

UNIFIED ACCESS POINT ADMINISTRATOR'S GUIDE

PRODUCT MODEL: DWL-6620APS, DWL-7620AP, DWL-8620AP, DWL-8620APE,
DWL-6720AP, DWL-8720AP, DWL-X8630AP

UNIFIED WIRED & WIRELESS ACCESS SYSTEM

RELEASE 7.00

Table of Contents

Section 1 - About This Document	6
Document Organization.....	6
Additional Documentation	6
Document Conventions	6
Online Help, Supported Browsers, and Limitations.....	7
Section 2 - Getting Started.....	8
Administrator's Computer Requirements	9
Wireless Client Requirements	9
Dynamic and Static IP Addressing on the AP	10
Recovering an IP Address.....	10
Discovering a Dynamically Assigned IP Address	10
Installing the UAP	10
Basic Settings.....	13
Connecting to the AP Web Interface by Using the IPv6 Address	14
Using the CLI to View the IP Address.....	14
Configuring the Ethernet Settings	14
Using the CLI to Configure Ethernet Settings	15
Configuring IEEE 802.1X Authentication.....	16
Verifying the Installation	16
Configuring Security on the Wireless Access Point.....	17
Section 3 - Viewing Access Point Status.....	18
Viewing Interface Status.....	18
Wired Settings (Internal Interface)	18
Wireless Settings	18
Viewing Events.....	19
Configuring the Log Relay Host for Kernel Messages	19
Enabling or Disabling the Log Relay Host on the Events Page	20
Viewing Transmit and Receive Statistics.....	20
Viewing Associated Wireless Client Information	21
Viewing Managed AP DHCP Information	22
Viewing Radio Statistics Information	22
Section 4 - Managing the Access Point.....	23
Ethernet Settings and Management IPv6.....	23
Ethernet Settings.....	23
Wireless Settings.....	25
Modifying Radio Settings.....	26
Configuring Radio and VAP Scheduler.....	29
Scheduler Association Settings.....	31
Virtual Access Point Settings.....	32
None (Plain-text)	35
WPA Personal	35
WPA Enterprise	36
Configuring Wireless Multicast Forwarding	38
Configuring the Wireless Distribution System (WDS)	38
WPA/PSK on WDS Links	40
Controlling Access by MAC Authentication	40
Configuring a MAC Filter and Station List on the AP.....	41
Configuring MAC Authentication on the RADIUS Server	42
Configuring Load Balancing	42
Managed Access Point Overview.....	43
Transition Between Modes.....	43
Configuring Managed Access Point Settings	43
Configuring 802.1X Authentication	44
Application Identification.....	45
Section 5 - Configuring Access Point Services	46
Web Server Settings	46

Setting the SSH Status.....	46
Setting the Telnet Status	47
Configuring Quality of Service.....	47
Configuring SNMP on the Access Point.....	48
Enabling the Time Settings (NTP).....	50
Section 6 - Configuring SNMPv3.....	52
Configuring SNMPv3 Views	52
Configuring SNMPv3 Groups	53
Configuring SNMPv3 Users	54
Configuring SNMPv3 Targets	55
Section 7 - Maintaining the Access Point.....	56
Saving the Current Configuration to a Backup File	56
Restoring the Configuration from a Previously Saved File.....	56
Resetting the Factory Default Configuration	57
Rebooting the Access Point	57
Upgrading the Firmware.....	57
Support Information Configuration and Settings	58
Section 8 - Configuring Client Quality of Service (QoS)	59
Configuring VAP QoS Parameters	59

List of Figures

Figure 1 - Administrator UI Online Help.....	7
Figure 2 - Web UI Login Prompt.....	12
Figure 3 - Provide Basic Settings	12
Figure 4 - Command Line Interface (CLI) Connection	14
Figure 5 - Viewing Interface Status	18
Figure 6 - Viewing Events.....	19
Figure 7 - Viewing Traffic Statistics	20
Figure 8 - Viewing Client Association Information	21
Figure 9 - Managed AP DHCP Information	22
Figure 10 - View Radio Statistics.....	22
Figure 11 - Modify Ethernet (Wired) settings	24
Figure 12 - Modify Wireless Settings.....	25
Figure 13 - Modify Radio Settings	27
Figure 14 - Scheduler Configuration	30
Figure 15 - Scheduler Configuration (Modify Rule)	31
Figure 16 - Scheduler Association Settings.....	32
Figure 17 - Modify Virtual Access Point Settings.....	33
Figure 18 - Modify Virtual Access Point Settings (WPA Personal)	36
Figure 19 - Modify Virtual Access Point Settings (WPA Enterprise)	36
Figure 20 - Wireless Multicast Forwarding	38
Figure 21 - Configure WDS Bridges.....	39
Figure 22 - Configure MAC Authentication.....	41
Figure 23 - Modify Load Balancing Settings.....	42
Figure 24 - Configure Managed AP Wireless Switch Parameters.....	44
Figure 25 - Modify 802.1X Supplicant Authentication Settings.....	45
Figure 26 - Application Identification	45
Figure 27 - Configure Web Server Settings.....	46
Figure 28 - Set SSH Status	47
Figure 29 - Set Telnet Status.....	47
Figure 30 - Modify QoS Queue Parameters.....	47
Figure 31 - SNMP Configuration	49
Figure 32 - Time Settings (NTP).....	51
Figure 33 - SNMPv3 Views Configuration.....	52
Figure 34 - SNMPv3 Groups Configuration.....	53
Figure 35 - SNMPv3 User Configuration	54
Figure 36 - SNMPv3 Targets Configuration.....	55
Figure 37 - Manage this Access Point's Configuration - Save.....	56
Figure 38 - Manage this Access Point's Configuration - Restore (HTTP)	56
Figure 39 - Performing AP Maintenance	57
Figure 40 - Manage Firmware (HTTP)	58
Figure 41 - Support Information	58
Figure 42 - Configure Client QoS VAP Settings.....	59

List of Tables

Table 1 - Typographical Conventions	7
Table 2 - Requirements for the Administrator's Computer.....	9
Table 3 - Requirements for Wireless Clients	10
Table 4 - Basic Settings Page	13
Table 5 - CLI Commands for Ethernet Setting	15
Table 6 - Logging Options	19
Table 7 - Log Relay Host.....	20
Table 8 - Transmit/Receive.....	21
Table 9 - Associated Clients	21
Table 10 - Radio Statistics Information.....	22
Table 11 - Ethernet Settings and Management IPv6	25
Table 12 - Wireless Settings.....	26
Table 13 - Radio Settings	29
Table 14 - Scheduler Configuration	30
Table 15 - Scheduler Association Settings	32
Table 16 - Virtual Access Point Settings.....	35
Table 17 - WPA Personal.....	36
Table 18 - WPA Enterprise.....	37
Table 19 - Wireless Multicast Forwarding.....	38
Table 20 - WDS Settings	40
Table 21 - WPA/PSK on WDS Links.....	40
Table 22 - MAC Authentication	42
Table 23 - RADIUS Server Attributes for MAC Authentication.....	42
Table 24 - Load Balancing.....	43
Table 25 - Managed Access Point	44
Table 26 - IEEE 802.1X Supplicant Authentication.....	45
Table 27 - Web Server Settings.....	46
Table 28 - SSH Settings	47
Table 29 - Telnet Settings	47
Table 30 - QoS Settings	48
Table 31 - SNMP Settings	50
Table 32 - NTP Settings.....	51
Table 33 - SNMPv3 Views	52
Table 34 - SNMPv3 Groups.....	54
Table 35 - SNMPv3 Users	54
Table 36 - SNMPv3 Targets.....	55
Table 37 - Support Information	58
Table 38 - VAP QoS Parameters	59

Section 1 - About This Document

This guide describes setup, configuration, administration and maintenance for the D-Link Unified Access Point (UAP) on a wireless network.

Document Organization

The *Unified Access Point Administrator's Guide* contains the following sections:

-) "Section 1 - About This Document" on page 6
-) "Section 2 - Getting Started" on page 8
-) "Section 3 - Viewing Access Point Status" on page 18
-) "Section 4 - Managing the Access Point" on page 23
-) "Section 5 - Configuring Access Point Services" on page 46
-) "Section 6 - Configuring SNMPv3" on page 52
-) "Section 7 - Maintaining the Access Point" on page 56
-) "Section 8 - Configuring Client Quality of Service (QoS)" on page 59


Additional Documentation


The following documentation provides additional information about Unified Access Point software:

-) The *Unified Access Point CLI Command Reference* describes the commands available from the command-line interface (CLI) for managing, monitoring, and configuring the switch.
-) The *User Manual* for the D-Link Unified Wired and Wireless System provides information about setting up and managing the Unified Wireless Switch (UWS), including information about how to use the switch to manage multiple UAPs.
-) Release notes for the D-Link Unified Wired and Wireless System detail the platform-specific functionality of the software packages, including issues and workarounds.

Document Conventions

This section describes the conventions this document uses.

	Note: A note provides more information about a feature or technology and cross-references to related topics.
---	---

	Caution! A caution provides information about critical aspects of AP configuration, combinations of settings, events, or procedures that can adversely affect network connectivity, security, and so on.
---	---

The following table describes the typographical conventions used in this guide.

Symbol	Example	Description
Bold	Click Apply to save your settings.	Menu titles, page names, and button names.
Blue Text	See "Document Conventions" on page 6	Hyperlink text.
Courier Font	WLAN-AP# show network	Screen text, file names, commands, user-typed command-line entries.
<i>Courier Font</i> <i>Italics</i>	Value	Command parameter, which might be a variable or fixed value.
Square Brackets []	[Value]	Indicates an optional fixed parameter.
Curly Braces { }	{Choice1 Choice2}	Indicates that you must select a parameter from the list of choices.

Symbol	Example	Description
Vertical Bars	Choice1 Choice2	Separates the mutually exclusive choices.
Braces within square brackets [{}]	[[Choice1 Choice2]]	Indicate a choice within an optional element.

Table 1 - Typographical Conventions

Online Help, Supported Browsers, and Limitations

Online help for the UAP Administration Web pages provides information about all fields and features available from the user interface (UI). The information in the online help is a subset of the information available in the *Unified Access Point Administrator's Guide*.

Online help information corresponds to each page on the UAP Administration UI.

For information about the settings on the current page, click the Help link on the upper right side of a page.

The following figure shows an example of the online help available from the links on the user interface.

Basic Settings

From the Basic Settings page, you can view various information about the UAP, including IP and MAC address information, and configure the administrator password for the UAP.

Field	Description
IP Address	Shows the IP address assigned to the AP. This field is not editable on this page because the IP address is already assigned (either by DHCP, or statically through the Ethernet Settings page).
IPv6 Address	Shows the IPv6 address assigned to the AP. This field is not editable on this page because the IP address is already assigned (either by DHCPv6, or statically through the Ethernet Settings page).
IPv6 Link Local Address	Shows the IPv6 Link Local address, which is the IPv6 address used by the local physical link. The link local address is not configurable and is assigned by using the IPv6 Neighbor Discovery process.
MAC Address	Shows the MAC address of the AP. The address shown here is the MAC address associated with the management interface. This is the address by which the AP is known externally to other networks.
Firmware Version	Shows version information about the firmware currently installed on the AP. As new versions of the WLAN AP firmware become available, you can upgrade the firmware on your APs.
Product Identifier	Identifies the AP hardware model.
Hardware Version	Identifies the AP hardware version.
Device Name	Generic name to identify the type of hardware.
Device Description	Provides information about the product hardware.
Current Password	Enter the current administrator password. You must correctly enter the current password before you are able to change it.
New Password	Enter a new administrator password. The characters you enter are displayed as bullet characters to prevent others from seeing your password as you type. The administrator password must be an alphanumeric string of up to 8 characters. Do not use special characters or spaces. Note: As an immediate first step in securing your wireless network, we recommend that you change the administrator password from the default.
Confirm New Password	Re-enter the new administrator password to confirm that you typed it as intended.
Baud Rate	Select a baud rate for the serial port connection. The baud rate on the AP must match the baud rate on the terminal or terminal emulator to connect to the AP command-line interface (CLI) by using a serial (console) connection. The following baud rates are available: <ul style="list-style-type: none"> • 9600 • 19200 • 38400 • 57000 • 115200
System Name	Enter a name for the AP. This name appears only on the Basic Settings page and is a name to identify the AP to the administrator. Use up to 64 alphanumeric characters, for example My AP.

Figure 1 - Administrator UI Online Help

Section 2 - Getting Started

The D-Link Unified Access Point (UAP) provides continuous, high-speed access between wireless devices and Ethernet devices. It is an advanced, standards-based solution for wireless networking in businesses of any size. The UAP enables wireless local area network (WLAN) deployment while providing state-of-the-art wireless networking features.

The UAP can operate in two modes: Standalone Mode or Managed Mode. In Standalone Mode, the UAP acts as an individual access point in the network, and you manage it by using the Administrator Web User Interface (UI), command-line interface (CLI), or SNMP. In Managed Mode, the UAP is part of the D-Link Unified Wired and Wireless System, and you manage it by using the D-Link Unified Wireless Switch. If an AP is in Managed Mode, the Administrator Web UI, Telnet, SSH, and SNMP services are disabled.

This document describes how to perform the setup, management, and maintenance of the UAP in Standalone Mode. For information about configuring the AP in Managed Mode by using the D-Link Unified Wireless Switch, see the *User Manual* for the switch.

Before you power on a new UAP, review the following sections to check required hardware and software components, client configurations, and compatibility issues. Make sure you have everything you need for a successful launch and test of your new or extended wireless network.

This section contains the following topics:

-) "Administrator's Computer Requirements" on page 9
-) "Wireless Client Requirements" on page 9
-) "Dynamic and Static IP Addressing on the AP" on page 10
-) "Installing the UAP" on page 10
-) "Basic Settings" on page 13
-) "Using the CLI to View the IP Address" on page 14
-) "Configuring the Ethernet Settings" on page 14
-) "Configuring IEEE 802.1X Authentication" on page 16
-) "Verifying the Installation" on page 16
-) "Configuring Security on the Wireless Access Point" on page 17

To manage the UAP by using the Web interface or by using the CLI through Telnet or SSH, the AP needs an IP address. If you use VLANs or IEEE 802.1X Authentication (port security) on your network, you might need to configure additional settings on the AP before it can connect to the network.



Note: The WLAN AP is not designed to function as a gateway to the Internet. To connect your WLAN to other LANs or the Internet, you need a gateway device.

Administrator's Computer Requirements

The following table describes the minimum requirements for the administrator's computer for configuration and administration of the UAP through a Web-based user interface (UI).

Required Software or Component	Description
Serial or Ethernet Connection to the Access Point	The computer used to configure the first access point must be connected to the access point by a serial cable or an Ethernet cable.
Wireless Connection to the Network	<p>After initial configuration and launch of the first access point on your new wireless network, you can make subsequent configuration changes through the Administration Web pages using a wireless connection to the internal network.</p> <p>For wireless connection to the access point, your administration device will need Wi-Fi capability similar to that of any wireless client:</p> <ul style="list-style-type: none"> •) Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.11 modes in which you plan to run the access point. •) Wireless client software configured to associate with the UAP.
Web Browser and Operating System	<p>Configuration and administration of the UAP is provided through a Web-based user interface hosted on the access point.</p> <p>We recommend using one of the following supported Web browsers to access the access point Administration Web pages:</p> <ul style="list-style-type: none"> •) Microsoft® Internet Explorer® version 8.x or 9.x (with up-to-date patch level for either major version) •) Mozilla® Firefox version 26.0 or later •) Chrome on Windows (for AP only) version 32.0 or later <p>The administration Web browser must have JavaScript™ enabled to support the interactive features of the administration interface.</p>
Security Settings	Ensure that security is disabled on the wireless client used to initially configure the access point.

Table 2 - Requirements for the Administrator's Computer

Wireless Client Requirements

The UAP provides wireless access to any client with a properly configured Wi-Fi client adapter for the 802.11 mode in which the access point is running. The UAP supports multiple client operating systems. Clients can be laptop or desktop computers, personal digital assistants (PDAs), or any other hand-held, portable or stationary device equipped with a Wi-Fi adapter and supporting drivers.

To connect to the access point, wireless clients need the software and hardware described in the following table.

Required Component	Description
Wi-Fi Client Adapter	Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.11 modes in which you plan to run the access point.
Wireless Client Software	Client software, such as Microsoft Windows Supplicant, configured to associate with the UAP.

Required Component	Description
Client Security Settings	<p>Security should be disabled on the client used to do initial configuration of the access point.</p> <p>If the Security mode on the access point is set to anything other than plain text, wireless clients will need to set a profile to the authentication mode used by the access point and provide a valid username and password, certificate, or similar user identity proof. Security modes are WPA/WPA2/WPA3-Enterprise, and WPA/WPA2/WPA3-Personal.</p> <p>For information about configuring security on the access point, see “Virtual Access Point Settings” on page 32</p>

Table 3 - Requirements for Wireless Clients

Dynamic and Static IP Addressing on the AP

When you power on the access point, the built-in DHCP client searches for a DHCP server on the network in order to obtain an IP Address and other network information. If the AP does not find a DHCP server on the network, the AP continues to use its default Static IP Address (10.90.90.91) until you re-assign it a new static IP address (and specify a static IP addressing policy) or until the AP successfully receives network information from a DHCP server.

To change the connection type and assign a static IP address by using the CLI, see [“Configuring the Ethernet Settings” on page 14](#) or, by using the Web UI, see [“Ethernet Settings” on page 23](#).



Caution! If you do not have a DHCP server on your internal network, and do not plan to use one, the first thing you must do after powering on the access point is change the connection type from DHCP to static IP. You can either assign a new static IP address to the AP or continue using the default address. We recommend assigning a new static IP address so that if you bring up another WLAN AP on the same network, the IP address for each AP will be unique.

Recovering an IP Address

If you experience trouble communicating with the access point, you can recover a static IP address by resetting the AP configuration to the factory defaults (see [“Resetting the Factory Default Configuration” on page 57](#)), or you can get a dynamically assigned address by connecting the AP to a network that has a DHCP server.

Discovering a Dynamically Assigned IP Address

If you have access to the DHCP server on your network and know the MAC address of your AP, you can view the new IP address associated with the MAC address of the AP.

If you do not have access to the DHCP server that assigned the IP address to the AP or do not know the MAC address of the AP, you might need to use the CLI to find out what the new IP address is. For information about how to discover a dynamically assigned IP address, see [“Using the CLI to View the IP Address” on page 14](#).

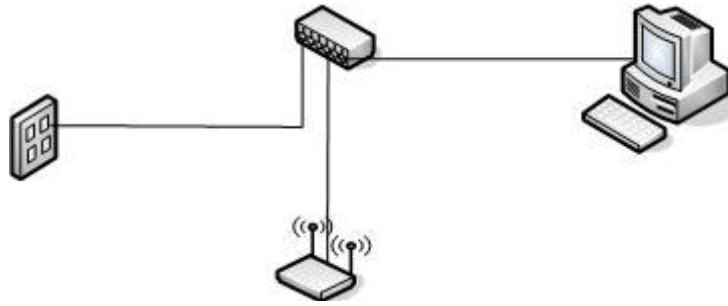
Installing the UAP

To access the Administration Web UI, you enter the IP address of the AP into a Web browser. You can use the default IP address of the AP (10.90.90.91) to log on to the AP and assign a static IP address, or you can use a DHCP server on your network to assign network information to the AP. The DHCP client on the AP is enabled by default.

