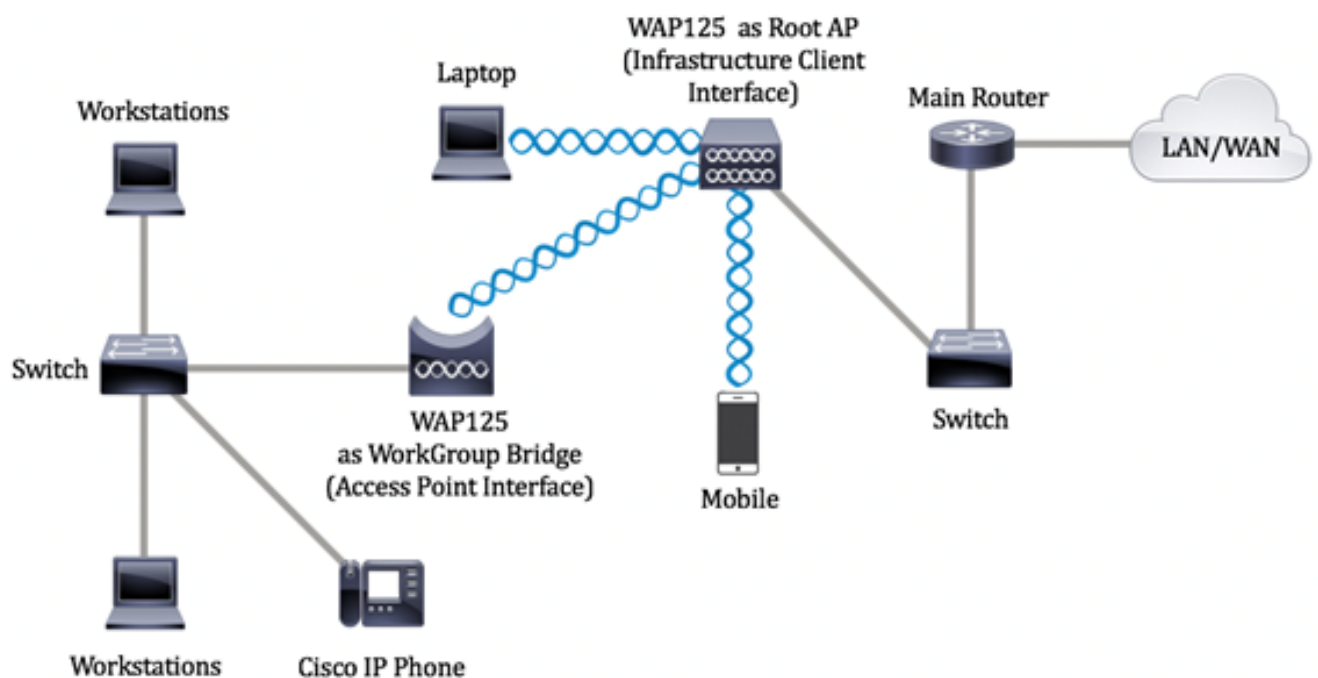


Instellingen werkgroepbridge voor WAP125 of WAP581 access points

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.

De topologie hieronder illustreert een model van de bridge van de steekproef. Draadloze apparaten zijn aangesloten op een switch die zich verbindt met de LAN-interface van de WAP. In het onderstaande voorbeeld werkt WAP125 als een access point interface die verbonden is met de infrastructuur client interface.



Dit artikel geeft instructies hoe u de instellingen van de werkgroepbridge tussen twee draadloze access points kunt configureren.

