RADIUS configureren in Cisco draadloos access point voor bedrijven

Doel

Het doel van dit document is om u te tonen hoe u RADIUS kunt configureren in Cisco Business Wireless (CBW) access point (AP).

Toepasselijke apparaten | Versie firmware

- 140 AC (gegevensblad) | 10.4.1.0 (laatste download)
- 145 AC (informatieblad) | 10.4.1.0 (laatste download)
- 240 AC (gegevensblad) | 10.4.1.0 (laatste download)

Inleiding

Als u RADIUS in uw CBW AP wilt configureren bent u op de juiste plaats gekomen! De CBW APs ondersteunen de nieuwste 802.11ac Wave 2 standaard voor hogere prestaties, grotere toegang en hoger-dichtheid netwerken. Zij leveren toonaangevende prestaties met zeer veilige en betrouwbare draadloze verbindingen, voor een robuuste, mobiele eindgebruikerservaring.

RADIUS (Remote Authentication Dial-User Service) is een verificatiemechanisme voor apparaten om een netwerkservice te verbinden en te gebruiken. Het wordt gebruikt voor gecentraliseerde authenticatie, autorisatie en boekhoudkundige doeleinden. Een RADIUS-server reguleert de toegang tot het netwerk door de identiteit van de gebruikers te controleren met behulp van de ingevoerde inlogaanmeldingsgegevens. Een openbaar Wi-Fi-netwerk is bijvoorbeeld geïnstalleerd op een universiteitscampus. Alleen studenten die het wachtwoord hebben, hebben toegang tot deze netwerken. De RADIUS-server controleert de wachtwoorden die door de gebruikers zijn ingevoerd, en verleent of ontkent toegang tot het Wireless Local Area Network (WLAN) naar behoren.

Als u klaar bent om RADIUS op uw CBW AP te configureren gaan we beginnen!

Inhoud

RADIUS op uw CBW-AP configureren

In dit ingesloten gedeelte worden tips voor beginners gemarkeerd.

Inloggen

Log in op de webgebruikersinterface (UI) van de primaire AP. Om dit te doen, open een web browser en voer https://ciscobusiness.cisco in. U kunt een waarschuwing ontvangen voordat u doorgaat. Voer uw aanmeldingsgegevens in.U kunt ook toegang krijgen tot de primaire AP door https://[ipaddress] (van de primaire AP) in een webbrowser in te voeren.

Tips voor gereedschap

Als u vragen hebt over een veld in de gebruikersinterface, controleert u op een snijpunt dat er als volgt uitziet:

Problemen met de locatie van het pictogram Hoofdmenu uitvouwen?

Navigeer naar het menu aan de linkerkant van het scherm, als u de menuknop niet ziet, klik dan op dit pictogram om het zijbalkmenu te openen.

Cisco Business-app

Deze apparaten hebben metgezelapps die bepaalde beheerfuncties delen met de web gebruikersinterface. Niet alle functies in de gebruikersinterface van het web zijn in de app beschikbaar.

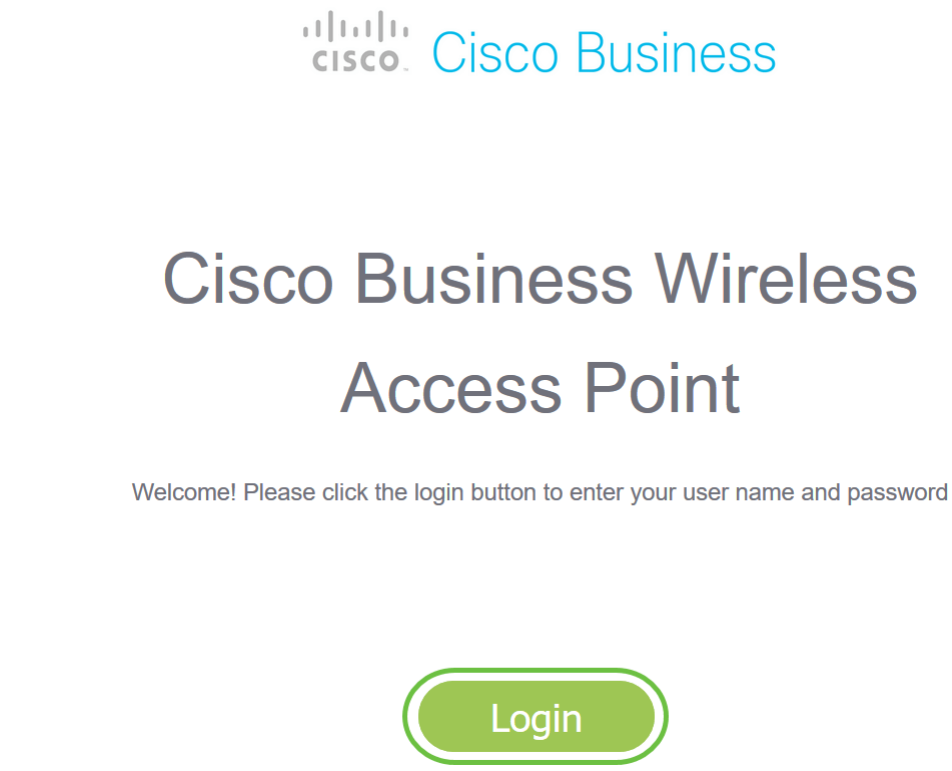
iOS-app downloaden Android-app downloaden

Veelgestelde vragen

Als u nog steeds onbeantwoorde vragen hebt, kunt u ons vaak gestelde vragen document controleren. FAQ

Stap 1

Meld u aan bij uw CBW AP met behulp van een geldig gebruikersnaam en wachtwoord.

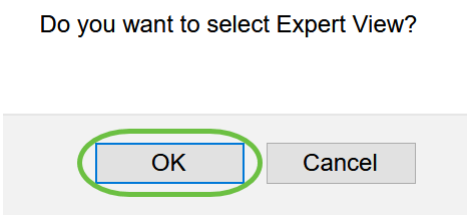


Stap 2

Klik op het symbool van de **bidirectionele pijl** boven in de web user-interface (UI) om *naar Expert*

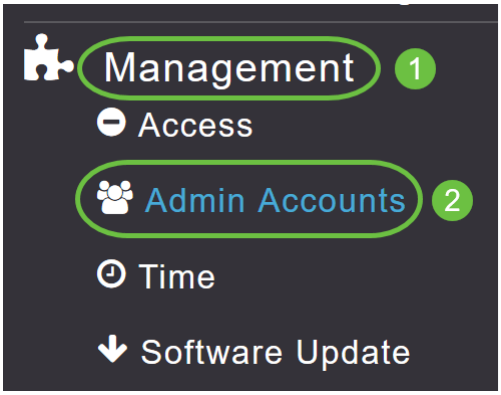
View te *Switches*.

Het volgende pop-upscherm wordt weergegeven. Klik op **OK** om verder te gaan.



