Configure a VAP on a WAP125 or WAP581 Access Point

Introduction

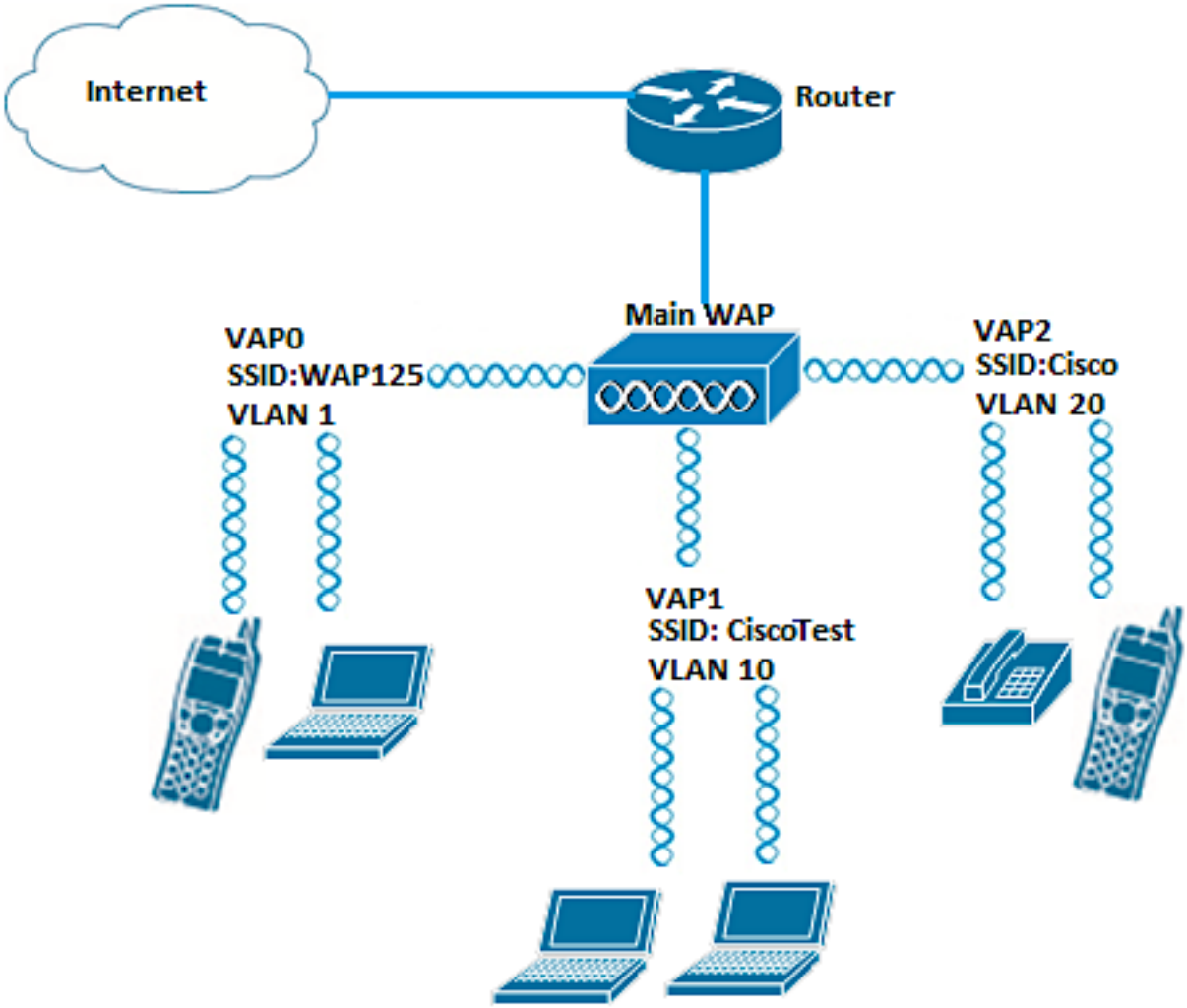
Virtual Access Points (VAPs) are virtual wireless networks that can be created in one physical access point. VAPs segment the Wireless Local Area Network (WLAN) into multiple broadcast domains. They are the equivalent of Ethernet Virtual Local Area Networks (VLANs). VAPs simulate up to four access points in the WAP125 and up to 16 access points in the WAP581. Each VAP can be enabled or disabled, except VAP0.

