

Een VAP configureren op WAP351, WAP131 en WAP371

Doel

Virtual Access Point (VAP's) segmenteert het draadloze LAN-netwerk in meerdere broadcast-domeinen die het draadloze equivalent van Ethernet VLAN's zijn. VAP's simuleren meerdere toegangspunten in één fysiek WAP-apparaat. Tot vier VAP's worden ondersteund op Cisco WAP131 en maximaal acht VAP's worden ondersteund op Cisco WAP351 en WAP371.

Het doel van dit document is om u te tonen hoe u een VAP op de access points WAP351, WAP131 en WAP371 moet configureren.

Toepasselijke apparaten

- WAP351
- WAP131
- WAP371

Softwareversie

- V1.0.0.39 (WAP351)
- V1.0.0.39 (WAP131)
- V1.2.0.2 (WAP371)

Een VAP toevoegen en configureren

Opmerking: Elke VAP wordt geïdentificeerd door een door de gebruiker ingesteld Service Set Identifier (SSID). Meerdere VAP's kunnen niet dezelfde SSID-naam hebben.

Opmerking: Om uw draadloos netwerk te laten functioneren, moet de radio waarin uw geconfigureerde VAP is gekoppeld, ingeschakeld en correct geconfigureerd zijn. Zie [Basisradio-instellingen configureren op WAP131 en WAP351](#) of [basisradio-instellingen configureren op WAP371](#) voor meer informatie

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en navigeer naar **draadloos > netwerken**. De pagina *Netwerken* verschijnt:

Networks

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

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

Save

Stap 2. Selecteer in het veld *Radio* de radioknop voor de draadloze radio waarop u VAPs wilt configureren.

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

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

Stap 3. Als u een nieuwe VAP wilt toevoegen, klikt u op **Toevoegen**. Er verschijnt een nieuwe VAP in de tabel.

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

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

Opmerking: WAP131 ondersteunt maximaal 4 VAP's, terwijl WAP371 en WAP351 ondersteuning bieden aan maximaal 8 VAP's.

Stap 4. Klik op het aanvinkvakje links van de tabel om het bewerken van een VAP te starten en vervolgens op **Bewerken**. U kunt de velden in de geselecteerde VAP met grijswaarden wijzigen.

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

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

Stap 5. Zorg ervoor dat het vakje *Enable* aangevinkt is om het gebruik van de VAP in te schakelen.

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

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

Virtual Access Points (SSIDs)								
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

Add Edit Delete

Stap 6. In het veld *VLAN-id* specificeert u de VLAN-id die u met de VAP wilt associëren. Als u WAP131 of WAP371 gebruikt, voer dan in de VLAN-ID. De max-waarde die u kunt invoeren is 4094.

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

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

Virtual Access Points (SSIDs)								
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

Add Edit Delete

Opmerking: De VLAN-id die wordt ingevoerd, moet op uw netwerk aanwezig zijn en op de juiste manier worden geconfigureerd. Zie [VLAN-configuratie op het WAP351 access point](#), [Tagged en Untagged VLAN-id's beheren op WAP131](#) of [VLAN-id's beheren op WAP371](#) voor meer informatie.

Stap 7. Voer de naam van het draadloze netwerk in het veld SSID Name. Elke VAP moet een unieke SSID naam hebben.

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

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

Virtual Access Points (SSIDs)								
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

Add Edit Delete

Stap 8. Als u wilt dat de naam van SSID aan klanten wordt uitgezonden, controleer dan het vakje *SSID Broadcast* check. Dit zal de naam van SSID aan cliënten in hun lijst van beschikbare netwerken tonen.

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

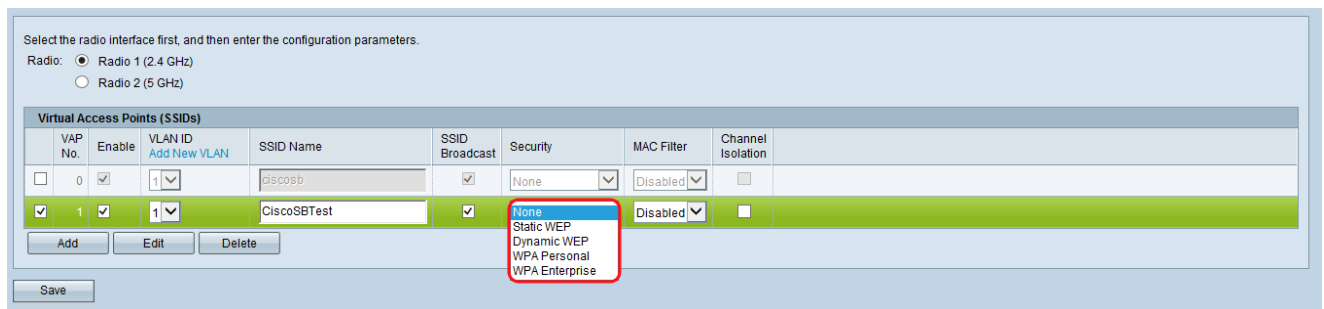
Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)								
VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