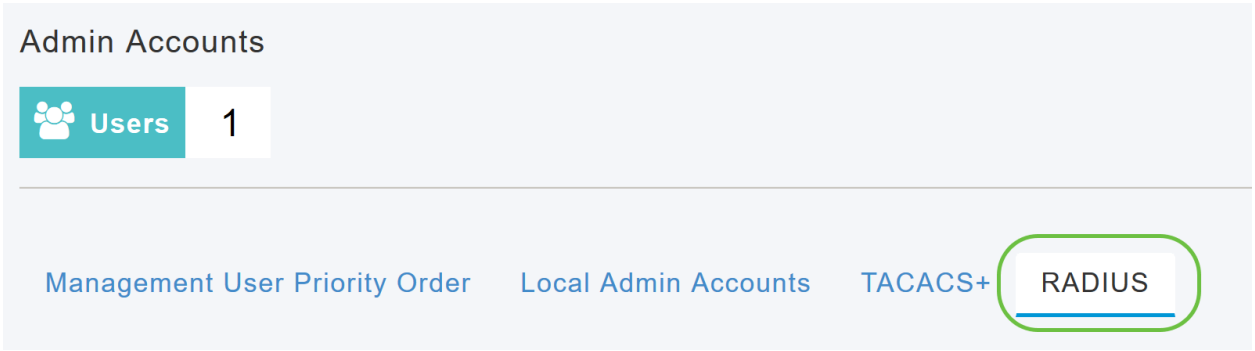
Stap 3

Navigeren in **beheer > Admin accounts**.



Stap 4

Als u de RADIUS-servers wilt toevoegen, klikt u op in het tabblad **RADIUS**.

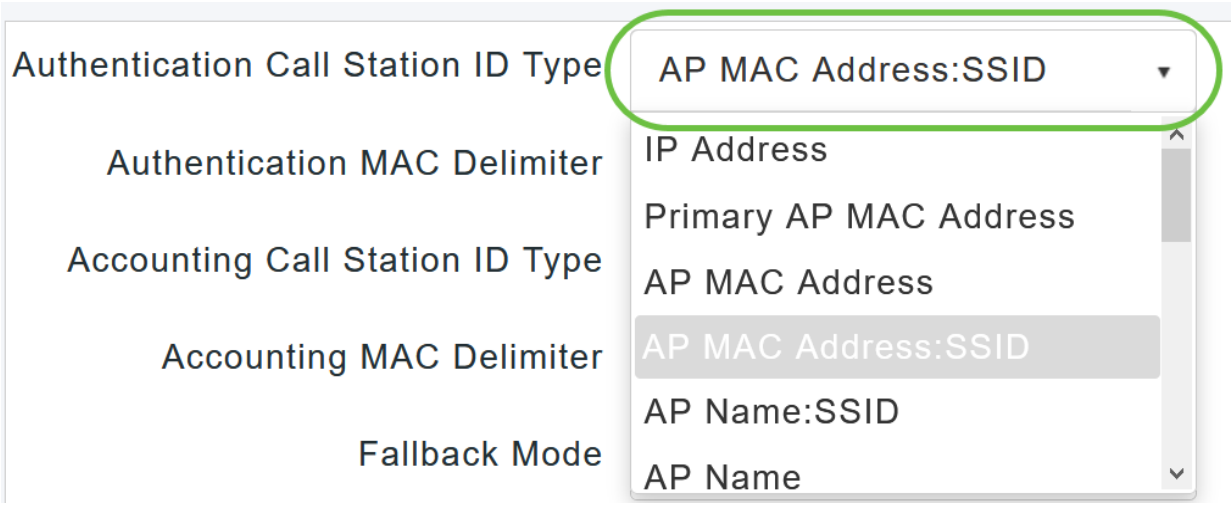


Stap 5

Kies in de vervolgkeuzelijst *Type* verificatie-id van het *verificatiestation* de optie die naar de RADIUS-server wordt verzonden in het bericht Access-Application. De volgende opties zijn beschikbaar:

- *IP-adres*

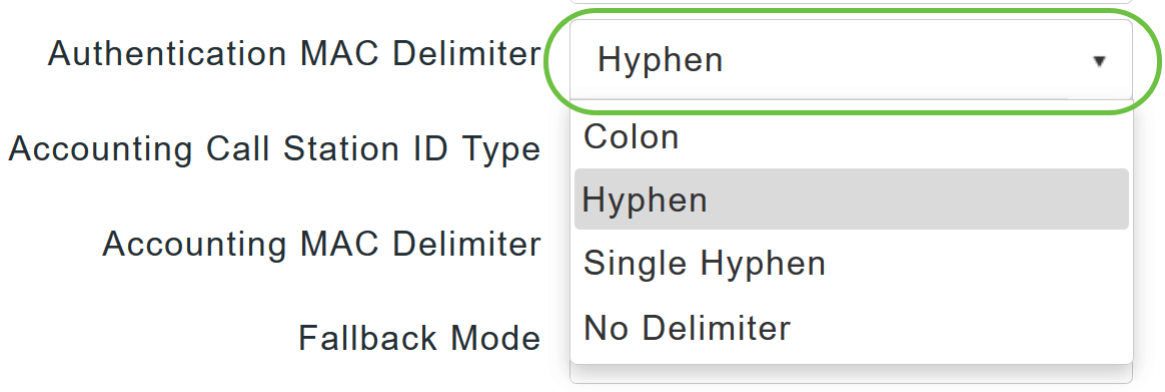
- *Primair AP-MAC-adres*
- *AP MAC-adres*
- *AP MAC-adres:SSID*
- *AP-naam:SSID*
- *AP-naam*
- *AP-groep*
- *Flex-groep*
- *AP-locatie*
- *VLAN-id*
- *AP Ethernet MAC-adres*
- *AP Ethernet MAC-adres:SSID*
- *AP-labeladres*
- *AP Label Address:SSID*
- *AP MAC:SSID AP-groep*
- *AP Eth MAC:SSID AP Group*



Stap 6

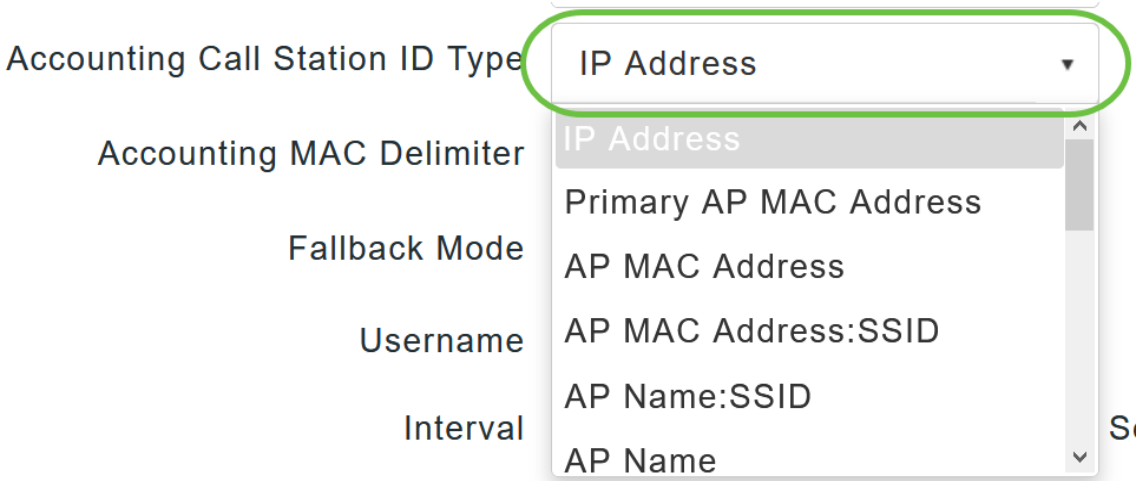
Selecteer de *MAC-scheidingsteken* voor verificatie in de vervolgkeuzelijst. De opties zijn:

- *Colon*
- *koppelteken*
- *eenkoppelteken*
- *Geen scheidingsteken*



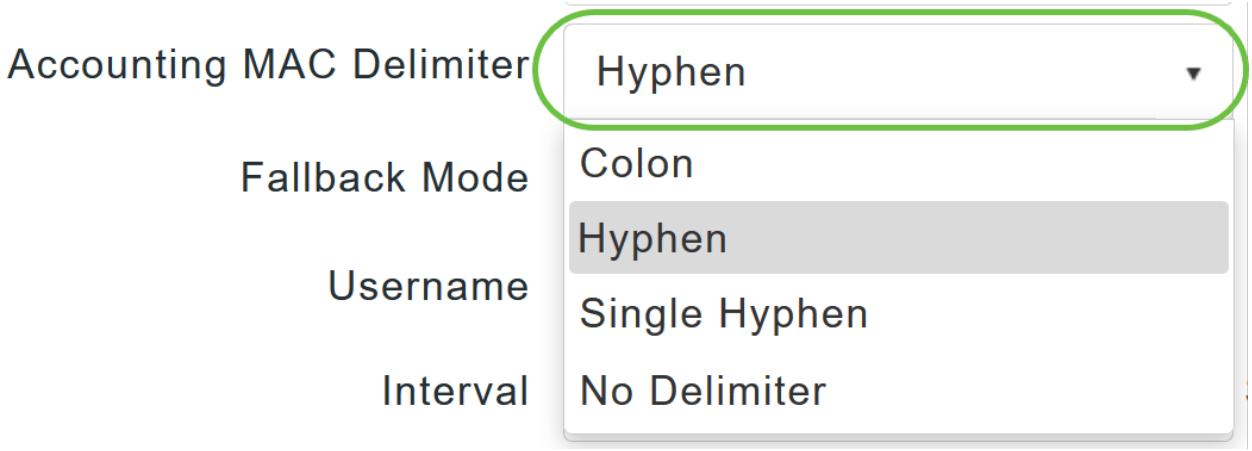
Stap 7

Kies het *type ID van het boekhoudingsstation* in de vervolgkeuzelijst.



Stap 8

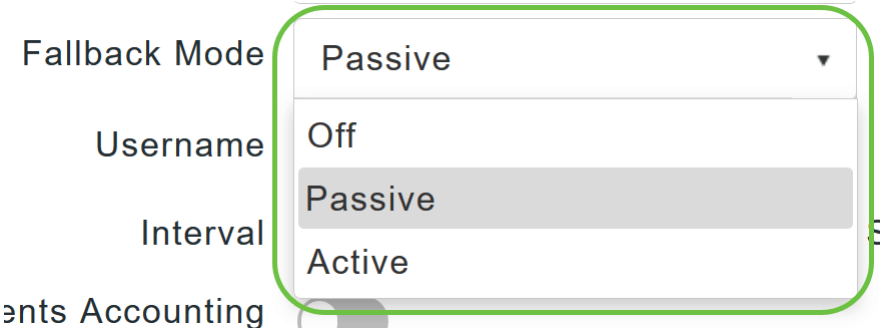
Kies de *MAC-scheidingsteken* voor *accounting* in de vervolgkeuzelijst.



Stap 9

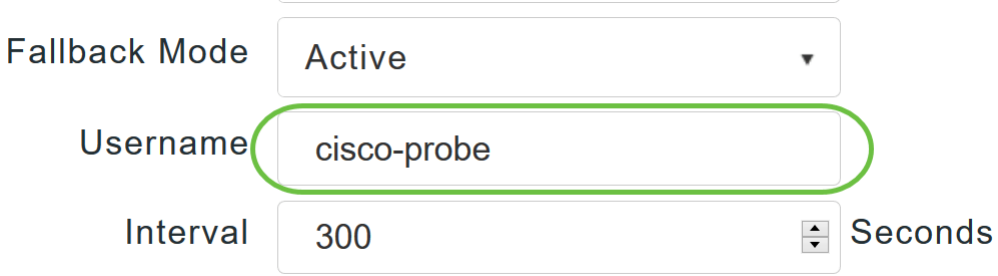
Specificeer de RADIUS-*serverreservemodus* in de vervolgkeuzelijst. Dit kan een van de volgende opties zijn:

- *Uit* - schakelt RADIUS-serverback uit. Dit is de standaardwaarde.
- *Passief* - veroorzaakt dat de primaire AP terugkeert naar een server met een lagere prioriteit van de beschikbare reserveservers zonder gebruik van buitenaardse sonde berichten. De primaire AP negeert alle inactieve servers voor een periode en probeert later opnieuw wanneer een RADIUS-bericht moet worden verzonden.
- *Active* - veroorzaakt dat de primaire AP terugkeert naar een server met een lagere prioriteit van de beschikbare reserveservers door RADIUS-probe-berichten te gebruiken om proactief te bepalen of een server die is gemarkeerd inactief terug online is. De primaire AP negeert alle inactieve servers voor alle actieve RADIUS-verzoeken. Zodra de primaire server een antwoord van de teruggevonden ACS server ontvangt, verstuurt de actieve terugval RADIUS-server niet langer probe-berichten naar de server die om de actieve probe-verificatie verzoekt.



Stap 10

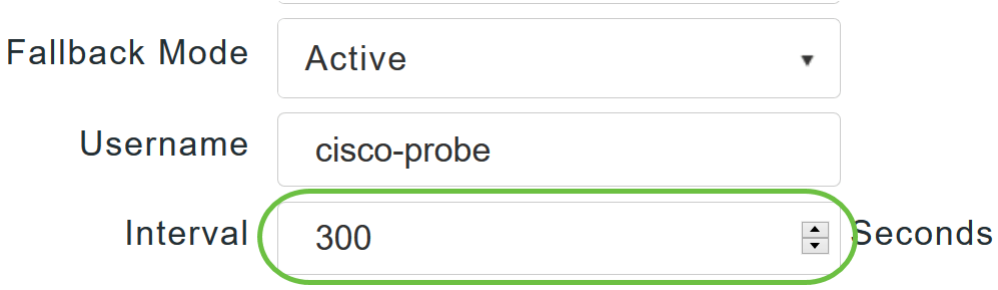
Als u *actieve* terugvalmodus hebt ingeschakeld, voert u de naam in die u in de inactieve serverproblemen in het veld *Gebruikersnaam wilt* versturen.



