D-Link®
Building Networks for People

DAP-2682
Version 1.01

Wireless AC1750
Wave 2 Dual-Band PoE Access Point

User Manual

Business Class Networking

Table of Contents

Product Overview 4
Introduction 4
Features 5
Package Contents 6
System Requirements 6

Hardware Overview 7
LEDs 7
Connections 7

Basic Installation 8
Hardware Setup 8
Configure the access point 8

Web User Interface 9
Wireless 10
Access Point Mode 10
WDS with AP Mode 12
WDS Mode 14
Wireless Client Mode 16
Wireless Security 17
Wired Equivalent Privacy (WEP) 17
Wi-Fi Protected Access (WPA / WPA2) 18
LAN 20
IPv6 21
Advanced Settings 22
Performance 23
Wireless Resource Control 25
Multi-SSID 27
VLAN 29
VLAN List 29
Port List 30
Add/Edit VLAN 31
PVID Settings 32
Intrusion 33
Schedule 34
Internal RADIUS Server 35
ARP Spoofing Prevention 36
Bandwidth Optimization 37
AP Array 39
AP Array Scan 39
Configuration Settings 40
Auto-RF 44
Load Balance 45
Captive Portal 46
Authentication Settings-Web Redirection Only 46
Authentication Settings- Username/Password .. 48
Authentication Settings- Passcode 50
Authentication Settings- Remote RADIUS 52
Authentication Settings- LDAP 54
Authentication Settings- POP3 56
Login Page Upload 58
IP Filter Settings 59
MAC Bypass 60

DHCP Server 61
Dynamic Pool Settings 61
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 70
Client Information 71
WDS Information Page 72
Channel Analyze 73
Stats Page 74
Ethernet Traffic Statistics 74
WLAN Traffic Statistics 75
Log 76
View Log 76
Log Settings 77
Maintenance Section 78
Administration 79
Limit Administrator 79
System Name Settings 80
Login Settings 80
Console Settings 80
SNMP Settings 81
Ping Control Setting 81
LED Settings 81
Central WiFiManager Settings 81
Firmware and SSL Upload 82
Configuration File Upload 83
Time and Date Settings 84
Configuration and System 85
System Settings 86
Help 87

Knowledge Base 88
Wireless Basics 88
Wireless Installation Considerations 89

Troubleshooting 90
Why can't I access the web-based configuration utility? 90
What can I do if I forgot my password? 90
How to check your IP address? 91
How to statically assign an IP address? 92

Technical Specifications 93

Warranty 94

Central WiFiManager 100

Registration 102

Product Overview

Introduction

D-Link, an industry pioneer in wireless networking, introduces a solution for businesses seeking to deploy next generation 802.11ac LANs. D-Link unveils its new DAP-2682, 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 DAP-2682 Access Point allows network administrators to deploy a highly manageable and extremely robust dual band wireless network. For advanced installations, this new high-speed Access Point has integrated 802.3at Power over Ethernet (PoE) support, allowing installation of this device in areas where power outlets are not readily available. In addition to bridging 802.11ac and 802.11b/g/n wireless networks, the DAP-2682 can bridge to wired networks with its integrated Gigabit (10/100/1000Mbps) Ethernet port.

Enhanced Performance

The DAP-2682 delivers reliable wireless performance with maximum wireless signal rates of up to 1750Mbps. 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-2682 supports load balance features to ensure maximum performance.

Security

To help maintain a secure wireless network, the DAP-2682 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 back end. 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 DAP-2682 includes support for up to 16 VLANs for implementing multiple SSIDs to further help segment users on the network. The DAP-2682 also includes a wireless client isolation mechanism, which limits direct client-to-client communication.

Power Usage

This device is an Energy Related Product (ErP) with High Network Availability (HiNA), and automatically switches to a power-saving Network Standby mode within 1 minute of no packets being transmitted. It can also be turned off through a power switch to save energy when it is not needed.
Network Standby: 3.10 watts

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

**Only compliant with 802.3at PoE switch and 802.3af standard can't supply sufficient power for DAP-2682

Features

- Provide Ethernet to Wireless LAN bridge fully IEEE 802.3/u/ab compatible on the Ethernet side and fully interoperable with IEEE 802.11ac and b/g/n/a compliant equipment
- Compatible with IEEE 802.11b high rate standard to provide wireless 11Mbps data rate
- Compatible with IEEE 802.11g higher speed standard to provide wireless 54Mbps data rate
- Compatible with IEEE 802.11a higher speed standard to provide wireless 54Mbps data rate
- Compatible with IEEE 802.11n higher speed standard to provide wireless 450Mbps data rate
- Compatible with 802.11ac higher speed standard to provide wireless 1300Mbps data rate
- Operation at 2.4~2.5GHz and 5.15~5.85GHz frequency band to meet worldwide regulations
- Supports IEEE 802.11ac and b/g/n/a wireless data encryption with 64/128-bit WEP for security
- Allows auto fallback data rate for reliability, optimized throughput and transmission range
- Web-based configuration and management
- Supports enhanced security – WPA-PSK and WPA2-PSK, RADIUS client, and Cipher negotiation
- Supports one 802.3at PoE port
- Supports two 10/100/1000M Ethernet ports
- AP Mode, WDS Mode, WDS with AP, and Wireless Client Mode
- Supports SNMP v1,v2,v3
- Support Trap server (SNMP v1, v2c)
- Support Central WiFiManager
- Support AP Array and AP Array Setup Tool

* Maximum wireless signal rate derived from IEEE Standard 802.11ac, 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-2682 isn't supported in the 5.25~5.35GHz and 5.47 ~ 5.725GHz frequency ranges in some regions.

***Only compliant with 802.3at PoE switch and 802.3af standard can't supply sufficient power for DAP-2682

Package Contents

- DAP-2682 802.11ac Power over Ethernet (PoE) Access Point
- Mounting Brackets
- Ceiling Brackets
- Ethernet Cable
- CD-ROM
- Quick Install Guide

Note: *No PSU supplied. To power the units use an D-Link 802.3at PoE switch or the D-Link DPE-301GI PoE injector.*

System Requirements

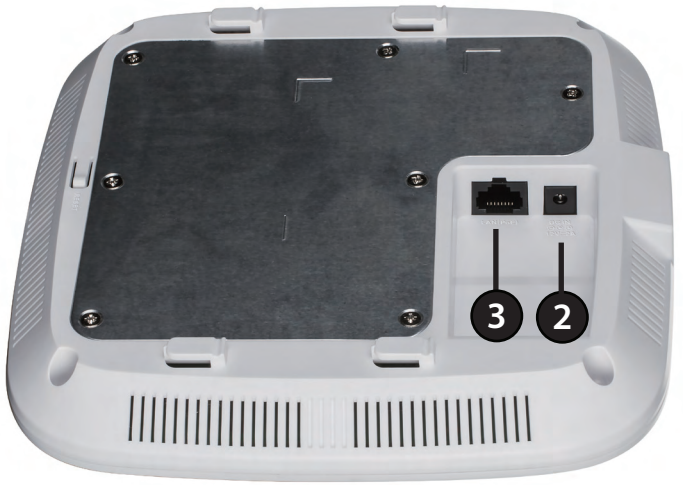
- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet Adapter
- Internet Explorer 11, Safari 7, Firefox 28, or Google Chrome 33 and Above (for configuration)

Hardware Overview

LEDs

1	Power/Status	Solid Red	Indicates the access point has malfunctioned.
		Blinking Red	This LED will blink during boot-up.
		Solid Green	Indicates that the DAP-2682 is working properly.

Connections

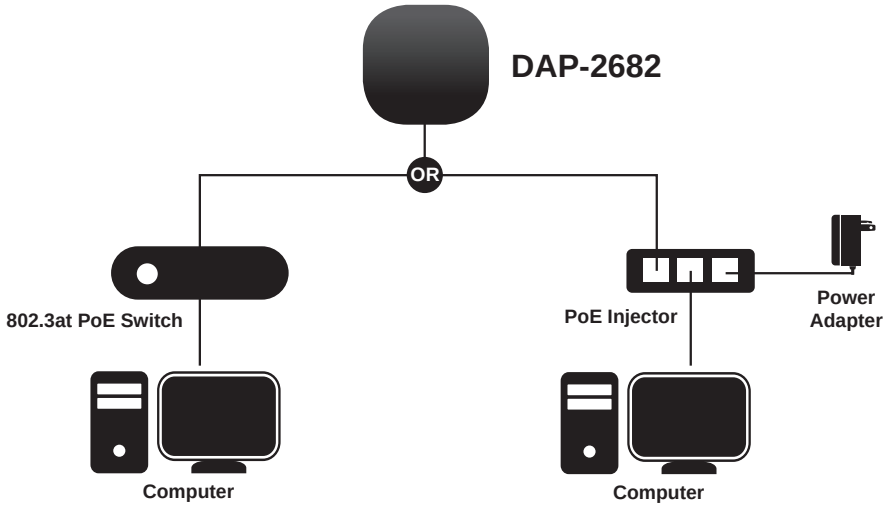


2	Power Receptor	Connect the supplied power adapter. Power Receptor (*Note no longer used, replaced by PoE)
3	LAN (PoE) Port	Connect to a Power over Ethernet (PoE) switch or router via an Ethernet cable.

Basic Installation
Hardware Setup

To power on the DAP-2682, you can use ONE of the following methods:
1. Plug one end of your Ethernet cable into the LAN port of the DAP-2682, and the other end into a port on a 802.3at PoE switch.
2. Purchase separately a DPE-301GI PoE injector if you need to connect the Access Point without a 802.3at PoE Switch.

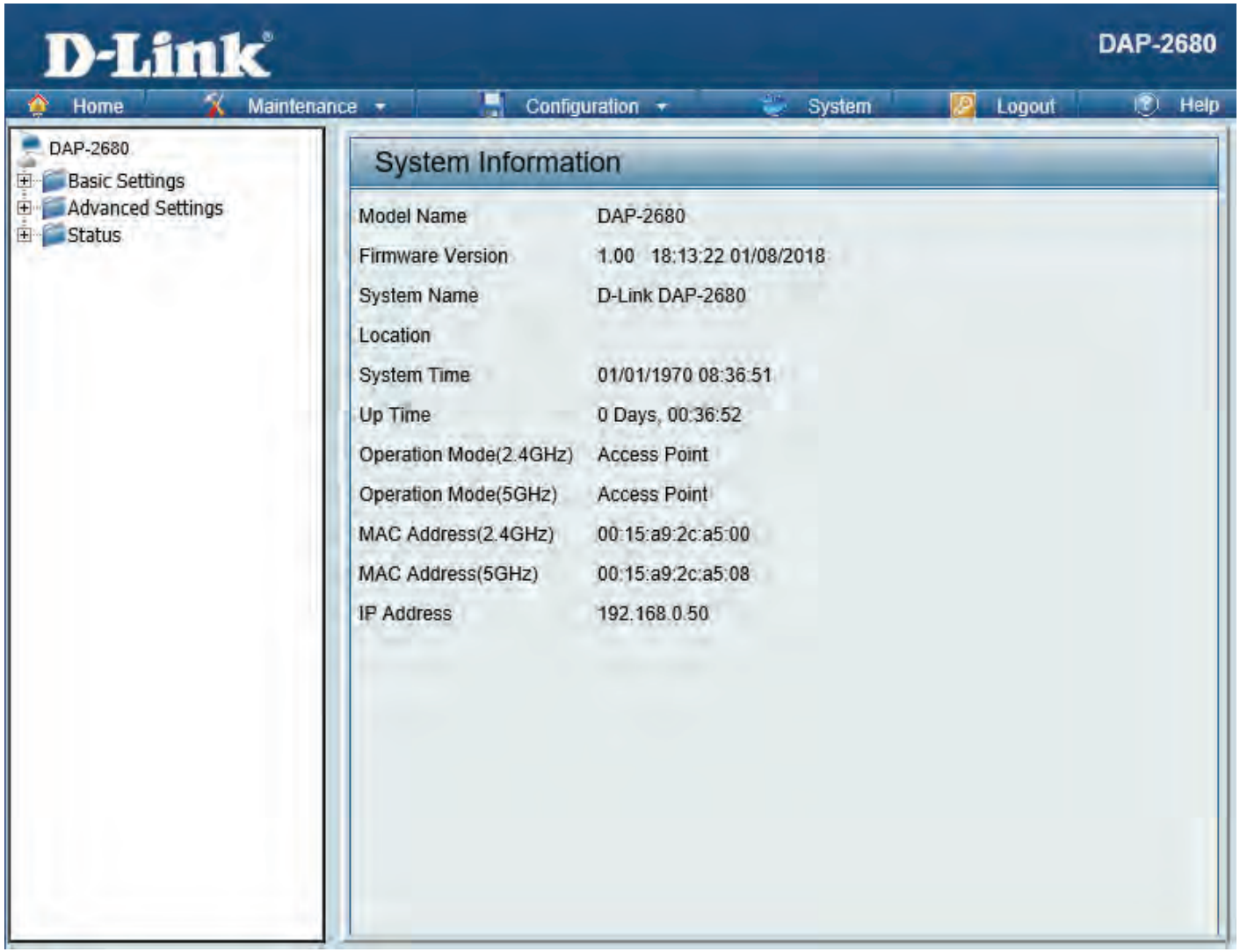
Configure the access point



To set up and manage the DAP-2682, use one of the following methods:
1. Connect the access point and your computer to the same switch. Manage the access point from the computer.
   Enter 192.168.0.50 in the address field of your browser, which is the default IP address of the access point.
   Log in to the Administration Web pages. The default login information is:
   Username: admin
   Password: (Leave the password field blank)
2. Connect the access point and your computer via DPE-301GI. Manage the access point from the computer.
   Ensure your computer is configured with a static IP address in 192.168.0.0/24 subnet.
   Launch a web browser, type the default IP address of the access point (http://192.168.0.50) and then press Enter.
   Log in to the Administration Web pages. The default login information is:
   Username: admin
   Password: (Leave the password field blank)

Web User Interface

The DAP-2682 supports an elaborate web user interface where the user can configure and monitor the device. Launch a web browser, type the IP address of the access point (Default setting is http://192.168.0.50 or https://192.168.0.50) and then press Enter to login. Most of the configurable settings are located in the left menu of the web GUI which contains section called **Basic Settings**, **Advanced Settings** and **Status**.



Wireless

On the wireless settings page, you can setup the basic wireless configuration for the access point. The user can choose from 4 different wireless modes:

Access Point - Used to create a wireless LAN
WDS with AP - Used to connect multiple wireless networks while still functioning as a wireless access point
WDS - Used to connect multiple wireless networks
Wireless Client - Used when the access point needs to act as a wireless network adapter for an Ethernet enabled device

Access Point Mode

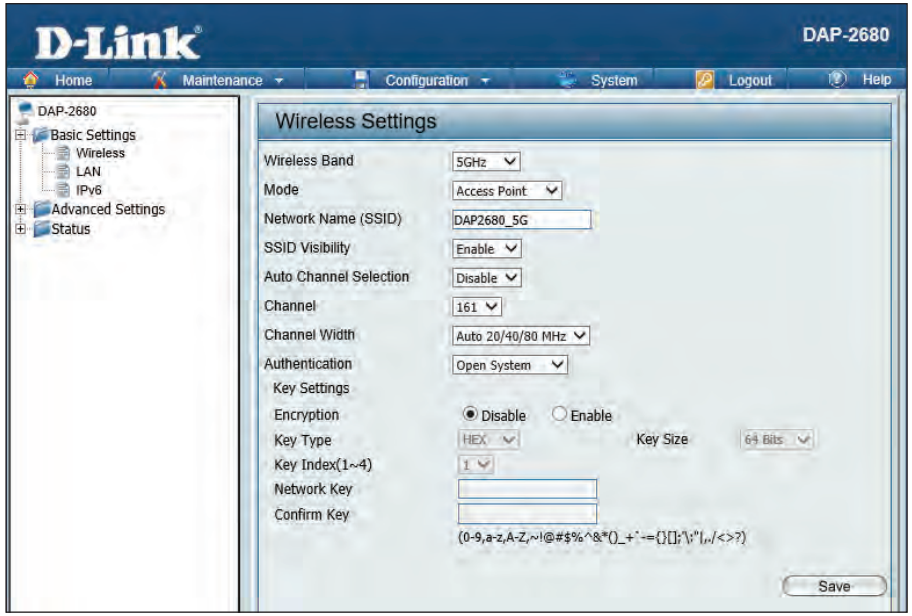
Wireless Band: Select either **2.4 GHz** or **5 GHz** from the drop-down menu.

Mode: Select **Access Point** 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. The SSID can be up to 32 characters and is case-sensitive.

SSID Visibility: Select **Enable** to broadcast the SSID across the network, thus making it visible to all network users. Select **Disable** to hide the SSID from the network.

Auto Channel Selection: This feature when enabled automatically selects the channel that provides the best wireless performance. The channel selection process only occurs when the AP is booting up. To manually select a channel, set this option to Disable and select a channel from the drop-down menu.



Channel: To change the channel, first toggle the *Auto Channel Selection* setting to **Disable**, and then use the drop-down menu to make the desired selection.

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

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

Authentication: Use the drop-down menu to choose **Open System**, **Shared Key**, **WPA-Personal**, **WPA-Enterprise**, or **802.1x**.

- Select **Open System** to communicate the key across the network (WEP).
- 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.

WDS with AP Mode

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

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

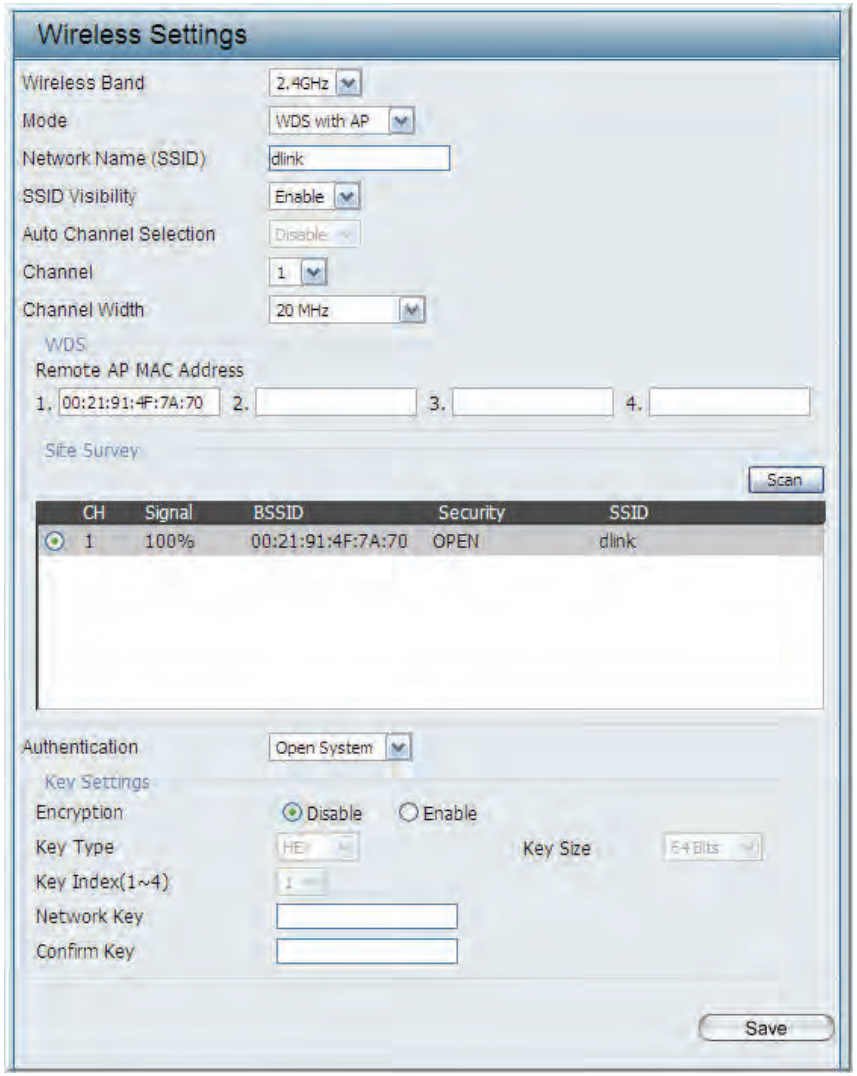
Network Name (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is dlink. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

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 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 drop-down menu to make the desired selection. (Note: The wireless adapters will automatically scan and match the wireless settings.)

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

WDS Mode

Wireless Band: Select either 2.4GHz or 5GHz 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.

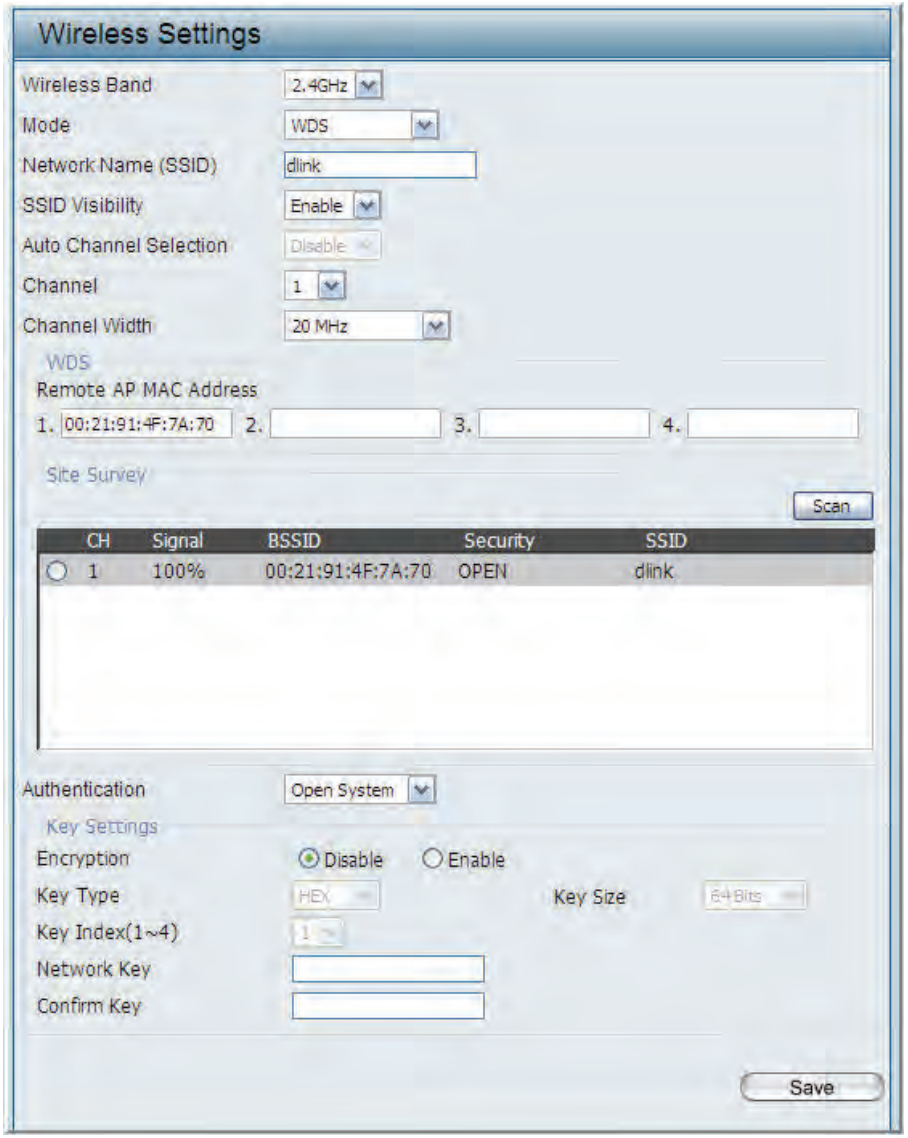
SSID Visibility: Enable or Disable SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.

