# Wireless

This chapter describes how to configure the wireless radio properties. It includes the following topics:



## Radio

The radio is the physical part of the WAP that creates a wireless network. The radio settings on the WAP control the behavior of the radio and determine what kind of wireless signals the WAP emits.

To configure the wireless radio settings:

**Step 1** Select **Wireless > Radio**.

**Step 2** Radio Interface:

- **Radio 1 (5 GHz)** — Support 5G Radio with a 3x3 MIMO mode.
- **Radio 2 (2.4 GHz)** — Support 2.4G Radio with a 3x3 MIMO mode.

**Step 3** Select the radio interface to which the configuration parameters will be applied.

**Step 4** In the **Basic Settings** area, configure these parameters for the selected radio interface:

**Note** Local regulations may prohibit the use of certain radio modes. Not all modes are available in all countries.

- **Radio** — Check **Enable** to enable the radio interface.

  **Note** If you enable the 5 GHz radio with 80 MHz bandwidth and if the radio carries a high amount of traffic, then the WAP device will need more power than what the IEEE 802.3af PoE standard provides (12.95 W). It is highly recommended that when 80-MHz channel is in use, the WAP device should be powered by an 802.3at Power Source Equipment (PSE). If the required power by the WAP device exceeds the maximum power delivered by the PSE, then the WAP device may reboot.

- **Wireless Network Mode** — The IEEE 802.11 standard and frequency the radio uses. The default value of Mode is 802.11b/g/n for Radio 2 and 802.11a/n/ac for Radio 1. For each radio, select one of the available modes.

**Radio 2 (2.4 GHz)** supports the following radio modes:

- **802.11b/g** — 802.11b and 802.11g clients can connect to the WAP device.
- **802.11b/g/n (default)** — 802.11b, 802.11g, and 802.11n clients operating in the 2.4-GHz frequency can connect to the WAP device.
- **2.4 GHz 802.11n** — 802.11n clients operating in the 2.4-GHz frequency can connect to the WAP device.

**Radio 1 (5 GHz)** supports the following radio modes:

- **802.11a** — 802.11a clients can connect to the WAP device.
- **802.11a/n/ac (default)**— 802.11a clients, 802.11n, and 802.11ac clients operating in the 5-GHz frequency can connect to the WAP device.
- **802.11n/ac** — 802.11n clients and 802.11ac clients operating in the 5-GHz frequency can connect to the WAP device

- **Wireless Band Selection (802.11n and 802.11ac modes only)** — The 802.11n specification allows a coexisting 20/40 MHz band in addition to the legacy 20 MHz band available with other modes. The 20/40 MHz band enables higher data rates but leaves fewer bands available for use by other 2.4 GHz and 5 GHz devices.

  The 802.11ac specification allows an 80 MHz-wide band in addition to the 20 MHz and 40 MHz band.

  Set the field to 20 MHz to restrict the use of the wireless band selection to a 20 MHz band. For the 802.11ac mode, set the field to 40 MHz to prevent the radio from using the 80 MHz wireless band selection.

- **Primary Channel (802.11n modes with 20/40 MHz bandwidth only)** — 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.

  Choose one of these options:

  - **Upper** — Sets the primary channel as the upper 20-MHz channel in the 40-MHz band.
  - **Lower** — Sets the primary channel as the lower 20-MHz channel in the 40-MHz band. Lower is the default selection.

- **Channel** — The portion of the radio spectrum that the radio uses for transmitting and receiving. The default value is **Auto**.

  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 WAP device scans available channels and selects a channel where the least amount of traffic is detected.

  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), the International Telecommunication Union (ITU-R) or the European Telecommunications Standards Institute (ETSI).

- **Scheduler** — For the radio interface, select the profile from the list. The default value is **None**.

  **Note** To create a profile, navigate to **Wireless** > **Scheduler**.

**Step 5** In the **Advanced Settings** area, configure these parameters:

- **DFS Support**—This field is available only if the selected radio mode operates in the 5GHz frequency. The default value is set to **On**.

  For radios in the 5 GHz band, when DFS support is on and the regulatory domain requires radar detection on the channel, the Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) features of 802.11h are activated.

  DFS is a mechanism that requires wireless devices to share spectrum and avoid co-channel operation with radar systems in the 5 GHz band. DFS requirements vary based on the regulatory domain, which is determined by the country code setting of the AP.