U kunt maximaal 16 alpha- numerieke tekens invoeren. De standaardwaarde is **cisco-sonde**.

Stap 11

Als u de *actieve* terugvalmodus hebt ingeschakeld, geeft u de waarde van het sonde-interval (in seconden) in het veld Interval in. Het interval dient als inactieve tijd in de passieve modus en sonde interval in de actieve modus.

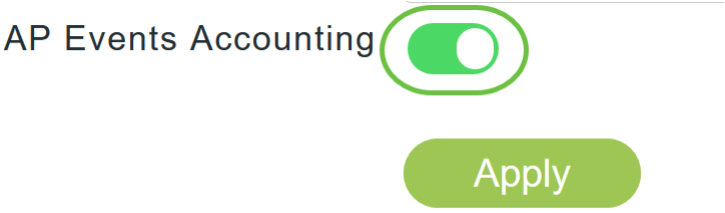


Het geldige bereik is 180 tot 3600 seconden en de standaardwaarde is **300** seconden.

Stap 12

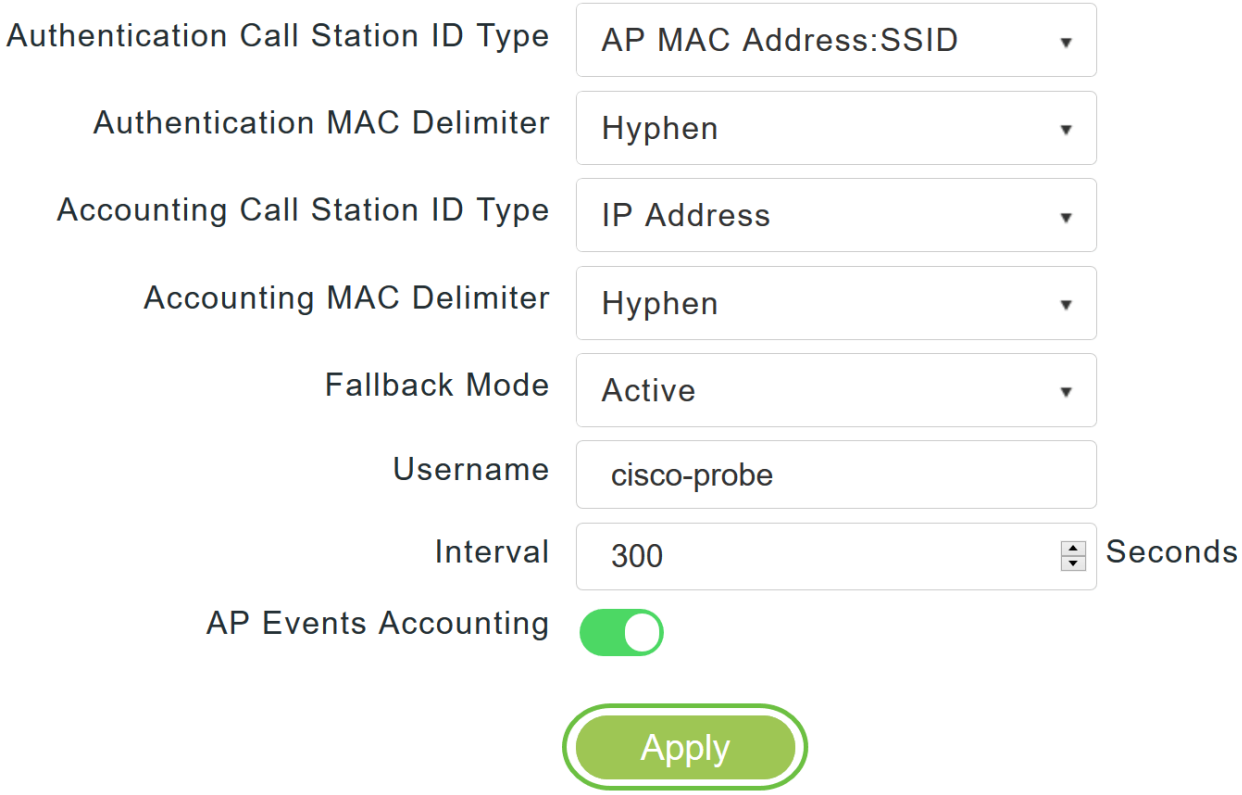
Schakel de knop *AP* Events Accounting (*AP*-gebeurtenissen *accounting)* in om het verzenden van accounting aanvragen naar een RADIUS-server te activeren.

Tijdens netwerkproblemen worden AP's aangesloten bij/ontkoppeld van de primaire AP. Deze optie inschakelen zorgt ervoor dat deze gebeurtenissen worden gevolgd en dat de accounting aanvragen naar de RADIUS-server worden verzonden om u te helpen bij het detecteren van netwerkproblemen.



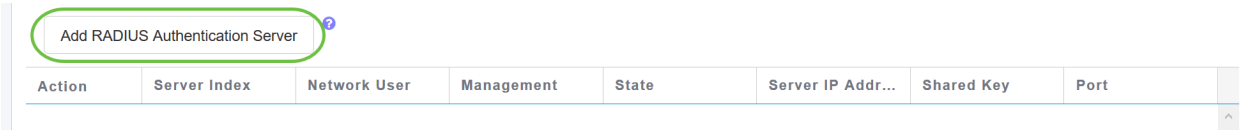
Stap 13

Klik op **Apply** (Toepassen).



Stap 14

Klik op **RADIUS-verificatieserver toevoegen** om de RADIUS-verificatie te configureren.