Add Edit Delete

Beveiligingsinstellingen configureren

Stap 1. Kies de authenticatiemethode die nodig is om verbinding te maken met de VAP in de vervolgkeuzelijst *Beveiliging*. Als er een andere optie dan **Geen** is geselecteerd, worden er extra velden weergegeven.



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

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

VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSB	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>

Buttons: Add, Edit, Delete, Save

Security dropdown options: None, Static WEP, Dynamic WEP, WPA Personal, WPA Enterprise

De beschikbare opties zijn:

- None
- Statistisch EFN
- Dynamisch EFN
- WPA Persoonlijk
- WAP Enterprise

Opmerking: Persoonlijk en de van WAP Enterprise zijn de geprefereerde authenticatietypen voor maximum veiligheid. Statische EFN en Dynamisch NUL mogen alleen worden gebruikt met oudere apparatuur en vereisen dat de radio wordt ingesteld op 802.11a of 802.11b/g modus. Zie [Basisradio-instellingen configureren op WAP131 en WAP351](#) of [basisradio-instellingen configureren op WAP371](#) voor meer informatie.

Statische Wi

Statische EFN is de minst beveiligde authenticatiemethode. Het versleutelt gegevens in het draadloze netwerk op basis van een statische toets. Het is eenvoudig geworden om deze statische sleutel illegaal te verkrijgen, zodat de authenticatie van de EVN alleen gebruikt zou moeten worden wanneer nodig met oudere apparaten.

Opmerking: Wanneer u *Statische* de optie *Alleen een* beveiligingsmethode selecteert, verschijnt er een melding en vertelt u dat de keuze van de beveiligingsmethode zeer onveilig is.

Stap 1. In de vervolgkeuzelijst *Transfer Key Index* selecteert u de index van de EFN-toets uit de lijst met toetsen hieronder die het apparaat zal gebruiken om gegevens te versleutelen.

Transfer Key Index: 1

Key Length: 2, 3 bits, 4 bits

Key Type: ASCII, Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication: Open System Shared Key

Stap 2. Kies een radioknop van het veld *Key Length* om te specificeren of de toets 64 bits of 128 bits in lengte is.

Transfer Key Index: 1

Key Length: 64 bits, 128 bits

Key Type: ASCII, Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication: Open System Shared Key

Stap 3. In het veld *Key Type* kiest u of u de toetsen in ASCII- of hexadecimale indeling wilt invoeren. ASCII bevat alle letters, cijfers en symbolen die op het toetsenbord aanwezig zijn, terwijl hexadecimaal alleen nummers of letters A-F moet gebruiken.

Transfer Key Index:

Key Length: 64 bits 128 bits

Key Type: ASCII Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication: Open System Shared Key

Stap 4. In het veld Eindtoetsen van EFN voert u maximaal 4 verschillende sleutels van de EFN in voor uw apparaat. Elke client die verbinding moet maken met dit netwerk moet één van de zelfde de sleutels hebben van EFN in de zelfde sleuf die door het apparaat wordt gespecificeerd.

Transfer Key Index:

Key Length: 64 bits 128 bits

Key Type: ASCII Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication: Open System Shared Key

Stap 5. (Optioneel) Klik op het aanvinkvakje in het veld *Weergave sleutel als* het veld *Wis tekst*, als u de tekenkoorden van de toetsen zichtbaar maakt.

Transfer Key Index: 1

Key Length: 64 bits 128 bits

Key Type: ASCII Hex

WEP Keys: (Required: 26)

1: ABCDFE123456789ABCDE34251

2: ABEDC43C2A1B56CD7AE494A56

3: BB4C56AD3E12CB78A9234BD23

4: BEE59A4C5D3E5B7B8AD23169B

Show Key as Clear Text

802.1X Authentication: Open System Shared Key

Opmerking: wanneer u een andere firmware gebruikt op WAP351, WAP131 of WAP371, ontbreekt de *Toon-toets als Clear Text* veld.

Stap 6. In het veld *802.1X-verificatie* specificeert u de verificatiealgoritme die u wilt gebruiken door de opties *Open System* en/of *Shared Key* te kiezen. De authenticatiealgoritme definieert de methode die wordt gebruikt om te bepalen of een clientstation geoorloofd is om met het WAP apparaat te associëren wanneer statische EFN de veiligheidsmodus is.

