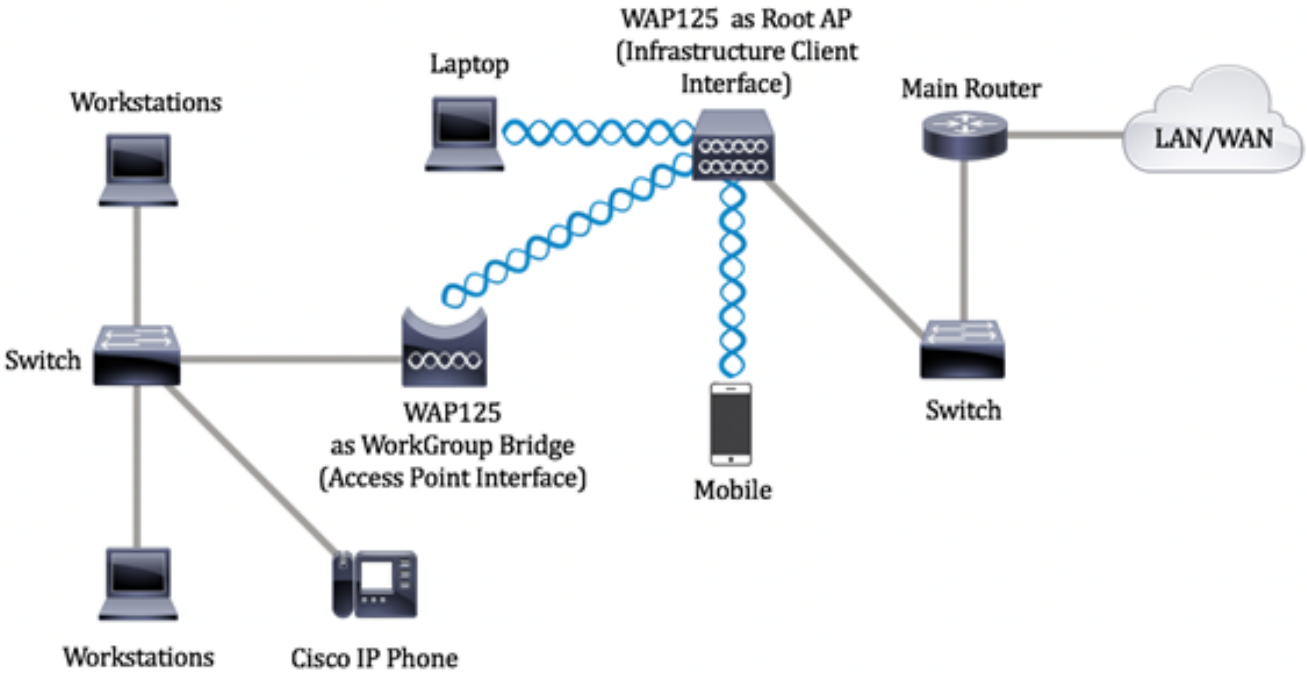
Konfigurieren der WorkGroup Bridge-Einstellungen auf WAP125- oder WAP581-Zugangspunkten

Ziel

Die WorkGroup Bridge-Funktion ermöglicht dem Wireless Access Point (WAP) die Überbrückung des Datenverkehrs zwischen einem Remote-Client und dem Wireless Local Area Network (LAN), das mit dem WorkGroup Bridge-Modus verbunden ist. Das der Remote-Schnittstelle zugeordnete WAP-Gerät wird als Access Point-Schnittstelle bezeichnet, während das dem WLAN zugeordnete WAP-Gerät als Infrastrukturschnittstelle bezeichnet wird. Mit der WorkGroup Bridge können Geräte, die nur über kabelgebundene Verbindungen verfügen, eine Verbindung zu einem Wireless-Netzwerk herstellen. Der Arbeitsgruppen-Bridge-Modus wird als Alternative empfohlen, wenn die Wireless Distribution System (WDS)-Funktion nicht verfügbar ist.

Die folgende Topologie veranschaulicht ein Beispiel für ein WorkGroup Bridge-Modell. Kabelgebundene Geräte sind an einen Switch angeschlossen, der mit der LAN-Schnittstelle des WAP verbunden ist. Im folgenden Beispiel fungiert der WAP125 als Access Point-Schnittstelle, die eine Verbindung zur Infrastruktur-Client-Schnittstelle herstellt.



Dieser Artikel enthält Anweisungen zum Konfigurieren der WorkGroup Bridge-Einstellungen zwischen zwei Wireless Access Points.

Anwendbare Geräte

- WAP125
- WAP581

Softwareversion

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

Konfigurieren der Einstellungen für die Arbeitsgruppen-Brücke

Beachten Sie vor der Konfiguration der Arbeitsgruppen-Bridge auf dem WAP-Gerät die folgenden Richtlinien:

- Alle an der WorkGroup Bridge teilnehmenden WAP-Geräte müssen die folgenden Einstellungen aufweisen:

- Radio

- IEEE 802.11-Modus

- Kanalbandbreite

- Kanal (Auto wird nicht empfohlen)

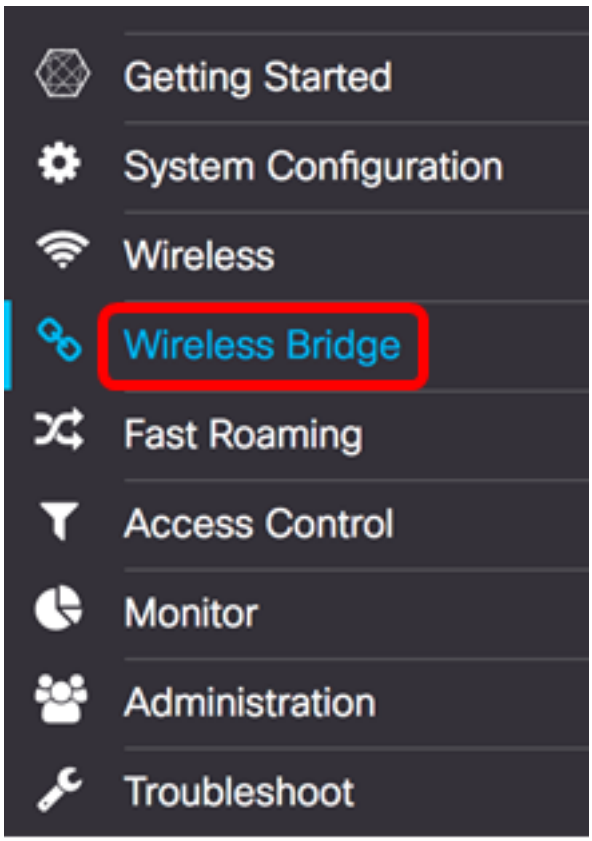
Hinweis: Um zu erfahren, wie Sie diese Einstellungen auf dem WAP125 konfigurieren, klicken Sie hier, um Anweisungen zu erhalten. Für WAP581 klicken Sie hier.

