Configure Wireless Security Settings on the WAP125 and WAP581

Objective

Wireless Security allows you to protect the wireless network from unauthorized access. The WAP125 and WAP 581 access points supports Static Wired Equivalent Protection (WEP), Wi-Fi Protected Access (WPA) Personal, and WPA Enterprise. These settings can be configured per Virtual Access Point (VAP). Putting these settings in place provides network security per VAP. It is typically configured when the access point is first deployed, or when updates are made to the wireless security settings of the network.

This article aims to show you how to configure wireless security on a WAP125 or WAP581 access point.

Applicable Devices

- WAP125
- WAP581

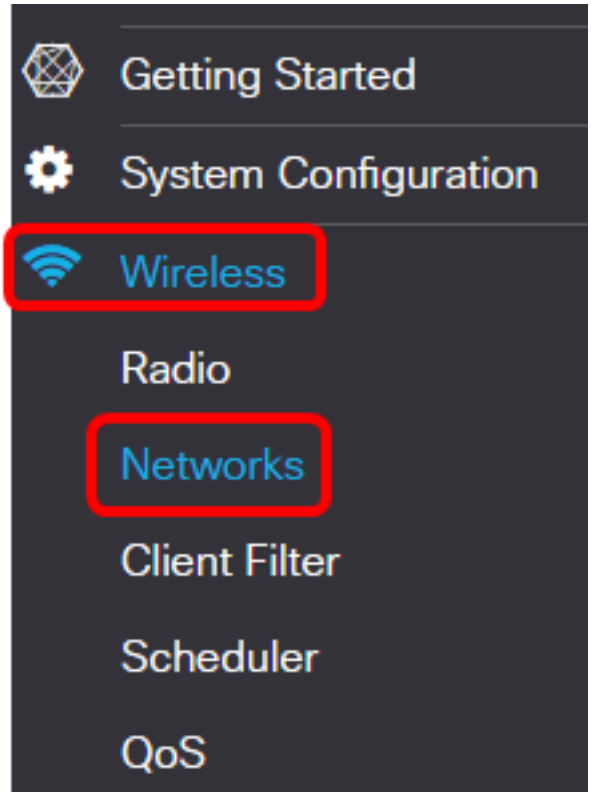
Software Version

- WAP125 - 1.0.0.3
- WAP581 - 1.0.0.4

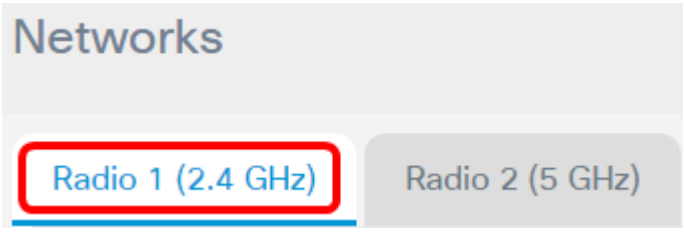
Configure Wireless Security Settings

Configure WPA Personal Security

Step 1. Log in to the web-based utility of the WAPand choose **Wireless > Networks**.

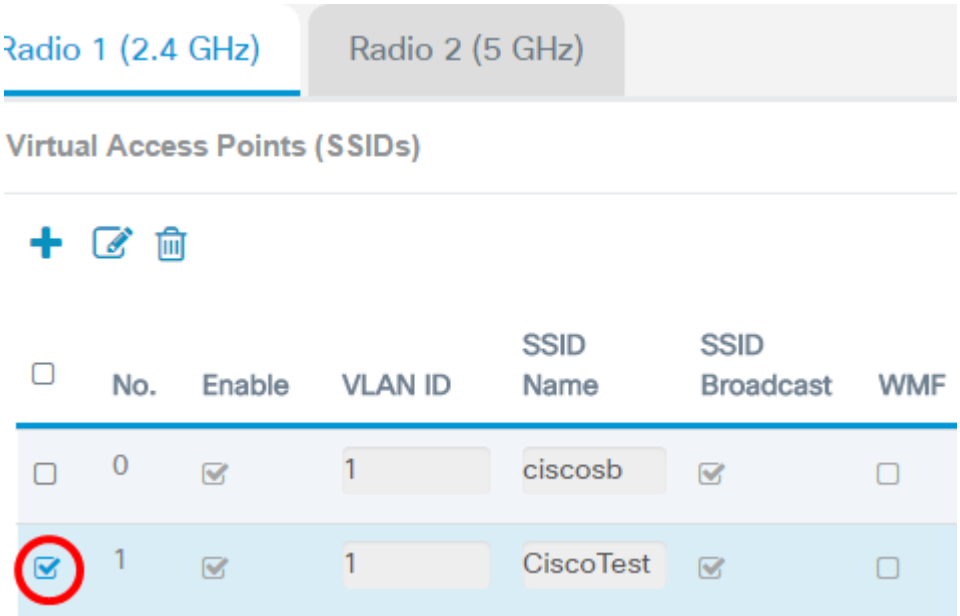


Step 2. Choose the Radio whose wireless security settings need to be configured.



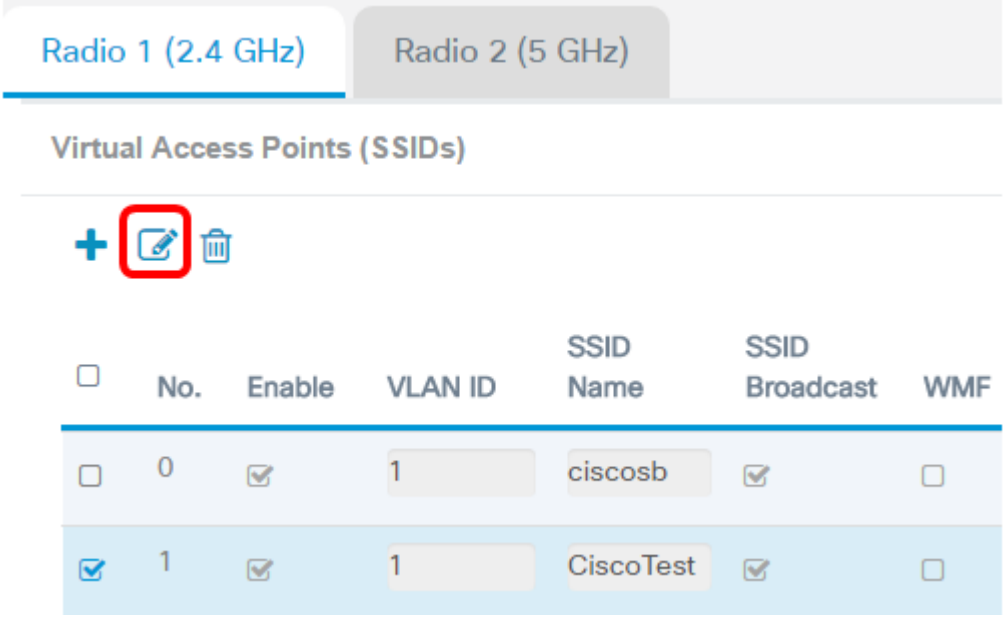
Note: In this example, Radio 1 (2.4 GHz) is chosen.

