

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.

Copyright © 2015 by D-Link Corporation, Inc.

All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from D-Link Corporation, Inc.

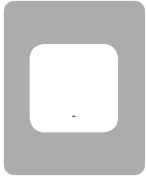
Table of Contents

Preface.....	i	Access Point mode	16
Product Overview.....	1	WDS with AP mode	18
Package Contents.....	1	WDS mode	20
System Requirements	2	Wireless Client mode	22
Introduction	3	Authentication Types	24
Features.....	4	Open System/Shared Key Authentication	24
Hardware Overview	5	WPA/WPA2-Personal Authentication.....	25
Top Panel	5	WPA/WPA2-Enterprise Authentication	26
Hardware Overview	6	802.1x Authentication.....	27
Bottom Panel.....	6	LAN	28
Physical Installation	7	IPv6	29
Before You Begin	7	Advanced Settings	30
Connect to your Network.....	8	Performance	30
Method 1 - Powered by PoE Switch	8	Wireless Resource Control.....	32
Method 2 - Powered by PoE Injector	9	Multi-SSID	34
Method 3 - DC Adapter.....	10	VLAN.....	35
Mounting the AP	11	VLAN List	35
Wireless Installation Considerations.....	12	Port List.....	36
Four Operational Modes	13	Add/Edit VLAN	37
Configuration.....	14	PVID Setting.....	38
Web-based Configuration Utility	14	Intrusion.....	39
Save and Activate Settings.....	15	Schedule	40
Basic Settings	16	Internal RADIUS Server	41
Wireless	16	ARP Spoofing Prevention Settings	42
		Bandwidth Optimization	43
		AP Array.....	45

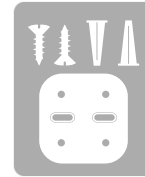
AP Array Scan	45	Client Information	68
Configuration Settings.....	46	WDS Information	69
Auto-RF.....	47	Channel Analyze	70
Load Balance	48	Statistics	71
Captive Portal Authentication.....	49	Ethernet.....	71
Web Redirection Only	49	WLAN Traffic	72
Username/Password.....	50	Log	73
Username/Password.....	50	View Log.....	73
Passcode	51	Log Settings.....	74
Remote Radius.....	52	Maintenance	76
LDAP	53	Administration Settings	76
POP3	55	Limit Administrator	77
Login Page Upload	56	System Name Settings.....	78
Login Page Upload	56	Login Settings	79
IP Filter	57	Console Settings	80
MAC Bypass.....	58	SNMP Settings	81
DHCP Server	59	Status:.....	82
Dynamic Pool Settings.....	59	Ping Control	82
Static Pool Setting	60	Central WiFiManager Settings.....	83
Current IP Mapping List.....	61	Firmware and SSL Certification Upload.....	84
Filters.....	62	Configuration File Upload	85
Wireless MAC ACL	62	Time and Date	86
WLAN Partition	63	System	87
Traffic Control.....	64	System Settings.....	87
Uplink/Downlink Settings	64	Help	88
QoS.....	65	Wireless Security	89
Traffic Manager.....	66	What is WEP?	90
Status	67	Configure WEP	91
Device Information	67		

What is WPA?	92
Configure WPA/WPA2 Personal	93
Configure WPA/WPA2 Enterprise	94
Connect to a Wireless Network.....	95
Using Windows® XP	95
Configure WPA-PSK.....	96
Using Windows Vista®	98
Configure WPA-PSK.....	100
Using Windows® 7	101
Troubleshooting	104
Wireless Basics	108
What is Wireless?	109
Tips.....	111
Wireless Modes.....	112
Networking Basics	113
Check your IP address	113
Statically Assign an IP address	114
Technical Specifications	115
Antenna Pattern	117
Regulatory Information	118

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 throughput 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

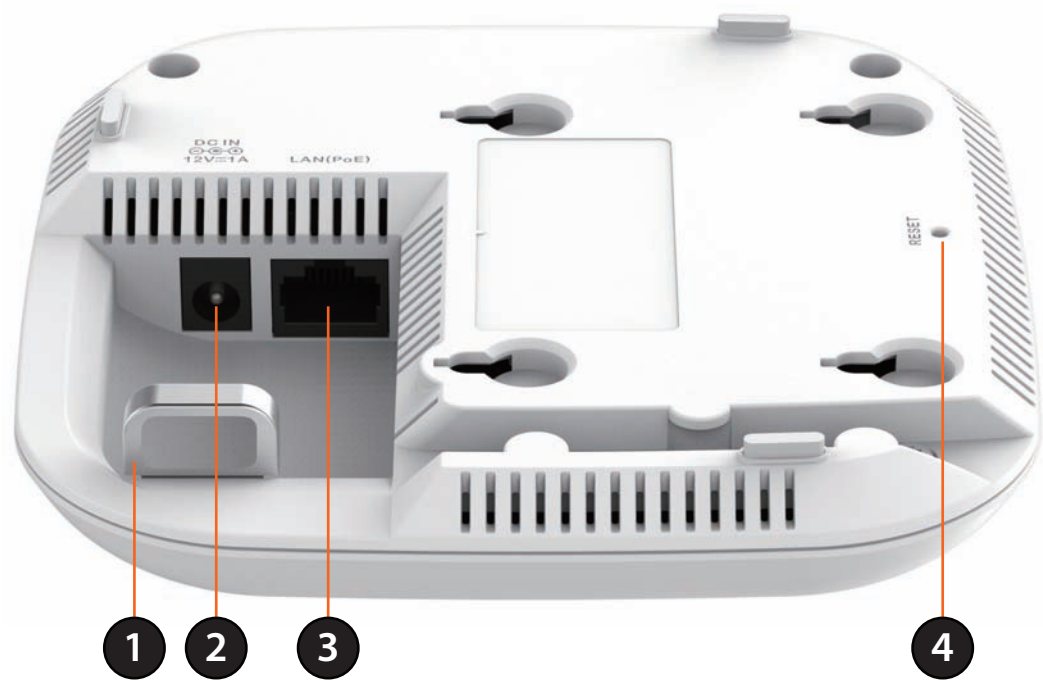
Top Panel



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:

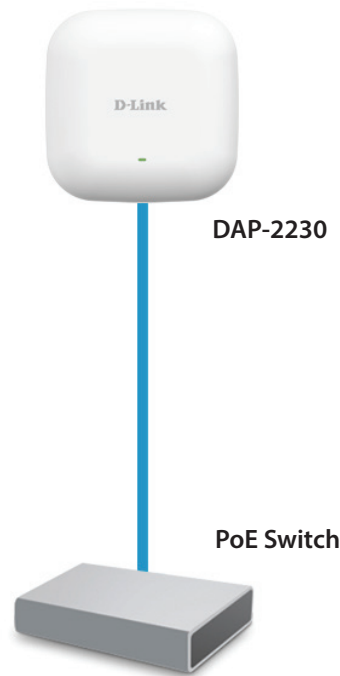
Method 1 - Powered by PoE Switch

Method 2 - Powered by PoE Injector

Method 3 - Powered by DC Adapter

Method 1 - Powered by PoE Switch

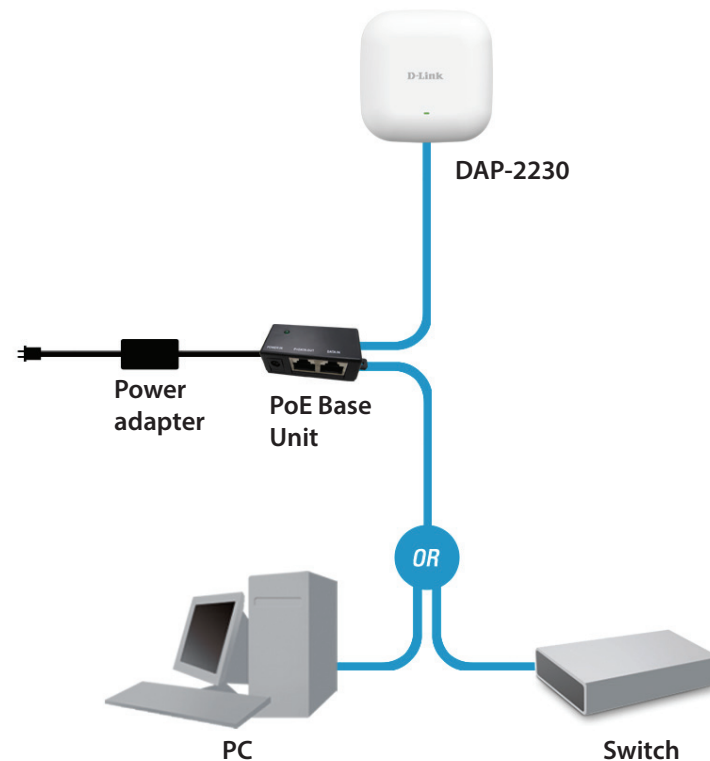
1. Connect one end of an Ethernet cable into the **LAN (PoE)** port on the DAP-2230 and then connect the other end to a PoE switch.