To install the UAP, use the following steps:

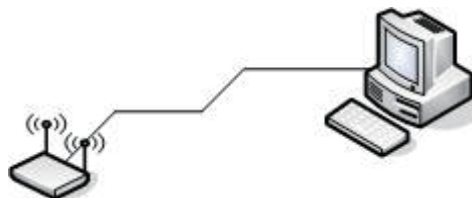
- 1.) Connect the AP to an administrative PC by using a LAN connection or a direct-cable connection.

-) To use a LAN connection, connect one end of an Ethernet cable to the network port on the access point and the other end to the same hub where your PC is connected, as shown in the following figure.



The hub or switch you use must permit broadcast signals from the access point to reach all other devices on the network.

-) To use a direct-cable connection, connect one end of an Ethernet straight-through or crossover cable to the network port on the access point and the other end of the cable to the Ethernet port on the PC, as shown in the following figure. You can also use a serial cable to connect the serial port on the AP to a serial port on the administrative computer.



For initial configuration with a direct Ethernet connection and no DHCP server, be sure to set your PC to a static IP address in the same subnet as the default IP address on the access point. (The default IP address for the access point is 10.90.90.91.)

If you use this method, you will need to reconfigure the cabling for subsequent startup and deployment of the access point so that the access point is no longer connected directly to the PC but instead is connected to the LAN (either by using a hub or directly).



Note: It is possible to detect access points on the network with a wireless connection. However, we strongly advise against using this method. In most environments you may have no way of knowing whether you are actually connecting to the intended AP. Also, many of the initial configuration changes required will cause you to lose connectivity with the AP over a wireless connection.

- 2.) Connect the power adapter to the power port on the back of the access point, and then plug the other end of the power cord into a power outlet.
- 3.) Use your Web browser to log on to the UAP Administration Web pages.
 -) If the AP did not acquire an IP address from a DHCP server on your network, enter 10.90.90.91 in the address field of your browser, which is the default IP address of the AP.
 -) If you used a DHCP server on your network to automatically configure network information for the AP, enter the new IP address of the AP into the Web browser.
 -) If you used a DHCP server and you do not know the new IP address of the AP, use the following procedures to obtain the information:
 -) Connect a serial cable from the administrative computer to the AP and use a terminal emulation program to access the command-line interface (CLI).
 -) At the login prompt, enter `admin` for the user name and `admin` for the password. At the command prompt, enter `get management`.
 -) The command output displays the IP address of the AP. Enter this address in the address field of your browser. For a more detailed explanation about how to log on to the CLI by using the console port, see "Using the CLI to View the IP Address" on page 24.
- 4.) When prompted, enter **admin** for the user name and **admin** for the password, then click **Logon**.

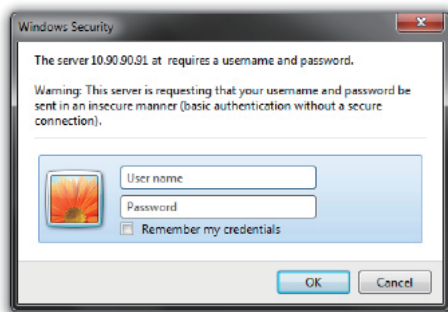


Figure 2 - Web UI Login Prompt

After you log in, the **Basic Settings** page for UAP administration is displayed, as the following figure shows.



Figure 3 - Provide Basic Settings

- 5.) Verify the settings on the **Basic Settings** page.
 - Review access point description and provide a new administrator password for the access point if you do not want to use the default password, which is **admin**.
 - Click the **Apply** button to activate the wireless network with these new settings.



Note: The changes you make are not saved or applied until you click Apply. Changing some access point settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change access point settings when WLAN traffic is low.

For information about the fields and configuration options on the Basic Settings page, see [“Basic Settings” on page 13](#).

- 6.) If you do not have a DHCP server on the management network and do not plan to use one, you must change the Connection Type from DHCP to Static IP.

You can either assign a new Static IP address to the AP or continue using the default address. We recommend assigning a new Static IP address so that if you bring up another UAP on the same network, the IP address for each AP will be unique. To change the connection type and assign a static IP address, see [“Configuring the Ethernet Settings” on page 14](#) (CLI) or [“Ethernet Settings” on page 23](#) (Web).

- 7.) If your network uses VLANs, you might need to configure the management VLAN ID or untagged VLAN ID on the UAP in order for it to work with your network.

For information about how to configure VLAN information, see [“Configuring the Ethernet Settings” on page 14](#) (CLI) or [“Ethernet Settings” on page 23](#) (Web).

- 8.) If your network uses IEEE 802.1X port security for network access control, you must configure the 802.1X supplicant information on the AP.

For information about how to configure the 802.1X user name and password, see [“Configuring IEEE 802.1X Authentication” on page 16](#).

Basic Settings

From the Basic Settings page, you can view various information about the UAP, including IP and MAC address information, and configure the administrator password for the UAP. The following table describes the fields and configuration options on the **Basic Settings** page.

Field	Description
IP Address	Shows the IP address assigned to the AP. This field is not editable on this page because the IP address is already assigned (either by DHCP, or statically through the Ethernet Settings page).
IPv6 Address	Shows the IPv6 address assigned to the AP. This field is not editable on this page because the IP address is already assigned (either by DHCPv6, or statically through the Ethernet Settings page).
IPv6 Address Status	Shows the operational status of the static IPv6 address assigned to the management interface of the AP. The possible values are Operational and Tentative.
IPv6 Auto-configured Global Addresses	Shows each automatically-configured global IPv6 address for the management interface of the AP.
IPv6 Link Local Address	Shows the IPv6 Link Local address, which is the IPv6 address used by the local physical link. The link local address is not configurable and is assigned by using the IPv6 Neighbor Discovery process.
MAC Address	Shows the MAC address of the AP. The address shown here is the MAC address associated with the management interface. This is the address by which the AP is known externally to other networks.
Firmware Version	Shows version information about the firmware currently installed on the AP. As new versions of the WLAN AP firmware become available, you can upgrade the firmware on your APs.
Model	Displays the AP model number.
Product Identifier	Identifies the AP hardware model.
Hardware Version	Identifies the AP hardware version.
Serial Number	Shows the AP serial number.
Device Name	Generic name to identify the type of hardware.
Device Description	Provides information about the product hardware.
New Password	<p>Enter a new administrator password. The characters you enter are displayed as bullet characters to prevent others from seeing your password as you type.</p> <p>The administrator password must be an alphanumeric string of up to 32 characters. The special characters are also supported.</p> <p>Note: As an immediate first step in securing your wireless network, we recommend that you change the administrator password from the default.</p>
Confirm New Password	Re-enter the new administrator password to confirm that you typed it as intended.
System Name	Enter a name for the AP. This name appears only on the Basic Settings page and is a name to identify the AP to the administrator. Use up to 64 alphanumeric characters, for example My AP.
System Contact	Enter the name, e-mail address, or phone number of the person to contact regarding issues related to the AP.
System Location	Enter the physical location of the AP, for example Conference Room A.

Table 4 - Basic Settings Page

Connecting to the AP Web Interface by Using the IPv6 Address

To connect to the AP by using the IPv6 global address or IPv6 link local address, you must enter the AP address into your browser in a special format.

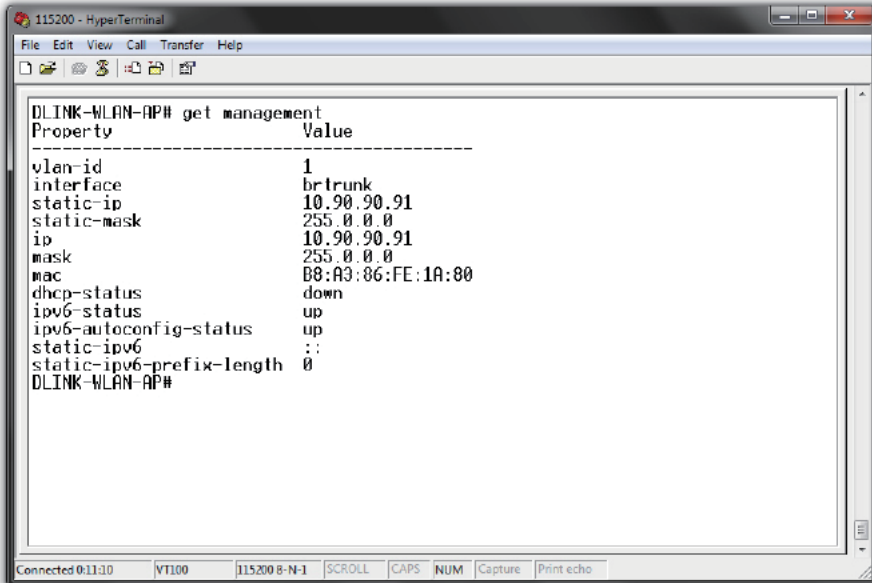
To connect to an IPv6 global address, add square brackets around the IPv6 address. For example, if the AP global IPv6 address is 2520::230:abff:fe00:2420, type the following address into the address field: `http://[2520::230:abff:fe00:2420]`.

Using the CLI to View the IP Address

The DHCP client on the UAP is enabled by default. If you connect the UAP to a network with a DHCP server, the AP automatically acquires an IP address. To manage the UAP by using the Administrator UI, you must enter the IP address of the access point into a Web browser.

If a DHCP server on your network assigns an IP address to the UAP, and you do not know the IP address, use the following steps to view the IP address of the UAP:

- 1.) Using a null-modem cable, connect a VT100/ANSI terminal or a workstation to the console (serial) port. If you attached a PC, Apple, or UNIX workstation, start a terminal-emulation program, such as HyperTerminal or TeraTerm.
- 2.) Configure the terminal-emulation program to use the following settings:
 -) Baud rate: 115200 bps
 -) Data bits: 8
 -) Parity: none
 -) Stop bit: 1
 -) Flow control: none
- 3.) Press the return key, and a login prompt should appear. The login name is **admin**. The default password is **admin**. After a successful login, the screen shows the (*Access Point Name*)# prompt.
- 4.) At the login prompt, enter `get management`. Information similar to the following prints to the screen.



```
DLINK-WLAN-AP# get management
Property      Value
-----
vlan-id      1
interface    brtrunk
static-ip    10.90.90.91
static-mask  255.0.0.0
ip           10.90.90.91
mask        255.0.0.0
mac         B8:A3:86:FE:1A:80
dhcp-status  down
ipv6-status  up
ipv6-autoconfig-status up
static-ipv6  ::
static-ipv6-prefix-length 0
DLINK-WLAN-AP#
```

Figure 4 - Command Line Interface (CLI) Connection

Configuring the Ethernet Settings

The default Ethernet settings, which include DHCP and VLAN information, might not work for all networks.

By default, the DHCP client on the UAP automatically broadcasts requests for network information. If you want to use a static IP address, you must disable the DHCP client and manually configure the IP address and other network information.

The management VLAN is VLAN 1 by default. This VLAN is also the default untagged VLAN. If you already have a management VLAN configured on your network with a different VLAN ID, you must change the VLAN ID of the management VLAN on the access point.

For information about using the Web interface to configure the Ethernet settings, see [“Ethernet Settings” on page 23](#). You can also use the CLI to configure the Ethernet settings, which the following section describes.

Using the CLI to Configure Ethernet Settings

Use the commands shown in the following table to view and set values for the Ethernet (wired) interface. For more information about each setting, see the description for the field in the following table.

Action	Commands
Get Current Settings for the Ethernet (Wired) Internal Interface	<code>get management</code>
Set the management VLAN ID	<code>set management vlan-id <1-4094></code>
View untagged VLAN information	<code>get untagged-vlan</code>
Enable the untagged VLAN	<code>set untagged-vlan status up</code>
Disable the untagged VLAN	<code>set untagged-vlan status down</code>
Set the untagged VLAN ID	<code>set untagged-vlan vlan-id <1-4094></code>
View the connection type	<code>get management dhcp-status</code>
Use DHCP as the connection type	<code>set management dhcp-status up</code>
Use a Static IP as the connection type	<code>set management dhcp-status down</code>
Set the Static IP address	<code>set management static-ip <ip_address></code> For example: <code>set management static-ip 10.10.12.221</code>
Set a Subnet Mask	<code>set management static-mask <netmask></code> For example: <code>set management static-mask 255.255.255.0</code>
Set the Default Gateway	<code>set static-ip-route gateway <ip_address></code> For example: <code>set static-ip-route gateway 10.10.12.1</code>

Table 5 - CLI Commands for Ethernet Setting

In the following example, the administrator uses the CLI to set the management VLAN ID to 123 and to disable the untagged VLAN so that all traffic is tagged with a VLAN ID.

```

DLINK-WLAN-AP# set management vlan-id 123
DLINK-WLAN-AP# set untagged-vlan status down
DLINK-WLAN-AP# get management
Property                               Value
-----
vlan-id                                123
interface                              brtrunk
static-ip                              10.90.90.91
static-mask                            255.0.0.0
ip                                      10.90.90.91
mask                                    255.0.0.0
mac                                     00:05:5E:80:70:00
dhcp-status                            down
ipv6-status                            up
ipv6-autoconfig-status                up
static-ipv6                            ::
static-ipv6-prefix-length             0

DLINK-WLAN-AP# get untagged-vlan
Property Value
-----
vlan-id  1
status   down

DLINK-WLAN-AP#

```

Configuring IEEE 802.1X Authentication

On networks that use IEEE 802.1X, port-based network access control, a supplicant (client) cannot gain access to the network until the 802.1X authenticator grants access. If your network uses 802.1X, you must configure 802.1X authentication information that the AP can supply to the authenticator.

If your network uses IEEE 802.1X see [“Configuring IEEE 802.1X Authentication” on page 16](#) for information about how to configure 802.1X by using the Web interface.

Verifying the Installation

Make sure the access point is connected to the LAN and associate some wireless clients with the network. Once you have tested the basics of your wireless network, you can enable more security and fine-tune the AP by modifying advanced configuration features.

- 1.) Connect the access point to the LAN.
 -) If you configured the access point and administrator PC by connecting both into a network hub, then your access point is already connected to the LAN. The next step is to test some wireless clients.
 -) If you configured the access point by using a direct cable connection from your computer to the access point, do the following procedures:
 -) Disconnect the cable from the computer and the access point.
 -) Connect an Ethernet cable from the access point to the LAN.
 -) Connect your computer to the LAN by using an Ethernet cable or a wireless card.
- 2.) Test LAN connectivity with wireless clients.

Test the UAP by trying to detect it and associate with it from some wireless client devices. For information about requirements for these clients, see [“Wireless Client Requirements” on page 9](#).
- 3.) Secure and configure the access point by using advanced features.

Once the wireless network is up and you can connect to the AP with some wireless clients, you can add in layers of security, create multiple virtual access points (VAPs), and configure performance settings.



Note: The WLAN AP is not designed for multiple, simultaneous configuration changes. If more than one administrator is logged onto the Administration Web pages and making changes to the configuration, there is no guarantee that all configuration changes specified by multiple users will be applied.

By default, no security is in place on the access point, so any wireless client can associate with it and access your LAN. An important next step is to configure security, as described in [“Virtual Access Point Settings” on page 32](#).

Configuring Security on the Wireless Access Point

You configure secure wireless client access by configuring security for each virtual access point (VAP) that you enable. You can configure up to 16 VAPs per radio that simulate multiple APs in one physical access point. By default, only one VAP is enabled. For each VAP, you can configure a unique security mode to control wireless client access.

Each radio has 16 VAPs, with VAP IDs from 0-15. By default, only VAP 0 on each radio is enabled. VAP0 has the following default settings:

-) VLAN ID: 1
-) Broadcast SSID: Enabled
-) SSID: dlink1
-) Security: None
-) MAC Authentication Type: None
-) Redirect Mode: None

All other VAPs are disabled by default. The default SSID for VAPs 1–15 is “dlinkx” where x is the VAP ID.

To prevent unauthorized access to the UAP, we recommend that you select and configure a security option other than None for the default VAP and for each VAP that you enable.

For information about how to configure the security settings on each VAP, see [“Virtual Access Point Settings” on page 32](#).

Section 3 - Viewing Access Point Status

This section describes the information you can view from the tabs under the **Status** heading on the Administration Web UI. This section contains the following subsections:

-) “Viewing Interface Status” on page 18
-) “Viewing Events” on page 19
-) “Viewing Transmit and Receive Statistics” on page 20
-) “Viewing Associated Wireless Client Information” on page 21
-) “Viewing Managed AP DHCP Information” on page 22
-) “Viewing Radio Statistics Information” on page 22

Viewing Interface Status

To monitor Ethernet LAN (wired) and wireless LAN (WLAN) settings, click the **Interfaces** tab.

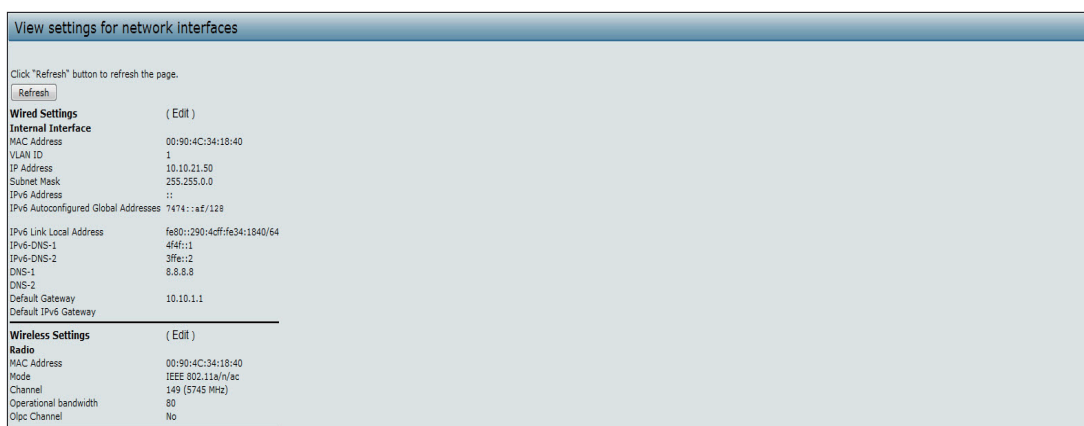


Figure 5 - Viewing Interface Status

This page displays the current settings of the UAP. It displays the **Wired Settings** and the **Wireless Settings**.

Wired Settings (Internal Interface)

The Internal interface includes the Ethernet MAC Address, Management VLAN ID, IP Address (IPv4 and IPv6), Subnet Mask, and DNS information. To change any of these settings, click the **Edit** link. After you click **Edit**, you are redirected to the **Ethernet Settings** page.

For information about configuring these settings, see “[Configuring the Ethernet Settings](#)” on page 14.

Wireless Settings

The Radio Interface includes the AeroScout™ Engine Communication status, Radio Mode and Channel. The **Wireless Settings** section also shows the MAC address (read-only) associated with each radio interface.