Step 3. Check the check box for the VAP whose wireless security settings need to be configured.



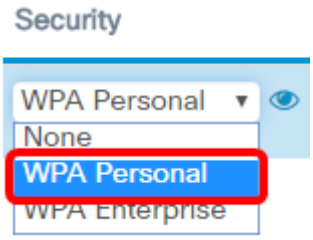
Note: In this example, VAP 1 is chosen.

Step 4. Click **Edit**.



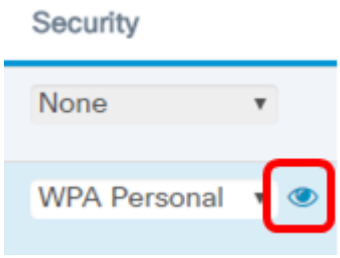
Step 5. Choose a security mode from the Security drop-down list. The options are:

- None — This option deactivates the wireless security settings of the selected VAP. Disabling security mode opens the wireless network and allows anybody with a wireless device to connect to your network, and its resources. While this mode is not recommended, it can be useful to networks in remote locations.
- WPA Personal — This option implements WPA security to the wireless network. It allows you to use the Temporal Key Integrity Protocol (TKIP) or the Advanced Encryption Standard (AES) algorithms. When mixed, it will allow devices that do not support the AES algorithm to connect to the network. WPA Personal allows you to use an alphanumeric password up to 64 characters long. WPA Personal is typically used in offices where a Remote Authentication Dial-In User Service (RADIUS) server is not used.
- WPA Enterprise — This option lets you combine the security features offered by WPA, while also using a RADIUS server. This is typically used in environments where a RADIUS server is used. If you choose this option, click here.



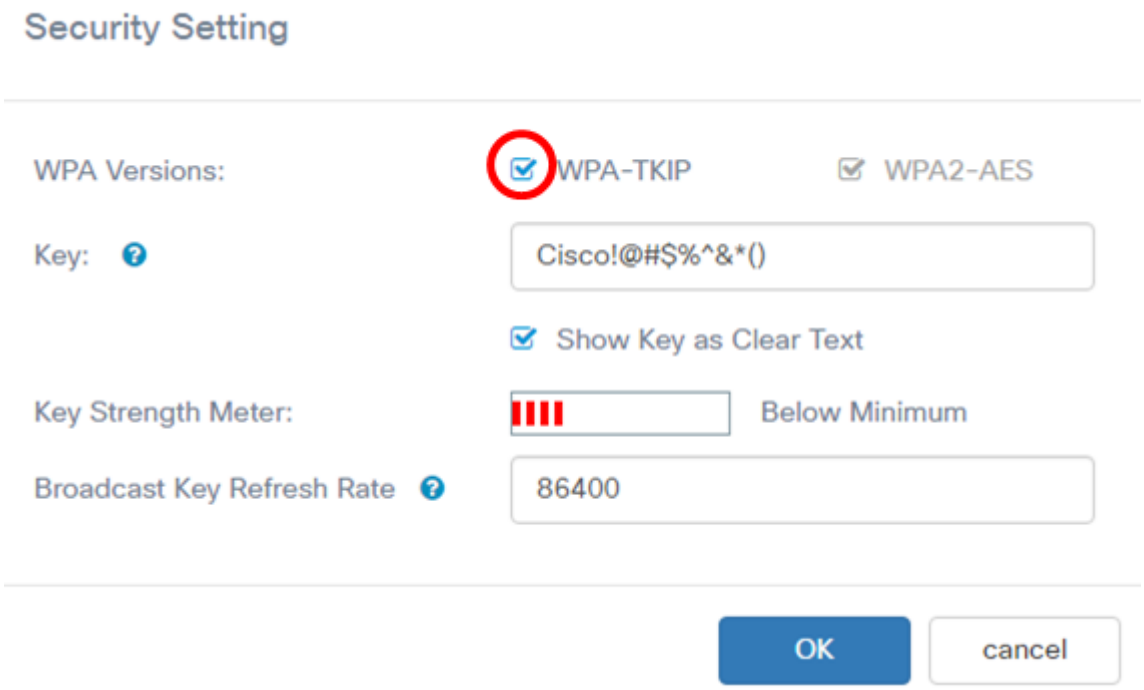
Note: In this example, WPA Personal is chosen.

Step 6. Click the view button to configure the WPA Personal parameters.



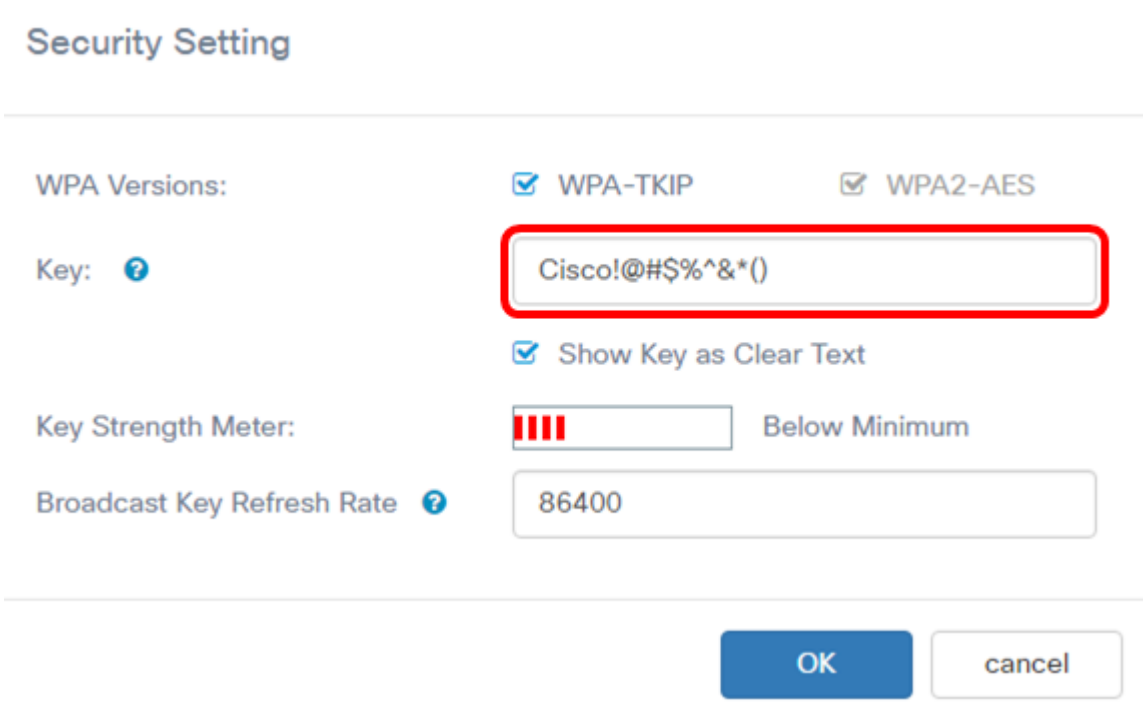
Step 7. Choose your WPA version in the WPA Versions area. The options are:

- WPA-TKIP — This option implements mixed security on the wireless network. It is ideal for networks with mixed wireless clients. This option is disabled by default.
- WPA2-AES — This option implements WPA2-AES security on the network. This is ideal for wireless networks with clients that support WPA2 security.



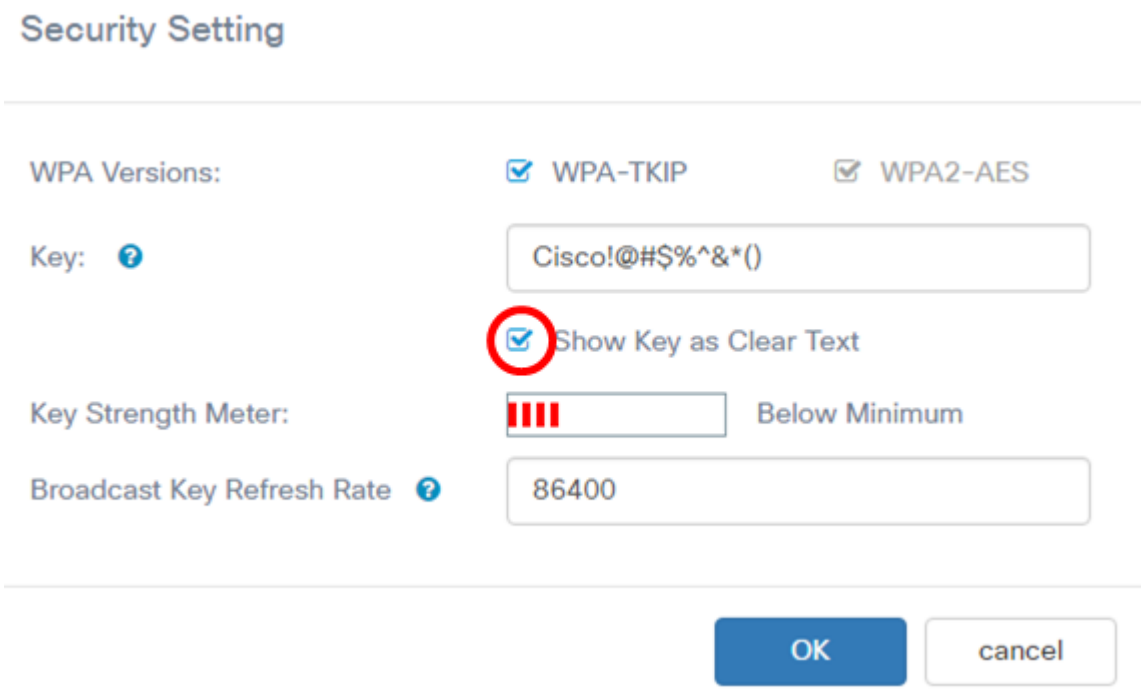
Note: In this example, WPA-TKIP is checked.

Step 8. Enter the network password in the *Key* field. The key can be a combination of letters and numbers, from 8 to 63 characters in length.



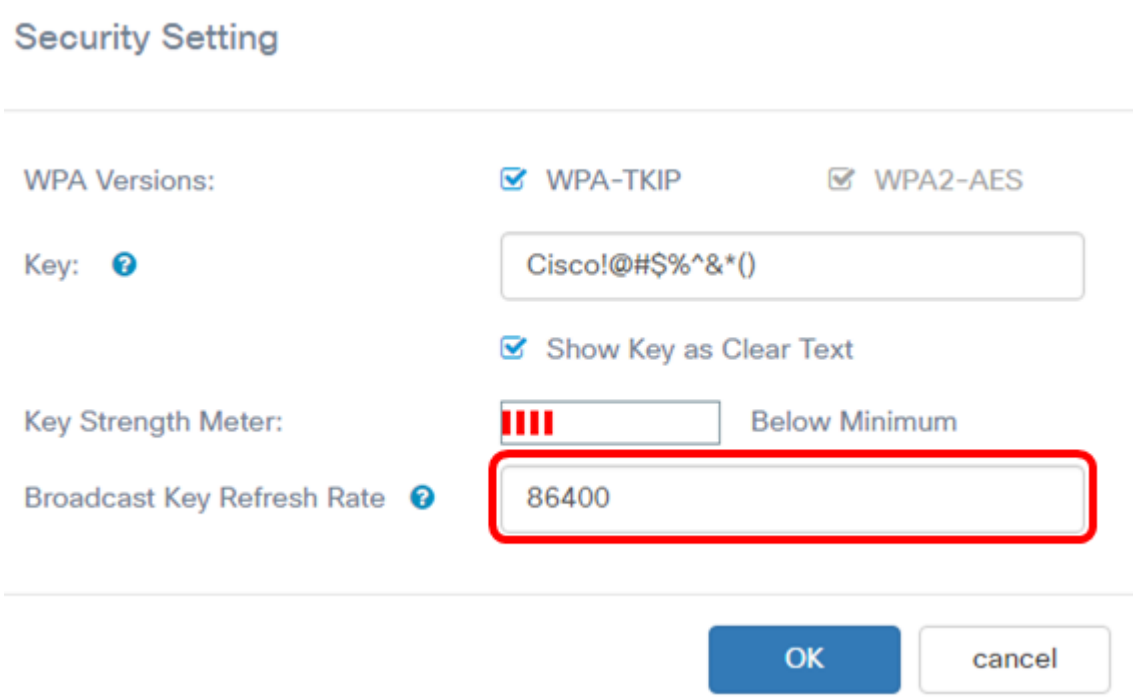
Note: In this example, Cisco!@#$%^&*() is entered.

Step 9. (Optional) Check the **Show Key as Clear Text** check box to view the Key in plain text.

