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

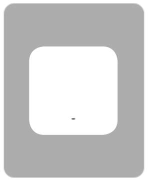
Revision	Date	Description
1.00	June 30, 2015	• Initial release for revision A1

Trademarks

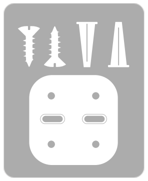
D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

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.

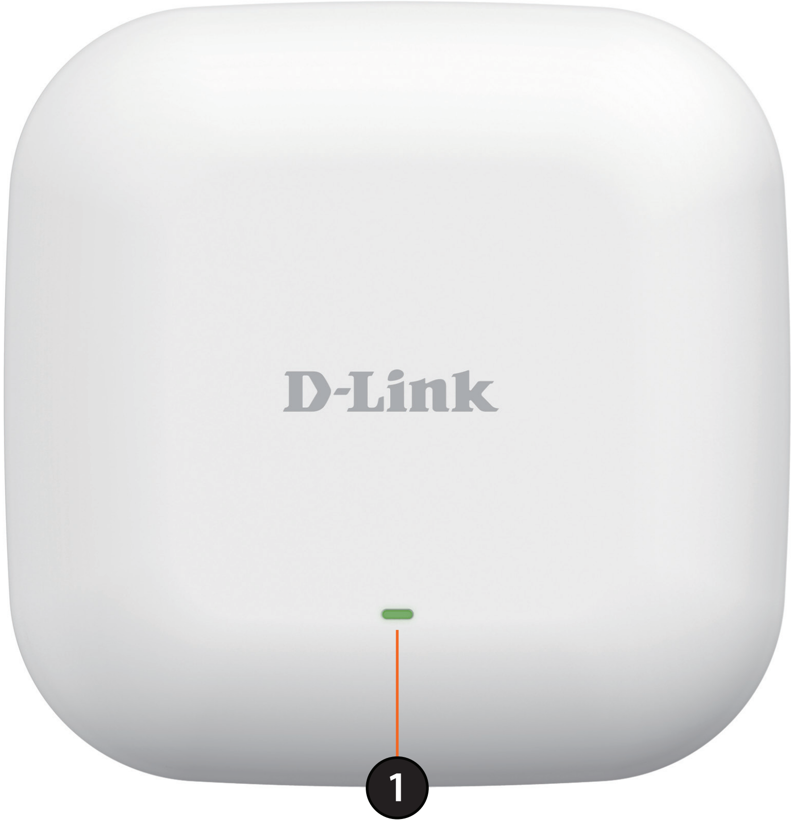
- **Central WiFiManager management software compatibility -** The real-time display of the network's topology and AP's information makes network configuration and management of multiple devices quick and simple.

- **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

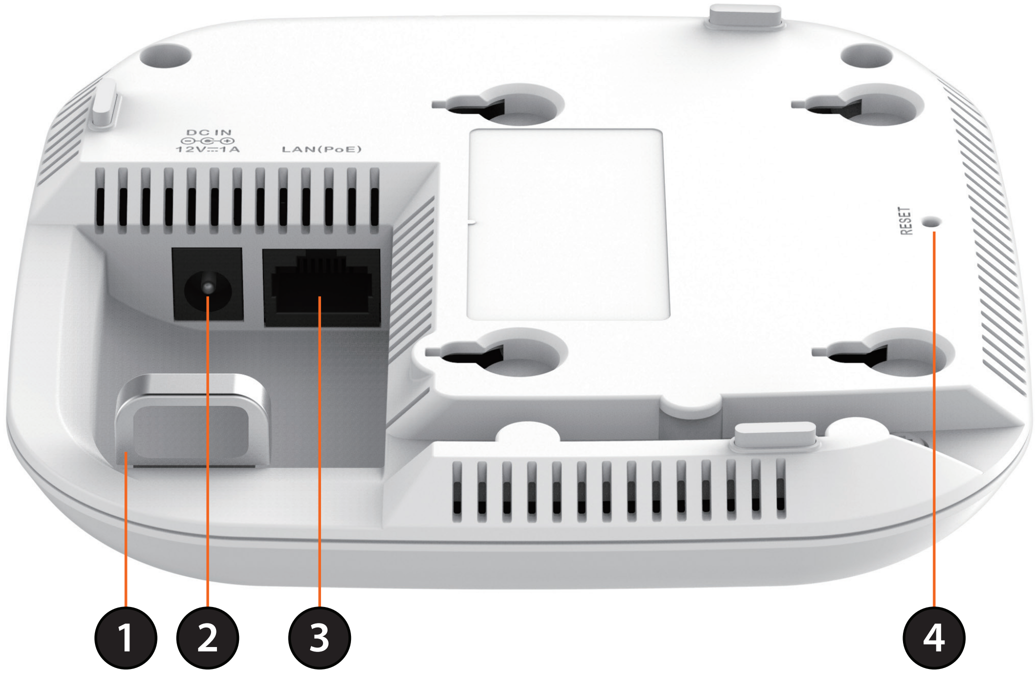
Top Panel



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:

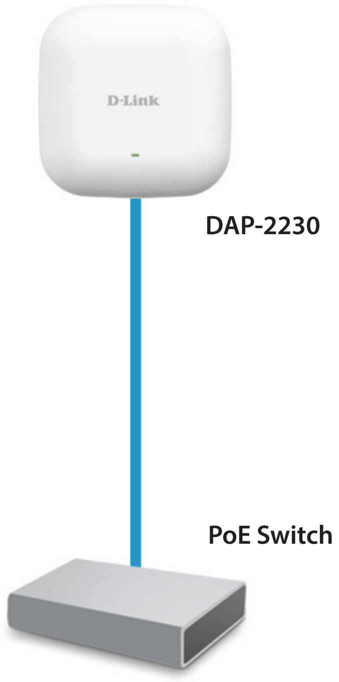
Method 1 - Powered by PoE Switch

Method 2 - Powered by PoE Injector

Method 3 - Powered by DC Adapter

Method 1 - Powered by PoE Switch

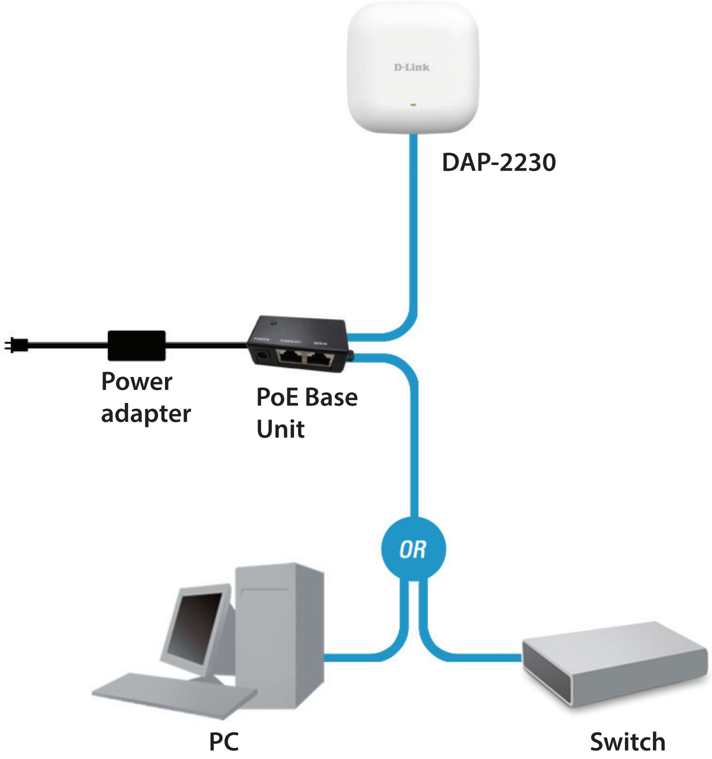
1. Connect one end of an Ethernet cable into the **LAN (PoE)** port on the DAP-2230 and then connect the other end to a PoE switch.



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.

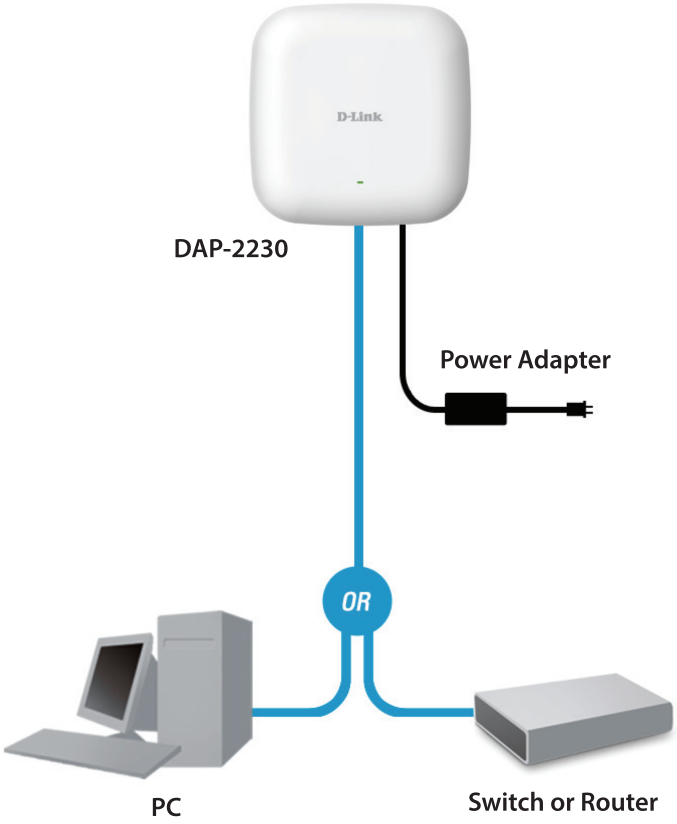
1. Connect one end of an Ethernet cable into the **DATA IN** port on the PoE injector and the other end into a port on a switch, router, or computer.
2. Connect one end of a different Ethernet cable into the **P+DATA OUT** port on the PoE injector and the other end into the **LAN (PoE)** port on the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

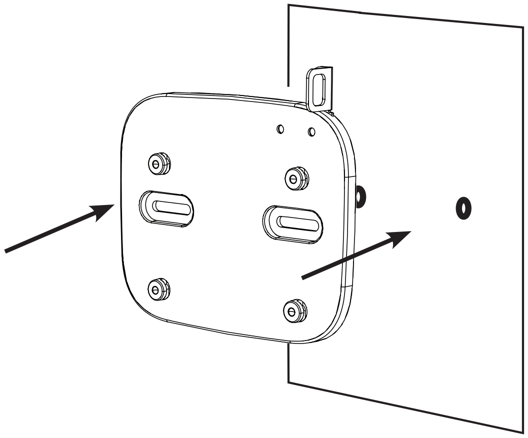
A power adapter is included with some DAP-2230 models.

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.

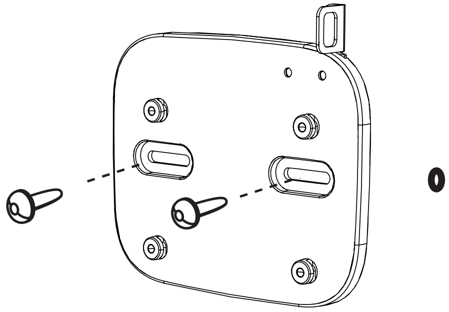


Mounting the AP

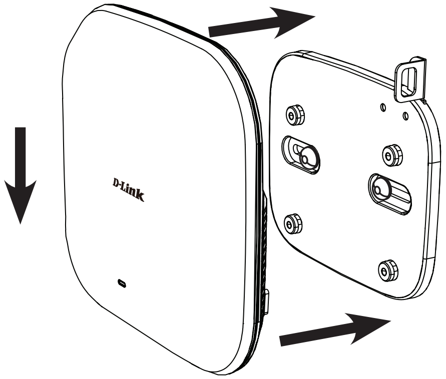
Place the mounting bracket on a wall or ceiling and mark holes where you will insert the screws with a marker. Drill holes in the marked points and insert the plastic wall anchors.



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

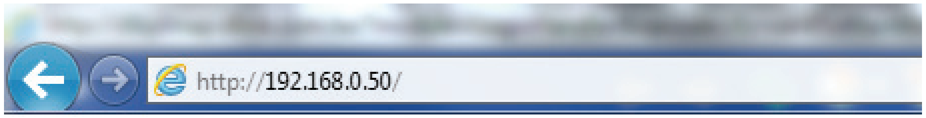
Operation Mode **(Only supports 1 mode at a time)**	**Function**
Access Point (AP)	Create a wireless LAN
WDS with AP	Wirelessly connect multiple networks while still functioning as a wireless AP
WDS	Wirelessly connect multiple networks
Wireless Client	AP acts as a wireless network adapter for your Ethernet-enabled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

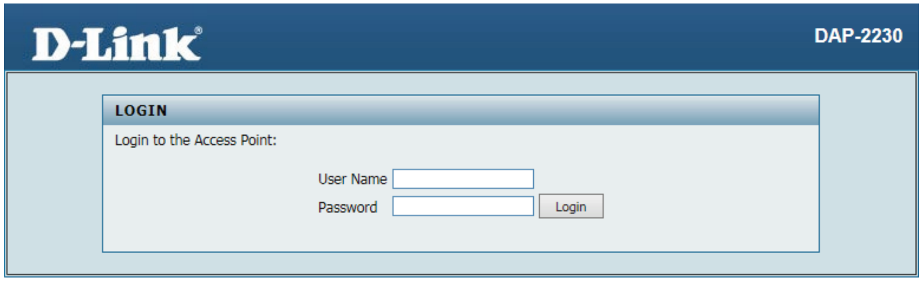
Web-based Configuration Utility

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/

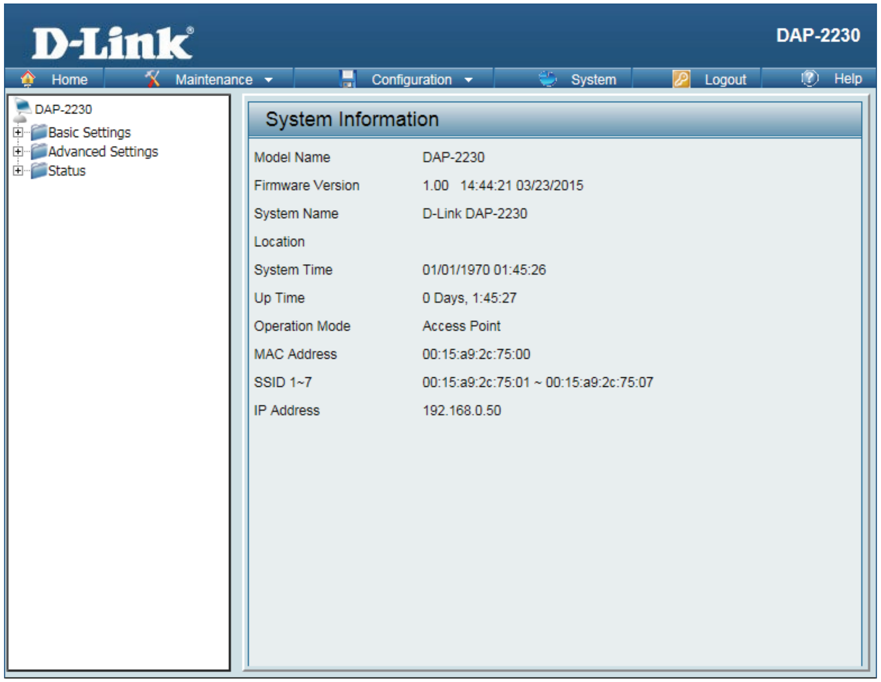
To access the configuration utility, open a web browser such as Internet Explorer and enter **http://192.168.0.50**



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:



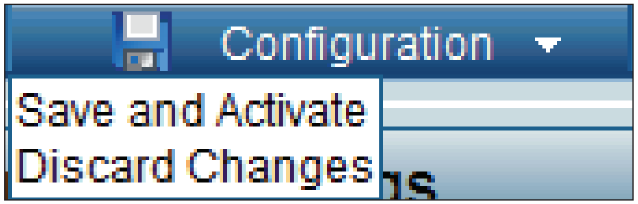
System Information

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.

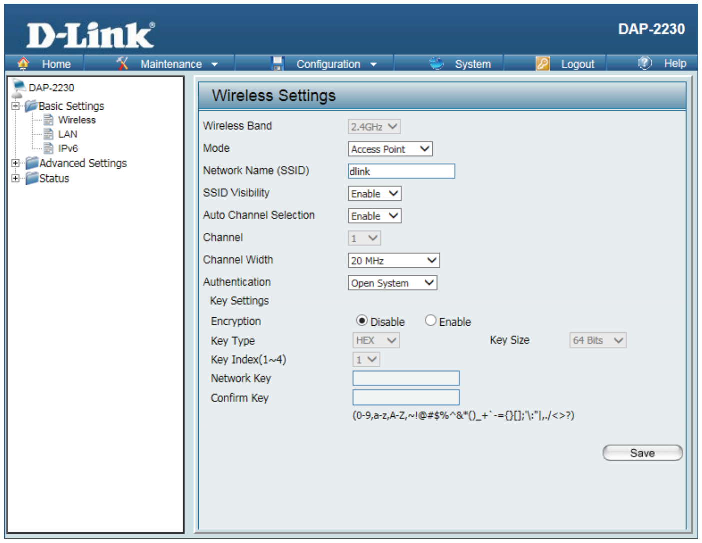
You may change settings to multiple pages before activating. Once you are finished, click the **Configuration** button located at the top of the page and then click **Save and Activate**.



Basic Settings

Wireless

Access Point mode



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

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.

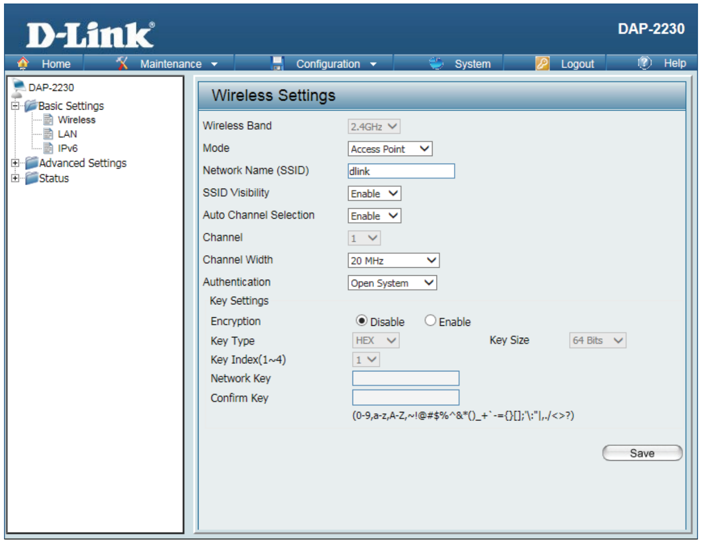
SSID Visibility: **Enable** or **Disable** SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users. This feature is enabled by default.

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.



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

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.

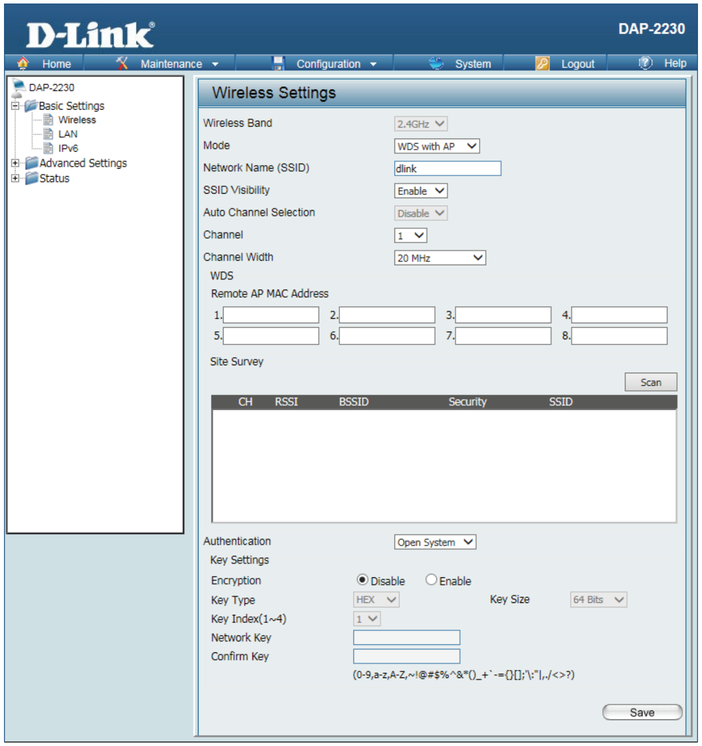
Select **WPA-Personal** to secure your network using a password and dynamic key changes. No RADIUS server is required.

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.

WDS with AP mode

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



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

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.

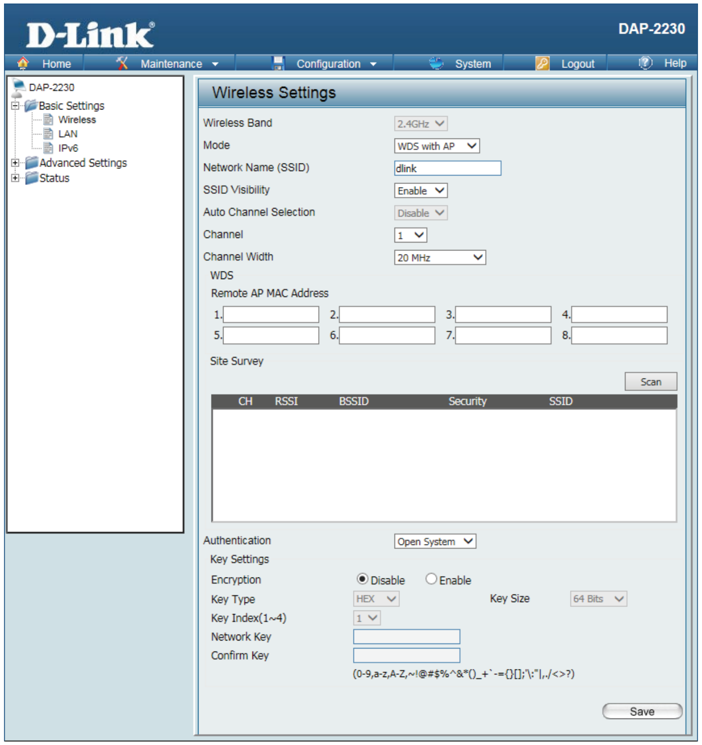
Remote AP MAC Address: Enter the MAC addresses of the APs on your network that will serve as bridges to wirelessly connect multiple networks.

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.

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

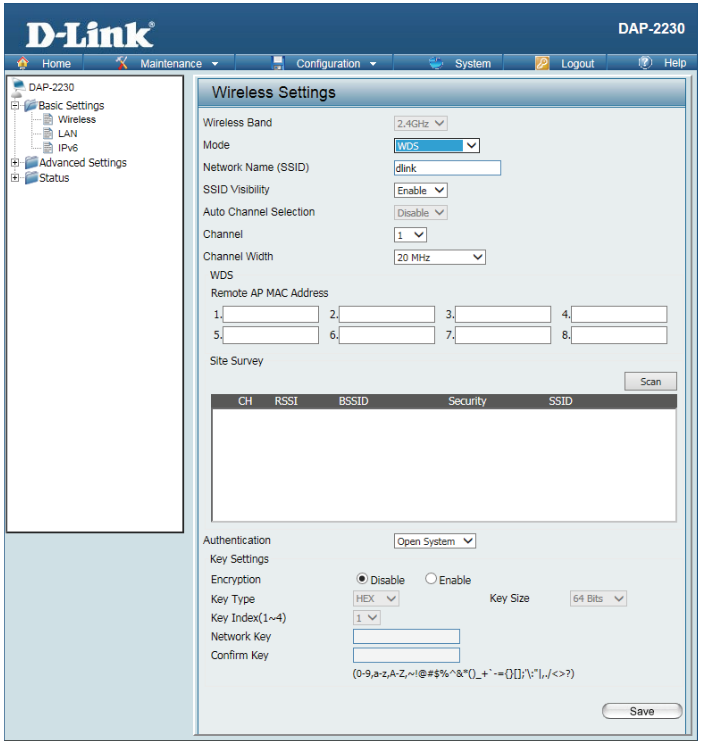
Key Settings

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.

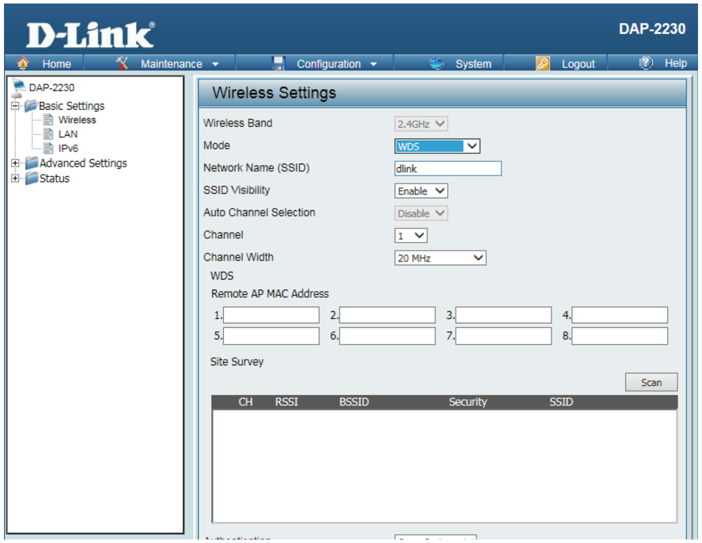
Remote AP MAC Address: Enter the MAC addresses of the APs on your network that will serve as bridges to wirelessly connect multiple networks.

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.

