D-Link®
Building Networks for People

DAP-3662

Version 1.00

Wireless AC1200

Concurrent Dual Band Outdoor PoE Access Point

User Manual

Business Class Networking

Table of Contents

Product Overview 4
Package Contents 4
System Requirements 4
Introduction 5
Features and Benefits 6
Hardware Overview 7
Front 7
Back 8
Bottom 9
Wireless Basics 10

Installation 11
Installation Considerations 11
Four Operational Modes 12
Connect to your Network 13

Configuration 14
Wireless Settings 16
Access Point Mode 16
WDS with AP Mode 18
WDS Mode 20
Wireless Client Mode 22
WPA-Personal Authentication 24
WPA-Enterprise Authentication 25
802.1X authentication 26
LAN 27
IPv6 28
Advanced Settings 29
Performance 29
Wireless Resource Control 31
Multi-SSID 33
VLAN Settings 35
VLAN Port List 36
VLAN Add/Edit 37
PVID Setting 38
Intrusion 39
Schedule 40
Internal RADIUS Server 41
ARP Spoofing Prevention 42
Bandwidth Optimization 43
AP Array 45
AP Array Scan 45
Configuration Settings 46
Auto-RF 50
Load Balance 51
Captive Portal 52
Authentication Settings - Passcode 52
Authentication Settings - Username/Password 53
Authentication Settings - Remote RADIUS 54
Authentication Settings - LDAP 55
Authentication Settings - POP3 56
Login Page Upload 57
Web Redirection 58
MAC Bypass 59

DHCP Server 60
Dynamic Pool Settings 60
Static Pool Setting 62
Current IP Mapping List 63
Filters 64
Wireless MAC ACL 64
WLAN Partition 65
Traffic Control 66
Uplink/Downlink Setting 66
QoS 67
Traffic Manager 68
Status 69
Device Information 69
Client Information 70
WDS Information 71
Channel Analyze 72
Stats 73
Ethernet 73
Wireless Traffic Stats 74
Log 75
View Log 75
Log Settings 76
Maintenance 77
Administrator Settings 77
Limit Administrator 77
System Name Settings 77
Login Settings 78
Console Settings 78
SNMP Settings 79
Ping Control Setting 79
Central WiFiManager Settings 79
Firmware and SSL Certification Upload 80
Configuration File 81
Time and Date 82
Configuration 83
Save and Activate 83
Discard Changes 83
System 84
System Settings 84
Help 85

Troubleshooting 86

Antenna Pattern 89

Technical Specifications 90

Package Contents

- DAP-3662 Wireless AC1200 Concurrent Dual Band Outdoor PoE Access Point
- Installation CD-ROM
- Installation Guide
- Mounting kit (Wall/Pole Mount)
  - Stainless steel mount base x 1
  - Stainless tie back straps x 2
  - Wall screw x 4
  - Wall plug x 4
  - Stainless mount screw (hexagonal hole)
- Hexagon Socket Spanner (Security screw)
- Two LAN Port Waterproof Enclosure
- Grounding Wire

Note: *PoE kit (injector and adapter) is NOT include in the package and it can be purchased with the model name "DPE-101GI".*

System Requirements

Network Requirements	• IEEE 802.11n/g wireless clients (AP/bridge modes) • IEEE 802.11n/g wireless router or access point (client mode)
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system **Browser Requirements:** • Internet Explorer Version 7.0, Chrome 12, Safari 4, or Firefox 12 and above (for web-based configuration)

Introduction

D-Link, an industry pioneer in wireless networking, introduces a solution for businesses seeking to deploy next generation draft 802.11n LANs. D-Link unveils its new Wireless AC1200 Concurrent Dual Band Outdoor PoE Access Point (DAP-3662), designed specifically for business-class environments such as large or enterprise corporations to provide secure and manageable dual-band wireless LAN options for network administrators.

Versatile Access Point
The Wireless AC1200 Concurrent Dual Band Outdoor PoE Access Point allows network administrators to deploy a highly manageable and extremely robust dual-band wireless network. All new embedded four dual-band antennas design can provide optimal wireless coverage in either 2.4 GHz (802.11g and 802.11n) or 5 GHz (802.11a, 802.11n, and 802.11ac) bands. Enclosed in a plenum-rated metal chassis, the DAP-3662 adheres to strict fire codes for placement in air passageways. For advanced installations, this new high-speed access point has integrated 802.3af Power over Ethernet (PoE) support, allowing installation of this device in areas where power outlets are not readily available.

Enhanced Performance
The DAP-3662 delivers reliable wireless performance with maximum wireless signal rates of up to 866 in 5 Ghz and 300 Mbps in 2.4 Ghz wireless band. This, coupled with support for Wi-Fi Multimedia™ (WMM) Quality of Service features, makes it an ideal access point for audio, video, and voice applications. Additionally, the DAP-3662 supports load balance features to ensure maximum performance.

Security
To help maintain a secure wireless network, the DAP-3662 provides the latest in wireless security technologies by supporting both Personal and Enterprise versions of WPA and WPA2 (802.11i) with support for RADIUS server backend. To further protect your wireless network, MAC Address Filtering, Wireless LAN segmentation, Disable SSID Broadcast, Rogue AP Detection, and Wireless Broadcast Scheduling are also included.

The Wireless AC1200 Concurrent Dual Band Outdoor PoE Access Point includes support for up to 16 VLANs for implementing multiple SSIDs to further help segment users on the network. The DAP-3662 also includes a wireless client isolation mechanism, which limits direct client-to-client communication.

Features and Benefits

- Four different operation modes - Capable of operating in one of four different operation modes to meet your wireless networking needs: Access Point(AP), WDS with AP, WDS, or Wireless Client.
- Faster wireless networking with the 802.11ac standard to provide a maximum wireless signal rate of up to 1200 Mbps*.
- Backward compatible with the 802.11a/b/g/n standard to maximum flexibility when migrating your network.
- Better security with WPA - The DAP-3662 can securely connect wireless clients on the network using WPA (Wi-Fi Protected Access) to provide a much higher level of security for your data and communications than its previous versions.
- Central WiFiManager management software - The real-time display of the network's topology and AP's information makes network configuration and management quick and simple.
- SNMP for management - The DAP-3662 is not just fast, but also supports SNMP v1 and v2c for better network management. Superior wireless AP manager software is bundled with the DAP-3662 for network configuration and firmware upgrade. Systems administrators can also set up the DAP-3662 easily with the Web-based configuration.
- Utilizes OFDM technology (Orthogonal Frequency Division Multiplexing).
- Supports 802.3af Power over Ethernet.
- Includes two 10/100/1000 Ethernet port.
- Operates in the 2.4~2.5 GHz or 5.15~5.85 GHz** frequency ranges.
- Web-based interface for managing and configuring.

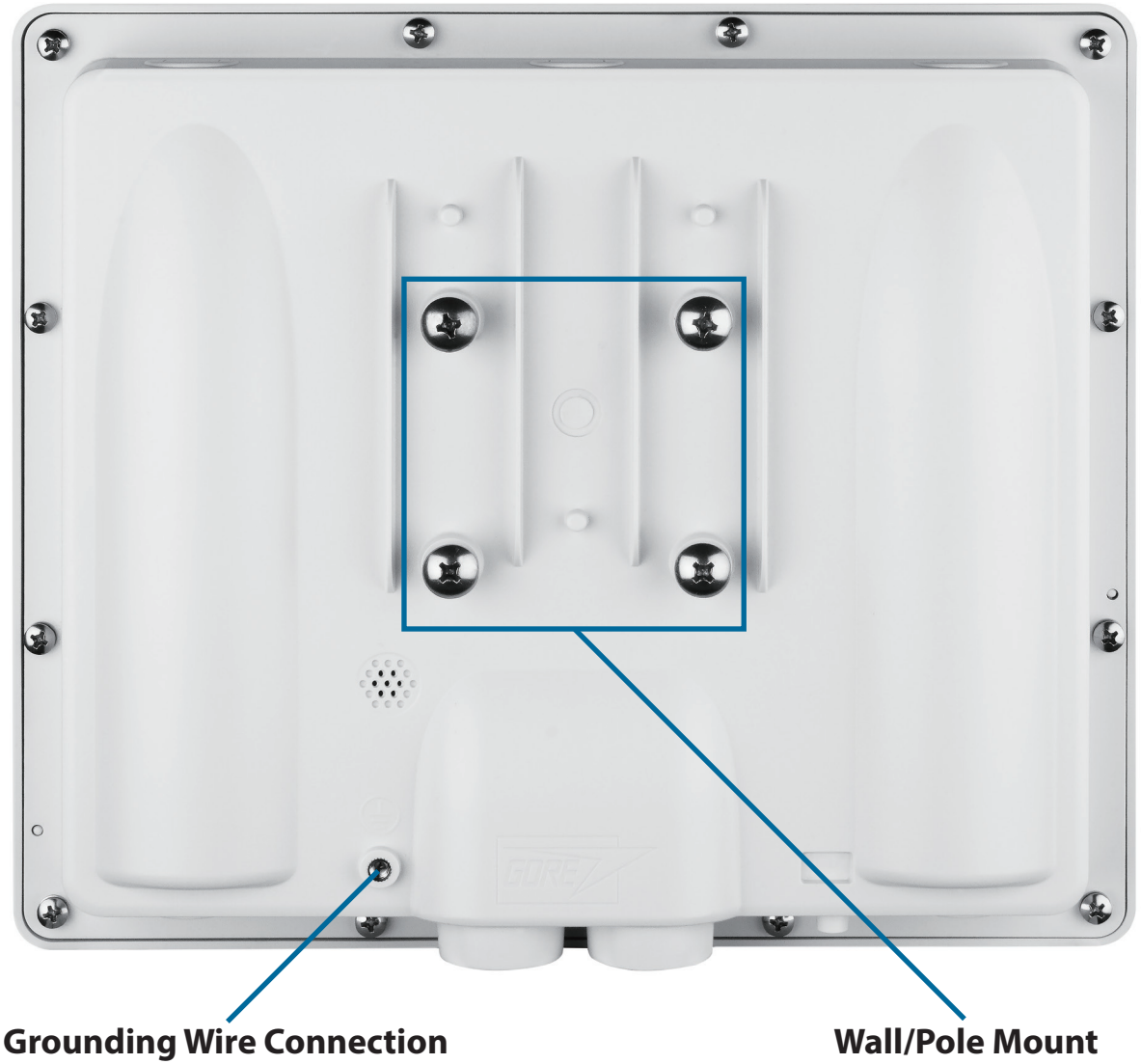
*Maximum wireless signal rate derived from IEEE Standard 802.11g, 802.11a and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

**Please note that operating frequency ranges vary depending on the regulations of individual countries and jurisdictions. The DAP-3662 isn't supported in the 5.25~5.35 GHz and 5.47 ~ 5.725 GHz frequency ranges in some regions.

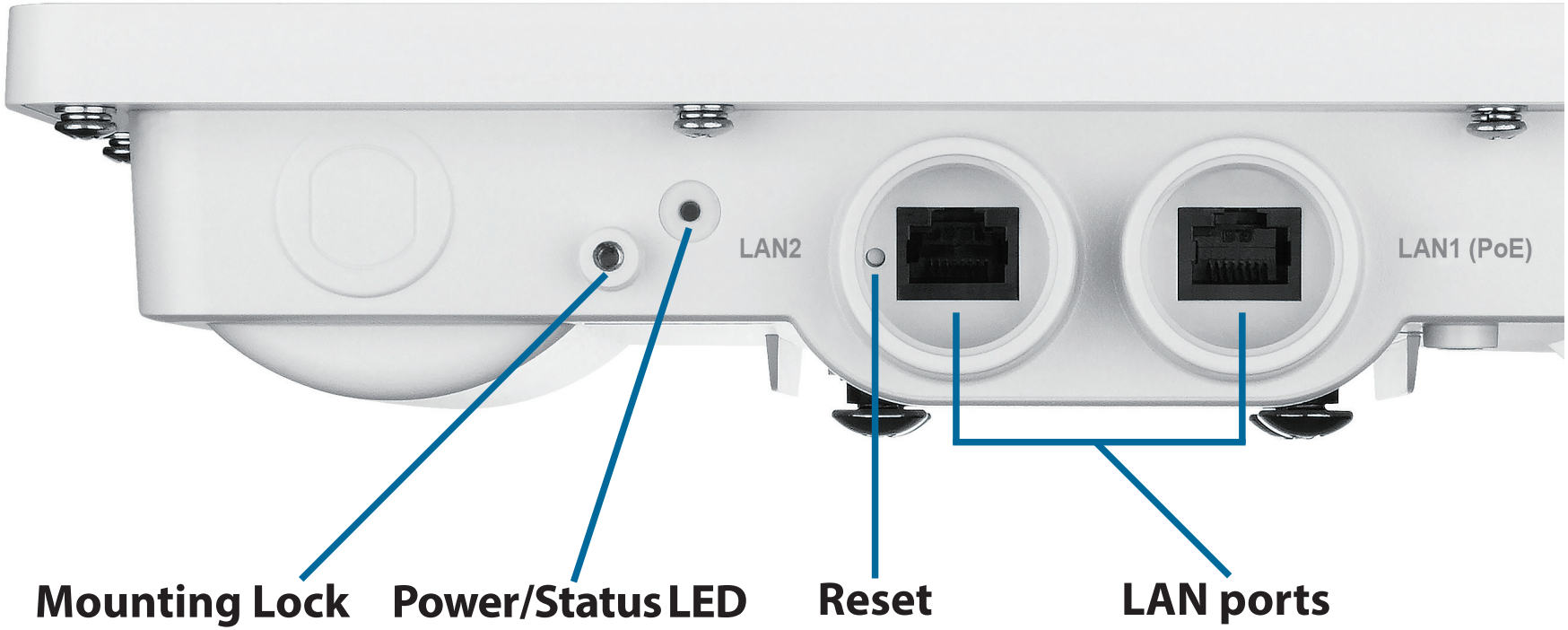
Hardware Overview

Front

Back



Bottom


LAN2
LAN1 (PoE)
Mounting Lock
Power/Status LED
Reset
LAN ports

Wireless Basics

D-Link wireless products are based on industry standards to provide high-speed wireless connectivity that is easy to use within your home, business or public access wireless networks. D-Link wireless products provides you with access to the data you want, whenever and wherever you want it. Enjoy the freedom that wireless networking can bring to you.

WLAN use is not only increasing in both home and office environments, but in public areas as well, such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are allowing people to work and communicate more efficiently. Increased mobility and the absence of cabling and other types of fixed infrastructure have proven to be beneficial to many users.

Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards, allowing wireless users to use the same applications as those used on a wired network.

People use WLAN technology for many different purposes:

Mobility - Productivity increases when people can have access to data in any location within the operating range of their WLAN. Management decisions based on real-time information can significantly improve the efficiency of a worker.

Low implementation costs - WLANs are easy to set up, manage, change and relocate. Networks that frequently change can benefit from WLAN's ease of implementation. WLANs can operate in locations where installation of wiring may be impractical.

Installation and network expansion - By avoiding the complications of troublesome cables, a WLAN system can be fast and easy during installation, especially since it can eliminate the need to pull cable through walls and ceilings. Wireless technology provides more versatility by extending the network beyond the home or office.

Inexpensive solution - Wireless network devices are as competitively priced as conventional Ethernet network devices. The DAP-3662 saves money by providing users with multi-functionality configurable in four different modes.

Scalability - Configurations can be easily changed and range from Peer-to-Peer networks, suitable for a small number of users to larger Infrastructure networks to accommodate hundreds or thousands of users, depending on the number of wireless devices deployed.

Installation
Installation Considerations

The D-Link wireless device 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 device 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 routers, 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.

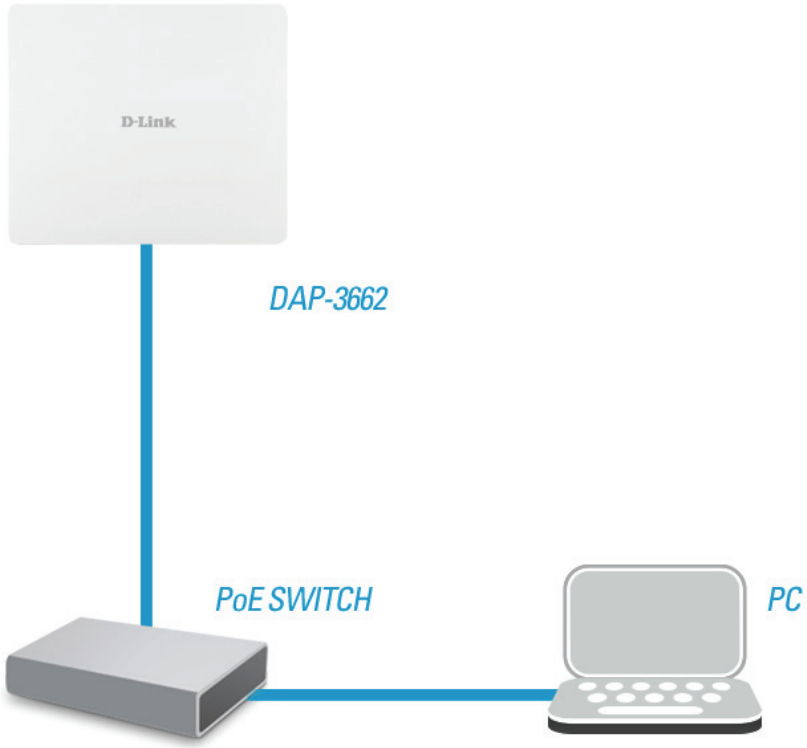
5. If you are using 2.4 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in 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

Connect to your Network

1. Connect an external Power-over-Ethernet (PoE) switch to the LAN1 (PoE) port to power on access point.
2. Connect PC to the switch and you can configure access point through web UI.
3. Open a web browser and go to https://IP address (default is https://192.168.0.50). Enter admin as your username and leave the password blank to log into the web UI. Now you can configure the AP via web UI.



Configuration

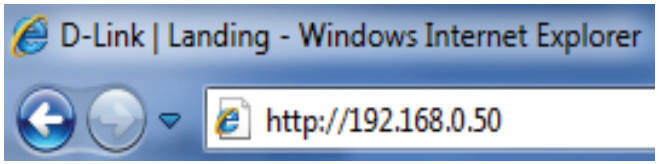
To configure the DAP-3662, use a computer that is connected to the DAP-3662 with an Ethernet cable.

Step 1 - Disable the **Access the Internet using a proxy server** function. To disable this function, go to **Control Panel** > **Internet Options** > **Connections** > **LAN Settings** and uncheck the enable box.

Step 2 - Open your web browser.

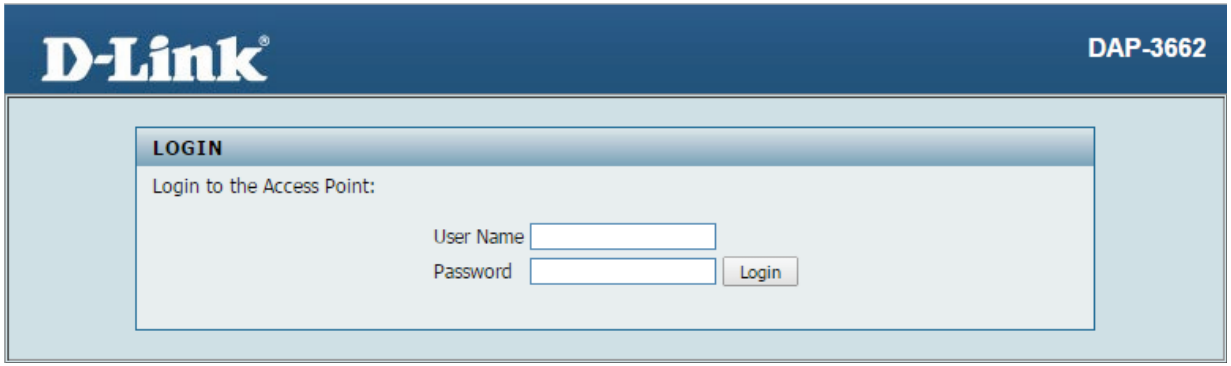
Step 3 - Type the IP address of the DAP-3662 in the address field (**http://192.168.0.50**) and press **Enter**. Make sure that the IP addresses of the DAP-3662 and your computer are in the same subnet.

Note: *If you have changed the default IP address assigned to the DAP-3662, make sure to enter the correct IP address.*

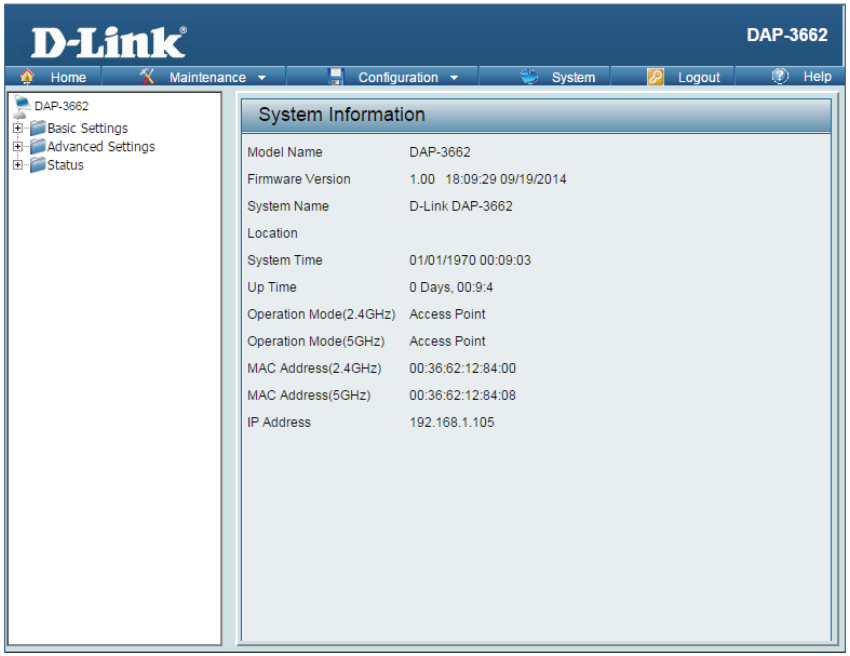


Step 4 - Enter admin for the User Name and then click **Login**. By default the password is blank.

Note: *If you have changed the password, make sure to enter the correct password.*



After successfully logging into the DAP-3662 the following window will appear:

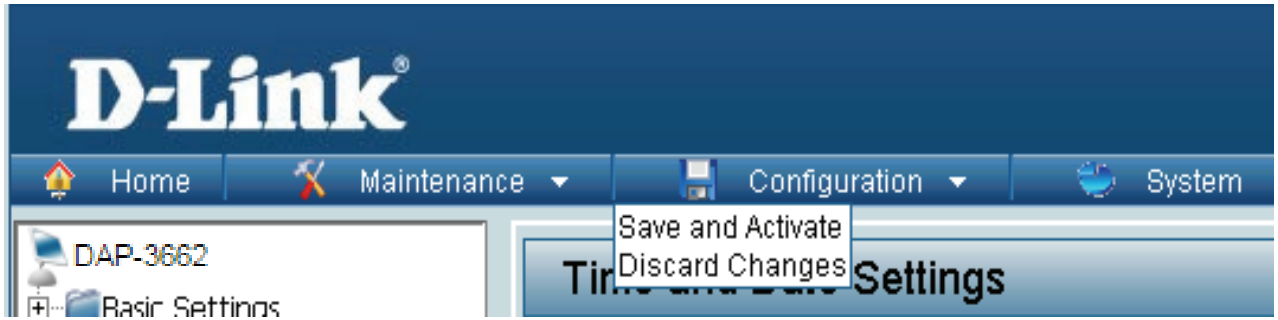


When making changes on most of the configuration windows in this section, use either the **Apply** button or the **Save** button to save your configuration changes.

Click the **Apply** button to configure changes.

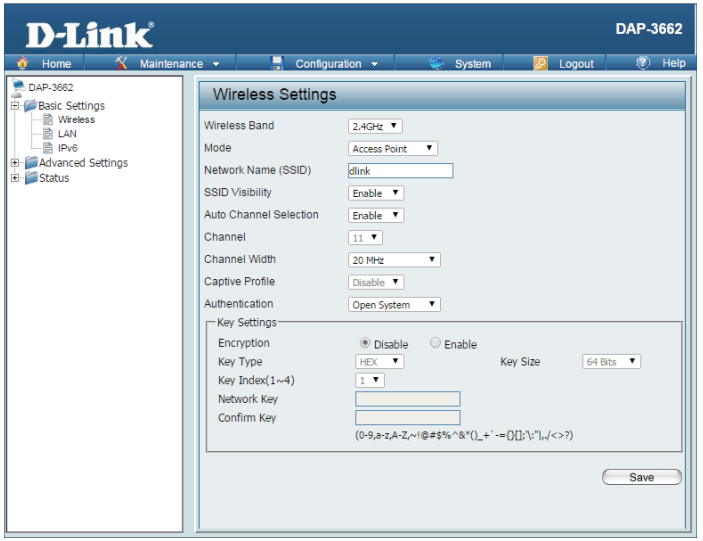
Click the **Save** button to configure changes.

Alternatively, click the **Save and Activate** option on the Configuration drop-down menu at the top of each DAP-3662 window. This will cause the DAP-3662 to save and reboot.



Wireless Settings
Access Point Mode

In Access Point mode, the DAP-3662 functions as a wireless AP. After configuring the desired settings, click the **Save** button.



Wireless Band: Select either **2.4 GHz** or **5 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 default setting is **dlink**. The SSID can easily be 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.