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: Use the drop-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 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

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.

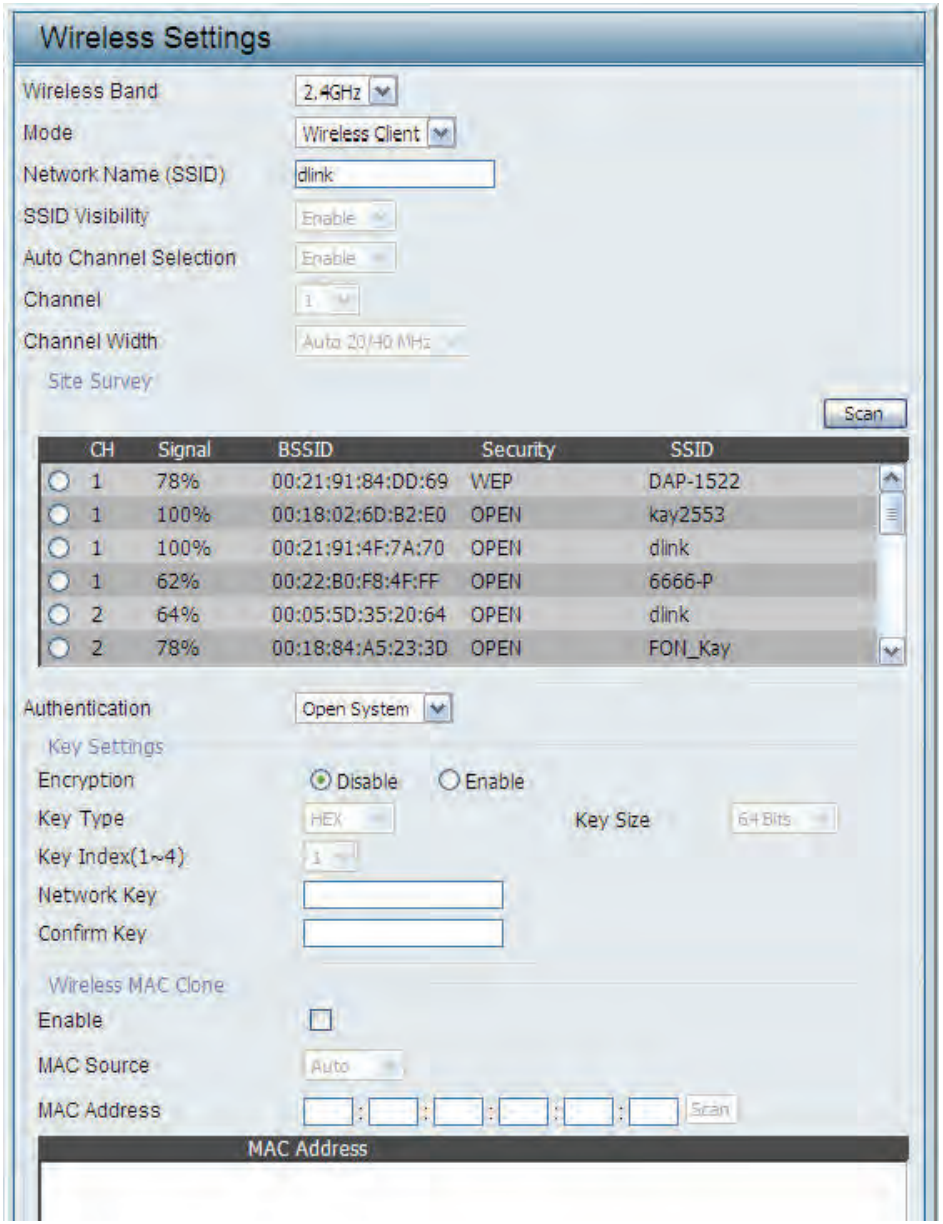
Auto Channel Selection: Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is not supported in Wireless Client mode.

Channel: The channel used will be displayed, and matches the AP that the DAP-2682 is connected to when set to Wireless Client mode.

Channel Width: Use the drop-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: Will be explained in the next topic.



Wireless Security

Wireless security is a key concern for any wireless network installed. Unlike any other networking method wireless networks will broadcast it's presence for anyone to connect to it. Today, wireless security has advanced to a level where it is virtually impenetrable.
There are mainly two forms of wireless encryption and they are called Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP was the first security method developed. It is a low level encryption but better than now encryption. WPA is the newest encryption standard and with the advanced WPA2 standard wireless networks have finally reach a point where the security is strong enough to give users the peace of mind when installing wireless networks.

Wired Equivalent Privacy (WEP)

WEP provides two variations called **Open System** and **Shared Key**.

Open System will send a request to the access point and if the key used matches the one configured on the access point, the access point will return a success message back to the wireless client. If the key does not match the one configured on the access point, the access point will deny the connection request from the wireless client.

Shared Key will send a request to the access point and if the key used matches the one configured on the access point, the access point will send a challenge to the client. The client will then again send a confirmation of the same key back to the access point where the access point will either return a successful or a denial packet back to the wireless client.

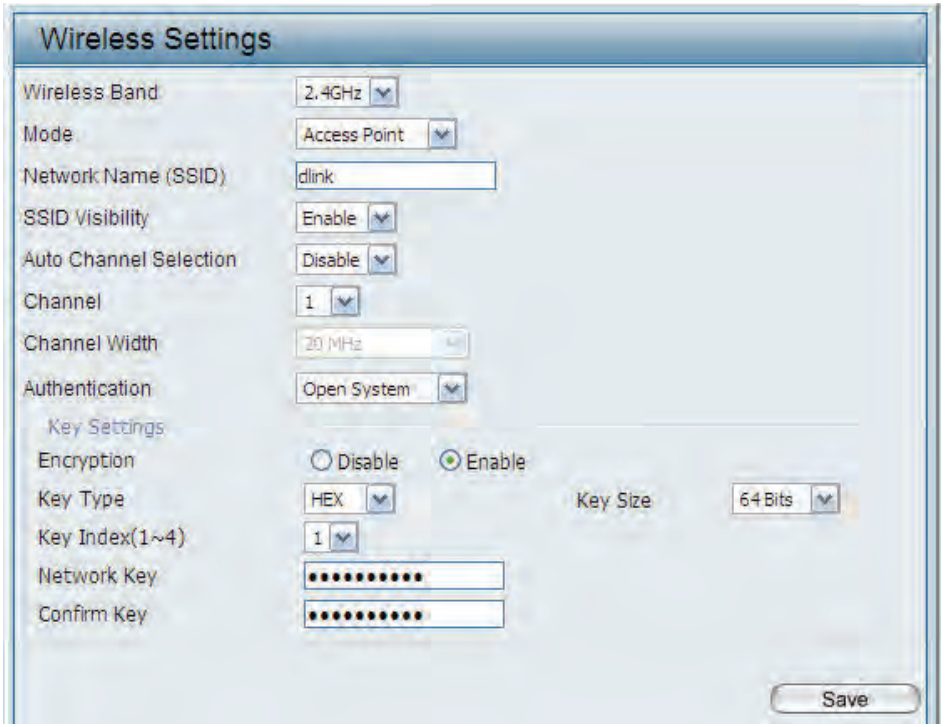
Encryption: Use the radio button to disable or enable encryption.

Key Type*: Select HEX or ASCII.

Key Size: Select 64 Bits or 128 Bits.

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

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



**Hexadecimal (HEX) digits consist of the numbers 0-9 and the letters A-F.
*ASCII (American Standard Code for Information Interchange) is a code that represents English letters using numbers ranging from 0-127.

Wi-Fi Protected Access (WPA / WPA2)

WPA was created by the Wi-Fi Alliance to address the limitations and weaknesses found in WEP. This protocol is mainly based on the 802.11i standard. There are also two variations found in WPA called WPA-Personal (PSK) and WPA-Enterprise (EAP).

WPA-EAP requires the user to install a Radius Server on the network for authentication.
WPA-Personal does not require the user to install a Radius Server on the network.

Comparing WPA-PSK with WPA-EAP, WPA-PSK is seen as a weaker authentication but comparing WPA-PSK to WEP, WPA-PSK is far more secure than WEP. WPA-EAP is the highest level of wireless security a user can use for wireless today.

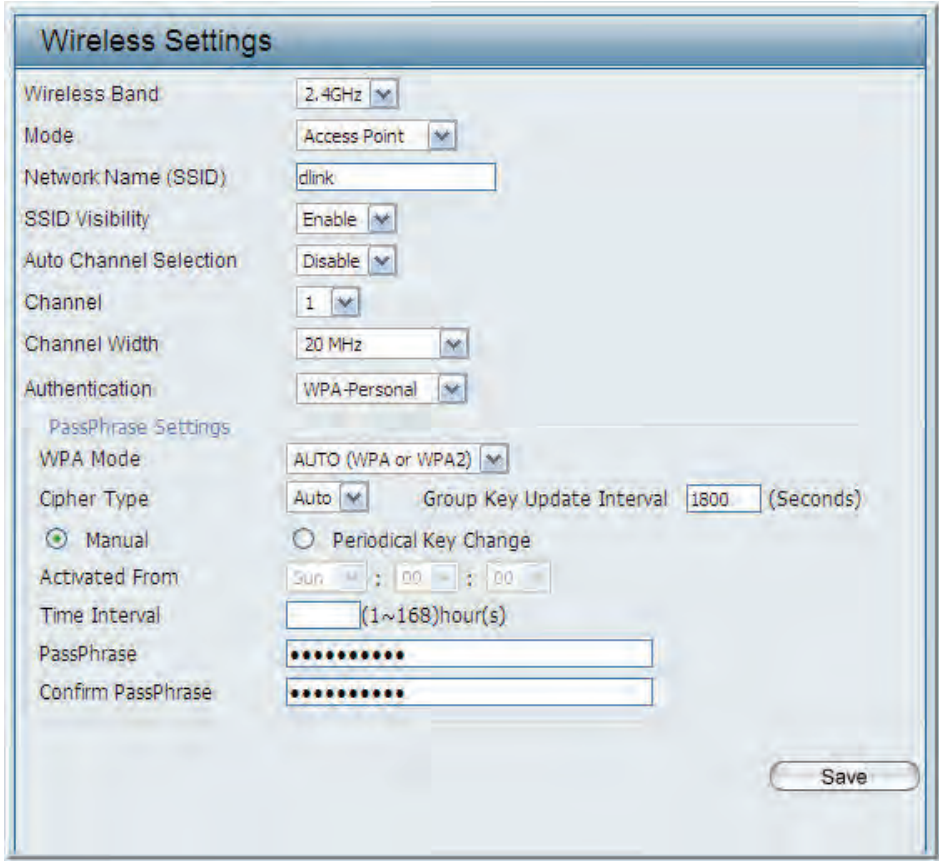
WPA2 is an upgrade of WPA. WPA2 yet again solves some possible security issues found in WPA. WPA2 has two variations called WPA2-Personal (PSK) and WPA2-Enterprise (EAP) which is the same as found with WPA.

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 pull down menu.

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

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



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.

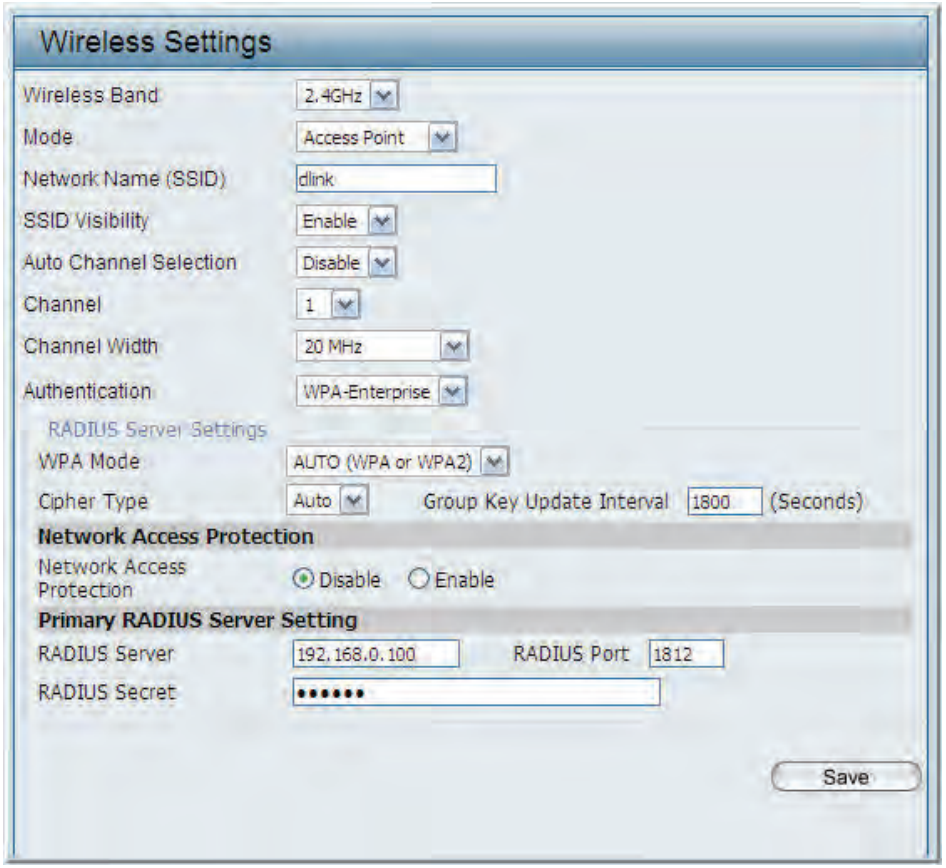
Group Key Update Interval: Select the interval during which the group key will be valid. 1800 is the recommended value as a lower interval may reduce data transfer rates.

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

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

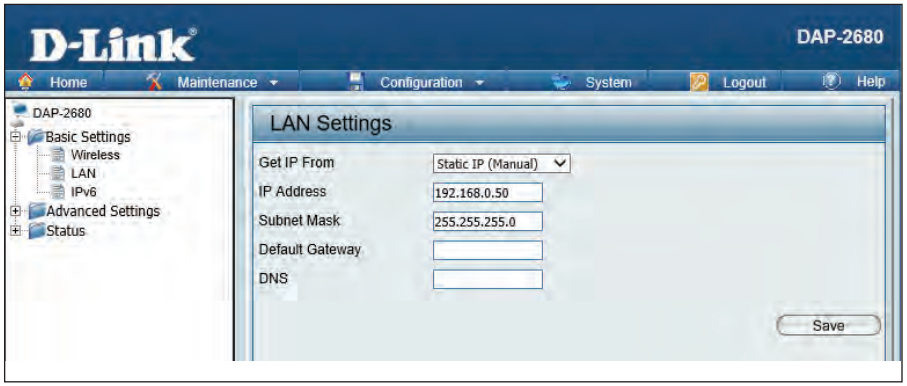
RADIUS Port: Enter the RADIUS port.

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-2682. 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-2682. 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/router in your network.

DNS: Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

IPv6

Enable IPv6: Check to enable the IPv6

Get IP From: Auto is chosen here. Choose this option the DAP-2682 can get IPv6 address automatically or use Static to set IPv6 address manually.
When Auto is selected, the other fields here will be grayed out.

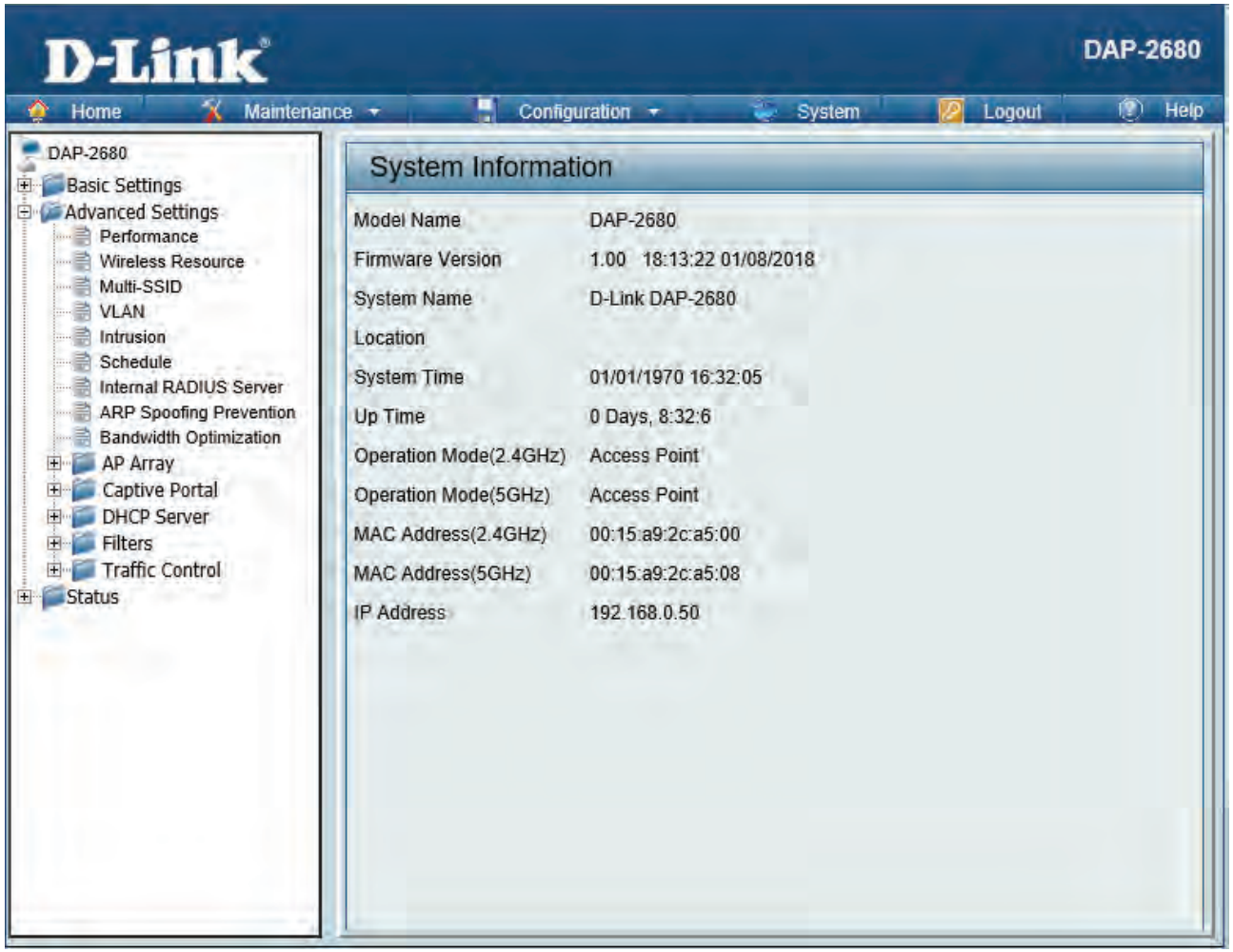
IP Address: Enter the LAN IPv6 address used here.

Prefix: Enter the LAN subnet prefix length value used here.

Default Gateway: Enter the LAN default gateway IPv6 address used here.

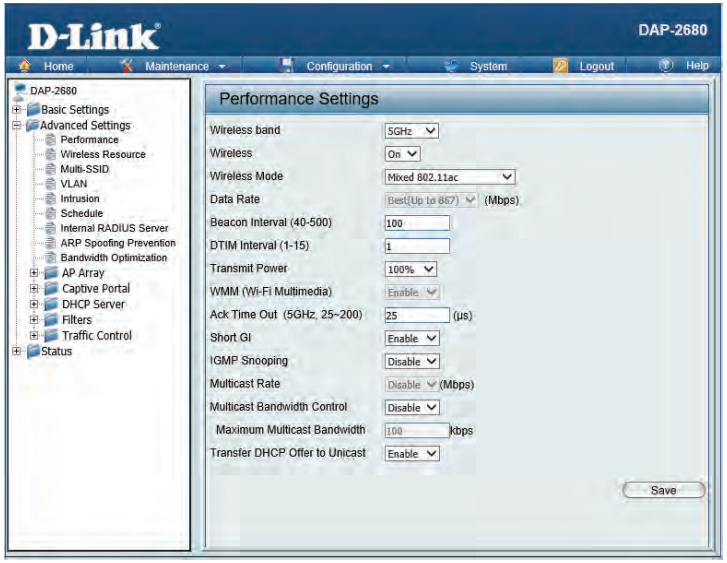
Advanced Settings

In the Advanced Settings Section the user can configure advanced settings concerning Performance, Multiple SSID, VLAN, Security, Quality of Service, AP Array, Web Redirection, DHCP Server, Filters and Scheduling. The following pages will explain settings found in the Advanced Settings section in more detail.



Performance

On the Performance Settings page the users can configure more advanced settings concerning the wireless signal and hosting.



Wireless Band: Select either 2.4GHz or 5GHz.

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, 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, 6 for 5 GHz and Best (Up to 54), 54, 48, 36, 24, 18, 12, 9, 6, 11, 5.5, 2 or 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.

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 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, 64~200): 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 64 to 200 microseconds in the 2.4 GHz in the field provided.

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

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

Multicast Rate : Select the multicast rate to adjust multicast packet data rates.