- Der WorkGroup Bridge-Modus unterstützt derzeit nur IPv4-Datenverkehr.
- Der WorkGroup-Bridge-Modus wird in einer Single-Point-Einrichtung nicht unterstützt. Wenn Sie über WAP581 Access Points verfügen, müssen Sie zuerst das SPS oder Clustering deaktivieren, bevor Sie die Einstellungen für die WorkGroup Bridge konfigurieren. Anweisungen zum Konfigurieren der SPS-Einstellungen auf Ihrem WAP erhalten Sie hier.

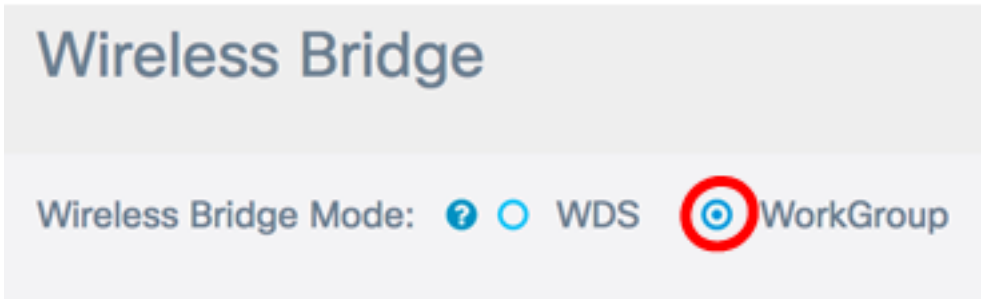
Konfigurieren der Infrastruktur-Client-Schnittstelle

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des WAP an, und wählen Sie dann **Wireless Bridge aus**.

Hinweis: Die verfügbaren Optionen können je nach Gerät variieren. In diesem Beispiel wird WAP125 verwendet.



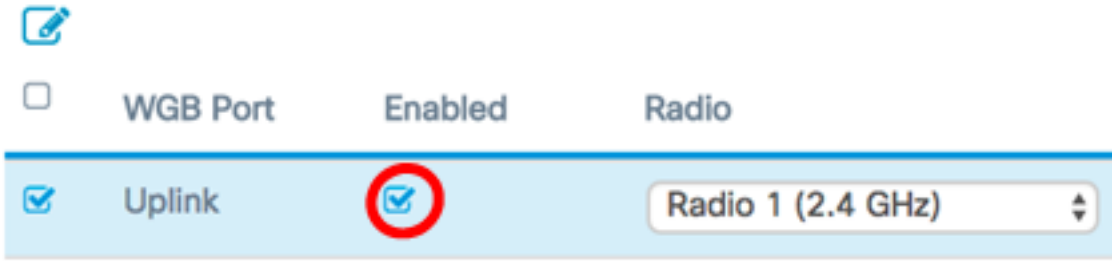
Schritt 2: Klicken Sie auf das Optionsfeld **WorkGroup**.



Schritt 3: Aktivieren Sie das Kontrollkästchen **Uplink**.

Schritt 4: Klicken Sie auf das Symbol **Bearbeiten**.

Schritt 5: Aktivieren Sie das Kontrollkästchen **Aktiviert**, um die Infrastruktur-Client-Schnittstelle zu aktivieren.



Schritt 6: Wählen Sie die Funkschnittstelle für die WorkGroup Bridge aus. Wenn Sie eine Funkeinheit als WorkGroup Bridge konfigurieren, bleibt die andere Funkeinheit betriebsbereit. Die Funkschnittstellen entsprechen den Funkfrequenzbändern des WAP. Der WAP ist für die Übertragung auf zwei verschiedenen Funkschnittstellen ausgerüstet. Die Konfiguration der Einstellungen für eine Funkschnittstelle hat keine Auswirkungen auf die andere.

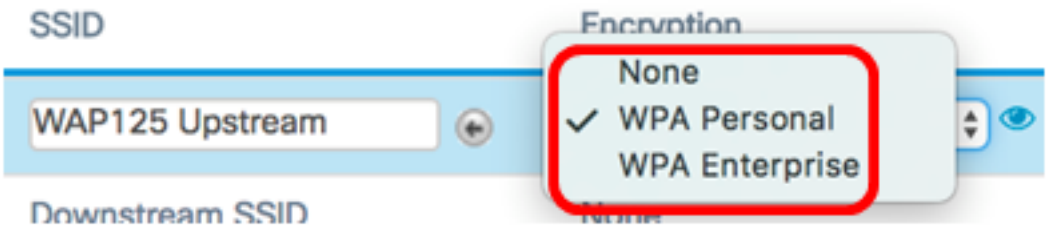
Hinweis: In diesem Beispiel wird Radio 2 (5 GHz) ausgewählt.

Schritt 7: Geben Sie den Namen Service Set Identifier (SSID) in das Feld *SSID ein*. Dies dient als Verbindung zwischen dem Gerät und dem Remote-Client. Sie können 2 bis 32 Zeichen für die Infrastruktur-Client-SSID eingeben.

Hinweis: In diesem Beispiel wird der WAP125 Upstream verwendet.

Hinweis: Der Pfeil neben der SSID ist für die SSID-Prüfung verfügbar. Diese Funktion ist standardmäßig deaktiviert und nur aktiviert, wenn die AP-Erkennung bei der Erkennung nicht autorisierter APs aktiviert ist, die standardmäßig ebenfalls deaktiviert ist.

