61700412E1-29.1H
August 2012

ADTRAN

Configuration Guide

NetVanta 150 Series Wireless Configuration Guide

This configuration guide provides an overview of wireless technology, the elements of wireless local area networks (WLANs), methods for configuring ADTRAN Operating System (AOS) NetVanta 150 access points (APs), radios, and virtual access points (VAPs), as well as WLAN topography overviews. For detailed information regarding specific command syntax, refer to the *AOS Command Reference Guide* available online at the ADTRAN support community (https://supportforums.adtran.com).

This guide consists of the following sections:

Introduction to Wireless Technology

WLANs are becoming the new standard in small- and medium-sized business models. By using wireless technology, users can become more productive while decreasing the cost of connectivity for the business. WLANs provide an excellent alternative for growing businesses to the costly procedure of extending wired local area networks (LANs).

WLANs replace Layer 1 transmission media, such as CAT 5 cabling, with radio transmissions that enable wireless user connectivity and the extension of a wired network.

ADTRAN WLAN Components

There are many ways to incorporate WLANs into existing LANs. ADTRAN creates WLANs by adding one or more AOS APs to an AC. In an ADTRAN WLAN network architecture, there are four primary components: an AC, APs, radios, and VAPs.

The AC is usually a router or a switch that controls and configures the behavior of the AP. Each AOS AC can control up to 24 AOS APs (either NetVanta 150 standalone APs or embedded APs such as the NetVanta 1335 Wi-Fi) and communicates with them using ADTRAN Wireless Control Protocol (AWCP) during configuration and status querying.

The AP is connected to the AC through the Layer 2 broadcast domain, and provides wireless access for mobile users. The AP is configured by the AC, and determines how users will connect to the network. Each AOS AP contains two antennas and two radios (one 802.11a radio and one 802.11b/g radio) for maximum network usability.

VAPs are logical entities that exist within the physical AP, yet appear to wireless clients as independent APs. Each AOS AP supports up to eight VAPs per radio, and each VAP is identified by a service set identifier (SSID).

Basic WLAN Structure

The basic structure of the WLAN is as follows: An AC resides on a wired network with Telnet and/or Web access enabled for configuration, and a desired number of APs (up to 24) are wired to the AC. The APs may be wired directly to the AC, or they may be connected to a switch port somewhere in the attached network. The APs receive and transmit data to wireless clients, allowing client access in a range of locations.

When arranging the WLAN components, there are a number of criteria to keep in mind.

1. The AOS APs will only operate in thin access point mode. This means the AOS AP must be hardwired to an AOS AC, router, or switch somewhere on the network, so consideration must be given to the distance and placement of the AOS AP in relation to the AC for the most coverage area for wireless clients.

2. Obstructions and metal surfaces can create disturbances and interference in the wireless signals, so consideration must be given to the area surrounding the AP.

3. Overlapping cells and channel reuse will occur when too many APs are placed too close together. This overlap will result in signal degradation. To maximize user throughput, APs should be placed such that overlapping of cells on the same channel does not occur.

WLAN Standards

Wireless technology uses standards of IEEE 802.11, namely 802.11b, 802.11g, and 802.11a, for communication. Each AOS AP has a radio for receiving and transmitting 802.11b/g, as well as one for 802.11a. The decision of which radio and standard to use should be based on a particular network’s needs. The standards are described in the following sections.

802.11b

802.11b is the earliest version of the 802.11 standard. In North America, 802.11b supports channels 1 through 11, which can be divided into three non-overlapping, non-interfering channel sets (channels 1, 6, and 11). This allows three 802.11b APs to operate in close proximity without interference.

802.11b supports rate shifting bandwidths of 1, 2, 5.5, and 11 Mbps. It operates on the 2.4 GHz frequency.

The 802.11b signal range reaches approximately 100 meters in an unobstructed area and approximately 60 meters in an office environment.

Points to remember when considering the use of 802.11b are that (1) the frequency it uses is potentially crowded by the use of other APs, cordless phones, and microwaves; (2) its speed capabilities are the lowest of the WLAN implementations; and (3) it does not allow for more than three non-overlapping channel assignments, thus restricting the number of users, as well as the data rate available.

802.11g

802.11g works on the same band as the 802.11b (2.4 GHz), but it operates at the higher data rate of 54 Mbps. 802.11g hardware is operable with 802.11b hardware; however, the presence of 802.11b participants in an 802.11g network significantly reduces the speed of the network.

The 802.11g signal range is approximately 100 meters in unobstructed areas and approximately 75 meters in an office environment.

One advantage to using 802.11g is that it has a higher data rate than the 802.11b, which allows for more bandwidth per user. Something to keep in mind with the 802.11g is that, like the 802.11b, its frequency allows for the interference of other APs, cordless phones, and microwaves.

802.11a

The 802.11a standard is the newest widely adopted standard in the 802.11 family. Operating in the 5 GHz band, the 802.11a provides 12 non-overlapping channels which are separated into three ranges. The lowest range is 5.15 to 5.25 GHz, which allows four non-overlapping channels; the middle range is 5.25 to 5.35 GHz, which also allows for four non-overlapping channels; and the highest range is 5.725 to 5.825 GHz, which is used for outside point-to-point or point-to-multipoint applications. Each range has its own regulated power and antenna requirements.

The 802.11a standard is inoperable with either 802.11b or 802.11g.

The 802.11a uses a higher band frequency than the 802.11b/g, so there is less interference to contend with. The 802.11a also provides more total bandwidth, which allows more bandwidth per user.

The 802.11a signal range is approximately 50 meters in an unobstructed area, and approximately 25 meters in an office environment.

Points to remember when considering the use of 802.11a include the fact that the higher frequency is more easily absorbed by less dense objects, such as walls and ceiling tiles. Also, for larger coverage areas the power input to the mobile device’s radio must be higher, resulting in reduced battery life and mobility connection time for the mobile user. The number of clients using A cards is also less than with B/G cards, an important factor in determining your network’s needs.

Comparing 802.11b/g/a

The following chart compares the major characteristics of all three standards.

Table 1. WLAN Standards Characteristics

Characteristic	802.11b	802.11g	802.11a
Frequency Band	2.4 GHz	2.4 GHz	5.8 GHz
Modulation	DSSS	DSSS/OFDM	OFDM
Data Rates	1, 2, 5.5,11 Mbps	DSSS-1, 2, 5.5, 11 Mbps OFDM-6, 9, 12, 15, 24, 36, 48, 54 Mbps	6, 9, 12, 15, 24, 36, 48, 54 Mbps
Max Data Rate	11 Mbps	54 Mbps	54 Mbps
Effective Data Throughput	5 Mbps	32 Mbps	32 Mbps
Advertised Range	100 m	100 m	75 m
Office Range	60 m	75 m	25 m
Non-overlapping Channels	3	3	8
Interfering Services	Cordless Phones, Microwaves, Blue-tooth Devices	Cordless Phones, Microwaves, Blue-tooth Devices	HyperLAN devices, Maritime, Satellite and RADAR Systems
Availability	Worldwide	Worldwide	Limited

WLAN Security

Wireless security is an important factor in the configuration of a WLAN. An AOS AP supports the 802.11 wired equivalent privacy (WEP), 802.1x, Wi-Fi protected access (WPA), and WPA2 security modes. An understanding of the security parameters necessary for a particular network is needed before configuring the WLAN. Review the following short descriptions of security commands.

Personal Modes: Preshared Keys (PSK)

- The **WEP: OPEN** security parameter allows clients to connect using WEP keys, based on the 802.11 standards. In this security mode, open authentication with static WEP keys is used.
- The **WEP: SHARED** security parameter allows clients to connect using WEP keys, based on the 802.11 standards. In this security mode, shared authentication with encrypted static keys is used.

NOTE *Although **WEP: SHARED** uses encrypted keys, plain-text challenge requests present security risks that must be taken into account when determining the correct network security parameters.*

- The **WPA: TKIP** parameter allows clients to connect using WPA personal and preshared keys, without requiring a RADIUS authentication server. Temporal Key Integrity Protocol (TKIP) specifies the algorithms used for rotating keys.
- The **WPA/WPA2: TKIP/AES-CCMP** parameter allows clients to connect through either WPA or WPA2 personal to associate with each other, also without requiring a RADIUS authentication server. TKIP specifies the algorithms used for rotating keys in conjunction with Advanced Encryption Standard and Counter Mode CBC MAC Protocol (AES-CCMP), which specifies the algorithms used for WPA2.

Enterprise Modes (Radius/802.1x)

- The **WPA: TKIP: EAP** parameter allows clients to connect using WPA enterprise and 802.1x authentication. A RADIUS authentication server is required. TKIP specifies the algorithms used for rotating keys, while Extensible Authentication Protocol (EAP) provides a universal authentication framework in the wireless network.
- The **WPA2: AES-CCMP: EAP** parameter allows clients to connect using WPA2 enterprise along with 802.1x authentication. A RADIUS authentication server is required. This parameter combines the use of AES-CCMP algorithms with the EAP universal wireless authentication framework.
- The **WPA/WPA2: TKIP AES-CCMP: EAP** parameter allows clients to connect using either WPA or WPA2 enterprise with 802.1x authentication. A RADIUS authentication server is required. By using this parameter, both WPA and WPA2 protocols are supported with a combination of TKIP, WPA2 algorithms (AES-CCMP), and the use of EAP universal wireless authentication framework.

Enterprise Modes (Radius/802.1x and PSK)

- The **WEP: OPEN: EAP: MD5-STATIC-KEY** allows clients using standard WEP keys to authenticate to a RADIUS authentication server using the message digest 5 (MD5) EAP type. This EAP type does not perform key generation and requires appropriate static WEP keys to be configured. The first WEP key is obtained from the RADIUS authentication server, and security WEP keys 2 through 4 are specified by the user.
- The **WEP: OPEN: EAP: MD5-STATIC-KEY OPTIONAL** command allows clients to use EAP types other than MD5 for authentication, allowing the RADIUS authentication server to negotiate the encryption keys with the client.

> NOTE *WEP has been proven to be easily broken and is not the recommended security option. WPA is the preferred security option. The strongest security is achieved with WPA AES-CCMP.*

> NOTE *For RADIUS authentication to function, the AP must be assigned an IP address and gateway. Refer to Step 5: RADIUS Server on page 14 of this guide for more information.*

For more detailed information regarding security options, refer to the *Wireless Interface Command Sets* in the *AOS Command Reference Guide* available online at https://supportforums.adtran.com.

Hardware and Software Requirements and Limitations

The NetVanta 150 WLAN basic features were introduced in AOS 15.1 for data products and AOS A1.01 for voice products. Advanced WLAN features, such as WEP key generation and reference VAP, were introduced in AOS 17.2. Support for WLAN, WEP key generation, and the number of supported access points (APs) are available on AOS products as outlined in the *AOS Feature Matrix* available online at https://supportforums.adtran.com.

Configuring the AOS AP

There are two ways to begin configuring an AOS AP: (1) the Web-based graphical user interface (GUI) and (2) the command line interface (CLI). The remainder of this configuration guide pertains particularly to the GUI; for descriptions of CLI functions, refer to the *AOS Command Reference Guide*.

Accessing the GUI

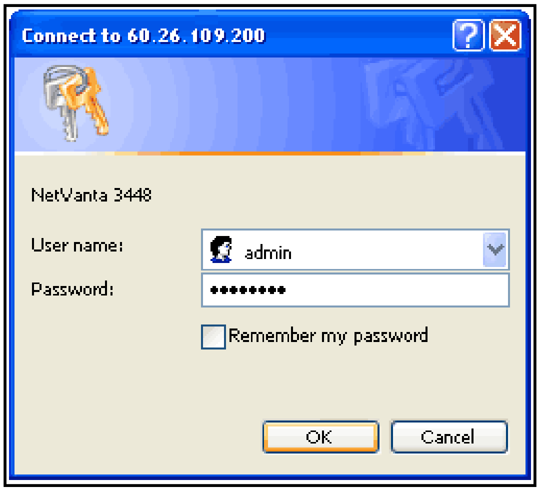
You can access the GUI from any Web browser by following these steps:

1. Connect the AC to your PC using the switch port labeled **0/1** to **0/n** or the **ETH 0/1** or **ETH 0/2** ports on either the back or the front of the unit depending on the product. Also, connect the AOS AP to the AC either by using the **ETH 0/1** or **ETH 0/2** ports on the back of the unit or by connecting the AP to a switch port somewhere in the attached network. As long as the controller and AP are connected by the same broadcast domain, control can be established.

2. Set your PC to a fixed IP address of 10.10.10.2. If you cannot change the PC's IP address, you will need to change the unit's IP address using the CLI. (Refer to the quick start guide shipped with your ADTRAN controlling unit for instructions.)

3. Enter the unit's IP address in your browser address line in the following form: **http://**<*ip address*>, for example: **http://60.26.109.200**.

4. At the prompt, enter your user name and password (the default settings are **admin** and **password**).



Connect to 60.26.109.200

NetVanta 3448

User name: admin

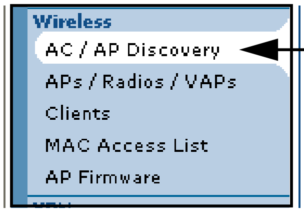
Password: ••••••••

□ Remember my password

5. The initial GUI menu appears.

Accessing the Configuration Wizard

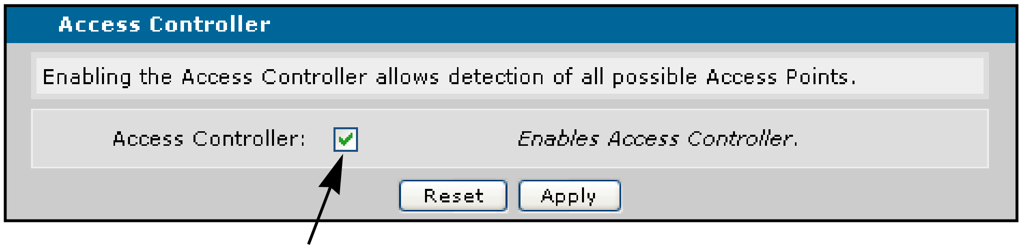
Once connected to the GUI, expand the **Data** tab on the left side of the menu if not expanded already. Navigate to **Data** > **Wireless** > **AC/AP Discovery** to gain access to the configurations of the AC and APs.



Select **AC/AP Discovery** to enter access point configuration.

Figure 1. Wireless Menu

The AC must be enabled to allow for automatic detection of APs. To enable the AC, check the box by **Access Controller** at the top of the menu and select **Apply**.


Access Controller

Enabling the Access Controller allows detection of all possible Access Points.

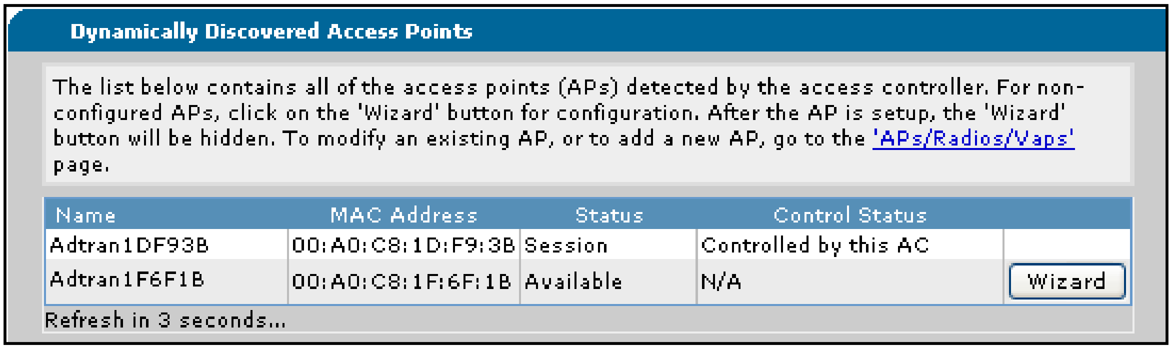
Access Controller: ☑ *Enables Access Controller.*

Select **Access Controller** to enable the AC.

Figure 2. Access Controller Menu

> NOTE
>
> *APs can be manually added to the AC. The wizard is only for the configuration of APs that are automatically detected.*

Once the AC is enabled, it will search for nearby APs. When APs are detected by the AC, they will appear in a menu at the bottom of the menu titled **Dynamically Discovered Access Points** (see *Figure 3*). The **Wizard** button will be located to the right of the discovered AP, verifying that the AC has detected an AP and it can now be added to the controller. Select the **Wizard** button to begin configuring the AP.



Dynamically Discovered Access Points

The list below contains all of the access points (APs) detected by the access controller. For non-configured APs, click on the 'Wizard' button for configuration. After the AP is setup, the 'Wizard' button will be hidden. To modify an existing AP, or to add a new AP, go to the 'APs/Radios/Vaps' page.

Name	MAC Address	Status	Control Status	
Adtran1DF93B	00:A0:C8:1D:F9:3B	Session	Controlled by this AC	
Adtran1F6F1B	00:A0:C8:1F:6F:1B	Available	N/A	Wizard

Refresh in 3 seconds...

Figure 3. Dynamically Discovered Access Points Menu

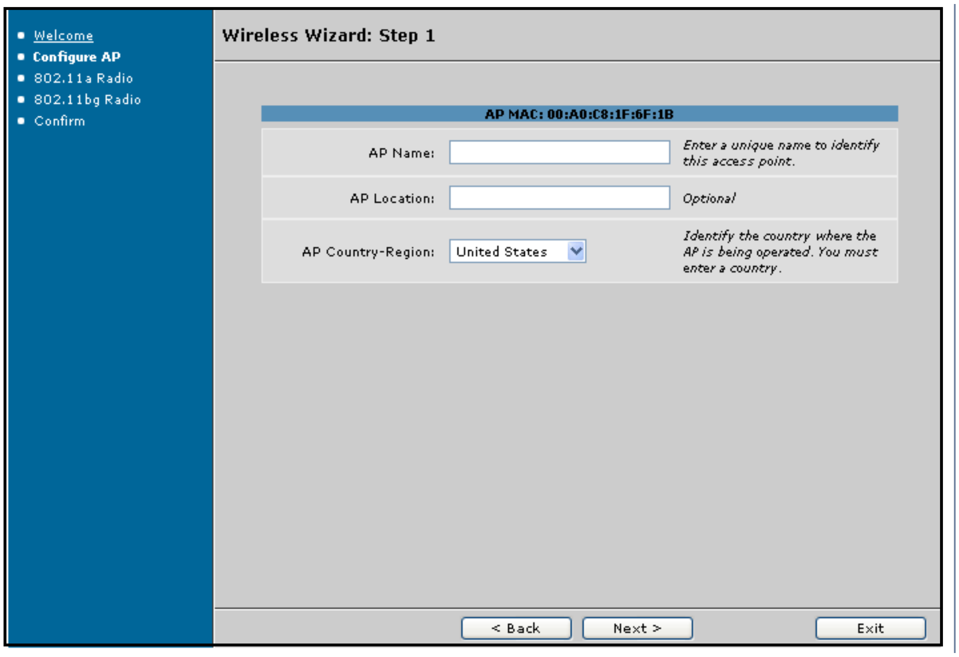
NOTE *An AP appearing in the **Dynamically Discovered Access Points** menu is not controlled by the AC until it is added individually.*

Using the Configuration Wizard

Once the **Wizard** button has been selected, a new window will open to guide you through adding an AP to the controller. After the introduction menu, select **Next** to proceed to *Step 1: AP Information on page 9*.