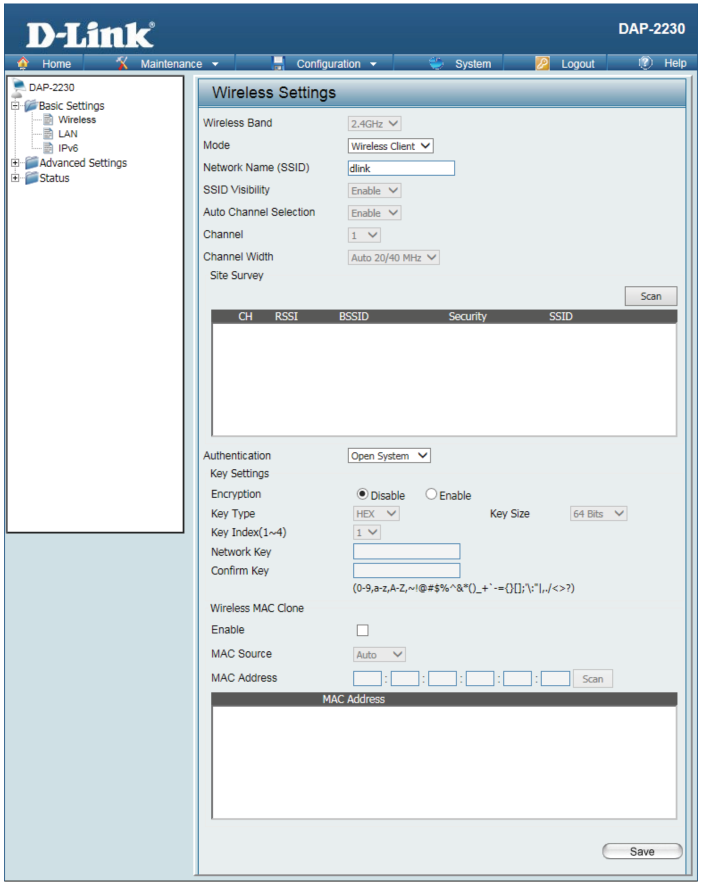
SSID Visibility: **Enable** or **Disable** SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users. Disabling SSID is not supported in Wireless Client mode.

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

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

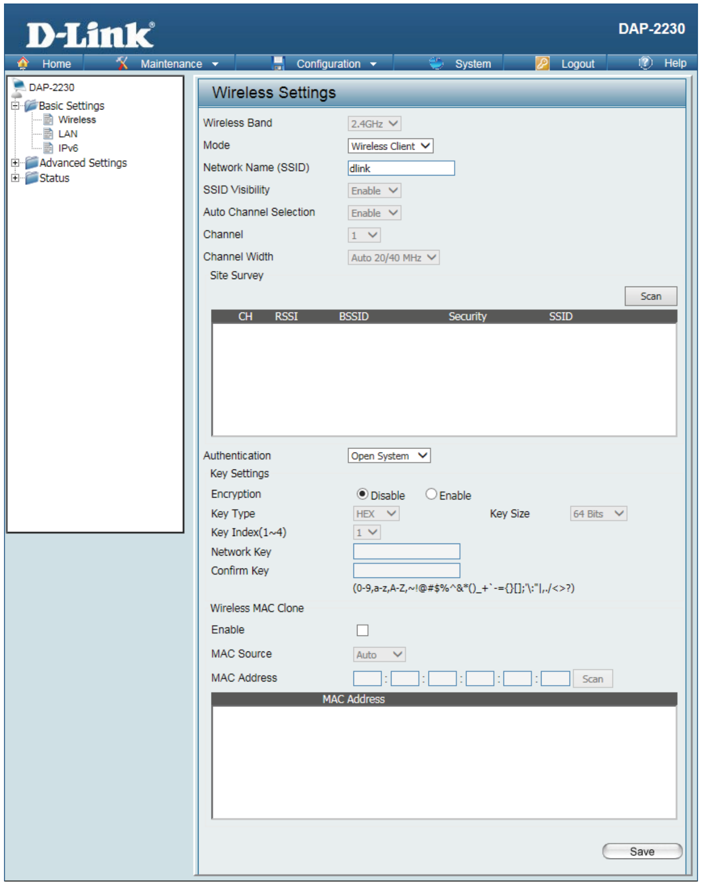
Select **Open System** to communicate the key across the network.

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

Scan

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	: : : : : Scan		

MAC Address

Save

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****.

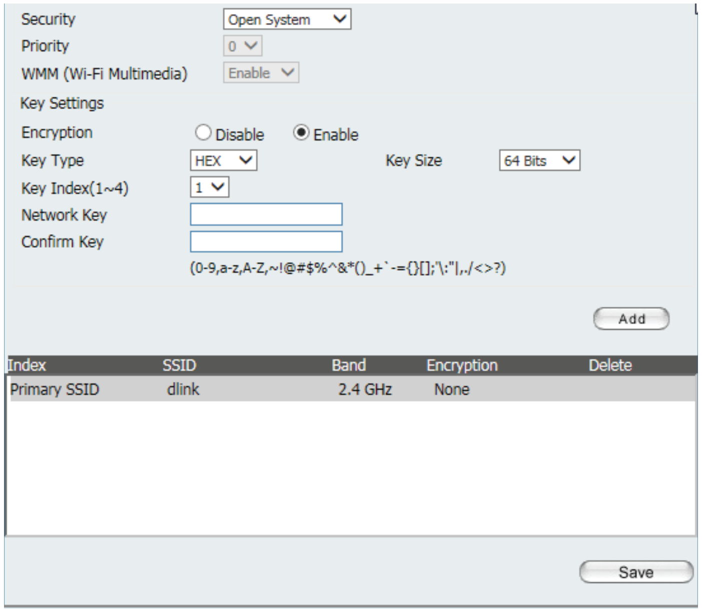
Key Size: Select **64 Bits** or **128 Bits**.

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.*

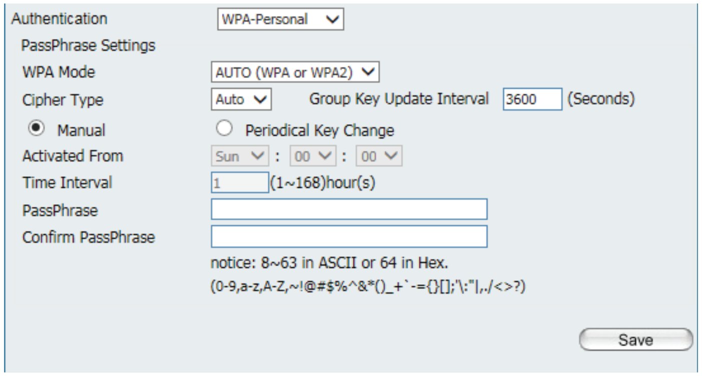


Security	Open System		
Priority	0		
WMM (Wi-Fi Multimedia)	Enable		
Key Settings			
Encryption	○ Disable ● Enable		
Key Type	HEX	Key Size	64 Bits
Key Index(1~4)	1		
Network Key			
Confirm Key			
	(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];'\:"|,./<>?)		

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**.

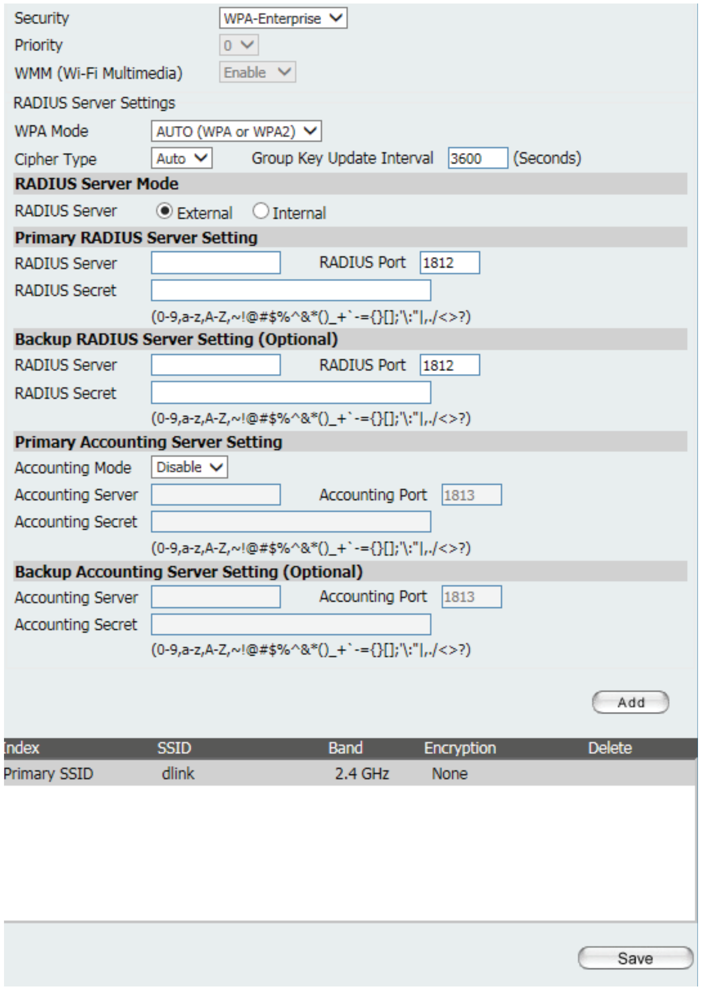
Group Key Update Interval: Select the interval during which the group key will be valid. The recommended value is **3600.** A lower interval may reduce data transfer rates.

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

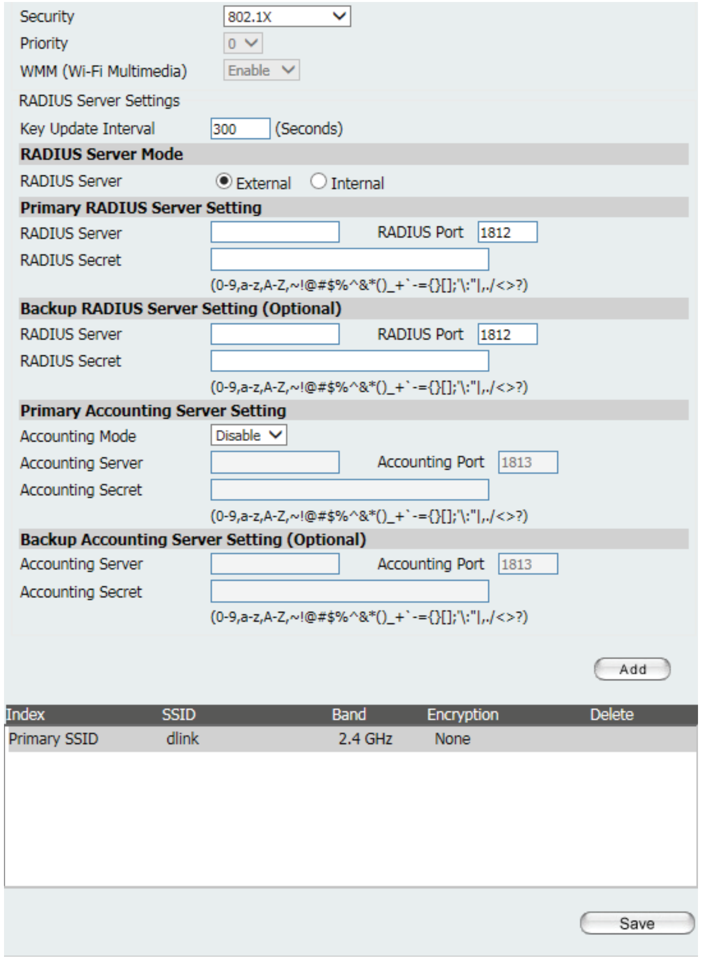
802.1x Authentication can only be enabled for **Access Point** mode.

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.

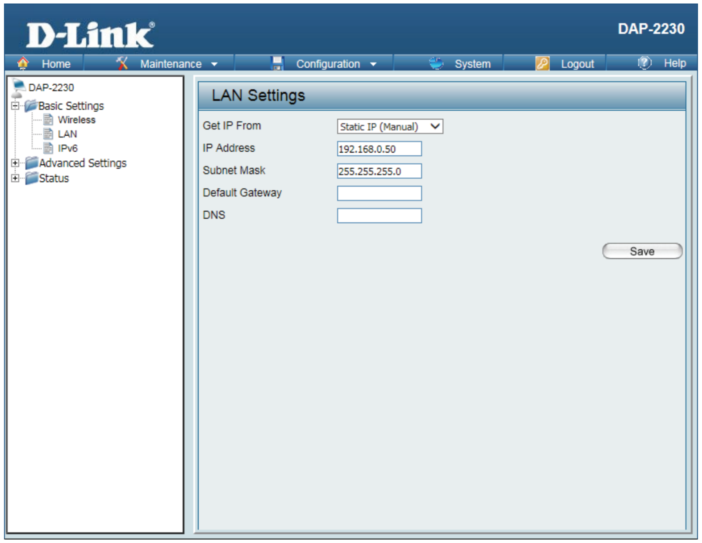
Get IP From: **Static IP (Manual)** is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2230. When **Dynamic IP (DHCP)** is selected, the other fields here will be grayed out. Please allow about two minutes for the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

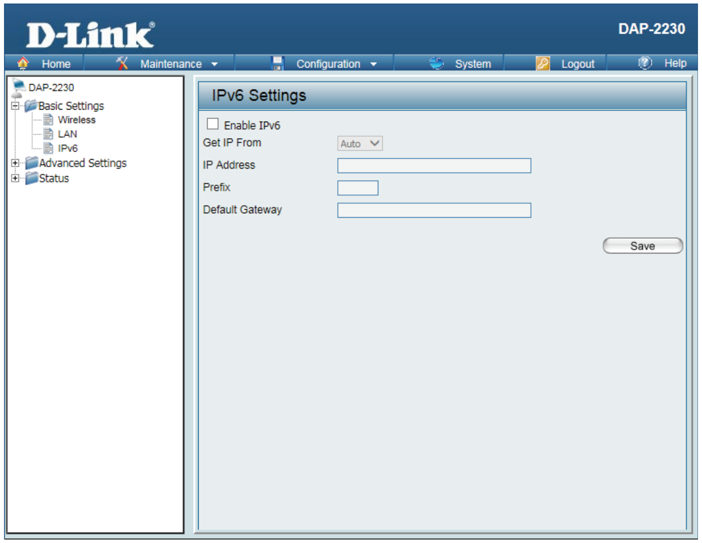
Enable IPv6: Check to enable the IPv6.

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

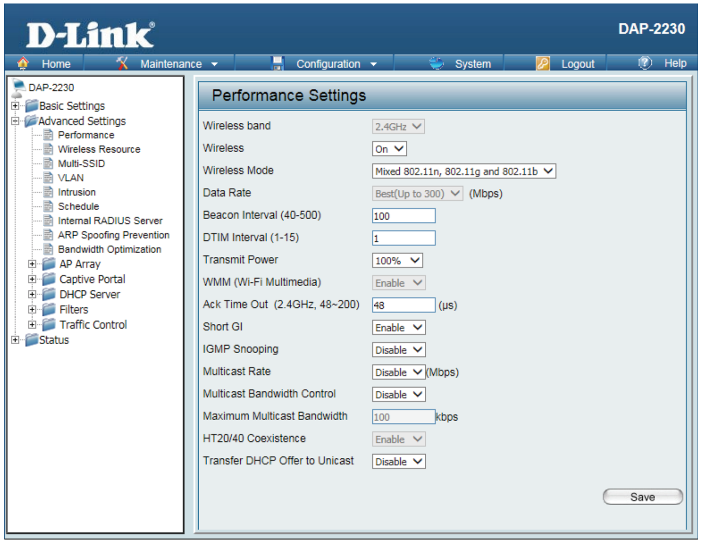
IP Address

Prefix

Default Gateway

Advanced Settings

Performance



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

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.

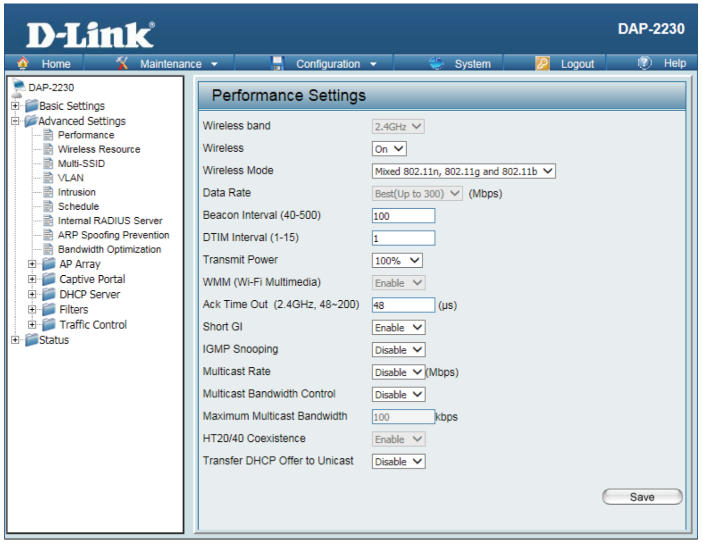
Data Rate*: Indicate the base transfer rate of wireless adapters on the wireless LAN. The AP will adjust the base transfer rate depending on the base rate of the connected device. If there are obstacles or interference, the AP will step down the rate. This option is enabled in **Mixed 802.11g and 802.11b** 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.



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.

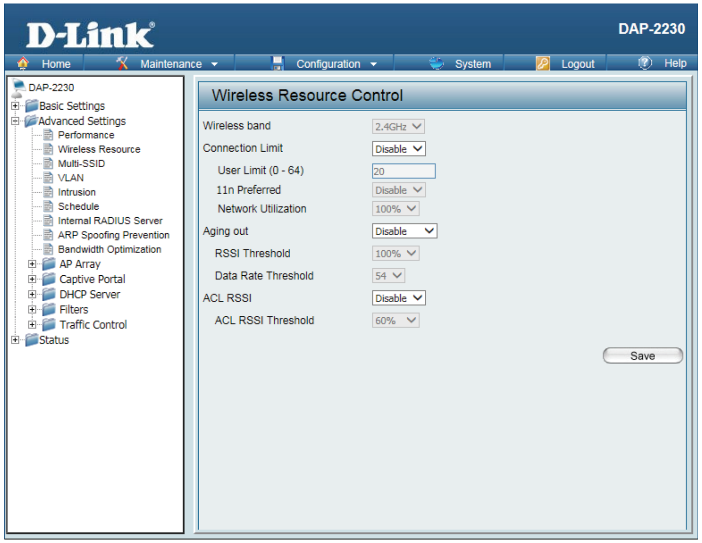
Maximum Multicast Bandwidth : Set the multicast packets maximum bandwidth pass through rate from the Ethernet interface to the Access Point.

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.

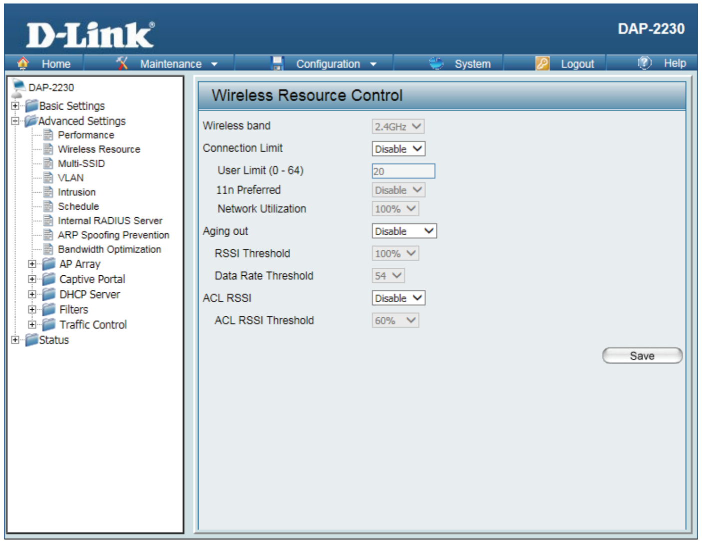
Aging out: Use the drop-down menu to select the criteria of disconnecting the wireless clients. Available options are **RSSI** and **Data Rate**.

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.

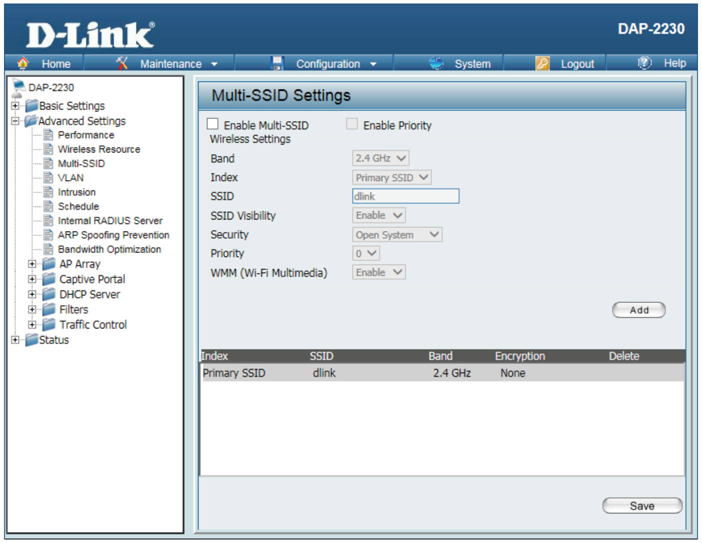


Wireless Resource Control

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**.

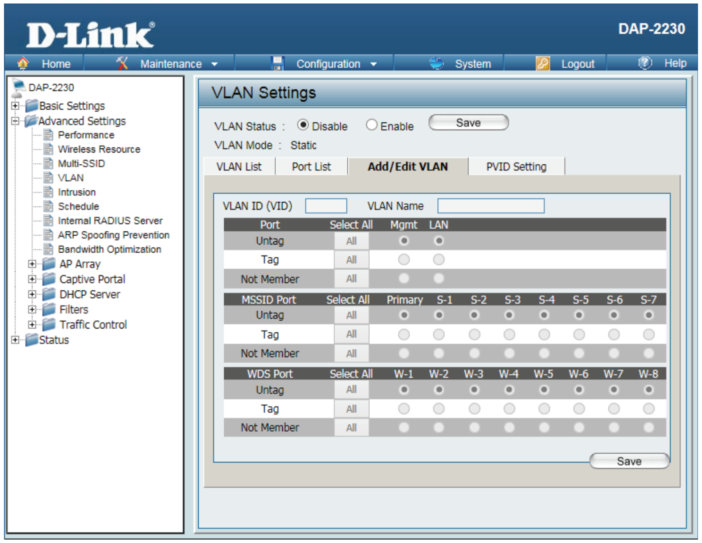
VLAN

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.

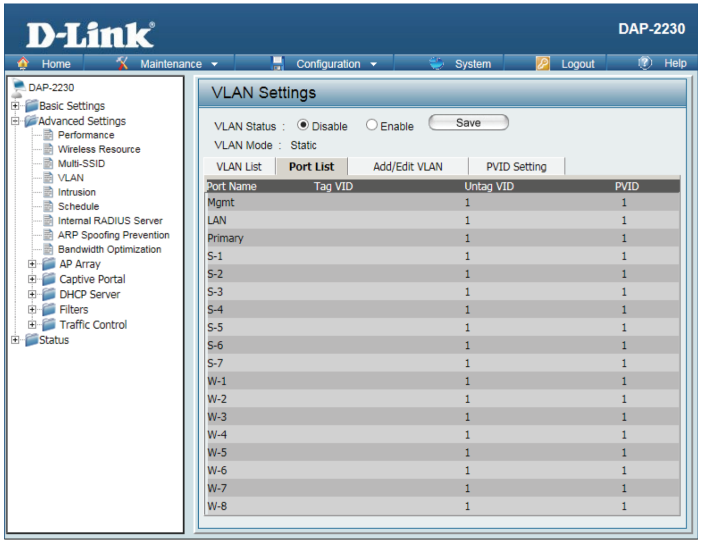
VLAN Status: Use the radio button to toggle to Enable. Next, go to the **Add/Edit VLAN** tab to add or modify an item on the **VLAN List** tab.

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

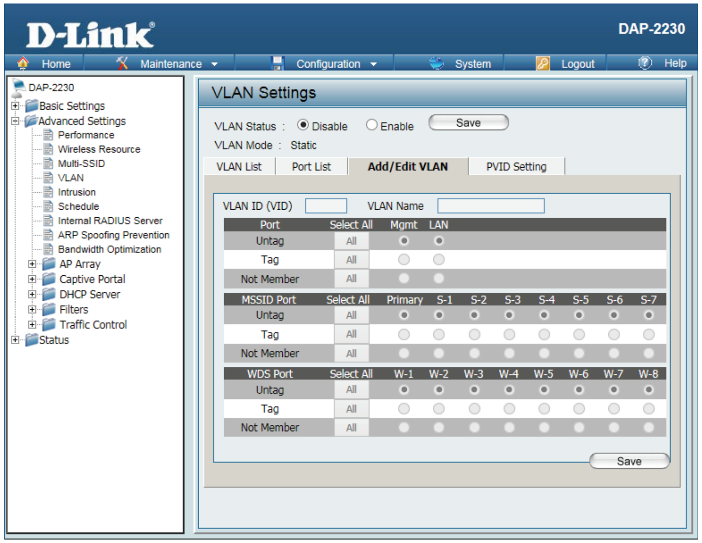
Add/Edit VLAN

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

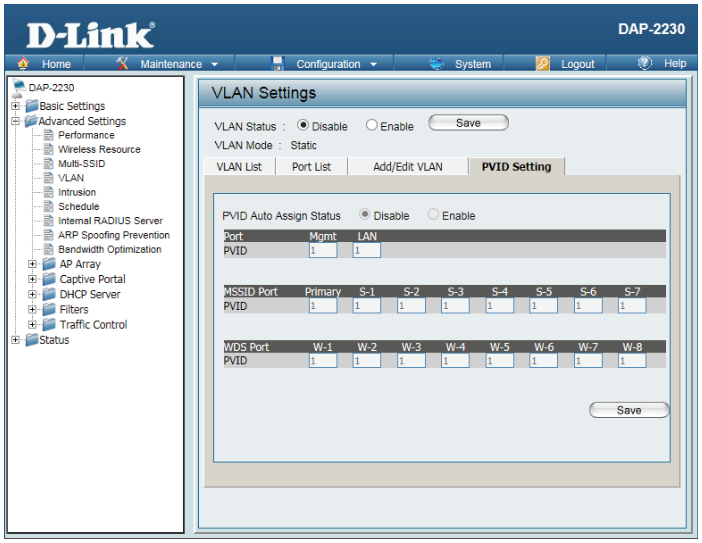
Port	Select All	Mgmt	LAN
Untag	All	●	●
Tag	All	○	○
Not Member	All	○	○

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 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

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

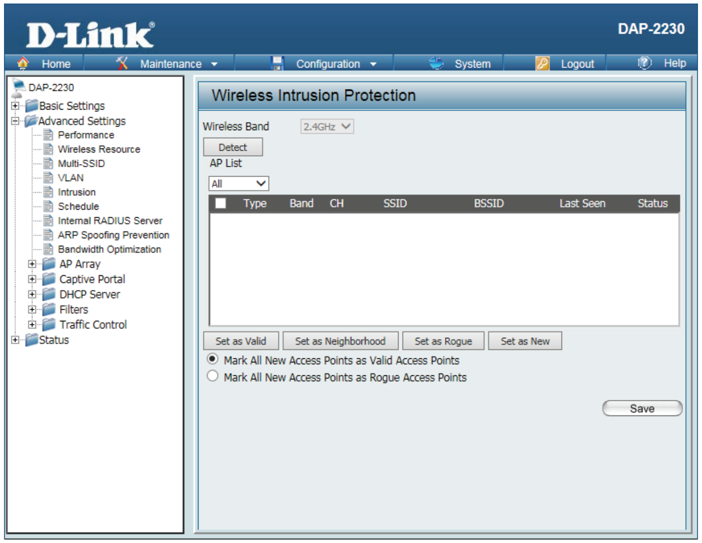
PVID Auto Assign Status: Use the radio button to toggle PVID auto assign status to Enable.

