Persoonlijke voorgedeelde toetstitel in CBW access point

Doel

Dit artikel zal de persoonlijke voorgedeelde sleutel (PSK) verklaren in Cisco Business Wireless (CBW) access point (AP) firmware versie 10.6.1.0.

Toepasselijke apparaten | Software versie

- Cisco Business Wireless 140 AC access point | 10.6.1.0 (laatste download)
- Cisco Business Wireless 145 AC access point | 10.6.1.0 (laatste download)
- Cisco Business Wireless-240 AC access point | 10.6.1.0 (laatste download)

Inleiding

Als u CBW-apparatuur in uw netwerk hebt, kunt u de persoonlijke PSK-functie nu gebruiken in firmware versie 10.6.1.0!

Persoonlijke PSK, ook bekend als Individual PSK (iPSK), is een functie waarmee een beheerder unieke pre-gedeelde toetsen kan uitgeven aan individuele apparaten voor hetzelfde Wi-Fi Protected Access II (WAP2) persoonlijk Wireless Local Area Network (WLAN). De unieke PSK is gebonden aan het MAC-adres van het apparaat. Dit wordt niet ondersteund in WLAN's waar het WAP3-beleid is ingeschakeld.

Deze eigenschap authenticeert de client met een RADIUS-server. Het is in het algemeen bedoeld voor gebruik door IoT-toestellen en door de onderneming verstrekte laptops en mobiele apparatuur.

Inhoud

Voorwaarden

- Zorg ervoor dat u de CBW AP firmware hebt bijgewerkt tot 10.6.1.0. Klik als u stap voor stap instructies wilt doen voor een firmware-update.
- U hebt een RADIUS-server nodig waarin de persoonlijke PSK- en het MAC-adres van het apparaat moeten worden ingesteld.
- Deze CBW-functie wordt ondersteund met drie verschillende RADIUS-servers: FreeRADIUS, Microsoft's NPS en Cisco ISE. De configuratie zal variëren afhankelijk van

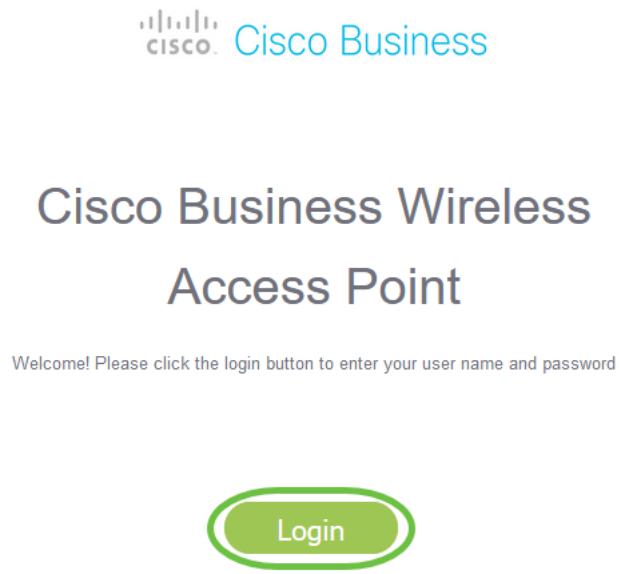
de gebruikte RADIUS-server.

CBW RADIUS-instellingen configureren

Om de RADIUS-instellingen op de CBW AP te configureren volgt u de stappen.

Stap 1

Meld u aan bij de webgebruikersinterface (UI) van de CBW AP.

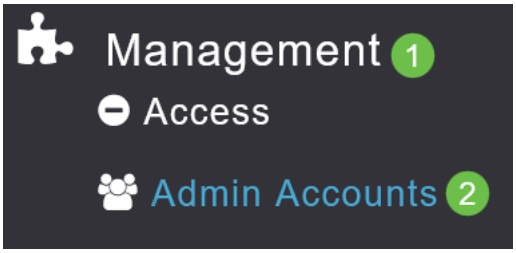


Stap 2

Klik op het symbool **van de tweerichtingspijl** om door een deskundige weergave te switches.

