D-Link®
Building Networks for People

DAP-2360
Release 1.00

AirPrimier N PoE Access Point

User Manual

Business Class Networking

Table of Contents

Product Overview 4
Package Contents 4
System Requirements 4
Introduction 5
Features 7

Wireless Basics 8
Standards-Based Technology 9
Wireless Installation Considerations 10

Four Operational Modes 11

Getting Started 12

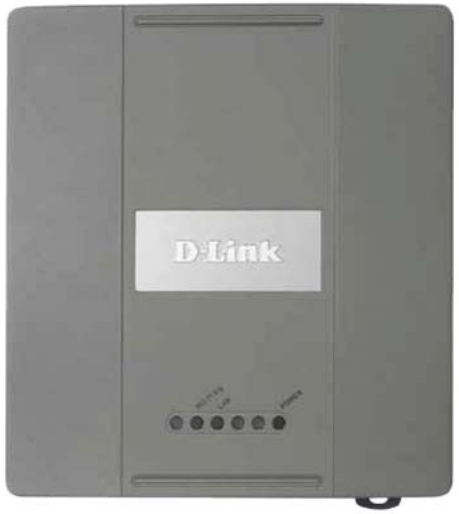
Configuration 14
Home > Basic Settings 16
Wireless 16
Access Point mode 16
WDS with AP mode 18
WDS mode 20
Wireless Client mode 22
Open System/Shared Key authentication 23
WPA-Personal authentication 24
WPA-Enterprise authentication 25
LAN 26
Home > Advanced Settings 27
Performance 27
Multi-SSID 29
VLAN 31
VLAN List 31
Port List 32
Add/Edit VLAN 33
PVID Setting 34
Intrusion 35
Schedule 36
QoS 37
DHCP Server 39
Dynamic Pool Settings 39
Static Pool Setting 41
Current IP Mapping List 43
Filters 44
Wireless MAC ACL 44
WLAN Partition 45
Home > Status 46
Device Information 46
Client Information 47
WDS Information 48
Stats 49
Ethernet 49
WLAN 50
Log 51

View Log 51
Log Settings 52
Maintenance 53
Administrator Settings 53
Limit Administrator 54
System Name Settings 55
Login Settings 56
Console Settings 57
SNMP Settings 58
Firmware and SSL Certification Upload 59
Configuration File 60
Time and Date 61
System 62
System Settings 62
Help 63

Troubleshooting 64

Package Contents

- D-Link DAP-2360 AirPremier N Single Band PoE Access Point
- Power Adapter
- CAT5 Ethernet Cable
- CD-ROM with User Manual
- Quick Install Guide
- 2 Detachable Antennas



Note: Using a power supply with a different voltage rating than the one included with the DAP-2360 will cause damage and void the warranty for this product.

System Requirements

- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet Adapter
- Internet Explorer Version 7.0 or Firefox 3.0 and Above (for configuration)

Introduction

The DAP-2360 802.11n 2.4GHZ AP increases productivity by allowing you to work faster and more efficiently. With the DAP-2360, bandwidth-intensive applications like graphics or multimedia will benefit significantly because large files are now able to move across the network quickly.

The DAP-2360 is capable of operating in one of four different wireless networking modes; access point, WDS (Wireless Distribution System) with AP, WDS, or Wireless Client mode.

An ideal solution for quickly creating and extending a wireless local area network (WLAN) in offices or other workplaces, trade shows, and special events, the DAP-2360 providing data transfer rates up to 300Mbps. (The 802.11n standard is backwards compatible with 802.11g, and 802.11b devices.)

WPA/WPA2 is offered in two flavors: Enterprise (used for corporations) and Personal (used for home users).

WPA-Personal and WPA2-Personal are directed towards home users who do not have the server-based equipment required for user authentication. The method of authentication is similar to WEP because you define a “Pre-Shared Key” on the wireless router/AP. Once the pre-shared key is confirmed and satisfied at both the client and access point, access is then granted. The encryption method used is referred to as the Temporal Key Integrity Protocol (TKIP), which offers per-packet dynamic hashing. It also includes an integrity checking feature which ensures that the packets were not tampered with during wireless transmission.

WPA-Enterprise and WPA2-Enterprise are ideal for businesses that already have existing security infrastructures established. Management and security implementation can now be centralized on a server participating on the network. Utilizing 802.1x with a RADIUS (Remote Authentication Dial-in User Service) server, a network administrator can define a list of authorized users who can access the wireless LAN. When attempting to access a wireless LAN with WPA-Enterprise configured, the new client will be requested to enter a username with a password. If the new client is authorized by the administration, and enters the correct username and password, then access is then granted. In the case where an employee leaves the company, the network administrator is able to remove the previous employee from the authorized list to avoid compromising the network.

EAP (Extensible Authentication Protocol) is available through the Windows® XP operating system. You will need to use the same type of EAP protocol on all devices in your network when using the 802.1x feature.

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

Features

- **Four different operation modes** - Capable of operating in one of four different operation modes to meet your wireless networking needs: Access Point, WDS with AP, WDS, or Wireless Client.
- Faster wireless networking with the 802.11n standard to provide a maximum wireless signal rate of up to 300 Mbps*.
- Compatible with the 802.11b standard to provide a wireless data rate of up to 11 Mbps, allowing you to migrate your system to the 802.11n and 802.11g standards on your own schedule without sacrificing connectivity.
- Better security with WPA - The DAP-2360 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.
- **AP Manager II 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-2360 is not just fast, but also supports SNMP v.3 for better network management. Superior wireless AP manager software is bundled with the DAP-2360 for network configuration and firmware upgrade. Systems administrators can also set up the DAP-2360 easily with the Web-based configuration. A D-Link D-View 6.0 module will be downloadable for network administration and real-time network traffic monitoring with D-Link D-View 6.0 software.
- Utilizes OFDM technology (Orthogonal Frequency Division Multiplexing).
- Supports one 10/100/1000M Ethernet port.
- Operates in the 2.4~2.5 GHz frequency ranges.
- Web-based interface for managing and configuring.

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

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-2360 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.

Standards-Based Technology

The DAP-2360 Wireless Access Point utilizes the 802.11b, 802.11g, and 802.11n standards.

The IEEE 802.11n standard is an extension of the 802.11b, and 802.1g standards that came before it. It increases the maximum wireless signal rate up to 300 Mbps* within 2.4 GHz bands, utilizing OFDM technology.

This means that in most environments - within the specified range of this device - you will be able to transfer large files quickly, or even watch a movie in MPEG format over your network without noticeable delays. This technology works by transmitting high-speed digital data over a radio wave utilizing OFDM (Orthogonal Frequency Division Multiplexing) technology. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then simultaneously transmitted at different frequencies to the receiver. OFDM reduces the amount of crosstalk (interference) in signal transmissions.

The D-Link DAP-2360 will automatically sense the best possible connection speed to ensure the greatest possible speed and range.

802.11n offers the most advanced network security features available today, including WPA.

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

Wireless Installation Considerations

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

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

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

3. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on the 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.

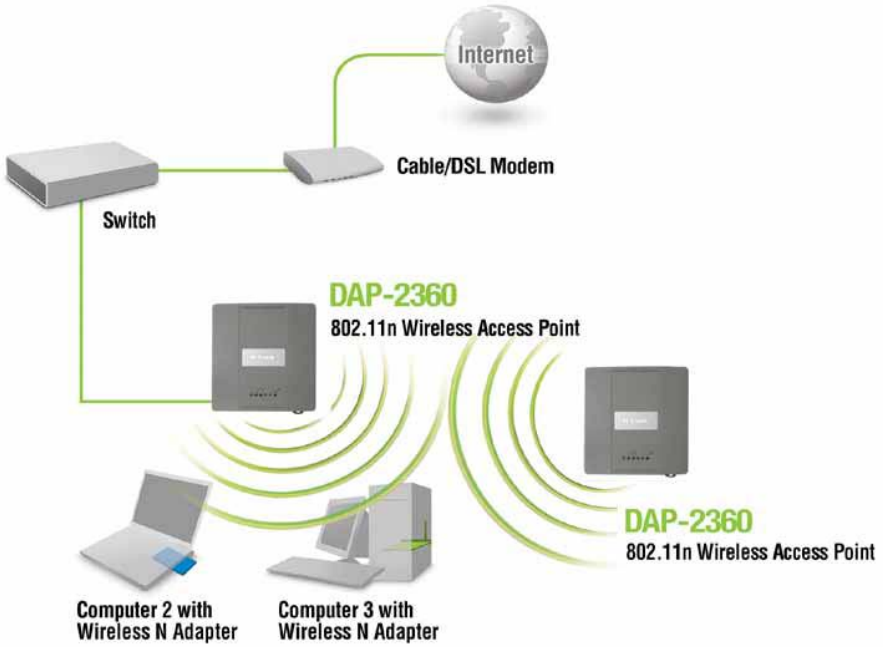
4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

5. If you are using 2.4GHz 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 2.4GHz 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

Getting Started



1. You will need broadband Internet access.
2. Consult with your cable or DSL provider for proper installation of the modem.
3. Connect the cable or DSL modem to a router. See the printed Install Guide included with your router.
4. If you are connecting a desktop computer to your network, install a wireless PCI adapter into an available PCI slot on your desktop computer.
5. Install the drivers for your wireless CardBus adapter into a laptop computer.

Connect one end of an Ethernet cable (included with your package) to the LAN port on the DAP-2360 and the other end of the Ethernet cable to your computer. The AP can be powered on by the power adapter shipped with the AP.

Configuration

To configure the DAP-2360, use a computer that is connected to the DAP-2360 with an Ethernet cable (see the *Network Layout diagram*).

First, 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.

Start your web browser program (Internet Explorer, Mozilla Firefox).

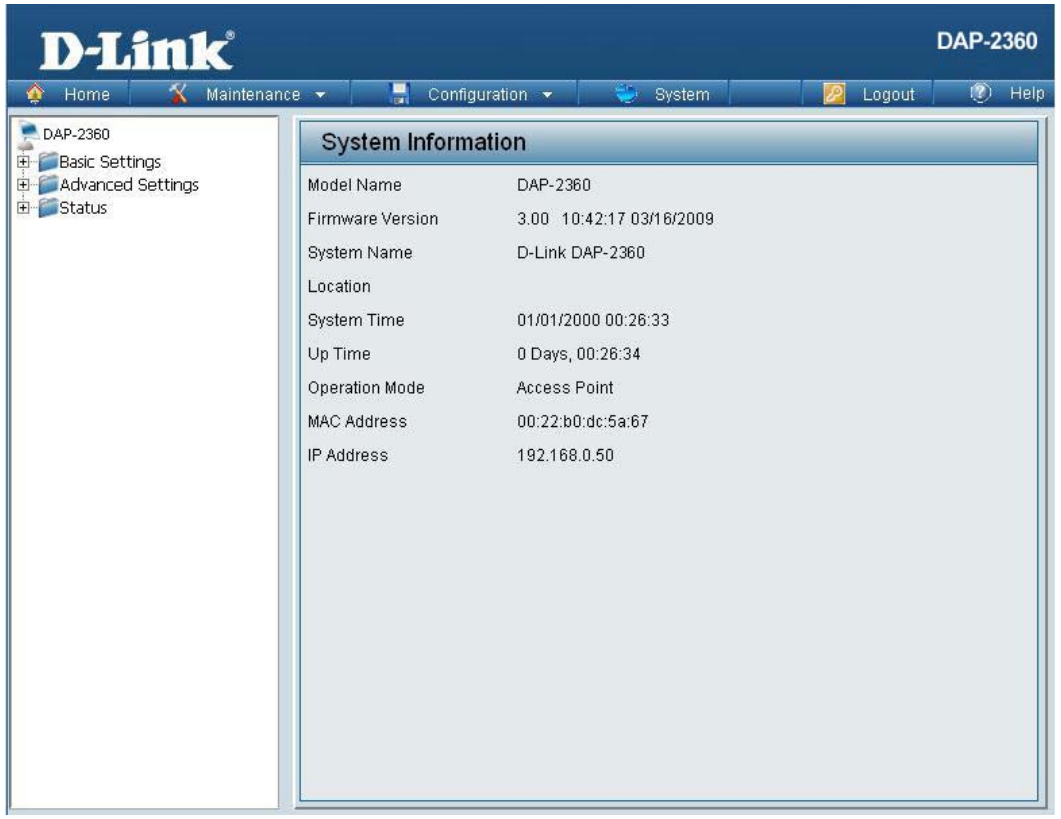
Type the IP address and http port of the DAP-2360 in the address field (**http://192.168.0.50**) and press **Enter**. Make sure that the IP addresses of the DAP-2360 and your computer are in the same subnet.

Note: *If you have changed the default IP address assigned to the DAP-2360, make sure to enter the correct IP address.*

Enter the user name (**admin**) and your password. Leave the password field blank by default, and click **Login**.

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

After successfully logging into the DAP-2360 the following screen will appear:



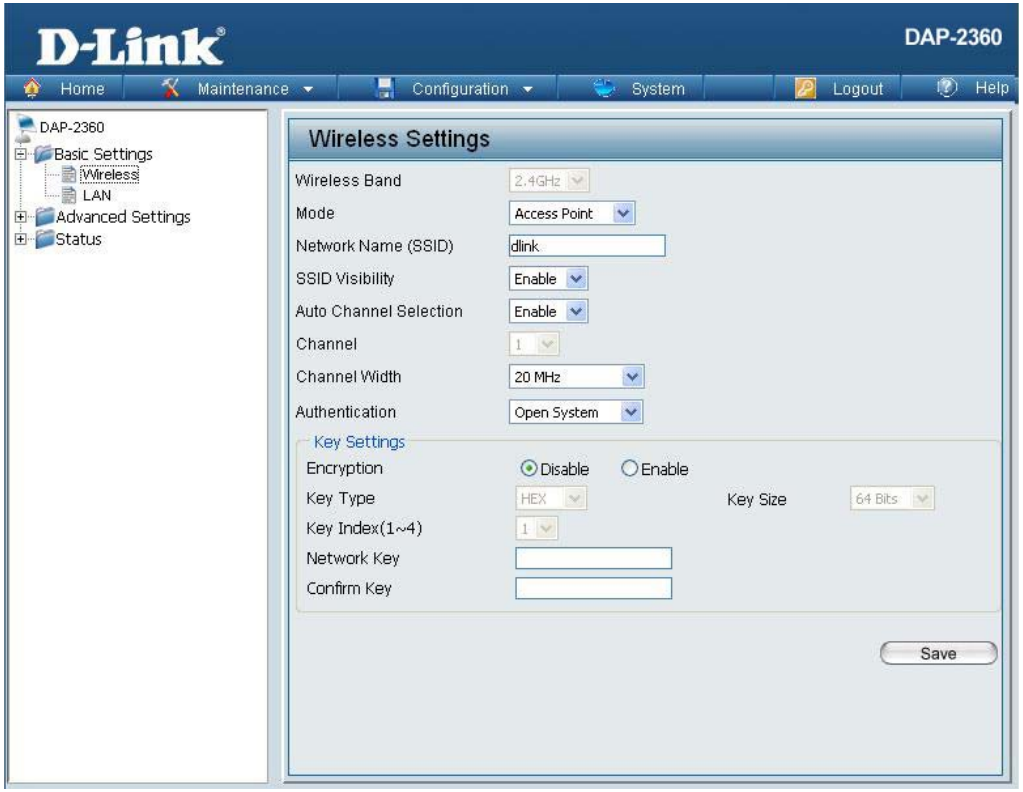
When making changes on most of the configuration screens in this section, use the **Apply** button at the bottom of each screen to save your configuration changes.

