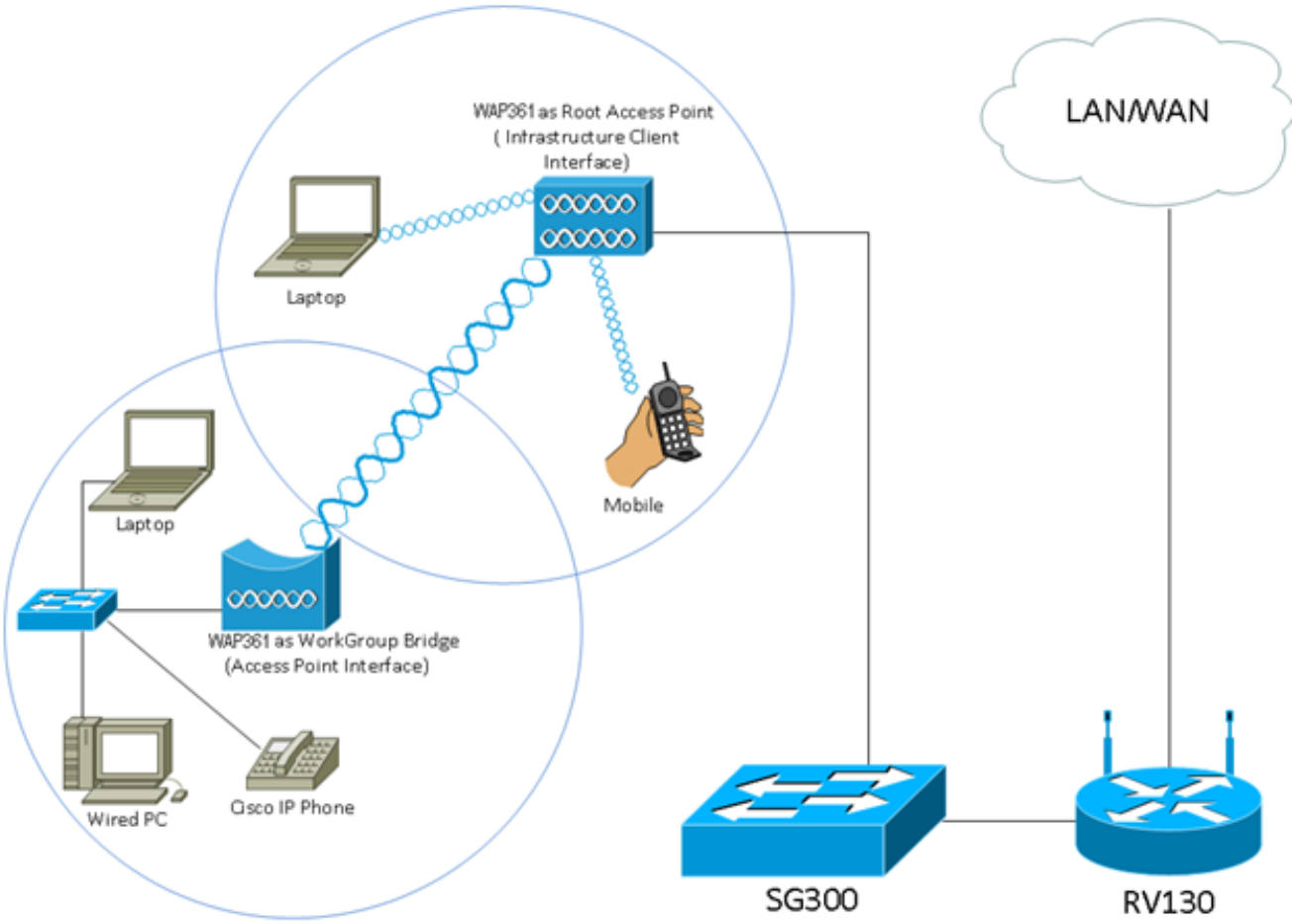
Workgroup Bridge op een draadloos access point (WAP) configureren

Doel

Met de functie Workgroup Bridge kunt u het Wireless Access Point (WAP) in staat stellen om verkeer te overbruggen tussen een externe client en het draadloze LAN-netwerk (Local Area Network) dat is aangesloten op de WorkGroup Bridge Mode. Het WAP-apparaat dat bij de externe interface is aangesloten, is bekend als een access point interface, terwijl het WAP-apparaat dat bij het draadloze LAN hoort, bekend is als een infrastructuur-interface. De WorkGroup Bridge laat apparaten die alleen bedrade verbindingen hebben, aansluiten op een draadloos netwerk. De werkgroepbridge-modus wordt als alternatief aanbevolen wanneer de functie Wireless Distribution System (WDS) niet beschikbaar is.



Opmerking: De topologie hierboven illustreert een model van de Brug van de steekproef. Draadloze apparaten zijn aangesloten op een schakelaar, die op de LAN interface van de WAP aangesloten is. WAP fungeert als een access point interface en sluit zich aan op de infrastructuur interface.

Dit artikel is bedoeld om u te laten zien hoe u de WorkGroup Bridge tussen twee WAP's kunt configureren.

Toepasselijke apparaten

- WAP100 Series switch

- WAP300 Series-switches
- WAP500 Series-switches

Softwareversie

- 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

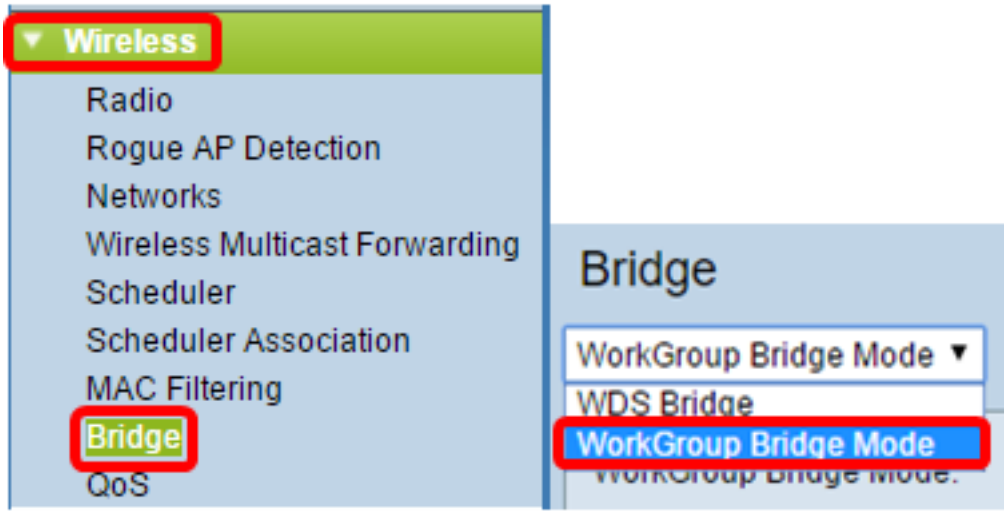
Werkgroepbridge configureren

Infrastructuurclientinterface

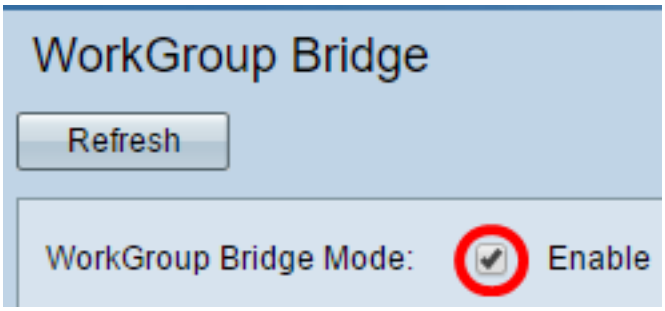
Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van WAP en kies **Wireless > Workgroup Bridge**.