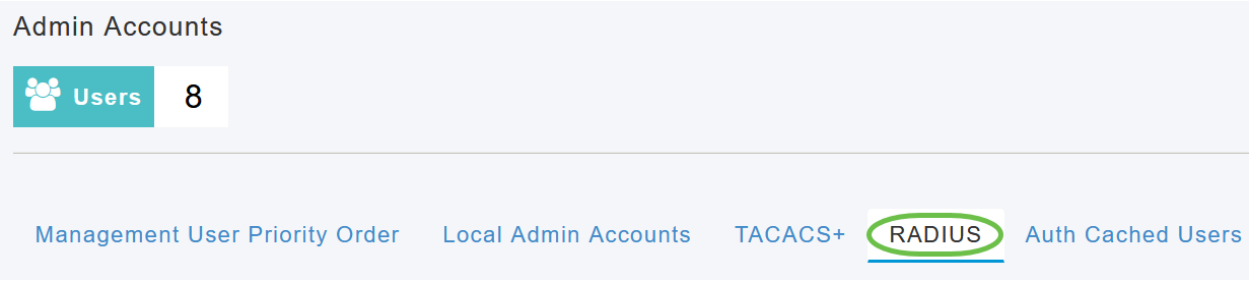
Stap 3

Navigeren in **beheer > Admin accounts.**



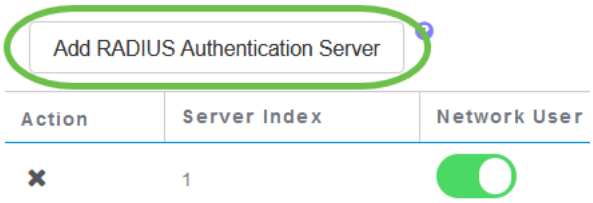
Stap 4

Selecteer het tabblad **RADIUS**.



Stap 5

Klik op **Add RADIUS-verificatieserver**.

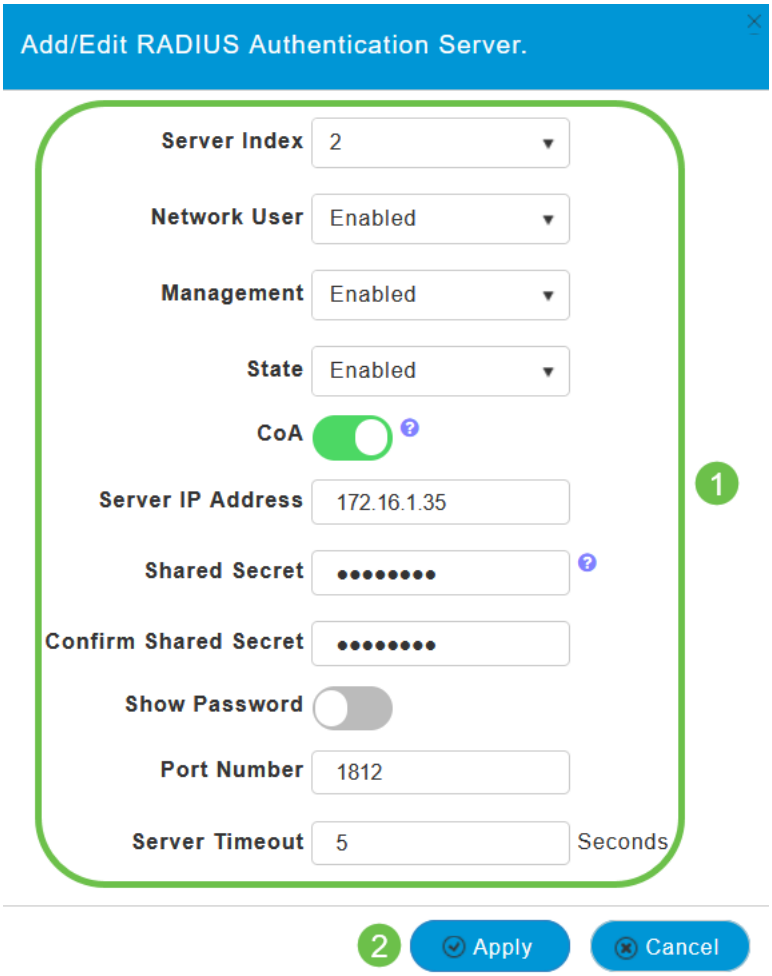


Stap 6

Het volgende configureren:

- *Server Index* - selecteer 1 tot en met 6
- *Netwerkgebruiker* - Schakel de staat in. Dit is standaard ingeschakeld
- *Beheer* - Schakel de staat in. Dit is standaard ingeschakeld
- *Staat* - Laat de staat in werking. Dit is standaard ingeschakeld
- *CoA* - Zorg ervoor dat het gezag is ingeschakeld.
- *IP-adres van de server* - Voer het IPv4-adres van de RADIUS-server in
- *Gedeeld geheim* - Voer de gedeelde geheime sleutel 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).



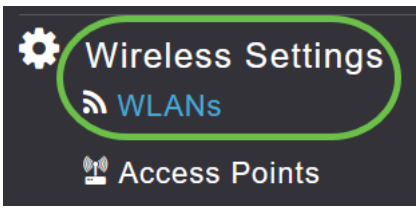
WLAN-instellingen configureren

Maak een WLAN als standaard WAP2 persoonlijk beveiligd WLAN.

De vooraf gedeelde sleutel wordt niet gebruikt voor de persoonlijke PSK-apparaten. Dit zou alleen worden gebruikt voor apparaten die NIET geauthentiseerd zijn op de RADIUS-server. U moet de MAC-adressen van ELK apparaat toevoegen dat met dit WLAN zal worden verbonden, aan de lijst met toegangsrechten van dit apparaat.

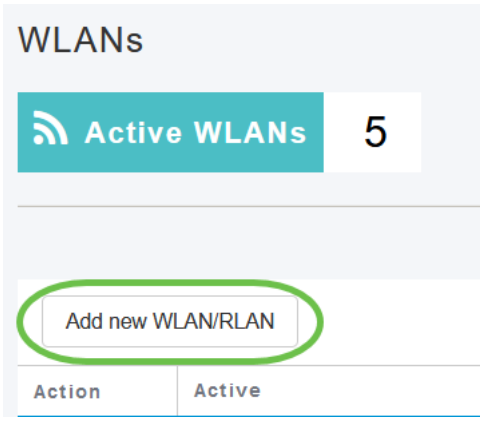
Stap 1

Navigeer naar **draadloze instellingen > WLAN's**.



