

Konfigurieren eines VAP auf einem WAP125 oder WAP581 Access Point

Einführung

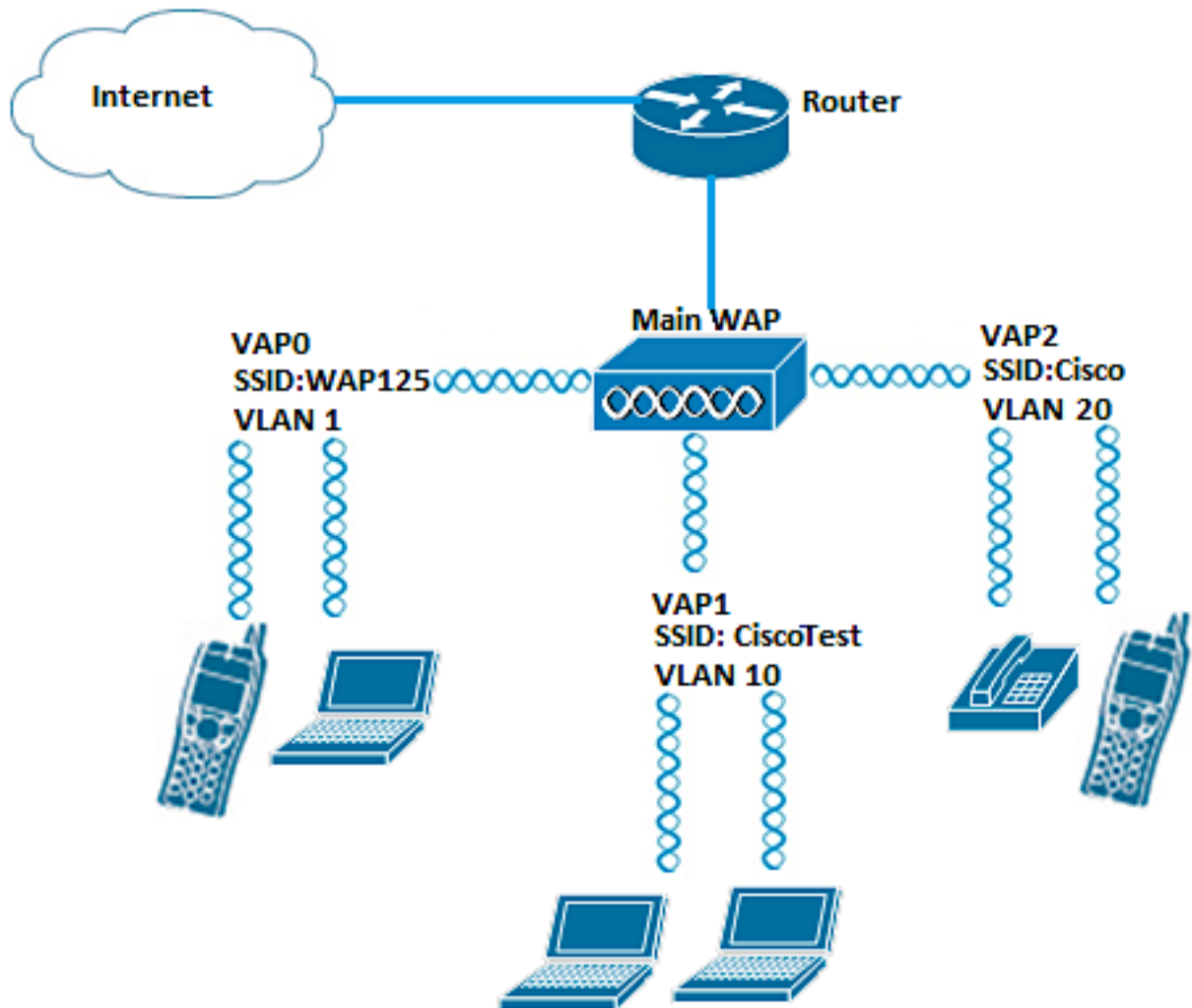
Virtual Access Points (VAPs) sind virtuelle Wireless-Netzwerke, die in einem physischen Access Point erstellt werden können. VAPs segmentieren das Wireless Local Area Network (WLAN) in mehrere Broadcast-Domänen. Sie entsprechen Ethernet Virtual Local Area Networks (VLANs). VAPs simulieren bis zu vier Access Points im WAP125 und bis zu 16 Access Points im WAP581. Jeder VAP kann aktiviert oder deaktiviert werden, mit Ausnahme von VAP0.