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.



Wireless Intrusion Protection

Wireless Band: 2.4GHz

AP List: All

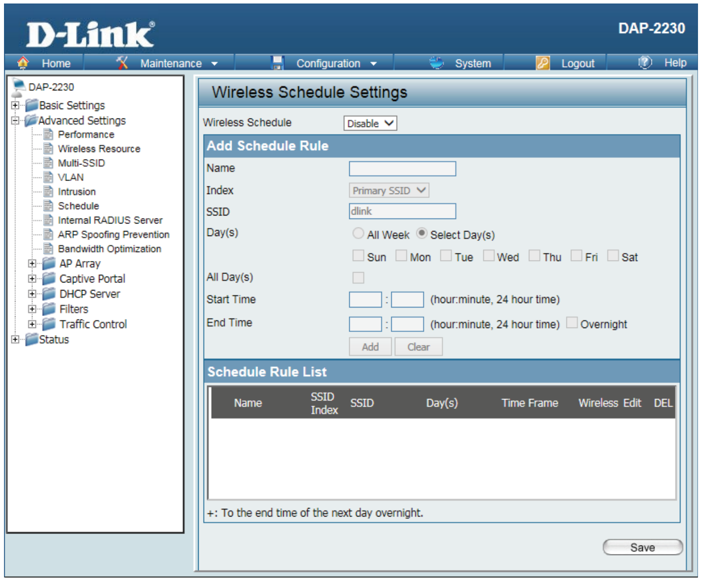
□	Type	Band	CH	SSID	BSSID	Last Seen	Status

● 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

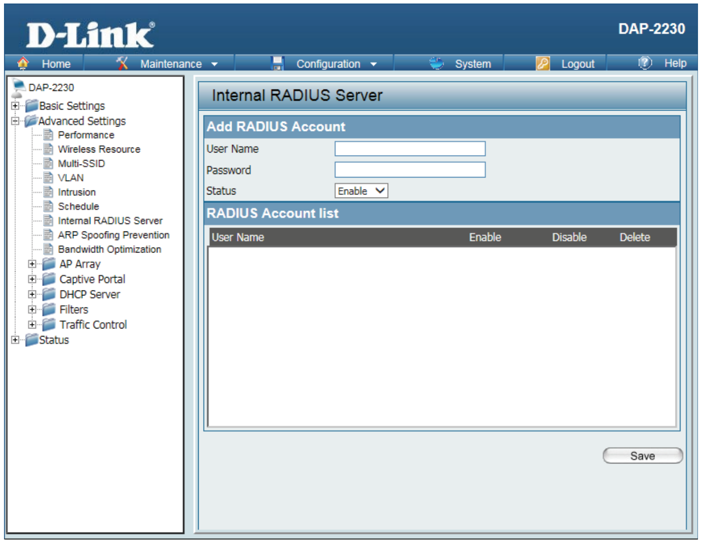
The DAP-2230 features a built-in RADIUS server. Once you have finished adding a RADIUS account, click the **Save** button to have your changes take effect. The newly-created account will appear in this RADIUS Account List. The radio buttons allow the user to enable or disable the RADIUS account. Click 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

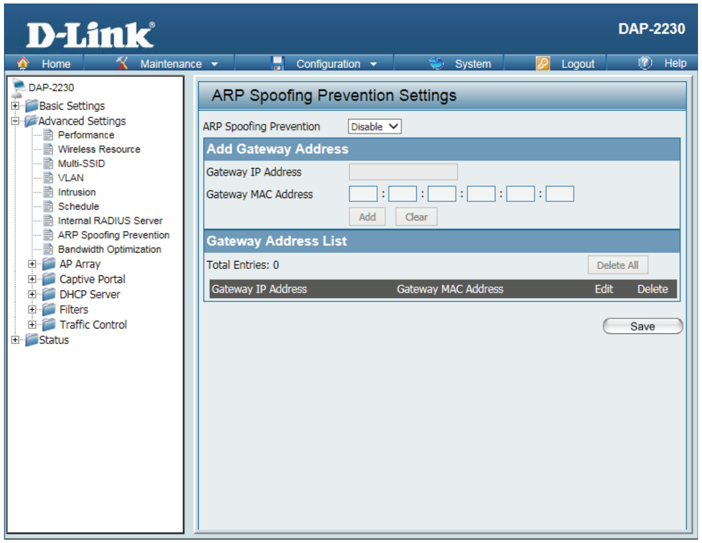
ARP Spoofing Prevention Settings

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 : : : : :

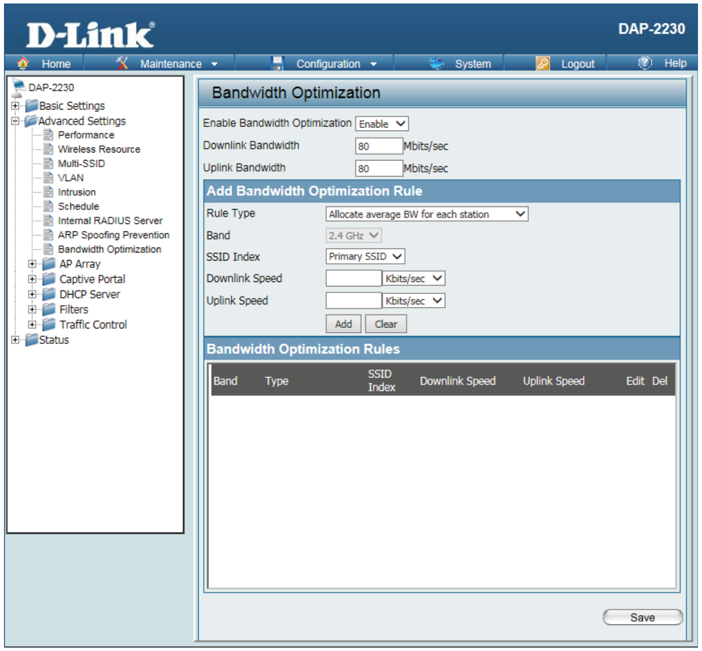
Gateway Address List

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.

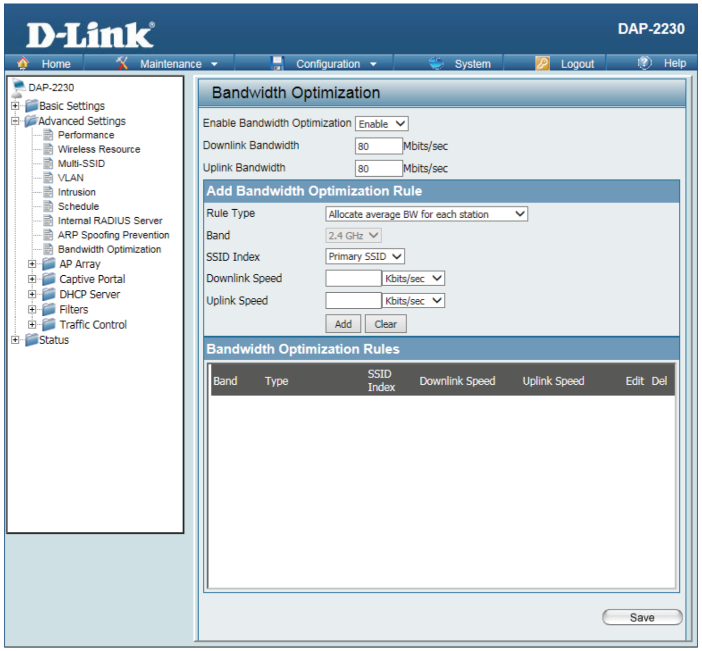
Allocate specific BW for SSID: All clients share the total bandwidth.

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.

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.

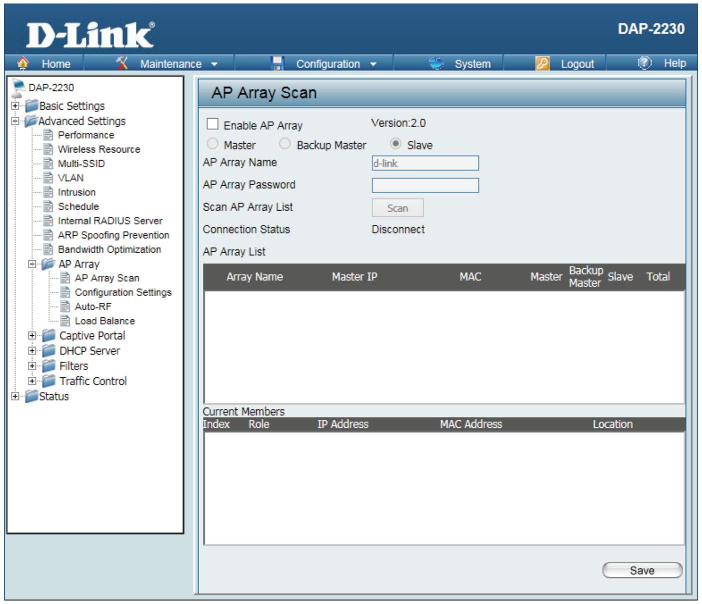
AP Array Password: Enter an AP array password for the group here. This password must be the same on all the APs in the group.

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.



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

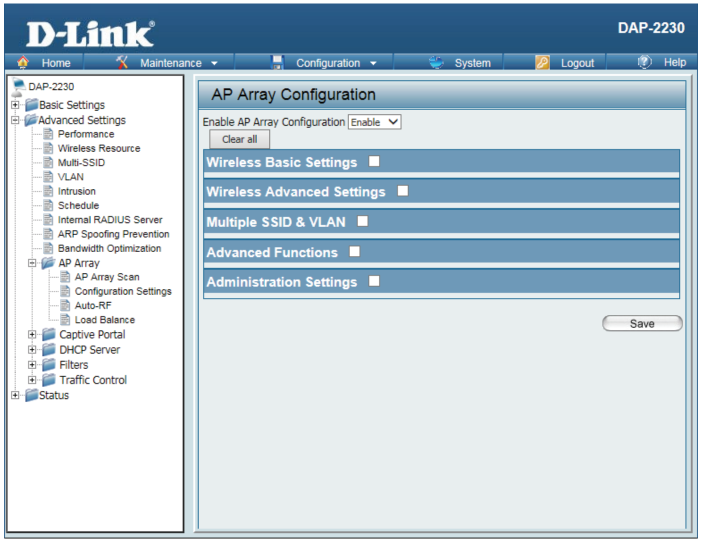
Array Name	Master IP	MAC	Master	Backup Master	Slave	Total

Current Members

Index	Role	IP Address	MAC Address	Location

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.



AP Array Configuration

Enable AP Array Configuration: Enable

Wireless Basic Settings □

Wireless Advanced Settings □

Multiple SSID & VLAN □

Advanced Functions □

Administration Settings □

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.

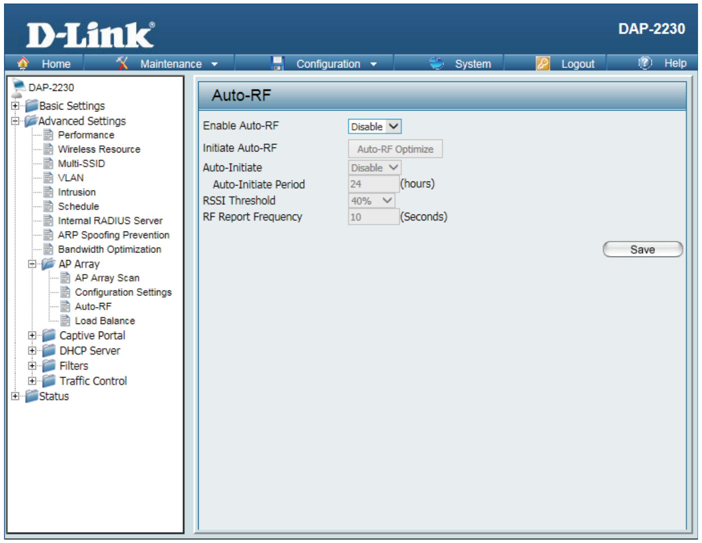
Multiple SSID & VLAN: Select this option to specify the multiple SSIDs and VLAN settings that the APs in the group will inherit.

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 Auto-RF: Disable
Initiate Auto-RF
Auto-Initiate: Disable
Auto-Initiate Period: 24 (hours)
RSSI Threshold: 40%
RF Report Frequency: 10 (Seconds)

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.

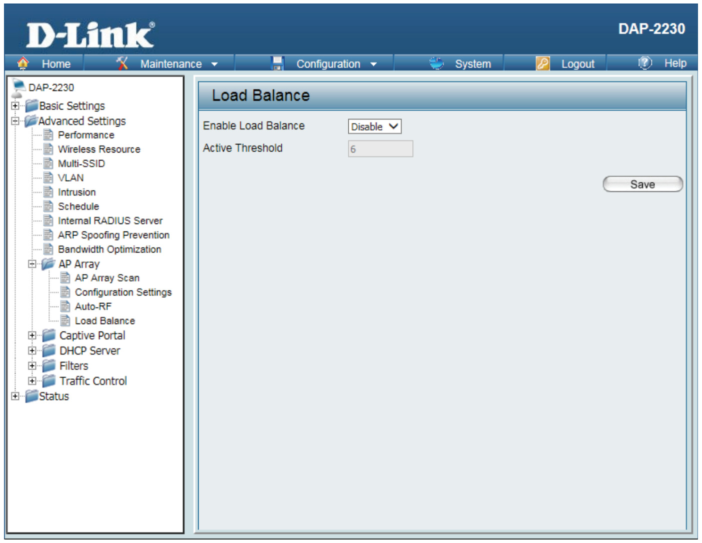
Auto-Initiate Period: After enabling the auto-initiate option, the auto-initiate period value can be entered here. This value must be between 1 and 24 hours.

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.

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.



Load Balance

Enable Load Balance: Disable

Active Threshold: 6

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.

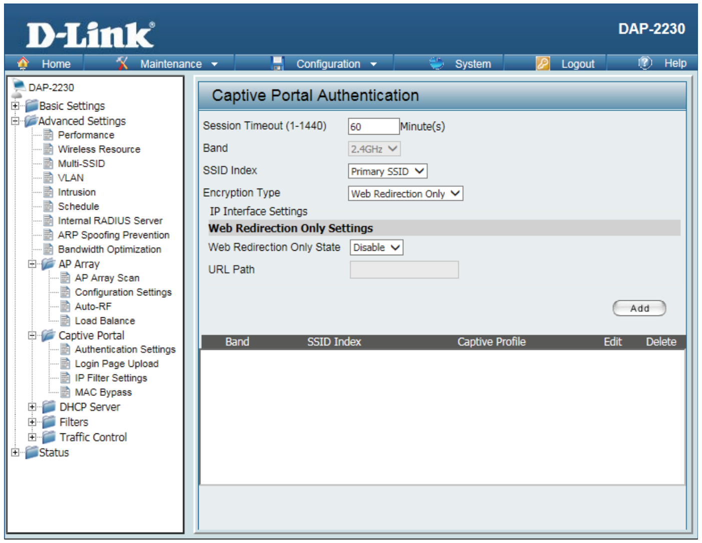
Band: Select 2.4 Ghz.

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.



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.

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.

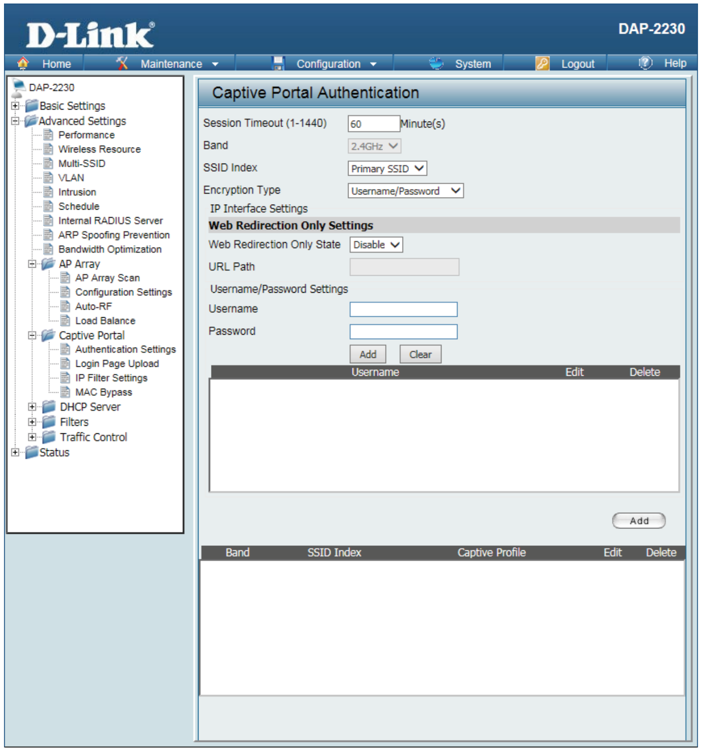
Authentication Type: Select the captive portal encryption type here. Options to choose from are **Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP** and **POP3.**

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.



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:

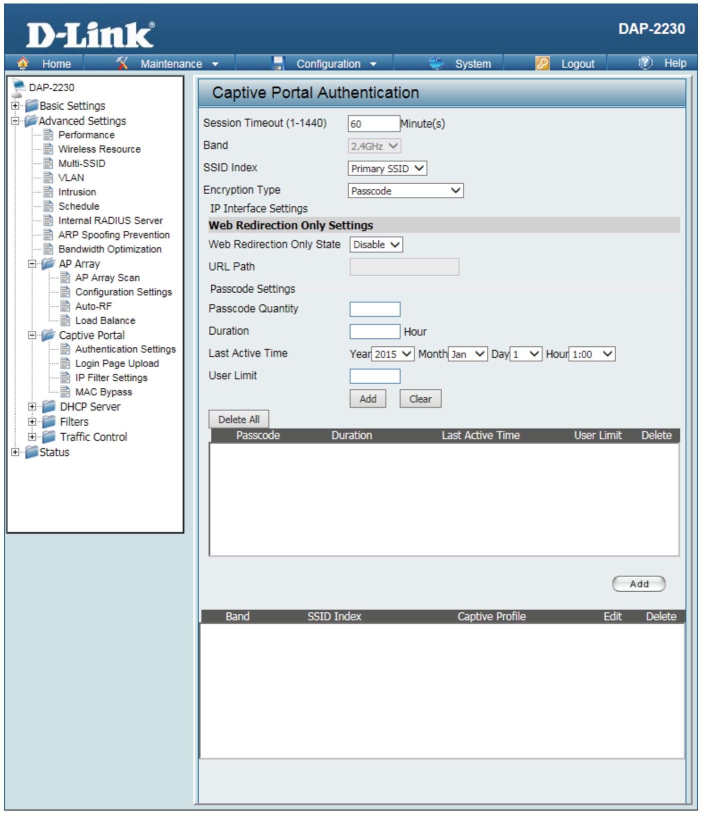
Password:

Username	Edit	Delete

Band	SSID Index	Captive Profile	Edit	Delete

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.

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.

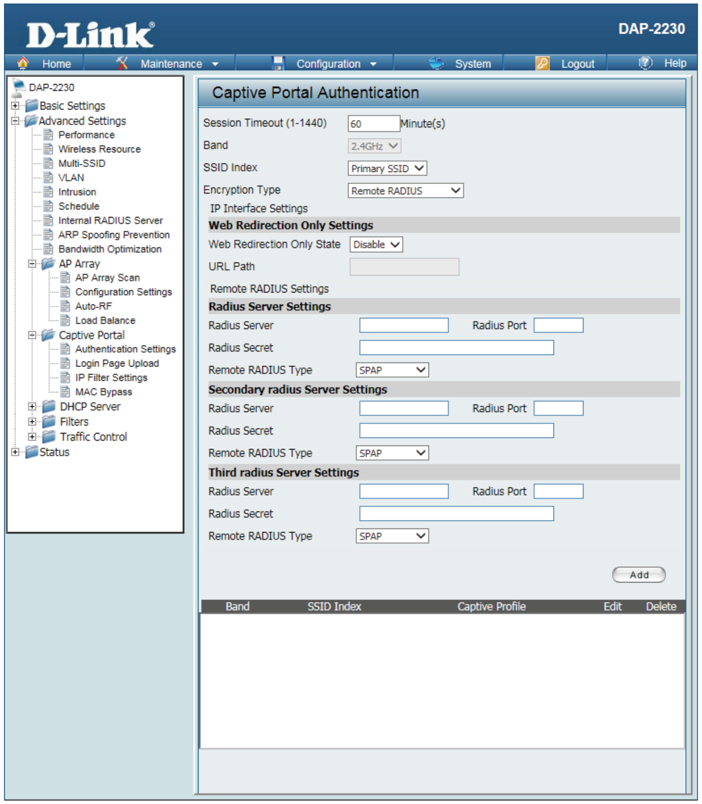
URL Path : Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.

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.



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

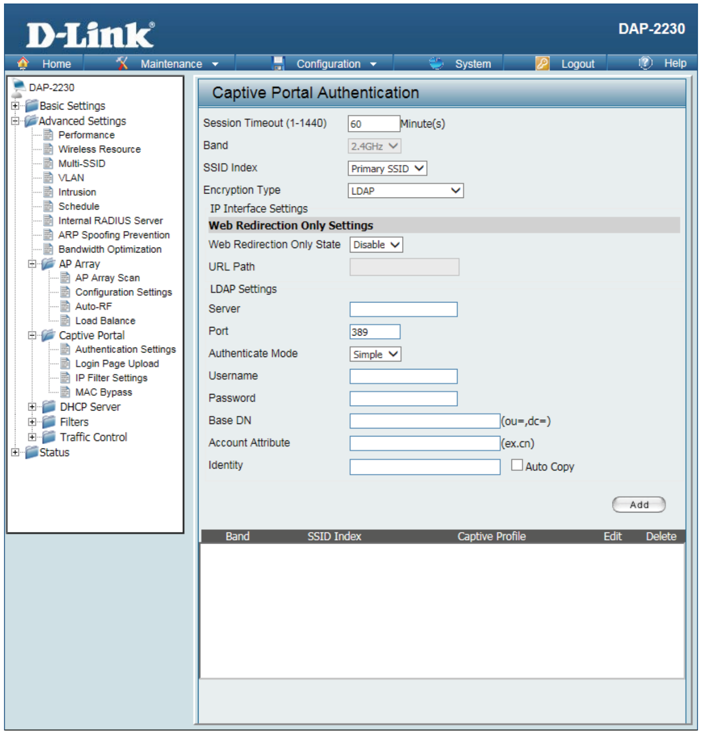
Secondary radius Server Settings
Radius Server Radius Port
Radius Secret
Remote RADIUS Type SPAP

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

Band	SSID Index	Captive Profile	Edit	Delete

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.

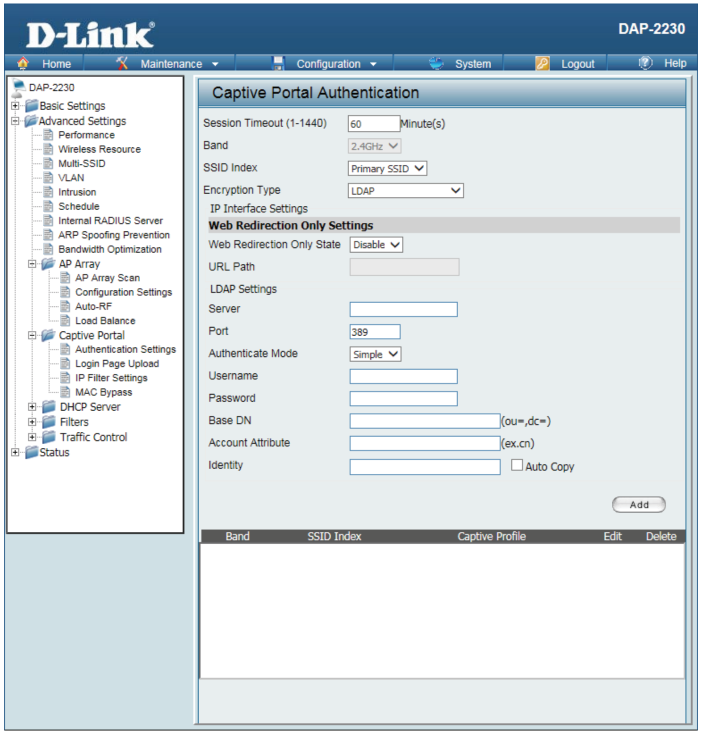
Password: Enter the LDAP server account's password here.