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.

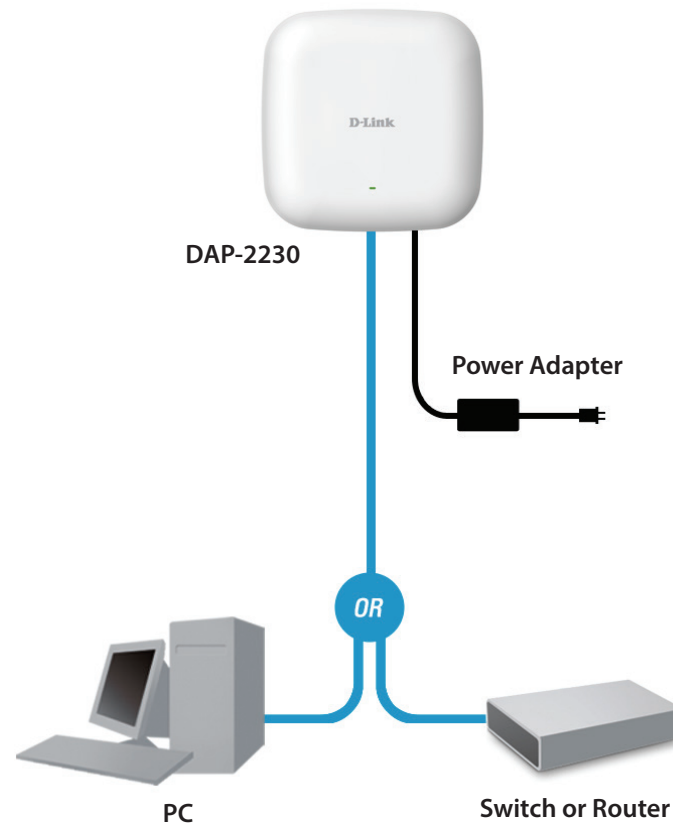
1. Connect one end of an Ethernet cable into the **DATA IN** port on the PoE injector and the other end into a port on a switch, router, or computer.
2. Connect one end of a different Ethernet cable into the **P+DATA OUT** port on the PoE injector and the other end into the **LAN (PoE)** port on the 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

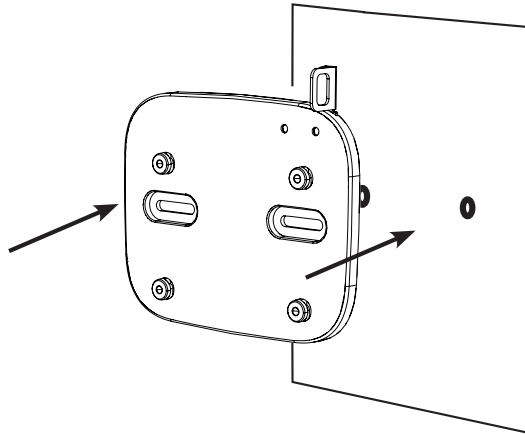
A power adapter is included with some DAP-2230 models.

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.

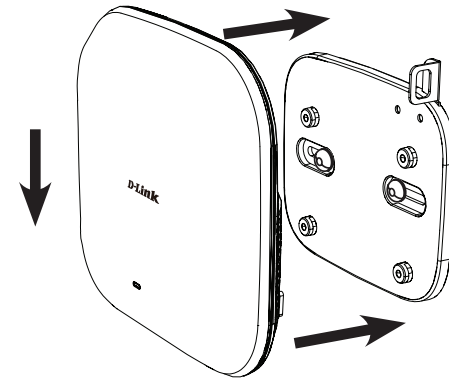


Mounting the AP

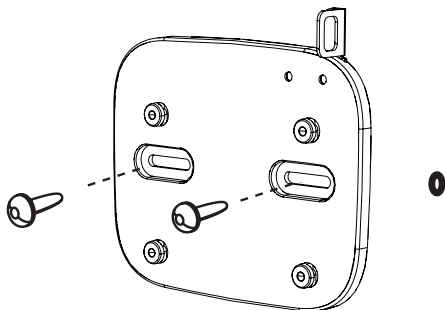
Place the mounting bracket on a wall or ceiling and mark holes where you will insert the screws with a marker. Drill holes in the marked points and insert the plastic wall anchors.



Reattach the DAP-2230 to the mounting bracket.



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



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.

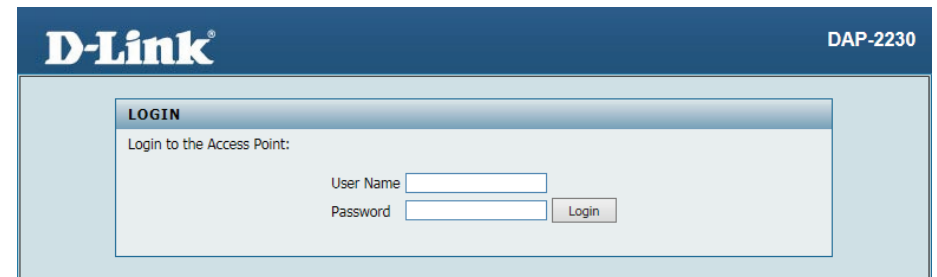
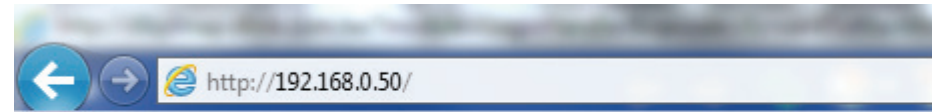
Web-based Configuration Utility

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

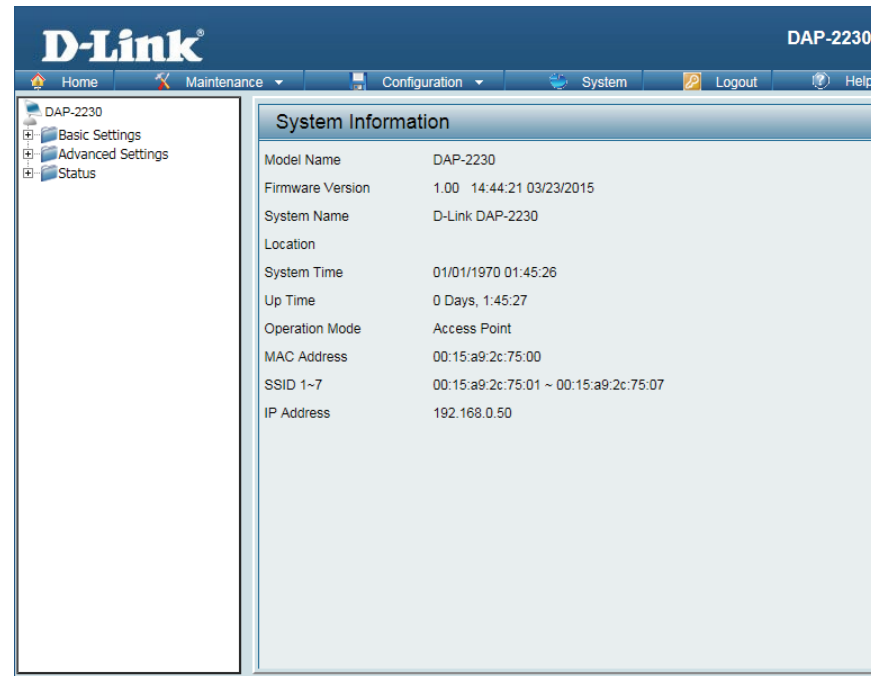
To access the configuration utility, open a web browser such as Internet Explorer and enter **http://192.168.0.50**

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.