Transfer Key Index: 1

Key Length: 64 bits 128 bits

Key Type: ASCII Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication: Open System Shared Key

De beschikbare opties zijn als volgt gedefinieerd:

- Open System - De authenticatie stelt elke client-station in staat om met het WAP-apparaat te associëren of dat clientstation al dan niet de juiste EFN-toets heeft. Dit algoritme wordt gebruikt in onbewerkte tekst, IEEE 802.1X, en de modi WAP. Wanneer het authenticatiealgoritme wordt ingesteld op *Open System*, kan elke client associëren met het WAP apparaat.
- Gedeelde sleutel — De authenticatie vereist dat het clientstation de juiste de sleutel van EFN heeft om met het WAP apparaat te associëren. Wanneer het authenticatiealgoritme op *Gedeelde Sleutel* wordt ingesteld, kan een station met een incorrecte sleutel van EFN

niet met het WAP apparaat associëren.

- Open System en Shared Key — Wanneer u beide van deze authenticatie-algoritmen hebt geselecteerd, moeten de clientstations die zijn ingesteld om EFN in gedeelde sleutelmodus te gebruiken, een geldige EFN-toets hebben om met het WAP-apparaat te associëren. Ook kunnen de clientstations die zijn ingesteld om EFN te gebruiken als een open systeem (gedeelde sleutelmodus niet ingeschakeld) zich associëren met het WAP-apparaat, zelfs als de juiste sleutel niet is gebruikt.

Stap 7. Klik op Opslaan.

Dynamisch EFN

Dynamisch EFN verwijst naar de combinatie van 802.1x-technologie en het Extensible Authentication Protocol (EAP). Deze modus vereist het gebruik van een externe RADIUS-server om gebruikers te authentifieren. Voor het WAP-apparaat is een RADIUS-server vereist die EAP ondersteunt, zoals de Microsoft Internet Authentication Server. Om met Microsoft Windows-clients te werken, moet de verificatieserver Protected EAP (PEAP) en MSCHAP v2 ondersteunen. U kunt een van een verscheidenheid aan authenticatiemethoden gebruiken die de IEEE 802.1X-modus ondersteunt, inclusief certificaten, Kerberos en openbare sleutelauthenticatie maar u moet de clientstations configureren om dezelfde verificatiemethode te gebruiken die het WAP-apparaat gebruikt.

Stap 1. Standaard worden de *instellingen van de global RADIUS-server* gebruikt. Schakel het aankruisvakje uit als u de VAP wilt configureren om een andere reeks RADIUS-servers te gebruiken. Anders overslaan naar Stap 8.

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Stap 2. Selecteer in het veld *IP-adres voor servers* het type WAP-apparaat. De opties zijn *IPv4* of *IPv6*. IPv4 gebruikt 32-bits binaire getallen in decimale notatie met punten. IPv6 gebruikt hexadecimale getallen en kolonies om een 128-bits binair getal weer te geven. Het

WAP-apparaat contacteert alleen de RADIUS-server of servers voor het adrestype dat u in dit veld hebt geselecteerd. Als u IPv6 kiest, sla dan over naar Stap 4.

The screenshot shows a configuration window titled "Use global RADIUS server settings". At the top, there is a checkbox for "Use global RADIUS server settings" which is unchecked. Below this, the "Server IP Address Type:" is set to "IPv4" (indicated by a red circle around the selected radio button). The "Server IP Address-1:" field contains "0.0.0.0". There are four empty fields for "Server IP Address-2:", "Server IP Address-3:", and "Server IP Address-4:". The "Key-1:" field is filled with 16 dots. There are four empty fields for "Key-2:", "Key-3:", and "Key-4:". Below the keys, there is an unchecked checkbox for "Enable RADIUS Accounting". The "Active Server:" dropdown menu is set to "Server IP Address-1". The "Broadcast Key Refresh Rate:" is set to "300" and the "Session Key Refresh Rate:" is set to "0".

Stap 3. Als u **IPv4** in stap 2 hebt geselecteerd, specificeert u het IP-adres van de RADIUS-server waarop alle VAP's standaard gebruik maken. Ga dan naar Stap 5.

This screenshot is similar to the previous one, but the "Server IP Address-1:" field is now filled with "192.168.10.23". The "Server IP Address-2:" field contains "192.168.11.1", "Server IP Address-3:" contains "192.168.12.2", and "Server IP Address-4:" contains "192.168.13.3". These four IP address fields are enclosed in a red rectangular box. All other fields and settings remain the same as in the previous screenshot.

