Lokale verificatie configureren in FlexConnect-modus

Inhoud

- Inleiding
  - Achtergrondinformatie
    - Overzicht en vereisten van FlexConnect
    - werkwijzen
    - Snelle en veilige roaming
    - FlexConnect High Scale-modus
    - Ondersteuning voor Wi-Fi 7 FlexConnect
    - FlexConnect-veerkrachtscenario's
- Voorwaarden
  - Vereisten
  - Gebruikte componenten
- Configureren
  - Netwerkdiagram
  - AAA-servers configureren
  - FlexConnect-modus op de externe site configureren
  - Configureer 802.1x WLAN met lokale verificatie met een externe RADIUS-server
  - ISE configureren
  - PSK WLAN configureren met lokale verificatie
- Verifiëren
- Problemen oplossen
  - Standalone scenario
- Gerelateerde informatie

Inleiding

In dit document wordt beschreven hoe lokale FlexConnect-verificatie werkt en hoe deze kan worden geconfigureerd met de Cisco Catalyst 9800 Series Wireless Controller (WLC)

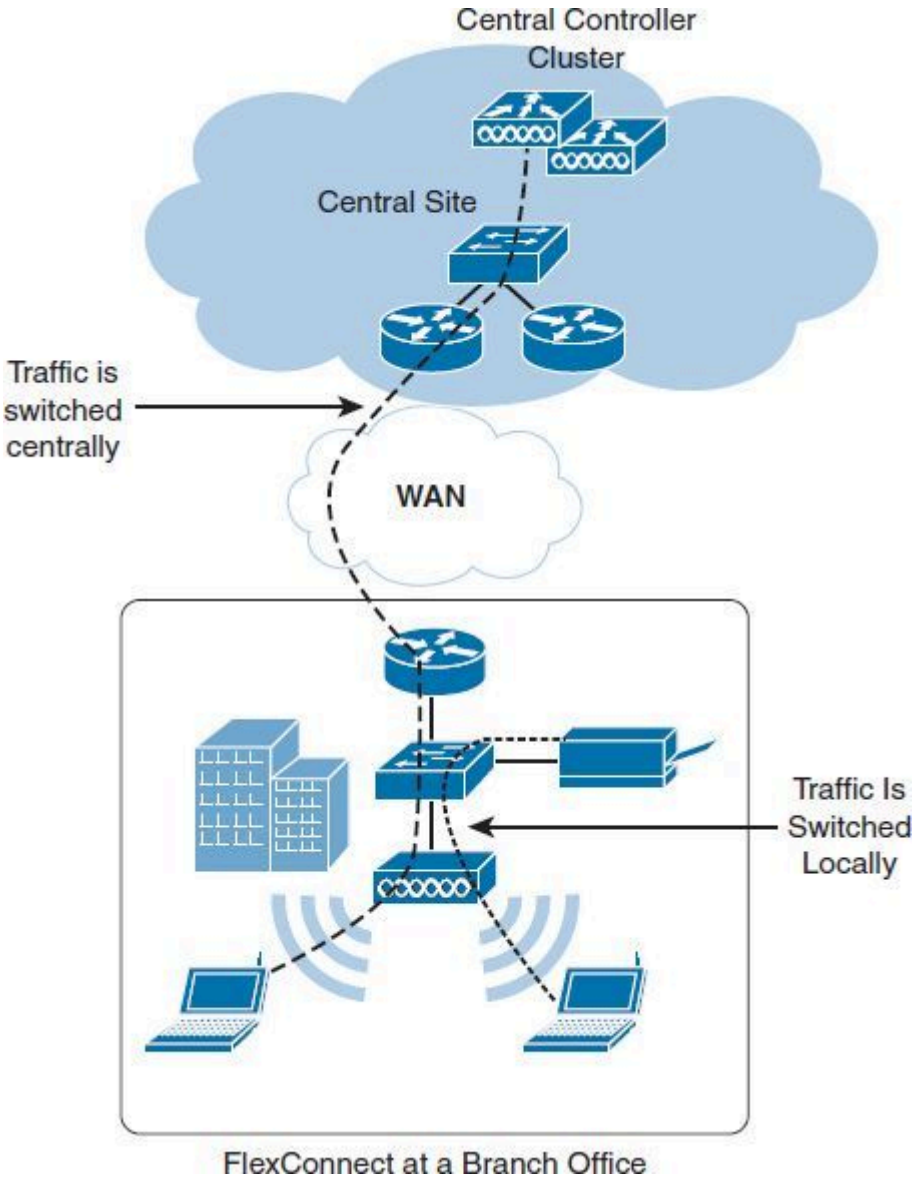
Achtergrondinformatie

Overzicht en vereisten van FlexConnect

Met FlexConnect kan Access Point (AP) op externe kantoren of filialen verbinding maken met een

gecentraliseerde controller, terwijl lokale verwerking van draadloos verkeer mogelijk is. In tegenstelling tot traditionele gecentraliseerde draadloze implementaties waarbij al het draadloze verkeer via CAPWAP (Control and Provisioning of Wireless Access Points) naar de controller wordt geleid, kan met FlexConnect het verkeer lokaal worden geschakeld en rechtstreeks door het toegangspunt van de vestiging worden verwerkt. Deze lokale switching biedt het toegangspunt een zekere mate van autonomie, waardoor belangrijke diensten zoals beveiliging, roaming en Quality of Service (QoS) onafhankelijk van de controller kunnen functioneren.

Hoewel FlexConnect voornamelijk is ontworpen voor het schakelen van lokaal verkeer, biedt het ook de mogelijkheid om specifieke SSID's (Service Set Identifier) centraal te switches wanneer dat nodig is. Als er bijvoorbeeld bepaald verkeer door een centrale firewall moet gaan, kunnen die SSID's via CAPWAP naar de controller worden teruggestuurd voor gecentraliseerde switching. Dankzij deze dubbele mogelijkheid kan één FlexConnect-toegangspunt tegelijk zowel lokaal als centraal geschakelde WLAN's (Wireless Local Area Network) ondersteunen.



Een FlexConnect-toegangspunt dat bij een vestiging wordt geïmplementeerd, Switch lokaal de ene SSID terwijl een andere centraal wordt geschakeld

werkwijzen

FlexConnect-toegangspunten werken in twee modi: verbonden modus en zelfstandige modus.

- In de verbonden modus onderhoudt het toegangspunt een actieve verbinding met de controller via het CAPWAP-controlekanaal.
- De stand-alone modus is een noodtoestand die optreedt wanneer het toegangspunt de verbinding met de controller verliest.

Onder normale omstandigheden werken FlexConnect-toegangspunten in de verbonden modus, waarbij de controller kritieke services beheert, zoals gecentraliseerde verificatie, clientprofilering en Radio Resource Management (RRM). Hoewel het toegangspunt naar verwachting het grootste deel van de tijd in deze modus blijft, wordt het automatisch naar de stand-alone modus switch als de communicatie met de controller verloren gaat. In de stand-alone modus blijft het toegangspunt actief, waarbij het verkeer lokaal wordt verwisseld en clients verbonden kunnen blijven. De toegangspunten verifiëren onafhankelijk clients zonder verificatieverzoeken door te sturen naar een centrale controller. Bepaalde van de controller afhankelijke services, zoals RRM en gecentraliseerde clientverificatie, zijn echter tijdelijk niet beschikbaar.

Als een storing in het WAN (Wide Area Network) bijvoorbeeld de verbinding tussen het toegangspunt en de controller verstoort, maar de internettoegang actief blijft, schakelt het toegangspunt over naar de stand-alone modus en blijft het lokaal geschakeld verkeer zonder onderbreking verwerken. Bestaande clients blijven verbonden, maar nieuwe clients waarvoor centrale verificatie is vereist, kunnen geen lid worden van het netwerk, tenzij lokale verificatie is geconfigureerd. FlexConnect-toegangspunten kunnen worden ingesteld om lokale verificatie uit te voeren tijdens WAN-storingen, zodat de service wordt voortgezet, zelfs wanneer de controller onbereikbaar is.

In de stand-alone modus zijn deze functies niet beschikbaar voor het toegangspunt:

- Client-webverificatie
- Gastverificatie (omleiding via portal)
- Alle centraal geschakelde SSID's
- RRM
- IPv6 Layer-3-mobiliteit
- Native profiling
- Beleidsclassificatie

- Service Discovery Gateway
- Configuratie-updates

Zie de functiematrix: Functiematrix voor Cisco Wireless Access Points voor een volledige lijst van functies en WLAN-configuraties die in de standalone modus (lokale verificatie) worden ondersteund

Een veelvoorkomend FlexConnect-storingsscenario houdt in dat het WAN volledig verloren gaat of aanzienlijk verslechtert, waardoor het CAPWAP-controlekanaal wordt verstoord. Wanneer het toegangspunt de connectiviteit met de controller verliest vanwege WAN-problemen, wordt het onmiddellijk naar de stand-alone modus switches.

Het primaire doel tijdens een WAN-storing is om de communicatie met de controller zo snel mogelijk te herstellen om de volledige functionaliteit te hervatten.

Wanneer een FlexConnect-toegangspunt de standalone-modus ingaat vanwege een WAN-storing, blijven actieve clients verbonden en kunnen ze naadloos tussen toegangspunten binnen de FlexConnect-domein-/sitetag roamen, maar voor roaming tussen verschillende FlexConnect-sitetags is volledige herverificatie vereist. Nieuwe clients die proberen lid te worden van het lokaal geschakelde WLAN kunnen echter niet worden geverifieerd omdat de AAA-server (Authentication, Authorisation, and Accounting Server) op de centrale locatie niet bereikbaar is.

Snelle en veilige roaming

EAP-verificatie (Extensible Authentication Protocol) introduceert een hogere latentie in vergelijking met PSK-verificatie (Pre-Shared Key) vanwege de uitwisseling van EAP-frames met de AAA-server. Met snelle en veilige roaming ondergaat een client echter alleen tijdens de eerste verbinding met het netwerk een volledige 802.1X/EAP-verificatie. Bij latere roams naar naburige AP's wordt de EAP-uitwisseling omzeild, waardoor alleen de viervoudige handdruk overblijft, wat aanzienlijk sneller is omdat de AAA-server er niet bij betrokken is. In deze tabel worden de verschillende snelle en veilige roamingmethoden beschreven die door de 9800 WLC worden ondersteund in zowel de lokale modus als FlexConnect-implementaties.

Feature	Lokale modus	FlexConnect (Connected Mode; centrale verificatie)	FlexConnect (Connected Mode—Lokale verificatie)	FlexConnect (zelfstandig)
Sticky Key	Niet ondersteund	Niet ondersteund	Niet ondersteund	Niet ondersteund

Caching (SKC)				
Opportunistische Key Caching (OKC)	ondersteund	ondersteund	ondersteund	Ondersteund (totdat de clientsessie verloopt)
Cisco Centralized Key Management (CCKM)	ondersteund	ondersteund	ondersteund	Niet ondersteund
FT-802.11r/ Adaptive 11r (snelle overgang) (via de lucht)	ondersteund	ondersteund	ondersteund	Ondersteund (totdat de clientsessie verloopt)
FT-802.11r/ Adaptive 11r (snelle overgang) (via de DS)	ondersteund	ondersteund	Niet ondersteund	Niet ondersteund

In de standalone-modus is snel roamen afhankelijk van het feit of het materiaal van de gecachte sleutel geldig blijft. Wanneer de PMK (Pairwise Master Key)/sessie in cache verloopt, kan het toegangspunt geen nieuwe van de controller afgeleide sleutelinformatie verkrijgen totdat de connectiviteit van de controller is hersteld.

FlexConnect High Scale-modus

Vanaf Cisco IOS XE 17.8.1 is de flexsitecapaciteit opgeschaald naar 300 AP's en 3000 802.1x-clients.

Met PMK-propagatie kunnen AP's binnen dezelfde FlexConnect-site PMK-informatie delen, waardoor er minder behoefte is aan een volledige EAP-uitwisseling tijdens roaming. PMK-propagatie is standaard niet ingeschakeld.