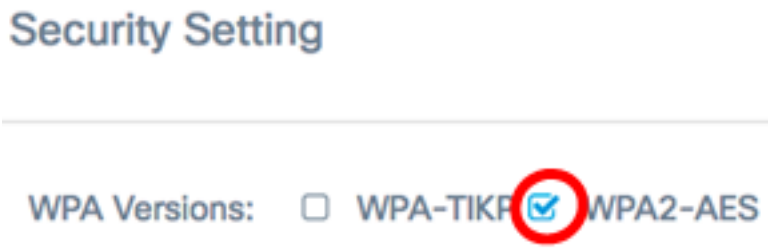
Schritt 8: Wählen Sie aus der Dropdown-Liste Verschlüsselung den Sicherheitstyp aus, der als Client-Station auf dem Upstream-WAP-Gerät authentifiziert werden soll. Folgende Optionen stehen zur Verfügung:



- Keine - offen oder keine Sicherheit. Dies ist die Standardeinstellung. Wenn Sie diese Option auswählen, fahren Sie mit Schritt 22 fort.
- WPA Personal: WPA Personal unterstützt Schlüssel mit einer Länge von 8-63 Zeichen. WPA2 wird empfohlen, da es über einen leistungsfähigeren Verschlüsselungsstandard verfügt.
- WPA Enterprise (WPA-Enterprise): WPA Enterprise ist fortgeschrittener als WPA Personal und stellt die empfohlene Sicherheit für die Authentifizierung dar. Es verwendet PEAP (Protected Extensible Authentication Protocol) und TLS (Transport Layer Security). Fahren Sie mit Schritt 12 fort. Dieser Sicherheitstyp wird häufig in einer Büroumgebung verwendet und benötigt einen RADIUS-Server (Remote Authentication Dial-In User Service). Klicken Sie hier, um mehr über RADIUS-Server zu erfahren.

Hinweis: In diesem Beispiel wird WPA Personal ausgewählt.

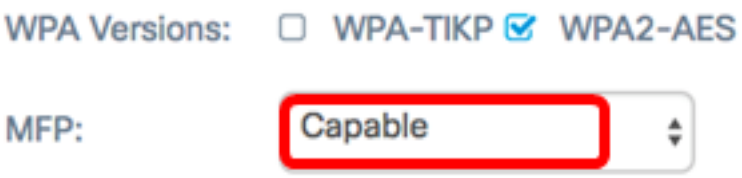
Schritt 9: Klicken Sie auf das Symbol, und aktivieren Sie das Kontrollkästchen WPA-TKIP oder WPA2-AES, um festzustellen, welche Art von WPA-Verschlüsselung die Infrastruktur-Client-Schnittstelle verwendet.



Hinweis: Wenn alle Wireless-Geräte WPA2 unterstützen, legen Sie für die Sicherheit des Infrastruktur-Client WPA2-AES fest. Die Verschlüsselungsmethode ist RC4 für WPA und Advanced Encryption Standard (AES) für WPA2. WPA2 wird empfohlen, da es über einen leistungsfähigeren Verschlüsselungsstandard verfügt. In diesem Beispiel wird WPA2-AES verwendet.

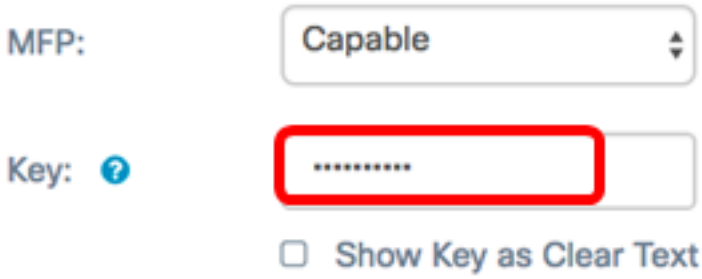
Schritt 10: (Optional) Wenn Sie WPA2-AES in Schritt 9 aktiviert haben, wählen Sie eine Option aus der Dropdown-Liste Management Frame Protection (MFP) aus, ob der WAP geschützte Frames enthalten soll oder nicht. Weitere Informationen zum MFP erhalten Sie hier. Folgende Optionen stehen zur Verfügung:

- Not Required (Nicht erforderlich) - Deaktiviert die Client-Unterstützung für MFP.
- Capable (MFP) - Ermöglicht MFP-fähigen und Clients, die MFP nicht unterstützen, dem Netzwerk beizutreten. Dies ist die Standard-MFP-Einstellung für den WAP.
- Erforderlich - Kunden können nur eine Verbindung herstellen, wenn ein MFP ausgehandelt wird. Wenn die Geräte MFP nicht unterstützen, sind sie nicht berechtigt, dem Netzwerk beizutreten.



Hinweis: In diesem Beispiel wird Capable ausgewählt.

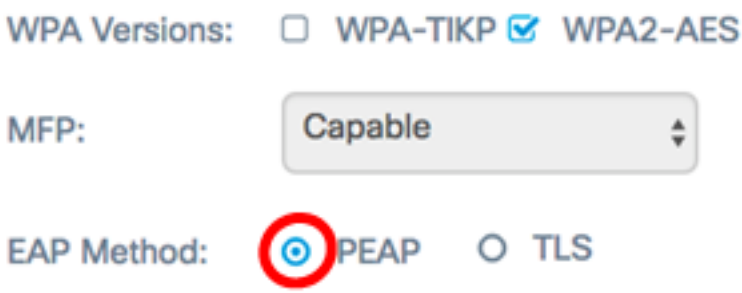
Schritt 11: Geben Sie den WPA-Verschlüsselungsschlüssel in das Feld *Schlüssel ein*. Der Schlüssel muss 8 bis 63 Zeichen lang sein. Dies ist eine Kombination aus Buchstaben, Zahlen und Sonderzeichen. Es ist das Kennwort, das bei der ersten Verbindung mit dem Wireless-Netzwerk verwendet wird. Fahren Sie anschließend mit Schritt 21 fort.



Schritt 12: Wenn Sie in Schritt 8 WPA Enterprise ausgewählt haben, klicken Sie auf ein Optionsfeld für die EAP-Methode.