Note: VAP0 in VLAN ID 1 is the default VAP.

Why do we configure a VAP on the WAP?

Configuring the VAP of the access point allows the WAP to extend its capabilities and match the settings of a network. This is typically done when the device is first deployed, or after the device has been reset to its factory default settings. Configuring a VAP means that the access point would be able to support more wireless clients through different Service Set Identifiers (SSIDs) in one physical access point.

The diagram below shows three VAPs are created in a wireless network where the main access point is the WAP125. Wireless devices are connected to each of the VAP. The VAPs serve as mini WAPs connected to the main WAP allowing the wireless devices to be connected with separate SSIDs but within one main wireless access point.



Objective

This article aims to show you how to configure the VAPs on a WAP125 or WAP581 Access Point.

Applicable Devices

- WAP125
- WAP581

Software Version

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

Configure a VAP

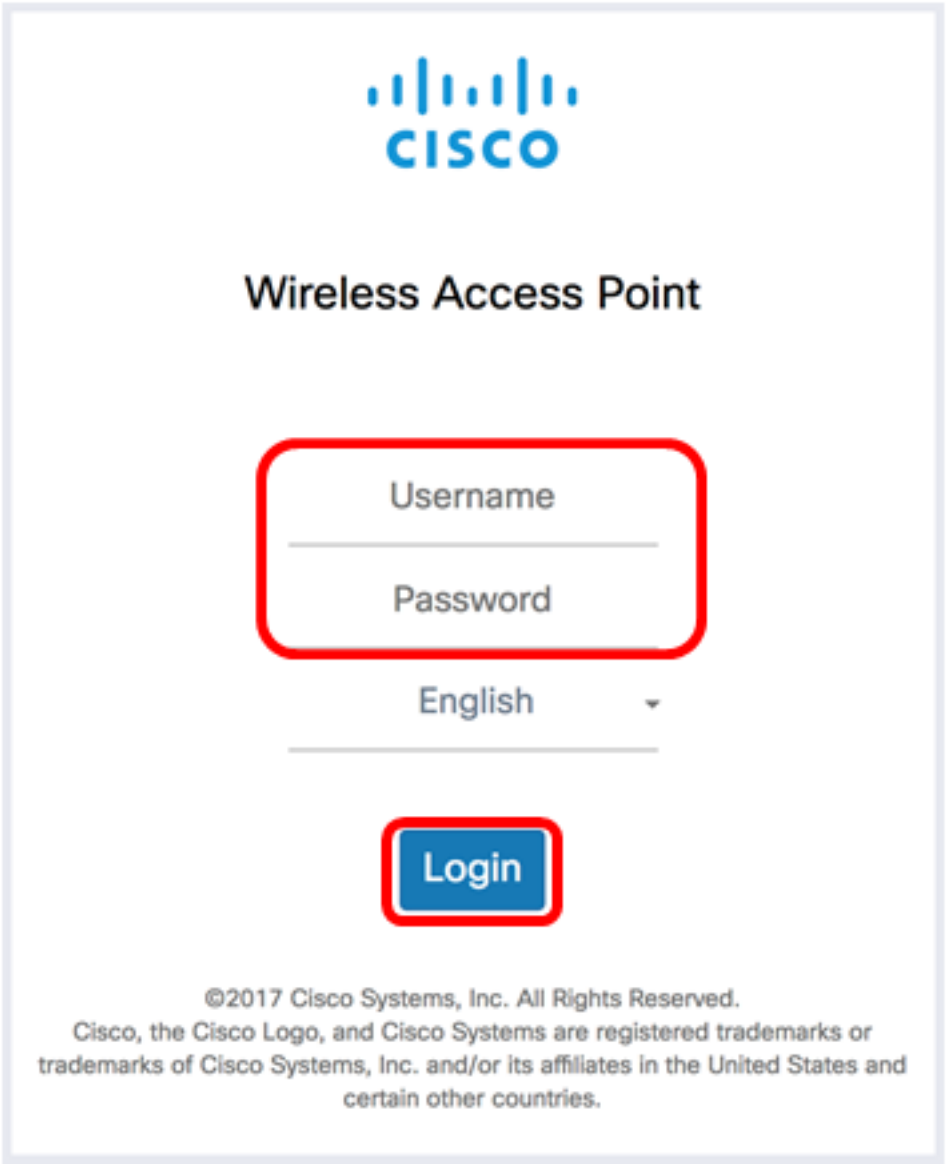
In this scenario, the default VAP0 has already been preconfigured and VAP1 in VLAN 10 with SSID CiscoTest will be added to be configured followed by VAP2 in VLAN 20 with SSID Cisco.