Gebruik deze opdrachten om de PMK-propagatie te controleren en PMK in te schakelen:

- Draadloze statistieken weergeven PMK-propagatie
- PMK-propageren

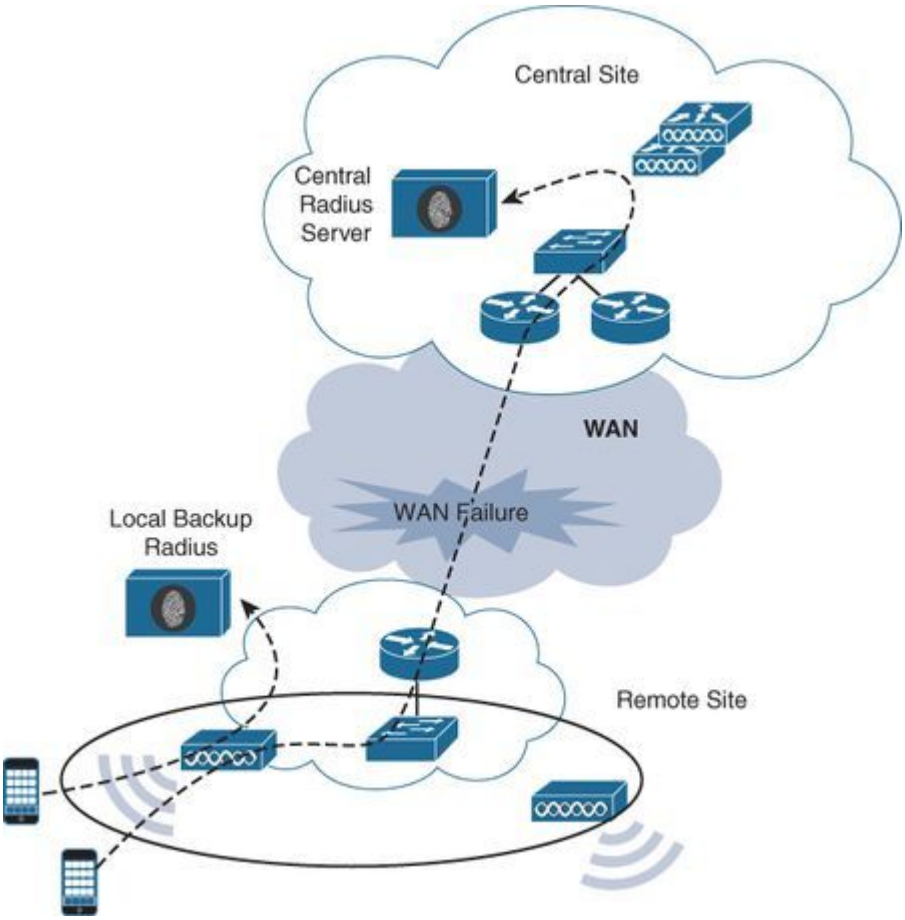
Ondersteuning voor Wi-Fi 7 FlexConnect

Deze tabel geeft een overzicht van de FlexConnect-functies die worden ondersteund in de CW917x Wi-Fi 7 AP-reeks.

Feature	steun
Lokaal schakelen	ondersteund
centrale omschakeling	ondersteund
WLAN-VLAN-toewijzing	ondersteund
Lokale verificatie met externe RADIUS	ondersteund
WPA3-Enterprise	ondersteund
FT-802.11r Fast Roaming	ondersteund
Multi Link Operation (MLO)	ondersteund
Lokale verificatie met interne STRAAL	Niet ondersteund
WPA3-Enterprise-192	Niet ondersteund

FlexConnect-veerkrachtscenario's

1. In een N+1-instelling voor veerkracht delen meerdere actieve controllers een gemeenschappelijke back-upcontroller die het overneemt als een actieve controller uitvalt. Wanneer een primaire controller offline gaat, switches FlexConnect-toegangspunten onmiddellijk naar de standalone-modus en beginnen ze te zoeken naar de back-upcontroller. Tijdens deze periode worden centraal geschakelde clients losgekoppeld van de toegangspunten. Zodra de toegangspunten de back-upcontroller hebben gevonden en gesynchroniseerd, worden clients die toegang tot centraal geschakelde SSID's nodig hebben, opnieuw verbonden. Ondertussen blijven lokaal geschakelde clients onaangetast en blijven ze actief zonder de onderbreking van de service op te merken.
2. Zorg voor een back-up AAA-server op de externe locatie die toegankelijk is voor de FlexConnect-groep. Als lokale verificatie is ingeschakeld, wordt deze RADIUS-back-upserver alleen gebruikt wanneer de toegangspunten in de standalone-modus worden gezet. Deze blijft inactief terwijl de toegangspunten in de verbonden modus staan. Wanneer FlexConnect-toegangspunten de lokale AAA-back-upserver gebruiken voor verificatie, worden de verificatiesleutels verspreid over alle toegangspunten in de FlexConnect-groep, net zoals ze zouden zijn met een gecentraliseerde AAA-server. Dit zorgt ervoor dat nieuwe clients nog steeds naadloos tussen AP's kunnen zwerven zonder opnieuw te hoeven verifiëren, zelfs wanneer de RADIUS-back-upserver in gebruik is.
3. Elke methode die aanwezig is op de Feature Matrix voor Cisco Wireless Access Points die lokale verificatie mogelijk maakt.



Clients verifiëren met een lokale back-up AAA-server wanneer de centrale AAA-server niet beschikbaar is vanwege een WAN-fout

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

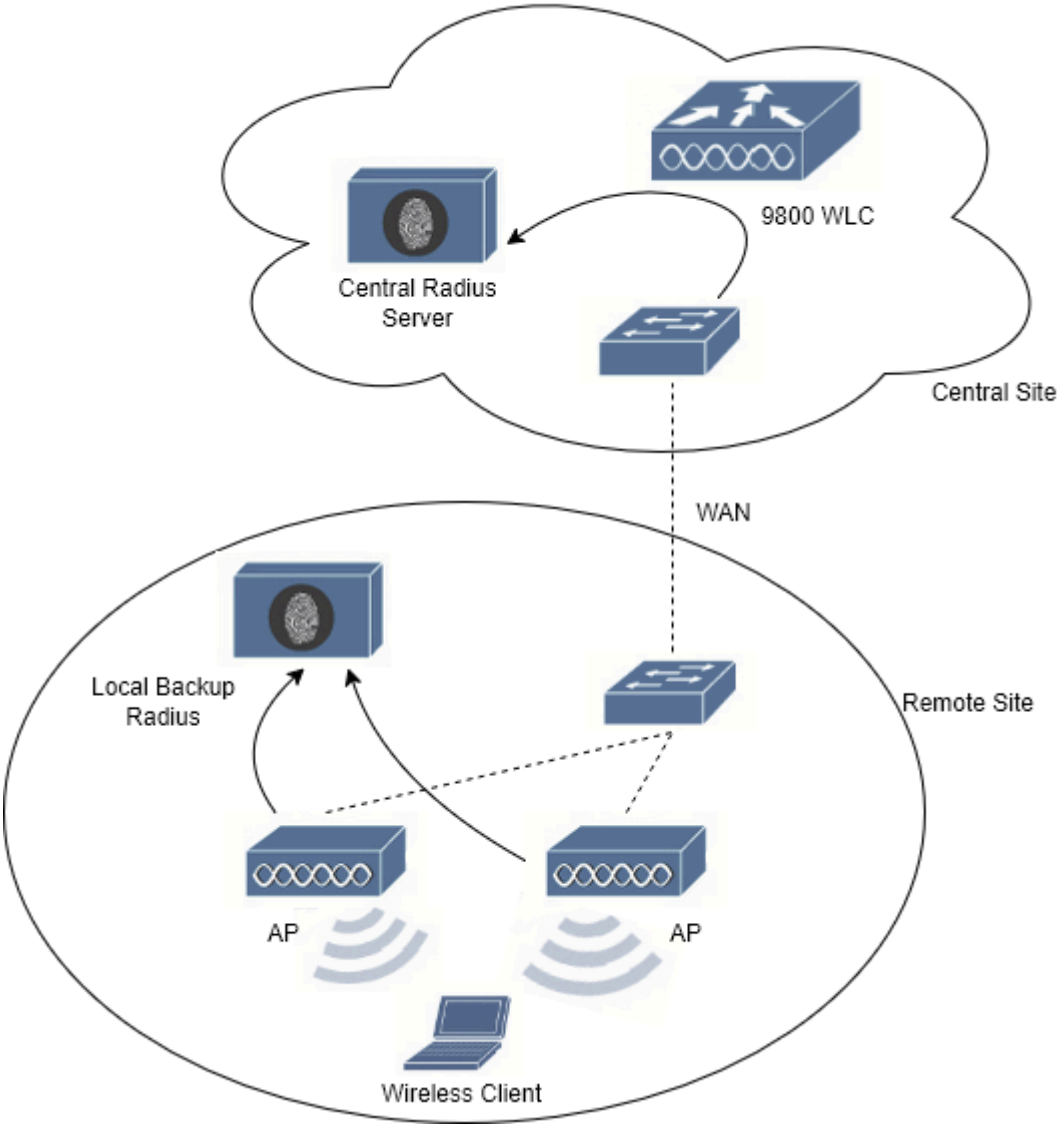
- Catalyst C9800-CL draadloze controller voor cloud met Cisco IOS® XE Dublin 17.18.3
- Catalyst CW9164I-ROW Access Point v17.18.3.18
- Aironet® AIR-AP2802I-E-K9 Access Point v17.18.3.18
- 2 x Identity Services Engine v3.2.0.542

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdiagram



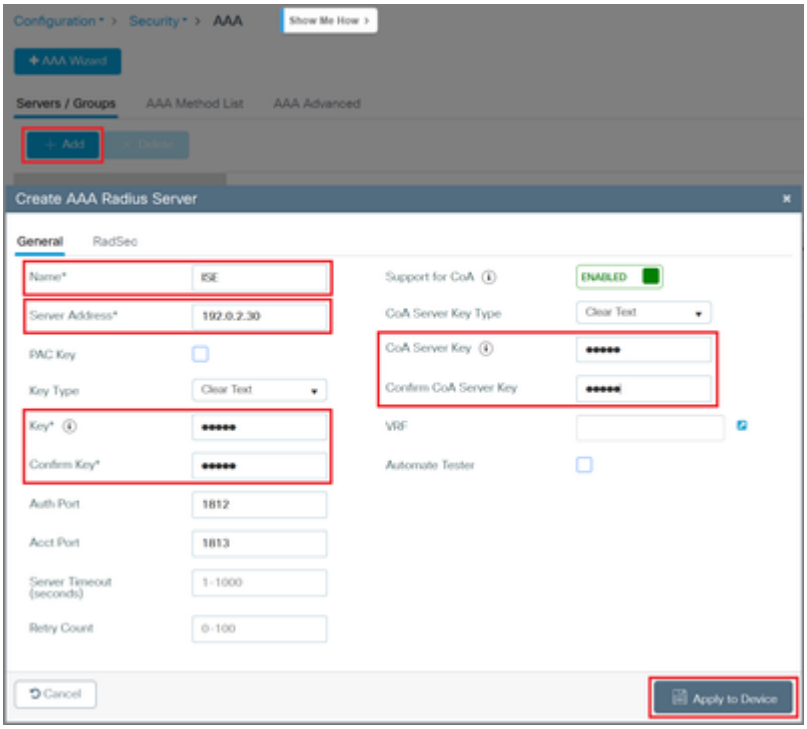
Netwerkdiagram

AAA-servers configureren

Stap 1. Als u een 802.1x WLAN wilt configureren, moet u de AAA-servergroep maken op de 9800 WLC.

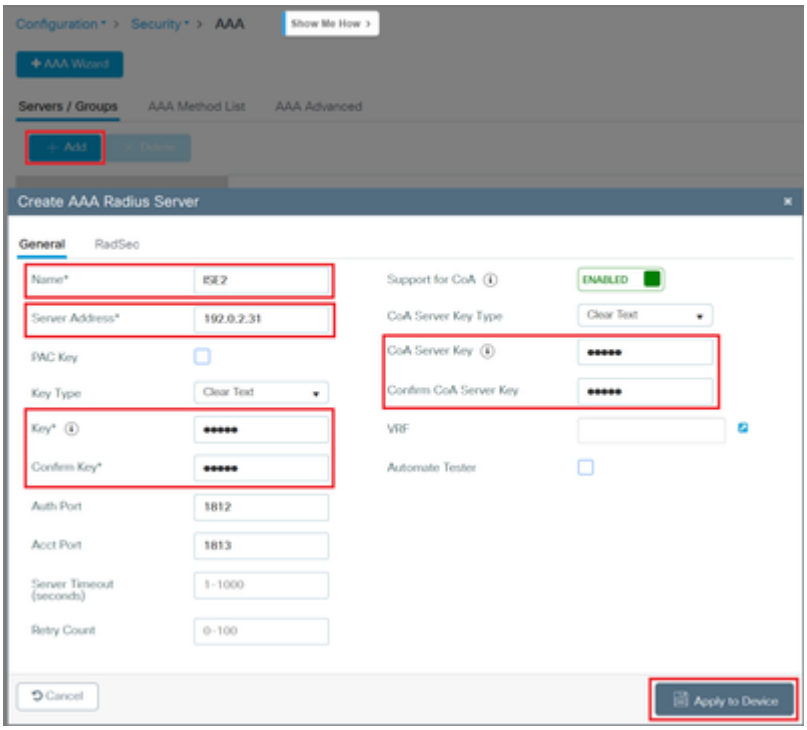
Maak een AAA-server voor elke site - die op de centrale site en de andere op de externe site.