  When using the 802.11h Wireless Mode, there are a number of key points about the IEEE 802.11h standard:

  - 802.11h only works for the 5 GHz band. It is not required for the 2.4 GHz band.
  - If you are operating in an 802.11h enabled domain, the AP attempts to use the channel you assign. If the channel has been blocked by a previous radar detection, or if the AP detects a radar on the channel, then the AP automatically selects a different channel.
  - When 802.11h is enabled, the AP will not be operational in the 5 GHz band for at least 60 seconds due to radar scanning.
  - Setting up WDS links may be difficult when 802.11h is operational. This is because the operating channels of the two APs on the WDS link may keep changing depending on channel usage and radar interference. WDS will only work if both the APs operate on the same channel. For more information on WDS, see WDS Bridge.

- **Short Guard Interval Supported** — This field is available only if the selected radio mode includes 802.11n. 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 percent improvement in data throughput. The client with which the WAP device is communicating must also support the short guard interval.

  Choose one of these options:

  - **Yes** — The WAP device transmits data using a 400-nanosecond guard interval when communicating with clients that also support the short guard interval. This is the default selection.
  - **No** — The WAP device transmits data using an 800-nanosecond guard interval.

- **Protection** — The protection feature contains rules to guarantee that 802.11 transmissions do not cause interference with legacy stations or applications. By default, protection is enabled **(Auto)**. With protection enabled, protection is invoked if the legacy devices are within the range of the WAP device.

  You can disable the protection **(Off)**; however, the legacy clients or the WAP devices within the range can be affected by 802.11n transmissions. Protection is also available when the mode is 802.11b/g. When protection is enabled in this mode, it protects 802.11b clients and the WAP devices from 802.11g transmissions.

  **Note** This setting does not affect the ability of the client to associate with the WAP device.

- **Beacon Interval** — The interval between the transmission of beacon frames. The WAP device transmits these frames at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second). Enter an integer from 20 to 2000 milliseconds. The default is 100 milliseconds.

- **DTIM Period** — The Delivery Traffic Information Map (DTIM) period. Enter an integer from 1 to 255 beacons. The default is 2 beacons.

The 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 WAP device awaiting pickup.

The DTIM period indicates how often the clients served by this WAP device should check for buffered data awaiting pickup.

The measurement is in beacons. For example, if you set it to 1, the clients check for buffered data on the WAP device at every beacon. If you set it to 10, the clients check on every 10th beacon.

- **Fragmentation Threshold** — The frame size threshold in bytes. The valid integer must be even and in the range of 256 to 2346. The default is 2346.

  The fragmentation threshold is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold set, the fragmentation is activated and the packet is sent as multiple 802.11 frames.

  If the packet being transmitted is equal to or less than the threshold, the fragmentation is not used. Setting the threshold to the largest value (2,346 bytes, which is the default) effectively disables the fragmentation.

  By default, the fragmentation is off. We recommend not using fragmentation unless you suspect the radio interference. The additional headers applied to each fragment increase the overhead on the network and can greatly reduce the throughput.

- **RTS Threshold** — The Request to Send (RTS) Threshold value. The valid integer range must be from 0 to 65535. The default is 65535 octets.

  The RTS threshold indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed.

  Changing the RTS threshold can help control the traffic flow through the WAP device. If you specify a low threshold value, the RTS packets are sent more frequently, which consumes more bandwidth and reduces the throughput of the packet. However, sending more RTS packets can help the network recover from interference or collisions that might occur on a busy network, or on a network experiencing electromagnetic interference.

- **Max Associated Clients** — The maximum number of stations allowed to access the WAP device at any one time. You can enter an integer between 0 and 200. The default is 200 stations.

- **Transmit Power** — A percentage value for the transmit power level for the WAP device.

  The default value of Full - 100 % can be more cost-efficient than a lower percentage because it gives the WAP device a maximum broadcast range and reduces the number of access points needed.

  To increase the capacity of the network, place the WAP devices closer together and reduce the value of the transmit power. This setting helps reduce overlap and interference among the access points. A lower transmit power setting can also keep your network more secure because the weaker wireless signals are less likely to propagate outside of the physical location of your network.

  Some channel ranges and country code combinations have relatively low maximum transmit power. When attempting to set the transmit power to the lower ranges (for example, Medium - 25 percent or Low -12 percent), the expected drop in power may not occur, because certain power amplifiers have minimum transmit power requirements.

- **Frame-burst Support** — Generally enabling Frame-burst support improves the radio performance in the downstream direction. The default value is set to **Off**.

- **Airtime Fairness Mode** — The airtime fairness (ATF) feature was implemented to address the issue of slower-data transfers throttling the higher-speed ones. The default value is set to **Off**.