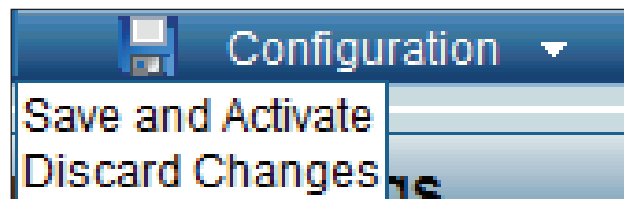
After successfully logging into the DAP-2230, the following screen will appear:



Save and Activate Settings

When making changes on most of the configuration screens in this section, use the  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**.

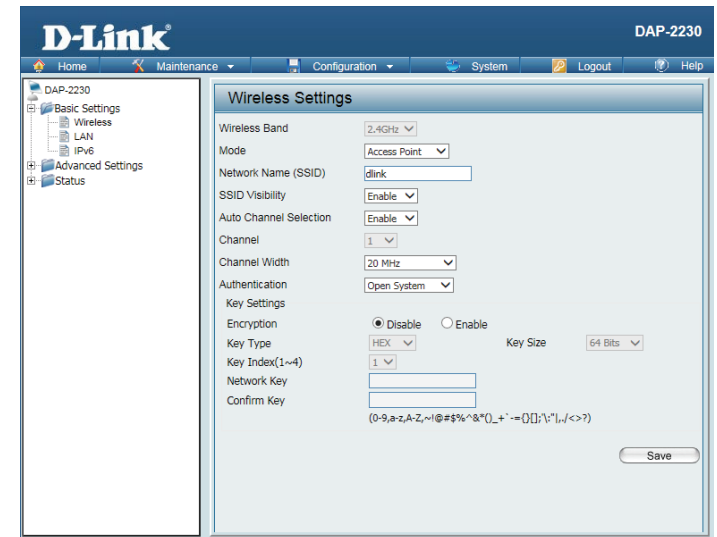
Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. The SSID can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



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.

The screenshot shows the D-Link DAP-2230 web interface. The 'Wireless Settings' tab is active. The 'Authentication' dropdown menu is set to 'Open System'. Other visible settings include 'Wireless Band' set to '2.4GHz', 'Mode' set to 'Access Point', 'Network Name (SSID)' set to 'dlink', 'SSID Visibility' set to 'Enable', 'Auto Channel Selection' set to 'Enable', 'Channel' set to '1', 'Channel Width' set to '20 MHz', 'Encryption' set to 'Disable', 'Key Type' set to 'HEX', 'Key Index' set to '1', and 'Network Key' set to a default value. A 'Save' button is located at the bottom right of the settings panel.

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.

The screenshot displays the 'Wireless Settings' page for a D-Link DAP-2230 device. The interface includes a navigation menu on the left with options like Basic Settings, Wireless, LAN, IPv6, Advanced Settings, and Status. The main content area is titled 'Wireless Settings' and contains several configuration sections. The 'Wireless Band' is set to '2.4GHz'. The 'Mode' is set to 'WDS with AP'. The 'Network Name (SSID)' is 'dlink', and 'SSID Visibility' is set to 'Enable'. 'Auto Channel Selection' is set to 'Disable', the 'Channel' is '1', and 'Channel Width' is '20 MHz'. The 'WDS' section has a 'Remote AP MAC Address' field with eight sub-fields numbered 1 through 8. Below this is a 'Site Survey' section with a 'Scan' button. The bottom section is for 'Authentication', with 'Open System' selected. It includes 'Key Settings' (set to 'Disable'), 'Encryption' (set to '64 Bits'), 'Key Type' (set to 'HEX'), 'Key Index' (set to '1'), 'Network Key', and 'Confirm Key' fields. A 'Save' button is at the bottom right.

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

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

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



WDS mode

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

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.

The screenshot displays the 'Wireless Settings' page for a D-Link DAP-2230 device. The left sidebar shows a navigation menu with 'Basic Settings', 'Wireless', 'LAN', 'IPv6', 'Advanced Settings', and 'Status'. The 'Wireless' section is expanded, showing 'Basic Settings', 'WDS', 'WDS with AP', and 'Wireless Client'. The 'WDS' option is selected. The main content area shows the following settings:

- Wireless Band:** 2.4GHz (dropdown)
- Mode:** WDS (dropdown)
- Network Name (SSID):** dlink (text field)
- SSID Visibility:** Enable (radio button selected)
- Auto Channel Selection:** Disable (radio button selected)
- Channel:** 1 (dropdown)
- Channel Width:** 20 MHz (dropdown)
- WDS Remote AP MAC Address:** Eight text fields for MAC addresses (1-8).
- Site Survey:** A 'Scan' button.
- Authentication:** Open System (dropdown).
- Key Settings:**
 - Encryption:** Disable (radio button selected), Enable (radio button).
 - Key Type:** HEX (dropdown).
 - Key Index(1~4):** 1 (dropdown).
 - Network Key:** Text field.
 - Confirm Key:** Text field.
 - Key Size:** 64 Bits (dropdown).
- Save:** A button at the bottom right.

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.

The screenshot shows the D-Link DAP-2230 web interface. The top navigation bar includes links for Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view with Basic Settings (selected), Wireless, LAN, IPv6, Advanced Settings, and Status. The main content area is titled 'Wireless Settings' and contains the following fields:

- Wireless Band: 2.4GHz (dropdown)
- Mode: WDS (dropdown)
- Network Name (SSID): dlink (text input)
- SSID Visibility: Enable (dropdown)
- Auto Channel Selection: Disable (dropdown)
- Channel: 1 (dropdown)
- Channel Width: 20 MHz (dropdown)
- WDS Remote AP MAC Address: Eight input fields labeled 1 through 8.
- Site Survey: A button labeled 'Scan'.

Below the settings is a table with the following headers: CH, RSSI, BSSID, Security, and SSID. The table body is currently empty.

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.

The screenshot displays the D-Link DAP-2230 configuration interface. The 'Wireless Settings' tab is active. The 'Wireless Band' is set to 2.4GHz, 'Mode' is Wireless Client, and 'Network Name (SSID)' is dlink. 'SSID Visibility' and 'Auto Channel Selection' are both enabled. The 'Channel' is set to 1, and 'Channel Width' is set to Auto 20/40 MHz. A 'Scan' button is present next to the channel width setting. Below these settings, there is a table for scanning available networks with columns for CH, RSSI, BSSID, Security, and SSID. Further down, the 'Authentication' section is set to Open System, and 'Key Settings' are configured with 'Disable' encryption, 'HEX' key type, 'Key Index' 1, and a 'Key Size' of 64 Bits. The 'Network Key' and 'Confirm Key' fields are empty. The 'Wireless MAC Clone' section has 'Enable' unchecked, 'MAC Source' set to Auto, and a 'MAC Address' field with a 'Scan' button. A 'Save' button is located at the bottom right of the page.

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.

The screenshot displays the D-Link DAP-2230 web interface, specifically the 'Wireless Settings' page. The interface is in English and features a navigation menu on the left with options like 'Basic Settings', 'Wireless', 'LAN', 'IPv6', 'Advanced Settings', and 'Status'. The main content area is titled 'Wireless Settings' and includes the following sections:

- Wireless Band:** Set to 2.4GHz.
- Mode:** Set to Wireless Client.
- Network Name (SSID):** Set to dlink.
- SSID Visibility:** Set to Enable.
- Auto Channel Selection:** Set to Enable.
- Channel:** Set to 1.
- Channel Width:** Set to Auto 20/40 MHz.
- Site Survey:** A button labeled 'Scan' is present.
- Authentication:** A dropdown menu is set to 'Open System'.
- Key Settings:**
 - Encryption:** Radio buttons for 'Disable' (selected) and 'Enable'.
 - Key Type:** Set to HEX.
 - Key Index(1~4):** Set to 1.
 - Key Size:** Set to 64 Bits.
 - Network Key:** A text input field.
 - Confirm Key:** A text input field with a hint: (0-9,a-z,A-Z,~!@#\$%^&*()_+~=<[]\';"/>?).
- Wireless MAC Clone:**
 - Enable:** An unchecked checkbox.
 - MAC Source:** A dropdown menu set to 'Auto'.
 - MAC Address:** A text input field with a hint: : : : : : . A 'Scan' button is next to it.