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

Home > Basic Settings

Wireless

Access Point mode



Wireless Band: **2.4 GHz**

Mode: Select **Access Point** from the pull-down menu. The other three choices are **WDS with AP**, **WDS**, and **Wireless Client**.

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

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

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 pull-down menu to make the desired selection.

Note: *The wireless adapters will automatically scan and match the wireless settings.*

Channel Width: Allows you to select the channel width you would like to operate in. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** allows you to connect to both 802.11n and 802.11b/g wireless devices on your network.

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

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.

WDS with AP mode

In WDS with AP mode, the DAP-2360 wirelessly connects multiple networks while still functioning as a wireless AP.

Wireless Band: **2.4GHz**.

Mode: **WDS with AP** mode is selected from the pull-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 with AP mode. The channel selection process only occurs when the AP is booting up.

Channel: All devices on the network must share the same channel. To change the channel, use the pull-down menu to make the desired selection. (Note: The wireless adapters will automatically scan and match the wireless settings.)

Channel Width: Allows you to select the channel width you would like to operate in. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** allows you to connect to both 802.11n and 802.11b/g wireless devices on your network.

Remote AP MAC Address:	Enter the MAC addresses of the APs on your network that will serve as bridges to wirelessly connect multiple networks.
Site Survey:	Click on the **Scan** button to search for available wireless networks, then click on the available network that you want to connect with.
Authentication:	Use the pull-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.

WDS mode

In WDS mode, the DAP-2360 wirelessly connects multiple networks, without functioning as a wireless AP.

Wireless Band: **2.4GHz**.

Mode: **WDS** is selected from the pull-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 pull-down menu to make the desired selection**.**

Channel Width: Use the pull-down menu to choose **20 MHz** or **Auto 20/40 MHz**.

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

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

Authentication: Use the pull-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

Wireless Band: **2.4 GHz**

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

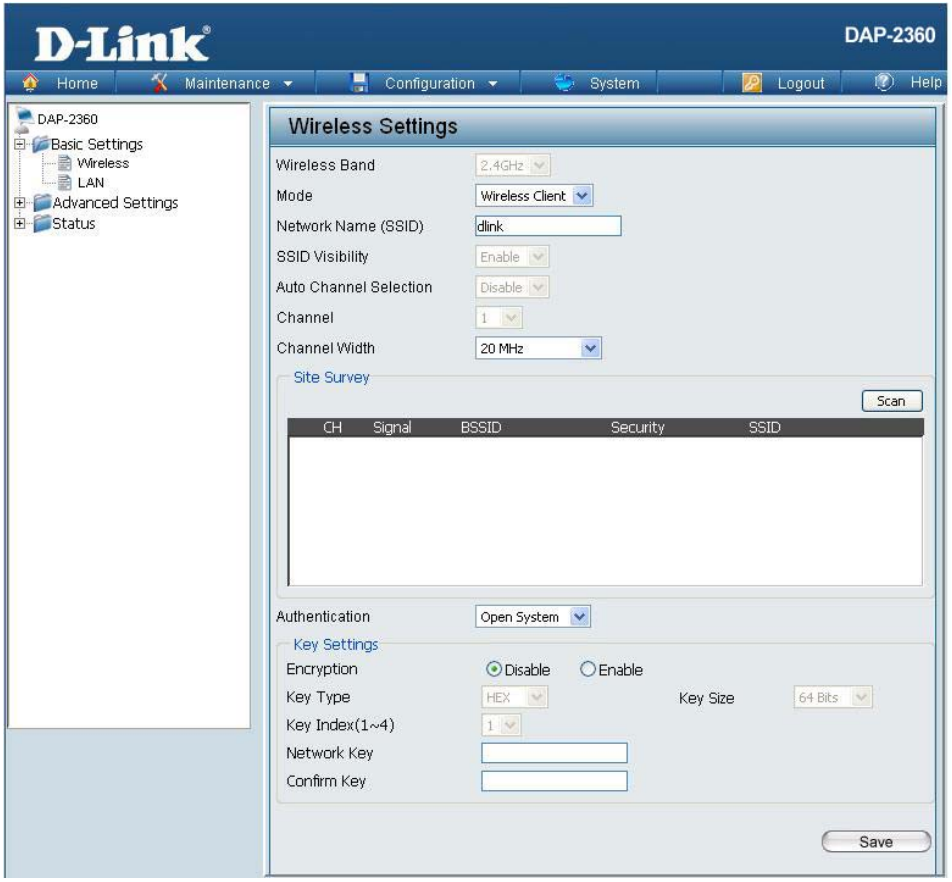
Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network.

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 matches the AP that the DAP-2360 is connected to when set to **Wireless Client** mode.

Channel Width: Use the pull-down menu to choose **20 MHz** or **Auto 20/40 MHz**.



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

Authentication: Use the pull-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.

Open System/Shared Key Authentication

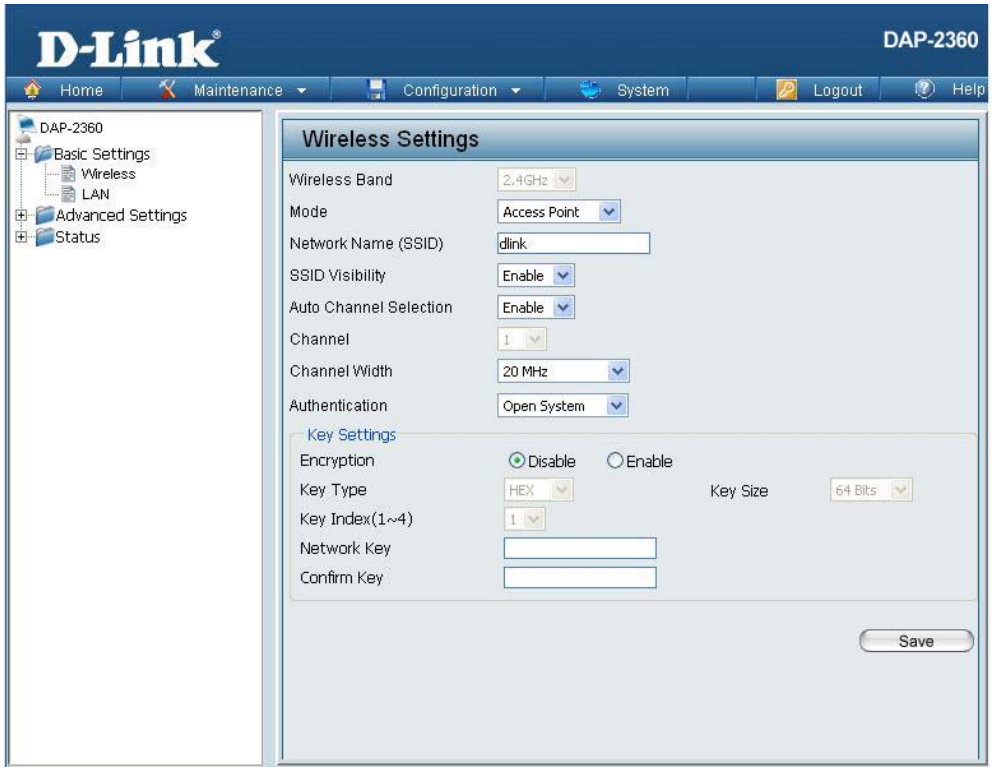
Encryption: Use the radio button to disable or enable encryption.

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

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

Key Index (1-4): Select the 1st through the 4th key to be the active key.

Key: Input up to four keys for encryption. You will select one of these keys in the Key Index pull-down menu.



***Hexadecimal (HEX) digits consist of the numbers 0-9 and the letters A-F.*

**ASCII (American Standard Code for Information Interchange) is a code that represents English letters using numbers ranging from 0-127.*

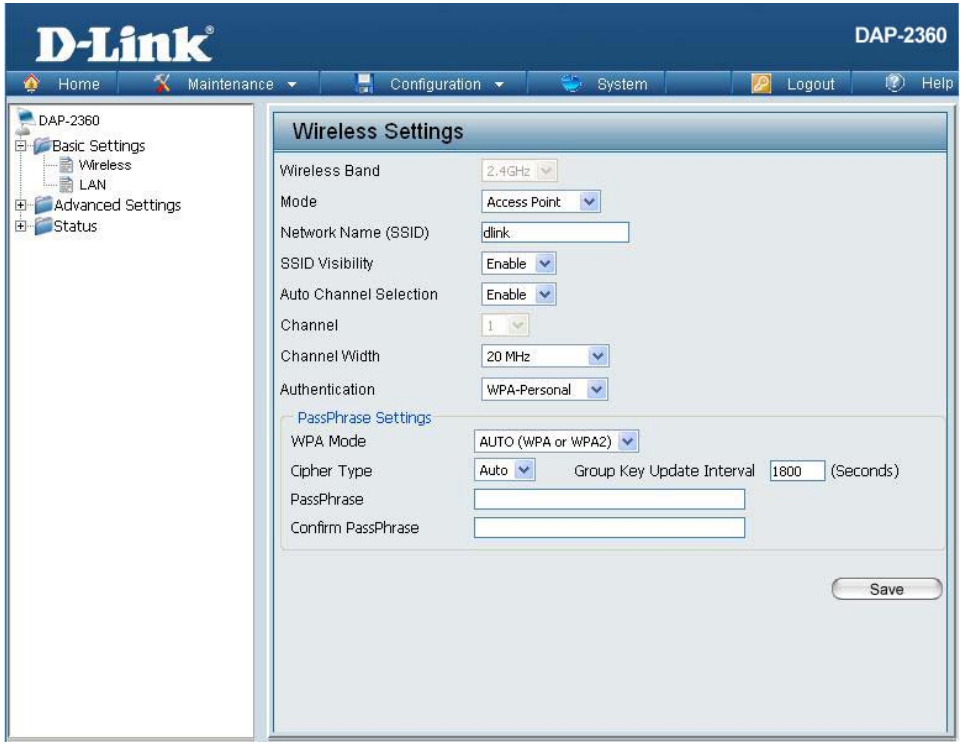
WPA-Personal authentication

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

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

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

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



WPA-Enterprise authentication

WPA Mode: When **WPA-Enterprise** is selected, you must also select a WPA mode from the pull-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 pull-down menu: **Auto**, **AES**, or **TKIP**.

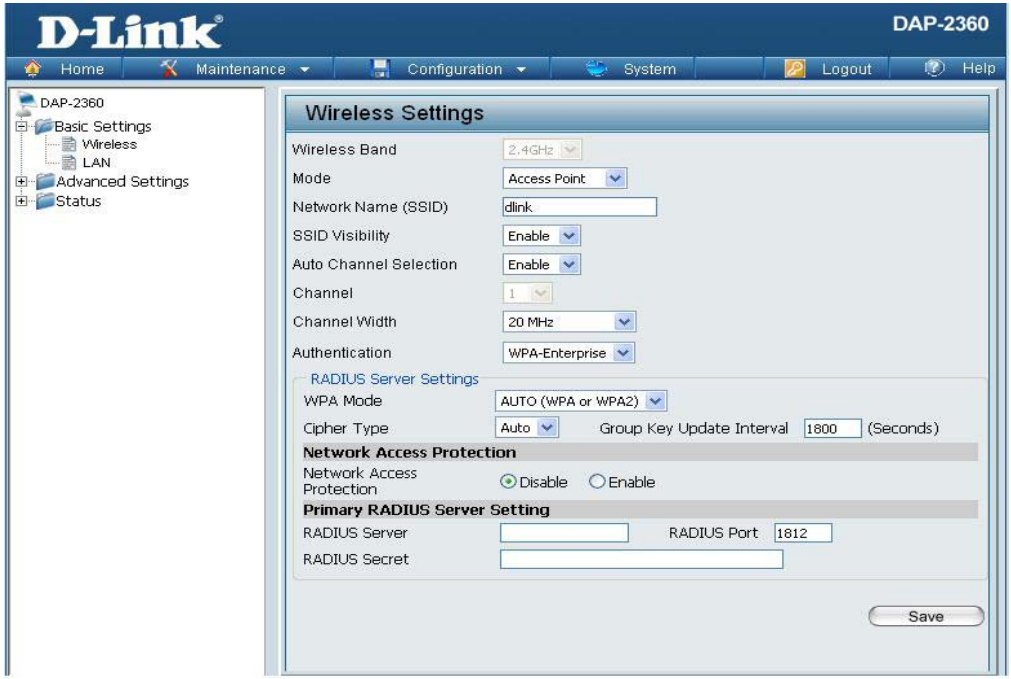
Group Key Update Interval: Select the interval during which the group key will be valid. **1800** is the recommended value as a lower interval may reduce data transfer rates.

Network Access Protection: Enable or disable Microsoft Network Access Protection.

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

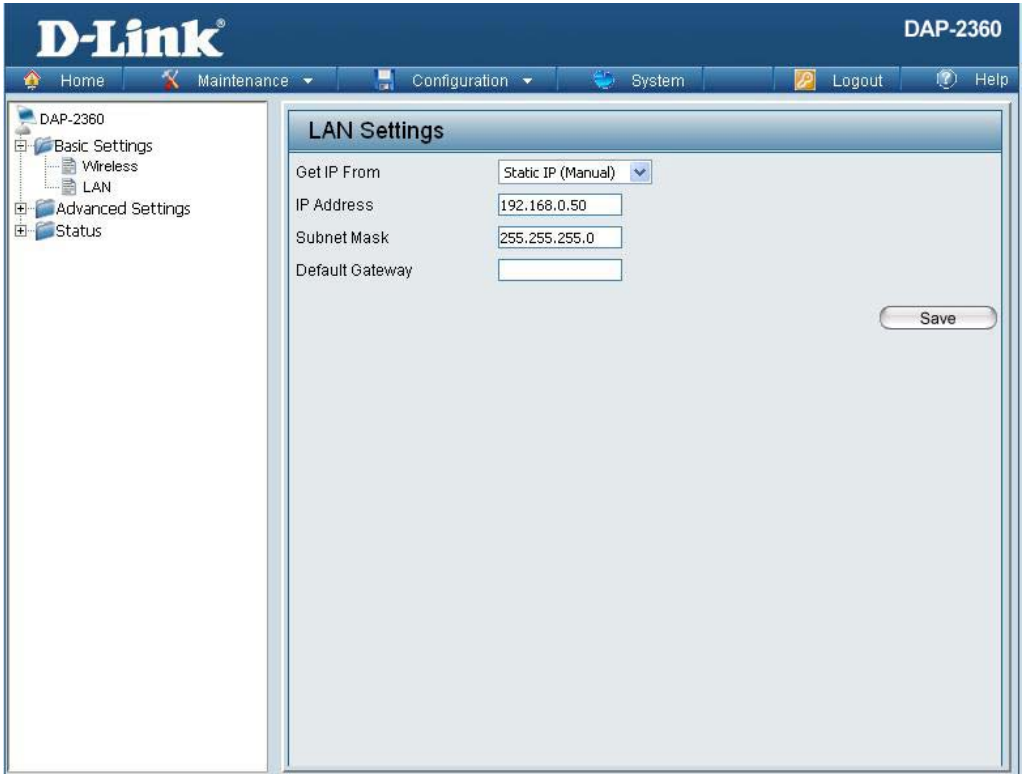
RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the RADIUS secret.