Note: Images may slightly vary depending on the WAP that you are using. The images

below are taken from the WAP125.

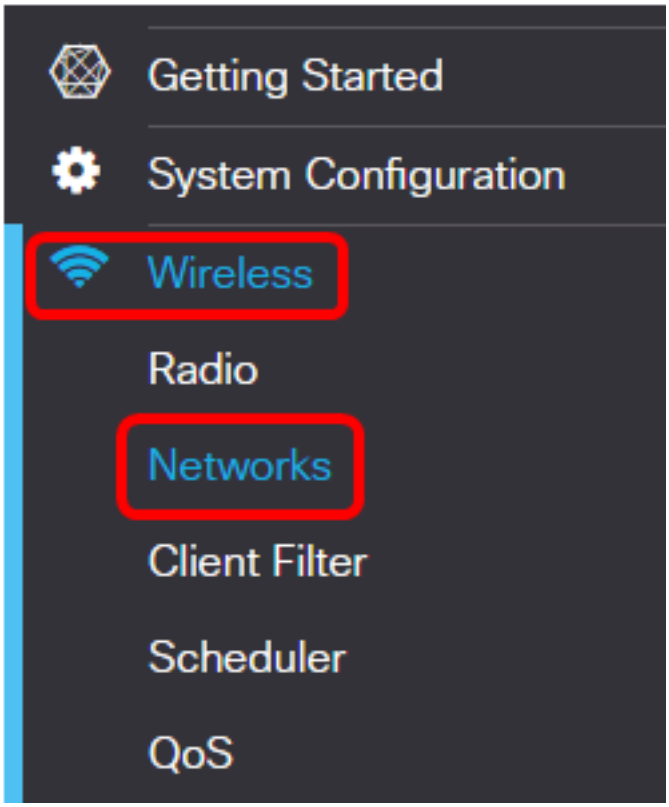
Step 1. Log in to the access point web-based utility by entering your Username and Password in the fields provided and then click **Login**.

Note: The default Username/Password for the WAP is cisco/cisco.



Note: The default username/password is cisco/cisco.

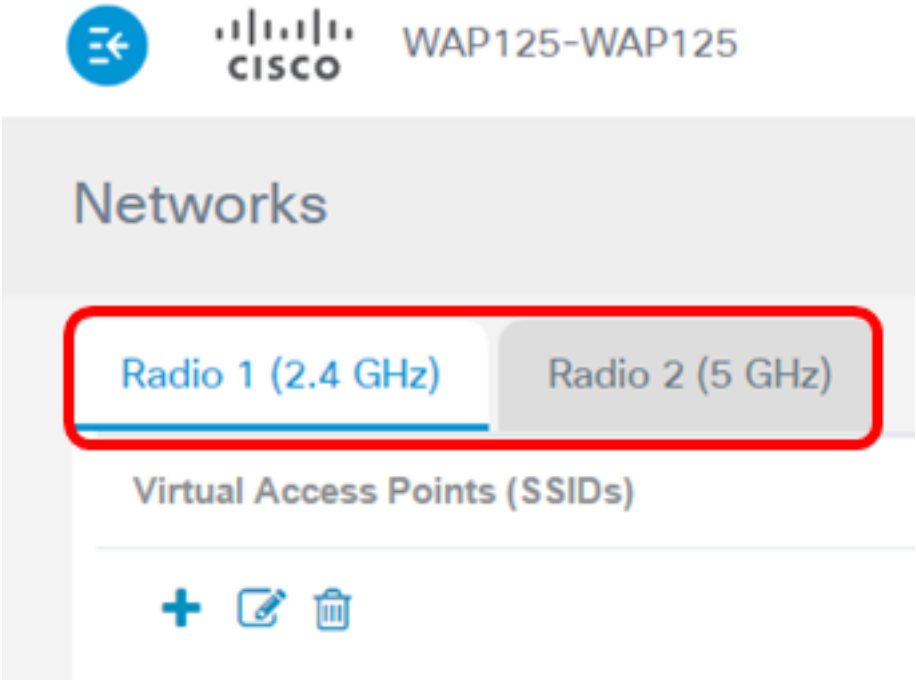
Step 2. Choose **Wireless > Networks**.