Opmerking: U kunt maximaal drie IPv4 RADIUS-serveradressen hebben. Als de authenticatie niet werkt met de primaire server, wordt elke geconfigureerde reserveserver achter elkaar geprobeerd.

Stap 4. Als u **IPv6** in stap 2 hebt geselecteerd, specificeert u het IPv6-adres van de primaire

wereldwijde RADIUS-server.

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IPv6 Address-1: 2001:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-2: 2002:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-3: 2003:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-4: 2004:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

Opmerking: U kunt maximaal drie IPv6 RADIUS-serveradressen hebben. Als de authenticatie niet werkt met de primaire server, wordt elke geconfigureerde reserveserver achter elkaar geprobeerd.

Stap 5. In het veld *Key-1* voert u de gedeelde geheime toets in die het WAP-apparaat gebruikt om te authenticeren aan de primaire RADIUS-server.

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

Stap 6. Voer in de velden *Key-2* to *Key-4* in de RADIUS-toets die is gekoppeld aan de geconfigureerde RADIUS-servers. Het IP-adres van de server gebruikt *Key-2*, IP-adres van

de server 3 gebruikt *Key-3* en IP-adres van de server 4 gebruikt *Key-4*.

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

Stap 7. (Optioneel) In het veld *RADIUS-accounting inschakelen*, schakelt u het aankruisvakje in als u het volgen en meten van de bronnen wilt inschakelen die een bepaalde gebruiker heeft verbruikt. Door de RADIUS-accounting mogelijk te maken, worden de systeemtijd en de hoeveelheid gegevens die worden verzonden en ontvangen, getraceerd. De informatie wordt opgeslagen in de Radius server. Dit wordt ingeschakeld voor de primaire RADIUS-server en alle reserveservers.

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

Opmerking: Als u RADIUS-accounting mogelijk hebt, is deze ingeschakeld voor de primaire RADIUS-server en alle reserveservers

Stap 8. Kies de eerste server die in het veld *actieve server* actief is. Dit maakt het mogelijk

om handmatige selectie van de actieve RADIUS-server te maken, in plaats van het WAP-apparaat dat probeert om achter elkaar contact op te nemen met elke geconfigureerde server en de eerste server te kiezen die actief is.

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1
Server IP Address-2
Server IP Address-3
Server IP Address-4

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

Stap 9. In het veld *Broadcast Key Refresh Rate* voert u in het interval in waarmee de uitzending (groep)-toets wordt teruggestuurd voor klanten die bij deze VAP zijn aangesloten. De standaardinstelling is 300 seconden.

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

Stap 10. In het veld *Session Key Refresh Rate* voert u het interval in waarmee het WAP-apparaat de sessie (unicast)-toets voor elke client die aan de VAP is gekoppeld, verfrist. De standaard is 0.

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

WAP persoonlijk

Persoonlijk ben ik een Wi-Fi Alliance IEEE 802.11i standaard, die AES-CCMP en TKIP-encryptie bevat. WAP gebruikt een vooraf gedeelde toets (PSK) in plaats van IEEE 802.1X en EAP zoals wordt gebruikt in de veiligheidsmodus van WAP voor ondernemingen. De PSK wordt alleen gebruikt voor een eerste onderzoek naar geloofsbrieven. WAP wordt ook aangeduid als WAP-PSK. Deze beveiligingsmodus is achterwaarts compatibel voor de draadloze clients die de oorspronkelijke WAP ondersteunen.

Stap 1. Controleer in het veld *WAP-versies* het dialoogvenster *WAP-TKIP* als u WAP-TKIP wilt inschakelen. U kunt WAP-TKIP en WAP2-AES tegelijkertijd hebben ingeschakeld. WAP ondersteunt altijd WAP2-AES zodat u deze niet kunt configureren.

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter: Below Minimum

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

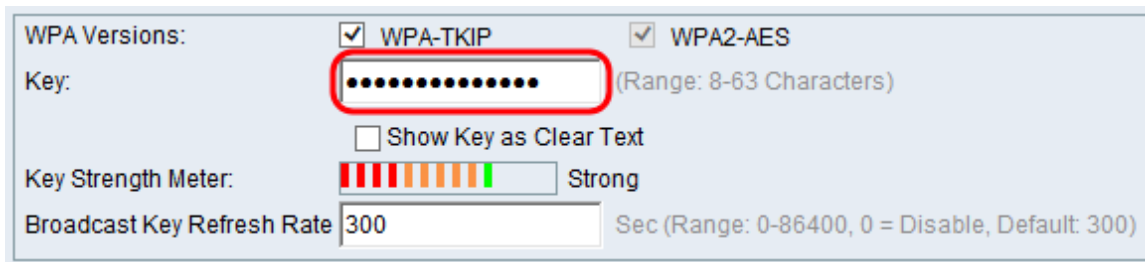
De beschikbare opties zijn als volgt gedefinieerd:


- WAP-TKIP — Het netwerk heeft bepaalde clientstations die alleen het oorspronkelijke protocol voor WAP- en TKIP-beveiliging ondersteunen. Volgens de laatste vereisten van WiFi Alliance wordt het kiezen van alleen WAP-TKIP niet aanbevolen.
- WAP2-AES — Alle clientstations op de netwerkondersteuning WAP2 en AES-CCMP algoritme/beveiligingsprotocol. Deze WAP-versie biedt de beste beveiliging volgens de IEEE 802.11i-standaard. Volgens de laatste WiFi Alliance-eis moet AP deze modus altijd ondersteunen.
- WAP-TKIP en WAP2-AES — Als het netwerk een mix van klanten heeft, waarvan

sommige WAP2 ondersteunen en andere die alleen de oorspronkelijke WAP ondersteunen, controleer beide de aankruisvakjes. Deze instelling laat zowel de de client van WAP als de van WAP2 associëren en authentiek verklaren, maar gebruikt robuustere WAP2 voor klanten die het steunen. Deze configuratie maakt meer interoperabiliteit mogelijk in plaats van enige beveiliging.

Opmerking: WAP-clients moeten over een van deze toetsen beschikken (een geldige TKIP-toets of een geldige AES-CCMP-toets) om met het WAP-apparaat te kunnen associëren.

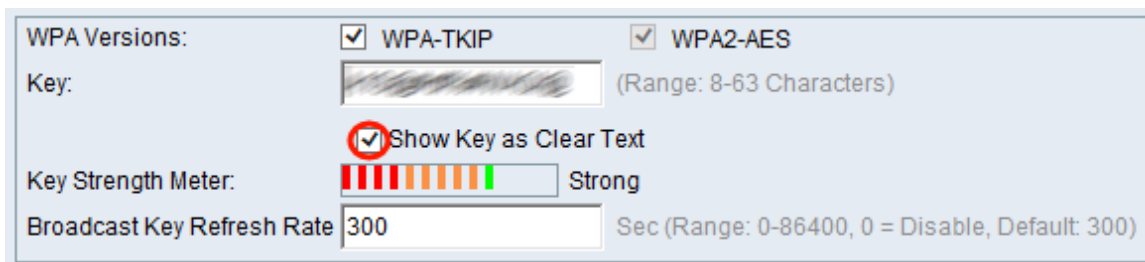
Stap 2. Voer in het veld *Key* in de gedeelde geheime sleutel van de WAP-beveiliging. Voer minimaal 8 tekens en maximaal 63 tekens in.




WPA Versions: WPA-TKIP WPA2-AES
Key: (Range: 8-63 Characters)
 Show Key as Clear Text
Key Strength Meter:  Strong
Broadcast Key Refresh Rate Sec (Range: 0-86400, 0 = Disable, Default: 300)

Opmerking: Acceptabele tekens zijn hoofdletters en kleine letters, numerieke cijfers en speciale symbolen (?!\@#\$\$%^&*).

Stap 3. (Optioneel) Controleer de *sleutel tonen als* het vakje *Tekst wissen* als u wilt dat de tekst die u typt zichtbaar is. Het selectieteken is standaard niet ingeschakeld.




WPA Versions: WPA-TKIP WPA2-AES
Key: (Range: 8-63 Characters)
 Show Key as Clear Text
Key Strength Meter:  Strong
Broadcast Key Refresh Rate Sec (Range: 0-86400, 0 = Disable, Default: 300)

Opmerking: wanneer u een andere firmware gebruikt op WAP351, WAP131 of WAP371, ontbreekt de *Toon-toets als Clear Text* veld.

Opmerking: Het veld *Key Sterth Meter* is waar het WAP-apparaat de toets controleert op basis van complexiteit, zoals hoeveel verschillende typen tekens worden gebruikt en hoe lang de toets is. Als de optie voor de WAP-PSK-complexiteit is ingeschakeld, wordt de toets niet geaccepteerd tenzij deze aan de minimumcriteria voldoet. Voor meer informatie over de complexiteit van WAP-PSK raadpleegt u [Wachtwoord instellen voor de complexiteit van WAP131, WAP351 en WAP371](#).




WPA Versions: WPA-TKIP WPA2-AES
Key: (Range: 8-63 Characters)
 Show Key as Clear Text
Key Strength Meter:  Strong
Broadcast Key Refresh Rate Sec (Range: 0-86400, 0 = Disable, Default: 300)

Stap 4. In het veld *Broadcast Key Refresh Rate* voert u in het interval in waarmee de uitzending (groep)-toets wordt teruggestuurd naar klanten die bij deze VAP zijn aangesloten. De standaardinstelling is 300 seconden.