Hinweis: VAP0 in VLAN-ID 1 ist der Standard-VAP.

Warum konfigurieren wir eine VAP auf dem WAP?

Durch die Konfiguration des VAPs des Access Points kann der WAP seine Funktionen erweitern und den Einstellungen eines Netzwerks entsprechen. Dies geschieht in der Regel, wenn das Gerät zum ersten Mal bereitgestellt wird oder das Gerät auf die werkseitigen Standardeinstellungen zurückgesetzt wurde. Die Konfiguration eines VAP bedeutet, dass der Access Point mehr Wireless-Clients über verschiedene Service Set Identifiers (SSIDs) in einem physischen Access Point unterstützen kann.

Das folgende Diagramm zeigt drei VAPs, die in einem Wireless-Netzwerk erstellt werden, in dem der Hauptzugangspunkt der WAP125 ist. Wireless-Geräte sind mit jedem VAP verbunden. Die VAPs dienen als Mini-WAPs, die mit dem WAP verbunden sind, sodass die Wireless-Geräte mit separaten SSIDs verbunden werden können, jedoch innerhalb eines zentralen Wireless Access Points.



Ziel

In diesem Artikel erfahren Sie, wie Sie die VAPs auf einem WAP125 oder WAP581 Access Point konfigurieren.

Anwendbare Geräte

- WAP125
- WAP581

Softwareversion

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

Konfigurieren eines VAP

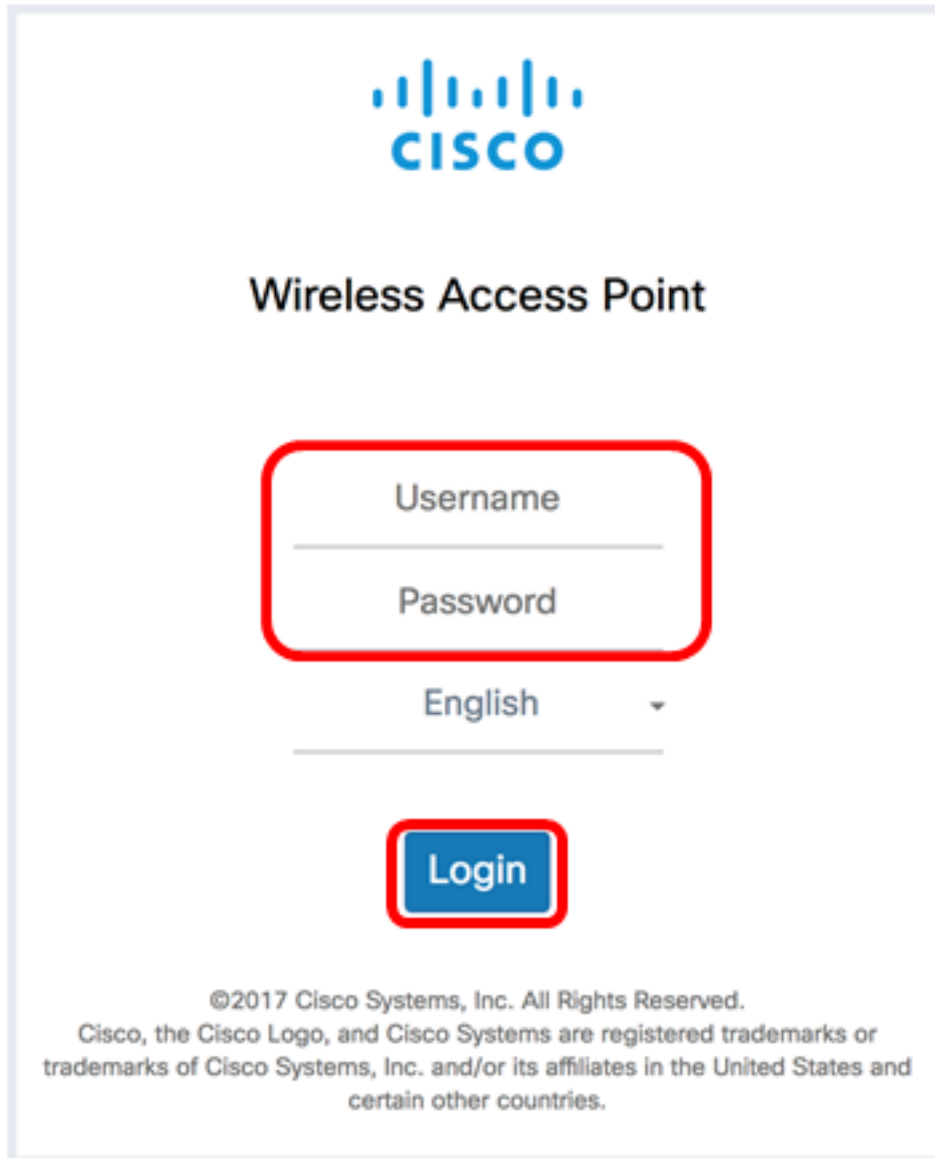
In diesem Szenario wurde VAP0 bereits vorkonfiguriert, und VAP1 in VLAN 10 mit SSID CiscoTest wird hinzugefügt, um konfiguriert zu werden, gefolgt von VAP2 in VLAN 20 mit SSID Cisco.


