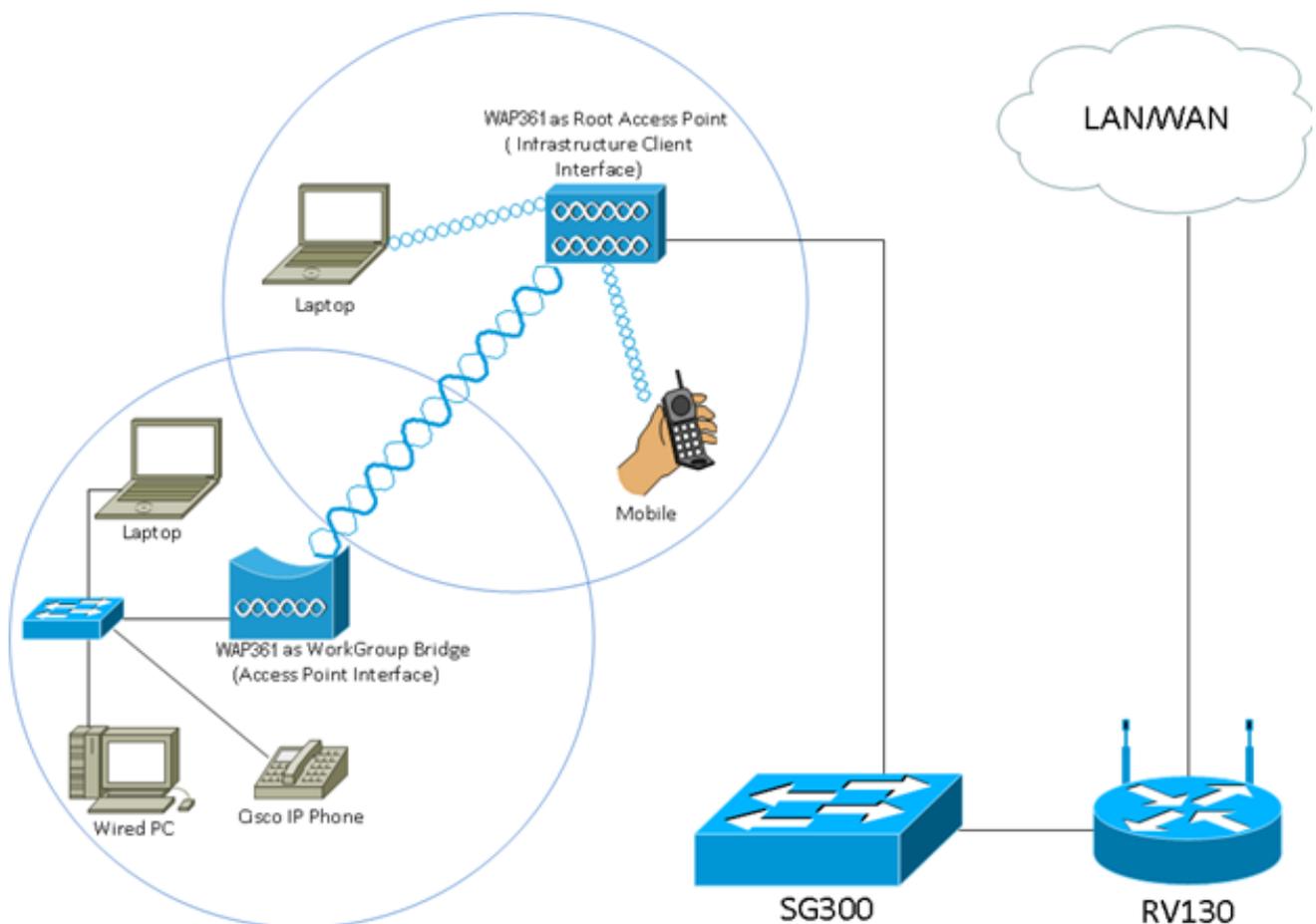


Workgroup Bridge auf einem Wireless Access Point (WAP) konfigurieren

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.



Hinweis: Die oben dargestellte 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. Der WAP fungiert als Access Point-Schnittstelle und stellt eine Verbindung zur Infrastrukturschnittstelle her.