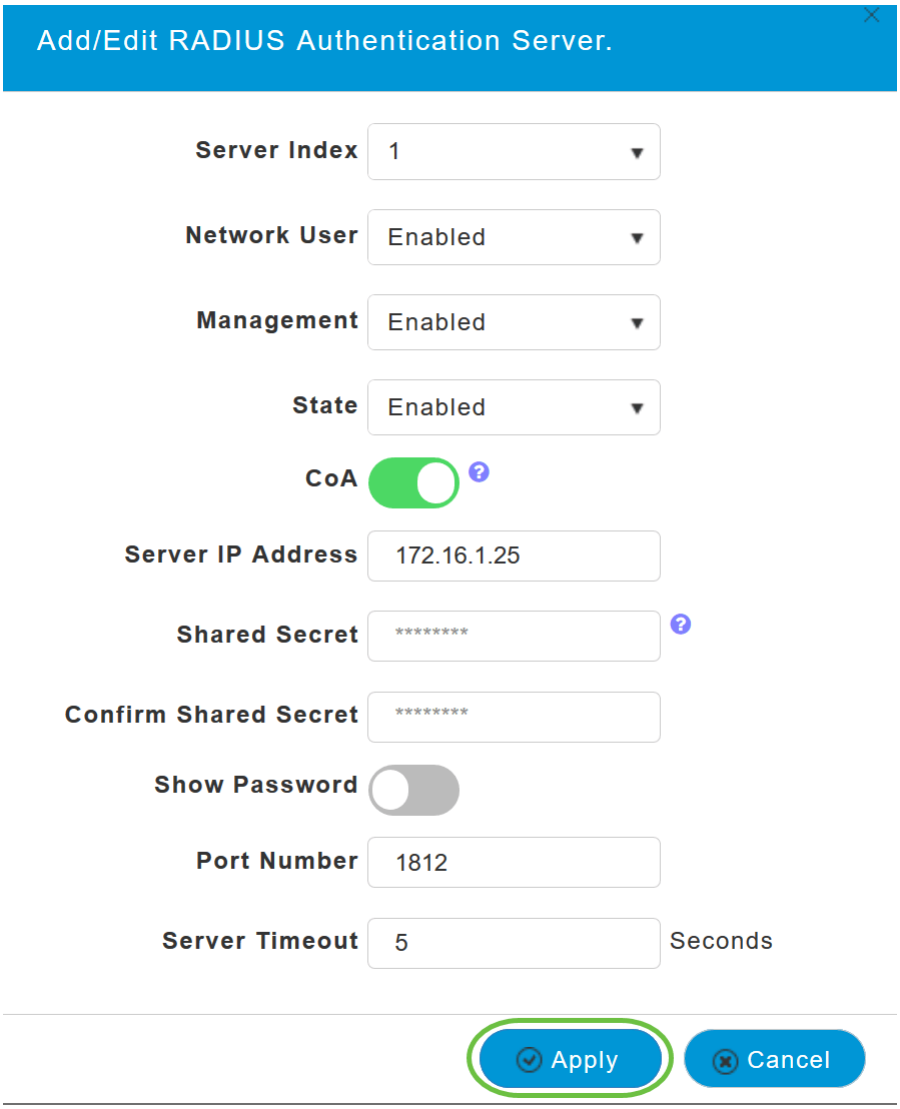
Stap 15

In het pop-upvenster *RADIUS-verificatie toevoegen/bewerken* moet u het volgende configureren:

- *Server Index* - selecteer 1 tot en met 6
- *Netwerkgebruiker* - Schakel de staat in. Standaard is dit ingeschakeld
- *Beheer* - Schakel de staat in. Standaard is dit ingeschakeld
- *Staat* - Laat de staat in werking. Standaard is dit ingeschakeld
- *CoA* - U kunt ervoor kiezen deze optie in te schakelen door de toets van de schuifschakelaar te verplaatsen
- *IP-adres van de server* - Voer het IPv4-adres van de RADIUS-server in

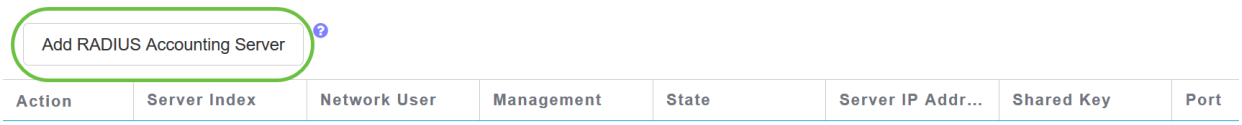
- *Gedeeld geheim* - Voer het gedeelde geheim in
- *Port Number* - Voer het poortnummer in dat wordt gebruikt voor communicatie met de RADIUS-server.
- *Time-out server* - Voer de tijdelijke oplossing voor de server in

Klik op **Apply** (Toepassen).



Stap 16

Om *RADIUS-accounting server* toe te voegen, volgt u dezelfde stappen als in Stap 15 als de pagina soortgelijke velden bevat.

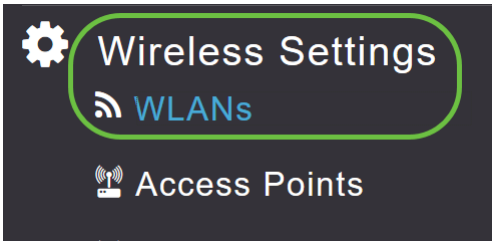


WLAN configureren

Stap 1

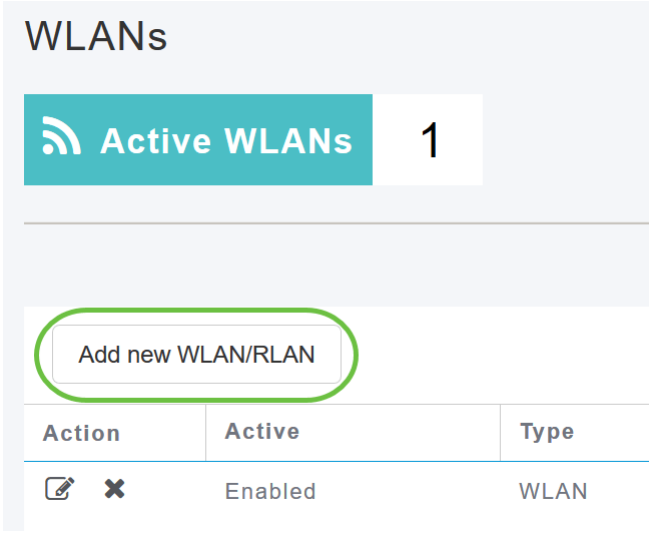
Om WLAN te configureren dat WAP2-verificatie met RADIUS gaat verwerken, navigeer naar

draadloze instellingen > WLAN.