Opmerking: De menuopties kunnen verschillen afhankelijk van het model van het apparaat dat u gebruikt. De onderstaande beelden worden uit WAP361 genomen, tenzij anders vermeld.

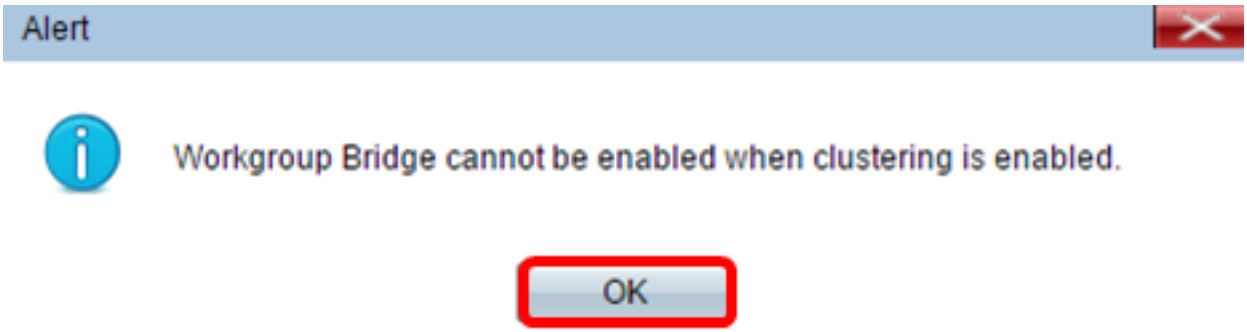
Kies voor WAP571 en WAP571E **draadloze > Bridge > Workgroup Bridge Mode**.



Stap 2. Controleer het vakje Workgroup Bridge Mode **inschakelen**.

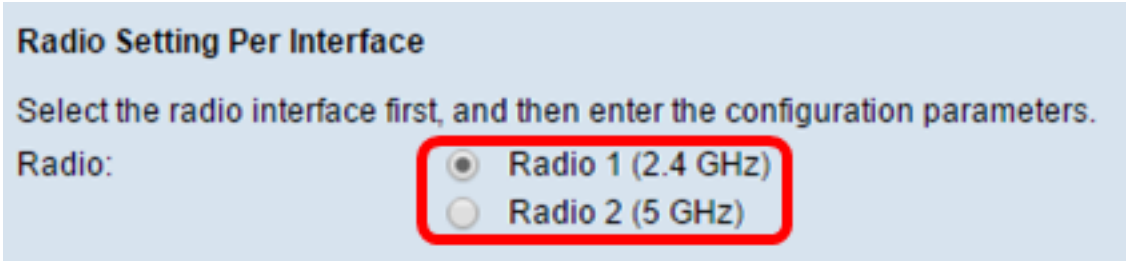


Opmerking: Als clustering op WAP is ingeschakeld, zal een pop-up u informeren om clustering uit te schakelen zodat de WorkGroup Bridge werkt. Klik op **OK** om verder te gaan. Om clustering uit te schakelen, kiest u **Single Point Setup** uit het navigatiedeelvenster en kiest u **Access Point > Single Point Setup uitschakelen**.



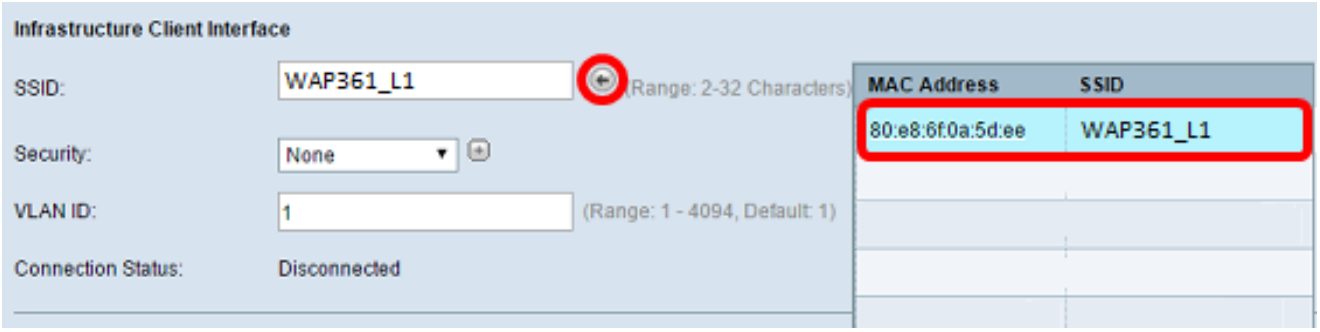
Stap 3. Klik op de radio-interface voor de WorkGroup Bridge. Wanneer u een radio als een WorkGroup Bridge configureren blijft de andere radio actief. De radiofrequentiebanden komen overeen met de radiofrequentiebanden van de WAP. WAP is uitgerust om op twee verschillende radio-interfaces uit te zenden. Het configureren van instellingen voor één radio interface heeft geen invloed op de andere. De radio-interfaceopties kunnen afhankelijk van het WAP-model verschillen. Sommige WAP's hebben radio 1 als 2,4 GHz terwijl sommige radio 2,4 GHz hebben.

Opmerking: Deze stap is alleen voor de volgende WAP's met dubbele band: WAP131, WAP150, WAP351, WAP361, WAP371, WAP561, WAP571, WAP571E. Bijvoorbeeld, wordt Radio 1 gekozen.



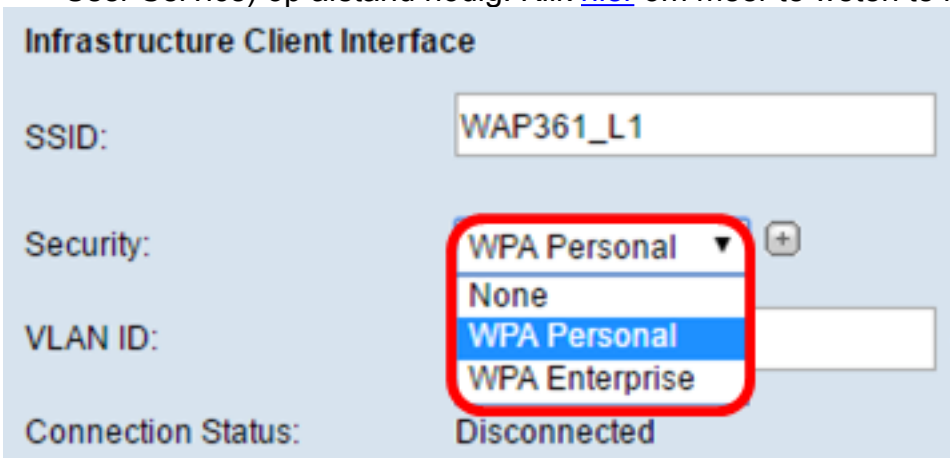
Stap 4. Voer de naam Service Set Identifier (SSID) in het veld *SSID* of klik op de pijlknop naast het veld om voor buren te scannen. Dit dient als de verbinding tussen het apparaat en de externe client. U kunt 2 tot 32 tekens invoeren voor de client van de infrastructuur.