At the bottom right of the page, there is a 'Save' button.

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,~!@#\$%^&*()_+`-={[]:;'\",./<>?)

Add

Index	SSID	Band	Encryption	Delete
Primary SSID	dlink	2.4 GHz	None	

Save

D-Link DAP-2230 User Manual

24

WPA/WPA2-Personal Authentication

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

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.

The screenshot shows a configuration window for WPA/WPA2-Personal Authentication. The 'Authentication' dropdown is set to 'WPA-Personal'. Under 'PassPhrase Settings', the 'WPA Mode' dropdown is set to 'AUTO (WPA or WPA2)'. The 'Cipher Type' dropdown is set to 'Auto'. The 'Group Key Update Interval' is set to '3600' seconds. The 'Activated From' field is set to 'Sun' at '00:00'. The 'Time Interval' is set to '1' hour. The 'Manual' radio button is selected for the key change method. The 'PassPhrase' and 'Confirm PassPhrase' fields are empty. A 'Save' button is at the bottom right. A notice at the bottom states: 'notice: 8~63 in ASCII or 64 in Hex. (0-9,a-z,A-Z,~!@#\$%^&*()_+`-={[];':",./<>?)'.

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,~!@#\$%^&*()_+`-={[];'\":/,<>?)

Add

Index	SSID	Band	Encryption	Delete
Primary SSID	dlink	2.4 GHz	None	

Save

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

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,~|@#%&*()_+`-={}[];'\:|,./<>?)

Add

Index	SSID	Band	Encryption	Delete
Primary SSID	dlink	2.4 GHz	None	

Save

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.

The screenshot shows the D-Link DAP-2230 web interface. The top navigation bar includes 'Home', 'Maintenance', 'Configuration', 'System', 'Logout', and 'Help'. The left sidebar shows a tree view with 'DAP-2230' expanded, containing 'Basic Settings', 'Wireless', 'LAN', 'IPv6', 'Advanced Settings', and 'Status'. The main content area is titled 'LAN Settings'. It features a 'Get IP From' dropdown menu set to 'Static IP (Manual)'. Below this are four input fields: 'IP Address' (containing '192.168.0.50'), 'Subnet Mask' (containing '255.255.255.0'), 'Default Gateway', and 'DNS'. A 'Save' button is located at the bottom right of the form.

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.

The screenshot shows the D-Link DAP-2230 web interface. The top navigation bar includes 'Home', 'Maintenance', 'Configuration', 'System', 'Logout', and 'Help'. The left sidebar shows a tree view with 'DAP-2230' expanded, containing 'Basic Settings', 'Wireless', 'LAN', 'IPv6', 'Advanced Settings', and 'Status'. The main content area is titled 'IPv6 Settings'. It features a checkbox for 'Enable IPv6'. Below it is a 'Get IP From' dropdown menu set to 'Auto'. There are three input fields: 'IP Address', 'Prefix', and 'Default Gateway'. A 'Save' button is located at the bottom right of the settings area.

Advanced Settings

Performance

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

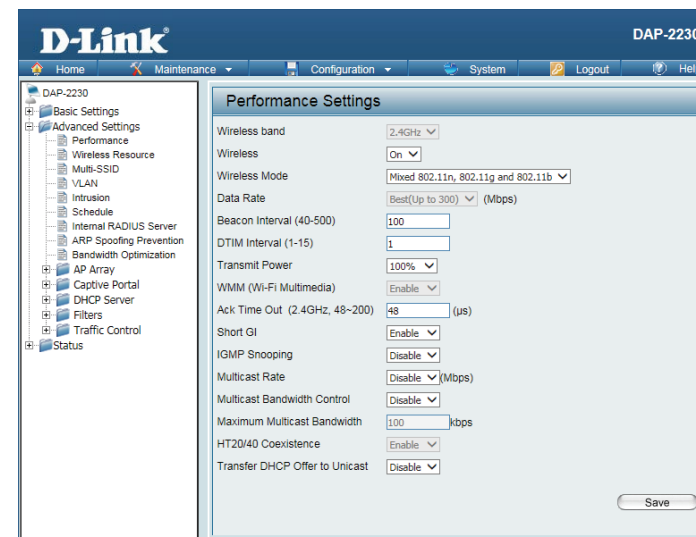
Wireless Mode: The different combination of clients that can be supported include **Mixed 802.11n, 802.11g and 802.11b, Mixed 802.11g and 802.11b** and **802.11n Only**. Please note that when backwards compatibility is enabled for legacy (802.11g/b) clients, degradation of 802.11n wireless performance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



*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 throughput rate.

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.

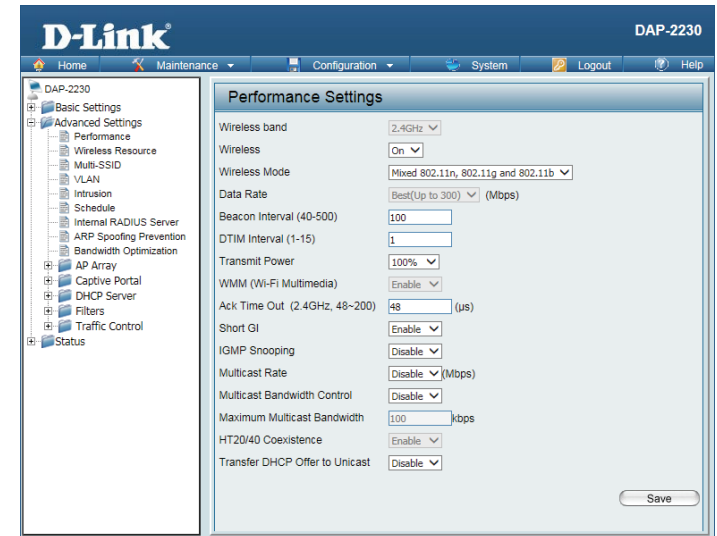
Multicast Rate: Select the multicast rate for 2.4G band.

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 band: Select **2.4 Ghz**.

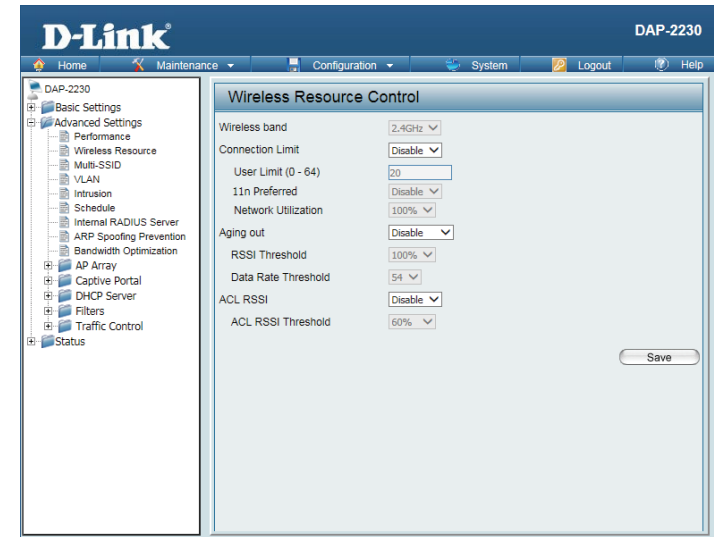
Connection Limit: Select **Enable** or **Disable**. This is an option for load balancing. This determines whether to limit the number of users accessing this device. The exact number is entered in the User Limit field below. This feature allows the user to share the wireless network traffic and the client 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**.