Ga naar Configuratie > Beveiliging > AAA > Server/groepen > Servers en selecteer +Toevoegen. Geef een naam aan de server, het IP-adres, de sleutel (en bevestig de sleutel), schakel de ondersteuning voor CoA (Wijziging van autorisatie) in en voer de coa-serversleutel in (en bevestig de coa-serversleutel). De sleutels moeten hetzelfde zijn.



Klik op Toepassen op apparaat.

Stap 2. De andere AAA-server maken:



Klik op Toepassen op apparaat.

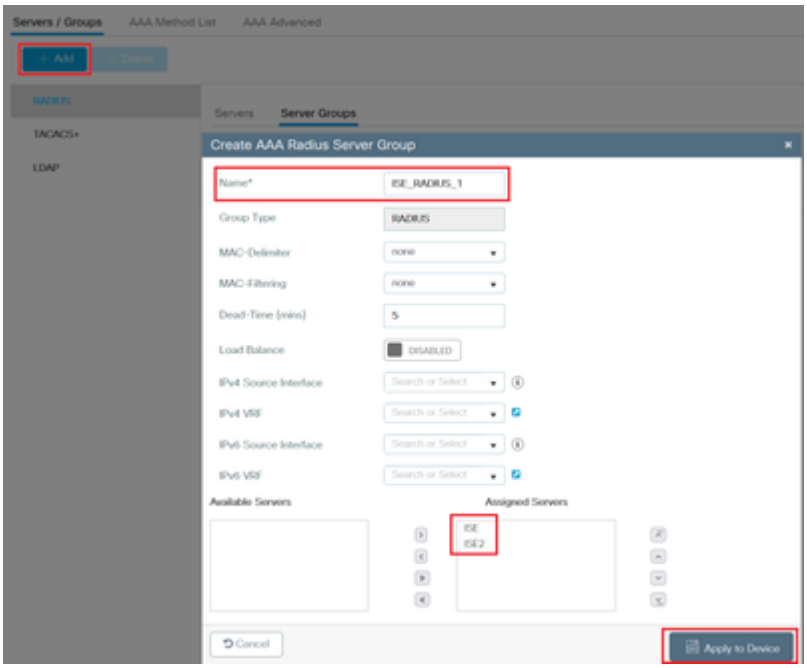
U ziet nu uw AAA-servers geconfigureerd:

Servers | Server Groups

	Name	Address	Auth Port	Acct Port
☐	ISE	192.0.2.30	1812	1813
☐	ISE2	192.0.2.31	1812	1813

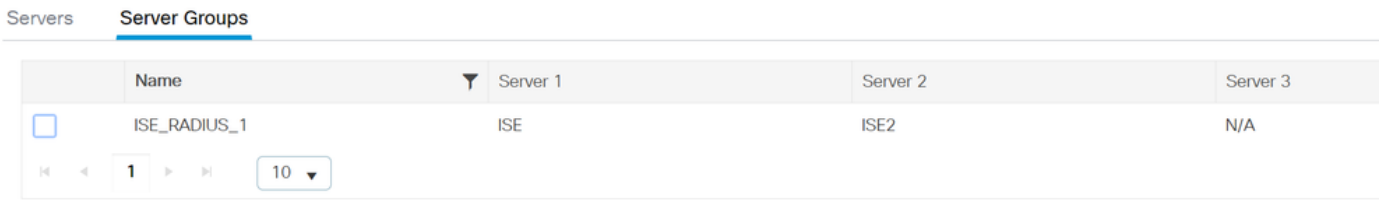
1 10 1 - 2 of 2 items

Stap 3. Ga naar Configuratie > Beveiliging > AAA > Server/groepen > Servergroepen en selecteer +Toevoegen. Geef een naam aan de groepsserver en selecteer de eerder gemaakte AAA-servers in de kolom Toegewezen servers:



Klik op Toepassen op apparaat.

Vervolgens ziet u de AAA-servergroep geconfigureerd:



CLI:

```
aaa new-model
!
radius server ISE
address ipv4 192.0.2.30 auth-port 1812 acct-port 1813
key keystring
!
radius server ISE2
address ipv4 192.0.2.31 auth-port 1812 acct-port 1813
key keystring
!
aaa server radius dynamic-author
client 192.0.2.30 server-key keystring
client 192.0.2.31 server-key keystring
!
aaa group server radius ISE_RADIUS_1
server name ISE
server name ISE2
deadtime 5
```

FlexConnect-modus op de externe site configureren

Stap 1. De eerste stap is het configureren van FlexConnect op de externe site.

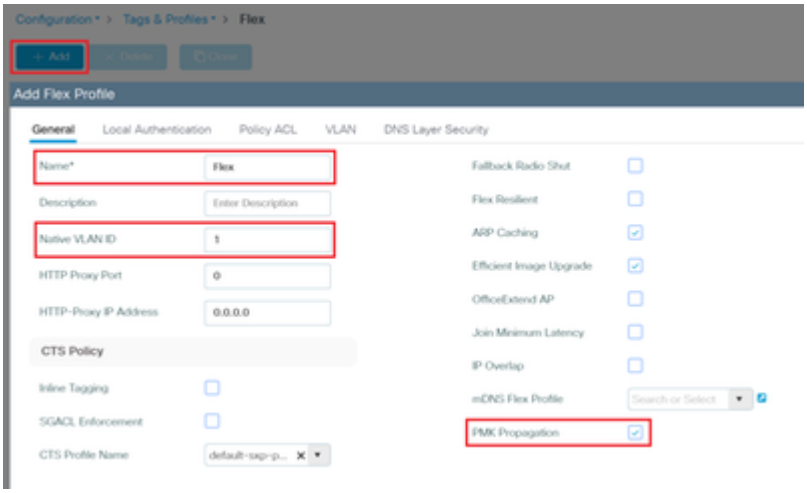
Gebruik deze handleiding om de modus voor toegangspunten te wijzigen in Flex: FlexConnect begrijpen op Catalyst 9800 Wireless Controller.

De toegangspunten in deze handleiding/het lab gebruiken hetzelfde flexprofiel.

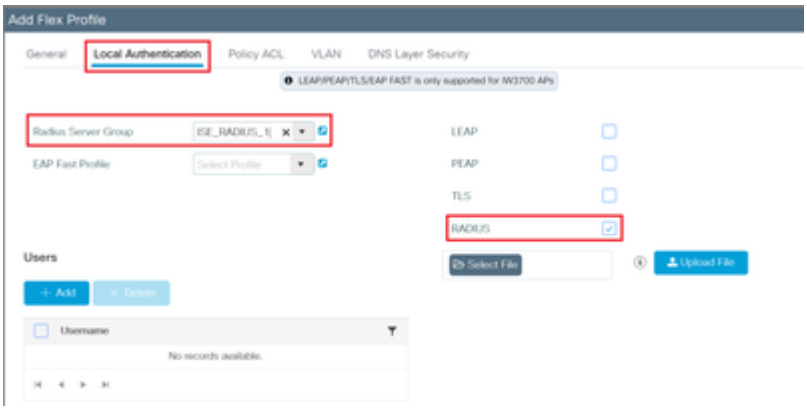
Stap 2. Navigeer naar Configuration > Tags & Profiles > Flex.

Maak een nieuwe Flex-profielnaam met +Toevoegen. Geef op het tabblad Algemeen een naam aan het profiel, voer de oorspronkelijke VLAN-ID (Virtual Local Area Network) in en schakel PMK-propagatie in.

PMK-propagatie inschakelen om naadloze draadloze clientroaming mogelijk te maken door PMK-informatie te delen tussen AP's binnen één site.

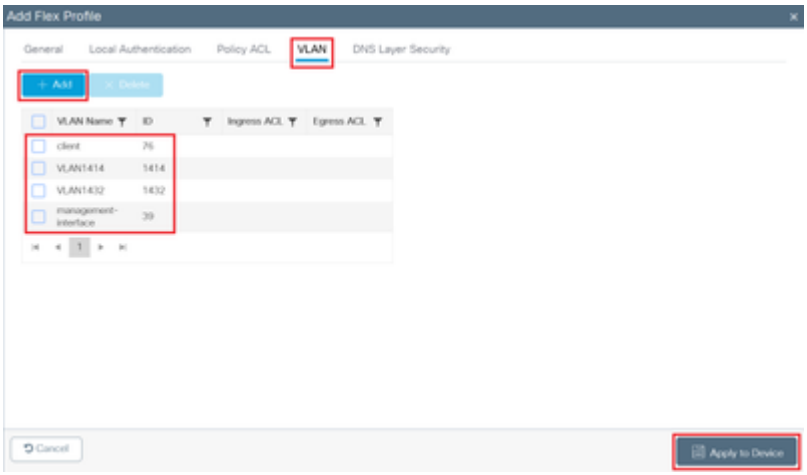


Stap 3. Voor 802.1x WLAN selecteert u op het tabblad Lokale verificatie de Radius-servergroep en schakelt u RADIUS in:



Tip: Voor een PSK WLAN hoeft u niets toe te voegen aan dit tabblad.

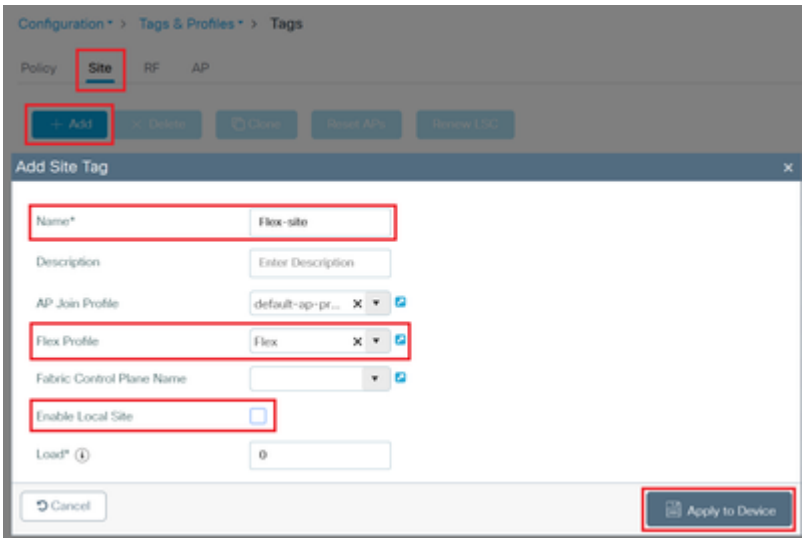
Stap 4. Op het tabblad VLAN voegt u alle VLAN's toe die door clients, AP's en RADIUS Server worden gebruikt. Zorg ervoor dat u de juiste correspondentie van elke VLAN-naam met de juiste VLAN-id maakt:



Klik aan het einde op Update & Apply to Device.

Stap 5. Navigeer naar Configuratie > Tags & Profielen > Tags > Site en selecteer +Add.

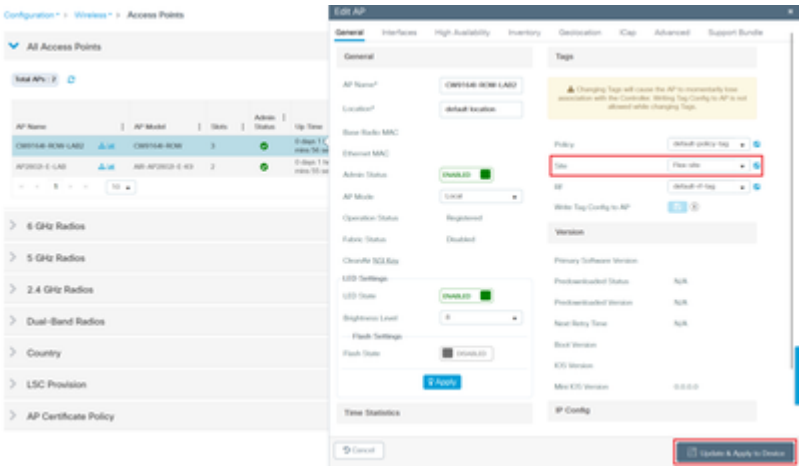
Maak de sitetag met het eerder gemaakte Flex-profiel. Geef het een naam, selecteer het juiste Flex-profiel en schakel Lokale site inschakelen uit. Zorg ervoor dat het profiel AP Join het juiste profiel heeft.