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter:  Strong

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

WAP-onderneming

WAP Enterprise met RADIUS is een implementatie van de standaard Wi-Fi Alliance IEEE 802.11i, die CCMP (AES) en TKIP-encryptie omvat. De modus Enterprise vereist dat er een RADIUS-server wordt gebruikt om de gebruikers voor het eerst te controleren. De veiligheidsmodus is achterwaarts compatibel met de draadloze clients die de oorspronkelijke WAP ondersteunen.

Opmerking: De dynamische VLAN-modus is standaard ingeschakeld, zodat de RADIUS-verificatieserver kan beslissen welke VLAN voor de stations wordt gebruikt.

Stap 1. Controleer in het veld *WAP-versies* op het aankruisvakje voor de typen clientstations die worden ondersteund. Ze zijn allemaal standaard ingeschakeld. AP moet de tijd van de steun aan WPA2-AES altijd ondersteunen zodat u het niet zult kunnen configureren.

WPA Versions: WPA-TKIP WPA2-AES

Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

De beschikbare opties zijn als volgt gedefinieerd:

- WPA-TKIP: het netwerk heeft bepaalde clientstations die alleen oorspronkelijke WAP- en TKIP-beveiligingsprotocol ondersteunen. Merk op dat het selecteren van alleen WPA-TKIP voor het access point niet is toegestaan volgens het laatste WiFi Alliance vereiste.
- WPA2-AES — Alle clientstations op de netwerkondersteuning van de WPA2-versie en

het AES-CCMP-algoritme/beveiligingsprotocol. Deze WAP-versie biedt de beste beveiliging volgens de IEEE 802.11i-standaard. Volgens de laatste Wi-Fi Alliance-eis moet WAP deze modus voortdurend ondersteunen.

- pre-verificatie inschakelen — Als u alleen voor WAP2 of zowel voor WAP als voor WAP2 als de WAP-versie kiest, kunt u pre-verificatie voor de WAP2-clients inschakelen. Controleer deze optie als u wilt dat de WAP2 draadloze klanten de pre-authenticatie pakketten verzenden. De informatie van vóór de verificatie wordt via het WAP-apparaat doorgegeven dat de client momenteel gebruikt voor het WAP-doelapparaat. Het inschakelen van deze functie kan ertoe bijdragen dat de authenticatie van roamende klanten die verbinding maken met meerdere WAP's, wordt versneld. Deze opties zijn niet van toepassing als u voor WAP versies hebt geselecteerd omdat het oorspronkelijke WAP deze optie niet ondersteunt.

Opmerking: Clientstations die zijn ingesteld om WAP met RADIUS te gebruiken, moeten een van deze adressen en toetsen hebben: Een geldig TKIP-RADIUS of geldig CMP-adres (AES) en een RADIUS-toets.

Stap 2. Standaard worden de *instellingen van de global RADIUS-server* gebruikt. Schakel het aankruisvakje uit als u de VAP wilt configureren om een andere reeks RADIUS-servers te gebruiken. Anders overslaan naar Stap 9.

The screenshot shows a configuration window for WPA. At the top, there are checkboxes for 'WPA Versions': 'WPA-TKIP' and 'WPA2-AES' are both checked. Below them, 'Enable pre-authentication' is also checked. A section titled 'Use global RADIUS server settings' has an unchecked checkbox, which is circled in red. Below this, there are radio buttons for 'Server IP Address Type': 'IPv4' is selected, and 'IPv6' is unselected. There are four input fields for 'Server IP Address-1' through 'Server IP Address-4', with the first containing '0.0.0.0'. Each field has a placeholder '(xxx.xxx.xxx.xxx)'. Below these are four input fields for 'Key-1' through 'Key-4', with the first containing a series of dots. Each key field has a placeholder '(Range: 1-64 Characters)'. At the bottom, there is an unchecked checkbox for 'Enable RADIUS Accounting'. Below that, there is a dropdown menu for 'Active Server' set to 'Server IP Address-1'. There are two more input fields: 'Broadcast Key Refresh Rate' set to '300' and 'Session Key Refresh Rate' set to '0'. Both have placeholders and ranges: 'Sec (Range: 0-86400, 0 = Disable, Default: 300)' and 'Sec (Range: 30-86400, 0 = Disable, Default: 0)' respectively.