To change the Radio Mode or Channel settings, click the **Edit** link. After you click **Edit**, you are redirected to the **Modify Wireless Settings** page.

For information about configuring these settings, see “[Wireless Settings](#)” on page 25 and “[Modifying Radio Settings](#)” on page 26.

Viewing Events

The **Events** page shows real-time system events on the AP such as wireless clients associating with the AP and being authenticated.

To view system events, click the **Events** tab.

Figure 6 - Viewing Events

Table 6 - Logging Options



Note: To apply your changes, click **Apply**. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

Configuring the Log Relay Host for Kernel Messages

The Kernel Log is a comprehensive list of system events (shown in the System Log) and kernel messages such as error conditions, like dropping frames.

You cannot view kernel log messages directly from the Administration Web UI for an AP. You must first set up a remote server running a syslog process and acting as a syslog log relay host on your network. Then, you can configure the UAP to send syslog messages to the remote server.

Remote log server collection for AP syslog messages provides the following features:

-) Allows aggregation of syslog messages from multiple APs
-) Stores a longer history of messages than kept on a single AP
-) Triggers scripted management operations and alerts

To use Kernel Log relaying, you must configure a remote server to receive the syslog messages. The procedure to configure a remote log host depends on the type of system you use as the remote host.



Note: The syslog process will default to use port 514. We recommend keeping this default port. However, if you choose to reconfigure the log port, make sure that the port number you assign to syslog is not being used by another process.

Enabling or Disabling the Log Relay Host on the Events Page

To enable and configure Log Relaying on the **Events** page, set the Log Relay options as described in the following table, and then click **Update**.

Field	Description
Relay Log	Select Enabled to allow the UAP to send log messages to a remote host. Select Disabled to keep all log messages on the local system.
Relay Host	Specify the IPv4 Address or DNS name of the remote log server.
Relay Port	Specify the Port number for the syslog process on the Relay Host. The default port is 514.

Table 7 - Log Relay Host



Note: To apply your changes, click **Apply**. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

If you enabled the Log Relay Host, clicking **Apply** will activate remote logging. The AP will send its kernel messages real-time for display to the remote log server monitor, a specified kernel log file, or other storage, depending on how you configured the Log Relay Host.

If you disabled the Log Relay Host, clicking **Apply** will disable remote logging.

Viewing Transmit and Receive Statistics

The **Transmit/Receive** page provides some basic information about the current AP and a real-time display of the transmit and receive statistics for the Ethernet interface on the AP and for the VAPs on all supported radio interfaces. All transmit and receive statistics shown are totals since the AP was last started. If you reboot the AP, these figures indicate transmit and receive totals since the reboot.

To view transmit and receive statistics for the AP, click the **Transmit/Receive** tab.

View transmit and receive statistics for this access point				
Interface	Status	MAC Address	VLAN ID	Name (SSID)
LAN	up	B8:A3:86:FE:1A:80	1	-
wlan0:vap0	up	B8:A3:86:FE:1A:80	1	dlink1
wlan0:vap1	down		1	dlink2
wlan0:vap2	down		1	dlink3
wlan0:vap3	down		1	dlink4
wlan0:vap4	down		1	dlink5
wlan0:vap5	down		1	dlink6
wlan0:vap6	down		1	dlink7
wlan0:vap7	down		1	dlink8
wlan0:vap8	down		1	dlink9
wlan0:vap9	down		1	dlink10
wlan0:vap10	down		1	dlink11
wlan0:vap11	down		1	dlink12
wlan0:vap12	down		1	dlink13
wlan0:vap13	down		1	dlink14
wlan0:vap14	down		1	dlink15
wlan0:vap15	down		1	dlink16
wlan1:vap0	up	D8:A3:86:FE:1A:90	1	dlink1
wlan1:vap1	down		1	dlink2
wlan1:vap2	down		1	dlink3
wlan1:vap3	down		1	dlink4
wlan1:vap4	down		1	dlink5
wlan1:vap5	down		1	dlink6
wlan1:vap6	down		1	dlink7
wlan1:vap7	down		1	dlink8
wlan1:vap8	down		1	dlink9
wlan1:vap9	down		1	dlink10
wlan1:vap10	down		1	dlink11
wlan1:vap11	down		1	dlink12

Figure 7 - Viewing Traffic Statistics

Field	Description
Interface	The name of the Ethernet or VAP interface.
Status	Shows whether the interface is up or down.
MAC Address	MAC address for the specified interface. The UAP has a unique MAC address for each interface. Each radio has a different MAC address for each interface on each of its two radios.
VLAN ID	Virtual LAN (VLAN) ID. You can use VLANs to establish multiple internal and guest networks on the same AP. The VLAN ID is set on the VAP page. (See “Configuring Load Balancing” on page 42)
Name (SSID)	Wireless network name. Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network. The SSID is set on the VAP page. (See “Configuring Load Balancing” on page 42)
Transmit and Receive Information	
Total Packets	Indicates total packets sent (in Transmit table) or received (in Received table) by this AP.
Total Bytes	Indicates total bytes sent (in Transmit table) or received (in Received table) by this AP.
Total Drop Packets	Indicates total number of packets sent (in Transmit table) or received (in Received table) by this AP that were dropped.
Errors	Indicates total errors related to sending and receiving data on this AP.

Table 8 - Transmit/Receive

Viewing Associated Wireless Client Information

To view the client stations associated with a particular access point, click the **Client Associations** tab.

Network	Station	TxRate	RxRate	RSSI	Mode	Assoc_time
wlan0	ea:ce:9c:73:02:ff	48M	6M	69	IEEE80211_MODE_11AC_VHT80	00:08:18
wlan0	44:03:2c:7f:3c:fd	48M	780M	61	IEEE80211_MODE_11AC_VHT80	00:02:52

Figure 8 - Viewing Client Association Information

The associated stations are displayed along with information about packet traffic transmitted and received for each station.

The following describes the fields on the **Client Associations** page.

Field	Description
Network	Shows which radio the client is associated with.
Station	Shows the MAC address of the associated wireless client.
TxRate	Shows the transmit data rates in Mbps.
RxRate	Shows the receive data rates in Mbps.
RSSI	Signal strength. Shows the measurement of how well the client can hear a signal from the associated access point.
Mode	Shows the signal strength
Assoc_time	Shows the amount of time that has passed since the client associated to the access point.

Table 9 - Associated Clients

Viewing Managed AP DHCP Information

The UAP can learn about D-Link Unified Wireless Switches on the network through DHCP responses to its initial DHCP request. The **Managed AP DHCP** page displays the DNS names or IP addresses of up to four D-Link Unified Wireless Switches that the AP learned about from a DHCP server on your network.

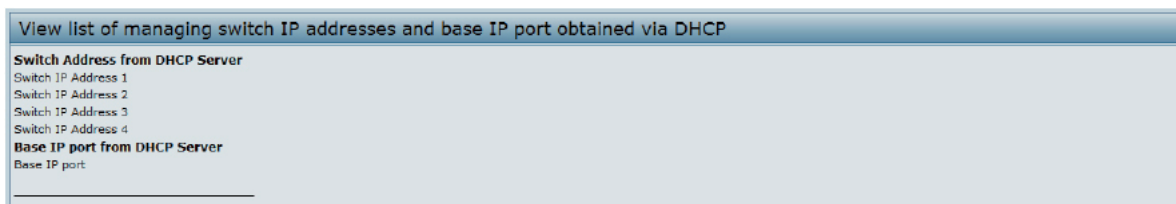


Figure 9 - Managed AP DHCP Information

For information about how to configure a DHCP server to respond to AP DHCP requests with the switch IP address information, see the *User Manual* for the switch.

Viewing Radio Statistics Information

The Radio Statistics page provides detailed information about the packets and bytes transmitted and received on the radio interface of this access point.

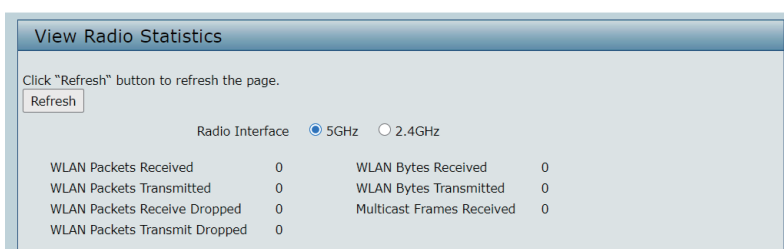


Figure 10 - View Radio Statistics

The following table describes details about the Radio Statistics information.

Field	Description
Radio	Choose either 5GHz radio or 2.4GHz radio to view statistics for the selected radio.
WLAN Packets Received	Total packets received by the AP on this radio interface.
WLAN Packets Transmitted	Total packets transmitted by the AP on this radio interface.
WLAN Packets Receive Dropped	Number of packets received by the AP on this radio interface that were dropped.
WLAN Packets Transmit Dropped	Number of packets transmitted by the AP on this radio interface that were dropped.
WLAN Bytes Received	Total bytes received by the AP on this radio interface.
WLAN Bytes Transmitted	Total bytes transmitted by the AP on this radio interface.
Multicast Frames Received	Count of MSDU frames received with the multicast bit set in the destination MAC address.

Table 10 - Radio Statistics Information

Section 4 - Managing the Access Point

This section describes how to manage the UAP and contains the following subsections:

-) "Ethernet Settings and Management IPv6" on page 23
-) "Wireless Settings" on page 25
-) "Modifying Radio Settings" on page 26
-) "Configuring Radio and VAP Scheduler" on page 29
-) "Scheduler Association Settings" on page 31
-) "Virtual Access Point Settings" on page 32
-) "Configuring Wireless Multicast Forwarding" on page 38
-) "Configuring the Wireless Distribution System (WDS)" on page 38
-) "Controlling Access by MAC Authentication" on page 40
-) "Configuring Load Balancing" on page 42
-) "Configuring 802.1X Authentication" on page 44
-) "Application Identification" on page 45

The configuration pages for the features in this section are located under the **Manage** heading on the Administration Web UI.

Ethernet Settings and Management IPv6

The default wired interface settings, which include DHCP and VLAN information, might not work for all networks.

Ethernet Settings

The default wired interface settings, which include DHCP and VLAN information, might not work for all networks.

By default, the DHCP client on the UAP automatically broadcasts requests for network information. If you want to use a static IP address, you must disable the DHCP client and manually configure the IP address and other network information.

The management VLAN is VLAN 1 by default. This VLAN is also the default untagged VLAN. If you already have a management VLAN configured on your network with a different VLAN ID, you must change the VLAN ID of the management VLAN on the AP.

Management IPv6 settings describe the IPv6 configuration of Management Interface. Use this page to configure the IPv6 admin mode, IPv6 auto-config admin mode, connection type (DHCPv6 or Static IPv6 addressing) and DNS servers. By default, the DHCPv6 client on the UAP automatically broadcasts requests for network information. If you want to use a static IPv6 address, you must disable the DHCPv6 client and manually configure the Static IPv6 address and other network information.

To configure the LAN settings, click the **Ethernet Settings** tab.

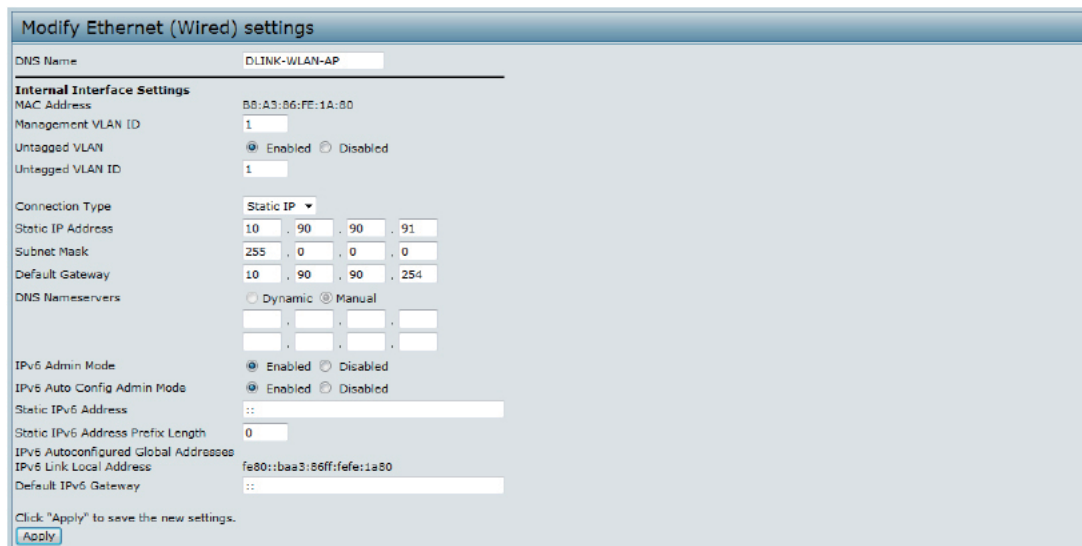



Figure 11 - Modify Ethernet (Wired) settings

The following table describes the fields to view or configure on the **Ethernet Settings** page.


Field	Description
Hostname	Enter a hostname for the AP. The hostname appears in the CLI prompt. <ul style="list-style-type: none"> • The hostname has the following requirements: • The length must be between 1 – 63 characters. • Upper and lower case characters, numbers, and hyphens are accepted. • The first character must be a letter (a – z or A – Z), and the last character cannot be a hyphen.
MAC Address	Shows the MAC address for the LAN interface for the Ethernet port on this AP. This is a read-only field that you cannot change.
Management VLAN ID	The management VLAN is the VLAN associated with the IP address you use to access the AP. The default management VLAN ID is 1. Provide a number between 1 and 4094 for the management VLAN ID.
Untagged VLAN	If you disable the untagged VLAN, all traffic is tagged with a VLAN ID. By default all traffic on the UAP uses VLAN 1, which is the default untagged VLAN. This means that all traffic is untagged until you disable the untagged VLAN, change the untagged traffic VLAN ID, or change the VLAN ID for a VAP or client using RADIUS.
Untagged VLAN ID	Provide a number between 1 and 4094 for the untagged VLAN ID. Traffic on the VLAN that you specify in this field will not be tagged with a VLAN ID.
Connection Type	If you select DHCP , the UAP acquires its IP address, subnet mask, DNS, and gateway information from a DHCP server. If you select Static IP , you must enter information in the Static IP Address, Subnet Mask, and Default Gateway fields.
Static IP Address	Enter the static IP address in the text boxes. This field is disabled if you use DHCP as the connection type.
Subnet Mask	Enter the Subnet Mask in the text boxes.
Default Gateway	Enter the Default Gateway in the text boxes.
DNS Nameservers	Select the mode for the DNS. In Dynamic mode, the IP addresses for the DNS servers are assigned automatically via DHCP. This option is only available if you specified DHCP for the Connection Type. In Manual mode, you must assign static IP addresses to resolve domain names.
Link Aggregation	Select the mode for the Link Aggregation. In LACP mode, to negotiate LAG settings between the two connected devices. We recommend using LACP mode instead of Static mode whenever both devices support LACP.
IPv6 Connection Type	If you select DHCPv6 , the UAP acquires its IPv6 address, DNS, and gateway information from a DHCPv6 server. If you select Static IPv6 , you must enter information in the Static IPv6 Address, Prefix length, and Default Gateway fields.

Field	Description
IPv6 Admin Mode	Enable or disable IPv6 management access to the AP
IPv6 Auto Config Admin Mode	Enable or disable IPv6 auto address configuration on the AP. When IPv6 Auto Config Mode is enabled, automatic IPv6 address configuration and gateway configuration is allowed by processing the Router Advertisements received on the LAN port. The AP can have multiple auto configured IPv6 addresses.
Static IPv6 Address	Enter a static IPv6 address. The AP can have a static IPv6 address even if addresses have already been configured automatically.
Static IPv6 Address Prefix Length	Enter the static IPv6 prefix length, which is an integer in the range of 0 – 128.
IPv6 Autoconfigured Global Addresses	If the AP has been assigned one or more IPv6 addresses automatically, the addresses are listed.
IPv6 Link Local Address	Shows the IPv6 Link Local address, which is the IPv6 address used by the local physical link. The link local address is not configurable and is assigned by using the IPv6 Neighbor Discovery process.
Default IPv6 Gateway	Enter the default IPv6 gateway.
IPv6 Domain Nameservers	Select the mode for the DNS. In Dynamic mode, the IPv6 addresses for the DNS servers are assigned automatically via DHCPv6. This option is available only if DHCPv6 is selected for the Connection Type. In Manual mode, you must assign static IPv6 addresses to resolve domain names.

Table 11 - Ethernet Settings and Management IPv6



Note: After you configure the wired settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.



Note: Management IPv6 is available as a separate tab in few models of DWL.

Wireless Settings

Wireless settings describe aspects of the local area network (LAN) related specifically to the radio device in the access point (802.11 Mode and Channel) and to the network interface to the access point (MAC address for access point and Wireless Network name, also known as SSID).

To configure the wireless interface, click the **Manage > Wireless Settings** tab.

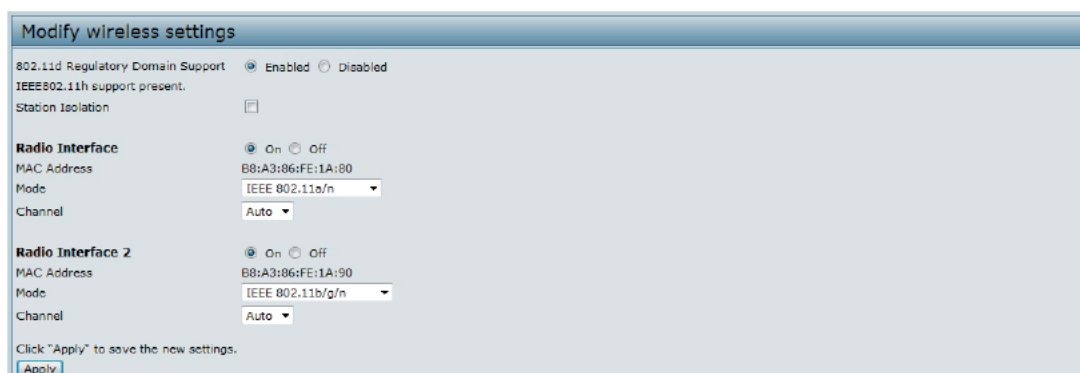


Figure 12 - Modify Wireless Settings

The following table describes the fields and configuration options available on the **Wireless Settings** page.