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	

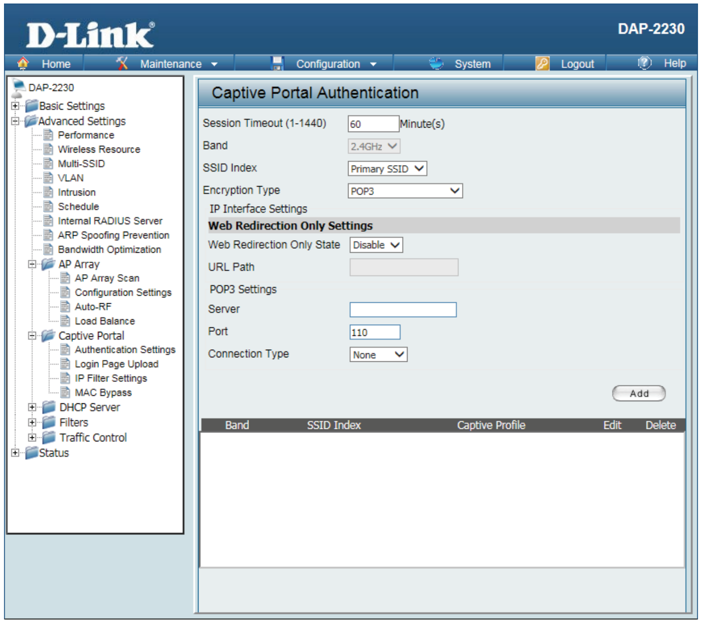
LDAP Settings

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.

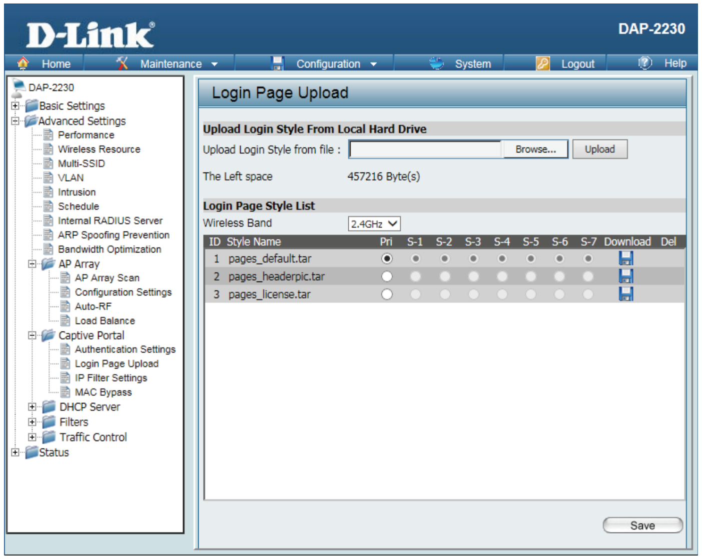
Connection Type: Select the connection type here; either None or SSL/TLS.

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 :

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.

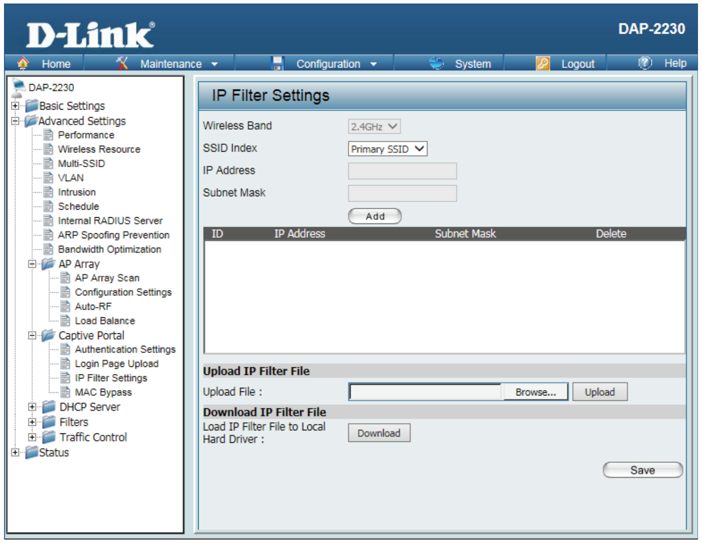
Wireless Band: Select the wireless band for MAC Bypass.

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

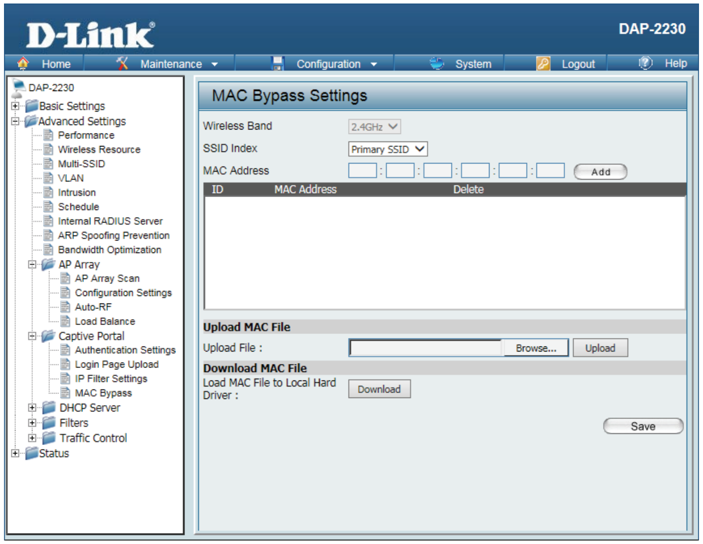
Upload File :

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.

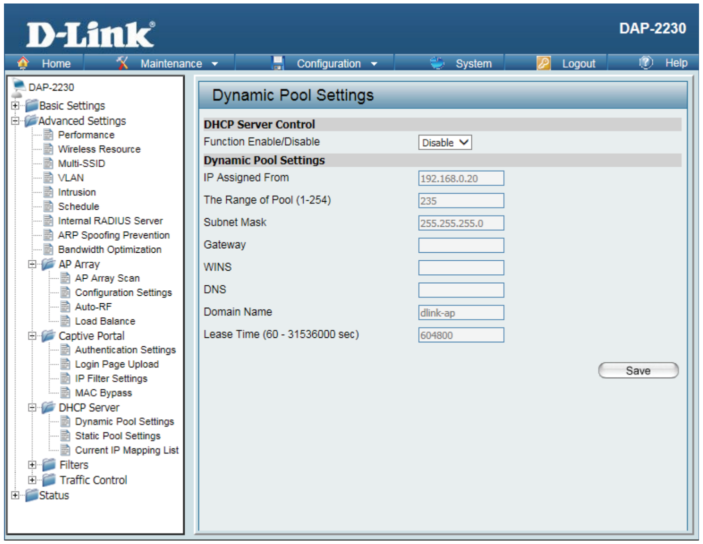
Upload File: To upload a MAC bypass list file, click Browse and navigate to the MAC bypass list file saved on the managing computer, and then click Upload.

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.



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

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)

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.

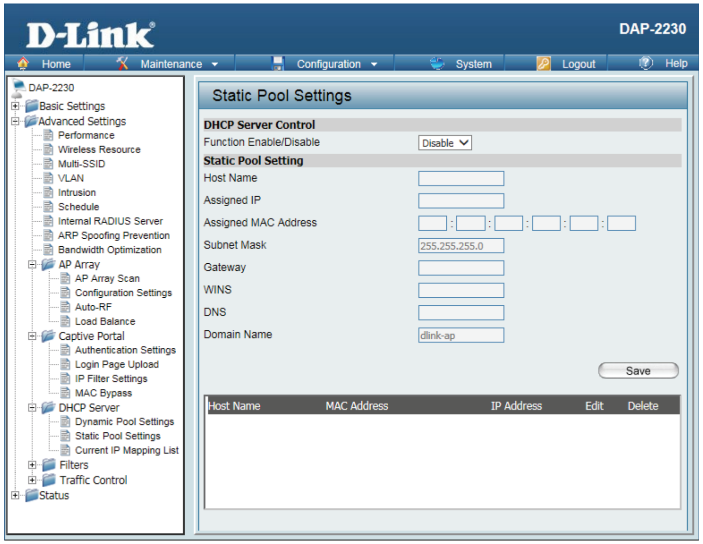
Subnet Mask: Define the submask of the IP address specified in the **IP Assigned From** field.

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.



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:

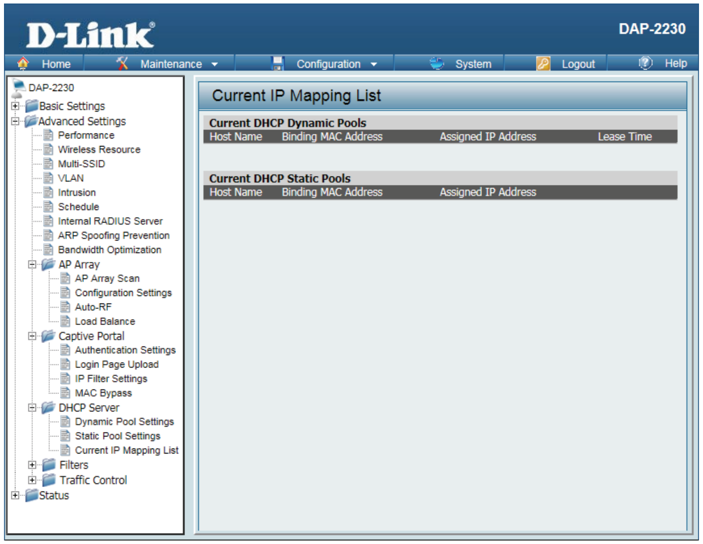
DNS:

Domain Name: dlink-ap

Host Name	MAC Address	IP Address	Edit	Delete

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.

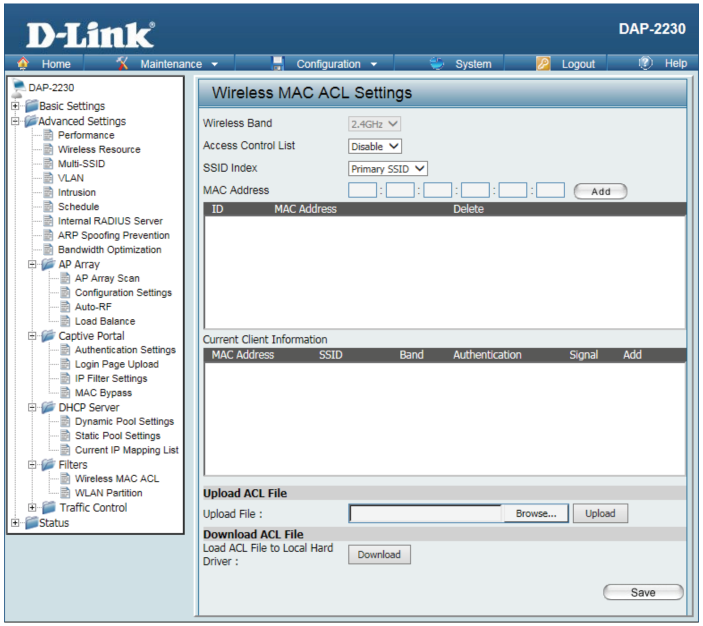
MAC Address List: Select **Reject** to reject the devices with MAC addresses on the Access Control List. All other devices not on the list will be accepted.

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: __ : __ : __ : __ : __ : __

ID	MAC Address	Delete

Current Client Information

MAC Address	SSID	Band	Authentication	Signal	Add

Upload ACL File

Upload File :

Download ACL File

Load ACL File to Local Hard Driver :

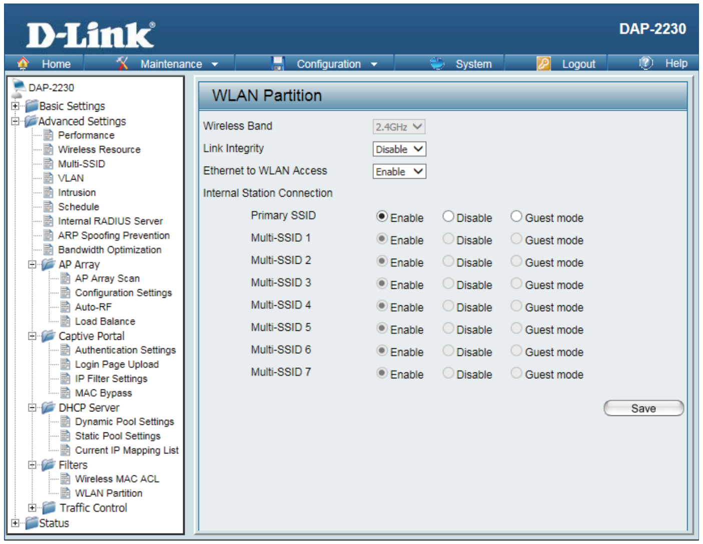
WLAN Partition

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

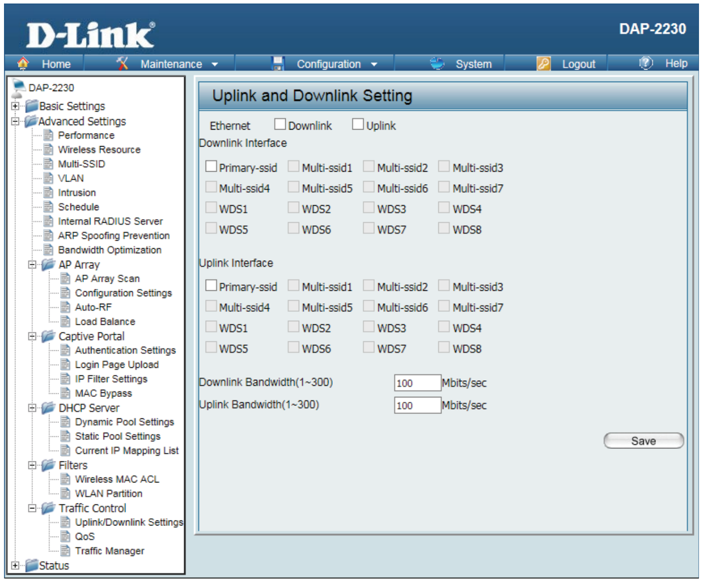
Traffic Control

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

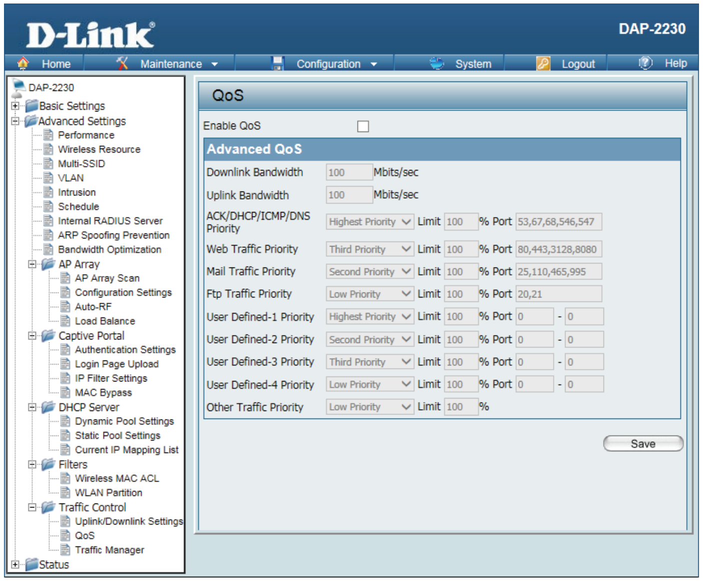
QoS

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	%			

Traffic Manager

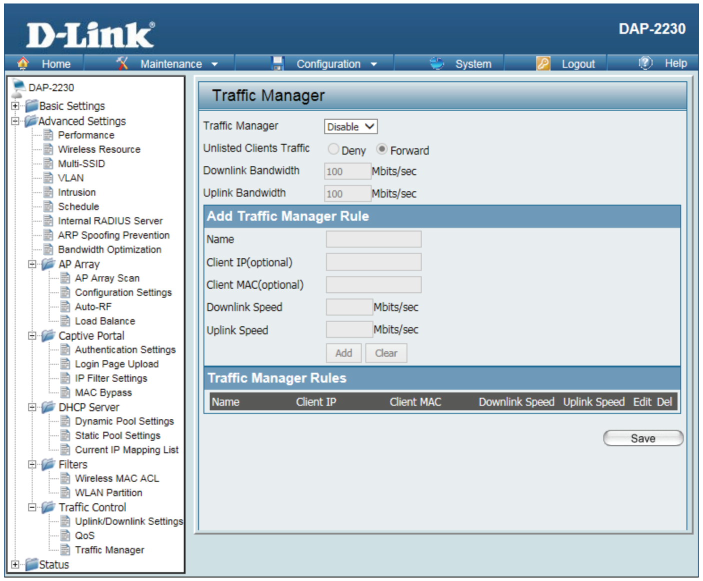
The traffic manager feature allows users to create traffic management rules that specify how to deal with listed client traffic and specify downlink/uplink speed for new traffic manager rules. Click the **Save** button to let your changes take effect.

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

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

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

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



Traffic Manager

Traffic Manager: Disable

Unlisted Clients Traffic: ○ Deny ● Forward

Downlink Bandwidth: 100 Mbits/sec

Uplink Bandwidth: 100 Mbits/sec

Add Traffic Manager Rule

Name:

Client IP(optional):

Client MAC(optional):

Downlink Speed: Mbits/sec

Uplink Speed: Mbits/sec

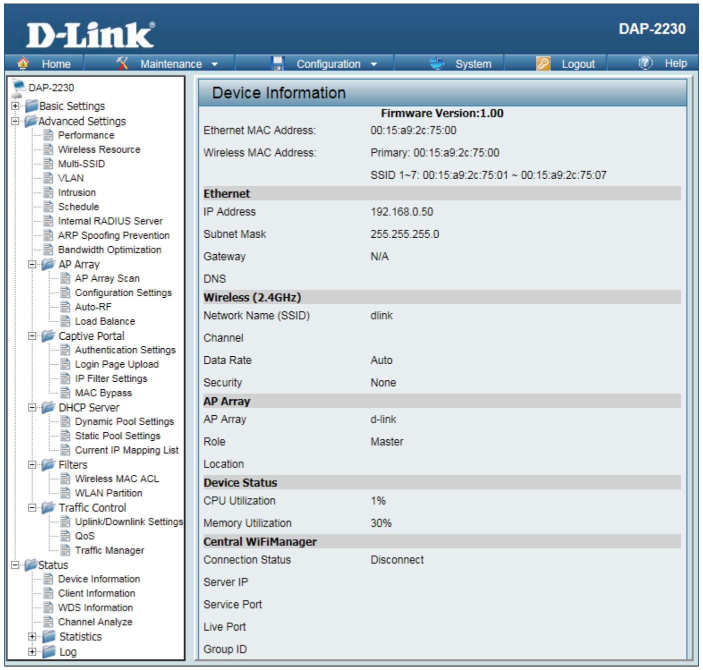
Traffic Manager Rules

Name	Client IP	Client MAC	Downlink Speed	Uplink Speed	Edit	Del

Status

Device Information

This read-only window displays the configuration settings of the DAP-2230, including the firmware version and the device's MAC address.



Device Information

Firmware Version:1.00

Ethernet MAC Address:	00:15:a9:2c:75:00
Wireless MAC Address:	Primary: 00:15:a9:2c:75:00
	SSID 1~7: 00:15:a9:2c:75:01 ~ 00:15:a9:2c:75:07
Ethernet	
IP Address	192.168.0.50
Subnet Mask	255.255.255.0
Gateway	N/A
DNS	
Wireless (2.4GHz)	
Network Name (SSID)	dlink
Channel	
Data Rate	Auto
Security	None
AP Array	
AP Array	d-link
Role	Master
Location	
Device Status	
CPU Utilization	1%
Memory Utilization	30%
Central WiFiManager	
Connection Status	Disconnect
Server IP	
Service Port	
Live Port	
Group ID	

Client Information

This window displays the wireless client information for clients currently connected to the DAP-2230. The following information is available for each client communicating with the DAP-2230.

SSID: Displays the SSID of the client.

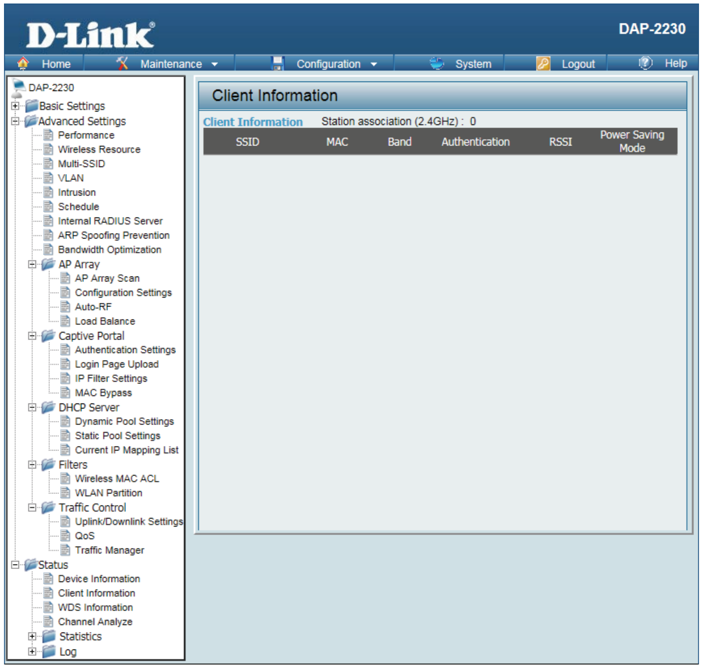
MAC: Displays the MAC address of the client.

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

Authentication: Displays the type of authentication being used.

Signal: Displays the client's signal strength.

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



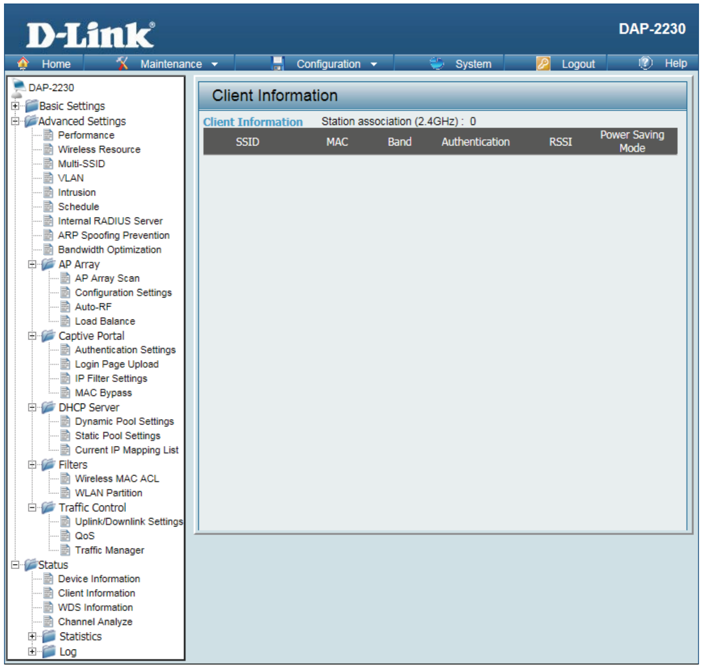
Client Information

Client Information   Station association (2.4GHz) : 0

SSID	MAC	Band	Authentication	RSSI	Power Saving Mode

WDS Information

This window displays the Wireless Distribution System information for clients currently connected to the DAP-2230. The following information is available for each client communicating with the DAP-2230.



Client Information

Client Information   Station association (2.4GHz) : 0

SSID	MAC	Band	Authentication	RSSI	Power Saving Mode

Name: Displays the SSID of the client.

MAC: Displays the MAC address of the client.

Authentication: Displays the type of authentication being used.

Signal: Displays the client's signal strength.

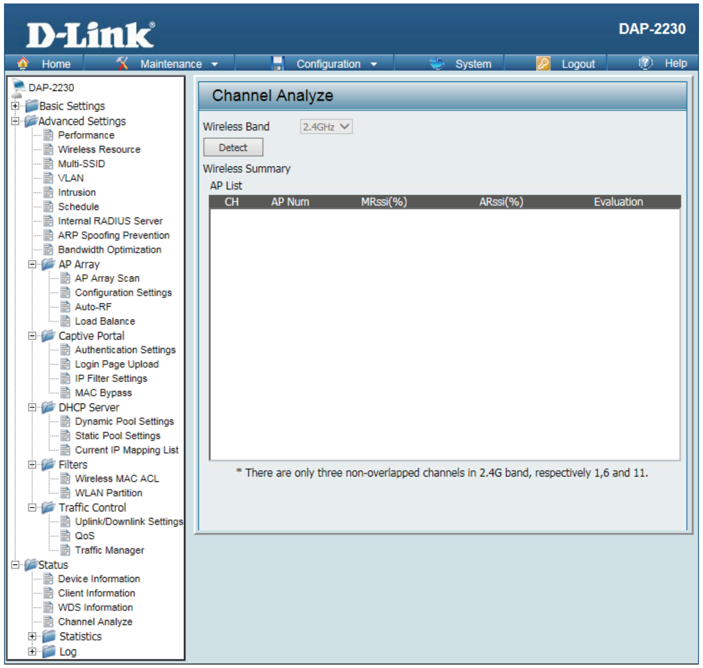
Status: Displays the status of the power saving feature.

Channel Analyze

Wireless Band: **2.4 Ghz**

Detect: Click the **Detect** button to scan.