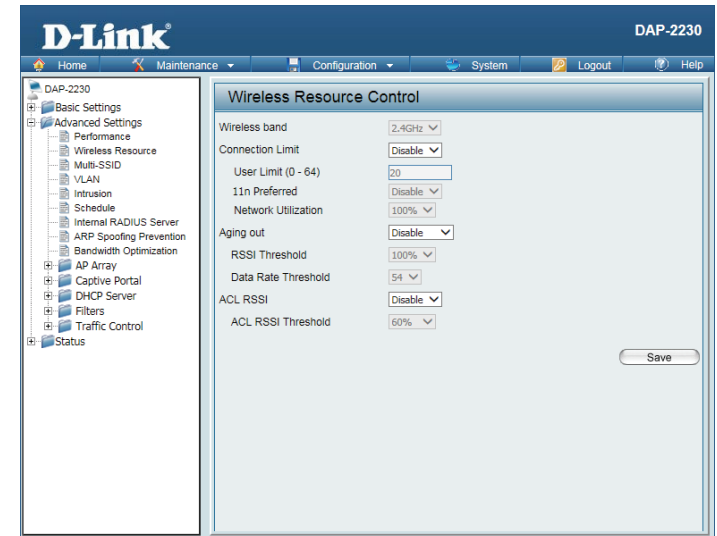


RSSI Threshold: When **RSSI** is selected in the **Aging out** drop-down menu, select the percentage of RSSI here. When the RSSI of wireless clients is lower than the specified percentage, the device disconnects the wireless clients.

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.

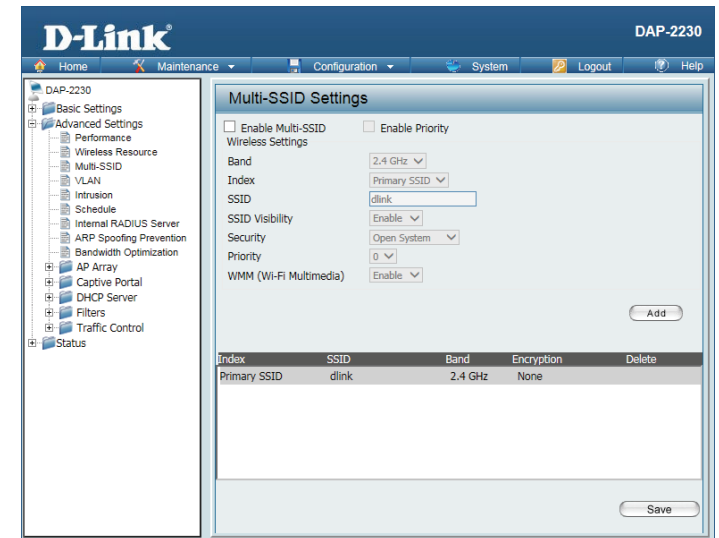
ACL RSSI Threshold: Set the ACL RSSI Threshold.



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.

- 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**.



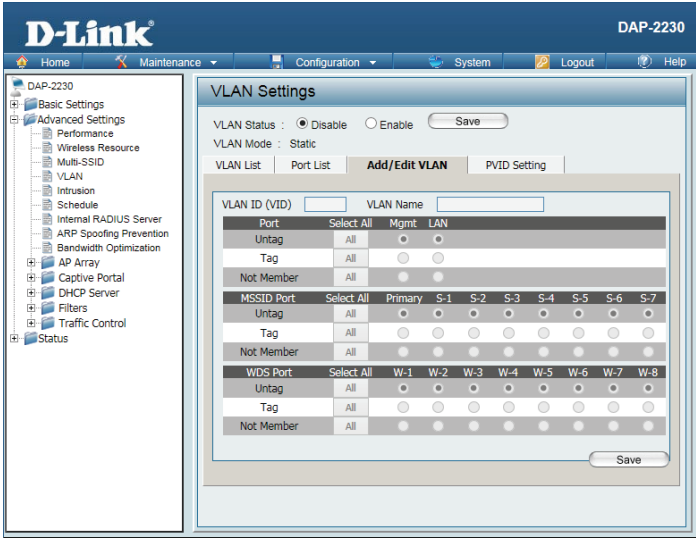
VLAN

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



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.

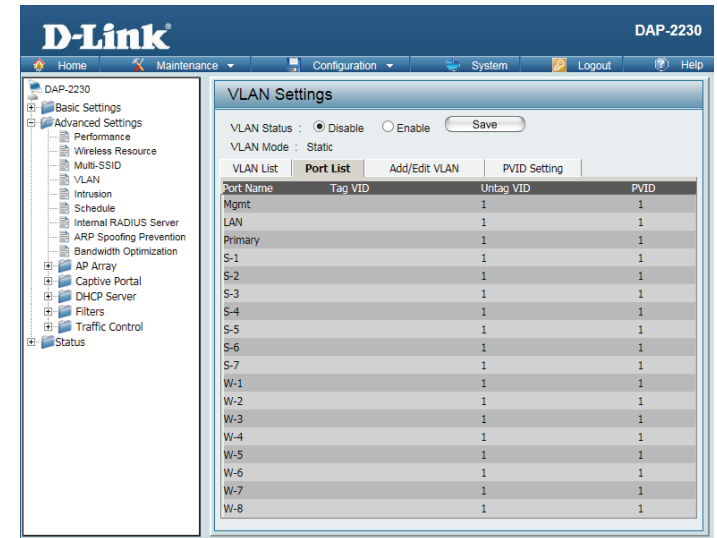
VLAN Status: Use the radio button to toggle to Enable. Next, go to the **Add/Edit VLAN** tab to add or modify an item on the **VLAN List** tab.

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.



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.

D-Link DAP-2230

Home Maintenance Configuration System Logout Help

VLAN Settings

VLAN Status : ☐ Disable ☐ Enable

VLAN Mode : Static

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

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	☐	☐	☐	☐	☐	☐	☐	☐

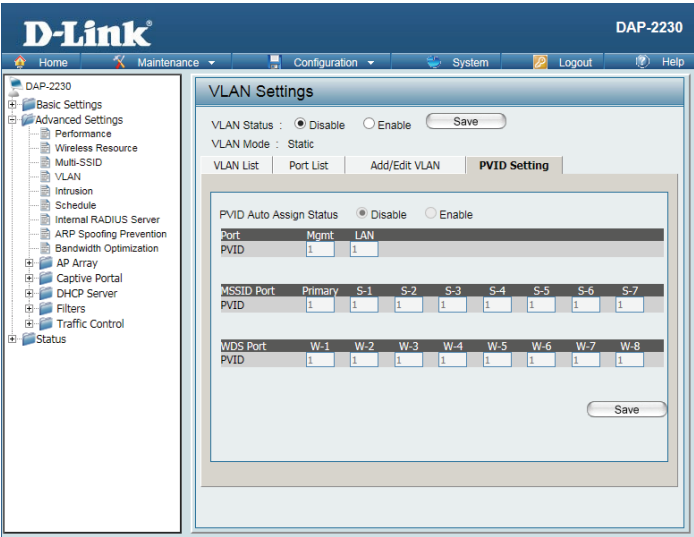
WDS Port	Select All	W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
Untag	All	☐	☐	☐	☐	☐	☐	☐	☐
Tag	All	☐	☐	☐	☐	☐	☐	☐	☐
Not Member	All	☐	☐	☐	☐	☐	☐	☐	☐

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**.

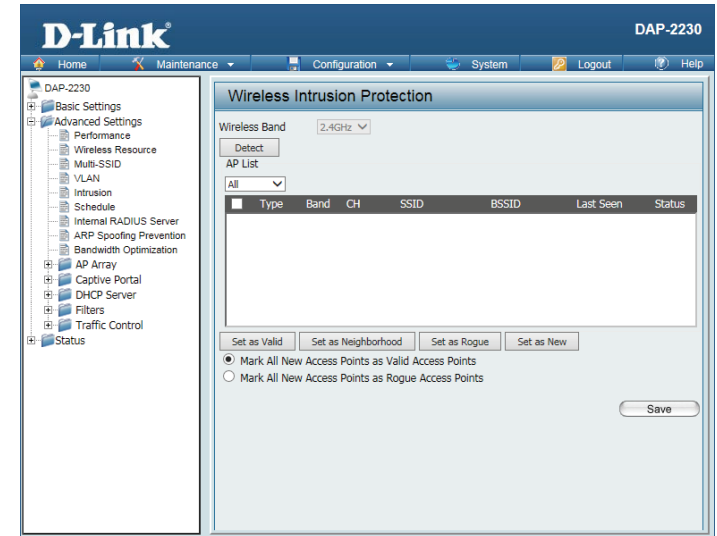


Intrusion

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.