- **Maximum Utilization Threshold**—Enter the percentage of network bandwidth utilization allowed on the radio before the WAP device stops accepting new client associations. The valid integer range is from 0 to 100 percent. The default is 0 percent. When set to 0, all new associations are allowed regardless of the utilization rate.

- **Fixed Multicast Rate** — The transmission rate in Mbps for broadcast and multicast packets. This setting can be useful in an environment where the wireless multicast video streaming occurs, provided the wireless clients are capable of handling the configured rate.

  When **Auto** is selected, the WAP device chooses the best rate for the associated clients. The range of valid values is determined by the configured radio mode. The default value is **Auto**.

- **Legacy Rate Sets** — Rates are expressed in megabits per second.

  The Supported Rate Sets indicate the rates that the WAP device supports. You can check multiple rates. The WAP device automatically chooses the most efficient rate based on the factors such as error rates and the distance of client stations from the WAP device. By default all the applicable supported rates for each radio are enabled. Radio 1 can be in the range of 6 to 54 Mbps and Radio 2 can be in the range of 1 to 54 Mbps.

  The Basic Rate Sets indicate the rates that the WAP device advertises to the network for the purposes of setting up communication with other access points and client stations on the network. It is generally more efficient to have a WAP device broadcast a subset of its supported rate sets. By default 6, 12 and 24 are selected for Radio 1 & 1, 2, 5.5 and 11 are selected for Radio 2 interfaces.

- **Broadcast/Multicast Rate Limiting** — Multicast and broadcast rate limiting can improve overall network performance by limiting the number of packets transmitted across the network.

  By default, this feature is disabled. Until you enable this feature, these fields are disabled:

  - **Rate Limit** — The rate limit for multicast and broadcast traffic. The limit should be greater than 1, but less than 50 packets per second. Any traffic that falls below this rate limit will always conform and be transmitted to the appropriate destination. The default and maximum rate limit setting is 50 packets per second.
  - **Rate Limit Burst** — An amount of traffic, measured in bytes, which is allowed to pass as a temporary burst even if it is above the defined maximum rate. The default and maximum rate limit burst setting is 75 packets per second.

- **Spectrum Analysis Mode**— The Spectrum Analysis Mode status can be one of the following:
  - **Dedicated Spectrum Analyzer**—In dedicated mode, the radio is used for spectrum analysis for more than 10% of the time and the client connections may work but are not guaranteed.
  - **Hybrid Spectrum Analyzer**—In hybrid mode, client connections are guaranteed but degradation is expected throughout.
  - **Disabled**—The default is Disabled

- **VHT Features** — The purpose of this feature is to enabled/disable Broadcom specific extensions in VHT for Broadcom-to-Broadcom links. VHT feature enables support for 256QAM VHT rates not specified by the 802.11 ac Draft. The rates are all VHT LDPC mode, MCS 9 Nss 1 20Mhz, MCS 9 Nss 2 20Mhz, MCS 6 Nss 3 80Mhz. The VHT feature is supported for 802.11 ac PHY.

**Step 6** Click **Configure TSPEC...** and configure the following parameters:

- **TSPEC Violation Interval** — In the TSPEC Violation Interval field, enter the time interval in seconds for the WAP device to report associated clients that do not adhere to mandatory admission control procedures. The reporting occurs through the system log and SNMP traps. Enter a time from 0 to 900 seconds. The default is 300 seconds.
- **TSPEC Mode** — Regulates the overall TSPEC mode on the WAP device. By default, the TSPEC mode is off. The options are:

- **On** — The WAP device handles TSPEC requests according to the TSPEC settings that you configure on the Radio page.
- **Off** — The WAP device ignores TSPEC requests from client stations.

