Configuring a VAP on the WAP351, WAP131, and WAP371

Objective

Virtual Access Points (VAPs) segment the wireless LAN into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. VAPs simulate multiple access points in one physical WAP device. Up to four VAPs are supported on the Cisco WAP131 and up to eight VAPs are supported on the Cisco WAP351 and WAP371.

The objective of this document is to show you how to configure a VAP on the WAP351, WAP131, and WAP371 access points.

Applicable Devices

- WAP351
- WAP131
- WAP371

Software Version

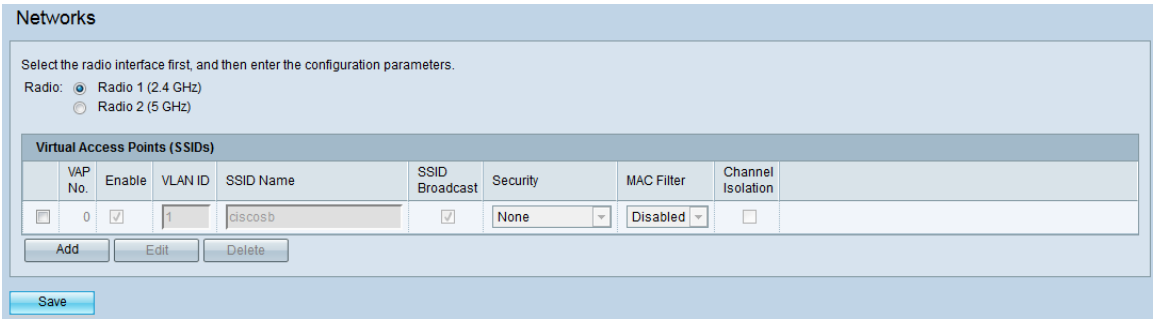
- V1.0.0.39 (WAP351)
- V1.0.0.39 (WAP131)
- V1.2.0.2 (WAP371)

Add and Configure a VAP

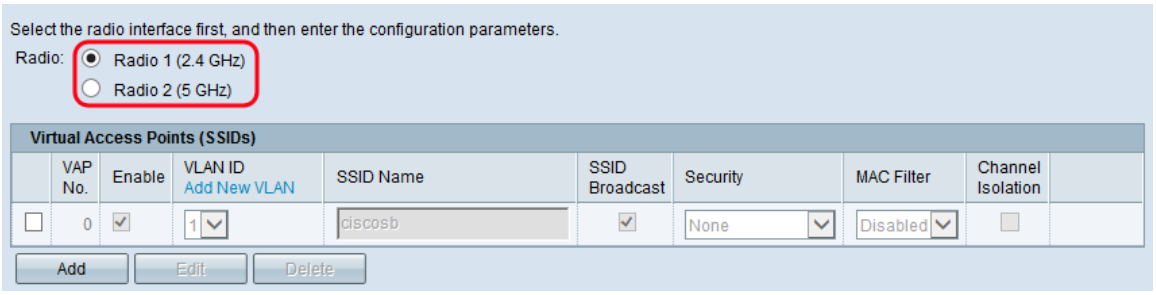
Note: Each VAP is identified by a user-configured Service Set Identifier (SSID). Multiple VAPs cannot have the same SSID name.

Note: In order for your wireless network to function, the radio that your configured VAP is associated with must be enabled and properly configured. See *Configuring Basic Radio Settings on the WAP131 and WAP351* or *Configuring Basic Radio Settings on the WAP371* for more information

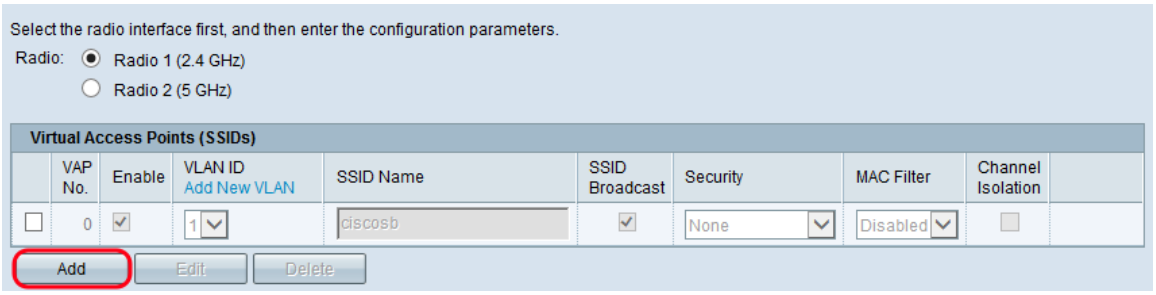
Step 1. Log in to the web configuration utility and navigate to **Wireless** > **Networks**. The *Networks* page appears:



Step 2. In the *Radio* field, select the radio button for the wireless radio on which you would like to configure VAPs.

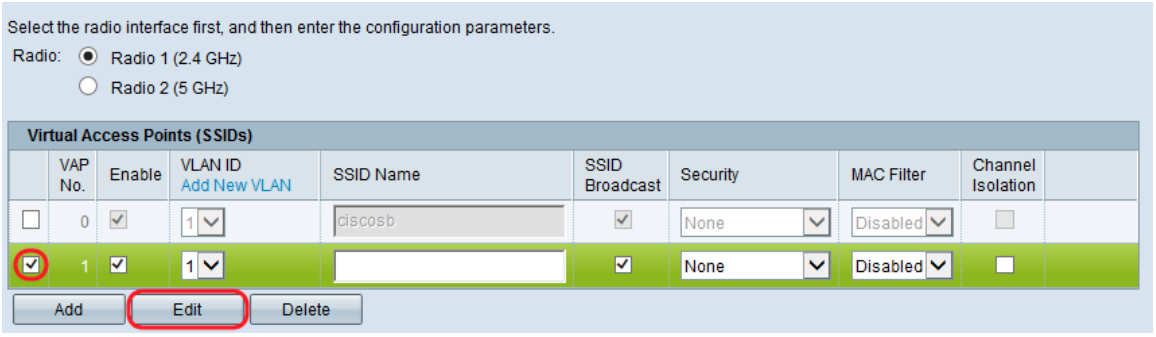


Step 3. To add a new VAP, click **Add**. A new VAP will appear in the table.

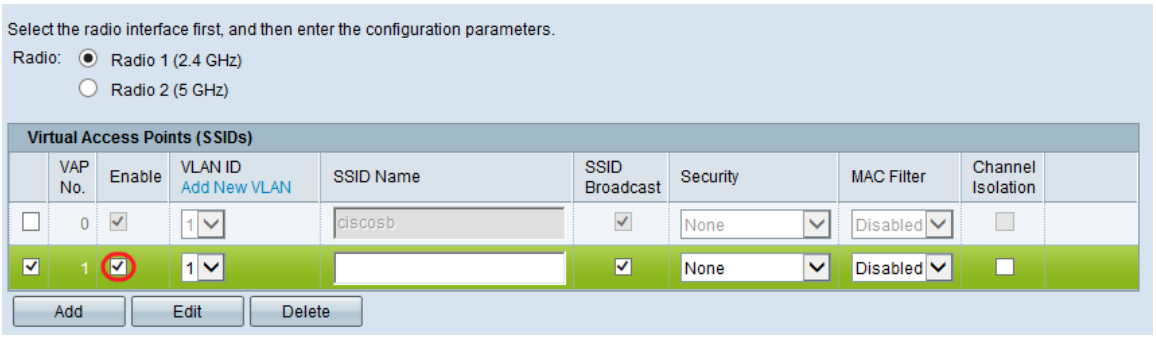


Note: The WAP131 supports up to 4 VAPs, while the WAP371 and WAP351 support up to 8 VAPs.

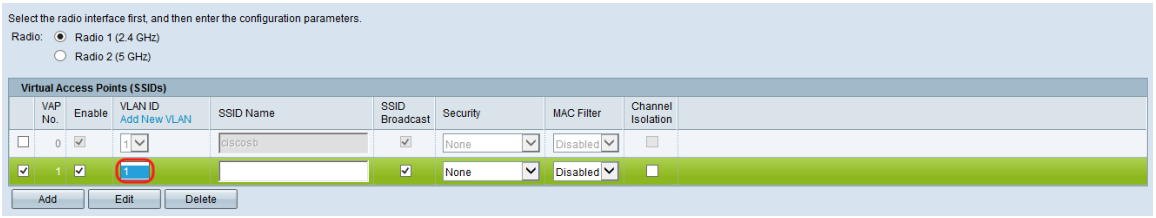
Step 4. To begin editing a VAP, click the check box on the far left of the table entry and then click **Edit**. This will allow you to modify the grayed out fields of the VAP you have selected.



Step 5. To enable usage of the VAP, ensure that the *Enable* check box is checked.

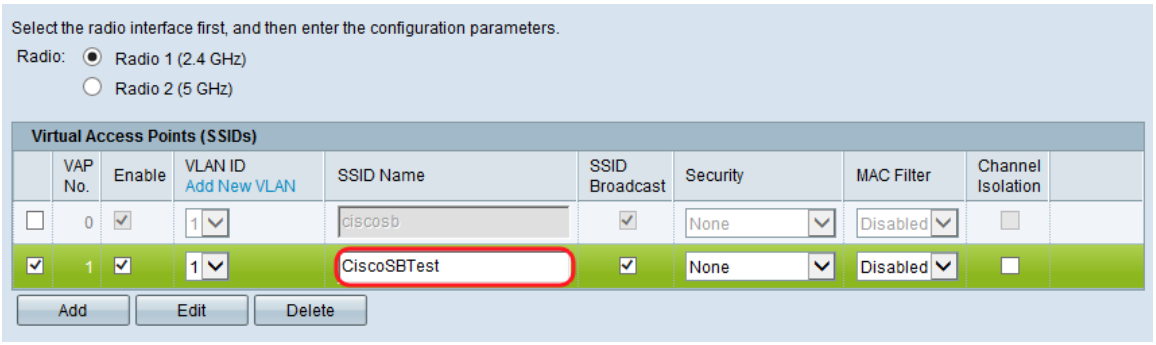


Step 6. In the *VLAN ID* field, specify the VLAN ID you would like to associate with the VAP. If you are using the WAP131 or WAP371, enter in the VLAN ID. The max value that you can enter is 4094.

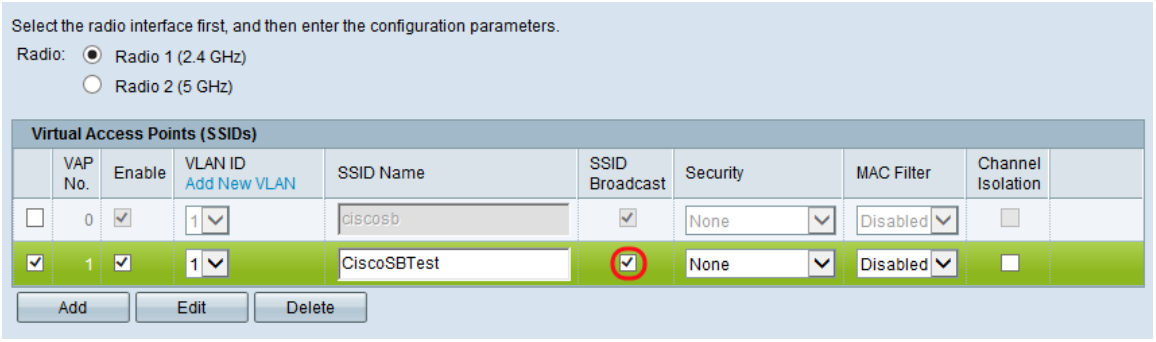


Note: The VLAN ID that is entered must exist on your network and be properly configured. See *VLAN Configuration on the WAP351 Access Point*, *Managing Tagged and Untagged VLAN IDs on WAP131*, or *Managing Tagged and Untagged VLAN IDs on the WAP371* for more information.

Step 7. Enter the name of the wireless network in the SSID Name field. Each VAP must have a unique SSID name.



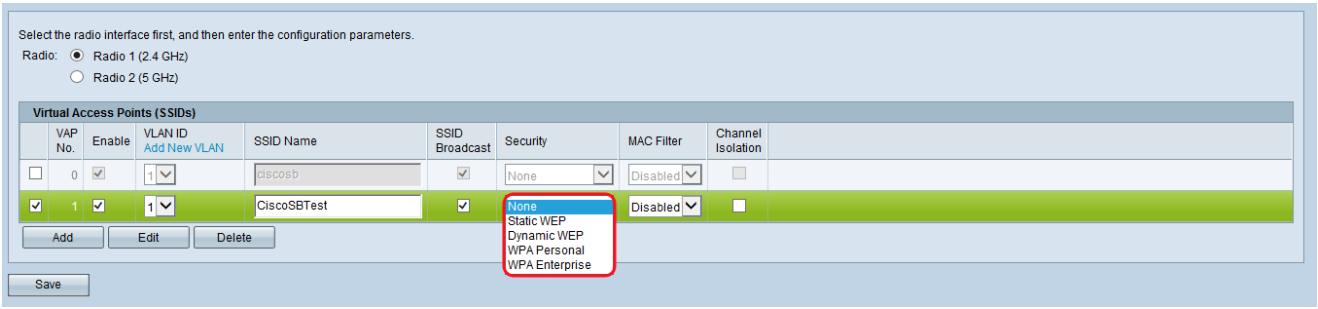
Step 8. If you would like the SSID name to be broadcast to clients check the *SSID Broadcast* check box. This will show the SSID name to clients on their list of available networks.



Configuring Security Settings

Step 1. Choose the authentication method that is required to connect to the VAP from the

Security drop-down list. If any option other than **None** is selected, additional fields will appear.