Hinweis: Die Bilder können je nach dem verwendeten WAP leicht abweichen. Die folgenden

Bilder stammen aus dem WAP125.

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Access Points an, indem Sie in die dafür vorgesehenen Felder Ihren Benutzernamen und Ihr Kennwort eingeben und dann auf **Anmelden** klicken.

Hinweis: Der Standard-Benutzername/Kennwort für den WAP lautet cisco/cisco.




CISCO

Wireless Access Point

Username

Password

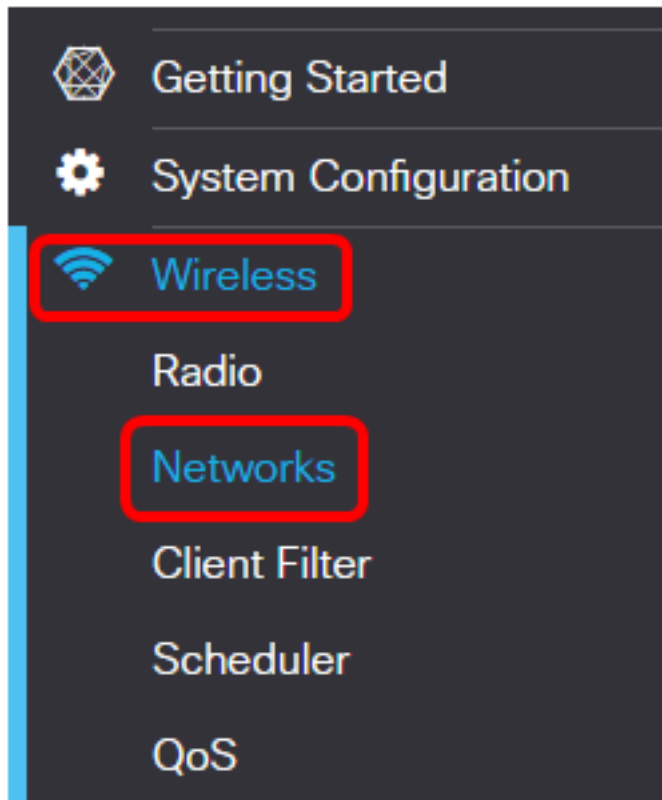
English ▼

Login

©2017 Cisco Systems, Inc. All Rights Reserved.
Cisco, the Cisco Logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Hinweis: Der Standard-Benutzername/Kennwort lautet cisco/cisco.

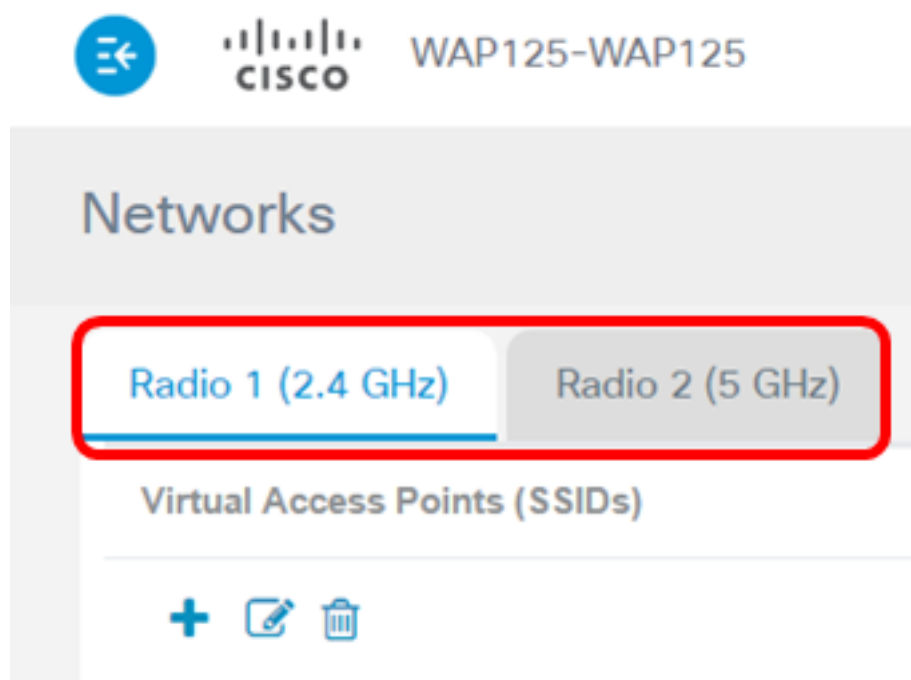
Schritt 2: Wählen Sie **Wireless > Networks** aus.