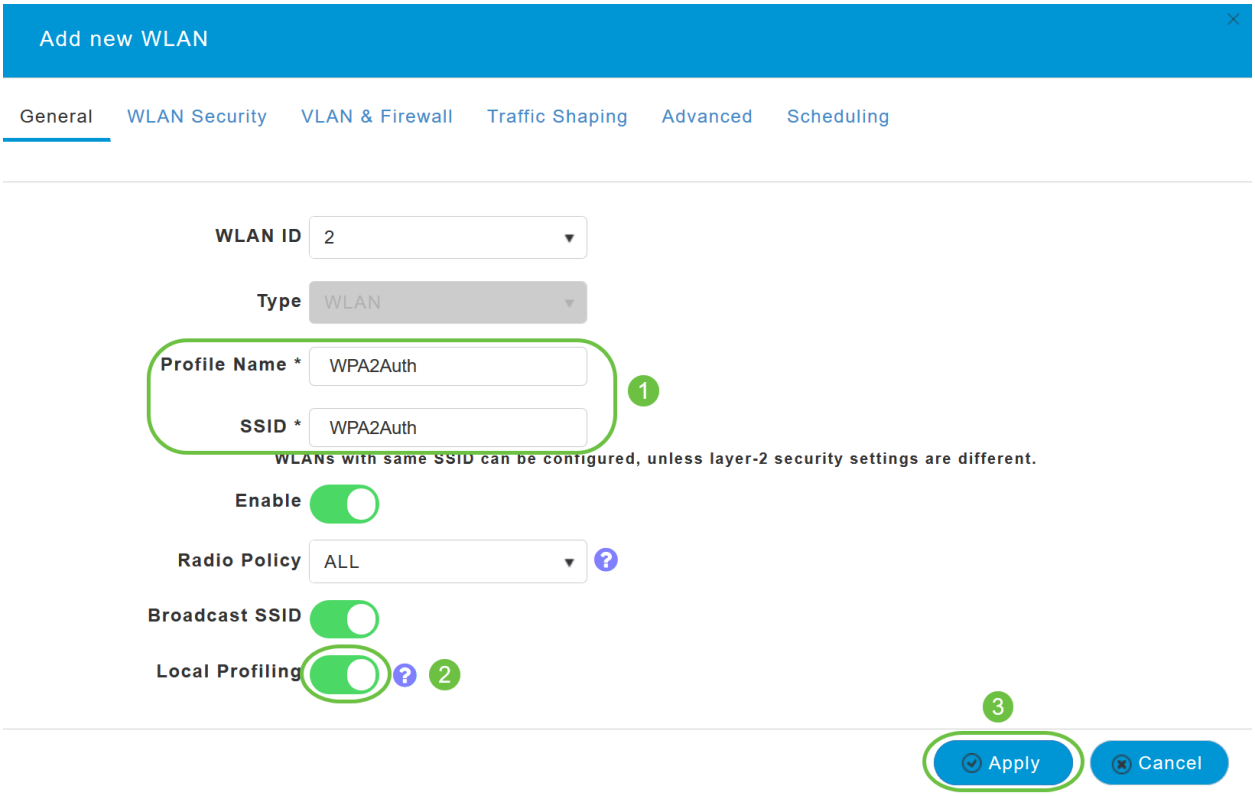
Stap 2

Klik op **Add New WLAN/LAN**.



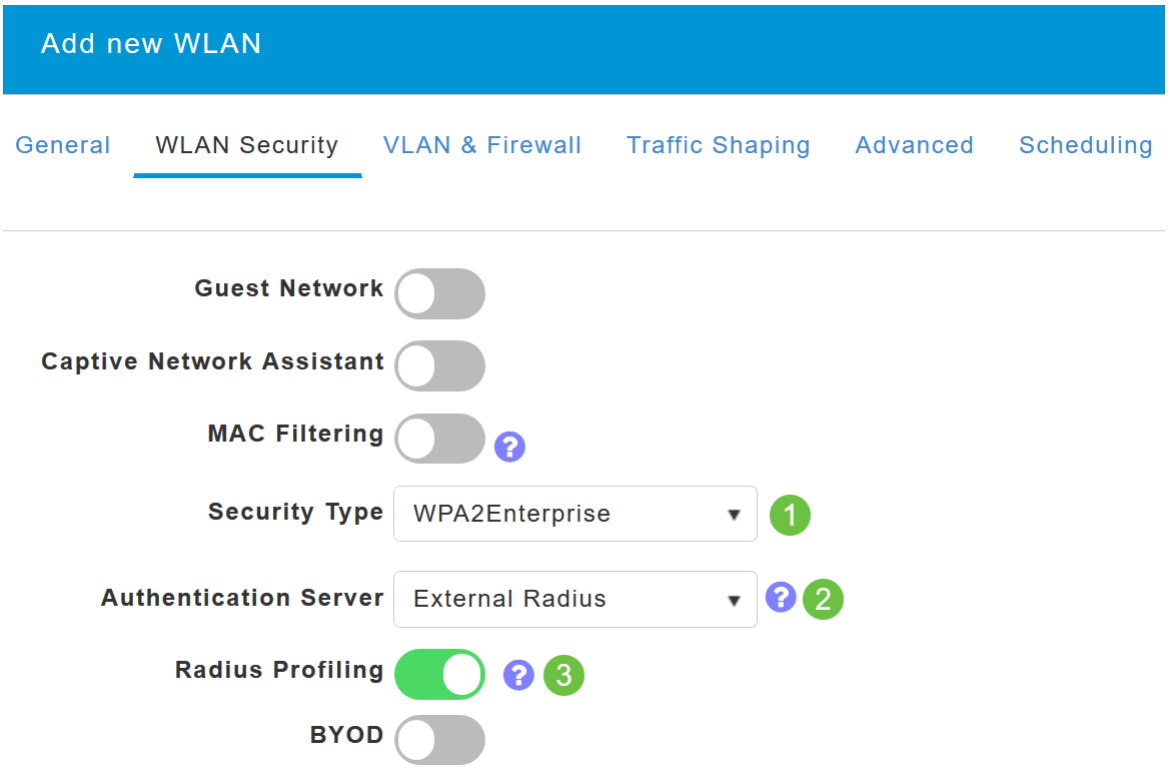
Stap 3

Voer in het *tabblad Algemeen* de *profielnaam in*. Het veld *SSID* vult het automatisch in. U kunt ervoor kiezen *Lokale profilering* in te schakelen. Klik op **Apply** (Toepassen).



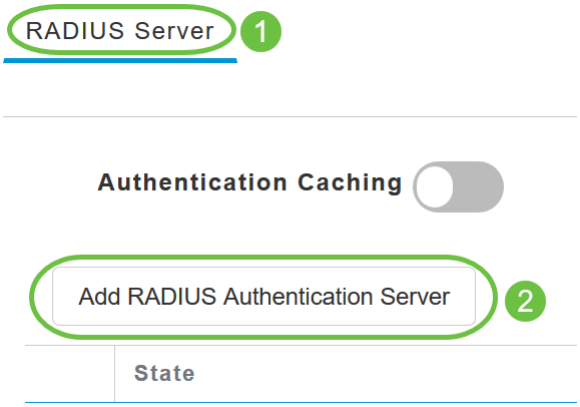
Stap 4

Navigeer naar het tabblad *WLAN-beveiliging*. Kies **WAP2Enterprise** in het vervolgkeuzemenu *Security Type*. Selecteer **Externe straal** als de *verificatieserver*. U kunt ervoor kiezen *Radius Profileren* in te schakelen.