The available options are as follows:

- None
- Static WEP
- Dynamic WEP
- WPA Personal
- WPA Enterprise

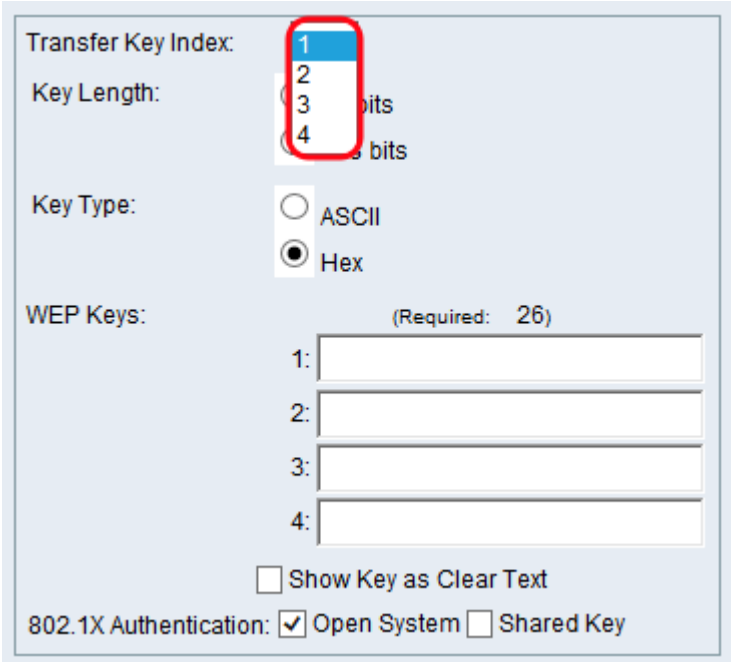
Note: WPA Personal and WPA Enterprise are the preferred authentication types for maximum security. Static WEP and Dynamic WEP should only be used with legacy equipment and requires that the radio be set to either 802.11a or 802.11b/g mode to be used. See *Configuring Basic Radio Settings on the WAP131 and WAP351* or *Configuring Basic Radio Settings on the WAP371* for more information.

Static WEP

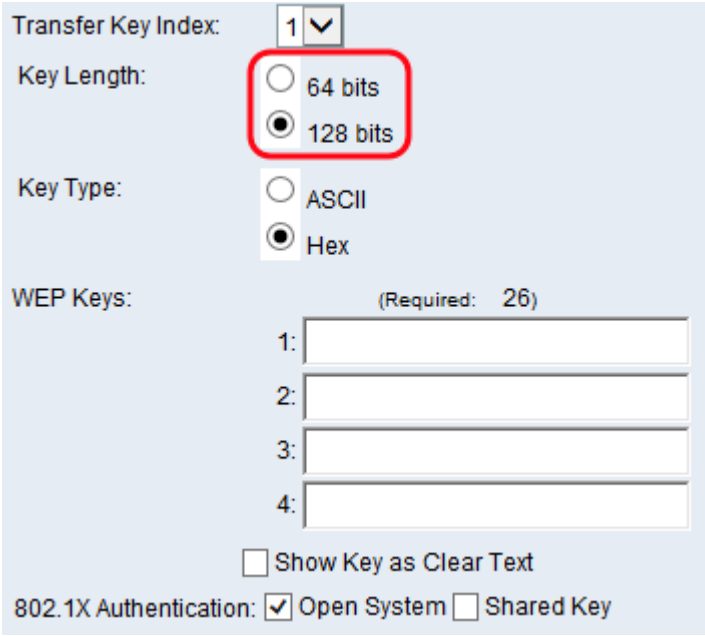
Static WEP is the least secure authentication method. It encrypts data in the wireless network based on a static key. It has become simple to obtain this static key illegitimately, so WEP authentication should only be used when necessary with legacy devices.

Note: When selecting *Static WEP* as your security method, a prompt will appear and tell you that your security method choice is very insecure.

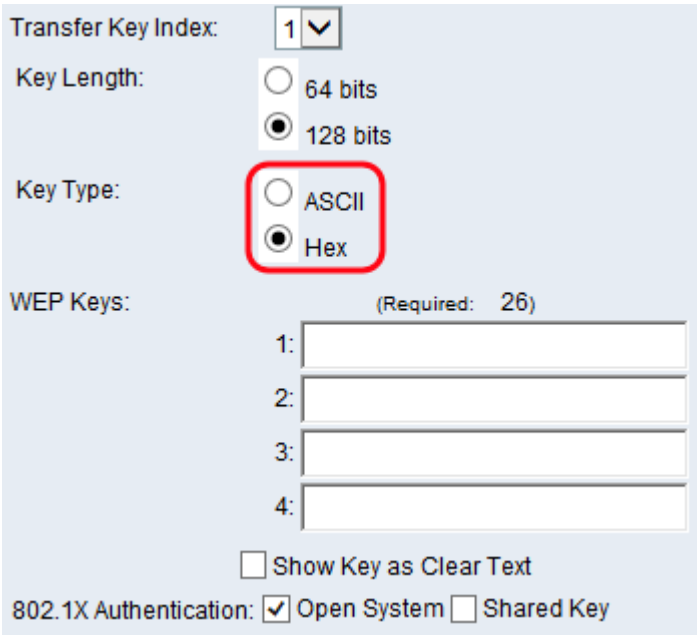
Step 1. In the *Transfer Key Index* drop-down list, select the index of the WEP key from the list of keys below that the device will use to encrypt data.



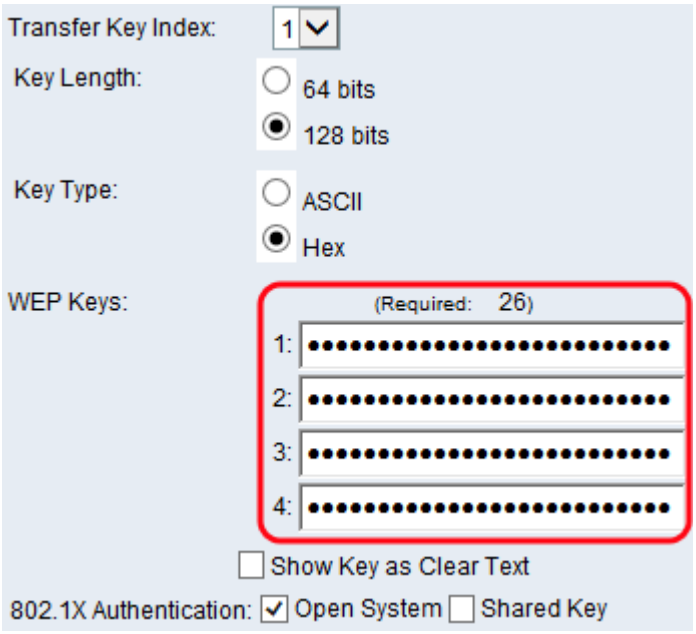
Step 2. Choose a radio button from the *Key Length* field to specify whether the key is 64 bits or 128 bits in length.



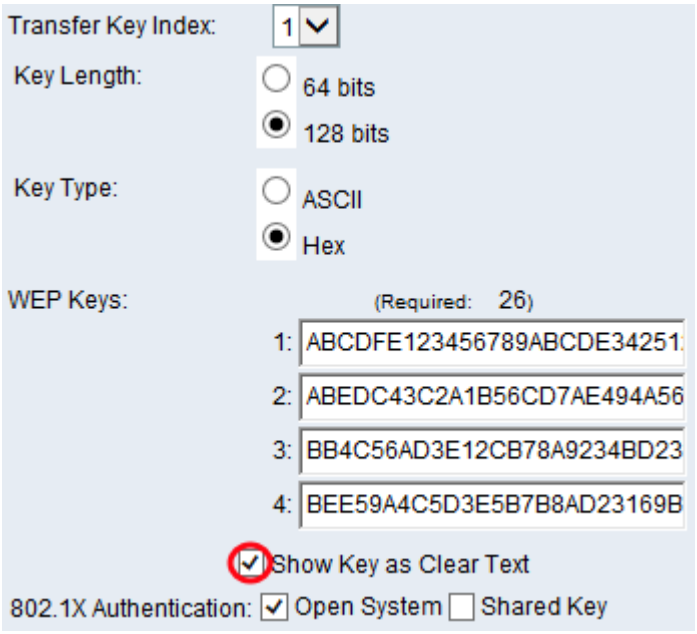
Step 3. In the *Key Type* field, choose whether you would like to enter the keys in ASCII or hexadecimal format. ASCII includes all letters, numbers, and symbols present on the keyboard while hexadecimal must use only numbers or letters A-F.



Step 4. In the *WEP Keys* field, enter up to 4 different WEP keys for your device. Each client that is to connect to this network must have one of the same WEP keys in the same slot specified by the device.

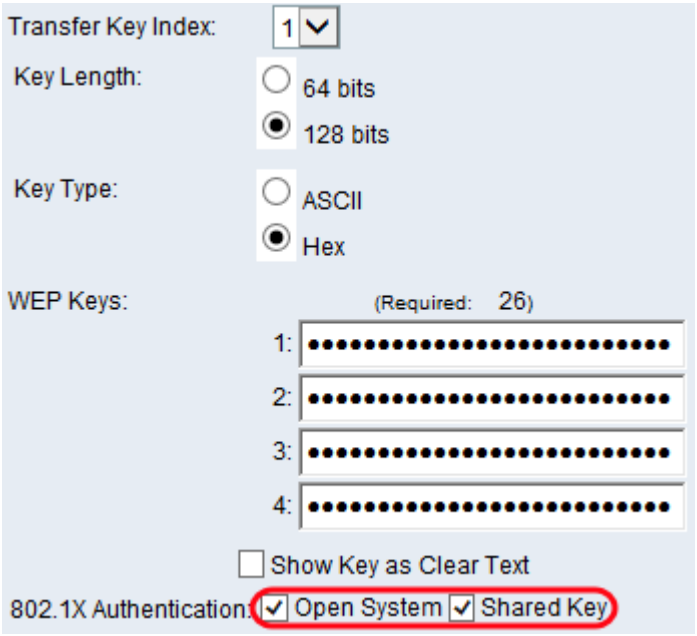


Step 5. (Optional) Click the check box in the *Show Key as Clear Text* field, if you reveal the character strings of the keys.



Note: When using a different firmware on the WAP351, WAP131, or WAP371, the *Show Key as Clear Text* field may be missing.

Step 6. In the *802.1X Authentication* field, specify the authentication algorithm that you want to use by choosing the options *Open System* and/or *Shared Key*. The authentication algorithm defines the method that is used to determine whether a client station is allowed to associate with the WAP device when static WEP is the security mode.



The available options are defined as follows:

- Open System — The authentication allows any client station to associate with the WAP device whether that client station has the correct WEP key or not. This algorithm is used in plain text, IEEE 802.1X, and WPA modes. When the authentication algorithm is set to *Open System*, any client can associate with the WAP device.

- Shared Key — The authentication requires the client station to have the correct WEP key in order to associate with the WAP device. When the authentication algorithm is set to *Shared Key*, a station with an incorrect WEP key cannot associate with the WAP device.

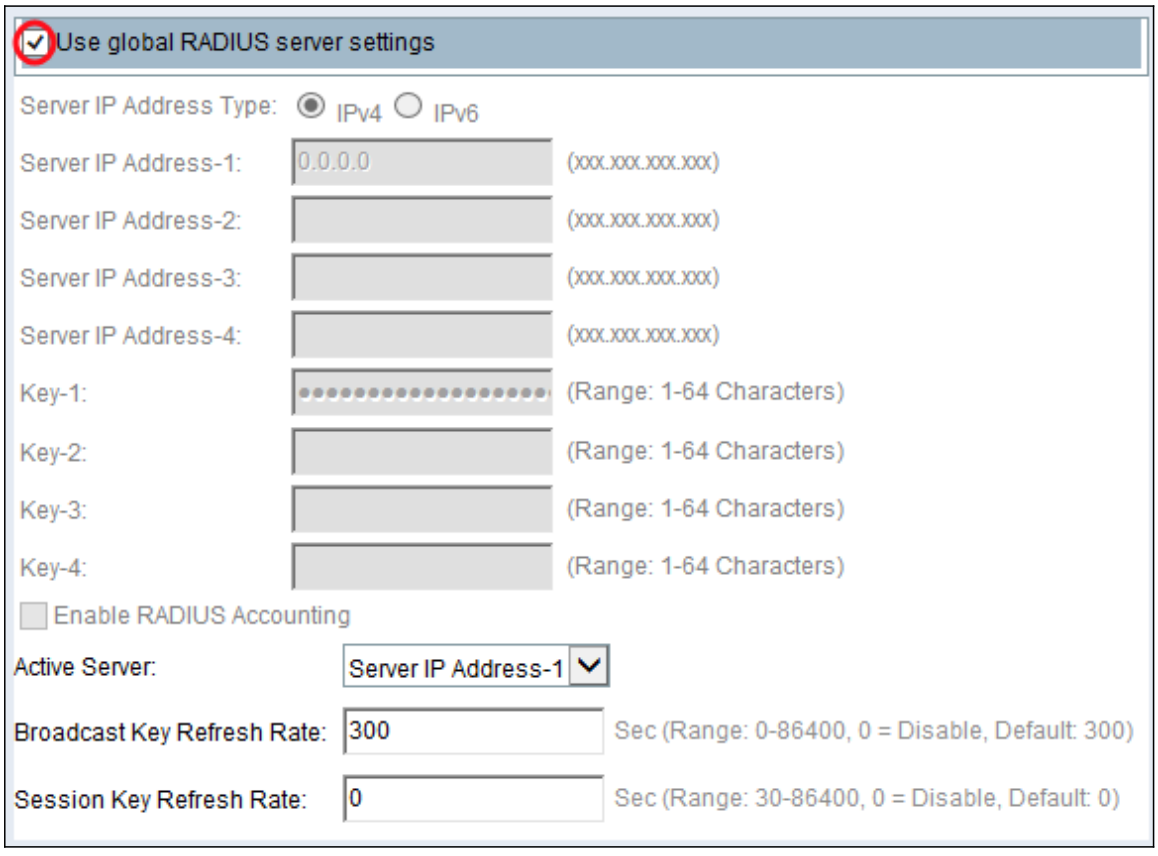
• Open System and Shared Key — When you have selected both of these authentication algorithms, the client stations configured to use WEP in shared key mode must have a valid WEP key in order to associate with the WAP device. Also, the client stations configured to use WEP as an open system (shared key mode not enabled) can associate with the WAP device even if they do not have the correct WEP key.