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

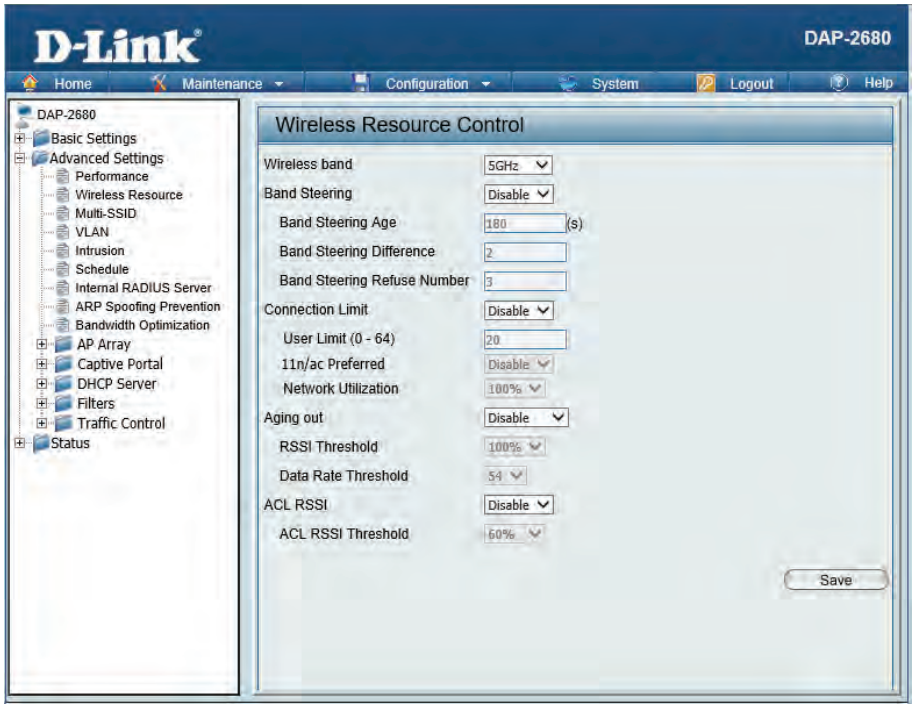
Multicast Bandwidth Control : Adjust the multicast packet data rate here. The multicast rate is supported in AP mode, (2.4 GHZ and 5 GHZ) and WDS with AP mode, including Multi-SSIDs.

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

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 **2.4GHz** or **5GHz**.

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

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

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

Band Steering Refuse Num: Enter the maximum 5GHz connection attempts allowed before the 5GHz 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-2682 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-2682 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.

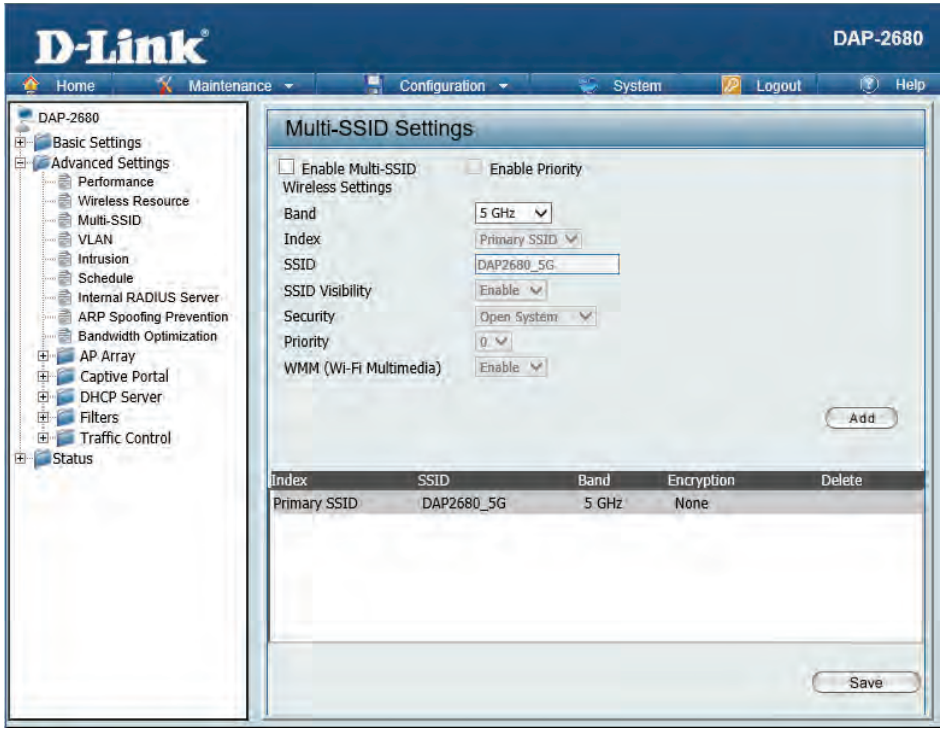
Data Rate Threshold: When **Data Rate** is selected in the **Aging out** drop-down menu, select the threshold of data rate here. When the data rate of wireless clients is lower than the specified number, the device disconnects the wireless clients.

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

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.

Priority: Select the priority level of the SSID selected.

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.

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-bit or 128-bit.

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 drop-down menu.

WPA Mode: When you select either WPA-Personal or WPA-Enterprise, you must also choose 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. In addition, you must configure Cipher Type, and Group Key Update Interval.

Cipher Type: 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 seconds is recommended.

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

Confirm Pass Phrase: When you select WPA-Personal, please re-enter the Pass Phrase 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.

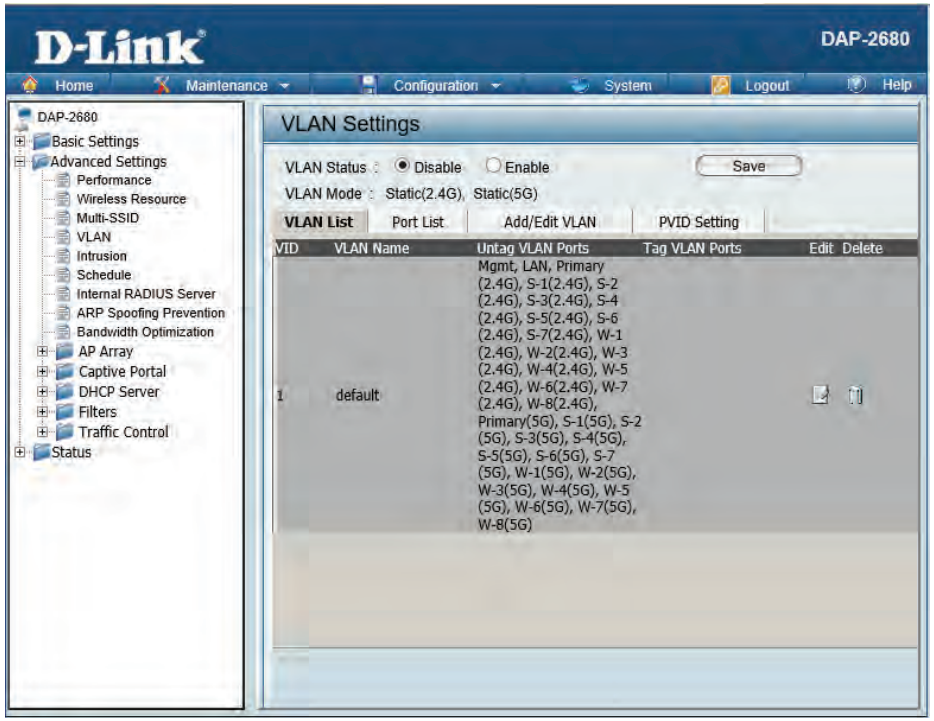
VLAN

VLAN List

The DAP-2682 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-2682 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 to Enable. 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.



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.

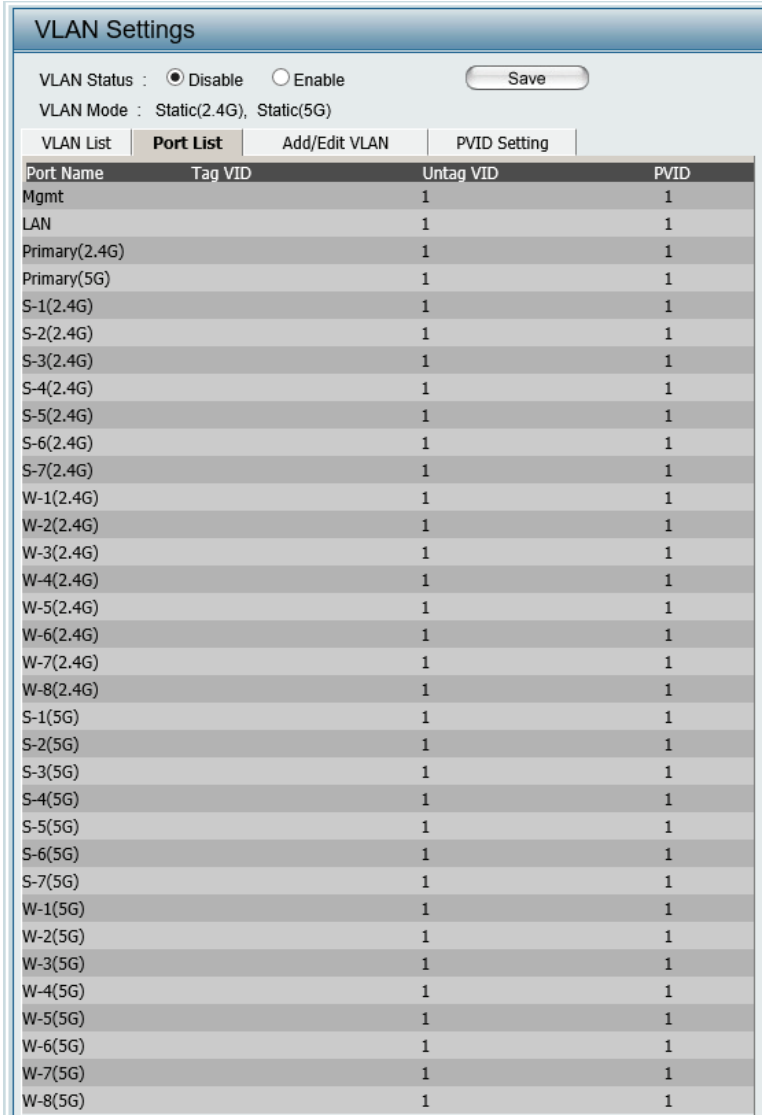
VLAN Status: Use the radio button to toggle to Enable. Next, go to the Add/Edit VLAN tab to add or modify an item on the VLAN List tab.

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.



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

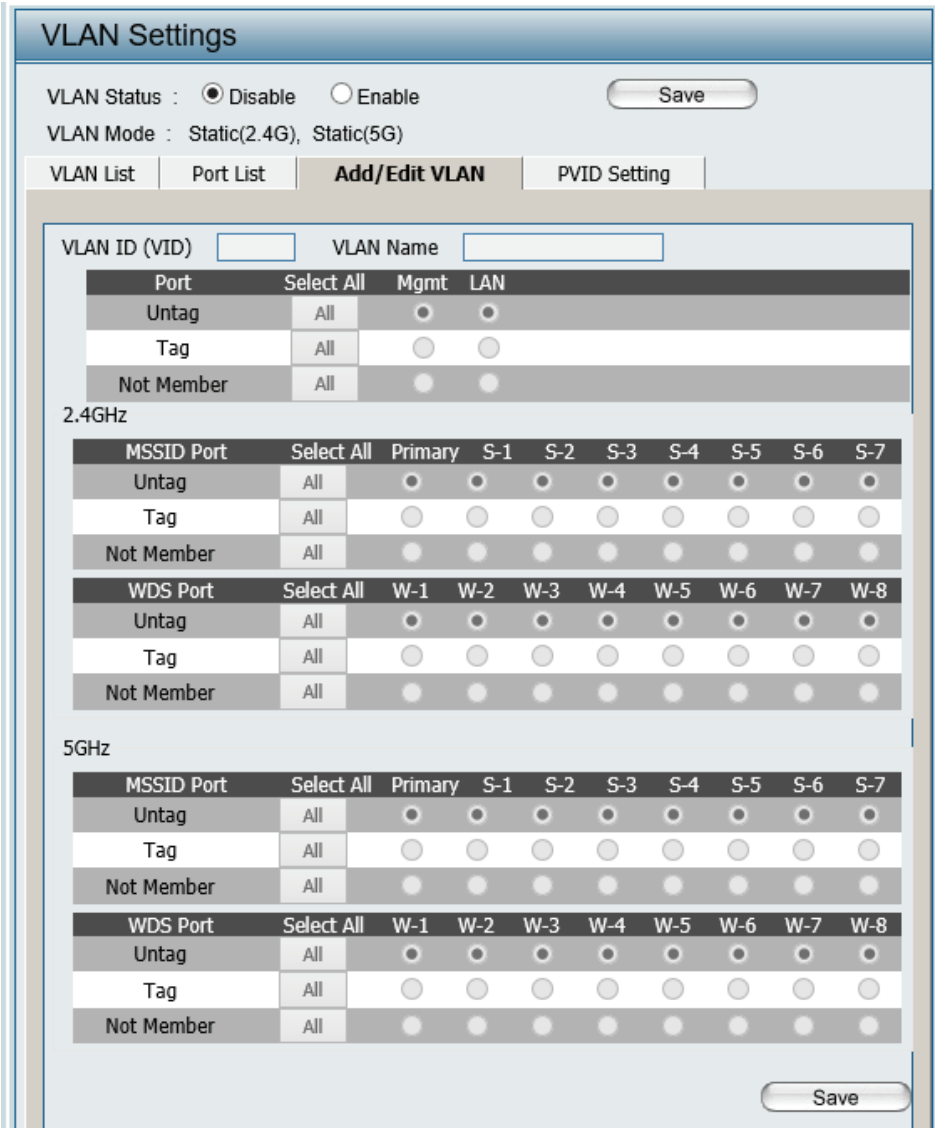
Add/Edit VLAN

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

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

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

VLAN Name: Enter the VLAN to add or modify.

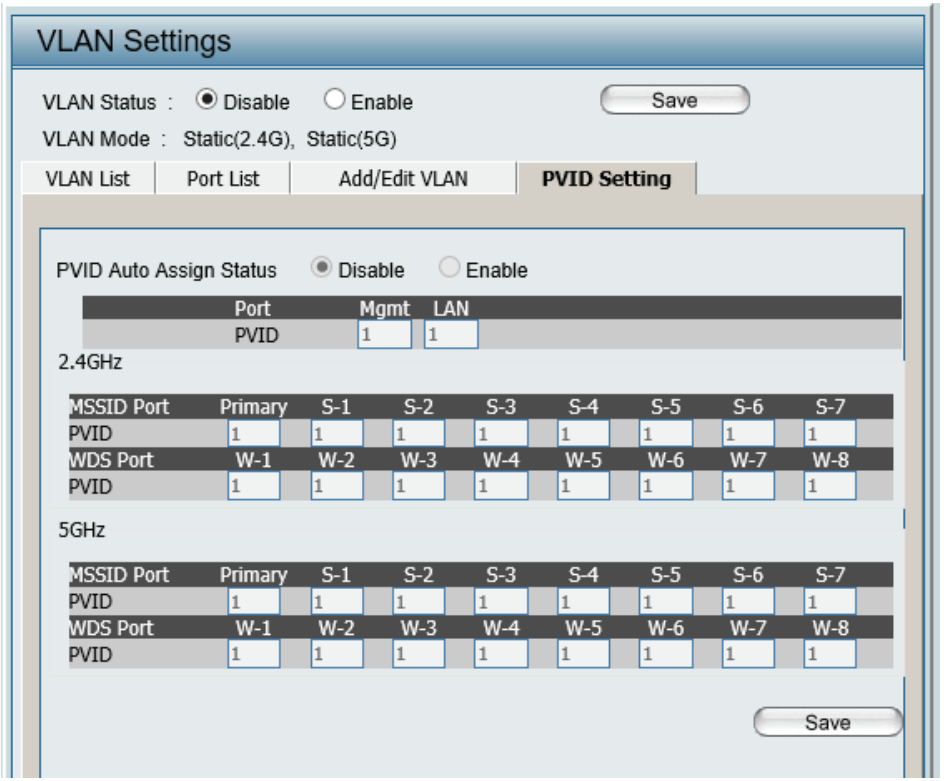


PVID Settings

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

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

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



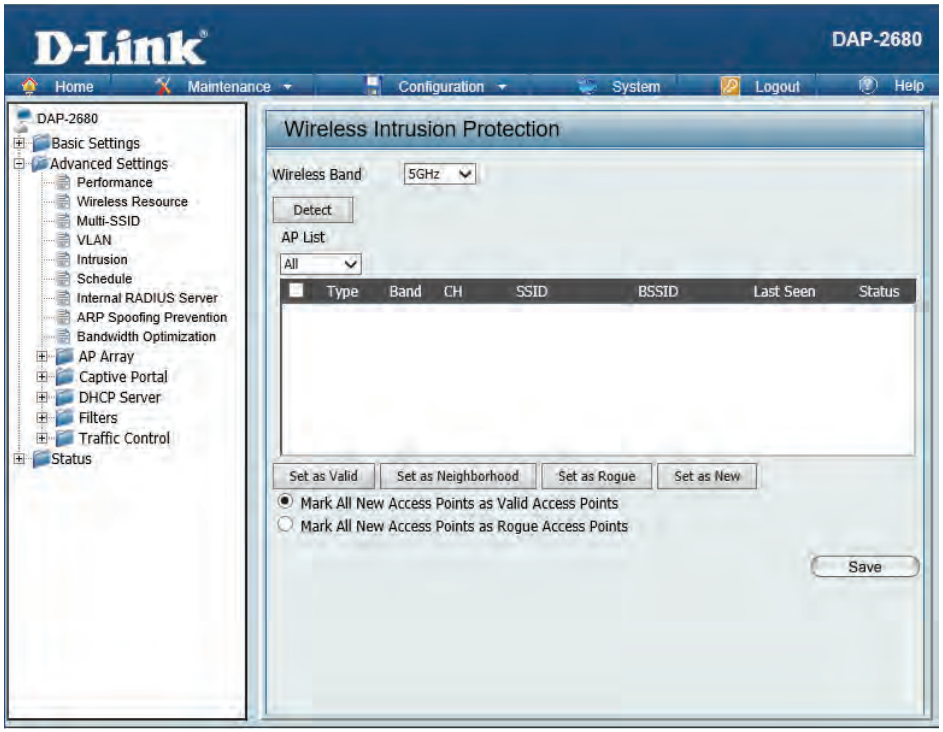
Intrusion

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

Wireless Band: Select 2.4GHz or 5GHz.

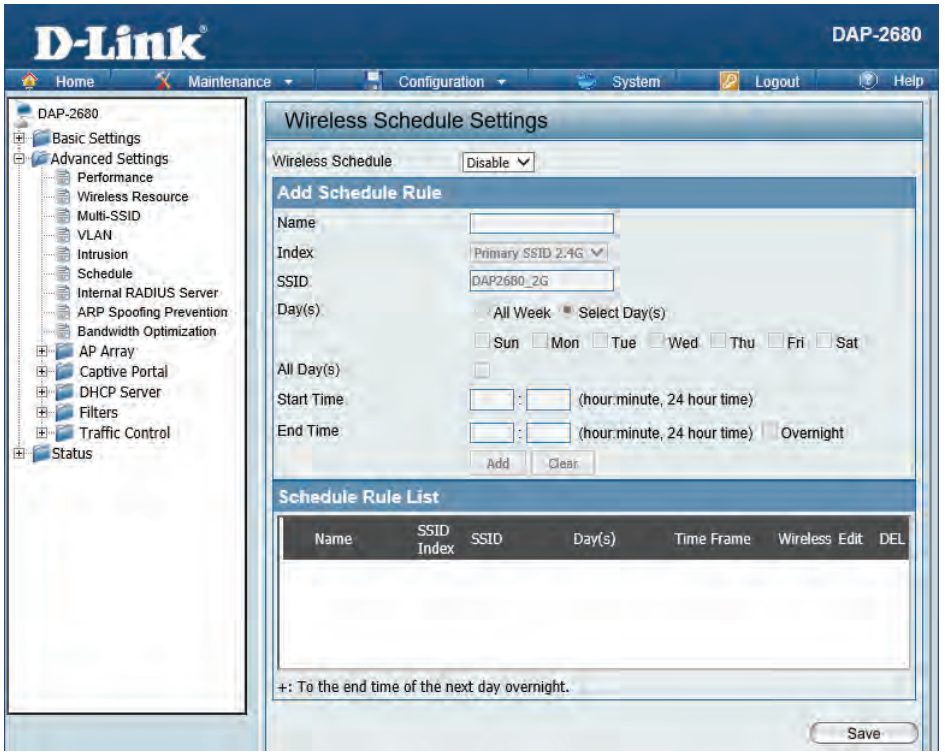
AP List: The choices include All, Valid, Neighbor, Rogue, and New.

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



Schedule

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



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

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

Index: 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 your settings apply 24 hours a day.

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

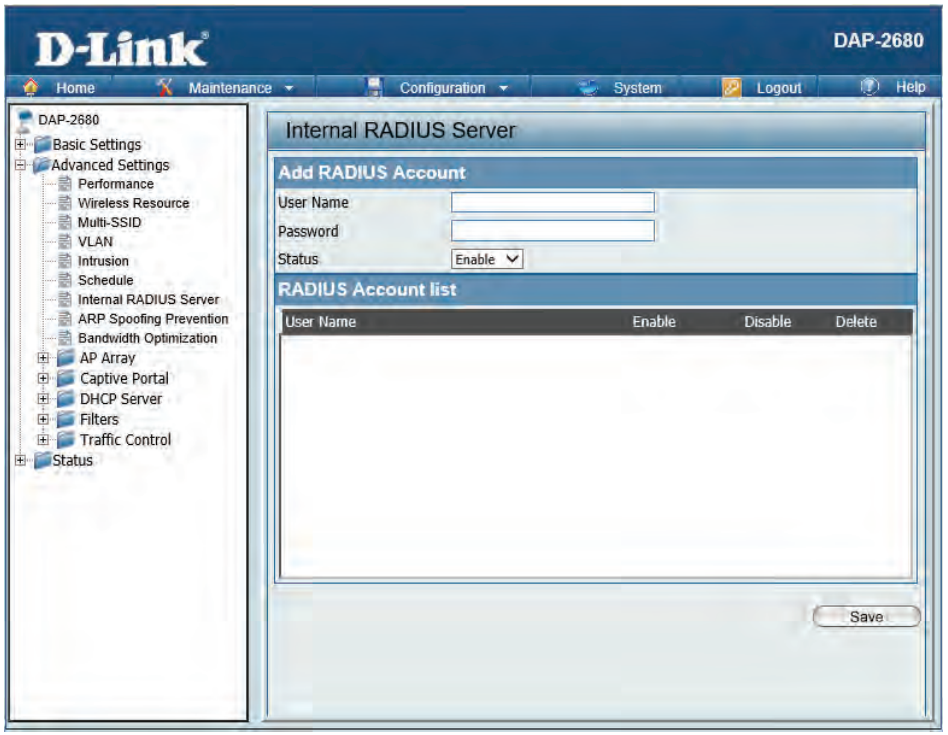
The DAP-2682 features a built-in RADIUS server. Once you have finished adding a RADIUS account, click the Save button to let your changes take effect. The newly-created account will appear in this RADIUS Account List. The radio buttons allow the user to enable or disable the RADIUS account. Click the 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: Toggle the drop-down menu between Enable and Disable.

RADIUS Account List: Displays the list of users.