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-2360. These settings may be referred to as private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.



Get IP From: **Static IP (Manual)** is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2360. 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 gateway in your network, please enter an IP address within the range of your network.

Home > Advanced Settings
Performance

Wireless: Use the pull-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. Please note that when backwards compatibility is enabled for legacy (802.11 g/b) clients, degradation of 802.11n (draft) wireless performance is expected.

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

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

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

DTM Interval (1-15): Select a Delivery Traffic Indication Message setting between **1** and **15**. **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 pull-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, 64~200) : To effectively optimize throughput over long distance links enter a value for Acknowledgement Time Out between **64** to **200** microseconds in the 2.4 GHz in the field provided.

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

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

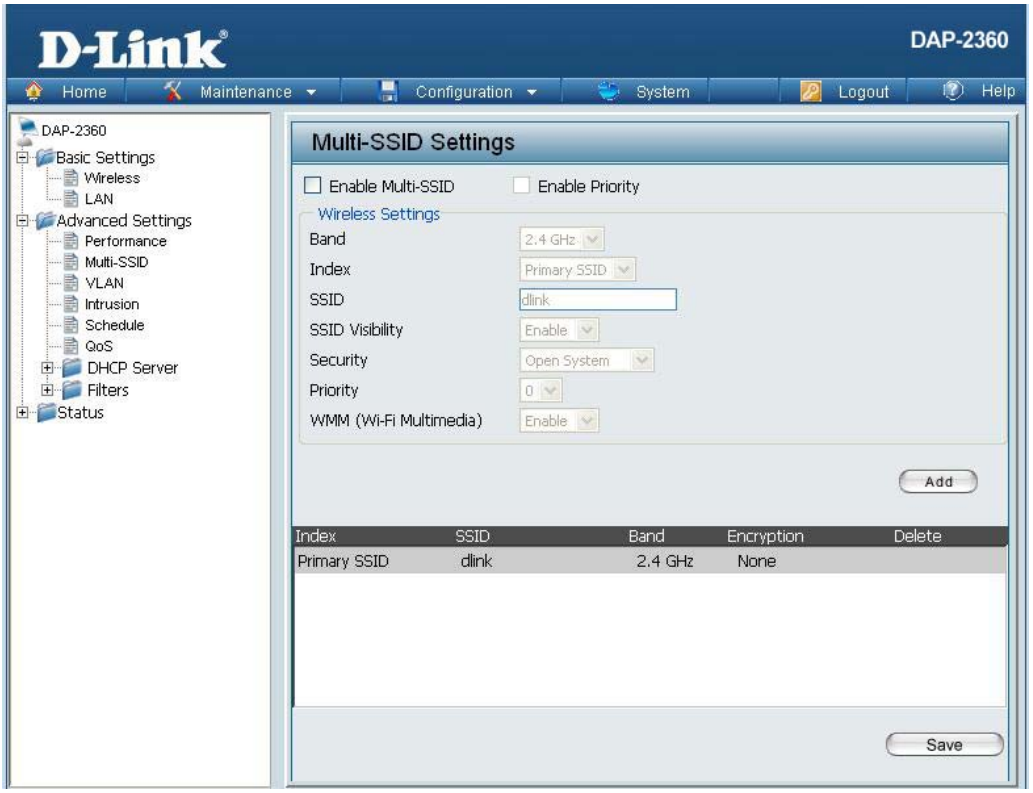
Link Integrity: Select **Enable** or **Disable**. If the Ethernet connection between the LAN and the AP is disconnected, enabling this feature will cause the wireless segment associated with the AP to be disassociated from the AP.

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, when the number of users exceeds this value, the DAP-2360 will not allow clients to associate with the AP.

User Limit (0-64): Set the maximum amount of users that are allowed access (**0-64** users). To use this feature, the Connection Limit above must be enabled. For most users, a limit of **10** is recommended. The default setting is **20**.

Multi-SSID

The device supports up to four 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.



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

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

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

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

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

Security: The Multi-SSID security can be **Open System**, **WPA-Personal**, or **WPA-Enterprise**. 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.

WMM (Wi-Fi Multimedia):	Select **Enable** or **Disable**.
Encryption:	When you select **Open System**, toggle between **Enable** and **Disable**. If **Enable** is selected, the Key Type, Key Size, Key Index (1~4), Key, and Confirm Keys must also be configured.
Key Type:	Select **HEX** or **ASCII**.
Key Size:	Select **64 Bits** or **128 Bits**.
Key Index (1-4):	Select from the 1st to 4th key to be set as the active key.
Key:	Input up to four keys for encryption. You will select one of these keys in the Key Index pull-down menu.
WPA Mode:	When you select either **WPA-Personal** or **WPA-Enterprise**, you must also choose a WPA mode from the pull-down menu: **AUTO (WPA or WPA2)**, **WPA2 Only**, or **WPA Only**. WPA and WPA2 use different algorithms. **AUTO (WPA or WPA2)** allows you to use both WPA and WPA2. In addition, you must configure Cipher Type, and Group Key Update Interval.
Cipher Type:	Select **Auto, AES,** or **TKIP** from the pull-down menu.
Group Key Update Interval:	Select the interval during which the group key will be valid. The default value of **1800** seconds is recommended.
PassPhrase:	When you select **WPA-Personal**, please enter a PassPhrase in the corresponding field.
Confirm PassPhrase:	When you select **WPA-Personal**, please re-enter the PassPhrase entered in the previous item in the corresponding field.
RADIUS Server:	When you select **WPA-Enterprise**, enter the IP address of the RADIUS server. In addition, you must configure RADIUS Port and RADIUS Secret.
RADIUS Port:	Enter the RADIUS port.
RADIUS Secret:	Enter the RADIUS secret.

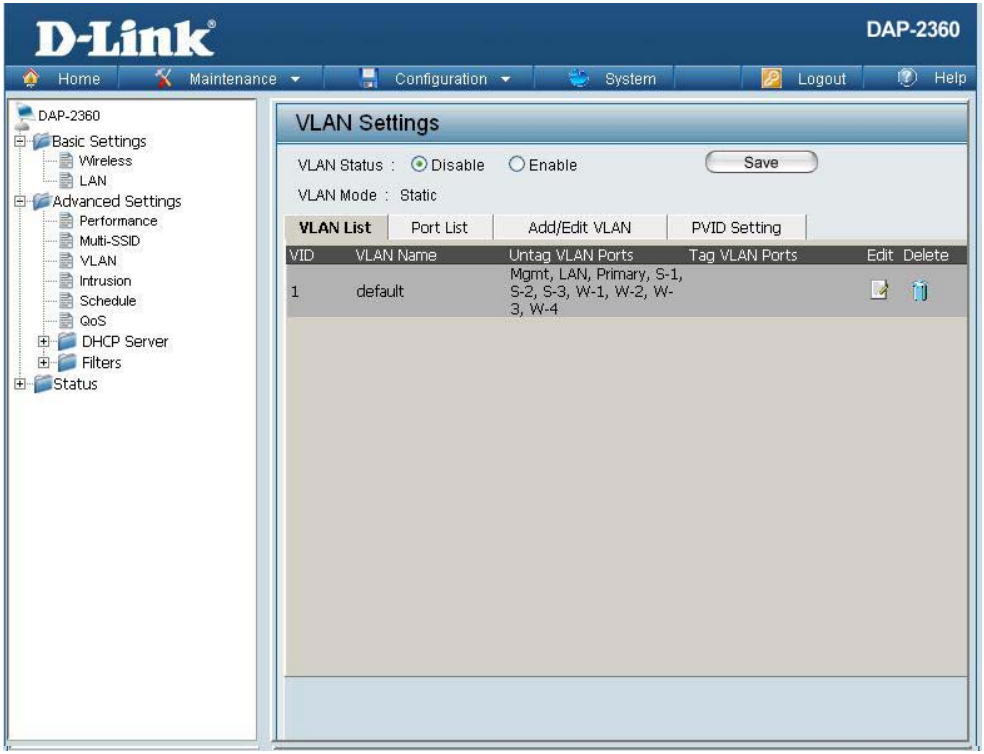
VLAN

VLAN List

The DAP-2360 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-2360 without a VLAN tag will have a VLAN tag inserted with a PVID.

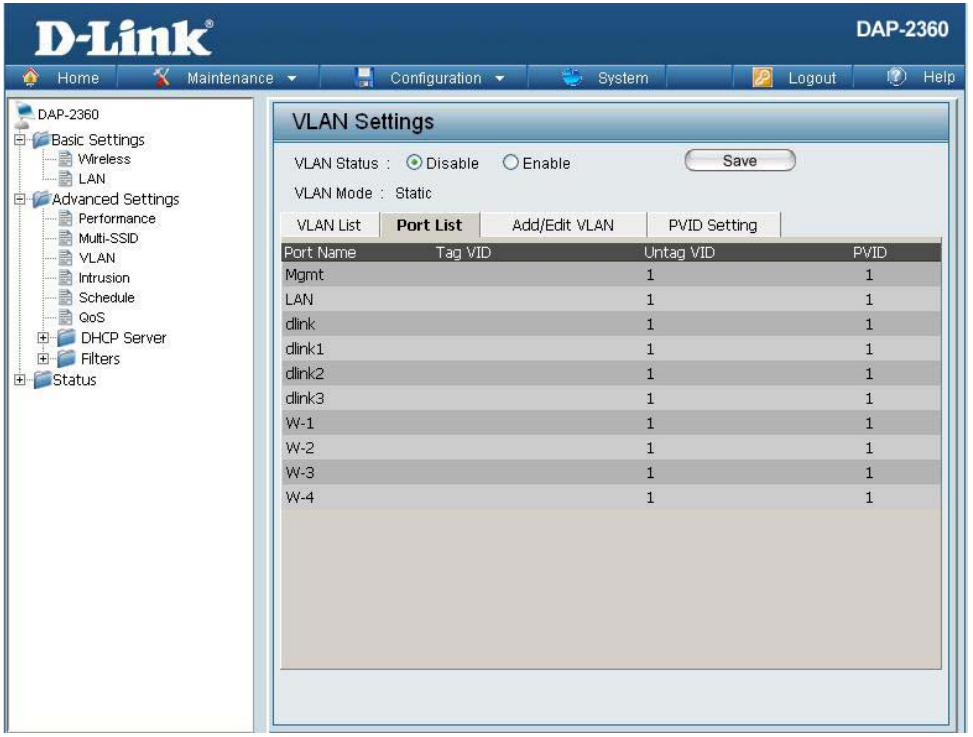
The VLAN List tab displays the current VLANs.

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



Port List

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



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

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

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

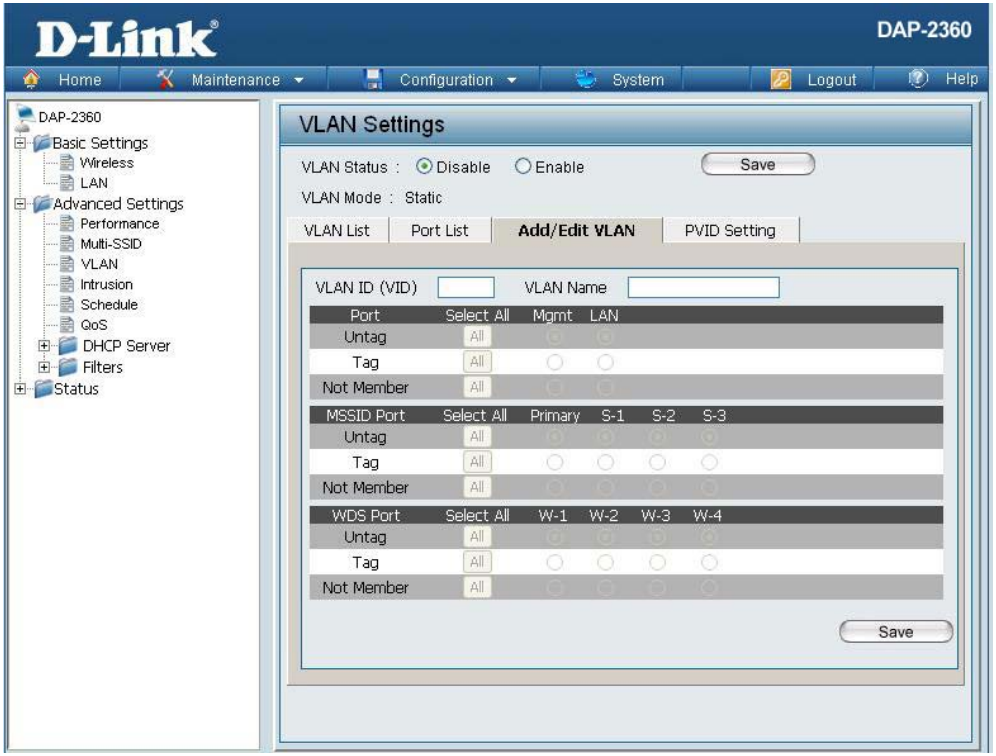
Untag VID: The Untagged VID is displayed in this column.

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

Add/Edit VLAN

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

VLAN Status:	Use the radio button to toggle to Enable.
VLAN ID:	Provide a number between **1** and **4094** for the Internal VLAN.
VLAN Name:	Enter the VLAN to add or modify.