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: 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.

The screenshot shows the D-Link DAP-2230 configuration interface. The 'Wireless Schedule Settings' window is open, displaying the 'Add Schedule Rule' section. The 'Wireless Schedule' dropdown is set to 'Disable'. The 'Add Schedule Rule' section includes fields for Name, Index (Primary SSID), SSID (dlink), Day(s) (radio buttons for All Week and Select Day(s)), All Day(s) (checkbox), Start Time, End Time, and an Overnight checkbox. At the bottom is a 'Schedule Rule List' table with columns: Name, SSID Index, SSID, Day(s), Time Frame, Wireless, Edit, and DEL. A 'Save' button is at the bottom right.

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.

The screenshot shows the D-Link DAP-2230 web interface. The left sidebar contains a tree view with categories like Basic Settings, Advanced Settings, Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, AP Array, Captive Portal, DHCP Server, Filters, Traffic Control, and Status. The 'Internal RADIUS Server' option is selected. The main content area is titled 'Internal RADIUS Server' and includes a section for 'Add RADIUS Account' with input fields for 'User Name', 'Password', and a 'Status' dropdown menu set to 'Enable'. Below this is a 'RADIUS Account list' table with columns for 'User Name', 'Enable', 'Disable', and 'Delete'. The table is currently empty. A 'Save' button is located at the bottom right of the configuration area.

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.

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.

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 **Allocate 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.

D-Link DAP-2230 Bandwidth Optimization Configuration

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
------	------	------------	----------------	--------------	------	-----

Save

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.

The screenshot shows the D-Link DAP-2230 web interface. The left sidebar contains a tree view with the following items: DAP-2230, Basic Settings, Advanced Settings, Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization (selected), AP Array, Captive Portal, DHCP Server, Filters, Traffic Control, and Status. The main content area is titled 'Bandwidth Optimization'. It includes a section for 'Enable Bandwidth Optimization' with a dropdown set to 'Enable'. Below this are input fields for 'Downlink Bandwidth' and 'Uplink Bandwidth', both set to '80' with units of 'Mbits/sec'. The 'Add Bandwidth Optimization Rule' section has a 'Rule Type' dropdown set to 'Allocate average BW for each station'. It also includes dropdowns for 'Band' (set to '2.4 GHz') and 'SSID Index' (set to 'Primary SSID'). There are input fields for 'Downlink Speed' and 'Uplink Speed' with units of 'Kbits/sec'. At the bottom of this section are 'Add' and 'Clear' buttons. The 'Bandwidth Optimization Rules' section features a table with columns: Band, Type, SSID Index, Downlink Speed, Uplink Speed, Edit, and Del. The table is currently empty. A 'Save' button is located at the bottom right of the main content area.

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.

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.

D-Link DAP-2230

Home Maintenance Configuration System Logout Help

AP Array Scan Version: 2.0

☐ Enable AP Array

☐ Master ☐ Backup Master ☒ Slave

AP Array Name:

AP Array Password:

Scan AP Array List:

Connection Status:

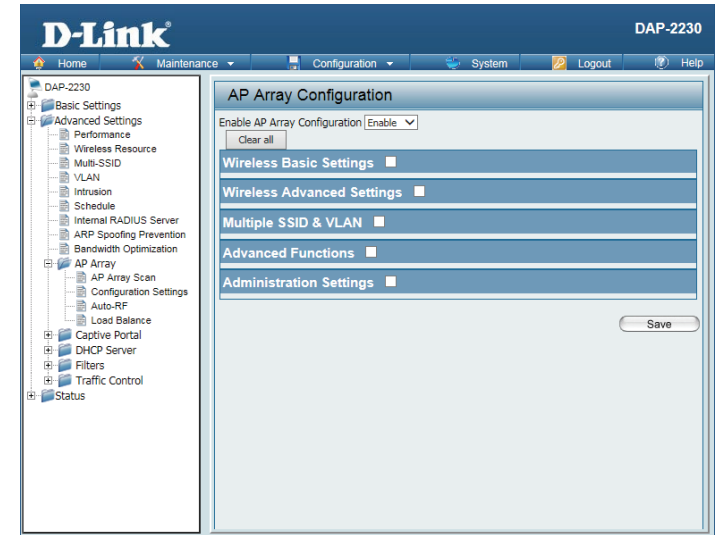
AP Array List						
Array Name	Master IP	MAC	Master	Backup Master	Slave	Total

Current Members				
Index	Role	IP Address	MAC Address	Location

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.



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

Auto-RF:

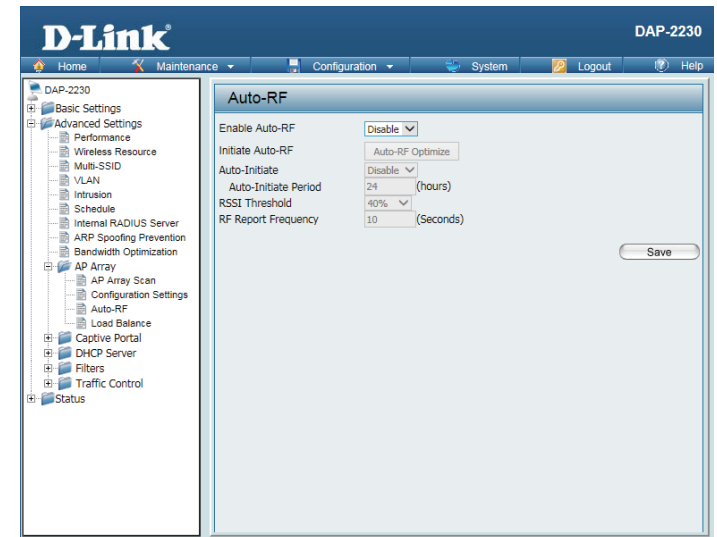
Initiate Click the Auto-RF Optimize button to initiate the auto-RF optimization
Auto-RF: feature.

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

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

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

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

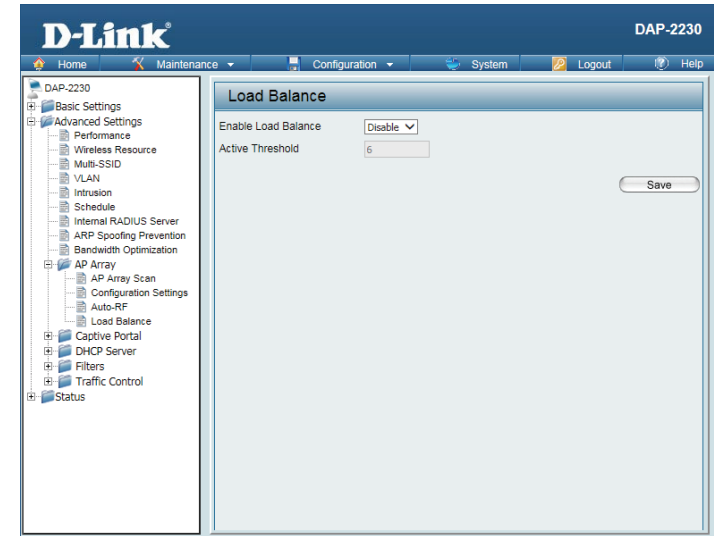


Load Balance

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.



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.

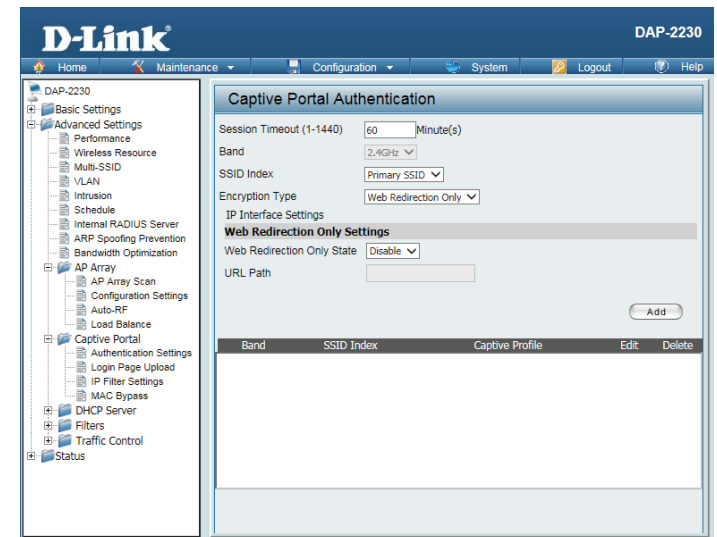
Band: Select 2.4 Ghz.