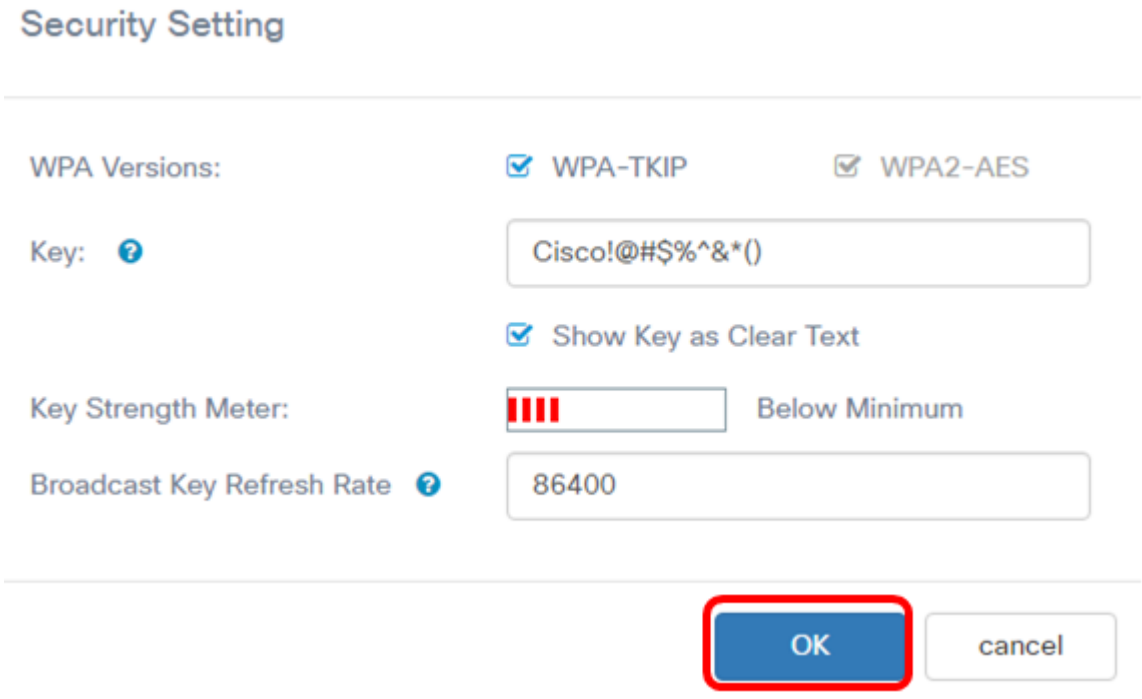


Note: In this example, Show Key as Clear Text is checked.

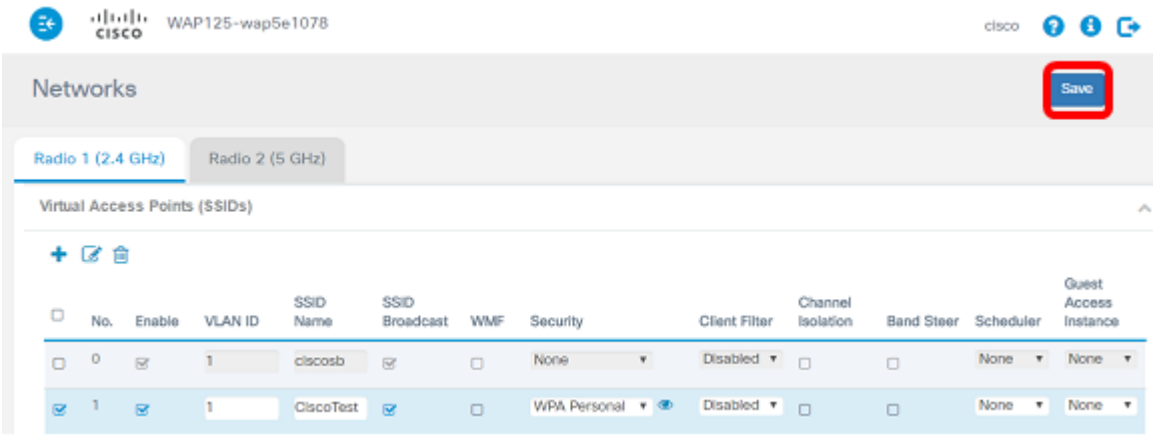
Step 10. Enter the number of seconds until your security key is replaced with a newly generated key in the *Broadcast Key Refresh Rate* field. The default value is 86400.



Step 11. Click **OK**.



Step 12. Click **Save**.

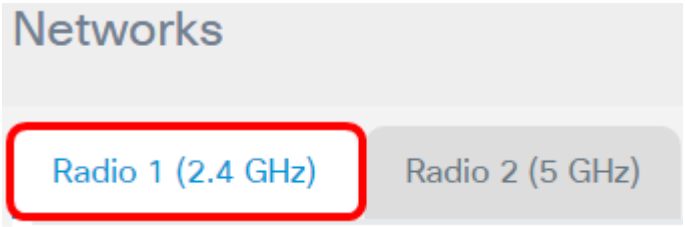


Step 13. Click **OK**.

The WPA Personal wireless security settings have now been configured on your WAP125.

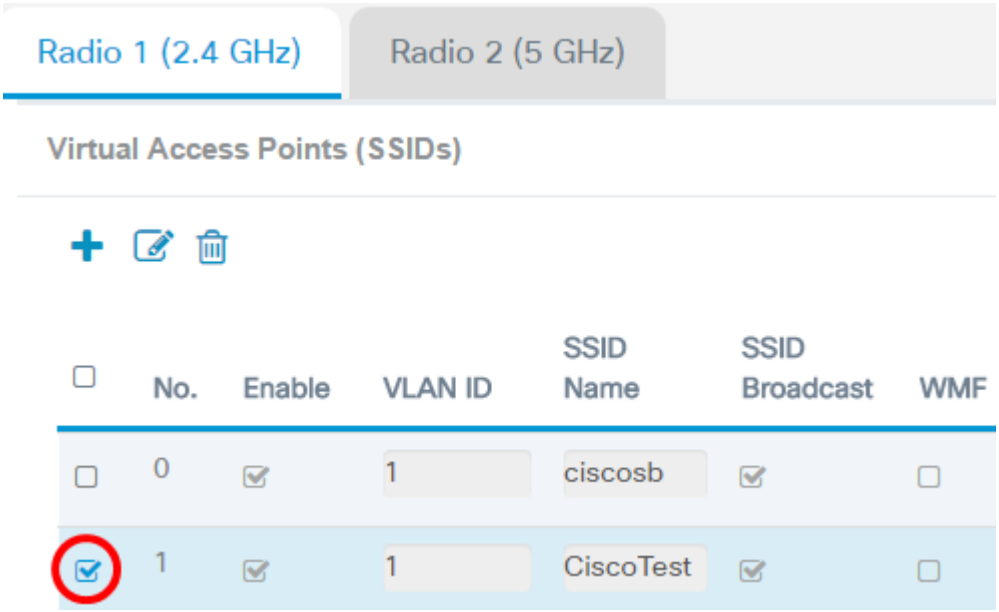
Configure WPA Enterprise Security

Step 1. Choose the Radio whose wireless security settings need to be configured.