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 selection of the channel width you would like to operate in. **20 MHz** and **Auto 20/40 MHz** allow both 802.11n and non-802.11n wireless devices on your network when the wireless mode is Mixed 802.11 b/g/n in 2.4G and Mixed 802.11 a/n in 5G. When the channel width is set to **Auto 20/40 MHz**, then 802.11n wireless devices are allowed to transmit data using 40 MHz.

Captive Profile: Enable or disable captive profile for user authentication.

Authentication: 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** if your network is using port-based Network Access Control.

For more information about the different types of Authentication offered on the DAP-3662 and the respective settings of each, please go to the first page of the "Authentication" explanations, which begins on page 23.

WDS with AP Mode

In WDS with AP mode, the DAP-3662 wirelessly connects multiple networks while still functioning as a wireless AP. After completing the desired settings, click the **Save** button to let your changes take effect.

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

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

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

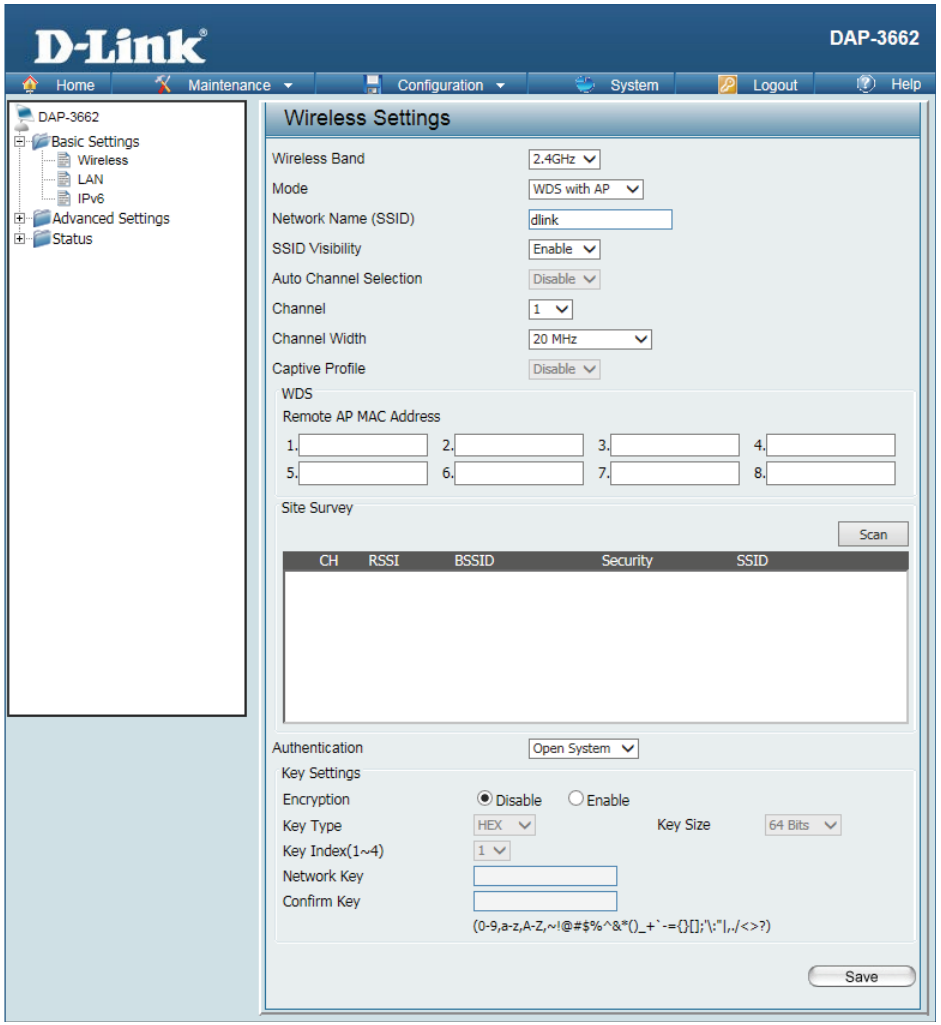
SSID Visibility: **Enable** or **Disable** SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.

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 selection of the channel width you would like to operate in. **20 MHz** and **Auto 20/40 MHz** allow both 802.11n and non-802.11n wireless devices on your network when the wireless mode is Mixed 802.11 b/g/n in 2.4G and Mixed 802.11 a/n in 5G. When the channel width is set to **Auto 20/40 MHz**, then 802.11n wireless devices are allowed to transmit data using 40 MHz.

Captive Profile: Enable or disable captive profile for user authentication.



Remote AP MAC Address: Allows selection of the channel width you would like to operate in. **20 MHz** and **Auto 20/40 MHz** allow both 802.11n and non-802.11n wireless devices on your network when the wireless mode is Mixed 802.11 b/g/n in 2.4G and Mixed 802.11 a/n in 5G. 802.11n wireless devices are allowed to transmit data using 40 MHz when the channel width is **Auto 20/40 MHz**.

Site Survey: Manually enter the MAC addresses of the APs on your network that will serve as bridges to wirelessly connect multiple networks. You may also click the **Scan** button to search for available wireless networks, then click on the available network that you want to connect to.

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

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.

For more information about the different types of Authentication offered on the DAP-3662 and the respective settings of each, please go to the first page of the "Authentication" explanations, which begins on page 23.

WDS Mode

In WDS mode, the DAP-3662 wirelessly connects multiple networks, without functioning as a wireless AP. After completing the desired settings, click the **Save** button to let your changes take effect.

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

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

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

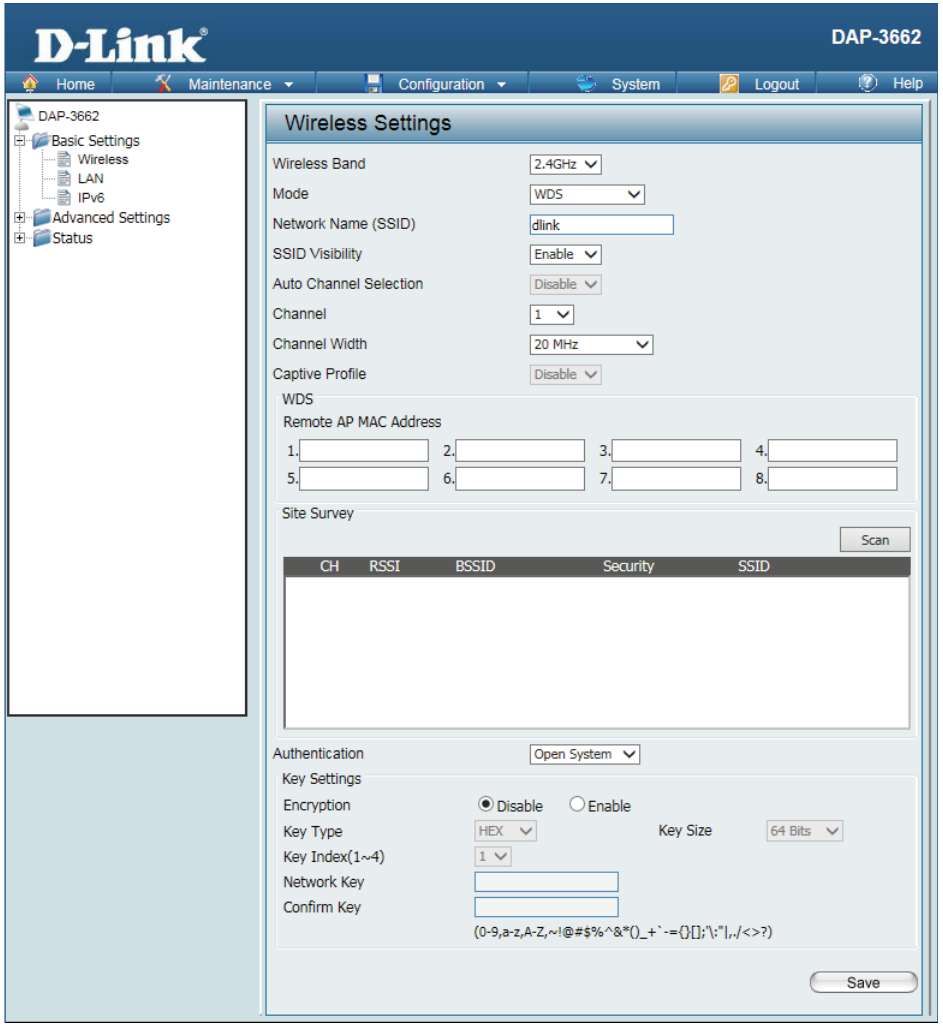
SSID Visibility: **Enable** or **Disable** SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.

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

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

Channel Width: Allows selection of the channel width you would like to operate in. **20 MHz** and **Auto 20/40 MHz** allow both 802.11n and non-802.11n wireless devices on your network when the wireless mode is Mixed 802.11 b/g/n in 2.4G and Mixed 802.11 a/n in 5G. 802.11n wireless devices are allowed to transmit data using 40 MHz when the channel width is **Auto 20/40 MHz**.

Captive Profile: Disable in WDS mode.



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 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**, **Shared Key**, or **WPA-Personal**.

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

Wireless Client Mode

In Wireless Client mode, the DAP-3662 functions as a wireless client on a wireless network in which an AP already exists. After completing the desired settings, click the **Save** button to let your changes take effect.

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

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

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

SSID Visibility: This option is unavailable in wireless client mode.

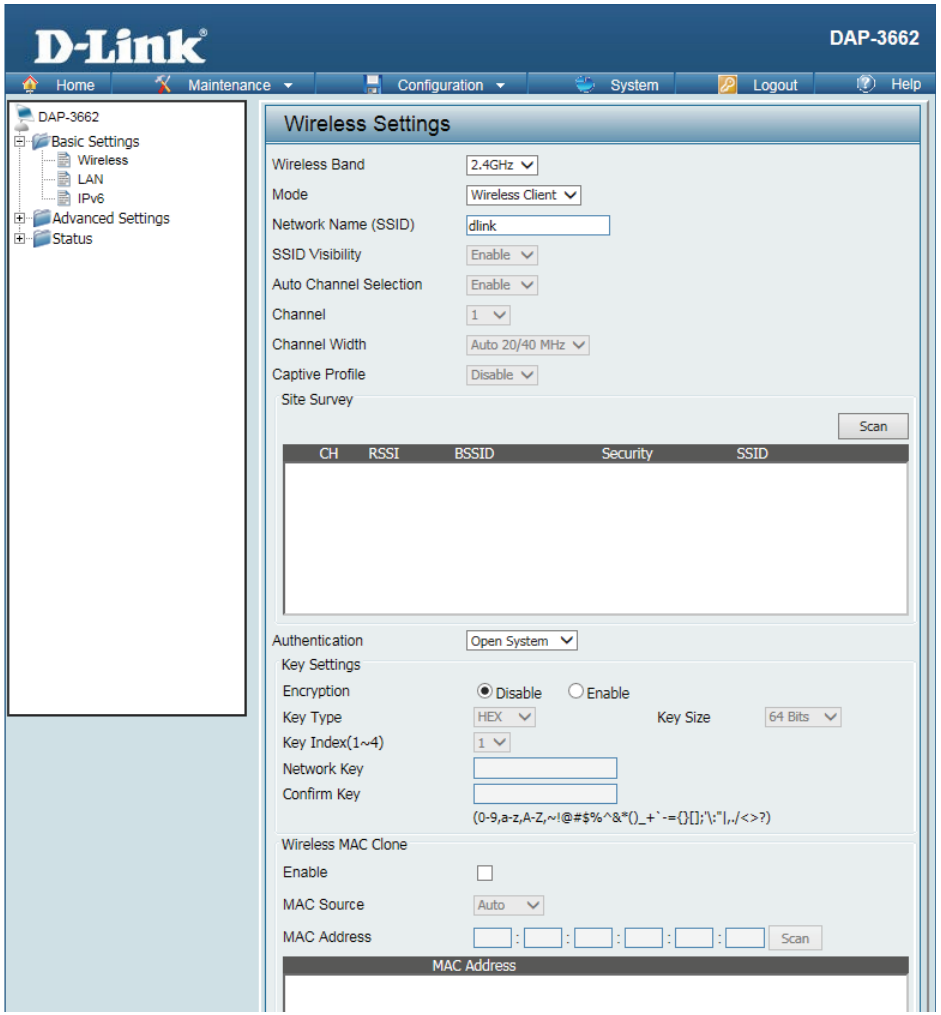
Auto Channel Selection: Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is not supported in Wireless Client mode.

Channel: The channel used will be displayed, and follow the root AP.

Channel Width: This option is unavailable in wireless client mode.

Captive Profile: Disable in Wireless Client mode.

Site Survey: Click 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.

For more information about the different types of Authentication offered on the DAP-3662 and the respective settings of each, please go to the first page of the Authentication explanations which begins on page 23.

Wireless MAC Clone

Enable: Click the box to enable the Wireless MAC Clone feature. Enabling this option allows the user to manually assign the source MAC address to packets forwarded by the DAP-3662. If disabled, the packet's source MAC address field will be automatically selected as the DAP-3662's MAC address.

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

MAC Address: If you selected **Manual** for the MAC Source above, you can either click the **Scan** button to search for all available devices connected to your DAP-3662's Ethernet port or manually enter a MAC address in the space provided.

WPA-Personal Authentication

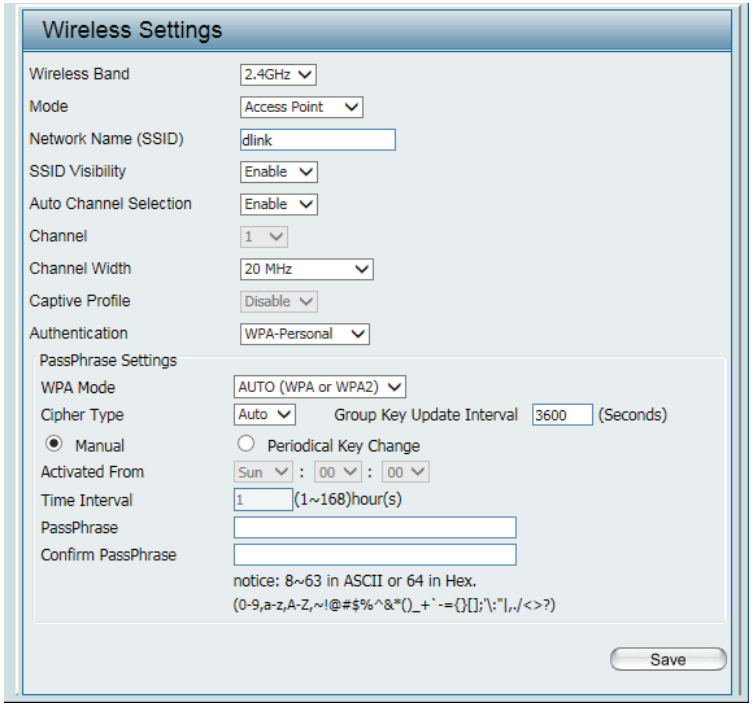
WPA Mode: When **WPA-Personal** is selected for Authentication type, you must also select a WPA mode from the drop-down menu: **AUTO (WPA or WPA2)**, **WPA2 Only**, or **WPA Only**. WPA and WPA2 use different algorithms. **AUTO (WPA or WPA2)** allows you to use both WPA and WPA2.

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

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

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

Confirm PassPhrase: Retype the Passphrase entered above in the corresponding field.



WPA-Enterprise Authentication

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 **1800**, as a lower interval may reduce data transfer rates.

Network Access Protection: Enable or disable Microsoft Network Access Protection. Enabling this will make the DAP-3662 a NAP enforcement point if you are running the Network Policy Server (NPS) service in Windows Server 2008.

RADIUS Server: Enter the IP address of the RADIUS server. Click External if the RADIUS server is on your network or Internal if you are using the RADIUS server on the DAP-3662.

RADIUS Port: Enter the RADIUS port (**1812** is the default).

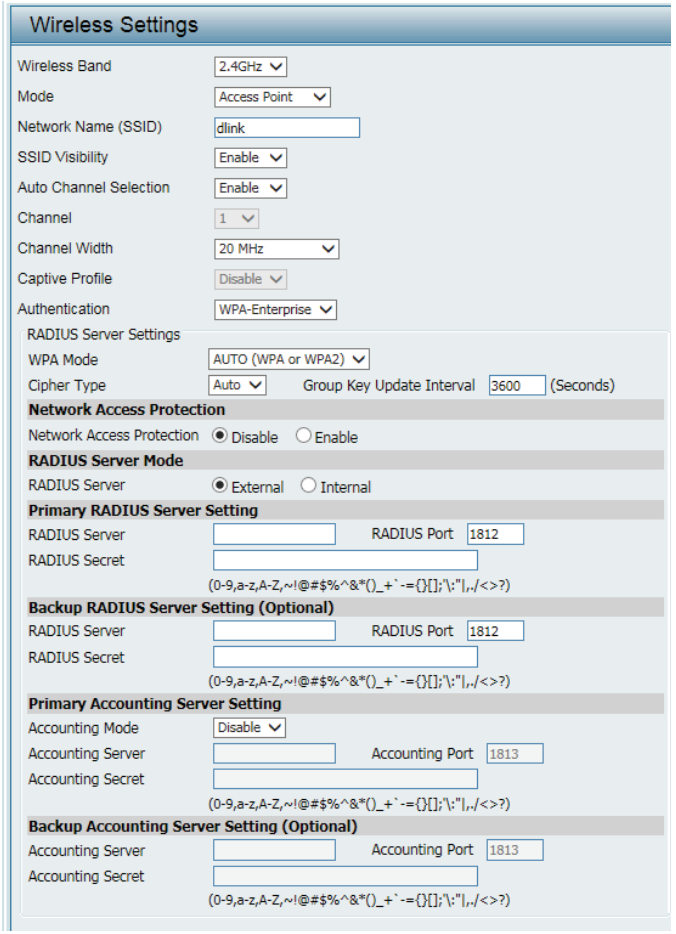
RADIUS Secret: Enter the RADIUS secret.

Accounting Mode: Select if you want to use a different server for accounting.

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

Accounting Port: Enter the Accounting port (**1813** is the default).

Accounting Secret: Enter the Accounting secret.



Note: *You can input the secondary RADIUS server and accounting server settings if you have a backup RADIUS and accounting server.*

802.1X authentication

Key Update Interval: Select the interval (in seconds) during which the key will be valid.

RADIUS Server: Enter the IP address of the RADIUS server. Click **External** if the RADIUS server is on your network or **Internal** if you are using the RADIUS server on the DAP-3662.

RADIUS Port: Enter the RADIUS port (**1812** is the default).

RADIUS Secret: Enter the RADIUS secret.

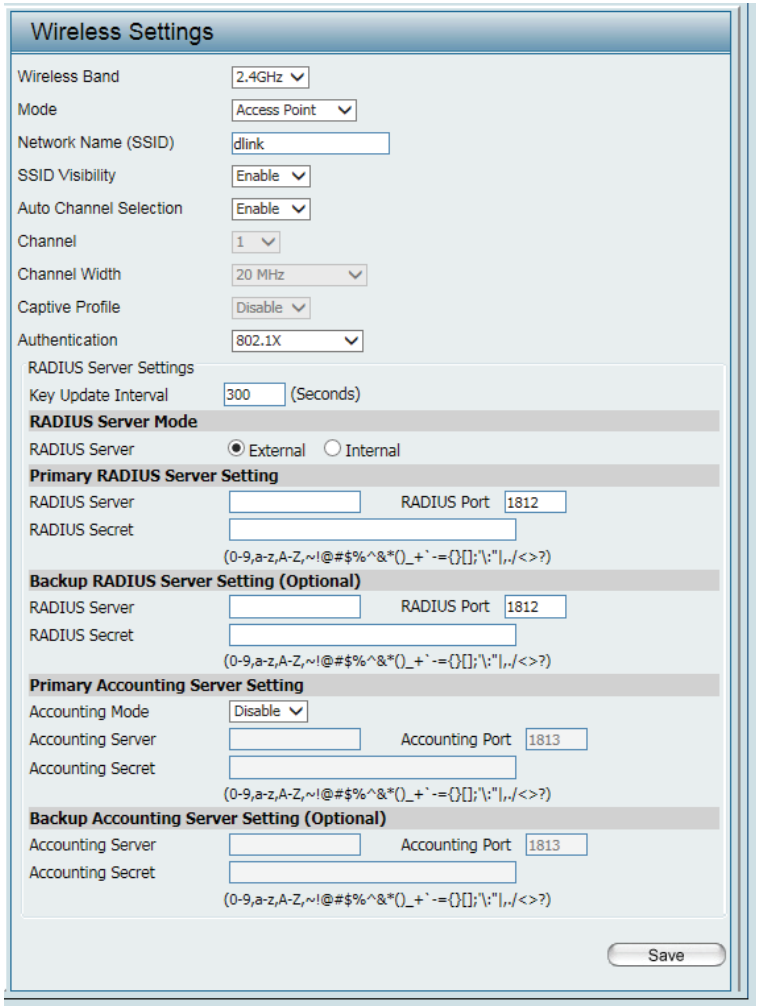
Accounting Mode: Select if you want to use a different server for accounting.

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

Accounting Port: Enter the Accounting port (**1813** is the default).

Accounting Secret: Enter the Accounting secret.

Note: *You can input the secondary RADIUS server and accounting server settings if you have a backup RADIUS and accounting server.*



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-3662. 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. After completing the desired LAN settings, click the **Save** button to let your changes take effect.

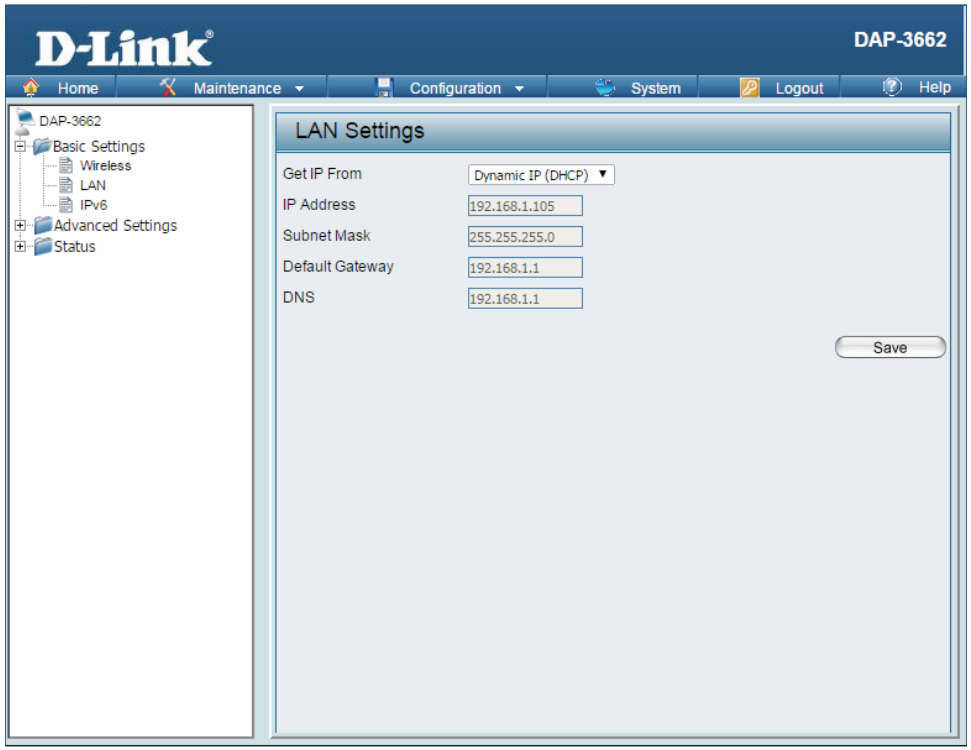
Get IP From: Select **Static IP (Manual)** if you do not have a DHCP server on your network, or if you wish to assign a static IP address to the DAP-3662. When **Dynamic IP (DHCP)** is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

IP Address: 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 router/gateway in your network, please enter its IP address.

DNS: Enter a DNS server IP address of your choice. In most cases, enter the LAN IP of your router.



IPv6

The IPv6 function allows you access DAP-3662 using an IPv6 address.

Enable IPv6: Check this box to enable IPv6.

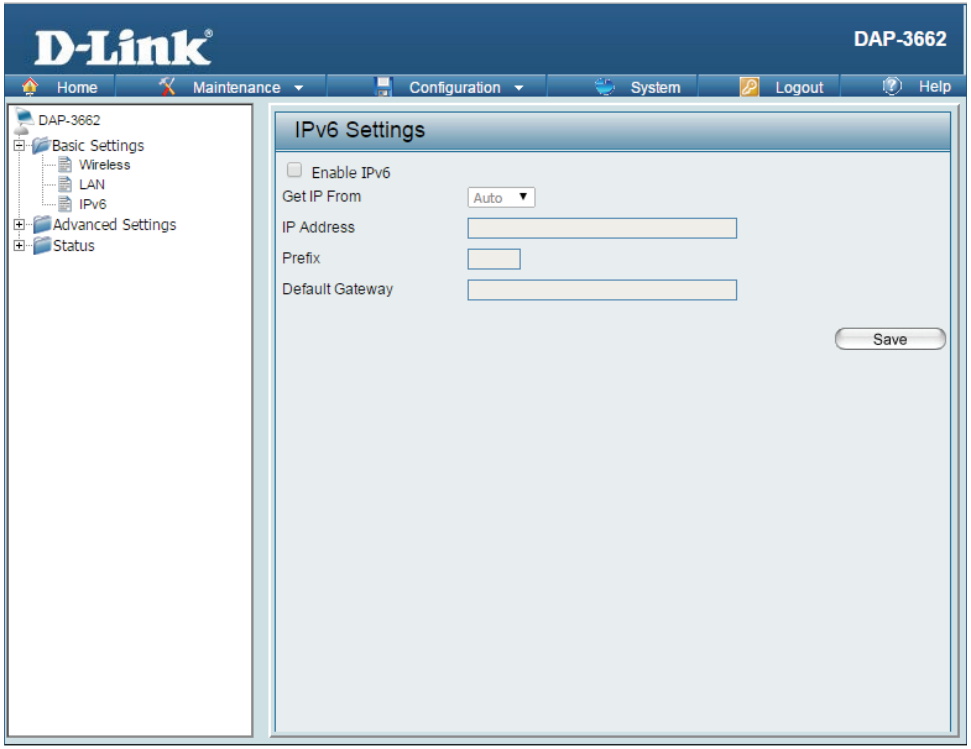
Get IP From: Select either **Static** to enter your own IP address or **Auto** to be automatically assigned by a DHCP server or IPv6 gateway.

