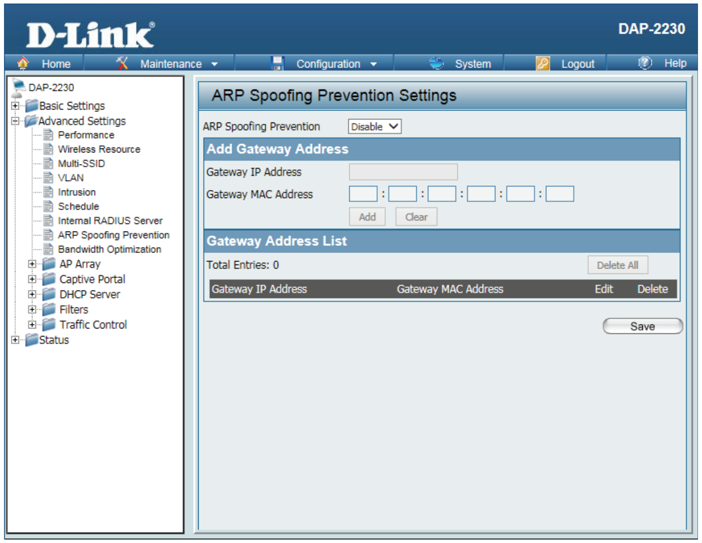
ARP Spoofing Prevention Settings

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.



ARP Spoofing Prevention Settings

ARP Spoofing Prevention: Disable

Add Gateway Address

Gateway IP Address

Gateway MAC Address : : : : :

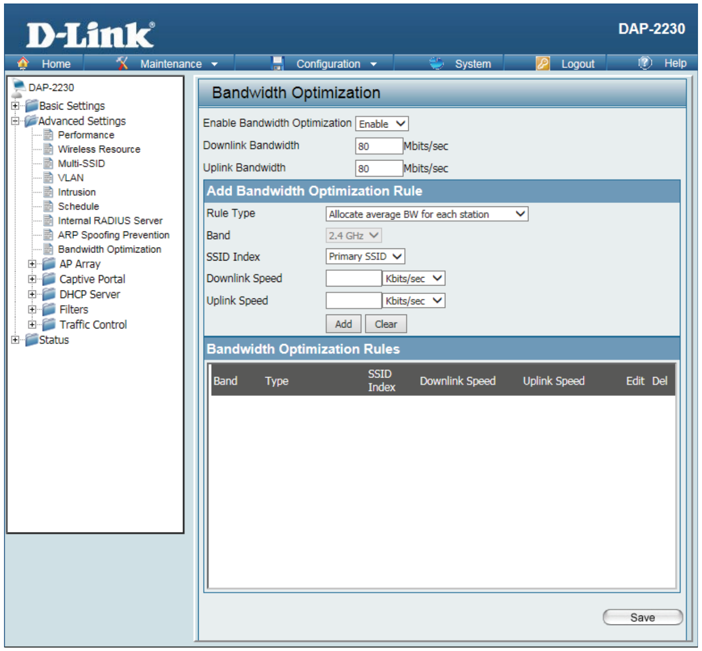
Gateway Address List

Total Entries: 0

Gateway IP Address	Gateway MAC Address	Edit	Delete

Bandwidth Optimization

The Bandwidth Optimization window allows the user to manage the bandwidth of the access point and adjust the bandwidth for various wireless clients. After inputting a Bandwidth Optimization rule, click the **Add** button. To discard a Bandwidth Optimization Rule setting, click the **Clear** button. Click the **Save** button to let your changes take effect.



Bandwidth Optimization

Enable Bandwidth Optimization: Enable

Downlink Bandwidth: 80 Mbits/sec

Uplink Bandwidth: 80 Mbits/sec

Add Bandwidth Optimization Rule

Rule Type: Allocate average BW for each station

Band: 2.4 GHz

SSID Index: Primary SSID

Downlink Speed: Kbits/sec

Uplink Speed: Kbits/sec

Bandwidth Optimization Rules

Band	Type	SSID Index	Downlink Speed	Uplink Speed	Edit	Del

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 11b/g/n stations**, and **Allocte specific BW for SSID**.

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

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

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

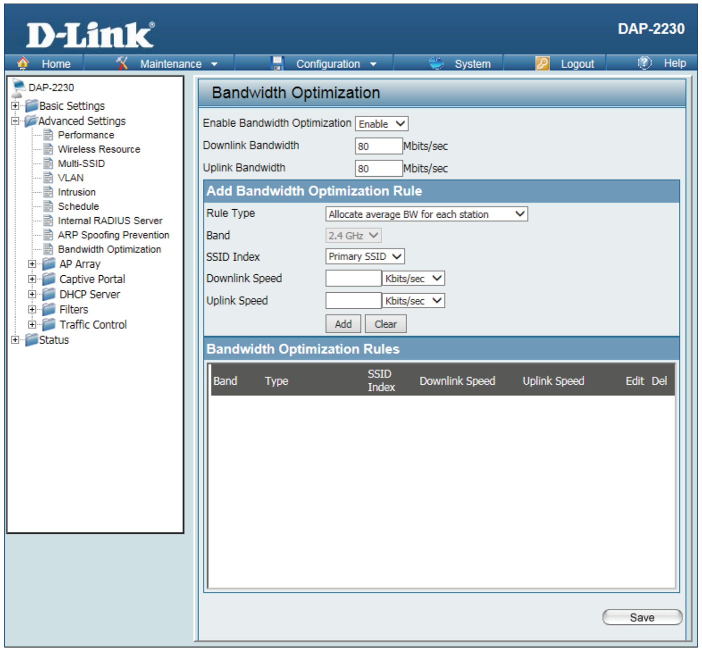
Allocate specific BW for SSID: All clients share the total bandwidth.

Band: Use the drop-down menu to toggle the wireless band 2.4 Ghz.

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

Downlink Speed: Enter the downlink speed limit in either Kbits/sec or Mbits/sec for the rule.

Uplink Speed: Enter the upload speed limit in either Kbits/sec or Mbits/sec for the rule.