- **TSPEC Voice ACM Mode** — Regulates mandatory admission control (ACM) for the voice access category. By default, TSPEC Voice ACM mode is off. The options are:
  - **On** — A station is required to send a TSPEC request for bandwidth to the WAP device before sending or receiving a voice traffic stream. The WAP device responds with the result of the request, which includes the allotted medium time if the TSPEC was admitted.
  - **Off** — A station can send and receive the voice priority traffic without requiring an admitted TSPEC. The WAP device ignores voice TSPEC requests from client stations.
- **TSPEC Voice ACM Limit** — The upper limit on the amount of traffic that the WAP device attempts to transmit on the wireless medium using a voice AC to gain access. The default limit is 20 percent of total traffic.
- **TSPEC Video ACM Mode** — Regulates mandatory admission control for the video access category. By default, TSPEC Video ACM mode is off. The options are:
  - **On** — A station is required to send a TSPEC request for bandwidth to the WAP device before sending or receiving a video traffic stream. The WAP device responds with the result of the request, which includes the allotted medium time if the TSPEC was admitted.
  - **Off** — A station can send and receive video priority traffic without requiring an admitted TSPEC; the WAP device ignores video TSPEC requests from client stations.
- **TSPEC Video ACM Limit** — The upper limit on the amount of traffic that the WAP device attempts to transmit on the wireless medium using a video AC to gain access. The default limit is 15 percent of total traffic.
- **TSPEC AP Inactivity Timeout** — The amount of time for a WAP device to detect a downlink traffic specification as idle before deleting it. The valid integer range is from 0 to 120 seconds and the default is 30 seconds.
- **TSPEC Station Inactivity Timeout** — The amount of time for a WAP device to detect an uplink traffic specification as idle before deleting it. The valid integer range is from 0 to 120 seconds and the default is 30 seconds.
- **TSPEC Legacy WMM Queue Map Mode** — Check Enable to enable the intermixing of legacy traffic on queues operating as ACM. By default, this mode is off.

**Step 7** Click **OK** and then click **Apply**.

# Networks

Virtual Access Points (VAPs), segment the wireless LAN into multiple broadcast domains that are wireless equivalent of the Ethernet VLANs. VAPs simulate multiple access points on one physical WAP device. Up to four VAPs are supported on this Cisco WAP device.

Each VAP can be independently enabled or disabled, with the exception of VAP0. The VAP0 is the physical radio interface and remains enabled as long as the radio is enabled. To disable the VAP0, the radio itself must be disabled.

Each VAP is identified by a user-configured Service Set Identifier (SSID). Multiple VAPs cannot have the same SSID name. SSID broadcasts can be enabled or disabled independently on each VAP. SSID broadcast is enabled by default.

**SSID Naming Conventions**

The default SSID for VAP0 is **ciscosb**. Every additional VAP created has a blank SSID name. The SSIDs for all VAPs can be configured to other values. The SSID can be any alphanumeric, case-sensitive entry from 2 to 32 characters.

The following characters are allowed:

- ASCII 0x20 through 0x7E.
- Trailing and leading spaces (ASCII 0x20) are not permitted.

**Note** This means that spaces are allowed within the SSID, but not as the first or last character including the period "**.**" (ASCII 0x2E).

**VLAN IDs**

Each VAP is associated with a VLAN, and is identified by a VLAN ID (VID). A VID can be any value from 1 to 4094, inclusive. The WAP571/E device supports 33 active VLANs (32 for WLAN plus one management VLAN).

By default, the VID assigned to the configuration utility for the WAP device is 1, which is also the default untagged VID. If the management VID is the same as the VID assigned to a VAP, then the WLAN clients associated with this specific VAP can administer the WAP device. If needed, an access control list (ACL) can be created to disable administration from WLAN clients.

# Configuring VAPs

To configure VAPs:

**Step 1** Select **Wireless** > **Networks**.

**Step 2** Click the radio interface (**Radio 1 (5 GHz)** or **Radio 2 (2.4 GHz)**) to which the VAP configuration parameters are applied.

**Step 3** If VAP0 is the only VAP configured on the system, and you want to add a VAP, click **+**. Then, check the VAP.

**Step 4** Configure the following:

- **VLAN ID** — Specify the VLAN ID of the VLAN to associate with the VAP.

  Be sure to select a VLAN ID that is properly configured on the network. Network problems can result if the VAP associates the wireless clients with an improperly configured VLAN.

  When a wireless client connects to the WAP device by using this VAP, the WAP device tags all traffic from the wireless client with the configured VLAN ID, unless you enter the port VLAN ID or use a RADIUS server to assign a wireless client to a VLAN. The range for the VLAN ID is from 1 to 4094.

  If you change the VLAN ID to a different ID than the current management VLAN ID, the WLAN clients associated with this specific VAP cannot administer the device. You can verify the configuration of the untagged and management VLAN IDs on the LAN page. See VLANs Setting Table for more information.

- **SSID Name** — Enter the name for the wireless network. The SSID is an alphanumeric string of up to 32 characters. Choose a unique SSID for each VAP.

  If you are connected as a wireless client to the same WAP device that you are administering, resetting the SSID will cause you to lose connectivity to the WAP device. You will need to reconnect to the new SSID after you save this new setting.

- **SSID Broadcast** — Enables and disables the broadcast of the SSID.