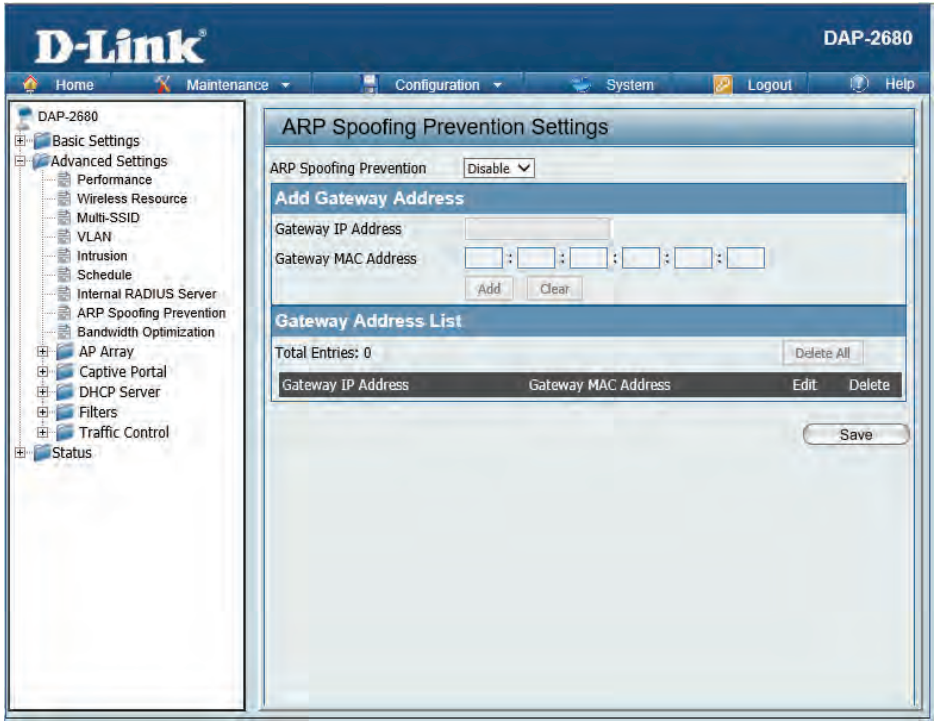
ARP Spoofing Prevention

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.

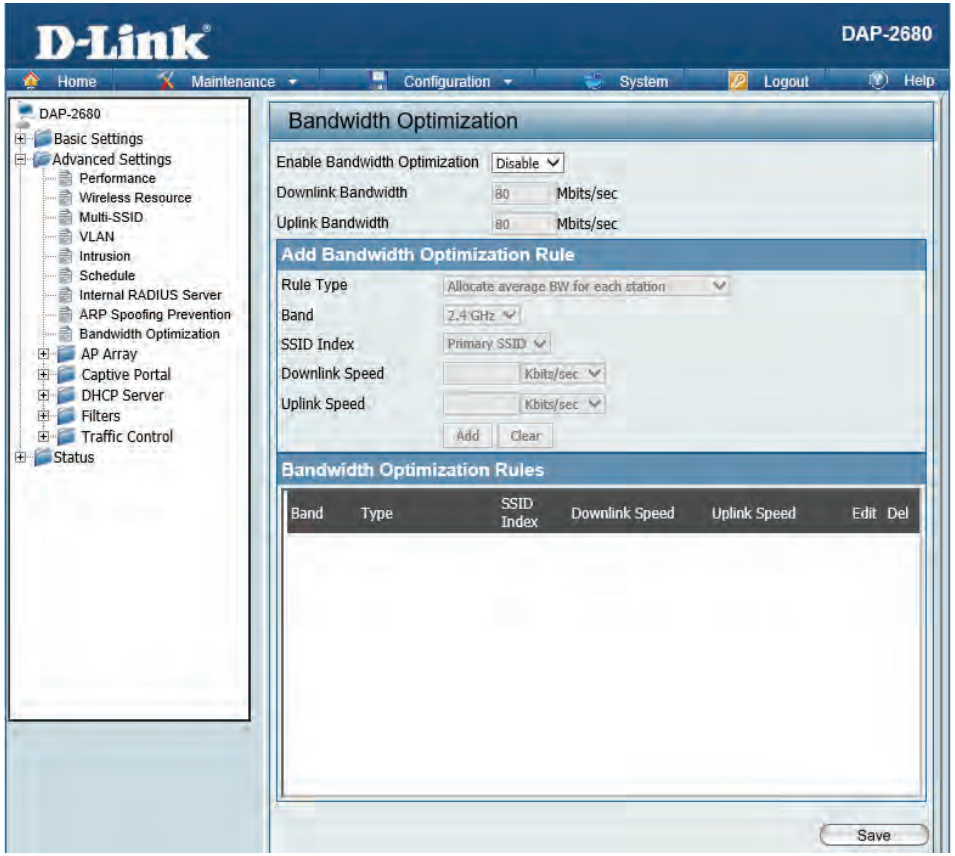
Gateway IP Address: Enter a gateway IP address.

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 11b/g/n and 11a/n client are 10%/20%/70% ; 20%/80%. AP will distribute different bandwidth for 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**.

Band: Use the drop-down menu to toggle the wireless band between 2.4GHz and 5GHz.

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

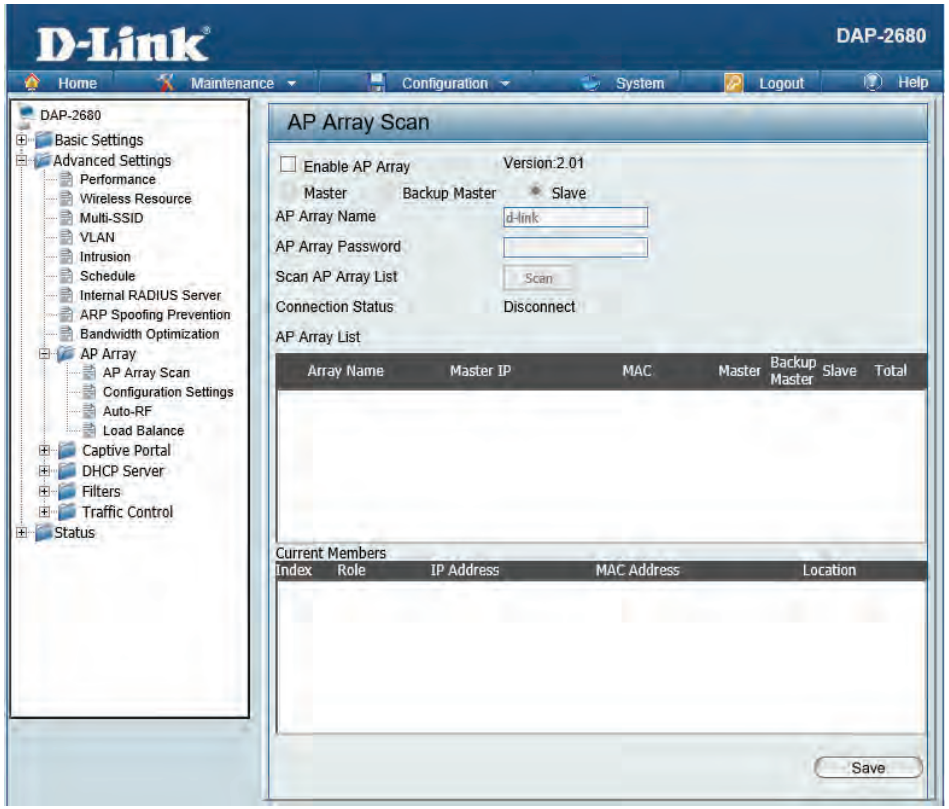
Downlink Speed: Enter the limitation of the downloading speed in either Kbits/sec or Mbits/sec for the rule.

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-2682 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.

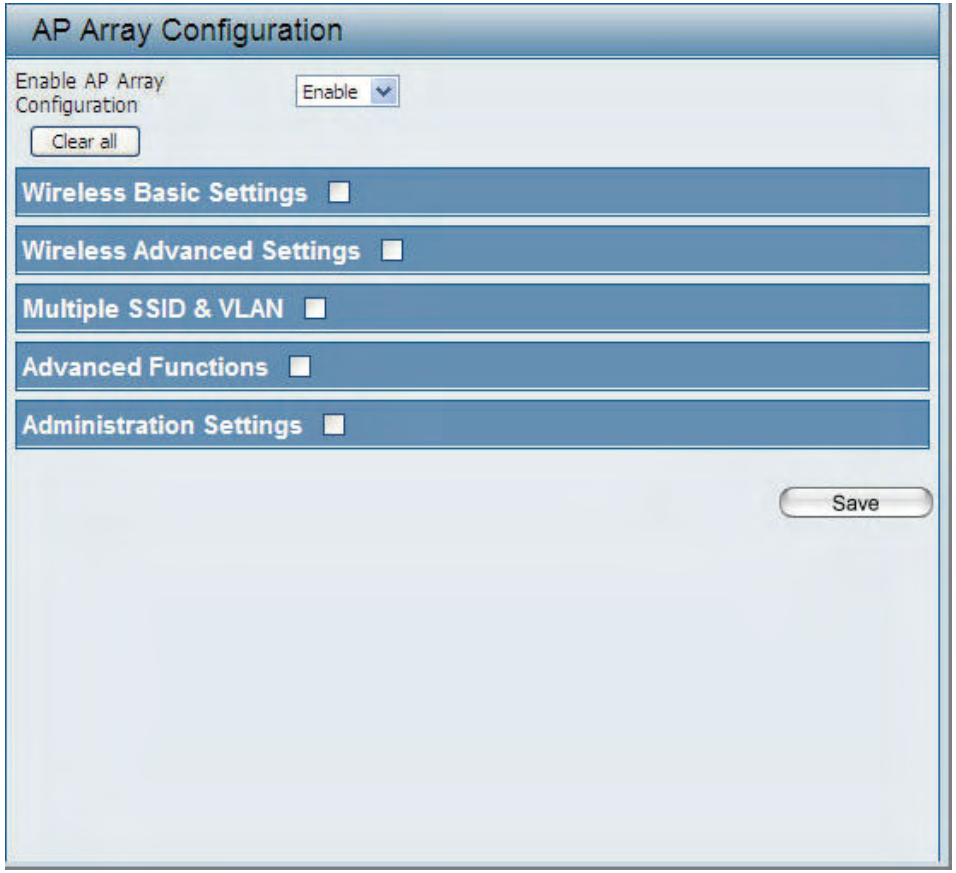
Wireless Basic Settings: Select this option to specify the basic wireless settings that the APs in the group will inherit.

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.

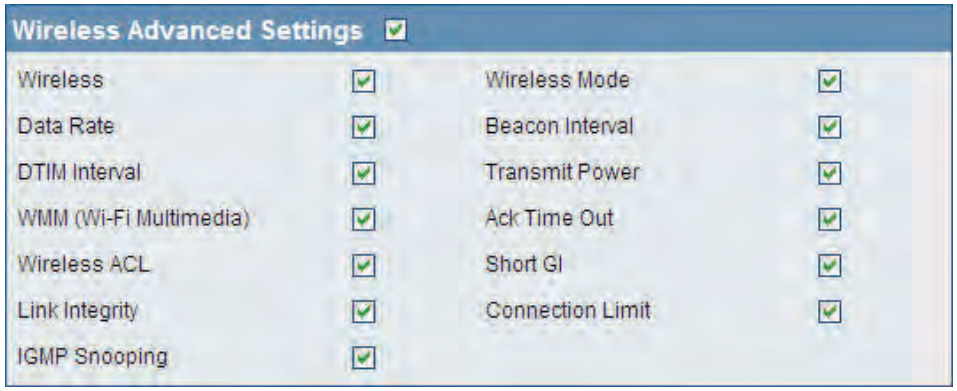
Channel Width: Select this option to use the same channel width.

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.

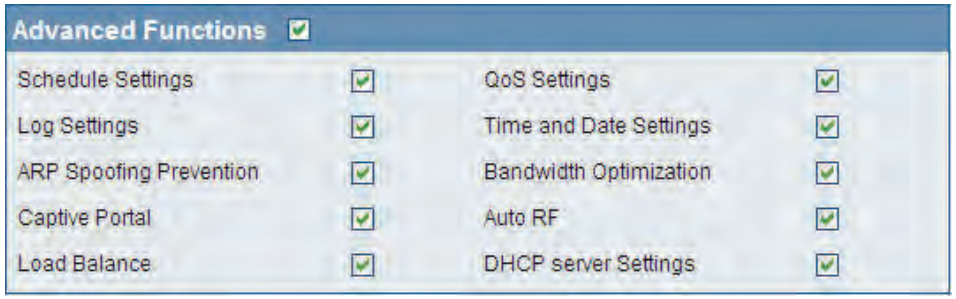
Advanced Functions

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.

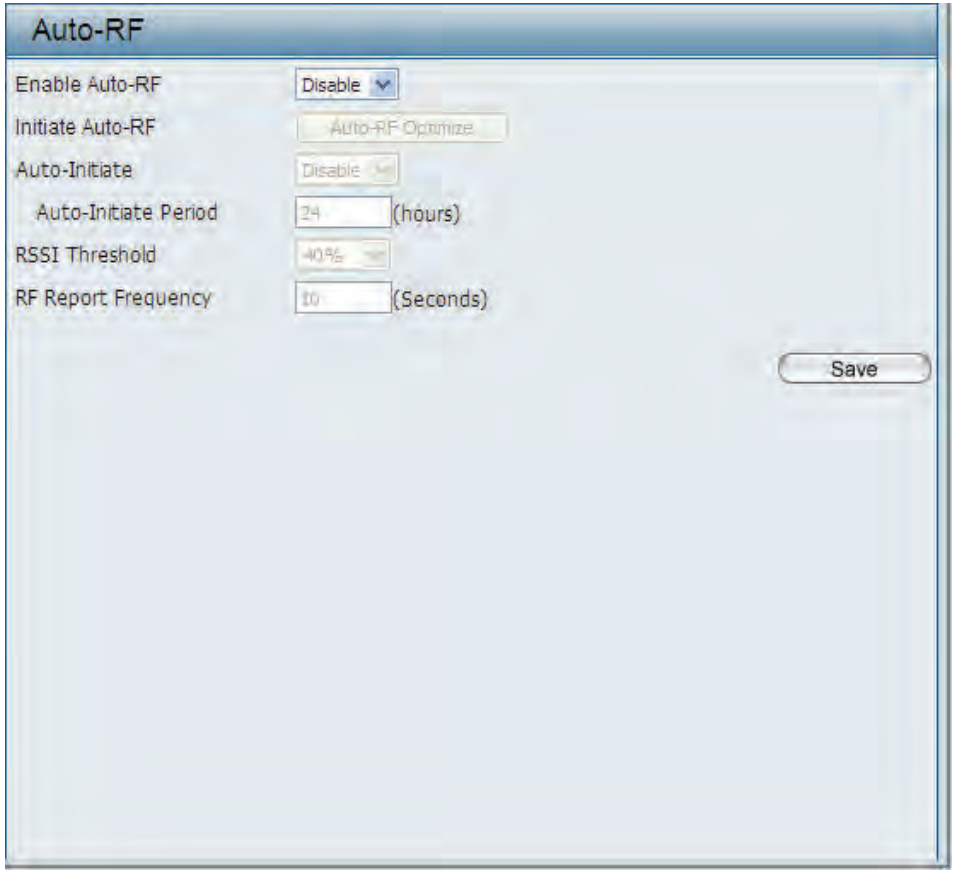
Console Settings: Select this option to use the same console settings.

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%**.

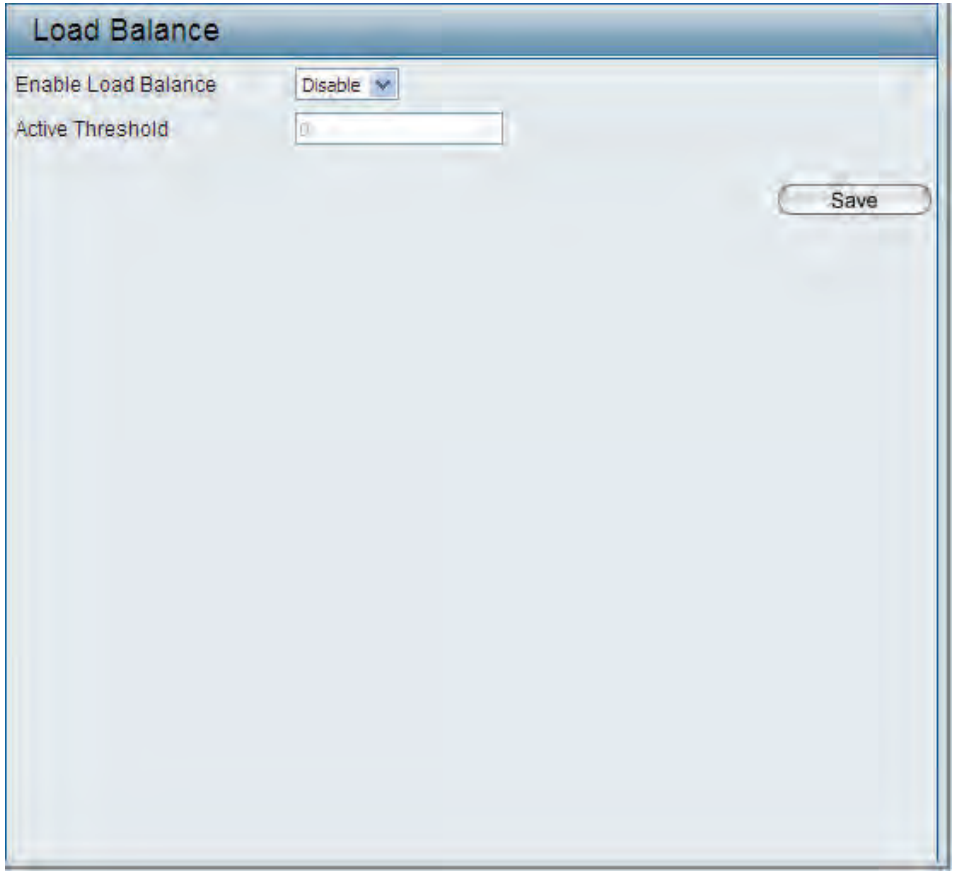
RF Report Frequency: Enter the RF report frequency value here.

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.

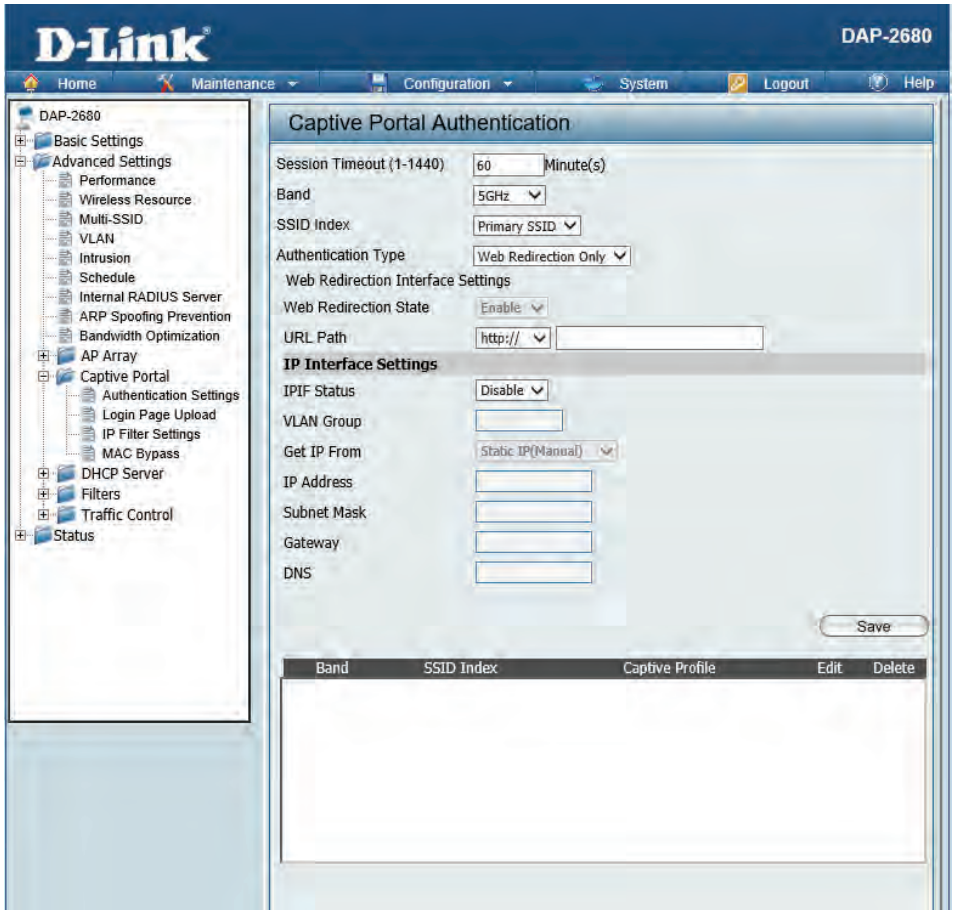
Active Threshold: Enter the active threshold value here.



Captive Portal

Authentication Settings-Web Redirection Only

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting Web Redirection Only as the Authentication Type, we can configure the redirection website URL that will be applied to each wireless client in this network.



Session timeout(1-1440) : Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

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

Web Redirection State : Default setting is Enable when select Web Redirection Only.

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

IPIF Status : Select to Enable or Disable the Captive Portal with its IP interface feature here.

VLAN Group : Enter the VLAN Group ID here.

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-2682. 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 : Assign a static IP address that is within the IP address range of your network.

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

Gateway : Enter the IP address of the gateway/router in your network.

DNS : Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

Authentication Settings- Username/Password

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting Username/Password as the Authentication Type, we can configure the Username/Password authentication that will be applied to each wireless client in this network.