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.



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.

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.

The screenshot shows the D-Link DAP-2230 web interface. The left sidebar contains a navigation tree with categories like Basic Settings, Advanced Settings, Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, AP Array, AP Array Scan, Configuration Settings, Auto-RF, Load Balance, Captive Portal, Authentication Settings, Login Page Upload, IP Filter Settings, DHCP Server, Filters, Traffic Control, and Status. The main content area is titled 'Captive Portal Authentication'. It includes fields for Session Timeout (1-1440) set to 60, Band set to 2.4Ghz, SSID Index set to Primary SSID, and Encryption Type set to Username/Password. Below these are 'Web Redirection Only Settings' with a 'Web Redirection Only State' dropdown set to 'Disable' and a 'URL Path' text box. The 'Username/Password Settings' section has input fields for Username and Password, with 'Add' and 'Clear' buttons. At the bottom, there is a table with columns: Band, SSID Index, Captive Profile, Edit, and Delete. The table is currently empty.

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**.

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

The screenshot shows the D-Link DAP-2230 web interface. The left sidebar contains a navigation menu with options like Basic Settings, Advanced Settings, Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, AP Array, AP Array Scan, Configuration Settings, Auto-RF, Load Balance, Captive Portal, Authentication Settings, Login Page Upload, IP Filter Settings, MAC Bypass, DHCP Server, Filters, Traffic Control, and Status. The main content area is titled 'Captive Portal Authentication'. It includes fields for Session Timeout (1-1440) set to 60, Band set to 2.4Ghz, SSID Index set to Primary SSID, and Encryption Type set to Passcode. Under 'Web Redirection Only Settings', the Web Redirection Only State is set to Disable. There are fields for URL Path, Passcode Settings, Passcode Quantity, Duration, Last Active Time (Year, Month, Day, Hour), and User Limit. At the bottom, there is a table with columns: Passcode, Duration, Last Active Time, User Limit, and Delete. An 'Add' button is located below the table.

Remote Radius

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

D-Link DAP-2230

Home Maintenance Configuration System Logout Help

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: 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

Add

Band	SSID Index	Captive Profile	Edit	Delete

LDAP

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

The screenshot displays the D-Link DAP-2230 web interface. The left sidebar shows a tree view of configuration options, with 'Captive Portal' expanded. The main panel, titled 'Captive Portal Authentication', contains the following settings:

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

An 'Add' button is located at the bottom right of the configuration area. Below the settings is a table with columns: Band, SSID Index, Captive Profile, Edit, and Delete.

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.

The screenshot shows the D-Link DAP-2230 web interface for Captive Portal Authentication. The left sidebar contains a tree view with categories like Basic Settings, Advanced Settings, Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, AP Array, AP Array Scan, Configuration Settings, Auto-RF, Load Balance, Captive Portal, Authentication Settings, Login Page Upload, IP Filter Settings, MAC Bypass, DHCP Server, Filters, Traffic Control, and Status. The main panel is titled 'Captive Portal Authentication' and includes the following settings:

- 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: (empty field)
- LDAP Settings: Server (empty field), Port: 389
- Authenticate Mode: Simple
- Username: (empty field)
- Password: (empty field)
- Base DN: (empty field) (ou=,dc=)
- Account Attribute: (empty field) (ex.cn)
- Identity: (empty field) ☐ Auto Copy

At the bottom right of the main panel is an 'Add' button. Below the settings is a table with columns: Band, SSID Index, Captive Profile, Edit, and Delete. The table is currently empty.

POP3

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

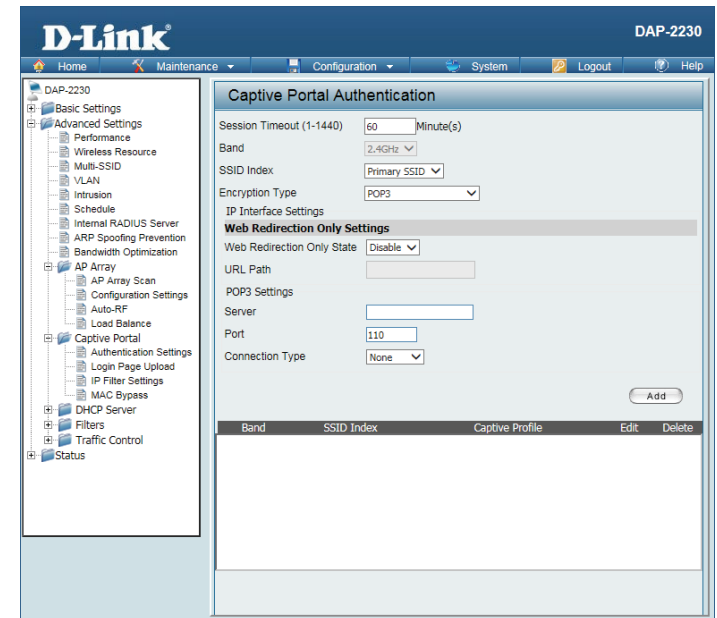
Web Redirection State: By default web redirection is disabled. Select enable to activate the website redirection feature.

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.



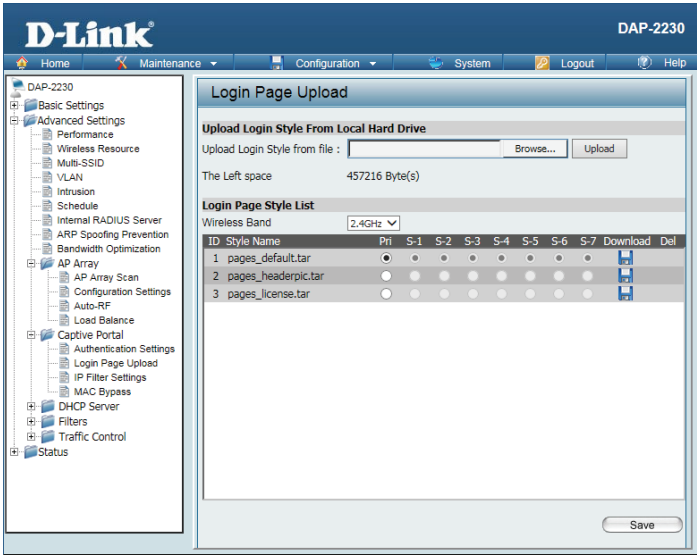
Login Page Upload

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.



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.

The screenshot shows the D-Link DAP-2230 web interface. The top navigation bar includes Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar lists various settings categories: Basic Settings, Advanced Settings (Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization), AP Array (AP Array Scan, Configuration Settings, Auto-RF, Load Balance), Captive Portal (Authentication Settings, Login Page Upload, IP Filter Settings, MAC Bypass), DHCP Server, Filters, Traffic Control, and Status. The main content area is titled 'IP Filter Settings'. It includes a 'Wireless Band' dropdown menu set to '2.4Ghz', an 'SSID Index' dropdown set to 'Primary SSID', and input fields for 'IP Address' and 'Subnet Mask' with an 'Add' button. Below this is a table with columns 'ID', 'IP Address', 'Subnet Mask', and 'Delete'. At the bottom, there are sections for 'Upload IP Filter File' (with 'Upload File' and 'Browse...' buttons) and 'Download IP Filter File' (with 'Load IP Filter File to Local Hard Drive' and 'Download' buttons). A 'Save' button is located at the bottom right.

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.

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.