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



Channel Analyze

Wireless Band: 2.4GHz

Wireless Summary

AP List

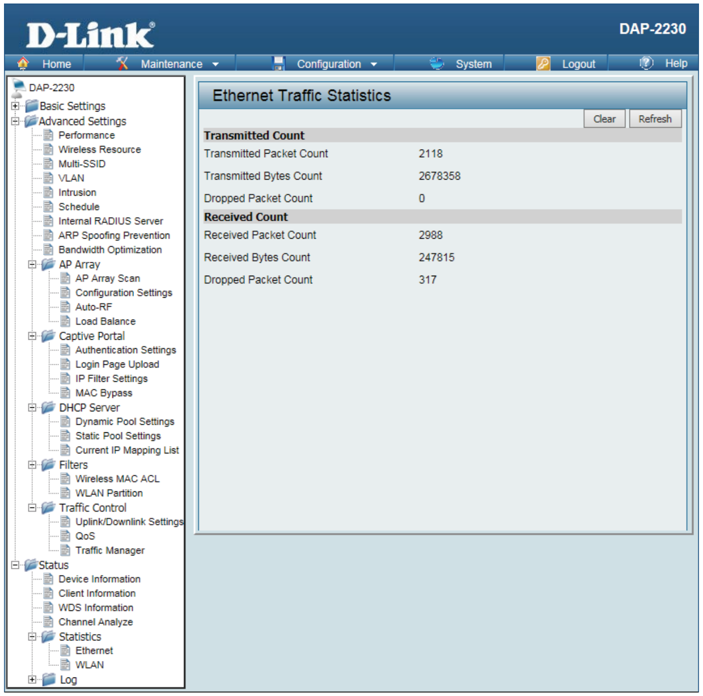
CH	AP Num	MRssi(%)	ARssi(%)	Evaluation

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

Statistics

Ethernet

This page displays transmitted and received count statistics for packets and bytes.

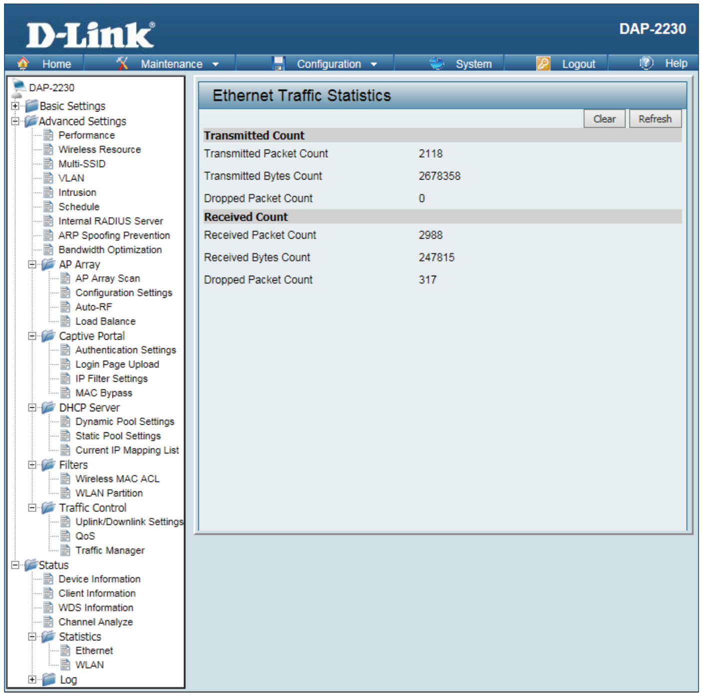


Ethernet Traffic Statistics

Transmitted Count	
Transmitted Packet Count	2118
Transmitted Bytes Count	2678358
Dropped Packet Count	0
Received Count	
Received Packet Count	2988
Received Bytes Count	247815
Dropped Packet Count	317

WLAN Traffic

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



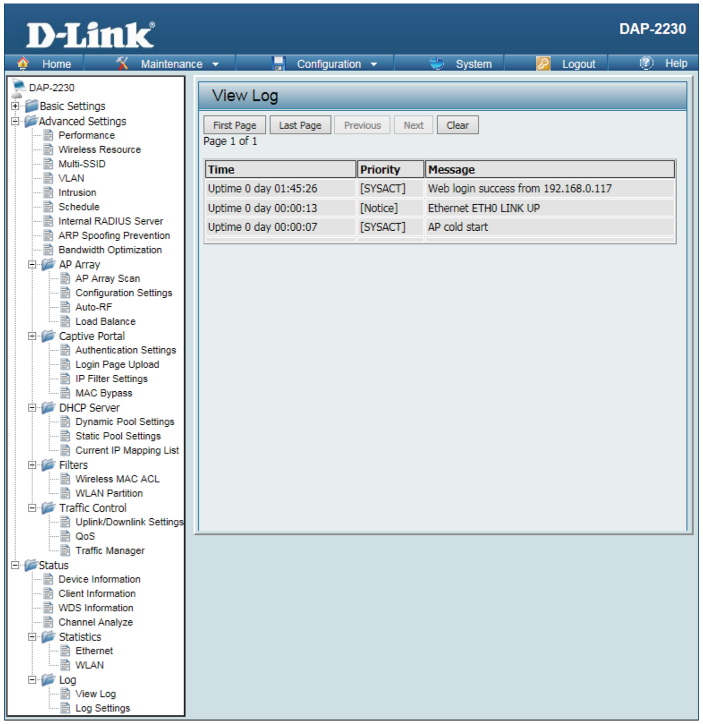
Ethernet Traffic Statistics

Transmitted Count	
Transmitted Packet Count	2118
Transmitted Bytes Count	2678358
Dropped Packet Count	0
Received Count	
Received Packet Count	2988
Received Bytes Count	247815
Dropped Packet Count	317

Log

View Log

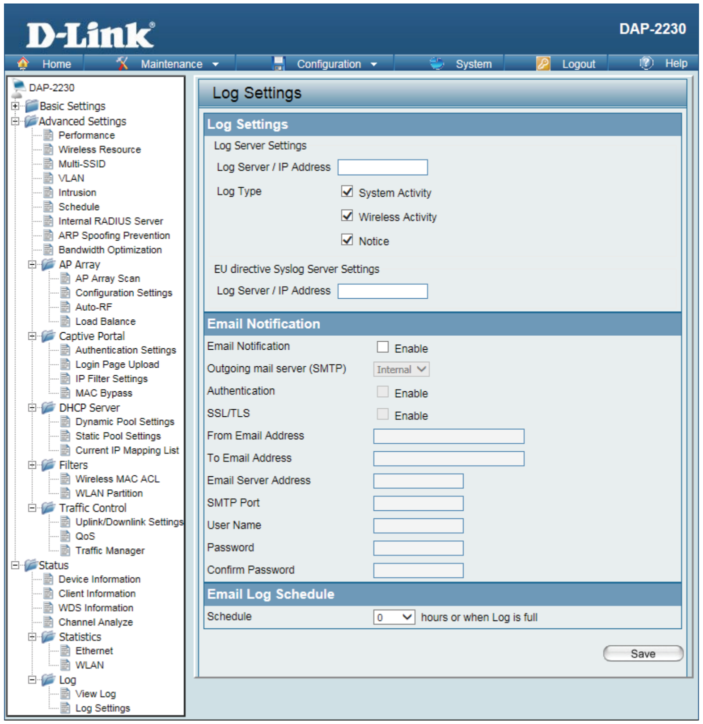
The AP's embedded memory displays system and network messages including a time stamp and message type. The log information includes but is not limited to the following items: cold start AP, upgrading firmware, client associate and disassociate with AP, and web login. The web page holds up to 500 logs.



Page 1 of 1

Time	Priority	Message
Uptime 0 day 01:45:26	[SYSACT]	Web login success from 192.168.0.117
Uptime 0 day 00:00:13	[Notice]	Ethernet ETH0 LINK UP
Uptime 0 day 00:00:07	[SYSACT]	AP cold start

Log Settings



Log Settings

Log Settings

Log Server Settings

Log Server / IP Address

Log Type ☑ System Activity ☑ Wireless Activity ☑ Notice

EU directive Syslog Server Settings

Log Server / IP Address

Email Notification

Email Notification □ Enable

Outgoing mail server (SMTP) Internal

Authentication □ Enable

SSL/TLS □ Enable

From Email Address

To Email Address

Email Server Address

SMTP Port

User Name

Password

Confirm Password

Email Log Schedule

Schedule 0 hours or when Log is full

Log Server/ IP Address: Enter the IP address of the server you would like to send the DAP-2230 log to.

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

EU directive Syslog Server Settings: Enter the EU Directive Log Server IP Address.

Email Notification: Check to enable Email notification.

Outgoing Mail Server (SMTP): Select the SMTP server from the drop-down menu.

Authentication: Check to enable authentication.

SSL / TLS: Check to enable SSL/TLS authentication.

From Email Address: Enter the “From” email address.

To Email Address: Enter the destination email address.

Email Server Address: Enter the Email Server Address.

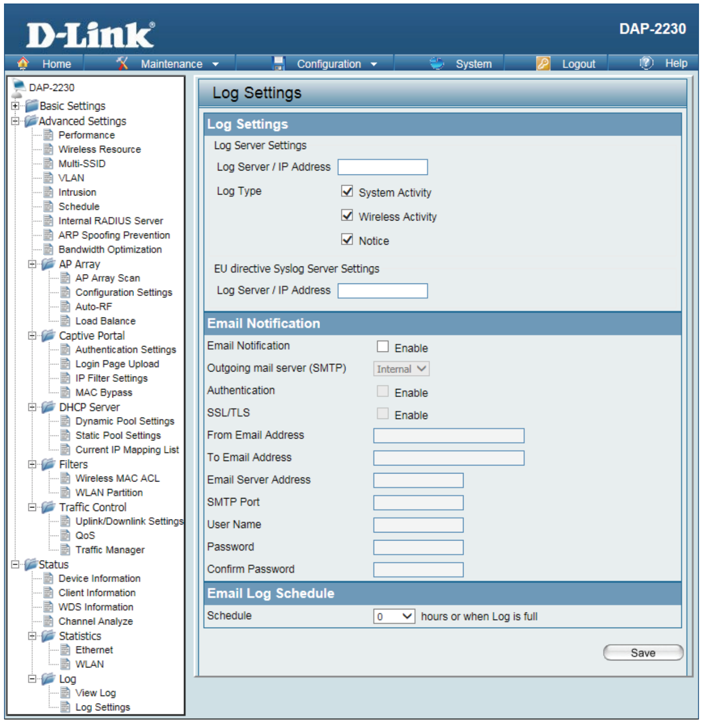
SMTP Port: Enter the SMTP port.

Username: Enter your email username.

Password: Enter your email password.

Confirm Password: Enter your email password again.

Schedule: Select when to send the log to your email (in hours). You will receive an email when the log is full too.



Log Settings

Log Settings

Log Server Settings

Log Server / IP Address	
Log Type	☑ System Activity ☑ Wireless Activity ☑ Notice

EU directive Syslog Server Settings

Log Server / IP Address	

Email Notification

Email Notification	□ Enable
Outgoing mail server (SMTP)	Internal
Authentication	□ Enable
SSL/TLS	□ Enable
From Email Address	
To Email Address	
Email Server Address	
SMTP Port	
User Name	
Password	
Confirm Password	

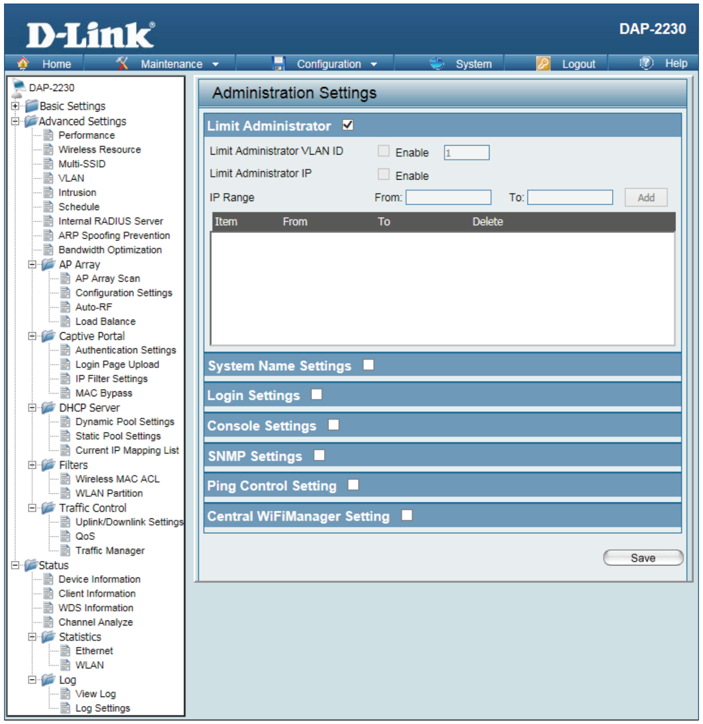
Email Log Schedule

Schedule	0 hours or when Log is full

Maintenance

Administration Settings

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



Administration Settings

Limit Administrator ☑

Limit Administrator VLAN ID □ Enable 1

Limit Administrator IP □ Enable

IP Range From: To:

Item	From	To	Delete

System Name Settings □

Login Settings □

Console Settings □

SNMP Settings □

Ping Control Setting □

Central WiFiManager Setting □

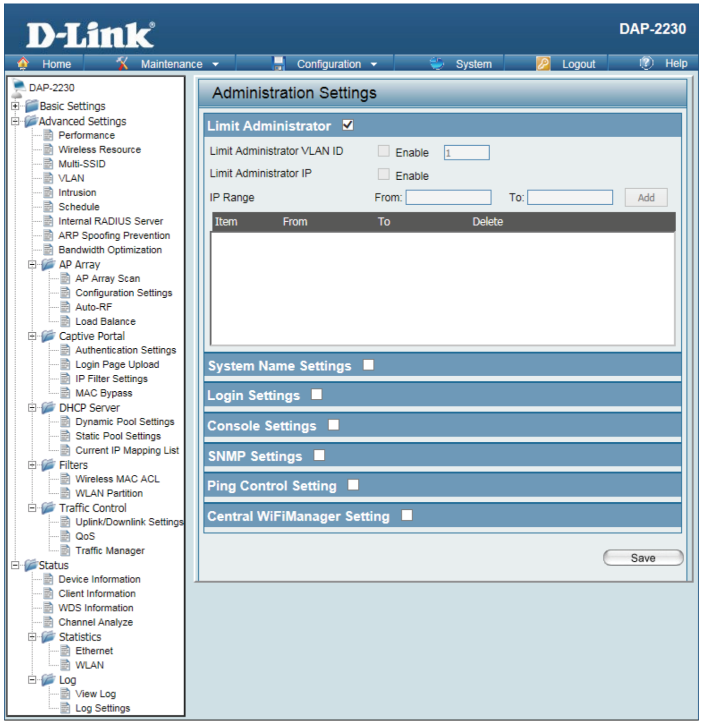
Limit Administrator

Each of the five main categories display various hidden administrator parameters and settings.

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

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

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



Administration Settings

Limit Administrator ☑

Limit Administrator VLAN ID □ Enable 1

Limit Administrator IP □ Enable

IP Range From: To:

Item	From	To	Delete

System Name Settings □

Login Settings □

Console Settings □

SNMP Settings □

Ping Control Setting □

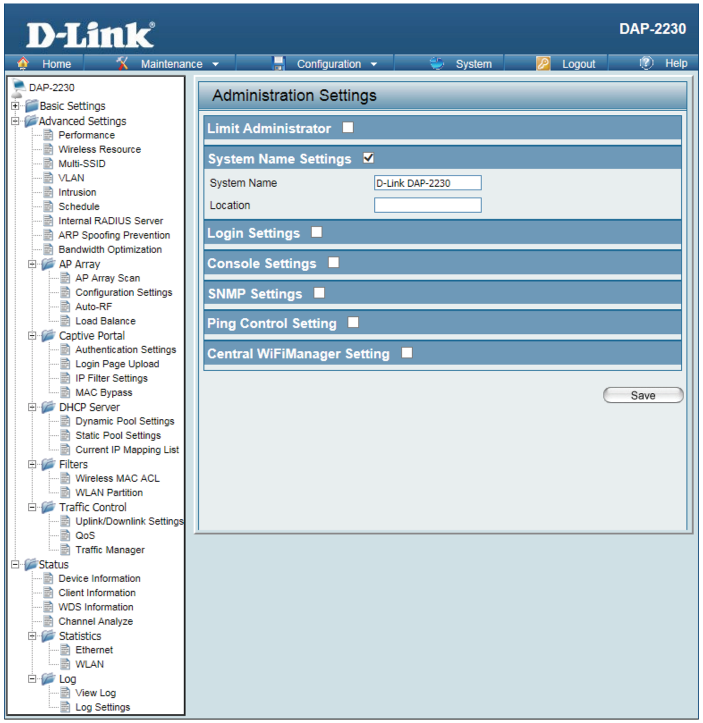
Central WiFiManager Setting □

System Name Settings

Each of the five main categories display various hidden administrator parameters and settings.

System Name: The name of the device. The default name is **D-Link DAP-2230**.

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



Administration Settings

Limit Administrator □

System Name Settings ☑

System Name: D-Link DAP-2230

Location:

Login Settings □

Console Settings □

SNMP Settings □

Ping Control Setting □

Central WiFiManager Setting □

Save

Login Settings

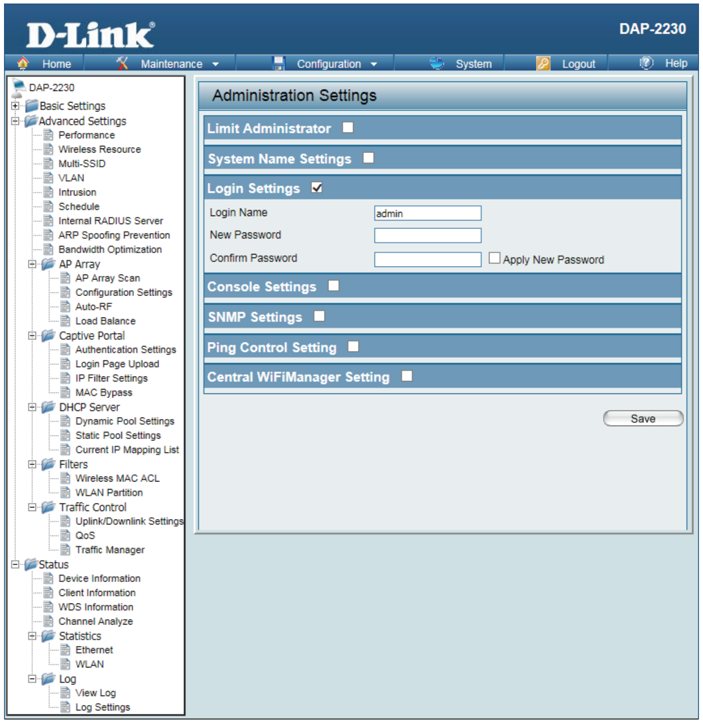
Each of the five main categories display various hidden administrator parameters and settings.

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

Old Password: When changing your password, enter the old password here.

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

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



Administration Settings

Limit Administrator □

System Name Settings □

Login Settings ☑

Login Name	admin
New Password	
Confirm Password	□ Apply New Password

Console Settings □

SNMP Settings □

Ping Control Setting □

Central WiFiManager Setting □

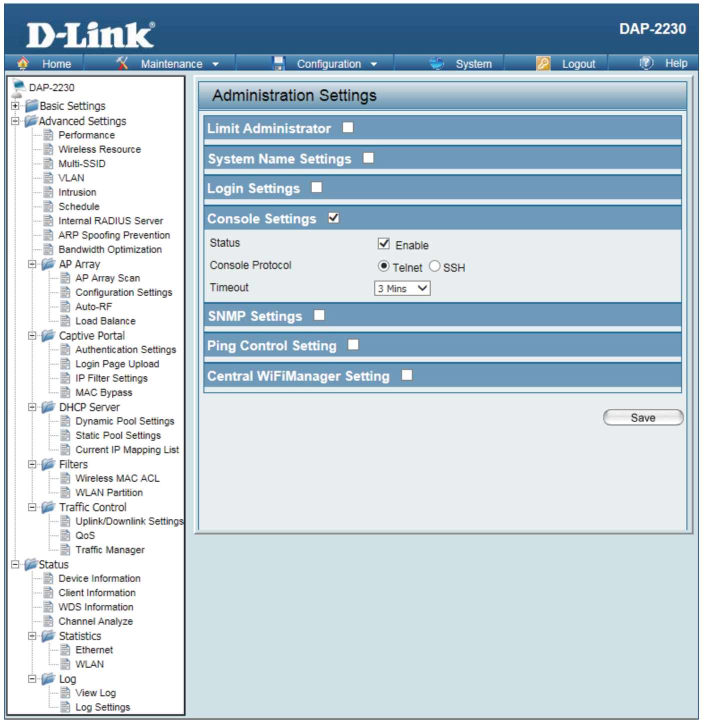
Console Settings

Each of the five main categories display various hidden administrator parameters and settings.

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

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

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



Administration Settings

Limit Administrator □

System Name Settings □

Login Settings □

Console Settings ☑

Status	☑ Enable
Console Protocol	● Telnet ○ SSH
Timeout	3 Mins

SNMP Settings □

Ping Control Setting □

Central WiFiManager Setting □

Save

SNMP Settings

Each of the five main categories display various hidden administrator parameters and settings.

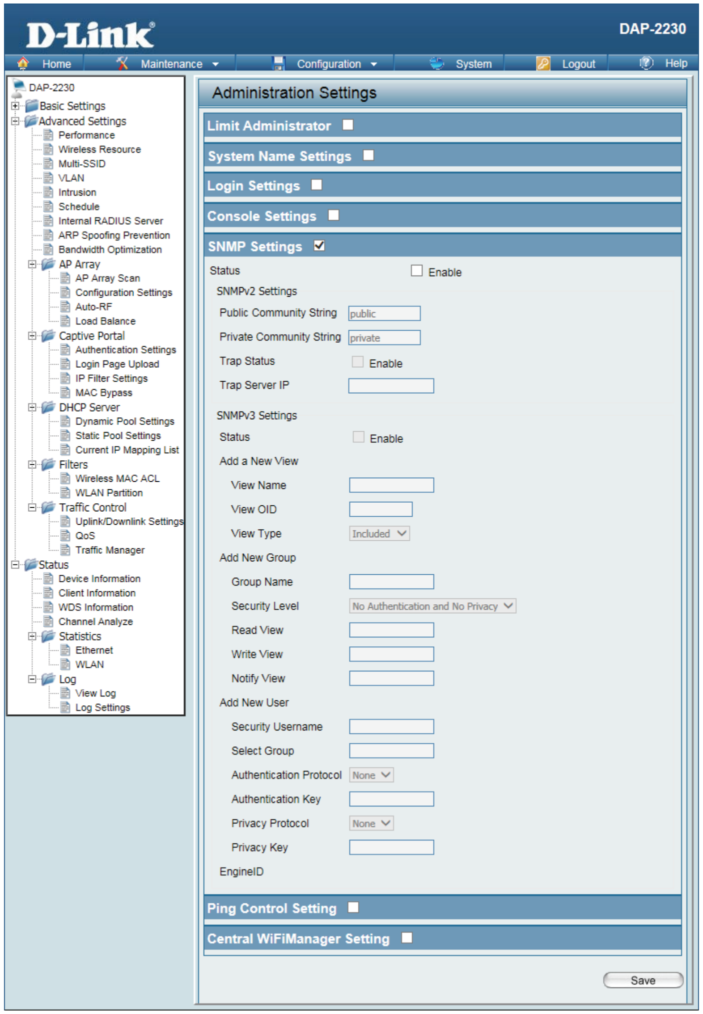
Status: Check the box to enable the SNMP functions. This option is disabled by default.

Public Community String: Enter the public SNMP community string.

Private Community String: Enter the private SNMP community string.

Trap Status: Check the box to enable Trap Status.

Trap Server IP: Enter the Trap Server IP address.



Administration Settings

Limit Administrator □

System Name Settings □

Login Settings □

Console Settings □

SNMP Settings ☑

Status □ Enable

SNMPv2 Settings

Public Community String: public

Private Community String: private

Trap Status □ Enable

Trap Server IP:

SNMPv3 Settings

Status □ Enable

Add a New View

View Name:

View OID:

View Type: Included

Add New Group

Group Name:

Security Level: No Authentication and No Privacy

Read View:

Write View:

Notify View:

Add New User

Security Username:

Select Group:

Authentication Protocol: None

Authentication Key:

Privacy Protocol: None

Privacy Key:

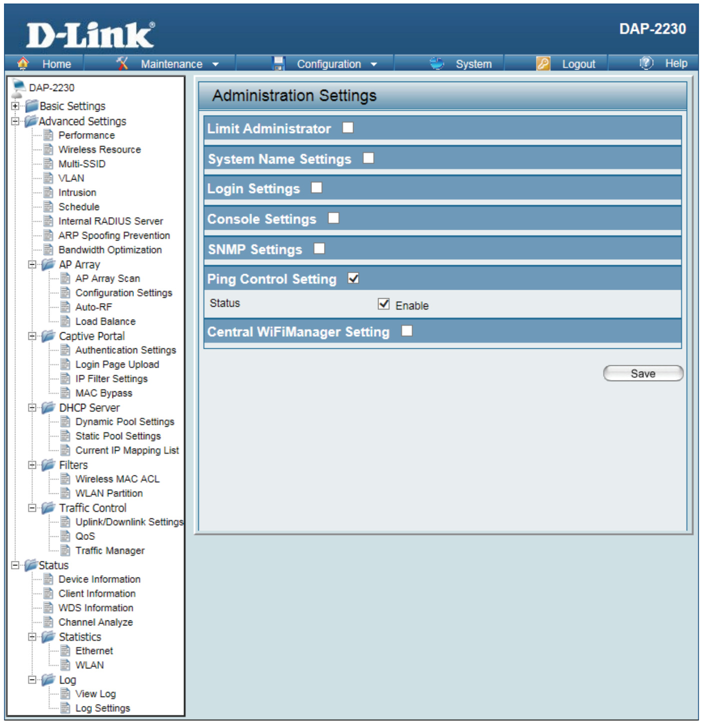
EngineID

Ping Control Setting □

Central WiFiManager Setting □

Ping Control

Status: Check the box to enable Ping control. Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP echo response replies. The default is enabled. If not enabled, the access point will not reply to pings.