  Specify whether to allow the WAP device to broadcast the 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 shown in the list of available networks on a client station. Instead, you must manually enter the exact network name into the wireless connection utility on the client so that it can connect.

  Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it does 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 to make it easy for clients to get a connection and where no sensitive information is available.

- **WMF** — The Wireless Multicast Forwarding provides an efficient way to transfer multicast traffic on the wireless device and overcome multicast transmission issues on the WLAN using the repeated unicast or multicast the frames.

- **Security** — Choose the type of authentication required for access to the VAP. The options are:

  - **None**
  - **WPA Personal**
  - **WPA Enterprise**

If you choose a security mode other than None, additional fields appear. For more information on configuring the wireless security settings, see Configuring Security Settings.

We recommend using WPA Personal or WPA Enterprise as the authentication type as it provides stronger security protection.

- **Client Filter** — Specifies whether the stations that can access the VAP are restricted to a configured global list of MAC addresses. You can choose one of these types of Client filter:

  - **Disabled** — Does not use the Client filter.
  - **Local** — Uses the MAC authentication list that is configured on the Client Filter page.
  - **RADIUS** — Uses the MAC authentication list on an external RADIUS server.

- **Channel Isolation** — Check to enable the channel isolation.

  When disabled, the wireless clients can communicate with one another normally by sending traffic through the WAP device.

  When enabled, the WAP device blocks communication between the wireless clients on the same VAP. The WAP device still allows data traffic between its wireless clients and the wired devices on the network, across a WDS link, and with other wireless clients associated with a different VAP, but not among the wireless clients

- **Band Steer** — Check to enable the band steer when both the radios are up. It effectively utilizes the 5-GHz band by steering dual-band supported clients from the 2.4-GHz band to the 5-GHz band.

  - It is configured on a per-VAP basis and needs to be enabled on both the radios.

- It is not encouraged on the VAPs with time-sensitive voice or video traffic.
- It does not consider the n-bandwidth of the radio. Even if the 5-GHz radio happens to use 20 MHz bandwidth, it tries to steer clients to that radio.

- **Scheduler** — Select a scheduler profile from the list, VAP0 can't be associated to a scheduler profile.
- **Guest Access Instance** — Associate a CP instance to a VAP. The associated CP instance settings applies to users who attempt to authenticate on the VAP. Select the instance name for each VAP you want to associate an instance with. The default value is **None**.

**Note** A VAP can associate to one Guest Access Instance in **Access Control** > **Guest Access** page. You must configure a **Guest Access Instance Table** first.

**Step 5** Click **Apply**.

**Caution** After new settings are saved, the corresponding processes may be stopped and restarted. When this condition happens, the WAP device may lose its connectivity. It is recommend that you change the WAP device settings at this time.

**Note** To delete a VAP, check the VAP and click **Delete**. To edit a VAP, check the VAP and click **Edit**. To save your changes, click **Apply** when complete.

# Configuring Security Settings

This section describes the security settings that can be configured on the WAP device on the **Networks** page. There are three security setting options to choose from: None, WPA Personal and WPA Enterprise.

### None

If you select **None** as your security mode, no additional security settings are required on the device. This mode means that any data transferred to and from the WAP device is not encrypted. This security mode can be used during initial network configuration or for troubleshooting, but the same is not recommended for a regular use on the internal network as this mode is not secure.

### WPA Personal

The WPA Personal is a Wi-Fi Alliance IEEE 802.11i standard, which includes AES-CCMP and TKIP encryption. The WPA Personal uses a pre-shared key (PSK) 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. WPA Personal is also referred to as WPA-PSK.

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

To configure WPA Personal, configure the following:

- **WPA Versions** — Choose the types of client stations from the following:
  - **WPA-TKIP** — This network has client stations that only support the original WPA and TKIP security protocol. Note that selecting the WPA-TKIP only is not allowed as per the latest Wi-Fi Alliance requirements.

- **WPA2-AES** — All client stations on the network support WPA2 and AES-CCMP cipher/security protocol. This provides the best security per IEEE 802.11i standard. As per the latest Wi-Fi Alliance requirement, the AP has to support this mode all the time.

  If the network has a mix of clients, some of which support WPA2 and others which support only the original WPA, select both. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability in place of some security.