Toepasselijke apparaten

- WAP125
- WAP581

Softwareversie

- 1.0.0.4 — WAP581

Instellingen werkgroepbridge instellen

Voordat u de werkgroepbridge op het WAP-apparaat configureren, houdt u deze richtlijnen in:

- Alle WAP-apparaten die aan WorkGroup Bridge deelnemen, moeten de volgende identieke instellingen hebben:
 - radio
 - IEEE 802.11-modus
 - kanaalbandbreedte
 - Kanaal (Auto wordt niet aanbevolen)

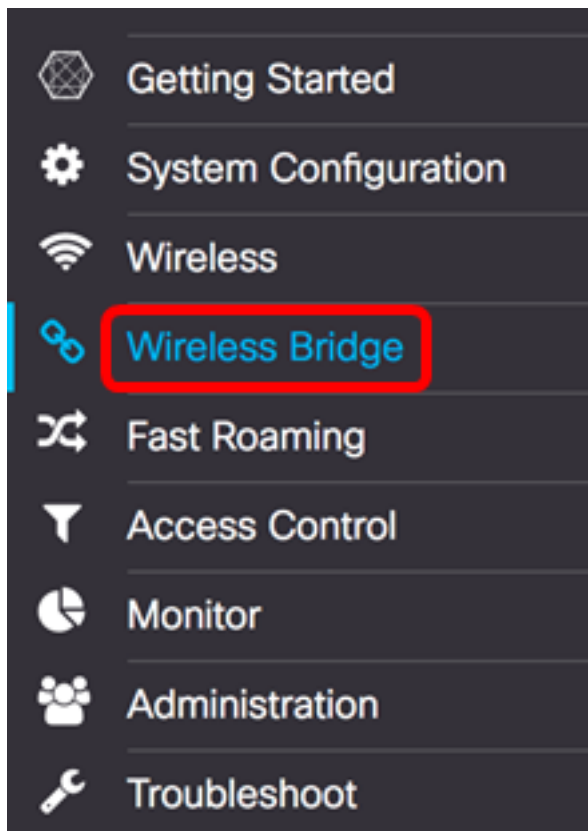
Opmerking: Om te leren hoe u deze instellingen op WAP125 kunt configureren klikt u [hier](#) voor instructies. Klik [hier](#) voor WAP581.

- De wijze van de bridge van het werk steunt momenteel slechts IPv4 verkeer.
- De modus Werkgroepbridge wordt niet ondersteund door een Single Point Setup. Als u WAP581 access points hebt, schakelt u SPS of clustering eerst uit voordat u de instellingen voor de werkgroepbridge configureren. Voor instructies hoe u de SPS-instellingen op uw WAP kunt configureren klikt u [hier](#) op.

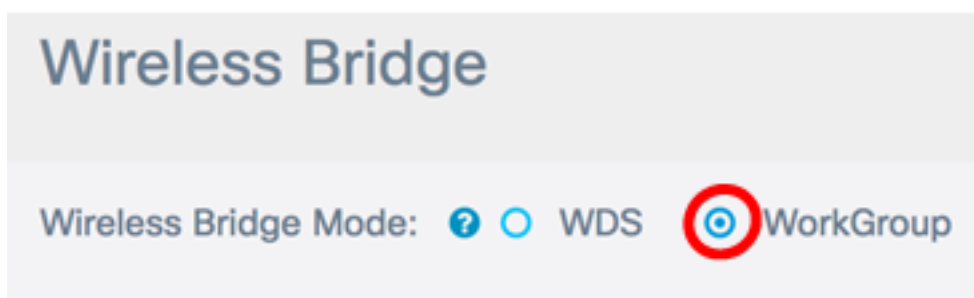
Infrastructuurclientinterface configureren

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van WAP en kies vervolgens **draadloze brug**.

Opmerking: Welke opties er beschikbaar zijn, is mede afhankelijk van het exacte model van het apparaat. In dit voorbeeld wordt WAP125 gebruikt.



Stap 2. Klik op de knop **Workgroup**.



Stap 3. Controleer het vakje **uplink**.

	WGB Port	Enabled	Radio	SSID
<input checked="" type="checkbox"/>	Uplink	<input type="checkbox"/>	Radio 1 (2.4 GHz)	Upstream SSID
<input type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)	Downstream SSID

Stap 4. Klik op het pictogram **Bewerken**.



<input type="checkbox"/>	WGB Port	Enabled	Radio	SSID
<input checked="" type="checkbox"/>	Uplink	<input type="checkbox"/>	Radio 1 (2.4 GHz)	Upstream SSID
<input type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)	Downstream SSID

Stap 5. Controleer het aankruisvakje Enabled om interface-infrastructuur in te schakelen.