Step 7. Click **Save**.

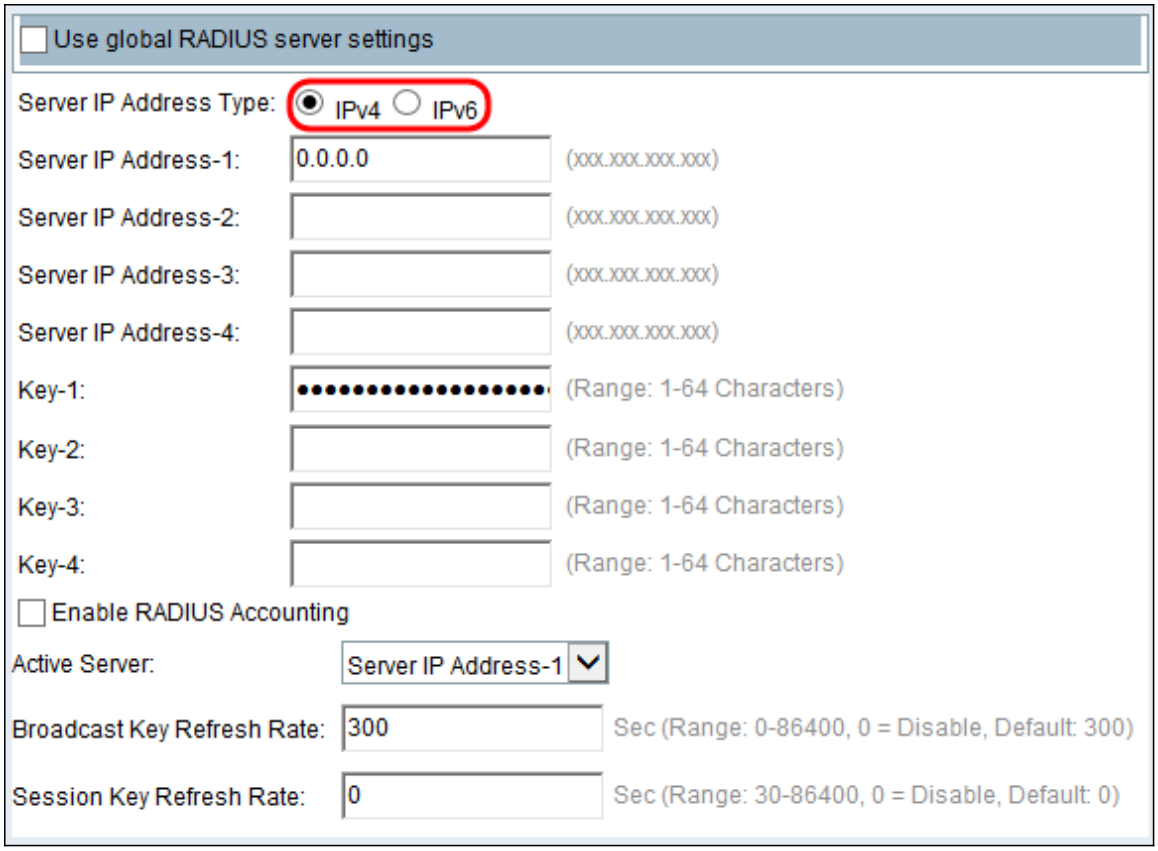
Dynamic WEP

Dynamic WEP refers to the combination of 802.1x technology and the Extensible Authentication Protocol (EAP). This mode requires the use of an external RADIUS server to authenticate users. The WAP device requires a RADIUS server that supports EAP, such as the Microsoft Internet Authentication Server. To work with Microsoft Windows clients, the authentication server must support Protected EAP (PEAP) and MSCHAP v2. You can use any of a variety of authentication methods that the IEEE 802.1X mode supports, including certificates, Kerberos, and public key authentication but you must configure the client stations to use the same authentication method the WAP device uses.

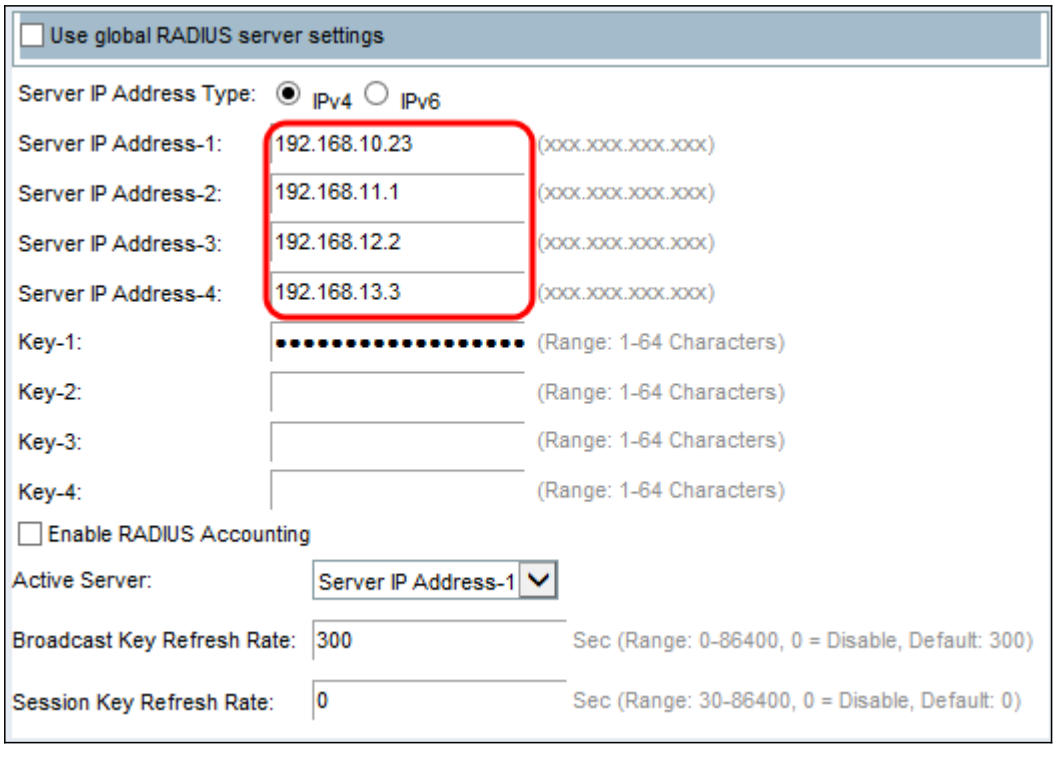
Step 1. By default the *Use global RADIUS server settings* is checked. Uncheck the check box if you want to configure the VAP to use a different set of RADIUS servers. Otherwise skip to Step 8.



Step 2. In the *Server IP Address Type* field, select the server IP address type your WAP device uses. The options are *IPv4* or *IPv6*. IPv4 uses 32-bit binary numbers represented in dotted decimal notation. IPv6 uses hexadecimal numbers and colons to represent a 128-bit binary number. The WAP device contacts only the RADIUS server or servers for the address type that you selected in this field. If you choose IPv6, then skip to Step 4.

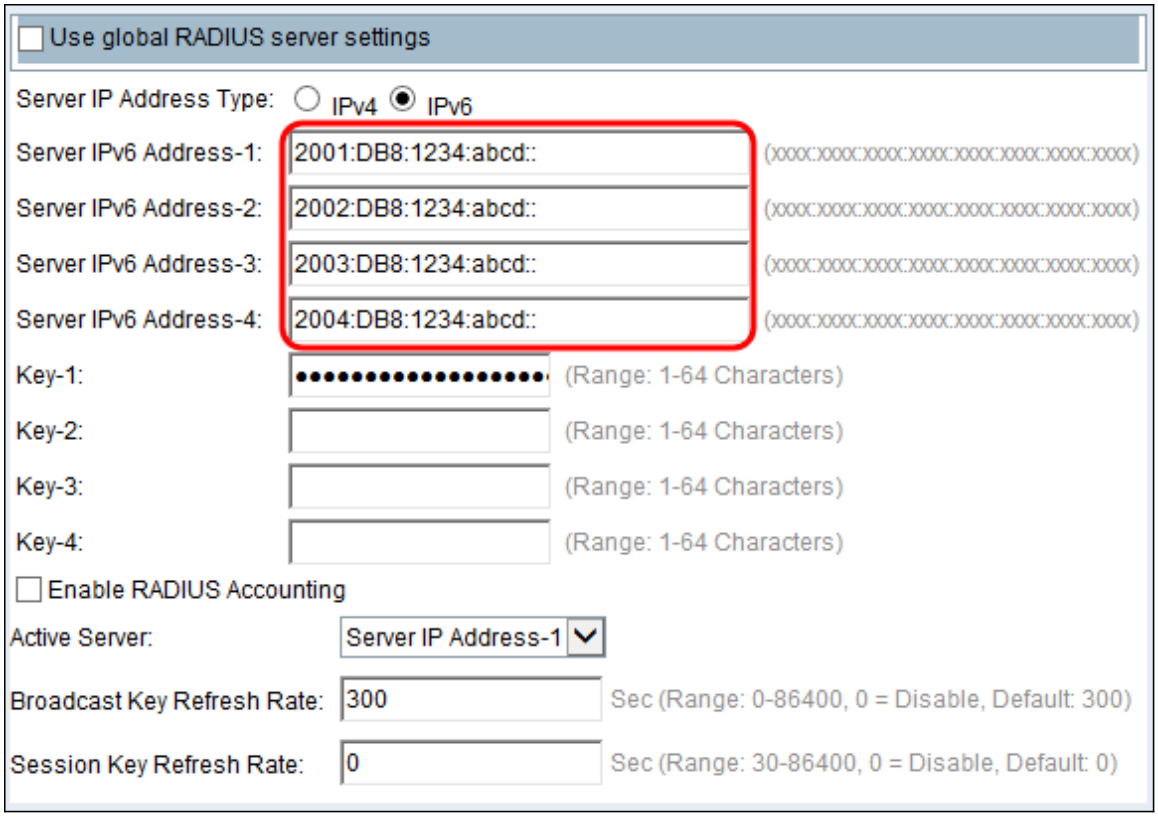


Step 3. If you selected **IPv4** in Step 2, enter the IP address of the RADIUS server that all VAPs use by default. Then skip to Step 5.



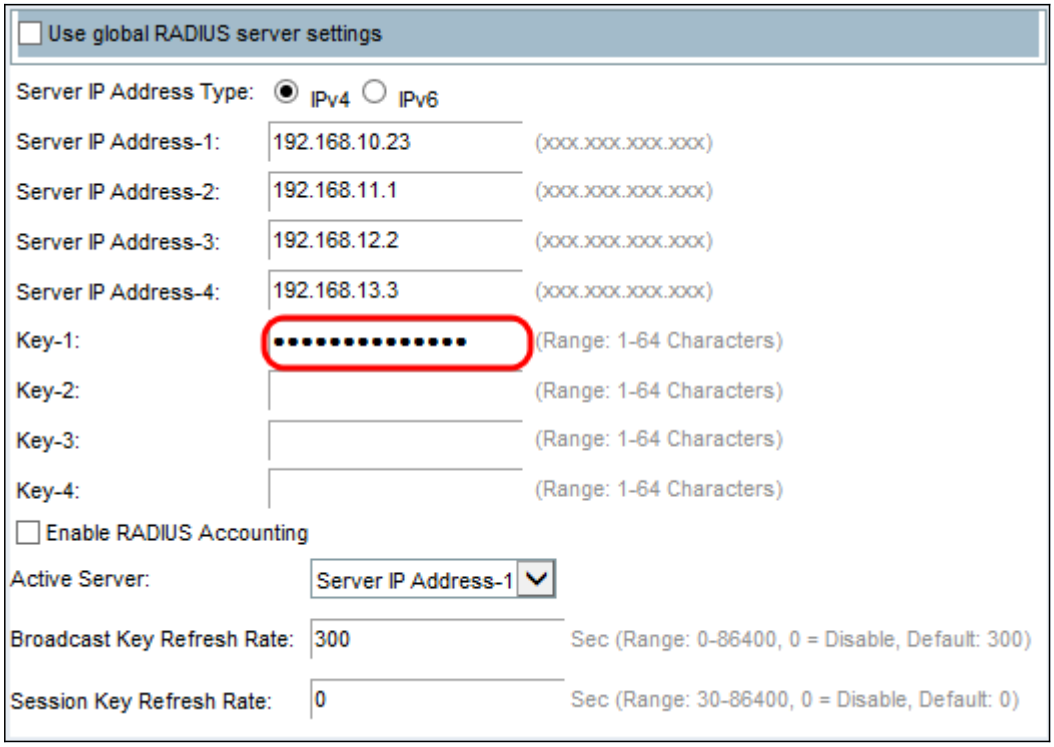
Note: You can have up to three IPv4 backup RADIUS server addresses. If the authentication fails with the primary server, each configured backup server is tried in sequence.