Field	Description
Radio Interface	Specify whether you want the radio interface on or off.
MAC Address	Indicates the Media Access Control (MAC) addresses for the interface. Dual-radio APs have a unique MAC address for each radio. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface.
Mode	The Mode defines the Physical Layer (PHY) standard the radio uses. Note: The modes available depend on the country code setting and the radio selected. Select one of the following modes for 5GHz radio: <ul style="list-style-type: none"> • IEEE 802.11a • IEEE 802.11a/n • IEEE 802.11n • IEEE 802.11a/n/ac • IEEE 802.11n/ac • IEEE 802.11a/n/ac/ax (DWL-X8630AP) Select one of the following modes for 2.4GHz radio: <ul style="list-style-type: none"> • IEEE 802.11n • IEEE 802.11b/g • IEEE 802.11b/g/n • IEEE 802.11b/g/n/ax (DWL-X8630AP)
Channel	Select the Channel . The range of available channels is determined by the mode of the radio interface and the country code setting. If you select Auto for the channel setting, the AP scans available channels and selects a channel where no traffic is detected. The Channel defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each mode offers a number of channels, depending on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R). When automatic channel assignment is enabled on the Channel Management page for Clustering, the channel policy for the radio is automatically set to static mode, and the Auto option is not available for the Channel field. This allows the automatic channel feature to set the channels for the radios in the cluster.
Station Isolation	To enable Station Isolation, select the check box directly beside it. When Station Isolation is disabled, wireless clients can communicate with one another normally by sending traffic through the AP. When Station Isolation is enabled, the AP blocks communication between wireless clients on the same radio and VAP. The AP still allows data traffic between its wireless clients and wired devices on the network, across a WDS link, and with other wireless clients associated with a different VAP, but not among wireless clients associated with the same VAP.

Table 12 - Wireless Settings



Note: After you configure the wireless settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

Modifying Radio Settings

Radio settings directly control the behaviour of the radio devices in the AP and its interaction with the physical medium; that is, how and what type of electromagnetic waves the AP emits.

To specify radio settings, click the **Radio** tab in the **Manage** section.

Different settings will be displayed depending on the mode you select. All settings are described in the table below.

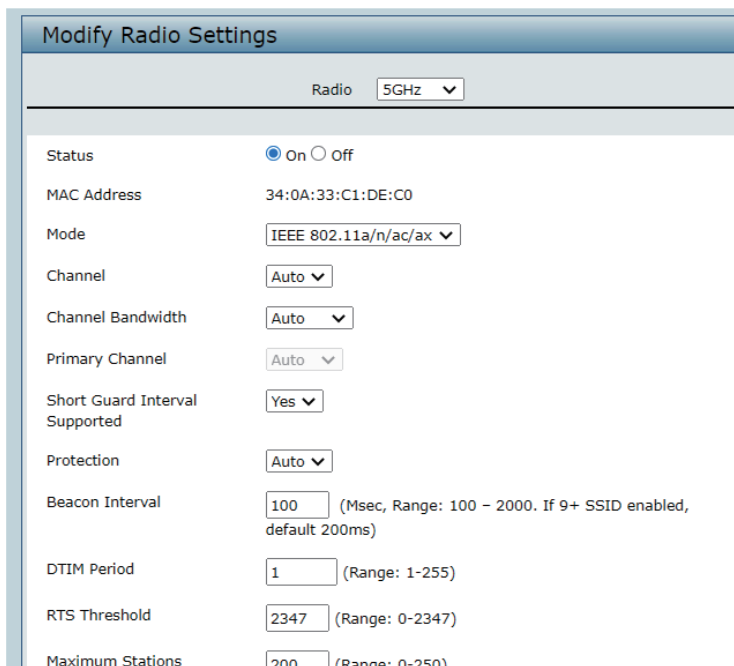


Figure 13 - Modify Radio Settings

The following table describes the fields and configuration options for the **Radio Settings** page.

Field	Description
Radio	Select Radio 5GHz or 2.4GHz Radio to specify which radio to configure.
Status (On/Off)	Specify whether you want the radio on or off by clicking On or Off . If you turn off a radio, the AP sends disassociation frames to all the wireless clients it is currently supporting so that the radio can be gracefully shutdown and the clients can start the association process with other available APs.
MAC Address	Indicates the Media Access Control (MAC) addresses for the interface. Dual-radio APs have a unique MAC address for each radio.
Mode	The Mode defines the Physical Layer (PHY) standard the radio uses. Note: The modes available depend on the country code setting and the radio selected. Select one of the following modes for 5GHz radio: <ul style="list-style-type: none"> • IEEE 802.11a • IEEE 802.11a/n • IEEE 802.11n • IEEE 802.11a/n/ac • IEEE 802.11n/ac • IEEE 802.11a/n/ac/ax (DWL-X8630AP) Select one of the following modes for 2.4GHz radio: <ul style="list-style-type: none"> • IEEE 802.11n • IEEE 802.11b/g • IEEE 802.11b/g/n • IEEE 802.11b/g/n/ax (DWL-X8630AP)
Channel	Select the Channel . The range of available channels is determined by the mode of the radio interface and the country code setting. If you select Auto for the channel setting, the AP scans available channels and selects a channel where no traffic is detected. The channel defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each mode offers a number of channels, depending on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R). When automatic channel assignment is enabled on the Channel Management page for Clustering, the channel policy for the radio is automatically set to static mode, and the Auto option is not available for the Channel field. This allows the automatic channel feature to set the channels for the radios in the cluster.

Field	Description
Channel Bandwidth (802.11n, 802.11ac and 802.11ax modes only)	<p>The 802.11n specification allows a 40 MHz wide channel in addition to the legacy 20 MHz channel available with other modes. The 40 MHz channel enables higher data rates but leaves fewer channels available for use by other 2.4 GHz and 5 GHz devices.</p> <p>The 802.11ac/ax specification allows an 80 MHz-wide channel in addition to the 20 MHz and 40 MHz channels.</p> <p>Set the field to 20 MHz to restrict the use of the channel bandwidth to a 20 MHz channel. For the 802.11ac/ax mode, set the field to 40 MHz to prevent the radio from using the 80 MHz channel bandwidth.</p>
Primary Channel (802.11n modes only)	<p>This setting can be changed only when the channel bandwidth is set to 40 MHz. A 40 MHz channel can be considered to consist of two 20 MHz channels that are contiguous in the frequency domain. These two 20 MHz channels are often referred to as the Primary and Secondary channels. The Primary Channel is used for 802.11n clients that support only a 20 MHz channel bandwidth and for legacy clients.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> •) Lower — Set the Primary Channel as the lower 20 MHz channel in the 40 MHz band. •) Upper — Set the Primary Channel as the upper 20 MHz channel in the 40 MHz band.
Short Guard Interval Supported	<p>This field is available only if the selected radio mode includes 802.11n.</p> <p>The guard interval is the dead time, in nanoseconds, between OFDM symbols. The guard interval prevents Inter-Symbol and Inter-Carrier Interference (ISI, ICI). The 802.11n mode allows for a reduction in this guard interval from the a and g definition of 800 nanoseconds to 400 nanoseconds. Reducing the guard interval can yield a 10% improvement in data throughput.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> •) Yes — The AP transmits data using a 400ns guard Interval when communicating with clients that also support the short guard interval. •) No — The AP transmits data using an 800ns guard interval.
Protection	<p>The protection feature contains rules to guarantee that 802.11n transmissions do not cause interference with legacy stations or APs. By default, these protection mechanisms are enabled (Auto). With protection enabled, protection mechanisms will be invoked if legacy devices are within range of the AP. This causes more overhead on every transmission, which will impact performance. However, there is no impact on performance if there are no legacy devices within range of the AP.</p> <p>You can disable (Off) these protection mechanisms; however, when 802.11n protection is off, legacy clients or APs within range can be affected by 802.11n transmissions. The 802.11 protection feature is also available when the mode is 802.11b/g. When protection is enabled in this mode, it protects 802.11b clients and APs from 802.11g transmissions.</p> <p>Note: This setting does not affect the ability of the client to associate with the AP.</p>
Beacon Interval	<p>Beacon frames are transmitted by an AP at regular intervals to announce the existence of the wireless network. The default behaviour is to send a beacon frame once every 100 milliseconds (or 10 per second).</p> <p>Enter a value from 20 to 2000 milliseconds.</p>
DTIM Period	<p>Specify a DTIM period from 1 to 255 beacons.</p> <p>The Delivery Traffic Information Map (DTIM) message is an element included in some Beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the AP awaiting pick-up.</p> <p>The DTIM period you specify indicates how often the clients served by this AP should check for buffered data still on the AP awaiting pickup.</p> <p>The measurement is in beacons. For example, if you set this field to 1, clients will check for buffered data on the AP at every beacon. If you set this field to 10, clients will check on every 10th beacon.</p>
RTS Threshold	<p>Specify a Request to Send (RTS) Threshold value between 0 and 2347.</p> <p>The RTS threshold indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed.</p> <p>Changing the RTS threshold can help control traffic flow through the AP, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.</p>

Field	Description
Maximum Stations	Specify the maximum number of stations allowed to access this AP at any one time. You can enter a value between 0 and 200.
Transmit Power	Enter a percentage value for the transmit power level for this AP. The default value, which is 100% , can be more cost-efficient than a lower percentage since it gives the AP a maximum broadcast range and reduces the number of APs needed. To increase capacity of the network, place APs closer together and reduce the value of the transmit power. This helps reduce overlap and interference among APs. A lower transmit power setting can also keep your network more secure because weaker wireless signals are less likely to propagate outside of the physical location of your network.
Fixed Multicast Rate	Select the multicast traffic transmission rate you want the AP to support.
Legacy Rate Sets	Check the transmission rate sets you want the AP to support and the basic rate sets you want the AP to advertise: <ul style="list-style-type: none"> •) Rates are expressed in megabits per second. •) Supported Rate Sets indicate rates that the AP supports. You can check multiple rates (click a check box to select or de-select a rate). The AP will automatically choose the most efficient rate based on factors like error rates and distance of client stations from the AP. •) Basic Rate Sets indicate rates that the AP will advertise to the network for the purposes of setting up communication with other APs and client stations on the network. It is generally more efficient to have an AP broadcast a subset of its supported rate sets.
DHCP Offer/ACK to Unicast	Enabling this feature will convert BOOTP replies from DHCP server to Unicast and send to the requesting wireless client.
Forced Roaming	Enabling this feature will detect and disconnect wireless clients based on the client RSSI. If the client RSSI falls below the roaming threshold value, the client will be disassociated. Further association attempts will be monitored and disconnected 3 times if its RSSI is below the threshold value. If still the client tries association 4th time, the association will be logged and allowed to connect.
Airtime Fairness	The purpose of this is to enable/disable Airtime Fairness. This feature addresses the issue of slower data transfers throttling the higher speed ones.

Table 13 - Radio Settings

Use the **Radio** page to configure both Radio One and Radio Two. The settings on the page apply only to the radio that you choose from the Radio drop-down list. After you configure settings for one of the radios, click **Apply** and then select and configure the other radio. Be sure to click **Apply** to apply the second set of configuration settings for the other radio.

Configuring Radio and VAP Scheduler

The Radio and VAP scheduler is a standalone AP feature. To configure the Radio and VAP scheduler, select the **Scheduler** tab in the **Manage** section. The Radio and VAP Scheduler allows you to configure a rule with a specific time interval for VAPs or radios to be operational, thereby automating the enabling or disabling of the VAPs and Radios.

One of the ways you can use this feature is to schedule radios to operate only during the office working hours in order to achieve security and reduce power consumption. You can also use the Scheduler to allow access to VAPs for wireless clients only during specific times of day.

Each rule specifies the start time, end time and day (or days) of the week the radio or VAP can be operational. The rules are periodic in nature and are repeated every week.

A valid rule must contain all of the following parameters:

-) Days of the Week.
-) Start Time (hour and minutes).
-) End Time (hour and minutes).

Only valid rules are added to the profile. Up to 16 rules are grouped together to form a scheduling profile. Any two periodic rules time entries belonging to the same profile must not overlap. The time granularity for the schedules is one minute. The AP supports up to 16 profiles.

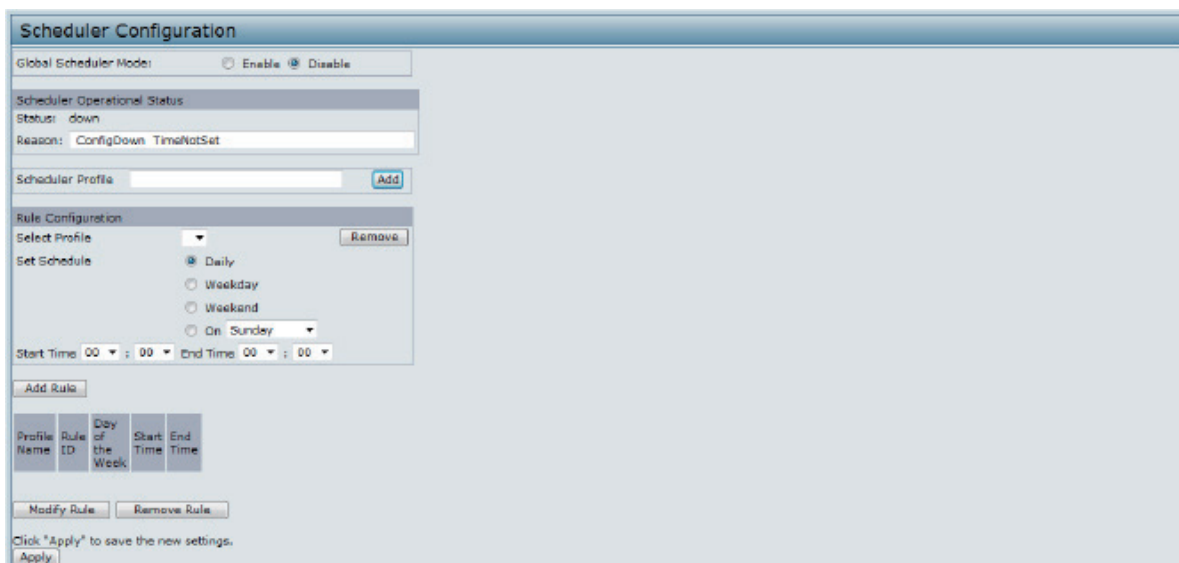


Figure 14 - Scheduler Configuration

Field	Description
Global Scheduler Mode	A global switch to enable or disable the scheduler feature. The default is Disable .
Scheduler Operational Status	
Status	The operational status of the Scheduler. The range is Up or Down . The default is Down .
Reason	Provides additional information about the status. The reason can be one or more of the following: <ul style="list-style-type: none"> •) IsActive – Operational status is up. •) ConfigDown – Operational status is down because global configuration is disabled. •) TimeNotSet – Operational status is down because the AP time has not been set, either manually or by specifying an NTP server to use. •) ManagedMode– Operational status is down because the AP is in managed mode.
Scheduler Profile	The Scheduler profile defines the list of profiles names that can be associated to the VAP or Radio configuration. Rules are associated with a named scheduler profile. You can define up to 16 scheduler profile names. By default, no profiles are created. The profile name can be up to 32 alphanumeric characters. Click Add to add the profile name.
Rule Configuration	Each scheduler profile may have up to 16 periodic rules. The list of parameters for each periodic rule are described below.
Select Profile	Select the profile name from the menu.
Set Schedule	The day of the week. Range is: Daily , Weekday (Monday to Friday), Weekend (Saturday and Sunday), Monday , Tuesday , Wednesday , Thursday , Friday , Saturday , Sunday . The default is Daily .
Start Time	The time when the radio or VAP will be operationally enabled. The time is in HH:MM 24-hour format. The range is <00-23>:<00-59>. The default is 00:00.
End Time	The time when the radio or VAP will be operationally disabled. The time is in HH:MM 24-hour format. The range is <00-23>:<00-59>. The default is 00:00.

Table 14 - Scheduler Configuration

After you select a profile from the **Select Profile** field, the rules that have been added to the selected profile appear in the table below the *Rule Configuration* area. When you add a new rule to a profile, it appears in the table. Use the **Modify Rule** and **Remove Rule** buttons to manage the rules associated with a profile.

Use the following buttons to perform their respective tasks:

-) **Add**: To add a scheduler profile, specify the name of the profile in the appropriate field and click **Add**.

-) **Remove:** To remove a scheduler profile, select it from the Select Profile field in the Rule Configuration table and click **Remove**.
-) **Add Rule:** After you configure the rule settings, click **Add Rule** to add the rule to the selected profile.
-) **Modify Rule:** To change an existing rule, select the rule, update the values in the **Rule Configuration** area, and click **Modify Rule**.
-) **Remove Rule:** To delete a rule from a profile, select the rule and click **Remove Rule**.
-) **Apply:** After making any modifications to the rules, click **Apply** to apply the changes and to save the settings.

Figure 15 - Scheduler Configuration (Modify Rule)

Click **Apply** to save the new configuration settings.



Note: After making any modifications, you must click **Apply** to apply the changes and to save the settings.

Scheduler Association Settings

For a Scheduler profile to take effect, you must associate it with at least one radio or VAP interface. To associate the Scheduler profiles, select the **Scheduler Association** tab in the **Manage** section. By default, there are no Scheduler profiles created, so no profile is associated to any radio or VAP. The Scheduler profile needs to be explicitly associated to a radio or VAP configuration. Only one Scheduler profile can be associated to any radio or VAP configuration; however, a single profile can be associated to multiple radios or VAPs. If the Scheduler profile associated with a VAP or radio is deleted, then the associated profile to the VAP or radio is removed implicitly. If the radio is operationally disabled, then all the VAPs associated to that radio are also operationally disabled irrespective of the VAP configuration.

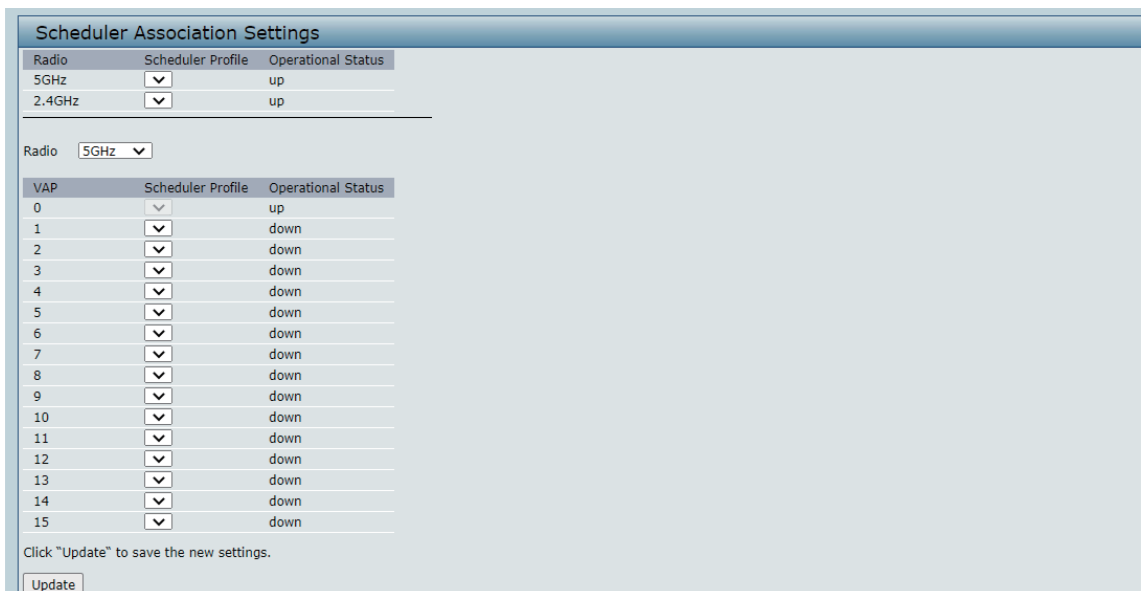


Figure 16 - Scheduler Association Settings

Field	Description
Radio Scheduler Profile Operational Status	
5GHz or 2.4GHz	From the menu, select the Scheduler profile to associate with 5GHz Radio or 2.4GHz Radio.
Scheduler Profile	From the menu, select the Scheduler profile to associate with the Radio.
Status	The operational status of the Scheduler, which is either Up or Down .
VAP Scheduler Profile Operational Status	
Radio	From the menu, select 5GHz Radio or 2.4GHz Radio to associate the VAP Scheduler Profile.
VAP	Identifies the VAP associated with the rest of the information in the row.
0-15 or Scheduler Profile	From the menu, select the Scheduler profile to associate with the respective VAP.
Operational Status	The operational status of the Scheduler. The range is Up or Down .