Session timeout(1-1440) : Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

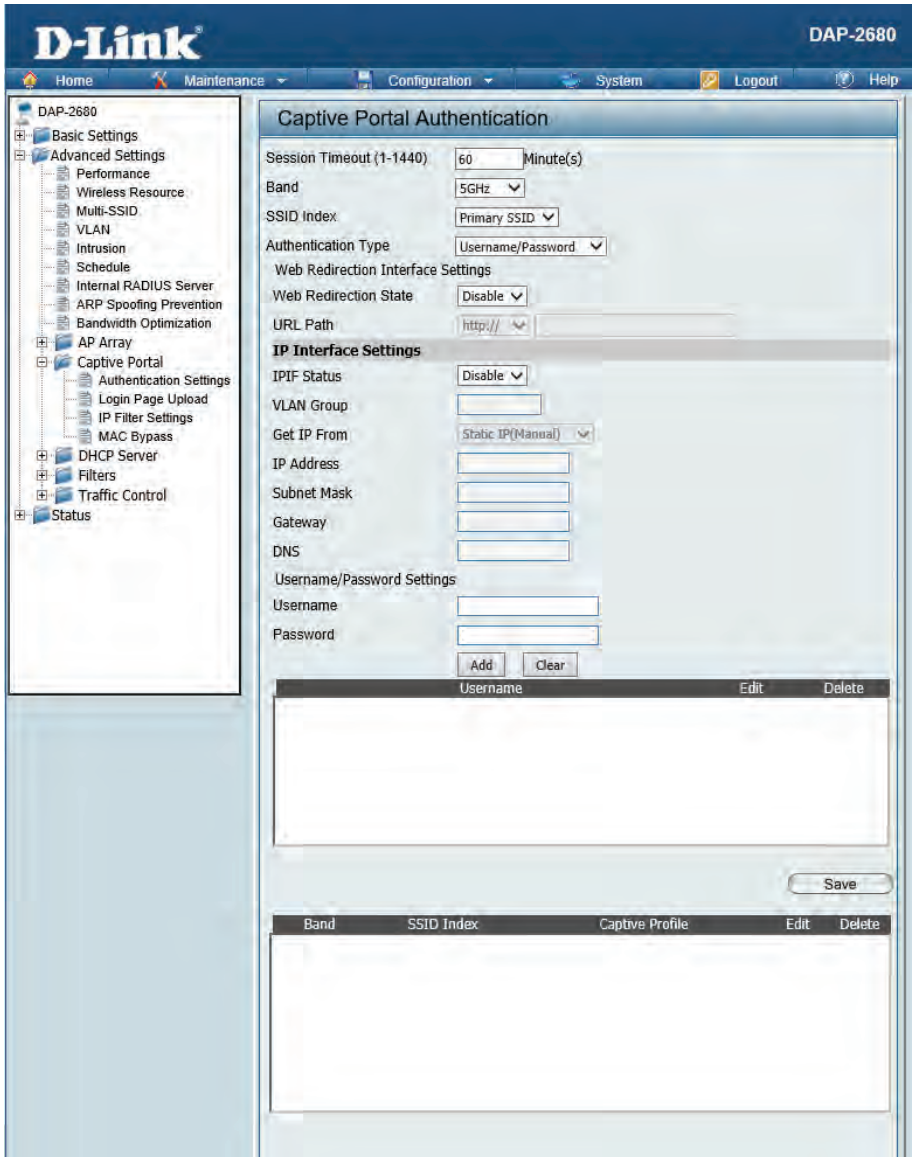
Authentication Type : Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Username/Password option.

Web Redirection State : Default is Disable or select Enable to enable the website redirection feature.

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

IPIF Status : Select to Enable or Disable the Captive Portal with its IP interface feature here.

VLAN Group : Enter the VLAN Group ID here.



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-2682. 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 : Assign a static IP address that is within the IP address range of your network.

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

Gateway : Enter the IP address of the gateway/router in your network.

DNS : Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

Username: Enter the username for the new account here.

Password: Enter the password for the new account here.

Authentication Settings- Passcode

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting Passcode as the Authentication Type, we can configure the Passcode authentication that will be applied to each wireless client in this network.

Session timeout(1-1440) : Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

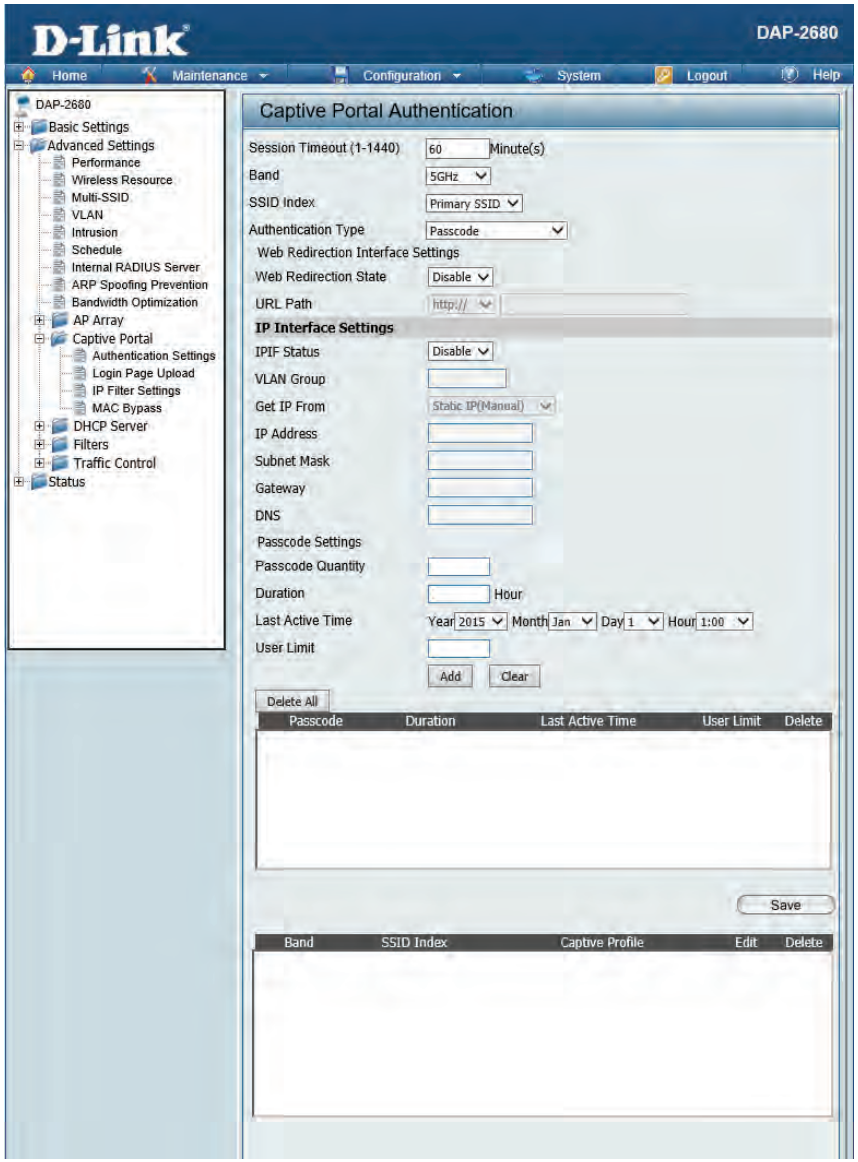
Authentication Type : Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Passcode option.

Web Redirection State : Default is Disable or select Enable to enable the website redirection feature.

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

IPIF Status : Select to Enable or Disable the Captive Portal with its IP interface feature here.

VLAN Group : Enter the VLAN Group ID here.



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-2682. 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 : Assign a static IP address that is within the IP address range of your network.

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

Gateway : Enter the IP address of the gateway/router in your network.

DNS : Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

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

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

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

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

Authentication Settings- Remote RADIUS

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting Remote RADIUS as the Authentication Type, we can configure the Remote RADIUS authentication that will be applied to each wireless client in this network.

Session timeout(1-1440) : Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

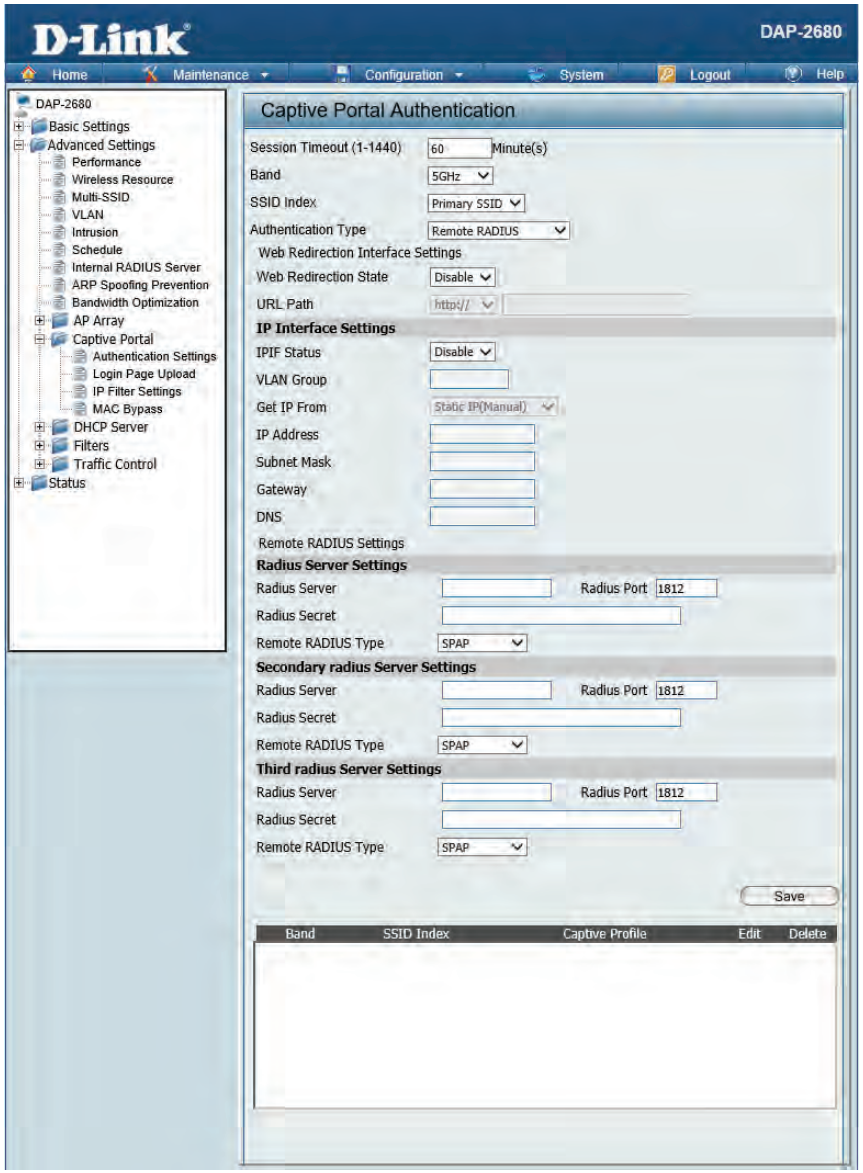
Authentication Type : Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Remote RADIUS option.

Web Redirection State : Default is Disable or select Enable to enable the website redirection feature.

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

IPIF Status : Select to Enable or Disable the Captive Portal with its IP interface feature here.

VLAN Group : Enter the VLAN Group ID here.



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-2682. 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 : Assign a static IP address that is within the IP address range of your network.

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

Gateway : Enter the IP address of the gateway/router in your network.

DNS : Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

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

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

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

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

Authentication Settings- LDAP

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting LDAP as the Authentication Type, we can configure the LDAP authentication that will be applied to each wireless client in this network.

Session timeout(1-1440) : Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

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

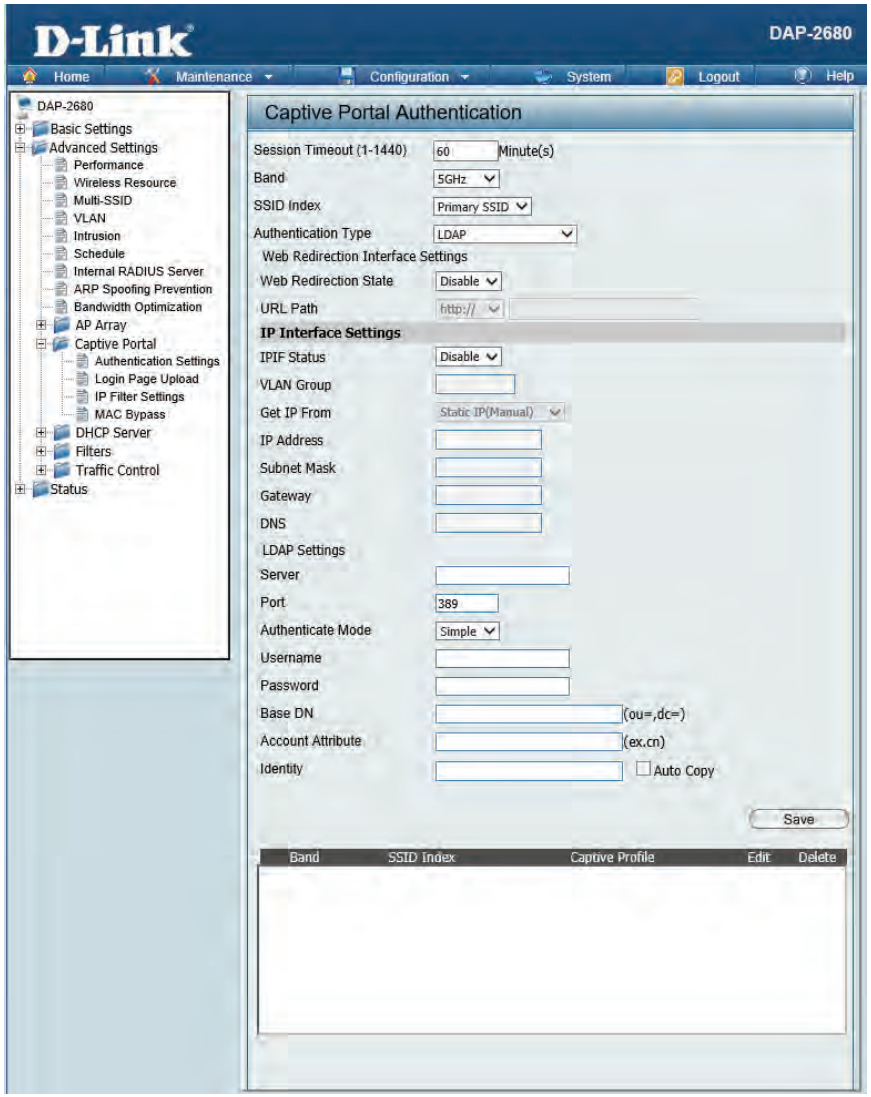
Web Redirection State : Default is Disable or select Enable to enable the website redirection feature.

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

IPIF Status : Select to Enable or Disable the Captive Portal with its IP interface feature here.

VLAN Group : Enter the VLAN Group ID here.

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-2682. 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 : Assign a static IP address that is within the IP address range of your network.

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

Gateway : Enter the IP address of the gateway/router in your network.

DNS : Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

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

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting POP3 as the Authentication Type, we can configure the POP3 authentication that will be applied to each wireless client in this network.

Session timeout(1-1440) : Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

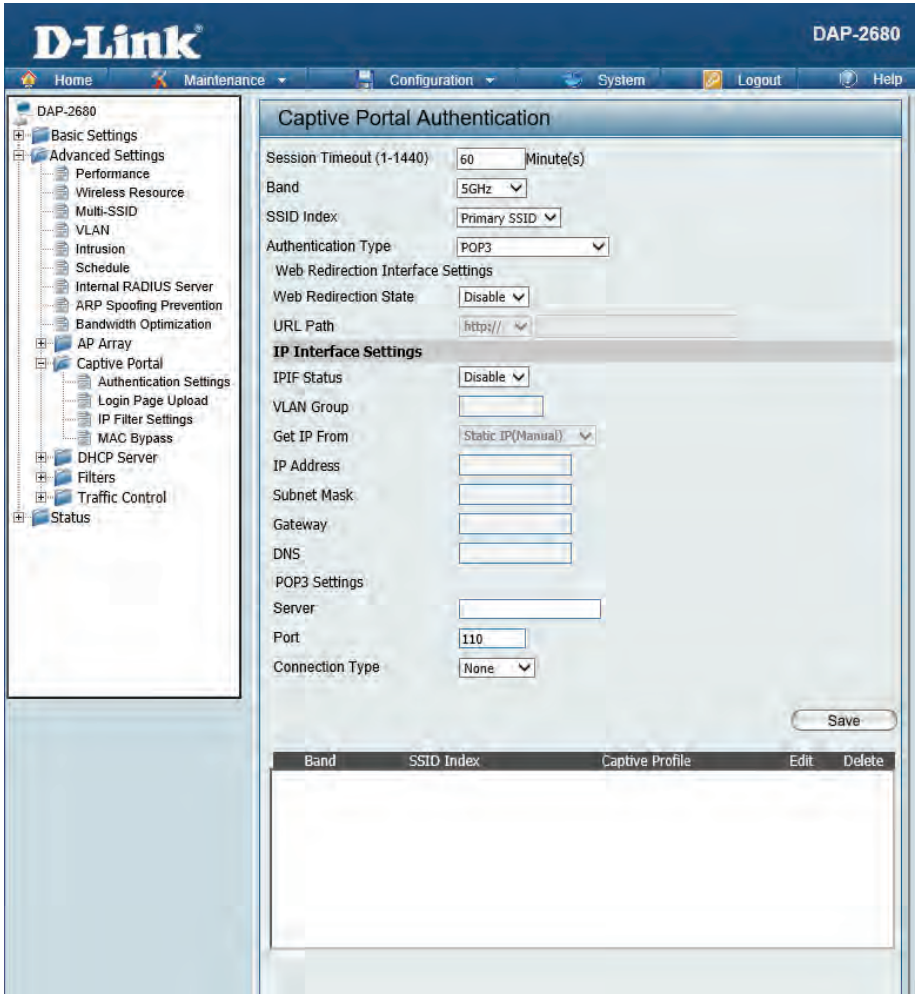
Authentication Type : Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the POP3 option.

Web Redirection State : Default is Disable or select Enable to enable the website redirection feature.

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

IPIF Status : Select to Enable or Disable the Captive Portal with its IP interface feature here.

VLAN Group : Enter the VLAN Group ID here.



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-2682. 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 : Assign a static IP address that is within the IP address range of your network.

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

Gateway : Enter the IP address of the gateway/router in your network.

DNS : Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

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

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

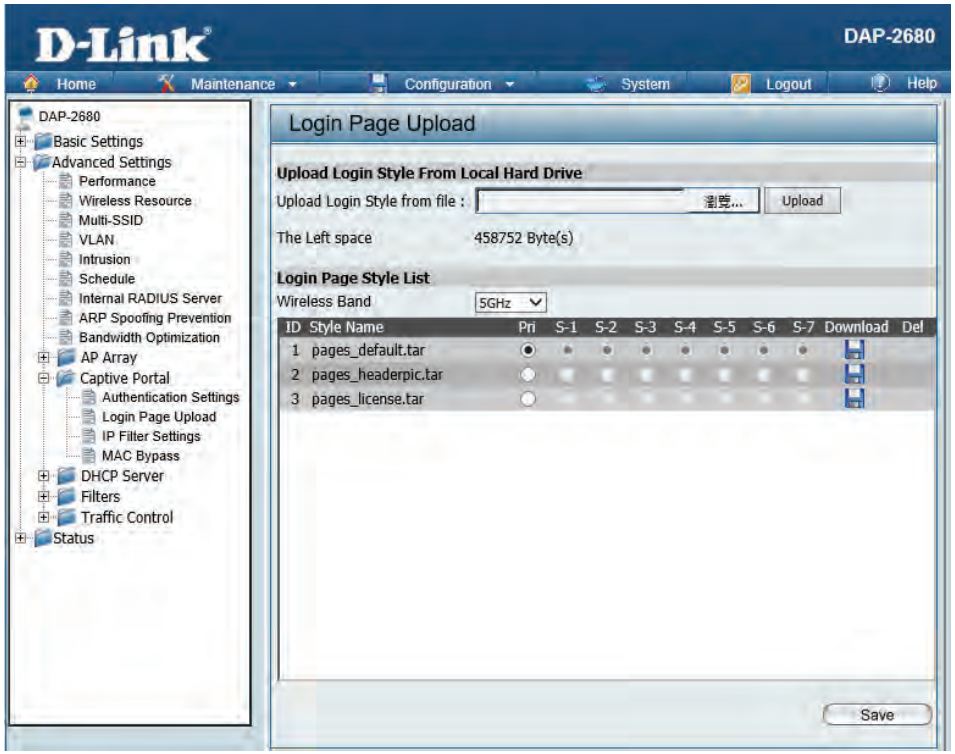
Connection Type: Select the connection type here. Options to choose from are None and SSL/TLS.

Login Page Upload

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

Upload Login Style From Local Hard Drive: In this field the path to the login style file, that will be uploaded, will be displayed. Alternatively, the path can be manually entered here.

Login Page Style List : Select the wireless band and login style that will be used in each SSID here. Click Download button to download the template file for login page and Click Del button to delete the template file.



IP Filter Settings

Enter the IP address or network address that will be used in the IP filter rule. For example, an IP address like 192.168.70.66 or a network address like 192.168.70.0. This IP address or network will be inaccessible to wireless clients in this network.

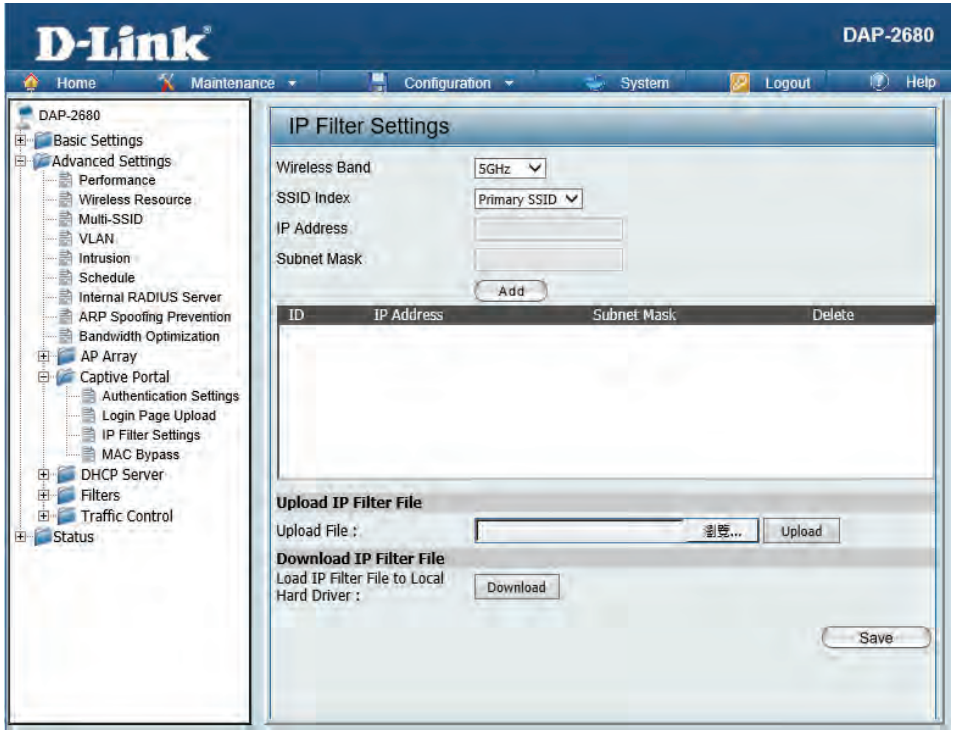
Wireless Band : Wireless Band : Select 2.4GHz or 5GHz.

IP Address: IP Address: Enter the IP address or network address

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

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

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



MAC Bypass

The DAP-2682 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.