Stap 3. Selecteer in het veld *IP-adres voor servers* het type WAP-apparaat. De opties zijn *IPv4* of *IPv6*. IPv4 gebruikt 32-bits binaire getallen in decimale notatie met punten. IPv6 gebruikt hexadecimale getallen en kolonies om een 128-bits binair getal weer te geven. Het WAP-apparaat contacteert alleen de RADIUS-server of servers voor het adrestype dat u in dit veld hebt geselecteerd.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▾

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Stap 4. Als u **IPv4** in stap 2 hebt geselecteerd, specificeert u het IP-adres van de RADIUS-server waarop alle VAP's standaard gebruik maken. Naar stap 6.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▾

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Opmerking: U kunt maximaal drie IPv4 RADIUS-serveradressen hebben. Als de authenticatie niet werkt met de primaire server, wordt elke geconfigureerde reserveserver achter elkaar geprobeerd.

Stap 5. Als u **IPv6** in stap 2 hebt geselecteerd, specificeert u het IPv6-adres van de primaire wereldwijde RADIUS-server.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IPv6 Address-1: 2001:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-2: 2002:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-3: 2003:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-4: 2004:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Key-1: (Range: 1-64 Characters)

Key-2: (Range: 1-64 Characters)

Key-3: (Range: 1-64 Characters)

Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

Opmerking: U kunt maximaal drie IPv6 RADIUS-serveradressen hebben. Als de authenticatie niet werkt met de primaire server, wordt elke geconfigureerde reserveserver achter elkaar geprobeerd.

Stap 6. In het veld *Key-1* voert u de gedeelde geheime sleutel in die het WAP-apparaat gebruikt om te authenticeren aan de primaire RADIUS-server.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Stap 7. Voer in de velden *Key-2* naar *Key-4* in de RADIUS-toets die is gekoppeld aan de geconfigureerde RADIUS-servers. Het IP-adres van de server gebruikt *Key-2*, IP-adres 3 voor de server *Key-3* en IP-adres 4 voor de server *Key-4*.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Stap 8. (Optioneel) In het veld *RADIUS-accounting inschakelen*, schakelt u het aankruisvakje in als u het volgen en meten van de bronnen wilt inschakelen die een

bepaalde gebruiker heeft verbruikt. Met behulp van RADIUS-accounting kunt u de systeemtijd van een bepaalde gebruiker en de hoeveelheid gegevens die worden verzonden en ontvangen, bijhouden.

WPA Versions: <input checked="" type="checkbox"/> WPA-TKIP <input checked="" type="checkbox"/> WPA2-AES	
<input checked="" type="checkbox"/> Enable pre-authentication	
<input type="checkbox"/> Use global RADIUS server settings	
Server IP Address Type:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Server IP Address-1:	<input type="text" value="192.168.10.23"/> (xxx.xxx.xxx.xxx)
Server IP Address-2:	<input type="text" value="192.168.10.24"/> (xxx.xxx.xxx.xxx)
Server IP Address-3:	<input type="text" value="192.168.10.25"/> (xxx.xxx.xxx.xxx)
Server IP Address-4:	<input type="text" value="192.168.10.26"/> (xxx.xxx.xxx.xxx)
Key-1:	<input type="text" value="••••••••"/> (Range: 1-64 Characters)
Key-2:	<input type="text" value="••••••••"/> (Range: 1-64 Characters)
Key-3:	<input type="text" value="••••~•••"/> (Range: 1-64 Characters)
Key-4:	<input type="text" value="••••••~••"/> (Range: 1-64 Characters)
<input checked="" type="checkbox"/> Enable RADIUS Accounting	
Active Server:	<input type="text" value="Server IP Address-1"/> ▼
Broadcast Key Refresh Rate:	<input type="text" value="300"/> Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate:	<input type="text" value="0"/> Sec (Range: 30-86400, 0 = Disable, Default: 0)

Opmerking: Als u RADIUS-accounting hebt ingeschakeld, is deze ingeschakeld voor de primaire RADIUS-server en alle reserveservers.

Stap 9. Kies de eerste server die in het veld *actieve server* actief is. Dit maakt het mogelijk om de actieve RADIUS-server handmatig te selecteren in plaats van de WAP-applicatie te gebruiken om achtereenvolgens contact op te nemen met elke geconfigureerde server.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
Server IP Address-2: (xxx.xxx.xxx.xxx)
Server IP Address-3: (xxx.xxx.xxx.xxx)
Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
Key-2: (Range: 1-64 Characters)
Key-3: (Range: 1-64 Characters)
Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1
Server IP Address-2
Server IP Address-3
Server IP Address-4

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Stap 10. Voer in het veld *Broadcast Key Refresh Rate* in het interval in waarin de uitzending (groep)-toets wordt teruggestuurd voor klanten die bij deze VAP zijn aangesloten. De standaardinstelling is 300 seconden.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
Server IP Address-2: (xxx.xxx.xxx.xxx)
Server IP Address-3: (xxx.xxx.xxx.xxx)
Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
Key-2: (Range: 1-64 Characters)
Key-3: (Range: 1-64 Characters)
Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Stap 1. In het veld *Session Key Refresh Rate* voert u het interval in waarmee het WAP-apparaat sessies (unicast) de toetsen verfrist voor elke client die aan de VAP gekoppeld zijn.