Table 15 - Scheduler Association Settings

	Note: After you associate a Scheduler profile with a Radio interface or a VAP interface, you must click Apply to apply the changes and to save the settings.
--	--

Virtual Access Point Settings

To change VAP 0 or to enable and configure additional VAPs, select the **VAP** tab in the **Manage** section.

VAPs segment the wireless LAN into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. VAPs simulate multiple APs in one physical AP. Each radio supports up to 16 VAPs.

For each VAP, you can customize the security mode to control wireless client access. Each VAP can also have a unique SSID. Multiple SSIDs make a single AP look like two or more APs to other systems on the network. By configuring VAPs, you can maintain better control over broadcast and multicast traffic, which affects network performance.

You can configure each VAP to use a different VLAN, or you can configure multiple VAPs to use the same VLAN, whether the VLAN is on the same radio or on a different radio. VAP0, which is always enabled on both radios, is assigned to the default VLAN 1.

The AP adds VLAN ID tags to wireless client traffic based on the VLAN ID you configure on the VAP page or by using the RADIUS server assignment. If you use an external RADIUS server, you can configure multiple VLANs on each

VAP. The external RADIUS server assigns wireless clients to the VLAN when the clients associate and authenticate.

You can configure up to four global IPv4 or IPv6 RADIUS servers. One of the servers always acts as a primary while the others act as backup servers. The network type (IPv4 or IPv6) and accounting mode are common across all configured RADIUS servers. You can configure each VAP to use the global RADIUS server settings, which is the default, or you can configure a per-VAP RADIUS server set. You can also configure separate RADIUS server settings for each VAP. For example, you can configure one VAP to use an IPv6 RADIUS server while other VAPs use the global IPv4 RADIUS server settings you configure.

If wireless clients use a security mode that does not communicate with the RADIUS server, or if the RADIUS server does not provide the VLAN information, you can assign a VLAN ID to each VAP. The AP assigns the VLAN to all wireless clients that connect to the AP through that VAP.



Note: Before you configure VLANs on the AP, be sure to verify that the switch and DHCP server the AP uses can support IEEE 802.1Q VLAN encapsulation.

To set up multiple VAPs, click **Manage > VAP**.

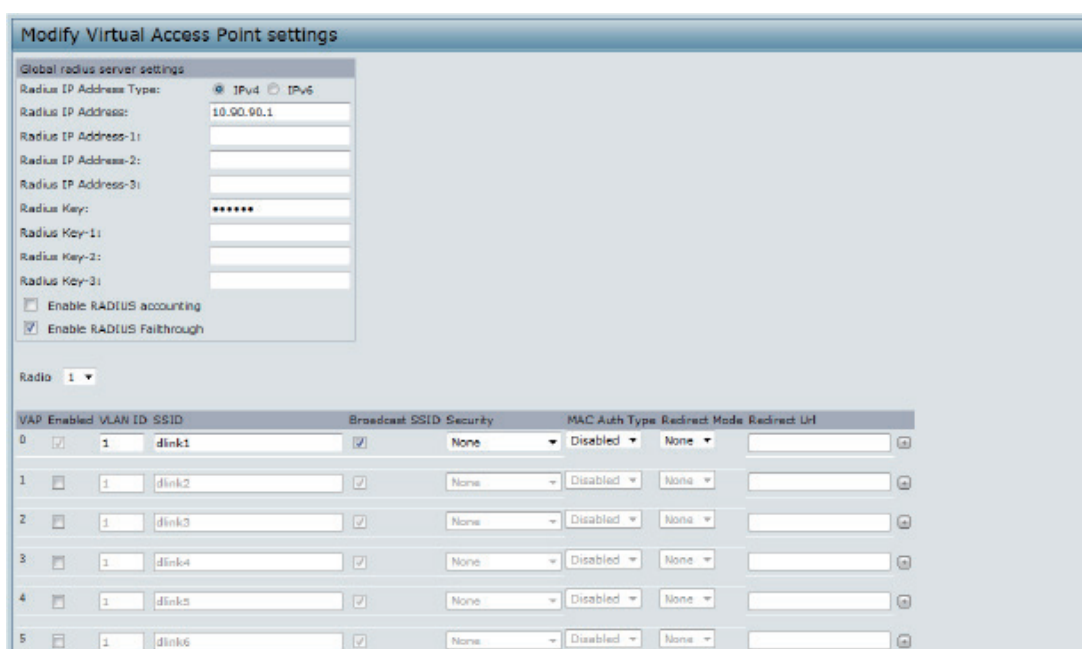


Figure 17 - Modify Virtual Access Point Settings

The following table describes the fields and configuration options on the **VAP** page.

Field	Description
RADIUS IP Address Type	Specify the IP version that the RADIUS server uses. You can toggle between the address types to configure IPv4 and IPv6 global RADIUS address settings, but the AP contacts only the RADIUS server or servers for the address type you select in this field.
RADIUS IP Address RADIUS IPv6 Address	Enter the IPv4 or IPv6 address for the primary global RADIUS server. By default, each VAP uses the global RADIUS settings that you define for the AP at the top of the VAP page. When the first wireless client tries to authenticate with the AP, the AP sends an authentication request to the primary server. If the primary server responds to the authentication request, the AP continues to use this RADIUS server as the primary server, and authentication requests are sent to the address you specify. If the IPv4 RADIUS IP Address Type option is selected in the previous field, enter the IP address of the RADIUS server that all VAPs use by default, for example 192.168.10.23. If the IPv6 RADIUS IP Address Type option is selected, enter the IPv6 address of the primary global RADIUS server, for example 2001:0db8:1234::abcd.

Field	Description
RADIUS IP or IPv6 Address 1-3	Enter up to three IPv4 or IPv6 addresses to use as the backup RADIUS servers. The field label is RADIUS IP Address when the IPv4 RADIUS IP Address Type option is selected and RADIUS IPv6 Address when the IPv6 RADIUS IP Address Type option is selected. If authentication fails with the primary server, each configured backup server is tried in sequence. The IPv4 or IPv6 address must be valid in order for the AP to attempt to contact the server.
RADIUS Key	Enter the RADIUS key in the text box. The <i>RADIUS Key</i> is the shared secret key for the global RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive, and you must configure the same key on the AP and on your RADIUS server. The text you enter will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type.
RADIUS Key 1-3	Enter the RADIUS key associated with the configured backup RADIUS servers. The server at RADIUS IP Address-1 uses RADIUS Key-1, RADIUS IP Address-2 uses RADIUS Key-2, and so on.
Enable RADIUS Accounting	Select this option to track and measure the resources a particular user has consumed such as system time, amount of data transmitted and received, and so on. If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers.
Enable RADIUS FailThrough	Select this option to allow the secondary RADIUS server to authenticate wireless clients if the authentication with the primary RADIUS server is unsuccessful, or if the primary RADIUS server is unavailable.
Radio	Select the radio to configure. VAPs are configured independently on each radio.
VAP	You can configure up to 16 VAPs for each radio. VAP0 is the physical radio interface, so to disable VAP0, you must disable the radio.
Enabled	You can enable or disable a configured network. <ul style="list-style-type: none"> •) To enable the specified network, select the Enabled option beside the appropriate VAP. •) To disable the specified network, clear the Enabled option beside the appropriate VAP. If you disable the specified network, you will lose the VLAN ID you entered.
VLAN ID	When a wireless client connects to the AP by using this VAP, the AP tags all traffic from the wireless client with the VLAN ID you enter in this field unless you enter the untagged VLAN ID or use a RADIUS server to assign a wireless client to a VLAN. The range for the VLAN ID is 1 – 4094. If you use RADIUS-based authentication for clients, you can optionally add the following attributes to the appropriate file in the RADIUS or AAA server to configure a VLAN for the client: <ul style="list-style-type: none"> •) "Tunnel-Type" •) "Tunnel-Medium-Type" •) "Tunnel-Private-Group-ID" The RADIUS-assigned VLAN ID overrides the VLAN ID you configure on the VAP page. You configure the untagged and management VLAN IDs on the Ethernet Settings page. For more information, see " Ethernet Settings " on page 23.
SSID	Enter a name for the wireless network. The SSID is an alphanumeric string of up to 32 characters. You can use the same SSID for multiple VAPs, or you can choose a unique SSID for each VAP. Note: If you are connected as a wireless client to the same AP that you are administering, resetting the SSID will cause you to lose connectivity to the AP. You will need to reconnect to the new SSID after you save this new setting.

Field	Description
Broadcast SSID	<p>Specify whether to allow the AP to broadcast the Service Set Identifier (SSID) in its beacon frames. The Broadcast SSID parameter is enabled by default. When the VAP does not broadcast its SSID, the network name is not displayed in the list of available networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it is able to connect.</p> <ul style="list-style-type: none"> •) To enable the SSID broadcast, select the Broadcast SSID check box. •) To prohibit the SSID broadcast, clear the Broadcast SSID check box. <p>Note: Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect or monitor unencrypted traffic. Suppressing the SSID broadcast offers a very minimal level of protection on an otherwise exposed network (such as a guest network) where the priority is making it easy for clients to get a connection and where no sensitive information is available.</p>
Security	<p>Select one of the following Security modes for this VAP:</p> <ul style="list-style-type: none"> •) None •) WPA Personal •) WPA Enterprise •) OWE <p>If you select a security mode other than None, additional fields appear. These fields are explained below.</p> <p>Note: The Security mode you set here is specifically for this VAP.</p>
MAC Authentication Type	<p>You can configure a global list of MAC addresses that are allowed or denied access to the network. The drop-down menu for this feature allows you to select the type of MAC Authentication to use:</p> <ul style="list-style-type: none"> •) Disabled: Do not use MAC Authentication. •) Local: Use the MAC Authentication list that you configure on the MAC Authentication page. •) RADIUS: Use the MAC Authentication list on the external RADIUS server. <p>For more information about MAC Authentication, see “Controlling Access by MAC Authentication” on page 40.</p>

Table 16 - Virtual Access Point Settings



Note: After you configure the VAP settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

None (Plain-text)

If you select **None** as your security mode, no further options are configurable on the AP. This mode means that any data transferred to and from the UAP is not encrypted. This security mode can be useful during initial network configuration or for problem solving, but it is not recommended for regular use on the Internal network because it is not secure.

WPA Personal

WPA Personal is a Wi-Fi Alliance IEEE 802.11i standard, which includes AES-CCMP and TKIP mechanisms. The Personal version of WPA employs a pre-shared key (instead of using IEEE 802.1X and EAP as is used in the Enterprise WPA security mode). The PSK is used for an initial check of credentials only.

This security mode is backwards-compatible for wireless clients that support the original WPA.

Figure 18 - Modify Virtual Access Point Settings (WPA Personal)

Field	Description
WPA Versions	<p>Select the types of client stations you want to support:</p> <ul style="list-style-type: none"> • WPA. If all client stations on the network support the original WPA but none support the newer WPA2/3, then select WPA. • WPA2. If all client stations on the network support WPA2, it provides the security per the IEEE 802.11i standard. • WPA3. If all client stations on the network support WPA3, we suggest using WPA3 which provides the cutting-edge security protocols, enables more robust authentication, delivers increased cryptographic strength for your network. • WPA2 and WPA3. If you have a mix of clients, some of which support WPA3 and others which support only the original WPA2, select both of the check boxes. This lets both WPA2 and WPA3 client stations associate and authenticate, but uses the more robust WPA3 for clients who support it.
Key	The Pre-shared Key is the shared secret key for WPA Personal. Enter a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.
Broadcast Key Refresh Rate	Enter a value to set the interval at which the broadcast (group) key is refreshed for clients associated to this VAP (the default is 3600). The valid range is 0–86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

Table 17 - WPA Personal



Note: After you configure the security settings, you must click **Apply** to apply the changes and to save the settings.

WPA Enterprise

WPA Enterprise with RADIUS is an implementation of the Wi-Fi Alliance IEEE 802.11i standard, which includes CCMP (AES), and TKIP mechanisms. The Enterprise mode requires the use of a RADIUS server to authenticate users.

This security mode is backwards-compatible with wireless clients that support the original WPA.

Figure 19 - Modify Virtual Access Point Settings (WPA Enterprise)

Field	Description
WPA Versions	Select the types of client stations you want to support: <ul style="list-style-type: none"> •) WPA. If all client stations on the network support the original WPA but none support the newer WPA2/3, then select WPA. •) WPA2. If all client stations on the network support WPA2, it provides the security per the IEEE 802.11i standard. •) WPA3. If all client stations on the network support WPA3, we suggest using WPA3 which provides the cutting-edge security protocols, enables more robust authentication, delivers increased cryptographic strength for your network.
Use Global RADIUS Server Settings	By default each VAP uses the global RADIUS settings that you define for the AP at the top of the VAP page. However, you can configure each VAP to use a different set of RADIUS servers. To use the global RADIUS server settings, make sure the check box is selected. To use a separate RADIUS server for the VAP, clear the check box and enter the RADIUS server IP address and key in the following fields.
RADIUS IP Address Type	Specify the IP version that the RADIUS server uses. You can toggle between the address types to configure IPv4 and IPv6 global RADIUS address settings, but the AP contacts only the RADIUS server or servers for the address type you select in this field.
RADIUS IP Address RADIUS IPv6 Address	Enter the IPv4 or IPv6 address for the primary RADIUS server for this VAP. If the IPv4 RADIUS IP Address Type option is selected in the previous field, enter the IP address of the RADIUS server that all VAPs use by default, for example 192.168.10.23. If the IPv6 RADIUS IP Address Type option is selected, enter the IPv6 address of the primary global RADIUS server, for example 2001:0db8:1234::abcd.
RADIUS IP or IPv6 Address 1–3	Enter up to three IPv4 and/or IPv6 addresses to use as the backup RADIUS servers for this VAP. The field label is RADIUS IP Address when the IPv4 RADIUS IP Address Type option is selected and RADIUS IPv6 Address when the IPv6 RADIUS IP Address Type option is selected. If authentication fails with the primary server, each configured backup server is tried in sequence.
RADIUS Key	Enter the RADIUS key in the text box. The <i>RADIUS Key</i> is the shared secret key for the global RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive, and you must configure the same key on the AP and on your RADIUS server. The text you enter will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type.
RADIUS Key 1–3	Enter the RADIUS key associated with the configured backup RADIUS servers. The server at RADIUS IP Address-1 uses RADIUS Key-1, RADIUS IP Address-2 uses RADIUS Key-2, and so on.
Enable RADIUS Accounting	Select this option to track and measure the resources a particular user has consumed such as system time, amount of data transmitted and received, and so on. If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers.
Active Server	Specify which configured RADIUS server to use as the active RADIUS server.
Broadcast Key Refresh Rate	Enter a value to set the interval at which the broadcast (group) key is refreshed for clients associated to this VAP (the default is 3600). The valid range is 0–86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.
Session Key Refresh Rate	Enter a value to set the interval at which the AP will refresh session (unicast) keys for each client associated to the VAP. The valid range is 0–86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

Table 18 - WPA Enterprise



Note: After you configure the security settings, you must click **Apply** to apply the changes and to save the settings.

Configuring Wireless Multicast Forwarding

The Wireless Multicast Forwarding provides an efficient way to forward the multicast traffic on the wireless medium and overcomes the multicast transmission issues on WLAN using the repeated unicast of multicast frames. It uses IGMP frames to keep track of participating group members, and multicast packets are transmitted only to the interested members after unicast MAC conversion .

With WMF, the data transfer is more reliable as the frames are sent as unicast, and robust transmission is possible as dynamic per station rate control can be done based on the link errors and noise conditions. The multicast group members can be a STA end point. Streaming between STA devices will also be supported. The multicast streaming server can be attached to any of the LAN ports.

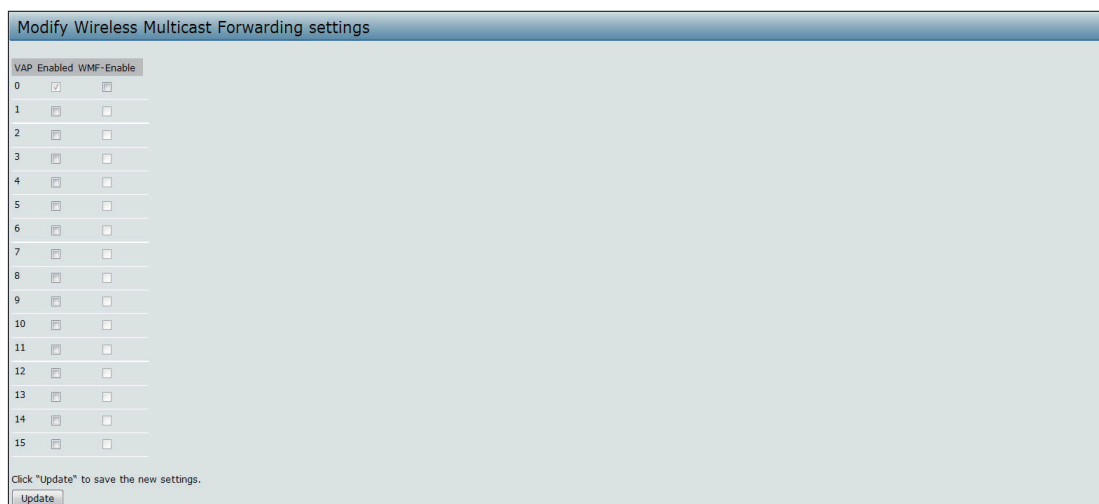


Figure 20 - Wireless Multicast Forwarding

Field	Description
VAP	<ul style="list-style-type: none"> •) You can configure up to 16 VAPs for each radio. •) VAP0 is the physical radio interface, so to disable VAP0, you must disable the radio.
Enabled	You can enable or disable a configured network. If you disable the specified network, you will lose the VLAN ID you enabled
WMF-Enable	Enable/Disable the WMF status in a VAP.

Table 19 - Wireless Multicast Forwarding

Configuring the Wireless Distribution System (WDS)

The Wireless Distribution System (WDS) allows you to connect multiple UAPs. With WDS, APs communicate with one another without wires in a standardized way. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required. You can configure the AP in point-to-point or point-to-multipoint bridge mode based on the number of links to connect.

In the point-to-point mode, the AP accepts client associations and communicates with wireless clients and other repeaters. The AP forwards all traffic meant for the other network over the tunnel that is established between the APs. The bridge does not add to the hop count. It functions as a simple OSI layer 2 network device.