Step 3. Choose the radio interface to configure. The options are:

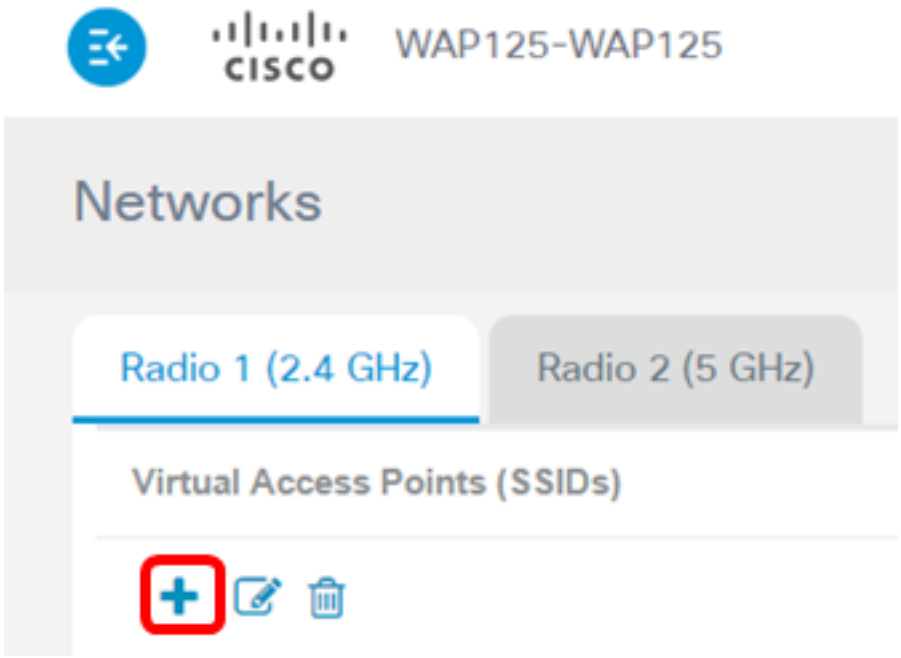
- Radio 1 (2.4 GHz) — This option will let you configure the settings of Radio 1.
- Radio 2 (5 GHz) — This option will let you configure the settings of Radio 2.

Note: If you are using the WAP581, Radio 1 is for 5 GHz and Radio 2 is for 2.4 GHz.