De standaard is 0.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication
 Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)
Server IP Address-2: 192.168.10.24 (xxx.xxx.xxx.xxx)
Server IP Address-3: 192.168.10.25 (xxx.xxx.xxx.xxx)
Server IP Address-4: 192.168.10.26 (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
Key-2: (Range: 1-64 Characters)
Key-3: (Range: 1-64 Characters)
Key-4: (Range: 1-64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

MAC-filter

MAC Filter specificeert of de stations die tot deze VAP toegang hebben beperkt zijn tot een geconfigureerde globale lijst van MAC-adressen.

Stap 1. Kies in de vervolgkeuzelijst *MAC-filter* het gewenste type MAC-filtering.

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

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

VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
0	<input checked="" type="checkbox"/>	1	DISCOFD	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled Local RADIUS	<input type="checkbox"/>

Add Edit Delete

De beschikbare opties zijn als volgt gedefinieerd:

- Uitgeschakeld — Gebruik geen MAC-filtering.
- Lokaal — Gebruik de MAC-verificatielijst die u configureren in het vak MAC-filtering, om meer te weten te komen over MAC-filtering, zie [Hoe u MAC-filtering op WAP351 en WAP131 configureren](#).
- RADIUS — Gebruik de MAC-verificatielijst op een externe RADIUS-server.

Kanaalisolatie

Wanneer de kanaalisolatie is uitgeschakeld, kunnen de draadloze clients normaal met elkaar communiceren door verkeer via het WAP-apparaat te verzenden. Als deze functie is

ingeschakeld, blokkeert het WAP-apparaat de communicatie tussen de draadloze clients op dezelfde VAP. Het WAP-apparaat staat nog steeds gegevensverkeer tussen zijn draadloze klanten en de bekabelde apparaten op het netwerk toe, via een WDS-link en met andere draadloze klanten die bij een andere VAP zijn betrokken, maar niet onder de draadloze klanten.

Stap 1. Controleer in het veld *Kanaalisolatie* het selectieteken als u kanaalisolatie wilt inschakelen.

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

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discoob	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input checked="" type="checkbox"/>		

Add Edit Delete

Stap 2. Klik op **Opslaan**.

Opmerking: Nadat de nieuwe instellingen zijn opgeslagen, kunnen de corresponderende processen worden gestopt en opnieuw worden gestart. Wanneer deze conditie gebeurt, kan het WAP apparaat connectiviteit verliezen. We raden u aan de WAP-apparaatinstellingen te wijzigen wanneer een connectiviteitsverlies het minst invloed heeft op uw draadloze klanten.

Band Steer

Band Steer is alleen beschikbaar op WAP371. Band Steer wordt effectief gebruikt voor de 5-GHz band door het besturen van dual-band ondersteunde clients van de 2,4-GHz band naar de 5-GHz band. Hierdoor wordt de 2,4 GHz-band bevrijd voor gebruik door oudere apparaten die geen dubbele radio-ondersteuning hebben.

Opmerking: Zowel de 5 GHz- als de 2,4 GHz-radio's moeten worden ingeschakeld om Band Steer te gebruiken. Voor meer informatie over het inschakelen van de radio's raadpleegt u [Hoe u fundamentele radio-instellingen op WAP371 kunt configureren](#).

Stap 1. Band Steer wordt ingesteld per VAP en moet op beide radio's zijn ingeschakeld. Als u Band Steer wilt in-, schakelt u het aanvinkvakje in het veld Band Steer in.

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

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discoob	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Add Edit Delete

Opmerking: Band Steer wordt niet op VAP's aangemoedigd met tijdgevoelige spraak- of videoverkeer. Zelfs als de 5 GHz-radio minder bandbreedte gebruikt, probeert het klanten naar die radio te sturen.

Stap 2. Klik op **Opslaan**.

Een VAP verwijderen

Stap 1. Controleer het vakje in de VAP dat u wilt verwijderen.

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

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
Show Details									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
Show Details									

Stap 2. Klik op **Verwijderen** om de VAP te verwijderen.

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

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
Show Details									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
Show Details									

Stap 3. Klik op **Opslaan** om het wissen permanent op te slaan.

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

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		