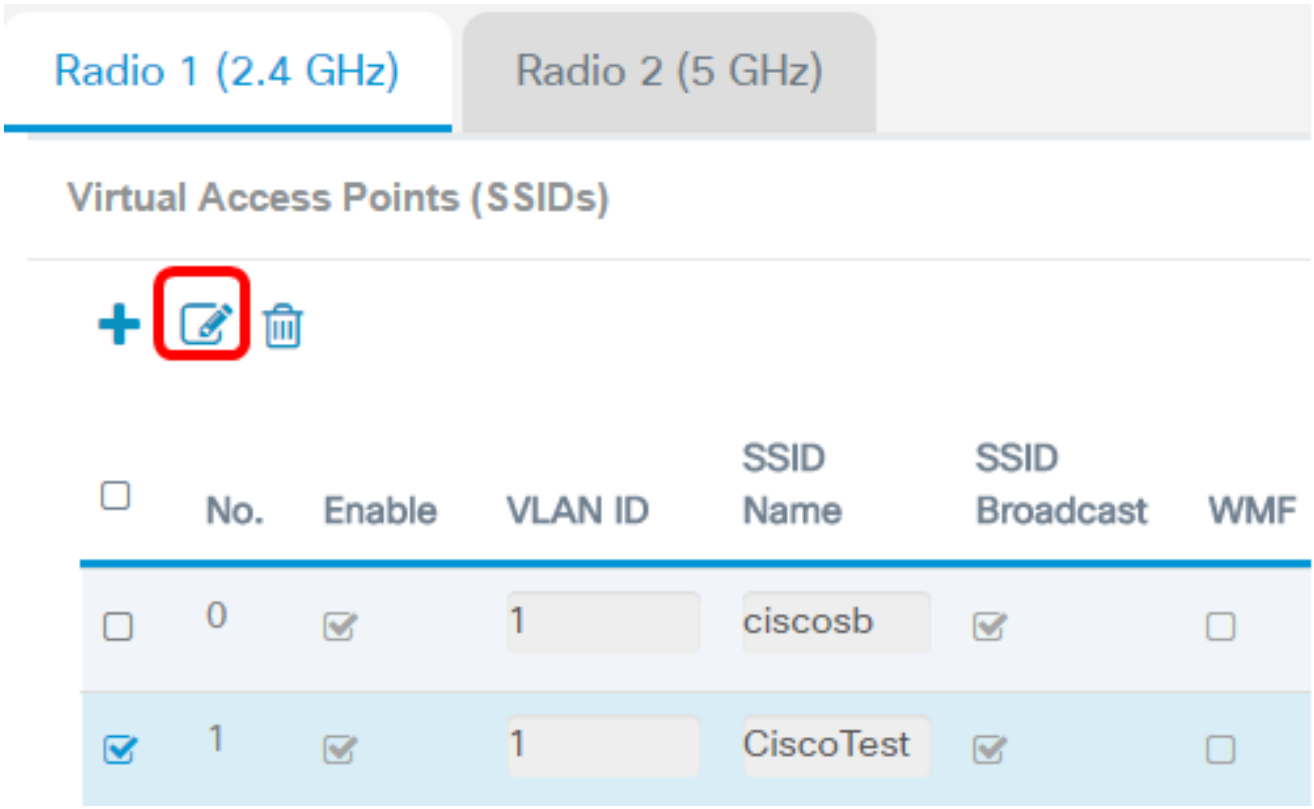
Note: In this example, Radio 1 (2.4 GHz) is chosen.

Step 2. Check the check box for the VAP whose wireless security settings need to be configured.

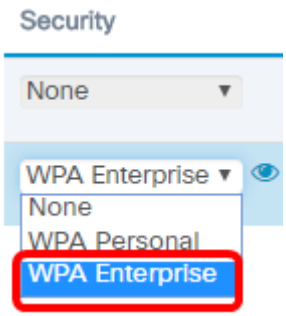


Note: In this example, VAP 1 is chosen.

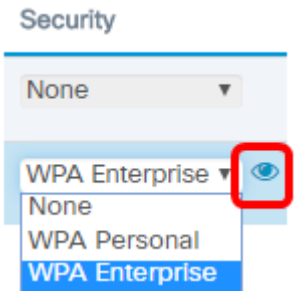
Step 3. Click **Edit**.



Step 4. Choose WPA Enterprise from the Security drop-down list.

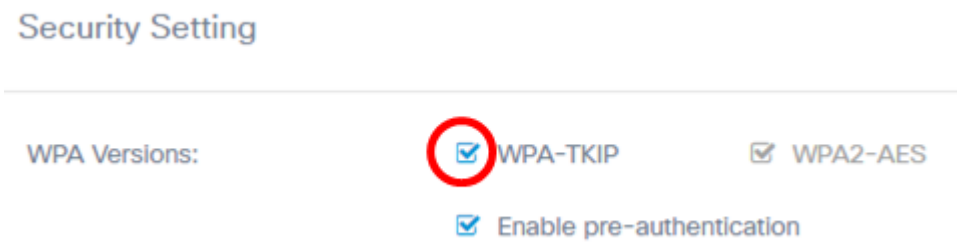


Step 5. Click the view button to configure the WPA Enterprise parameters.



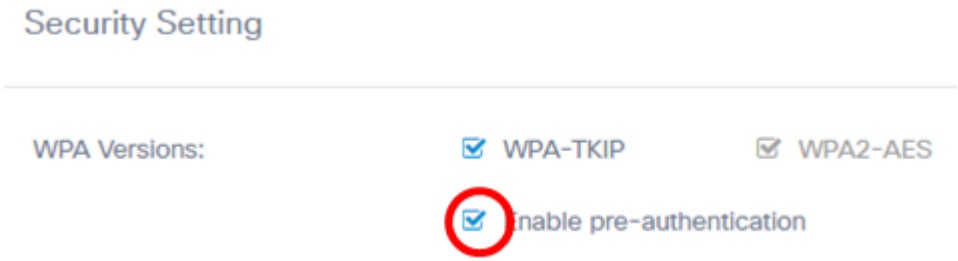
Step 6. Choose your WPA version in the WPA Versions area. The options are:

- WPA-TKIP — This option implements mixed security on the wireless network. It is ideal for networks with mixed wireless clients. This option is disabled by default.
- WPA2-AES — This option implements WPA2-AES security on the network. This is ideal for wireless networks with clients that support WPA2 security.