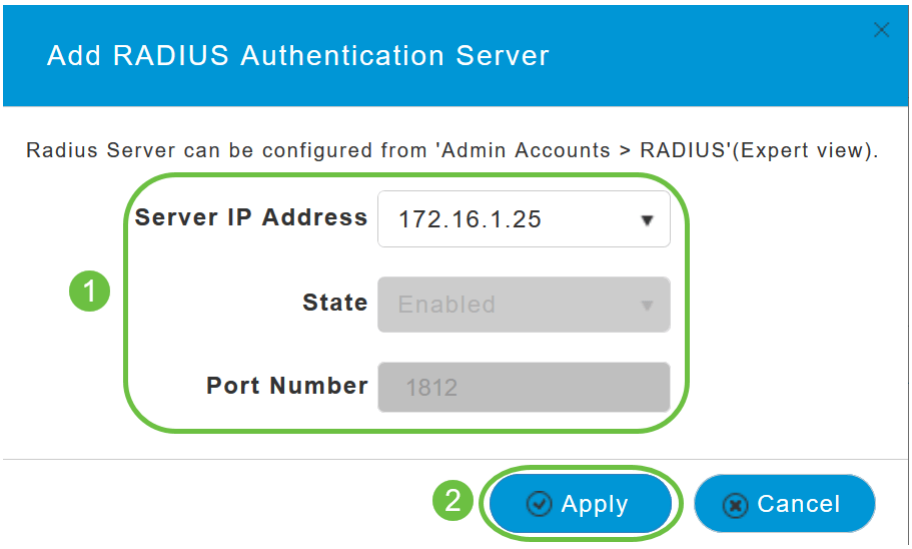
Stap 5

Navigeer naar *RADIUS Server* sectie. Klik op **Add RADIUS-verificatieserver**.



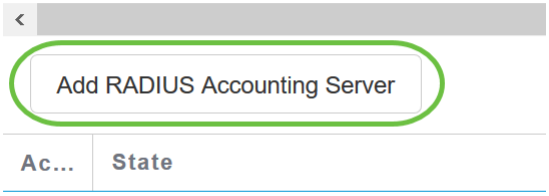
Stap 6

Controleer de details van de RADIUS-verificatieserver die u hebt ingesteld en klik op **Toepassen**.



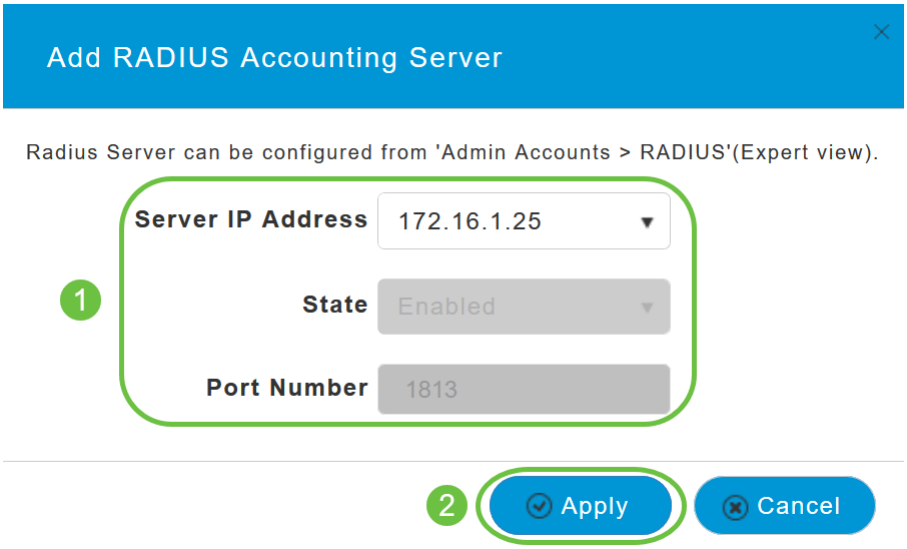
Stap 7

Klik op **Add RADIUS Accounting Server**.



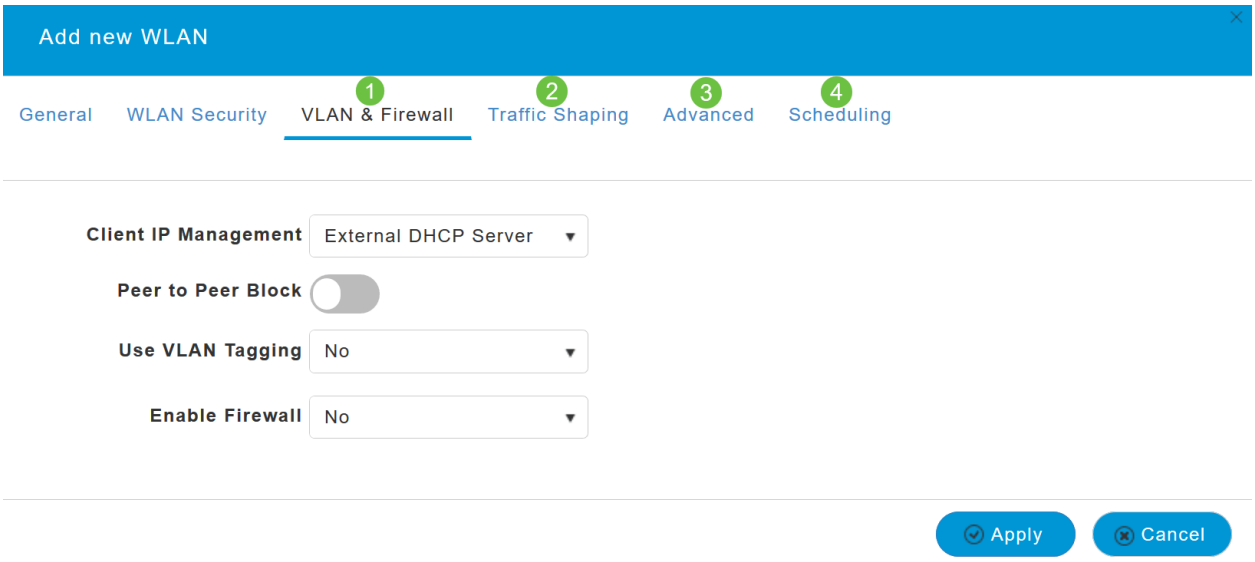
Stap 8

Controleer de details van de RADIUS-accounting server die u hebt ingesteld en klik op **Toepassen**
.



Stap 9

Navigeer naar *VLAN & Firewall*, *Traffic Shaping*, *Geavanceerd* en *Scheduling* om de instellingen te configureren op basis van uw netwerkvoorkeuren. Klik op **Apply** (Toepassen).