Schritt 3: Wählen Sie die zu konfigurierende Funkschnittstelle aus. Folgende Optionen stehen zur Verfügung:

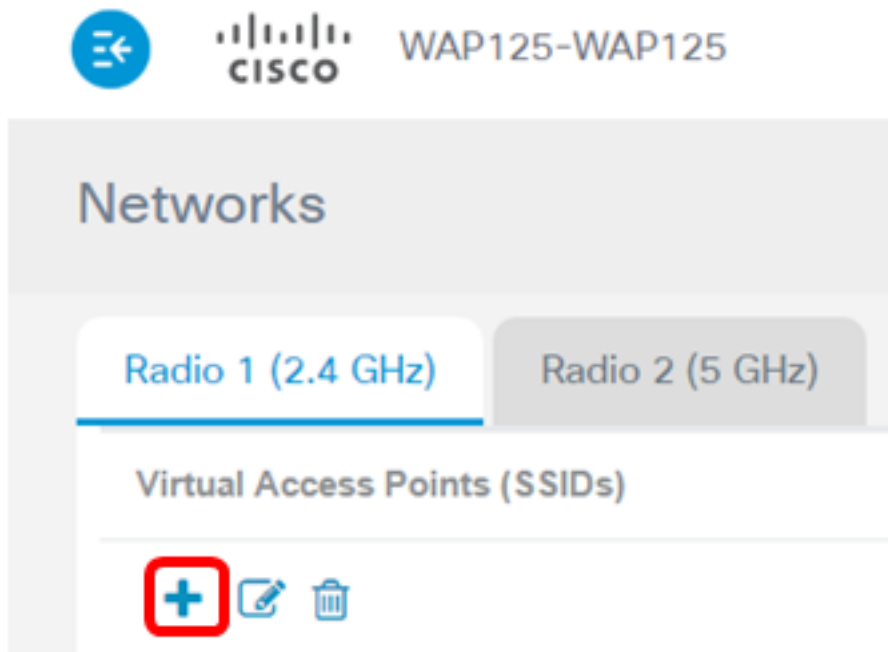
- Funk 1 (2,4 GHz): Mit dieser Option können Sie die Einstellungen von Funk 1 konfigurieren.
- Funk 2 (5 GHz): Mit dieser Option können Sie die Einstellungen von Funk 2 konfigurieren.

Hinweis: Wenn Sie den WAP581 verwenden, ist Radio 1 für 5 GHz und Radio 2 für 2,4 GHz ausgelegt.



Hinweis: In diesem Beispiel wird Radio 1 (2,4 GHz) ausgewählt.

[Schritt 8:](#) Klicken Sie auf die **+** Schaltfläche, um einen VAP hinzuzufügen.



Schritt 5: Überprüfen Sie, ob das Kontrollkästchen **Aktivieren** aktiviert ist. Dies ist standardmäßig aktiviert.

<input type="checkbox"/>	No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	WAP125	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	10	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Schritt 6: Geben Sie die VLAN-ID ein, die dem VAP zugeordnet werden soll.

<input type="checkbox"/>	No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	WAP125	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	10	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Hinweis: In diesem Beispiel wird der VAP für VLAN 10 eingerichtet.

Schritt 7: Geben Sie den Namen des Wireless-Netzwerks ein. Dies wird auch als Service Set Identifier (SSID) bezeichnet. Es handelt sich um eine Kombination aus Buchstaben und Zahlen mit einer Länge von bis zu 32 Zeichen.