<input type="checkbox"/>	WGB Port	Enabled	Radio
<input checked="" type="checkbox"/>	Uplink	<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)

Stap 6. Kies 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.

Enabled	Radio
<input checked="" type="checkbox"/>	Radio 1 (2.4 GHz)
<input checked="" type="checkbox"/>	Radio 2 (5 GHz)

Opmerking: In dit voorbeeld wordt Radio 2 (5 GHz) gekozen.

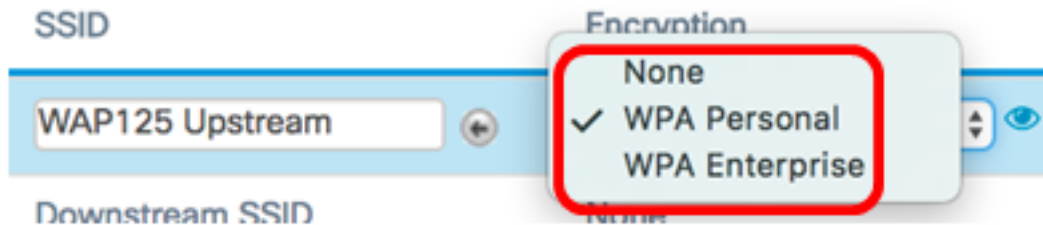
Stap 7. Voer de naam van de Service Set Identifier (SSID) in het veld *SSID*. Dit dient als de verbinding tussen het apparaat en de externe client. U kunt 2 tot 32 tekens invoeren voor de client van de infrastructuur.

Opmerking: In dit voorbeeld wordt WAP125 Upstream gebruikt.

Radio	SSID
Radio 2 (5 GHz)	WAP125 Upstream


Opmerking: De pijl naast SSID is beschikbaar voor SSID Scannen. Deze optie is standaard uitgeschakeld en is alleen ingeschakeld als AP Detectie is ingeschakeld in de detectie van AP-schurken, die standaard ook uitgeschakeld wordt.

Stap 8. Kies het type beveiliging dat u als een client-station op het WAP-apparaat wilt authenticeren in de vervolkeuzelijst Encryption. De opties zijn:



- Geen — Open of geen beveiliging. Dit is de standaard. Als dit is geselecteerd, slaat u over naar [Stap 2](#).
- Persoonlijk - WAP Persoonlijk kan de sleutels van lengte 8-63 tekens ondersteunen. WAP2 wordt aanbevolen omdat het een krachtiger coderingsstandaard heeft.
- WAP Enterprise — WAP Enterprise is geavanceerder dan WAP Persoonlijk en is de aanbevolen beveiliging voor verificatie. Het maakt gebruik van Protected Extensibility Verifier Protocol (PEAP) en Transport Layer Security (TLS). Naar [Stap 12](#) om te configureren. Dit type beveiliging wordt vaak in een kantooromgeving 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 9. Klik op het  pictogram en controleer het aanvinkvakje WAP-TKIP of WAP2-AES om te bepalen welk soort WAP-encryptie de interface van de infrastructuurclient zal gebruiken.

Security Setting

WPA Versions: WPA-TKIP WPA2-AES

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. In dit voorbeeld wordt WAP2-AES gebruikt.

Stap 10. (Optioneel) Als u WAP2-AES in Stap 9 hebt ingeschakeld, kies dan 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.

WPA Versions: WPA-TKIP WPA2-AES

MFP:

Opmerking: In dit voorbeeld wordt Capable gekozen.

Stap 1. Voer de sleutel van de WAP-encryptie 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 21](#).

MFP:

Key: ?

Show Key as Clear Text

[Stap 12](#). Als u in Stap 8 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 authenticeren. Als u deze optie kiest, slaat u over naar [Stap 14](#).

WPA Versions: WPA-TKIP WPA2-AES

MFP:

EAP Method:

 PEAP TLS

Opmerking: Voor dit voorbeeld wordt PEAP gekozen.