Step 4. If you have selected **IPv6** in Step 2, enter the IPv6 address of the primary global RADIUS server.

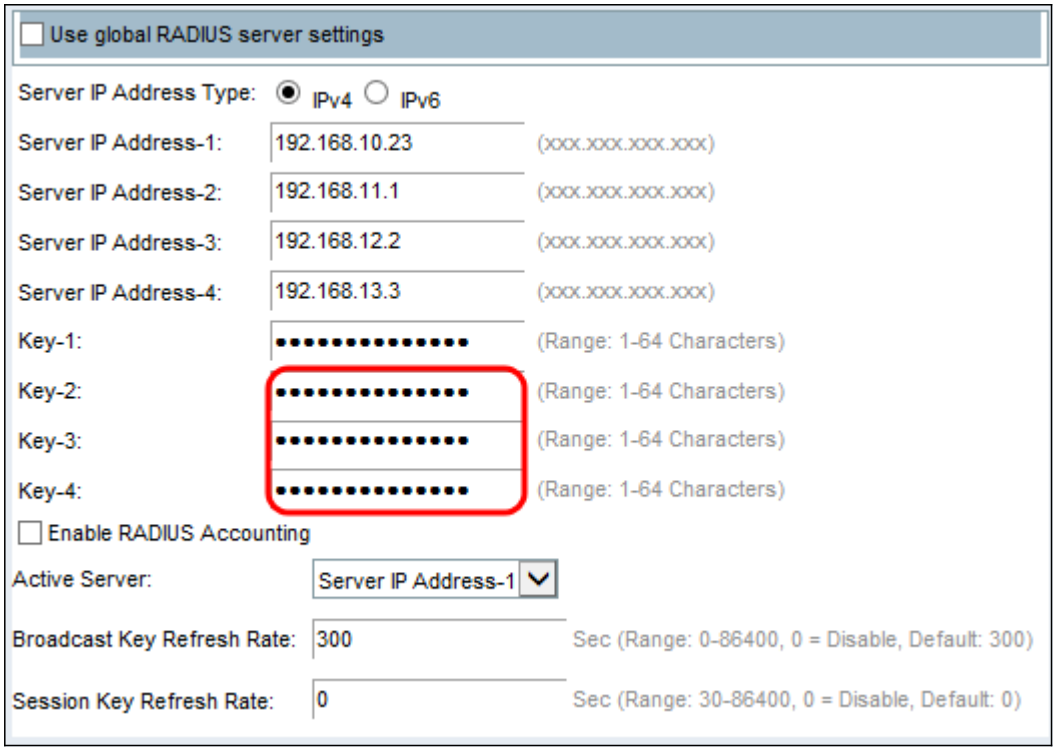


Note: You can have up to three IPv6 backup RADIUS server addresses. If the authentication fails with the primary server, each configured backup server is tried in sequence.

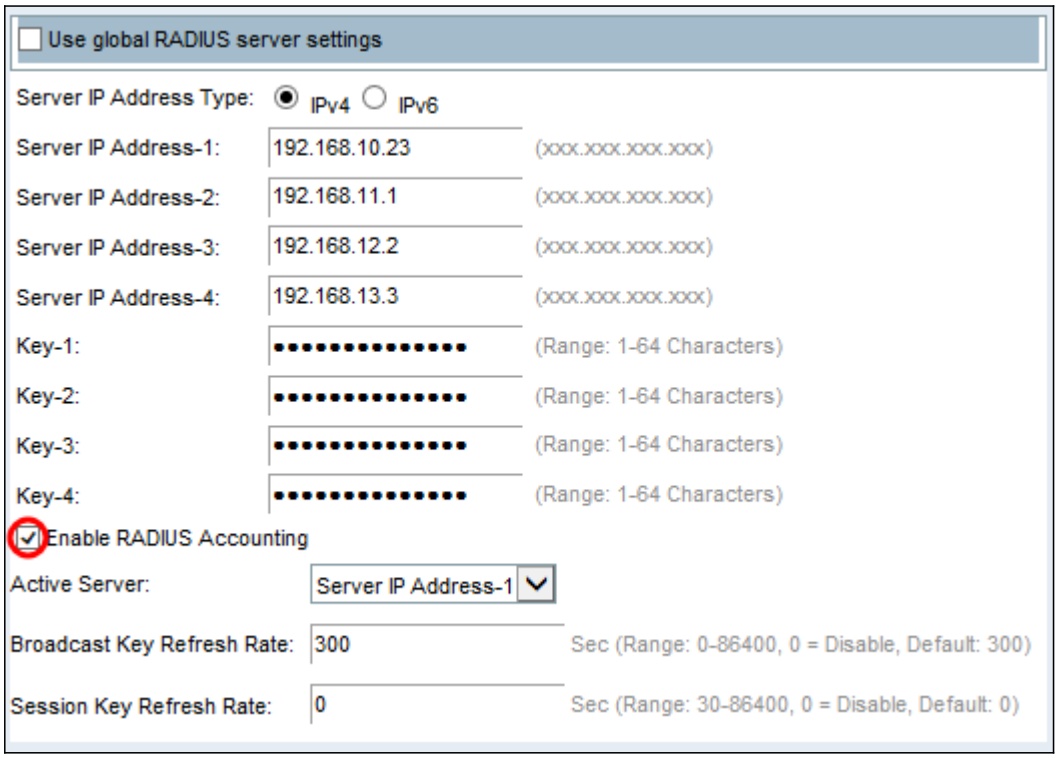
Step 5. In the *Key-1* field, enter in the shared secret key that the WAP device uses to authenticate to the primary RADIUS server.



Step 6. In the *Key-2* to *Key-4* fields, enter in the RADIUS key associated with the configured backup RADIUS servers. The Server IP Address-2 uses *Key-2*, Server IP Address 3 uses *Key-3*, and Server IP Address 4 uses *Key-4*.

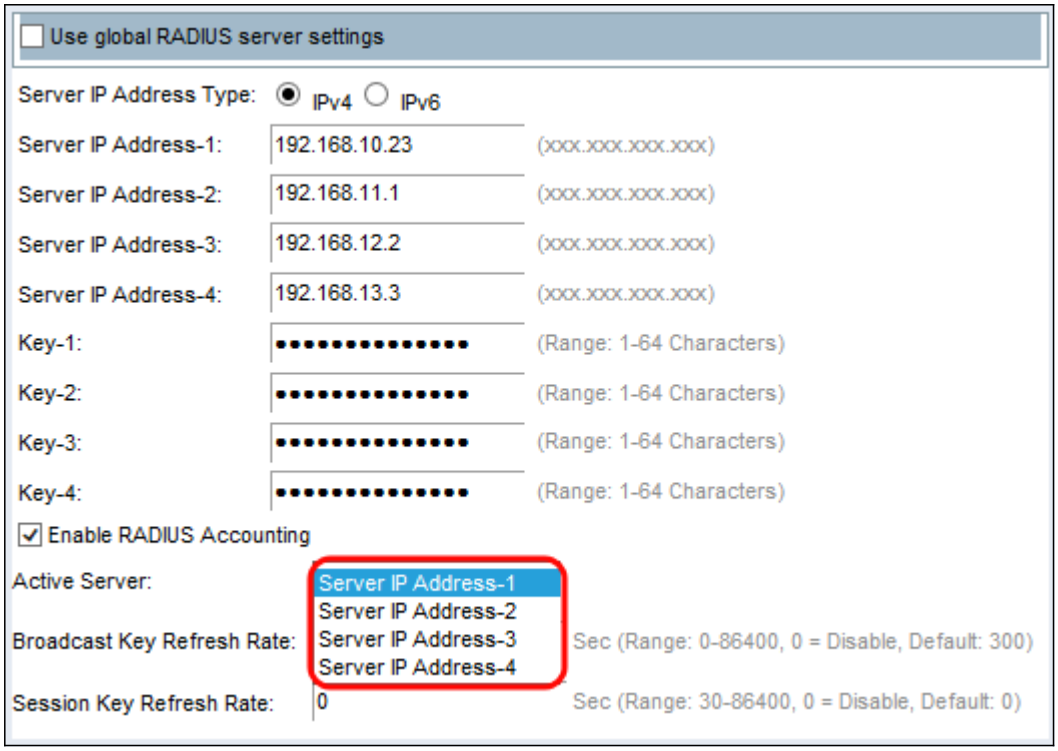


Step 7. (Optional) In the *Enable RADIUS Accounting* field, check the check box if you want to enable the tracking and measuring of the resources a particular user has consumed. Enabling RADIUS accounting will track the system time and the amount of data transmitted and received. The information will be stored in the Radius server. This will be enabled for the primary RADIUS server and all backup servers.

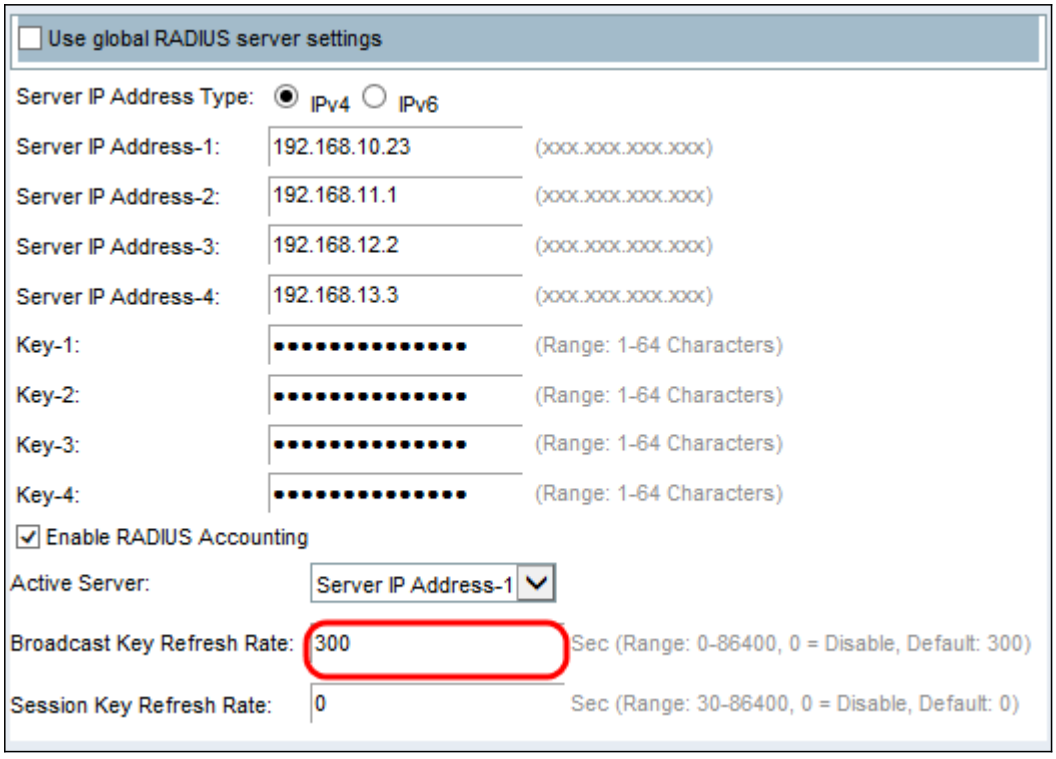


Note: If you have enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers

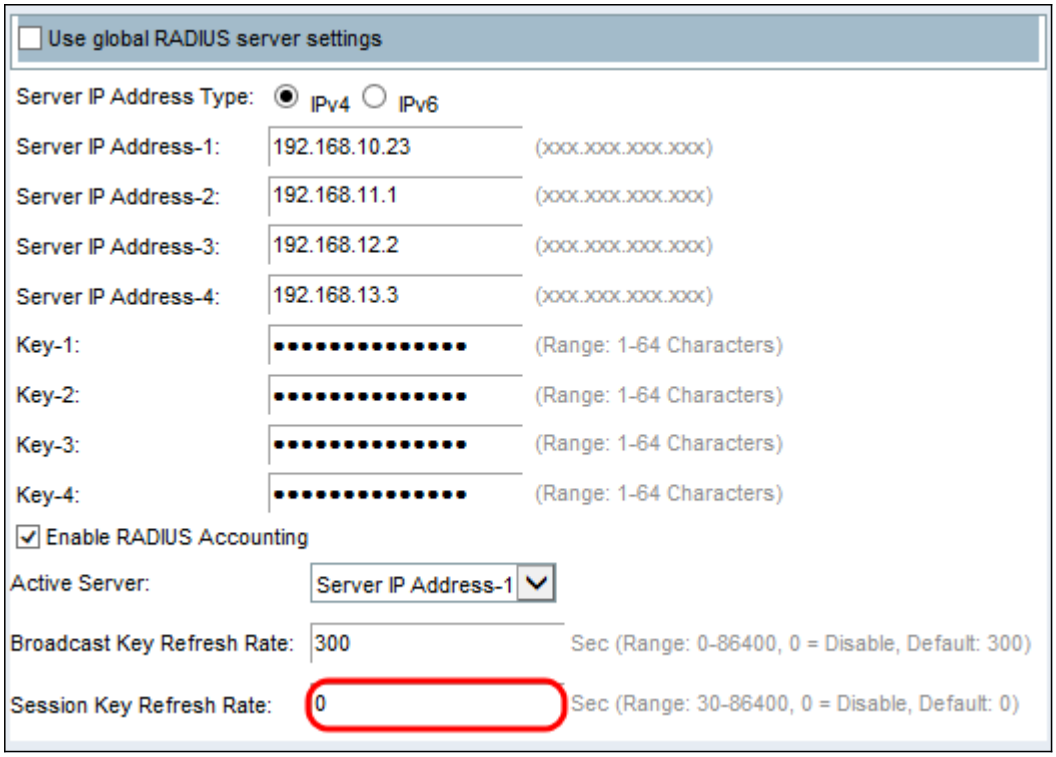
Step 8. Choose the first server that is active in the *Active Server* field. This enables manual selection of the active RADIUS server, rather than having the WAP device attempt to contact each configured server in sequence and choose the first server that is active.