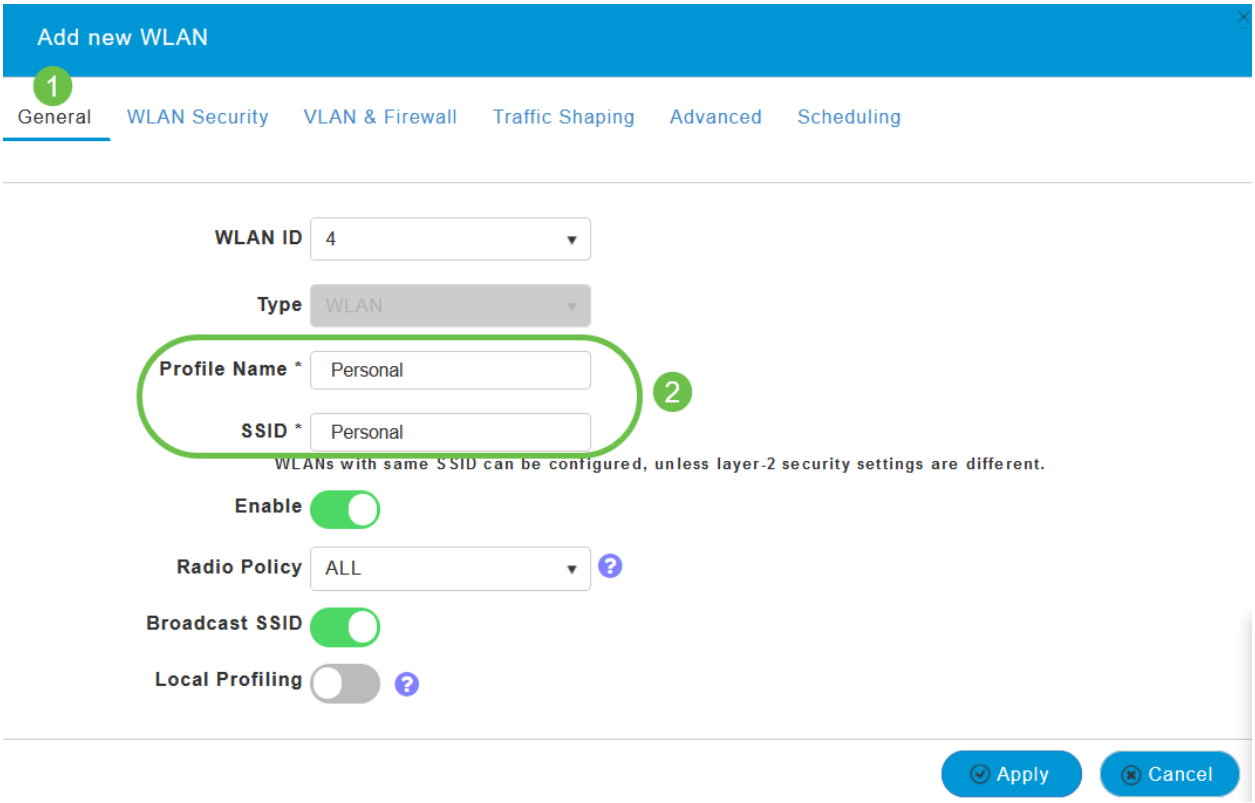
Stap 2

Klik op **Add new WLAN/RLAN**.



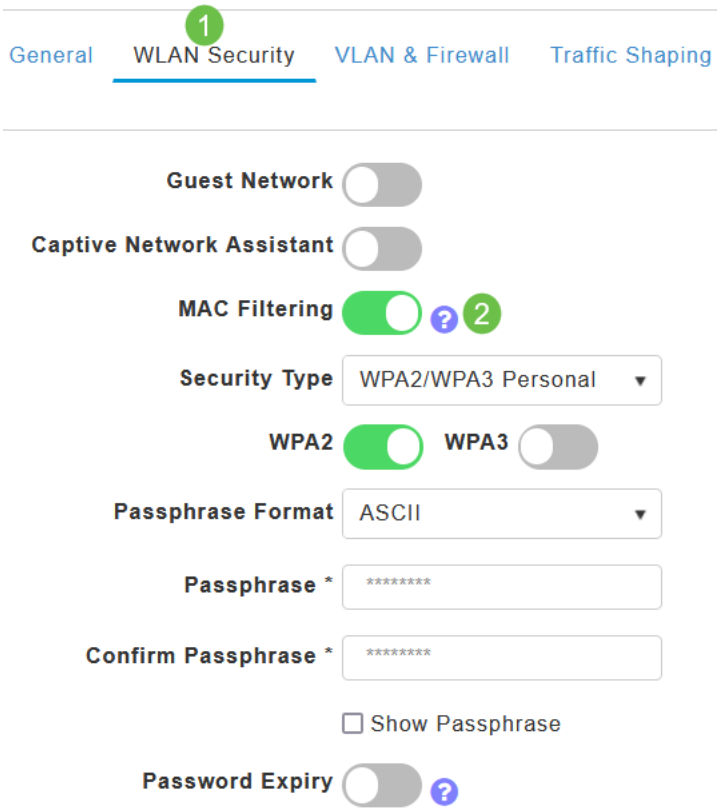
Stap 3

Voer onder *het* tabblad *General* een *Profile Name* in voor WLAN.