Stap 13. Voer de gebruikersnaam en het wachtwoord voor de infrastructuurclient in de velden *Naam* 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 21](#).

EAP Method: PEAP TLS

Username:

Password:

Show Key as Clear Text

[Stap 14](#) . Als u in Stap 12 op TLS hebt geklikt, specificeert u de identiteit en de privé-sleutel van de infrastructuurclient in de velden Identity en Private Key.

EAP Method: PEAP TLS

Identity

Private Key

Show Key as Clear Text

Stap 15. Klik in het gebied met 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 authenticeren. Als u op TFTP klikt, slaat u over naar [Stap 18](#).
- HTTP — Hypertext Transfer Protocol (HTTP) biedt een eenvoudig uitdaging-responsverificatiekader dat door een client kan worden gebruikt om een verificatiekader te bieden.

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Opmerking: Als er al een certificaatbestand in het WAP aanwezig is, worden de velden Aanwezigheidsbestand en Vervaldatum certificaat al met de relevante informatie ingevuld. Anders zijn ze leeg.

HTTP

Stap 16. Klik op de knop **Bladeren** 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 Certificate.pfx geselecteerd.

Stap 17. Klik op **Upload** om het geselecteerde certificaatbestand te uploaden. Naar [Stap 21](#).

Certificate File Present:

Certificate Expiration Date:

Transfer Method: HTTP TFTP

Certificate File: Certificate.pfx

De velden Aanwezigheidsbestand en Vervaldatum certificaat worden automatisch bijgewerkt.

TFTP

[Stap 18](#). (Optioneel) Als u in Stap 15 op TFTP hebt gedrukt, specificeert u de bestandsnaam van het certificaatbestand in het veld *Bestandsnaam*.

Transfer Method: HTTP TFTP

Filename

Opmerking: In dit voorbeeld wordt certificaat.pfx gebruikt.

Stap 19. Voer het adres van de TFTP-server in het veld *IPv4-adres van de TFTP-server*.

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

Opmerking: In dit voorbeeld. 192.168.100.108 wordt gebruikt als het TFTP-serveradres.

Stap 20. Klik op de knop **Upload** om het gespecificeerde certificaatbestand te uploaden.

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

De velden Aanwezigheidsbestand en Vervaldatum certificaat worden automatisch bijgewerkt.

[Stap 21.](#) Klik op **OK** om het Security SETTING-venster te sluiten.

Het gebied met de verbindingstatus geeft aan of de WAP is aangesloten op het WAP-apparaat.

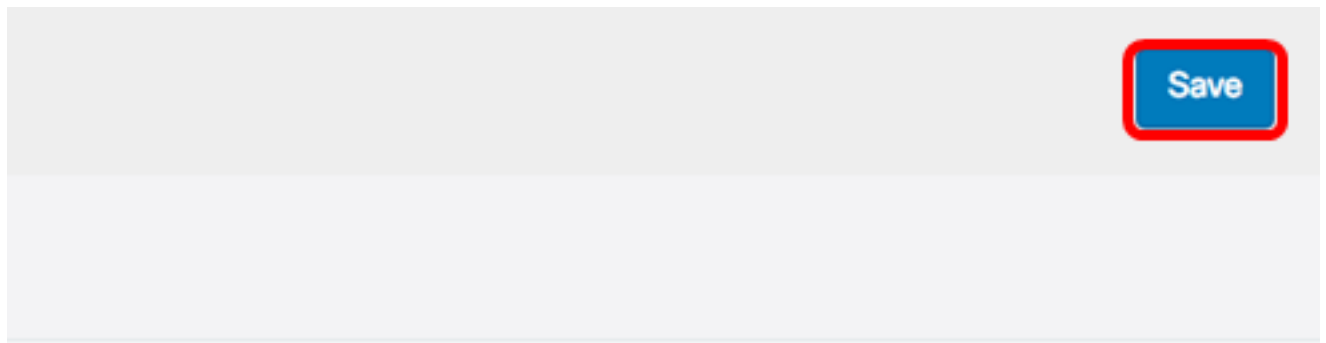
Encryption	Connection Status
<input type="text" value="WPA Personal"/>	<input type="text" value="Disconnected"/>

[Stap 22.](#) Voer de VLAN-id in voor de interface van de infrastructuurclient. De standaardinstelling is 1.