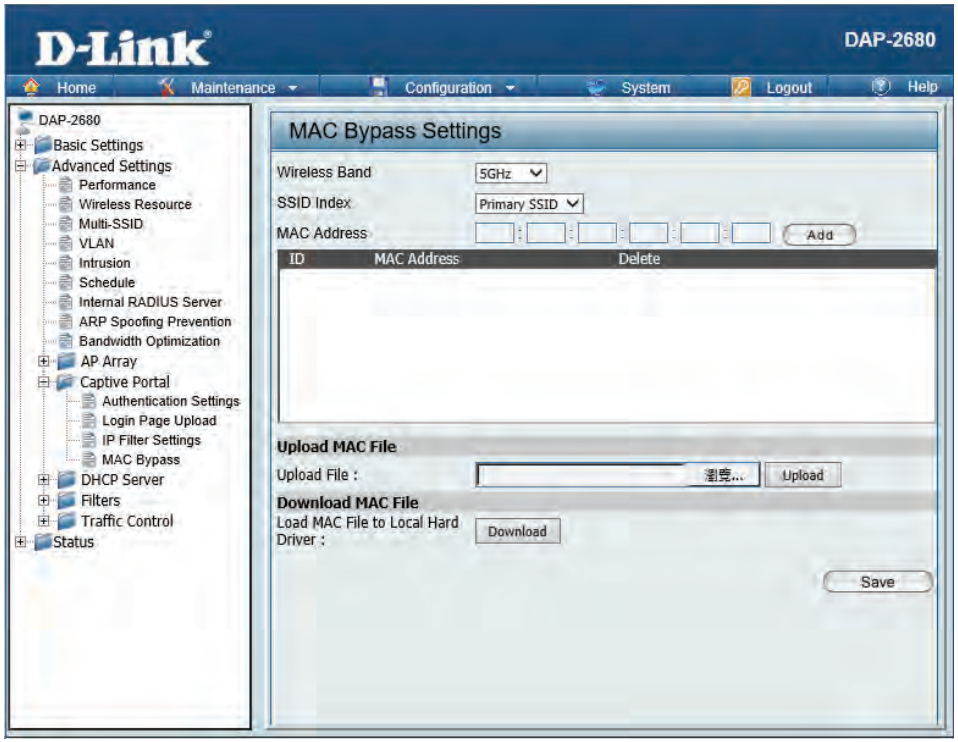
SSID Index: Select the SSID for MAC Bypass.

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.

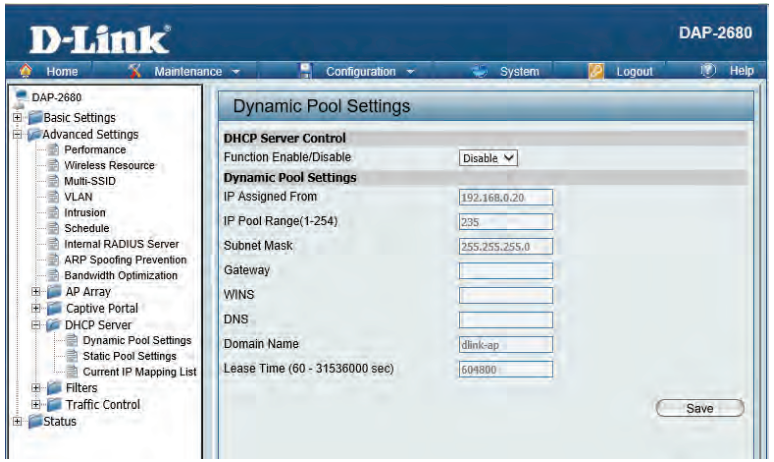
Load MAC File to Local Hard Driver: To download MAC bypass list file, click Download and to save the MAC bypass list.



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. If needed or required in the network, the DAP-2682 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-2682 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 subnet mask 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.

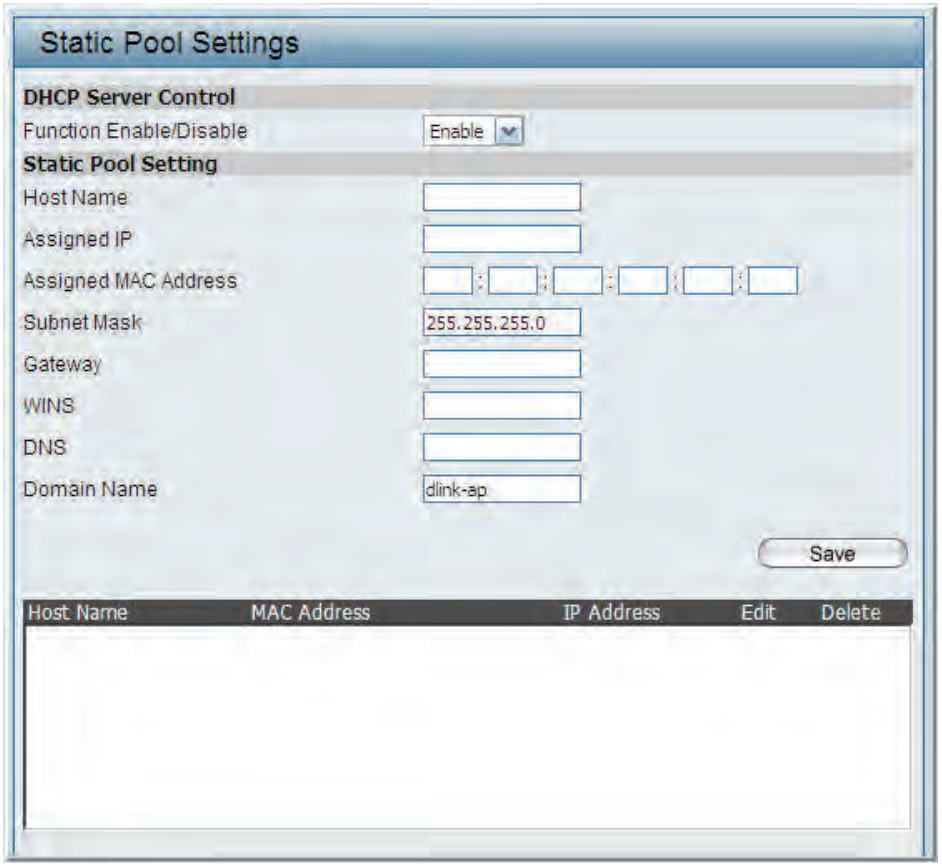
DNS: Enter the IP address of the Domain Name System (DNS) server. The DNS server translates domain names such as www.dlink.com into IP addresses.

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.



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-2682 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 subnet mask of the IP address specified in the "IP Assigned From" field.

Gateway: Specify the Gateway address for the wireless network.

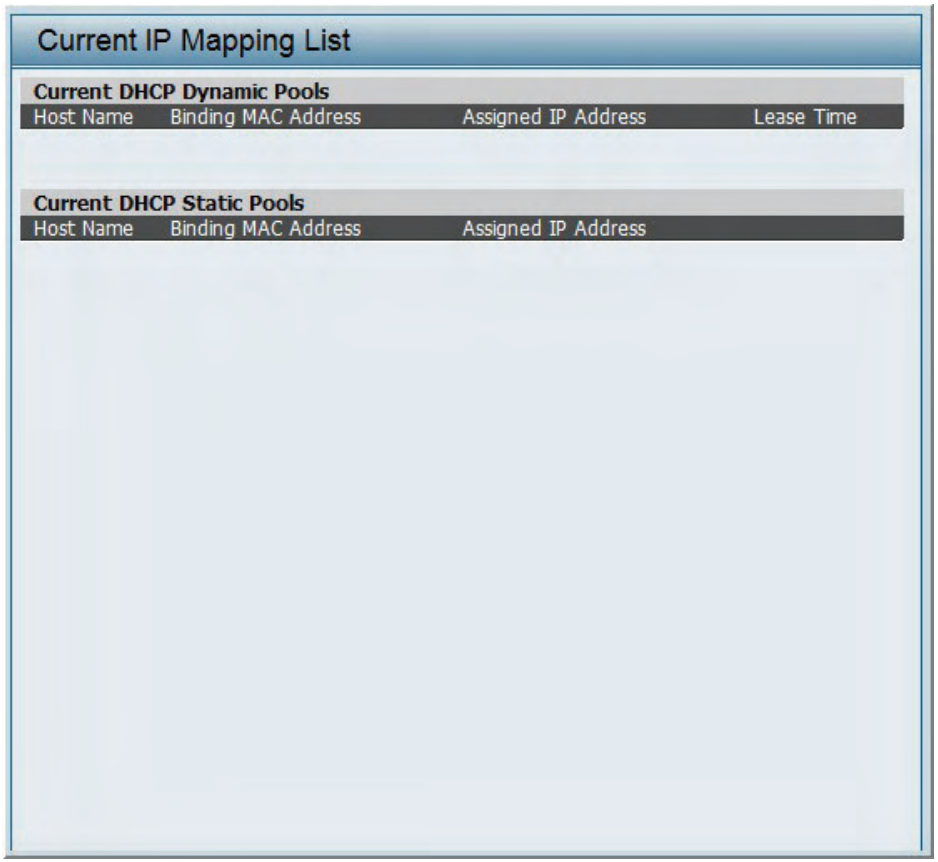
WINS: Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.

DNS: Enter the DNS server address for your wireless network.

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.

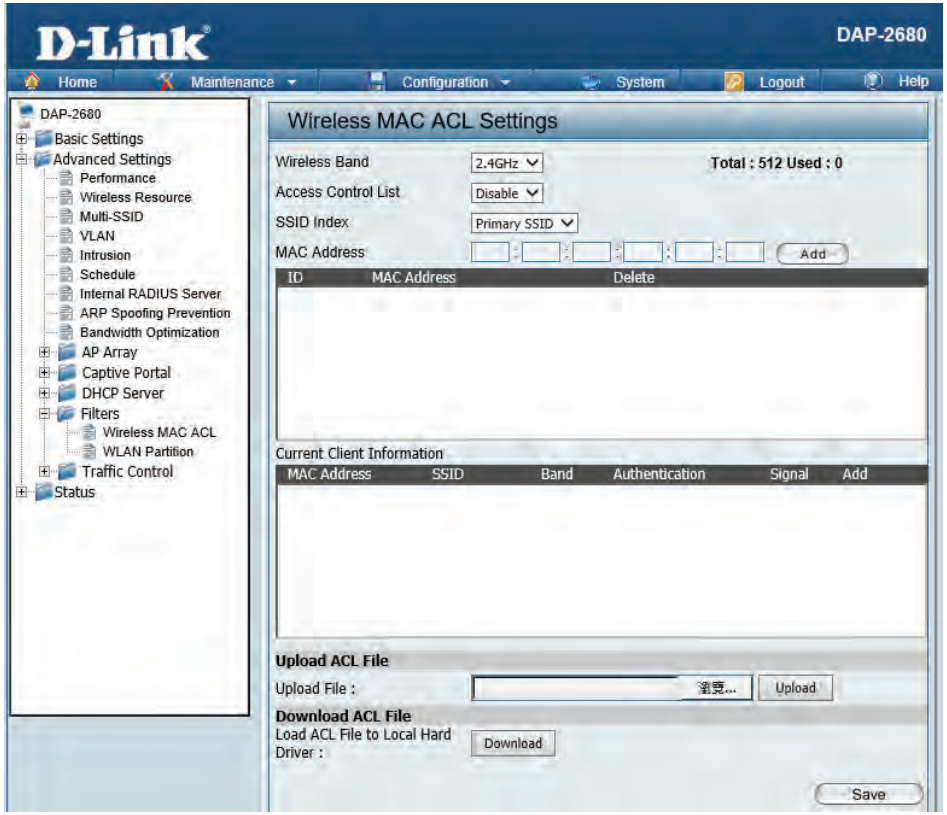
Binding MAC Address: The MAC address of a device on the network that is assigned an IP address from the DHCP dynamic pool.

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

Filters

Wireless MAC ACL

This page allows the user to configure Wireless MAC ACL settings for access control.



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.

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

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

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

WLAN Partition

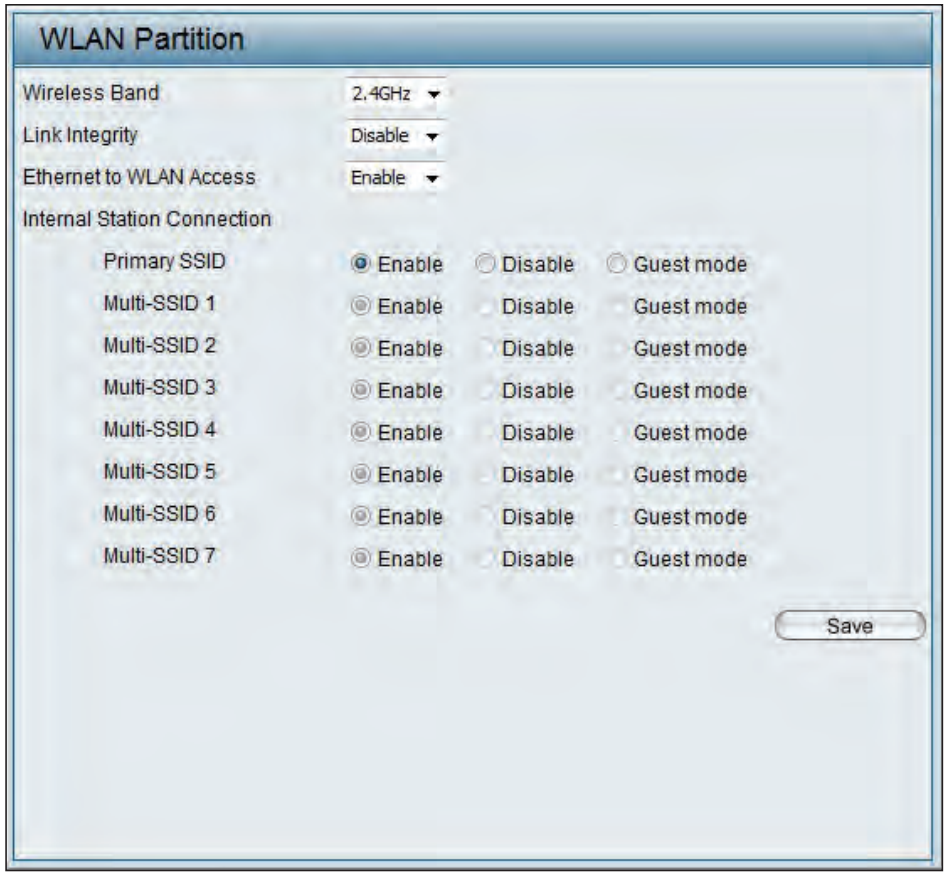
This page allows the user to configure a WLAN Partition.

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 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.



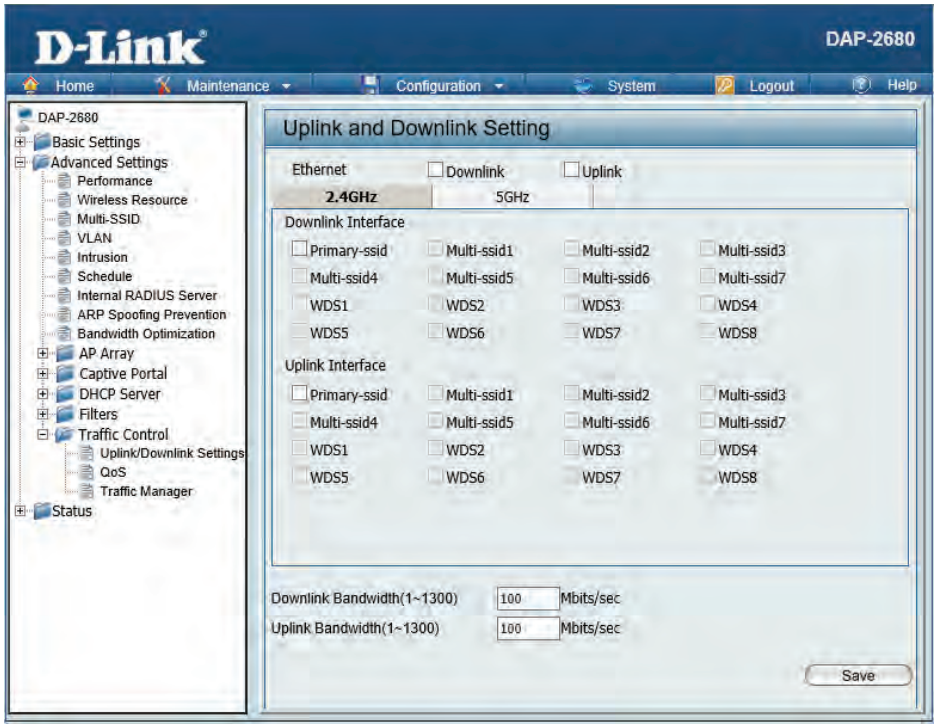
Traffic Control

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



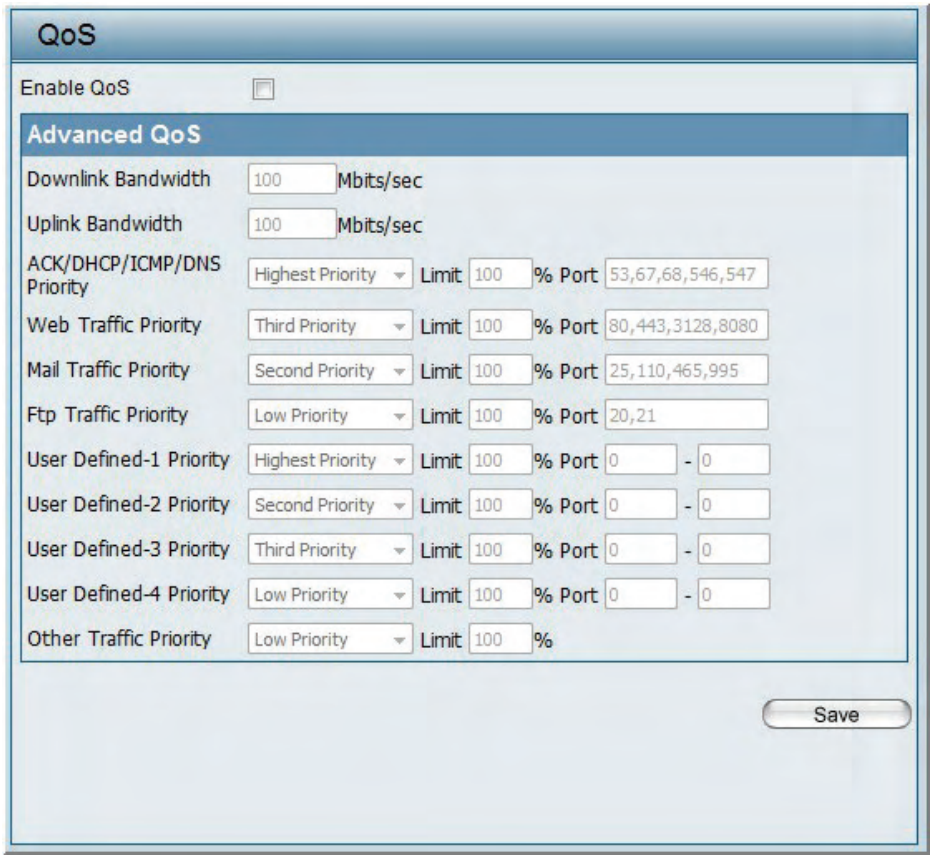
QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications. The DAP-2682 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: Downlink Bandwidth: The downlink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

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



Traffic Manager

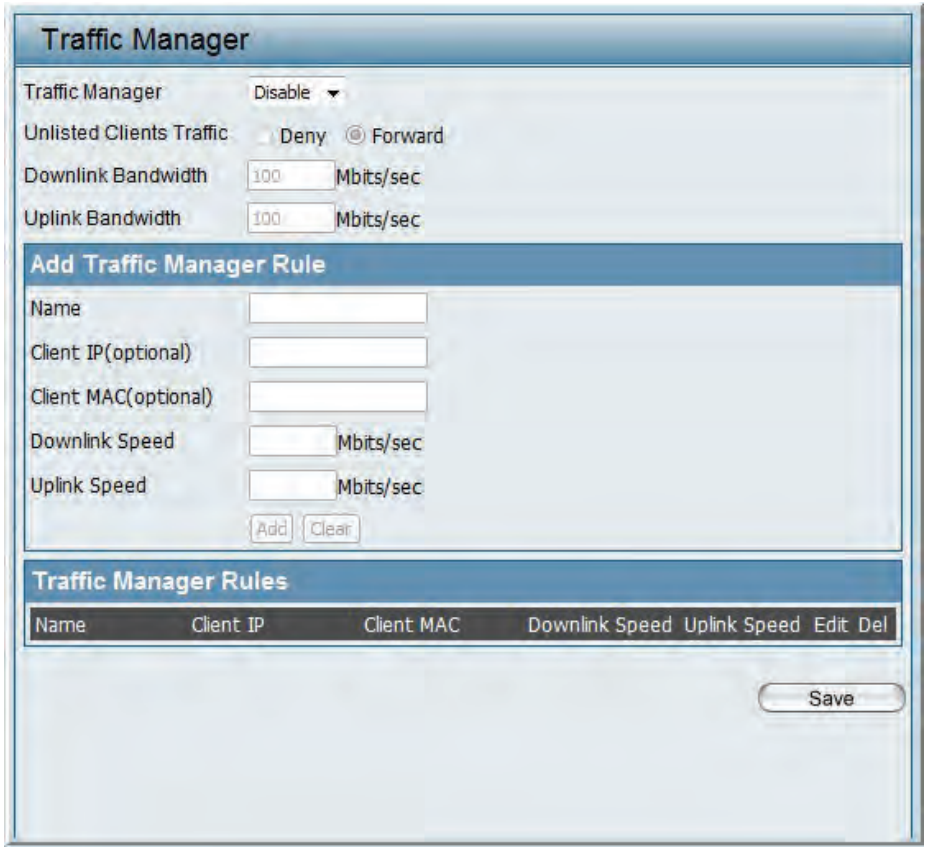
The traffic manager feature allows users to create traffic management rules that specify how to deal with listed client traffic and specify downlink/ uplink speed for new traffic manager rules. Click the **Save** button to let your changes take effect.

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.