In the point-to-multipoint bridge mode, one AP acts as the common link between multiple APs. In this mode, the central AP accepts client associations and communicates with the clients and other repeaters. All other APs associate only with the central AP that forwards the packets to the appropriate wireless bridge for routing purposes.

The UAP can also act as a repeater. In this mode, the AP serves as a connection between two APs that might be too far apart to be within cell range. When acting as a repeater, the AP does not have a wired connection to the LAN

and repeats signals by using the wireless connection. No special configuration is required for the AP to function as a repeater, and there are no repeater mode settings. Wireless clients can still connect to an AP that is operating as a repeater.



Note: When you move an AP from Standalone Mode to Managed Mode, WDS is disabled. In Managed Mode, you configure the AP by using the D-Link Unified Wireless Switch. The Administrator UI, as well as Telnet, SSH, and SNMP access are disabled when the AP is in Managed Mode.

To specify the details of traffic exchange from this access point to others, click the **WDS** tab.

Figure 21 - Configure WDS Bridges

Before you configure WDS on the AP, note the following guidelines:

-) When using WDS, be sure to configure WDS settings on *both* APs participating in the WDS link.
-) You can have only one WDS link between any pair of APs. That is, a remote MAC address may appear only once on the WDS page for a particular AP.
-) Both APs participating in a WDS link must be on the same Radio channel and using the same IEEE 802.11 mode. (See “[Modifying Radio Settings](#)” on page 26 for information on configuring the Radio mode and channel.)
-) When 802.11h is operational, setting up two WDS links can be difficult.


To configure WDS on this AP, describe each AP intended to receive handoffs and send information to this AP. For each destination AP, configure the fields listed in the table below.

Field	Description
Spanning Tree Mode	Spanning Tree Protocol (STP) prevents switching loops. STP is recommended if you configure WDS links. Select Enabled to use STP Select Disabled to turn off STP links (not recommended)
Radio	For each WDS link on a two-radio AP, select 5GHz Radio or 2.4GHz Radio. The rest of the settings for the link apply to the radio selected in this field. The read-only Local Address will change depending on which Radio you select in this field.
Local Address	Indicates the MAC addresses for this AP. For each WDS link on a two-radio AP, the Local Address reflects the MAC address for the internal interface on the selected radio (Radio One on wlan0 or Radio Two on wlan1).

Field	Description
Remote Address	Specify the MAC address of the destination AP; that is, the AP on the other end of the WDS link to which data will be sent or handed-off and from which data will be received. Click the drop-down arrow to the right of the Remote Address field to see a list of all the available MAC Addresses and their associated SSIDs on the network. Select the appropriate MAC address from the list. Note: The SSID displayed in the drop-down list is simply to help you identify the correct MAC Address for the destination AP. This SSID is a separate SSID to that which you set for the WDS link. The two do not (and should not) be the same value or name.
Encryption	You can use None or WPA on the WDS link. If you are unconcerned about security issues on the WDS link you may decide not to set any type of encryption.


Table 20 - WDS Settings

If you select **None** as your preferred WDS encryption option, you will not be asked to fill in any more fields on the **WDS** page. All data transferred between the two APs on the WDS link will be unencrypted.

	Note: To disable a WDS link, you must remove the value configured in the Remote Address field.
---	---


WPA/PSK on WDS Links

The following table describes the additional fields that appear when you select WPA/PSK as the encryption type.

	Note: In order to configure WPA-PSK on any WDS link, VAP0 of the selected radio must be configured for WPA-PSK or WPA-Enterprise.
--	--

Field	Description
Encryption	WPA (PSK)
SSID	Enter an appropriate name for the new WDS link you have created. This SSID should be different from the other SSIDs used by this AP. However, it is important that the same SSID is also entered at the other end of the WDS link. If this SSID is not the same for both APs on the WDS link, they will not be able to communicate and exchange data. The SSID can be any alphanumeric combination.
Key	Enter a unique shared key for the WDS bridge. This unique shared key must also be entered for the AP at the other end of the WDS link. If this key is not the same for both APs, they will not be able to communicate and exchange data. The WPA-PSK key is a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.

Table 21 - WPA/PSK on WDS Links

	Note: After you configure the WDS settings, you must click Apply to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.
---	--

Controlling Access by MAC Authentication

A Media Access Control (MAC) address is a hardware address that uniquely identifies each node of a network. All IEEE 802 network devices share a common 48-bit MAC address format, usually displayed as a string of 12 hexadecimal digits separated by colons, for example 00:DC:BA:09:87:65. Each wireless network interface card (NIC) used by a wireless client has a unique MAC address.

You can use the Administrator UI on the AP or use an external RADIUS server to control access to the network through the AP based on the MAC address of the wireless client. This feature is called MAC Authentication or MAC Filtering. To control access, you configure a global list of MAC addresses locally on the AP or on an external RADIUS server. Then, you set a filter to specify whether the clients with those MAC addresses are allowed or denied access to the network. When a wireless client attempts to associate with an AP, the AP looks up the MAC address of the client in the local Stations List or on the RADIUS server. If it is found, the global allow or deny setting is applied. If it is not found, the opposite is applied.

On the **VAP** page, the MAC Authentication Type setting controls whether the AP uses the station list configured locally on the **MAC Authentication** page or the external RADIUS server. The Allow/Block filter setting on the **MAC Authentication** page determines whether the clients in the station list (local or RADIUS) can access the network through the AP. For more information about setting the MAC authentication type, see “Virtual Access Point Settings” on page 32.

Configuring a MAC Filter and Station List on the AP

The **MAC Authentication** page allows you to control access to UAP based on MAC addresses. Based on how you set the filter, you can *allow* only client stations with a listed MAC address or *deny* access to the stations listed.

When you enable MAC Authentication and specify a list of approved MAC addresses, only clients with a listed MAC address can access the network. If you specify MAC addresses to deny, all clients can access the network except for the clients on the deny list.

To enable filtering by MAC address, click the **MAC Authentication** tab.



Figure 22 - Configure MAC Authentication




Note: Global MAC Authentication settings apply to all VAPs on all supported radios.

The following table describes the fields and configuration options available on the MAC Authentication page.

Field	Description
Filter	<p>To set the MAC Address Filter, select one of the following options:</p> <ul style="list-style-type: none"> • Allow only stations in the list. Any station that is not in the Stations List is denied access to the network through the AP. • Block all stations in list. Only the stations that appear in the list are denied access to the network through the AP. All other stations are permitted access. <p>Note: The filter you select is applied to the clients in the station list, regardless of whether that station list is local or on the RADIUS server.</p>

Field	Description
Stations List	<p>This is the local list of clients that are either permitted or denied access to the network through the AP. To add a MAC Address to the local Stations List, enter its 48-bit MAC address into the lower text boxes, then click Add.</p> <p>To remove a MAC Address from the Stations List, select its 48-bit MAC address, then click Remove.</p> <p>The stations in the list will either be allowed or denied access based on how you set the filter in the previous field.</p> <p>Note: If the MAC authentication type for the VAP is set to Local, the AP uses the Stations List to permit or deny the clients access to the network. If the MAC authentication type is set to RADIUS, the AP ignores the MAC addresses configured in this list and uses the list that is stored on the RADIUS server. The MAC authentication type is set on the VAP configuration page.</p>

Table 22 - MAC Authentication

	<p>Note: After you configure local MAC Authentication settings, you must click Apply to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.</p>
---	--

Configuring MAC Authentication on the RADIUS Server

If you use RADIUS MAC authentication for MAC-based access control, you must configure a station list on the RADIUS server. The station list contains client MAC address entries, and the format for the list is described in the following table.

RADIUS Server Attribute	Description	Value
User-Name (1)	MAC address of the client station.	Valid Ethernet MAC Address.
User-Password (2)	A fixed global password used to lookup a client MAC entry.	NOPASSWORD

Table 23 - RADIUS Server Attributes for MAC Authentication

Configuring Load Balancing

You can set network utilization thresholds on the UAP to maintain the speed and performance of the wireless network as clients associate and disassociate with the AP. The load balancing settings apply to all supported radios.

To configure load balancing and set limits and behaviour to be triggered by a specified utilization rate of the access point, click the **Load Balancing** tab and update the fields shown in the following figure.

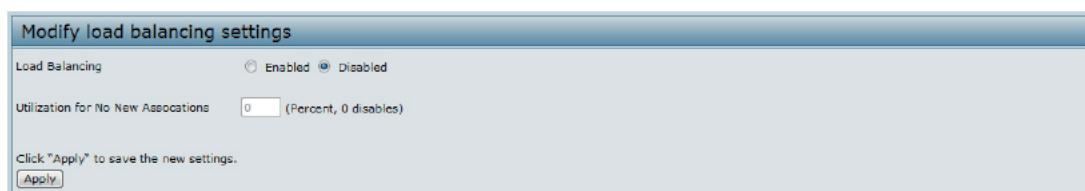


Figure 23 - Modify Load Balancing Settings

Field	Description
Load Balancing	<p>Enable or disable load balancing:</p> <p>To enable load balancing on this AP, click Enable.</p> <p>To disable load balancing on this AP, click Disable.</p>
Utilization for No New Associations	<p>Provide the percentage of network bandwidth utilization allowed on the radio before the AP stops accepting new client associations.</p> <p>The default is 0, which means that all new associations will be allowed regardless of the utilization rate.</p>

Table 24 - Load Balancing



Note: After you configure the load balancing settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

Managed Access Point Overview

The UAP can operate in two modes: **Standalone Mode** or **Managed Mode**. In Standalone Mode, the UAP acts as an individual AP in the network, and you manage it by using the Administrator Web User Interface (UI), CLI, or SNMP. In Managed Mode, the UAP is part of the D-Link Unified Wired and Wireless System, and you manage it by using the D-Link Unified Wireless Switch. If an AP is in Managed Mode, the Administrator Web UI, Telnet, SSH, and SNMP services are disabled.

On the UAP, you can configure the IP addresses of up to four D-Link Unified Wireless Switches that can manage it. In order to manage the AP, the switch and AP must discover each other. There are multiple ways for a switch to discover an AP. Adding the IP address of the switch to the AP while it is in Standalone Mode is one way to enable switch-to-AP discovery.

Transition Between Modes

Every 30 seconds, the D-Link Unified Wireless Switch sends a keepalive message to all of the access points it manages. Each AP checks for the keepalive messages on the SSL TCP connection. As long as the AP maintains communication with the switch through the keepalive messages, it remains in Managed Mode.

If the AP does not receive a message within 45 seconds of the last keepalive message, the AP assumes the switch has failed and terminates its TCP connection to the switch, and the AP enters Standalone Mode.

Once the AP transitions to Standalone Mode, it continues to forward traffic without any loss. The AP uses the configuration on the VAPs configured in VLAN Forwarding mode (the standard, non-tunneled mode).

While the AP is in Standalone Mode, you can manage it by using the Web interface or the CLI (through Telnet or SSH).

For any clients that are connected to the AP through tunneled VAPs, the AP sends disassociate messages and disables the tunneled VAPs.

As long as the Managed AP Administrative Mode is set to Enabled, the AP starts discovery procedures. If the AP establishes a connection with a wireless switch, which may or may not be the same switch it was connected to before, the switch sends the AP its configuration and the AP sends the wireless switch information about all currently associated clients.

After the configuration from the switch is applied, the AP radio(s) restart. Client traffic is briefly interrupted until the radio(s) are up and the clients are re-associated.

Configuring Managed Access Point Settings

To add the IP address of a D-Link Unified Wireless Switch to the AP, click the **Managed Access Point** tab under the **Manage** heading and update the fields shown in the table below.

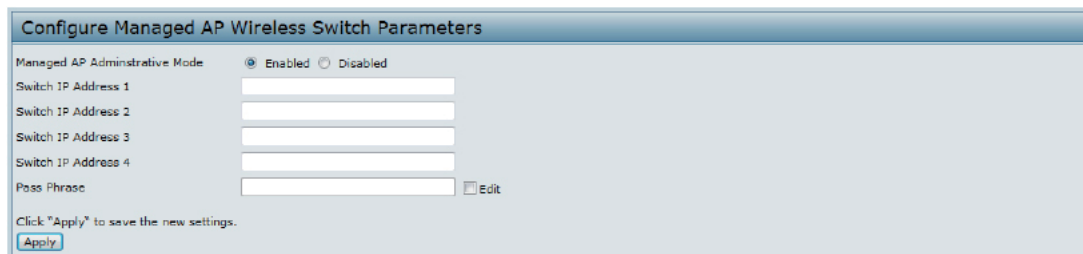



Figure 24 - Configure Managed AP Wireless Switch Parameters

Field	Description
Managed AP Administrative Mode	Click Enabled to allow the AP and switch to discover each other. If the AP successfully authenticates itself with a wireless switch, you will not be able to access the Administrator UI. Click Disabled to prevent the AP from contacting wireless switches.
Switch IP Address (1-4)	Enter the IP address of up to four wireless switches that can manage the AP. You can enter the IP address in dotted format or as a DNS name. You can view a list of wireless switches on your network that were configured by using a DHCP server. The AP attempts to contact Switch IP Address 1 first.
Base IP Port	The starting IP port number used by the wireless feature (in a range of 10 consecutive port numbers). Only the first number in the range is configurable. The default value is 5775 (through 57784). Note: When the wireless Base IP Port number is changed on the switch, the wireless feature is automatically disabled and re-enabled. The new value is not sent as part of the global switch configuration in the cluster configuration distribution command; every switch in the cluster must be configured independently with the new Wireless IP port number. Note: When the wireless Base IP Port number is changed from its default value on the switch, it must also be changed on the Access Points.
Pass Phrase	Select the Edit option and enter a passphrase to allow the AP to authenticate itself with the wireless switch. The passphrase must be between 8 and 63 characters. To remove the password, select Edit , delete the existing password, and then click Apply . You must configure the same passphrase on the switch.

Table 25 - Managed Access Point

	Note: After you configure the settings on the Managed Access Point page, you must click Apply to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.
---	---

If the UAP successfully authenticates with a D-Link Unified Wireless Switch, you will lose access to the AP through the Administrator UI.

Configuring 802.1X Authentication

On networks that use IEEE 802.1X, port-based network access control, a supplicant (client) cannot gain access to the network until the 802.1X authenticator grants access. If your network uses 802.1X, you must configure 802.1X authentication information that the AP can supply to the authenticator.

To configure the UAP 802.1X supplicant user name and password by using the Web interface, click the **Authentication** tab and configure the fields shown in the table below.

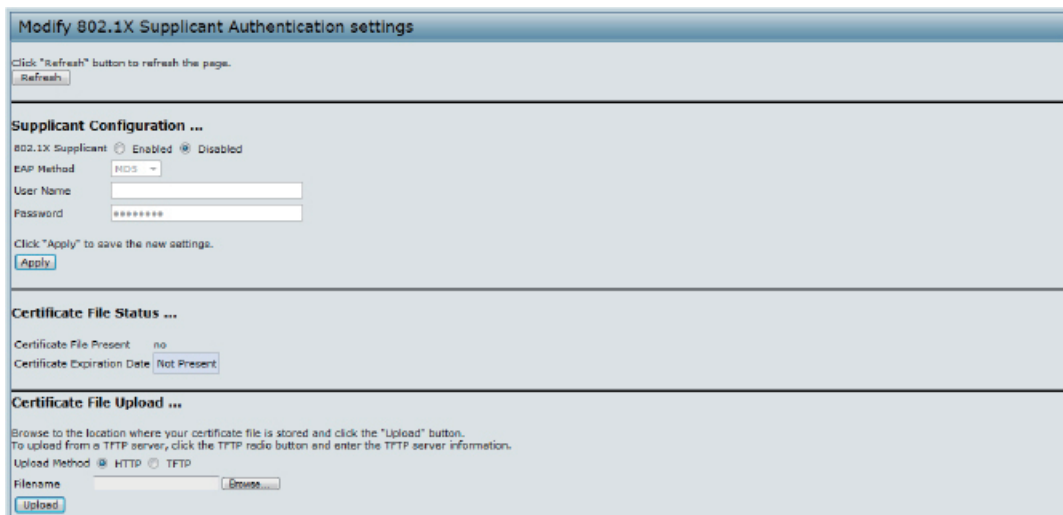



Figure 25 - Modify 802.1X Supplicant Authentication Settings

Field	Description
802.1X Supplicant	Click Enabled to enable the Administrative status of the 802.1X Supplicant. Click Disabled to disable the Administrative status of the 802.1X Supplicant.
EAP Method	MD5 as default.
Username	Enter the user name for the AP to use when responding to requests from an 802.1X authenticator. The user name can be 1 to 64 characters in length. ASCII printable characters are allowed, which includes upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.
Password	Enter the password for the AP to use when responding to requests from an 802.1X authenticator. The password can be 1 to 64 characters in length. ASCII printable characters are allowed, which includes upper and lower case letters, numbers, and special symbols such as @ and #.

Table 26 - IEEE 802.1X Supplicant Authentication

	Note: After you configure the settings on the Authentication page, you must click Apply to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.
---	---

Application Identification

The library package auto upgrade settings, automatically check the latest application library version based on given time interval.

Note: In managed mode, the controller will still sync the latest library version and request AP to upgrade latest library even the auto upgrade is disabled in the standalone mode.

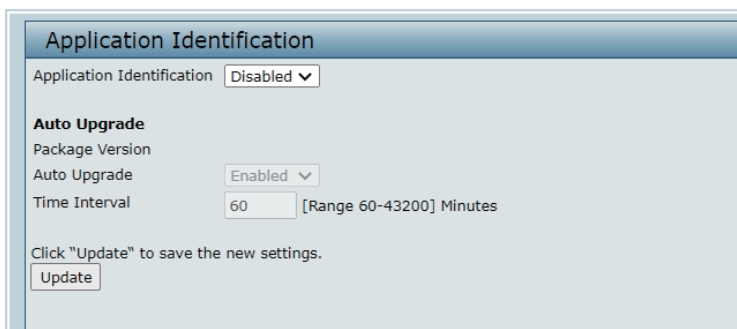


Figure 26 - Application Identification

Section 5 - Configuring Access Point Services

This section describes how to configure services on the UAP and contains the following subsections:

-) "Web Server Settings" on page 46
-) "Setting the SSH Status" on page 46
-) "Setting the Telnet Status" on page 47
-) "Configuring Quality of Service" on page 47
-) "Configuring SNMP on the Access Point" on page 48
-) "Enabling the Time Settings (NTP)" on page 50

Web Server Settings

The AP can be managed through HTTP or secure HTTP (HTTPS) sessions. By default both HTTP and HTTPS access are enabled. Either access type can be disabled separately.

To configure Web server settings, click **Web Server** tab.