+ ✎ 🗑

<input type="checkbox"/>	No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	WAP125	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	10	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Hinweis: In diesem Beispiel wird CiscoTest eingegeben.

Schritt 8: Überprüfen Sie, ob SSID-Broadcast aktiviert ist. Dadurch wird die SSID sichtbar, wenn ein Wireless-Client nach einem Wireless-Netzwerk sucht. Diese Option ist standardmäßig aktiviert. Deaktivieren Sie diese Option, wenn die SSID in der Liste der Netzwerke nicht sichtbar sein soll. Wenn der SSID-Broadcast deaktiviert ist, muss die Verbindung zum Wireless-Netzwerk manuell hergestellt werden.

+ ✎ 🗑

<input type="checkbox"/>	No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	WAP125	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	10	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Schritt 9: (Optional) Aktivieren Sie das Kontrollkästchen Wireless Multicast Forwarding (WMF), um WMF zu aktivieren. Durch die Aktivierung von WMF kann Multicast-Datenverkehr effizient auf die Wireless-Geräte übertragen werden.

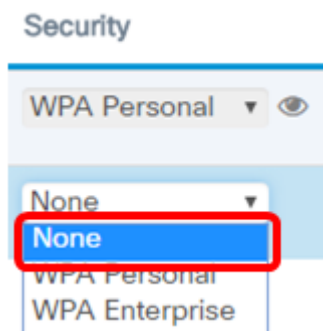
+ ✎ 🗑

<input type="checkbox"/>	No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	WAP125	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	10	CiscoTest	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Schritt 10: Wählen Sie aus der Dropdown-Liste einen Sicherheitstyp aus. Folgende Optionen stehen zur Verfügung:

None (Keine): Diese Option bedeutet, dass die Wireless-Sicherheit auf dem VAP deaktiviert ist. Dies wird nicht empfohlen, da der Zugriff nicht autorisiert werden kann.

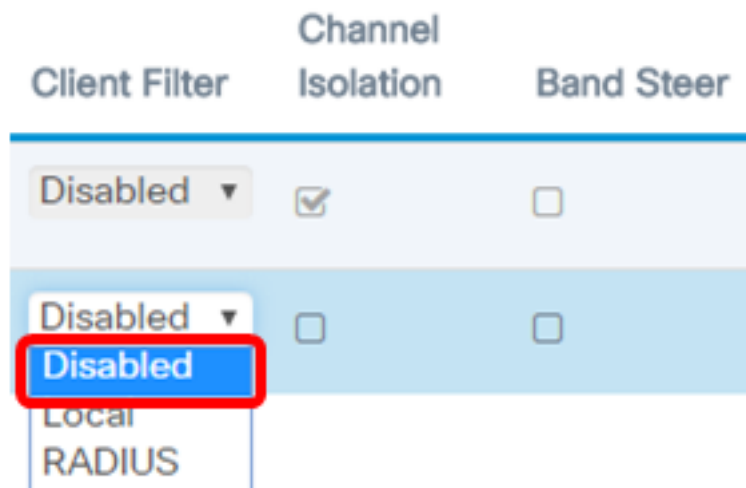
- WPA Personal: Diese Option implementiert die persönliche Sicherheit von Wi-Fi Protected Access (WPA) auf dem VAP. Dies wird in der Regel in kleinen Büroumgebungen verwendet, in denen kein RADIUS-Server (Remote Authentication Dial-In User Service) erforderlich ist.
- WPA Enterprise (WPA-Enterprise): Diese Option implementiert WPA-Sicherheit auf dem VAP. Sie wird in der Regel in größeren Büroumgebungen mit einem RADIUS-Server eingesetzt.



Hinweis: Anweisungen zum Einrichten der Wireless-Sicherheit auf einem WAP erhalten Sie [hier](#). In diesem Beispiel wird None ausgewählt.

Schritt 11: (Optional) Wählen Sie aus der Dropdown-Liste einen Client Filter-Modus aus. Folgende Optionen stehen zur Verfügung:

- Disabled (Deaktiviert): Diese Option bedeutet, dass die Client-Filter-Funktion deaktiviert ist.
- Local (Lokal): Diese Option bedeutet, dass die Client-Filterliste lokal im Access Point gespeichert wird.
- RADIUS (RADIUS): Diese Option bedeutet, dass die Client-Filterliste in einem RADIUS-Server gespeichert wird.



Hinweis: In diesem Beispiel wird Disabled (Deaktiviert) ausgewählt.