The screenshot shows the D-Link DAP-2230 configuration page for MAC Bypass Settings. The interface includes a navigation tree on the left with categories like Basic Settings, Advanced Settings, Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, AP Array, AP Array Scan, Configuration Settings, Auto-RF, Load Balance, Captive Portal, Authentication Settings, Login Page Upload, IP Filter Settings, MAC Bypass, DHCP Server, Filters, Traffic Control, and Status. The main content area is titled 'MAC Bypass Settings' and contains the following fields and controls:

- Wireless Band:** A dropdown menu currently set to '2.4GHz'.
- SSID Index:** A dropdown menu currently set to 'Primary SSID'.
- MAC Address:** A form with five input boxes for the MAC address (XX:XX:XX:XX:XX:XX) and an 'Add' button.
- MAC Address List:** A table with columns for 'ID', 'MAC Address', and 'Delete'. It is currently empty.
- Upload MAC File:** A section with an 'Upload File' label, a text input field, a 'Browse...' button, and an 'Upload' button.
- Download MAC File:** A section with a 'Load MAC File to Local Hard Drive' label, a 'Download' button, and a 'Save' button at the bottom right.

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.

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)

The screenshot shows the D-Link DAP-2230 web interface. The left sidebar contains a tree view with categories like Basic Settings, Advanced Settings, and DHCP Server. The main content area is titled 'Dynamic Pool Settings'. Under 'DHCP Server Control', the 'Function Enable/Disable' is set to 'Disable'. Under 'Dynamic Pool Settings', the 'IP Assigned From' is '192.168.0.20', 'The Range of Pool (1-254)' is '235', 'Subnet Mask' is '255.255.255.0', 'Gateway' is empty, 'WINS' is empty, 'DNS' is empty, 'Domain Name' is 'dlink-ap', and 'Lease Time (60 - 31536000 sec)' is '604800'. A 'Save' button is at the bottom right.

Static Pool Setting

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

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.

The screenshot shows the D-Link DAP-2230 web interface. The left sidebar contains a navigation tree with categories like Basic Settings, Advanced Settings, Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, AP Array, AP Array Scan, Configuration Settings, Auto-RF, Load Balance, Captive Portal, Authentication Settings, Login Page Upload, IP Filter Settings, MAC Bypass, DHCP Server, Dynamic Pool Settings, Static Pool Settings, Current IP Mapping List, Filters, and Traffic Control. The main content area is titled 'Static Pool Settings'. It includes a 'DHCP Server Control' section with a 'Function Enable/Disable' dropdown set to 'Disable'. Below this is the 'Static Pool Setting' section with fields for Host Name, Assigned IP, Assigned MAC Address, Subnet Mask (pre-filled with 255.255.255.0), Gateway, WINS, DNS, and Domain Name (pre-filled with dlink-ap). A 'Save' button is located at the bottom right of this section. At the bottom of the page, there is a table with columns: Host Name, MAC Address, IP Address, Edit, and Delete. The table is currently empty.

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 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.

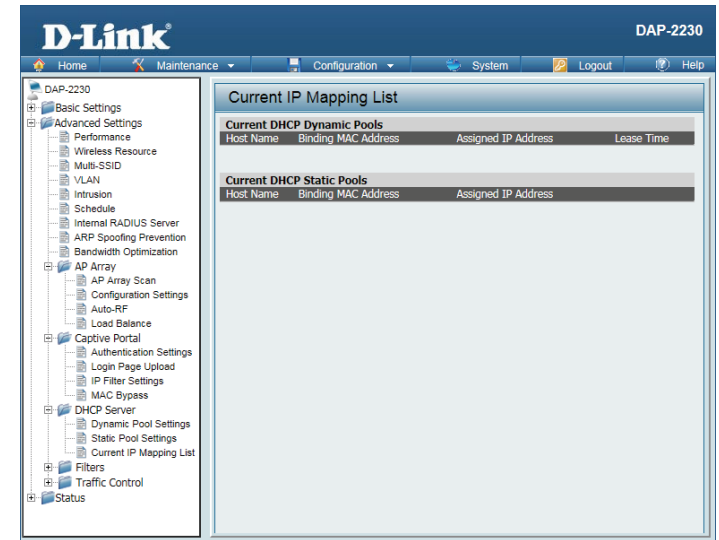
Lease Time: The length of time that the dynamic IP address will be valid.

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.

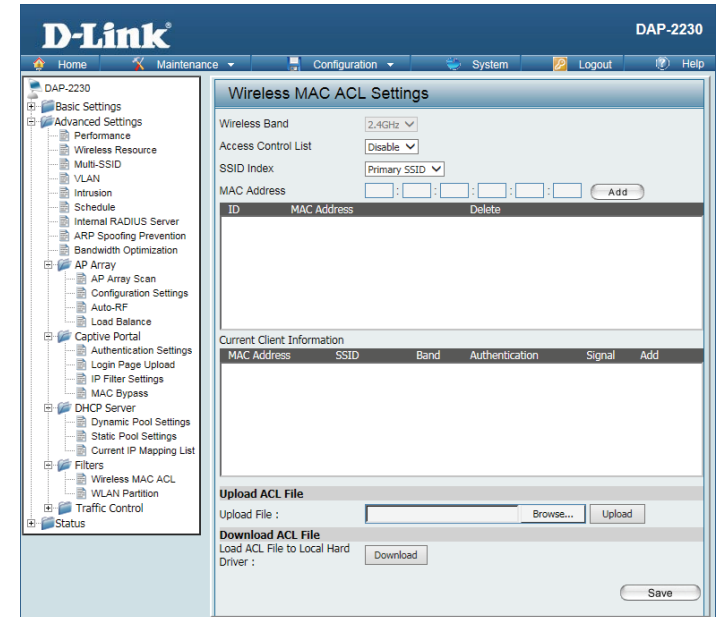
MAC Address List: Select **Reject** to reject the devices with MAC addresses on the Access Control List. All other devices not on the list will be accepted.

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.



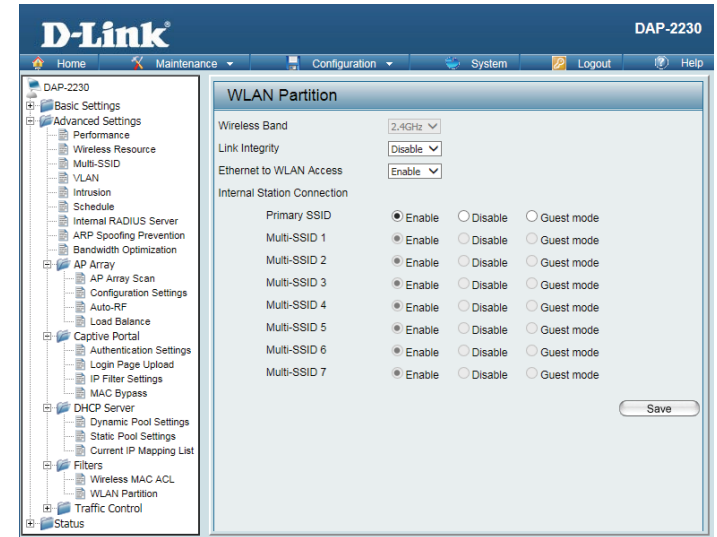
WLAN Partition

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.



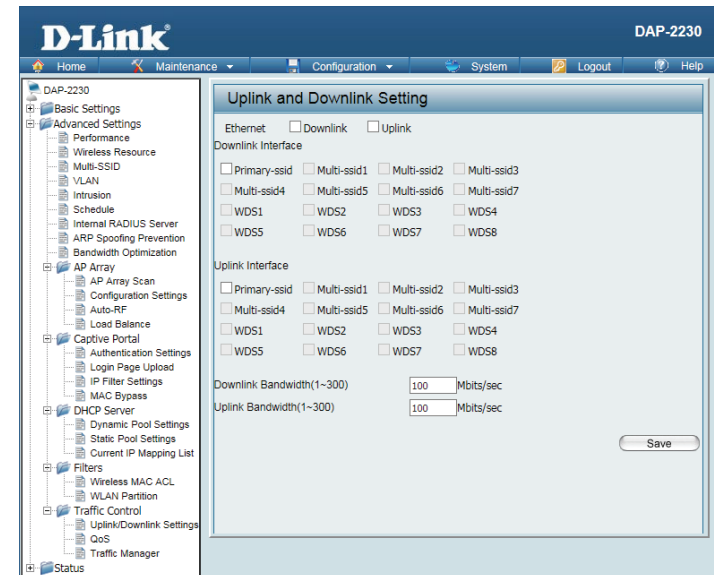
Traffic Control

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.



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.