In diesem Artikel erfahren Sie, wie Sie die WorkGroup Bridge zwischen zwei WAPs konfigurieren.

Anwendbare Geräte

- WAP100-Serie
- WAP300-Serie
- WAP500-Serie

Softwareversion

- 1.0.0.17 - WAP571, WAP571E
- 1.0.1.7 — WAP150, WAP361
- 1.0.2.5 — WAP131, WAP351
- 1.0.6.5 — WAP121, WAP321
- 1.2.1.3 — WAP551, WAP561
- 1.3.0.3 — WAP371

Konfigurieren der WorkGroup-Bridge

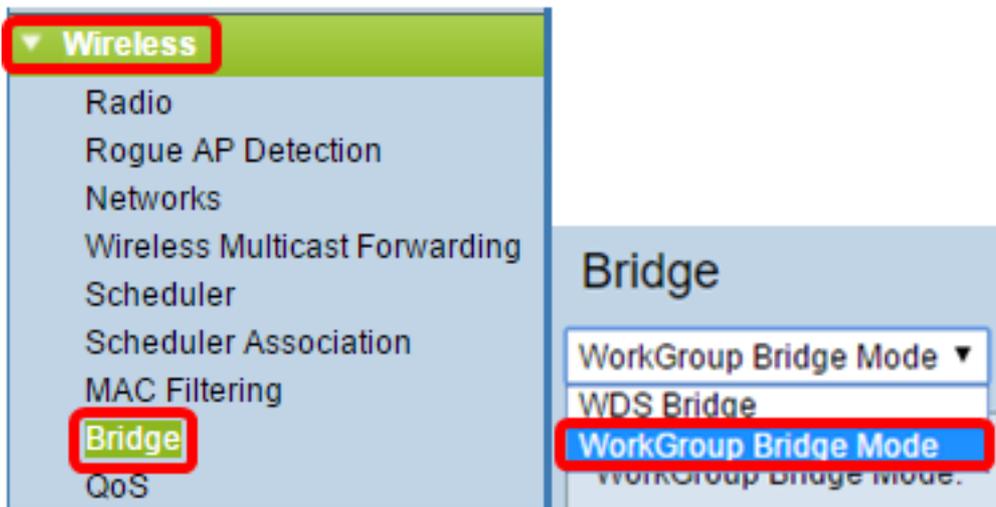
Infrastruktur-Client-Schnittstelle

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

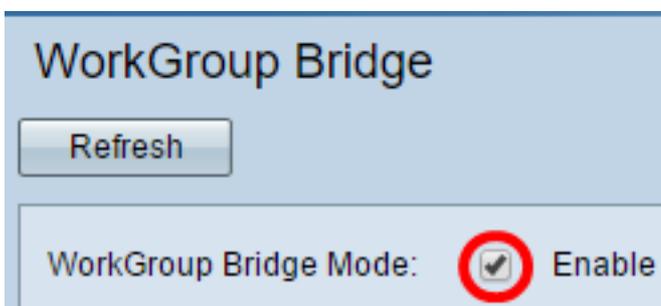
Hinweis: Die Menüoptionen können je nach verwendetem Gerät variieren. Die folgenden Bilder stammen aus dem WAP361, sofern nicht anders angegeben.



Wählen Sie für WAP571 und WAP571E **Wireless > Bridge > WorkGroup Bridge Mode** (**Wireless > Bridge > Arbeitsgruppen-Bridge-Modus**).



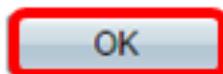
Schritt 2: Aktivieren Sie das Kontrollkästchen **Enable WorkGroup Bridge Mode** (Arbeitsgruppen-Bridge-Modus aktivieren).



Hinweis: Wenn Clustering auf dem WAP aktiviert ist, werden Sie in einem Popup-Fenster darüber informiert, dass Clustering deaktiviert werden soll, damit die WorkGroup Bridge funktioniert. Klicken Sie auf **OK**, um fortzufahren. Um Clustering zu deaktivieren, wählen Sie im Navigationsbereich **Single Point Setup (Single-Point-Einrichtung)** aus, und wählen Sie dann **Access Points > Disable Single-Point Setup (Zugangspunkte > Single-Point-Einrichtung deaktivieren)**.