Bandwidth Optimization

Enable Bandwidth Optimization: Enable

Downlink Bandwidth: 80 Mbits/sec

Uplink Bandwidth: 80 Mbits/sec

Add Bandwidth Optimization Rule

Rule Type: Allocate average BW for each station

Band: 2.4 GHz

SSID Index: Primary SSID

Downlink Speed: Kbits/sec

Uplink Speed: Kbits/sec

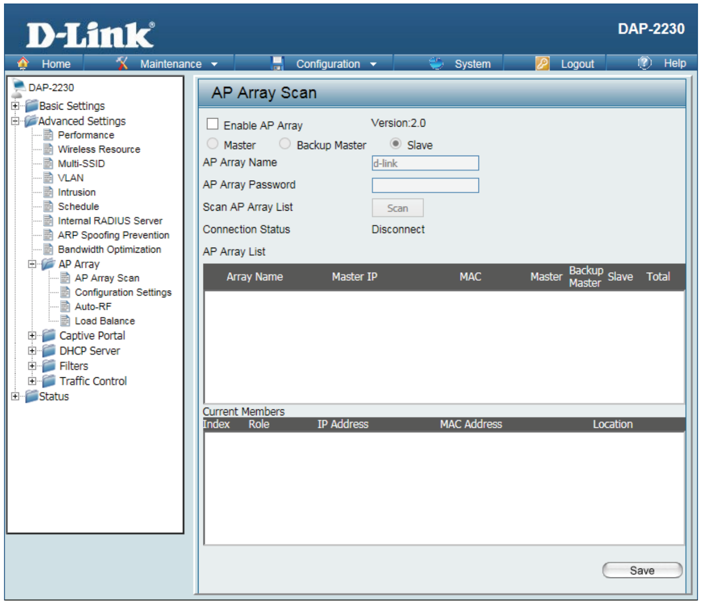
Bandwidth Optimization Rules

Band	Type	SSID Index	Downlink Speed	Uplink Speed	Edit	Del

AP Array

AP Array Scan

The AP Array window is used to create up to 32 APs on a local network to be organized into a single group in order to simplify management. Click the **Save** button to let your changes take effect. Central WiFiManager and AP Array are mutually exclusive functions.



AP Array Scan

□ Enable AP Array Version:2.0

○ Master ○ Backup Master ● Slave

AP Array Name: d-link

AP Array Password:

Scan AP Array List: Scan

Connection Status: Disconnect

AP Array List

Array Name	Master IP	MAC	Master	Backup Master	Slave	Total

Current Members

Index	Role	IP Address	MAC Address	Location

Enable AP Array: Select the check box to enable the AP array function. The three modes that are available are Master, Backup Master, and Slave. APs in the same array will use the same configuration. The configuration will sync the Master AP to the Slave AP and the Backup Master AP when a Slave AP and a Backup Master AP join the AP array.

AP Array Name: Enter an AP array name for the group here.

AP Array Password: Enter an AP array password for the group here. This password must be the same on all the APs in the group.

Scan AP Array List: Click this button to initiate a scan of all the available APs currently on the network.

Connection Status: Display the AP array connection status.

AP Array List: This table displays the current AP array status for the following parameters: Array Name, Master IP, MAC, Master, Backup Master, Slave, and Total.

Current Members: This table displays all the current array members. The DAP-2230 AP array feature supports up to eight AP array members.

Configuration Settings

In the AP array configuration settings windows, users can specify which settings all the APs in the group will inherit from the master AP. Make the desired selections in this window and click the **Save** button to accept the changes.

Enable AP Array Configuration: Select to Enable or Disable the AP array configure feature here.

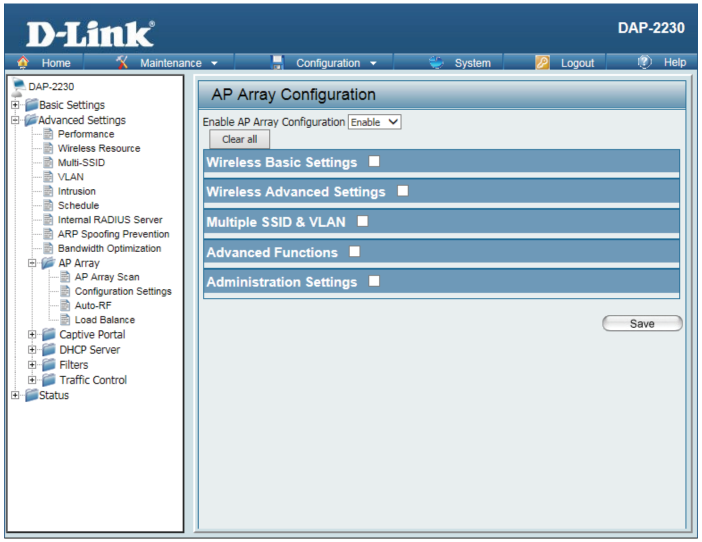
Wireless Basic Settings: Select this option to specify the basic wireless settings that the APs in the group will inherit.

Wireless Advanced Settings: Select this option to specify the advanced wireless settings that the APs in the group will inherit.

Multiple SSID & VLAN: Select this option to specify the multiple SSIDs and VLAN settings that the APs in the group will inherit.

Advanced Functions: Select this option to specify the other advanced settings that the APs in the group will inherit.

Administration Settings: Select this option to specify the administrative settings that the APs in the group will inherit.



AP Array Configuration

Enable AP Array Configuration: Enable

Clear all

Wireless Basic Settings ☐

Wireless Advanced Settings ☐

Multiple SSID & VLAN ☐

Advanced Functions ☐

Administration Settings ☐

Save

Auto-RF

In this window, users can view and configure the automatic radio frequency settings as well as configure the auto-initiate period and threshold values. Click the **Save** button to accept the changes made.

Enable: Auto-RF: Select to Enable or Disable the auto-RF feature here.

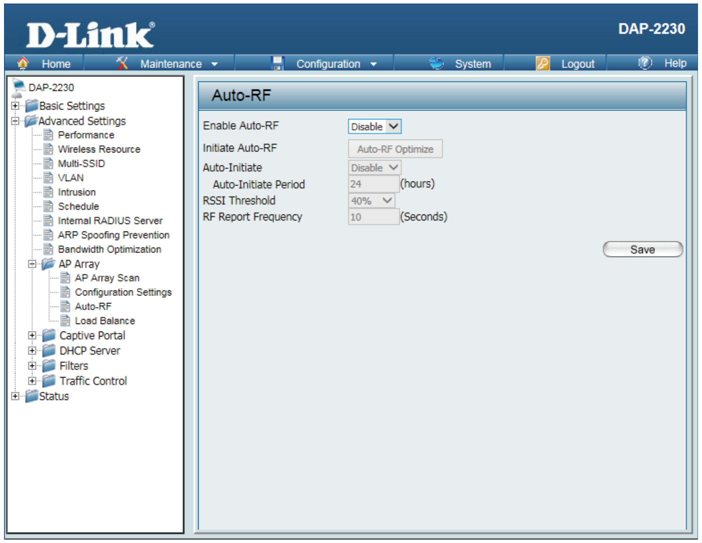
Initiate Auto-RF: Click the Auto-RF Optimize button to initiate the auto-RF optimization feature.

Auto-Initiate: Select the Enable or Disable the auto-initiate feature here.

Auto-Initiate Period: After enabling the auto-initiate option, the auto-initiate period value can be entered here. This value must be between 1 and 24 hours.

RSSI Threshold: Select the RSSI threshold value here. This value is listed in the drop-down menu in increments of 10% from 10% to 100%.

RF Report Frequency: Enter the RF report frequency value here.