Step 9. In the *Broadcast Key Refresh Rate* field, enter in the interval at which the broadcast (group) key is refreshed for clients associated with this VAP. The default is 300 seconds.



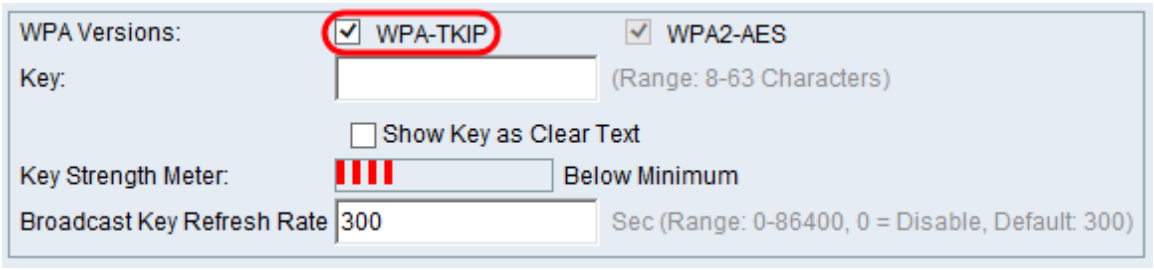
Step 10. In the *Session Key Refresh Rate* field, enter the interval at which the WAP device refreshes session (unicast) key for each client associated with the VAP. The default is 0.



WPA Personal

WPA Personal is a Wi-Fi Alliance IEEE 802.11i standard, which includes AES-CCMP and TKIP encryption. WPA 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 for credentials only. WPA is also referred to as WPA-PSK. This security mode is backwards-compatible for the wireless clients that support the original WPA.

Step 1. In the *WPA Versions* field, check the *WPA-TKIP* check box if you want to enable WPA-TKIP. You can have WPA-TKIP and WPA2-AES enabled at the same time. The WAP always supports WPA2-AES so you will not be able to configure it.



The available options are defined as follows:

- WPA-TKIP — The network has some client stations that only support the original WPA and TKIP security protocol. According to the latest WiFi Alliance requirements, choosing only WPA-TKIP is not recommended.

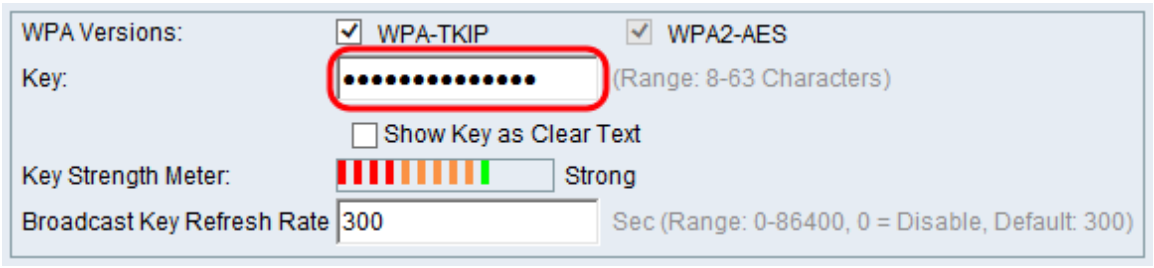
- WPA2-AES — All client stations on the network support WPA2 and AES-CCMP cipher/security protocol. This WPA version provides the best security per IEEE 802.11i standard. According to the latest WiFi Alliance requirement, the AP has to support this mode all the time.

- WPA-TKIP and WPA2-AES — If the network has a mix of clients, some of which support WPA2 and others which support only the original WPA, check both of the check boxes.

This setting 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.

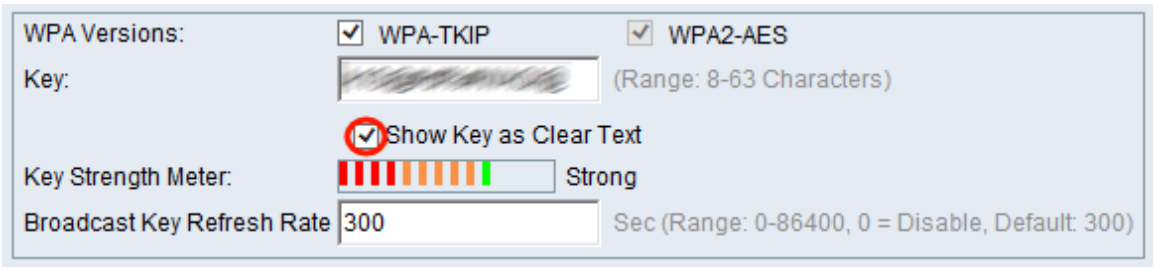
Note: WPA clients must have one of these keys (a valid TKIP key or a valid AES-CCMP key) to be able to associate with the WAP device.

Step 2. In the *Key* field, enter in the shared secret key for WPA Personal security. Enter at least 8 characters and a maximum of 63 characters.



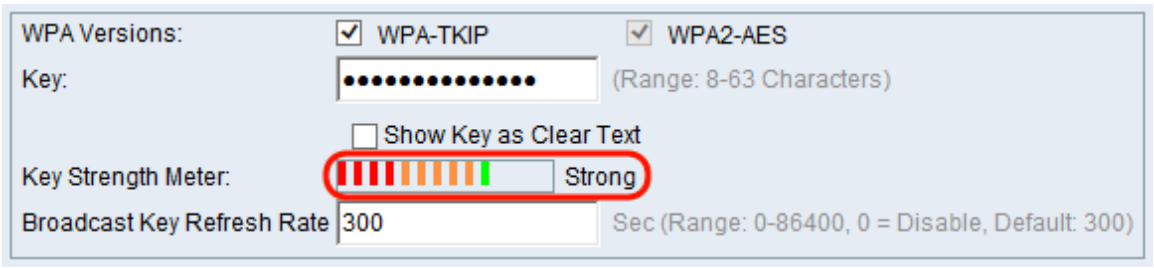
Note: Acceptable characters include uppercase and lowercase alphabetic letters, numeric digits, and special symbols (?!/\@#$%^&*).

Step 3. (Optional) Check the *Show Key as Clear Text* check box if you want the text you type to be visible. The checkbox is unchecked by default.

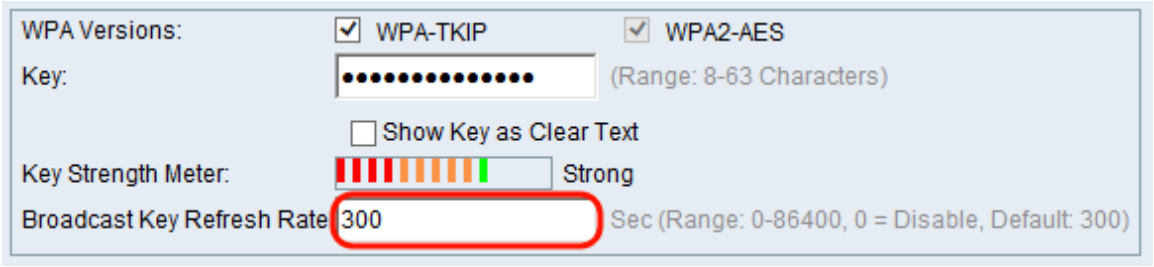


Note: When using a different firmware on the WAP351, WAP131, or WAP371, the *Show Key as Clear Text* field may be missing.

Note: The *Key Strength Meter* field is where the WAP device checks the key against complexity criteria such as how many different types of characters are used and how long the key is. If the WPA-PSK complexity check feature is enabled, the key is not accepted unless it meets the minimum criteria. For more information about WPA-PSK complexity, *refer to* Configuring Password Complexity for the WAP131, WAP351, and WAP371.



Step 4. In the *Broadcast Key Refresh Rate* field, enter in the interval at which the broadcast (group) key is refreshed for clients associated with this VAP. The default is 300 seconds.

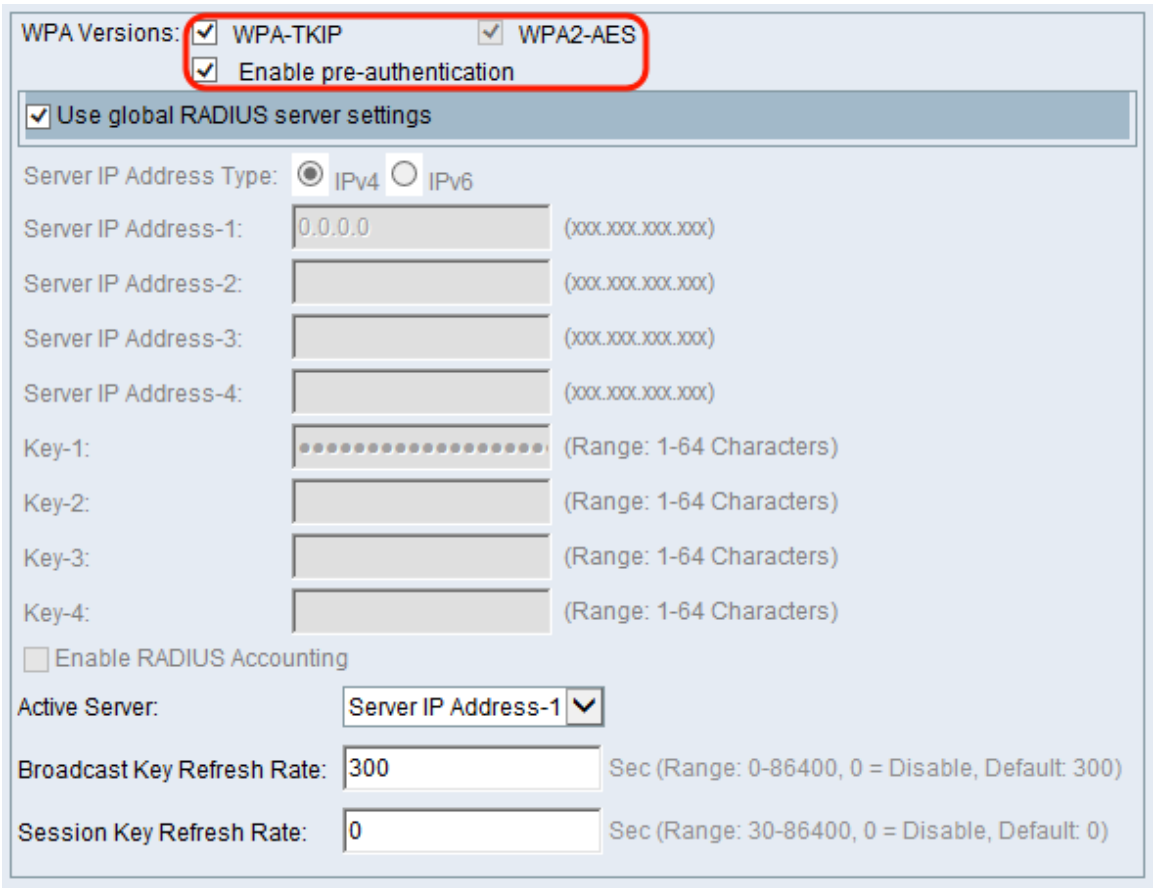


WPA Enterprise

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

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

Step 1. In the *WPA Versions* field, check the check box for the types of client stations to be supported. They are all enabled by default. The AP must support WPA2-AES all the time so you will not be able to configure it.



The available options are defined as follows:

• 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 WiFi Alliance requirement.