Die verfügbaren Optionen sind wie folgt definiert:

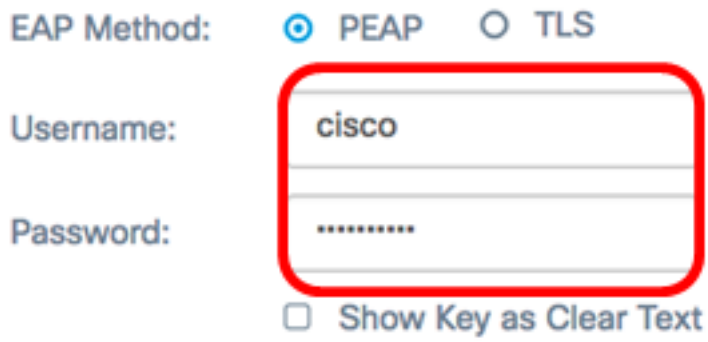
- PEAP: Dieses Protokoll gibt jedem Wireless-Benutzer die individuellen Benutzernamen und Kennwörter des WAP an, die AES-Verschlüsselungsstandards unterstützen. Da PEAP eine kennwortbasierte Sicherheitsmethode ist, basiert Ihre Wi-Fi-Sicherheit auf den Geräteanmeldeinformationen des Clients. PEAP kann ein potenziell schwerwiegendes Sicherheitsrisiko darstellen, wenn Sie über schwache Passwörter oder ungesicherte Clients verfügen. Sie stützt sich auf TLS, vermeidet jedoch die Installation digitaler Zertifikate auf jedem Client. Stattdessen wird die Authentifizierung über einen Benutzernamen und ein Kennwort bereitgestellt.
- TLS - Für TLS muss jedem Benutzer ein zusätzliches Zertifikat für den Zugriff zugewiesen werden. TLS ist sicherer, wenn Sie über zusätzliche Server und die erforderliche Infrastruktur verfügen, um Benutzer in Ihrem Netzwerk zu authentifizieren. Wenn Sie diese Option auswählen, fahren Sie mit Schritt 14 fort.



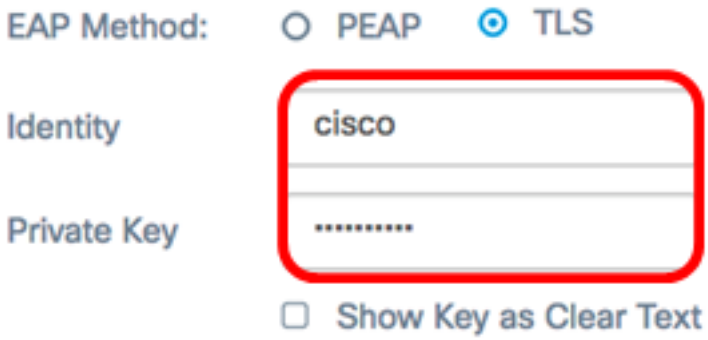
Hinweis: In diesem Beispiel wird PEAP ausgewählt.

Schritt 13: Geben Sie den Benutzernamen und das Kennwort für den Infrastruktur-Client in die Felder Benutzername und Kennwort ein. Dies sind die Anmeldeinformationen, die für die Verbindung mit der Infrastruktur-Client-Schnittstelle verwendet werden. Weitere

Informationen finden Sie in Ihrer Infrastruktur-Client-Schnittstelle. Fahren Sie anschließend mit Schritt 21 fort.

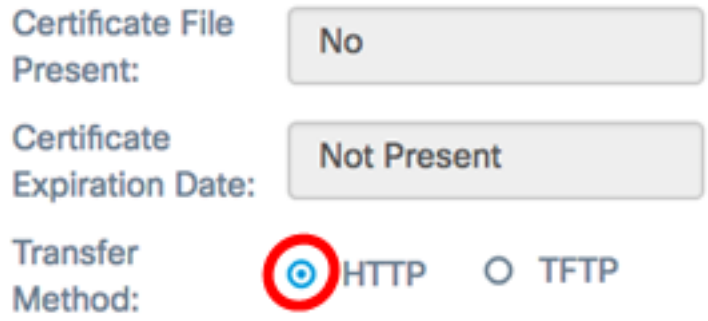


Schritt 14: Wenn Sie in Schritt 12 auf TLS geklickt haben, geben Sie die Identität und den privaten Schlüssel des Infrastruktur-Clients in die Felder "Identity" (Identität) und "Private Key" (Privater Schlüssel) ein.



Schritt 15: Klicken Sie im Bereich Übertragungsmethode auf ein Optionsfeld der folgenden Optionen:

- TFTP — Trivial File Transfer Protocol (TFTP) ist eine vereinfachte, ungesicherte Version von File Transfer Protocol (FTP). Er wird hauptsächlich zur Verteilung von Software oder zur Authentifizierung von Geräten zwischen Unternehmensnetzwerken verwendet. Wenn Sie auf TFTP geklickt haben, fahren Sie mit Schritt 18 fort.
- HTTP - Hypertext Transfer Protocol (HTTP) bietet ein einfaches Challenge-Response-Authentifizierungs-Framework, das von einem Client zur Bereitstellung eines Authentifizierungs-Frameworks verwendet werden kann.



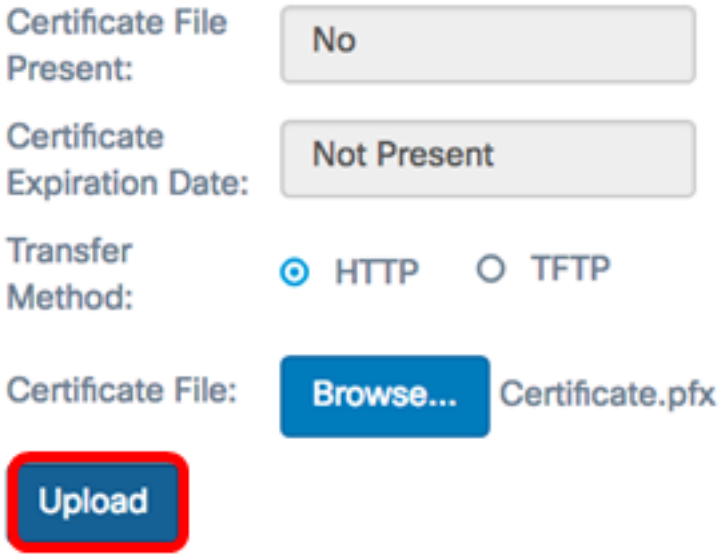
Hinweis: Wenn auf dem WAP bereits eine Zertifikatsdatei vorhanden ist, werden die Felder für das Vorhandensein der Zertifikatsdatei und das Ablaufdatum des Zertifikats bereits mit den entsprechenden Informationen ausgefüllt. Andernfalls sind sie leer.

HTTP

Schritt 16: Klicken Sie auf die Schaltfläche **Durchsuchen**, um eine Zertifikatsdatei zu suchen und auszuwählen. Die Datei muss über die entsprechende Zertifikatsdateierweiterung verfügen (z. B. .pem oder .pfx), andernfalls wird die Datei nicht akzeptiert.

Hinweis: In diesem Beispiel wird Certificate.pfx ausgewählt.