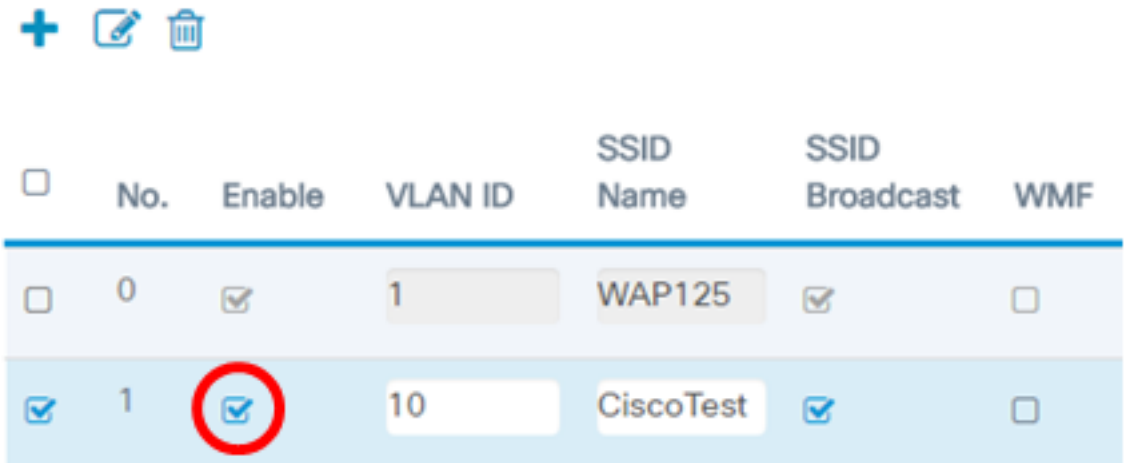


Note: In this example, Radio 1 (2.4 GHz) is chosen.

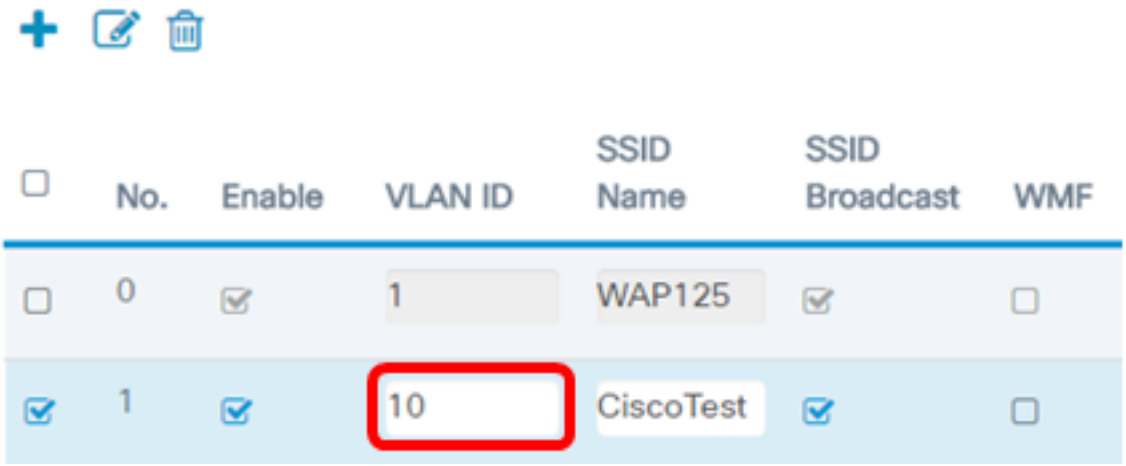
Step 4. Click the + button to add a VAP.



Step 5. Verify that the **Enable** checkbox is checked. This is checked by default.

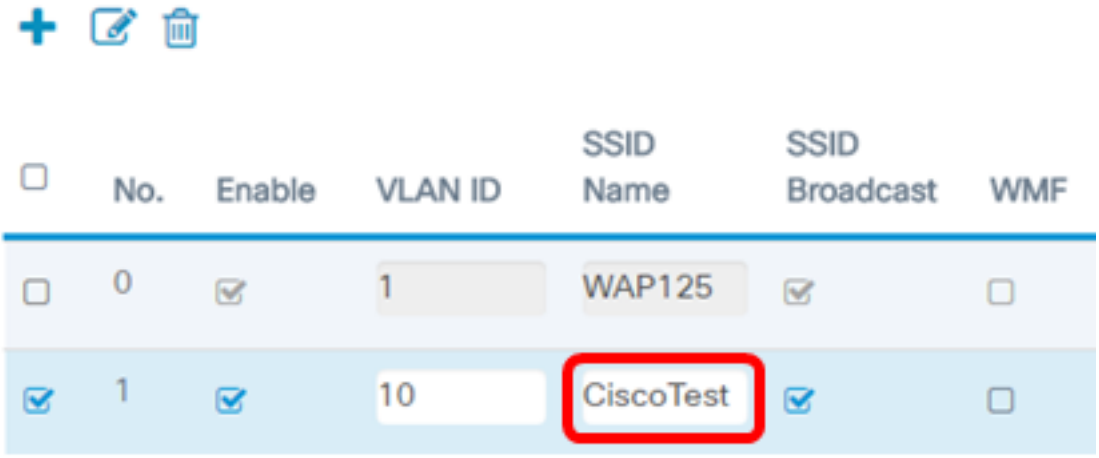


Step 6. Enter the VLAN ID that needs to be associated with the VAP.