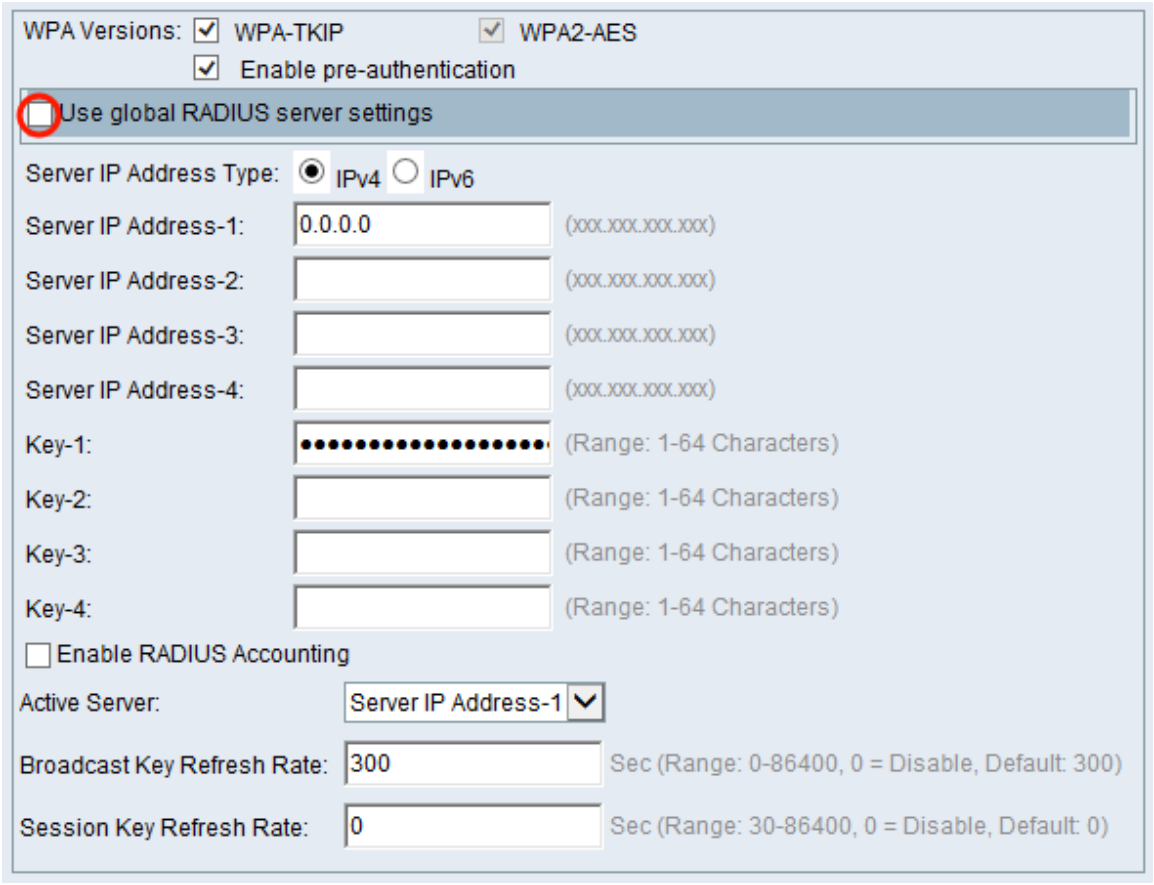
• WPA2-AES — All client stations on the network support WPA2 version and AES-CCMP cipher/ security protocol. This WPA version provides the best security per the IEEE 802.11i

standard. As per the latest Wi-Fi Alliance requirement, the WAP has to support this mode all the time.

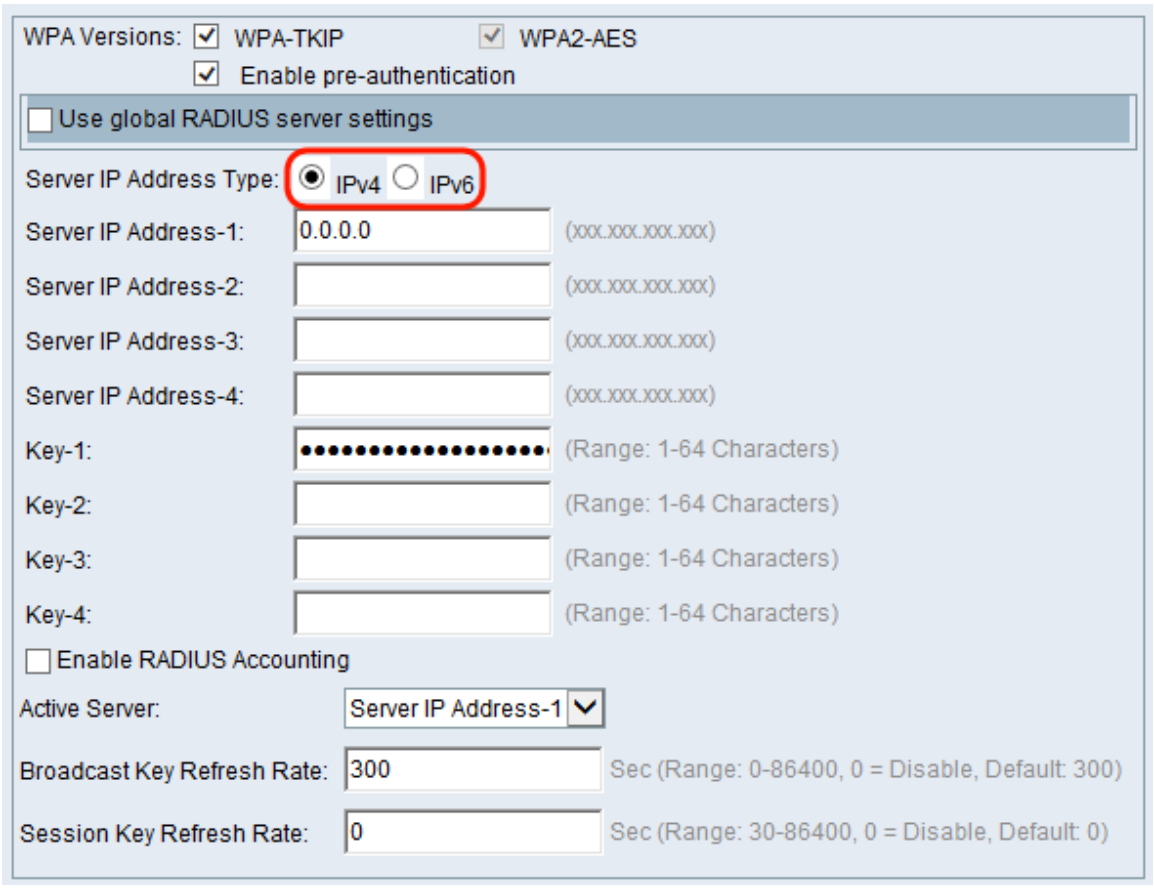
• Enable pre-authentication — If you choose only WPA2 or both WPA and WPA2 as the WPA version, you can enable pre-authentication for the WPA2 clients. Check this option if you want the WPA2 wireless clients to send the pre-authentication packets. The pre-authentication information is relayed from the 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 WAPs. This options does not apply if you selected WPA for WPA versions because the original WPA does not support this feature.

Note: Client stations configured to use WPA with RADIUS must have one of these addresses and keys: A valid TKIP RADIUS or valid CCMP (AES) IP Address and a RADIUS key.

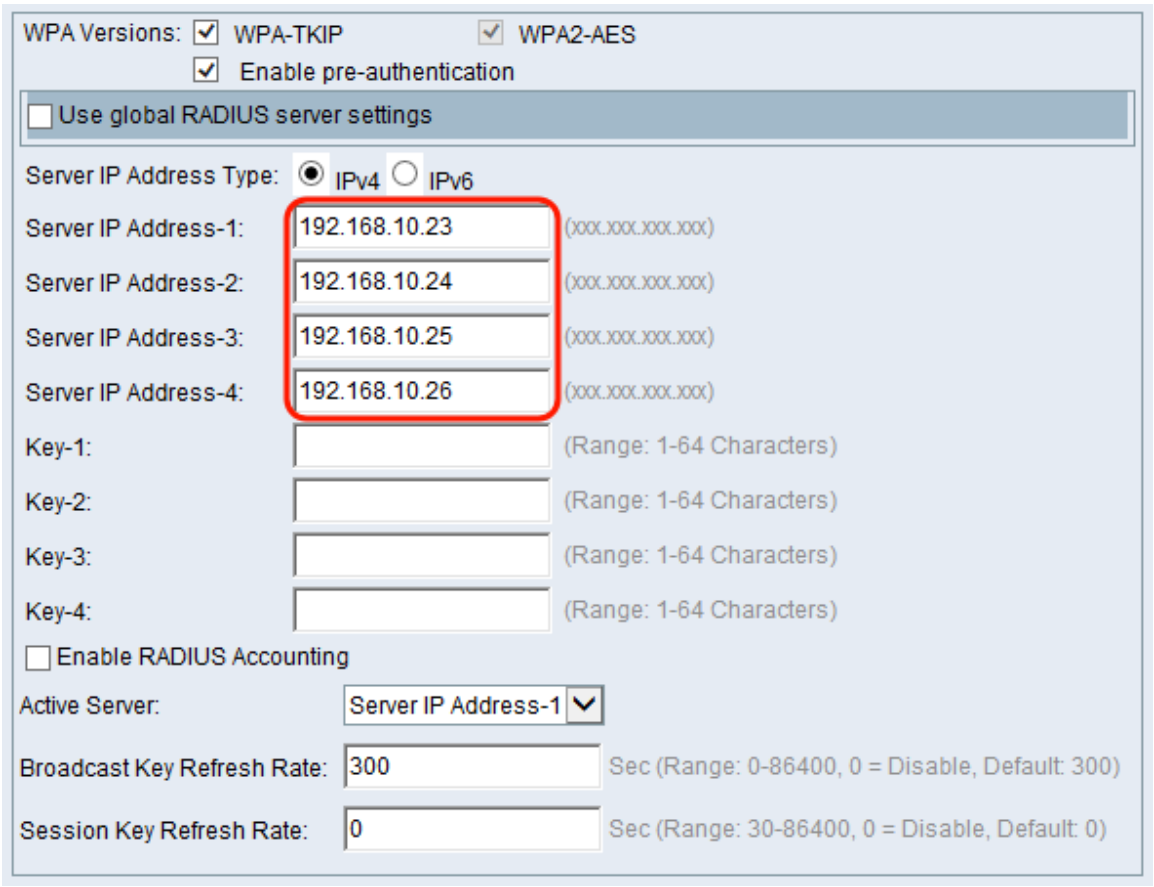
Step 2. By default the *Use global RADIUS server settings* is checked. Uncheck the check box if you want to configure the VAP to use a different set of RADIUS servers. Otherwise skip to Step 9.



Step 3. In the *Server IP Address Type* field, select the server IP address type your WAP device uses. The options are *IPv4* or *IPv6*. IPv4 uses 32-bit binary numbers represented in dotted decimal notation. IPv6 uses hexadecimal numbers and colons to represent a 128-bit binary number. The WAP device contacts only the RADIUS server or servers for the address type that you selected in this field.

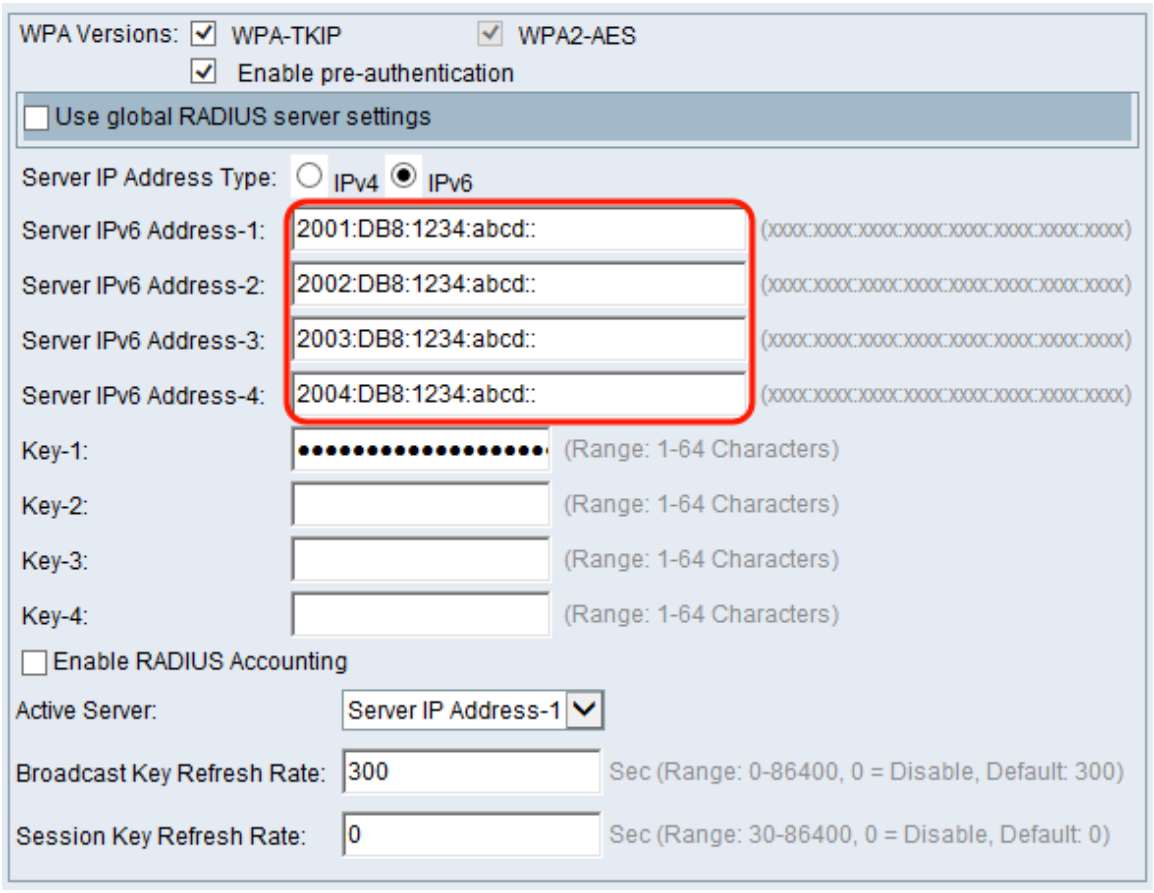


Step 4. If you selected **IPv4** in Step 2, enter the IP address of the RADIUS server that all VAPs use by default. Then Skip to Step 6.