IP Address: Assign an IPv6 IP address.

Prefix: The Prefix is used to determine what subnet an IP address belongs to. It must be 0~128..

Dafault Gateway: Enter the default gateway address. This is usually the IP address of your router.

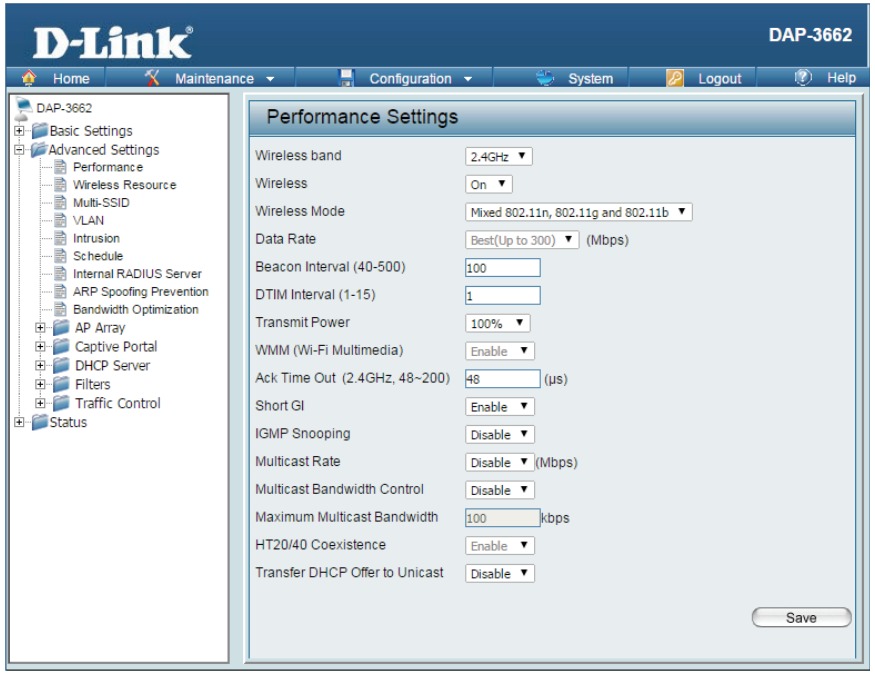
Note: *If IPv6 is enabled, AP Array, QoS, and Traffic Manager will all be disabled. Also, AP Client mode will change to AP mode.*



Advanced Settings

Performance

The Performance Settings window offers a number of user-controlled settings designed to optimize the performance of the DAP-3662. After completing the desired settings, click the **Save** button to let your changes take effect.



Wireless Band: Select either 2.4 GHz or 5 GHz.

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

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

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

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

*Maximum wireless signal rate derived from IEEE Standard 802.11g, 802.11a 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.

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

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

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

Ack Time Out (2.4 GHZ) or Ack Time Out (5 GHZ): To effectively optimize throughput over long distance links enter a value for Acknowledgement Time Out between **25** and **200** microseconds for 5 GHz or from **48** to **200** microseconds 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: Adjust the multicast packet data rate here. The multicast rate is supported in **AP mode**, (2.4 GHZ and 5 GHZ) and **WDS with AP mode**, including Multi-SSIDs.

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

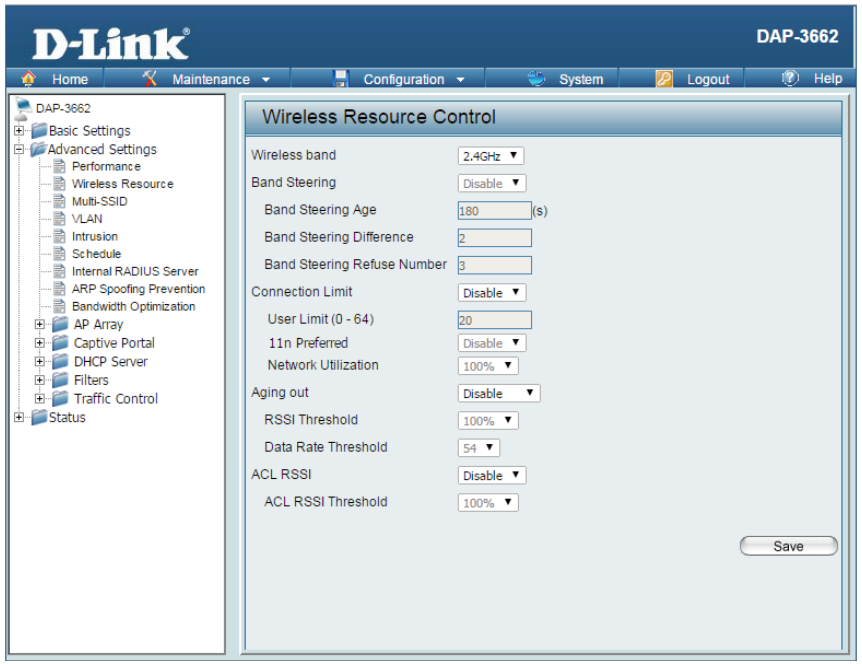
Maximum Multicast Bandwidth : Set the multicast packets maximum bandwidth pass through rate from the Ethernet interface to the DAP-3662.

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 DAP-3662 will automatically change to 20 MHz.

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

Wireless Resource Control

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



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

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

Band Steering Age: Enter the time in seconds to specify the interval of updating information.

Band Steering Difference: The 5G preferred difference value is equal to the number of 5 GHz wireless client connections minus the number of 2.4 GHz wireless client connections. If the number of 5 GHz wireless client connections minus the number of 2.4 GHz wireless client connections exceed this value, the extra 5 GHz wireless client connections will be forced to connect to the 2.4 GHz band and not the 5 GHz band.

Band Steering Refuse Number: Enter the maximum 5G connection attempts allowed before the 5G preferred function will be disabled for the wireless station connection.

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-3662 will not allow clients to associate with the AP.

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

11n Preferred: Use the drop-down menu to **Enable** the 11n Preferred function. The wireless clients with 802.11n protocol will have higher priority to connect to the device.

Network Utilization: Set the maximum utilization of this access point for service. The DAP-3662 will not allow any new clients to associate with the AP if the utilization exceeds the value the user specifies. Select a utilization percentage between 100%, 80%, 60%, 40%, 20%, or 0%. When this network utilization threshold is reached, the device will pause one minute to allow network congestion to dissipate.

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

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

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

ACL RSSI: Use the drop-down menu to **Enable** the function. When enabled, the device denies the connection request from the wireless clients with the RSSI lower than the specified threshold below.

ACL RSSI Threshold: Set the ACL RSSI Threshold.

Multi-SSID

The device supports up to eight multiple Service Set Identifiers. You can set the Primary SSID in the **Basic > Wireless** section. The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. When the information for the new SSID is finished, click the **Add** button. Click the **Save** button to let your changes take effect.

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

Enable Priority: Check to enable the priority feature.

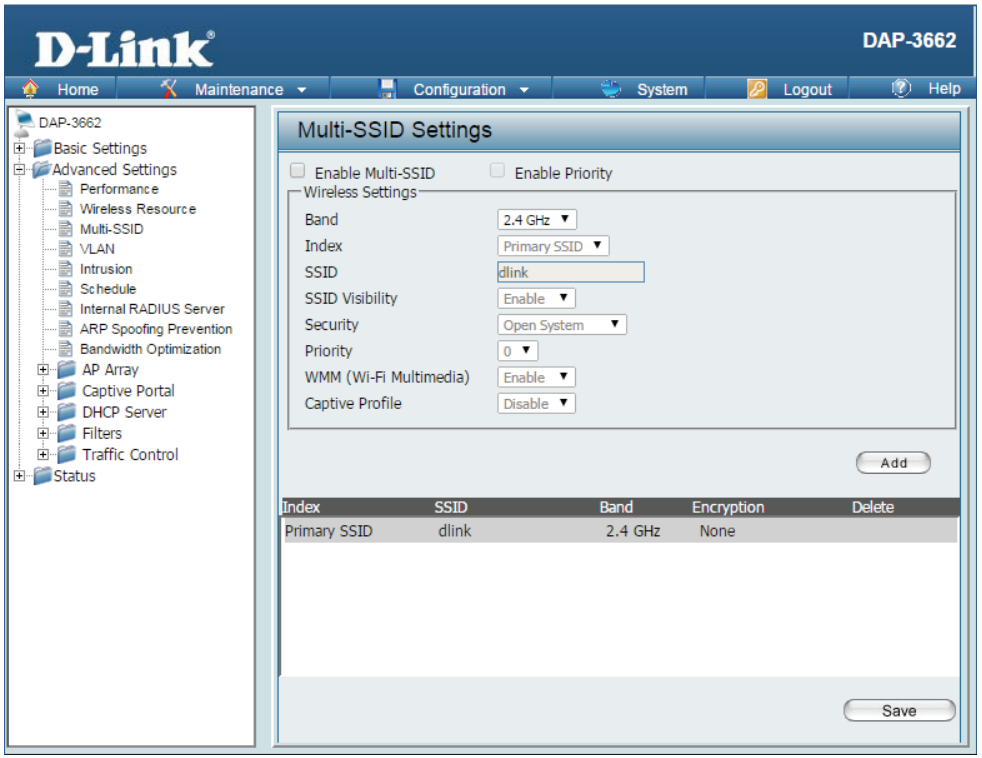
Band: This read-only value is the current band setting.

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

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 23. For a detailed description of the WPA-Personal parameters please go to page 24. For a detailed description of the WPA-Enterprise parameters please go to page 25. For a detailed description of the 802.1X parameters please go to page 26.



Priority: When the Enable Priority check box is checked at the top of this window, this drop-down menu is used to select a priority between **0** and **7**.

WMM (Wi-Fi Multimedia): Select **Enable** to provide basic Quality of Service features.

Captive Profile: Enable or disable captive profile for user authentication.

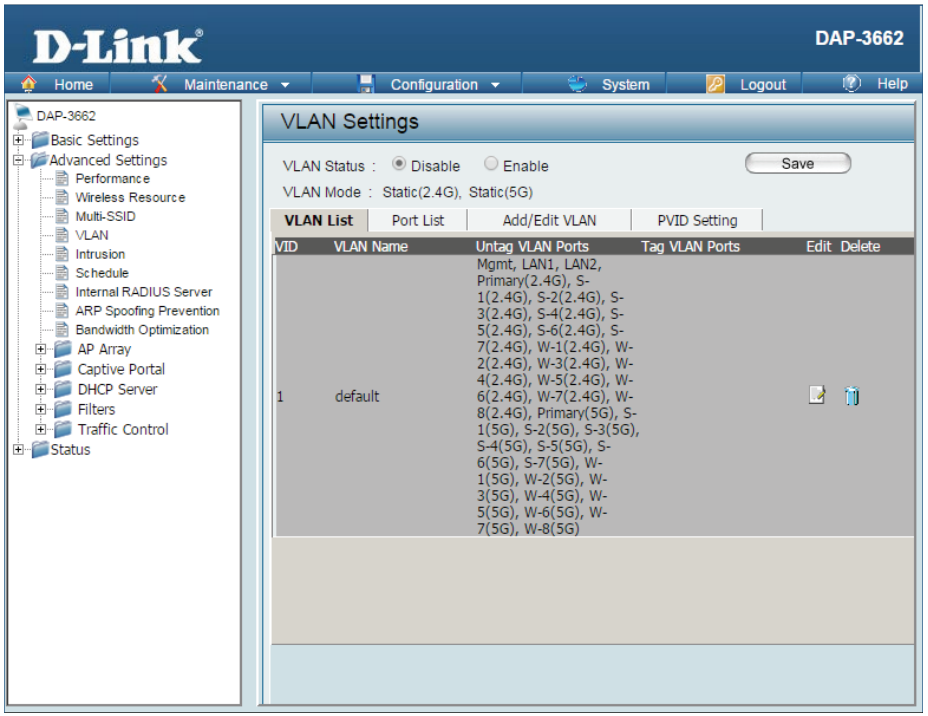
VLAN Settings

The DAP-3662 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-3662 without a VLAN tag will have a VLAN tag inserted with a PVID. Once you have made the desired settings, click the **Save** button to let your changes take effect.

The VLAN List tab displays the current VLANs.

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

VLAN Mode: The current VLAN mode is displayed.



VLAN Port List

The Port List tab displays the current ports. If you want to configure the guest and internal networks on a Virtual LAN (VLAN), the switch and DHCP server you are using must also support VLANs. As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE 802.1Q standard. Once you have made the desired settings, click the **Save** button to let your changes take effect.

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

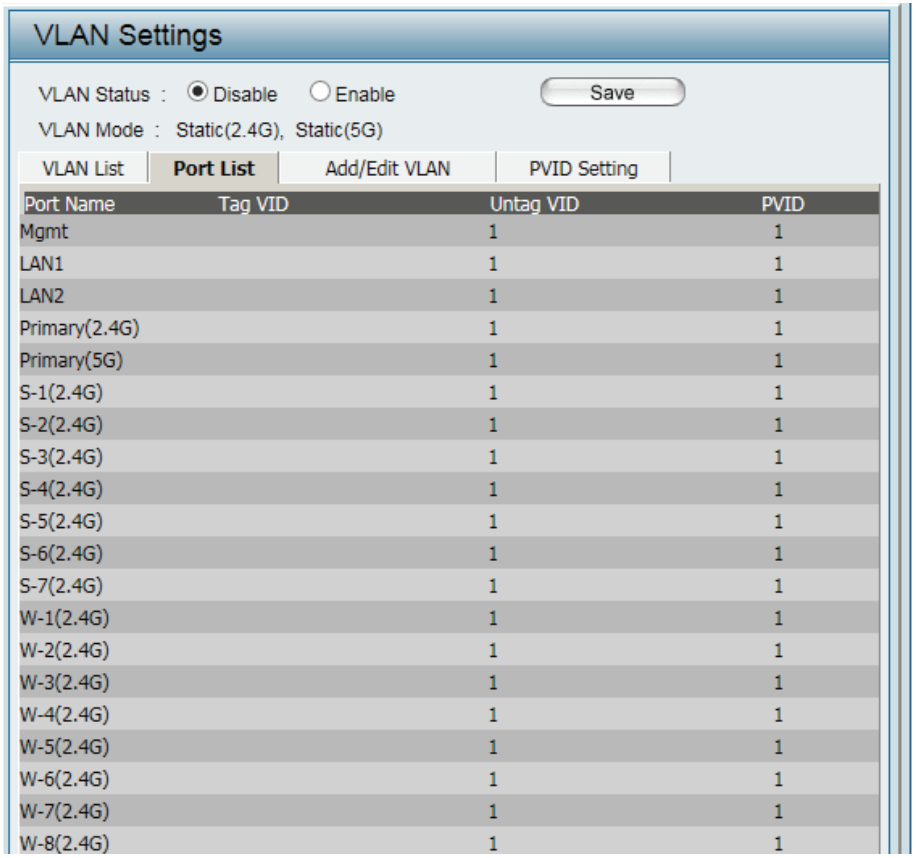
VLAN Mode: The current VLAN mode is displayed.

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

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

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

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



Port Name	Tag VID	Untag VID	PVID
Mgmt		1	1
LAN1		1	1
LAN2		1	1
Primary(2.4G)		1	1
Primary(5G)		1	1
S-1(2.4G)		1	1
S-2(2.4G)		1	1
S-3(2.4G)		1	1
S-4(2.4G)		1	1
S-5(2.4G)		1	1
S-6(2.4G)		1	1
S-7(2.4G)		1	1
W-1(2.4G)		1	1
W-2(2.4G)		1	1
W-3(2.4G)		1	1
W-4(2.4G)		1	1
W-5(2.4G)		1	1
W-6(2.4G)		1	1
W-7(2.4G)		1	1
W-8(2.4G)		1	1

VLAN Add/Edit

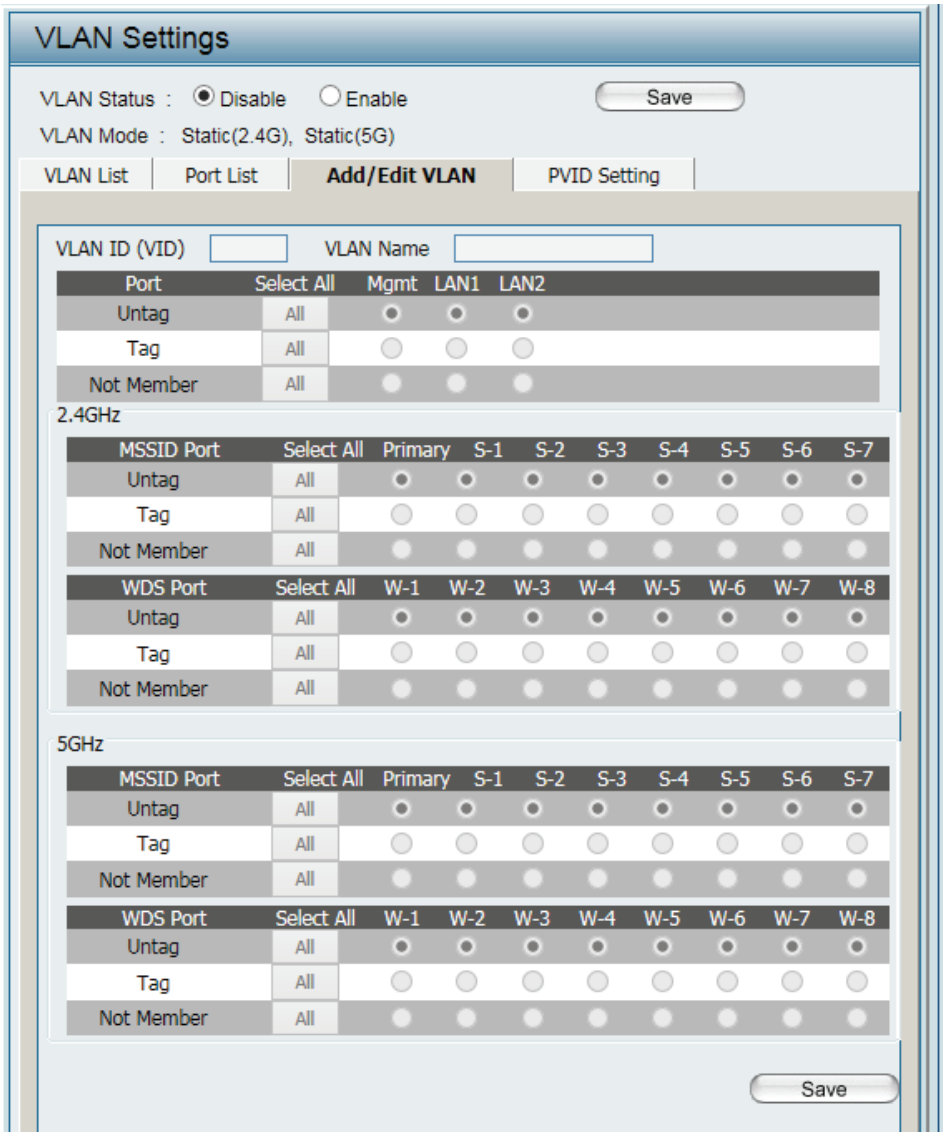
The Add/Edit VLAN tab is used to configure VLANs. Once you have made the desired settings, click the **Save** button to let your changes take effect.

VLAN Status: Click the **Enable** radio button.

VLAN Mode: The current VLAN mode is displayed.

VLAN ID (VID): Provide a number between **1** and **4094** for the Internal VLAN.

VLAN Name: Enter the VLAN to add or modify.



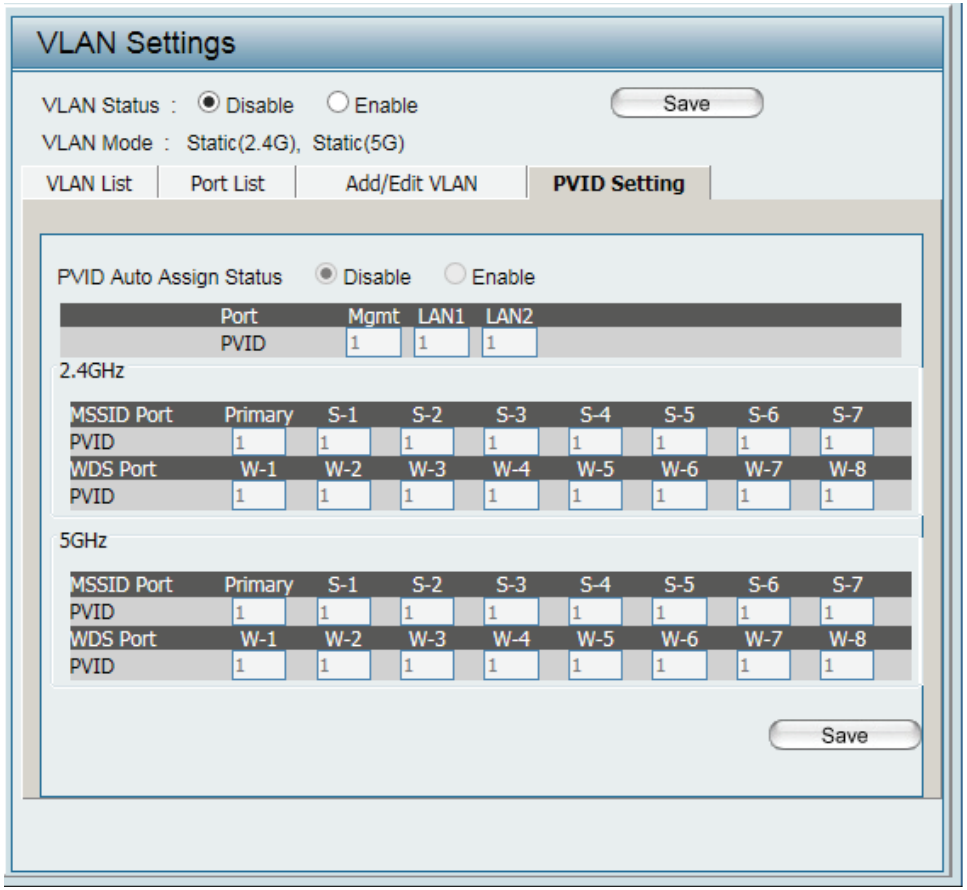
PVID Setting

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. Once you have made the desired settings, click the **Save** button to let your changes take effect.

VLAN Status: Click the **Enable** radio button.

VLAN Mode: The current VLAN mode is displayed.

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



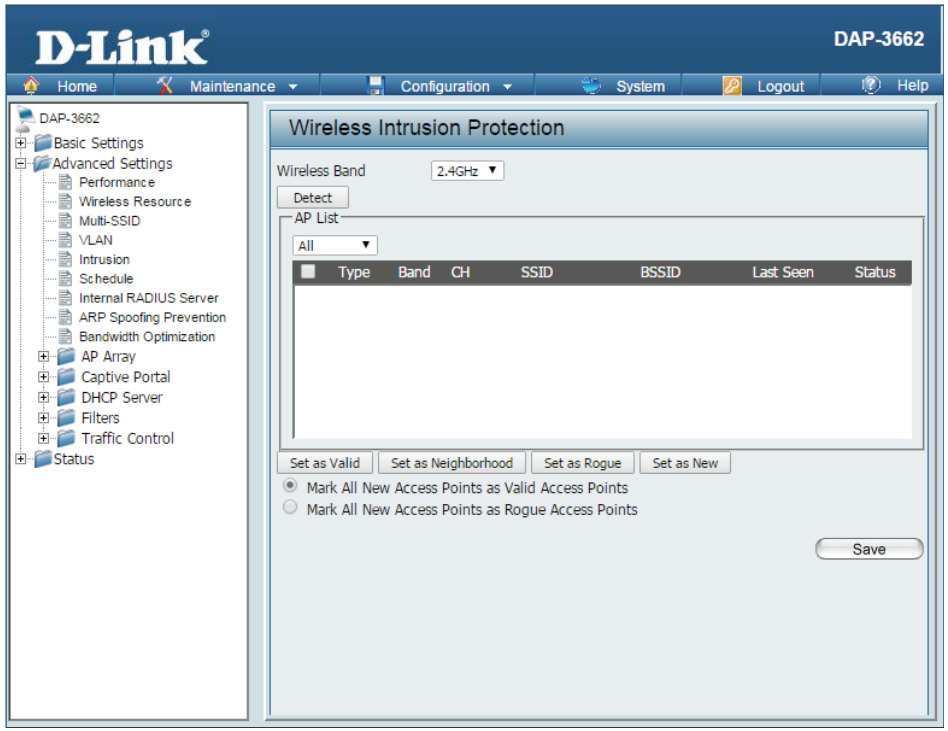
Intrusion

The Wireless Intrusion Protection window is used to set APs as All, Valid, Neighborhood, Rogue, and New. Once you have made the desired settings, click the **Save** button to let your changes take effect.