Step 1: AP Information

The first step of the Wireless Wizard will ask for information regarding the AP's name, location, and the country in which it is operated.



Wireless Wizard: Step 1

AP MAC: 00:A0:C8:1F:6F:1B

AP Name: *Enter a unique name to identify this access point.*

AP Location: *Optional*

AP Country-Region: United States *Identify the country where the AP is being operated. You must enter a country.*

Figure 4. Identifying the Access Point

Use a unique name to identify this particular AP. The AP location is optional, and only serves to further identify this AP. The country parameter specifies the country in which the AP will operate.

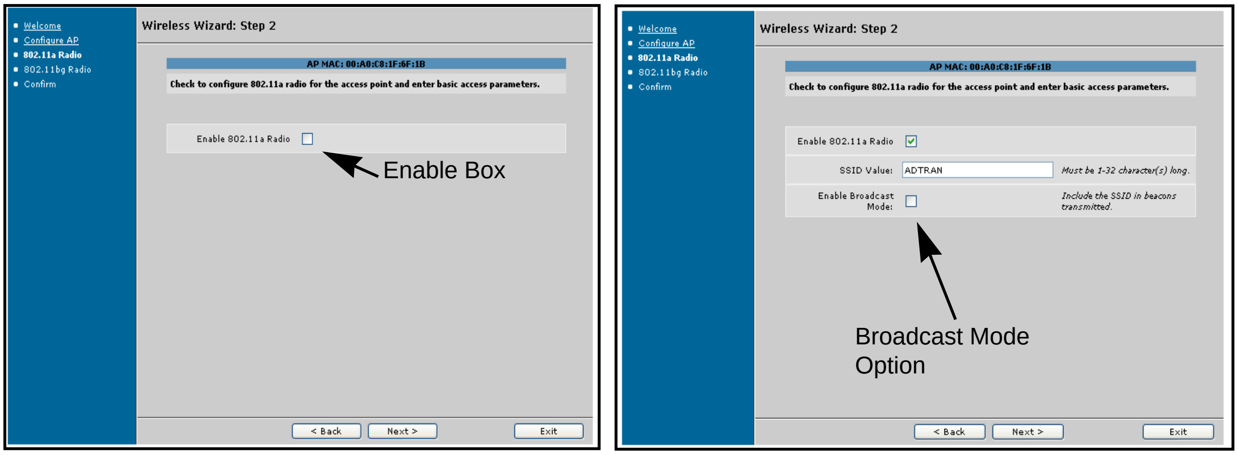
Once the required information has been entered, select **Next** to move to Step 2.

Step 2: Enabling 802.11a Radio

Step 2 provides the settings for enabling radio 802.11a. If an 802.11a radio is not necessary for your network, do not check the enable box; instead select **Next** at the bottom of the menu. Selecting **Next** will take you to the enabling menu for the 802.11b/g radio (*Steps 6 through 8: Configuring the 802.11b/g Radio on page 14*).

If you wish to use the 802.11a radio in your network, check the enable box and enter the required information (SSID value and broadcast mode).

The **SSID** value is attached to the packet header. It consists of up to 32 case-sensitive characters and can include spaces. SSIDs serve to differentiate WLANs from one another and VAPs from one another. They are included in the beacon frames in plain text, but the radio may be configured so that the SSID is not broadcast in the beacon.



Wireless Wizard: Step 2

AP MAC: 00:A0:C8:1F:6F:1B

Check to configure 802.11a radio for the access point and enter basic access parameters.

Enable 802.11a Radio □

Wireless Wizard: Step 2

AP MAC: 00:A0:C8:1F:6F:1B

Check to configure 802.11a radio for the access point and enter basic access parameters.

Enable 802.11a Radio ☑

SSID Value: ADTRAN *Must be 1-32 character(s) long.*

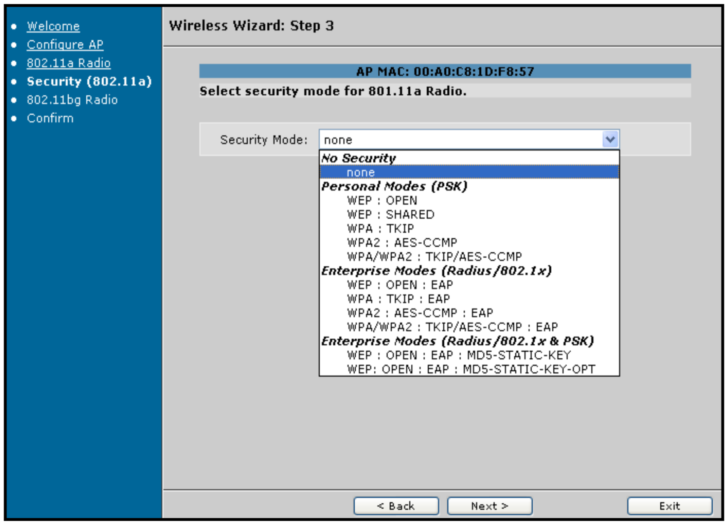
Enable Broadcast Mode: □ *Include the SSID in beacons transmitted.*

Figure 5. Enabling the 802.11a Radio

Once you have entered the required information, select **Next** at the bottom of the menu to proceed to Step 3.

Steps 3 through 5: Radio Security Configuration

In Step 3, the radio security mode is set by choosing from the drop-down menu. Choose the security mode that best fits your network.



Wireless Wizard: Step 3

AP MAC: 00:A0:C8:1D:F8:57

Select security mode for 801.11a Radio.

Security Mode: none

No Security
none
Personal Modes (PSK)
WEP : OPEN
WEP : SHARED
WPA : TKIP
WPA2 : AES-CCMP
WPA/WPA2 : TKIP/AES-CCMP
Enterprise Modes (Radius/802.1x)
WEP : OPEN : EAP
WPA : TKIP : EAP
WPA2 : AES-CCMP : EAP
WPA/WPA2 : TKIP/AES-CCMP : EAP
Enterprise Modes (Radius/802.1x & PSK)
WEP : OPEN : EAP : MD5-STATIC-KEY
WEP: OPEN : EAP : MD5-STATIC-KEY-OPT

Figure 6. Security Mode Configuration Menu

NOTE *The default security mode is **none**. Leaving the security setting as **none** will result in no authentication required to connect to the network and no encryption provided on the wireless connection.*

Different security modes require different information for configuration. The three major types of information needed for security parameters are **Preshared Keys**, **WEP keys**, and **RADIUS Server** information. The following is a breakdown of each type of security option, and the steps needed for configuration.

Preshared Key Security Choices

- **WPA2: AES-CCMP**
- **WPA/WPA2: TKIP/AES-CCMP**
- **WPA: TKIP**

Selecting one of these security options in Step 3 will take you to *Step 4A: Preshared Keys on page 12* to enter the preshared key.

WEP Key Security Choices

- **WEP: SHARED**
- **WEP: OPEN**
- **WEP: OPEN: EAP: MD5-STATIC-KEY**
- **WEP: OPEN: EAP: MD5-STATIC-KEY-OPTIONAL**

Selecting one of these security options in Step 3 will take you to *Step 4B: WEP Keys on page 12* to enter the WEP key information.

NOTE

*Both **WEP: OPEN: EAP: MD5** options require the use of both WEP keys and a RADIUS server. If either of these choices are selected in Steps 3 through 5: Radio Security Configuration on page 10, the WEP Key information is entered in Step 4B: WEP Keys on page 12, and the RADIUS information is entered in Step 5: RADIUS Server on page 14.*

RADIUS Server Security Choices

- **WPA/WPA2: TKIP/AES-CCMP: EAP**
- **WPA2: AES-CCMP: EAP**
- **WPA: TKIP: EAP**
- **WEP: OPEN: EAP**
- **WEP: OPEN: EAP: MD5-STATIC-KEY**
- **WEP: OPEN: EAP: MD5-STATIC-KEY-OPTIONAL**

Selecting one of these security options in Step 3 will take you to *Step 5: RADIUS Server on page 14* to enter the RADIUS information.

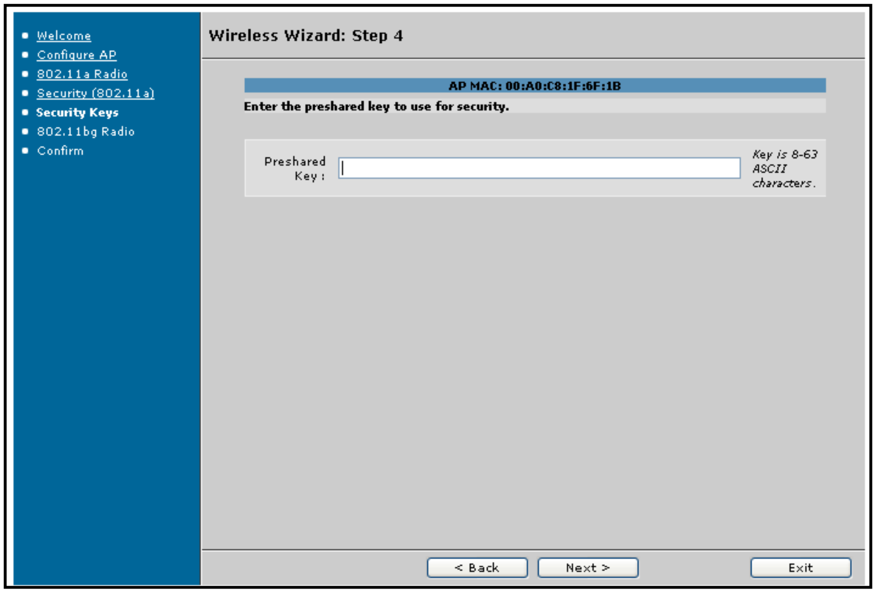
NOTE

*Both **WEP: OPEN: EAP: MD5** options require the use of both WEP keys and a RADIUS server. If either of these choices are selected in Steps 3 through 5: Radio Security Configuration on page 10, the WEP Key information is entered in Step 4B: WEP Keys on page 12, and the RADIUS information is entered in Step 5: RADIUS Server on page 14.*

Once the appropriate security mode has been selected, select **Next** to proceed.

Step 4A: Preshared Keys

Some security modes require the use of preshared keys for generation of a unicast session for each client. After entering the predetermined key name in the **Preshared Key** field, select **Next** to continue to *Steps 6 through 8: Configuring the 802.11b/g Radio on page 14*.



Wireless Wizard: Step 4

AP MAC: 00:A0:C8:1F:6F:1B

Enter the preshared key to use for security.

Preshared Key :

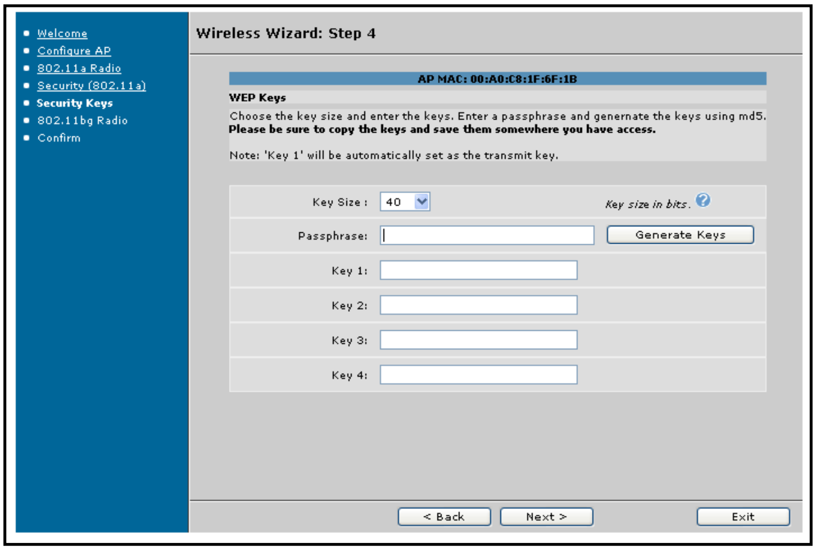
Key is 8-63 ASCII characters.

Figure 7. Preshared Key Configuration

Step 4B: WEP Keys

Certain security modes require the use of WEP keys. To use WEP keys, the key size in bits must be entered, along with up to four key names. It is important to remember that in WEP keys with the addition of a 24-bit initialization vector, the 40-bit key becomes 64 bits, the 104-bit key becomes 128 bits, and the 128-bit key becomes 152 bits on the client.

> *In AOS Release 17.2, a WEP key generator feature was added. The WEP key generator may be used to generate all four keys from a passphrase. Refer to WEP Key Generator on page 26 for more information.*



Wireless Wizard: Step 4

AP MAC: 00:A0:C8:1F:6F:1B

WEP Keys

Choose the key size and enter the keys. Enter a passphrase and genernate the keys using md5.
Please be sure to copy the keys and save them somewhere you have access.

Note: 'Key 1' will be automatically set as the transmit key.

Key Size : 40 *Key size in bits.*

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

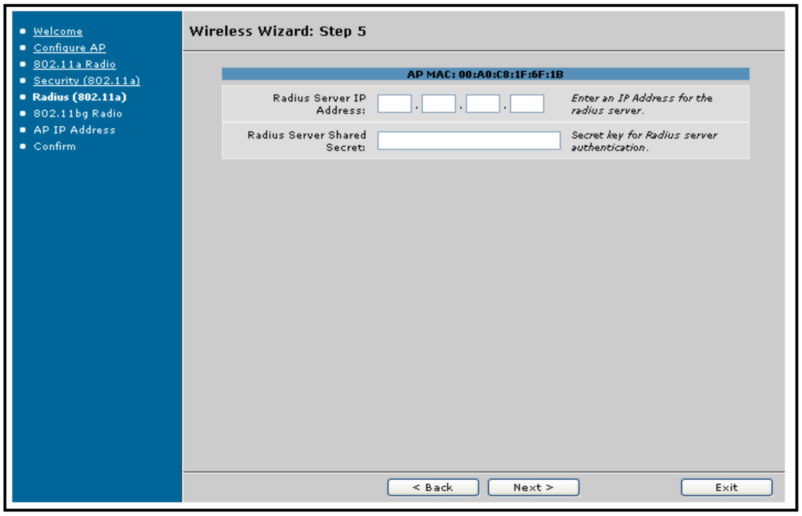
Figure 8. WEP Keys Configuration

NOTE *The first key name entered is automatically set to be the transmit key. All four key names must be entered either manually or through the WEP key generator.*

After the key information has been entered, select **Next** to continue to *Steps 6 through 8: Configuring the 802.11b/g Radio on page 14*.

Step 5: RADIUS Server

Certain security modes require the use of a RADIUS server for authentication. Configure the RADIUS server by entering the IP address of the server along with the secret key for authentication. After this information has been entered, select **Next** to continue to Step 6.



Wireless Wizard: Step 5

AP MAC: 00:A0:C8:1F:6F:1B

Radius Server IP Address:	. . .	*Enter an IP Address for the radius server.*
Radius Server Shared Secret:		*Secret key for Radius server authentication.*

Figure 9. Radius Server Configuration

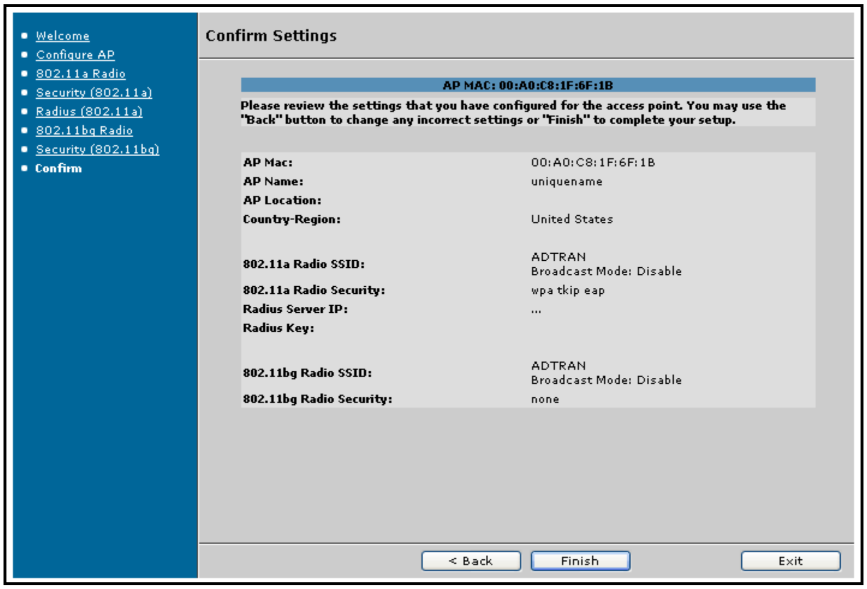
An IP address for the AP must be set in the ***IP Settings*** *tab (refer to IP Settings on page 18) for communication with the RADIUS server.*

Steps 6 through 8: Configuring the 802.11b/g Radio

Steps 6 through 8 are exactly the same as *Step 2: Enabling 802.11a Radio on page 9* and *Steps 3 through 5: Radio Security Configuration on page 10*. The configuration process is repeated for the 802.11b/g radio. Once the configurations for the second radio are complete, selecting **Next** will continue on to a confirmation menu.

Confirmation

Once security settings have been configured for both radios, a confirmation menu appears, presenting an opportunity to review and validate information that has been entered. Verify the information and select **Finish** to complete the wizard.



Confirm Settings

AP MAC: 00:A0:C8:1F:6F:1B

Please review the settings that you have configured for the access point. You may use the "Back" button to change any incorrect settings or "Finish" to complete your setup.

AP Mac:	00:A0:C8:1F:6F:1B
AP Name:	uniquename
AP Location:	
Country-Region:	United States
802.11a Radio SSID:	ADTRAN Broadcast Mode: Disable
802.11a Radio Security:	wpa tkip eap
Radius Server IP:	...
Radius Key:	
802.11bg Radio SSID:	ADTRAN Broadcast Mode: Disable
802.11bg Radio Security:	none

Figure 10. Confirm Settings Menu

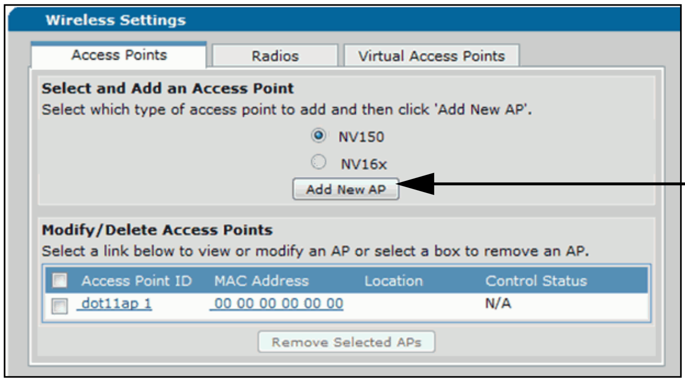
The configured APs will appear in the main menu under **Configured Access Points** and will be under the control of the AC. The APs are now accessible for specific configurations.