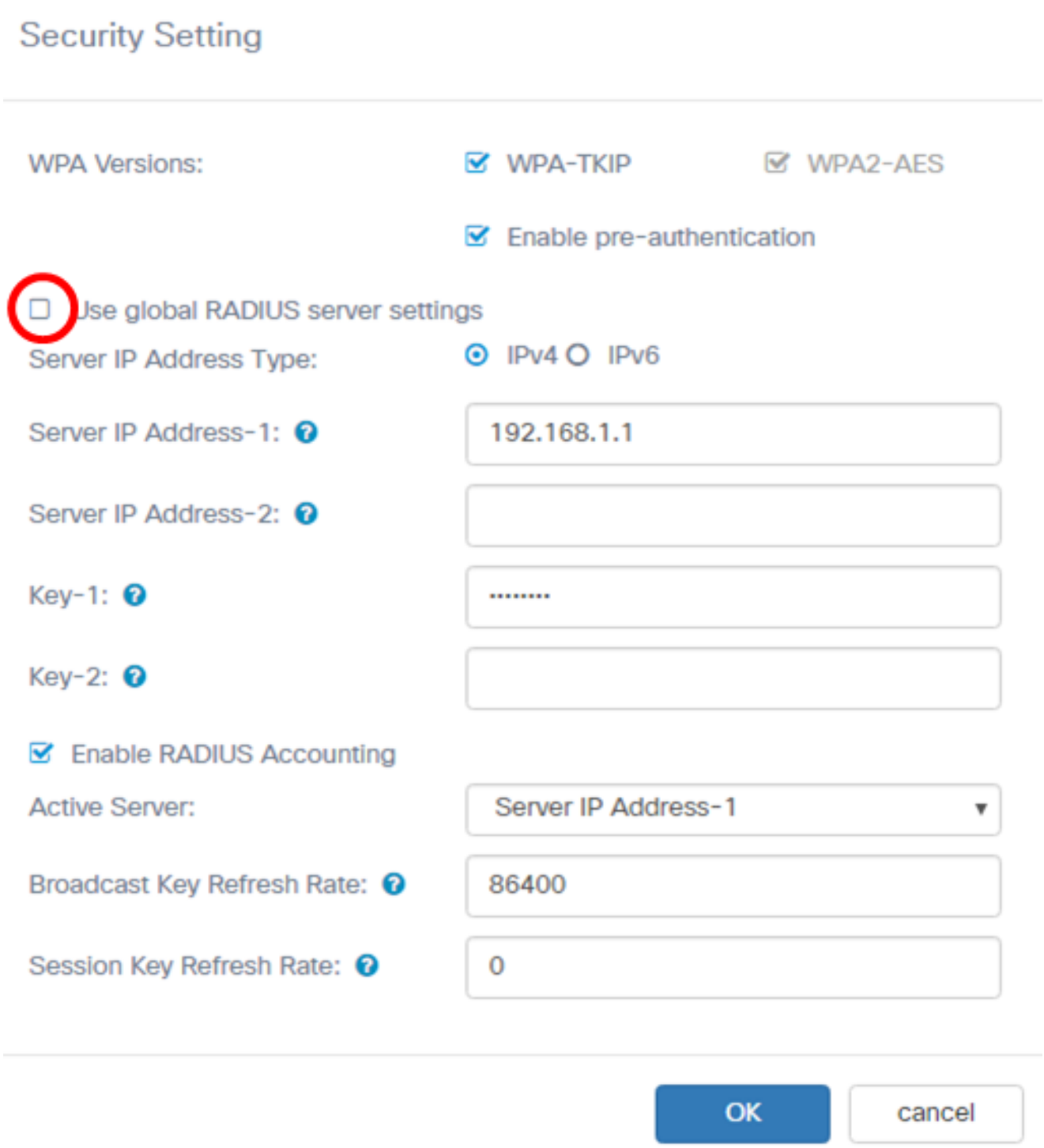


Note: In this example, WPA-TKIP is checked.

Step 7. (Optional) Check the **Enable pre-authentication** check box to activate the feature. When checked, the pre-authentication information is relayed from the WAP that the wireless client is currently connected to the target WAP. Enabling this feature can help speed up the authentication for roaming clients who connect to multiple Access Points. When security mode is disabled, this option is also disabled and cannot be edited.