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

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

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



Schedule

The Wireless Schedule Settings window is used to add and modify scheduling rules on the device. When the information for the new schedule rule is finished, click the **Add** button. To discard the new schedule rule settings, click the **Clear** button. Click the **Save** button to let your changes take effect.

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

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

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

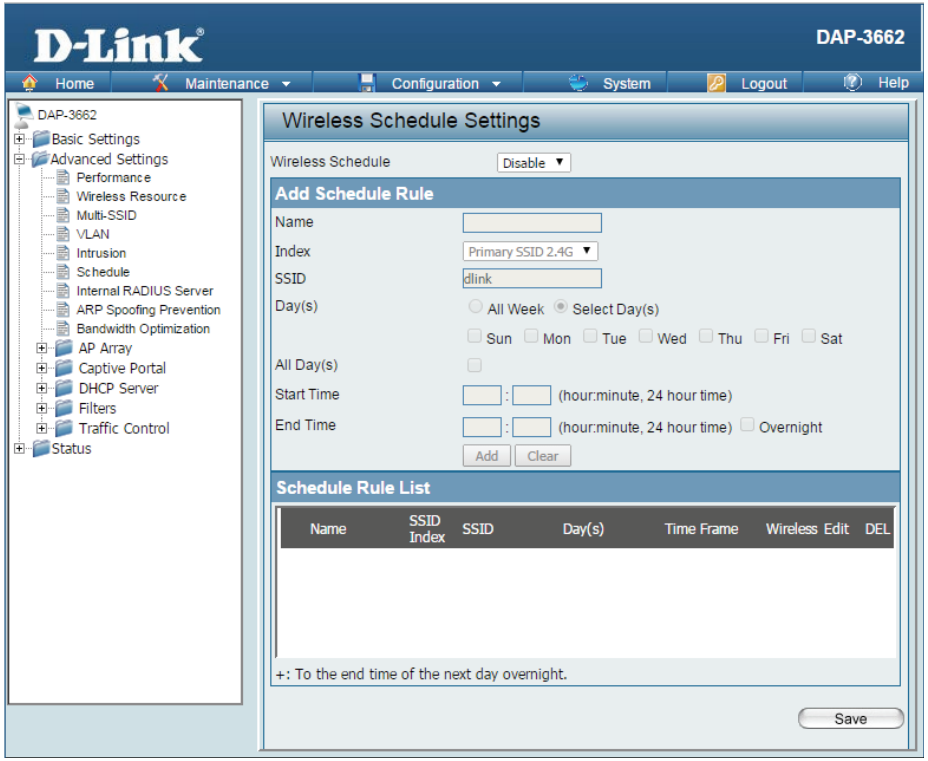
SSID: This read-only field indicates the current SSID in use. To create a new SSID, go to the Wireless Settings window (**Basic Settings > Wireless**).

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

All Day(s): Check this box to have settings apply 24 hours a day. If the settings are not to apply 24 hours a day, enter the desired starting and ending times in the next two fields.

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

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



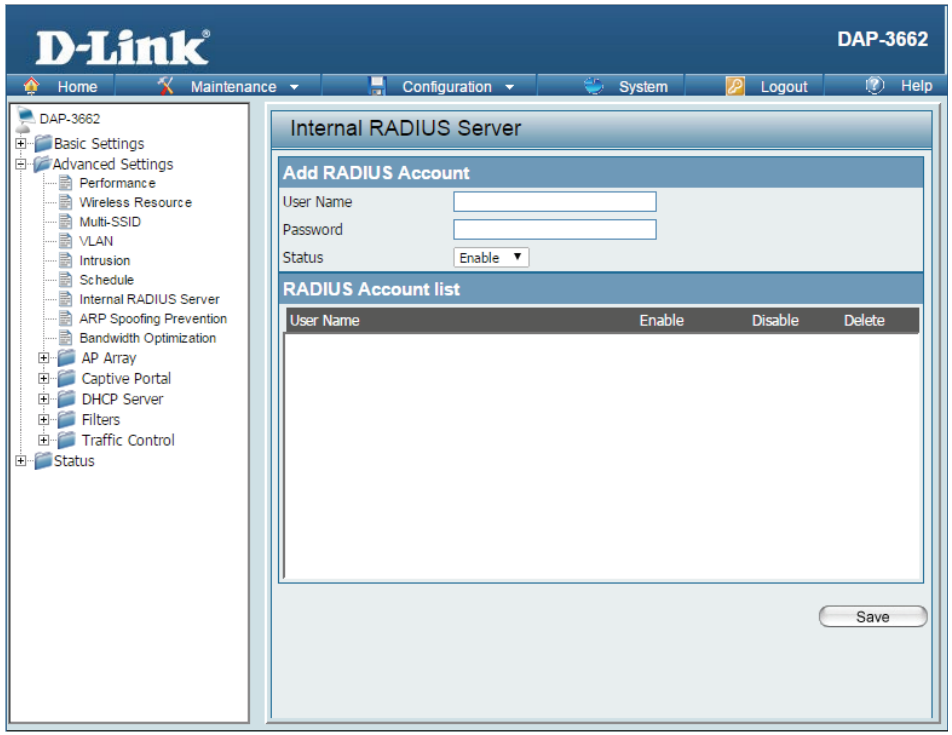
Internal RADIUS Server

The DAP-3662 features a built-in RADIUS server. Once you have finished adding a RADIUS account, click the **Save** button to let your changes take effect. The newly-created account will appear in this RADIUS Account List. The radio buttons allow the user to enable or disable the RADIUS account. Click the icon in the delete column to remove the RADIUS account. We suggest you limit the number of accounts below 30.

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

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

Status: Select **Enable** or **Disable** from the drop-down menu.



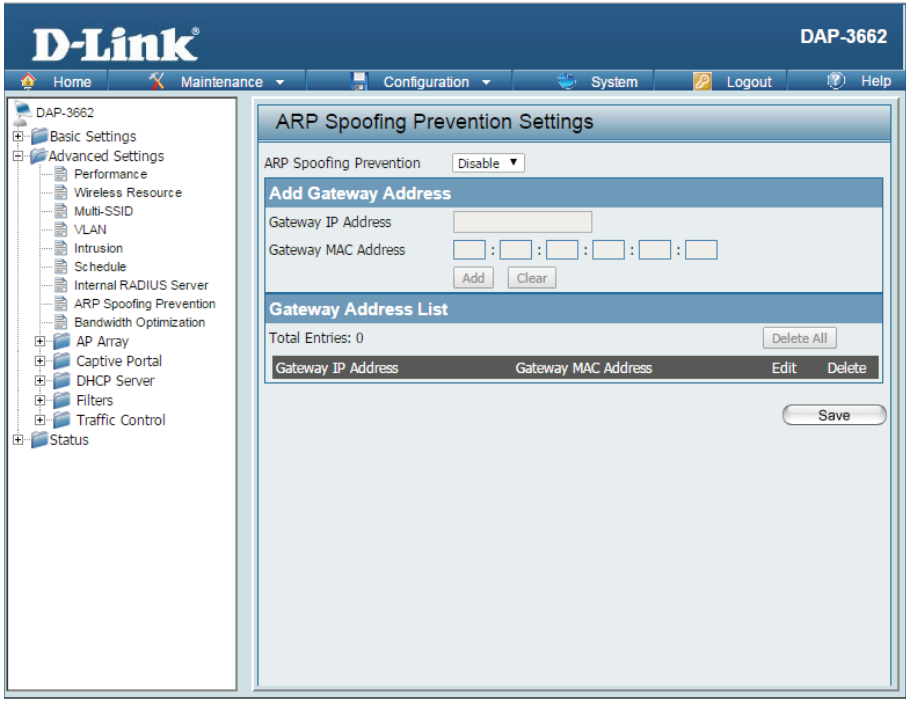
ARP Spoofing Prevention

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

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

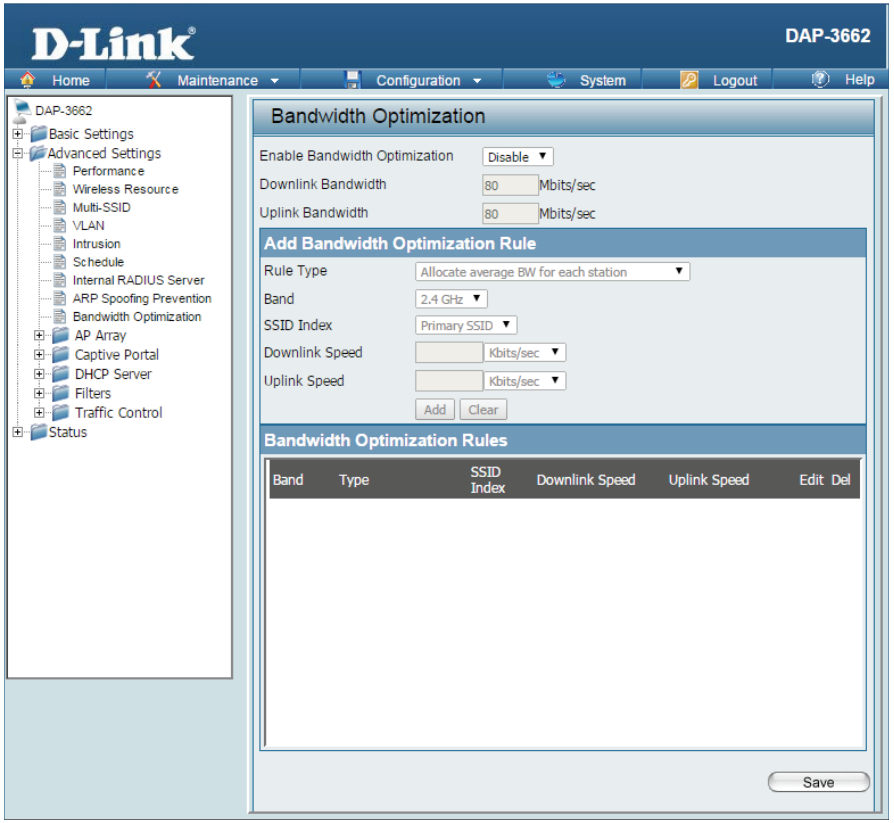
Gateway IP Address: Enter a gateway IP address.

Gateway MAC Address: Enter a gateway MAC address.



Bandwidth Optimization

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



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

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

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

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

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

Allocate different BW for a/b/g/n stations: The weight of 802.11b/g/n and 802. 11a/n client are 10%/20%/70% ; 20%/80%. AP will distribute different bandwidth for 802. 11a/b/g/n clients.

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

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

Use the drop-down menu to toggle the wireless

Band: band between 2.4 GHz and 5 GHz.

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

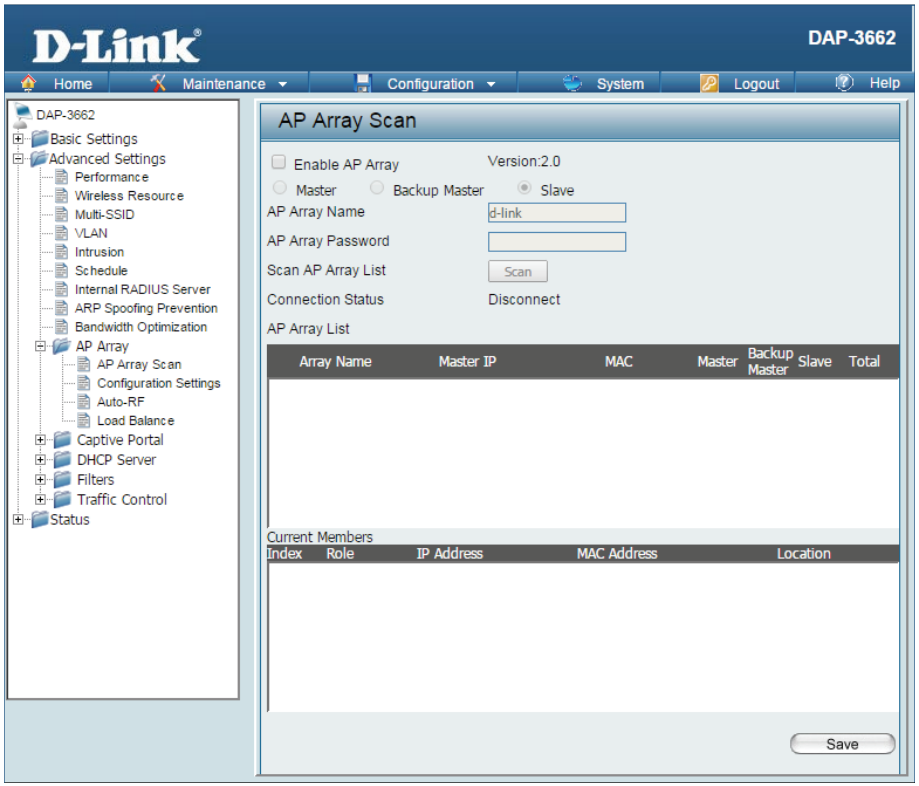
Downlink Speed: Enter the limitation of the downloading speed in either Kbits/sec or Mbits/sec for the rule.

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

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 increase ease of 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-3662 AP array feature supports up to eight AP array members.

Configuration Settings

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

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

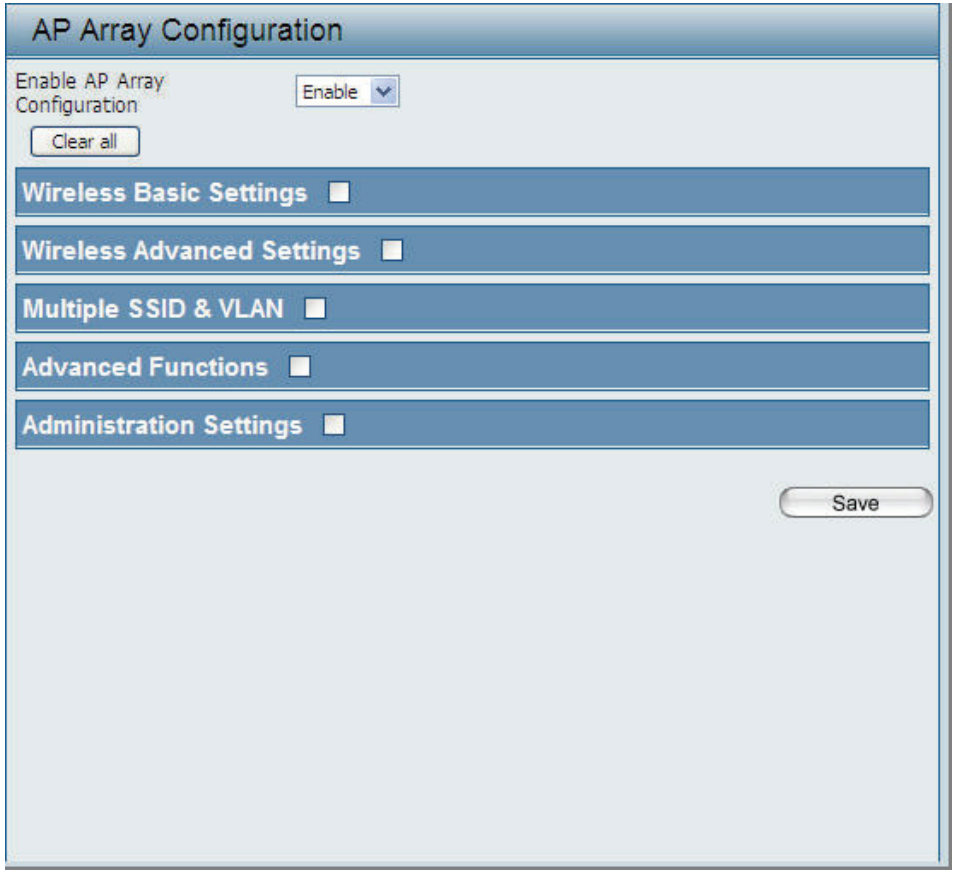
Wireless Basic Settings: Select this option to specify the basic wireless settings that the APs in the group will inherit.

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.



Wireless Basic Settings

Network Name (SSID): Select this option to use the same SSID.

SSID Visibility: Select this option to enable SSID visibility.

Auto Channel Selection: Select this option to use auto channel selection.

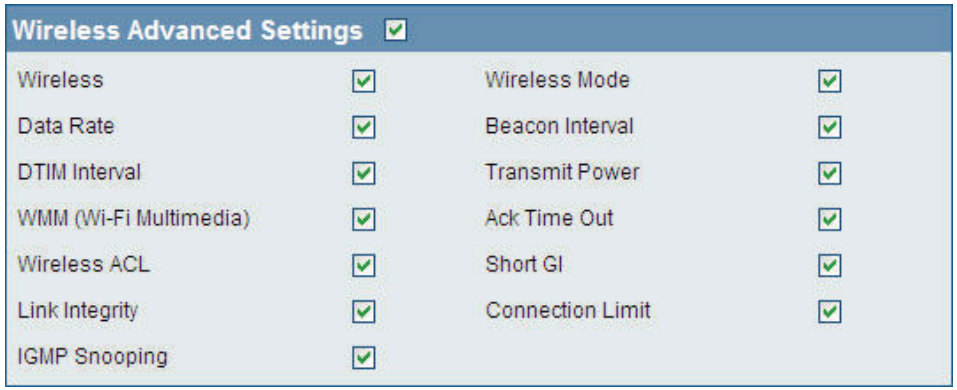
Channel Width: Select this option to use the same channel width.

Security: Select this option to use the same wireless security.

Captive Profile: Select this option to use the same captive profile settings.

Band: Select this option to use the same wireless band.

Wireless Advanced Settings



Wireless: Select this option to use the same wireless settings.

Wireless Mode: Select this option to use the same wireless mode.

Data Rate: Select this option to use the same data rate.

Beacon Interval: Select this option to use the same beacon interval.

DTIM Interval: Select this option to use the same DTIM interval.

Transmit Power: Select this option to use the same transmit power.

WMM (Wi-Fi Multimedia): Select this option to use the same WMM settings.

Ack Time Out: Select this option to use the same ACK timeout value.

Wireless ACL: Select this option to use the same wireless ACL settings.

Short GI: Select this option to use the same short GI settings.

Link Integrity: Select this option to use the same link integrity settings.

Connection Limit: Select this option to use the same connection limit value.

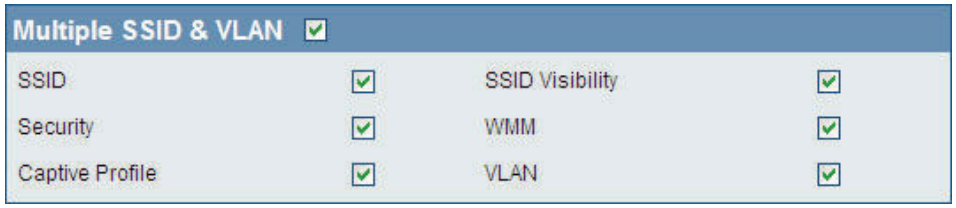
IGMP Snooping:: Select this option to use the same IGMP snooping settings.

Multiple SSID & VLAN

SSID: Select this option to use the same multi-SSIDs.

SSID Visibility: Select this option to use the same SSID visible.

Security: Select this option to use the same wireless security settings.



WMM: Select this option to use the same WMM settings.

Captive Profile: Select this option to use the same captive profile settings.

VLAN: Select this option to use the same VLAN settings.

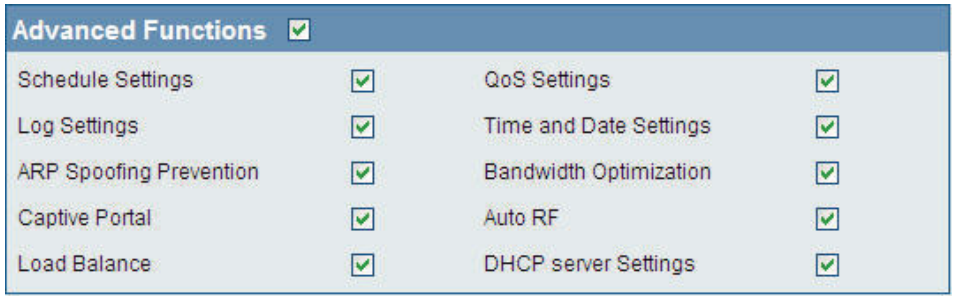
Advanced Functions

Schedule Settings: Select this option to use the same schedule settings.

QoS Settings: Select this option to use the same Quality of Service settings.

Log Settings: Select this option to use the same log settings.

Time and Date Settings: Select this option to use the same time and date settings.



ARP Spoofing Prevention: Select this option to use the same ARP spoofing prevention settings.

Bandwidth Optimization: Select this option to use the same bandwidth optimization settings.

Captive Portal: Select this option to use the same captive portal settings.

Auto RF: Select this option to use the same auto-RF settings.

Load Balance: Select this option to use the same load balancing settings.

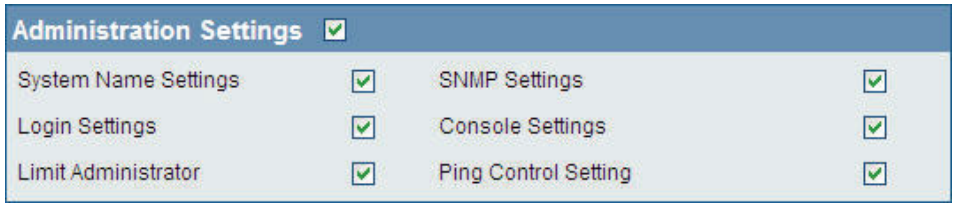
DHCP Server Settings: Select this option to use the same DHCP server settings.

Administration Settings

System Name Settings: Select this option to use the same system name.

SNMP Settings: Select this option to use the same SNMP settings.

Login Settings: Select this option to use the same login settings.



Console Settings: Select this option to use the same console settings.

Limit Administrator: Select this option to use the same limit administrator settings.

Ping Control Setting: Select this option to use the same ping control settings.

Auto-RF

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

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

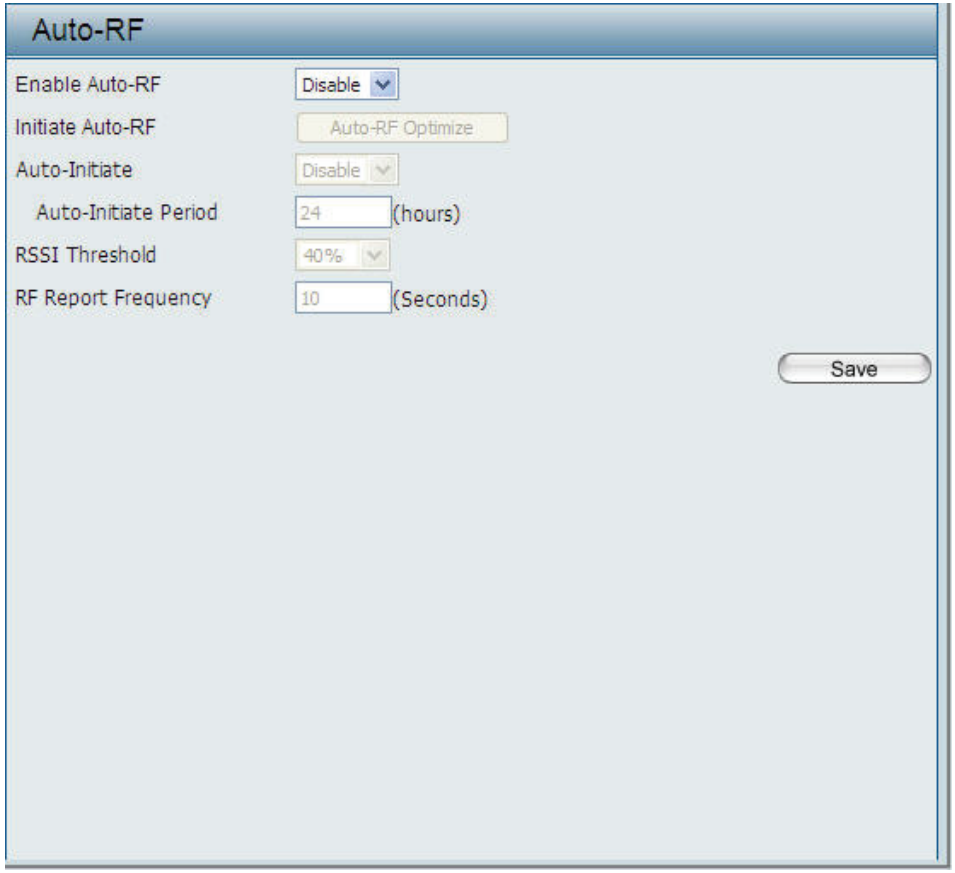
Initiate Auto-RF: Click the Auto-RF Optimize button to initiate the auto-RF optimization feature.