NOTE

Once an AP is controlled by the AC, the wizard button option will no longer be available.

Manually Adding an Access Point

APs can also be manually added to the AC. To add an AP, select **Data** > **APs/Radios/VAPs** > **Access Points** tab, select **NV 150**, and then select the **Add New AP** button.



Select and Add an Access Point

Select which type of access point to add and then click 'Add New AP'.

● NV150

○ NV16x

Modify/Delete Access Points

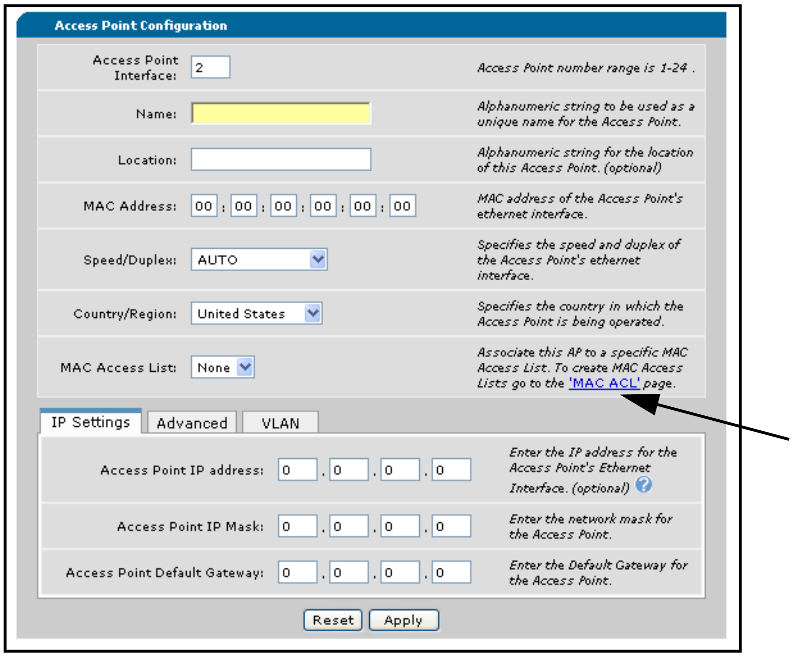
Select a link below to view or modify an AP or select a box to remove an AP.

□	Access Point ID	MAC Address	Location	Control Status
□	dot11ap 1	00 00 00 00 00 00		N/A

Select **Add New AP** to manually add an interface.

Figure 11. Access Points Tab Menu

After selecting the **Add New AP** button, the following configuration settings are available.



Access Point Configuration

Access Point Interface:	2	Access Point number range is 1-24 .
Name:		Alphanumeric string to be used as a unique name for the Access Point.
Location:		Alphanumeric string for the location of this Access Point. (optional)
MAC Address:	00 : 00 : 00 : 00 : 00 : 00	MAC address of the Access Point's ethernet interface.
Speed/Duplex:	AUTO	Specifies the speed and duplex of the Access Point's ethernet interface.
Country/Region:	United States	Specifies the country in which the Access Point is being operated.
MAC Access List:	None	Associate this AP to a specific MAC Access List. To create MAC Access Lists go to the 'MAC ACL' page.

Access Point IP address:	0 . 0 . 0 . 0	Enter the IP address for the Access Point's Ethernet Interface. (optional)
Access Point IP Mask:	0 . 0 . 0 . 0	Enter the network mask for the Access Point.
Access Point Default Gateway:	0 . 0 . 0 . 0	Enter the Default Gateway for the Access Point.

Link to the **MAC ACL**.

Figure 12. Access Point Configuration Menu

The media access control (MAC) address of the AP can be obtained by looking at the label on the bottom of the unit. The unit’s MAC address will also show in the **Dynamically Discovered Access Points** menu when the AP is first discovered.

The Ethernet speed, duplex, and 802.1q settings are configured from the **Access Point Configuration** menu. A MAC address filter can also be applied to allow only specific clients to communicate with the AP. The MAC access control list (ACL), accessible from a hyperlink on the right of the menu, must be created before you can apply the MAC address filter to the AP.

NOTE

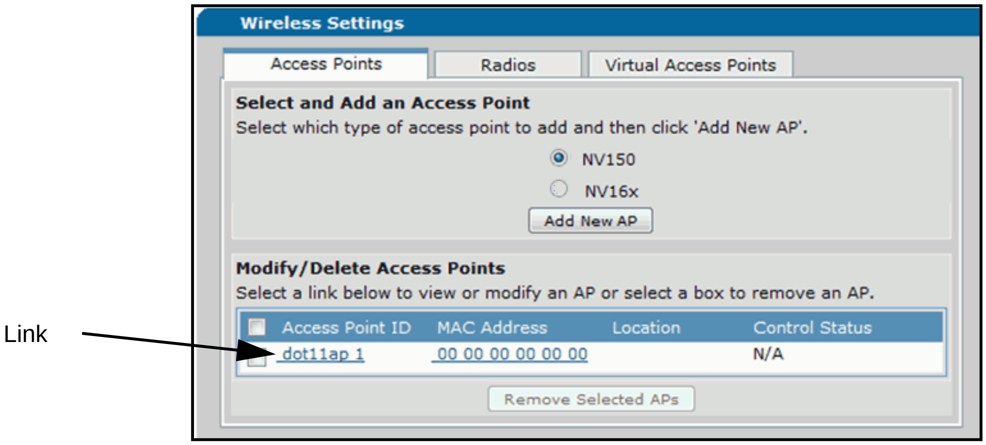
For more information regarding the configuration of MAC ACLs, refer to Appendix A. Creating MAC ACLs Using the CLI and GUI on page 38 of this guide.

NOTE

*Each AP ID is designated in the form **dot11ap** <ap>. The <ap> represents the interface number to which the AP is assigned.*

Modifying AP Configuration

To modify or view a configured AP, select the link of the AP you wish to view or modify.



Select and Add an Access Point

Select which type of access point to add and then click 'Add New AP'.

● NV150

○ NV16x

Modify/Delete Access Points

Select a link below to view or modify an AP or select a box to remove an AP.

□	Access Point ID	MAC Address	Location	Control Status
□	dot11ap 1	00 00 00 00 00 00		N/A

Figure 13. Modify/Delete Access Points Menu

General Parameters

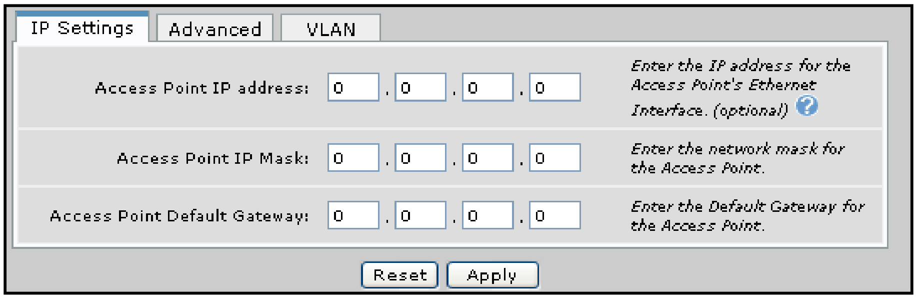
Once you have selected the link, the **Access Point Configuration** menu (the same menu used to statically add an AP) will open. The menu displays information for a specific AP, including **Access Point Interface**, **Name**, **Location**, **MAC Address**, **Speed/Duplex** settings, **Country/Region**, and **MAC Access List**. From this menu, changes can be made to the preceding parameters.

NOTE

Multiple ACs can be configured to control a single AP. The first to complete the negotiation handshake will establish control. After an AP reboot, the AP will initially attempt to re-establish communication with that AC. If not successful, it will then allow another valid AC to take control. The controlling AC applies its configuration to a controlled AP. If control is passed to another AC, that AC's configuration for the AP will be applied, even if it is different than that of the previous controlling AC. If using multiple ACs to control an AP, it is important that the configuration settings be coordinated and applicable for the overall network design.

IP Settings

The optional IP Settings for the AP can be configured from the **IP Settings** tab at the bottom of the **Access Point Configuration** menu. These settings are optional, and only used if using a RADIUS server.



Access Point IP address: 0 . 0 . 0 . 0 — *Enter the IP address for the Access Point's Ethernet Interface. (optional)*

Access Point IP Mask: 0 . 0 . 0 . 0 — *Enter the network mask for the Access Point.*

Access Point Default Gateway: 0 . 0 . 0 . 0 — *Enter the Default Gateway for the Access Point.*

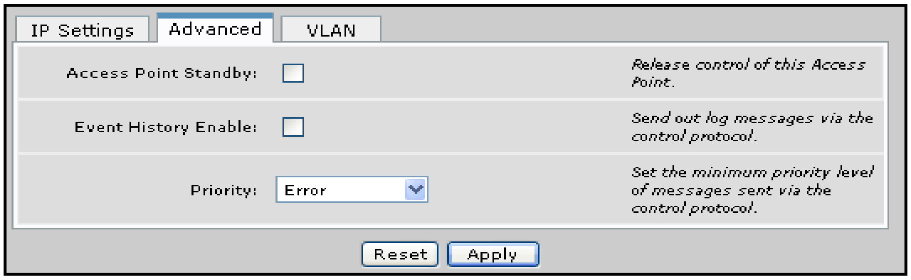
Figure 14. IP Settings Tab Menu

From the **IP Settings** tab, the AOS AP can be assigned an IP address, IP mask, and default gateway.

NOTE *You will not be able to configure the AP (Telnet, SSH, or HTTP/HTTPS) from its IP address. The IP information is used to communicate with a RADIUS authentication server when using 802.1x. It will also respond to Internet Control Message Protocol (ICMP) echo requests (ping) for connectivity testing.*

Advanced Settings

Use the **Advanced** settings tab to release control of a specific AP, enable event history logs, and select the type of messages sent via the control protocol. To access the **Advanced** settings menu, select the **Advanced** tab at the bottom of the **Access Point Configuration** menu.



Access Point Standby: □ — *Release control of this Access Point.*

Event History Enable: □ — *Send out log messages via the control protocol.*

Priority: Error — *Set the minimum priority level of messages sent via the control protocol.*

Figure 15. Advanced Tab Menu

Check the **Access Point Standby** box to release control of the AP. By checking this box, the AC will no longer send responses to echos from this particular AP.

Check the **Event History Enable** box to enable log messages.

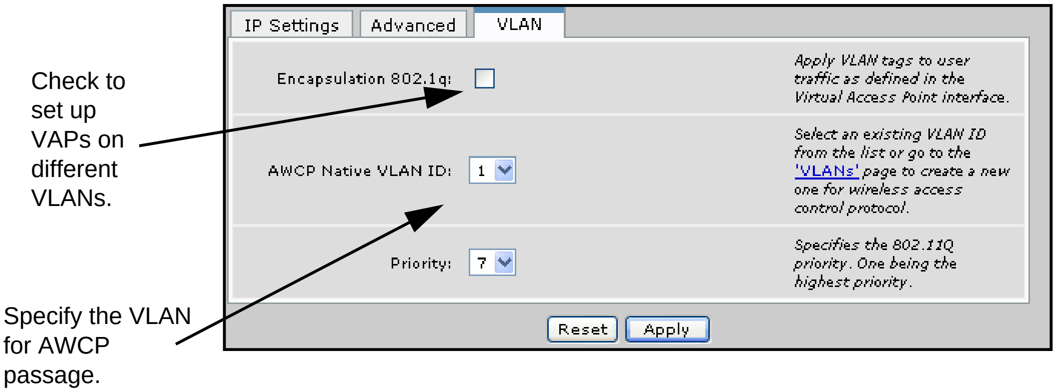
In the **Priority** drop-down menu, choose the message type to be sent via the control protocol. Choices include: **Alert**, **Critical**, **Error**, **Warning**, **Notice**, and **Informational**.

VLAN Settings

The virtual local area network (VLAN) settings are used primarily in the creation of VAPs. The VLAN settings are located on the **VLAN** tab at the bottom of the **Access Point Configuration** menu. Configurations under the **VLAN** menu include enabling 802.1q encapsulation, setting a native VLAN ID, and setting the priority level for 802.1q communication.

The 802.1q encapsulation should be enabled in order to set up VAPs operating on different VLANs. The 802.1q protocol maps VAPs to specific VLANs within the network via trunking, thus dividing the network among specific groups of users.

The specification of the native VLAN ID specifies the VLAN over which the AWCP will pass.



Encapsulation 802.1q: □

Apply VLAN tags to user traffic as defined in the Virtual Access Point interface.

AWCP Native VLAN ID: 1

Select an existing VLAN ID from the list or go to the 'VLANs' page to create a new one for wireless access control protocol.

Priority: 7

Specifies the 802.11Q priority. One being the highest priority.

Check to set up VAPs on different VLANs.

Specify the VLAN for AWCP passage.

Figure 16. VLAN Tab Menu

For more information regarding VAPs, refer to *Configuring AOS AP Virtual Access Points on page 22* of this guide. For an example VAP/VLAN topography, refer to *Virtual Access Point Model on page 33* of this guide.

Applying the Settings

When all parameters for the AP are configured, selecting the **Apply** button at the bottom of the **Access Point Configuration** menu will apply all modifications to the AP.

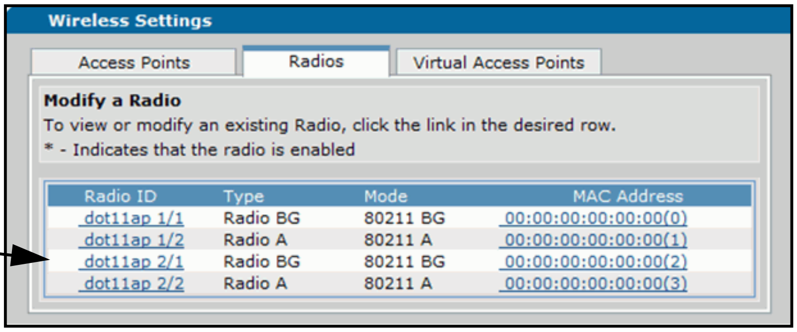
Repeat the process for any additional APs you wish to configure or add.

Configuring the AOS AP Radios

When the AP is configured, both radios are detected and given an interface. Selecting **Data** > **Wireless** > **APs/Radios/VAPs** > **Radio Tab** will show both radios associated with an AP.

The radio ID is based on the interface to which the AP is mapped (**dot11ap** <*ap/radio*>, where <*ap*> is the AP interface number and <*radio*> is the radio interface number). The asterisk beside the radio ID indicates that the radio is enabled. Each **Radio ID** is a hyperlink that brings up a configuration page for the radio’s basic and advanced settings.

Select the **Radio ID** link to bring up radio settings.



Modify a Radio

To view or modify an existing Radio, click the link in the desired row.

* - Indicates that the radio is enabled

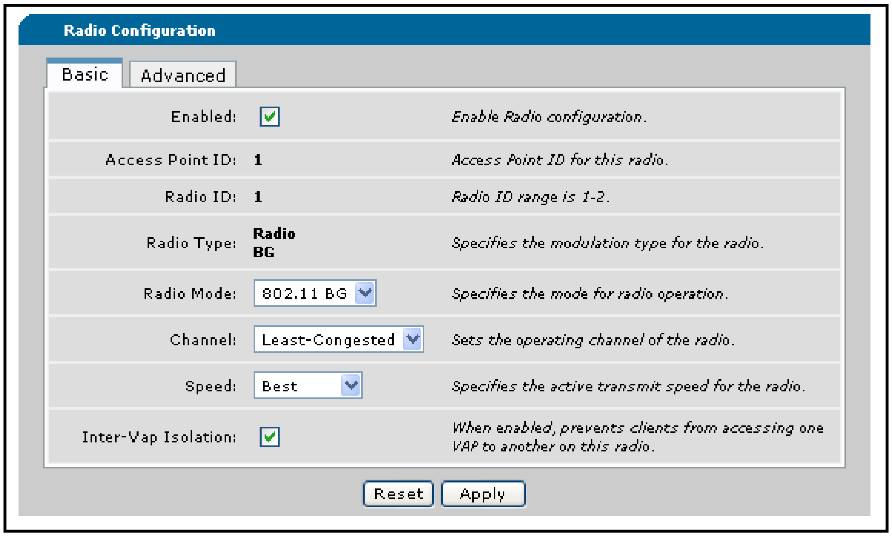
Radio ID	Type	Mode	MAC Address
dot11ap 1/1	Radio BG	80211 BG	00:00:00:00:00:00(0)
dot11ap 1/2	Radio A	80211 A	00:00:00:00:00:00(1)
dot11ap 2/1	Radio BG	80211 BG	00:00:00:00:00:00(2)
dot11ap 2/2	Radio A	80211 A	00:00:00:00:00:00(3)

Figure 17. Radios Tab Menu

NOTE *The radios are automatically detected. You cannot manually add or delete radios.*

Basic Settings

Basic radio settings include enabling the radio; selecting the station role, radio channel, and rate; and enabling inter-VAP isolation. To enter the basic configuration menu, select the **Basic** tab.



Enabled:	☑	Enable Radio configuration.
Access Point ID:	1	Access Point ID for this radio.
Radio ID:	1	Radio ID range is 1-2.
Radio Type:	Radio BG	Specifies the modulation type for the radio.
Radio Mode:	802.11 BG	Specifies the mode for radio operation.
Channel:	Least-Congested	Sets the operating channel of the radio.
Speed:	Best	Specifies the active transmit speed for the radio.
Inter-Vap Isolation:	☑	When enabled, prevents clients from accessing one VAP to another on this radio.

Figure 18. Radio Configuration Basic Tab Menu

Selecting Enabled

Enabling the radio will determine whether the radio is broadcasting.

Selecting the Radio Mode

The drop-down menu specifies in which mode the radio will be operating. BG Radios can operate in either B mode, G mode, or BG mode. A radios will always operate in A mode.