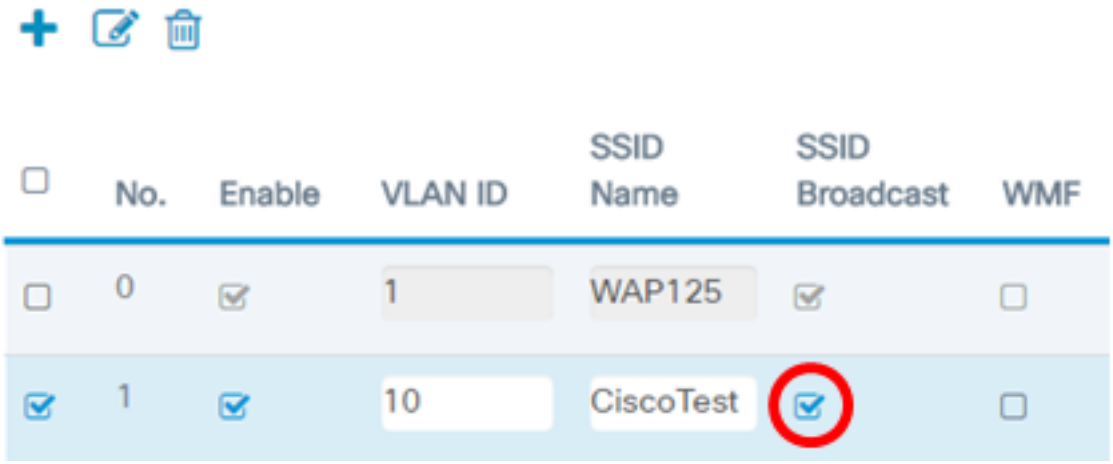
Note: In this example, the VAP will be set up for VLAN 10.

Step 7. Enter the name of the wireless network. This is also called the Service Set Identifier (SSID). It is a combination of letters and numbers up to 32 characters long.

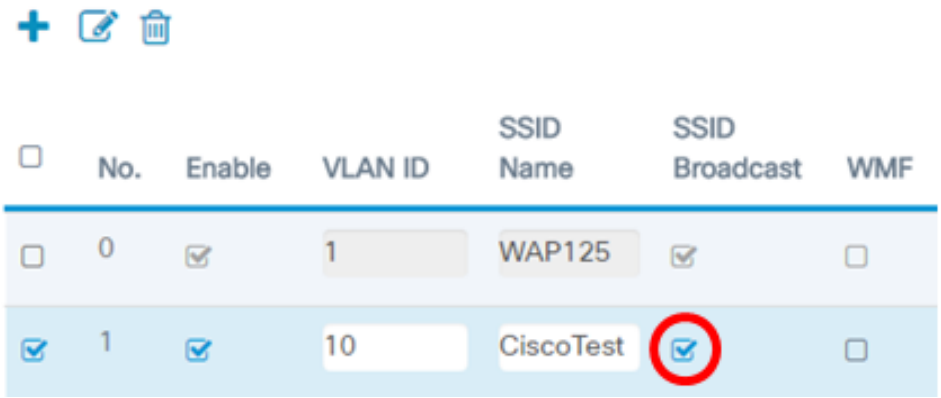


Note: In this example, CiscoTest is entered.

Step 8. Verify that SSID Broadcast is checked. This will make the SSID visible when a wireless client searches for a wireless network. This option is checked by default. Uncheck this option if you do not want the SSID visible in the list of networks. When SSID Broadcast is disabled, connecting to the wireless network must be done manually.



Step 9. (Optional) Check the Wireless Multicast Forwarding (WMF) check box to enable WMF. Enabling WMF provides an efficient way to transfer multicast traffic to the wireless devices.