Klik op Toepassen op apparaat.

Stap 6. Navigeer naar Configuration > Wireless > Access Points.

Selecteer uw toegangspunt op Algemeen > Tags en wijzig de sitetag in de eerder geconfigureerde tag:



Klik op Bijwerken en toepassen op apparaat.

Het toegangspunt verbreekt de verbinding met de WLC en sluit zich opnieuw aan bij de Flex AP-modus.

Op dezelfde pagina kunt u, wanneer het toegangspunt opnieuw wordt aangesloten, de toegangsmodus in de kolom AP-modus controleren.

Als u het toegangspunt selecteert, wordt de nieuwe sitetag weergegeven:



CLI:

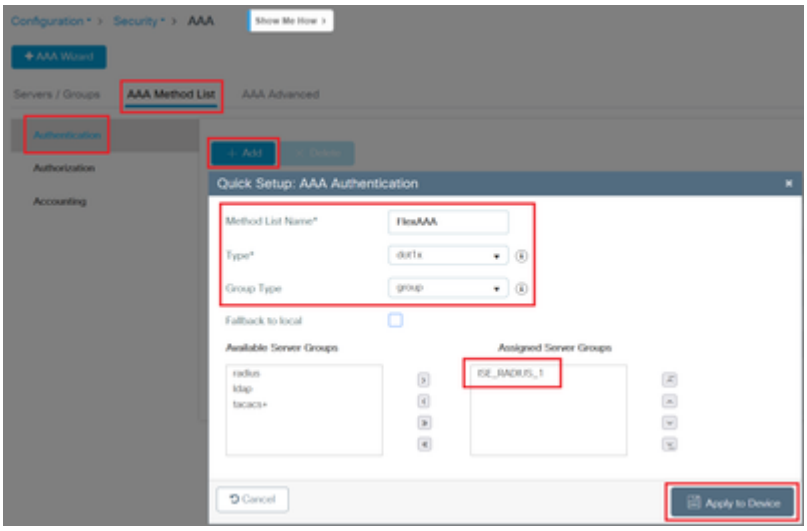
```
wireless profile flex Flex
ip http client proxy 0.0.0.0 0
local-auth radius-server-group ISE_RADIUS_1
vlan-name client
vlan-id 76
vlan-name VLAN1414
vlan-id 1414
vlan-name VLAN1432
vlan-id 1432
vlan-name management-interface
vlan-id 39
pmk propagate
!
wireless tag site Flex-site
ap-profile default-ap-profile
no local-site
flex-profile Flex
!
ap h.h.h (AP Radio MAC address)
policy-tag default-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

Configureer 802.1x WLAN met lokale verificatie met een externe RADIUS-server

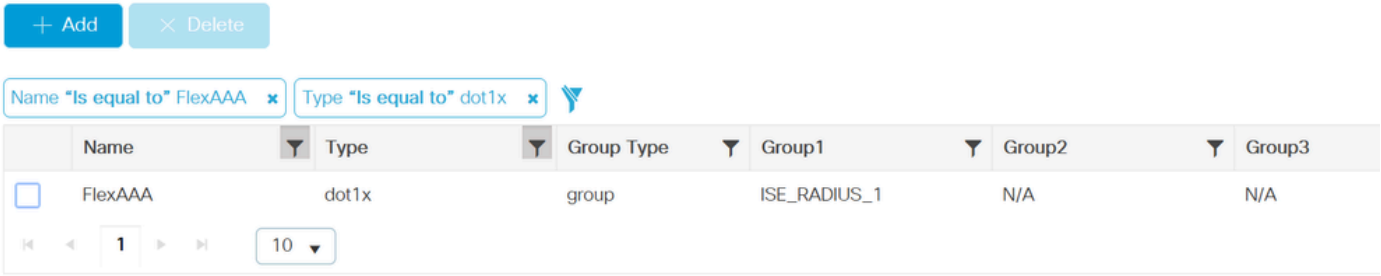
Stap 1. Maak de lijst met verificatiemethoden.

Navigeer naar Configuratie > Beveiliging > AAA, op het tabblad AAA Methodenlijst > Verificatie.

Selecteer +Toevoegen, geef een naam aan de naam van de lijst met methoden, selecteer punt1x als type, selecteer groep als groepstype en wijs de AAA-servergroep toe in de kolom Toegewezen servergroepen:



U ziet nu de gemaakte AAA-methodenlijst:



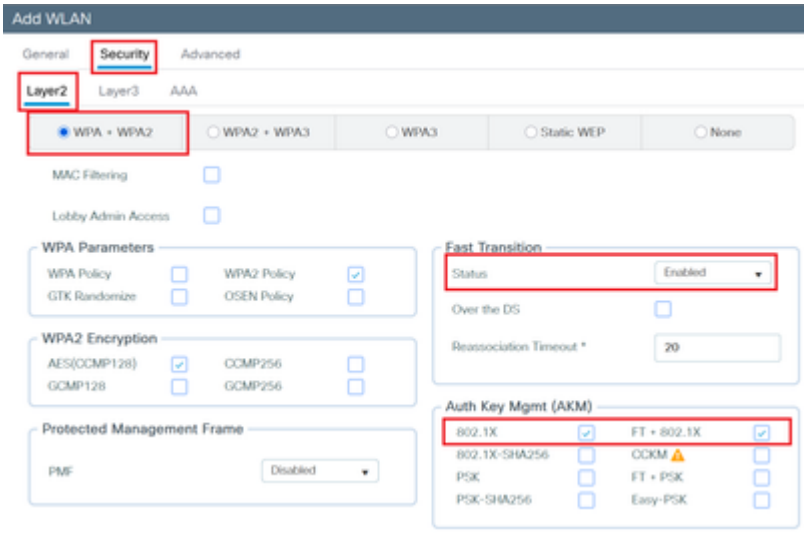
Stap 2. Maak het WLAN.

Navigeer naar Configuration > Tags & Profiles > WLAN's, selecteer +Add.

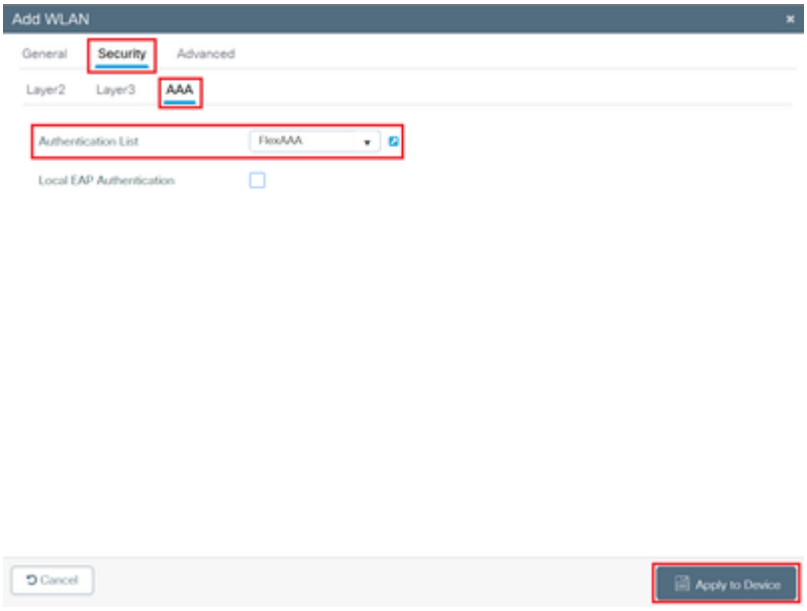
Maak op de General-tag een naam voor de profielnaam, SSID en schakel Status in:



Stap 3. Navigeer naar Beveiliging > Layer 2 tabblad, selecteer WPA+WPA2 (Wi-Fi Protected Access), Fast Transition as Enabled, Auth Key Management 802.1X en FT+802.1X:



Stap 4. Navigeer naar Beveiliging > AAA-tabblad, selecteer in het vervolgkeuzemenu Verificatielijst de lijst die eerder is gemaakt:



Klik op Bijwerken en toepassen op apparaat.

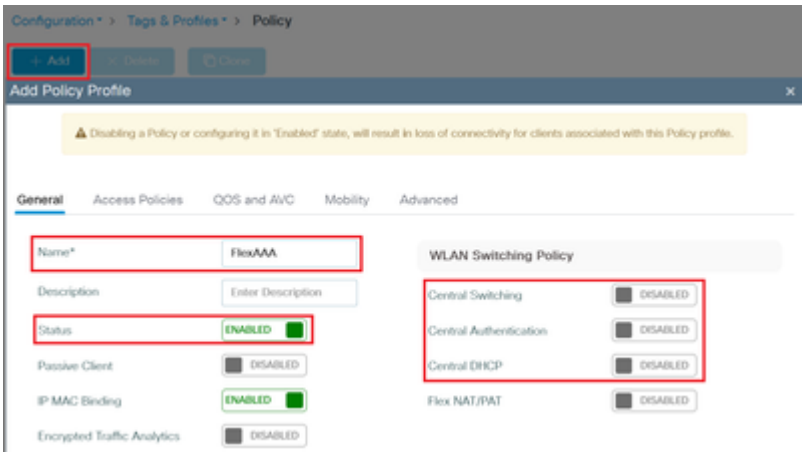
Vervolgens ziet u het aangemaakte WLAN:



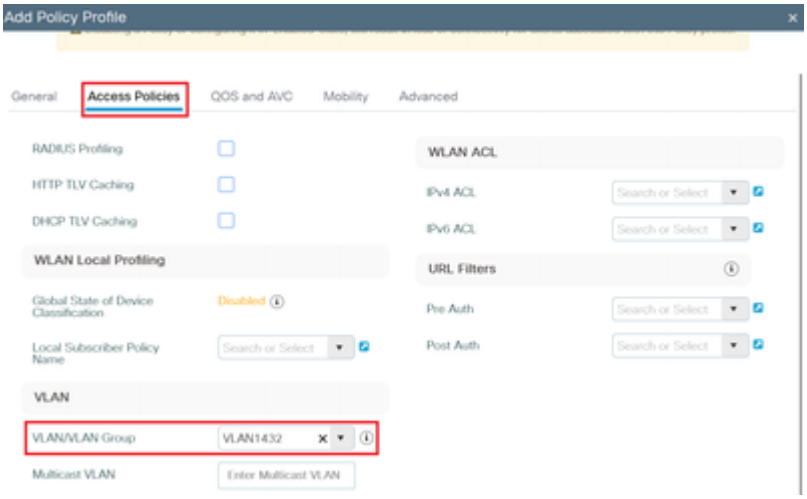
Stap 5. Maak het beleidsprofiel aan.

Navigeer naar Configuration > Tags & Profiles > Policy.

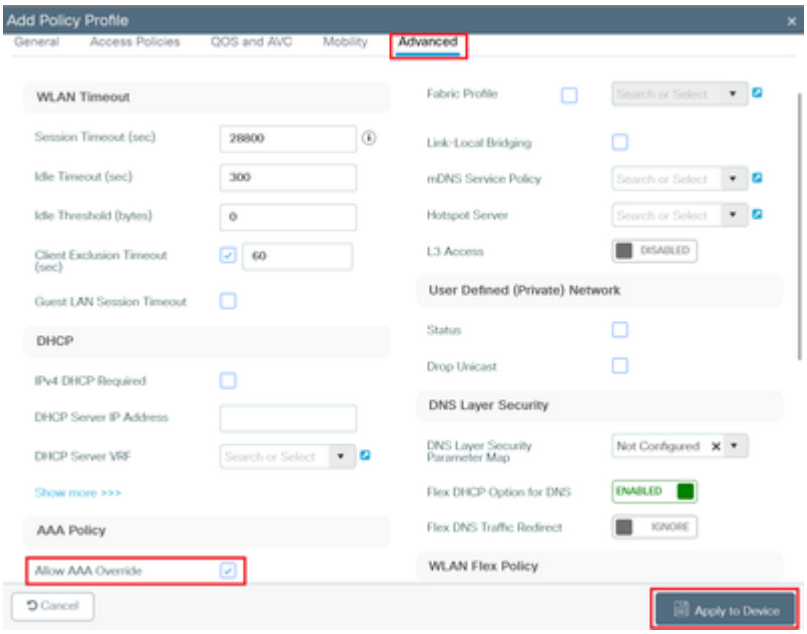
Selecteer +Toevoegen en op het tabblad Algemeen geef een naam aan het beleidsprofiel, schakel de status in en schakel centraal schakelen, centrale verificatie en centraal DHCP (Dynamic Host Configuration Protocol) uit:



Stap 6. Blader naar het tabblad Toegangsbeleid, selecteer het VLAN:

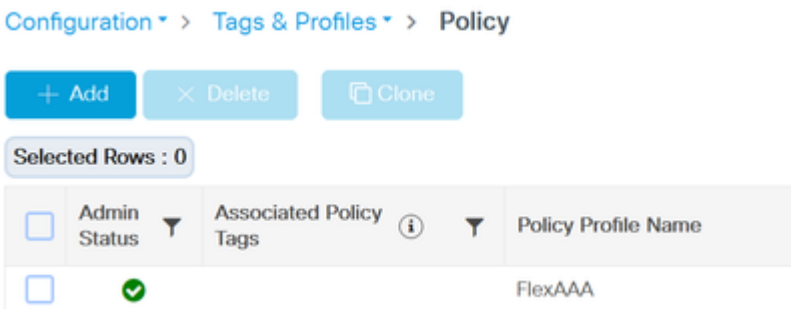


Stap 7. Navigeer naar het tabblad Geavanceerd, schakel AAA-overschrijving toestaan in.:



Klik op Bijwerken en toepassen op apparaat.

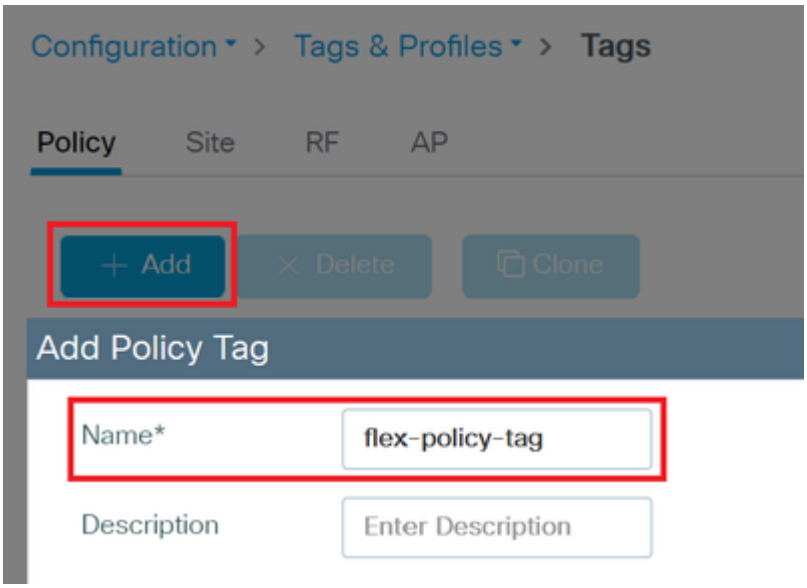
U kunt het beleidsprofiel in de lijst zien:



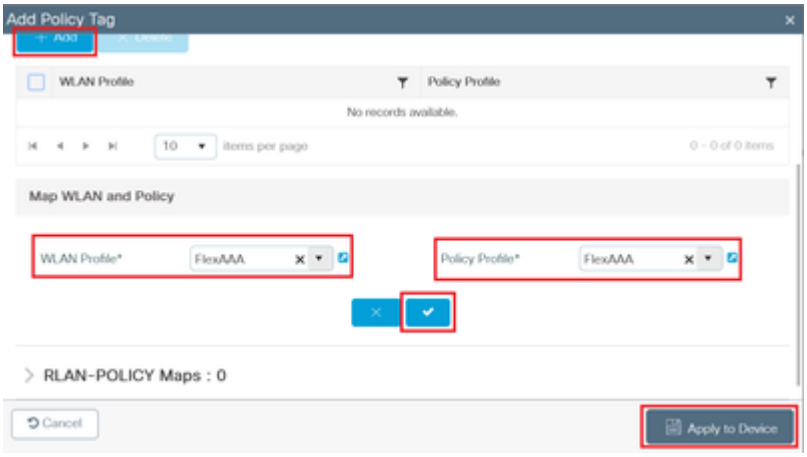
Stap 8. Beleidstag maken.

Navigeer naar Configuratie > Tags & Profielen > Tags

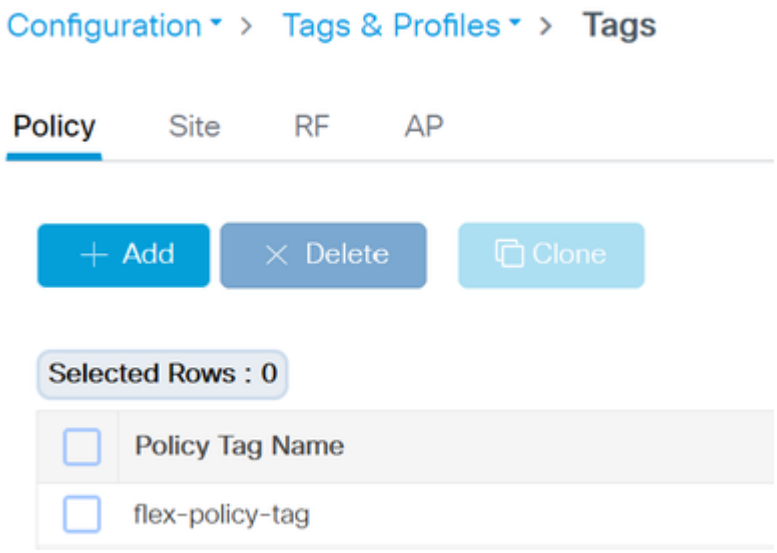
Op het tabblad Beleid selecteert u +Toevoegen. Geef een naam aan de Policy Tag:



Blader omlaag en selecteer +Toevoegen onder WLAN-BELEIDSKAARTEN. Selecteer in het WLAN-profiel de eerder gemaakte WLAN in het keuzemenu. Selecteer in Beleidsprofiel het eerder gemaakte beleidsprofiel in het vervolgkeuzemenu. Klik op de knop Controleren en vervolgens op Toepassen op apparaat:

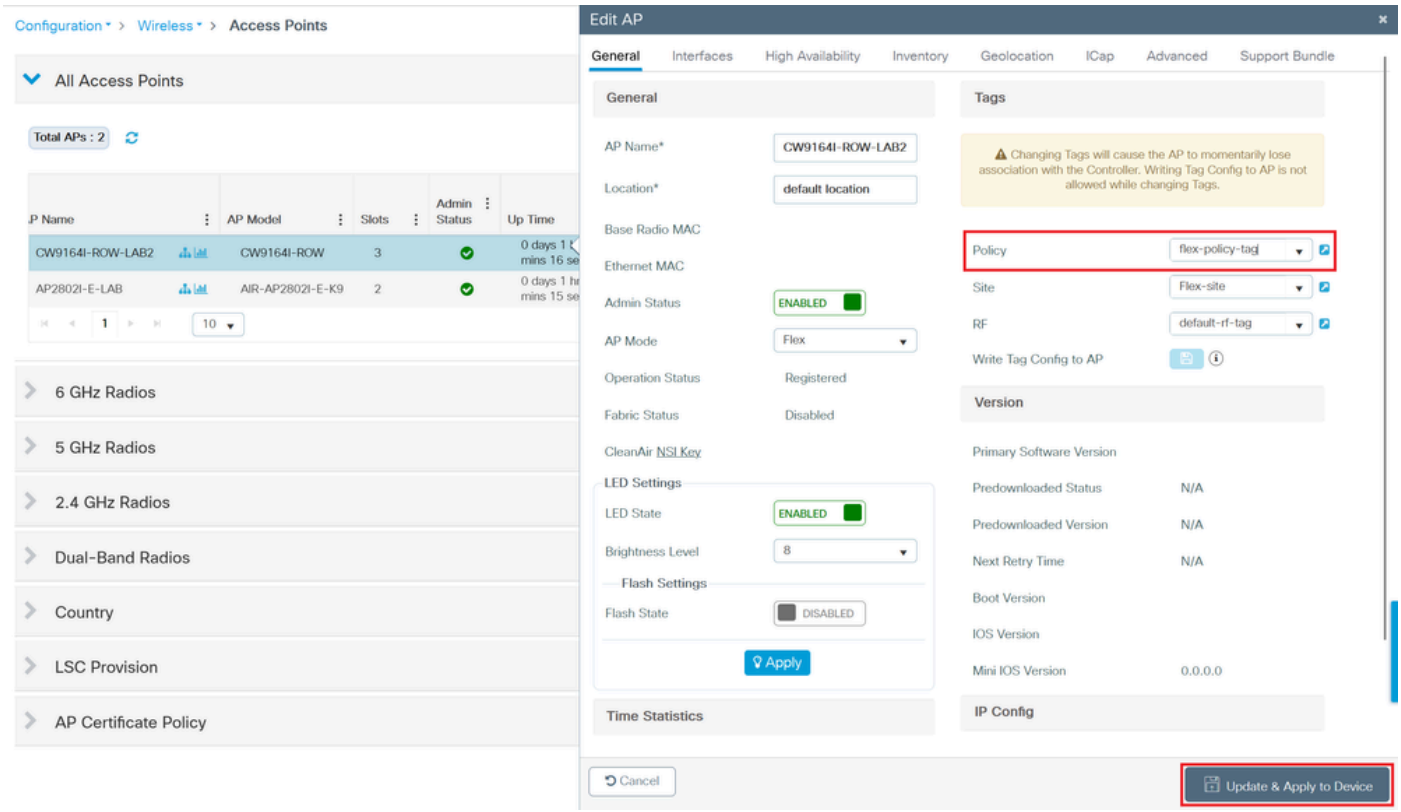


U kunt de beleidstag in de lijst zien:



Stap 9. Wijs de beleidstag toe op de tag AP's.

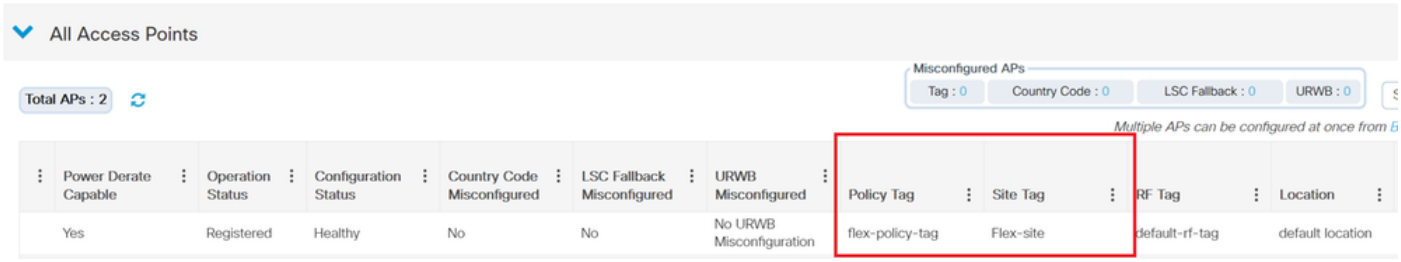
Navigeer naar Configuration > Wireless > Access Points. Selecteer het toegangspunt om de tag te wijzigen.



Klik op Bijwerken en toepassen op apparaat.

Het toegangspunt wordt losgekoppeld en voegt zich weer bij de nieuwe beleidstag.

Wanneer het toegangspunt zich weer aanmeldt, kunt u de lijst met toegangspunten controleren, bevestigen dat het toegangspunt in de Flex-modus staat en de toegewezen tags:



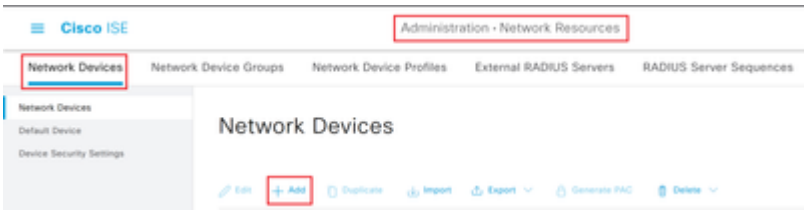
CLI:

```
aaa authentication dot1x FlexAAA group ISE_RADIUS_1
!
wlan FlexAAA 4 FlexAAA
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa akm ft dot1x
security dot1x authentication-list FlexAAA
no shutdown
!
wireless profile policy FlexAAA
aaa-override
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

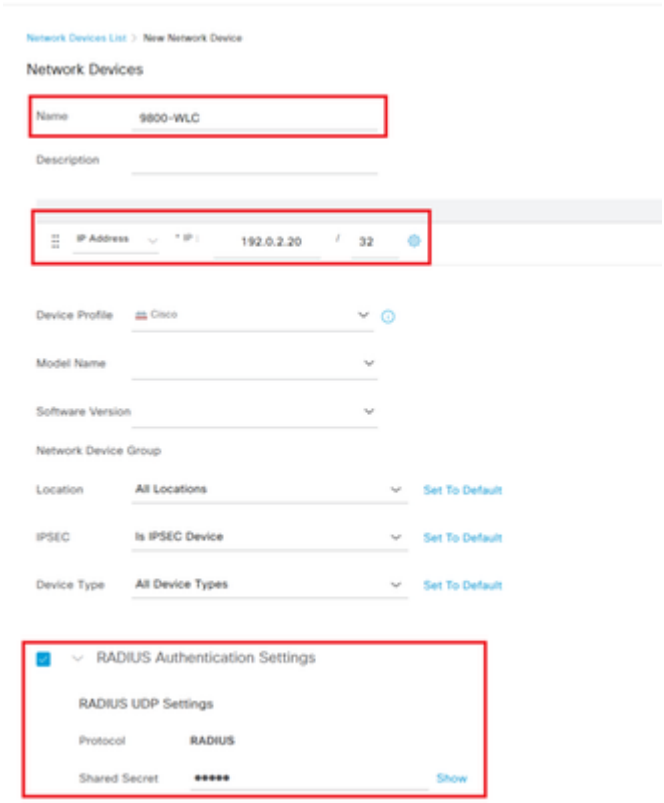
ISE configureren

Nu moet u ISE configureren om clients te kunnen verifiëren wanneer ze zich in lokale verificatie bevinden.