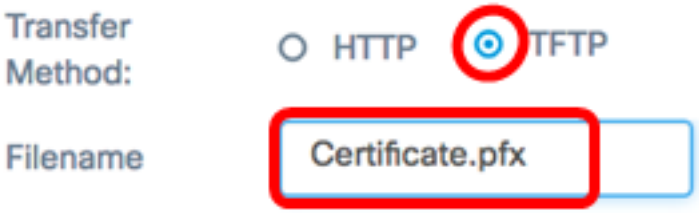
Schritt 17: Klicken Sie auf **Hochladen**, um die ausgewählte Zertifikatsdatei hochzuladen. Fahren Sie mit Schritt 21 fort.



Die Felder für die Zertifikatsdatei Gegenwart und Zertifikatsablaufdatum werden automatisch aktualisiert.

TFTP

Schritt 18: (Optional) Wenn Sie in Schritt 15 auf TFTP geklickt haben, geben Sie den Dateinamen der Zertifikatsdatei im Feld *Dateiname ein*.



Hinweis: In diesem Beispiel wird Certificate.pfx verwendet.

Schritt 19: Geben Sie die Adresse des TFTP-Servers in das Feld *IPv4-Adresse* des *TFTP-Servers ein*.

Hinweis: In diesem Beispiel. 192.168.100.108 wird als TFTP-Serveradresse verwendet.

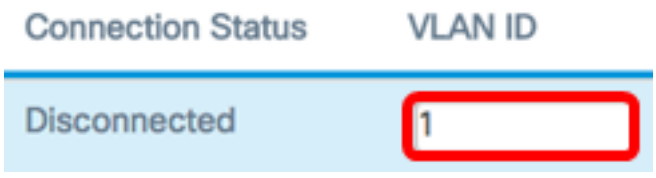
Schritt 20: Klicken Sie auf die Schaltfläche **Hochladen**, um die angegebene Zertifikatsdatei hochzuladen.

Die Felder für die Zertifikatsdatei Gegenwart und Zertifikatsablaufdatum werden automatisch aktualisiert.

Schritt 21: Klicken Sie auf **OK**, um das Fenster Sicherheitseinstellungen zu schließen.

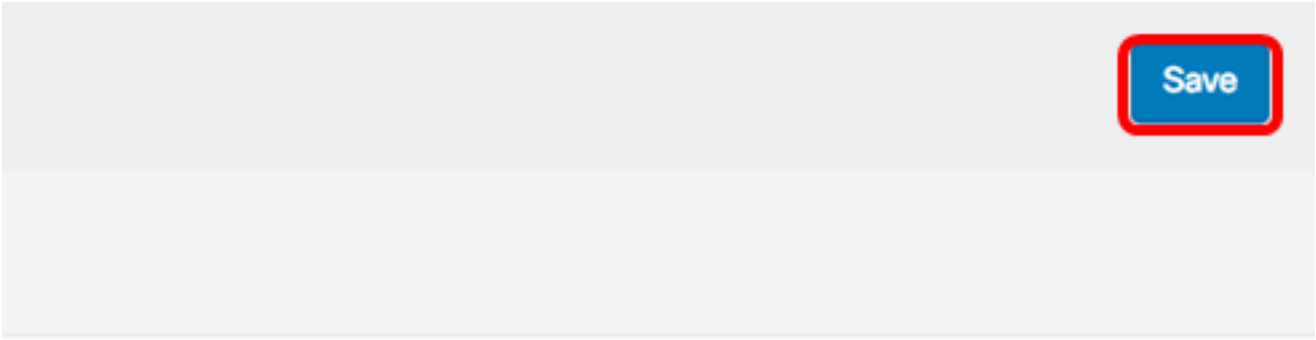
Der Bereich Verbindungsstatus gibt an, ob der WAP mit dem Upstream-WAP-Gerät verbunden ist.

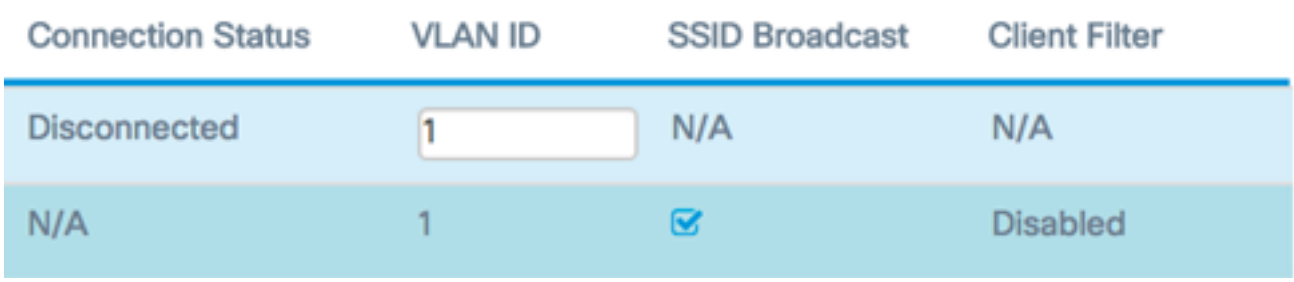
Schritt 22: Geben Sie die VLAN-ID für die Infrastruktur-Client-Schnittstelle ein. Der Standardwert ist 1.



Hinweis: In diesem Beispiel wird die Standard-VLAN-ID verwendet.

Schritt 23: Klicken Sie auf **Speichern**, um die konfigurierten Einstellungen zu speichern.



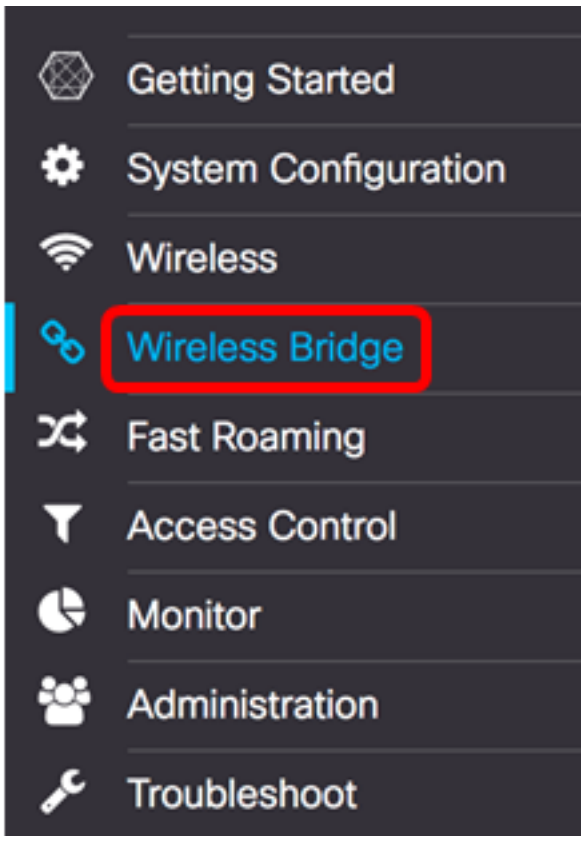


Sie sollten jetzt die Einstellungen für die Infrastruktur-Client-Schnittstelle auf Ihrem WAP erfolgreich konfiguriert haben.