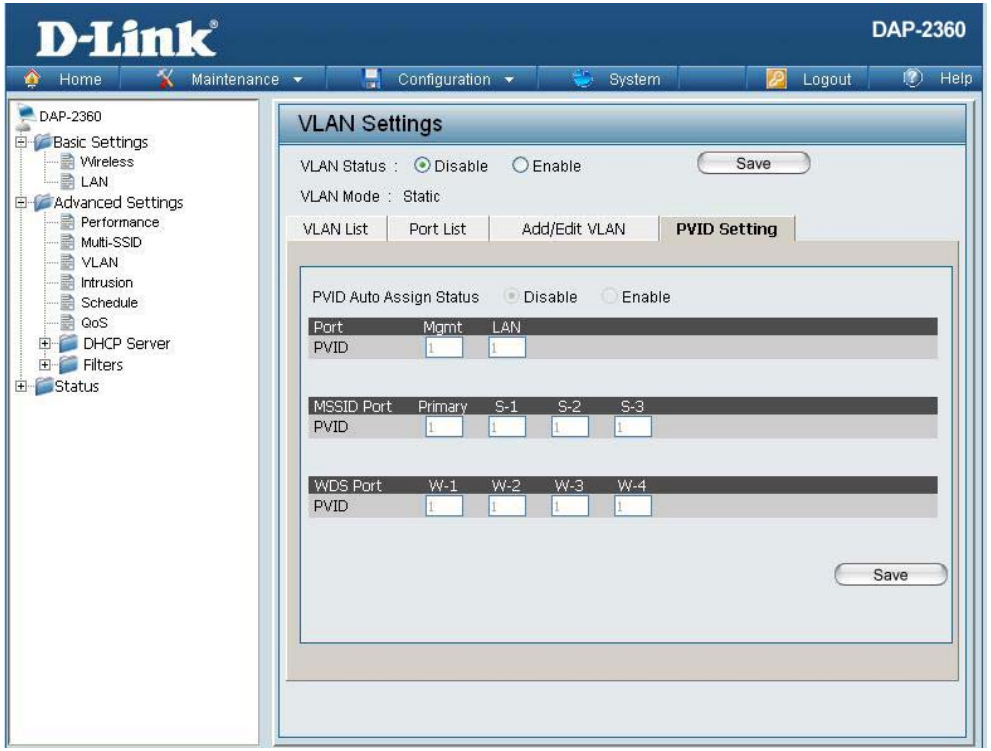


PVID Setting

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. Click the **Apply** button to let your changes take effect.

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

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

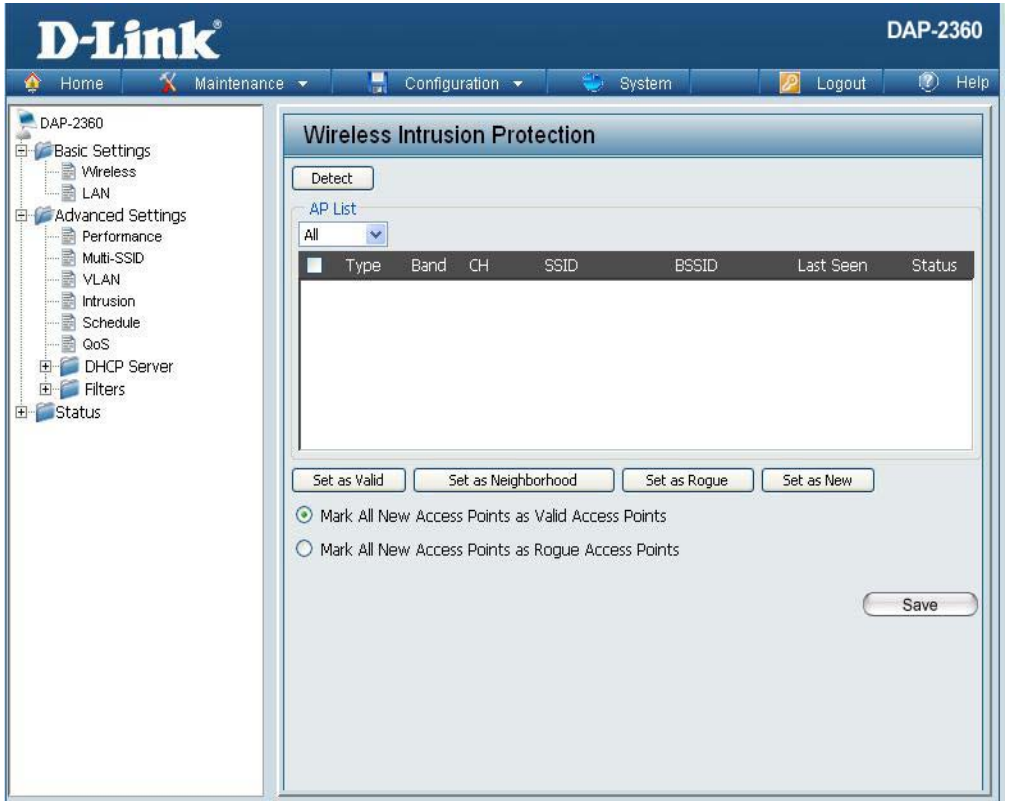


Intrusion

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

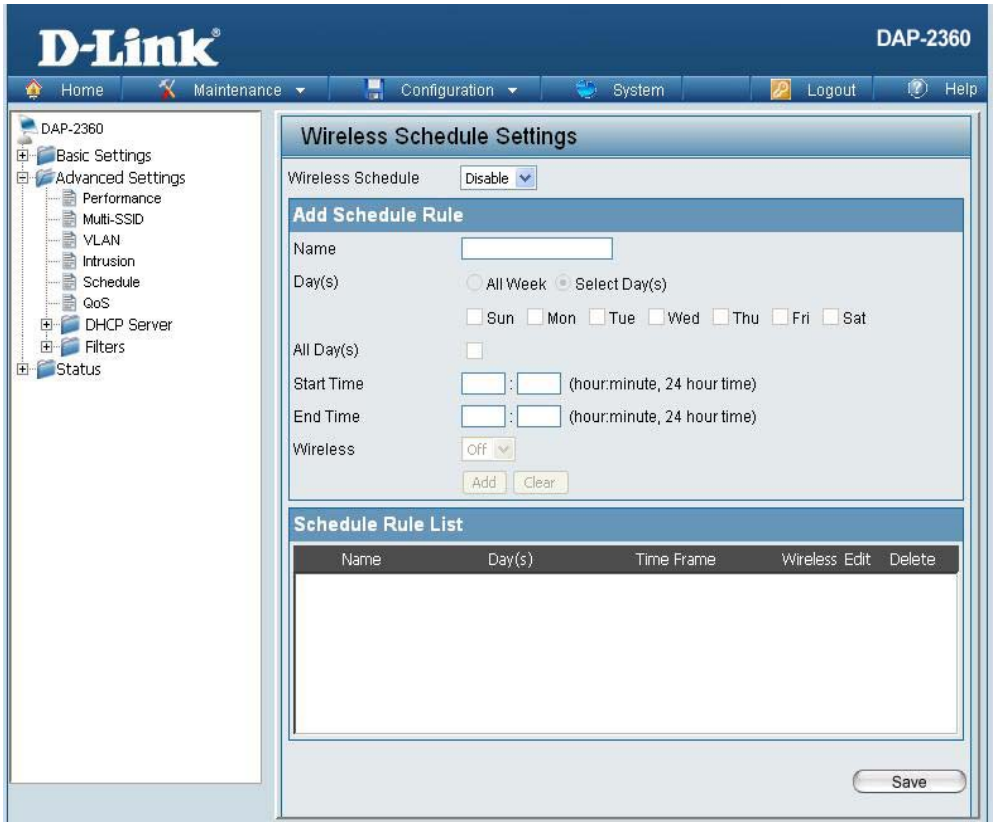
AP List: The choices include **All**, **Valid**, **Neighbor**, **Rogue**, and **New**.

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



Schedule

The Wireless Schedule Settings window is used to add and modify scheduling rules on the device. Click the **Apply** button to let your changes take effect.



Wireless Schedule: Use the pull-down menu to enable the device's scheduling feature.

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

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

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

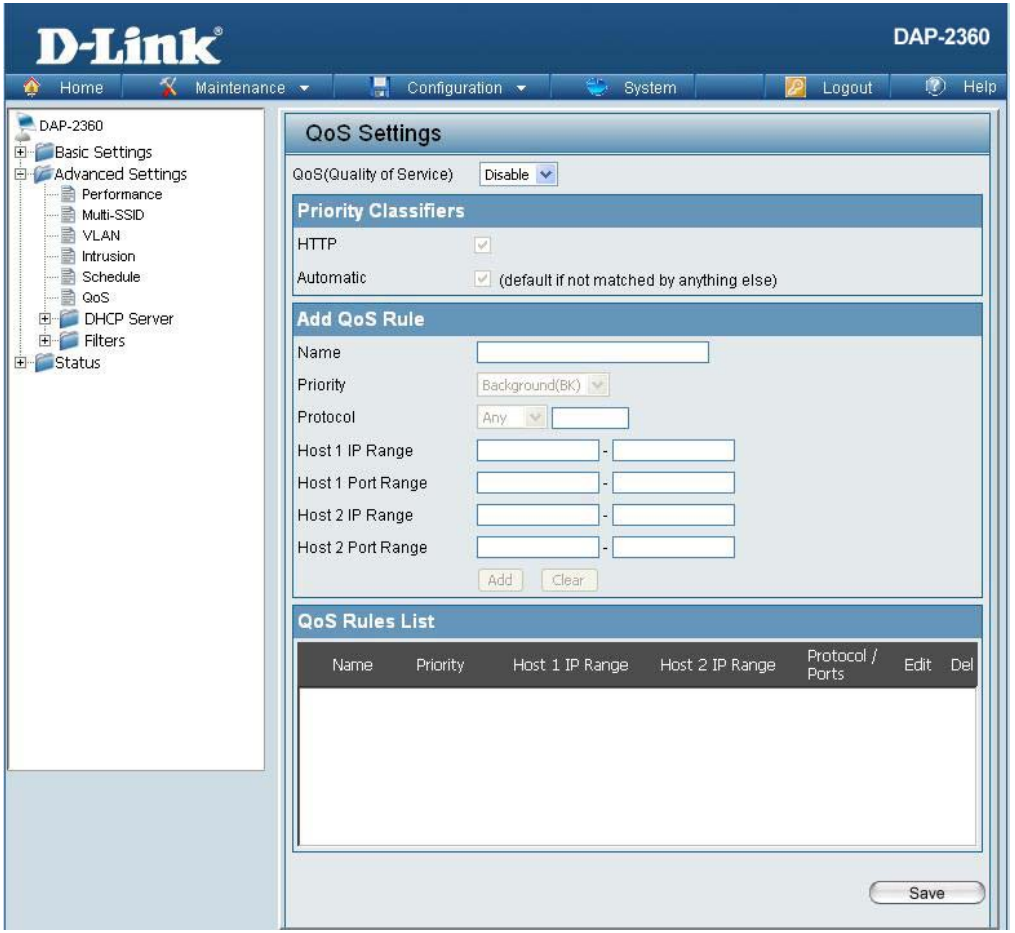
Wireless: Toggle the pull-down menu between **Off** and **On**.

QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications.

A QoS Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific QoS Rules are not required.

QoS supports overlaps between rules. If more than one rule matches a specific message flow, the rule with the highest priority will be used.



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

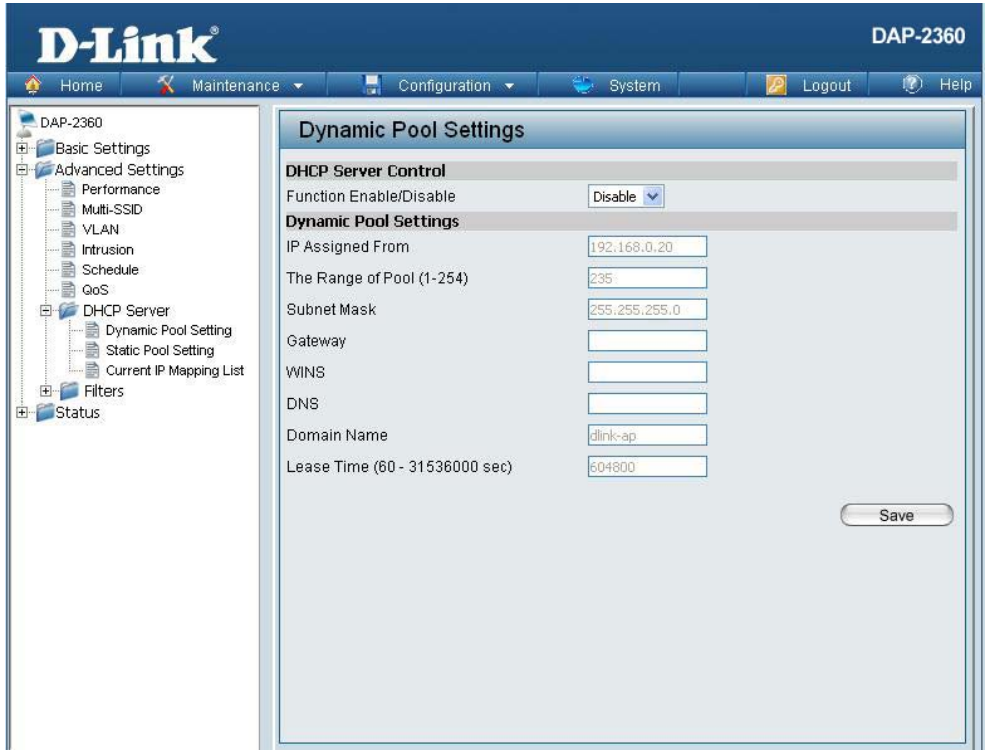
HTTP: Allows the access point to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

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

Name:	Enter a name for the new QoS rule in the field provided.
Priority:	Use the pull-down menu to select the desired priority: **Background (BK)**, **Best Effort (BE)**, **Video (VI)**, or **Voice (VO)**.
Protocol:	Use the pull-down menu to choose the appropriate protocol used by the messages: **Any**, **TCP**, **UDP**, **Both**, **IMCP**, or **Other**.
Host 1 IP Range:	The rule applies to a flow of messages for which one computer's IP address falls within the range set here.
Host 1 Port Range:	The rule applies to a flow of messages for which host 1's port number is within the range set here when the Protocol is set to **TCP**, **UDP**, or **Both**.
Host 2 IP Range:	The rule applies to a flow of messages for which the other computer's IP address falls within the range set here.
Host 2 Port Range:	The rule applies to a flow of messages for which host 2's port number is within the range set here when the Protocol is set to **TCP**, **UDP**, or **Both**.

DHCP Server
Dynamic Pool Settings

The DHCP address pool defines the range of the IP address that can be assigned to stations in the network. A Dynamic Pool allows wireless stations to receive an available IP with lease time control. If needed or required in the network, the DAP-2360 is capable of acting as a DHCP server.



Function Enable/ Disable: Dynamic Host Configuration Protocol (DHCP) assigns dynamic IP addresses to devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses. Select **Enable** to allow the DAP-2360 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.