Opmerking: Het is belangrijk om de detectie van Rogue AP mogelijk te maken. Klik hier voor meer informatie over het inschakelen van deze functie. Bij dit voorbeeld wordt op de knop pijl geklikt om WAP361_L1 als SSID van de interface van de infrastructuurclient te kiezen.



Stap 5. Kies in het gebied Interface van de Infrastructuur het type beveiliging om als een clientstation op het upstream WAP-apparaat te authentiseren uit de vervolgkeuzelijst Beveiligingsinstellingen. De opties zijn:

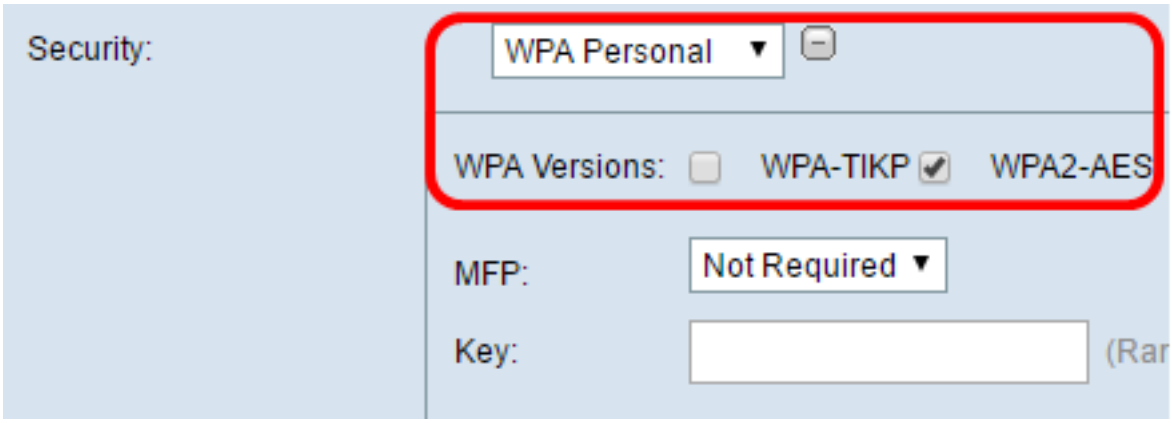
- Geen — Open of geen beveiliging. Dit is de standaard. Als dit is geselecteerd, slaat u over naar Stap 18.
- Persoonlijk - WAP Persoonlijk kan de sleutels van lengte 8-63 tekens ondersteunen. WAP2 wordt aanbevolen omdat het een krachtiger coderingsstandaard heeft. Naar Stap 6 om te configureren.
- WAP Enterprise — WAP Enterprise is geavanceerder dan WAP Persoonlijk en is de aanbevolen beveiliging voor verificatie. Het maakt gebruik van Protected Extenability Verifier Protocol (PEAP) en Transport Layer Security (TLS). Naar Stap 9 om te configureren. Dit type beveiliging wordt vaak in een Office-omgeving gebruikt en heeft een RADIUS-server (Dial-In User Service) op afstand nodig. Klik hier om meer te weten te komen over RADIUS-servers.



Opmerking: In dit voorbeeld, wordt de Persoonlijke van WAP gekozen.

Stap 6. Klik op **+** en controleer het dialoogvenster WAP ofWAP2-AES om te bepalen welk type WAP-encryptie de interface van de infrastructuurclient zal gebruiken.

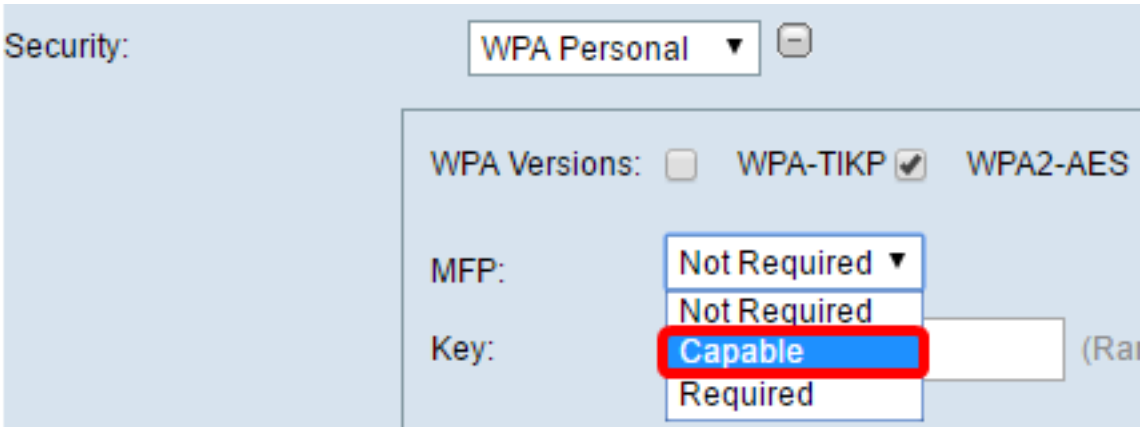
Opmerking: Als al uw draadloze apparatuur WAP2 ondersteunt, stelt u de beveiliging van de infrastructuurclient in op WAP2-AES. De coderingsmethode is RC4 voor WAP en Advanced Encryption Standard (AES) voor WAP2. WAP2 wordt aanbevolen omdat deze een krachtigere coderingsstandaard heeft. Bijvoorbeeld, wordt WAP2-AES gebruikt.