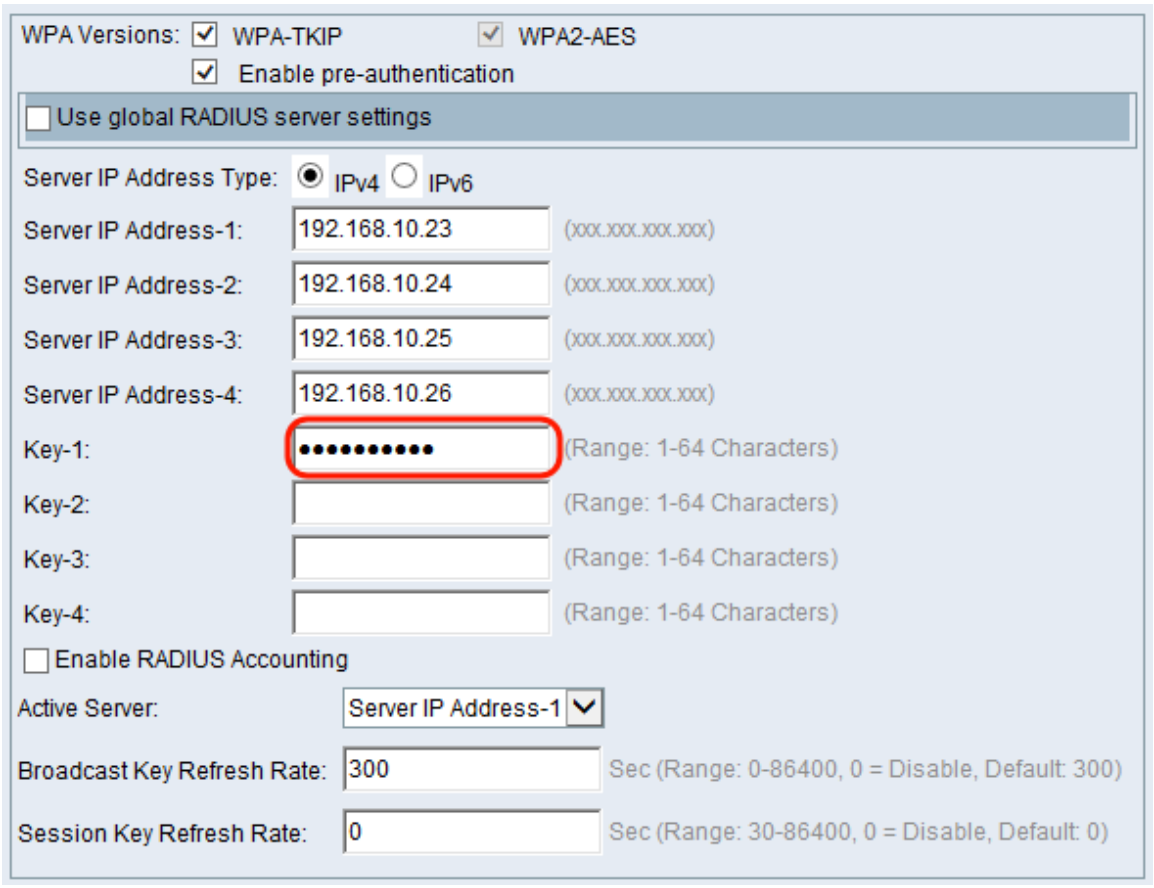
Note: You can have up to three IPv4 backup RADIUS server addresses. If the authentication fails with the primary server, each configured backup server is tried in sequence.

Step 5. If you selected **IPv6** in Step 2, enter the IPv6 address of the primary global RADIUS server.

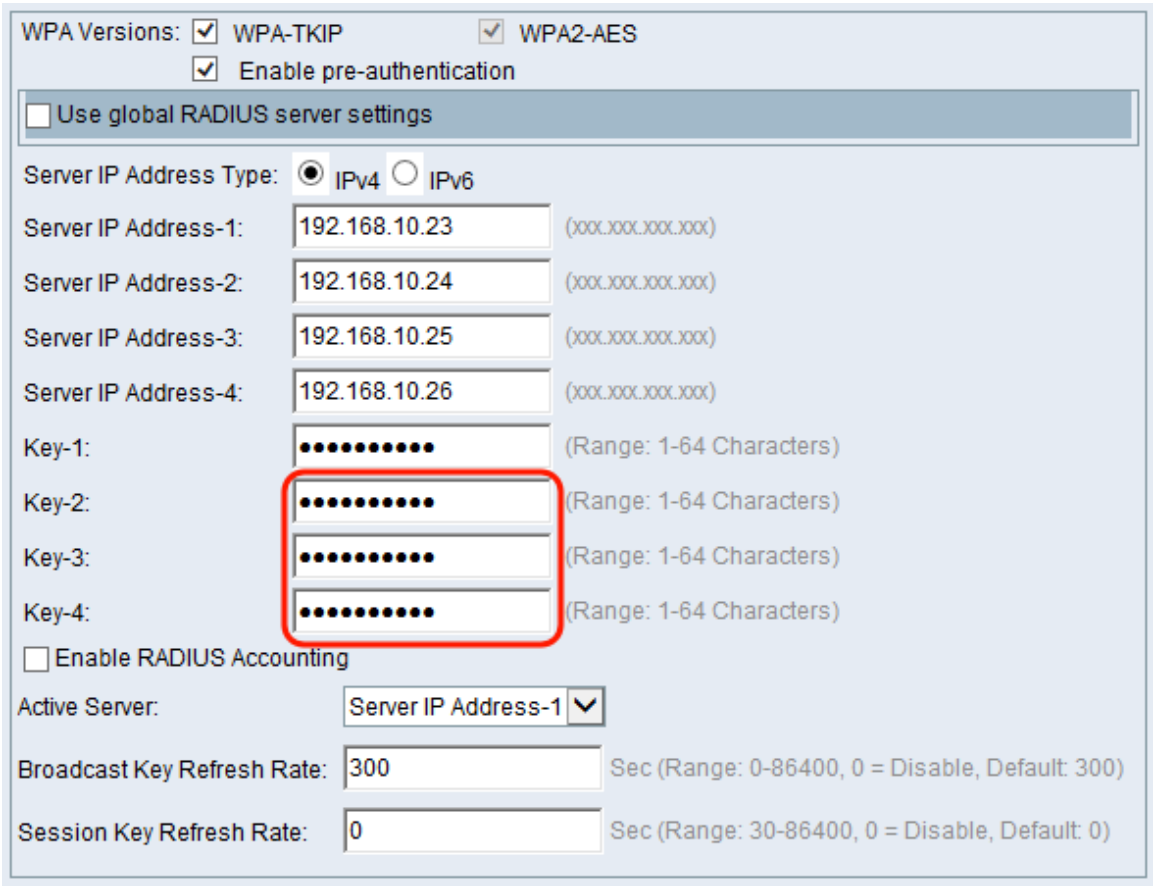


Note: You can have up to three IPv6 backup RADIUS server addresses. If the authentication fails with the primary server, each configured backup server is tried in sequence.

Step 6. In the *Key-1* field, enter in the shared secret key that the WAP device uses to authenticate to the primary RADIUS server.

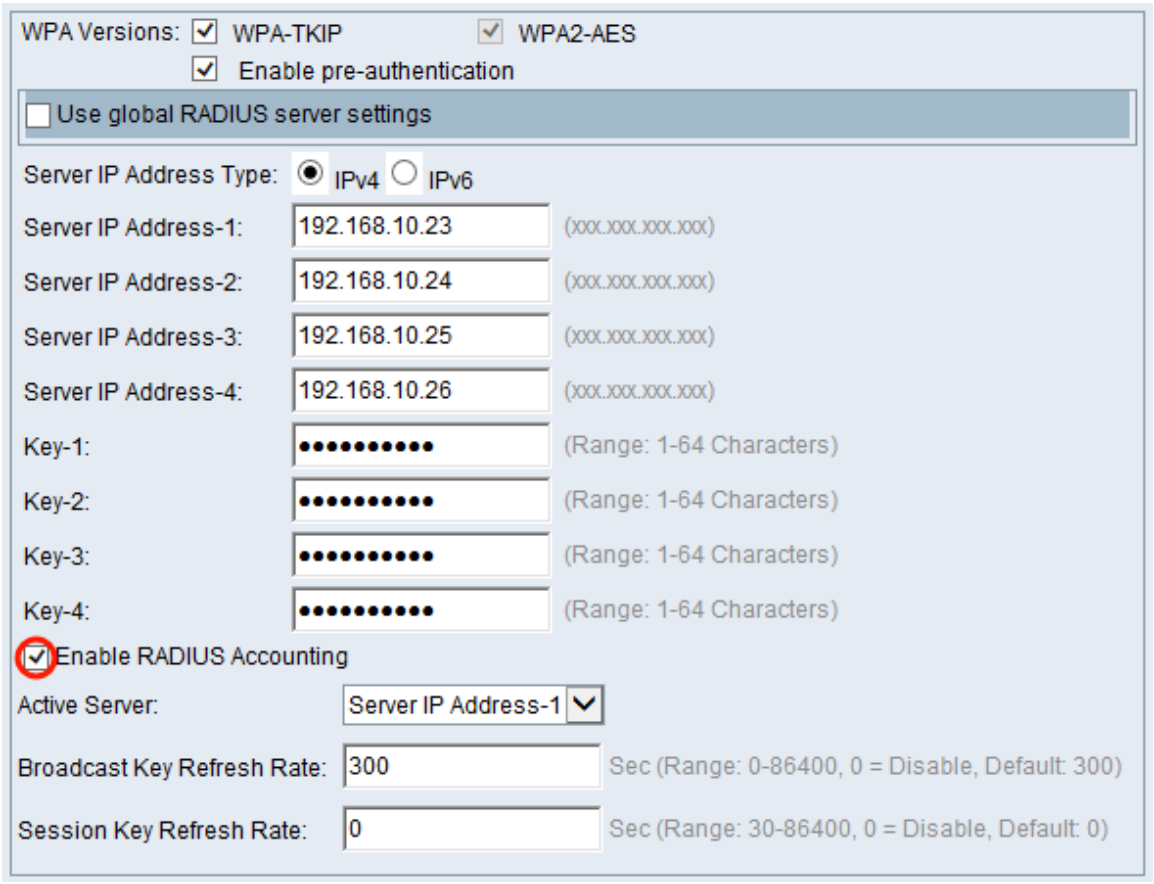


Step 7. In the *Key-2* to *Key-4* fields, enter in the RADIUS key associated with the configured backup RADIUS servers. The Server IP Address-2 uses *Key-2*, Server IP Address 3 uses *Key-3*, and Server IP Address 4 uses *Key-4*.



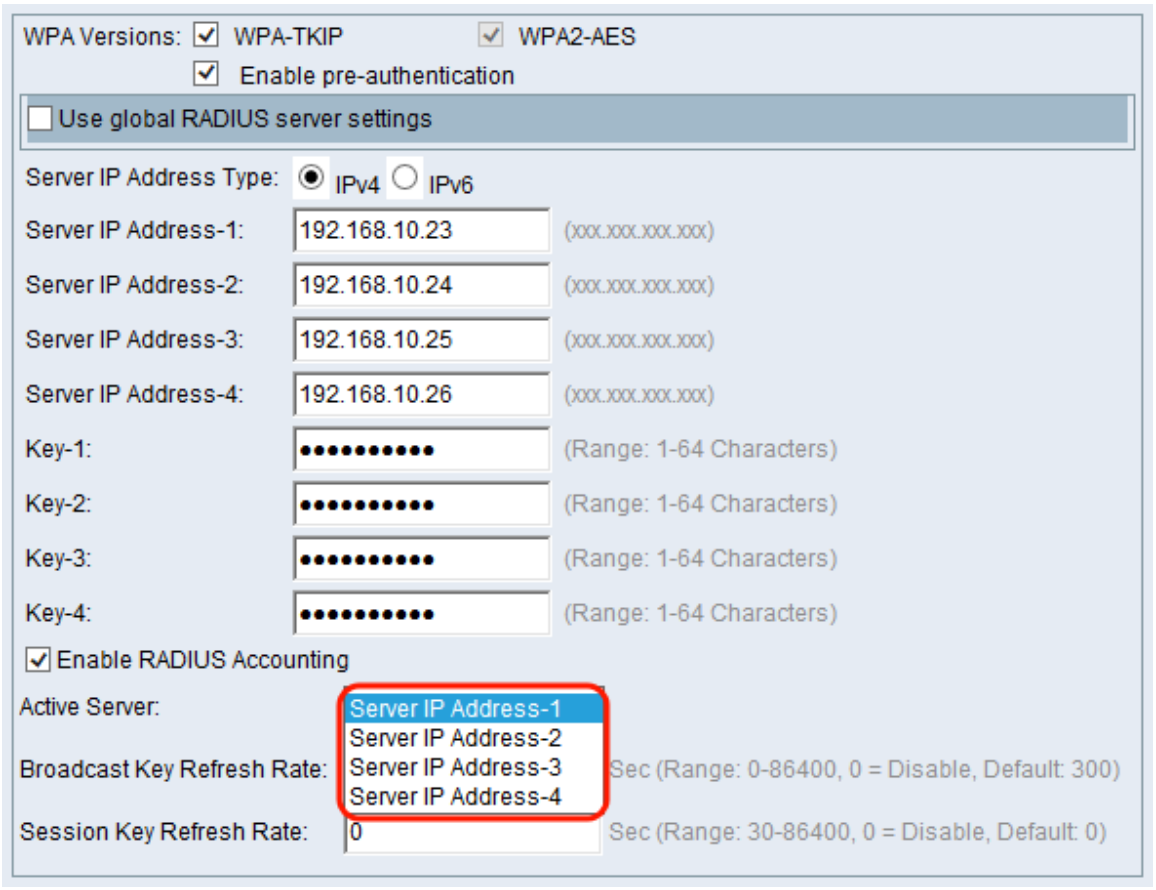
Step 8. (Optional) In the *Enable RADIUS Accounting* field, check the check box if you want to enable the tracking and measuring of the resources a particular user has consumed.

Enabling RADIUS accounting will allow you to track a particular user's system time and the amount of data transmitted and received.