Selecting Radio Channel and Speed

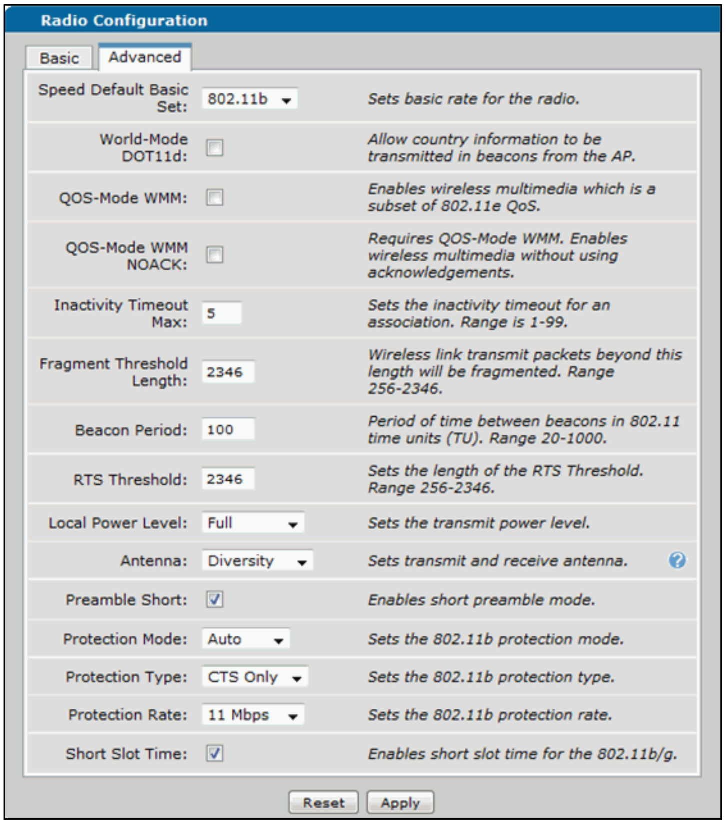
Radio **Channel** and **Speed** selections set the operating channel and the speed of active transmit for the radio. The **Channel** can be set to zero to scan for the best channel. The **Speed** selection can be set to **Best** for the best available speed, or to a specific speed.

Selecting Inter-VAP Isolation

Inter-VAP Isolation, when enabled, prevents a client associated with one VAP from communicating with clients associated with different VAPs without going through a router.

Advanced Settings

The **Advanced** tab provides many options for radio configuration, including antenna settings and power options.



Radio Configuration

Speed Default Basic Set:	802.11b	*Sets basic rate for the radio.*
World-Mode DOT11d:	□	*Allow country information to be transmitted in beacons from the AP.*
QOS-Mode WMM:	□	*Enables wireless multimedia which is a subset of 802.11e QoS.*
QOS-Mode WMM NOACK:	□	*Requires QOS-Mode WMM. Enables wireless multimedia without using acknowledgements.*
Inactivity Timeout Max:	5	*Sets the inactivity timeout for an association. Range is 1-99.*
Fragment Threshold Length:	2346	*Wireless link transmit packets beyond this length will be fragmented. Range 256-2346.*
Beacon Period:	100	*Period of time between beacons in 802.11 time units (TU). Range 20-1000.*
RTS Threshold:	2346	*Sets the length of the RTS Threshold. Range 256-2346.*
Local Power Level:	Full	*Sets the transmit power level.*
Antenna:	Diversity	*Sets transmit and receive antenna.*
Preamble Short:	☑	*Enables short preamble mode.*
Protection Mode:	Auto	*Sets the 802.11b protection mode.*
Protection Type:	CTS Only	*Sets the 802.11b protection type.*
Protection Rate:	11 Mbps	*Sets the 802.11b protection rate.*
Short Slot Time:	☑	*Enables short slot time for the 802.11b/g.*

Figure 19. Radio Configuration Advanced Tab

For optimal radio operation, most of the advanced setting defaults should remain unchanged. The default values are described in the following table:

Table 2. Radio Default Settings

Parameter	802.11 b/g Radio Defaults	802.11a Radio Defaults
Speed Default Basic Set	802.11	802.11
Inactivity Timeout Max	5	5
Fragment Threshold Length	2346	2346
Beacon Period	100	100
RTS Threshold	2346	2346
Local Power Level	Full	Full
Antenna	Diversity	Diversity
Preamble Short	Enabled	N/A
Protection Mode	Auto	N/A
Protection Type	CTS Only	N/A
Protection Rate	11 Mbps	N/A
Short Slot Time	Enabled	N/A

NOTE

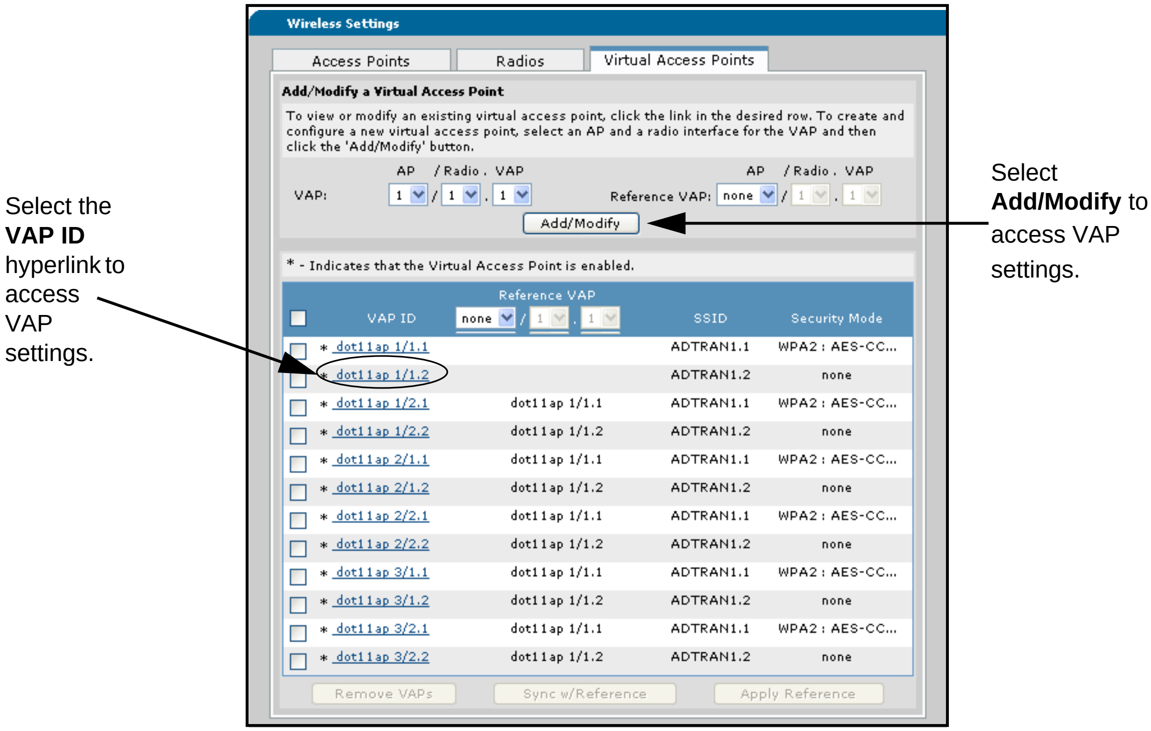
*Setting the antenna to **Diversity** means using both antennas for the best transmission signal. If using a single directional antenna, the appropriate antenna (Antenna 1 or Antenna 2) must be specified in the radio **Advanced** menu.*

When radio configuration is complete, select the **Apply** button at the bottom of the menu to apply the settings.

Configuring AOS AP Virtual Access Points

A VAP is a logical representation of a wireless network. VAPs are distinguished by an SSID and can be mapped to a VLAN. VLAN information can be shared across switches with Ethernet trunks. An AOS AP can terminate Ethernet trunks and associate a VAP with a VLAN. A common example of this is having two VAPs, one associated to a corporate VLAN, and one associated to a guest VLAN.

To configure a VAP, select **Data** > **Wireless** > **APs/Radios/VAPs** > **Virtual Access Point Tab**. Each radio will have a default VAP configured. The VAP name is based on the interface the AP and radio are mapped to (**dot11ap** <*ap/radio.vap*>,where <*ap*> is the AP interface number, <*radio*> is the radio interface number, and <*.vap*> is the VAP interface number). To add a VAP, select the appropriate **AP**, **Radio Interface**, and **VAP Interface** numbers, and then select **Add/Modify**.



Select the **VAP ID** hyperlink to access VAP settings.

Select **Add/Modify** to access VAP settings.

Wireless Settings

Add/Modify a Virtual Access Point

To view or modify an existing virtual access point, click the link in the desired row. To create and configure a new virtual access point, select an AP and a radio interface for the VAP and then click the 'Add/Modify' button.

VAP: AP 1 / Radio 1 . VAP 1   Reference VAP: AP none / Radio 1 . VAP 1

* - Indicates that the Virtual Access Point is enabled.

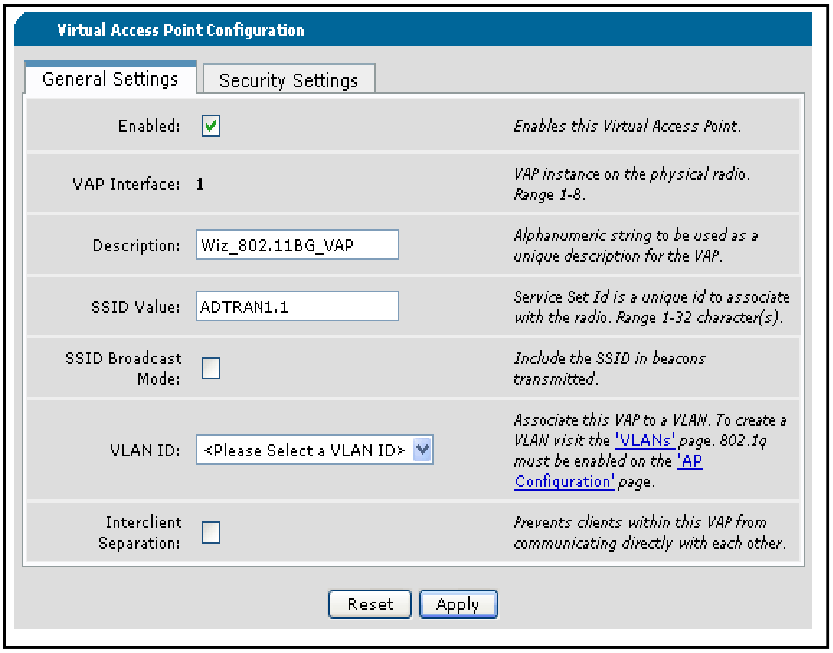
	VAP ID	Reference VAP none / 1 . 1	SSID	Security Mode
□	* dot11ap 1/1.1		ADTRAN1.1	WPA2 : AES-CC...
□	* dot11ap 1/1.2		ADTRAN1.2	none
□	* dot11ap 1/2.1	dot11ap 1/1.1	ADTRAN1.1	WPA2 : AES-CC...
□	* dot11ap 1/2.2	dot11ap 1/1.2	ADTRAN1.2	none
□	* dot11ap 2/1.1	dot11ap 1/1.1	ADTRAN1.1	WPA2 : AES-CC...
□	* dot11ap 2/1.2	dot11ap 1/1.2	ADTRAN1.2	none
□	* dot11ap 2/2.1	dot11ap 1/1.1	ADTRAN1.1	WPA2 : AES-CC...
□	* dot11ap 2/2.2	dot11ap 1/1.2	ADTRAN1.2	none
□	* dot11ap 3/1.1	dot11ap 1/1.1	ADTRAN1.1	WPA2 : AES-CC...
□	* dot11ap 3/1.2	dot11ap 1/1.2	ADTRAN1.2	none
□	* dot11ap 3/2.1	dot11ap 1/1.1	ADTRAN1.1	WPA2 : AES-CC...
□	* dot11ap 3/2.2	dot11ap 1/1.2	ADTRAN1.2	none

Figure 20. Add/Modify a Virtual Access Point Menu

Once a VAP has been added, it can be accessed either through the **Add/Modify** button or the **VAP ID** hyperlink.

General VAP Settings

The **General Settings** tab for the VAP is located in the **Virtual Access Point Configuration** menu, accessed by selecting the **VAP ID** hyperlink or **Add/Modify** button on the menu shown in *Figure 20 on page 23*. On the **General Settings** tab (*Figure 21*), you can define the SSID, turn off SSID broadcast, enable interclient separation, and describe the VAP.



Enabled:	☑	Enables this Virtual Access Point.
VAP Interface:	1	VAP instance on the physical radio. Range 1-8.
Description:	Wiz_802.11BG_VAP	Alphanumeric string to be used as a unique description for the VAP.
SSID Value:	ADTRAN1.1	Service Set Id is a unique id to associate with the radio. Range 1-32 character(s).
SSID Broadcast Mode:	□	Include the SSID in beacons transmitted.
VLAN ID:	<Please Select a VLAN ID>	Associate this VAP to a VLAN. To create a VLAN visit the 'VLANs' page. 802.1q must be enabled on the 'AP Configuration' page.
Interclient Separation:	□	Prevents clients within this VAP from communicating directly with each other.

Figure 21. VAP General Settings Tab Menu

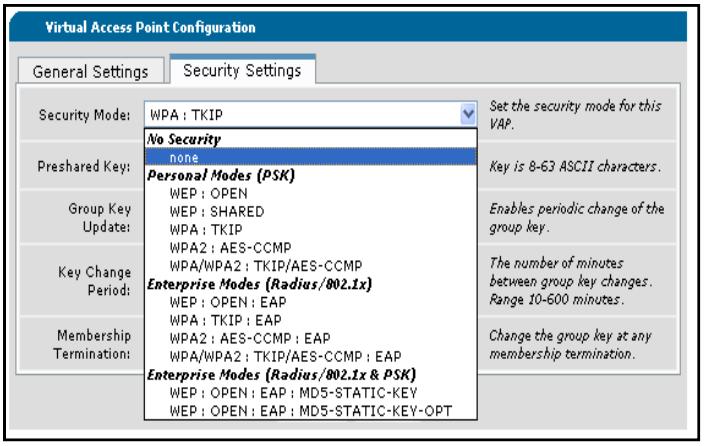
If the SSID broadcast mode is not checked, the AP beacon will no longer broadcast the SSID. This provides a minimal amount of security and it is recommended.

Enabling **Interclient Separation** prevents clients within the VAP from communicating directly with each other.

When the general settings are configured, select the **Apply** button to activate them.

VAP Security Settings

The VAP **Security Settings** tab is located in the **Virtual Access Point Configuration** menu. Choose the security mode of your preference from the drop-down menu.



Virtual Access Point Configuration

General Settings | Security Settings

Security Mode: WPA : TKIP — Set the security mode for this VAP.

Preshared Key: — Key is 8-63 ASCII characters.

Group Key Update: — Enables periodic change of the group key.

Key Change Period: — The number of minutes between group key changes. Range 10-600 minutes.

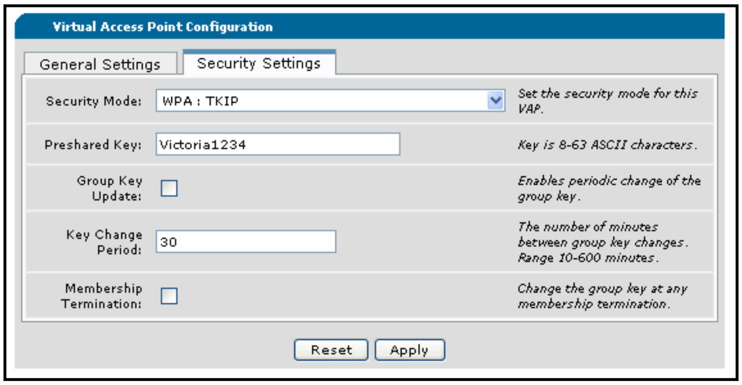
Membership Termination: — Change the group key at any membership termination.

No Security
none
Personal Modes (PSK)
WEP : OPEN
WEP : SHARED
WPA : TKIP
WPA2 : AES-CCMP
WPA/WPA2 : TKIP/AES-CCMP
Enterprise Modes (Radius/802.1x)
WEP : OPEN : EAP
WPA : TKIP : EAP
WPA2 : AES-CCMP : EAP
WPA/WPA2 : TKIP/AES-CCMP : EAP
Enterprise Modes (Radius/802.1x & PSK)
WEP : OPEN : EAP : MD5-STATIC-KEY
WEP : OPEN : EAP : MD5-STATIC-KEY-OPT

Figure 22. VAP Security Settings Tab Menu

NOTE *The AP and the client must have matching security settings. If using an authentication server, the server settings will have to match the client's as well. If using EAP, the client and authentication server (RADIUS) must use the same EAP types.*

Once the security setting is chosen from the drop-down menu, there will be an automatic prompt for the appropriate information for the particular security setting. The example in *Figure 23* uses a WPA setting (**WPA: TKIP**).



Virtual Access Point Configuration

General Settings | Security Settings

Security Mode: WPA : TKIP — Set the security mode for this VAP.

Preshared Key: Victoria1234 — Key is 8-63 ASCII characters.

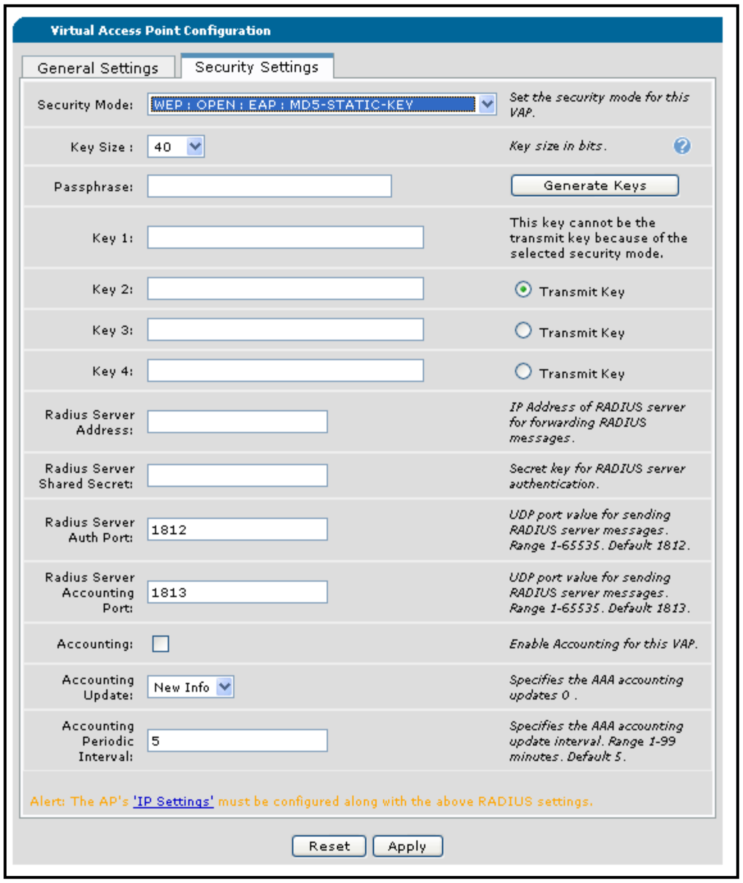
Group Key Update: □ — Enables periodic change of the group key.

Key Change Period: 30 — The number of minutes between group key changes. Range 10-600 minutes.

Membership Termination: □ — Change the group key at any membership termination.

Figure 23. WPA: TKIP Security Settings Example

The example in *Figure 24* uses a WEP setting (**WEP: OPEN: EAP: MD5-STATIC-KEY**).