Administration Settings

Limit Administrator □

System Name Settings □

Login Settings □

Console Settings □

SNMP Settings □

Ping Control Setting ☑

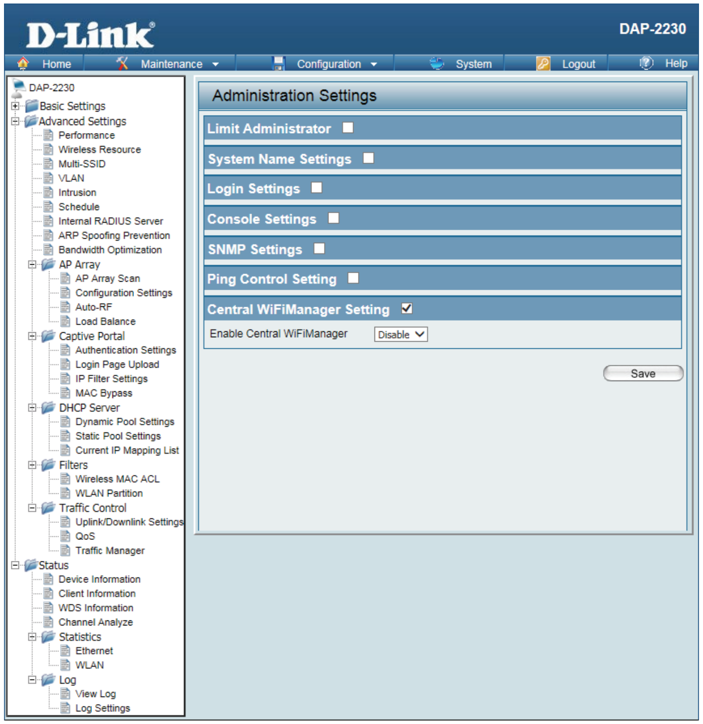
Status ☑ Enable

Central WiFiManager Setting □

Central WiFiManager Settings

The Central WiFiManager section is used to configure and manage a set of APs on the network into a single group in order to simplify management. Central WiFiManager and AP Array may not be used simultaneously.

Enable Central WiFiManager: Select to enable or disable the Central WiFiManager.



Administration Settings

Limit Administrator □

System Name Settings □

Login Settings □

Console Settings □

SNMP Settings □

Ping Control Setting □

Central WiFiManager Setting ☑

Enable Central WiFiManager: Disable

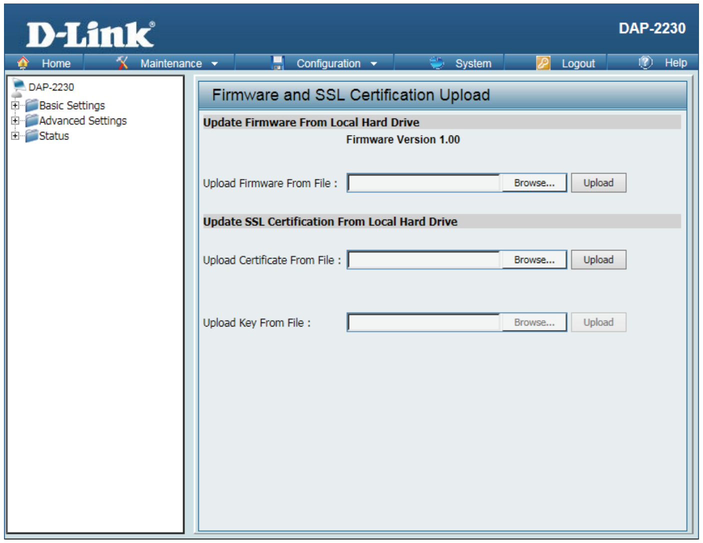
Firmware and SSL Certification Upload

This page allows the user to perform a firmware upgrade. Be sure to check the **support.dlink.com** website periodically for the latest firmware updates to keep your product up to date with the latest features.

Upload Firmware From Local Hard Drive: The current firmware version is displayed above the file location field. After downloading the most recent version of the firmware for the DAP-2230 from h**ttp://support.dlink.com** to your local computer, use the **Browse** button to locate the firmware file on your computer. Click **Upload** to update the firmware version. Please don't turn the power off while upgrading.

Language Pack Upgrade: You may load a language pack to display the utility in another language. Click **Browse** to locate the language pack file on your local computer. After selecting and opening the file, click **Upload** to upload the file to the DAP-2230.

Upload SSL Certification From Local Hard Drive: Click **Browse** to locate the SSL Certification file on your local computer. After selecting and opening the file, click **Upload** to upload the file to the DAP-2230.



Firmware and SSL Certification Upload

Update Firmware From Local Hard Drive

Firmware Version 1.00

Upload Firmware From File :

Update SSL Certification From Local Hard Drive

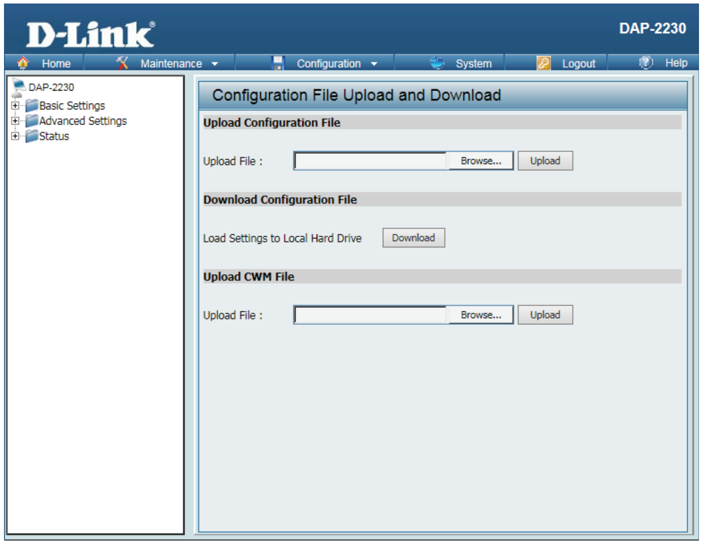
Upload Certificate From File :

Upload Key From File :

Configuration File Upload

Upload File: Click the **Browse** button to locate a previously saved configuration file on your local computer. After selecting the file, click **Upload** to apply the configuration settings to the DAP-2230.

Download Configuration File: Click **Download** to save the current DAP-2230 configuration to your local computer.



Time and Date

Current Time: Displays the current time and date settings.

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

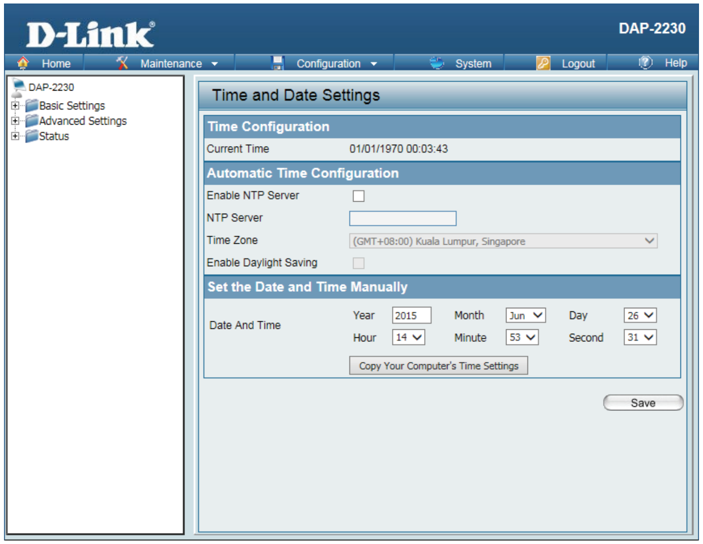
NTP Server: Enter the NTP server URL or IP address.

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

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

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

Set the Date and Time Manually: You can either manually set the time for your AP here, or you can click the **Copy Your Computer's Time Settings** button to copy the time from the computer you are using (Make sure that the computer's time is set correctly).



Time and Date Settings

Time Configuration

Current Time	01/01/1970 00:03:43

Automatic Time Configuration

Enable NTP Server	□
NTP Server	
Time Zone	(GMT+08:00) Kuala Lumpur, Singapore
Enable Daylight Saving	□

Set the Date and Time Manually

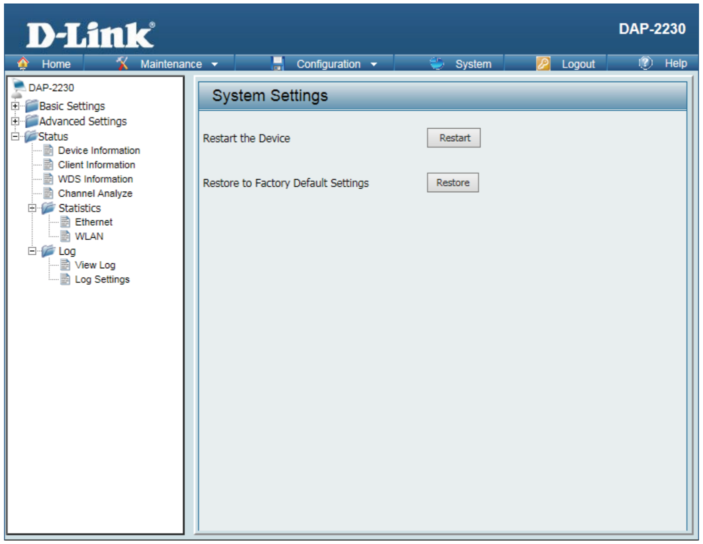
Date And Time	Year	2015	Month	Jun	Day	26
	Hour	14	Minute	53	Second	31

System

System Settings

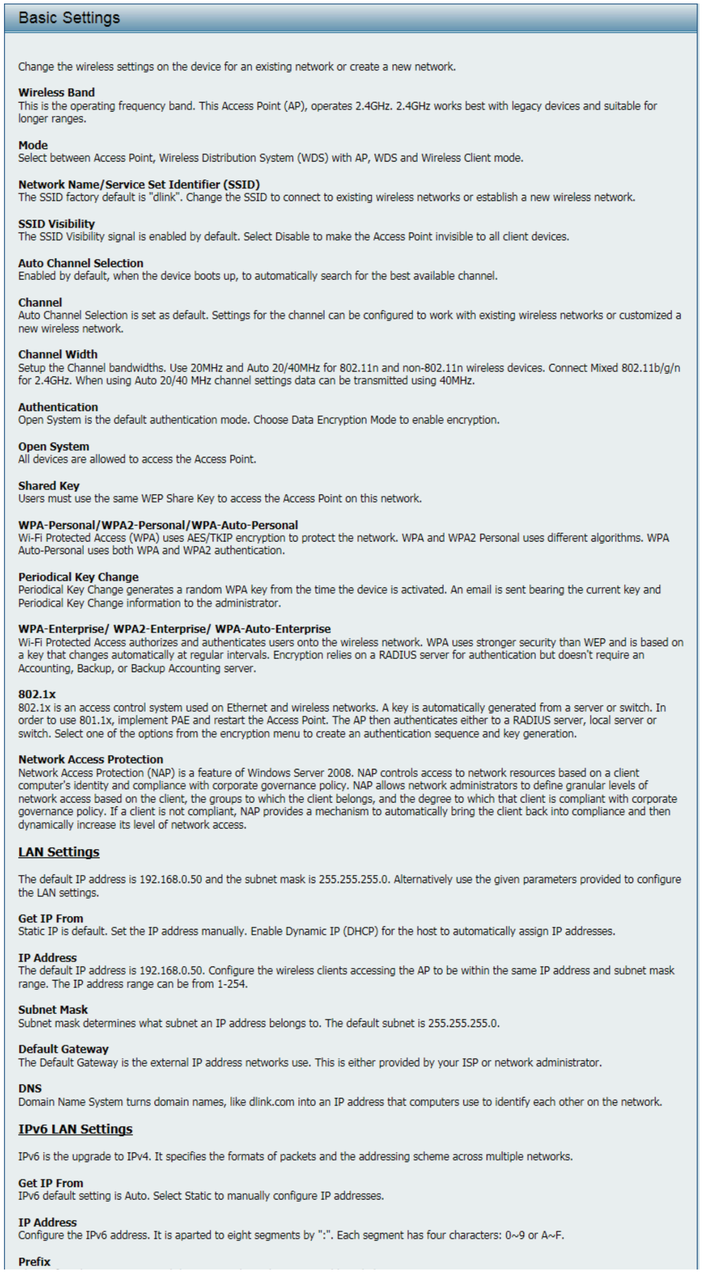
Restart the Device: Click **Restart** to restart the DAP-2230.

Restore to Factory Default Settings: Click **Restore** to restore the DAP-2230 back to factory default settings.



Help

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



Basic Settings

Change the wireless settings on the device for an existing network or create a new network.

Wireless Band
This is the operating frequency band. This Access Point (AP), operates 2.4GHz. 2.4GHz works best with legacy devices and suitable for longer ranges.

Mode
Select between Access Point, Wireless Distribution System (WDS) with AP, WDS and Wireless Client mode.

Network Name/Service Set Identifier (SSID)
The SSID factory default is "dlink". Change the SSID to connect to existing wireless networks or establish a new wireless network.

SSID Visibility
The SSID Visibility signal is enabled by default. Select Disable to make the Access Point invisible to all client devices.

Auto Channel Selection
Enabled by default, when the device boots up, to automatically search for the best available channel.

Channel
Auto Channel Selection is set as default. Settings for the channel can be configured to work with existing wireless networks or customized a new wireless network.

Channel Width
Setup the Channel bandwidths. Use 20MHz and Auto 20/40MHz for 802.11n and non-802.11n wireless devices. Connect Mixed 802.11b/g/n for 2.4GHz. When using Auto 20/40 MHz channel settings data can be transmitted using 40MHz.

Authentication
Open System is the default authentication mode. Choose Data Encryption Mode to enable encryption.

Open System
All devices are allowed to access the Access Point.

Shared Key
Users must use the same WEP Share Key to access the Access Point on this network.

WPA-Personal/WPA2-Personal/WPA-Auto-Personal
Wi-Fi Protected Access (WPA) uses AES/TKIP encryption to protect the network. WPA and WPA2 Personal uses different algorithms. WPA Auto-Personal uses both WPA and WPA2 authentication.

Periodical Key Change
Periodical Key Change generates a random WPA key from the time the device is activated. An email is sent bearing the current key and Periodical Key Change information to the administrator.

WPA-Enterprise/ WPA2-Enterprise/ WPA-Auto-Enterprise
Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. WPA uses stronger security than WEP and is based on a key that changes automatically at regular intervals. Encryption relies on a RADIUS server for authentication but doesn't require an Accounting, Backup, or Backup Accounting server.

802.1x
802.1x is an access control system used on Ethernet and wireless networks. A key is automatically generated from a server or switch. In order to use 801.1x, implement PAE and restart the Access Point. The AP then authenticates either to a RADIUS server, local server or switch. Select one of the options from the encryption menu to create an authentication sequence and key generation.

Network Access Protection
Network Access Protection (NAP) is a feature of Windows Server 2008. NAP controls access to network resources based on a client computer's identity and compliance with corporate governance policy. NAP allows network administrators to define granular levels of network access based on the client, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

LAN Settings

The default IP address is 192.168.0.50 and the subnet mask is 255.255.255.0. Alternatively use the given parameters provided to configure the LAN settings.

Get IP From
Static IP is default. Set the IP address manually. Enable Dynamic IP (DHCP) for the host to automatically assign IP addresses.

IP Address
The default IP address is 192.168.0.50. Configure the wireless clients accessing the AP to be within the same IP address and subnet mask range. The IP address range can be from 1-254.

Subnet Mask
Subnet mask determines what subnet an IP address belongs to. The default subnet is 255.255.255.0.

Default Gateway
The Default Gateway is the external IP address networks use. This is either provided by your ISP or network administrator.

DNS
Domain Name System turns domain names, like dlink.com into an IP address that computers use to identify each other on the network.

IPv6 LAN Settings

IPv6 is the upgrade to IPv4. It specifies the formats of packets and the addressing scheme across multiple networks.

Get IP From
IPv6 default setting is Auto. Select Static to manually configure IP addresses.

IP Address
Configure the IPv6 address. It is aparted to eight segments by ":". Each segment has four characters: 0~9 or A~F.

Prefix

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DAP-2230 offers the following types of security:

- WEP (Wired Equivalent Privacy)
- WPA-Personal (Wi-Fi Protected Access)
- WPA-Enterprise (Wi-Fi Protected Access)

What is WEP?

WEP, or Wired Equivalent Privacy, is a Wi-Fi security protocol that encrypts transmitted data. WEP is an older protocol that is not believed to be as effective anymore.

WEP uses a passphrase or key to authenticate your wireless connection. For 64-Bit WEP, the key is an alpha-numeric password that is 10 hex digits or an ASCII password consisting of 5 text characters. The hex digits are either numbers from 0 to 9 or letters from A to F. For 128-Bit WEP, the key is an alpha-numeric password that is 26 hex digits or an ASCII password with 13 text characters.

Configure WEP

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the access point (dlinkap.local). Click on **Setup** and then click **Wireless Setup** on the left side.

2. Next to *Security Mode*, select **WEP**.
   Note: Choosing WEP means the device will only operate in Legacy wireless mode (802.11B/G) and will not provide 802.11N performance.

3. Next to *WEP Encryption*, select **64 Bit(10 hex digits)**, **64 Bit(5 ASCII characters)**, **128 Bit(26 hex digits)** or **128 Bit(13 ASCII characters)**.

4. Next to *WEP Key 1*, enter a set of digits or letters from A to F, or a string of text.

5. Next to *Authentication,* select **Both** or **Shared Key**.

6. Click **Save Settings** at the top of the window to save your settings. If you are configuring the access point with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the access point.

What is WPA?

WPA, or Wi-Fi Protected Access, is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.

- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless bridge or access point.

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

Configure WPA/WPA2 Personal

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the access point (dlinkap.local). Click on **Setup** and then click **Wireless Setup** on the left side.

2. Next to *Security Mode*, select **WPA-Personal**.

3. Next to *WPA Mode*, select **Auto(WPA or WPA2)**, **WPA2 only**, or **WPA only**.

4. Next to *Cipher Type*, select **TKIP**, **AES**, or **TKIP and AES**.

5. Next to *Pre-Shared Key,* enter a key. The key is entered as a passphrase in ASCII format at both ends of the wireless connection. The passphrase must be between 8-63 characters.

6. Click **Save Settings** at the top of the window to save your settings. If you are configuring the access point with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the access point.

Configure WPA/WPA2 Enterprise

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the access point (dlinkap.local). Click on **Setup** and then click **Wireless Setup** on the left side.

2. Next to *Security Mode*, select **WPA-Enterprise**.

3. Next to *WPA Mode*, select **Auto(WPA or WPA2)**, **WPA2 only**, or **WPA only**.

4. Next to *Cipher Mode*, select **TKIP**, **AES**, or **Auto**.

5. Next to *RADIUS Server IP Address*, enter the IP Address of your RADIUS server.

6. Next to *RADIUS Server Port*, enter the port you are using with your RADIUS server. 1812 is the default port.

7. Next to *RADIUS Server Shared Secret*, enter the security key.

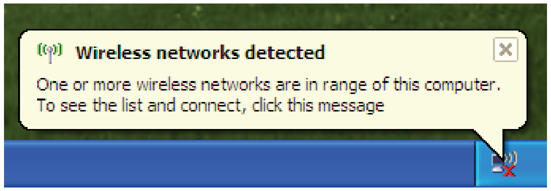
8. Click **Advanced** to enter settings for a secondary RADIUS Server.

9. Click **Save Settings** to save your settings.

Connect to a Wireless Network
Using Windows® XP

Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

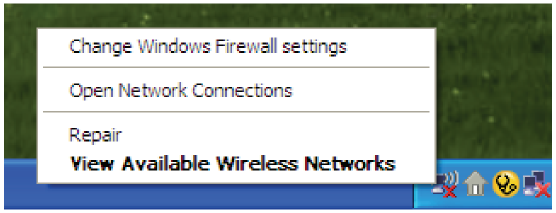


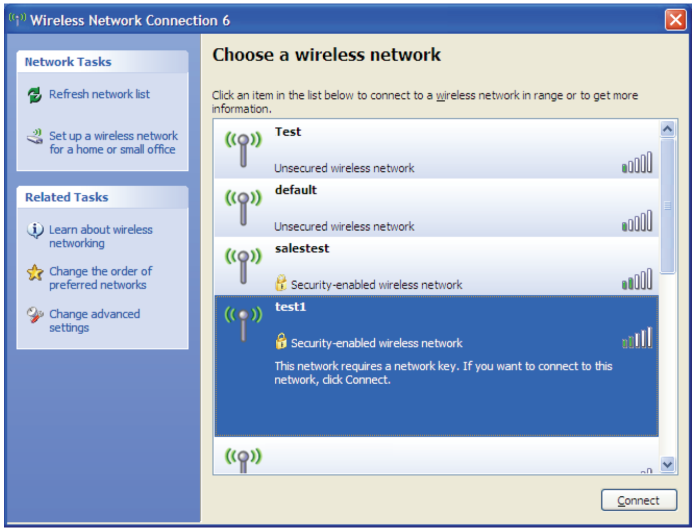
Wireless networks detected

One or more wireless networks are in range of this computer.
To see the list and connect, click this message

or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **View Available Wireless Networks**.


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks



Wireless Network Connection 6

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Test
Unsecured wireless network

default
Unsecured wireless network

salestest
Security-enabled wireless network

test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

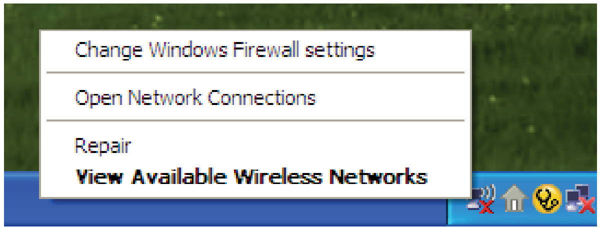
The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

If you get a good signal, but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.

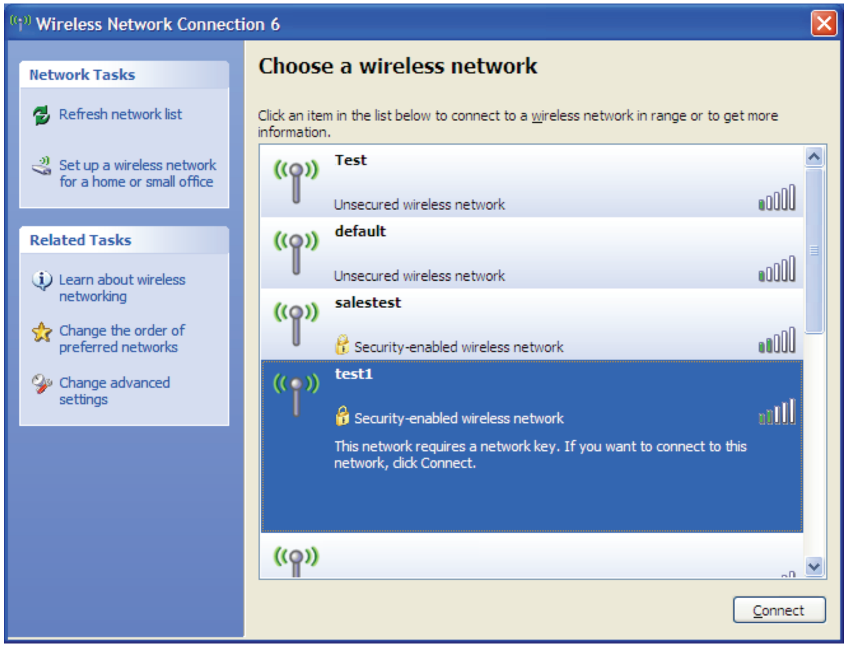
Configure WPA-PSK

It is recommended to enable WEP on your wireless bridge or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WEP key being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks.**


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks

2. Highlight the wireless network (SSID) you would like to connect to and click **Connect.**


Wireless Network Connection 6
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Test
Unsecured wireless network

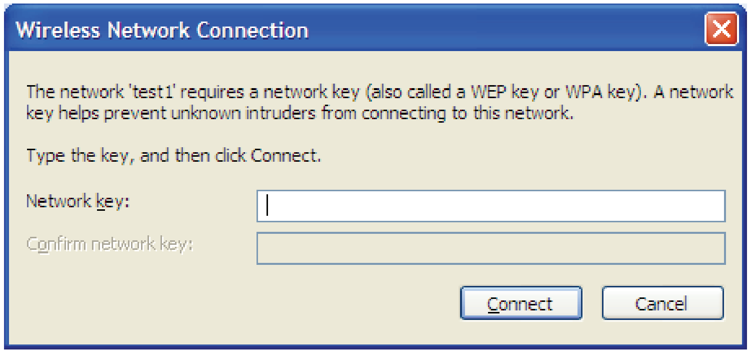
default
Unsecured wireless network

salestest
Security-enabled wireless network

test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK passphrase and click **Connect.**

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA-PSK settings are correct. The WPA-PSK passphrase must be exactly the same as on the wireless access point.


Wireless Network Connection

The network 'test1' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

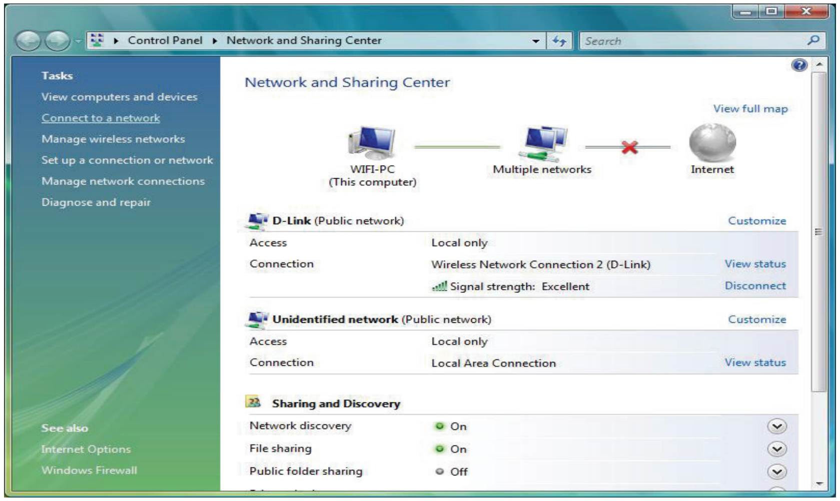
Network key:

Confirm network key:

Using Windows Vista®

Windows Vista® users may use the convenient, built-in wireless utility. Follow these instructions:

From the Start menu, go to Control Panel, and then click on **Network and Sharing Center**.