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

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

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

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

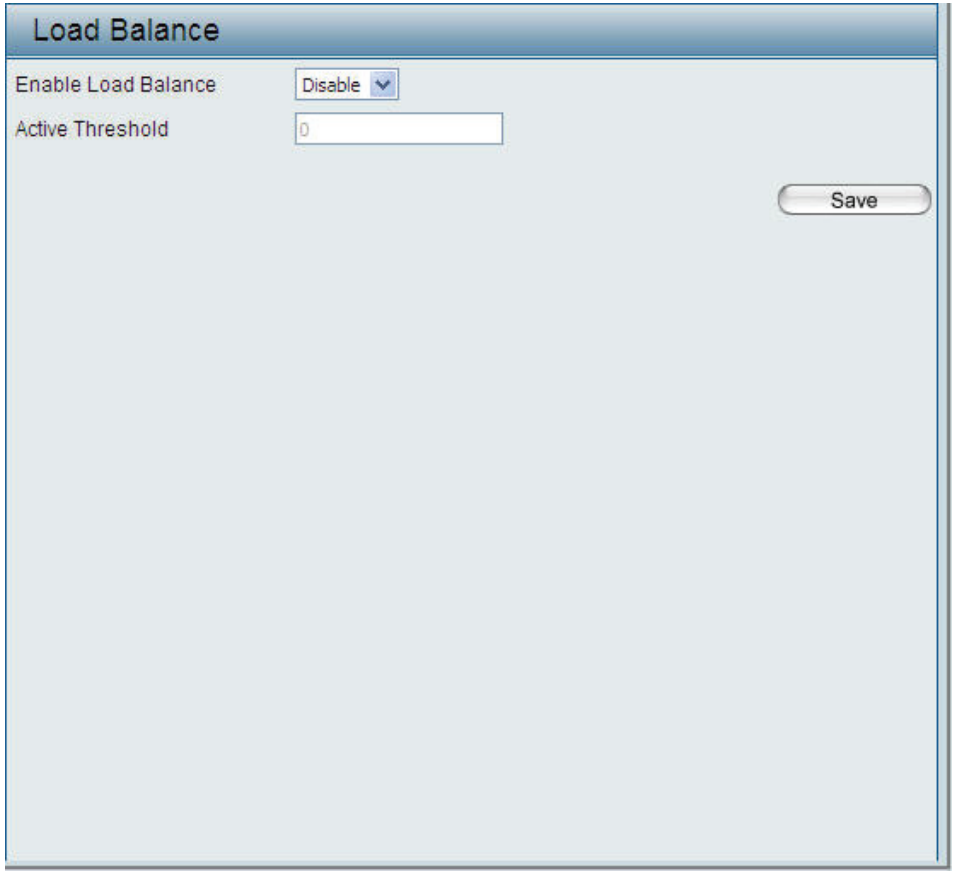


Load Balance

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

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

Active Threshold: Enter the active threshold value here.



Captive Portal

Authentication Settings - Passcode

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web brower will be redirected to a web authentication page. In this windows, user can view and configure the Captive Portal settings. Click the Add button to add a new entry. Click the Delete or Delete All button to remove a specific entry or all the entries configured.

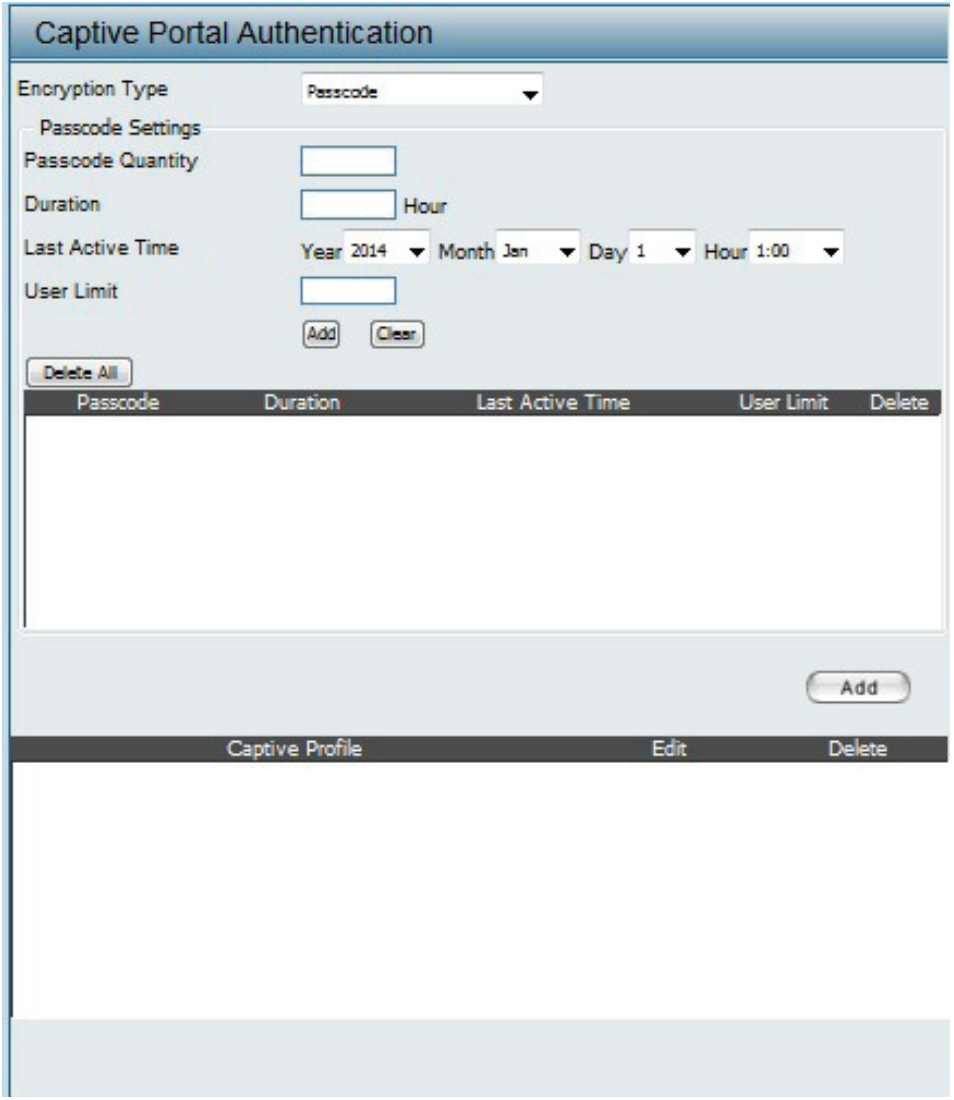
Encryption Type: Select the captive portal encryption type here. Options to choose from are Passcode, Username/ Password, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Passcode option.

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

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

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

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



Authentication Settings - Username/Password

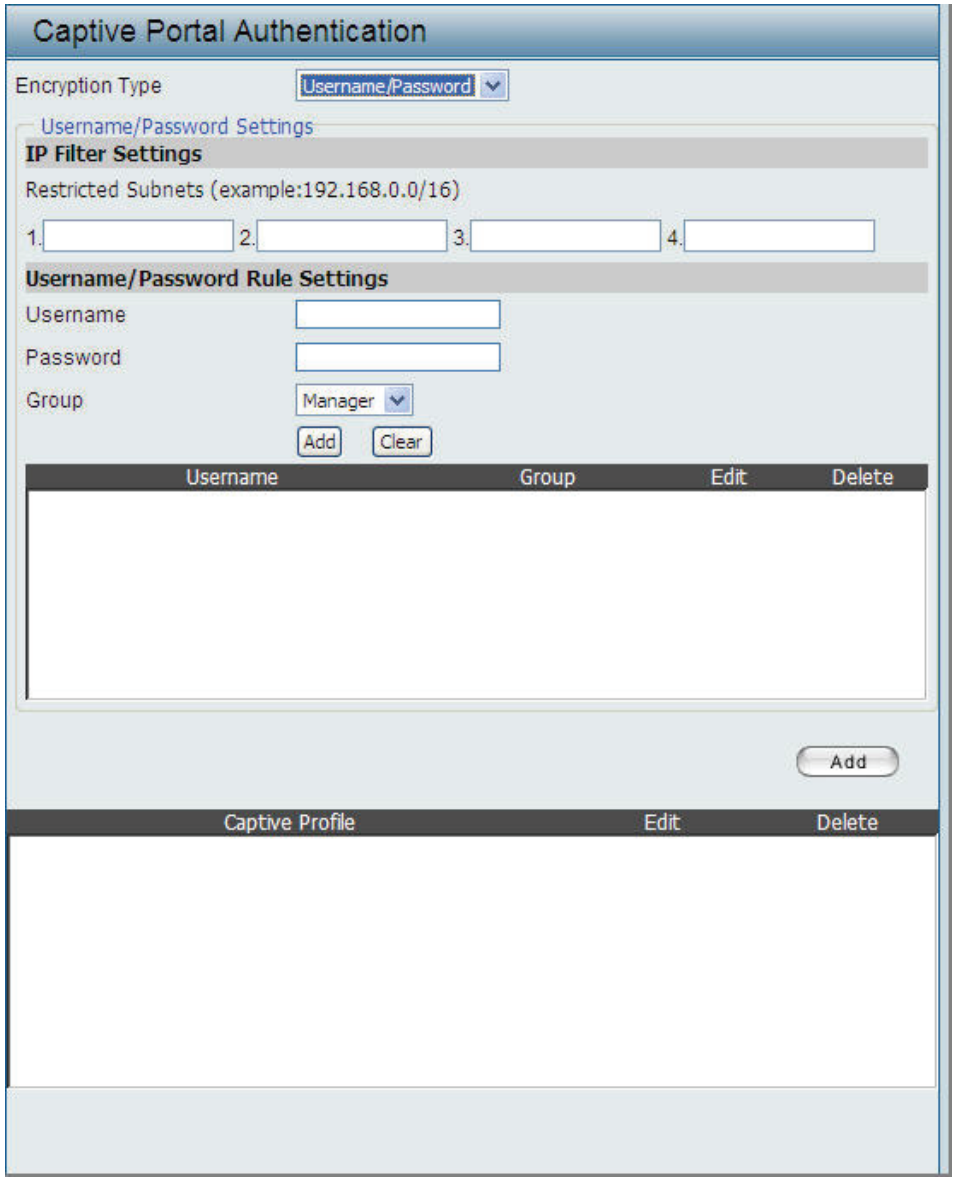
Encryption Type: Select the captive portal encryption type here. Options to choose from are Passcode, Username/Password, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Username/Password option.

Restricted Subnets: Enter the restricted subnets here. Access to these subnets will denied to guest accounts. Up to four restricted subnet entries can be defined.

Username: Enter the username for the new account here.

Password: Enter the password for the new account here.

Group: Select the group for the new account here. Options to choose from are Manager and Guest. Guest accounts will have limited access.



Authentication Settings - Remote RADIUS

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

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

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

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

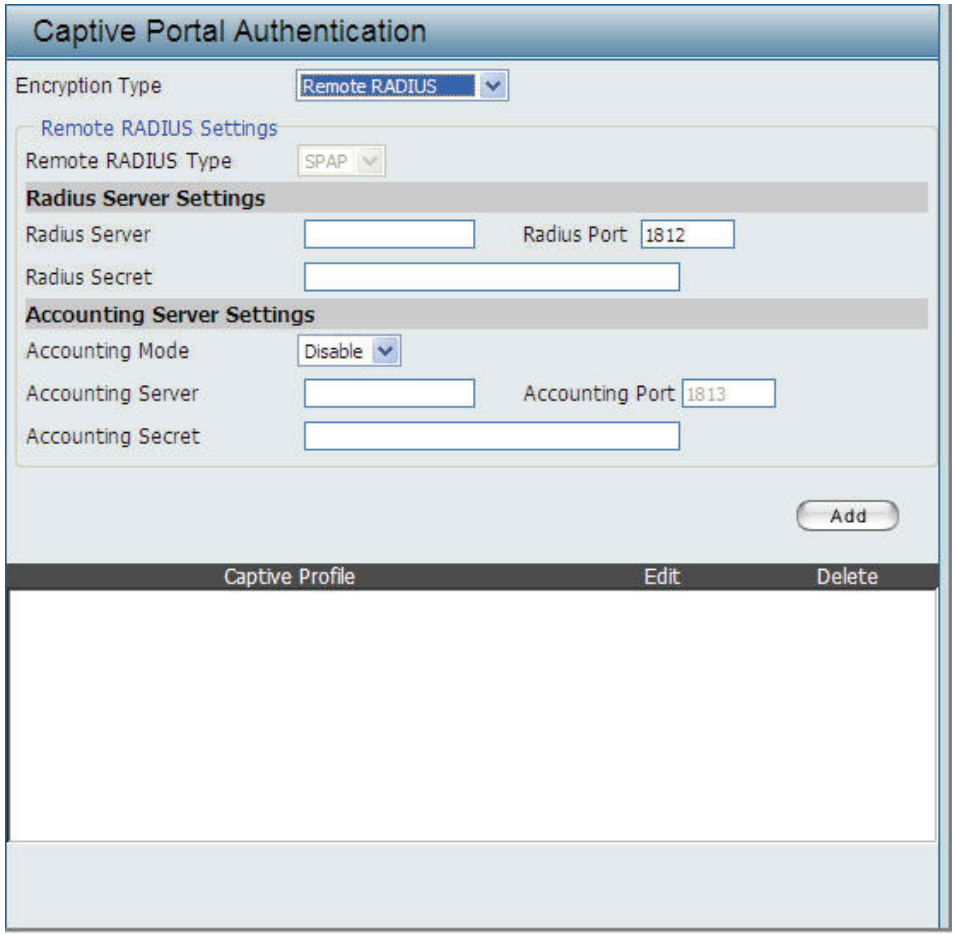
Radius Secret: Enter the RADIUS server's shared secret here.

Accounting Mode: Select to Enable or Disable the accounting mode here.

Accounting Server: Enter the accounting server's IP address here.

Accounting Port: Enter the accounting server's port number here.

Accounting Secret: Enter the accounting server's shared serect here.



Authentication Settings - LDAP

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

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

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

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

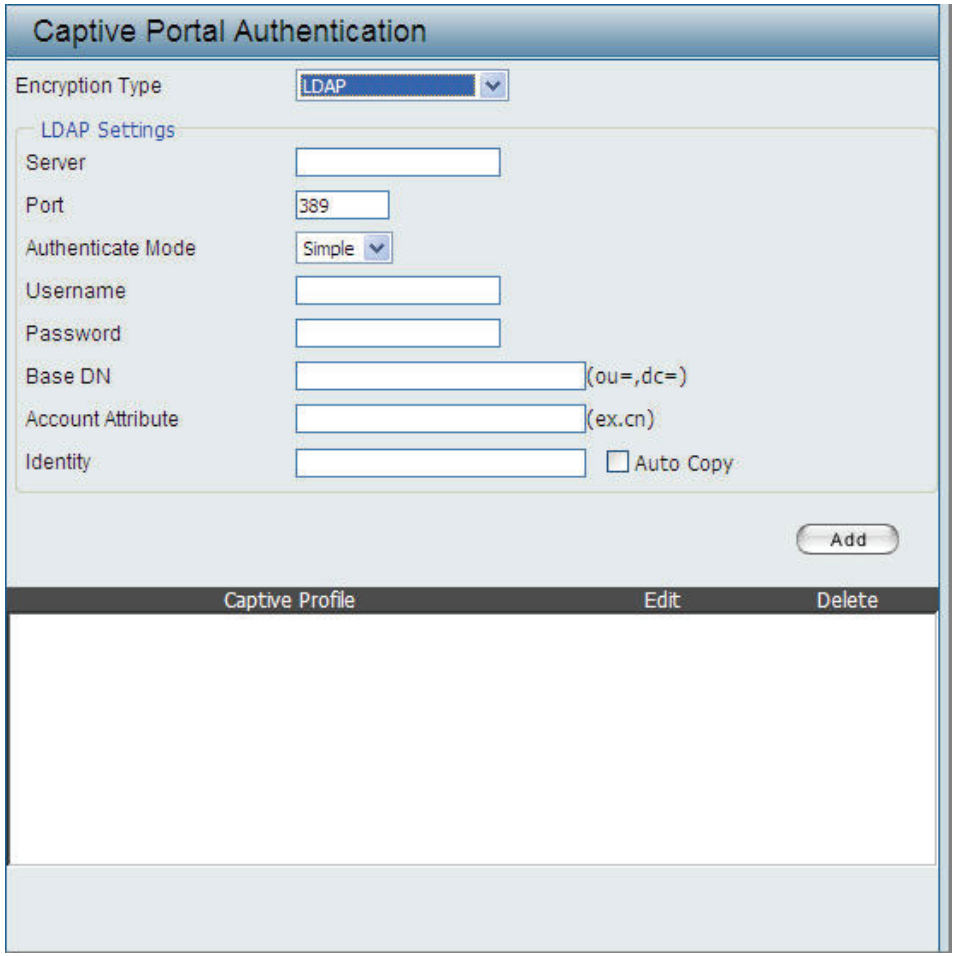
Username: Enter the LDAP server account's username here.

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

Base DN: Enter the administrator's domain name here.

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

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



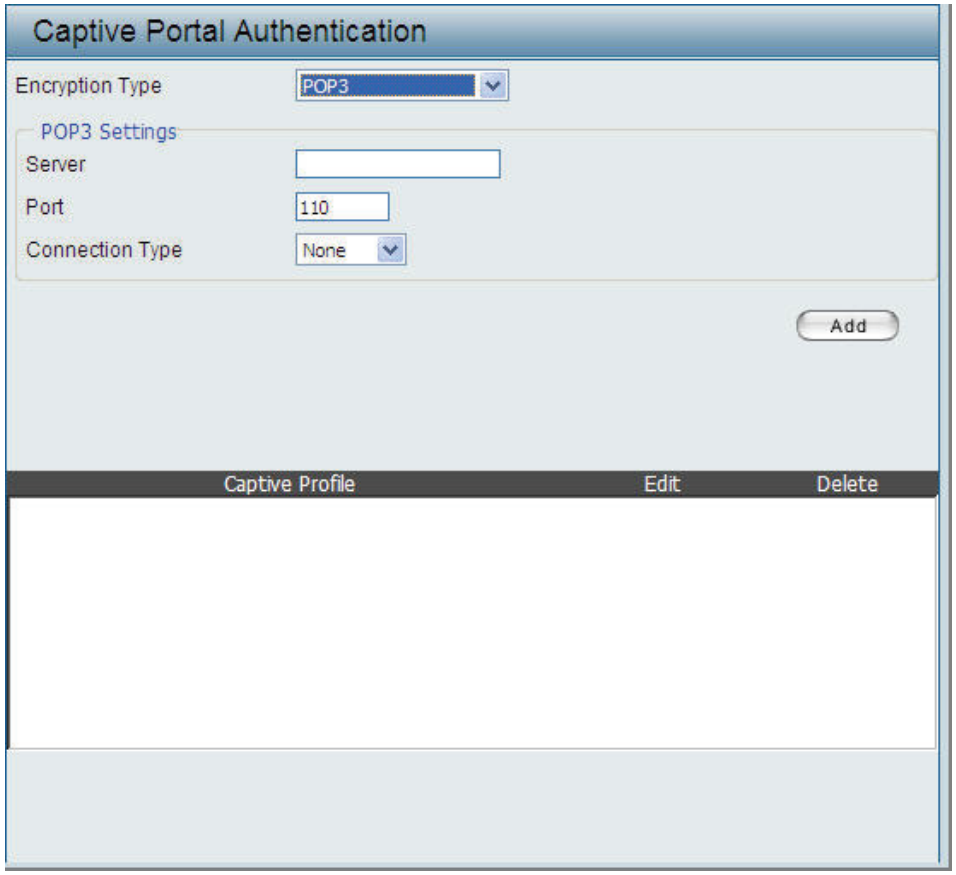
Authentication Settings - POP3

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

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

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

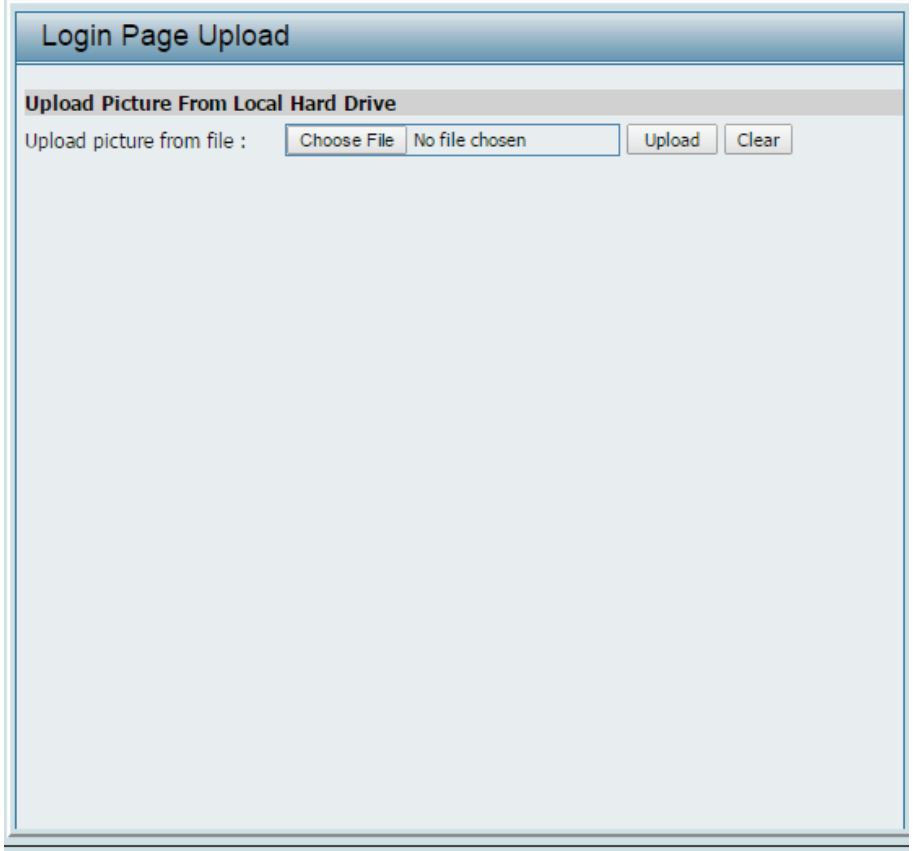
Connection Type: Select the connection type here. Options to choose from are None and SSL/TLS.



Login Page Upload

In this window, users can upload a custom login 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.

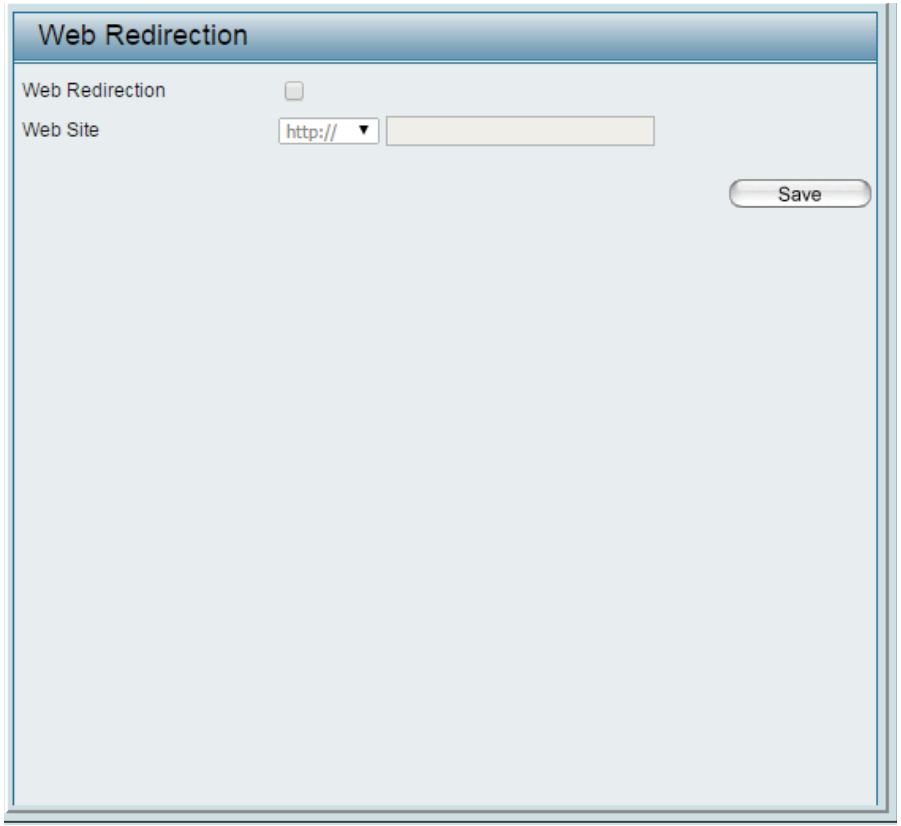


Web Redirection

In this windows, users can view and configure the Web redirection settings for the captive portal hosted by this access point. Wireless clients will be redirected to this web site prior and after authentication. Click the Save button to accept the changes made.

Web Redirection: Select this checkbox to enable the Web redirection feature.

Web Site: Enter the destination web site's address here.



MAC Bypass

The DAP-3662 features a wireless MAC Bypass. Once a user is finished with these settings, click the Save button to let the changes take effect.

Wireless Band: Select the wireless band for MAC Bypass.