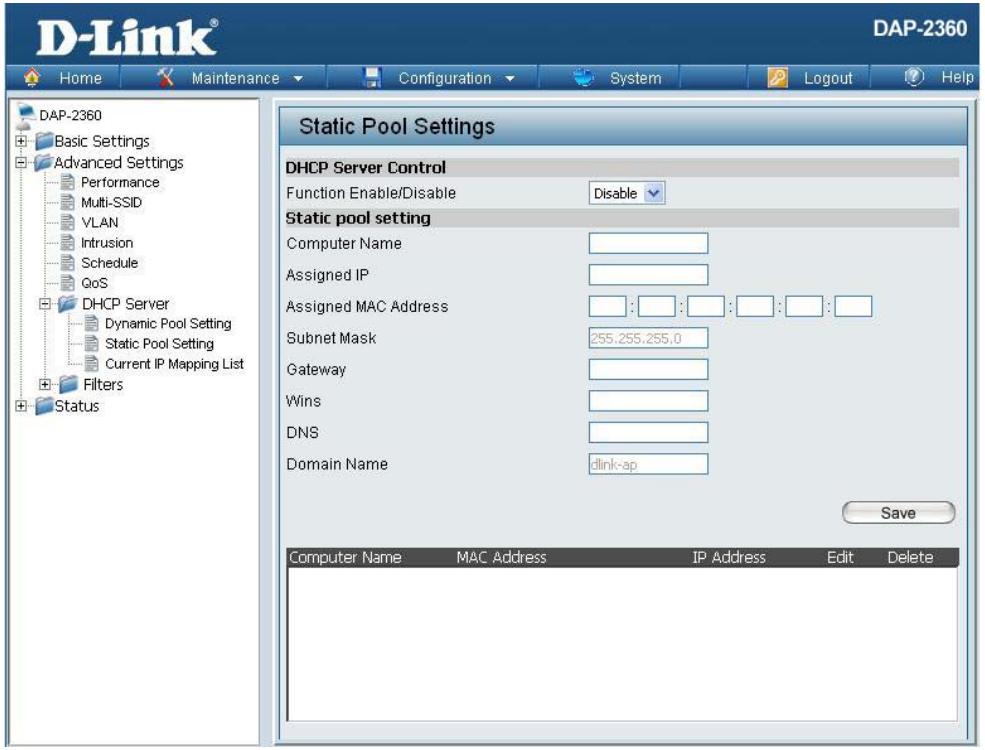
Gateway: Enter the IP address of the gateway on the network.

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

Static Pool Setting

The DHCP address pool defines the range of IP addresses that can be assigned to stations on the network. A static pool allows specific wireless stations to receive a fixed IP without time control.



Function Enable/ Disable: Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to wireless devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign IP addresses. Select **Enable** to allow the DAP-2360 to function as a DHCP server.

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

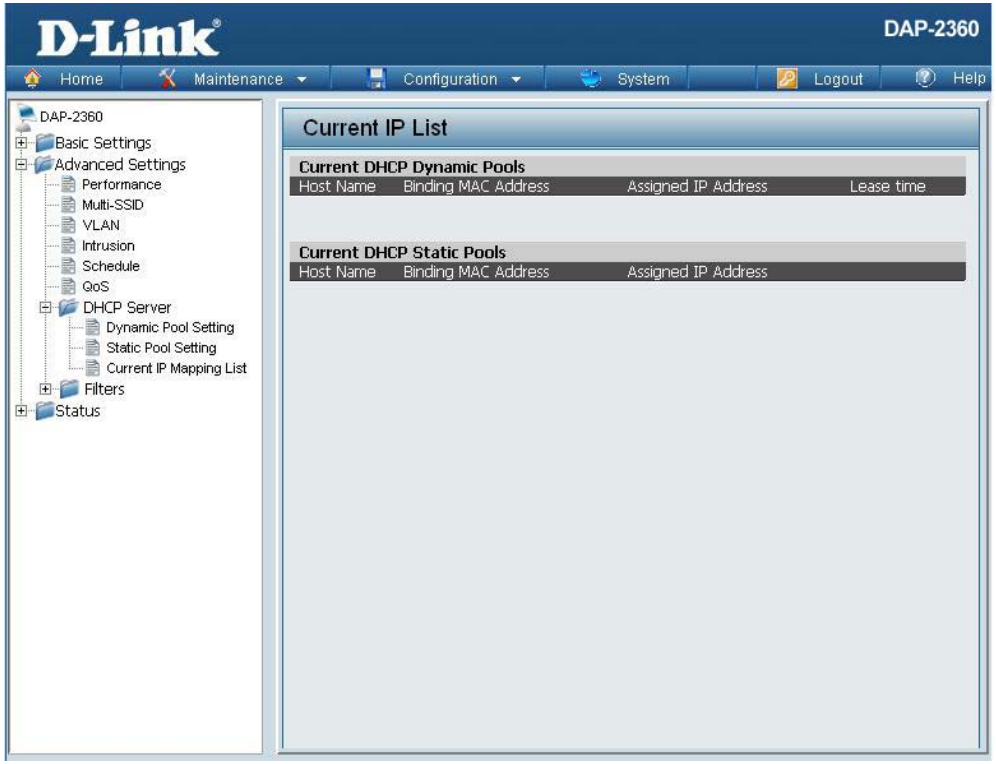
Assigned MAC Address: Enter the MAC address of the device requesting association here.

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

Gateway:	Specify the Gateway address for the wireless network.
WINS:	Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.
DNS:	Enter the Domain Name System (DNS) server address for the wireless network. The DNS server translates domain names such as www.dlink.com into IP addresses.
Domain Name:	Specify the domain name for the network.

Current IP Mapping List

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



Current DHCP Dynamic Profile: 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.

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

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

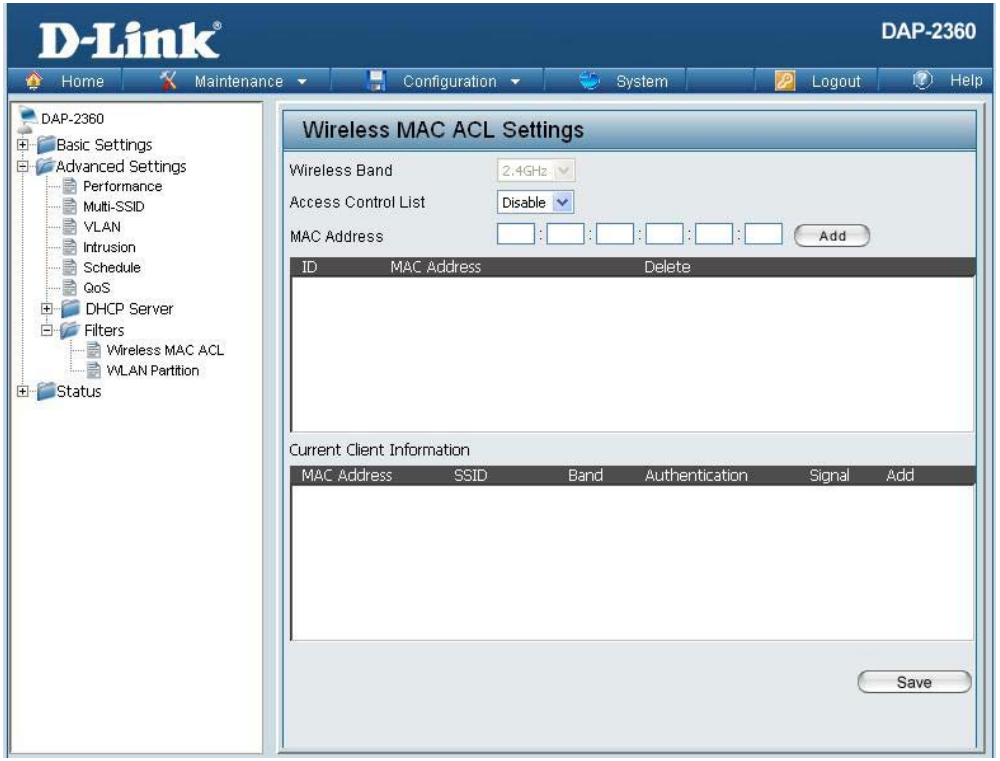
Filters
Wireless MAC ACL

Wireless Band: Displays the current wireless band rate.

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

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

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

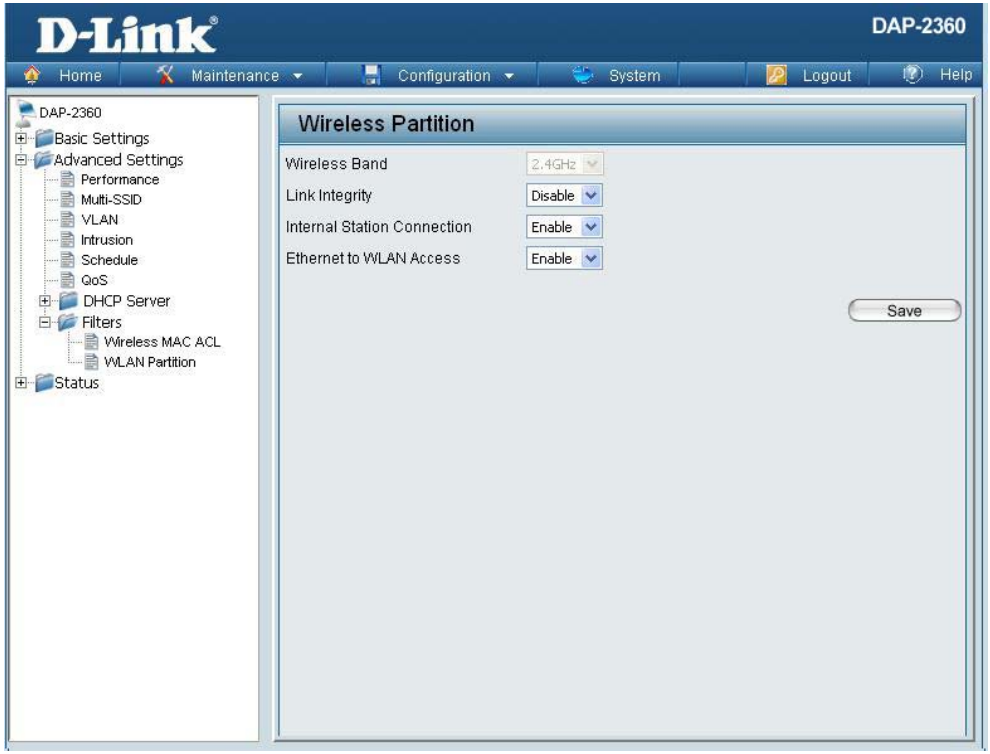


WLAN Partition

Wireless Band: Displays the current wireless band rate.

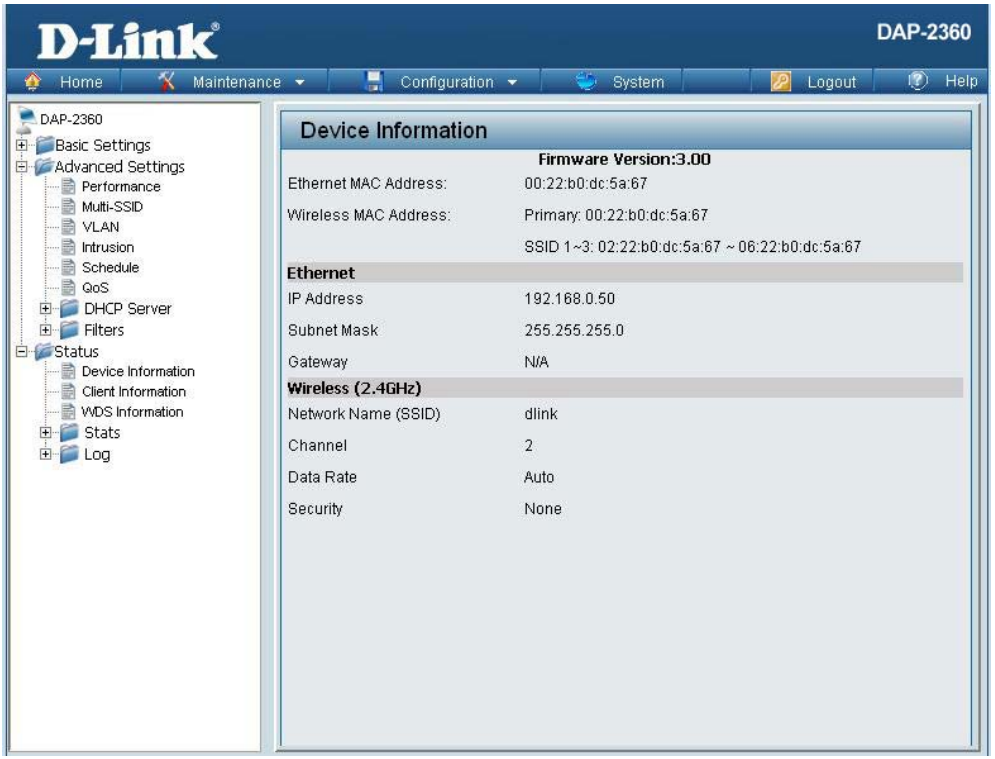
Internal Station Connection: The default value is **Enable**, which allows stations to inter-communicate by connecting to a target AP. When disabled, wireless stations cannot exchange data through the AP.

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



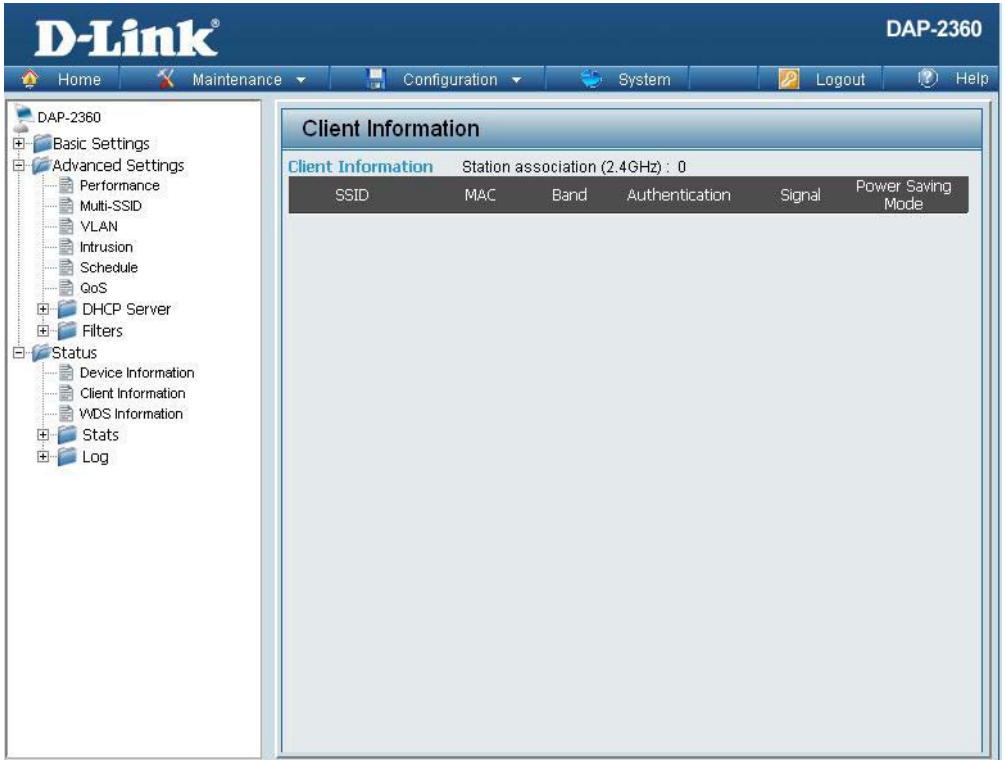
Home > Status
Device Information

Device Information: This read-only window displays the configuration settings of the DAP-2360, 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-2360.