D-Link (Public network)

Access	Local only
Connection	Wireless Network Connection 2 (D-Link)
	Signal strength: Excellent

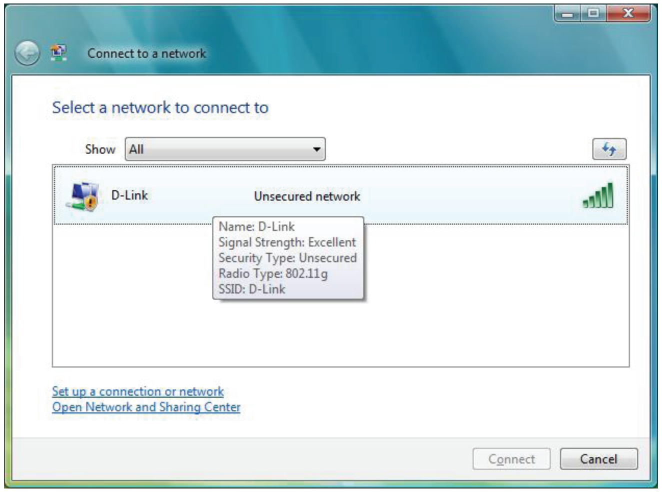
Unidentified network (Public network)

Access	Local only
Connection	Local Area Connection

Sharing and Discovery

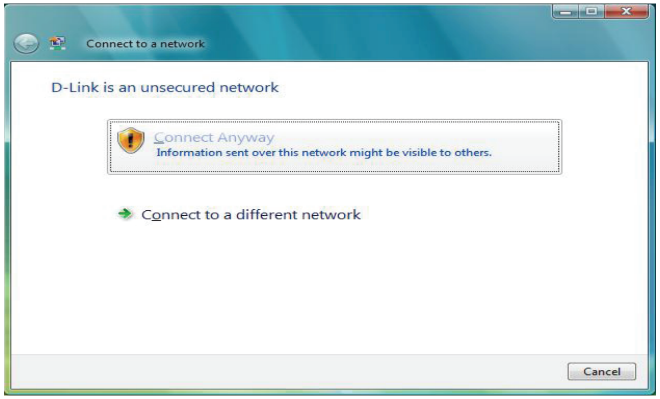
Network discovery	● On
File sharing	● On
Public folder sharing	○ Off

The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) under Select a network to connect to and then click the **Connect** button.


Connect to a network
Select a network to connect to
Show
All
D-Link
Unsecured network
Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

Name: D-Link
Signal Strength: Excellent
Security Type: Unsecured
Radio Type: 802.11g
SSID: D-Link

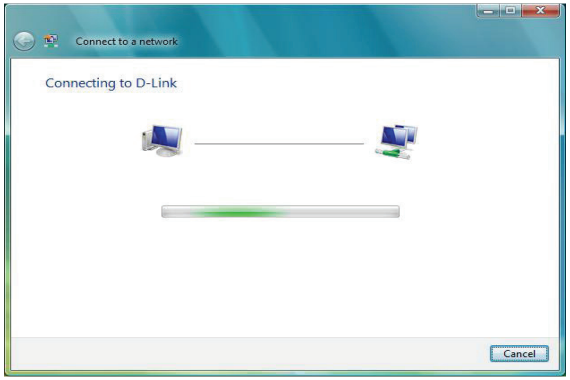
Click **Connect Anyway** to continue.



D-Link is an unsecured network

Information sent over this network might be visible to others.

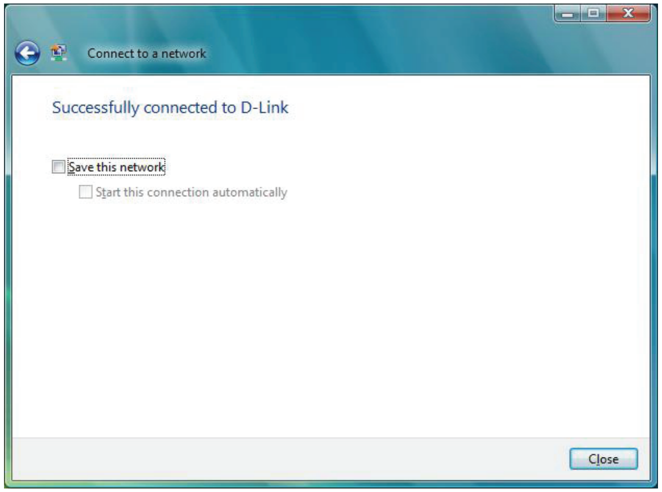
The utility will display the following window to indicate a connection is being made.



Connecting to D-Link

The final window indicates the establishment of a successful connection.

The next two pages display the windows used to connect to either a WEP or a WPA-PSK wireless network.



Successfully connected to D-Link

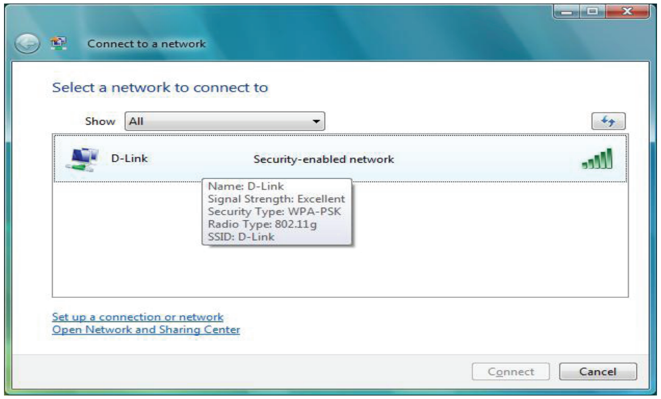
□ Save this network

□ Start this connection automatically

Configure WPA-PSK

It is recommended to enable WEP on your wireless bridge or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WEP key being used.

Click on a network (displayed using the SSID) using WPA-PSK under Select a network to connect to and then click the **Connect** button.

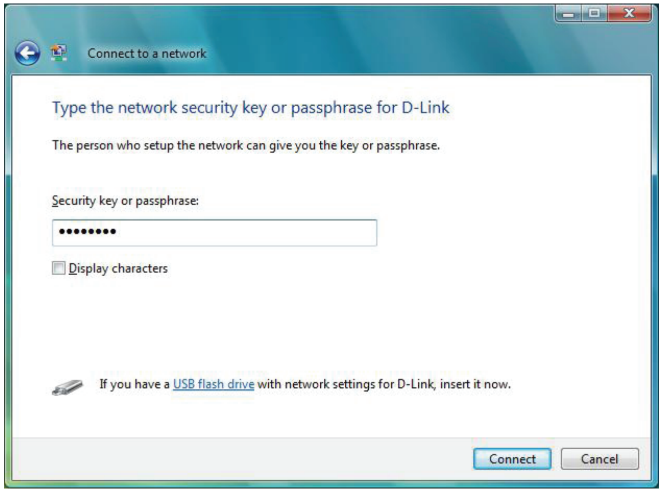

Connect to a network
Show
All
Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

Select a network to connect to

D-Link Security-enabled network

Name: D-Link
Signal Strength: Excellent
Security Type: WPA-PSK
Radio Type: 802.11g
SSID: D-Link

Enter the appropriate security key or passphrase in the field provided and then click the **Connect** button.



Type the network security key or passphrase for D-Link

The person who setup the network can give you the key or passphrase.

Security key or passphrase: ••••••••

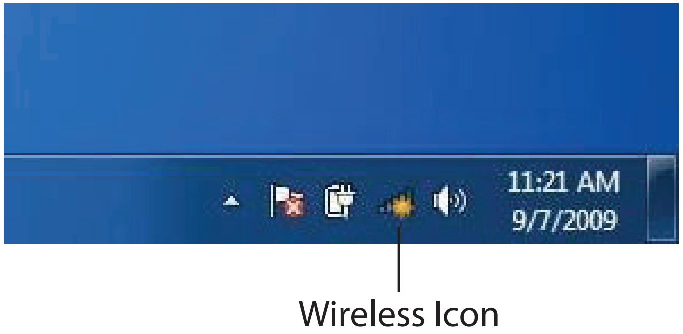
□ Display characters

If you have a USB flash drive with network settings for D-Link, insert it now.

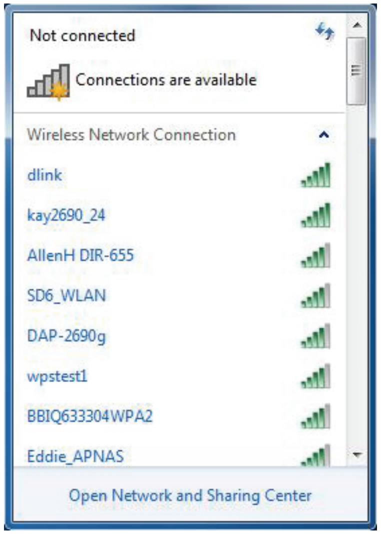
Using Windows® 7

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Click on the wireless icon in your system tray (lower-right corner).



2. The utility will display any available wireless networks in your area.


Not connected

Connections are available

Wireless Network Connection

dlink

kay2690_24

AllenH DIR-655

SD6_WLAN

DAP-2690g

wpstest1

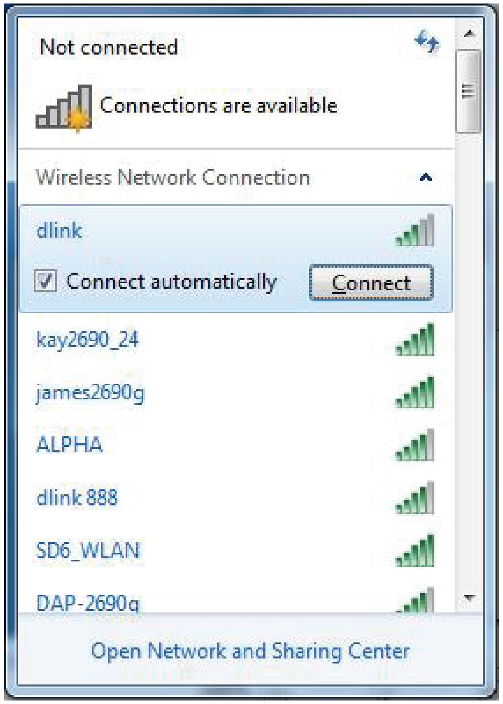
BBIQ633304WPA2

Eddie_APNAS

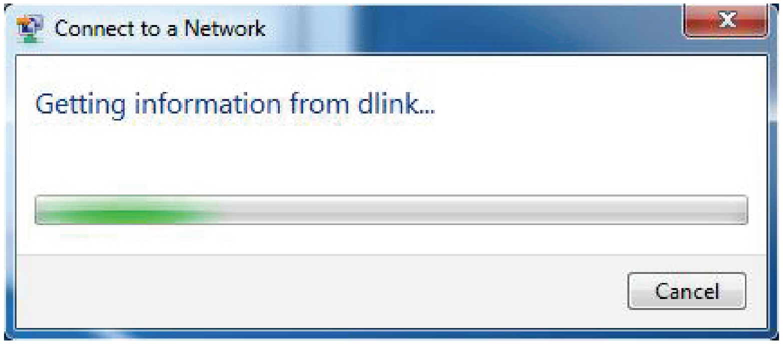
Open Network and Sharing Center

3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

   If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.

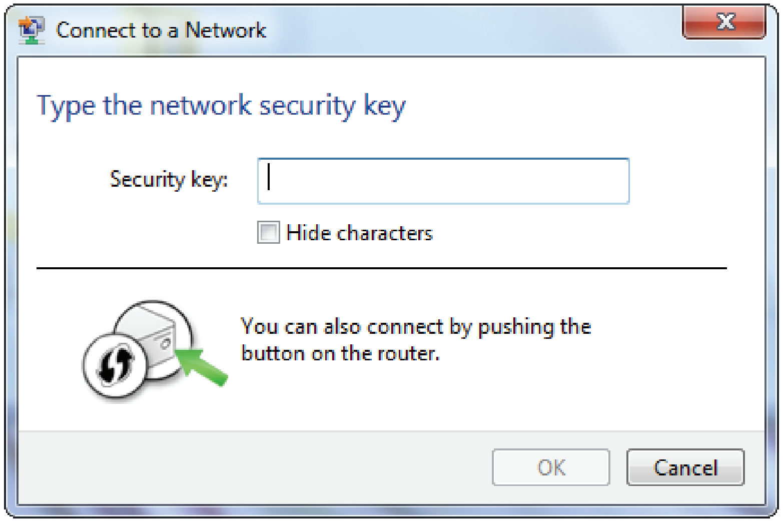


4. The following window appears while your computer tries to connect to the router.



Getting information from dlink...

5. Enter the same security key or passphrase that is on your router and click **Connect**. You can also connect by pushing the WPS button on the router.



Connect to a Network

Type the network security key

Security key:

□ Hide characters

You can also connect by pushing the button on the router.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-2230. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

1. Why can't I access the web-based configuration utility?

When entering the IP address of the D-Link access point (**dlinkapwxyz.local** for example, with **wxyz** the last four digits of the AP's MAC Address), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:

  - Microsoft Internet Explorer® 7 and higher
  - Mozilla Firefox 12.0 and higher
  - Google™ Chrome 20.0 and higher
  - Apple Safari 4 and higher

- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.

- Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:

    - Go to **Start > Settings > Control Panel**. Double-click the **Internet Options** Icon. From the Security tab, click the button to restore the settings to their defaults.

    - Click the Connection tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click OK.

    - Go to the Advanced tab and click the button to restore these settings to their defaults. Click OK three times.

    - Close your web browser (if open) and open it.

- Access the web management. Open your web browser and enter the IP address of your D-Link access point in the address bar. This should open the login page for your the web management.

- If you still cannot access the configuration, unplug the power to the access point for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

2. What can I do if I forgot my password?

If you forgot your password, you must reset your access point. Unfortunately this process will change all your settings back to the factory defaults.

To reset the access point, locate the reset button (hole) on the rear panel of the unit. With the access point powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the access point will go through its reboot process. Wait about 30 seconds to access the access point. The default IP address is 192.168.0.50. When logging in, the username is Admin and leave the password box empty.

3. Why can’t I connect to certain sites or send and receive emails when connecting through my access point?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

Note: AOL DSL+ users must use MTU of 1400.

To find the proper MTU Size, you’ll have to do a special ping of the destination you’re trying to go to. A destination could be another computer, or a URL.

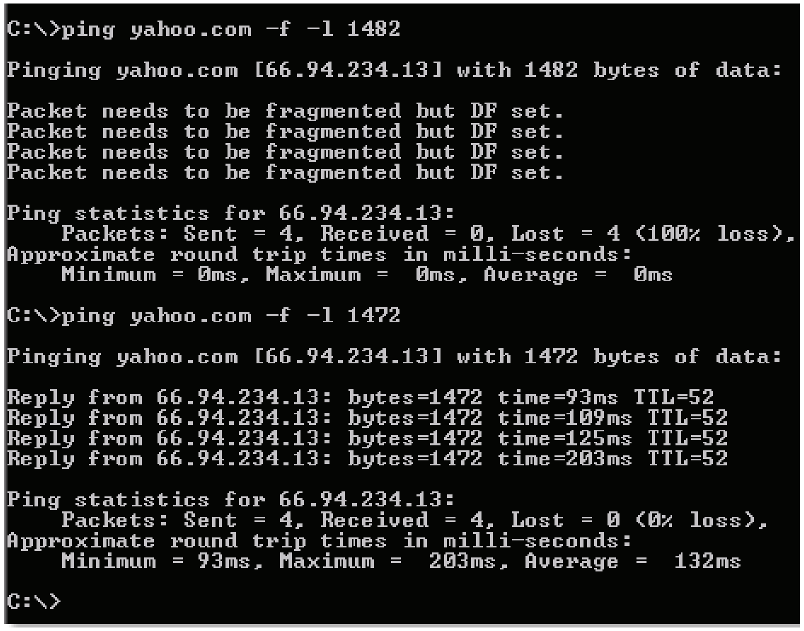
- Click on **Start** and then click **Run**.

- Windows® 95, 98, and Me users type in command (Windows® NT, 2000, and XP users type in cmd) and press **Enter** (or click **OK**).

- Once the window opens, you’ll need to do a special ping. Use the following syntax:

  ping [url] [-f] [-l] [MTU value]

Example: **ping yahoo.com -f -l 1472**



```
C:\>ping yahoo.com -f -l 1482

Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:

Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ping yahoo.com -f -l 1472

Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:

Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum =  203ms, Average =  132ms

C:\>
```

You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, lets say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with (1452+28=1480).

Once you find your MTU, you can now configure your access point with the proper MTU size.

To change the MTU rate on your access point follow the steps below:

- Open your browser, enter the IP address of your access point (192.168.0.50) and click **OK.**

- Enter your username (Admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.

- Click on **Setup** and then click **Manual Configure.**

- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.

- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Wireless Basics

D-Link wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, the D-Link wireless family of products will allow you to securely access the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A Wireless Access point is a device used to provide this link.

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office.

D-Link is the worldwide leader and award winning designer, developer, and manufacturer of networking products. D-Link delivers the performance you need at a price you can afford. D-Link has all the products you need to build your network.

How does wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away.

Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn’t use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology has become so popular in recent years that almost everyone is using it, whether it’s for home, office, business, D-Link has a wireless solution for it.

Home

- Gives everyone at home broadband access
- Surf the web, check email, instant message, etc.
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

- Stay on top of everything at home as you would at office
- Remotely access your office network from home
- Share Internet connection and printer with multiple computers
- No need to dedicate office space

Where is wireless used?

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it’s becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called “hotspots”.

Using a D-Link Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

Wireless network is easy to setup, but if you’re installing it for the first time it could be quite a task not knowing where to start. That’s why we’ve put together a few setup steps and tips to help you through the process of setting up a wireless network.

Tips

Here are a few things to keep in mind, when you install a wireless network.

Centralize your access point or Access Point

Make sure you place the bridge/access point in a centralized location within your network for the best performance. Try to place the bridge/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a Repeater to boost the signal to extend the range.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, wireless speakers, and televisions as far away as possible from the bridge/access point. This would significantly reduce any interference that the appliances might cause since they operate on same frequency.

Security

Don’t let your next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the access point. Refer to product manual for detail information on how to set it up.

Wireless Modes

There are basically two modes of networking:

- **Infrastructure –** All wireless clients will connect to an access point or wireless bridge.
- **Ad-Hoc –** Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more wireless network Cardbus adapters.

An Infrastructure network contains an Access Point or wireless bridge. All the wireless devices, or clients, will connect to the wireless bridge or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

Networking Basics

Check your IP address

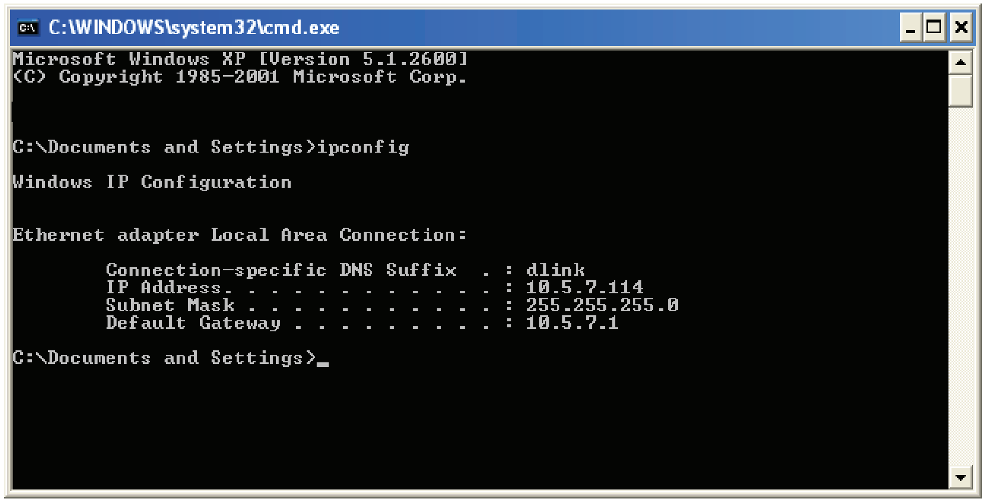
After you install your adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on Start > Run. In the run box type **cmd** and click **OK**. (Windows® 7/Vista® users type cmd in the Start Search box.)

At the prompt, type **ipconfig** and press **Enter**.

This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.


C:\Documents and Settings>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : dlink
        IP Address. . . . . . . . . . . . : 10.5.7.114
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.5.7.1