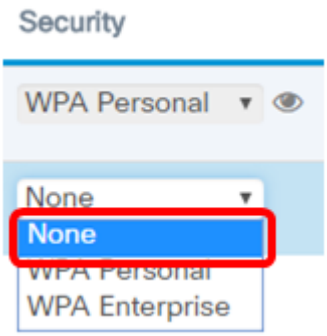
Step 10. Choose a Security type from the drop-down list. The options are:

None — This option means that wireless security is disabled on the VAP. This is not recommended as it would be prone to unauthorized access.

- WPA Personal — This option implements Wi-Fi Protected Access (WPA) Personal

security on the VAP. This is typically used in small office environments where a Remote Authentication Dial-In User Service (RADIUS) server is not required.

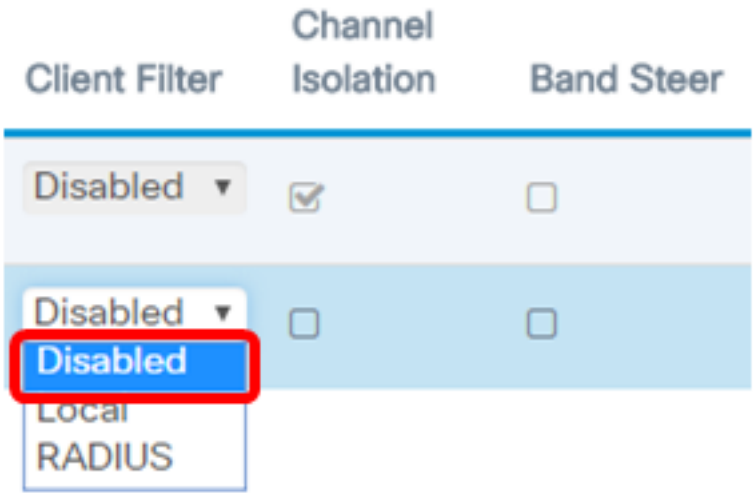
- WPA Enterprise — This option implements WPA security on the VAP. It is typically used in bigger office environments that have a RADIUS server in place.



Note: For instructions on setting up wireless security on a WAP, click here. In this example, None is chosen.

Step 11. (Optional) Choose a Client Filter mode from the drop-down list. The options are:

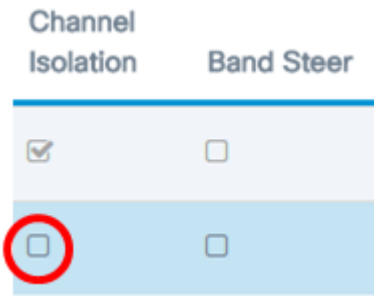
- Disabled — This option means that the Client Filter feature is disabled.
- Local — This option means that the client filter list is stored locally in the access point.
- RADIUS — This option means that the client filter list is stored in a RADIUS server.



Note: In this example, Disabled is chosen.

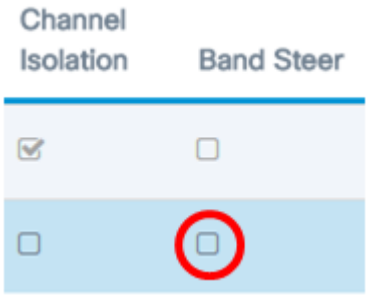
Step 12. (Optional) Check the Channel Isolation check box to enable the feature. When enabled, the WAP blocks communication between wireless clients on the same VAP. The WAP device will still allow data traffic between its wireless clients and the wired devices on the network, across a Wireless Distribution System (WDS) link, and with other wireless clients associated with another VAP.

When Channel isolation is disabled, the WAP would allow clients to communicate with one another normally.



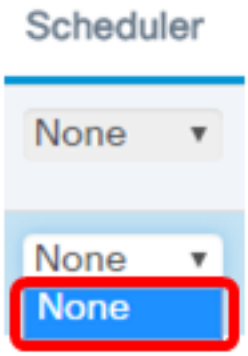
Note: In this example, Channel Isolation is disabled.

Step 13. (Optional) Check the **Band Steer** check box to enable the feature. When band steer is enabled, the WAP will utilize the 5 GHz band by steering dual-band supported clients from the 2.4 GHz band to the 5 GHz band.