The following information is available for each client communicating with the DAP-2360.

SSID: Displays the SSID of the client.

MAC: Displays the MAC address of the client.

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

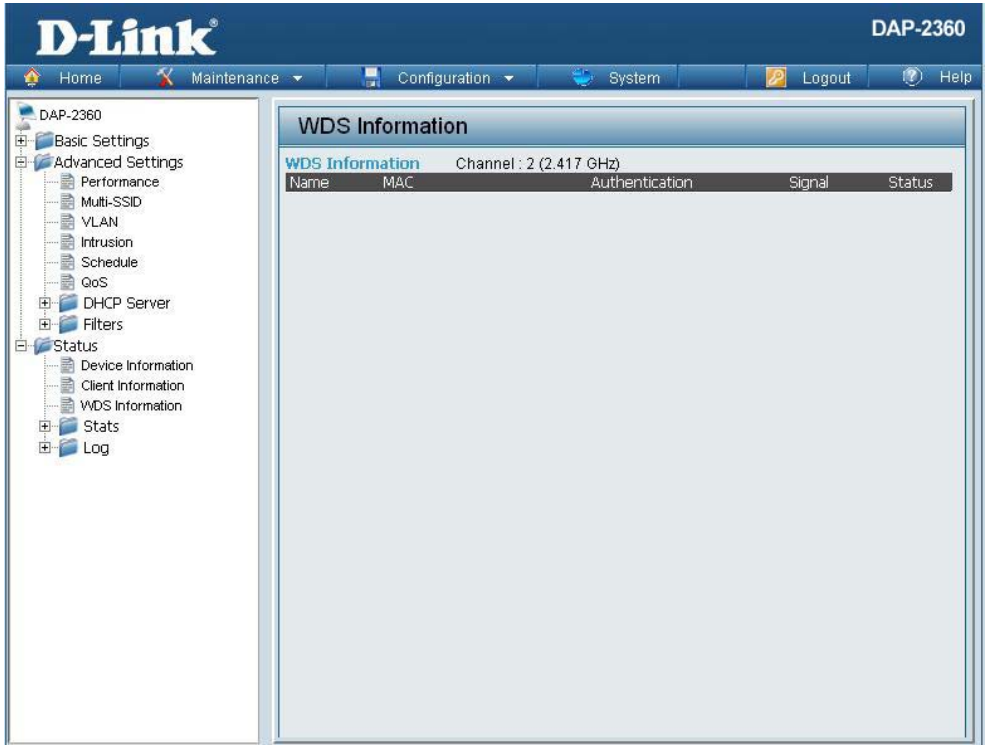
Authentication: Displays the type of authentication being used.

Signal: Displays the client's signal strength.

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

WDS Information

WDS Information: This window displays the Wireless Distribution System information for clients currently connected to the DAP-2360.



The following information is available for each client communicating with the DAP-2360.

Name: Displays the SSID of the client.

MAC: Displays the MAC address of the client.

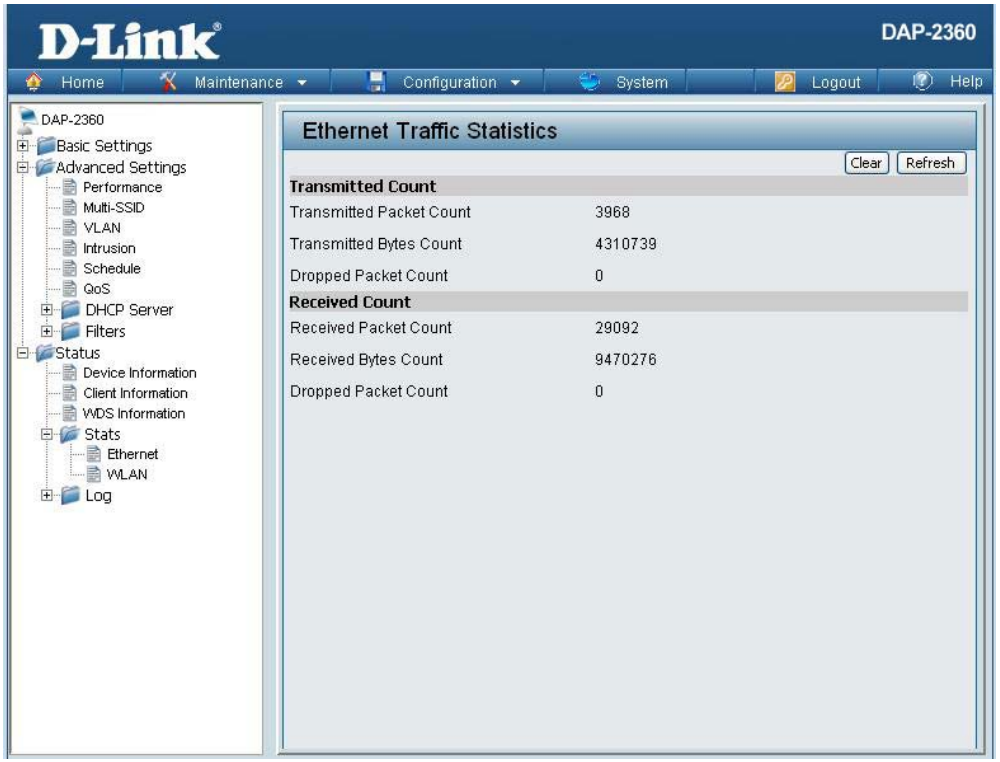
Authentication: Displays the type of authentication being used.

Signal: Displays the client's signal strength.

Status: Displays the status of the power saving feature.

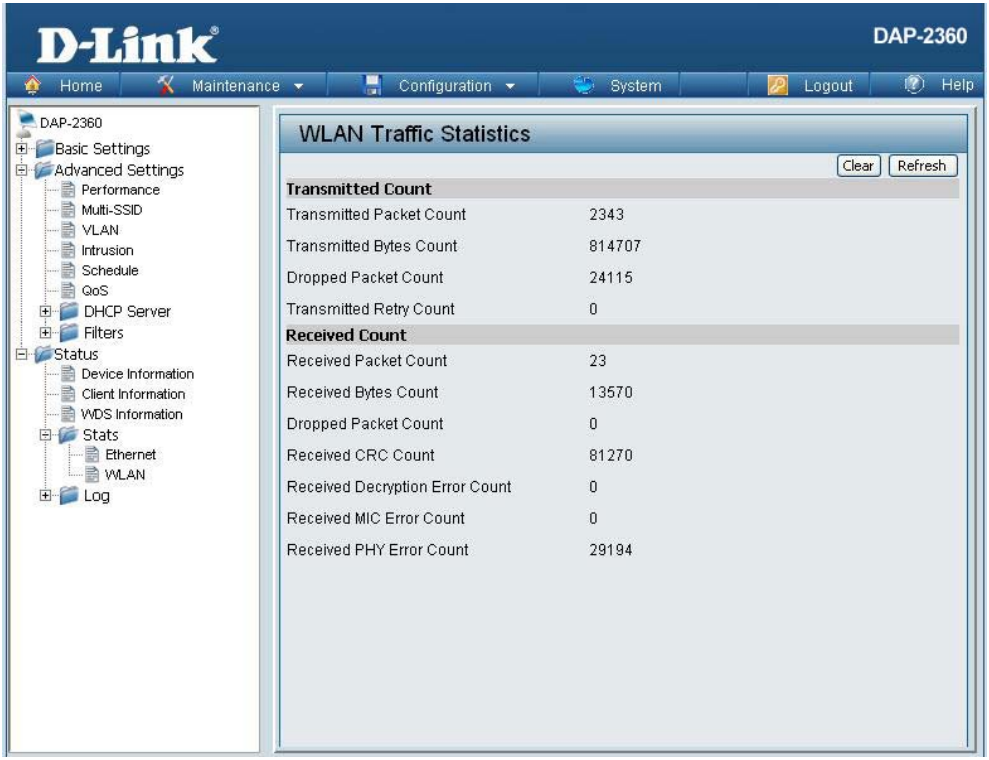
Stats
Ethernet

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



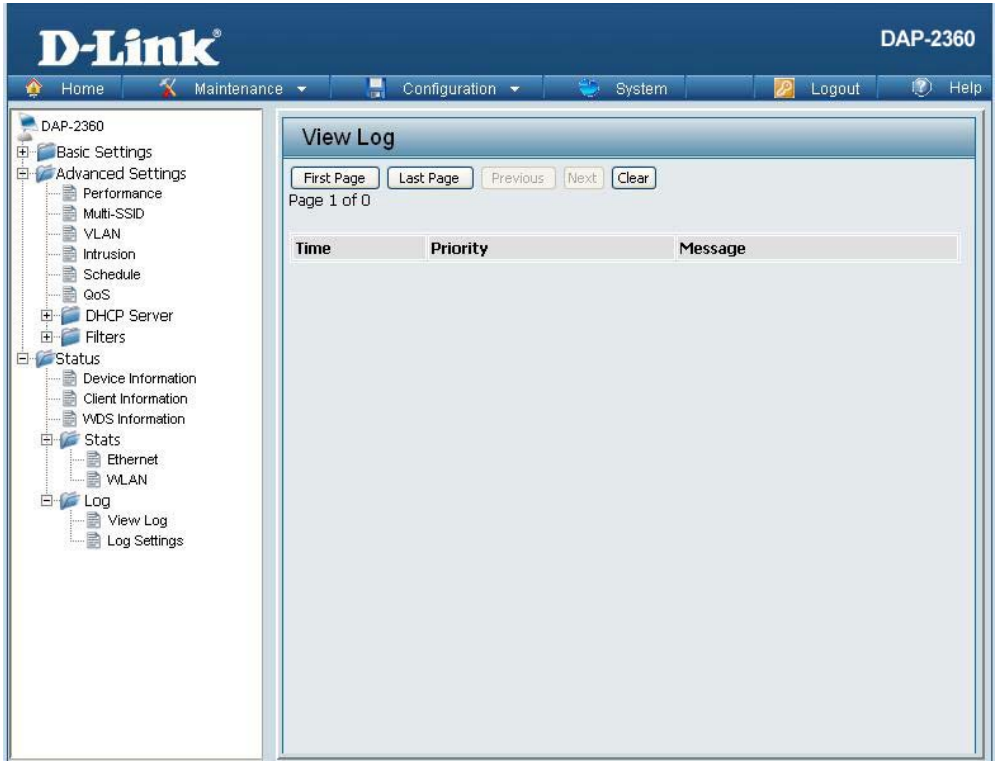
WLAN

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



Log
View Log

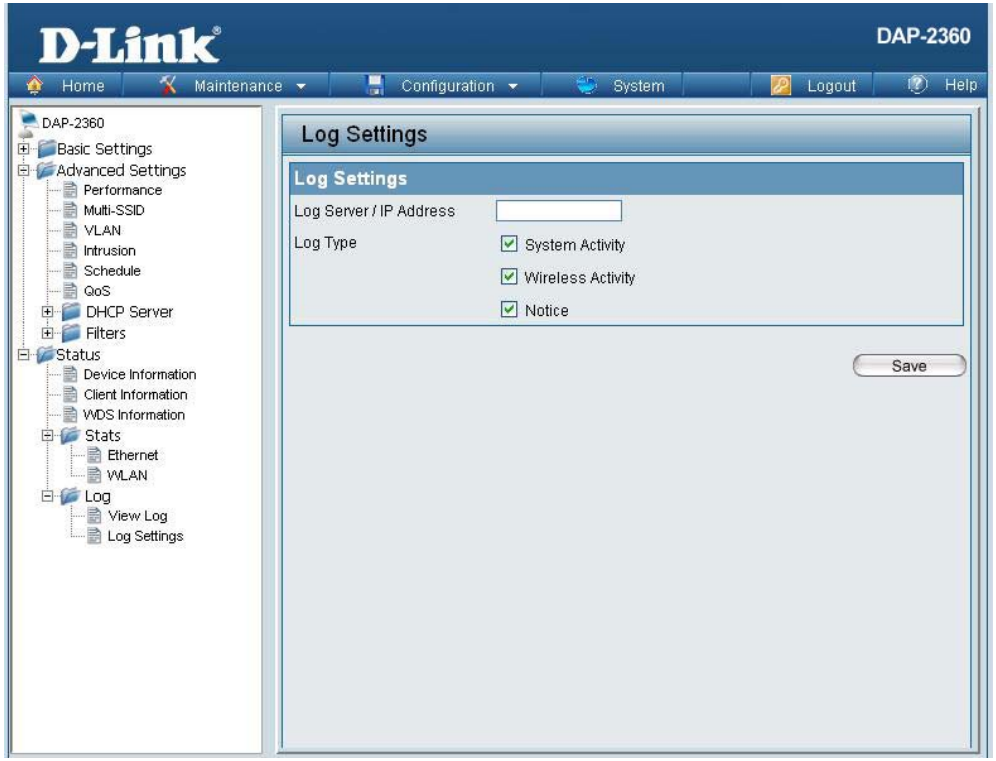
View Log: The AP's embedded memory displays system and network messages including a time stamp and message type. The log information includes but is not limited to the following items: cold start AP, upgrading firmware, client associate and disassociate with AP, and web login. The web page holds up to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



Log Settings

Log Server/IP Address: Enter the IP address of the server you would like to send the DAP-2360 log to.

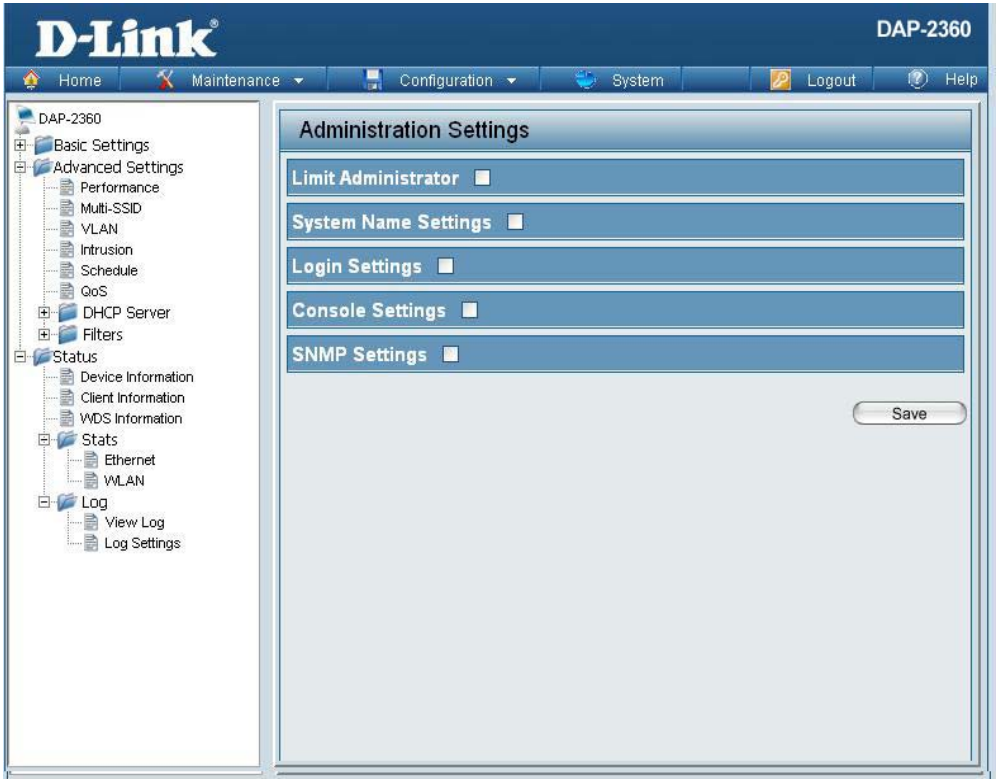
Log Type: Check the box for the type of activity you want to log. There are three types: System Activity, Wireless Activity, and Notice.