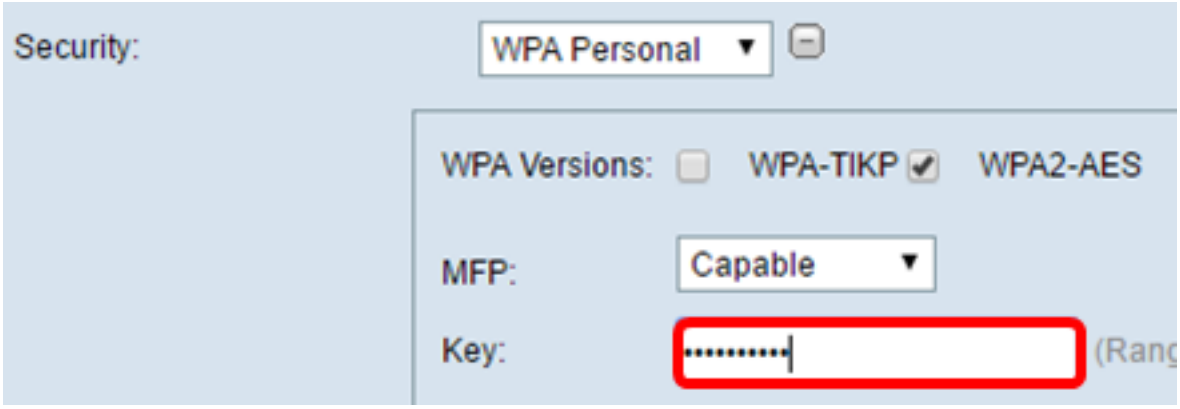
Stap 7. (Optioneel) Als u WAP2-AES in Stap 6 hebt ingeschakeld, kiest u een optie uit de vervolgkeuzelijst Management Frame Protection (MFP) of u wilt dat de WAP beschermde frames heeft. Klik hier voor meer informatie over MFP. De opties zijn:

- Niet vereist — schakelt de clientondersteuning voor MFP uit.
- Geschikt — staat zowel MFP-capabel als klanten die MFP niet ondersteunen toe om zich bij het netwerk aan te sluiten. Dit is de standaard MFP-instelling in WAP.
- Vereist — Clients mogen alleen worden geassocieerd als MFP is overeengekomen. Als de apparaten geen MFP ondersteunen, mogen ze zich niet bij het netwerk aansluiten.

Opmerking: Bijvoorbeeld, Capable wordt gekozen.



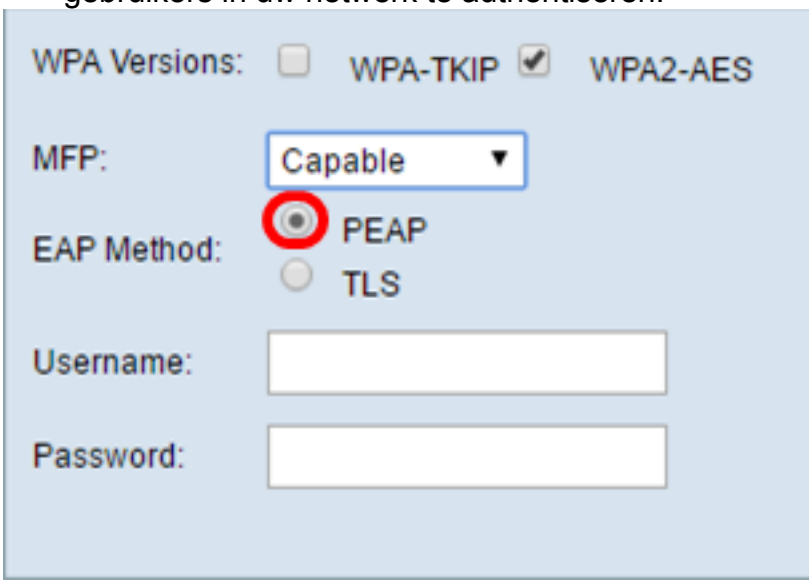
Stap 8. Voer de WAP-encryptie-toets in het veld *Key*. De toets moet 8-63 tekens lang zijn. Dit is een combinatie van letters, cijfers en speciale tekens. Het is het wachtwoord dat wordt gebruikt bij de eerste verbinding met het draadloze netwerk. Ga dan naar Stap 18.



Stap 9. Als u in Stap 5 voor WAP Enterprise hebt gekozen, klikt u op een radioknop voor de MAP-methode.

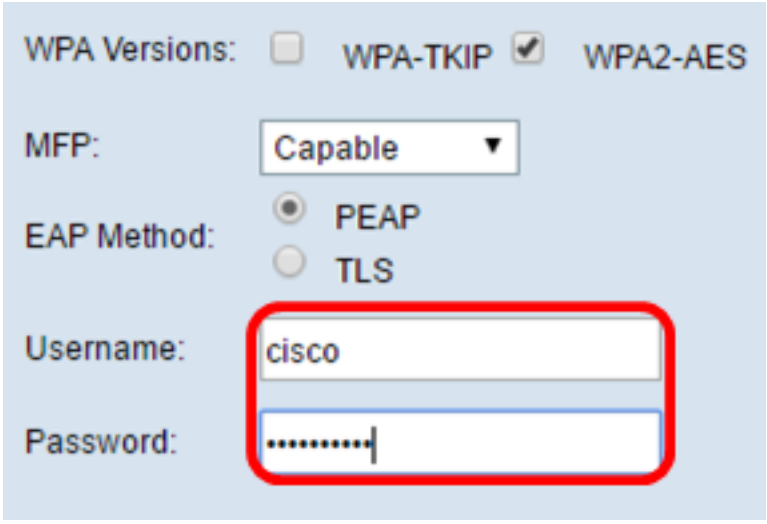
De beschikbare opties zijn als volgt gedefinieerd:

- PEAP —Dit protocol geeft elke draadloze gebruiker onder de WAP individuele gebruikersnamen en wachtwoorden die AES-encryptie-standaarden ondersteunen. Aangezien PEAP een op wachtwoord gebaseerde veiligheidsmethode is, is uw WiFi-beveiliging gebaseerd op de apparaatreferenties van de client. PEAP kan een potentieel ernstig veiligheidsrisico opleveren als je zwakke wachtwoorden of ongedekte klanten hebt. Het maakt gebruik van TLS, maar vermijdt de installatie van digitale certificaten op elke cliënt. In plaats daarvan biedt het authenticatie door een gebruikersnaam en wachtwoord.
- TLS — TLS vereist dat elke gebruiker over een aanvullend certificaat beschikt om toegang te krijgen. TLS is veiliger als u de extra servers en de noodzakelijke infrastructuur hebt om gebruikers in uw netwerk te authentiseren.



Opmerking: Voor dit voorbeeld wordt PEAP gekozen.