Auto-RF

Enable Auto-RF: Disable

Initiate Auto-RF

Auto-Initiate: Disable

Auto-Initiate Period: 24 (hours)

RSSI Threshold: 40%

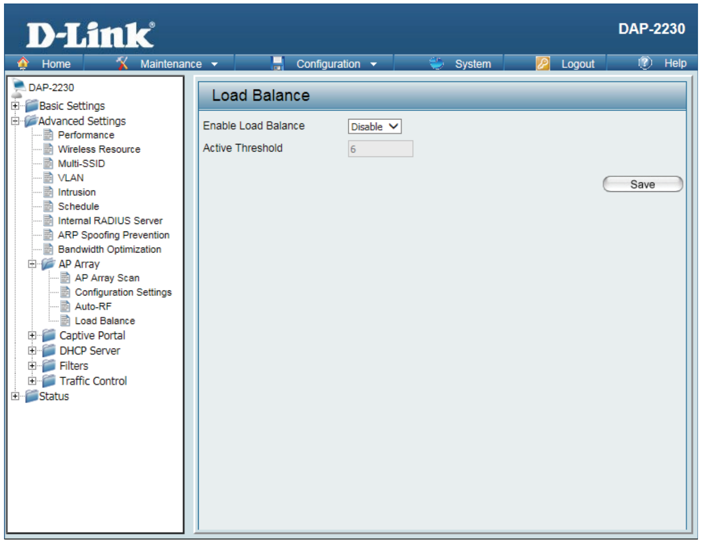
RF Report Frequency: 10 (Seconds)

Load Balance

In this window, users can view and configure the AP array's load balancing settings. Click the **Save** button to accept the changes made.

Enable Load Balance: Select to Enable or Disable the load balance feature here.

Active Threshold: Enter the active threshold value here.



Load Balance

Enable Load Balance: Disable

Active Threshold: 6

Captive Portal Authentication

Captive Portal is a built-in web authentication server. When a client connects to an AP, the user's web browser will be redirected to a web authentication page. In this configuration option, administrators can view and configure the Captive Portal settings.

Web Redirection Only

After selecting **Web Redirection Only** as the Authentication Type, you can configure the redirection website URL that will be applied to each wireless client that connects to 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.

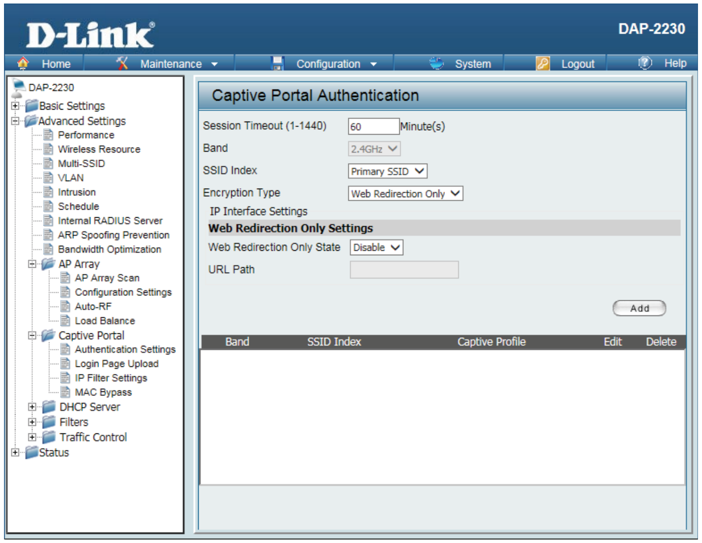
Band: Select 2.4 Ghz.

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.**

Web Redirection State: Web Redirection State is automatically enabled when **Web Redirection** Authentication is selected.

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.



Captive Portal Authentication

Session Timeout (1-1440): 60 Minute(s)

Band: 2.4GHz

SSID Index: Primary SSID

Encryption Type: Web Redirection Only

IP Interface Settings

Web Redirection Only Settings

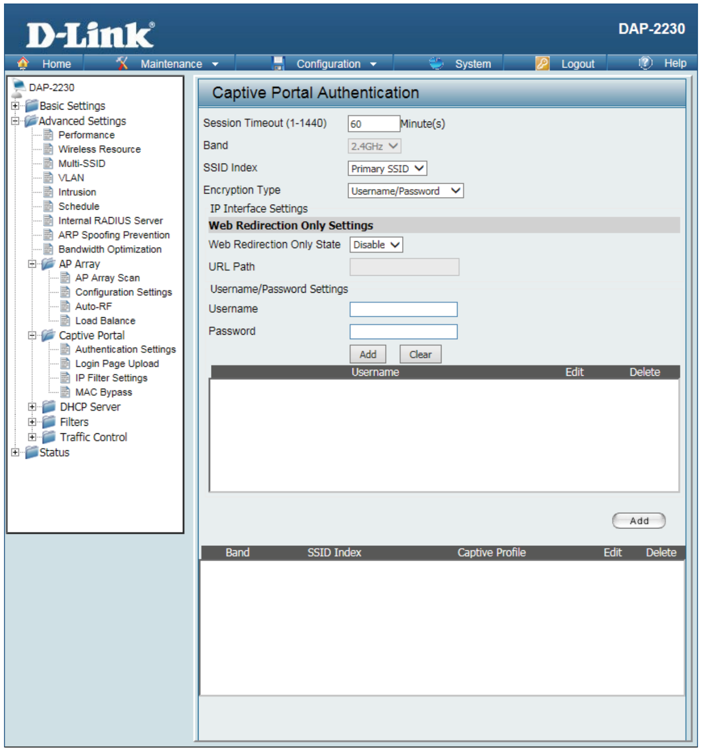
Web Redirection Only State: Disable

URL Path:

Band	SSID Index	Captive Profile	Edit	Delete

Username/Password

After selecting **Username/Password** as the Authentication Type, administrators can configure the Username and Password that each wireless client will be prompted for when requesting access to the network.



Captive Portal Authentication

Session Timeout (1-1440): 60 Minute(s)

Band: 2.4GHz

SSID Index: Primary SSID

Encryption Type: Username/Password

IP Interface Settings

Web Redirection Only Settings

Web Redirection Only State: Disable

URL Path

Username/Password Settings

Username

Password

Username	Edit	Delete

Band	SSID Index	Captive Profile	Edit	Delete

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 2.4 Ghz.

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**.

Web Redirection State: By default web redirection is disabled. Select enable to activate the website redirection feature.