C:\Documents and Settings>_
```

Statically Assign an IP address

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Step 1

Windows® 7 - Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Change Adapter Setting.**

Windows Vista® - Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Manage Network Connections.**

Windows® XP - Click on **Start** > **Control Panel** > **Network Connections**.

Windows® 2000 - From the desktop, right-click **My Network Places** > **Properties**.

Step 2

Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.

Step 3

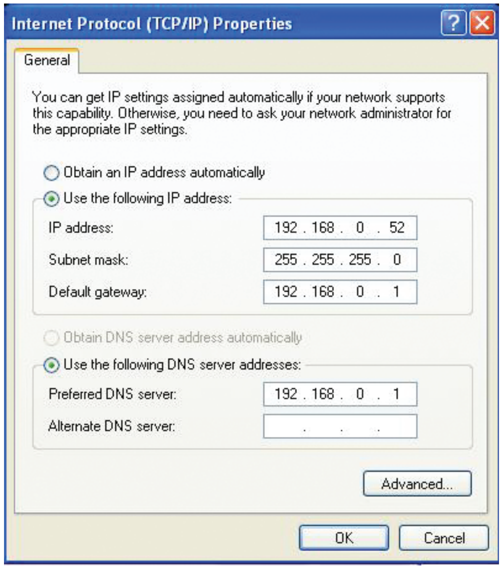
Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

Step 4

Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router´s LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 52

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1

Alternate DNS server: . . .

Step 5

Click **OK** twice to save your settings.

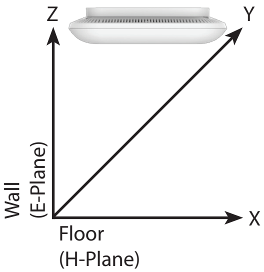
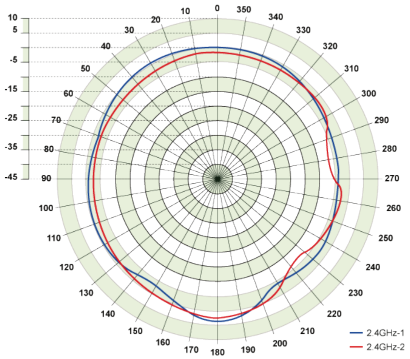
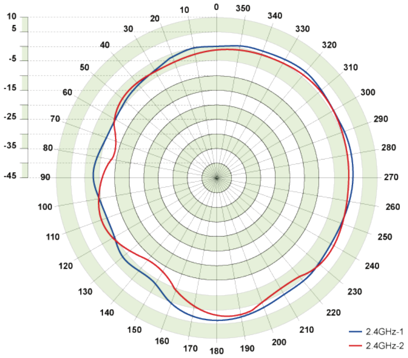
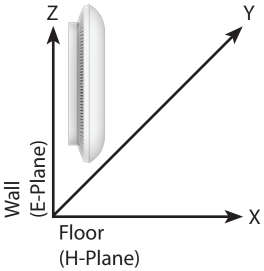
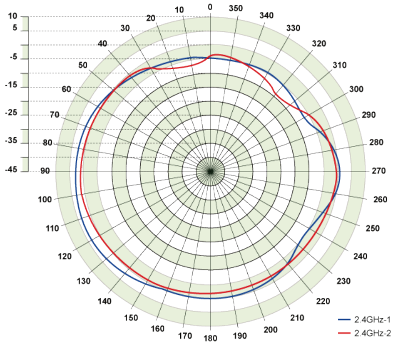
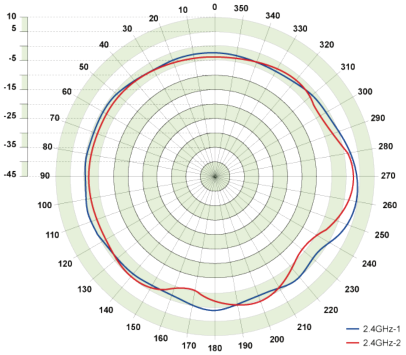
Technical Specifications

DAP-2230			
Functionality	Standards	▪ IEEE 802.11n/g/b ▪ IEEE 802.3	▪ IEEE 802.3u ▪ IEEE 802.3af
	Network Management	▪ Web Browser Interface ▪ HTTP, Secure HTTP (HTTPS) ▪ Telnet, Secure Telnet (SSH)	▪ SNMP v1, v2c, and v3 ▪ Traffic Control ▪ D-Link Central WiFiManager ▪ AP Array
	Security	▪ WPA-Personal & Enterprise ▪ WPA2-Personal & Enterprise ▪ WEP 64/128 bit Encryption ▪ 802.1X	▪ SSID Broadcast disable ▪ MAC Address Control ▪ Network Access Protection (NAP) ▪ Internal Radius Server
	Operational Modes	▪ Access Point ▪ Wireless Distribution System	▪ Wireless Distribution System with AP ▪ Wireless Client
Physical	LEDs	▪ Power	
	Device Interfaces	▪ 802.11b/g/n wireless	▪ One 10/100 LAN port (PoE support)
	Antenna	▪ Built-in 3 dBi antenna	
	Wireless Frequency	▪ 2.4 GHz to 2.4835 GHz	
	Maximum Transmit Power Ouput[1]	▪ 29.84dBm (964mW)	
	Operating voltage	▪ 48 VDC 0.5A, or 802.3af PoE compliant ▪ 12 VDC 1 A auxillary power input	
	Maximum Power Consumption	▪ 16.8 watts	
	Operating Temperature	▪ 0 to 40 °C (32 to 104 °F)	
	Storage Temperature	▪ -20 to 65 °C (-4 to 149 °F)	
	Operating Humidity	▪ 0 to 90% (non-condensing)	
	Storage Humidity	▪ 5 to 95% (non-condensing)	
	Dimensions (L x W x H)	▪ 129 x 129 x 29 mm (5.08 x 5.08 x 1.14 inches)	
	Weight	▪ 101.4 grams (3.56 ounces)	▪ 213.6 grams (7.5 ounces) with wall plate

[1] Range will vary depending on country's maximum transmit power output regulation. Maximum wireless signal rate derived from IEEE Standard 802.11g and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

Certifications	Safety & Emissions	▪ FCC ▪ IC ▪ CE	▪ UL ▪ Wi-Fi Certified

Antenna Pattern

Antenna Pattern		
Orientation	**H-Plane**	**E-Plane**
Ceiling Mounted  	 	
Wall Mounted  	 	

Regulatory Information

Caution: Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adapter first before connecting it to a power outlet.

Federal Communication Commission Interference Statement:
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Non-modifications Statement:
Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

Caution:
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

Note:
The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all Wi-Fi product marketed in US must fixed to US operation channels only.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

Industry Canada Statement:
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) this device may not cause interference, and
(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Radiation Exposure Statement
This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

Déclaration d'exposition aux radiations
Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

European Union:

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. For more information, please refer to the Declaration of Conformity.

Notice of Wireless Radio LAN Usage in The European Community:

• At the time of writing this addendum, some countries such as Italy, Greece, Portugal and Spain have not allowed operation of radio devices in the 5 Ghz bands, although operation of 2.4 Ghz radio devices are allowed. Please check with your local authority to confirm.
• This device is restricted to indoor use when operated in the European Community using channels in the 5.15-5.35 GHz band to reduce the potential for interference.
• This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France where restrictive use applies. This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIR P in the frequency range of 2454 –2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

This equipment may be operated in AL, AD , BE , BG, DK, DE , FI, FR, GR, GW, IS, IT , HR , LI, LU, MT , MK, MD , MC , NL, NO, AT, OL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Usage Notes:

• To remain in conformance with European National spectrum usage regulations, frequency and channel limitations will be applied on the products according to the country where the equipment will be deployed.
• This device is restricted from functioning in Ad-hoc mode while operating in 5 Ghz. Ad-hoc mode is direct peer-to-peer communication between two client devices without an Access Point.
• Access points will support DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control) functionality as required when operating in 5 Ghz within the EU.

2.4 GHz Wireless Frequency and Channel Operation in EEC Countries:

CE

Region	Frequency Band	Max output power (EIRP)
Metropolitan	2400 - 2454 MHz	100 mW
Guadeloupe, Martinique, St Pierre et Miquelon, Mayotte	2454 - 2483.5 MHz	100 mW indoor, 10 mW outdoor
Reunion et Guyane	2400 - 2483.5 MHz	100 mW
Rest of EU community	2420 - 2483.5 MHz	100 mW

<table>
<tr><th colspan="4">R&TTE 1999/5/EC</th></tr>
<tr><th colspan="4">WLAN 2.4 - 2.4835 GHz</th></tr>
<tr><th colspan="4">IEEE 802.11b/g/n</th></tr>
<tr><th>Spectrum Regulation</th><th>MHz, Europa (ETSI)</th><th>max. EIRP Innenbereich</th><th>max. EIRP Außenbereich</th></tr>
<tr><td>Europa</td><td>2400 - 2483,5 MHz</td><td>100 mW</td><td>100 mW</td></tr>
<tr><td rowspan="2">Frankreich</td><td>2400 - 2454 MHz</td><td>100 mW</td><td>100 mW</td></tr>
<tr><td>2454 - 2483,5 MHz</td><td>100 mW</td><td>10 mW</td></tr>
</table>

European Community Declaration of Conformity:

Česky [Czech]	D-Link tímto prohlašuje, že tento DAP-2230 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede D-Link erklærer herved, at følgende udstyr DAP-2230 overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt D-Link, dass sich das Gerät DAP-2230 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab D-Link seadme DAP-2230 vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, D-Link, declares that this DAP-2230 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente D-Link declara que el DAP-2230 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ D-Link ΔΗΛΩΝΕΙ ΟΤΙ DAP-2230 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente D-Link déclare que l'appareil DAP-2230 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente D-Link dichiara che questo DAP-2230 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo D-Link deklarē, ka DAP-2230 atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo D-Link deklaruoja, kad šis DAP-2230 atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart D-Link dat het toestel DAP-2230 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

Malti [Maltese]	Hawnhekk, D-Link, jiddikjara li dan DAP-2230 jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, D-Link nyilatkozom, hogy a DAP-2230 megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym D-Link oświadcza, że DAP-2230 jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	D-Link declara que este DAP-2230 está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	D-Link izjavlja, da je ta DAP-2230 v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	D-Link týmto vyhlasuje, že DAP-2230 spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	D-Link vakuuttaa täten että DAP-2230 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Warning Statement:
The power outlet should be near the device and easily accessible.

Safety Instructions

Please adhere to the following safety guidelines to help ensure your own personal safety and protect your system from potential damage. Any acts taken that are inconsistent with ordinary use of the product, including improper testing, etc., and those not expressly approved by D-Link may result in the loss of product warranty.

Unless expressly approved by an authorized representative of D-Link in writing, you may not and may not permit others to:

- Disassemble or reverse engineer the device or attempt to derive source code (underlying ideas, algorithms, or structure) from the device or from any other information provided by D-Link, except to the extent that this restriction is expressly prohibited by local law.
- Modify or alter the device.
- Remove from the device any product identification or other notices, including copyright notices and patent markings, if any.

To reduce the risk of bodily injury, electrical shock, fire, and damage to the device and other equipment, observe the following precautions:

Power Sources

- Observe and follow service markings.
- Do not push any objects into the openings of your device unless consistent with the authorized operation of the device. Doing so can cause a fire or an electrical shock by shorting out interior components.
- The powering of this device must adhere to the power specifications indicated for this product.
- Do not overload wall outlets and/or extension cords as this will increase the risk of fire or electrical shock.
- Do not rest anything on the power cord or on the device (unless the device is made and expressly approved as suitable for stacking).
- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Operate the device only from the type of external power source indicated on the electrical ratings label.
- To help avoid damaging your device, be sure the voltage selection switch (if provided) on the power supply is set to match the power available at your location.
- Also be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided a power cable for your device or for any AC -powered option intended for your device, purchase a power cable that is approved for use in your country and is suitable for use with your device. The power cable must be rated for the device and for the voltage and current marked on the device's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the device.

- To help prevent an electrical shock, plug the device and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Ensure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your device from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your device, observe the following guidelines.
- Install the power supply before connecting the power cable to the power supply.
- Unplug the power cable before removing the power supply.
- If the system has multiple sources of power, disconnect power from the device by unplugging all power cables from the power supplies.

Servicing/Disassembling

- Do not service any product except as expressly set forth in your system documentation.
- Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to an electrical shock. Only a trained service technician should service components inside these compartments.
- To reduce the risk of electrical shock, never disassemble this device. None of its internal parts are user-replaceable; therefore, there is no reason to access the interior.
- Do not spill food or liquids on your system components, and never operate the device in a wet environment. If the device gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Use the device only with approved equipment.
- Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

Environment

- Do not use this device near water (e.g. near a bathtub, sink, laundry tub, fish tank, in a wet basement or near a swimming pool).
- Do not use this device in areas with high humidity.

- This device must not be subjected to water or condensation.
- Keep your device away from radiators and heat sources. Also, do not block cooling vents.

Cleaning

- Always unplug the power before cleaning this device.
- Do not use liquid or aerosol cleaners of any kind. Use only compressed air that is recommended for electronic devices.
- Use a dry cloth for cleaning.

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside your system. To prevent static damage, discharge static electricity from your body before you touch any of the electronic components, such as the microprocessor. You can do so by periodically touching an unpainted metal surface on the chassis.

You can also take the following steps to help prevent damage from electrostatic discharge (ESD):

1. When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
2. When transporting a sensitive component, first place it in an antistatic container or packaging.
3. Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads, workbench pads, and an antistatic grounding strap.

Environmental

This product may contain a battery. Recycle or dispose of batteries in accordance with the battery manufacturer's instructions and local/national disposal and recycling regulations. For more information, please refer to the warranty guide.

Disposing of and Recycling Your Product

ENGLISH

This symbol on the product or packaging means that according to local laws and regulations this product should be not be disposed of in the household waste but sent for recycling. Please take it to a collection point designated by your local authorities once it has reached the end of its life, some will accept products for free. By recycling the product and its packaging in this manner you help to conserve the environment and protect human health.

D-Link and the Environment

At D-Link, we understand and are committed to reducing any impact our operations and products may have on the environment. To minimise this impact D-Link designs and builds its products to be as environmentally friendly as possible, by using recyclable, low toxic materials in both products and packaging.

D-Link recommends that you always switch off or unplug your D-Link products when they are not in use. By doing so you will help to save energy and reduce CO2 emissions.

To learn more about our environmentally responsible products and packaging please visit www.dlinkgreen.com

DEUTSCH DE

Dieses Symbol auf dem Produkt oder der Verpackung weist darauf hin, dass dieses Produkt gemäß bestehender örtlicher Gesetze und Vorschriften nicht über den normalen Hausmüll entsorgt werden sollte, sondern einer Wiederverwertung zuzuführen ist. Bringen Sie es bitte zu einer von Ihrer Kommunalbehörde entsprechend amtlich ausgewiesenen Sammelstelle, sobald das Produkt das Ende seiner Nutzungsdauer erreicht hat. Für die Annahme solcher Produkte erheben einige dieser Stellen keine Gebühren. Durch ein auf diese Weise durchgeführtes Recycling des Produkts und seiner Verpackung helfen Sie, die Umwelt zu schonen und die menschliche Gesundheit zu schützen.

D-Link und die Umwelt

D-Link ist sich den möglichen Auswirkungen seiner Geschäftstätigkeiten und seiner Produkte auf die Umwelt bewusst und fühlt sich verpflichtet, diese entsprechend zu mindern. Zu diesem Zweck entwickelt und stellt D-Link seine Produkte mit dem Ziel größtmöglicher Umweltfreundlichkeit her und verwendet wiederverwertbare, schadstoffarme Materialien bei Produktherstellung und Verpackung.

D-Link empfiehlt, Ihre Produkte von D-Link, wenn nicht in Gebrauch, immer auszuschalten oder vom Netz zu nehmen. Auf

diese Weise helfen Sie, Energie zu sparen und CO2-Emissionen zu reduzieren.
Wenn Sie mehr über unsere umweltgerechten Produkte und Verpackungen wissen möchten, finden Sie entsprechende Informationen im Internet unter www.dlinkgreen.com.

FRANÇAIS FR

Ce symbole apposé sur le produit ou son emballage signifie que, conformément aux lois et règlementations locales, ce produit ne doit pas être éliminé avec les déchets domestiques mais recyclé. Veuillez le rapporter à un point de collecte prévu à cet effet par les autorités locales; certains accepteront vos produits gratuitement. En recyclant le produit et son emballage de cette manière, vous aidez à préserver l'environnement et à protéger la santé de l'homme.

D-Link et l'environnement

Chez D-Link, nous sommes conscients de l'impact de nos opérations et produits sur l'environnement et nous engageons à le réduire. Pour limiter cet impact, D-Link conçoit et fabrique ses produits de manière aussi écologique que possible, en utilisant des matériaux recyclables et faiblement toxiques, tant dans ses produits que ses emballages.
D-Link recommande de toujours éteindre ou débrancher vos produits D-Link lorsque vous ne les utilisez pas. Vous réaliserez ainsi des économies d'énergie et réduirez vos émissions de CO2.
Pour en savoir plus sur les produits et emballages respectueux de l'environnement, veuillez consulter le www.dlinkgreen.com

ESPAÑOL ES

Este símbolo en el producto o el embalaje significa que, de acuerdo con la legislación y la normativa local, este producto no se debe desechar en la basura doméstica sino que se debe reciclar. Llévelo a un punto de recogida designado por las autoridades locales una vez que ha llegado al fin de su vida útil; algunos de ellos aceptan recogerlos de forma gratuita. Al reciclar el producto y su embalaje de esta forma, contribuye a preservar el medio ambiente y a proteger la salud de los seres humanos.

D-Link y el medio ambiente

En D-Link, comprendemos y estamos comprometidos con la reducción del impacto que puedan tener nuestras actividades y nuestros productos en el medio ambiente. Para reducir este impacto, D-Link diseña y fabrica sus productos para que sean lo más ecológicos posible, utilizando materiales reciclables y de baja toxicidad tanto en los productos como en el embalaje.

D-Link recomienda apagar o desenchufar los productos D-Link cuando no se estén utilizando. Al hacerlo, contribuirá a ahorrar energía y a reducir las emisiones de CO2.
Para obtener más información acerca de nuestros productos y embalajes ecológicos, visite el sitio www.dlinkgreen.com

ITALIANO IT

La presenza di questo simbolo sul prodotto o sulla confezione del prodotto indica che, in conformità alle leggi e alle normative locali, questo prodotto non deve essere smaltito nei rifiuti domestici, ma avviato al riciclo. Una volta terminato il ciclo di vita utile, portare il prodotto presso un punto di raccolta indicato dalle autorità locali. Alcuni questi punti di raccolta accettano gratuitamente i prodotti da riciclare. Scegliendo di riciclare il prodotto e il relativo imballaggio, si contribuirà a preservare l'ambiente e a salvaguardare la salute umana.

D-Link e l'ambiente

D-Link cerca da sempre di ridurre l'impatto ambientale dei propri stabilimenti e dei propri prodotti. Allo scopo di ridurre al minimo tale impatto, D-Link progetta e realizza i propri prodotti in modo che rispettino il più possibile l'ambiente, utilizzando materiali riciclabili a basso tasso di tossicità sia per i prodotti che per gli imballaggi.
D-Link raccomanda di spegnere sempre i prodotti D-Link o di scollegarne la spina quando non vengono utilizzati. In questo modo si contribuirà a risparmiare energia e a ridurre le emissioni di anidride carbonica.
Per ulteriori informazioni sui prodotti e sugli imballaggi D-Link a ridotto impatto ambientale, visitate il sito all'indirizzo www.dlinkgreen.com

NEDERLANDS NL

Dit symbool op het product of de verpakking betekent dat dit product volgens de plaatselijke wetgeving niet mag worden weggegooid met het huishoudelijk afval, maar voor recyclage moeten worden ingeleverd. Zodra het product het einde van de levensduur heeft bereikt, dient u het naar een inzamelpunt te brengen dat hiertoe werd aangeduid door uw plaatselijke autoriteiten, sommige autoriteiten accepteren producten zonder dat u hiervoor dient te betalen.
Door het product en de verpakking op deze manier te recyclen helpt u het milieu en de gezondheid van de mens te beschermen.

D-Link en het milieu

Bij D-Link spannen we ons in om de impact van onze handelingen en producten op het milieu te beperken. Om deze impact te beperken, ontwerpt en bouwt D-Link zijn producten zo milieuvriendelijk mogelijk, door het gebruik van recycleerbare producten met lage toxiciteit in product en verpakking.

D-Link raadt aan om steeds uw D-Link producten uit te schakelen of uit de stekker te halen wanneer u ze niet gebruikt. Door dit te doen bespaart u energie en beperkt u de CO2-emissies.

Breng een bezoek aan www.dlinkgreen.com voor meer informatie over onze milieuverantwoorde producten en verpakkingen

POLSKI PL

Ten symbol umieszczony na produkcie lub opakowaniu oznacza, że zgodnie z miejscowym prawem i lokalnymi przepisami niniejszego produktu nie wolno wyrzucać jak odpady czy śmieci z gospodarstwa domowego, lecz należy go poddać procesowi recyklingu. Po zakończeniu użytkowania produktu, niektóre odpowiednie do tego celu podmioty przyjmą takie produkty nieodpłatnie, dlatego prosimy dostarczyć go do punktu zbiórki wskazanego przez lokalne władze.

Poprzez proces recyklingu i dzięki takiemu postępowaniu z produktem oraz jego opakowaniem, pomogą Państwo chronić środowisko naturalne i dbać o ludzkie zdrowie.

D-Link i środowisko

W D-Link podchodzimy w sposób świadomy do ochrony otoczenia oraz jesteśmy zaangażowani w zmniejszanie wpływu naszych działań i produktów na środowisko naturalne. W celu zminimalizowania takiego wpływu firma D-Link konstruuje i wytwarza swoje produkty w taki sposób, aby były one jak najbardziej przyjazne środowisku, stosując do tych celów materiały nadające się do powtórnego wykorzystania, charakteryzujące się małą toksycznością zarówno w przypadku samych produktów jak i opakowań.

Firma D-Link zaleca, aby Państwo zawsze prawidłowo wyłączali z użytku swoje produkty D-Link, gdy nie są one wykorzystywane. Postępując w ten sposób pozwalają Państwo oszczędzać energię i zmniejszać emisje CO2.

"Aby dowiedzieć się więcej na temat produktów i opakowań mających wpływ na środowisko prosimy zapoznać się ze stroną Internetową www.dlinkgreen.com."

ČESKY CZ

Tento symbol na výrobku nebo jeho obalu znamená, že podle místně platných předpisů se výrobek nesmí vyhazovat do komunálního odpadu, ale odeslat k recyklaci. Až výrobek doslouží, odneste jej prosím na sběrné místo určené místními úřady k tomuto účelu. Některá sběrná místa přijímají výrobky zdarma. Recyklací výrobku i obalu pomáháte chránit životní prostředí i lidské zdraví.

D-Link a životní prostředí

"Ve společnosti D-Link jsme si vědomi vlivu našich provozů a výrobků na životní prostředí a snažíme se o minimalizaci těchto vlivů. Proto své výrobky navrhujeme a vyrábíme tak, aby byly co nejekologičtější, a ve výrobcích i obalech používáme recyklovatelné a nízkotoxické materiály."
"Společnost D-Link doporučuje, abyste své výrobky značky D-Link vypnuli nebo vytáhli ze zásuvky vždy, když je nepoužíváte. Pomůžete tak šetřit energii a snížit emise CO2."
Více informací o našich ekologických výrobcích a obalech najdete na adrese www.dlinkgreen.com.

MAGYAR HU

Ez a szimbólum a terméken vagy a csomagoláson azt jelenti, hogy a helyi törvényeknek és szabályoknak megfelelően ez a termék nem semmisíthető meg a háztartási hulladékkal együtt, hanem újrahasznosításra kell küldeni. Kérjük, hogy a termék élettartamának elteltét követően vigye azt a helyi hatóság által kijelölt gyűjtőhelyre. A termékek egyes helyeken ingyen elhelyezhetők. A termék és a csomagolás újrahasznosításával segíti védeni a környezetet és az emberek egészségét.

A D-Link és a környezet

A D-Linknél megértjük és elkötelezettek vagyunk a műveleteink és termékeink környezetre gyakorolt hatásainak csökkentésére. Az ezen hatás csökkentése érdekében a D-Link a lehető leginkább környezetbarát termékeket tervez és gyárt azáltal, hogy újrahasznosítható, alacsony károsanyag-tartalmú termékeket gyárt és csomagolásokat alkalmaz.
A D-Link azt javasolja, hogy mindig kapcsolja ki vagy húzza ki a D-Link termékeket a
tápforrásból, ha nem használja azokat. Ezzel segít az energia megtakarításában és a széndioxid kibocsátásának csökkentésében.
Környezetbarát termékeinkről és csomagolásainkról további információkat a www.dlinkgreen.com weboldalon tudhat meg.

NORSK NO

Dette symbolet på produktet eller forpakningen betyr at dette produktet ifølge lokale lover og forskrifter ikke skal kastes sammen med husholdningsavfall, men leveres inn til gjenvinning. Vennligst ta det til et innsamlingssted anvist av lokale myndigheter når det er kommet til slutten av levetiden. Noen steder aksepteres produkter uten avgift. Ved på denne måten å gjenvinne produktet og forpakningen hjelper du å verne miljøet og beskytte folks helse.

D-Link og miljøet

Hos D-Link forstår vi oss på og er forpliktet til å minske innvirkningen som vår drift og våre produkter kan ha på miljøet. For å minimalisere denne innvirkningen designer og lager D-Link produkter som er så miljøvennlig som mulig, ved å bruke resirkulerbare, lav-toksiske materialer både i produktene og forpakningen.

D-Link anbefaler at du alltid slår av eller frakobler D-Link-produkter når de ikke er i bruk. Ved å gjøre dette hjelper du å spare energi og å redusere CO2-utslipp.

"For mer informasjon angående våre miljøansvarlige produkter og forpakninger kan du gå til www.dlinkgreen.com"

DANSK DK

Dette symbol på produktet eller emballagen betyder, at dette produkt i henhold til lokale love og regler ikke må bortskaffes som husholdningsaffald, mens skal sendes til genbrug. Indlever produktet til et indsamlingssted som angivet af de lokale myndigheder, når det er nået til slutningen af dets levetid. I nogle tilfælde vil produktet blive modtaget gratis. Ved at indlevere produktet og dets emballage til genbrug på denne måde bidrager du til at beskytte miljøet og den menneskelige sundhed.

D-Link og miljøet

Hos D-Link forstår vi og bestræber os på at reducere enhver indvirkning, som vores aktiviteter og produkter kan have på miljøet. For at minimere denne indvirkning designer og producerer D-Link sine produkter, så de er så miljøvenlige som muligt, ved at bruge genanvendelige materialer med lavt giftighedsniveau i både produkter og emballage.

D-Link anbefaler, at du altid slukker eller frakobler dine D-Link-produkter, når de ikke er i brug. Ved at gøre det bidrager du til at spare energi og reducere CO2-udledningerne.

Du kan finde flere oplysninger om vores miljømæssigt ansvarlige produkter og emballage på www.dlinkgreen.com

SUOMI FI

Tämä symboli tuotteen pakkauksessa tarkoittaa, että paikallisten lakien ja säännösten mukaisesti tätä tuotetta ei pidä hävittää yleisen kotitalousjätteen seassa vaan se tulee toimittaa kierrätettäväksi. Kun tuote on elinkaarensa päässä, toimita se lähimpään viranomaisten hyväksymään kierrätyspisteeseen. Kierrättämällä käytetyn tuotteen ja sen pakkauksen autat tukemaan sekä ympäristön että ihmisten terveyttä ja hyvinvointia.

D-Link ja ympäristö

D-Link ymmärtää ympäristönsuojelun tärkeyden ja on sitoutunut vähentämään tuotteistaan ja niiden valmistuksesta ympäristölle mahdollisesti aiheutuvia haittavaikutuksia. Nämä negatiiviset vaikutukset minimoidakseen D-Link suunnittelee ja valmistaa tuotteensa mahdollisimman ympäristöystävällisiksi käyttämällä kierrätettäviä, alhaisia pitoisuuksia haitallisia aineita sisältäviä materiaaleja sekä tuotteissaan että niiden pakkauksissa.

Suosittelemme, että irrotat D-Link-tuotteesi virtalähteestä tai sammutat ne aina, kun ne eivät ole käytössä. Toimimalla näin autat säästämään energiaa ja vähentämään hiilidioksiidipäästöjä.

"Lue lisää ympäristöystävällisistä D-Link-tuotteista ja pakkauksistamme osoitteesta www.dlinkgreen.com"

SVENSKA SE

Den här symbolen på produkten eller förpackningen betyder att produkten enligt lokala lagar och föreskrifter inte skall kastas i hushållssoporna utan i stället återvinnas. Ta den vid slutet av dess livslängd till en av din lokala myndighet utsedd uppsamlingsplats, vissa accepterar produkter utan kostnad. Genom att på detta sätt återvinna produkten och förpackningen hjälper du till att bevara miljön och skydda människors hälsa.

D-Link och miljön

På D-Link förstår vi och är fast beslutna att minska den påverkan våra verksamheter och produkter kan ha på miljön. För att minska denna påverkan utformar och bygger D-Link sina produkter för att de ska vara så miljövänliga som möjligt, genom att använda återvinningsbara material med låg gifthalt i både produkter och förpackningar.

D-Link rekommenderar att du alltid stänger av eller kopplar ur dina D-Link produkter när du inte använder dem. Genom att göra detta hjälper du till att spara energi och minska utsläpp av koldioxid.

För mer information om våra miljöansvariga produkter och förpackningar www.dlinkgreen.com

PORTUGUÊS PT

Este símbolo no produto ou embalagem significa que, de acordo com as leis e regulamentações locais, este produto não deverá ser eliminado juntamente com o lixo doméstico mas enviado para a reciclagem. Transporte-o para um ponto de recolha designado pelas suas autoridades locais quando este tiver atingido o fim da sua vida útil, alguns destes pontos aceitam produtos gratuitamente. Ao reciclar o produto e respectiva embalagem desta forma, ajuda a preservar o ambiente e protege a saúde humana.

A D-Link e o ambiente

Na D-Link compreendemos e comprometemo-nos com a redução do impacto que as nossas operações e produtos possam ter no ambiente. Para minimizar este impacto a D-Link concebe e constrói os seus produtos para que estes sejam o mais inofensivos para o ambiente possível, utilizando meteriais recicláveis e não tóxicos tanto nos produtos como nas embalagens.

A D-Link recomenda que desligue os seus produtos D-Link quando estes não se encontrarem em utilização. Com esta acção ajudará a poupar energia e reduzir as emissões de CO2.

Para saber mais sobre os nossos produtos e embalagens responsáveis a nível ambiental visite www.dlinkgreen.com