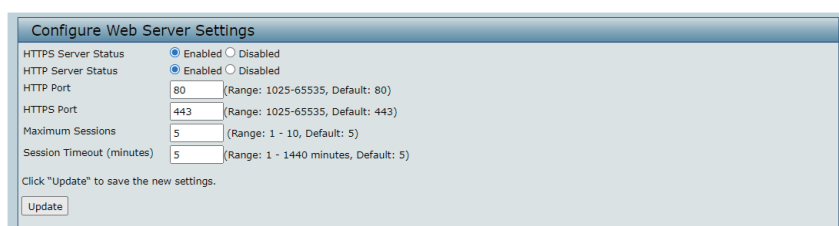


Figure 27 - Configure Web Server Settings

Field	Description
HTTPS Server Status	Enable or disable access through a Secure HTTP Server (HTTPS).
HTTP Server Status	Enable or disable access through HTTP. This setting is independent of the HTTPS server status setting.
HTTP Port	Specify the port number for HTTP traffic (default is 80).
HTTPS Port	Specify the port number for HTTPS traffic (default is 443).
Maximum Sessions	When a user logs on to the AP web interface, a session is created. This session is maintained until the user logs off or the session inactivity timer expires. Enter the number web sessions, including both HTTP and HTTPSs, that can exist at the same time. The range is 1–10 sessions. If the maximum number of sessions is reached, the next user who attempts to log on to the AP web interface receives an error message about the session limit.
Session Timeout	Enter the maximum amount of time, in minutes, an inactive user remains logged on to the AP web interface. When the configured timeout is reached, the user is automatically logged off the AP. The range is 1–1440 minutes (1440 minutes = 1 day).

Table 27 - Web Server Settings

	Note: Click Apply to apply the changes and to save the settings. If you disable the protocol you are currently using to access the AP management interface, the current connection will end and you will not be able to access the AP by using that protocol until it is enabled.
--	---

Setting the SSH Status

Secure Shell (SSH) is a program that provides access to the AP CLI from a remote host. SSH is more secure than Telnet for remote access because it provides strong authentication and secure communications over insecure channels. From the SSH page, you can enable or disable SSH access to the system.

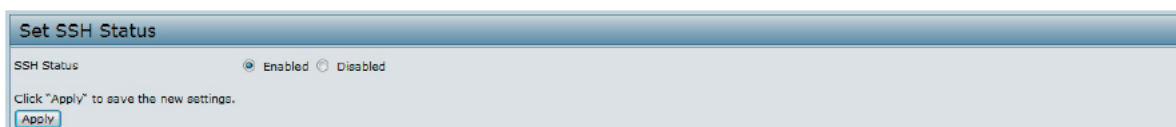


Figure 28 - Set SSH Status

Field	Description
SSH Status	Choose to either enable or disable SSH access to the AP CLI: <ul style="list-style-type: none"> • To permit remote access to the AP by using SSH, click Enabled. • To prevent remote access to the AP by using SSH, click Disabled.

Table 28 - SSH Settings

Setting the Telnet Status

Telnet is a program that provides access to the AP CLI from a remote host. From the Telnet page, you can enable or disable Telnet access to the system.

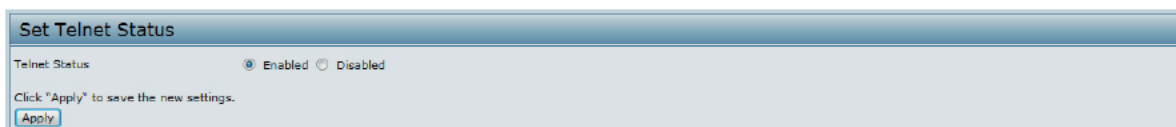


Figure 29 - Set Telnet Status

Field	Description
Telnet Status	Choose to either enable or disable Telnet access to the AP CLI: <ul style="list-style-type: none"> • To permit remote access to the AP by using Telnet, click Enabled. • To prevent remote access to the AP by using Telnet, click Disabled.

Table 29 - Telnet Settings

Configuring Quality of Service

Quality of Service (QoS) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like Voice-over-IP (VoIP), other types of audio, video, and streaming media, as well as traditional IP data over the UAP.

Configuring QoS on the UAP consists of setting parameters on existing queues for different types of wireless traffic, and effectively specifying minimum and maximum wait times (through Contention Windows) for transmission. The settings described here apply to data transmission behavior on the AP only, not to that of the client stations.

To set up queues for QoS, click the **QoS** tab under the **Services** heading and configure settings as described in the table below.

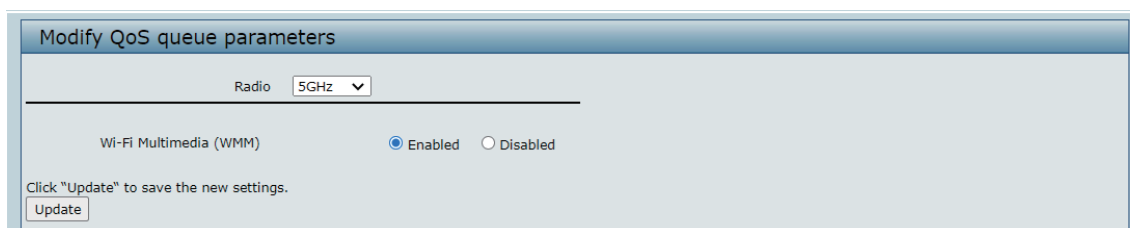


Figure 30 - Modify QoS Queue Parameters

Field	Description
Radio	Select the radio with the QoS settings to view or configure
Wi-Fi MultiMedia (WMM)	<p>Wi-Fi MultiMedia (WMM) is enabled by default. With WMM enabled, QoS prioritization and coordination of wireless medium access is on. With WMM enabled, QoS settings on the UAP control downstream traffic flowing from the AP to client station (AP EDCA parameters) and the upstream traffic flowing from the station to the AP (station EDCA parameters). Disabling WMM deactivates QoS control of station EDCA parameters on upstream traffic flowing from the station to the AP.</p> <p>With WMM disabled, you can still set some parameters on the downstream traffic flowing from the AP to the client station (AP EDCA parameters). To disable WMM extensions, click Disabled. To enable WMM extensions, click Enabled.</p>



Note: After you configure the QoS settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

Table 30 - QoS Settings

Configuring SNMP on the Access Point

Simple Network Management Protocol (SNMP) defines a standard for recording, storing, and sharing information about network devices. SNMP facilitates network management, troubleshooting, and maintenance. The AP supports SNMP versions 1, 2, and 3. Unless specifically noted, all configuration parameters on this page apply to SNMPv1 and SNMPv2c only.

Key components of any SNMP-managed network are managed devices, SNMP agents, and a management system. The agents store data about their devices in Management Information Bases (MIBs) and return this data to the SNMP manager when requested. Managed devices can be network nodes such as APs, routers, switches, bridges, hubs, servers, or printers.

The UAP can function as an SNMP managed device for seamless integration into network management systems such as HP OpenView.

From the **SNMP** page under the Services heading, you can start or stop control of SNMP agents, configure community passwords, access MIBs, and configure SNMP Trap destinations.

From the pages under the SNMPv3 heading, you can manage SNMPv3 users and their security levels and define access control to the SNMP MIBs. For information about how to configure SNMPv3 views, groups, users, and targets, see [“Section 6 - Configuring SNMPv3” on page 52](#).

To configure SNMP, click the **SNMP** tab under the **Services** heading and update the fields described in the table below.

The screenshot shows the 'SNMP Configuration' page. At the top, there are radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected. Below this, several fields are visible: 'Read-only community name' (public), 'Port number the SNMP agent will listen to' (161), 'Allow SNMP set requests' (Enabled), 'Read-write community name' (private), 'Restrict the source of SNMP requests to only the designated hosts or subnets' (Disabled), 'Hostname, address, or subnet of Network Management System' (default), and 'IPv6 hostname, address, or subnet of Network Management System' (default). A 'Trap Destinations' section includes a 'Community name for traps' (public) and three rows for 'Enabled Host Type' (IPv4) and 'Hostname or IP Address'. An 'Update' button is at the bottom.

Figure 31 - SNMP Configuration

Field	Description
SNMP Enabled/ Disabled	You can specify the SNMP administrative mode on your network. By default SNMP is enabled. To enable SNMP, click Enabled . To disable SNMP, click Disabled . After changing the mode, you must click Apply to save your configuration changes. Note: If SNMP is disabled, all remaining fields on the SNMP page are disabled. This is a global SNMP parameter which applies to SNMPv1, SNMPv2c, and SNMPv3.
Read-only community name (for permitted SNMP get operations)	Enter a read-only community name. The valid range is 1-256 characters. The community name, as defined in SNMPv2c, acts as a simple authentication mechanism to restrict the machines on the network that can request data to the SNMP agent. The name functions as a password, and the request is assumed to be authentic if the sender knows the password. The community name can be in any alphanumeric format.
Port number the SNMP agent will listen to	By default an SNMP agent only listens to requests from port 161 . However, you can configure this so the agent listens to requests on another port. Enter the port number on which you want the SNMP agents to listen to requests. The valid range is 1025-65535. Note: This is a global SNMP parameter that applies to SNMPv1, SNMPv2c, and SNMPv3.
Allow SNMP set requests	You can choose whether or not to allow SNMP set requests on the AP. Enabling SNMP set requests means that machines on the network can execute configuration changes via the SNMP agent on the AP to the D-Link System MIB. To enable SNMP set requests, click Enabled . To disable SNMP set requests, click Disabled .
Read-write community name (for permitted SNMP set operations)	If you have enabled SNMP set requests you can set a read-write community name. The valid range is 1-256 characters. Setting a community name is similar to setting a password. Only requests from the machines that identify themselves with this community name will be accepted. The community name can be in any alphanumeric format.
Restrict the source of SNMP requests to only the designated hosts or subnets	You can restrict the source of permitted SNMP requests. To restrict the source of permitted SNMP requests, click Enabled . To permit any source submitting an SNMP request, click Disabled .

Field	Description
Hostname, address or subnet of Network Management System	<p>Specify the IPv4 DNS hostname or subnet of the machines that can execute get and set requests to the managed devices. The valid range is 1-256 characters.</p> <p>As with community names, this provides a level of security on SNMP settings. The SNMP agent will only accept requests from the hostname or subnet specified here.</p> <p>To specify a subnet, enter one or more subnetwork address ranges in the form <code>address/mask_length</code> where <code>address</code> is an IP address and <code>mask_length</code> is the number of mask bits. Both formats <code>address/mask</code> and <code>address/mask_length</code> are supported. Individual hosts can be provided for this, i.e. IP Address or Hostname. For example, if you enter a range of 192.168.1.0/24 this specifies a subnetwork with address 192.168.1.0 and a subnet mask of 255.255.255.0.</p> <p>The address range is used to specify the subnet of the designated NMS. Only machines with IP addresses in this range are permitted to execute get and set requests on the managed device. Given the example above, the machines with addresses from 192.168.1.1 through 192.168.1.254 can execute SNMP commands on the device. (The address identified by suffix .0 in a subnetwork range is always reserved for the subnet address, and the address identified by .255 in the range is always reserved for the broadcast address).</p> <p>As another example, if you enter a range of 10.10.1.128/25 machines with IP addresses from 10.10.1.129 through 10.10.1.254 can execute SNMP requests on managed devices. In this example, 10.10.1.128 is the network address and 10.10.1.255 is the broadcast address. 126 addresses would be designated.</p>
IPv6 Hostname or IPv6 subnet of Network Management System	Specify the IPv6 DNS hostname or subnet of the machines that can execute get and set requests to the managed devices.
Community name for traps	<p>Enter the global community string associated with SNMP traps. The valid range is 1-256 characters.</p> <p>Traps sent from the device will provide this string as a community name.</p> <p>The community name can be in any alphanumeric format. Special characters are not permitted.</p>
Host Type	Specify whether the enabled host is an IPv4 host or an IPv6 host.
Hostname or IP address	<p>Enter the DNS hostname of the computer to which you want to send SNMP traps. The valid range is 1-256 characters.</p> <p>An example of a DNS hostname is: <code>snmptraps.foo.com</code>. Since SNMP traps are sent randomly from the SNMP agent, it makes sense to specify where exactly the traps should be sent. You can add up to a maximum of three DNS hostnames. Ensure you select the Enabled check box beside the appropriate hostname.</p>

Table 31 - SNMP Settings



Note: After you configure the SNMP settings, you must click **Apply** to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

Enabling the Time Settings (NTP)

Use the **Time Settings** page to specify the Network Time Protocol (NTP) server to use to provide time and date information to the AP or to configure the time and date information manually.

NTP is an Internet standard protocol that synchronizes computer clock times on your network. NTP servers transmit Coordinated Universal Time (UTC, also known as Greenwich Mean Time) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock. The timestamp is used to indicate the date and time of each event in log messages.

See <http://www.ntp.org> for more information about NTP.

To set the system time either manually or by specifying the address of the NTP server for the AP to use, click the **Services > Time Settings (NTP)** tab and update the fields as described in the table below.

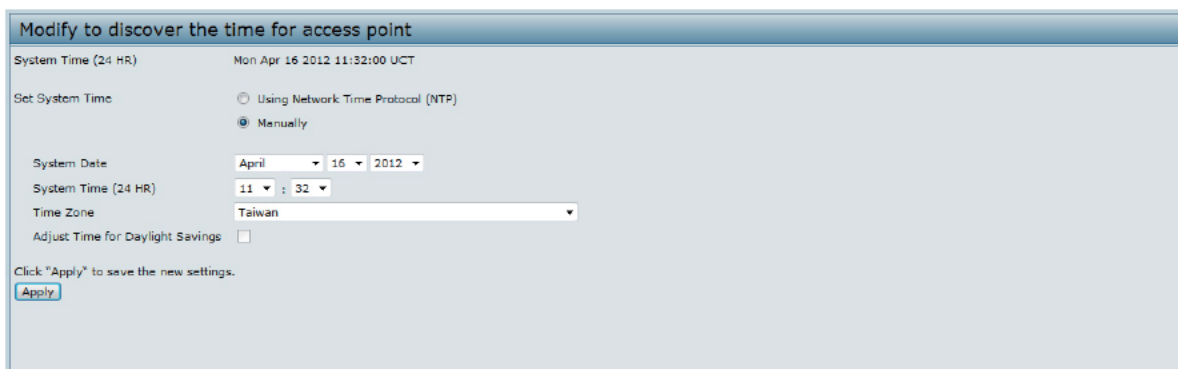



Figure 32 - Time Settings (NTP)

Field	Description
Set System Time	NTP provides a way for the AP to obtain and maintain its time from a server on the network. Using an NTP server gives your AP the ability to provide the correct time of day in log messages and session information. Choose to use a network time protocol (NTP) server to determine the system time, or set the system time manually: <ul style="list-style-type: none"> • To permit the AP to poll an NTP server, click Using Network Time Protocol (NTP). • To prevent the AP from polling an NTP server, click Manually.
NTP Server (Use NTP)	If NTP is enabled, specify the NTP server to use. You can specify the NTP server by hostname, IPv4 or IPv6 address, although using the IPv4 or IPv6 address is not recommended as these can change more readily. If you specify a hostname, note the following requirements: <ul style="list-style-type: none"> • The length must be between 1 – 63 characters. • Upper and lower case characters, numbers, and hyphens are accepted. • The first character must be a letter (a–z or A–Z), and the last character cannot be a hyphen.
System Date (Manual configuration)	Specify the current month, day, and year.
System Time (Manual configuration)	Specify the current time in hours and minutes. The system uses a 24-hour clock, so 6:00 PM is configured as 18:00.
Time Zone	Select your local time zone from the menu. The default is USA (Pacific) .
Adjust Time for Daylight Savings	Select to have the system adjust the reported time for Daylight Savings Time (DST). When this field is selected, fields to configure Daylight Savings Time settings appear.
DST Start (24 HR)	Configure the date and time to begin Daylight Savings Time for the System Time.
DST End (24 HR)	Configure the date and time to end Daylight Savings Time for the System Time.
DST Offset (minutes)	Select the number of minutes to offset DST. The default is 60 minutes.

Table 32 - NTP Settings

	<p>Note: After you configure the Time settings, you must click Apply to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.</p>
---	--

Section 6 - Configuring SNMPv3

This section describes how to configure the SNMPv3 settings on the UAP and contains the following subsections:

-) "Configuring SNMPv3 Views" on page 52
-) "Configuring SNMPv3 Groups" on page 53
-) "Configuring SNMPv3 Users" on page 54
-) "Configuring SNMPv3 Targets" on page 55

Configuring SNMPv3 Views

A MIB view is a combination of a set of view subtrees or a family of view subtrees where each view subtree is a subtree within the managed object naming tree. You can create MIB views to control the OID range that SNMPv3 users can access.

A MIB view called "all" is created by default in the system. This view contains all management objects supported by the system.



Note: If you create an *excluded* view subtree, create a corresponding *included* entry with the same view name to allow subtrees outside of the excluded subtree to be included. For example, to create a view that excludes the subtree 1.3.6.1.4, create an *excluded* entry with the OID 1.3.6.1.4. Then, create an *included* entry with OID .1 with the same view name.

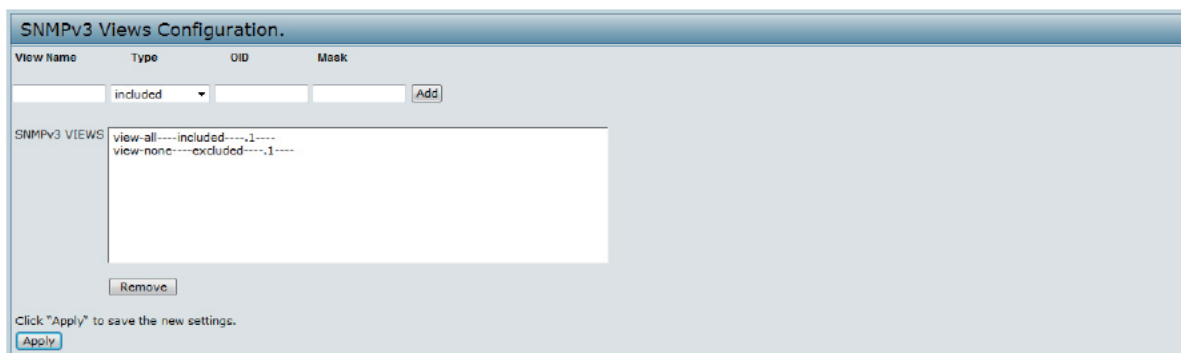


Figure 33 - SNMPv3 Views Configuration

The following table describes the fields you can configure on the SNMPv3 Views page.

Field	Description
View Name	Enter a name to identify the MIB view. View names can contain up to 32 alphanumeric characters.
Type	Specifies whether to include or exclude the view subtree or family of subtrees from the MIB view.
OID	Enter an OID string for the subtree to include or exclude from the view. For example, the system subtree is specified by the OID string .1.3.6.1.2.1.1.
Mask	The OID mask is 47 characters in length. The format of the OID mask is xx.xx.xx (.)... or xx:xx:xx... (:) and is 16 octets in length. Each octet is 2 hexadecimal characters separated by either . (period) or : (colon). Only hex characters are accepted in this field. For example, OID mask FA.80 is 11111010.10000000. A family mask is used to define a family of view subtrees. The family mask indicates which sub-identifiers of the associated family OID string are significant to the family's definition. A family of view subtrees allows control access to one row in a table, in a more efficient manner.
SNMPv3 Views	This field shows the MIB views on the UAP. To remove a view, select it and click Remove .