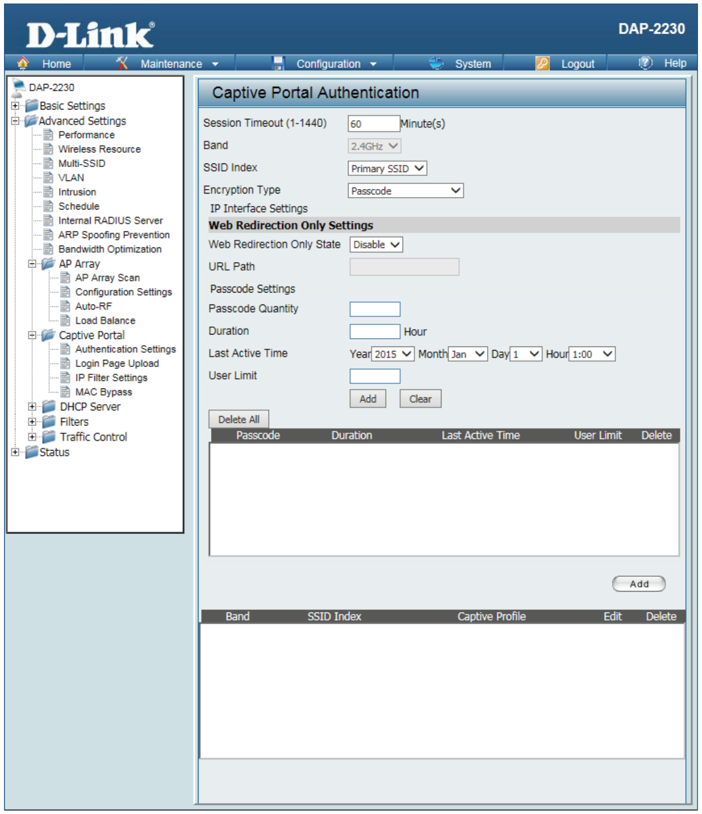
URL Path : Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.

Username: Enter the username for the new account here.

Password: Enter the password for the new account here.

Passcode

After selecting **Passcode** as the Authentication Type, administrators can configure the Passcode that each wireless client will be prompted for when requesting access to the network. A passcode will be randomly generated upon clicking **Add**.



Captive Portal Authentication

Session Timeout (1-1440): 60 Minute(s)
Band: 2.4GHz
SSID Index: Primary SSID
Encryption Type: Passcode

IP Interface Settings

Web Redirection Only Settings

Web Redirection Only State: Disable
URL Path:

Passcode Settings

Passcode Quantity:
Duration: Hour
Last Active Time: Year 2015 Month Jan Day 1 Hour 1:00
User Limit:

Passcode	Duration	Last Active Time	User Limit	Delete

Band	SSID Index	Captive Profile	Edit	Delete

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 2.4 Ghz.

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.**

Web Redirection State: By default web redirection is disabled. Select enable to activate 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.

Passcode Quantity: Enter the number of passcodes to generate.

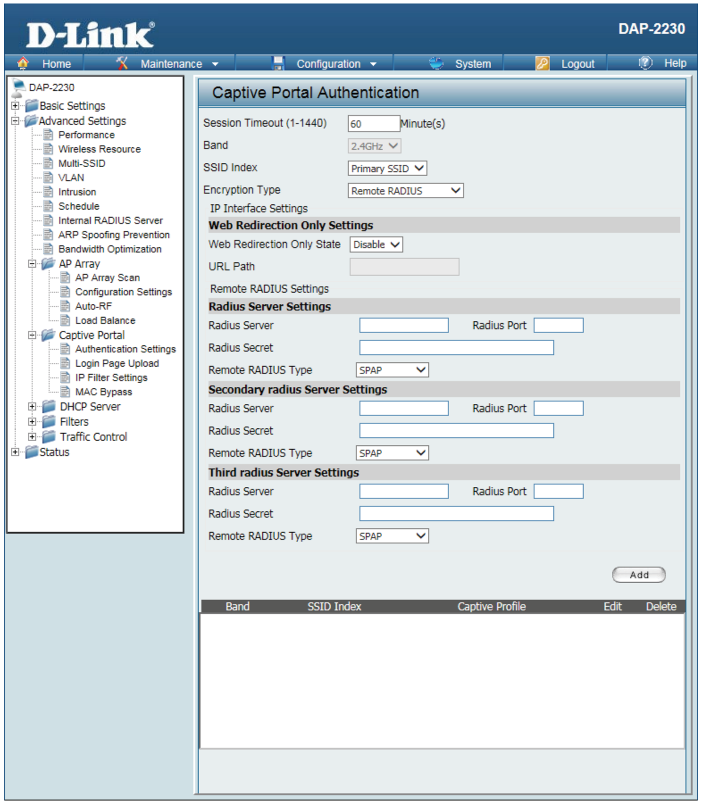
Duration: Enter the duration value, in hours, for the passcode(s).

Last Active Day: Select the year, month, day, and hour when this passcode will expire.

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

Remote Radius

After selecting **Remote RADIUS** as the Authentication Type, administrators can configure the Remote RADIUS authentication settings required to join the network.



Captive Portal Authentication

Session Timeout (1-1440): 60 Minute(s)
Band: 2.4GHz
SSID Index: Primary SSID
Encryption Type: Remote RADIUS
IP Interface Settings

Web Redirection Only Settings
Web Redirection Only State: Disable
URL Path:

Remote RADIUS Settings

Radius Server Settings
Radius Server: Radius Port:
Radius Secret:
Remote RADIUS Type: SPAP

Secondary radius Server Settings
Radius Server: Radius Port:
Radius Secret:
Remote RADIUS Type: SPAP

Third radius Server Settings
Radius Server: Radius Port:
Radius Secret:
Remote RADIUS Type: SPAP

Band	SSID Index	Captive Profile	Edit	Delete

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 2.4 Ghz.

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**.

Web Redirection State: By default web redirection is disabled. Select enable to activate 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.

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

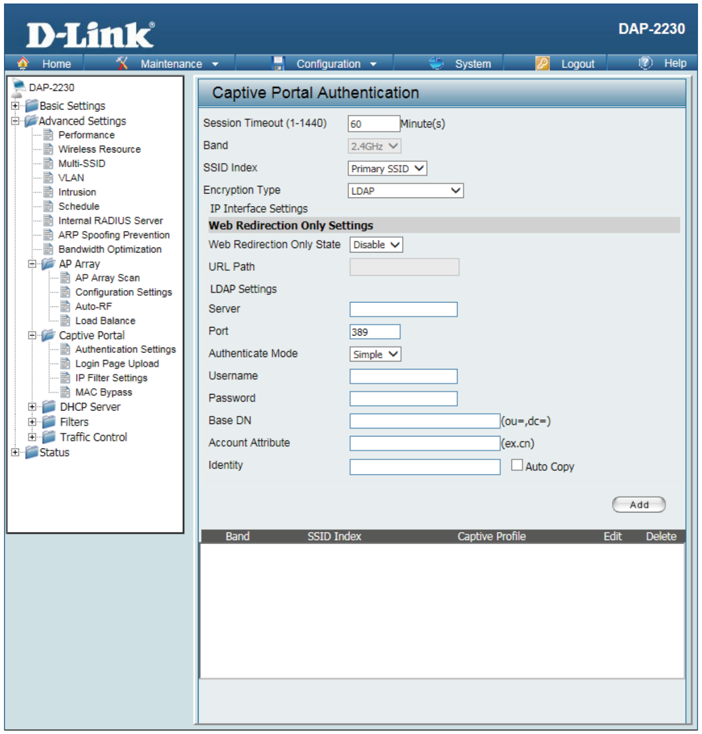
Radius Port: Enter the RADIUS server's port number here

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

Remote Radius Type: Select the remote RADIUS server type here.