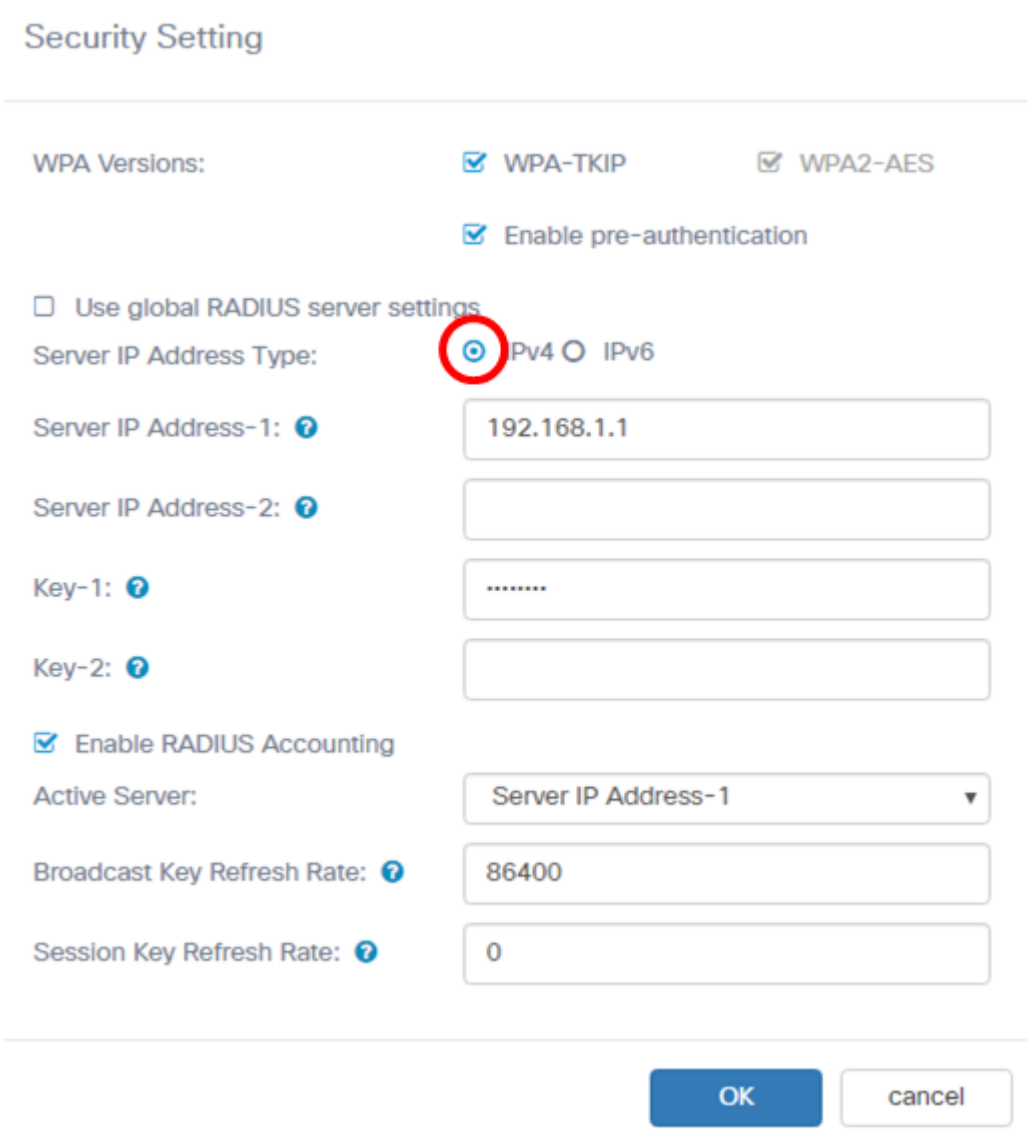
Step 8. (Optional) Uncheck the Use global RADIUS server settings check box to be able to specify a different set of RADIUS servers. By default, each VAP uses the global RADIUS settings defined for the WAP.



Note: In this example, Use global RADIUS server settings is not checked. If this is checked, proceed to Step 17.

Step 9. (Optional) Choose a Server IP Address Type. The options are:

- IPv4 — This option lets the WAP contact the IPv4 RADIUS server.
- IPv6 — This option lets the WAP contact the IPv6 RADIUS server.



Note: In this example, IPv4 is chosen.

Step 10. (Optional) Enter the primary RADIUS server IP address for the VAP in the *Server IP Address -1* field.

Note: In this example, 192.168.1.1 is entered.

Step 11. (Optional) Enter the backup RADIUS server IP address for the VAP in the *Server IP Address -2* field.

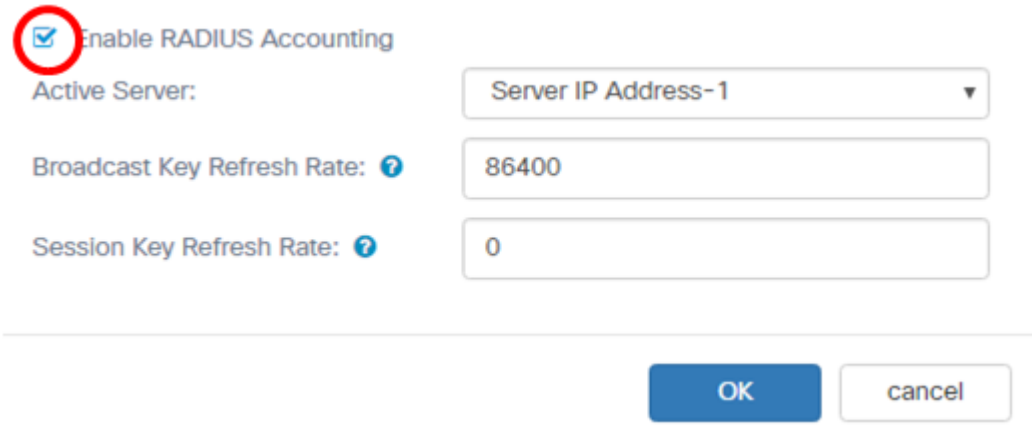
Note: In this example, no backup IP address is entered.

Step 12. (Optional) Enter a password for the primary server address in the *Key-1* field.

Step 13. (Optional) Enter a password for the backup server address in the *Key-2* field.

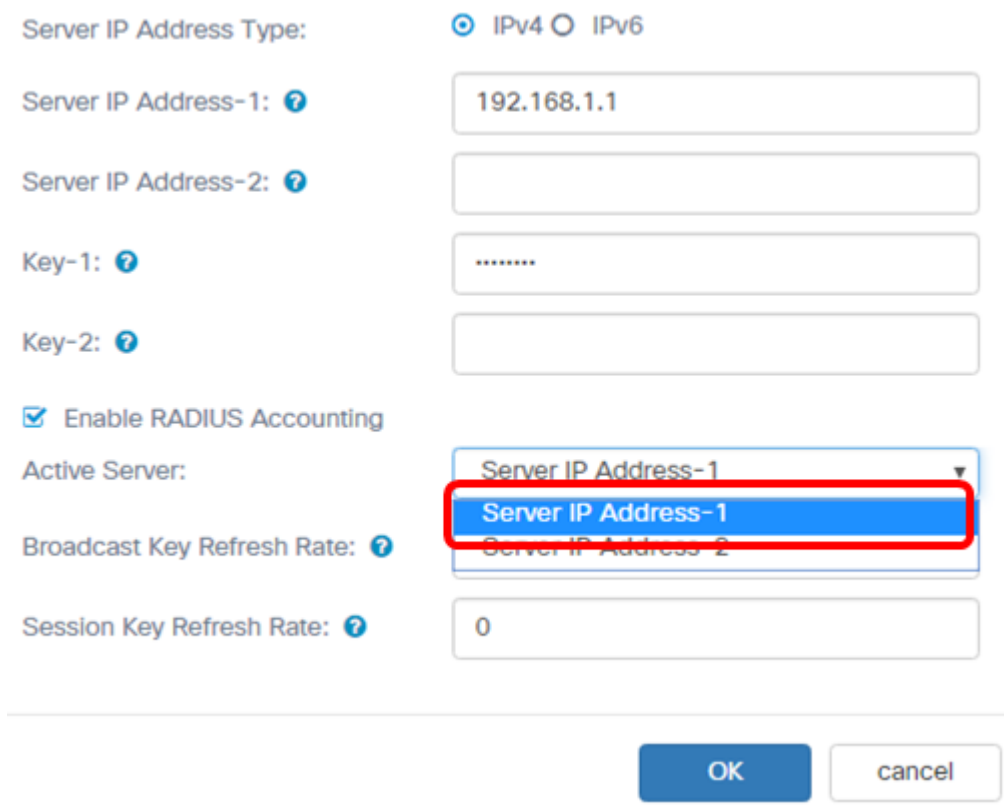
Note: In this example, no password is entered.