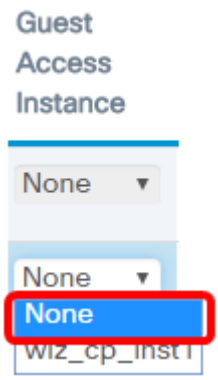
Note: In this example, Band Steer is disabled.

Step 14. (Optional) Choose a scheduler profile from the drop-down list. For instructions on setting up Scheduler, click here.



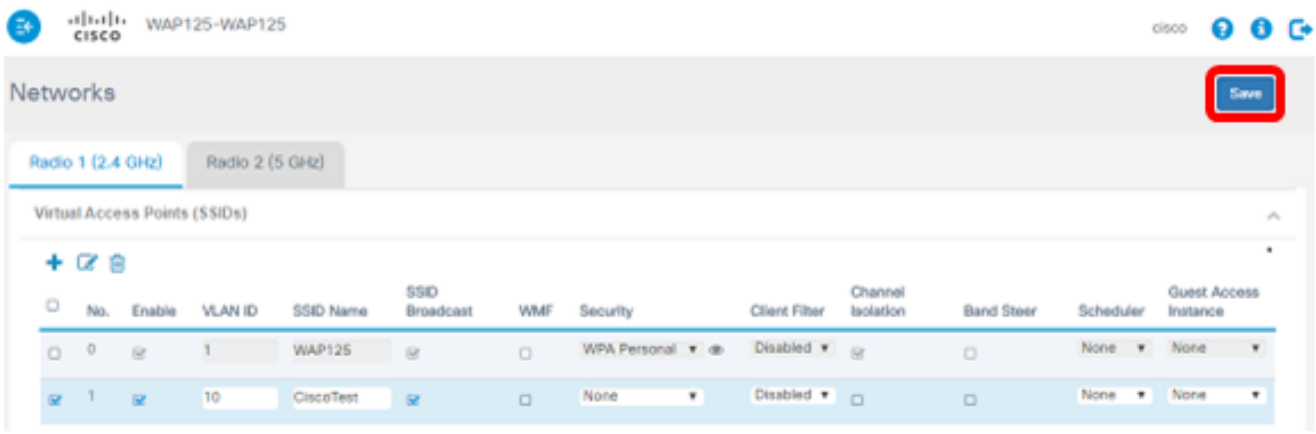
Note: In this example, there is no Scheduler profile configured on the WAP.

Step 15. (Optional) Associate a Captive Portal (CP) instance to a VAP. The settings of the CP instance associated to the VAP will apply to clients who attempt to associate on the VAP. For instructions on how to configure Guest Access Instance, click here.

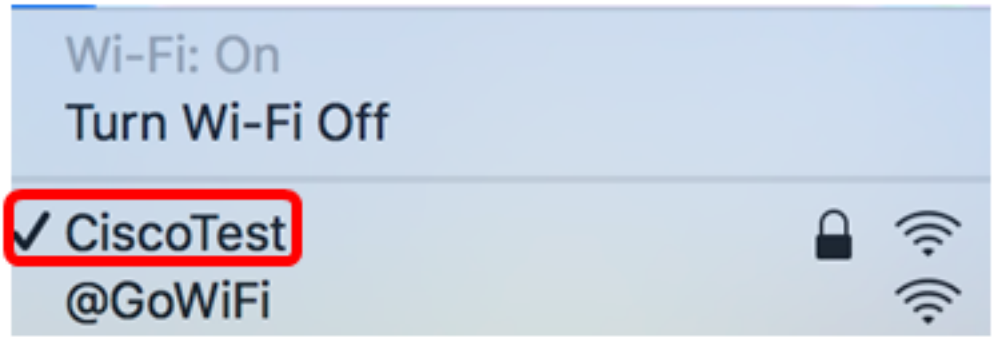


Note: In this example, None is chosen.

Step 16. Click **Save**.



Step 17. Verify that the VAP is now configured by viewing the networks in the range of your wireless computer.



Note: In this example, a Mac computer is used and it is now connected wirelessly to the newly configured CiscoTest VAP1 network.

Step 18. Repeat Step 4 to Step 17 to add and configure VAP2 in VLAN20 with SSID Cisco.

The configuration of the VAPs on your WAP is now complete.

View a video related to this article...

Click here to view other Tech Talks from Cisco