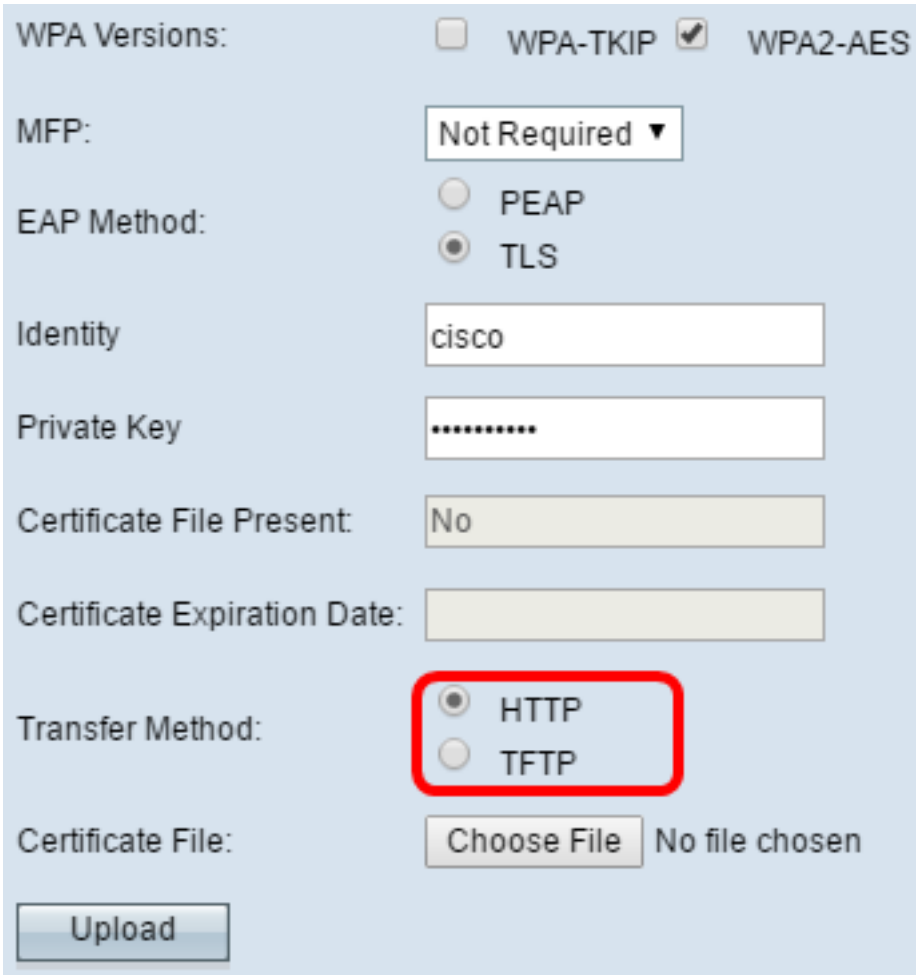
Stap 10. Voer de gebruikersnaam en het wachtwoord voor de infrastructuurclient in de velden *Gebruikersnaam* en *Wachtwoord in*. Dit is de inloginformatie die wordt gebruikt om verbinding te maken met de interface van de infrastructuurclient. raadpleeg de interface van uw infrastructuurclient om deze informatie te vinden. Ga dan naar Stap 18.



Stap 1. Als u in Stap 9 op TLS hebt geklikt, specificeert u de identiteit en de privé-sleutel van de infrastructuurclient in de velden *Identity* en *Private Key.*

Stap 12. Klik in het gebied van de overdrachtmethode op een radioknop van de volgende opties:

- TFTP — Trial File Transfer Protocol (TFTP) is een vereenvoudigde ongedekte versie van File Transfer Protocol (FTP). Het wordt hoofdzakelijk gebruikt om software te distribueren of apparaten tussen bedrijfsnetwerken te authentiseren. Als u op TFTP klikte, slaat u over naar Stap 15.
- HTTP — Hypertext Transfer Protocol (HTTP) biedt een eenvoudig uitdaging-responsverificatiekader dat door een client kan worden gebruikt om een verificatiekader te bieden.

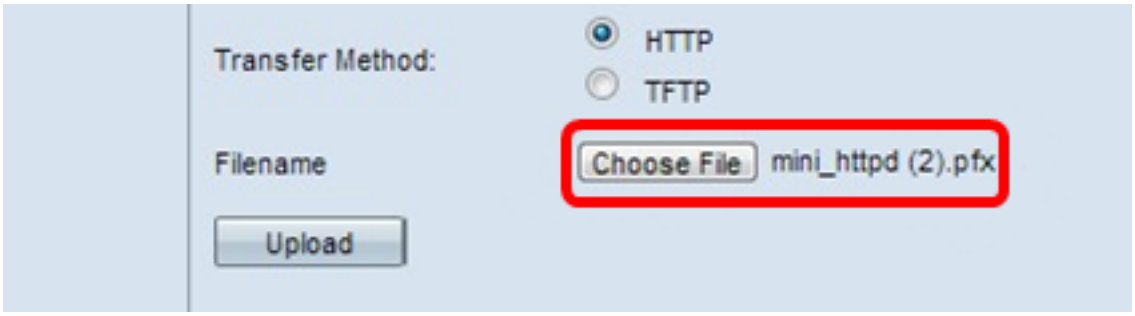


Opmerking: Als er al een certificaatbestand op de WAP aanwezig is, worden de velden *certificaatbestand* en *certificaatverloopdatum* reeds met de relevante informatie ingevuld. Anders zijn ze leeg.

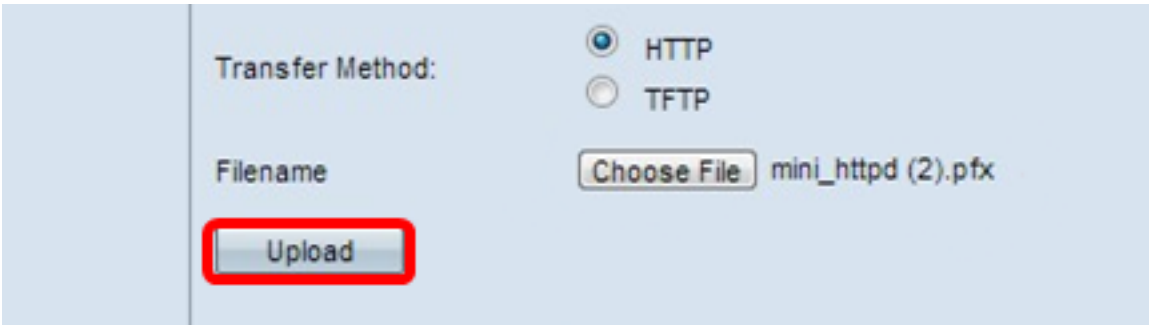
HTTP

Stap 13. Klik op de knop **Bestand kiezen** om een certificaatbestand te vinden en te selecteren. Het bestand moet de juiste bestandsextensie hebben (zoals .pem of .pfx), anders wordt het bestand niet geaccepteerd.