Virtual Access Point Configuration

General Settings | Security Settings

Security Mode:	WEP : OPEN : EAP : MD5-STATIC-KEY	*Set the security mode for this VAP.*
Key Size :	40	*Key size in bits.*
Passphrase:		Generate Keys
Key 1:		This key cannot be the transmit key because of the selected security mode.
Key 2:		● Transmit Key
Key 3:		○ Transmit Key
Key 4:		○ Transmit Key
Radius Server Address:		*IP Address of RADIUS server for forwarding RADIUS messages.*
Radius Server Shared Secret:		*Secret key for RADIUS server authentication.*
Radius Server Auth Port:	1812	*UDP port value for sending RADIUS server messages. Range 1-65535. Default 1812.*
Radius Server Accounting Port:	1813	*UDP port value for sending RADIUS server messages. Range 1-65535. Default 1813.*
Accounting:	□	*Enable Accounting for this VAP.*
Accounting Update:	New Info	*Specifies the AAA accounting updates 0 .*
Accounting Periodic Interval:	5	*Specifies the AAA accounting update interval. Range 1-99 minutes. Default 5.*

Alert: The AP's 'IP Settings' must be configured along with the above RADIUS settings.

Reset Apply

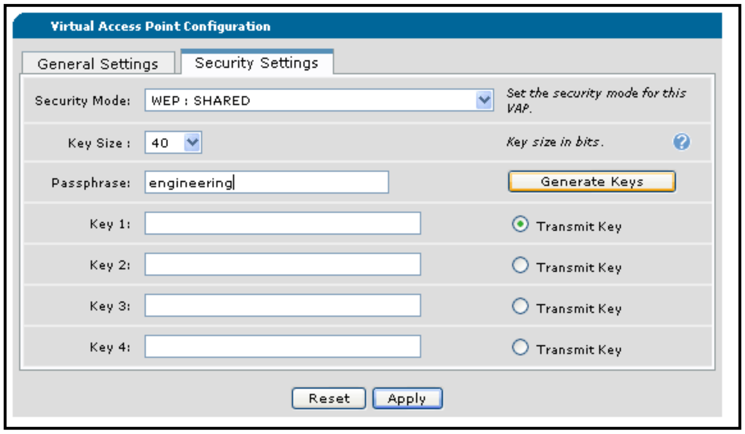
Figure 24. MD5 Security Settings Example

WEP Key Generator

Beginning in AOS Release 17.2, all WEP security options include a WEP key generator feature. The feature operates by using a passphrase to generate WEP keys through a standard MD5 key generator.

The feature allows for keys to be quickly produced if the passphrase is known. Most mobile clients have the ability to generate keys, and through this feature VAPs will also have the ability to produce these keys. To use the WEP key generator, follow these steps:

1. From the appropriate V**AP Security Settings** menu (any menu that requires a WEP key), enter the passphrase in the appropriate field.



Virtual Access Point Configuration

General Settings | Security Settings

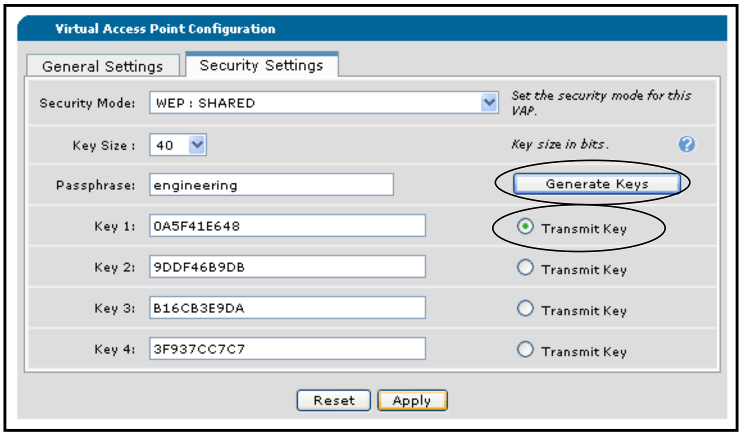
Security Mode:	WEP : SHARED	*Set the security mode for this VAP.*
Key Size :	40	*Key size in bits.*
Passphrase:	engineering	Generate Keys
Key 1:		● Transmit Key
Key 2:		○ Transmit Key
Key 3:		○ Transmit Key
Key 4:		○ Transmit Key

Reset Apply

Figure 25. WEP Key Generator Passphrase Menu

The passphrase is a phrase 1 to 32 characters in length. When the **Generate Keys** button is selected, the key generator will generate random values for each element (letter or number) in the passphrase, thus creating secure WEP keys.

2. Once the passphrase has been entered, select **Generate Keys**. Four keys are generated from the single passphrase.



Virtual Access Point Configuration

General Settings | Security Settings

Security Mode:	WEP : SHARED	*Set the security mode for this VAP.*
Key Size :	40	*Key size in bits.*
Passphrase:	engineering	Generate Keys
Key 1:	0A5F41E648	● Transmit Key
Key 2:	9DDF46B9DB	○ Transmit Key
Key 3:	B16CB3E9DA	○ Transmit Key
Key 4:	3F937CC7C7	○ Transmit Key

Reset Apply

Figure 26. Generated WEP Keys

3. The first key generated is automatically set to transmit. To change the transmitted key, select **Transmit Key** next to the key you wish to transmit. Selecting **Reset** will clear the generated keys and set the VAP security to **none**.

4. Once the security settings have been entered, select **Apply** to add them to the VAP's configuration.

> NOTE
>
> *Generated WEP keys will not be part of the VAP configuration until the* ***Apply*** *button is selected.*

The basic parameters of the AOS AP and VAP have now been configured. For more information about specific configurations and commands using the CLI, refer to the *AOS Command Reference Guide* available online at https://supportforums.adtran.com.

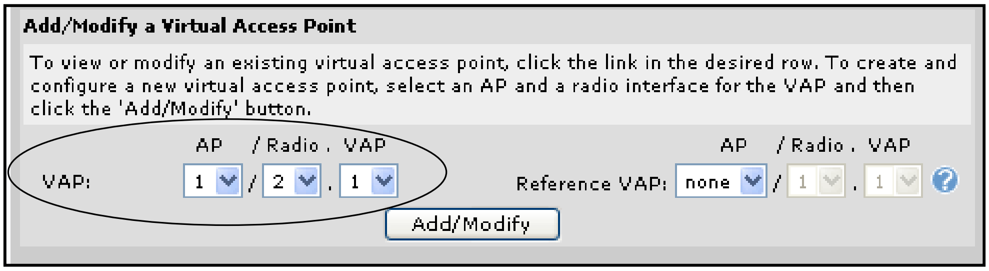
Referencing VAPs

VAP referencing is a feature introduced in AOS Release 17.2. The feature allows a single VAP configuration to serve as a reference for quickly configuring other VAPs. This feature facilitates consistent settings across APs, which aids in smooth transitions between APs for mobile wireless clients. The feature allows a VAP configuration to be copied as a reference configuration for configuring other VAPs, tracks the synchronization between referenced VAPs, and also enables quick copying of a VAP configuration to other VAPs even if it is not the reference configuration.

Once a VAP configuration exists to use as a reference, the configuration can be copied to other VAPs either as they are created or as they are modified.

To copy a reference configuration as a new VAP is created, follow these steps:

1. To add a VAP, select the appropriate **AP**, **Radio Interface**, and **VAP** numbers. In the following examples, VAP 1/2.1 is created by copying the VAP configuration of VAP 1/1.1.



Add/Modify a Virtual Access Point

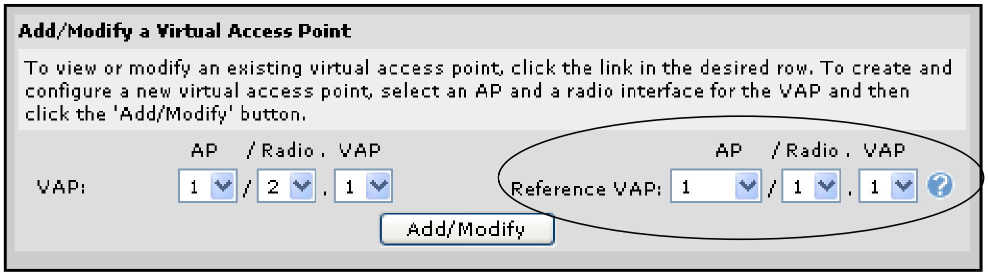
To view or modify an existing virtual access point, click the link in the desired row. To create and configure a new virtual access point, select an AP and a radio interface for the VAP and then click the 'Add/Modify' button.

VAP: AP 1 / Radio 2 . VAP 1

Reference VAP: AP none / Radio 1 . VAP 1

Figure 27. Adding a VAP for VAP Referencing

2. Select the **AP**, **Radio Interface**, and **VAP** numbers to be referenced from the **Reference VAP** menu.



Add/Modify a Virtual Access Point

To view or modify an existing virtual access point, click the link in the desired row. To create and configure a new virtual access point, select an AP and a radio interface for the VAP and then click the 'Add/Modify' button.

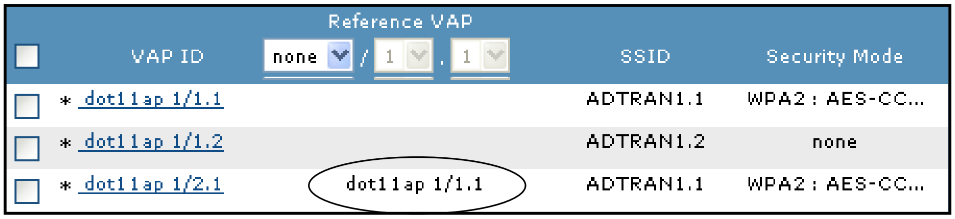
VAP: AP 1 / Radio 2 . VAP 1

Reference VAP: AP 1 / Radio 1 . VAP 1

Figure 28. Entering Reference VAP Information

3. Select **Add/Modify** to create a new VAP with the same configuration settings as the selected reference VAP.

4. The new VAP will appear at the bottom of the menu, with a VAP reference listed.

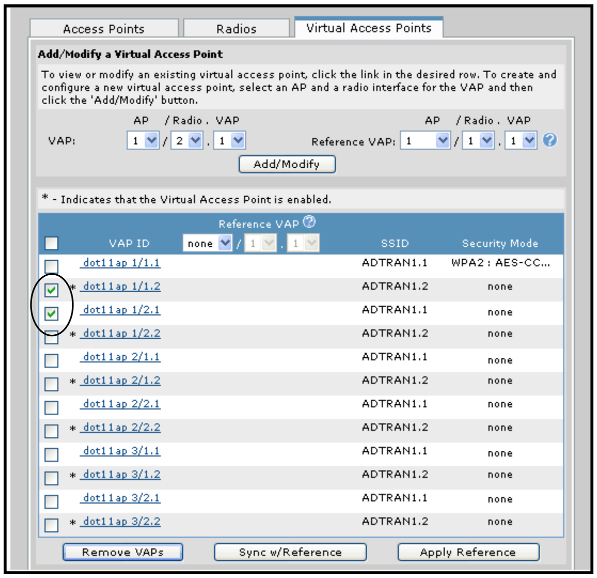


□	VAP ID	Reference VAP none / 1 . 1	SSID	Security Mode
□	* dot11ap 1/1.1		ADTRAN1.1	WPA2 : AES-CC...
□	* dot11ap 1/1.2		ADTRAN1.2	none
□	* dot11ap 1/2.1	dot11ap 1/1.1	ADTRAN1.1	WPA2 : AES-CC...

Figure 29. Reference VAP Appearance

To reference a VAP configuration on a VAP that is already configured, follow these steps:

1. Select the VAP to which you want to add the reference by checking the box. One or more boxes can be selected.



Add/Modify a Virtual Access Point

To view or modify an existing virtual access point, click the link in the desired row. To create and configure a new virtual access point, select an AP and a radio interface for the VAP and then click the 'Add/Modify' button.

VAP: AP 1 / Radio 2 . VAP 1

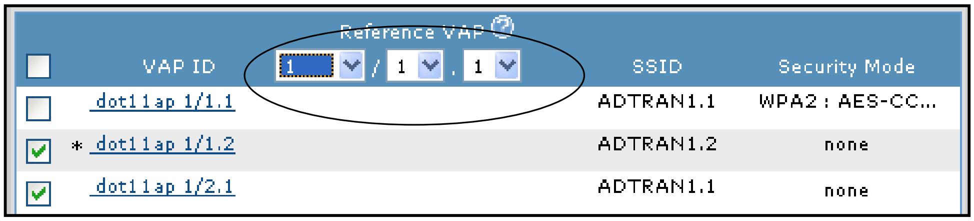
Reference VAP: AP 1 / Radio 1 . VAP 1

* - Indicates that the Virtual Access Point is enabled.

□	VAP ID	Reference VAP none / 1 . 1	SSID	Security Mode
□	dot11ap 1/1.1		ADTRAN1.1	WPA2 : AES-CC...
☑	* dot11ap 1/1.2		ADTRAN1.2	none
☑	dot11ap 1/2.1		ADTRAN1.1	none
□	* dot11ap 1/2.2		ADTRAN1.2	none
□	dot11ap 2/1.1		ADTRAN1.1	none
□	* dot11ap 2/1.2		ADTRAN1.2	none
□	dot11ap 2/2.1		ADTRAN1.1	none
□	* dot11ap 2/2.2		ADTRAN1.2	none
□	dot11ap 3/1.1		ADTRAN1.1	none
□	* dot11ap 3/1.2		ADTRAN1.2	none
□	dot11ap 3/2.1		ADTRAN1.1	none
□	* dot11ap 3/2.2		ADTRAN1.2	none

Figure 30. Adding a Reference VAP Manually

2. Select the appropriate **AP**, **Radio Interface**, and **VAP** numbers from the **Reference VAP** menu.



□	VAP ID	Reference VAP 1 / 1 . 1	SSID	Security Mode
□	dot11ap 1/1.1		ADTRAN1.1	WPA2 : AES-CC...
☑	* dot11ap 1/1.2		ADTRAN1.2	none
☑	dot11ap 1/2.1		ADTRAN1.1	none

Figure 31. Reference VAP Information

3. Select the **Apply Reference** button at the bottom of the menu to copy the configuration settings from the reference VAP to the selected VAP configuration.

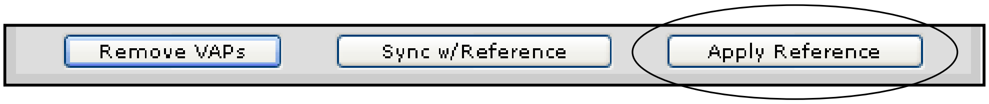
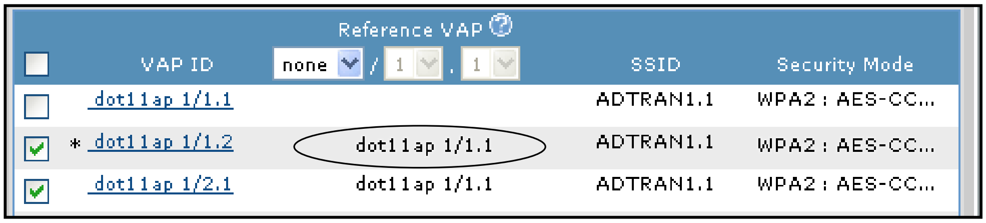


Figure 32. Apply Reference

4. The referenced VAP will appear listed next to the modified VAP.



☐	VAP ID	Reference VAP none / 1 . 1	SSID	Security Mode
☐	dot11ap 1/1.1		ADTRAN1.1	WPA2 : AES-CC...
☑	* dot11ap 1/1.2	dot11ap 1/1.1	ADTRAN1.1	WPA2 : AES-CC...
☑	dot11ap 1/2.1	dot11ap 1/1.1	ADTRAN1.1	WPA2 : AES-CC...

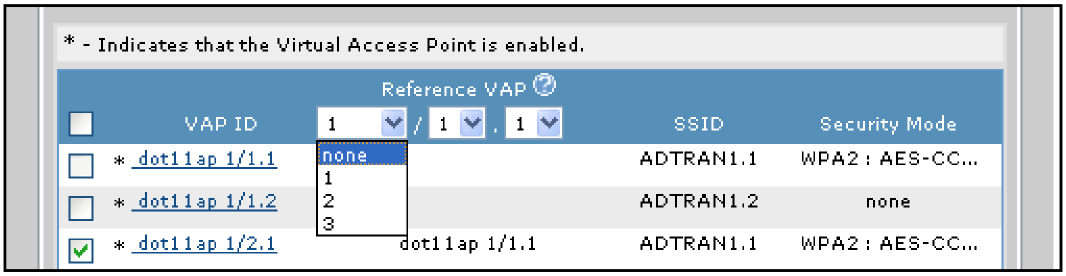
Figure 33. Referenced VAP Appearance

Synchronizing VAP References

The GUI indicates if the VAP and referenced VAP configurations are synchronized. If VAP references are not synchronized, the referenced VAPs will appear in orange. If the referenced VAP no longer exists, the referenced VAP will appear in red. The **Sync w/Reference** button allows the VAP configuration to be updated to match the referenced VAP configuration. The button can be used on a per VAP basis, or by selecting all VAPs, and then selecting the **Sync w/Reference** button.

Removing VAP References

References to a VAP configuration can be removed by selecting the VAP with the reference and then selecting **none** from the AP drop-down menu.



* - Indicates that the Virtual Access Point is enabled.

☐	VAP ID	Reference VAP 1 / 1 . 1	SSID	Security Mode
☐	* dot11ap 1/1.1		ADTRAN1.1	WPA2 : AES-CC...
☐	* dot11ap 1/1.2		ADTRAN1.2	none
☑	* dot11ap 1/2.1	dot11ap 1/1.1	ADTRAN1.1	WPA2 : AES-CC...

Figure 34. Reference VAP Drop-Down Menu

Once **none** is selected, select the **Apply Reference** button at the bottom of the menu. The reference VAP is removed, and will no longer appear in the referenced VAP list. Removing a referenced VAP does not change the VAP configuration settings.

WLAN Topographies

The following are a few examples of typical WLAN network configurations:

- *General Hotspot Connectivity*
- *Small-Medium Business Company Model*
- *Virtual Access Point Model*

General Hotspot Connectivity

The general hotspot connectivity model is a common application of an AOS AP. In this model, there are two T1s coming into the building and a NetVanta 150 coming off of the router/switch. This type of setup can be used for guest access, such as in an internal corporate hotspot in the lobby of a building. This model can also be used for a lab environment in which the server connects back to the LAN via the wireless connection, or for a conference room so that attendees do not have to connect to the wire line LAN for access to corporate resources.