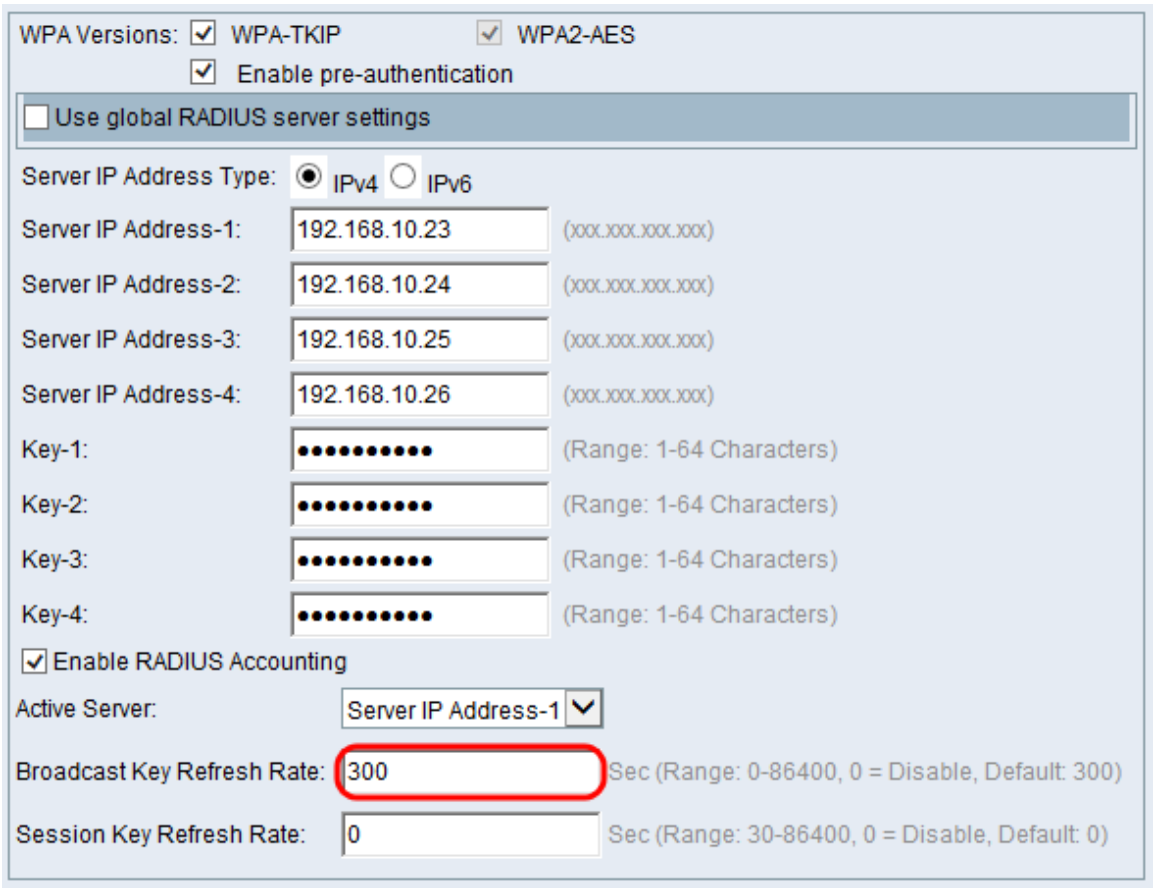


Note: If you enabled RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers.

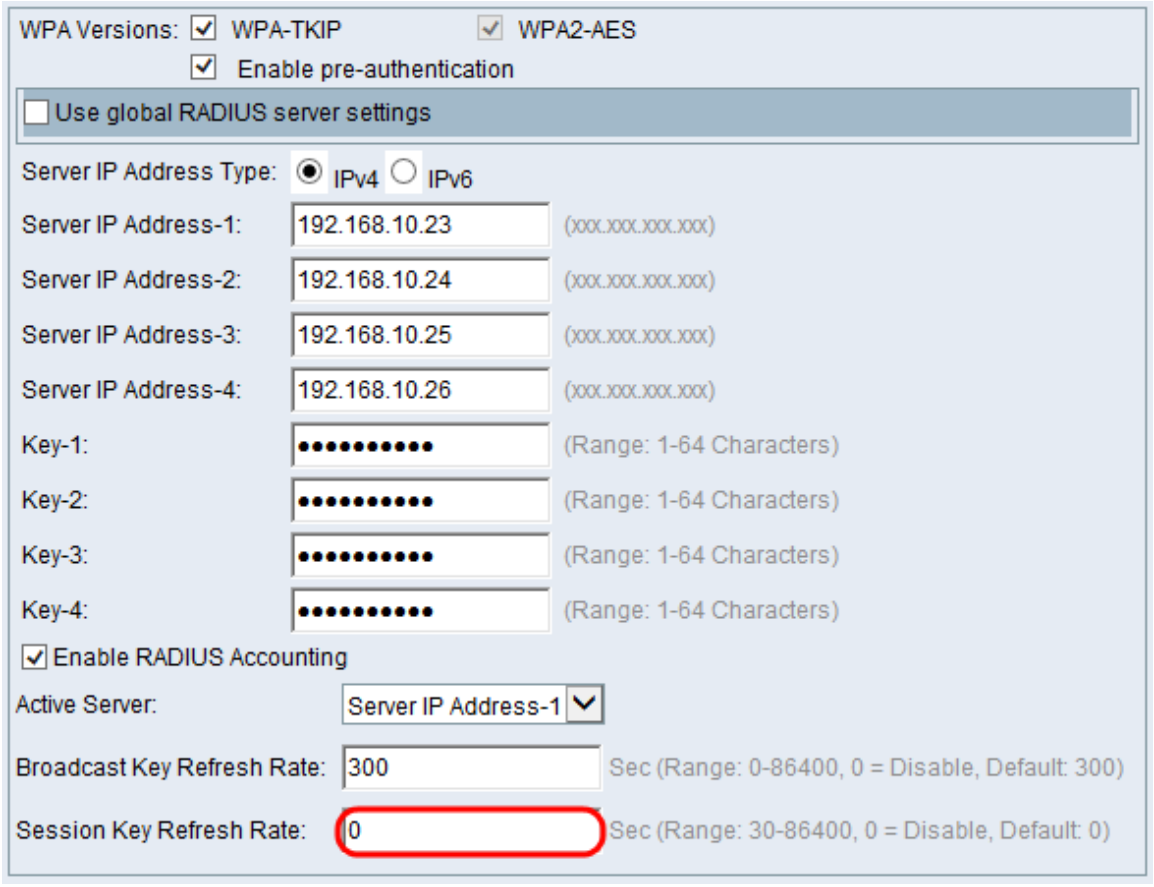
Step 9. Choose the first server that is active in the *Active Server* field. This enables manual selection of the active RADIUS server, rather than having the WAP device attempt to contact each configured server in sequence.



Step 10. In the *Broadcast Key Refresh Rate* field, enter in the interval at which the broadcast (group) key is refreshed for clients associated with this VAP. The default is 300 seconds.



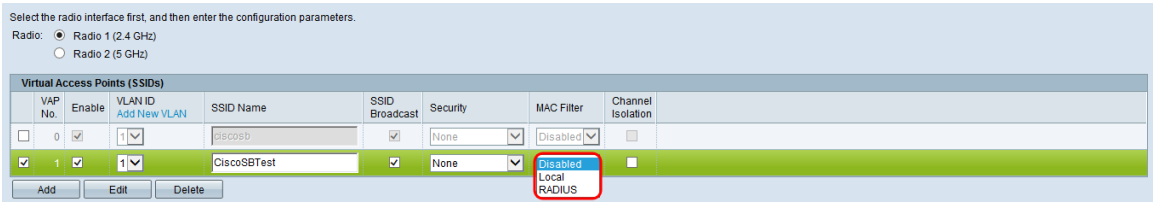
Step 11. In the *Session Key Refresh Rate* field, enter the interval at which the WAP device refreshes session (unicast) keys for each client associated with the VAP. The default is 0.



MAC Filter

MAC Filter specifies whether the stations that can access this VAP are restricted to a configured global list of MAC addresses.

Step 1. In the *MAC Filter* drop-down list, choose the desired type of MAC filtering.



The available options are defined as follows:

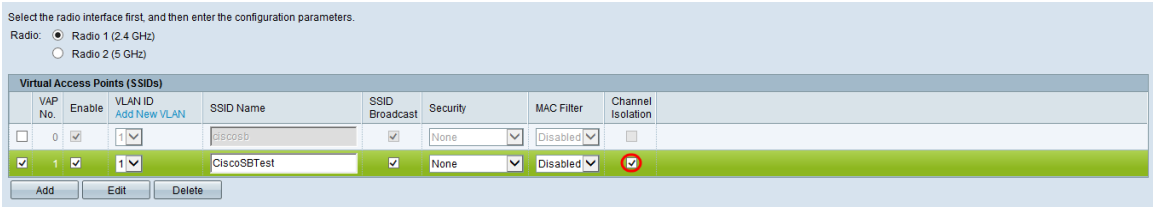
- Disabled — Does not use MAC filtering.
- Local — Uses the MAC authentication list that you configure on the MAC Filtering section, to learn more about MAC Filtering, refer to *How to configure MAC Filtering on the WAP351 and WAP131*.
- RADIUS — Uses the MAC authentication list on an external RADIUS server.

Channel Isolation

When Channel Isolation is 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.

Step 1. In the *Channel Isolation* field, check the checkbox if you want to enable Channel Isolation.



Step 2. Click **Save**.

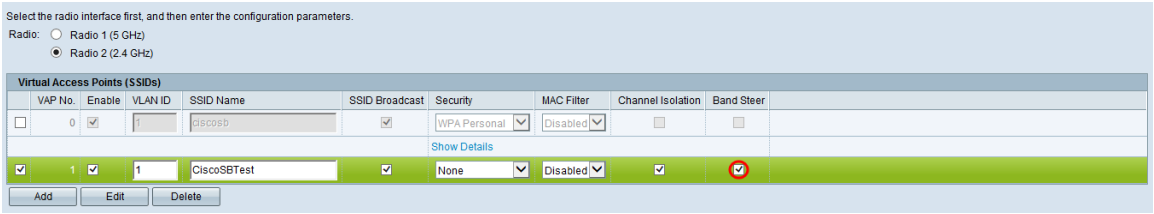
Note: After new settings are saved, the corresponding processes may be stopped and restarted. When this condition happens, the WAP device may lose connectivity. We recommend that you change the WAP device settings when a loss of connectivity will least affect your wireless clients.

Band Steer

Band Steer is only available on the WAP371. Band Steer is effectively utilizes the 5-GHz band by steering dual-band supported clients from the 2.4-GHz band to the 5-GHz band. This frees up the 2.4GHz band for use by legacy device which do not have dual radio support.

Note: Both the 5 GHz and 2.4 GHz radios need to be enabled to use Band Steer. For more information about enabling the radios refer to *How to Configure Basic Radio Settings on the WAP371*.

Step 1. Band Steer is configured on a per-VAP basis and needs to be enabled on both the radios. If you want to enable Band Steer, check the check box in the Band Steer field.

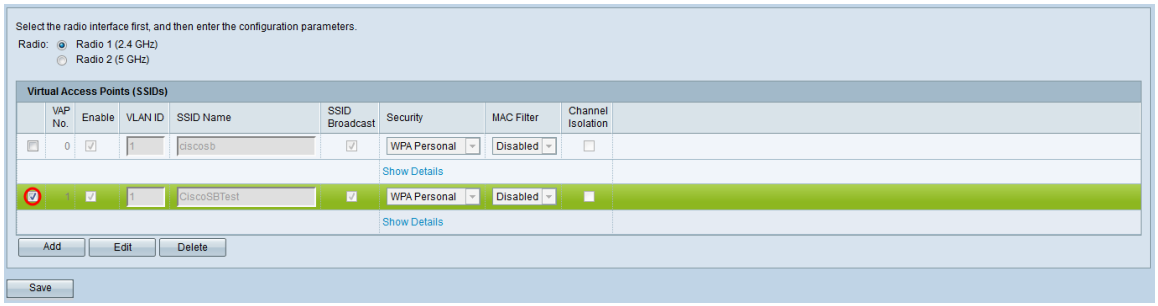


Note: Band Steer is not encouraged on VAPs with time-sensitive voice or video traffic. Even if the 5-GHz radio happens to use less bandwidth, it tries to steer clients to that radio.

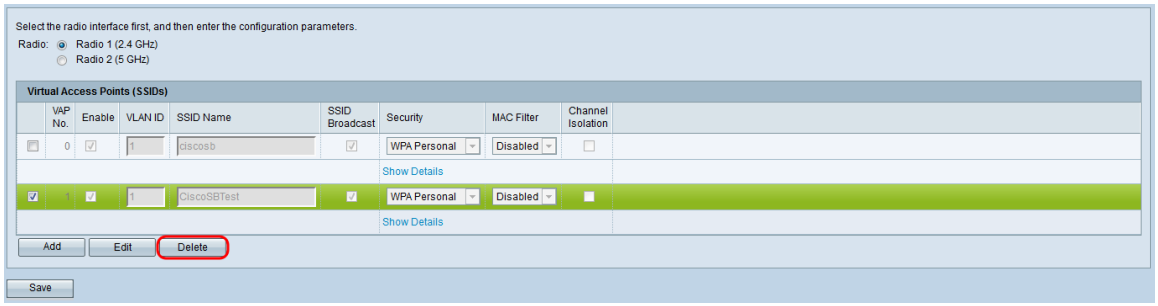
Step 2. Click **Save**.

Deleting a VAP

Step 1. Check the check box of the VAP that you want to delete.



Step 2. Click **Delete** to delete the VAP.



Step 3. Click **Save** to save your deletion permanently.