Maintenance

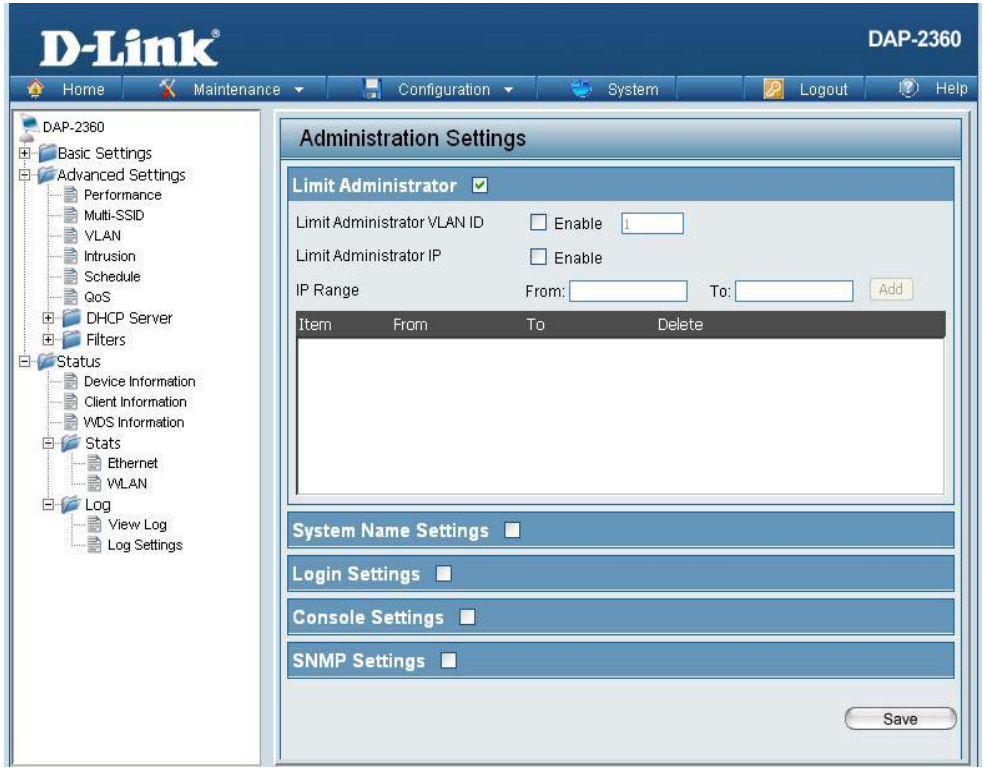
Administrator Settings

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



Limit Administrator

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



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

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

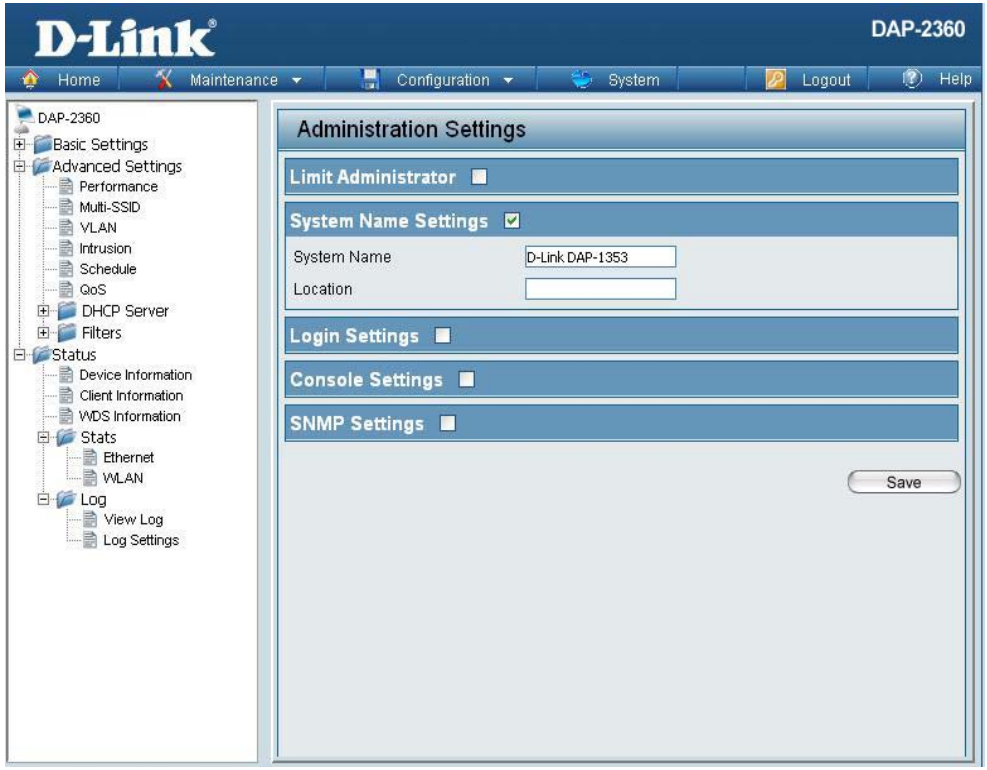
IP Range: Enter the IP address range that the administrator will be allowed to log in from and then click the Add button.

System Name Settings

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

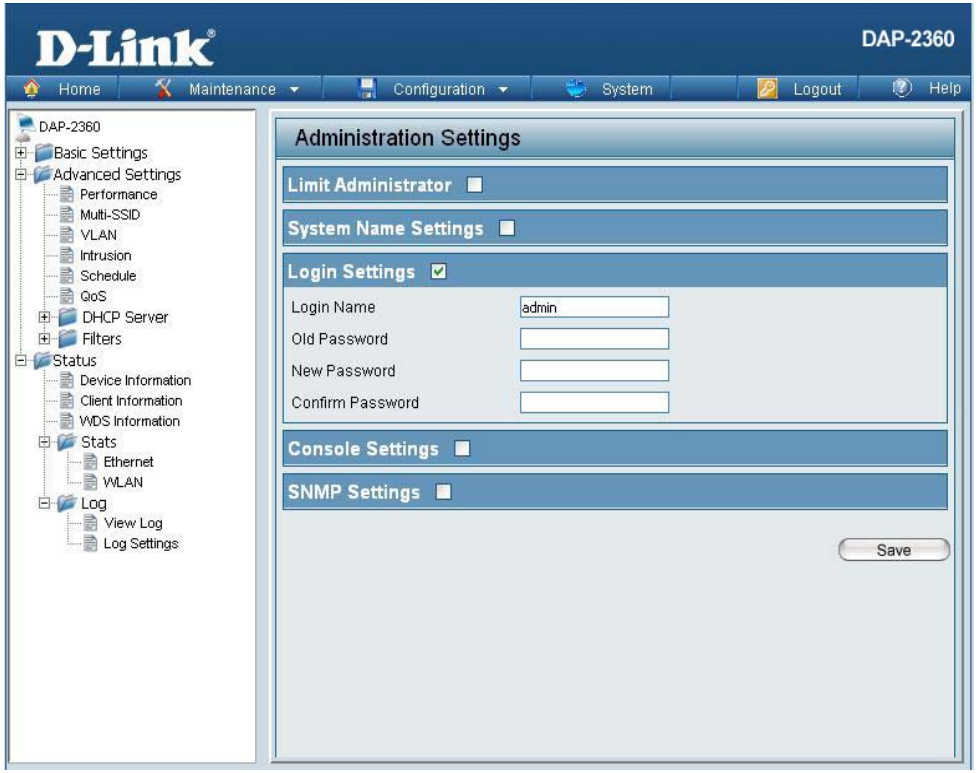
System Name: The name of the device. The default name is **D-Link DAP-2360**.

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



Login Settings

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



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

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

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

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

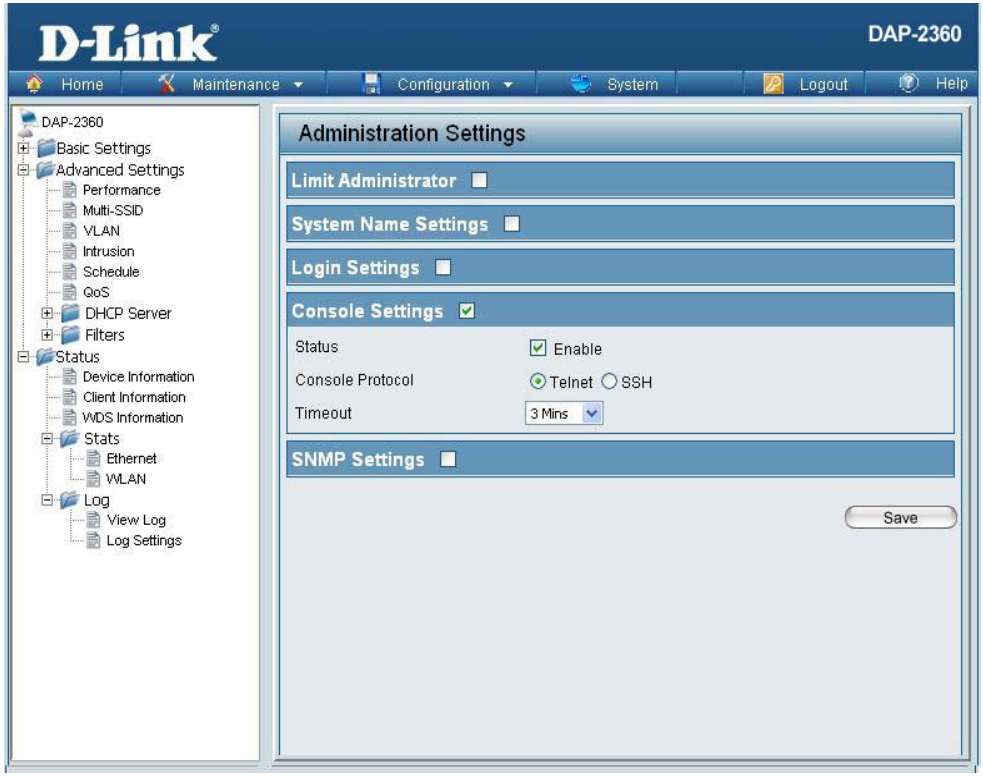
Console Settings

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

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

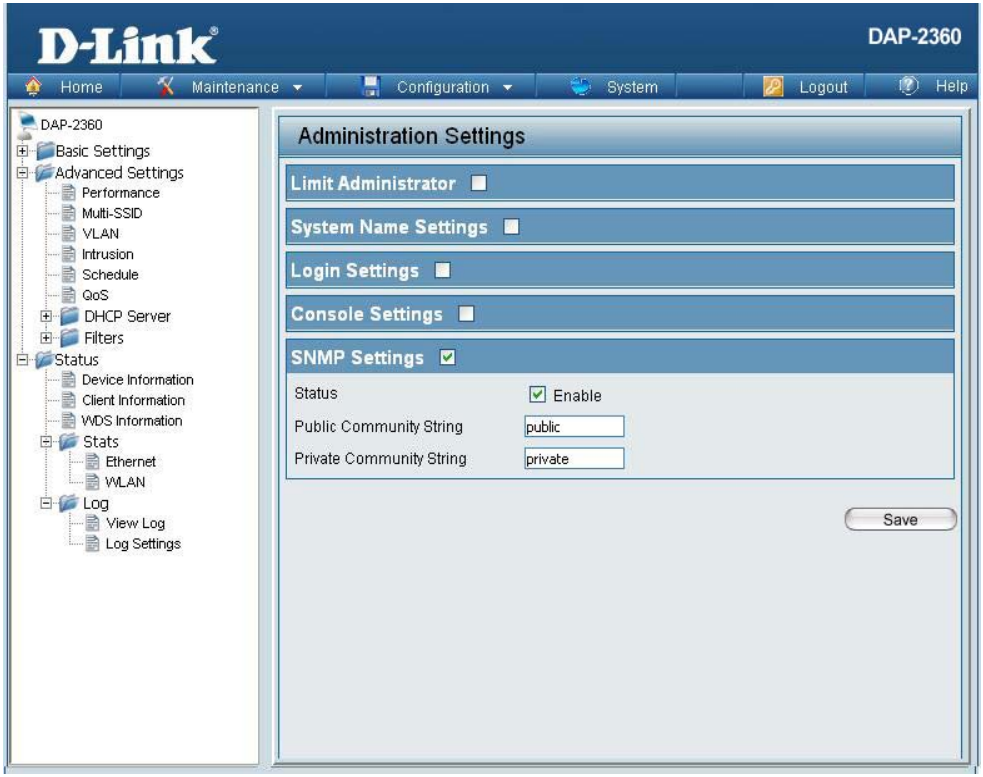
Console Protocol: Select the type of protocol you would like to use, **Telnet** or **SSH**.

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



SNMP Settings

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



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

Public Community String: Enter the public SNMP community string.

Private Community String: Enter the private SNMP community string.