LDAP

After selecting **LDAP** as the Authentication Type, administrators can configure the LDAP authentication settings required to join the network.



Captive Portal Authentication

Session Timeout (1-1440)	60 Minute(s)
Band	2.4GHz
SSID Index	Primary SSID
Encryption Type	LDAP
IP Interface Settings	
Web Redirection Only Settings	
Web Redirection Only State	Disable
URL Path	
LDAP Settings	
Server	
Port	389
Authenticate Mode	Simple
Username	
Password	
Base DN	(ou=,dc=)
Account Attribute	(ex.cn)
Identity	□ Auto Copy

Band	SSID Index	Captive Profile	Edit	Delete

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 2.4 Ghz.

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**.

Web Redirection State: By default web redirection is disabled. Select enable to activate 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.

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.

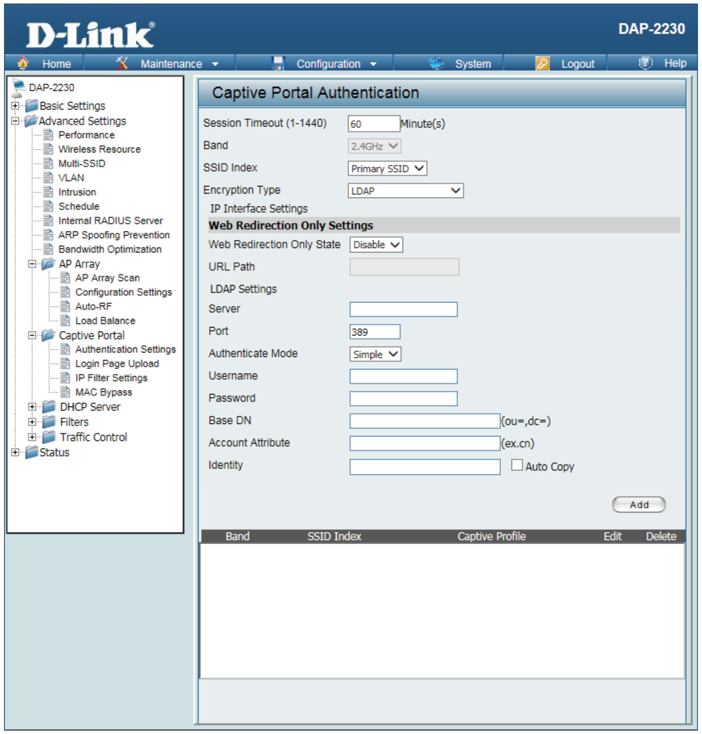
Password: Enter the LDAP server account's password here.

Base DN: Enter the administrator's domain name here

Account Attribute: Enter the LDAP account attribute string here.

Identity: This string will be used to search for clients.

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.



Captive Portal Authentication

Session Timeout (1-1440)	60 Minute(s)
Band	2.4GHz
SSID Index	Primary SSID
Encryption Type	LDAP

IP Interface Settings

Web Redirection Only Settings

Web Redirection Only State	Disable
URL Path	

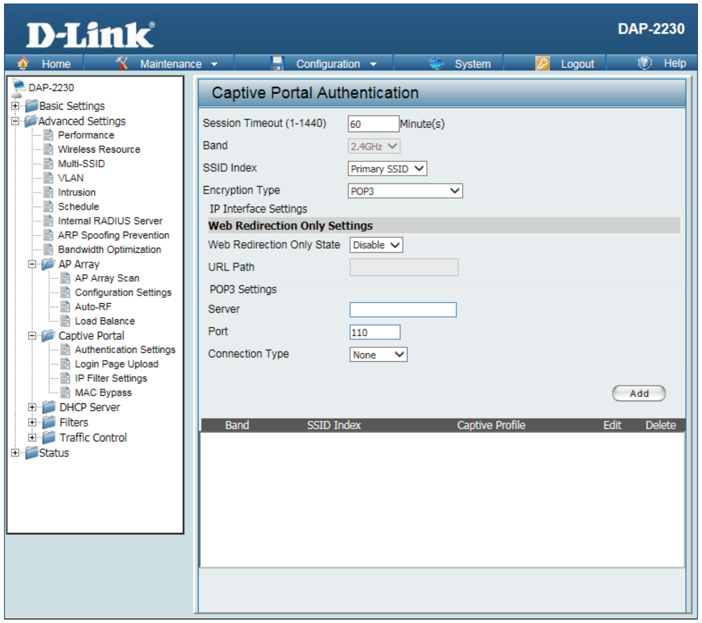
LDAP Settings

Server	
Port	389
Authenticate Mode	Simple
Username	
Password	
Base DN	(ou=,dc=)
Account Attribute	(ex.cn)
Identity	□ Auto Copy

Band	SSID Index	Captive Profile	Edit	Delete

POP3

After selecting **POP3** as the Authentication Type, administrators can configure the POP3 authentication settings required to join the network.



Captive Portal Authentication

Session Timeout (1-1440): 60 Minute(s)
Band: 2.4GHz
SSID Index: Primary SSID
Encryption Type: POP3
IP Interface Settings

Web Redirection Only Settings
Web Redirection Only State: Disable
URL Path:

POP3 Settings
Server:
Port: 110
Connection Type: None

Band	SSID Index	Captive Profile	Edit	Delete

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 2.4 Ghz.

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**.

Web Redirection State: By default web redirection is disabled. Select enable to activate 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.

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

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

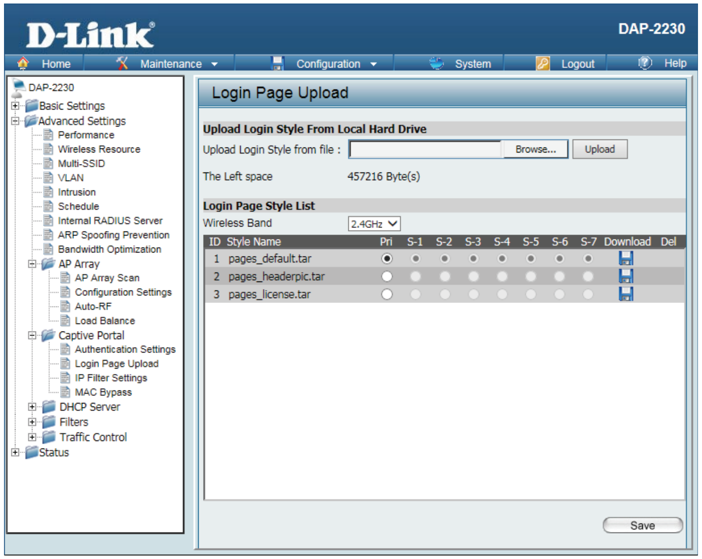
Connection Type: Select the connection type here; either None or SSL/TLS.