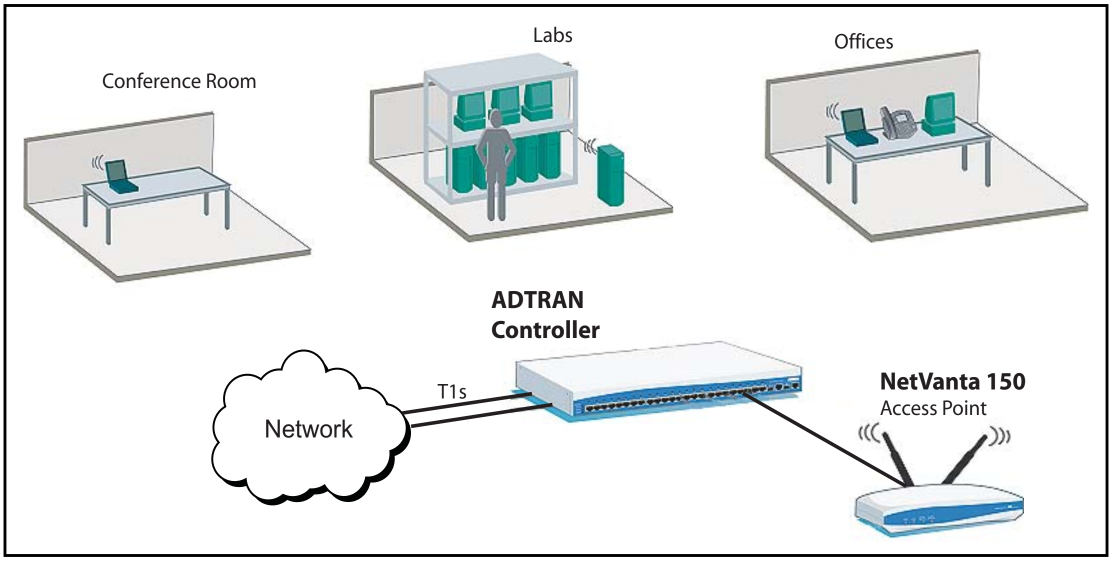


Figure 35. General Hotspot Connectivity

Small-Medium Business Company Model

This is a typical small- to medium-sized business model. There are two T1 lines coming into the router/switch, to which several devices are connected. These devices are connected to the network both wired and wirelessly.

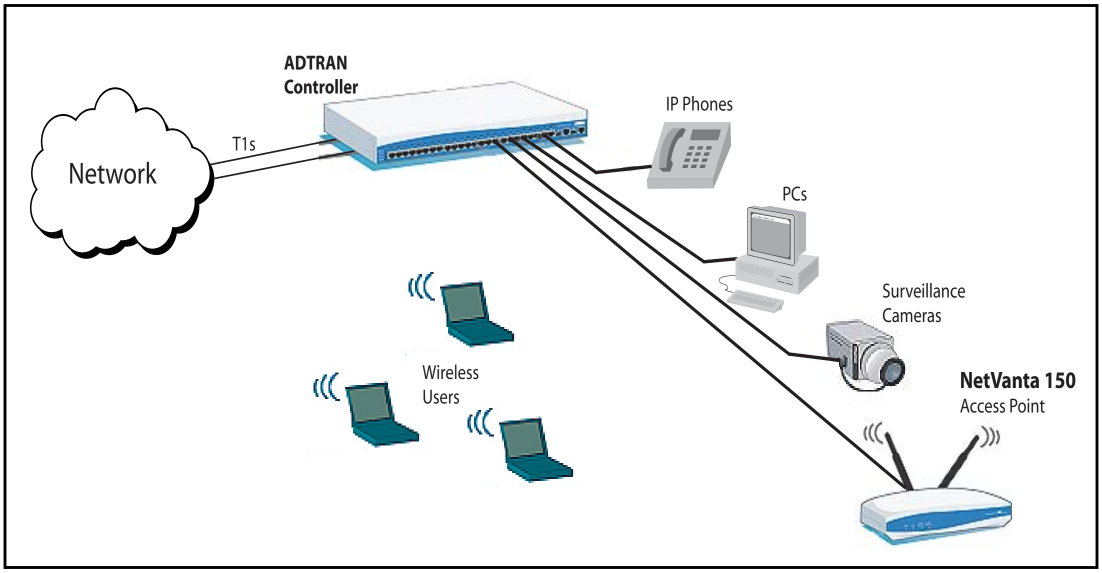


Figure 36. Small-Medium Business Company Model

Virtual Access Point Model

By using VAPs, which are identified by SSIDs, wireless users can be separated into VLANs. This allows for separation between divisions of a company (for example, marketing, engineering, and accounting) on both the wired and wireless LANs.

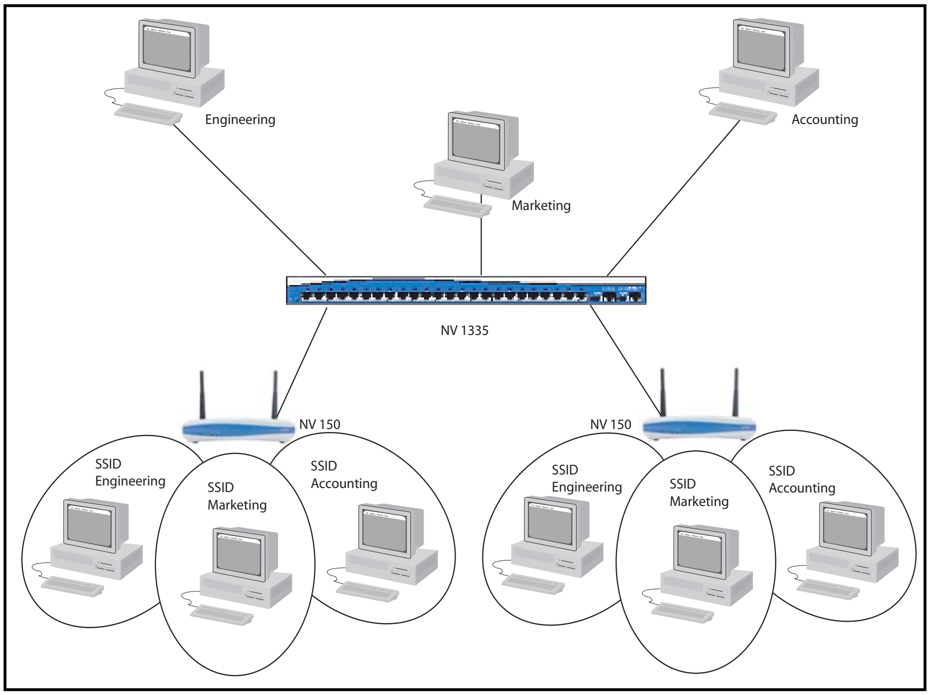


Figure 37. Virtual Access Point Model

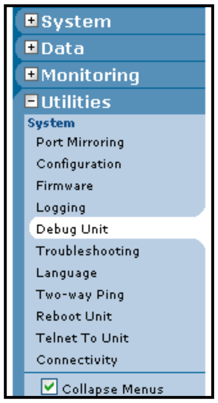
Troubleshooting

Debug statistics and general statistics for each AP, radio, and VAP are available through the GUI. These statistics aid in verifying configuration and troubleshooting.

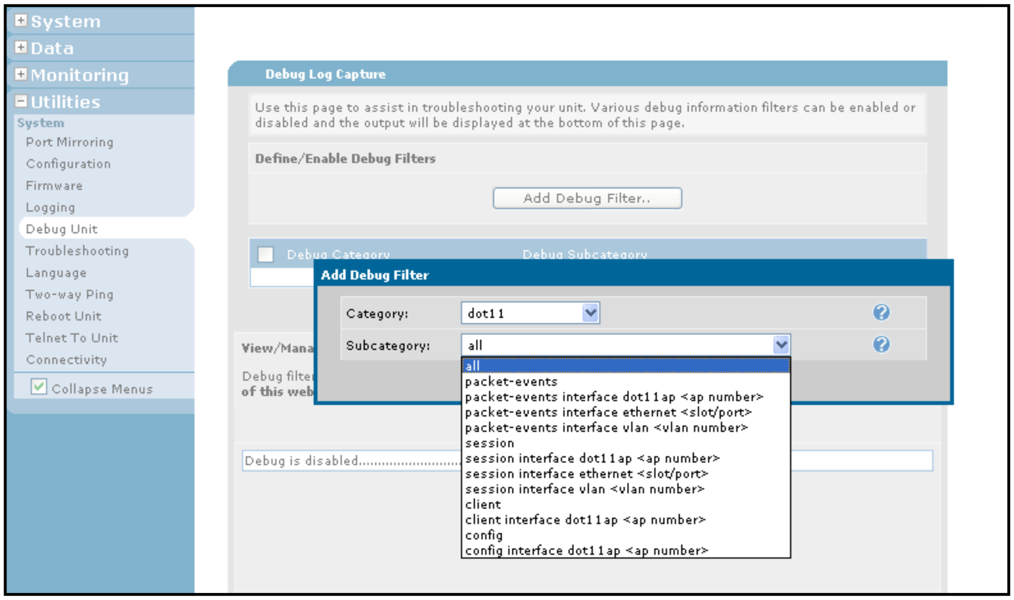
Using Debug Messaging

To access GUI debug messaging abilities, follow these steps:

1. Select **Debug Unit** from the **Utilities** menu.



2. Select **Add Debug Filter** and choose the desired item to debug from the **Category** drop-down menu. Select the appropriate entries from the **Subcategory** menu if necessary.



Debug Log Capture

Use this page to assist in troubleshooting your unit. Various debug information filters can be enabled or disabled and the output will be displayed at the bottom of this page.

Define/Enable Debug Filters

Add Debug Filter..

□ Debug Category Debug Subcategory

View/Mana

Debug filte
of this web

Debug is disabled..............................

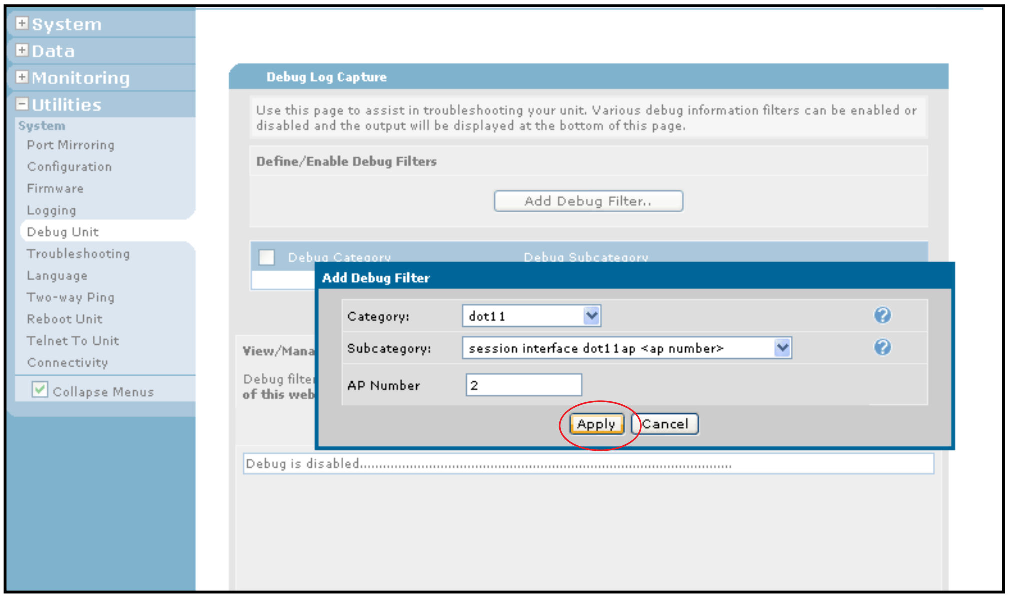
Add Debug Filter

Category: dot11

Subcategory: all

all
packet-events
packet-events interface dot11ap <ap number>
packet-events interface ethernet <slot/port>
packet-events interface vlan <vlan number>
session
session interface dot11ap <ap number>
session interface ethernet <slot/port>
session interface vlan <vlan number>
client
client interface dot11ap <ap number>
config
config interface dot11ap <ap number>

3. Select **Apply** when the correct item is chosen.



Debug Log Capture

Use this page to assist in troubleshooting your unit. Various debug information filters can be enabled or disabled and the output will be displayed at the bottom of this page.

Define/Enable Debug Filters

Add Debug Filter

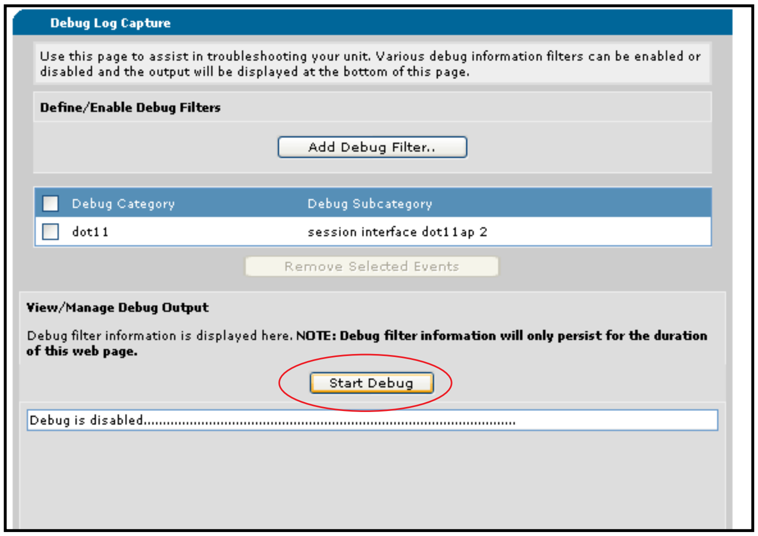
Category: dot11

Subcategory: session interface dot11ap <ap number>

AP Number 2

Debug is disabled...

4. The item you have selected will appear in the **Debug Category** list in the middle of the menu. To start receiving debug information, select the **Start Debug** tab.



Debug Log Capture

Use this page to assist in troubleshooting your unit. Various debug information filters can be enabled or disabled and the output will be displayed at the bottom of this page.

Define/Enable Debug Filters

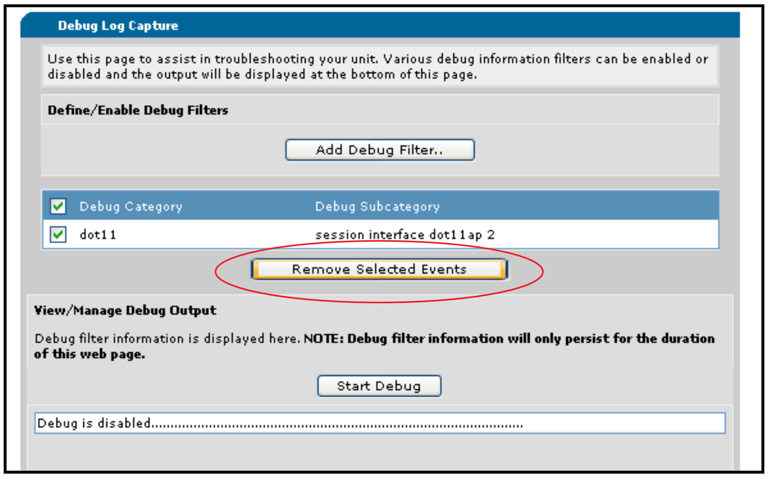
□ Debug Category	Debug Subcategory
□ dot11	session interface dot11ap 2

View/Manage Debug Output

Debug filter information is displayed here. **NOTE: Debug filter information will only persist for the duration of this web page.**

Debug is disabled...

5. To remove a debug filter, check the box next to the filter to remove and select **Remove Selected Events**.



Debug Log Capture

Use this page to assist in troubleshooting your unit. Various debug information filters can be enabled or disabled and the output will be displayed at the bottom of this page.

Define/Enable Debug Filters

Add Debug Filter..

☑ Debug Category	Debug Subcategory
☑ dot11	session interface dot11ap 2

Remove Selected Events

View/Manage Debug Output

Debug filter information is displayed here. **NOTE: Debug filter information will only persist for the duration of this web page.**

Start Debug

Debug is disabled...

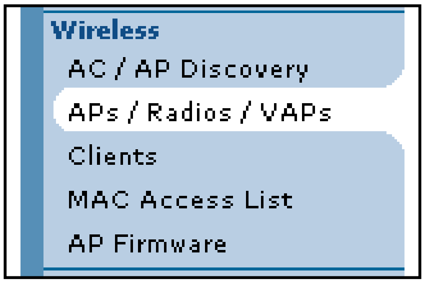
NOTE

Enabling debug messaging can be very processor intensive. Use debug messaging with caution.

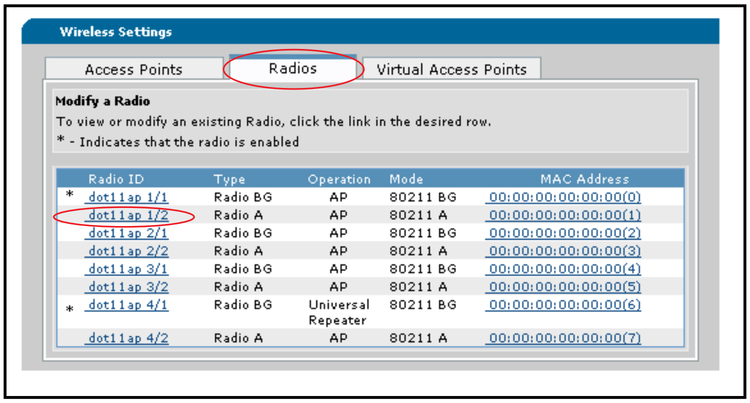
Viewing Unit Statistics

To view statistics for an AP, radio, or VAP, follow these steps:

1. Select **Data** > **Wireless** > **APs/Radios/VAPs**.



2. Select the appropriate tab (**Access Points**, **Radios**, or **Virtual Access Points**) and select the appropriate interface by using its hyperlink.



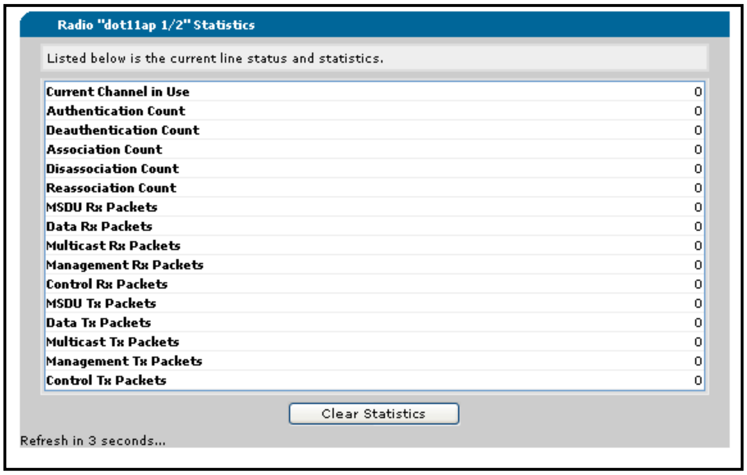
Modify a Radio

To view or modify an existing Radio, click the link in the desired row.