Table 33 - SNMPv3 Views



Note: After you configure the SNMPv3 Views settings, you must click **Apply** to apply the changes and to save the settings.

Configuring SNMPv3 Groups

SNMPv3 groups allow you to combine users into groups of different authorization and access privileges.

By default, the UAP has two groups:

-) **RO** — A read-only group using authentication and data encryption. Users in this group use an MD5 key/password for authentication and a DES key/password for encryption. Both the MD5 and DES key/passwords must be defined. By default, users of this group will have read only access to the default all MIB view, which can be modified by the user.
-) **RW** — A read/write group using authentication and data encryption. Users in this group use an MD5 key/password for authentication and a DES key/password for encryption. Both the MD5 and DES key/passwords must be defined. By default, users of this group will have read and write access to the default all MIB view, which can be modified by the user.

RW and RO groups are defined by default.



Note: The UAP supports maximum of eight groups.

To define additional groups, navigate to the **SNMPv3 Groups** page and configure the settings that the table below describes.

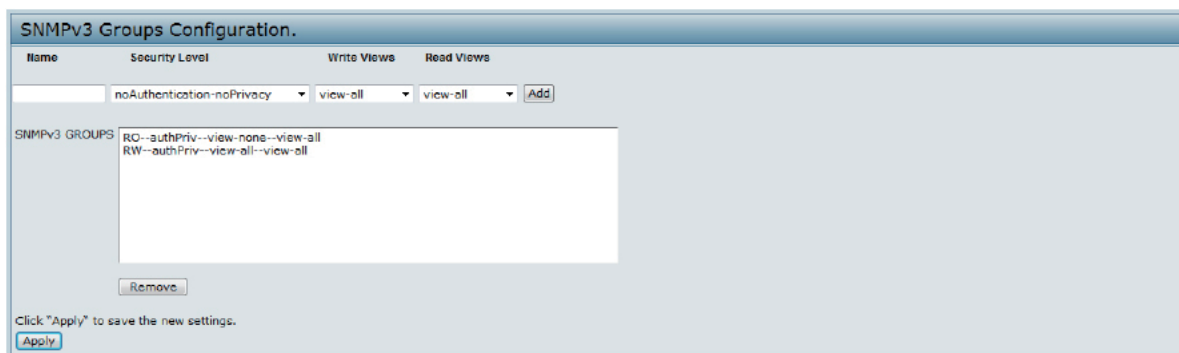



Figure 34 - SNMPv3 Groups Configuration

Field	Description
Name	Specify a name to use to identify the group. The default group names are RW and RO. Group names can contain up to 32 alphanumeric characters.
Security Level	Select one of the following security levels for the group: <ul style="list-style-type: none"> •) noAuthentication-noPrivacy — No authentication and no data encryption (no security). •) Authentication-noPrivacy — Authentication, but no data encryption. With this security level, users send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption. •) Authentication-Privacy — Authentication and data encryption. With this security level, users send an MD5 key/password for authentication and a DES key/password for encryption. For groups that require authentication, encryption, or both, you must define the MD5 and DES key/passwords on the SNMPv3 Users page.
Write Views	Select the write access to management objects (MIBs) for the group: <ul style="list-style-type: none"> •) write-all — The group can create, alter, and delete MIBs. •) write-none — The group is not allowed to create, alter, or delete MIBs.

Field	Description
Read Views	Select the read access to management objects (MIBs) for the group: <ul style="list-style-type: none"> •) view-all — The group is allowed to view and read all MIBs. •) view-none — The group cannot view or read MIBs.
SNMPv3 Groups	This field shows the default groups and the groups that you have defined on the AP. To remove a group, select the group, and click Remove .

Table 34 - SNMPv3 Groups



Note: After you configure the SNMPv3 Groups settings, you must click **Apply** to apply the changes and to save the settings.

Configuring SNMPv3 Users

From the **SNMPv3 Users** page, you can define multiple users, associate the desired security level to each user, and configure security keys.

For authentication, only MD5 type is supported, and for encryption only DES type is supported. There are no default SNMPv3 users on the UAP.



Figure 35 - SNMPv3 User Configuration

The following table describes the fields to configure SNMPv3 users.

Field	Description
Name	Enter the user name to identify the SNMPv3 user. User names can contain up to 32 alphanumeric characters.
Group	Map the user to a group. The default groups are RWAuth , RWPriv , and RO . You can define additional groups on the SNMPv3 Groups page.
Authentication Type	Select the type of authentication to use on SNMP requests from the user: <ul style="list-style-type: none"> •) MD5 — Require MD5 authentication on SNMPv3 requests from the user. •) None — SNMPv3 requests from this user require no authentication.
Authentication Key	If you specify MD5 as the authentication type, enter a password to enable the SNMP agent to authenticate requests sent by the user. The passphrase must be between 8 and 32 characters in length.
Encryption Type	Select the type of privacy to use on SNMP requests from the user: <ul style="list-style-type: none"> •) DES — Use DES encryption on SNMPv3 requests from the user. •) None — SNMPv3 requests from this user require no privacy.
Encryption Key	If you specify DES as the privacy type, enter a key to use to encrypt the SNMP requests. The passphrase must be between 8 and 32 characters in length.
SNMPv3 Users	This field shows the users that you have defined on the AP. To remove a user, select the user and click Remove .

Table 35 - SNMPv3 Users

Use the buttons on the page to perform the following tasks:

-) **Add:** Add the new user to the SNMPv3 users table.
-) **Remove:** Remove the selected user from the SNMPv3 users table.
-) **Update:** Apply and save the changed SNMPv3 user settings.



Note: After you configure the SNMPv3 Users settings, you must click **Apply** to apply the changes and to save the settings.

Configuring SNMPv3 Targets

SNMPv3 Targets send “inform” messages to the SNMP manager. Each target is identified by a target name and associated with target IP address, UDP port, and SNMP user name.

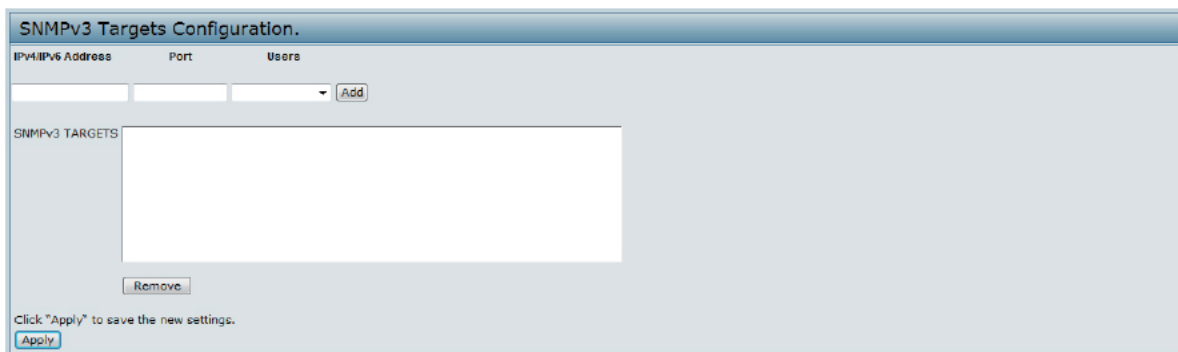


Figure 36 - SNMPv3 Targets Configuration

Field	Description
IPv4/IPv6 Address	Enter the IP address of the remote SNMP manager to receive the target.
Port	Enter the UDP port to use for sending SNMP targets.
Users	Select the name of the SNMP user to associate with the target. To configure SNMP users, see “ Configuring SNMPv3 Users ” on page 54.
SNMPv3 Targets	This field shows the SNMPv3 Targets on the UAP. To remove a target, select it, and click Remove .

Table 36 - SNMPv3 Targets



Note: After you configure the SNMPv3 Target settings, you must click **Apply** to apply the changes and to save the settings.

Section 7 - Maintaining the Access Point

This section describes how to maintain the UAP.

From the UAP Administrator UI, you can perform the following maintenance tasks:

-) "Performing AP Maintenance" on page 57
-) "Upgrading the Firmware" on page 57
-) "Support Information Configuration and Settings" on page 58

Saving the Current Configuration to a Backup File

The AP configuration file is in binary format and contains all of the information about the AP settings. You can download the configuration file to a management station to manually edit the content or to save as a back-up copy.

Click the Download button to save a copy of the current settings on an AP to a backup configuration file.

Click the **Download** button to save a copy of the current settings on an AP to a backup configuration file.

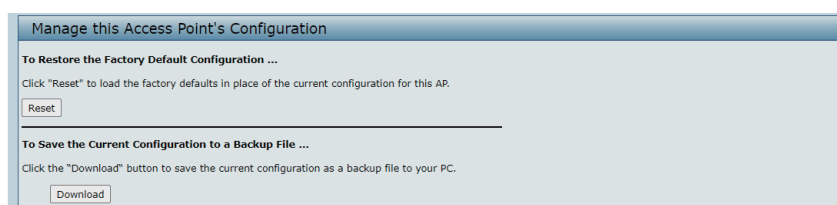


Figure 37 - Manage this Access Point's Configuration - Save

Restoring the Configuration from a Previously Saved File

After you download a configuration file to the management station, you can manually edit the file, which is in binary format. Then, you can upload the edited configuration file to apply those configuration settings to the AP.

Use the following steps to save a copy of the current settings on an AP to a backup configuration file

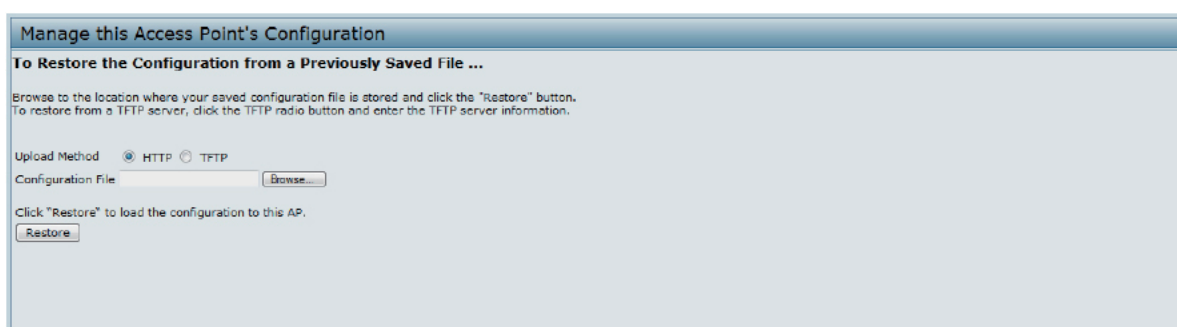


Figure 38 - Manage this Access Point's Configuration - Restore (HTTP)

- 1.) Use the **Browse** button to select the file to restore.
- 2.) Click the **Restore** button.
A File Upload or Choose File dialog box displays.
- 3.) Navigate to the directory that contains the file, then select the file to upload and click **Open**.
(Only those files created with the Backup function and saved as .bin backup configuration files are valid to use with Restore; for example, WLAN-EAP_config.bin.)
- 4.) Click the **Restore** button.
A dialog box opens verifying the restore.
- 5.) Click **OK** to proceed.
The AP reboots. A reboot confirmation dialog and follow-on rebooting status message displays. Please wait for the reboot process to complete, which might take several minutes.

The Administration Web UI is not accessible until the AP has rebooted.

Performing AP Maintenance

From the **Maintenance** page, you can reset the AP to its factory default settings or reboot the AP.

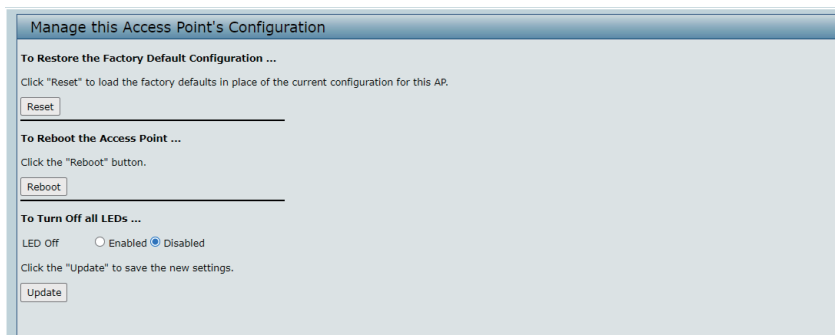


Figure 39 - Performing AP Maintenance

Resetting the Factory Default Configuration

If you are experiencing problems with the UAP and have tried all other troubleshooting measures, click **Reset**. This restores factory defaults and clears all settings, including settings such as a new password or wireless settings. You can also use the reset button on the back panel to reset the system to the default configuration.

Rebooting the Access Point

For maintenance purposes or as a troubleshooting measure, you can reboot the UAP. To reboot the AP, click the **Reboot** button.

Turn Off all LEDs

Enable the LED off to turn off all LEDs.

Upgrading the Firmware

As new versions of the UAP firmware become available, you can upgrade the firmware on your devices to take advantage of new features and enhancements.

After you upload new firmware and the system reboots, the newly added firmware becomes the primary image. If the upgrade fails, the original firmware remains as the primary image.



Note: When you upgrade the firmware, the access point retains the existing configuration information.

Use the following steps to upgrade the firmware on an access point

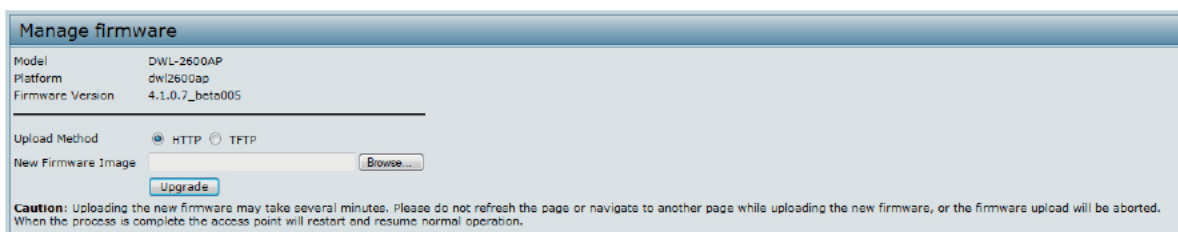



Figure 40 - Manage Firmware (HTTP)

- 1.) If you know the path to the new firmware image file, enter it in the **Image Filename** field. Otherwise, click the **Browse** button and locate the firmware image file.
The firmware upgrade file supplied must be a *tar* file. Do not attempt to use *bin* files or files of other formats for the upgrade; these types of files will not work.
- 2.) Click **Upgrade** to apply the new firmware image.
Upon clicking **Upgrade** for the firmware upgrade, a popup confirmation window is displayed that describes the upgrade process.
- 3.) Click **OK** to confirm the upgrade and start the process.

 **Note:** The firmware upgrade process begins once you click **Upgrade** and then **OK** in the popup confirmation window.

The upgrade process may take several minutes during which time the access point will be unavailable. Do not power down the access point while the upgrade is in process. When the upgrade is complete, the access point restarts. The AP resumes normal operation with the same configuration settings it had before the upgrade.

- 4.) To verify that the firmware upgrade completed successfully, check the firmware version shown on the **Upgrade** page (or the **Basic Settings** page). If the upgrade was successful, the updated version name or number is indicated.

Support Information Configuration and Settings

The Support Information page provides a way to gather the diagnostic/troubleshooting information about the AP beyond what is available through the Web UI.

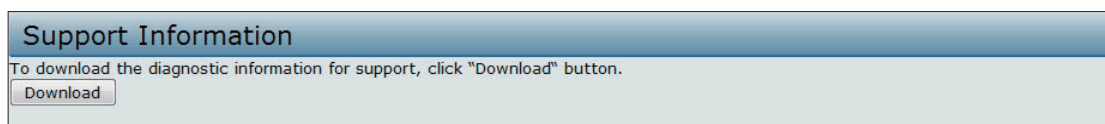


Figure 41 - Support Information

Field	Description
Download	To download the diagnostic information for support, click "Download" button.

Table 37 - Support Information

Section 8 - Configuring Client Quality of Service (QoS)

This section describes how to configure QoS settings that affect traffic from the wireless clients to the AP. By using the UAP Client QoS features, you can limit bandwidth.

This section describes the following features:

-) "Configuring VAP QoS Parameters" on page 59

Configuring VAP QoS Parameters

The client QoS features on the UAP provide additional control over certain QoS aspects of wireless clients that connect to the network, such as the amount of bandwidth an individual client is allowed to send and receive.

To configure the Client QoS administrative mode and to configure the QoS settings for a VAP, click the **VAP QoS Parameters** tab.

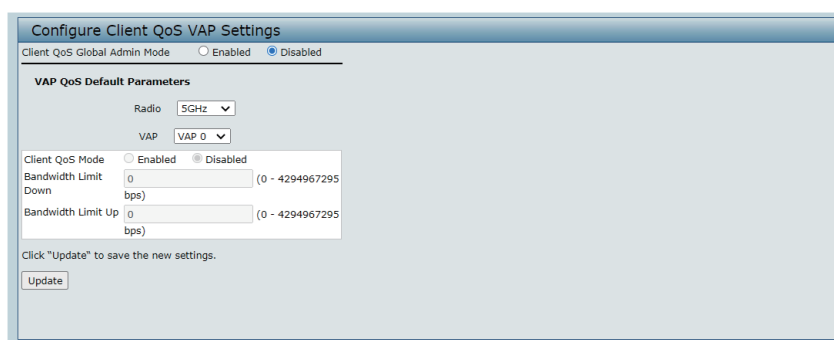


Figure 42 - Configure Client QoS VAP Settings

Field	Description
Client QoS Global Admin Mode	Enable or disable Client QoS operation on the AP. Changing this setting will not affect the WMM settings you configure on the QoS page.
Radio	For dual-radio APs, select 5GHz Radio or 2.4GHz Radio to specify which radio to configure.
VAP	Specify the VAP that will have the Client QoS settings that you configure. The QoS settings you configure for the selected VAP will not affect clients that access the network through other VAPs.
Client QoS Mode	Enable or disable QoS operation on the VAP selected in the VAP menu. QoS must be enabled globally (from the Client QoS Global Admin Mode field) and on the VAP (QoS Mode field) for the Client QoS settings to be applied to wireless clients.
Bandwidth Limit Down	Enter the maximum allowed transmission rate from the AP to the wireless client in bits per second. The valid range is 0 – 429496000 bits/sec. The value you enter must be a multiple of 8000 bits/sec, in other words, the value must be $n \times 8000$ bits/sec, where $n = 0, 1, 2, 3...$ If you attempt to set the limit to a value that is not a multiple of 8000 bits/sec, the configuration will be rejected. A value of 0 means that the bandwidth maximum limit is not enforced in this direction.
Bandwidth Limit Up	Enter the maximum allowed client transmission rate to the AP in bits per second. The valid range is 0 – 4294967295 bps. The value you enter must be $n \times 8000$ bits/sec, where $n = 0, 1, 2, 3...$ If you attempt to set the limit to a value that is not a multiple of 8000 bits/sec, the configuration will be rejected. A value of 0 means that the bandwidth maximum limit is not enforced in this direction.

Table 38 - VAP QoS Parameters