Login Page Upload

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

Upload picture from file: In this field the path to the image 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 for each SSID. Click the Download button to download the login page template file and Click the Del button to delete the template file.



Login Page Upload

Upload Login Style From Local Hard Drive

Upload Login Style from file : [ ] Browse... Upload

The Left space 457216 Byte(s)

Login Page Style List

Wireless Band 2.4GHz

ID	Style Name	Pri	S-1	S-2	S-3	S-4	S-5	S-6	S-7	Download	Del
1	pages_default.tar	●	●	●	●	●	●	●	●	💾	
2	pages_headerpic.tar	○	○	○	○	○	○	○	○	💾	
3	pages_license.tar	○	○	○	○	○	○	○	○	💾	

IP Filter

Enter the IP address or network address that will be used in the IP filter rule. For 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 on this network.

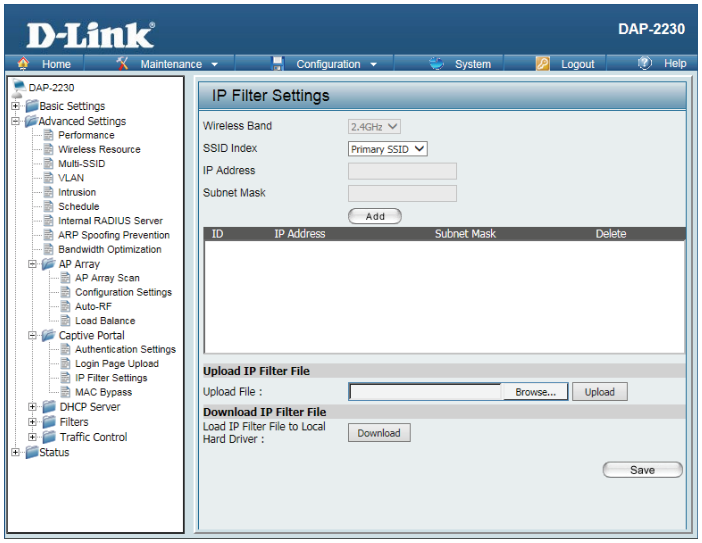
Wireless Band: Select the wireless band for MAC Bypass.

IP Address: Enter the IP address or network address.

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

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

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



IP Filter Settings

Wireless Band: 2.4GHz

SSID Index: Primary SSID

IP Address:

Subnet Mask:

ID	IP Address	Subnet Mask	Delete

Upload IP Filter File

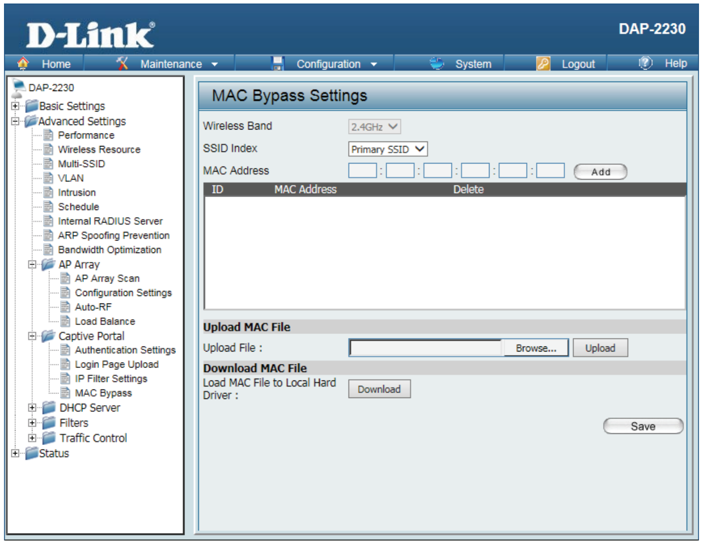
Upload File :

Download IP Filter File

Load IP Filter File to Local Hard Driver :

MAC Bypass

The DAP-2230 features a wireless MAC Bypass. Once a MAC address is added to the bypass list, that client will skip the Captive Portal Authentication process when joining a network. Once an administrator is finished adjusting these settings, click the **Save** button to have the changes take effect.



MAC Bypass Settings

Wireless Band: 2.4GHz

SSID Index: Primary SSID

MAC Address: __ : __ : __ : __ : __ : __

ID	MAC Address	Delete

Upload MAC File

Upload File :

Download MAC File

Load MAC File to Local Hard Driver :

Wireless Band: Select the wireless band for MAC Bypass.

SSID Index: Select the SSID for MAC Bypass.

MAC Address: Enter each MAC address that you wish to include in your bypass list and then 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 managing computer, and then click Upload.

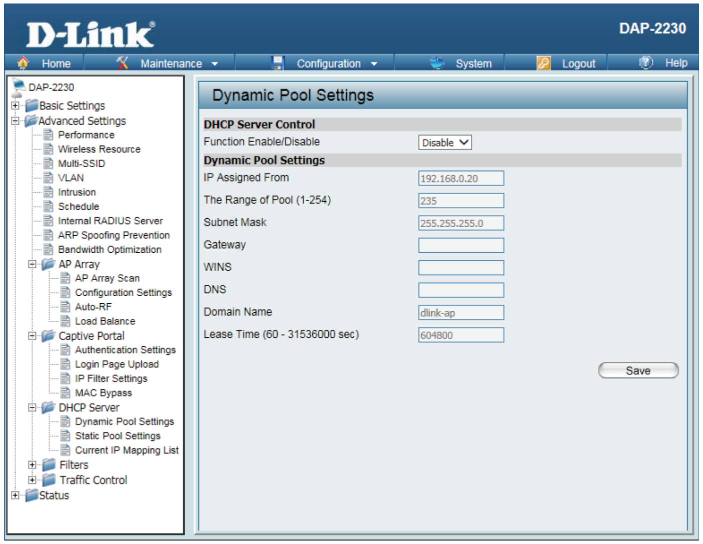
Load MAC File to Local Hard Drive: Click **Download** to save the MAC bypass list file.

DHCP Server

Dynamic Pool Settings

The DHCP address pool defines the range of the IP addresses that can be assigned to stations on the network. A Dynamic Pool allows wireless stations to receive an available IP with lease time control. If needed or required for the network, the DAP-2230 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-2230 to function as a DHCP server.