Stap 1. Navigeer naar Beheer > Netwerkbronnen > Netwerkapparaten. Selecteer +Toevoegen.



Stap 2. De 9800 WLC. Geef het een naam, voeg het IP-adres toe, schakel de RADIUS-verificatie-instellingen in en voeg de sleutel Gedeeld geheim toe. Deze sleutel moet dezelfde sleutel zijn die u eerder hebt geconfigureerd toen u de AAA-servers op de 9800 WLC hebt gemaakt.



Klik rechtsonder op Opslaan.

Stap 3. We moeten de toegangspunten toevoegen aan de lijst Netwerkapparaten, zodat ze kunnen fungeren als AAA-verificateurs/doorgevers wanneer de externe site de WAN-koppeling verliest (en wanneer de toegangspunten naar de stand-alone modus gaan).

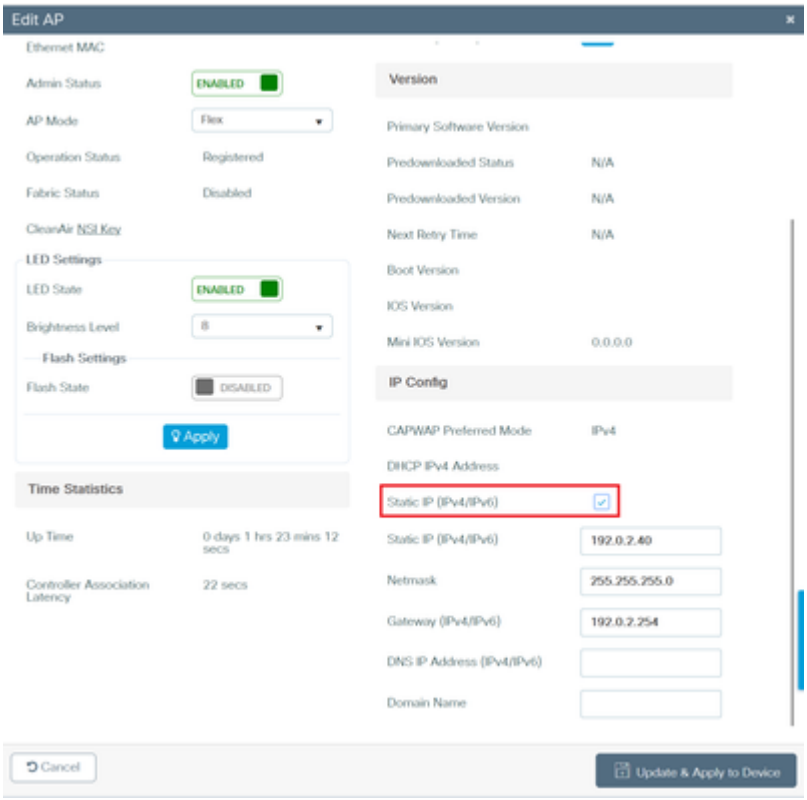
Navigeer naar Configuration > Wireless > Access Points op de 9800 WLC GUI en noteer elk IP-adres van het toegangspunt.

Opmerking: configureer het IP-adres van elk Flex AP in Static. Wanneer de toegangspunten losraken en opnieuw verbinding maken met de 9800 WLC, kunnen ze

---

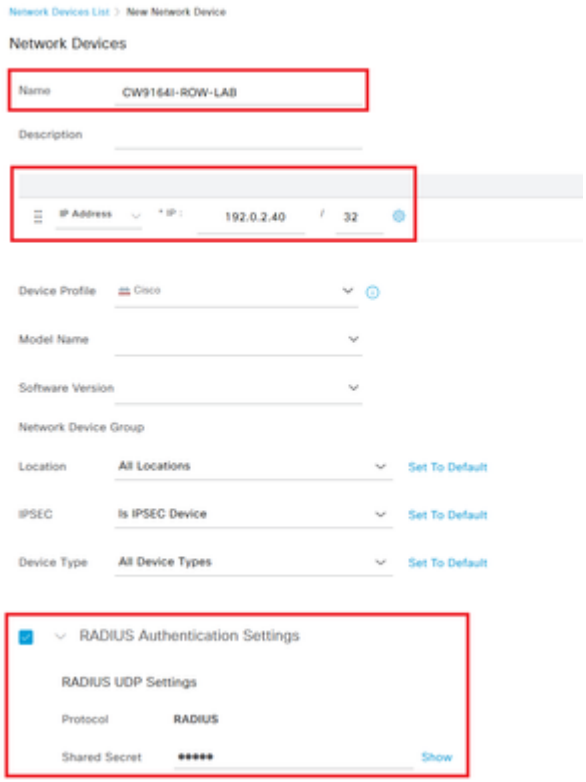
terugkomen met een ander IP-adres dan DHCP en daardoor de communicatie met ISE verliezen.

Statisch IP (IPv4/IPv6) inschakelen. Klik op Bijwerken en toepassen op apparaat:



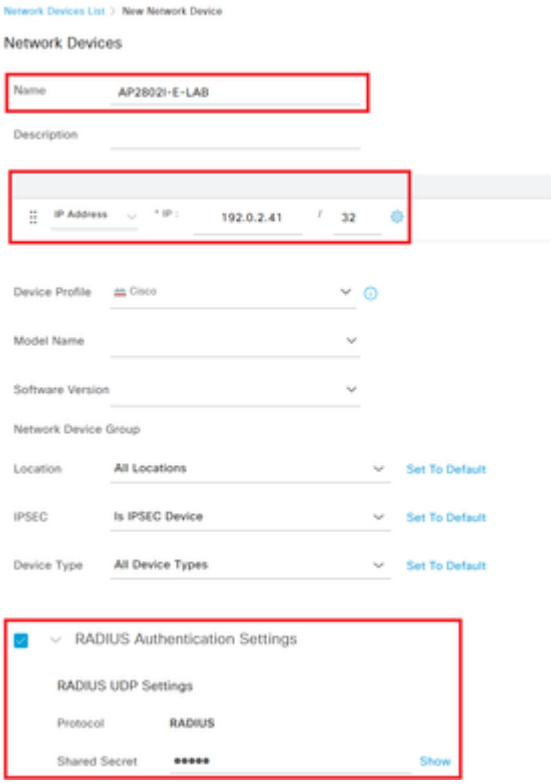
Stap 4. Ga terug op ISE naar Beheer > Netwerkbronnen > Netwerkapparaten. Selecteer +Toevoegen.

Voeg uw toegangspunten toe als netwerkapparaten, dezelfde configuratie als de 9800 WLC:



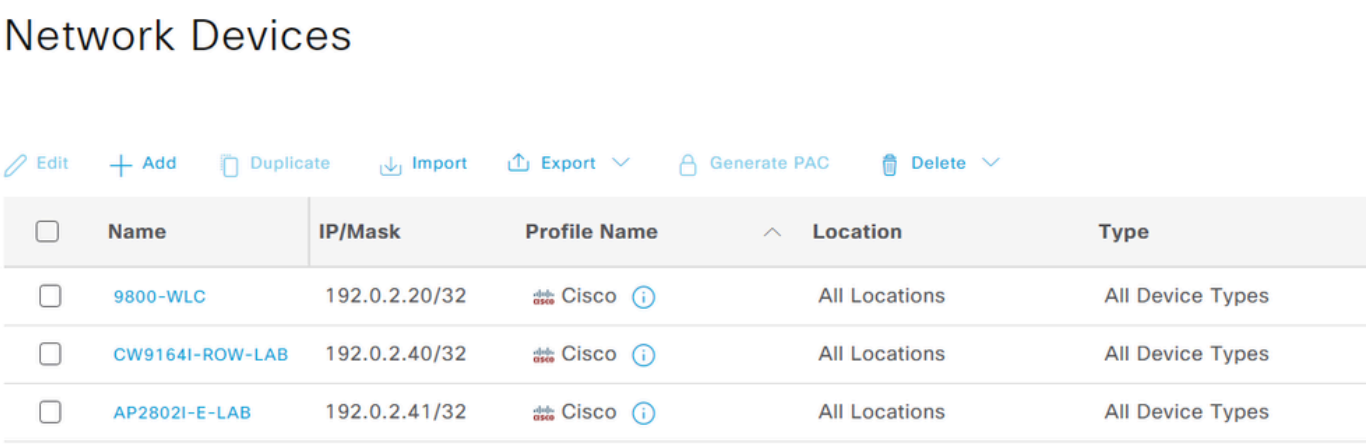
Klik rechtsonder op Opslaan.

Voor de tweede AP:



Klik rechtsonder op Opslaan.

U kunt deze lijst met netwerkapparaten bekijken:

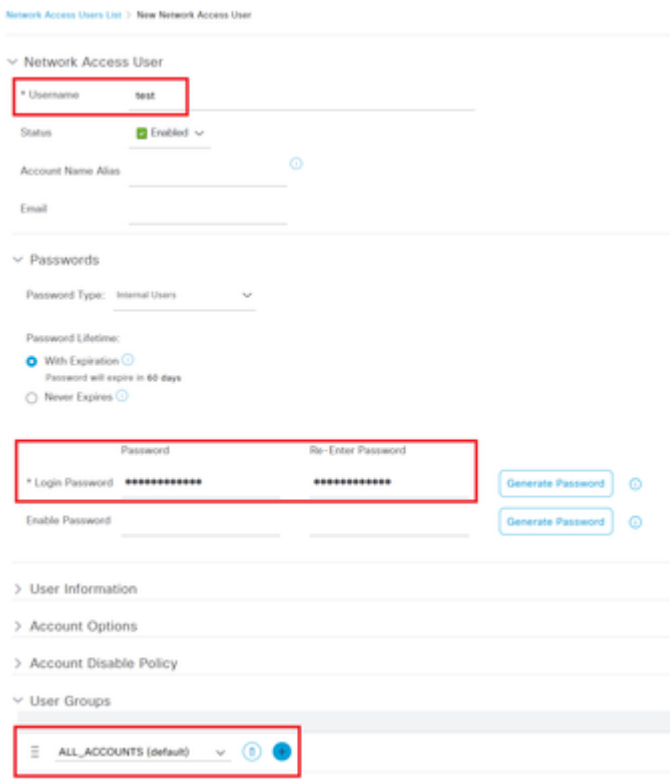


Als uw toegangspunten zich in aaneengesloten IP-bereiken bevinden, kunt u de maskerfunctie gebruiken om een enkel item te configureren dat het gedeelde geheim definieert voor een hele groep (zo niet alle) toegangspunten. Er is geen werkelijke noodzaak om één netwerkapparaat per toegangspunt in ISE te configureren. Merk echter op dat door het gebruik van jokertekens en maskers, je wat ruimte laat voor een schurkenapparaat om te proberen als expediteur naar ISE te fungeren.