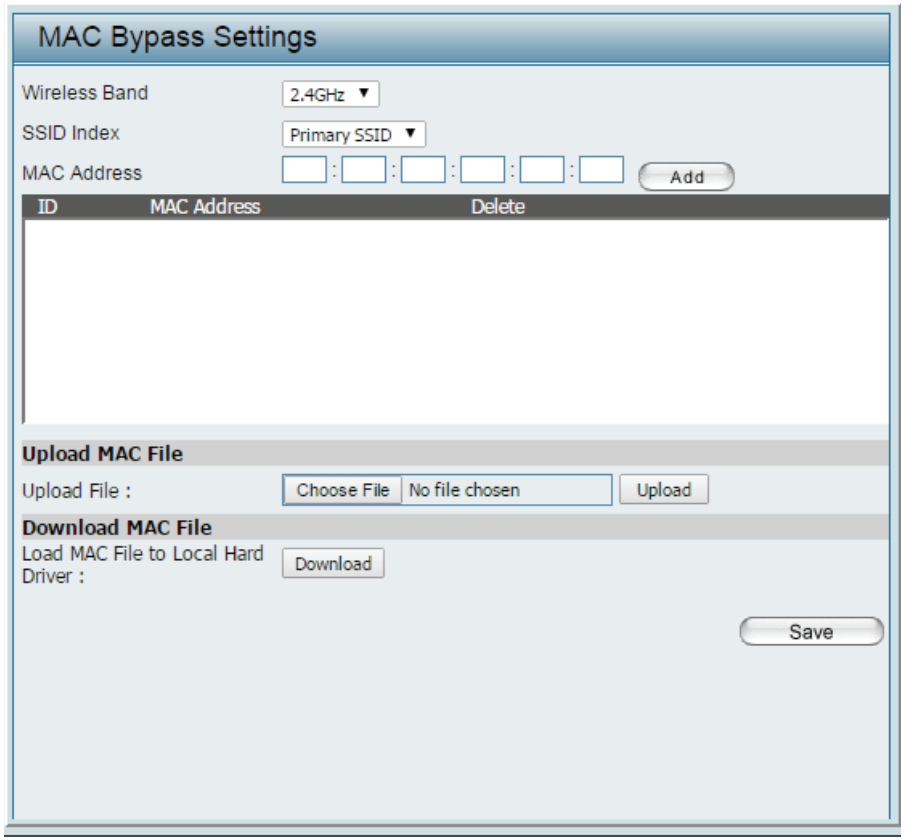
SSID Index: Select the SSID for MAC Bypass.

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

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

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

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



DHCP Server

Dynamic Pool Settings

The DHCP address pool defines the range of the IP address that can be assigned to stations in the network. A Dynamic Pool allows wireless stations to receive an available IP with lease time control. Once a user is finished, click the **Save** button to let the changes take effect.

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-3662 to function as a DHCP server.

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

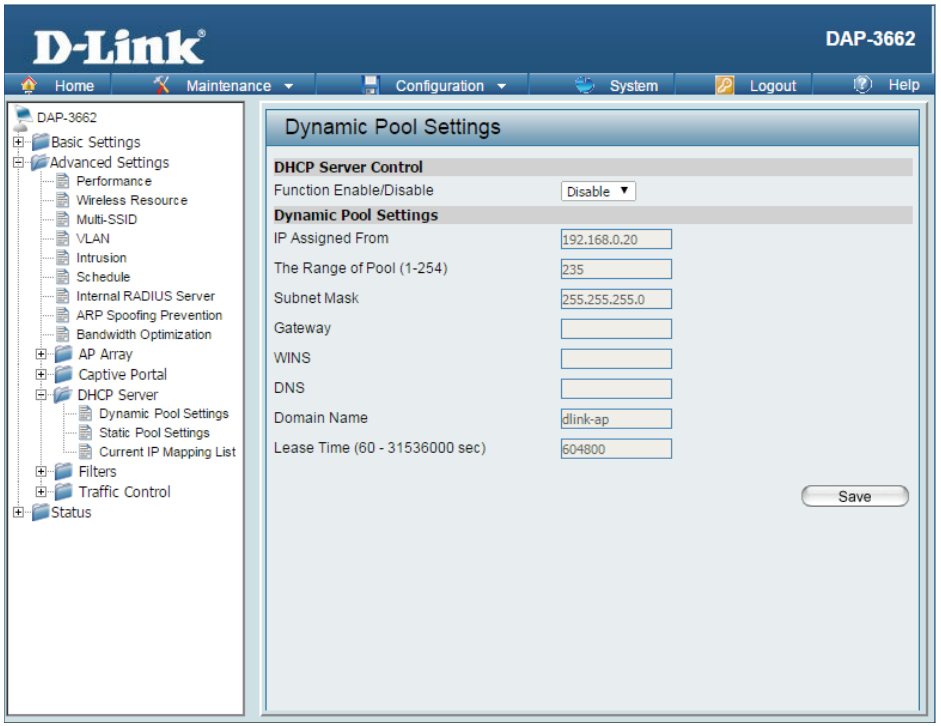
The Range of Pool (1-254): Enter the number of IP addresses available for assignment. IP addresses are increments of the IP address specified in the "IP Assigned From" field.

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.

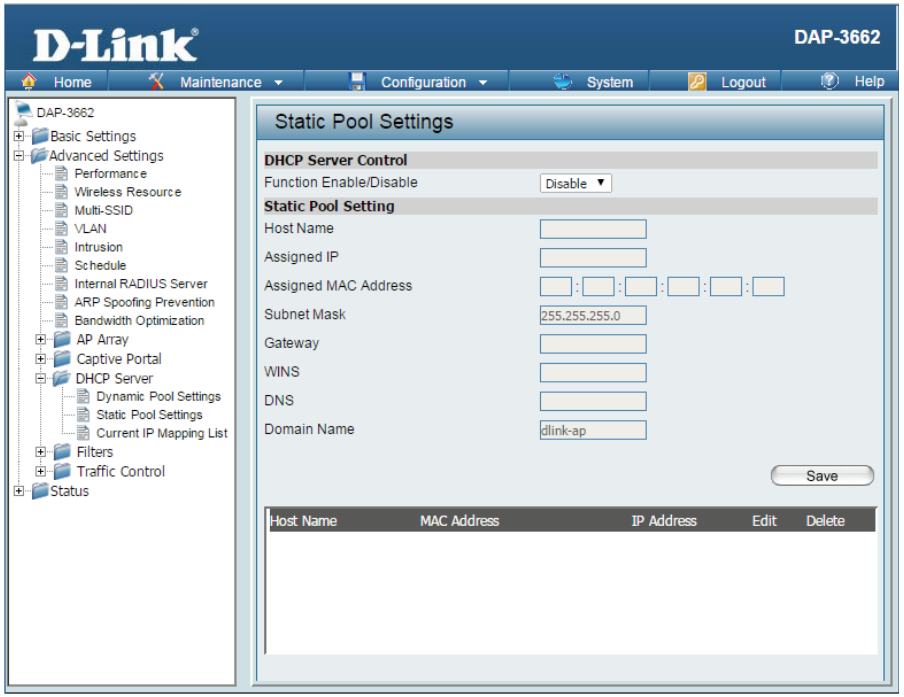


Domain Name: Enter the domain name of the network, if applicable. (An example of a domain name is **www.dlink.com**.)

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

Static Pool Setting

The DHCP address pool defines the range of IP addresses that can be assigned to stations on the network. A static pool allows specific wireless stations to receive a fixed IP without time control. Once a user is finished, click the **Save** button to let the changes take effect.



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-3662 to function as a DHCP server.

Host Name: Enter the name of the host computer in this text box.

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

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

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

Gateway: Specify the Gateway address for the wireless network.

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

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

Domain Name: Specify the domain name for the network.

Current IP Mapping List

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

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

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

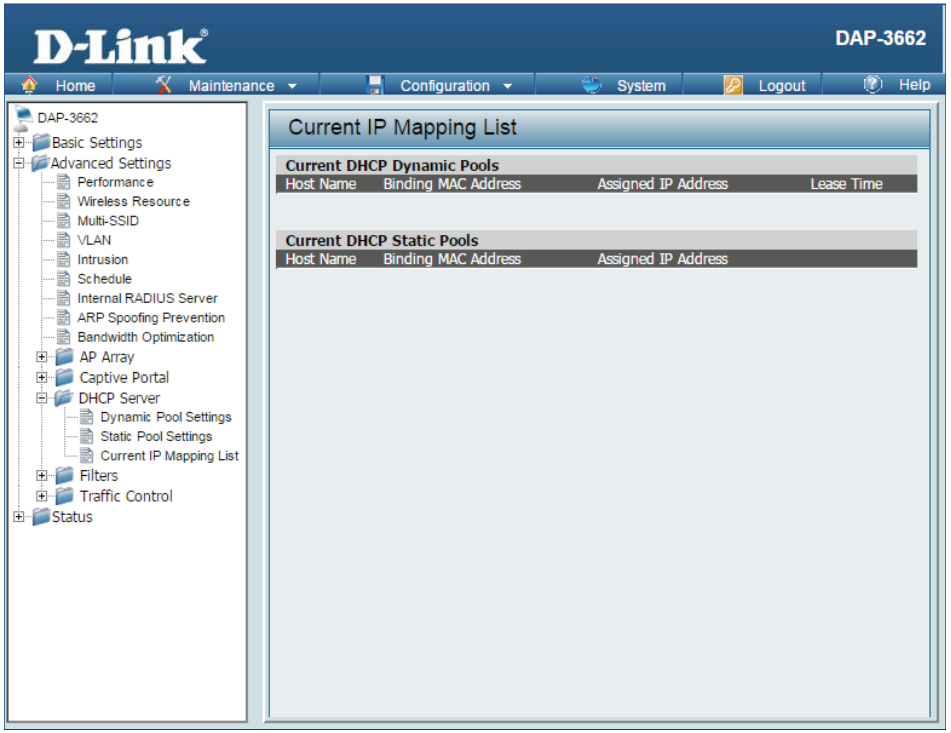
Assigned IP Address: The current corresponding DHCP-assigned IP address of the device.

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

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

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

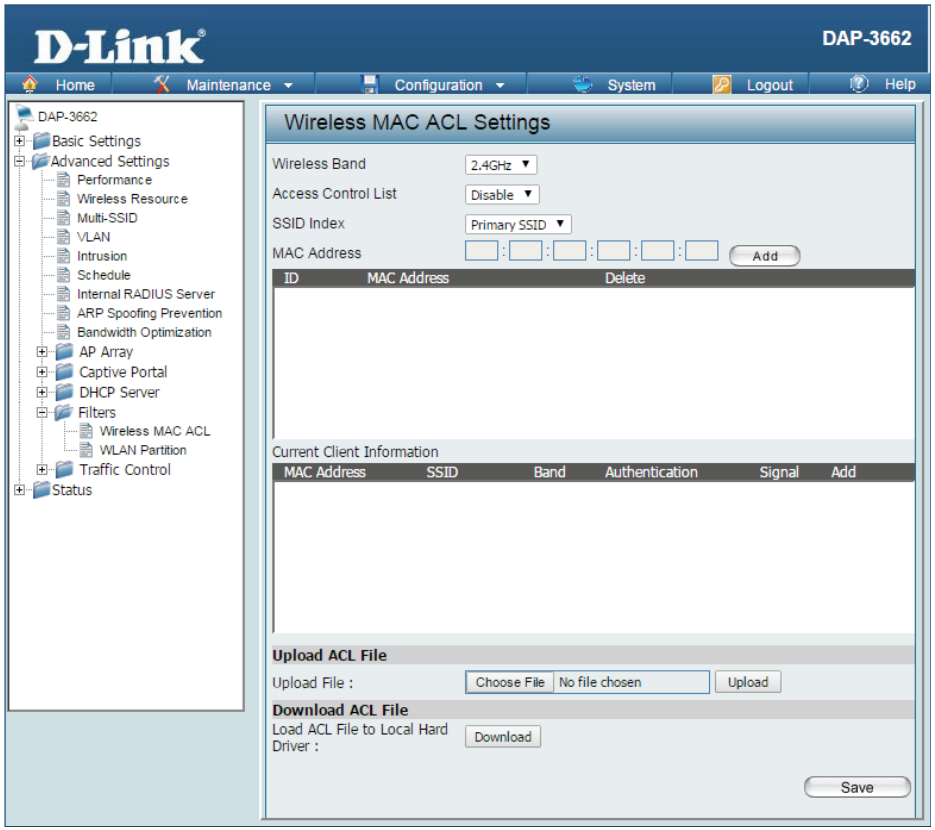
Assigned IP Address: The current corresponding DHCP-assigned static IP address of the device.



Filters

Wireless MAC ACL

The DAP-3662 features a wireless MAC Access Control List filter. Once a user is finished with these settings, click the **Save** button to let the changes take effect.



Wireless Band: Select the wireless band for Wireless MAC ACL.

Access Control List: Select **Disable** to disable the filters function.
Select **Accept** to accept only those devices with MAC addresses in the *Access Control List*. All other devices not on the list will be rejected.
Select **Reject** to reject the devices with MAC addresses on the *Access Control List*. All other devices not on the list will be accepted.

SSID Index: Select the SSID for Wireless MAC ACL.

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

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

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

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

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

WLAN Partition

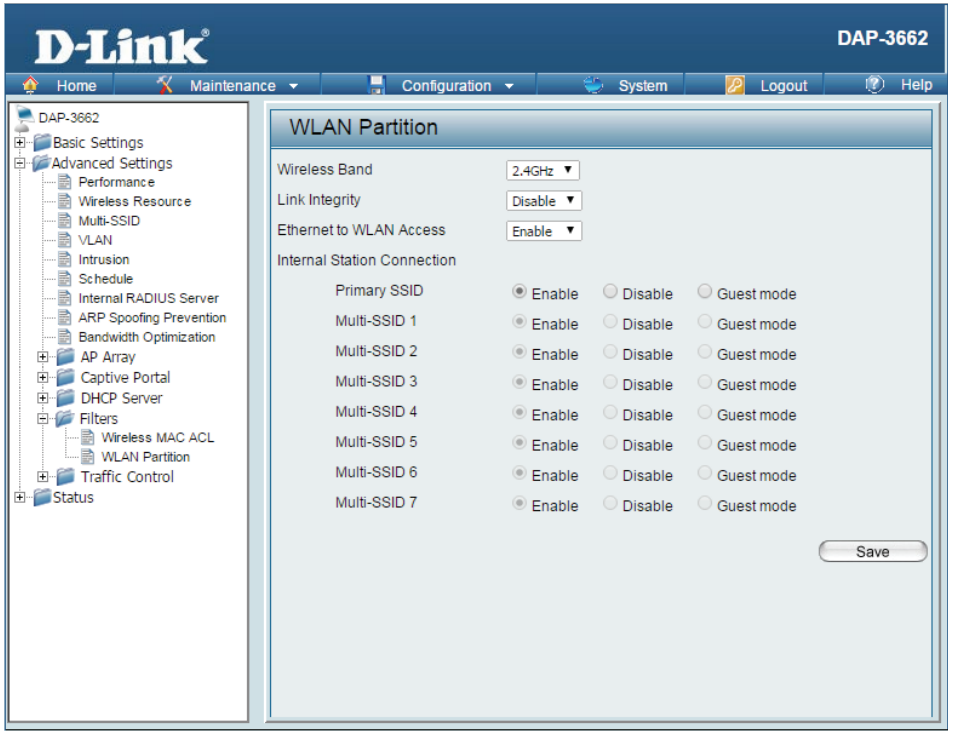
The DAP-3662 features a wireless partition. Once a user is finished with these settings, click the **Save** button to let the changes take effect.

Wireless Band: Displays the current wireless band.

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

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

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



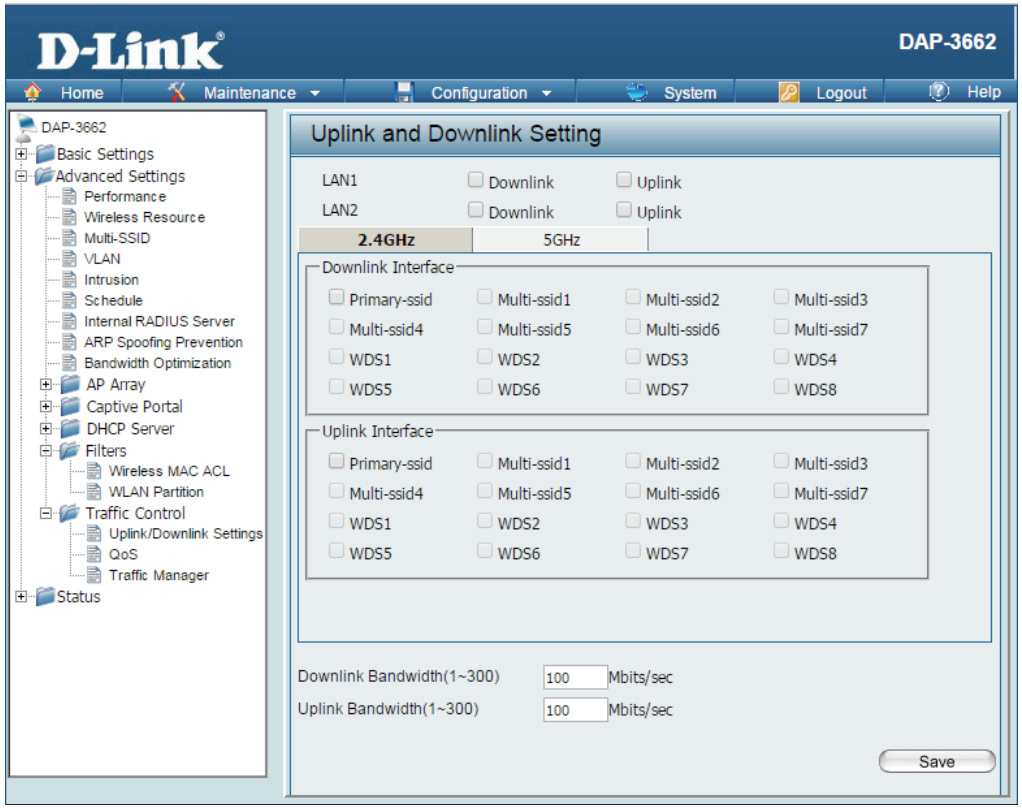
Traffic Control

Uplink/Downlink Setting

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

Downlink Bandwidth: The downlink bandwidth in Mbits per second.

Uplink Bandwidth: The uplink bandwidth in Mbits per second.



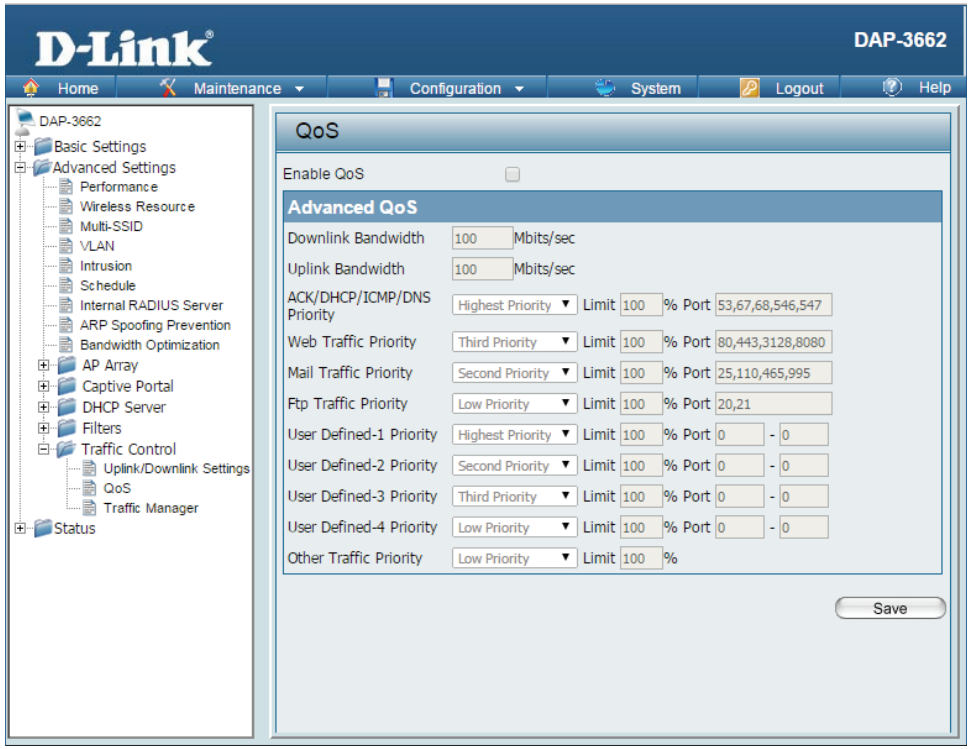
QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications. The DAP-3662 supports four priority levels. Once the desired QoS settings are finished, click the **Save** button to let your changes take effect.

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

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

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



Traffic Manager

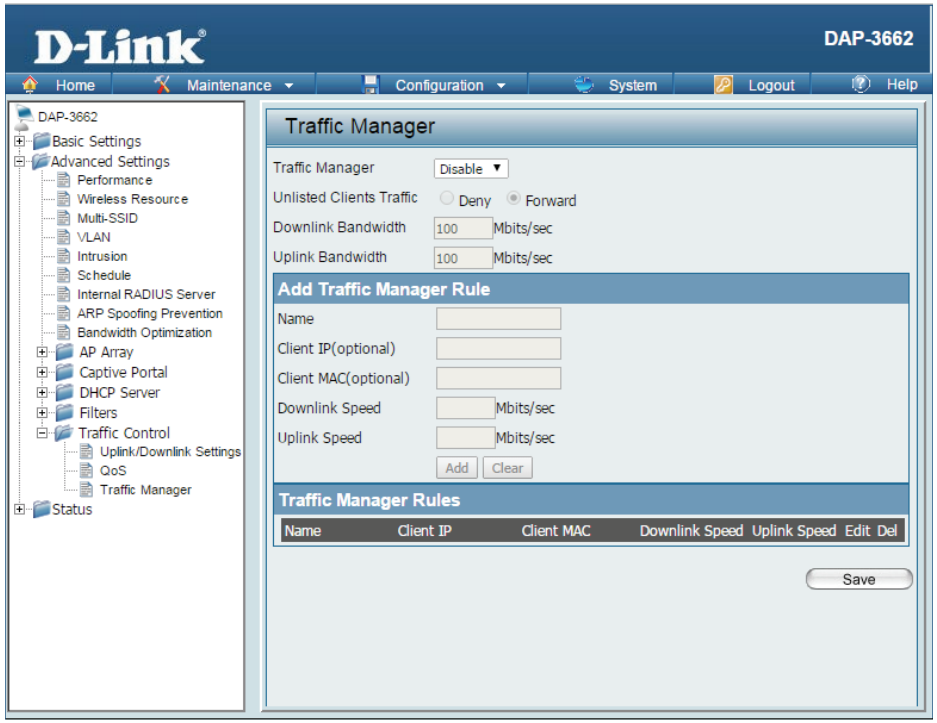
The traffic manager feature allows users to create traffic management rules that specify how to deal with listed client traffic and specify downlink/uplink speed for new traffic manager rules. Click the **Save** button to let your changes take effect.

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.

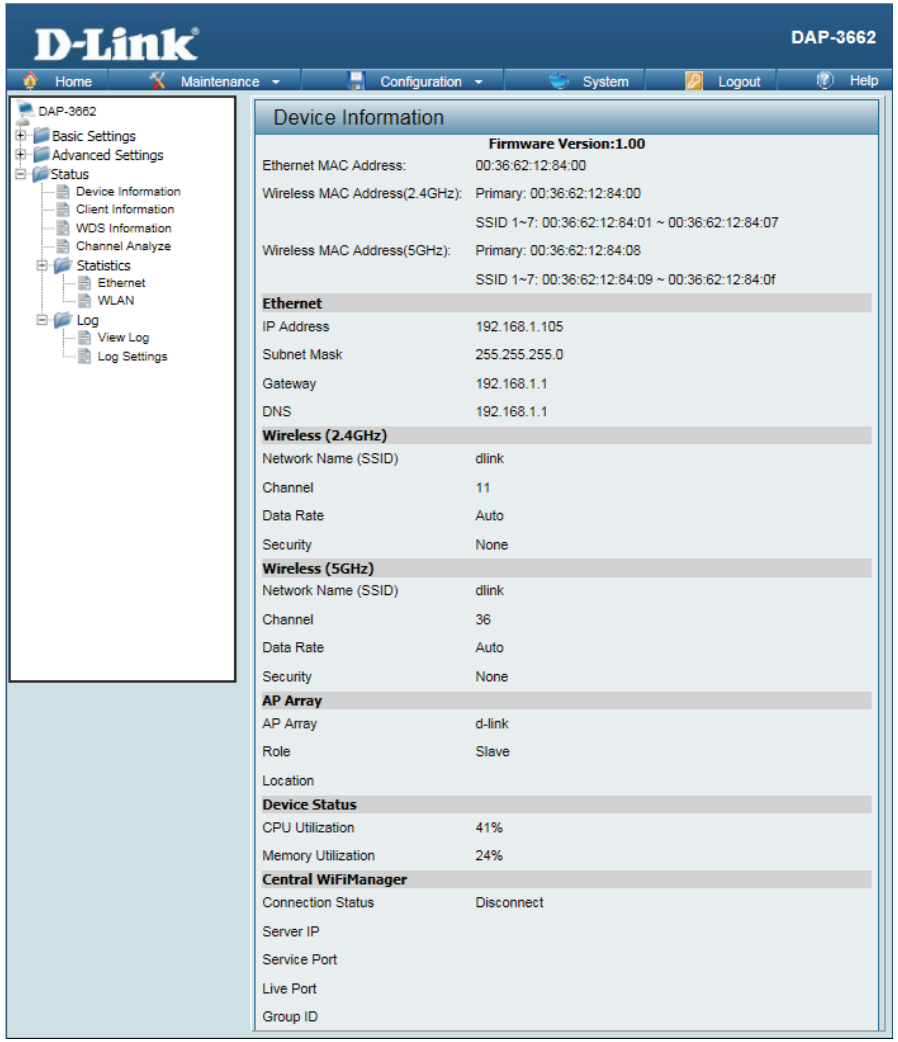
Uplink Bandwidth: The uplink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.