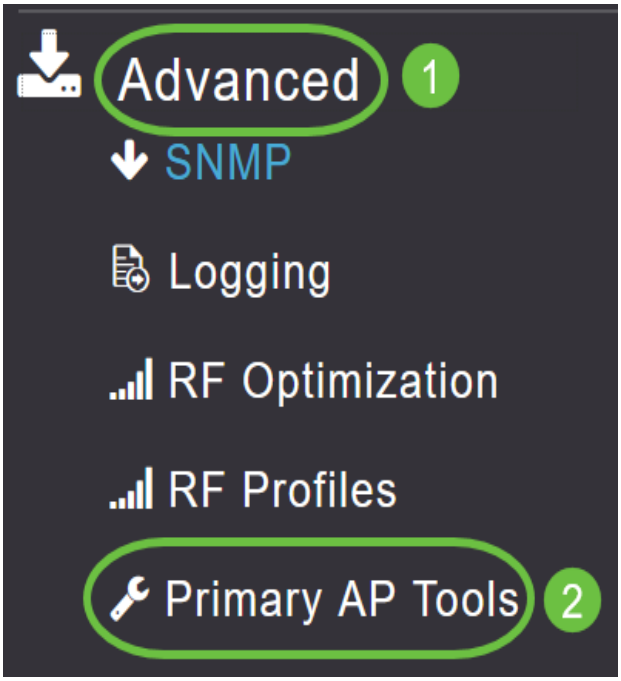


Verificatie

U kunt de RADIUS-verificatie op de volgende manieren testen:

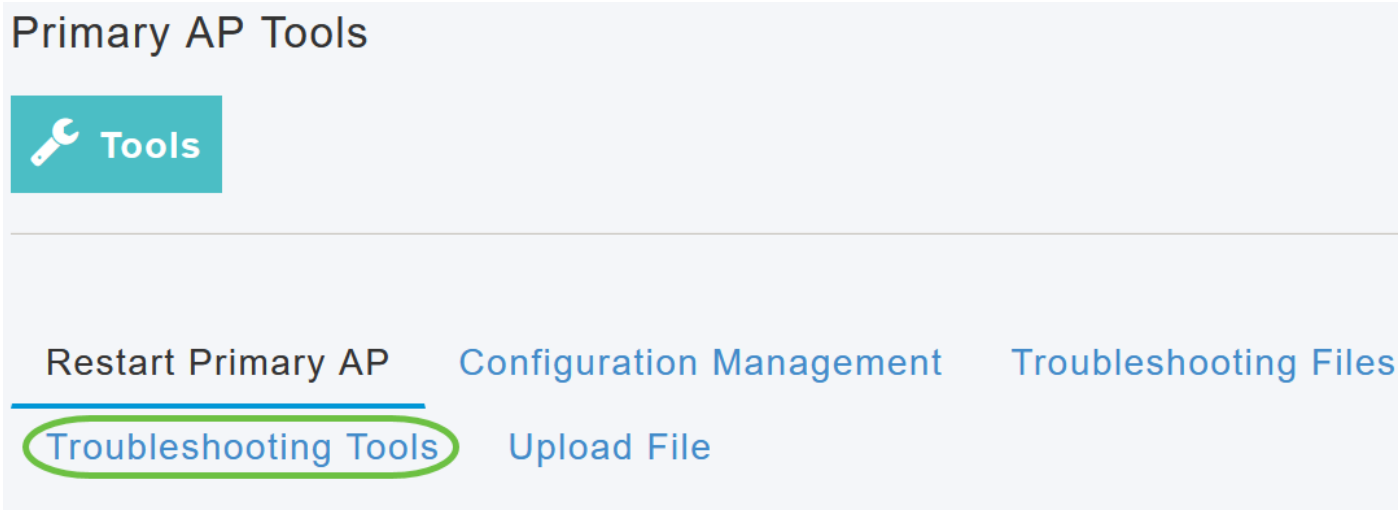
Stap 1

Navigeer naar **geavanceerde > Primaire AP tools**.



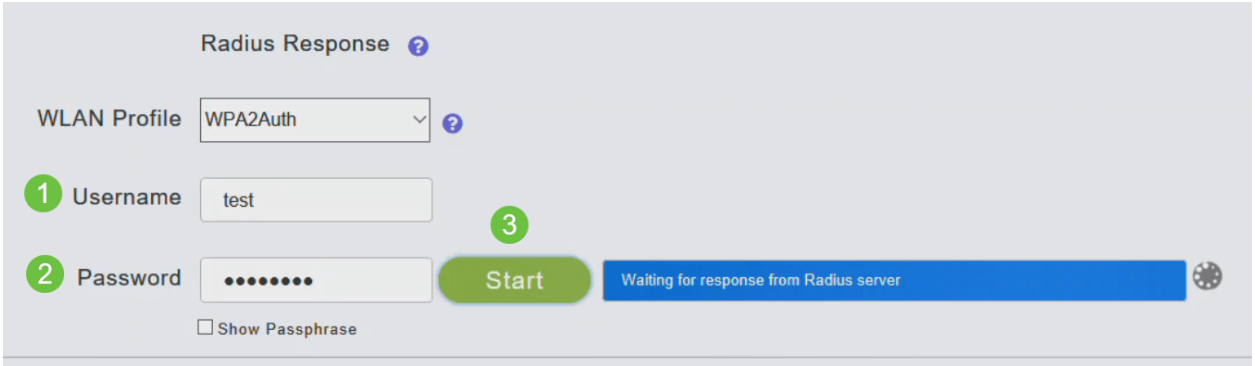
Stap 2

Klik op **Gereedschappen voor probleemoplossing**.



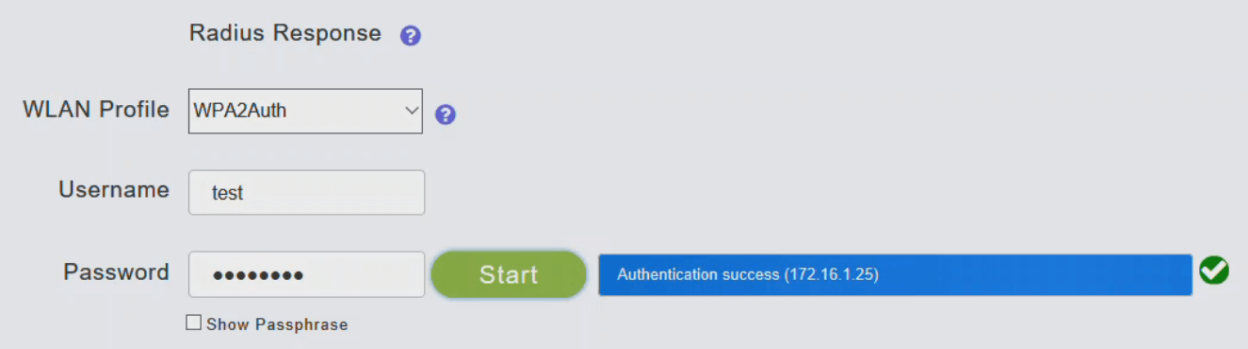
Stap 3

Voer in het gedeelte *Radius Response* de *gebruikersnaam* en *wachtwoord in* voor het WLAN-profiel dat u eerder hebt ingesteld en klik op **Start**.



Stap 4

Nadat de verificatie is voltooid, verschijnt het volgende bericht op het scherm.



Conclusie

Daar heb je het! U hebt nu de stappen geleerd om RADIUS op uw CBW AP te configureren. Raadpleeg voor meer geavanceerde configuraties de *Cisco Business Wireless Access Point Management-gids.*

Veelgestelde vragen upgrade van firmware RLAN's Toepassingsprofielen Clientprofielen Primaire AP-tools Umbrella WLAN-gebruikers Vastlegging traffic shaping Rogues Interferiers Configuratie-beheer mesh-poortconfiguratie