Workgroup Bridge cannot be enabled when clustering is enabled.



Schritt 3: Klicken Sie auf das Optionsfeld für die WorkGroup Bridge. 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. Die Optionen für die Funkschnittstellen können je nach WAP-Modell variieren. Einige WAPs zeigen Radio 1 (Funkmodul 1) mit 2,4 GHz an, während einige mit Radio 2 (Funkmodul) mit 2,4 GHz ausgestattet sind.

Hinweis: Dieser Schritt gilt nur für die folgenden WAPs mit Dual-Band: WAP131, WAP150, WAP351, WAP361, WAP371, WAP561, WAP571, WAP571E. Für dieses Beispiel wird Radio 1 ausgewählt.

Radio Setting Per Interface

Select the radio interface first, and then enter the configuration parameters.

Radio:

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

Schritt 4: Geben Sie den Namen Service Set Identifier (SSID) in das *SSID*-Feld ein, oder klicken Sie auf den Pfeil neben dem Feld, um nach Nachbarn zu suchen. Dies dient als Verbindung zwischen dem Gerät und dem Remote-Client. Sie können 2 bis 32 Zeichen für die Infrastruktur-Client-SSID eingeben.

Hinweis: Es ist wichtig, die Erkennung nicht autorisierter APs zu aktivieren. Weitere Informationen zur Aktivierung dieser Funktion erhalten Sie [hier](#). In diesem Beispiel wird auf die Pfeiltaste geklickt, um WAP361_L1 als SSID der Infrastruktur-Client-Schnittstelle auszuwählen.

MAC Address	SSID
80:e8:6f:0a:5d:ee	WAP361_L1

Schritt 5: Wählen Sie im Bereich Infrastruktur-Client-Schnittstelle aus der Dropdown-Liste Security (Sicherheit) 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 18 fort](#).
- WPA Personal: WPA Personal unterstützt Schlüssel mit einer Länge von 8-63 Zeichen. WPA2 wird empfohlen, da es über einen leistungsfähigeren Verschlüsselungsstandard verfügt. Fahren Sie mit [Schritt 6](#) für die Konfiguration fort.
- 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 9](#) für die Konfiguration 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.

Infrastructure Client Interface

SSID:

Security: WPA Personal ▼ (+)

VLAN ID:

Connection Status: Disconnected

Hinweis: In diesem Beispiel wird WPA Personal ausgewählt.

Schritt 6: Klicken Sie auf das +, 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.

Security: WPA Personal ▼ (-)

WPA Versions: WPA-TKIP WPA2-AES

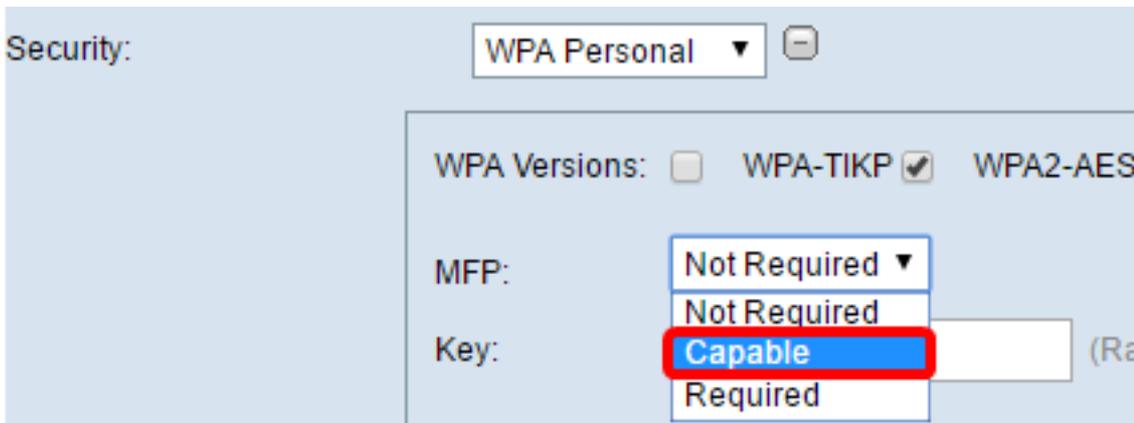
MFP:

Key: (Rare)

Schritt 7: (Optional) Wenn Sie WPA2-AES in Schritt 6 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 8: 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 18 fort](#).