Stap 5. Navigeer naar Beheer > Identiteitsbeheer > Identiteiten, op het tabblad Gebruikers, en maak een gebruiker voor 802.1x-verificatie. Selecteer +Toevoegen:

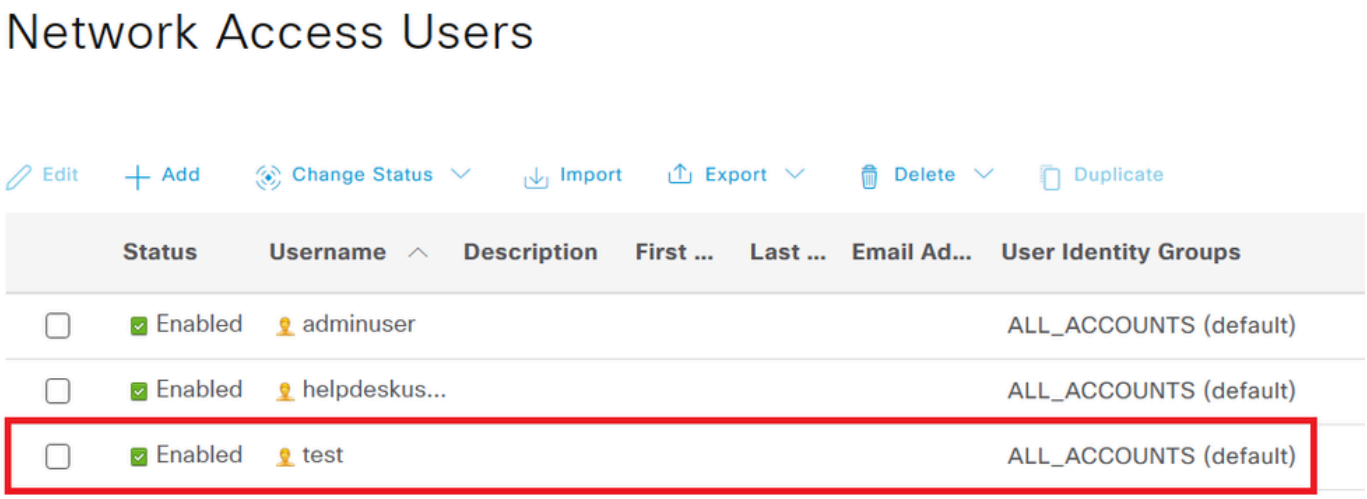


Maak een gebruikersnaam, het wachtwoord (en typ hetzelfde wachtwoord op Wachtwoord opnieuw invoeren) en selecteer ALL_ACCOUNTS (standaard) in het vervolgkeuzemenu Gebruikersgroepen:

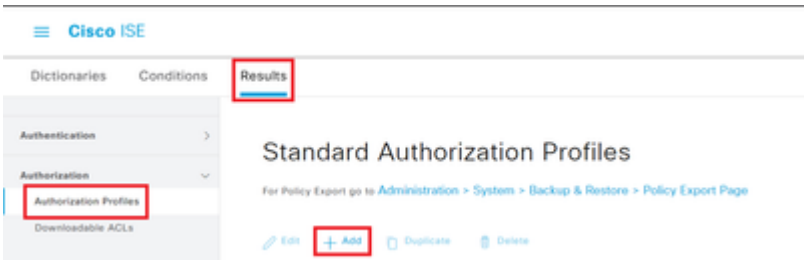


Klik rechtsonder op Verzenden.

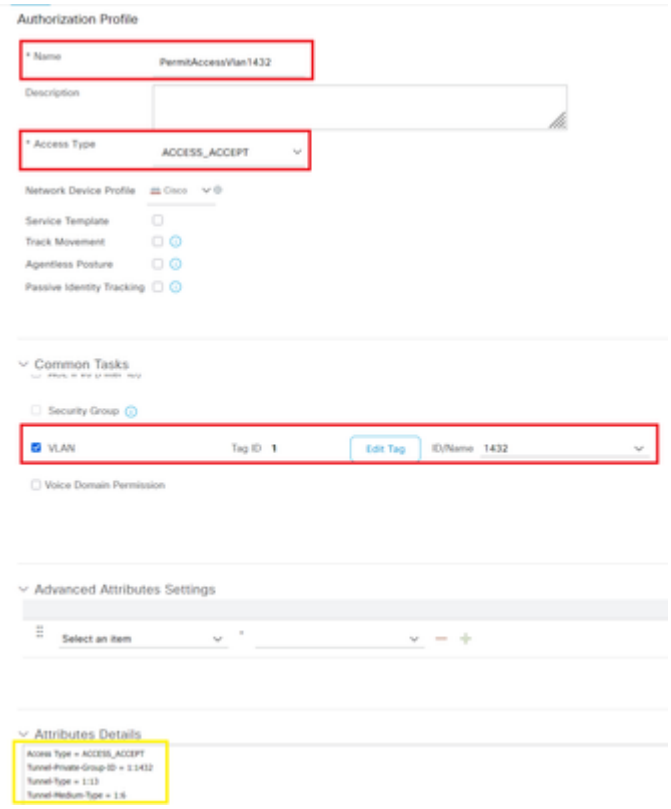
U kunt de gebruiker zien in de lijst met netwerktoegangsgebruikers:



Stap 6. Navigeer naar Beleid > Beleidselementen > Resultaten. Op het tabblad Autorisatie > Autorisatieprofielen selecteert u +Toevoegen.



Maak het machtigingsprofiel voor het VLAN dat aan de lokale verificatieclients is toegewezen:

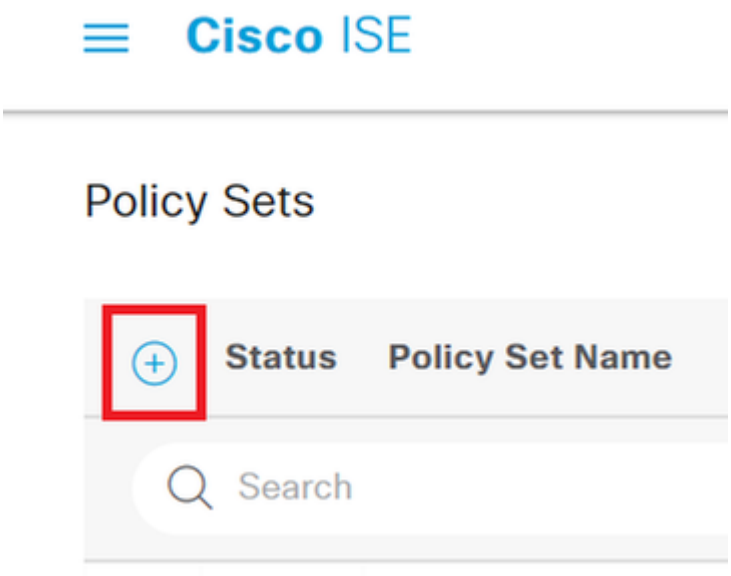


Klik rechtsonder op Verzenden.

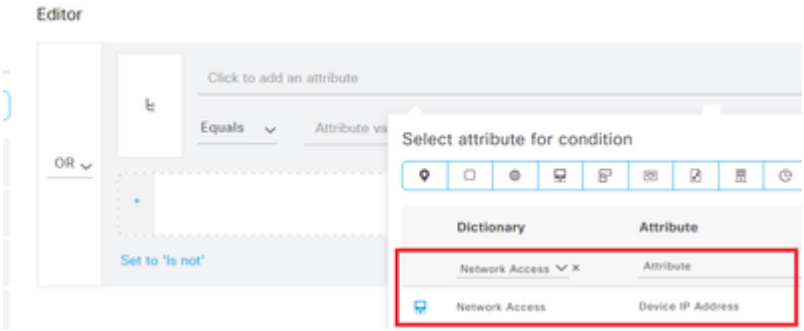
U ziet de attributen en details die ISE naar de WLC/AP's stuurt in een succesvol scenario.

Stap 7. Navigeer naar Beleid > Beleidssets. Maak een nieuwe beleidsset.

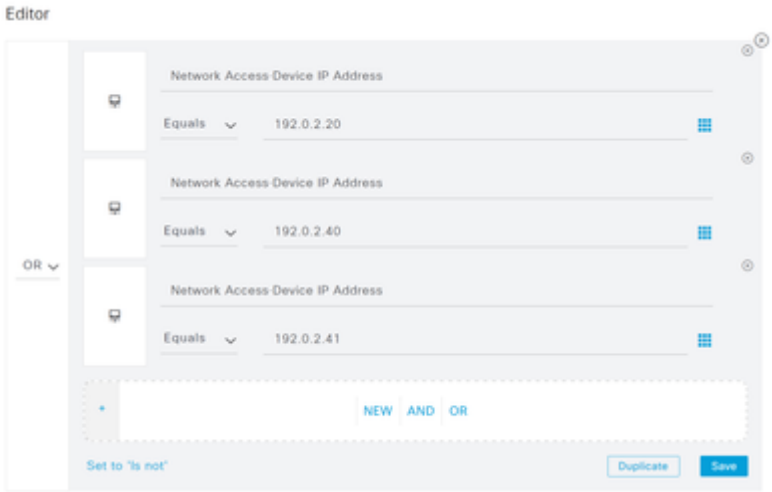
Klik op het + teken:



Geef een naam aan het beleid. In de kolom Voorwaarden voegt u de OR-regel toe en voegt u het woordenboek Netwerktoegang toe. Selecteer met het IP-adres van het attribuutapparaat de optie Gelijken:

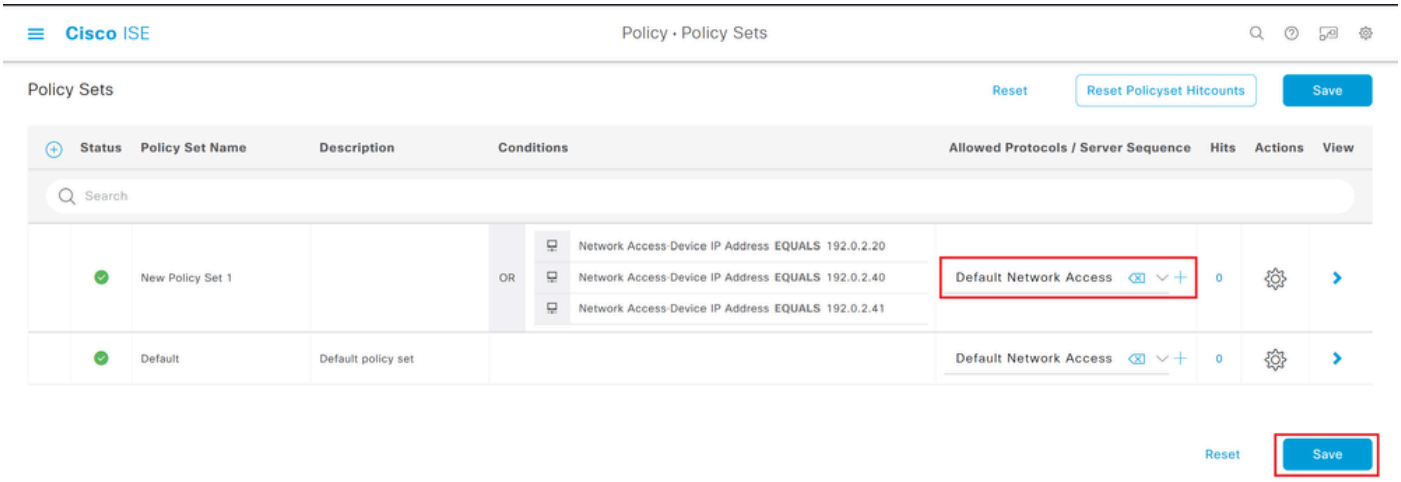


Voeg de 9800 WLC en de IP-adressen van de AP's toe:

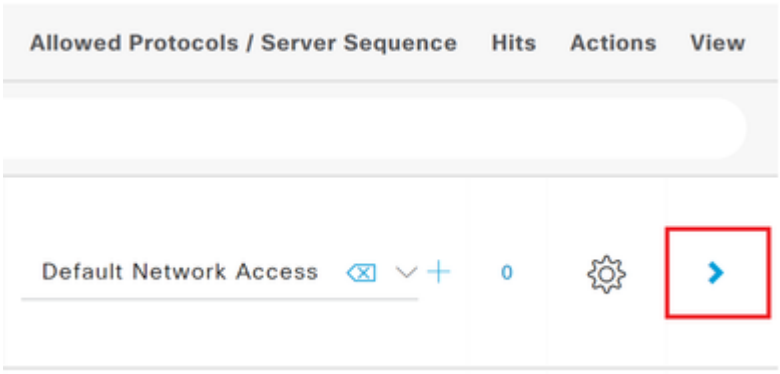


Klik rechtsonder op Gebruik.