Dynamic Pool Settings

DHCP Server Control

Function Enable/Disable	Disable

Dynamic Pool Settings

IP Assigned From	192.168.0.20
The Range of Pool (1-254)	235
Subnet Mask	255.255.255.0
Gateway	
WINS	
DNS	
Domain Name	dlink-ap
Lease Time (60 - 31536000 sec)	604800

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 submask for the network here.

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

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

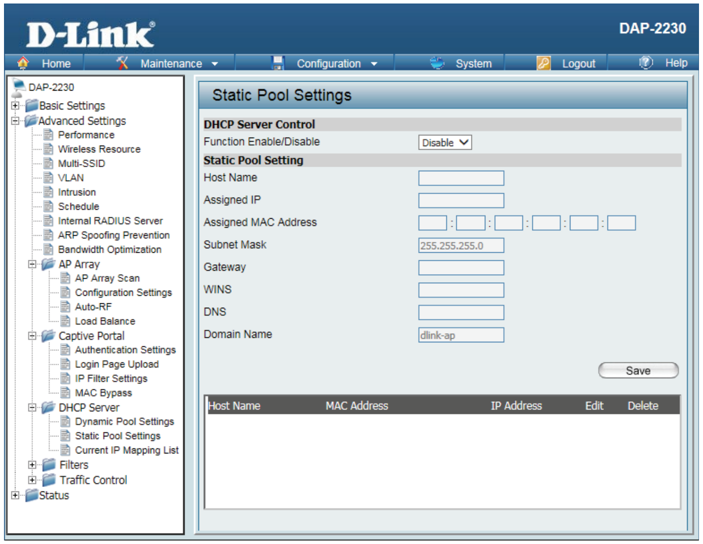
DNS: Enter the IP address of the Domain Name System (DNS) server. The DNS server translates domain names such as **www.dlink.com** into IP addresses.

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

Lease Time : The lease time is the period of time before the DHCP server will assign new IP addresses. (60-31536000 sec)

Static Pool Setting

A static pool allows specific IP addresses to be reserved to wireless stations.



Static Pool Settings

DHCP Server Control

Function Enable/Disable: Disable

Static Pool Setting

Host Name:

Assigned IP:

Assigned MAC Address: __ : __ : __ : __ : __ : __

Subnet Mask: 255.255.255.0

Gateway:

WINS:

DNS:

Domain Name: dlink-ap

Host Name	MAC Address	IP Address	Edit	Delete

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-2230 to function as a DHCP server.

Assigned IP: Use the Static Pool Settings to reserve IP addresses to specific devices. 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 **Save**; the device will appear in the Assigned Static Pool at the bottom of the screen. You can edit or delete the device in this list.

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

Subnet Mask: Define the submask of the IP address specified in the **IP Assigned From** field.

Gateway: Specify the Gateway address for the wireless network.

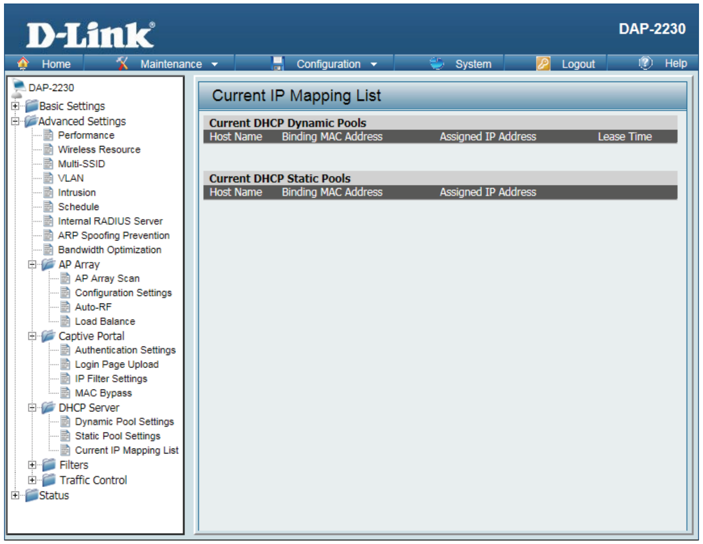
WINS: Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.

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

Domain Name: Specify the domain name for the network.

Current IP Mapping List

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



Current IP Mapping List

Current DHCP Dynamic Pools

Host Name	Binding MAC Address	Assigned IP Address	Lease Time

Current DHCP Static Pools

Host Name	Binding MAC Address	Assigned IP Address

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

Host Name: The host name of a device on the network that is assigned an IP address from the DHCP dynamic pool.

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.

Host Name: The host name of a device on the network that is assigned an IP address from the DHCP dynamic pool.

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.

Filters

Wireless MAC ACL

Wireless Band: Displays the current wireless band rate.

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

MAC Address: 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.

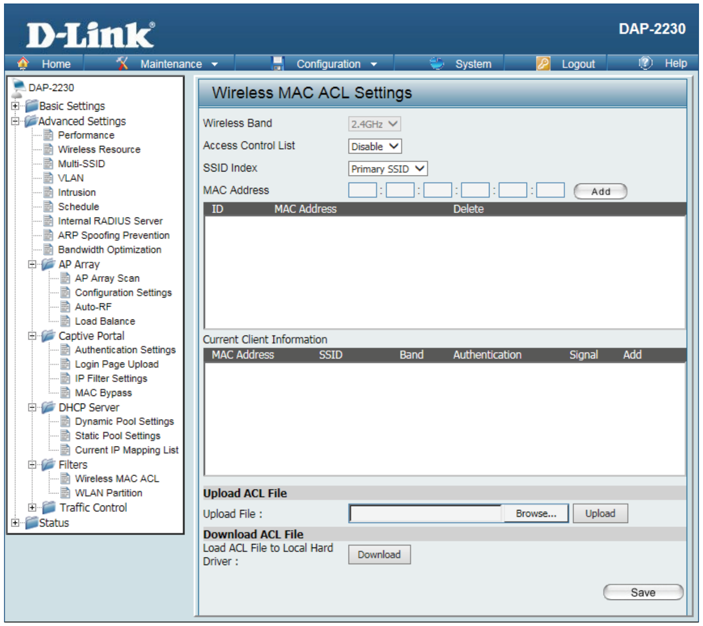
MAC Address List: Select **Reject** to reject the devices with MAC addresses on the Access Control List. All other devices not on the list will be accepted.

Upload ACL File: Enter each MAC address that you wish to include in your filter list, and click **Add**.

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

You may create an ACL list and upload it to the access point instead of manually entering the information. Once created, click the **Browse** button and locate your file. Select it and then click **Upload**.

Download ACL File: Click **Download** to export the ACL to a file on your computer.