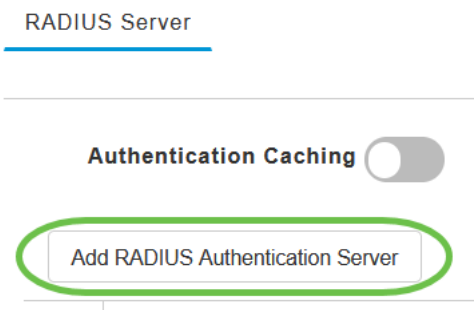
Stap 4

Navigeer naar het tabblad **WLAN** Security en selecteer **MAC-filtering** door de draaiknop te schuiven.



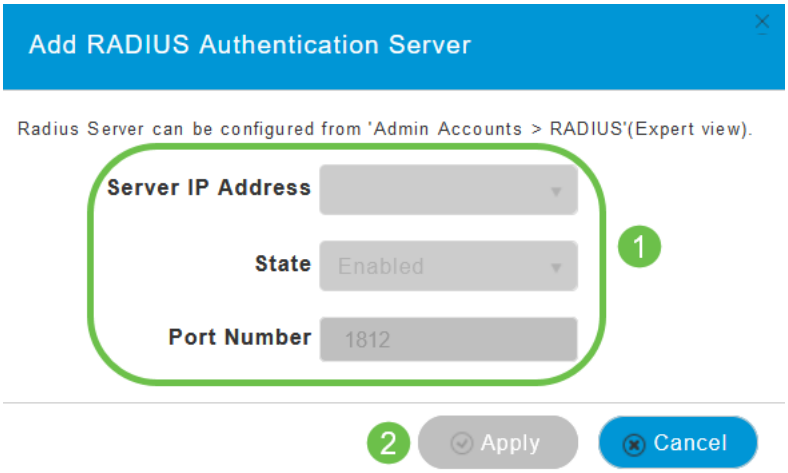
Stap 5

Klik op **Add RADIUS-verificatieserver** om de RADIUS-server toe te voegen die in de vorige sectie is ingesteld om verificatie voor deze WLAN-server te leveren.



Stap 6

Er verschijnt een pop-upvenster. Voer het *IP-adres, de staat en het poortnummer van de server in*. Klik op **Apply** (Toepassen).

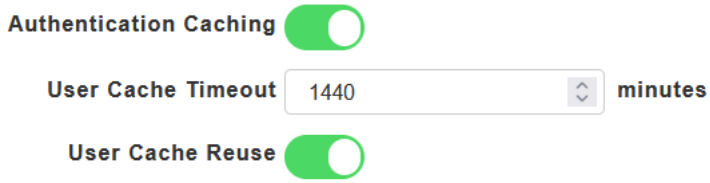


Stap 7

(Optioneel)

Verificatie inschakelen. Wanneer u deze optie activeert, worden de volgende velden weergegeven.

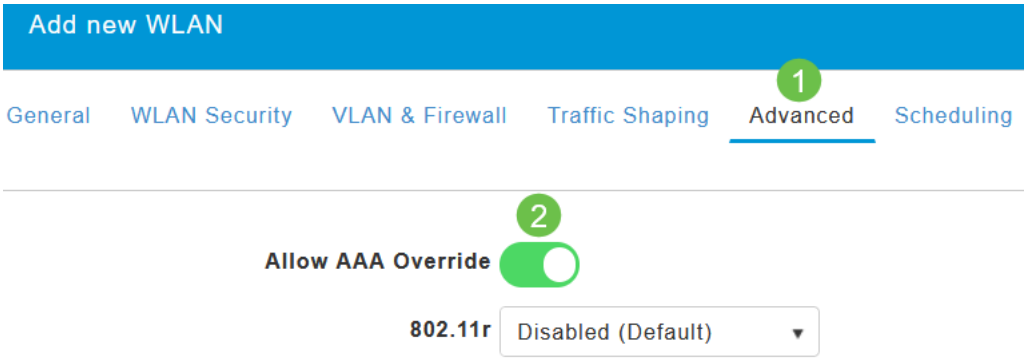
- *Time-out bij gebruikerscache* - Specificeert de periode waarin de geauthenticeerde gecrediteerde waarde in het cache vervalt.
- *Gebruiker Cache Reuse* - Gebruik de aanmeldingsgegevens in het cachegeheugen voor de cachetijd. Standaard wordt dit
is uitgeschakeld.