  WPA clients must have one of these keys to be able to associate with the WAP device:

  - A valid TKIP key
  - A valid AES-CCMP key

- **PMF (Protection Management Frame)** — Provides security for the unencrypted 802.11 management frames. When Security Mode is disabled, the PMF is set to No PMF and is not editable (Hidden or Grey). When the security Mode is set to WPA2-xxx, the PMF is Capable by default and is editable. The following three check box values can be configured for it.
  - **Not Required**
  - **Capable**
  - **Required**

  **Note** The WiFi Alliance requires the PMF to be enabled and set to Capable (Default). You may disable it when the non-compliant wireless clients experience instability or connectivity issues.

- **Key** — The shared secret key for WPA Personal security. Enter a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include uppercase and lowercase alphabetic letters, the numeric digits, and special symbols such as @ and #.
- **Show Key as Clear Text** —When enabled, the text you type is visible. When disabled, the text is not masked as you enter it.
- **Key Strength Meter** — The WAP device checks the key against complexity criteria such as how many different types of characters (uppercase and lowercase alphabetic letters, numbers, and special characters) are used and how long is the string. If the WPA-PSK complexity check feature is enabled, the key is not accepted unless it meets the minimum criteria. See Configure WAP-PSK Complexity for information on configuring the complexity check.
- **Broadcast Key Refresh Rate** — The interval at which the broadcast (group) key is refreshed for clients associated with this VAP. The default is 86400 seconds and the valid range is from 0 to 86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

### WPA Enterprise

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

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

The dynamic VLAN mode is enabled by default, which allows RADIUS authentication server to decide which VLAN is used for the stations.

These parameters configure WPA Enterprise:

- **WPA Versions** — Choose the types of client stations to be supported. The options are:
  - **WPA-TKIP** — The network has some client stations that only support original WPA and TKIP security protocol. Note that selecting only WPA-TKIP for the access point is not allowed as per the latest Wi-Fi Alliance requirement.
  - **WPA2-AES** — All client stations on the network support WPA2 version and AES-CCMP cipher/ security protocol. This provides the best security per the IEEE 802.11i standard. As per the latest Wi-Fi Alliance requirement, the AP has to support this mode all the time.
- **Enable Pre-authentication** — If you choose only WPA2 or both WPA and WPA2 as the WPA version, you can enable pre-authentication for the WPA2 clients.

  Check this option if you want the WPA2 wireless clients to send the pre-authentication packets. The pre-authentication information is relayed from the WAP device that the client is currently using to the target WAP device. Enabling this feature can help speed up the authentication for roaming clients who connect to multiple APs.

  This option does not apply if you selected WPA for WPA versions because the original WPA does not support this feature.

  Client stations configured to use WPA with RADIUS must have one of these addresses and keys:
  - A valid TKIP RADIUS IP address and RADIUS key
  - A valid CCMP (AES) IP address and RADIUS key
- **PMF (Protection Management Frame)**— Provides security for the unencrypted 802.11 management frames. When Security Mode is disabled or WEP, the PMF is set to **No PMF** and is not editable (Hidden or Grey).When the security Mode is set to **WPA2-xxx**, the PMF is **Capable** by default and is editable. The following three check box values can be configured for it.
  - **Not Required**
  - **Capable**
  - **Required**

**Note** WiFi Alliance requires PMF to be enabled with default setting of **Capable**. You may disable it when non-compliant wireless clients experience instability or connectivity issues.

- **Use Global RADIUS Server Settings** — By default, each VAP uses the global RADIUS settings that you define for the WAP device. However, you can configure each VAP to use a different set of RADIUS servers.

  Check this option to use the global RADIUS server settings, or uncheck this option to use a separate RADIUS server for the VAP and enter the RADIUS server IP address and key in the appropriate fields.

- **Server IP Address Type** — The IP version that the RADIUS server uses. You can toggle between the address types to configure the IPv4 and IPv6 global RADIUS address settings, but the WAP device contacts only the RADIUS server or servers for the address type that you select in this field.
- **Server IP Address-1 or Server IPv6 Address-1** — The address for the primary RADIUS server for this VAP.
- **Server IP Address-2 or Server IPv6 Address-2** — Up to three IPv4 and/or IPv6 addresses to use as the backup RADIUS servers for this VAP. If authentication fails with the primary server, each configured backup server is tried in sequence.
- **Key-1** — 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 WAP device and on your RADIUS server. The text that you enter is shown as asterisks to prevent others from seeing the RADIUS key as you type.
- **Key-2** — The RADIUS key associated with the configured backup RADIUS servers. The server at Server IP (IPv6) Address 2 uses Key 2.
- **Enable RADIUS Accounting** — Tracks and measures 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** — Enables the administrative selection of the active RADIUS server, rather than having the WAP device attempt to contact each configured server in sequence and choose the first server that is up.
- **Broadcast Key Refresh Rate** — The interval at which the broadcast (group) key is refreshed for clients associated with this VAP. The default is 86400 seconds. The valid range is from 0 to 86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.
- **Session Key Refresh Rate** — The interval at which the WAP device refreshes session (unicast) keys for each client associated with the VAP. The valid range is from 30 to 86400 seconds. A value of 0 indicates that the session key is not refreshed. The default value is **0**.