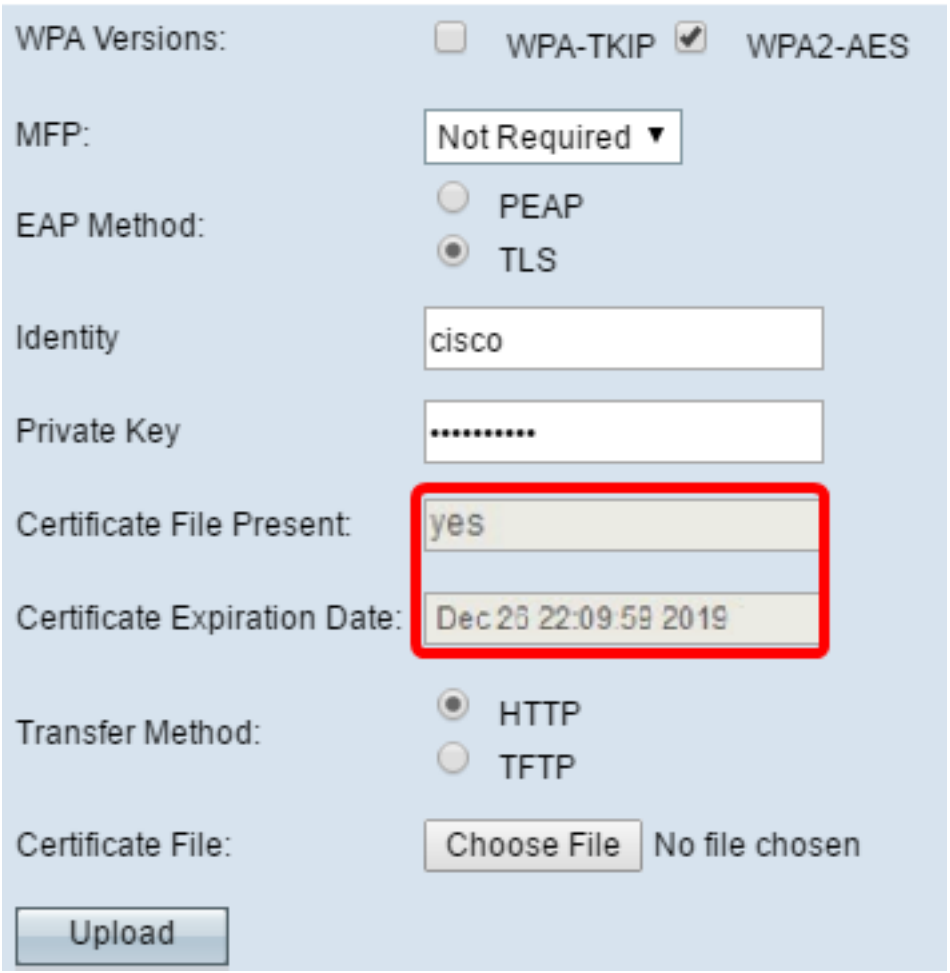
Opmerking: In dit voorbeeld wordt mini_httpd(2).pfx gekozen.



Stap 14. Klik op **Upload** om het geselecteerde certificaatbestand te uploaden. Naar Stap 18.



De velden *certificaatbestand* en *certificaatverloopdatum* worden automatisch bijgewerkt.



TFTP

Stap 15. Als u op TFTP hebt geklikt in Stap 12, specificeert u de bestandsnaam van het certificaatbestand in het veld *Bestandsnaam*.

Opmerking: In dit voorbeeld wordt mini_httpd.pem gebruikt.

Stap 16. Voer het adres van de TFTP-server in het veld *IPv4-adres van de TFTP-server*.

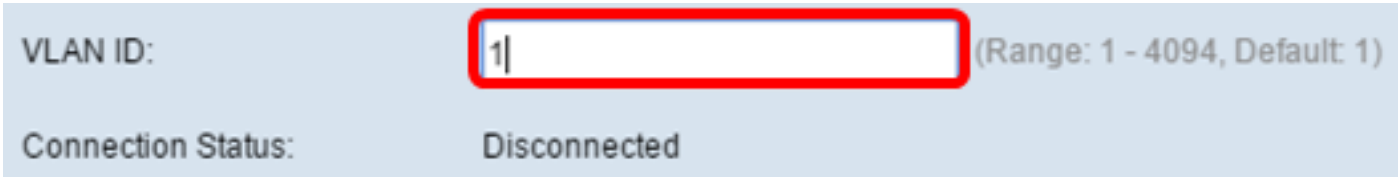
Opmerking: In dit voorbeeld. 192.168.1.20 wordt gebruikt als het TFTP-serveradres.

Stap 17. Klik op de knop **Upload** om het gespecificeerde certificaatbestand te uploaden.

De velden *certificaatbestand* en *certificaatverloopdatum* worden automatisch bijgewerkt.

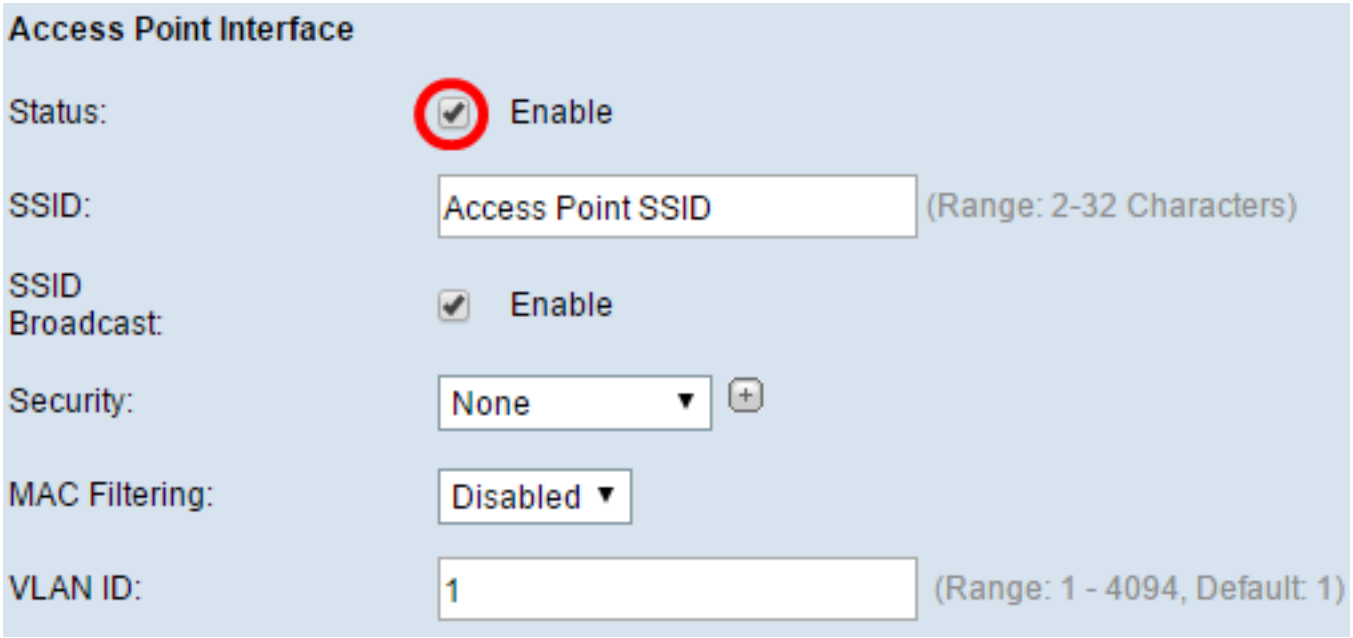
Stap 18. Voer de VLAN-id in voor de interface van de infrastructuurclient. De standaardinstelling is 1.

Opmerking: Bijvoorbeeld, de standaard VLAN ID wordt gebruikt.