* - Indicates that the radio is enabled

	Radio ID	Type	Operation	Mode	MAC Address
*	dot11ap 1/1	Radio BG	AP	80211 BG	00:00:00:00:00:00(0)
	dot11ap 1/2	Radio A	AP	80211 A	00:00:00:00:00:00(1)
	dot11ap 2/1	Radio BG	AP	80211 BG	00:00:00:00:00:00(2)
	dot11ap 2/2	Radio A	AP	80211 A	00:00:00:00:00:00(3)
	dot11ap 3/1	Radio BG	AP	80211 BG	00:00:00:00:00:00(4)
	dot11ap 3/2	Radio A	AP	80211 A	00:00:00:00:00:00(5)
*	dot11ap 4/1	Radio BG	Universal Repeater	80211 BG	00:00:00:00:00:00(6)
	dot11ap 4/2	Radio A	AP	80211 A	00:00:00:00:00:00(7)

3. Scroll to the bottom of the menu for statistics of the selected interface.



Listed below is the current line status and statistics.

Current Channel in Use	0
Authentication Count	0
Deauthentication Count	0
Association Count	0
Disassociation Count	0
Reassociation Count	0
MSDU Rx Packets	0
Data Rx Packets	0
Multicast Rx Packets	0
Management Rx Packets	0
Control Rx Packets	0
MSDU Tx Packets	0
Data Tx Packets	0
Multicast Tx Packets	0
Management Tx Packets	0
Control Tx Packets	0

Refresh in 3 seconds...

4. To clear statistics, select the **Clear Statistics** button.

Appendix A. Creating MAC ACLs Using the CLI and GUI

MAC ACLs allow tighter security in wireless networks by blocking unwanted computer or device connections. The MAC ACL is a common filtering option, based on source MAC addresses, that only allows specified devices to access the network. MAC ACLs are applicable to the NetVanta 150 Wireless Access Point and any unit acting as an access controller. A MAC ACL can be created by entering the MAC address for each computer or device that you want to allow access through either the CLI or GUI. The CLI provides direct interaction with your unit through a text-based user interface, and the GUI provides direct interaction with your unit through a Web-based user interface.

> NOTE *MAC ACLs are used as packet selectors by the wireless features. By themselves, the MAC ACLs do nothing. AOS provides only standard MAC ACLs, that match based on the source of the packet.*

Creating a MAC ACL Using the GUI

The GUI is an online configuration tool that allows you to easily configure and view system settings, as well as the status of your AOS product.

> NOTE *If restrictions in your network prevent you from accessing the GUI, proceed to Creating a MAC ACL Using the CLI on page 44.*

To create a MAC ACL using the GUI, follow these steps:

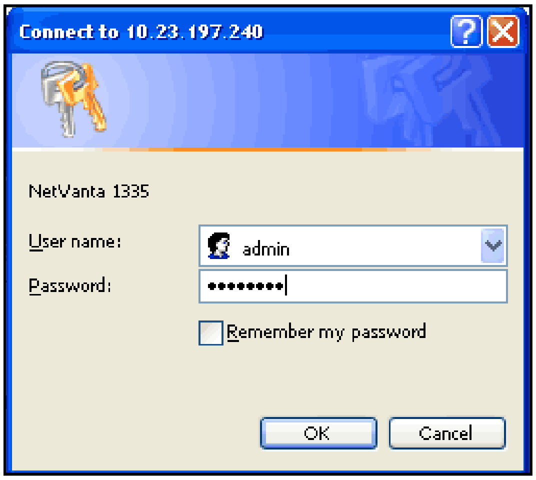
1. Open a new page in your Web browser.

2. Type your unit's IP address in the browser's address field in the following form:

   http://*<ip address>*

   > NOTE *The IP address may also be entered in* ***https://*** *if your unit has* ***ip http secure-server*** *enabled.*

3. At the prompt, enter your user name and password and select **OK**.



Connect to 10.23.197.240

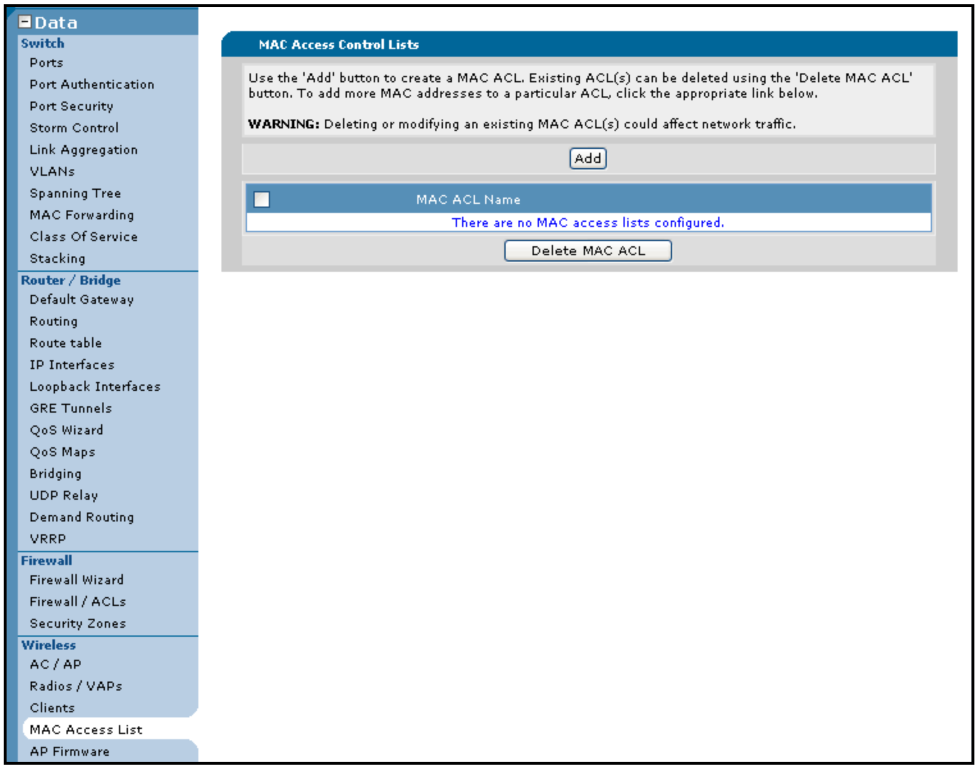
NetVanta 1335

User name: admin

Password: ••••••••

□ Remember my password

4. Navigate to **Data** > **Wireless** > **MAC Access List** on the left of the GUI menu as seen below:



MAC Access Control Lists

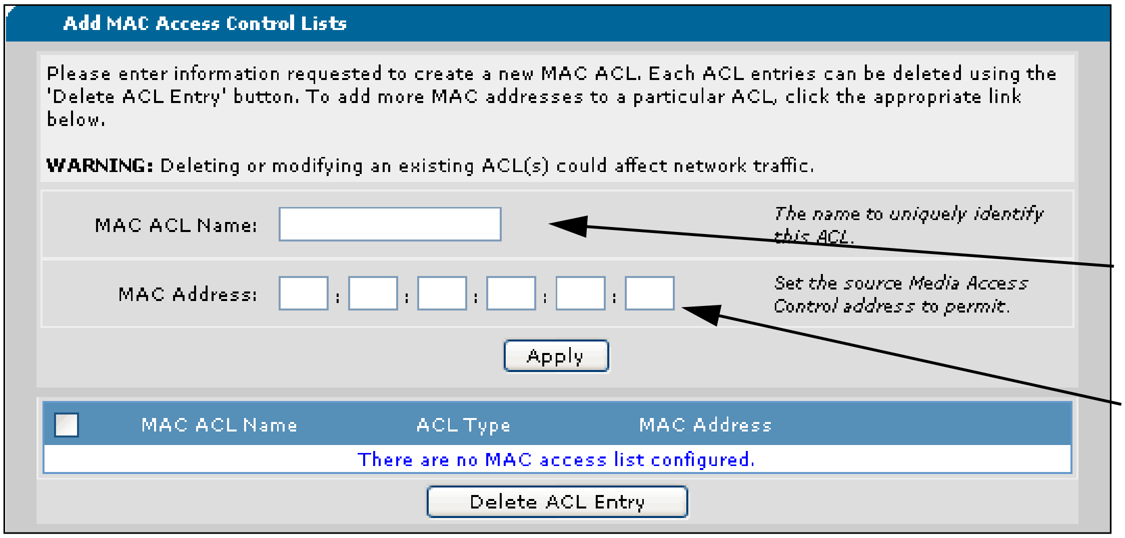
Use the 'Add' button to create a MAC ACL. Existing ACL(s) can be deleted using the 'Delete MAC ACL' button. To add more MAC addresses to a particular ACL, click the appropriate link below.

WARNING: Deleting or modifying an existing MAC ACL(s) could affect network traffic.

□ MAC ACL Name
There are no MAC access lists configured.

5. Select **Add** to add a MAC ACL.

6. Enter the **MAC ACL Name** and the source **MAC Address** in the appropriate fields.



Add MAC Access Control Lists

Please enter information requested to create a new MAC ACL. Each ACL entries can be deleted using the 'Delete ACL Entry' button. To add more MAC addresses to a particular ACL, click the appropriate link below.

WARNING: Deleting or modifying an existing ACL(s) could affect network traffic.

MAC ACL Name: ______ *The name to uniquely identify this ACL.*

MAC Address: __ : __ : __ : __ : __ : __ *Set the source Media Access Control address to permit.*

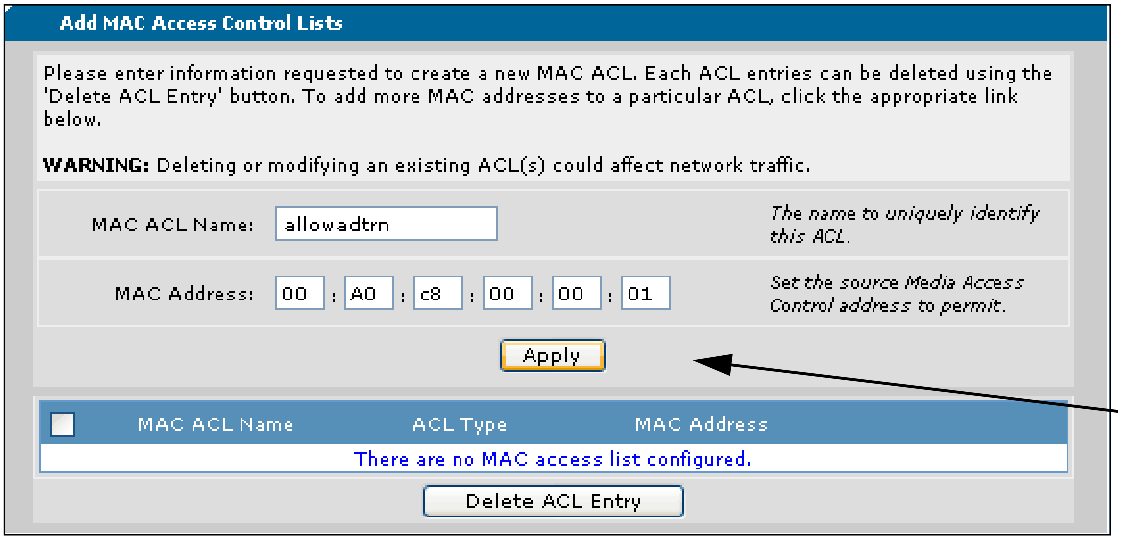
□	MAC ACL Name	ACL Type	MAC Address
There are no MAC access list configured.			

Enter the **MAC ACL Name**.

Enter the **MAC Address**.

All MAC ACLs are case sensitive. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, ***00:A0:C8:00:00:01****).*

7. Select **Apply** to create the MAC ACL.



Add MAC Access Control Lists

Please enter information requested to create a new MAC ACL. Each ACL entries can be deleted using the 'Delete ACL Entry' button. To add more MAC addresses to a particular ACL, click the appropriate link below.

WARNING: Deleting or modifying an existing ACL(s) could affect network traffic.

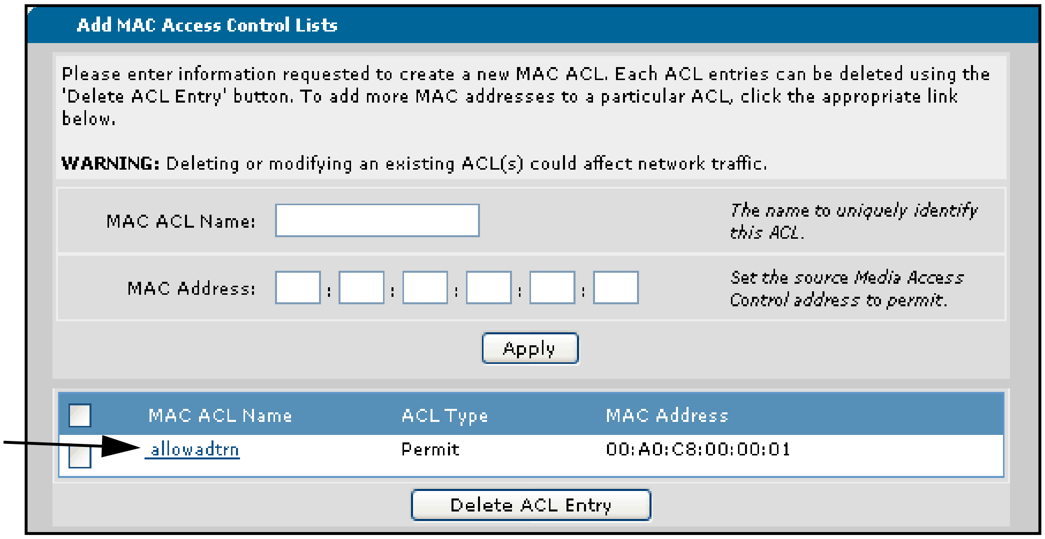
MAC ACL Name: allowadtrn *The name to uniquely identify this ACL.*

MAC Address: 00 : A0 : c8 : 00 : 00 : 01 *Set the source Media Access Control address to permit.*

□	MAC ACL Name	ACL Type	MAC Address
There are no MAC access list configured.			

Select **Apply**.

8. The new MAC ACL will appear on the bottom portion of the menu.



Add MAC Access Control Lists

Please enter information requested to create a new MAC ACL. Each ACL entries can be deleted using the 'Delete ACL Entry' button. To add more MAC addresses to a particular ACL, click the appropriate link below.

WARNING: Deleting or modifying an existing ACL(s) could affect network traffic.

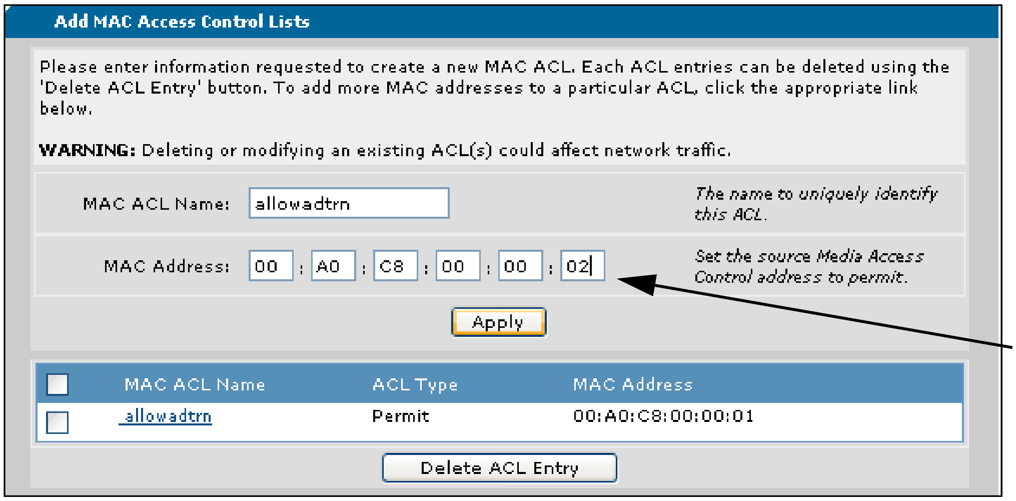
MAC ACL Name: ____ *The name to uniquely identify this ACL.*

MAC Address: ___ : ___ : ___ : ___ : ___ : ___ *Set the source Media Access Control address to permit.*

□	MAC ACL Name	ACL Type	MAC Address
□	allowadtrn	Permit	00:A0:C8:00:00:01

New **MAC ACL.**

9. To add additional source MAC addresses to the MAC ACL, select the MAC ACL name from the bottom of the menu. Enter additional MAC addresses you want to give access to your network and select **Apply**. You can add as many new addresses to the MAC ACL as you need.



Add MAC Access Control Lists

Please enter information requested to create a new MAC ACL. Each ACL entries can be deleted using the 'Delete ACL Entry' button. To add more MAC addresses to a particular ACL, click the appropriate link below.

WARNING: Deleting or modifying an existing ACL(s) could affect network traffic.

MAC ACL Name: allowadtrn *The name to uniquely identify this ACL.*

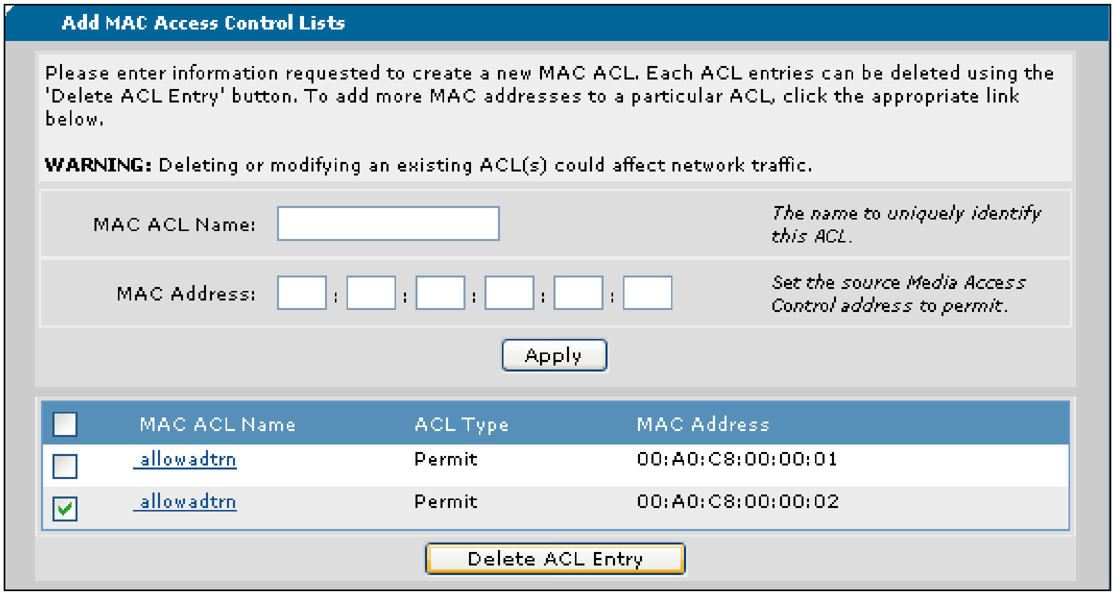
MAC Address: 00 : A0 : C8 : 00 : 00 : 02 *Set the source Media Access Control address to permit.*

□	MAC ACL Name	ACL Type	MAC Address
□	allowadtrn	Permit	00:A0:C8:00:00:01

Second MAC address for **allowadtrn** MAC ACL.