# Client Filter

Client filter can be used to permit or deny listed client stations to authenticate with the WAP device. MAC authentication is configured on the Networks, on page 6 page. Based on the VAP configuration, the WAP device may refer to a Client filter list stored on an external RADIUS server, or may refer a Client filter list stored locally on the WAP device.

## Configuring a Client Filter List Locally on the WAP device

The WAP device supports one local Client filter list only. The filter can be configured to grant access only to the MAC addresses on the list, or to deny access only to addresses on the list.

Up to 512 Client addresses can be added to the filter list.

To configure the Client filter follow these steps:

**Step 1** Select **Wireless** > **Client Filter**.

**Step 2** Choose how the WAP device uses the filter list:

- **Permit (Permit Only Clients in the List)** —Any station that is not in the Stations List is denied access to the network through the WAP device.
- **Deny (Deny All Clients in the List)**—Only the stations that appear in the list are denied access to the network through the WAP device. All other stations are permitted access.

**Note** The filter setting also applies to the Client filter list stored on the RADIUS server, if one exists.

**Step 3** Continue entering MAC addresses until the list is complete. Click the arrow next to **Associated Clients** to display the list. Choose one of the MAC address and then click **Add**. One rule will be added to the **MAC Address Table**. The **Associated Clients** list includes the following:

- **MAC Address**—The MAC address of the associated wireless client.
- **Host Name**—The hostname of the associated wireless client.
- **IP Address**—The IP address of the associated wireless client.
- **Network (SSID)**— The Service Set Identifier (SSID) for the WAP device. The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the Network Name.

**Step 4** Click **Apply**.

## Configuring MAC Authentication on the Radius Server

If one or more VAPs are configured to use a Client filter you must configure the station list on the RADIUS server. The format for the list is described in this 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 look up a client MAC entry. | NOPASSWORD |

# Scheduler

The Radio and VAP scheduler allows you to configure a rule with a specific time interval for the VAPs or radios to be operational.

You can use this feature is to schedule the radio to operate or allow access to the VAPs only during the office working hours in order to achieve security and reduce power consumption.

The WAP device supports up to 16 profiles. Only valid rules are added to the profile. Up to 16 rules are grouped together to form a scheduling profile. Periodic time entries belonging to the same profile cannot overlap.

# Scheduler Profile Configuration

You can create up to 16 scheduler profile names. By default, no profiles are created.

To view the scheduler status and add a scheduler profile:

**Step 1** Select **Wireless > Scheduler**.

**Step 2** Check **Enable** to ensure that the **Administrative Mode** is enabled. By default it is disabled.

The **Scheduler Operational Status** area indicates the current operation status of the Scheduler:

- **Status** — The operational status (Enabled or Disabled) of the Scheduler. The default is Disabled.
- **Reason** — The reason for the scheduler operational status. Possible values are:
  - **Is Active** — The scheduler is administratively enabled.
  - **Administrative Mode is disabled** — The scheduler administrative mode is disabled.
  - **System Time is outdated** — The system time is outdated.
  - **Managed Mode** — The scheduler is in managed mode.

**Step 3** To add a profile, enter a profile name in the **Create a Profile Name** text box and click **Add**. The profile name can be up to 32 alphanumeric characters.

# Profile Rule Configuration

You can configure up to 16 rules for a profile. Each rule specifies the start time, end time, and day (or days) of the week that 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, hour, and minute) for the start and end time. Rules cannot conflict; for example, you can configure one rule to start on each weekday and another to start on each weekend day, but you cannot configure one rule to begin daily and another rule to begin on weekends.

To configure a profile rule:

**Step 1** Choose the profile from the **Select a Profile Name** list.

**Step 2** Click **+**.

The new rule is displayed in the **Profile Rule Table**.

**Step 3** Check the check box before the **Profile Name** and click **Edit**.

**Step 4** From the **Day of the Week** menu, choose the recurring schedule for the rule. You can configure the rule to occur daily, each weekday, each weekend day (Saturday and Sunday), or any single day of the week.