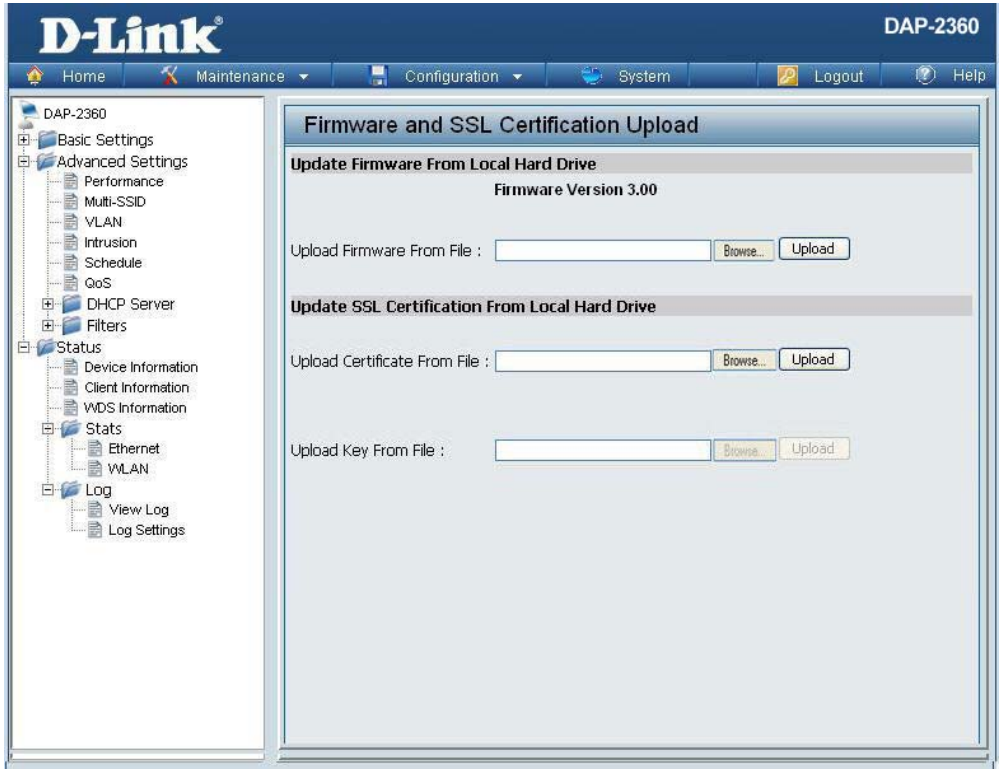
Firmware and SSL Certification Upload

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-2360 from http://support.dlink.com to your local computer, use the **Browse** button to locate the firmware file on your computer. Click **Upload** to update the firmware version. Please don't turn the power off while upgrading.

Upload SSL Certification From Local Hard Drive:

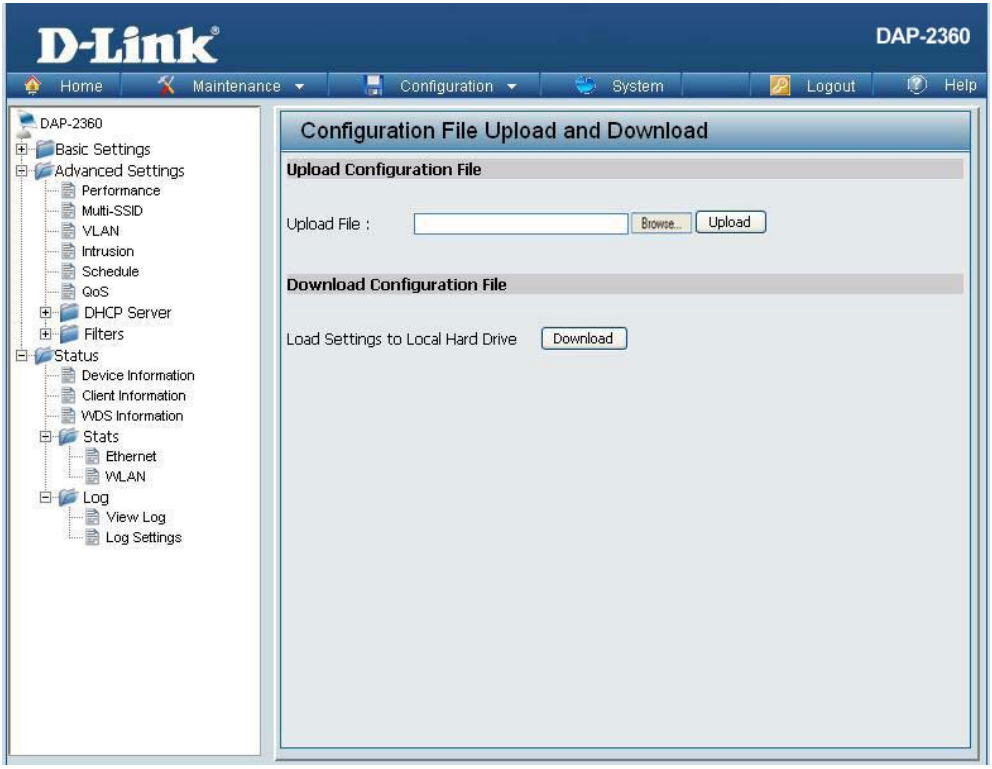
Click **Browse** to locate the SSL Certification file on your local computer. After selecting and opening the file, click **Upload** to upload the file to the DAP-2360.



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-2360.

Download Configuration File: Click **Download** to save the current DAP-2360 configuration to your local computer. Note that if you save one configuration with the administrator's password now, after resetting your DAP-2360, 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.

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

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

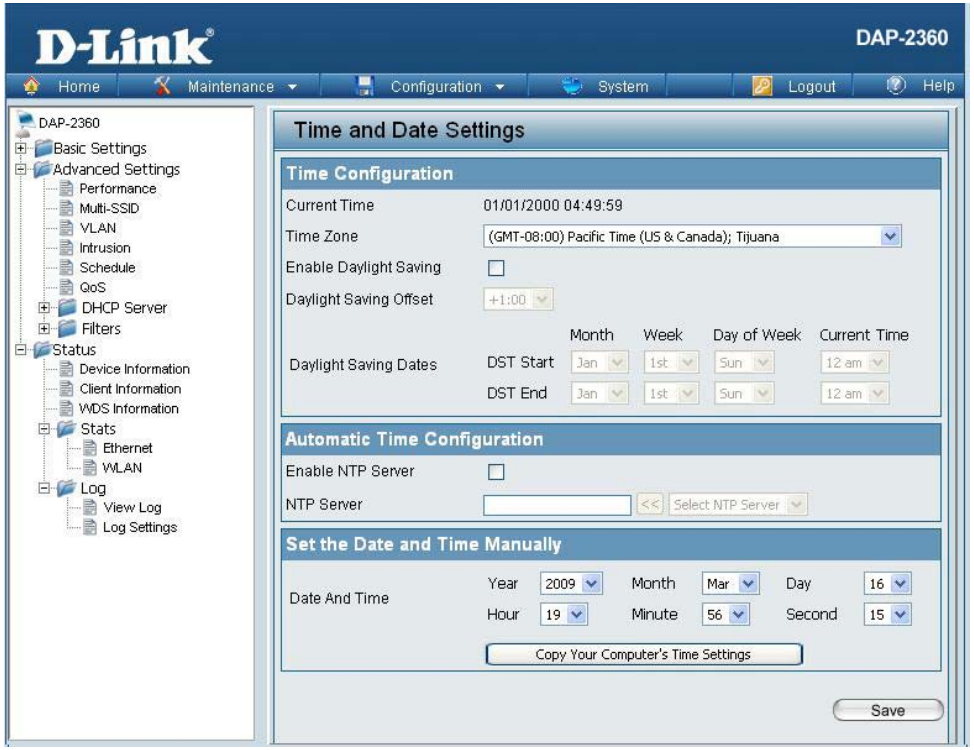
Daylight Saving Offset: Use the pull-down menu to select the correct Daylight Saving period.

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

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

NTP Server: Enter the NTP server IP address.

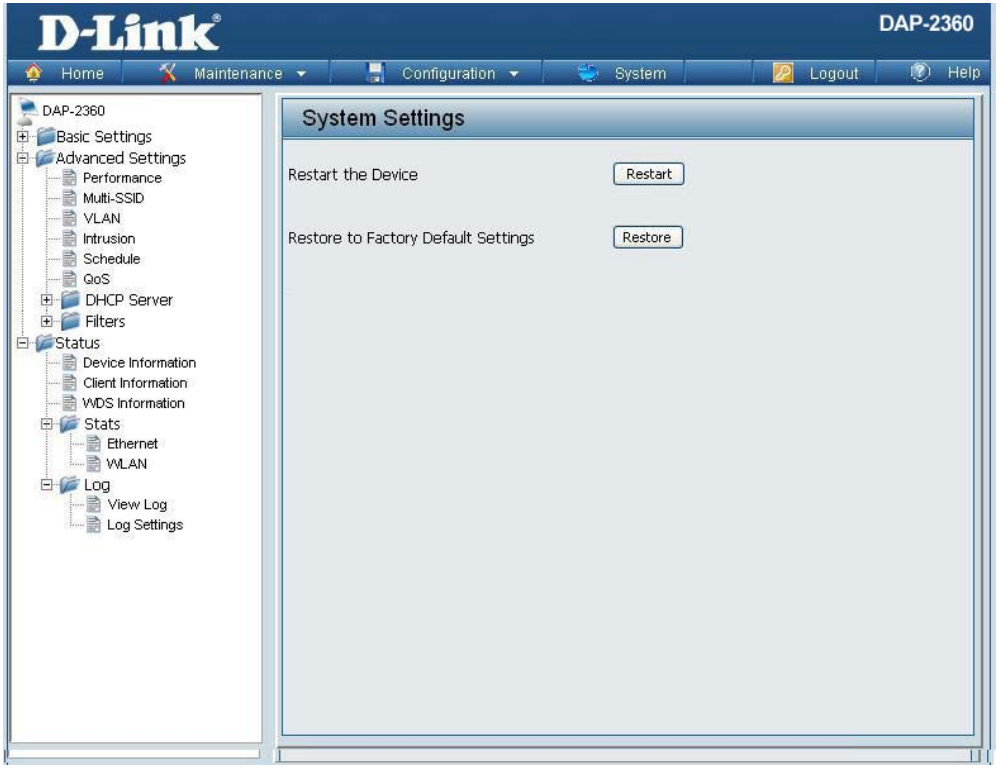
Set the Date and Time Manually: You can either manually set the time for your AP here, or you can click the **Copy Your Computer's Time Settings** button to copy the time from the computer you are using (Make sure that the computer's time is set correctly).



System
System Settings

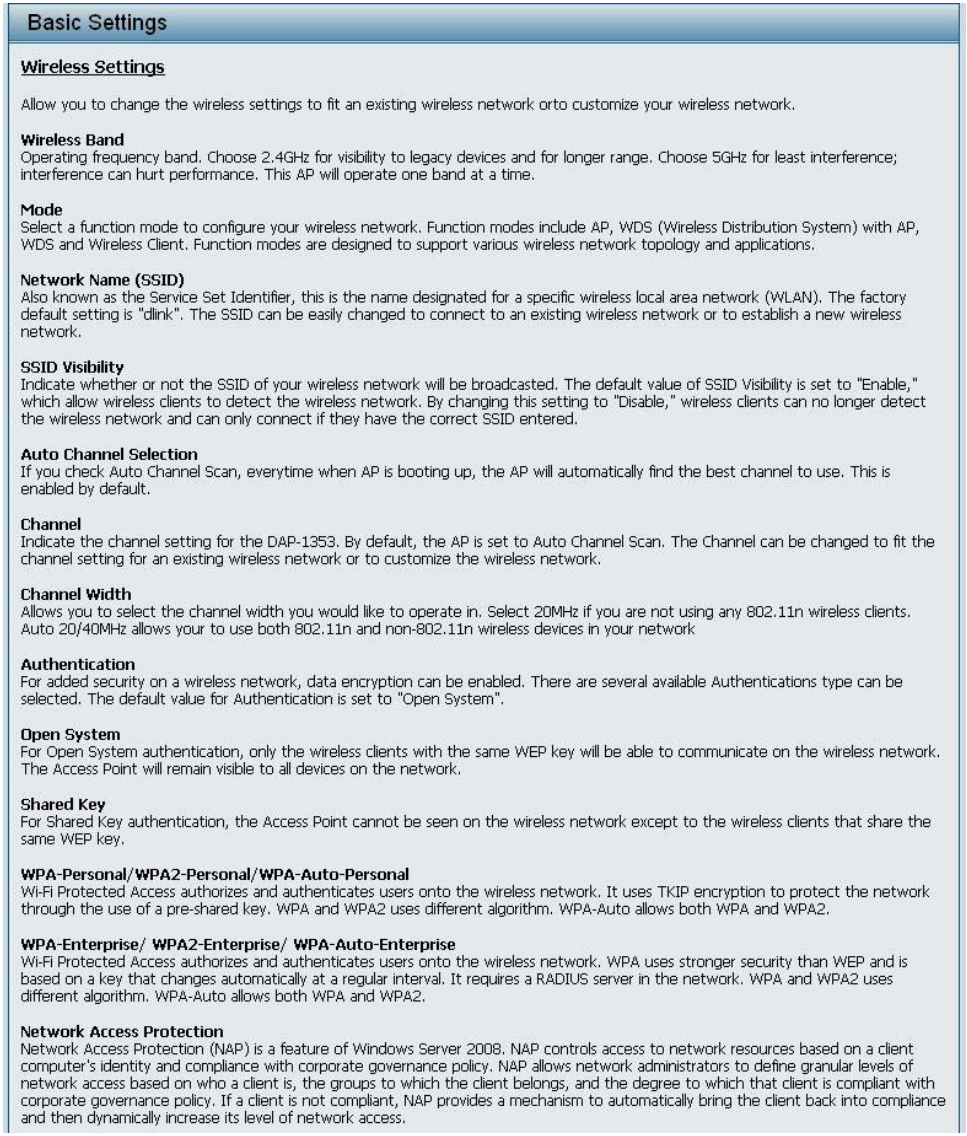
Restart the Device: Click **Restart** to restart the DAP-2360.

Restore to Factory Default Settings: Click **Restore** to restore the DAP-2360 back to factory default settings.



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 orto customize your wireless network.

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

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

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

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

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

Channel
Indicate the channel setting for the DAP-1353. By default, the AP is set to Auto Channel Scan. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

Channel Width
Allows you to select the channel width you would like to operate in. Select 20MHz if you are not using any 802.11n wireless clients. Auto 20/40MHz allows your to use both 802.11n and non-802.11n wireless devices in your network

Authentication
For added security on a wireless network, data encryption can be enabled. There are several available Authentications type can be selected. The default value for Authentication is set to "Open System".

Open System
For Open System authentication, only the wireless clients with the same WEP key will be able to communicate on the wireless network. The Access Point will remain visible to all devices on the network.

Shared Key
For Shared Key authentication, the Access Point cannot be seen on the wireless network except to the wireless clients that share the same WEP key.

WPA-Personal/WPA2-Personal/WPA-Auto-Personal
Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. It uses TKIP encryption to protect the network through the use of a pre-shared key. WPA and WPA2 uses different algorithm. WPA-Auto allows both WPA and WPA2.

WPA-Enterprise/ WPA2-Enterprise/ WPA-Auto-Enterprise
Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. WPA uses stronger security than WEP and is based on a key that changes automatically at a regular interval. It requires a RADIUS server in the network. WPA and WPA2 uses different algorithm. WPA-Auto allows both WPA and WPA2.

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

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-2360. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

When entering the IP address of the D-Link access point (192.168.0.50 for example), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
    - Internet Explorer 7.0 or higher
    - Netscape 9.0 or higher
    - Firefox 3.0 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

Federal Communication Commission Interference Statement

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

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

1) this device may not cause interference and

2) this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 4.85dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that

the EIRP is not more than required for successful communication.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

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

以下警語適用台灣地區

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。