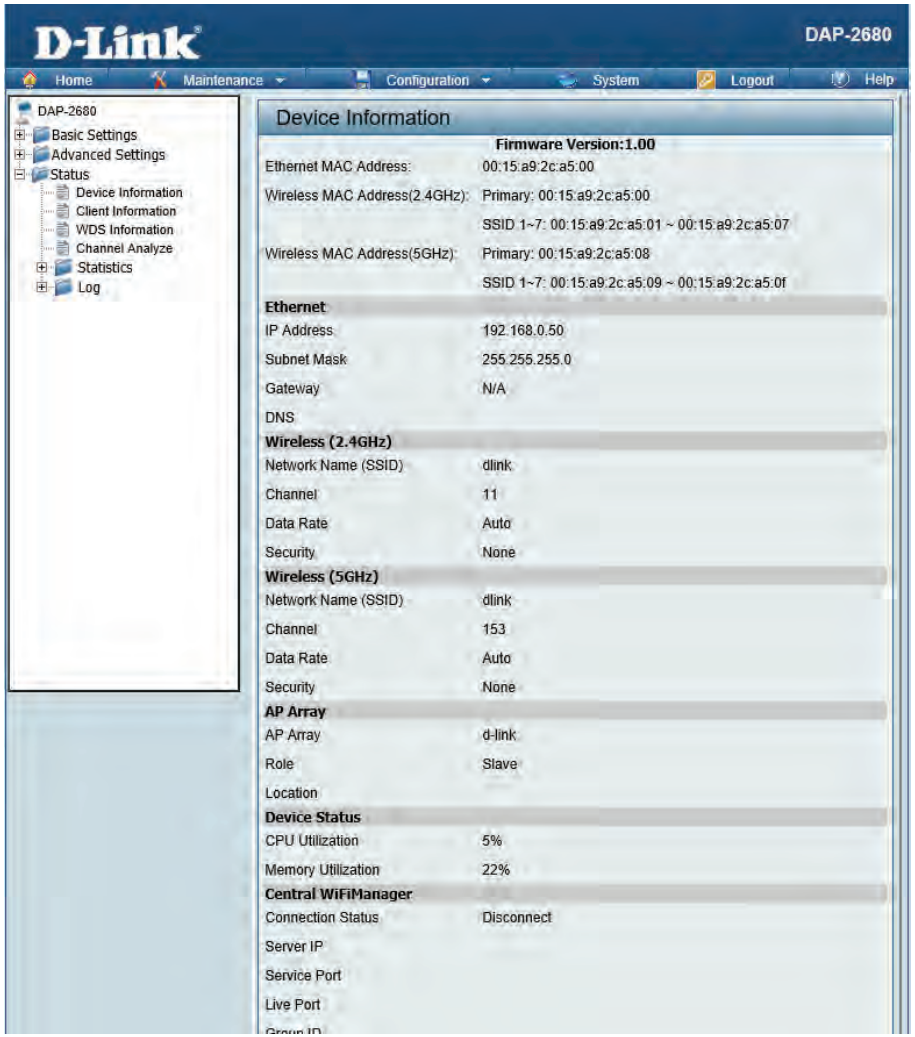
Downlink Bandwidth: The downlink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

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



Status

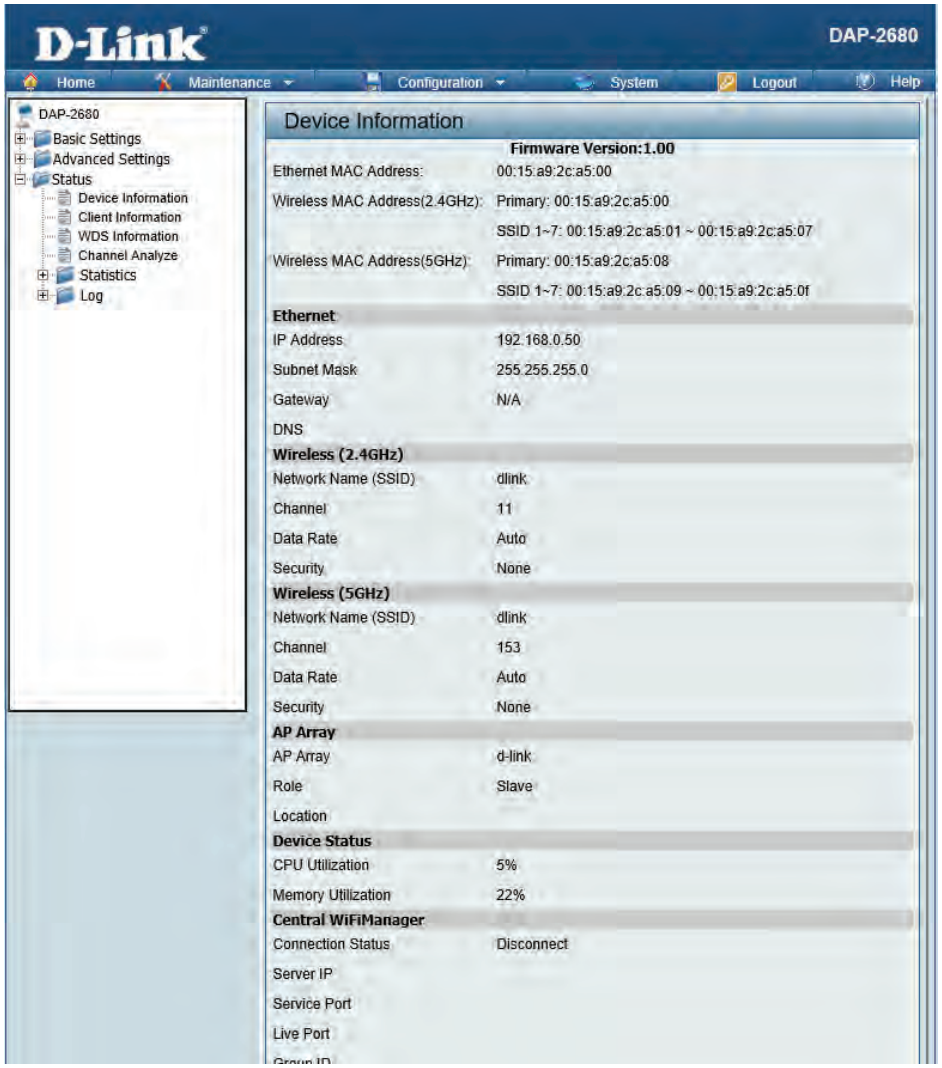
In the Status Section the user can monitor and view configuration settings of the access point. Here the user can also view statistics about client information, WDS information and more. The following pages will explain settings found in the Status section in more detail.



Device Information

This page displays the current information like firmware version, Ethernet and wireless parameters, as well as the information regarding CPU and memory utilization.

Device Information: This read-only window displays the configuration settings of the DAP-2682, including the firmware version and the device's MAC address.



Client Information

This page displays the associated clients SSID, MAC, band, authentication method, signal strength, and power saving mode for the DAP-2682 network.

Client Information: This window displays the wireless client information for clients currently connected to the DAP-2682.

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.

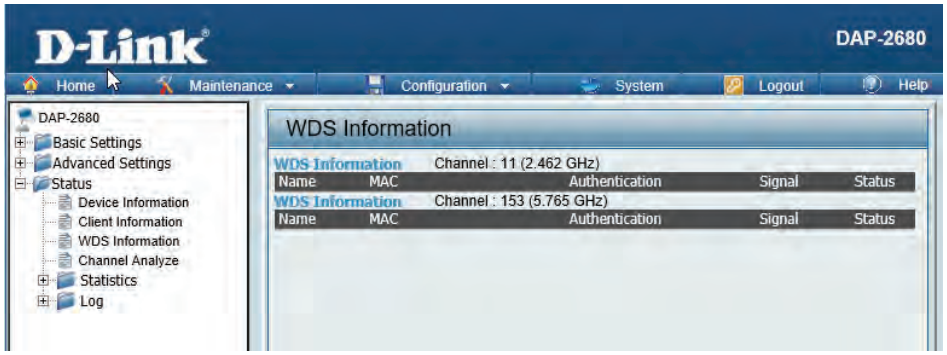
Authentication: Displays the type of authentication being used.

RSSI: Displays the client's signal strength.

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

WDS Information Page

This page displays the access points SSID, MAC, band, authentication method, signal strength, and status for the DAP-2682's Wireless Distribution System network.



WDS Information: This window displays the Wireless Distribution System information for clients currently connected to the DAP-2682.

Name: Displays the SSID of the client.

MAC: Displays the MAC address of the client.

Authentication: Displays the type of authentication being used.

Signal: Displays the client's signal strength.

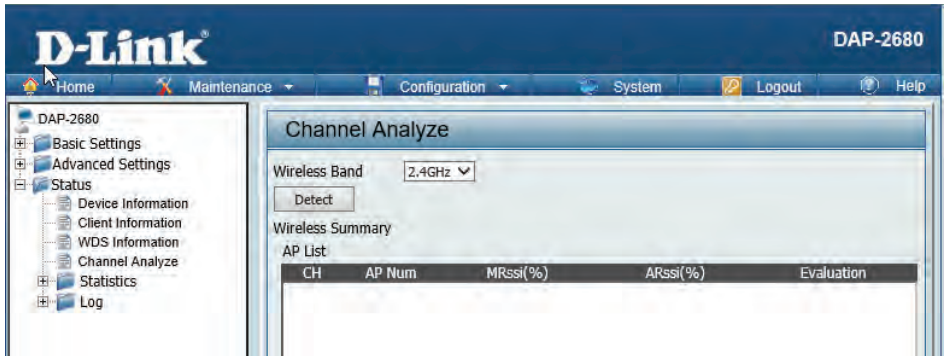
Status: Displays the status of the power saving feature.

Channel Analyze

Wireless Band: Select either 2.4Ghz or 5GHz.

Detect: Click the Detect button to scan.

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

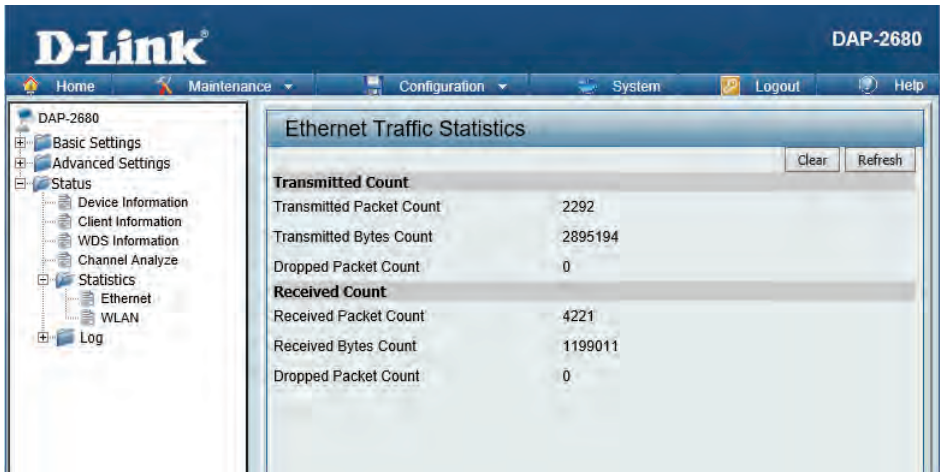


Stats Page

Ethernet Traffic Statistics

Displays wired interface network traffic information.

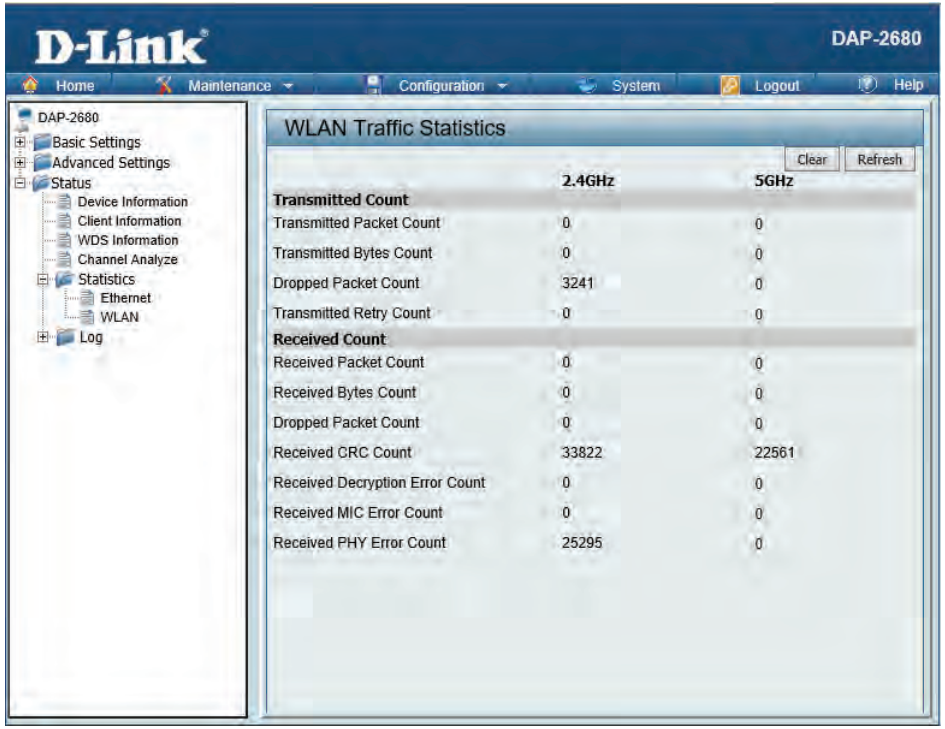
Ethernet Traffic Statistics: This page displays transmitted and received count statistics for packets and bytes.



WLAN Traffic Statistics

Displays throughput, transmitted frame, received frame, and WEP frame error information for the AP network.

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

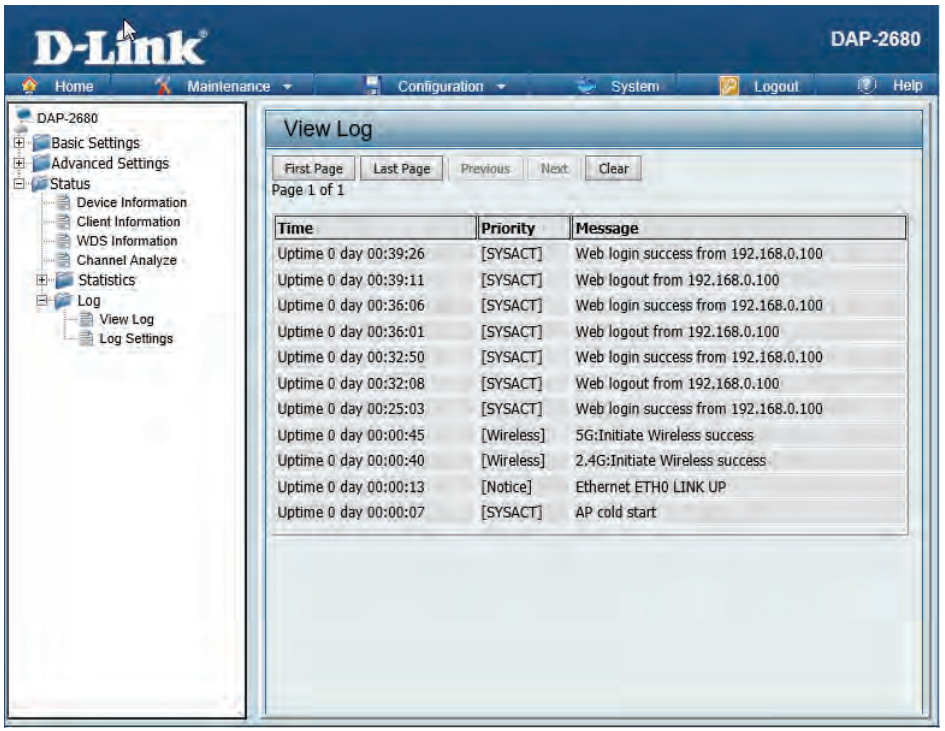


Log

View Log

The AP's embedded memory holds logs here. 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.

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

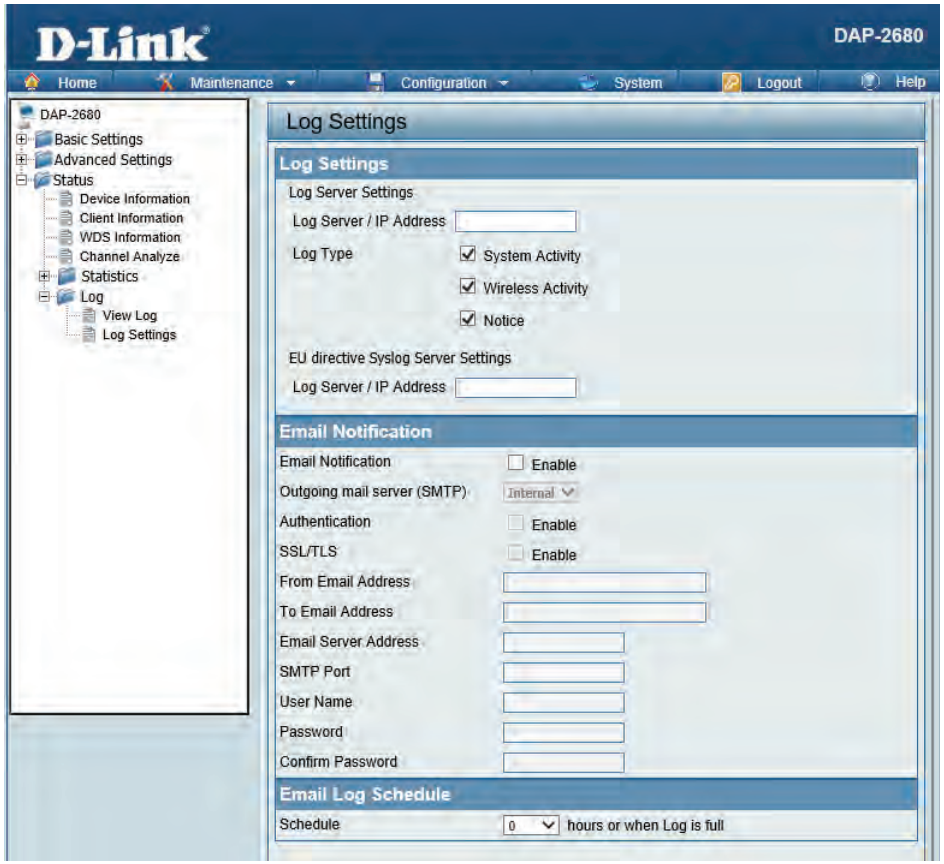
Enter the log server's IP address to send the log to that server. Check or uncheck System Activity, Wireless Activity, or Notice to specify what kind of log type you want it to log.

Log Server/IP Address: Enter the IP address of the server you would like to send the DAP-2682 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.

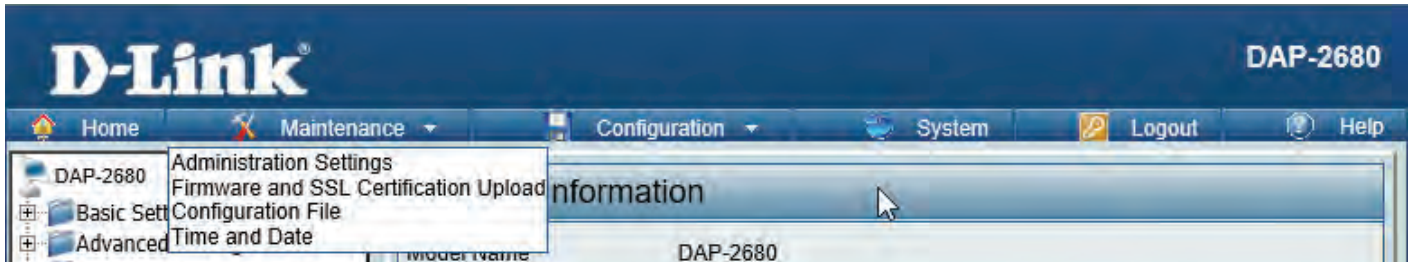
E-mail Notification: Support Simple Mail Transfer Protocol for log schedule and periodical change key. It can not support Gmail SMTP port 465. Please set to Gmail SMTP port 25 or 587.

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



Maintenance Section

In the Status Section the user can monitor and view configuration settings of the access point. Here the user can also view statistics about client information, WDS information and more. The following pages will explain settings found in the maintenance section in more detail.



Administration

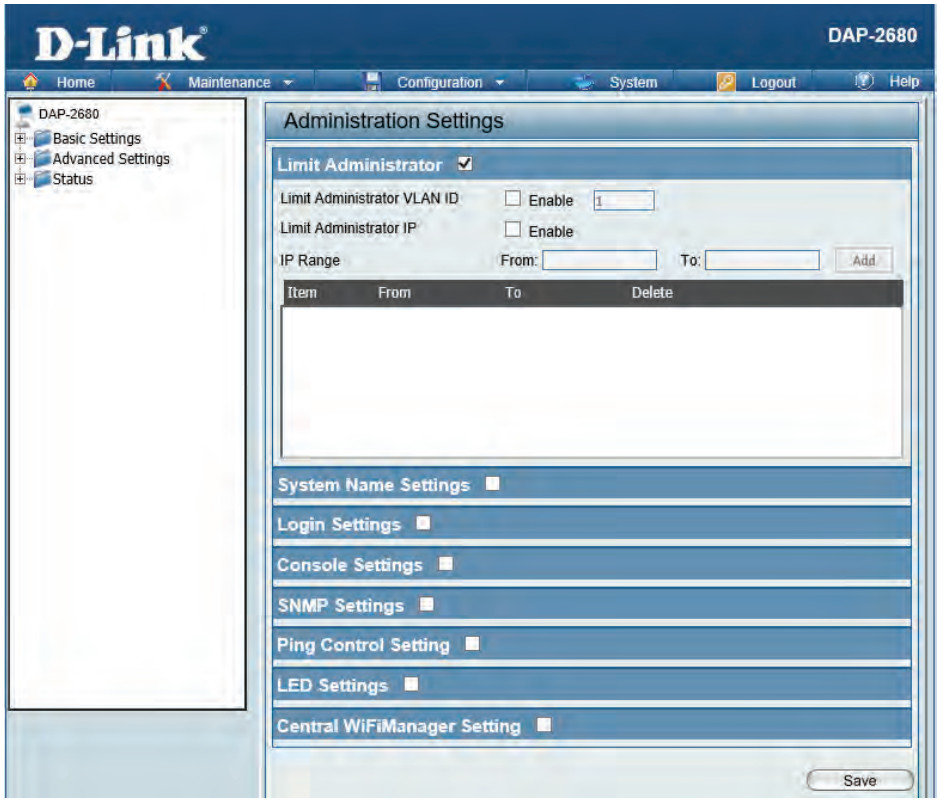
Limit Administrator

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

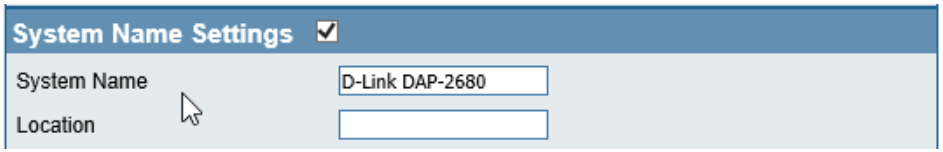
Limit Administrator IP: Check to enable the Limit Administrator IP address.

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 eight main categories display various hidden administrator parameters and settings.

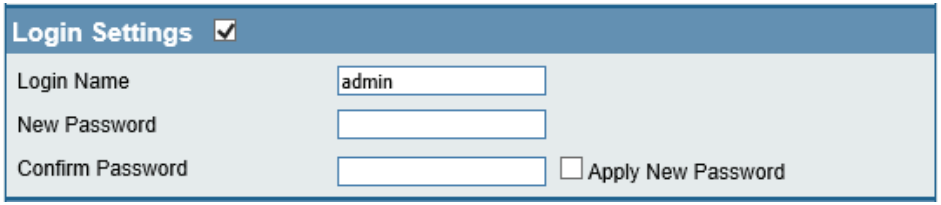


System Name: The name of the device. The default name is D-Link DAP-2682.