Schritt 12: (Optional) Aktivieren Sie das Kontrollkästchen Kanalisierung, um die Funktion zu aktivieren. Wenn diese Funktion aktiviert ist, blockiert der WAP die Kommunikation zwischen Wireless-Clients auf demselben VAP. Das WAP-Gerät lässt weiterhin Datenverkehr zwischen seinen Wireless-Clients und den kabelgebundenen Geräten im Netzwerk, über eine WDS-Verbindung (Wireless Distribution System) und mit anderen Wireless-Clients zu, die einem anderen VAP zugeordnet sind.

Wenn die Kanalisierung deaktiviert ist, ermöglicht der WAP Clients normalerweise die Kommunikation untereinander.

Channel Isolation	Band Steer
<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Hinweis: In diesem Beispiel ist die Kanalisierung deaktiviert.

Schritt 13: (Optional) Aktivieren Sie das Kontrollkästchen **Bandsteuerung**, um die Funktion zu aktivieren. Wenn die Bandsteuerung aktiviert ist, nutzt der WAP das 5-GHz-Band, indem er Dual-Band-unterstützte Clients vom 2,4-GHz-Band bis zum 5-GHz-Band steuert.

Channel Isolation	Band Steer
<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Hinweis: In diesem Beispiel ist Band Steer deaktiviert.

Schritt 14: (Optional) Wählen Sie aus der Dropdown-Liste ein Scheduler-Profil aus. Anweisungen zur Einrichtung des Schedulers erhalten Sie [hier](#).

Scheduler

None ▼

None ▼

None

Hinweis: In diesem Beispiel ist auf dem WAP kein Scheduler-Profil konfiguriert.

Schritt 15: (Optional) Verknüpfen Sie eine Captive Portal (CP)-Instanz mit einem VAP. Die Einstellungen der dem VAP zugeordneten CP-Instanz gelten für Clients, die versuchen, eine Verbindung zum VAP herzustellen. Anweisungen zum Konfigurieren der Instanz für den

Gastzugriff erhalten Sie [hier](#).

Guest
Access
Instance

None ▾
None ▾
None
wiz_cp_inst1

Hinweis: In diesem Beispiel wird None ausgewählt.

Schritt 16: Klicken Sie auf **Speichern**.

Networks Cisco ? i ↵

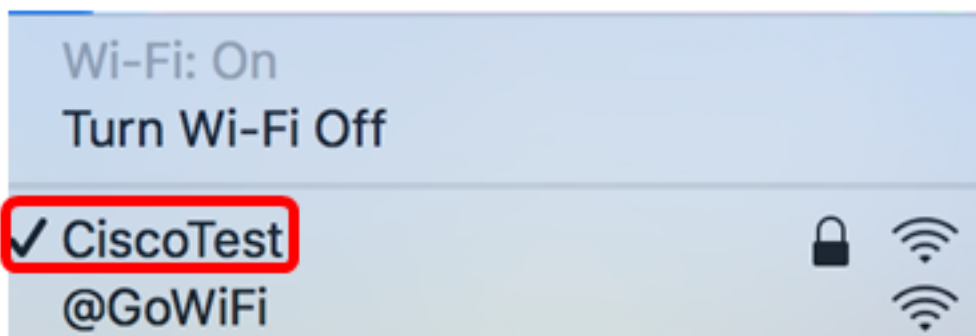
Radio 1 (2.4 GHz) Radio 2 (5 GHz)

Virtual Access Points (SSIDs)

No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMM	Security	Client Filter	Channel Isolation	Band Steer	Scheduler	Guest Access Instance
0	<input type="checkbox"/>	1	WAP125	<input type="checkbox"/>	<input type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None
1	<input checked="" type="checkbox"/>	10	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None

Save

Schritt 17: Stellen Sie sicher, dass der VAP jetzt konfiguriert ist, indem Sie die Netzwerke im Bereich Ihres Wireless-Computers anzeigen.



Hinweis: In diesem Beispiel wird ein Mac-Computer verwendet, der nun drahtlos mit dem neu konfigurierten CiscoTest VAP1-Netzwerk verbunden ist.

Schritt 18: Wiederholen Sie [Schritt 4](#) bis [Schritt 17](#), um VAP2 in VLAN20 mit SSID Cisco hinzuzufügen und zu konfigurieren.

Die Konfiguration der VAPs auf Ihrem WAP ist nun abgeschlossen.

Sehen Sie sich ein Video zu diesem Artikel an..

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)