Als deze functie is ingeschakeld, hoeft een client die al geauthentiseerd is op deze server geen gegevens naar de RADIUS-server door te geven wanneer ze binnen de komende 24 uur opnieuw verbinding maken met dit WLAN.

Stap 8

Blader naar het tabblad Geavanceerd. Schakel **in om AAA-override** toe te **staan** door door de kneep te schuiven.

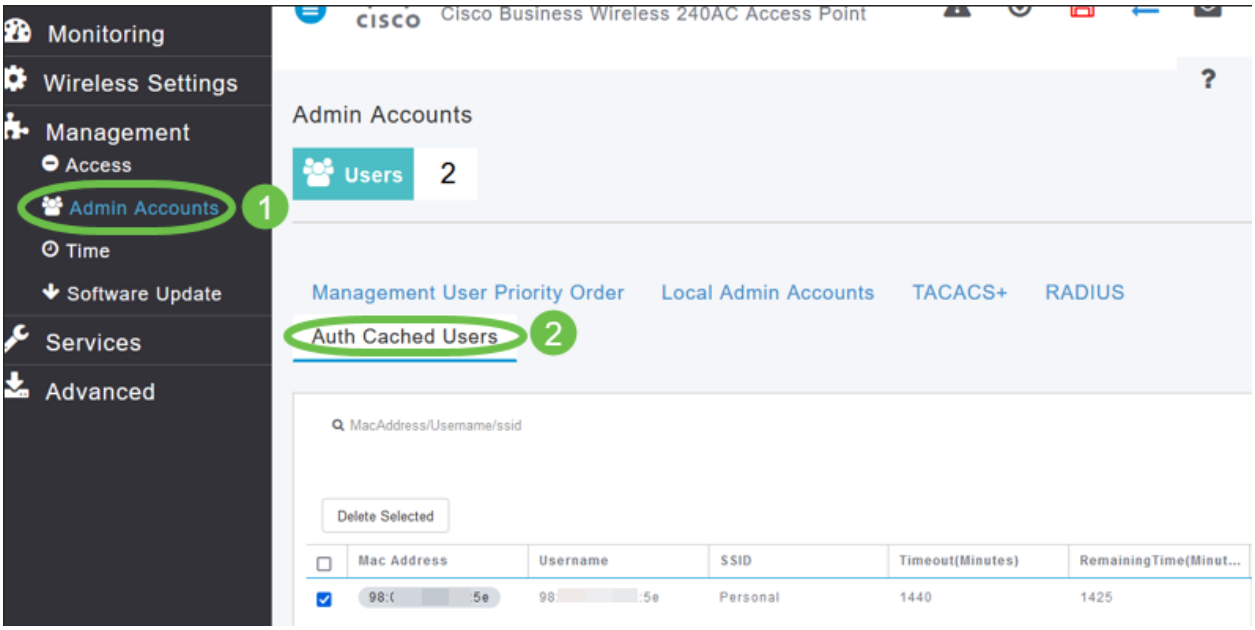


Het tabblad *Geavanceerd* is alleen zichtbaar als u in de *deskundigenweergave* bent.

Volgende stappen

Nadat u de instellingen op uw CBW AP hebt ingesteld en uw RADIUS server hebt ingesteld, kunt u uw apparaat aansluiten. Voer de aangepaste PSK in die voor dat MAC-adres is ingesteld en deze sluit zich aan bij het netwerk.

Als u authenticatie caching hebt ingesteld, kunt u de apparaten zien die zich bij het WLAN hebben aangesloten door naar het *Auth Cwel* tabblad Gebruikers te gaan onder *Admin Account*. Indien nodig kan dit worden verwijderd.



Conclusie

Daar ga je. U kunt nu profiteren van de voordelen van de persoonlijke PSK-functie op uw CBW AP.