[Schritt 9](#): Wenn Sie in Schritt 5 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.

WPA Versions: WPA-TKIP WPA2-AES

MFP:

EAP Method: PEAP TLS

Username:

Password:

Hinweis: In diesem Beispiel wird PEAP ausgewählt.

Schritt 10: 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 18 fort](#).

WPA Versions: WPA-TKIP WPA2-AES

MFP:

EAP Method: PEAP TLS

Username:

Password:

Schritt 11: Wenn Sie in Schritt 9 auf TLS geklickt haben, geben Sie die Identität und den privaten Schlüssel des Infrastruktur-Clients in die Felder *Identity* und *Private Key ein*.

WPA Versions: WPA-TKIP WPA2-AES

MFP:

EAP Method: PEAP TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Certificate File: No file chosen

[Schritt 12](#): 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 15 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.

WPA Versions: WPA-TKIP WPA2-AES

MFP:

EAP Method: PEAP TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Certificate File: No file chosen

Hinweis: Wenn bereits eine Zertifikatsdatei im WAP vorhanden ist, werden die Felder für die Zertifikatsdatei und das Zertifikatsablaufdatum bereits mit den entsprechenden Informationen ausgefüllt. Andernfalls sind sie leer.

HTTP

Schritt 13: Klicken Sie auf die Schaltfläche **Datei auswählen**, 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 mini_httpd(2).pfx ausgewählt.

Transfer Method: HTTP TFTP

Filename: mini_httpd (2).pfx

Schritt 14: Klicken Sie auf **Hochladen**, um die ausgewählte Zertifikatsdatei hochzuladen. Fahren Sie mit [Schritt 18 fort](#).

Transfer Method: HTTP TFTP

Filename mini_httpd (2).pfx

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

WPA Versions: WPA-TKIP WPA2-AES

MFP:

EAP Method: PEAP TLS

Identity

Private Key

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Certificate File: No file chosen

TFTP

[Schritt 15](#): Wenn Sie in [Schritt 12](#) auf TFTP geklickt haben, geben Sie den Dateinamen der Zertifikatsdatei in das Feld *Dateiname* ein.

Hinweis: In diesem Beispiel wird mini_httpd.pem verwendet.

Transfer Method: HTTP
 TFTP

Filename:

TFTP Server IPv4 Address:

Schritt 16: Geben Sie die Adresse des TFTP-Servers in das Feld *IPv4-Adresse des TFTP-Servers* ein.

Hinweis: In diesem Beispiel. 192.168.1.20 wird als TFTP-Serveradresse verwendet.

Transfer Method: HTTP
 TFTP

Filename:

TFTP Server IPv4 Address:

Schritt 17: Klicken Sie auf die Schaltfläche **Hochladen**, um die angegebene Zertifikatsdatei hochzuladen.

Transfer Method: HTTP
 TFTP

Filename:

TFTP Server IPv4 Address:

Die Felder *für die Zertifikatsdatei* und das *Zertifikatsablaufdatum* werden automatisch aktualisiert.

WPA Versions: WPA-TKIP WPA2-AES

EAP Method: PEAP TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

[Schritt 18:](#) 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.

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Access Point-Schnittstelle

Schritt 1: Aktivieren Sie das Kontrollkästchen **Enable** Status (Status aktivieren), um das Bridging auf der Access Point-Schnittstelle zu aktivieren.

Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: ▼

MAC Filtering: ▼

VLAN ID: (Range: 1 - 4094, Default: 1)

Schritt 2: 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 "Access Point SSID".

Hinweis: In diesem Beispiel wird die SSID `bridge_lobby` verwendet.



Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: +

MAC Filtering: ▾

VLAN ID: (Range: 1 - 4094, Default: 1)

Schritt 3: (Optional) Wenn Sie die SSID nicht übertragen möchten, deaktivieren Sie das Kontrollkästchen **SSID-Broadcast aktivieren**. Dadurch wird der Access Point für die Suche nach Wireless Access Points unsichtbar. kann nur von einem Benutzer mit einer SSID verbunden werden, der die SSID bereits kennt. SSID-Broadcast ist standardmäßig aktiviert.



Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: +

MAC Filtering: ▾

VLAN ID: (Range: 1 - 4094, Default: 1)

Schritt 4: 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:

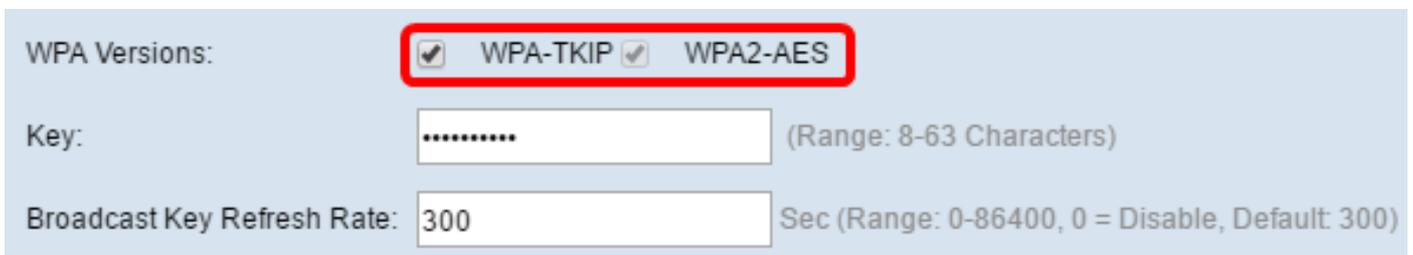
- Keine - offen oder keine Sicherheit. Dies ist der Standardwert. Fahren Sie mit [Schritt 10 fort](#), wenn Sie diese Option auswählen.
- WPA Personal - Wi-Fi Protected Access (WPA) Personal unterstützt Schlüssel mit einer Länge von 8 bis 63 Zeichen. Die Verschlüsselungsmethode ist entweder TKIP oder 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 5: Aktivieren Sie das Kontrollkästchen **WPA-TKIP** oder **WPA2-AES**, um festzustellen, welche Art von WPA-Verschlüsselung von der Access Point-Schnittstelle verwendet wird. Diese sind standardmäßig aktiviert.

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



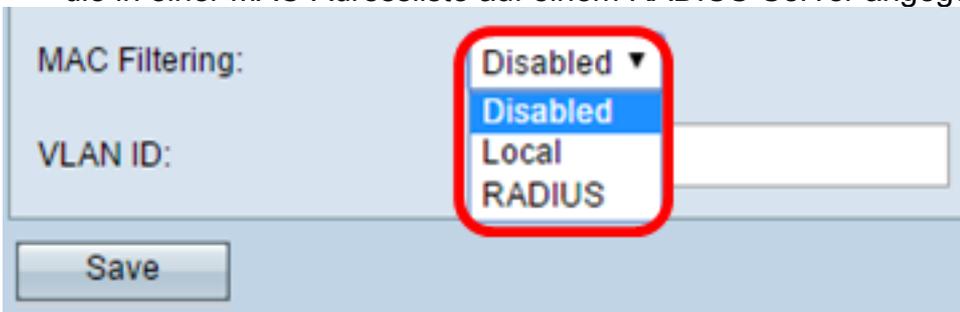
Schritt 7: Geben Sie die Rate im Feld *Aktualisierungsrate* für den *Sendeschlüssel* ein. Die Aktualisierungsrate für den Broadcast-Schlüssel gibt das Intervall an, in dem der Sicherheitsschlüssel für Clients aktualisiert wird, die diesem Access Point zugeordnet sind. Die Rate muss zwischen 0 und 86400 liegen, wobei der Wert 0 die Funktion deaktiviert. Der Standardwert ist 300.



Schritt 8: 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.



MAC Filtering: Disabled ▼
Disabled
Local
RADIUS

VLAN ID:

Save

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

Schritt 9: Geben Sie die VLAN-ID im Feld *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.



MAC Filtering: Disabled ▼

VLAN ID:

Save

[Schritt 10](#): Klicken Sie auf **Speichern**, um die Änderungen zu speichern.



MAC Filtering: Disabled ▼

VLAN ID:

Save

Sie sollten jetzt eine WorkGroup Bridge auf einem Wireless Access Point erfolgreich konfiguriert haben.