Access point-interface

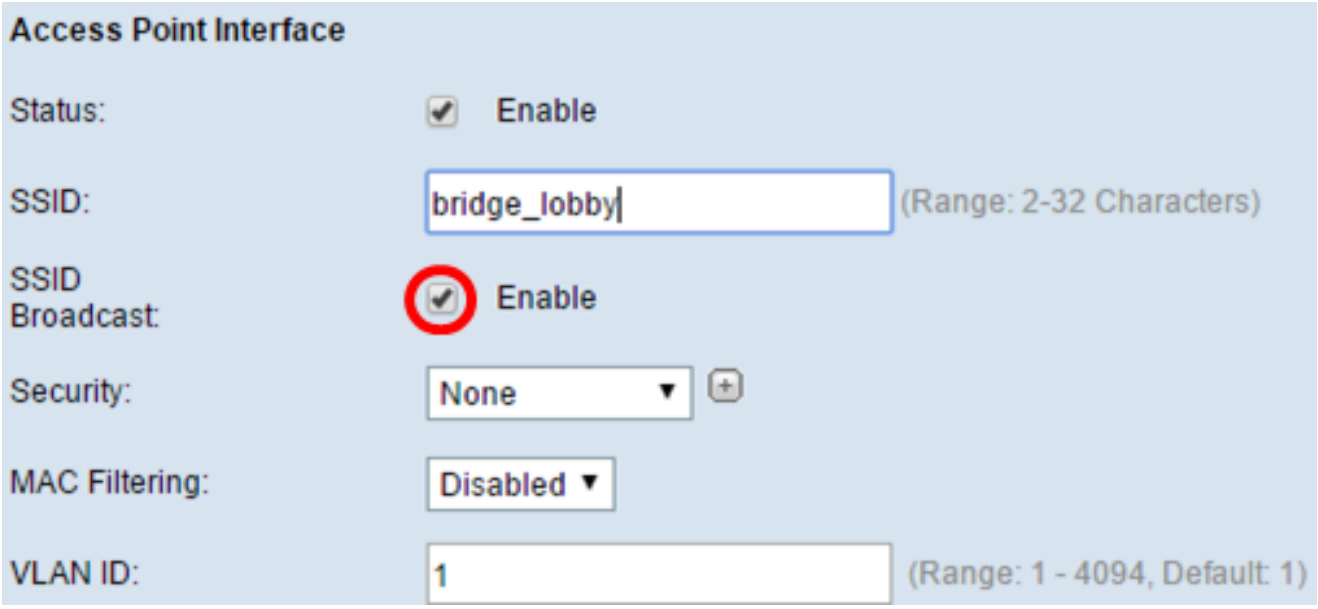
Stap 1. Controleer het dialoogvenster Status **inschakelen** om overbrugging op de interface van het access point mogelijk te maken.



Stap 2. Voer de SSID voor het access point in het veld *SSID in*. De lengte van SSID moet tussen 2 tot 32 tekens liggen. De standaard is Access Point SSID.

Opmerking: Bijvoorbeeld, SSID gebruikt is bridge_lobby.

Stap 3. (Optioneel) Als u de SSID niet wilt uitzenden, schakelt u het vakje SSID Broadcast **inschakelen** uit. Door dit te doen wordt het toegangspunt onzichtbaar voor hen die op zoek zijn naar draadloze toegangspunten; het kan alleen worden verbonden door iemand die de SSID al kent. SSID Broadcast wordt standaard ingeschakeld.

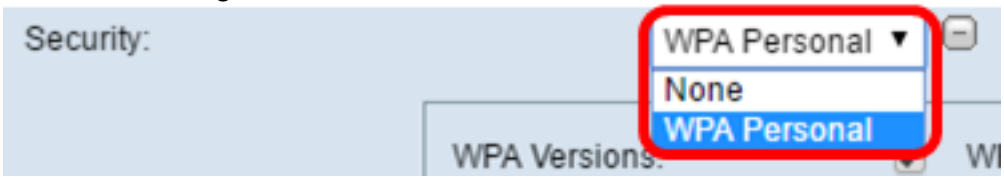


Stap 4. Kies het type beveiliging om downloads naar de WAP-indeling te controleren in de vervolgkeuzelijst Beveiliging.

De beschikbare opties zijn als volgt gedefinieerd:

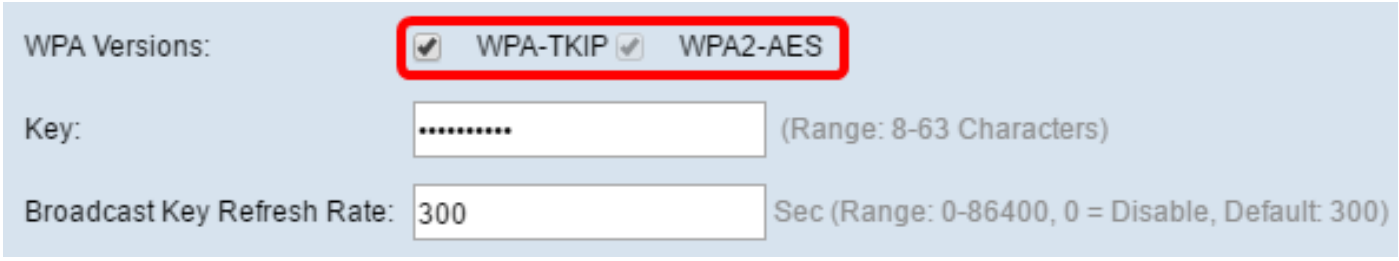
- Geen — Open of geen beveiliging. Dit is de standaardwaarde. Naar Stap 10 indien u dit kiest.
- Persoonlijk - Wi-Fi Protected Access (WAP) Persoonlijk kan toetsen van 8 tot 63 tekens lang ondersteunen. De coderingsmethode is TKIP of de Coax Cipher Mode met Block Chaining Message Verification Code Protocol (CCMP). WAP2 met CCMP wordt aanbevolen omdat deze een krachtiger coderingsstandaard heeft, Advanced Encryption Standard (AES),

vergeleken met het Temporal Key Integrity Protocol (TKIP) dat slechts een 64-bits RC4-standaard gebruikt.

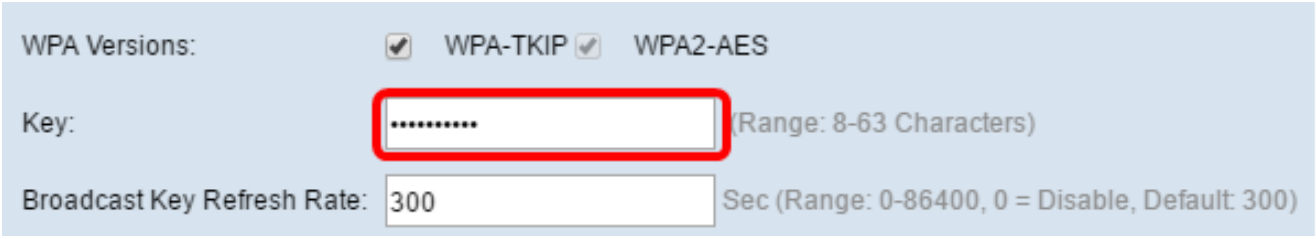


Stap 5. Controleer **WAP-TKIP** of **WAP2-AES** aanvinkvakje om te bepalen welk type WAP-encryptie de interface van het access point zal gebruiken. Deze zijn standaard ingeschakeld.