Status

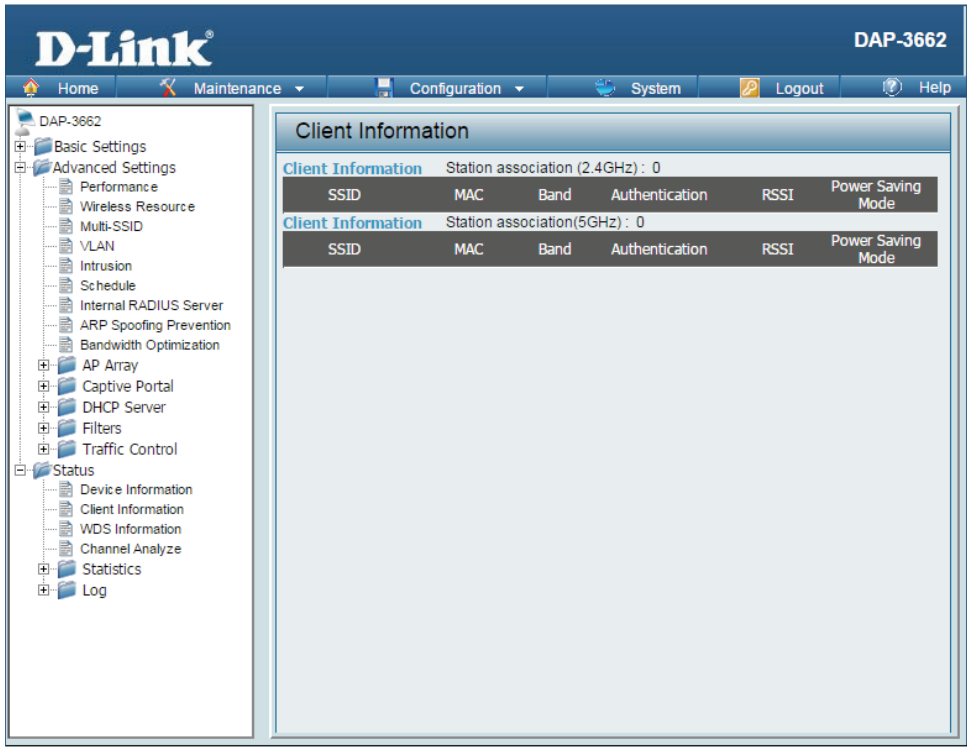
Device Information

Device Information: This read-only window displays the configuration settings of the DAP-3662, including the firmware version and the device's MAC address.



Client Information

Client Information: This window displays the wireless client information for clients currently connected to the DAP-3662.



The following information is available for each client communicating with the DAP-3662.

SSID: Displays the SSID of the client.

MAC: Displays the MAC address of the client.

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

Authentication: Displays the type of authentication being used.

RSSI: Displays the client's signal strength (received signal strength indicator).

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

WDS Information

WDS Information: This window displays the Wireless Distribution System information for clients currently connected to the DAP-3662.

The following information is available for each client communicating with the DAP-3662.

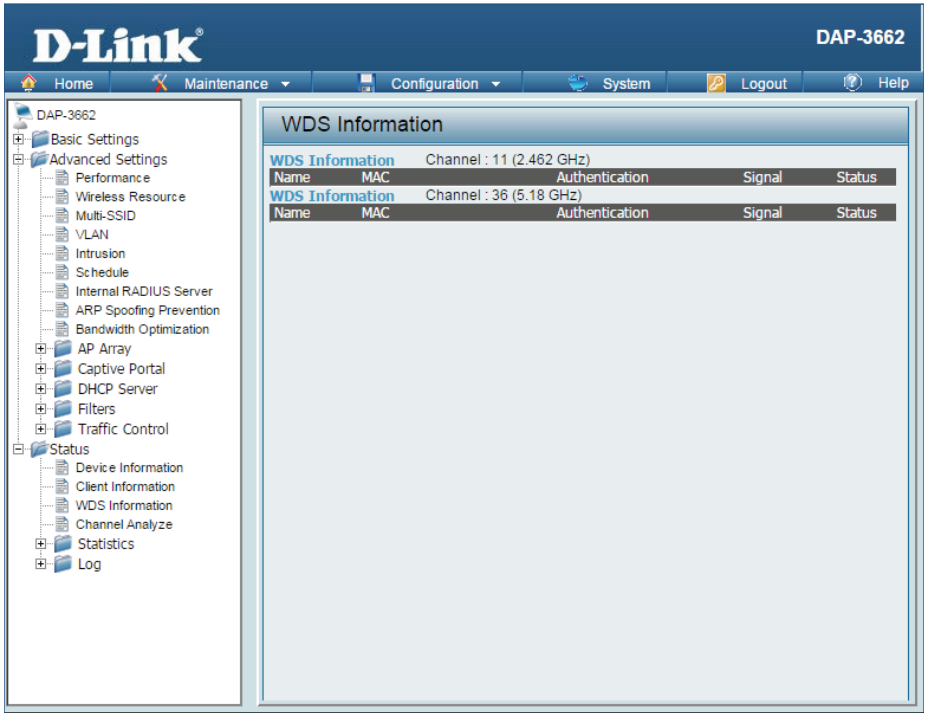
Name: Displays the name of the client.

MAC: Displays the MAC address of the client.

Authentication: Displays the type of authentication being used.

Signal: Displays the WDS link signal strength.

Status: Displays the status of the power saving feature.

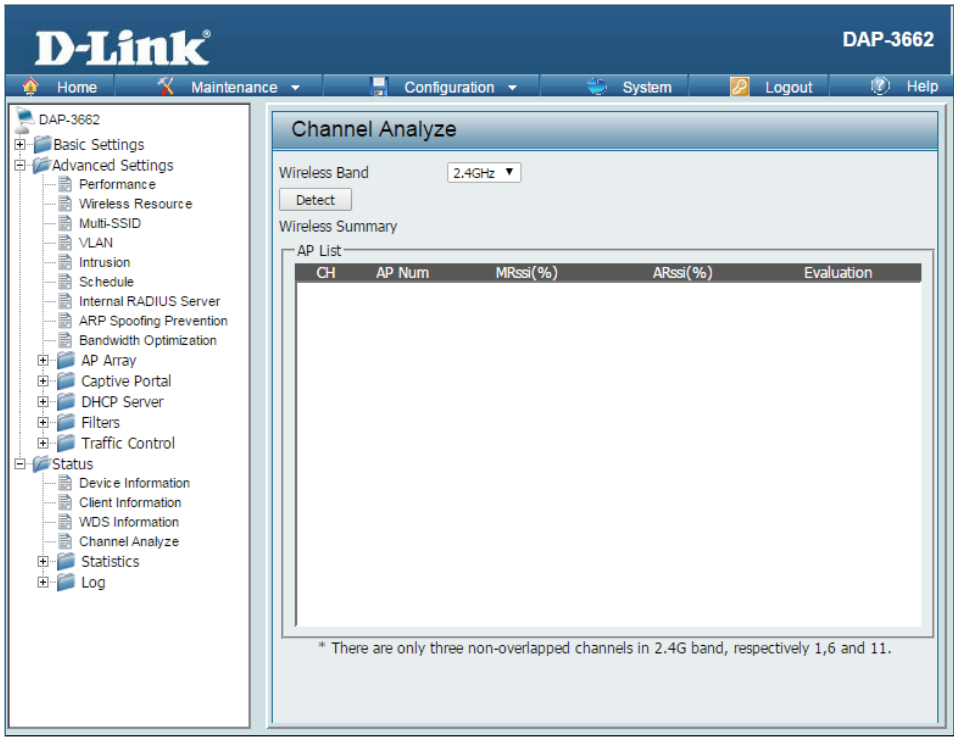


Channel Analyze

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

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

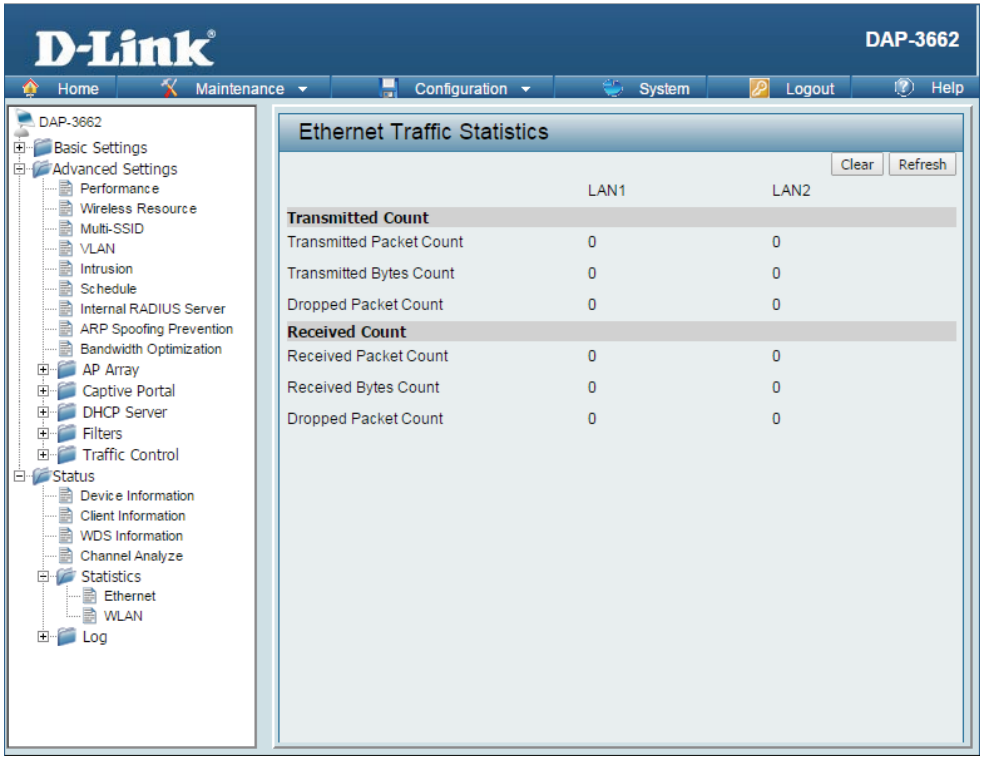
AP List: This will list the transmitting channels and quality.



Stats

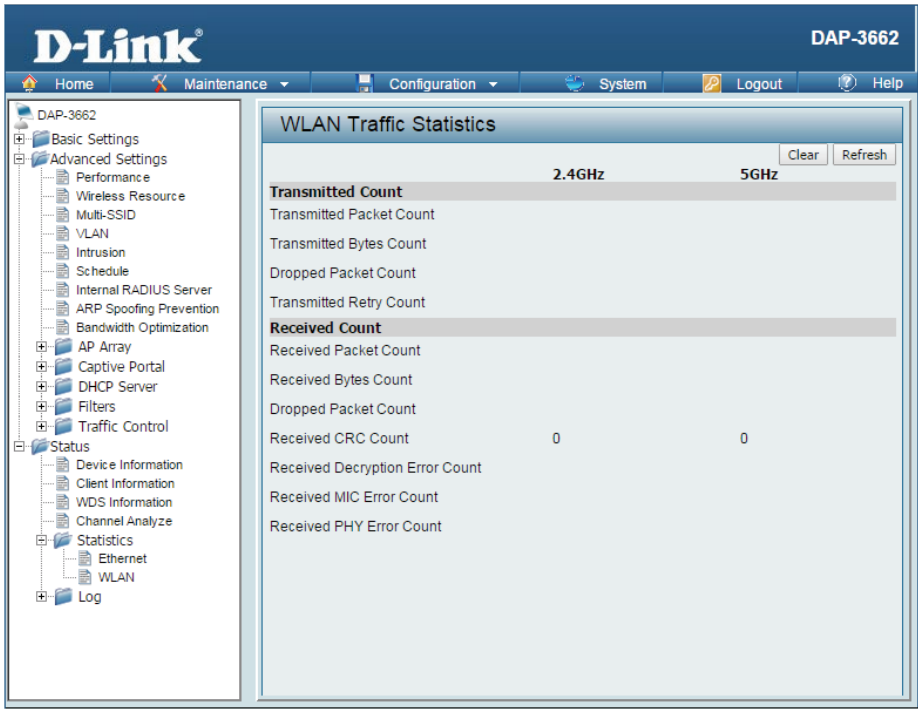
Ethernet

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



Wireless Traffic Stats

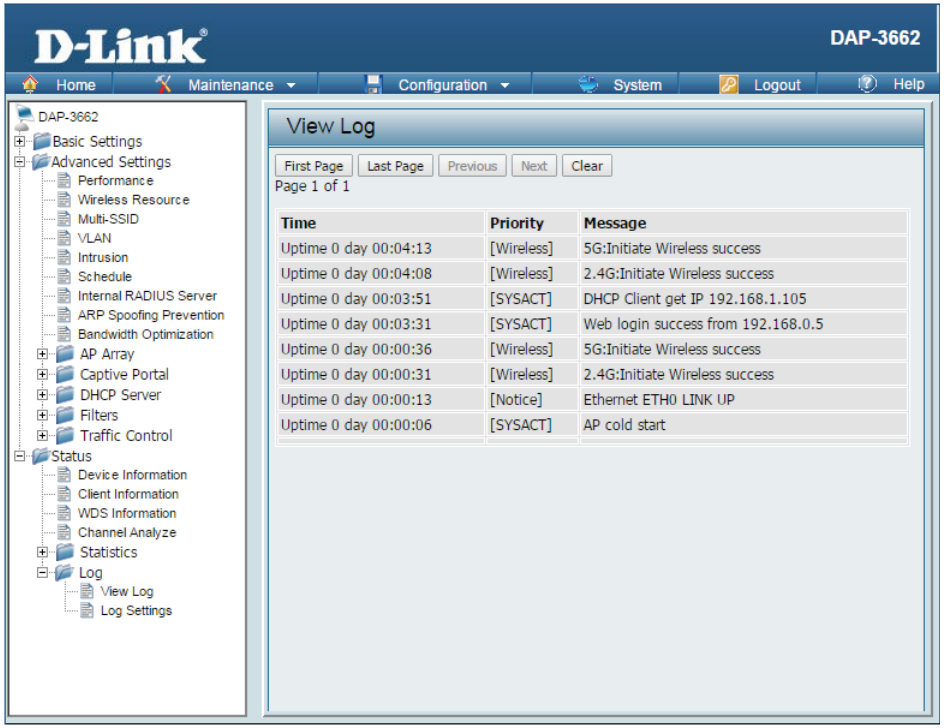
WLAN Traffic Statistics: This window displays wireless network statistics for data throughput, transmitted and received frames, and frame errors.



Log

View 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.



Log Settings

Log Server/IP Address: Enter the IP address of the server you would like to send the DAP-3662 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.

Email Notification: Check the box to enable Simple Mail Transfer Protocol.

From Email Address: Enter the e-mail address of the e-mail/SMTP sender.

To Email Address: Enter the e-mail address of the e-mail/SMTP recipient.

Email Server Address: Enter the IP address of the e-mail/SMTP server.

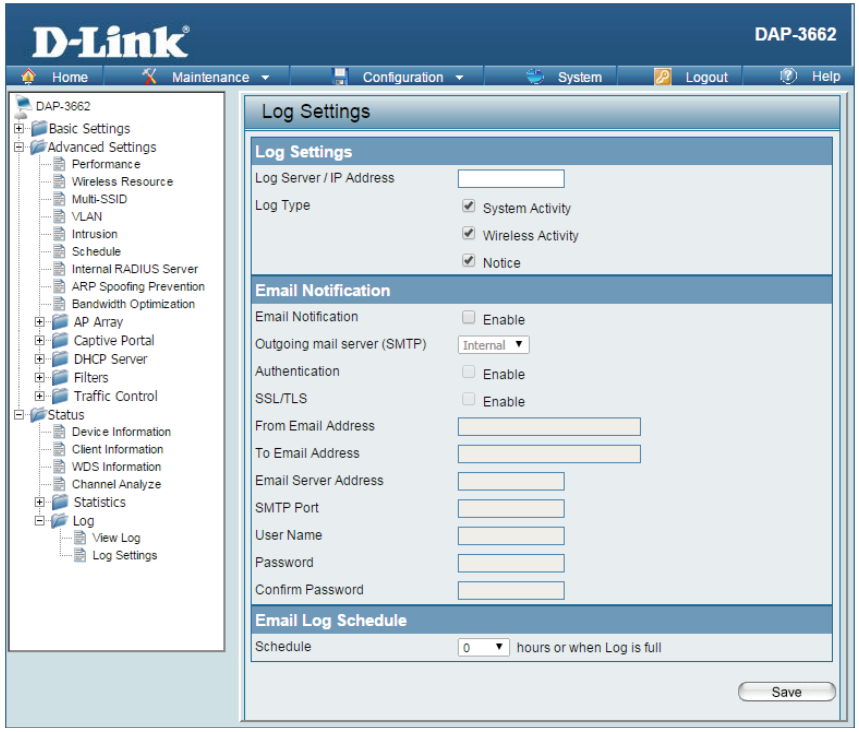
SMTP Port: Enter the desired SMTP port number. The default value is 25.

User Name: Enter a user name for the SMTP server.

Password: Enter a password for the SMTP server.

Confirm Password: Confirm the password for the SMTP server by retyping it.

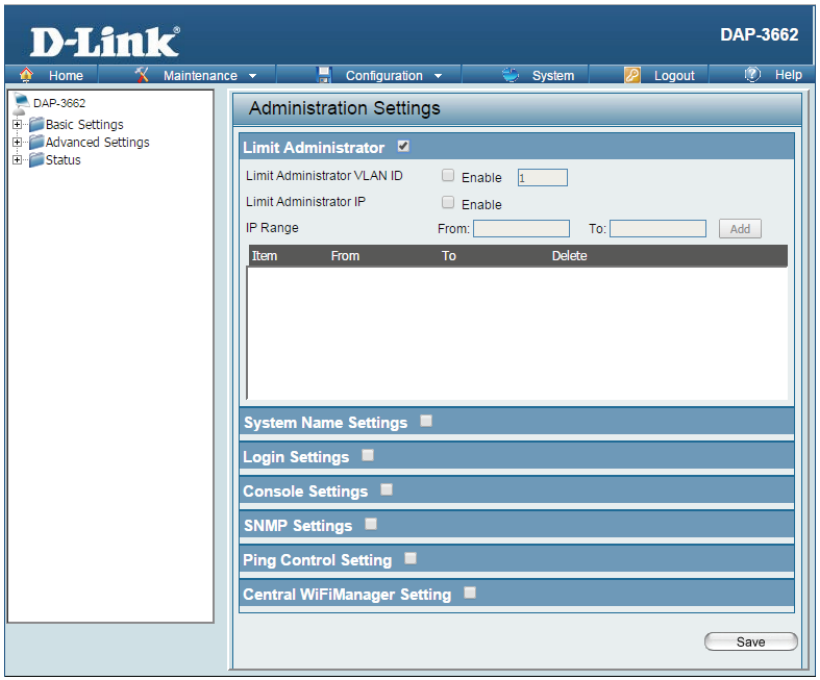
Schedule: Use the drop-down menu to set the e-mail log schedule.



Maintenance
Administrator Settings

Check one or more of the six main categories to display the various hidden administrator parameters and settings displayed on the next six windows.

Limit Administrator



Limit Administrator VLAN ID: Check the box and then 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.

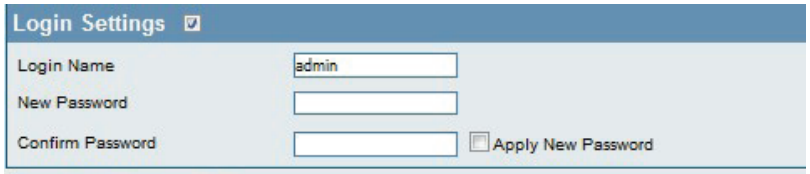
IP Range: Enter the IP address range that the administrator will be allowed to log in from and then click the **Add** button.

System Name Settings

System Name: The name of the device. The default name is **D-Link DAP-3662**.

Location: The physical location of the device, e.g. "office".

Login Settings

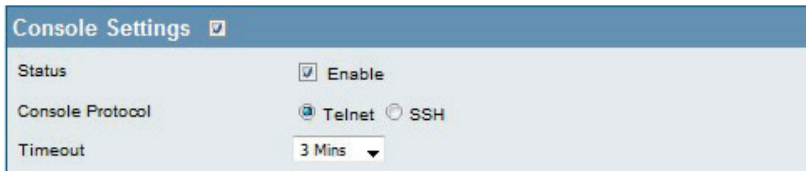


User Name: Enter a user name. The default is **admin**.

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

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

Console Settings



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

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**.

SNMP Settings

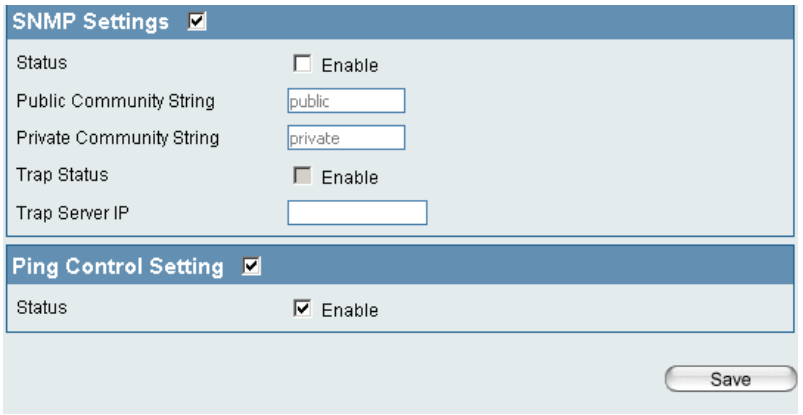
Status: Check the box to enable the SNMP functions. This is enabled by default.

Public Comminity String: Enter the public SNMP community string.

Private Community String: Enter the private SNMP community string.

Trap Status: Check the box to enable the trap status.

Trap Server IP: Enter the trap server IP address. This is the IP address of the SNMP manager to receive traps sent from the wireless access point.



Ping Control Setting

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

Central WiFiManager Settings

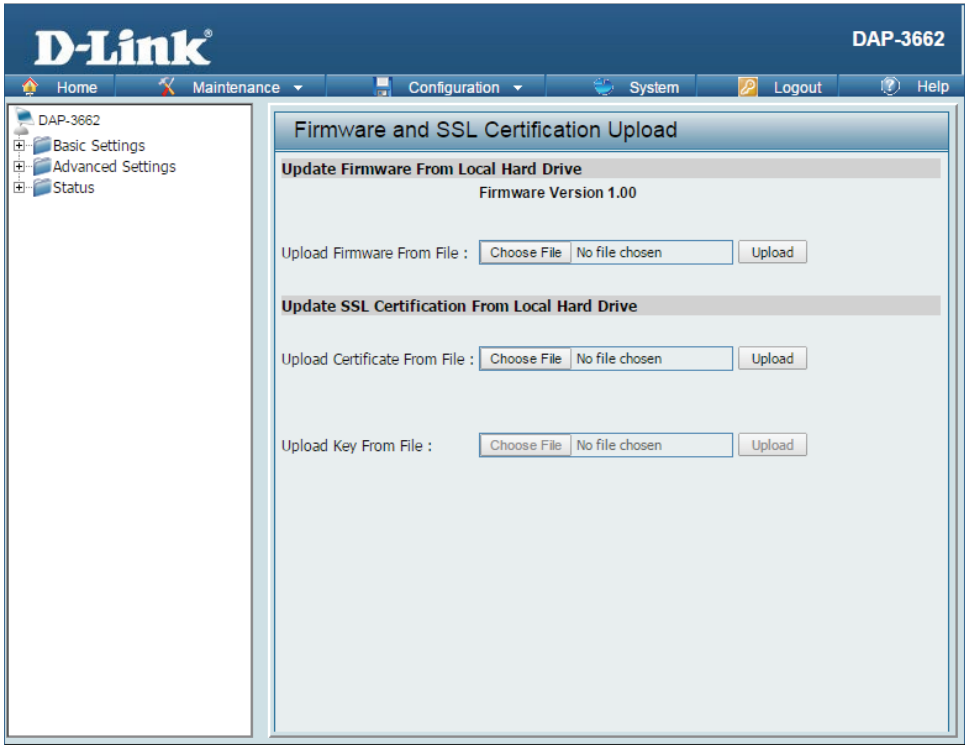
Enable Central WiFiManager : Select to enable or disable the Central WiFiManager.

Firmware and SSL Certification Upload

Upload Firmware From Local Hard Drive: The current firmware version is displayed above the file location field. After downloading the most recent version of firmware for the DAP-3662 from **http://dlink.com/support** 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: Click **Browse** to locate the language pack upgrade on your local computer. After selecting and opening the file, click **Upload** to upload the file to the DAP-3662.