Connection Status	VLAN ID
<input type="text" value="Disconnected"/>	<input type="text" value="1"/>

Opmerking: Bijvoorbeeld, de standaard VLAN ID wordt gebruikt.

Stap 23. Klik op **Opslaan** om de geconfigureerde instellingen op te slaan.



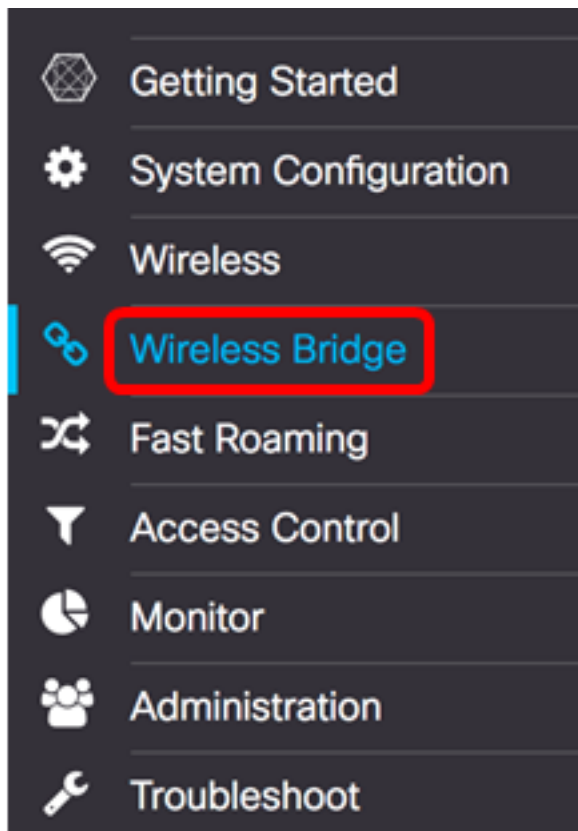
Connection Status	VLAN ID	SSID Broadcast	Client Filter
Disconnected	<input type="text" value="1"/>	N/A	N/A
N/A	1	<input checked="" type="checkbox"/>	Disabled

U hebt nu de instellingen voor interface-interface van infrastructuur op uw WAP met succes ingesteld.

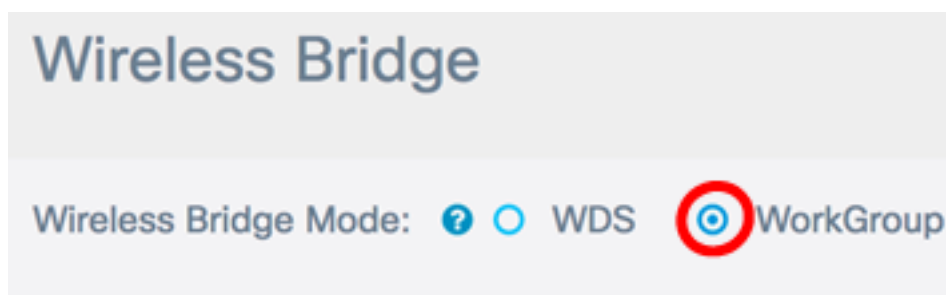
Interface voor access point

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma van WAP en kies vervolgens **draadloze brug**.


Opmerking: Welke opties er beschikbaar zijn, is mede afhankelijk van het exacte model van het apparaat. In dit voorbeeld wordt WAP125 gebruikt.



Stap 2. Klik op de knop **Workgroup**.



Stap 3. Controleer het vakje **Downlink**.

	WGB Port	Enabled	Radio
<input type="checkbox"/>	Uplink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)
<input checked="" type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)

Stap 4. Klik op de knop **Bewerken**.



<input type="checkbox"/>	WGB Port	Enabled	Radio
<input type="checkbox"/>	Uplink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)
<input checked="" type="checkbox"/>	Downlink	<input checked="" type="checkbox"/>	Radio 2 (5 GHz)

Stap 5. Controleer het aankruisvakje Enabled om overbrugging op de interface van het access point mogelijk te maken.