Step 14.(Optional) Check the **Enable RADIUS Accounting** check box. This option tracks and measures the resources a particular user has consumed such as system time and amount of data transmitted and received. When enabled, it will be enabled for the primary and backup servers.



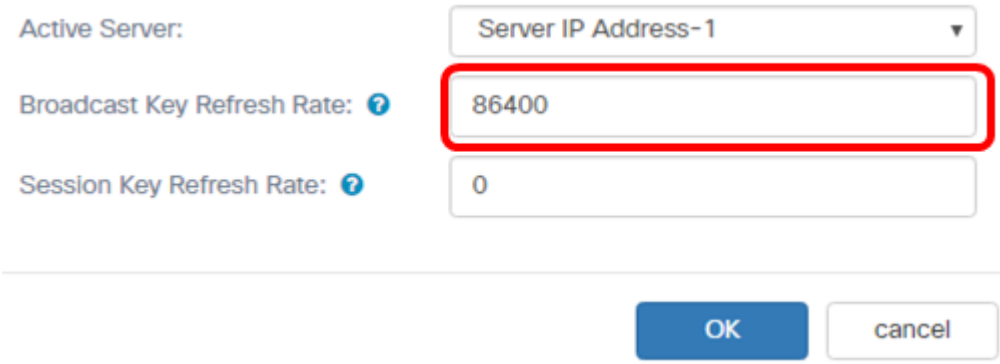
Note: In this example, Enable RADIUS Accounting is checked.

Step 15. (Optional) Choose an active server from the Active Server drop-down list.



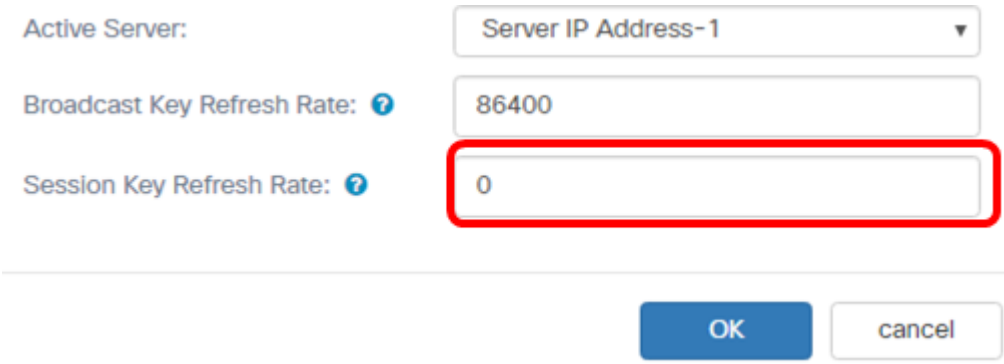
Note: In this example, Server IP Address-1 is chosen.

Step 16. (Optional) Enter the number of seconds until your security key is replaced with a newly generated key in the *Broadcast Key Refresh Rate* field. The default value is 86400.

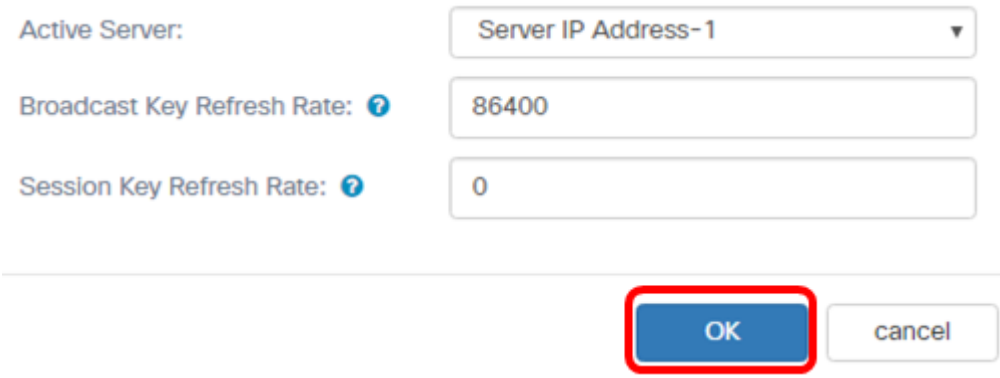


Note: In this example, the Broadcast Key Refresh Rate is left at its default value.

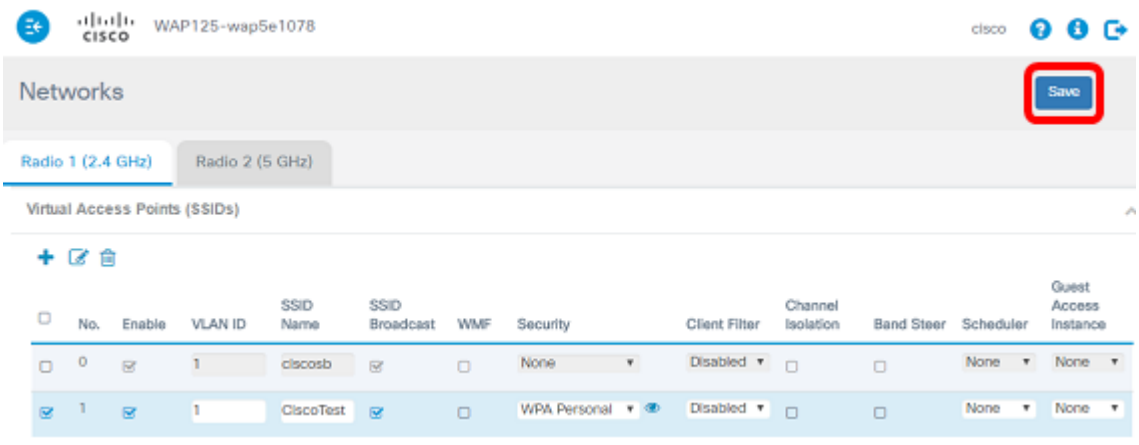
Step 17. Enter the interval at which the WAP refreshes session keys for each client associated with the VAP. It can be from 30 to 86400 seconds.



Step 18. Click **OK**.



Step 19. Click **Save**.



You should now have configured WPA Enterprise security on your wireless network.

View a video related to this article...

Click here to view other Tech Talks from Cisco