Wireless MAC ACL Settings

Wireless Band: 2.4GHz

Access Control List: Disable

SSID Index: Primary SSID

MAC Address: __ : __ : __ : __ : __ : __ Add

ID	MAC Address	Delete

Current Client Information

MAC Address	SSID	Band	Authentication	Signal	Add

Upload ACL File

Upload File : Browse... Upload

Download ACL File

Load ACL File to Local Hard Driver : Download

Save

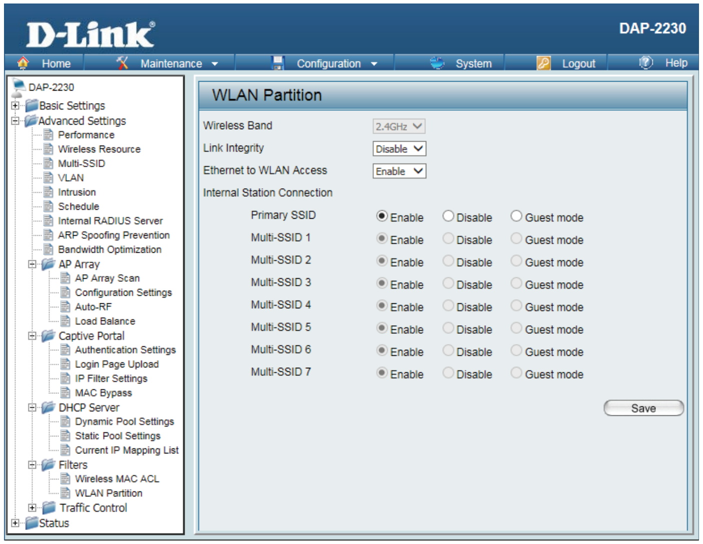
WLAN Partition

Wireless Band: Displays the current wireless band rate.

Link Integrity: Select **Enable** or **Disable**.

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

Internal Station Connection: The default value is **Enable**, which allows stations to inter-communicate by connecting to a target AP. When disabled, wireless stations cannot exchange data through the AP.



WLAN Partition

Wireless Band: 2.4GHz

Link Integrity: Disable

Ethernet to WLAN Access: Enable

Internal Station Connection

Primary SSID	● Enable	○ Disable	○ Guest mode
Multi-SSID 1	● Enable	○ Disable	○ Guest mode
Multi-SSID 2	● Enable	○ Disable	○ Guest mode
Multi-SSID 3	● Enable	○ Disable	○ Guest mode
Multi-SSID 4	● Enable	○ Disable	○ Guest mode
Multi-SSID 5	● Enable	○ Disable	○ Guest mode
Multi-SSID 6	● Enable	○ Disable	○ Guest mode
Multi-SSID 7	● Enable	○ Disable	○ Guest mode

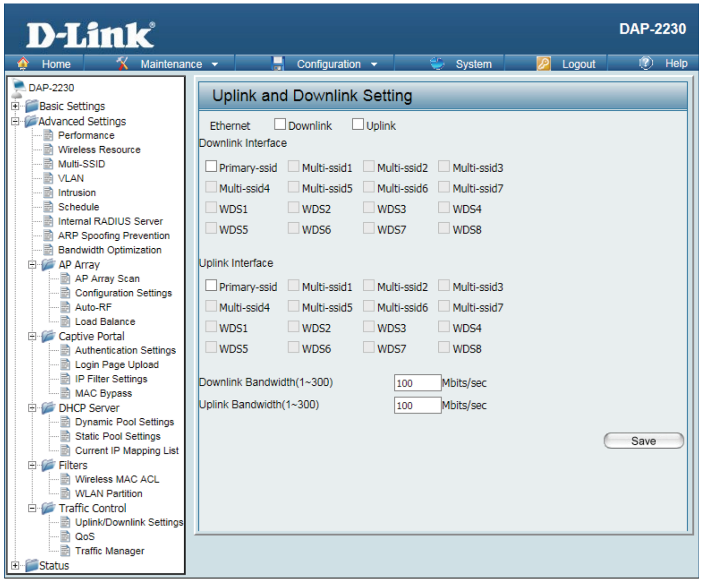
Traffic Control

Uplink/Downlink Settings

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

Downlink Bandwidth: The downlink bandwidth in Mbits per second.

Uplink Bandwidth: Uplink Bandwidth: The uplink bandwidth in Mbits per second.



Uplink and Downlink Setting

Ethernet □ Downlink □ Uplink

Downlink Interface

□ Primary-ssid □ Multi-ssid1 □ Multi-ssid2 □ Multi-ssid3
□ Multi-ssid4 □ Multi-ssid5 □ Multi-ssid6 □ Multi-ssid7
□ WDS1 □ WDS2 □ WDS3 □ WDS4
□ WDS5 □ WDS6 □ WDS7 □ WDS8

Uplink Interface

□ Primary-ssid □ Multi-ssid1 □ Multi-ssid2 □ Multi-ssid3
□ Multi-ssid4 □ Multi-ssid5 □ Multi-ssid6 □ Multi-ssid7
□ WDS1 □ WDS2 □ WDS3 □ WDS4
□ WDS5 □ WDS6 □ WDS7 □ WDS8

Downlink Bandwidth(1~300) 100 Mbits/sec

Uplink Bandwidth(1~300) 100 Mbits/sec

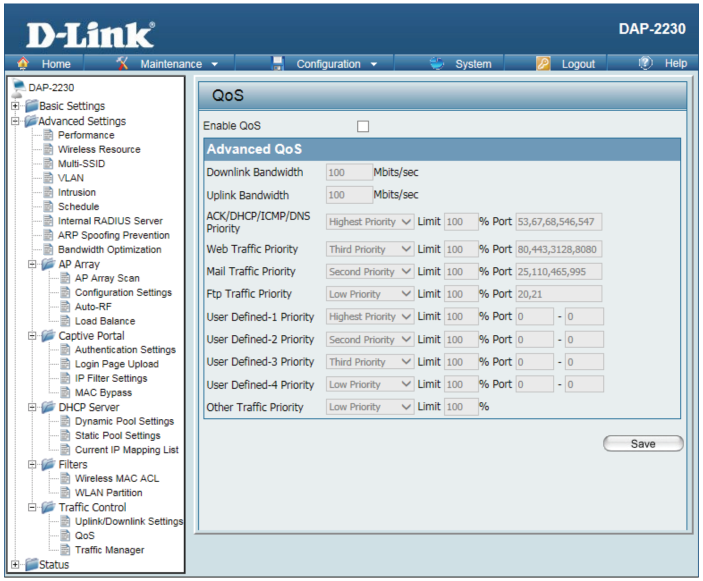
QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications. A QoS Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific QoS Rules are not required. QoS supports overlapping rules. If more than one rule matches a specific message flow, the rule with the highest priority will be used.

QoS (Quality of Service): Enable this option if you want to allow QoS to prioritize your traffic Priority Classifiers.

HTTP: Allows the access point to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

Automatic: When enabled, this option causes the access point to automatically attempt to prioritize traffic streams that it does not otherwise recognize, based on the behavior that the streams exhibit. This acts to de-prioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.



QoS

Enable QoS □

Advanced QoS

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