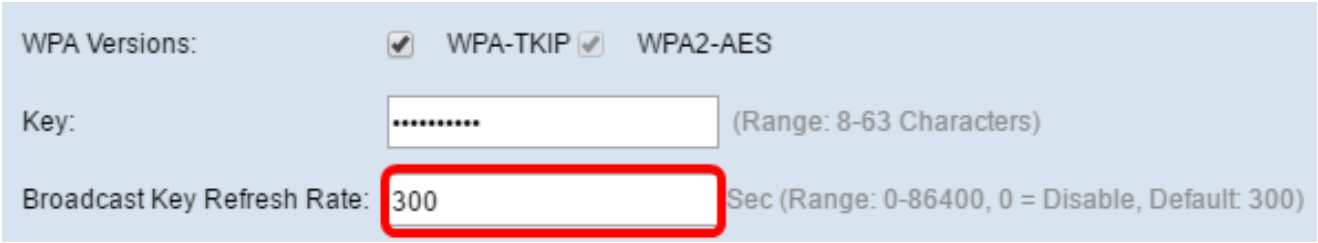
Opmerking: Als al uw draadloze apparatuur WAP2 ondersteunt, stelt u de beveiliging van de infrastructuurclient in op WAP2-AES. De coderingsmethode is RC4 voor WAP en Advanced Encryption Standard (AES) voor WAP2. WAP2 wordt aanbevolen omdat deze een krachtigere coderingsstandaard heeft. Bijvoorbeeld, wordt WAP2-AES gebruikt.



Stap 6. Voer de gedeelde WAP-toets in het veld *Key*. De toets moet 8-63 tekens lang zijn en kan alfanumerieke tekens, hoofdletters en kleine letters en speciale tekens bevatten.



Stap 7. Voer het tarief in het veld *Broadcast Key Refresh Rate* in. Met de uitzending-toets wordt het interval gespecificeerd waarmee de beveiligingstoets wordt ververst voor klanten die aan dit toegangspunt zijn gekoppeld. Het tarief moet tussen 0-86400 liggen, met een waarde van 0 die de functie uitschakelt. De standaard is 300.

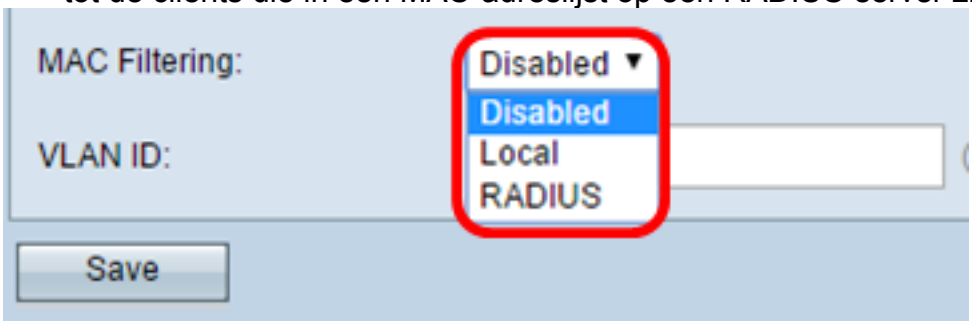


Stap 8. Kies het type MAC-filtering dat u wilt configureren voor de interface van het access point uit de vervolgkeuzelijst MAC-filtering. Indien ingeschakeld, worden gebruikers toegang tot de WAP verleend of geweigerd op basis van het MAC-adres van de client die zij gebruiken.

De beschikbare opties zijn als volgt gedefinieerd:

- Uitgeschakeld — Alle klanten hebben toegang tot het stroomopwaarts netwerk. Dit is de standaardwaarde.

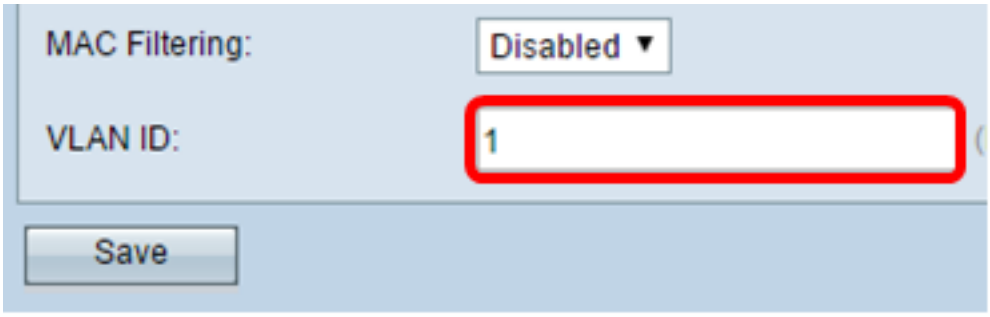
- Lokaal — De reeks klanten die toegang kunnen krijgen tot het upstream netwerk is beperkt tot de klanten die zijn gespecificeerd in een lokaal gedefinieerde MAC-adreslijst.
- RADIUS - De reeks clients die toegang kunnen hebben tot het upstream netwerk is beperkt tot de clients die in een MAC-adreslijst op een RADIUS-server zijn gespecificeerd.



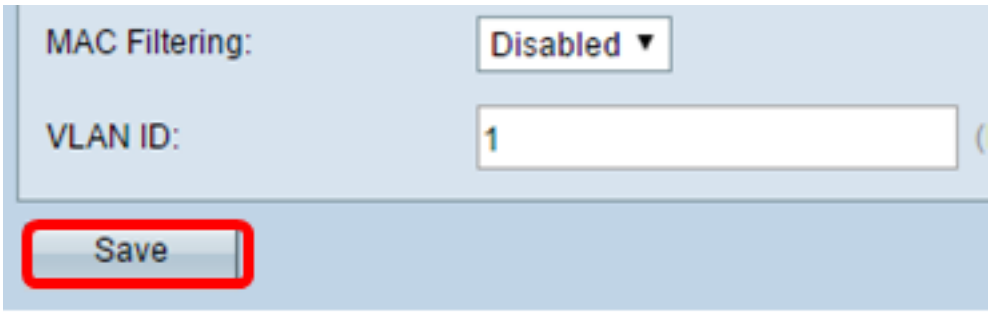
Opmerking: Bijvoorbeeld, Gehandicapten wordt geselecteerd.

Stap 9. Voer de VLAN-id in het veld *VLAN-ID* in voor de interface van het access point.

Opmerking: Om het overbruggen van pakketten mogelijk te maken, zou de configuratie van VLAN voor de interface van het toegangspunt en de bekabelde interface moeten overeenkomen met die van de interface van de infrastructuurclient.



Stap 10. Klik op **Opslaan** om uw wijzigingen op te slaan.



U hebt nu een werkgroepbridge op een draadloos access point ingesteld.