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

Login Settings

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



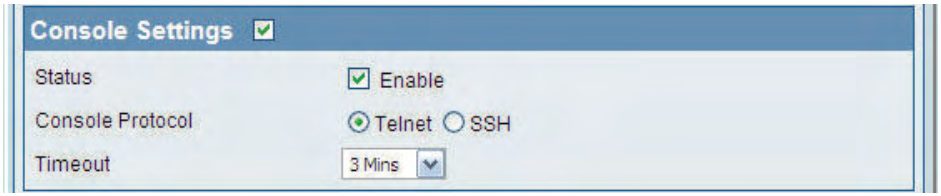
Login Name: Enter a user name. The default is admin.

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

Each of the eight 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.

Time-out: Set to 1 Min, 3 Mins, 5 Mins, 10 Mins, 15 Mins or Never.

SNMP Settings

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

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

Public Community String: Enter the public SNMP community string.

Private Community String: Enter the private SNMP community string.

Trap Status: Check the box to enable the Trap function. This is disabled by default.

Trap Server IP : Enter the Trap sever IP address.

Ping Control Setting

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

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

LED Settings

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

LED Status : Select the LED on/off you would like to use.

Central WiFiManager Settings

The Central WiFiManager section is used to create a set of APs on the Internet to be organized into a single group in order to increase ease of management. Central WiFiManager and AP Array are mutually exclusive functions.

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

Firmware and SSL Upload

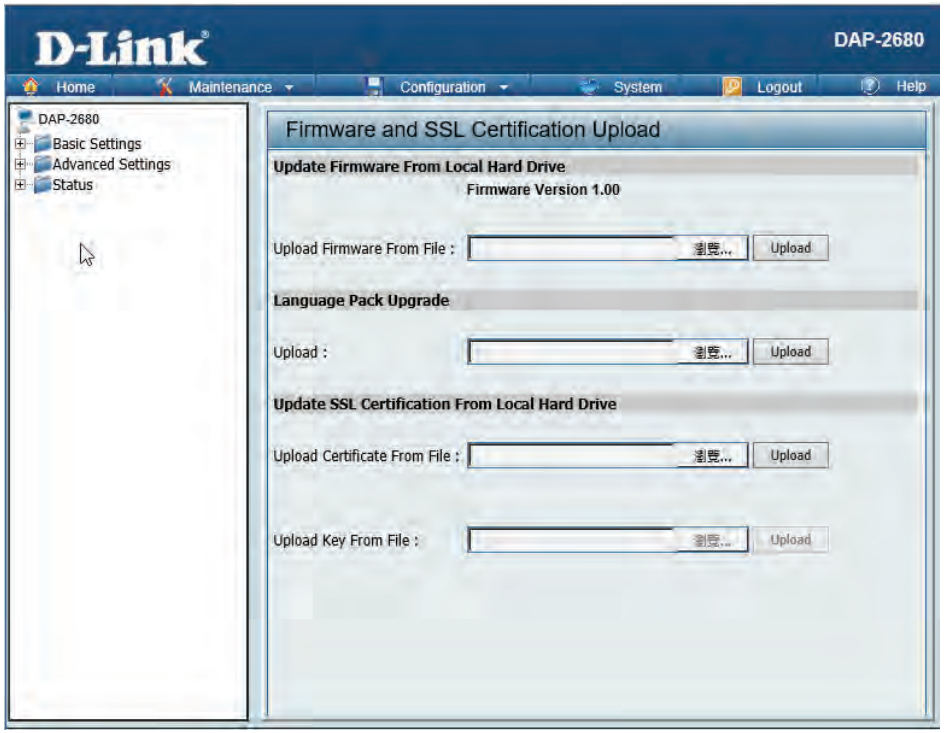
This page allows the user to perform a firmware upgrade. A Firmware upgrade is a function that upgrade the running software used by the access point. This is a useful feature that prevents future bugs and allows for new features to be added to this product. Please go to your local D-Link website to see if there is a newer version firmware available.

Firmware and SSL Certification Upload: You can upload files to the access point.

Upload Firmware from Local Hard Drive: The current firmware version is displayed above the file location field. After the latest firmware is downloaded, click on the "Choose File" button to locate the new firmware. Once the file is selected, click on the "Open" and "Upload" button to begin updating the firmware. Please don't turn the power off while upgrading.

Language Pack Upgrade : After you have downloaded a language pack to your local drive, click "Choose File." Select the language pack and click "Open" and "Upload" to complete the upgrade.

Upload SSL Certification from Local Hard Drive: After you have downloaded a SSL certification to your local drive, click "Choose File." Select the certification and click "Open" and "Upload" to complete the upgrade.



Configuration File Upload

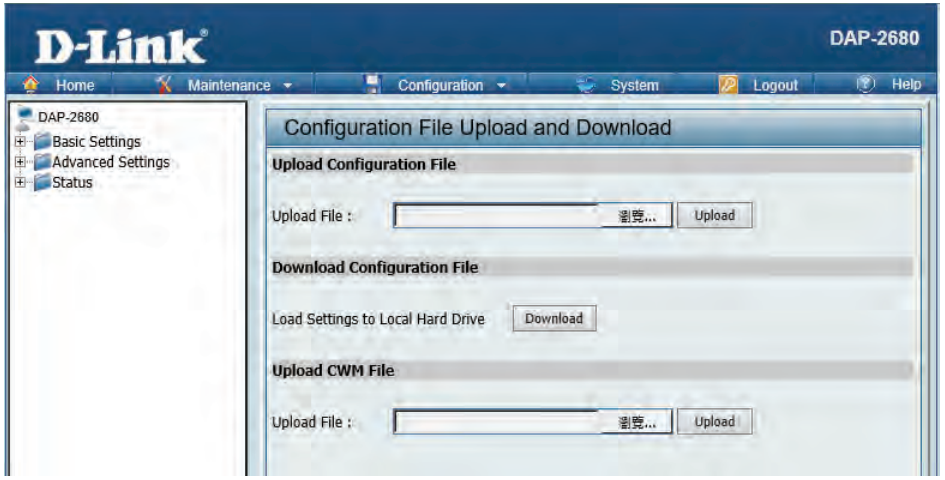
This page allows the user to backup and recover the current configuration of the access point in case of a unit failure.

Configuration File Upload and Download: You can upload and download configuration files of the access point.

Upload Configuration File: Browse to the saved configuration file you have in local drive and click "Open" and "Upload" to update the configuration.

Download Configuration File: Click "Download" to save the current configuration file to your local disk. Note that if you save one configuration file with the administrator's password now, after resetting your DAP-2682 and then updating to this saved configuration file, the password will be gone.

Upload CWM File : Browse to the saved CWM file you have in local drive and click "Open" and "Upload" to upload the CWM file .



Time and Date Settings

Enter the NTP server IP, choose the time zone, and enable or disable daylight saving time.

Current Time: Displays the current time and date settings.

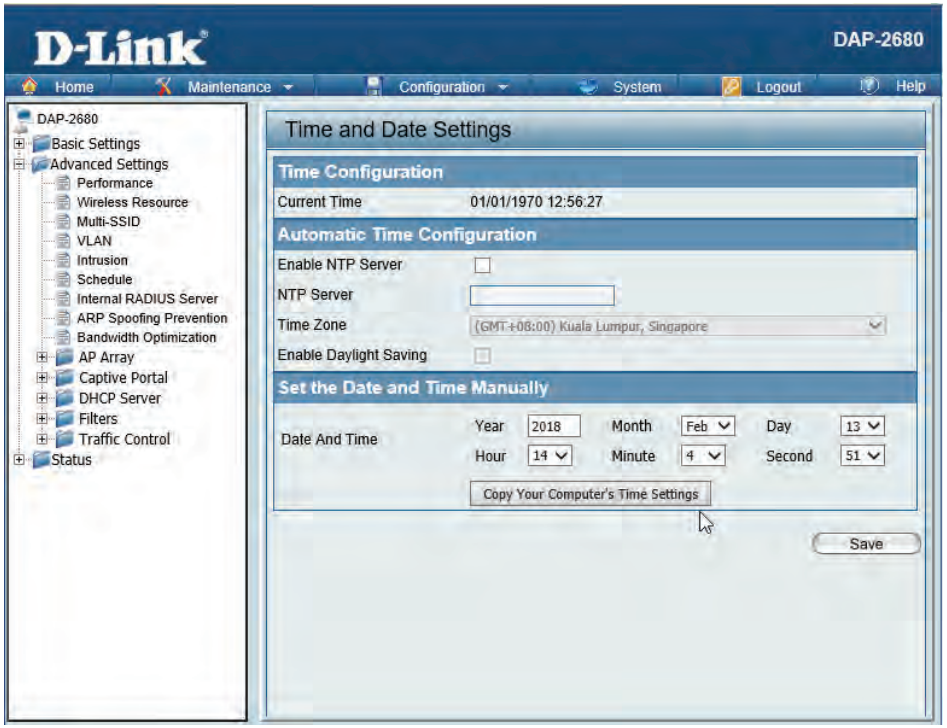
Enable NTP Server: Check to enable the AP to get system time from an NTP server from the Internet.

NTP Server: Enter the NTP server IP address.

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

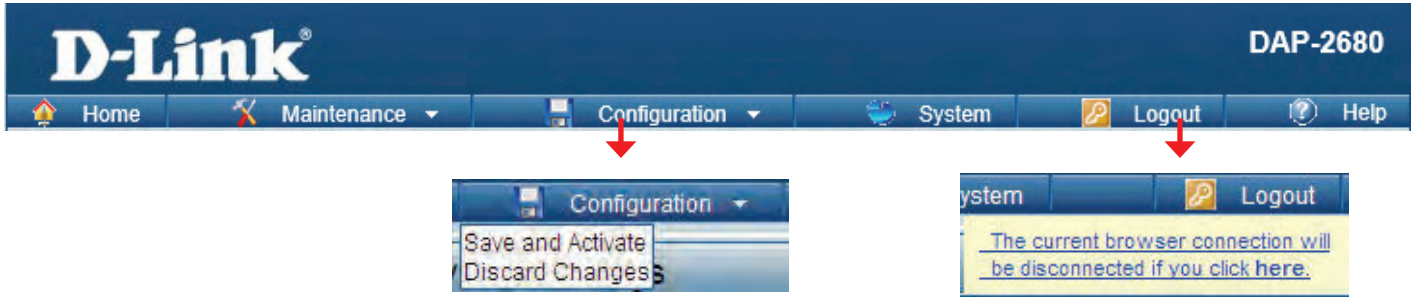
Enable Daylight Saving: Check the box to enable Daylight Saving Time.

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 and System

These options are the remaining option to choose from in the top menu. Configuration allows the user to save and activate or discard the configurations done. System allows the user to restart the unit, perform a factory reset or clear the language pack settings. Logout allows the user to safely log out from the access point's web configuration. Help allows the user to read more about the given options to configure without the need to consult the manual. The following pages will explain settings found in the configuration and system section in more detail.



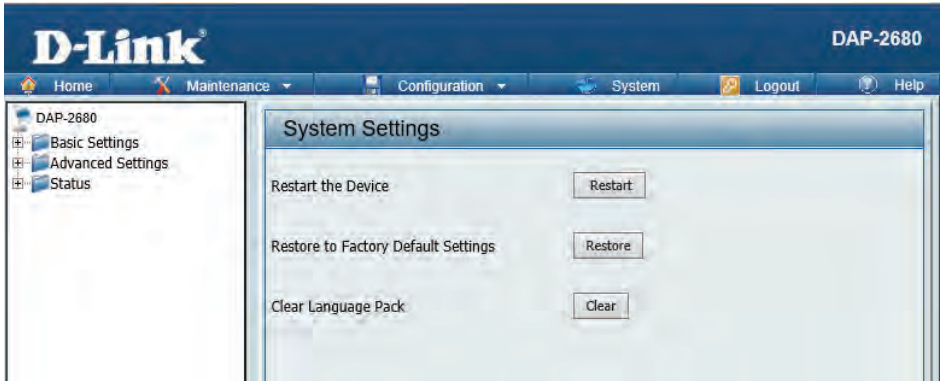
System Settings

On this page the user can restart the unit, perform a factory reset of the access point or clear the added language pack.

Restart the Device: Click Restart to restart the DAP-2682.

Restore to Factory Default Settings: Click Restore to restore the DAP-2682 back to factory default settings.

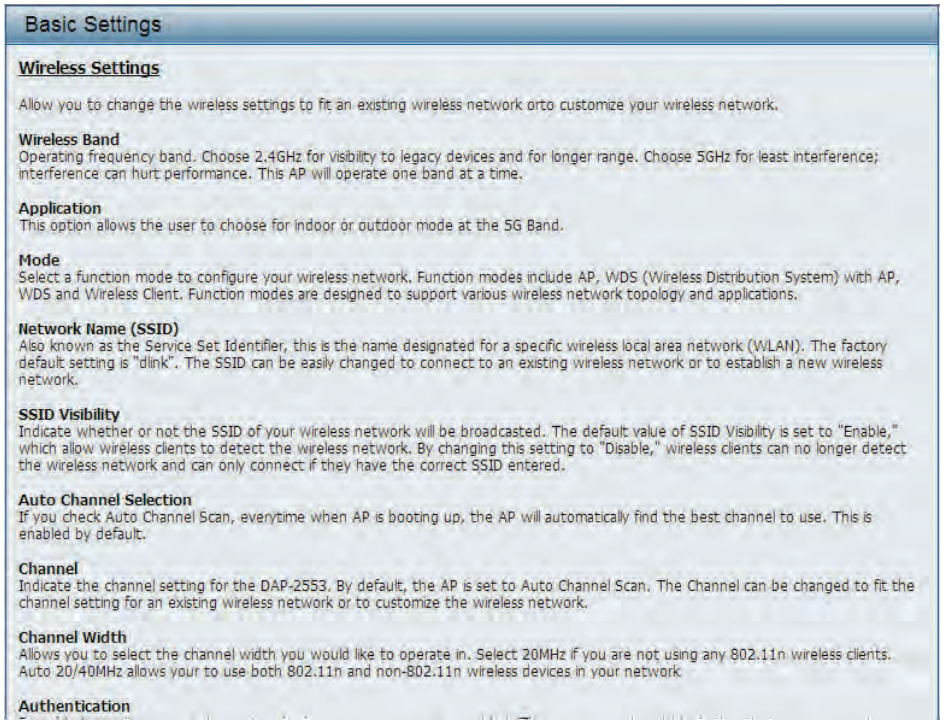
Clear Language Pack: Click to clear the current Language pack running.



Help

The help page is useful to view a brief description of a function available on the access point in case the manual is not present.

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.

Application
This option allows the user to choose for indoor or outdoor mode at the 5G Band.

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-2553. 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

Knowledge Base
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-2682 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.

Wireless Installation Considerations

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

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-2682. 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.)

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, Chrome, Firefox, or Safari 4 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® firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.
- Configure your Internet settings:

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

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

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

    Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link access point in the address bar. This should open the login page for your the web management.
- If you still cannot access the configuration, unplug the power to the access point for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

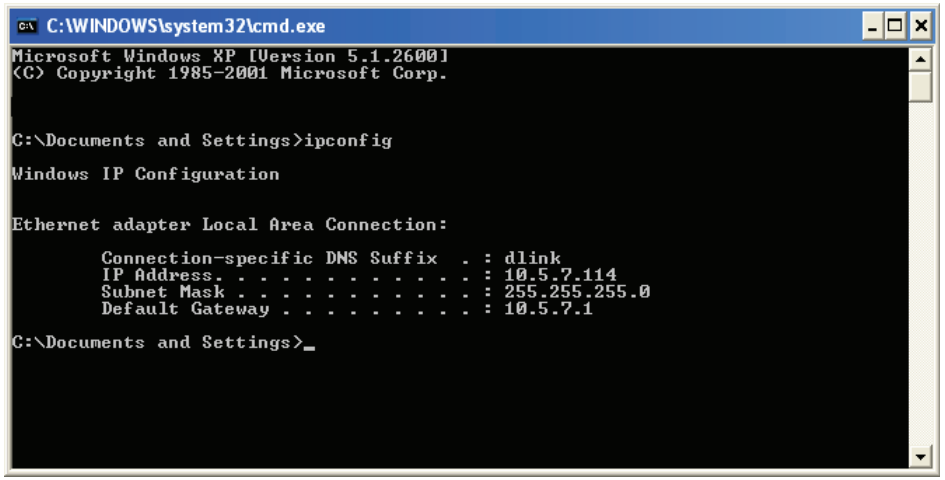
What can I do if I forgot my password?

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

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

How to check your IP address?

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



Click on Start > Run. In the run box type cmd and click OK.

At the prompt, type ipconfig and press Enter.

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

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

If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.

How to statically assign an IP address?

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

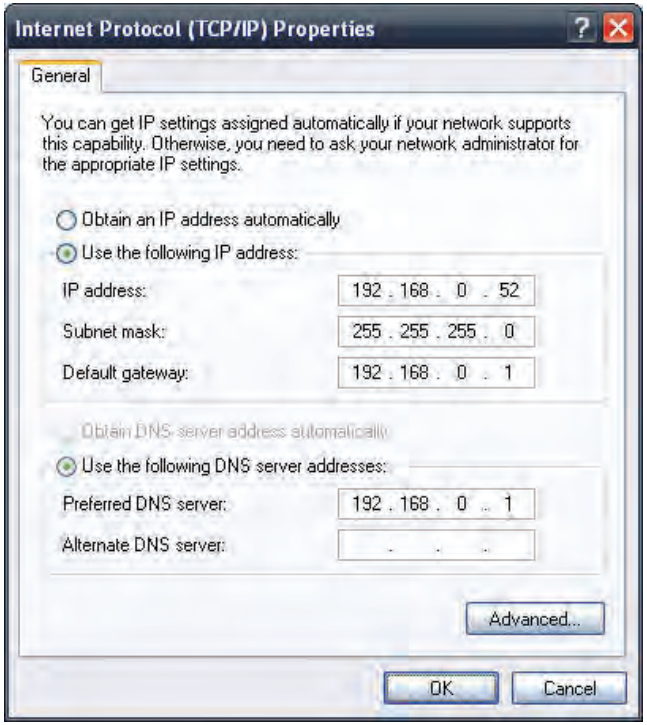
Step 1:
Windows® 2000: Click on Start > Settings > Control Panel > Network Connections
Windows XP: Click on Start > Control Panel > Network Connections
Windows Vista®: Click on Start > Control Panel > Network and Internet > Network and Sharing Center > Manage network connections

Step 2:
Right-click on the Local Area Connection which represents your network adapter and select Properties.

Step 3:
Highlight Internet Protocol (TCP/IP) and click Properties.

Step 4:
Click Use the following IP address and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.
Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).
Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5:
Click OK twice to save your settings.



Technical Specifications

Standards
- IEEE 802.11ac
- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.11a
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3at
- IEEE 802.3x

Network Management
- Web Browser interface (HTTP, Secure HTTP (HTTPS))
- Center WiFiManager
- SNMP Support
- Command Line Interface (Telnet, Secure SSH Telnet)

Security
- WPA™ Personal/Enterprise
- WPA2™ Personal/Enterprise
- WEP™ 64-/128-bit

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

Operating Voltage
- 12V/2A or 802.3at PoE

Antenna Type
- Four Dual Band Internal Antennas (2.4Ghz 3.6dBi & 5Ghz 4.2dBi)

LEDs
- Power/tatus

Temperature
- Operating: 0˚C to 40˚C
- Storing: -20˚C to 65˚C

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

Certifications
- FCC Class B
- CE
- UL

Dimensions
- L = 190 mm
- W = 190 mm
- H = 44.8 mm

Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. (“D-Link”) provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty:

D-Link warrants that the hardware portion of the D-Link product described below (“Hardware”) will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below (“Warranty Period”), except as otherwise stated herein.

- Hardware (excluding power supplies and fans): One (1) year
- Power supplies and fans: One (1) year
- Spare parts and spare kits: Ninety (90) days

The customer’s sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link’s option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty:

D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by DLink in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty:

The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim:

The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support (USA 1-877-453-5465 or Canada 1-800-361-5265), who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form. Enter the assigned Case ID Number at https://rma.dlink.com/ (USA only) or https://rma.dlink.ca (Canada only).

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc.
- **USA residents** send to 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.
- **Canadian residents** send to D-Link Networks, Inc., 2525 Meadowvale Boulevard Mississauga, Ontario, L5N 5S2 Canada. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via Purolator Canada or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in Canada, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming. RMA phone number: 1-800-361-5265 Hours of Operation: Monday-Friday, 9:00AM – 9:00PM EST

What Is Not Covered:

The Limited Warranty provided herein by D-Link does not cover:

Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product.

While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties:

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability:

TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law:

This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks:

D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

Copyright Statement:

No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any

derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice.

Copyright ©2018 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

Federal Communication Commission Interference Statement

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.

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.

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.

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

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

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 41 cm between the radiator & your body.

IMPORTANT NOTE:

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

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

FREE Central WiFiManager Software

DOWNLOAD NOW
DLINK.COM/WIFIDOWNLOAD

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

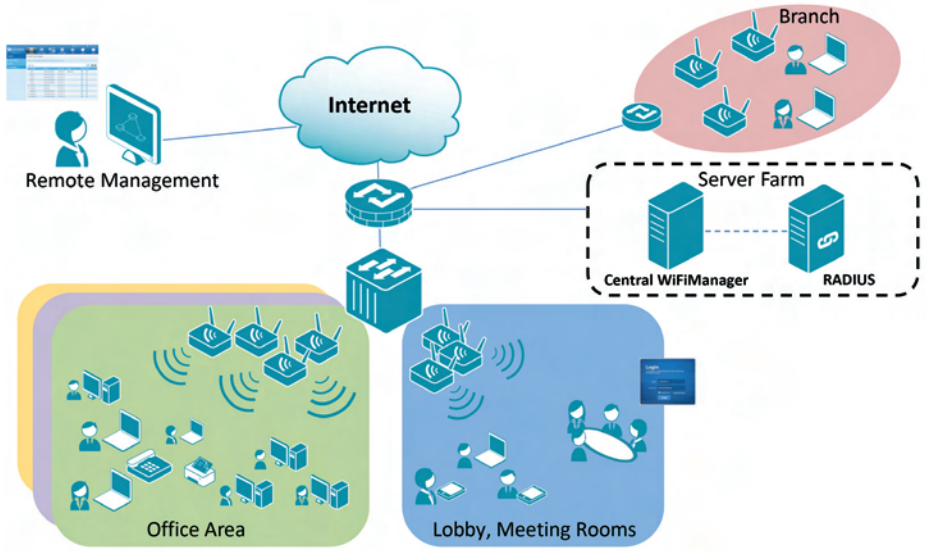
- Configure once and apply to multiple Access Points
- Install on Windows PC
- Access on any device using a web-browser, e.g. smartphone or notebook
- Utilise user authentication and access control
- Monitor your entire wireless network in real time[1]
- Access detailed reports
- Optimise your bandwidth

FREE Central WiFiManager User Interface

Supports multiple languages

1. see overleaf for selected product information.

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-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.

Registration

Register your product online at www.onlineregister.com/dlink

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.