**Step 5** Set the start and end times:

- **Start Time (24hh:mm)**— Set the time when the radio or VAP is enabled. The time is in hh:mm 24-hour format. The range is <00-23>:<00-59>. The default is 00:00.

- **End Time (24hh:mm)** — Set the time when the radio or VAP is disabled. The time is in hh:mm 24-hour format. The range is <00-23>:<00-59>. The default is 00:00.

**Step 6** Click **Apply**.

**Note** A scheduler profile must be associated with a radio interface or a VAP interface to be in effect.

To delete a rule, select the profile from the **Profile Name** column and click **Delete**.

# QoS

The Quality of Service (QoS) settings allow for configuration of the transmission queues for optimized throughput and enhanced performance when handling differentiated wireless traffic. This traffic can be VoIP, other types of audio, video, streaming media, and traditional IP data.

To configure QoS on the WAP device, set the parameters on the transmission queues for different types of wireless traffic and specify the minimum and maximum wait times for transmission.

The WAP Enhanced Distributed Channel Access (EDCA) parameters affect the traffic flowing from the WAP device to the client station. The station EDCA parameters affect the traffic flowing from the client station to the WAP device.

In normal use, the default values for the WAP device and the station EDCA should not be changed. Changing these values affects the QoS provided.

To configure the WAP device and EDCA parameters:

**Step 1** Select **Wireless > QoS**.

**Step 2** Choose the radio interface (**Radio 1 (5 GHz) or Radio 2 (2.4 GHz)**).

**Step 3** Choose one of these options from the **EDCA (Enhanced Distributed Channel Access) Template**:

- **WFA Defaults** — Populates the WAP device and the Station EDCA parameters with Wi-Fi Alliance default values, which are best for general, mixed traffic.
- **Optimized For Voice** — Populates the WAP device and the Station EDCA parameters with values that are best for voice traffic.
- **Custom** — Enables you to choose custom EDCA parameters.

These four queues are defined for different types of data transmitted from WAP- to-station. If you choose a Custom template, the parameters that define the queues are configurable; otherwise, they are set to predefined values appropriate to your selection. The four queues are:

- **Data 0 (Voice)** — High priority queue, with minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
- **Data 1 (Video)** — High priority queue, with minimum delay. Time-sensitive video data is automatically sent to this queue.
- **Data 2 (Best Effort)** — Medium priority queue, with medium throughput and delay. Most traditional IP data is sent to this queue.

- **Data 3 (Background)** — Lowest priority queue, with high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

**Step 4** Check **Enable** to enable **Wi-Fi MultiMedia (WMM)** extensions.

**Wi-Fi MultiMedia (WMM)**— This field is enabled by default. With WMM enabled, QoS prioritization and coordination of wireless medium access is on. With WMM enabled, QoS settings on the WAP device control downstream traffic flowing from the WAP device 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 WAP device. With WMM disabled, you can still set some parameters on the downstream traffic flowing from the WAP device to the client station (AP EDCA parameters).

**Step 5** Configure the following **WAP EDCA** and **Station EDCA** parameters:

- **Arbitration Inter-Frame Space** — Wait time for the data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 255.
- **Minimum Contention Window** — An input to the algorithm that determines the initial random backoff wait time (window) for a retry of a transmission failure.

  This value is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated is a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling continues until the size of the random backoff value reaches the number defined in the Maximum Contention Window.

  Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. This value must be lower than the value for the Maximum Contention Window.
- **Maximum Contention Window** — The upper limit in milliseconds for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.

  After the Maximum Contention Window size is reached, retries continue until a maximum number of retries allowed is reached.

  Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. This value must be higher than the value for the Minimum Contention Window.
- **Maximum Burst** — A WAP EDCA parameter that applies only to traffic flowing from the WAP to the client station.

  This value specifies (in milliseconds) the maximum burst length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance. Valid values are 0.0 through 999.
- **TXOP Limit (Station only)** — The TXOP Limit is a station EDCA parameter that only applies to traffic flowing from the client station to the WAP device. The Transmission Opportunity (TXOP) is an interval of time, in milliseconds, when a WME client station has the right to initiate transmissions onto the wireless medium (WM) towards the WAP device. The TXOP Limit maximum value is 65535.

**Step 6** Configure the following additional settings:

- **No Acknowledgement** — Check **Enable** to specify that the WAP device should not acknowledge frames with QosNoAck as the service class value.

- **Unscheduled Automatic Power Save Delivery** — Check **Enable** to enable APSD. The APSD is recommended if VoIP phones access the network through the WAP device.

**Step 7** Click **Apply**.