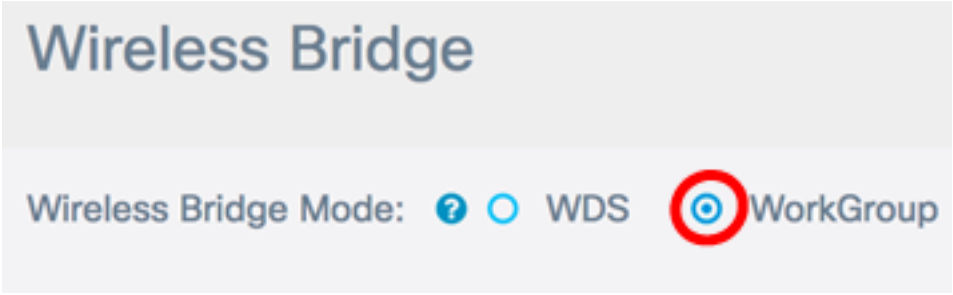
Konfigurieren der Access Point-Client-Schnittstelle

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des WAP an, und wählen Sie dann **Wireless Bridge aus**.

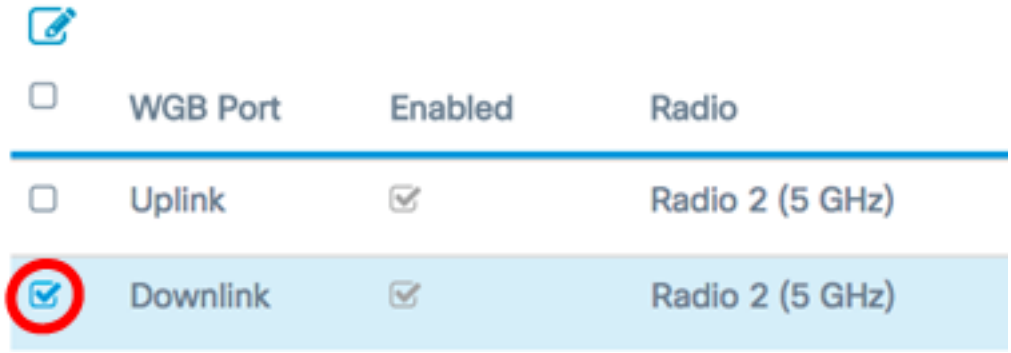
Hinweis: Die verfügbaren Optionen können je nach Gerät variieren. In diesem Beispiel wird WAP125 verwendet.



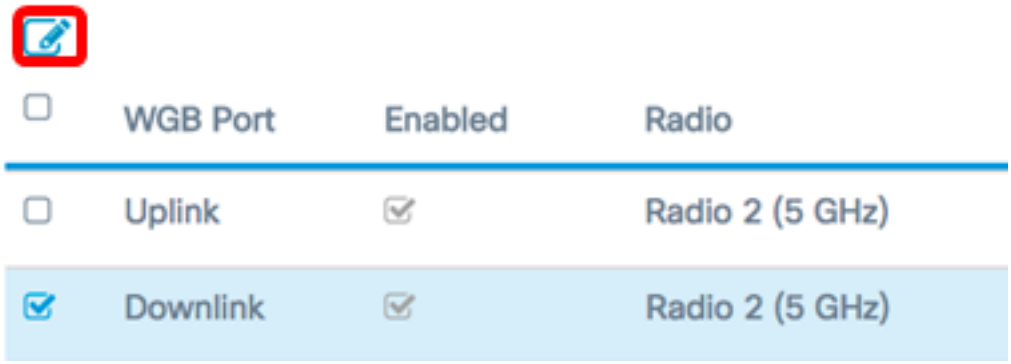
Schritt 2: Klicken Sie auf das Optionsfeld **WorkGroup**.



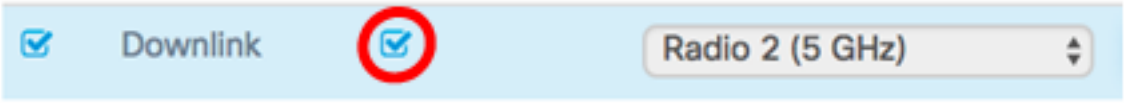
Schritt 3: Aktivieren Sie das Kontrollkästchen **Downlink**.



Schritt 4: Klicken Sie auf die Schaltfläche **Bearbeiten**.



Schritt 5: Aktivieren Sie das Kontrollkästchen **Enabled** (Aktiviert), um Bridging auf der Access Point-Schnittstelle zu aktivieren.



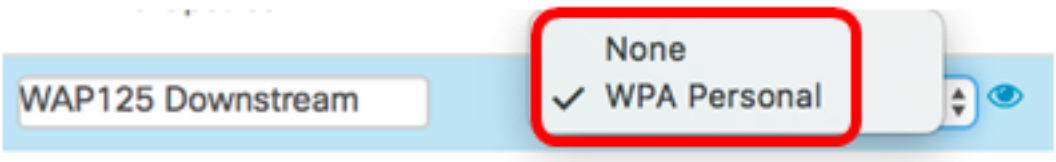
Schritt 6: Geben Sie die SSID für den Access Point in das *SSID*-Feld ein. Die SSID-Länge muss zwischen 2 und 32 Zeichen betragen. Der Standardwert ist Downstream-SSID.

Hinweis: In diesem Beispiel wird als SSID WAP125 Downstream verwendet.

Schritt 7: Wählen Sie aus der Dropdown-Liste Security (Sicherheit) den Sicherheitstyp aus, um Downstream-Client-Stationen für den WAP zu authentifizieren.