10. Configuration of the MAC ACL is complete. You can make additional changes to each MAC ACL by selecting its hyperlink.

11. To delete an address from a MAC ACL, check the box next to the MAC address you want to delete and select the **Delete ACL Entry** button at the bottom of the menu.



Add MAC Access Control Lists

Please enter information requested to create a new MAC ACL. Each ACL entries can be deleted using the 'Delete ACL Entry' button. To add more MAC addresses to a particular ACL, click the appropriate link below.

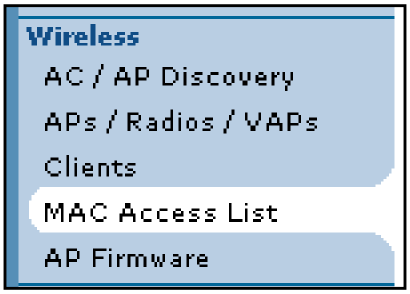
WARNING: Deleting or modifying an existing ACL(s) could affect network traffic.

MAC ACL Name:		*The name to uniquely identify this ACL.*
MAC Address:	: : : : :	*Set the source Media Access Control address to permit.*

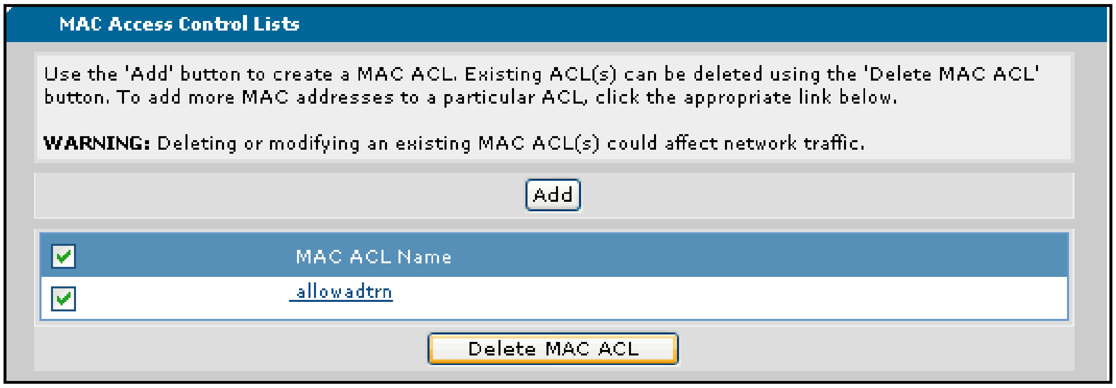
□	MAC ACL Name	ACL Type	MAC Address
□	allowadtrn	Permit	00:A0:C8:00:00:01
☑	allowadtrn	Permit	00:A0:C8:00:00:02

NOTE *Deleting MAC ACL entries will only delete the selected MAC address entries in the ACL, not the MAC ACL itself.*

12. To delete an entire MAC ACL, return to the main MAC ACL menu by selecting **MAC Access List** from the menu on the left.



13. Check the box next to the MAC ACL you want to delete, and select **Delete MAC ACL**.



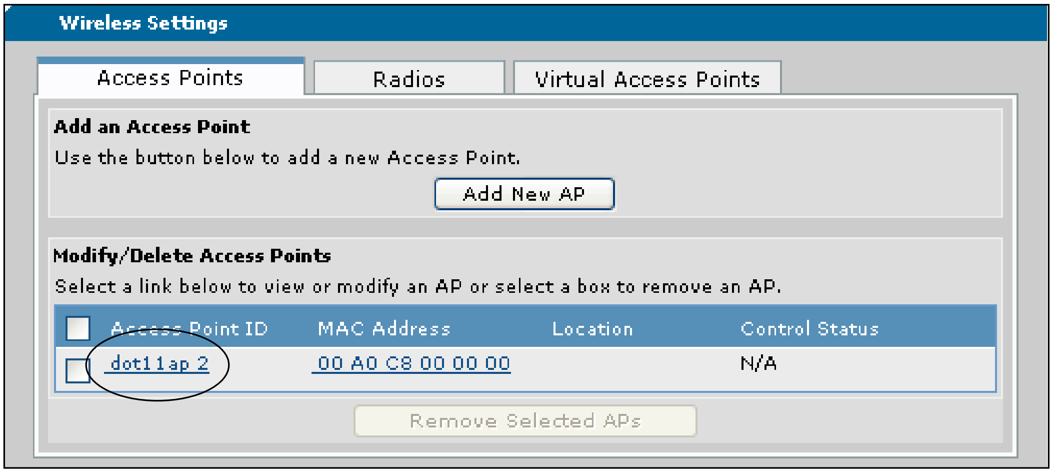
MAC Access Control Lists

Use the 'Add' button to create a MAC ACL. Existing ACL(s) can be deleted using the 'Delete MAC ACL' button. To add more MAC addresses to a particular ACL, click the appropriate link below.

WARNING: Deleting or modifying an existing MAC ACL(s) could affect network traffic.

☑	MAC ACL Name
☑	allowadtrn

14. Once the MAC ACL is configured, it must be applied to the radio. To apply the ACL to the radio, navigate to **Wireless** > **APs/Radios/VAPs** and select the access point (AP) ID from the list.



Wireless Settings

Add an Access Point

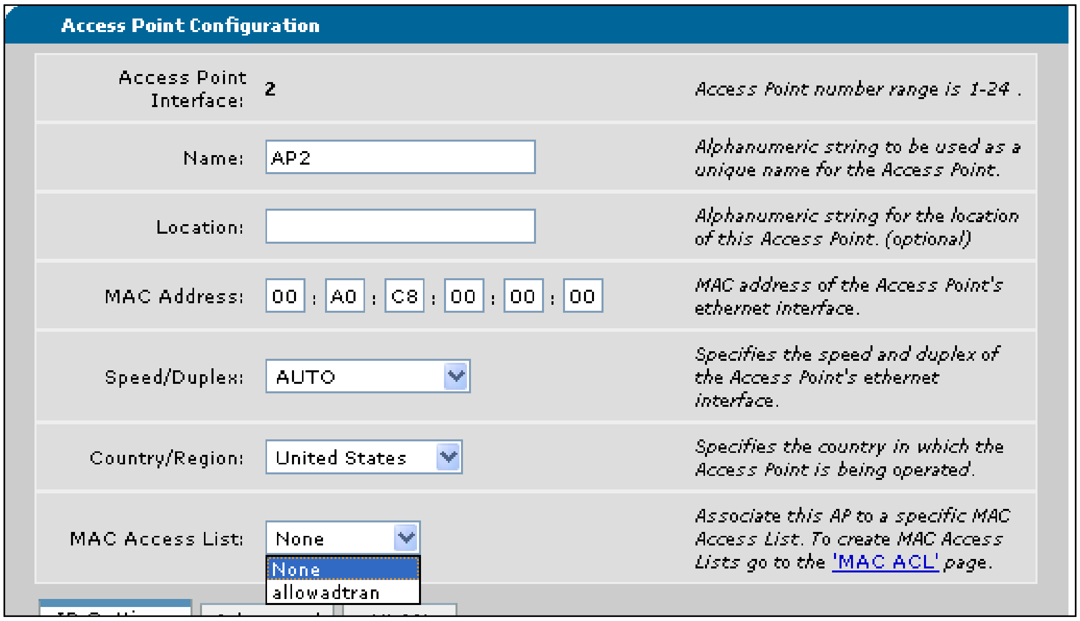
Use the button below to add a new Access Point.

Modify/Delete Access Points

Select a link below to view or modify an AP or select a box to remove an AP.

□	Access Point ID	MAC Address	Location	Control Status
□	dot11ap 2	00 A0 C8 00 00 00		N/A

15. After selecting the appropriate AP ID, select the MAC ACL you want to apply to the radio from the drop-down menu.



Access Point Configuration

Access Point Interface:	2	*Access Point number range is 1-24 .*
Name:	AP2	*Alphanumeric string to be used as a unique name for the Access Point.*
Location:		*Alphanumeric string for the location of this Access Point. (optional)*
MAC Address:	00 : A0 : C8 : 00 : 00 : 00	*MAC address of the Access Point's ethernet interface.*
Speed/Duplex:	AUTO	*Specifies the speed and duplex of the Access Point's ethernet interface.*
Country/Region:	United States	*Specifies the country in which the Access Point is being operated.*
MAC Access List:	None None allowadtran	*Associate this AP to a specific MAC Access List. To create MAC Access Lists go to the 'MAC ACL' page.*

16. After selecting the MAC ACL, apply it to the radio using the **Apply** button at the bottom of the menu. The ACL is now applied to the radio.

17. You can save your configuration (recommended) and exit the GUI using the **Save** and **Logout** links (at the upper right corner of your current menu).

Creating a MAC ACL Using the CLI

As a text-based user interface, the AOS CLI prompts you to input commands line by line when you interface with your AOS product. To create a MAC ACL through the CLI, follow these steps:

1. Boot up the unit.

2. Telnet to the unit using the format **telnet** <*ip address*>, for example: **telnet 208.61.209.1**

3. Enter your user name and password at the prompt.

> NOTE *The AOS default user name is **admin** and the default password is **password**. If your product no longer has the default user name and password, contact your system administrator for the appropriate user name and password.*

4. Enable your unit by entering **enable** at the > prompt as follows:

   >enable

5. Enter your Enable mode password at the prompt.

6. Enter the Global Configuration mode by entering the following command at the **#** prompt:

   ```
   #configure terminal
   ```

7. From the Global Configuration mode prompt, enter the **mac access-list standard** command followed by the MAC ACL name. In the following example, a MAC ACL name **Allowadtrn** will be created.

   ```
   (config)#mac access-list standard Allowadtrn
   (config-std-mac-acl)#
   ```

8. You have now entered the Standard MAC Access List Configuration mode. Here you can enter the MAC addresses to be included in the MAC ACL that will allow other devices to connect to your network. To give access to a specific MAC address, enter the **permit** command followed by the MAC address. Enter addresses in the following format: **xx:xx:xx:xx:xx:xx**. For example:

   ```
   (config-std-mac-acl)# permit 00:A0:C8:00:00:01
   (config-std-mac-acl)#
   ```

   Enter each address to add to the specified MAC ACL. Address entries can be removed from the list by using the **no** parameter in the following manner:

   ```
   (config-std-mac-acl)#no permit 00:A0:C8:00:00:01
   ```

   To exit the Standard MAC Access List Configuration mode, enter the **exit** keyword at the prompt. For example:

   ```
   (config-std-mac-acl)#exit
   (config)#
   ```

   From the Global Configuration mode, entire MAC ACLs can be deleted by using the **no** parameter of the **mac access-list standard** command followed by the MAC ACL name. For example:

   ```
   (config)#no mac access-list standard Allowadtrn
   ```

9. The MAC ACL has been created, and you should save the configuration. Multiple MAC ACLs can be created by using the same process, either through the GUI or CLI.

10. After creating and saving the MAC ACL, it must be applied to the radio. To apply the ACL, use the **association access-list** <*name*> command from the radio interface configuration mode (reached by using the **interface dot11ap** command). For example:

    ```
    (config)#interface dot11ap 1 ap-type nv150
    (config)#association access-list Allowadtrn
    ```

11. Save your configuration using the **do write memory** command from the Global Configuration mode prompt as follows:

    ```
    (config)#do write memory
    ```

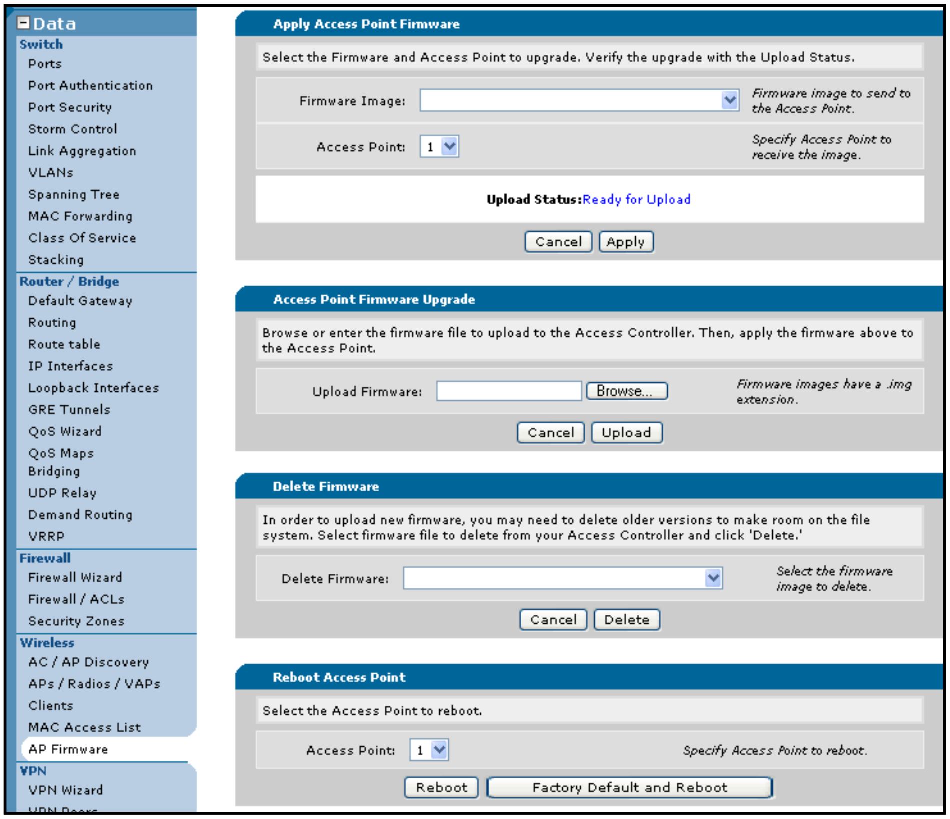
Troubleshooting Note

If unwanted clients or devices have connected to the wireless AP radio before the MAC ACL has been applied, the AP radio must be rebooted for the applied MAC ACL to filter out the unwanted client. To reboot the AP, follow the steps outlined in the following sections.

Rebooting the AP Using the GUI

To reboot the AP radio using the GUI, follow these steps:

1. Navigate to **Data** > **Wireless** > **AP Firmware** in the menu on the left.



Apply Access Point Firmware

Select the Firmware and Access Point to upgrade. Verify the upgrade with the Upload Status.

Firmware Image: *Firmware image to send to the Access Point.*

Access Point: 1 *Specify Access Point to receive the image.*

Upload Status: Ready for Upload

Access Point Firmware Upgrade

Browse or enter the firmware file to upload to the Access Controller. Then, apply the firmware above to the Access Point.

Upload Firmware: *Firmware images have a .img extension.*

Delete Firmware

In order to upload new firmware, you may need to delete older versions to make room on the file system. Select firmware file to delete from your Access Controller and click 'Delete.'

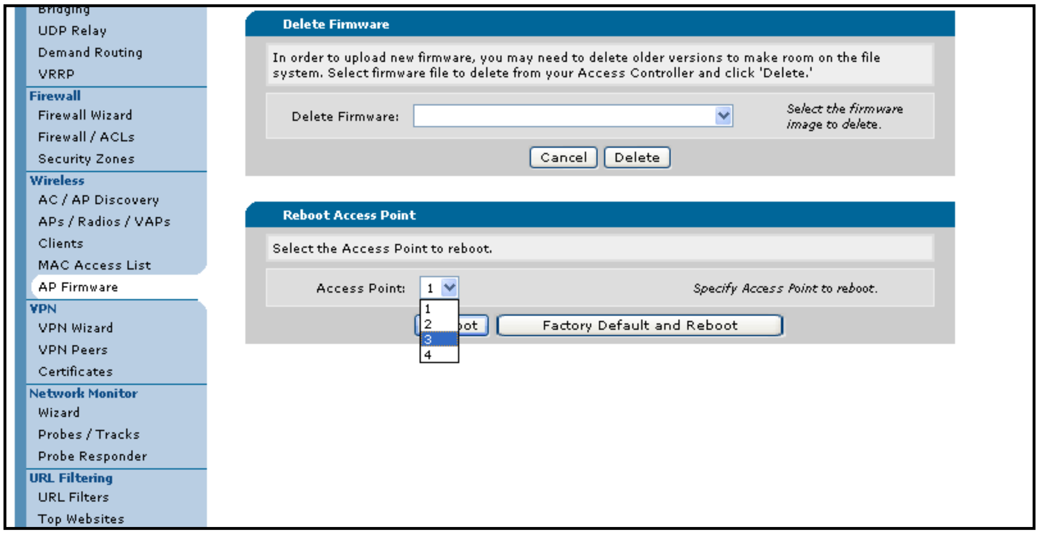
Delete Firmware: *Select the firmware image to delete.*

Reboot Access Point

Select the Access Point to reboot.

Access Point: 1 *Specify Access Point to reboot.*

2. Select the **Access Point** number to reboot from the drop-down menu.



Delete Firmware

In order to upload new firmware, you may need to delete older versions to make room on the file system. Select firmware file to delete from your Access Controller and click 'Delete.'

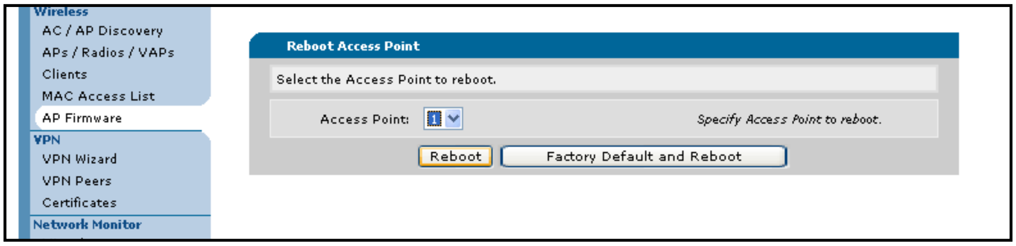
Delete Firmware: *Select the firmware image to delete.*

Reboot Access Point

Select the Access Point to reboot.

Access Point: 1 *Specify Access Point to reboot.*

3. Select the **Reboot** button. The unit will take approximately 60 seconds to reboot, so traffic will be disrupted during this period.



Reboot Access Point

Select the Access Point to reboot.

Access Point: 1 *Specify Access Point to reboot.*

Rebooting the AP Using the CLI

To reboot the AP using the CLI, use the following steps:

1. To reboot the unit while saving the current configuration, enter the following command from the Enable prompt:

   #reload dot11 interface dot11ap <*number*>

   The <*number*> parameter is used to specify the AP to reboot.