Stap 6. Voer de SSID voor het access point in het veld *SSID in*. De lengte van SSID moet tussen 2 tot 32 tekens liggen. Het standaard is Downstream SSID.



Opmerking: Bijvoorbeeld, is SSID gebruikt WAP125 Downstream.

Stap 7. 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 13](#) als u deze optie kiest.
- Persoonlijk - Wi-Fi Protected Access (WPA) 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 8. (Optioneel) Controleer het aankruisvakje WAP-TKIP om de WAP-TKIP-encryptie te bepalen die de interface van het access point zal gebruiken. Dit is standaard ingeschakeld.

Opmerking: WPA-AES is grijselijk en kan niet worden uitgeschakeld. In dit voorbeeld is WAP-TKIP niet ingeschakeld.

Security Setting

WPA Versions:

WPA-TKIP WPA2-AES

Stap 9. Voer de gedeelde WAP-toets in het veld Sleutel in. De toets moet 8-63 tekens lang zijn en kan alfanumerieke tekens, hoofdletters en kleine letters en speciale tekens bevatten.

WPA Versions:

WPA-TKIP WPA2-AES

Key: 

.....

Show Key as Clear Text

Stap 10. Voer het tarief in het veld Vernieuwingsnelheid van de uitzending in. Met de uitzending-toets wordt het interval gespecificeerd waarmee de beveiligingstoets wordt verversd voor klanten die aan dit toegangspunt zijn gekoppeld. Het tarief moet tussen 0-86400 liggen, met een waarde van 0 die de functie uitschakelt.

Broadcast Key Refresh Rate: 

86400

Opmerking: In dit voorbeeld wordt 86400 gebruikt.

Stap 1. Kies een optie uit de MFP vervolgkeuzelijst 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.

Broadcast Key Refresh Rate: 

86400

MFP:

Capable 

Opmerking: Bijvoorbeeld, Capable wordt gekozen.

Stap 12. Klik op **OK** om de beveiligingsinstellingen op te slaan.

Security Setting

WPA Versions:

WPA-TIKP WPA2-AES

Key: [?](#)

.....

Show Key as Clear Text

Broadcast Key Refresh Rate: [?](#)

86400


MFP:

Capable

OK

cancel

Het gebied met de verbindingstatus geeft niet van toepassing of N.B. aan.


Encryption	Connection Status
WPA Personal	Disconnected
WPA Personal 	N/A

[Stap 13](#). Voer de VLAN-id in het veld VLAN-id in voor de interface van het access point.

Opmerking: Om het overbruggen van pakketten toe te staan, zou de configuratie van VLAN voor de interface van het toegangspunt en de bekabelde interface die van de interface van de infrastructuurclient moeten passen.

N/A	1 
-----	---

Stap 14. Controleer het veld SSID Broadcast als u wilt dat de downstreamSSID wordt uitgezonden. SSID Broadcast wordt standaard ingeschakeld.

VLAN ID	SSID Broadcast	Client Filter
1	N/A	N/A
1		Disabled

Stap 15. 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: In dit voorbeeld, Gehandicapten wordt geselecteerd.

Stap 16. Klik op **Opslaan** om uw wijzigingen op te slaan.



The screenshot shows a configuration interface. At the top right, there is a blue 'Save' button with a red border. Below it is a table with the following columns: 'Connection Status', 'VLAN ID', 'SSID Broadcast', and 'Client Filter'. The table has two rows. The first row shows 'Disconnected', '1', 'N/A', and 'N/A'. The second row is highlighted in light blue and shows 'N/A', a text input field containing '1', a checked checkbox, and a dropdown menu set to 'Disabled'.

Connection Status	VLAN ID	SSID Broadcast	Client Filter
Disconnected	1	N/A	N/A
N/A	<input type="text" value="1"/>	<input checked="" type="checkbox"/>	Disabled

U hebt nu de instellingen voor de werkgroepbridge op uw draadloze toegangspunten met succes ingesteld.