Die verfügbaren Optionen sind wie folgt definiert:

- Keine - offen oder keine Sicherheit. Dies ist der Standardwert. Fahren Sie mit Schritt 13 fort, wenn Sie diese Option auswählen.
- WPA Personal - Wi-Fi Protected Access (WPA) Personal unterstützt Schlüssel mit einer Länge von 8 bis 63 Zeichen. Die Verschlüsselungsmethode ist entweder TKIP oder Counter Cipher Mode mit Block Chaining Message Authentication Code Protocol (CCMP). WPA2 mit CCMP wird empfohlen, da es über einen leistungsfähigeren Verschlüsselungsstandard, Advanced Encryption Standard (AES), verfügt, verglichen mit dem Temporal Key Integrity Protocol (TKIP), das nur einen 64-Bit-RC4-Standard verwendet.



Schritt 8: (Optional) Aktivieren Sie das Kontrollkästchen WPA-TKIP, um die WPA-TKIP-Verschlüsselung zu bestimmen, die von der Schnittstelle des Access Points verwendet wird. Dies ist standardmäßig aktiviert.

Hinweis: WPA-AES ist abgeblendet und kann nicht deaktiviert werden. In diesem Beispiel ist WPA-TKIP deaktiviert.

Schritt 9: Geben Sie den gemeinsamen WPA-Schlüssel in das Feld Schlüssel ein. Der Schlüssel muss 8 bis 63 Zeichen lang sein und kann alphanumerische Zeichen, Groß- und Kleinbuchstaben sowie Sonderzeichen enthalten.

Schritt 10: Geben Sie im Feld "Broadcast Key Refresh Rate" (Aktualisierungsrate für Sendeschlüssel) die Rate ein. Die Aktualisierungsrate für den Broadcast-Schlüssel gibt das Intervall an, in dem der Sicherheitsschlüssel für Clients aktualisiert wird, die diesem Access Point zugeordnet sind. Die Rate muss zwischen 0 und 86400 liegen, wobei der Wert 0 die Funktion deaktiviert.

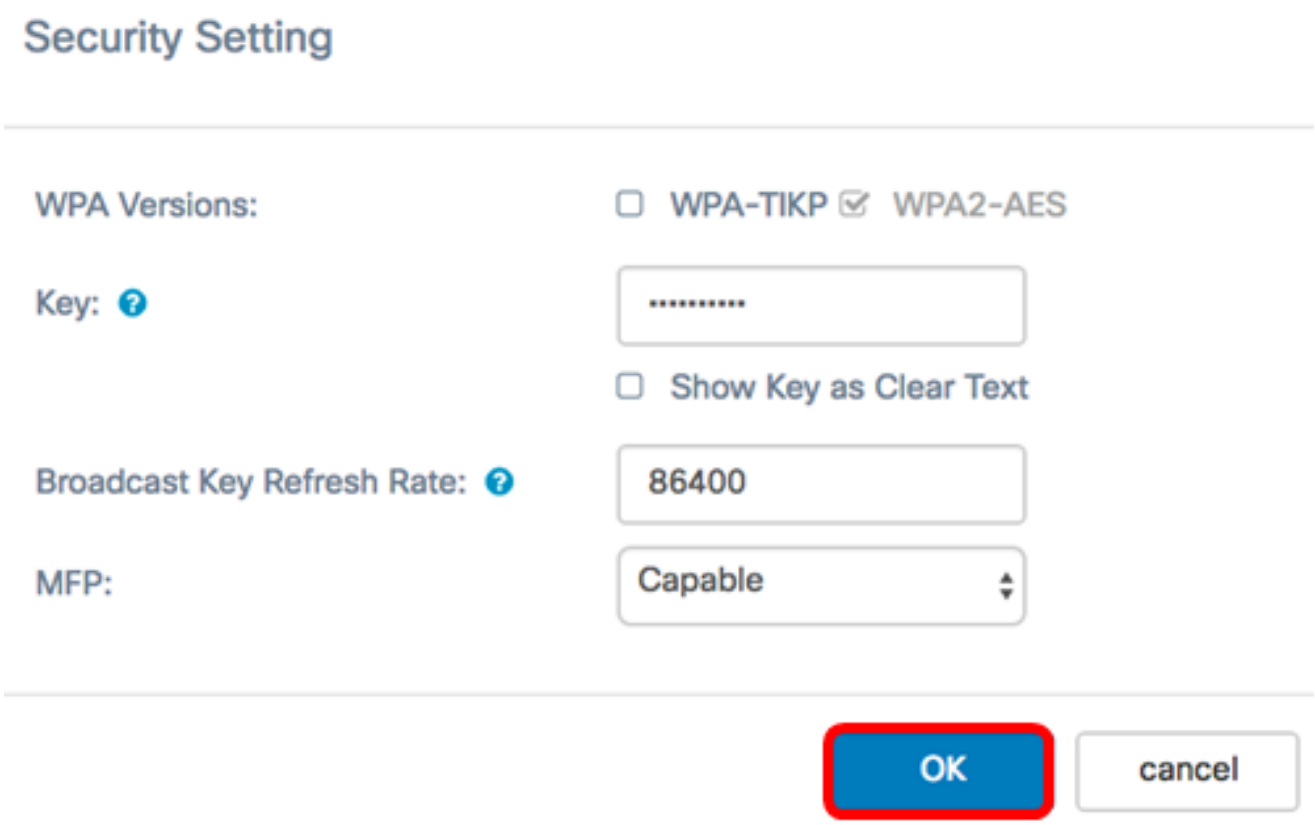
Hinweis: In diesem Beispiel wird 86400 verwendet.

Schritt 11: Wählen Sie aus der MFP-Dropdown-Liste eine Option aus, ob der WAP geschützte Frames enthalten soll oder nicht. Weitere Informationen zum MFP erhalten Sie hier. Folgende Optionen stehen zur Verfügung:

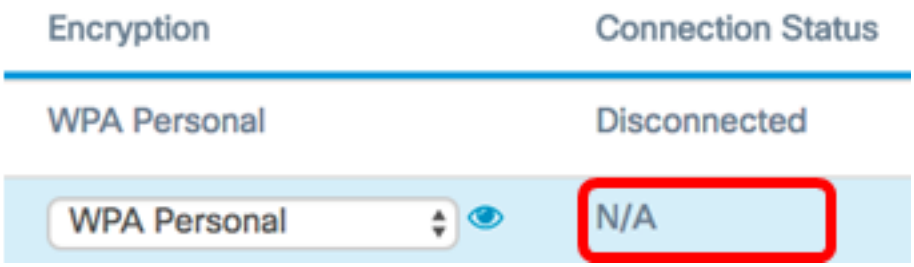
- Not Required (Nicht erforderlich) - Deaktiviert die Client-Unterstützung für MFP.
- Capable (MFP) - Ermöglicht MFP-fähigen und Clients, die MFP nicht unterstützen, dem Netzwerk beizutreten. Dies ist die Standard-MFP-Einstellung für den WAP.
- Erforderlich - Kunden können nur eine Verbindung herstellen, wenn ein MFP ausgehandelt wird. Wenn die Geräte MFP nicht unterstützen, sind sie nicht berechtigt, dem Netzwerk beizutreten.