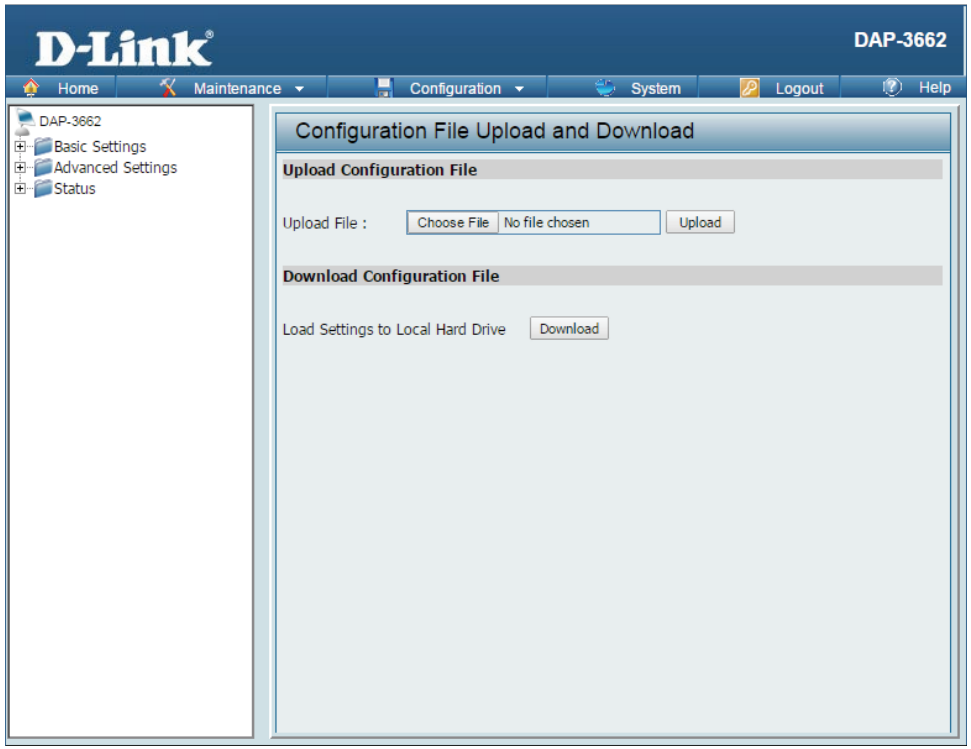
Upload SSL Certification From Local Hard Drive: Click **Browse** to locate the SSL Certification file on your local computer. After selecting and opening the file, click **Upload** to upload the file to the DAP-3662.



Configuration File

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-3662.

Download Configuration File: Click **Download** to save the current DAP-3662 configuration to your local computer. Note that if you save one configuration with the administrator's password now, after resetting your DAP-3662, and then updating to this saved configuration file, the password will be gone.



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 from the Internet.

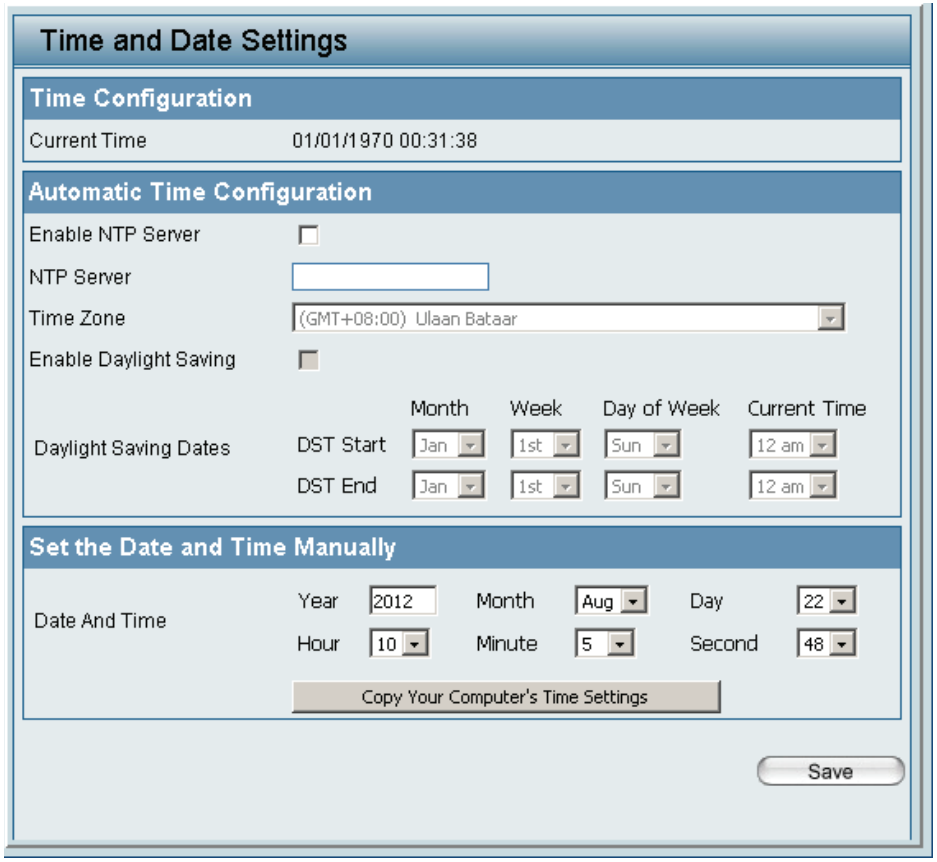
NTP Server: Enter the NTP server IP address.

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

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

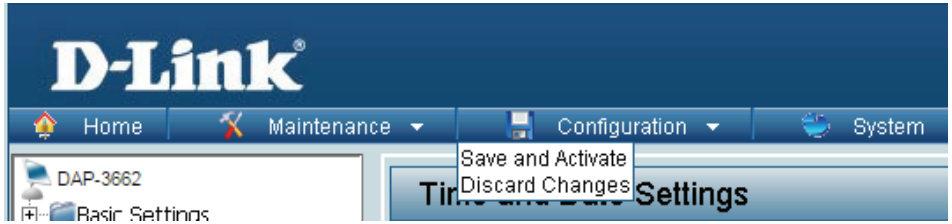
Daylight Saving Dates: Use the drop-down menu to select the correct Daylight Saving offset.

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



Configuration

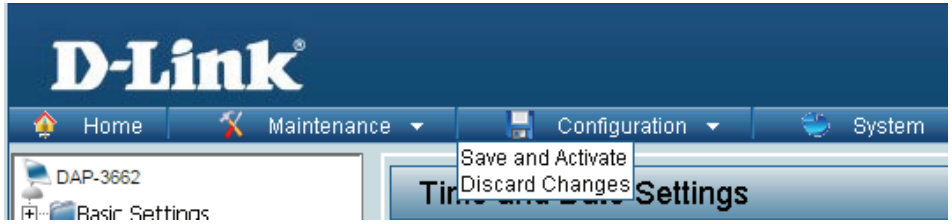
Save and Activate



The drop-down Configuration menu allows users to save the current changes and reboot the DAP-3662 by clicking "Save and Activate".

If the "Save and Activate" option is selected, the following window will appear to display how many seconds remain before the save settings and reboot system action is completed.

Discard Changes



The drop-down Configuration menu allows users to drop the latest changes by clicking "Discard Changes."

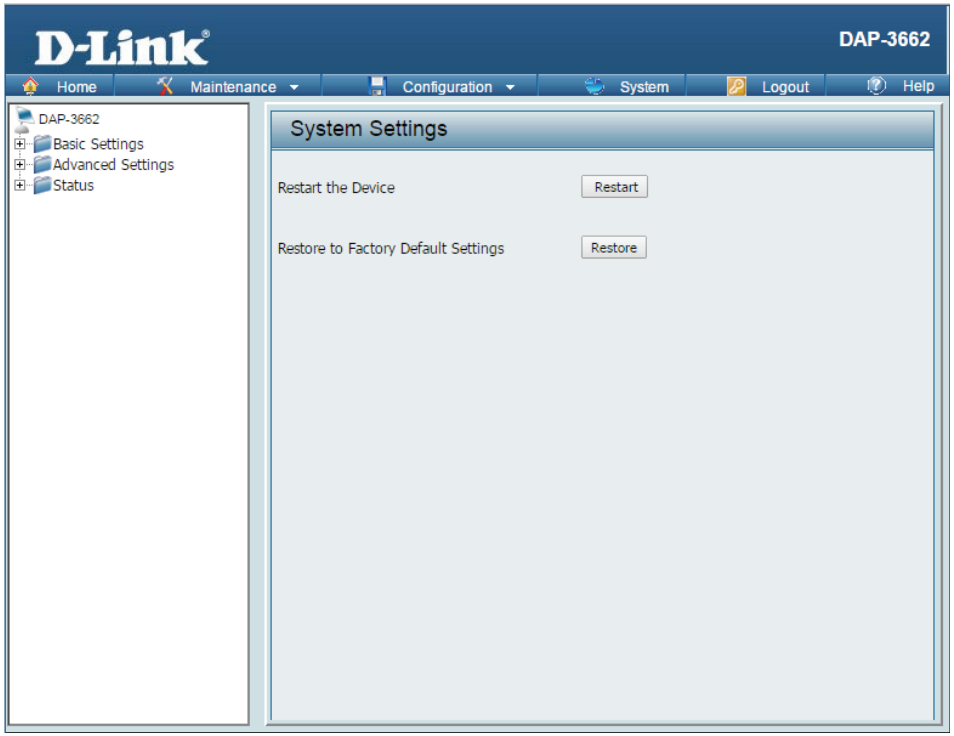
System

System Settings

Restart the Device: Click **Restart** to restart the DAP-3662.

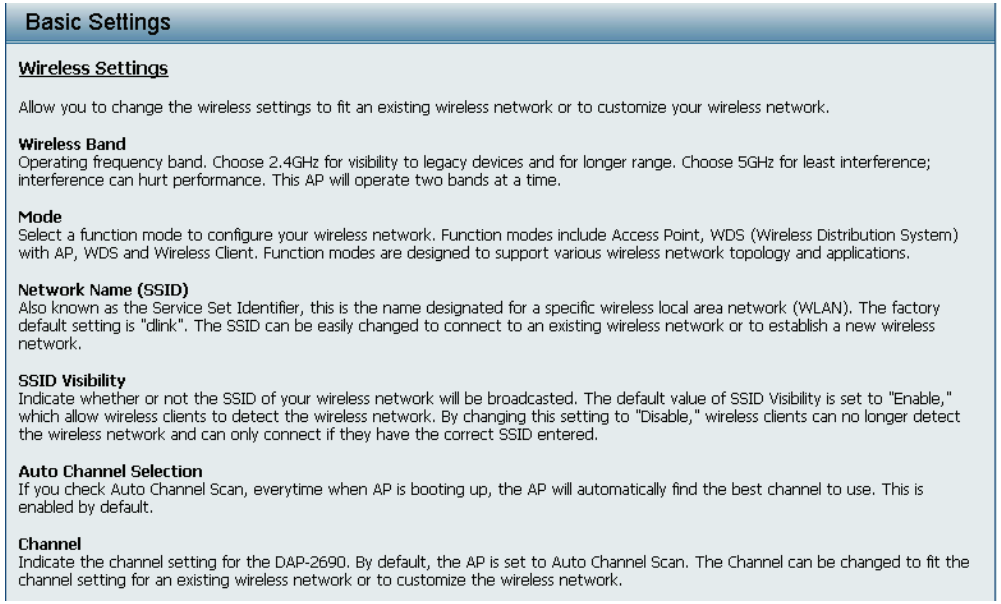
Restore to Factory Default Settings: Click **Restore** to restore the DAP-3662 back to factory default settings.

Clear Language Pack: Click **Clear** to remove the DAP-3662 language pack.



Help

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



Basic Settings

Wireless Settings

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

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

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

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

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

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

Channel
Indicate the channel setting for the DAP-2690. By default, the AP is set to Auto Channel Scan. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-3662. We will cover various aspects of the network setup, especially the network adapters. Please read the following if you are having any technical difficulties.

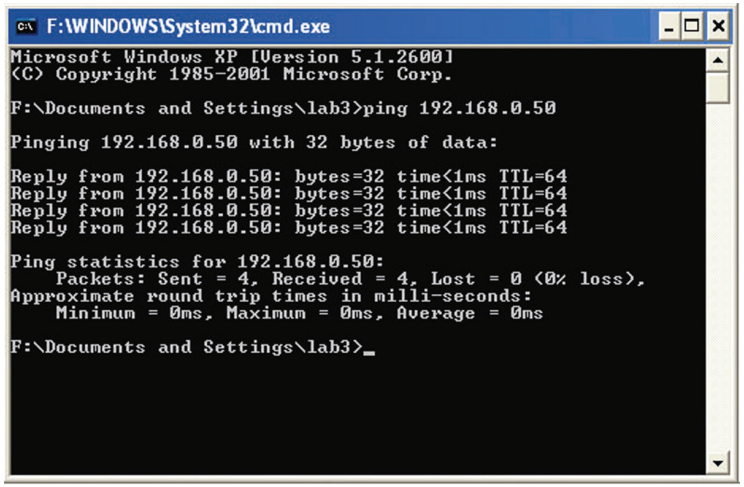
Note: *It is recommended that you use an Ethernet connection to configure the DAP-3662.*

1. The computer used to configure the DAP-3662 cannot access the Configuration menu.
   - Check if the LAN LED on the DAP-3662 is ON. If the LED is not ON, check if the cable for the Ethernet connection is securely inserted.
   - Check if the Ethernet adapter is working properly. Please see item 3 of this Troubleshooting section to check that the drivers for the network adapters are loaded properly.
   - Check if the IP address is in the same range and subnet as the DAP-3662.

Note: *The default IP address of the DAP-3662 is 192.168.0.50. All the computers on the network must have a unique IP address in the same range, e.g. 192.168.0.x. Any computers that have identical IP addresses will not be visible on the network. They must all have the same subnet mask, e.g. 255.255.255.0.*

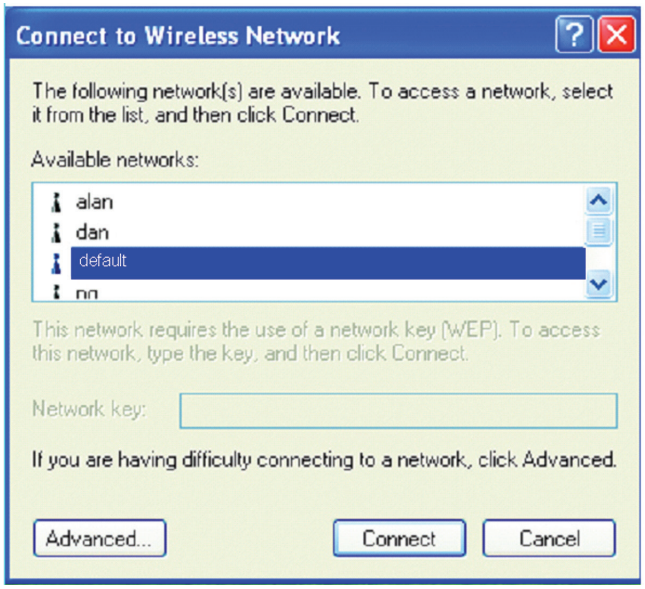
   - Perform a Ping test to make sure that the DAP-3662 is responding. Go to **Start** > **Run**, type **cmd**, and then press **Enter**. At the DOS prompt, type **ping 192.168.0.50**. A successful ping will show four replies.

Note: *If you have changed the default IP address, make sure to ping the correct IP address assigned to the DAP-3662.*



2. The wireless client cannot access the Internet within Infrastructure mode.

Make sure the wireless client is associated and joined with the correct access point. To check this connection, right-click on the *Local Area Connection* icon in the taskbar and select **View Available Wireless Networks**. The *Connect to Wireless Network* screen will appear. Please make sure you have selected the correct available network, as shown in the illustrations below.



- Check that the IP address assigned to the wireless adapter is within the same IP address range as the access point and gateway. Since the DAP-3662 has an IP address of 192.168.0.50, wireless adapters must have an IP address in the same range, e.g. 192.168.0.x. Each device must have a unique IP address; there may be no two devices with the same IP address. The subnet mask must be the same for all the computers on the network. To check the IP address assigned to the wireless adapter, double-click the Local Area Connection icon in the taskbar, then select the Support tab and the IP address will be displayed.

- If it is necessary to assign a Static IP Address to the wireless adapter. If you are entering a DNS Server address, you must also enter the Default Gateway Address. *Remember that if you have a DHCP-capable router, you will not need to assign a static IP address.*

3. What variables may cause my wireless products to lose reception?

D-Link products let you access your network from virtually anywhere you want, however, the positioning of the products within your environment will affect its wireless range.

4. Why does my wireless connection keep dropping?

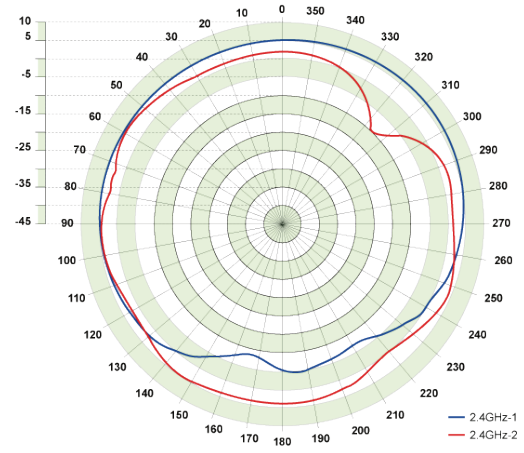
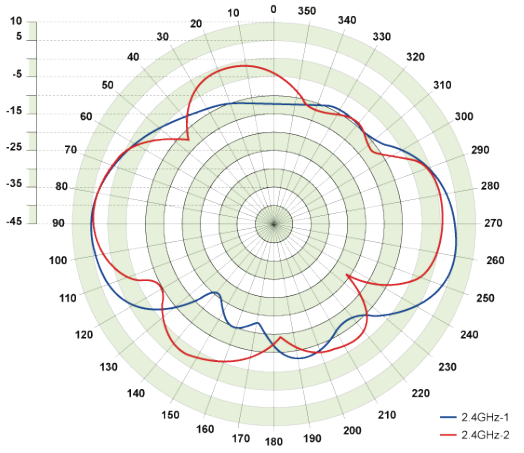
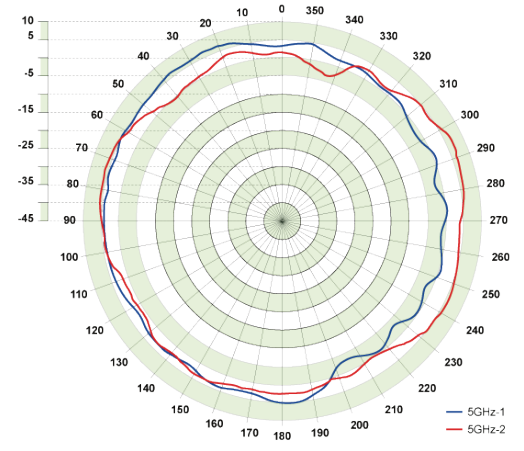
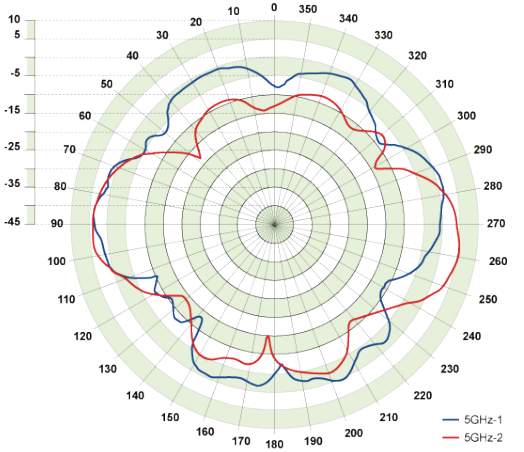
- Antenna Orientation - try different antenna orientations for the DAP-3662. Try to keep the antenna at least 6 inches away from the wall or other objects.
- If you are using 2.4 GHz cordless phones, X-10 equipment or other home security systems, ceiling fans, or lights, your wireless connection will degrade dramatically or even drop. Try changing the channel of your router, access point and wireless adapter to a different channel to avoid interference.
- Keep your product away - at least 3-6 feet - from electrical devices that generate RF noise like microwaves, monitors, electric motors, etc.

5. Why can't I get a wireless connection?

If you have enabled encryption on the DAP-3662, you must also enable encryption on all wireless clients in order to establish a wireless connection.

- Make sure that the SSID on the AP and the wireless client are exactly the same. If they are not, wireless connection cannot be established.
- Move the DAP-3662 and the wireless client into the same room and then test the wireless connection.
- Disable all security settings.
- Turn off your DAP-3662 and the client. Turn the DAP-3662 back on again, and then turn on the client.
- Make sure that all devices are set to Infrastructure mode.
- Check that the LED indicators are indicating normal activity. If not, check that the AC power and Ethernet cables are firmly connected.
- Check that the IP address, subnet mask, gateway, and DNS settings are correctly entered for the network.
- If you are using 2.4 GHz cordless phones, X-10 equipment, or other home security systems, ceiling fans, or lights, your wireless connection will degrade dramatically or drop altogether. Try changing the channel on your DAP-3662, and on all the devices in your network to avoid interference.
- Keep your product away - at least 3-6 feet - from electrical devices that generate RF noise like microwaves, monitors, electric motors, etc.

Antenna Pattern

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

Technical Specifications

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

Network Management
- Web Browser interface
  - HTTP
  - Secure HTTP (HTTPS)
- AP Array
- Central WiFiManager
- SNMP Support
  - Private MIB
- Command Line Interface
  - Telnet
  - Secure SSH Telnet

Security
- WPA™ Personal/Enterprise
- WPA2™ Personal/Enterprise
- WEP™ 64-/128-bit
- SSID Broadcast Disable
- MAC Address Access Control

Wireless Frequency Range
- 2.4 to 2.4835 GHz and 5.15 to 5.85 GHz**

Operating Voltage
- 48 V/0.5A Power Adapter or 802.3af PoE

Omni antenna
Two embedded 6dBi gain @ 2.4GHz
Two embedded 6dBi gain @ 5 GHz

LEDs
- Power
- Status

Temperature
- Operating: -30˚C to 60˚C
- Storing: -30˚C to 65˚C

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

Certifications
- FCC
- CE
- IC
- C-Tick
- UL
- WiFi

Dimensions
- L = 277.11 mm
- W = 240.03 mm
- H = 50.04 mm

*Maximum wireless signal rate derived from IEEE Standard 802.11g, 802.11a 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.

**Please note that operating frequency ranges vary depending on the regulations of individual countries and jurisdictions. The DAP-3662 isn't supported in the 5.25~5.35 GHz and 5.47 ~ 5.725 GHz frequency ranges in some regions.

FREE Central WiFiManager Software

DOWNLOAD NOW
DLINK.COM/WIFIDOWNLOAD

With the easy-to-use web-based interface you can...

- Configure once and apply to multiple Access Points
- Install on Windows PC
- Access on any device using a web-browser, e.g. smartphone or notebook
- Utilise user authentication and access control
- Monitor your entire wireless network in real time[1]
- Access detailed reports
- Optimise your bandwidth

FREE Central WiFiManager User Interface

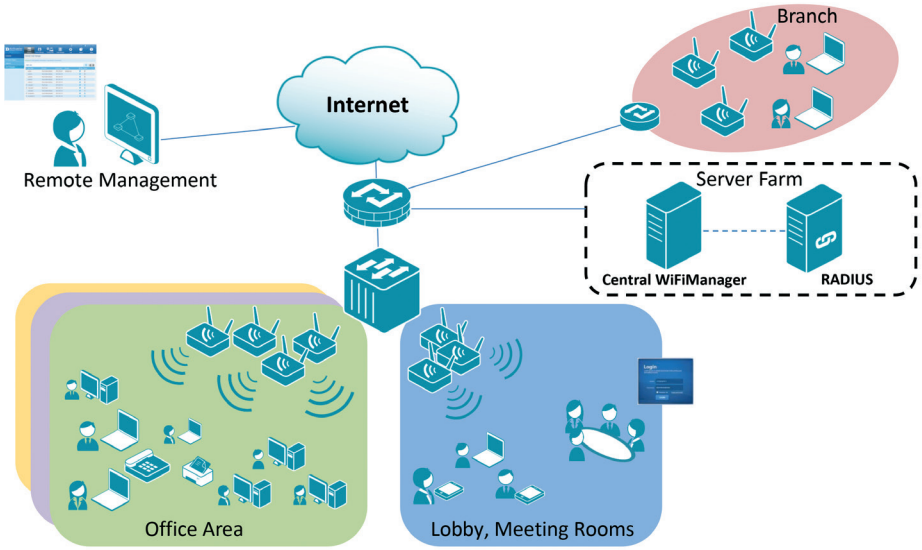
Supports multiple languages

1. see overleaf for selected product information.

Connect to More
www.dlink.com/wifidownload

D-Link®
Building Networks for People

FREE Central WiFiManager



Available on the following products[2]:

DAP-2695
Wireless AC1750 Indoor Access Point
Designed to support small to medium business or enterprise environments. Secure, manageable dual-band wireless LAN options.

DAP-2660
Wireless AC1200 Indoor Ceiling Access Point
Providing enhanced speeds of Wireless AC as well as dual-band connectivity to reduce interference, for a faster and more efficient network.

DAP-2310
Wireless N Indoor Access Point
Ideal for creating or expanding capacity of a wireless network; mainly used in high-traffic areas such as airports, coffee shops, sports venues, and university campus deployments.

DAP-2360
Wireless N PoE Access Point
For advanced indoor installations, this high-speed Access Point has integrated PoE support, allowing installation in areas where power outlets are not readily available.

DAP-2690
Wireless N Simultaneous Dual-Band PoE Access Point
Designed for indoor installation where power outlets are not readily available. Enables deployment of a highly manageable, robust and secure wireless network.

DAP-2330
Wireless N PoE Access Point
Ideal for wireless networks in high- traffic areas such as airports, coffee shops, shopping centres, sporting venues, hotels and campus deployments. PoE offers installation where power outlets are not available.

2. Visit dlink.com for selected Hardware & Software versions.