Hinweis: In diesem Beispiel wird Capable ausgewählt.

Schritt 12: Klicken Sie auf **OK**, um die Sicherheitseinstellungen zu speichern.



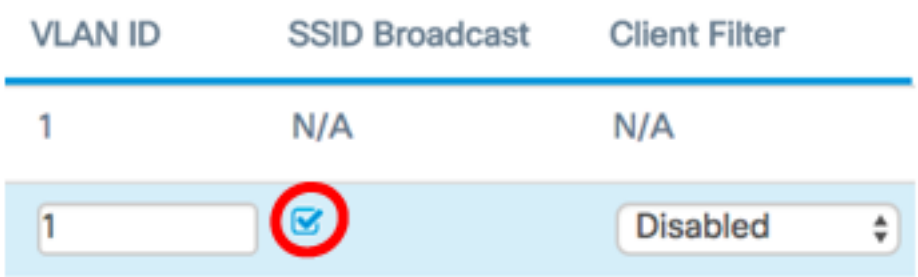
Im Bereich Verbindungsstatus wird die Meldung "Nicht zutreffend" oder "Nein" angezeigt.



Schritt 13: Geben Sie die VLAN-ID im Feld "VLAN ID" (VLAN-ID) für die Schnittstelle des Access Points ein.

Hinweis: Um das Bridging von Paketen zu ermöglichen, sollte die VLAN-Konfiguration für die Access Point-Schnittstelle und die kabelgebundene Schnittstelle mit der der Infrastruktur-Client-Schnittstelle übereinstimmen.

Schritt 14: Aktivieren Sie das Kontrollkästchen SSID-Broadcast, wenn die Downstream-SSID übertragen werden soll. SSID-Broadcast ist standardmäßig aktiviert.



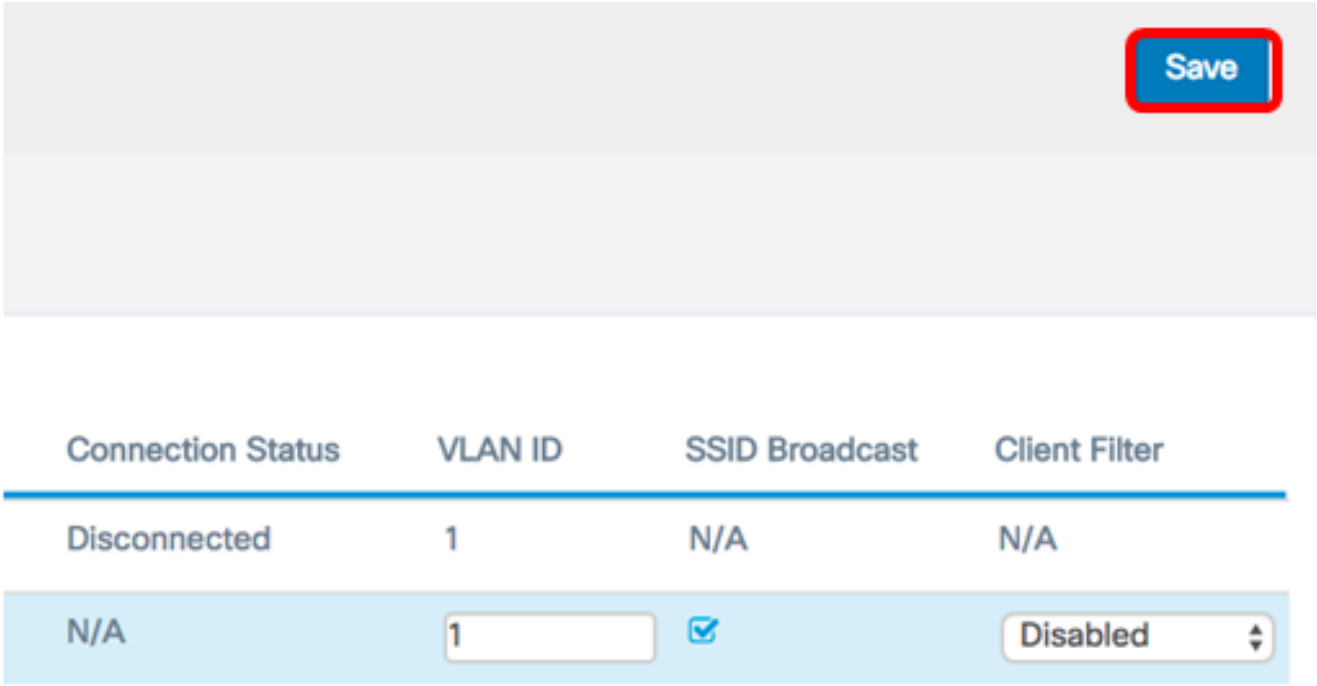
Schritt 15: Wählen Sie aus der Dropdown-Liste MAC Filtering (MAC-Filterung) den Typ der MAC-Filterung aus, die für die Access Point-Schnittstelle konfiguriert werden soll. Wenn diese Funktion aktiviert ist, wird Benutzern basierend auf der MAC-Adresse des Clients, den sie verwenden, der Zugriff auf den WAP gewährt oder verweigert.

Die verfügbaren Optionen sind wie folgt definiert:

- Disabled (Deaktiviert): Alle Clients können auf das Upstream-Netzwerk zugreifen. Dies ist der Standardwert.
- Local (Lokal) - Der Client-Satz, der auf das Upstream-Netzwerk zugreifen kann, ist auf die Clients beschränkt, die in einer lokal definierten MAC-Adressliste angegeben sind.
- RADIUS (RADIUS) - Der Client-Satz, der auf das Upstream-Netzwerk zugreifen kann, ist auf die in einer MAC-Adressliste auf einem RADIUS-Server angegebenen Clients beschränkt.

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

Schritt 16: Klicken Sie auf **Speichern**, um die Änderungen zu speichern.



Sie sollten jetzt die WorkGroup Bridge-Einstellungen für Ihre Wireless Access Points erfolgreich konfiguriert haben.