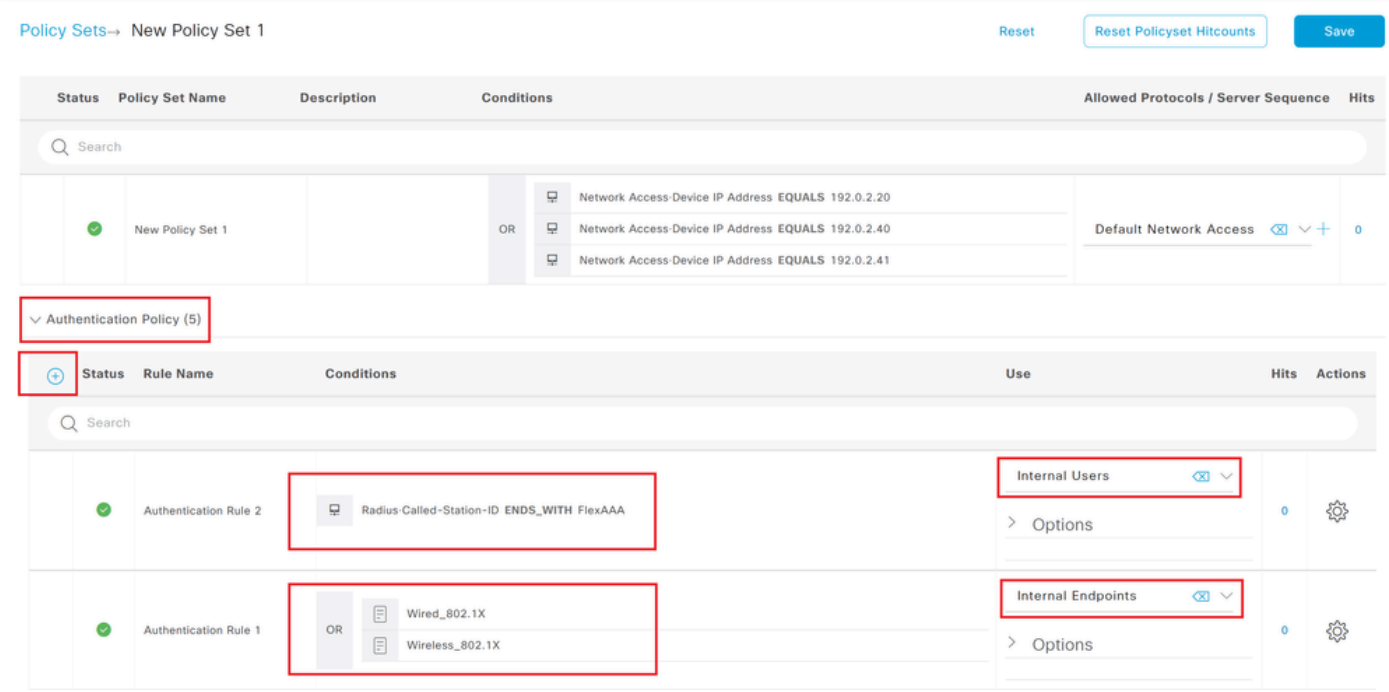
Stap 8. In de kolom Toegestane protocollen selecteert u Standaardnetwerktoegang. Klik aan het einde op Opslaan:



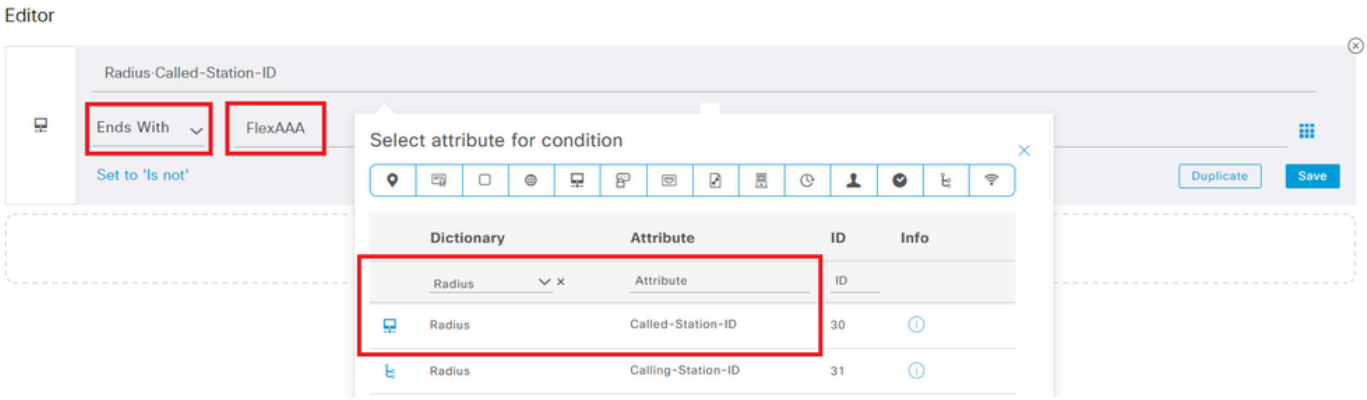
Stap 9. Klik in de kolomweergave op het pijlteken:



Stap 10. Vouw het verificatiebeleid uit, maak twee nieuwe beleidsregels: een voor de WLAN-naam en een voor de 802.1X-configuratie:

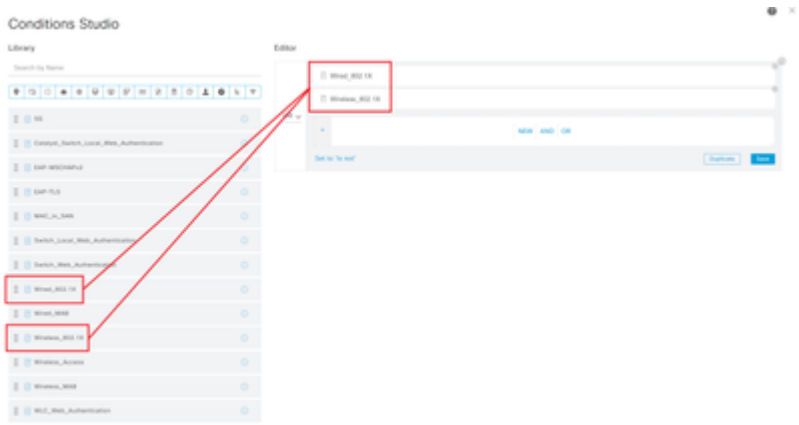


Maak voor de WLAN-naam de voorwaarde met het woordenboek Radius en Attribuut Called-Station-ID. Selecteer Beëindigt met en typ de WLAN-naam:



Klik rechtsonder op Gebruik. Selecteer Interne gebruikers in de kolom Gebruik voor dit beleid.

Stap 11. Maak voor het 802.1X-beleid de Voorwaarde met de bibliotheek Wired_802.1X en Wireless_802.1X beschikbaar op ISE. U kunt deze items slepen en neerzetten en de voorwaarde OF selecteren:



Klik rechtsonder op Gebruik. Voor dit beleid selecteert u Interne eindpunten in de kolom Gebruik.

Stap 12. Scroll naar beneden naar Autorisatiebeleid en maak een nieuw beleid. Geef het een naam en maak dezelfde voorwaarde als die voor de WLAN-naam in het verificatiebeleid.

In de kolom Profielen selecteert u in de vervolgkeuzelijst het profiel PermitAccessVlan1432:



Klik rechtsonder op Opslaan.

PSK WLAN configureren met lokale verificatie

Stap 1. Configureer eerst de toegangspunten in de Flex-modus zoals beschreven in het gedeelte FlexConnect-modus configureren op de externe site.

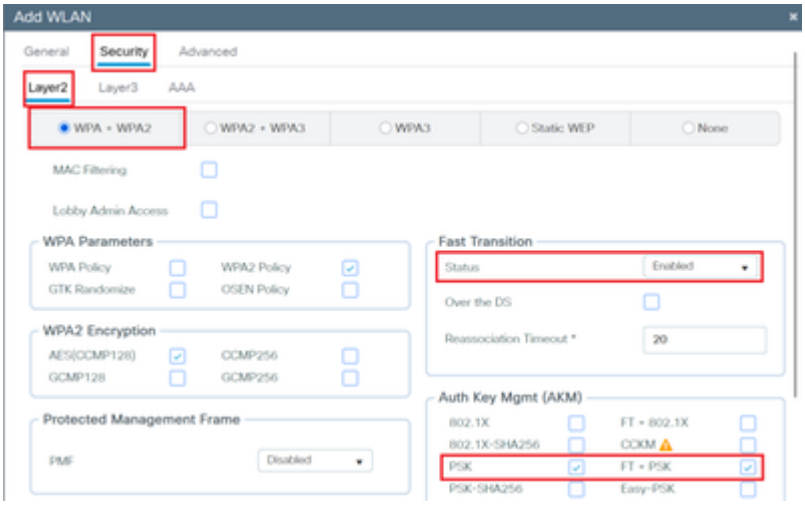
Stap 2. Maak het WLAN.

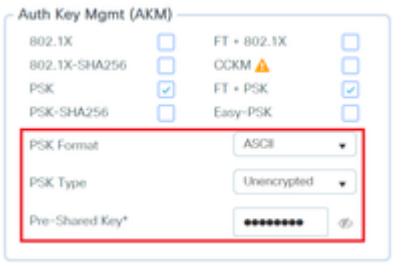
Navigeer naar Configuration > Tags & Profiles > WLAN's, selecteer +Add.

Maak op de General-tag een naam voor de profielnaam, SSID en schakel Status in:



Stap 3. Navigeer naar Beveiliging > Layer 2 tab selecteer WPA+WPA2, Snelle overgang als ingeschakeld, Auth Key Management PSK en FT+PSK, kies de PSK-indeling en het PSK-type die u wilt, en typ de vooraf gedeelde sleutel die uw clients moeten gebruiken:





Klik op Bijwerken en toepassen op apparaat.

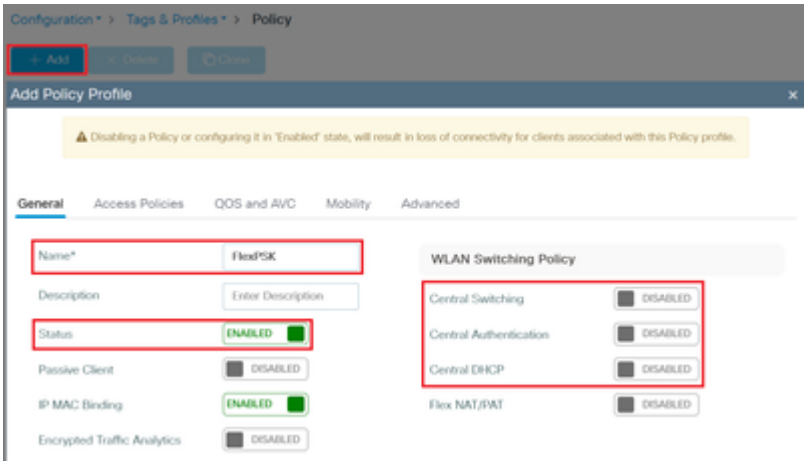
U kunt het aangemaakte WLAN zien:



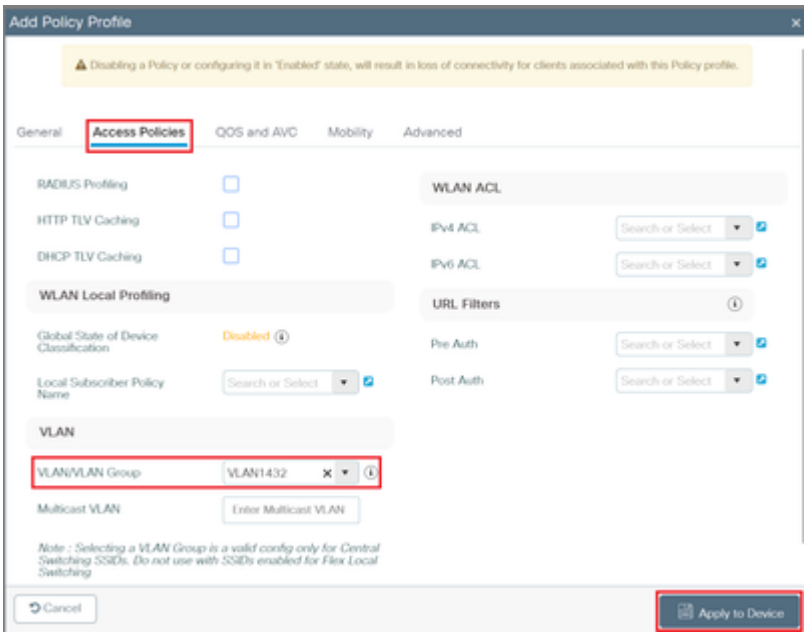
Stap 4. Maak het beleidsprofiel aan.

Navigeer naar Configuratie > Tags & Profielen > Beleid.

Selecteer +Toevoegen en op het tabblad Algemeen geef een naam aan het beleidsprofiel, schakel de status in en schakel centrale switching, centrale verificatie en centrale DHCP uit:

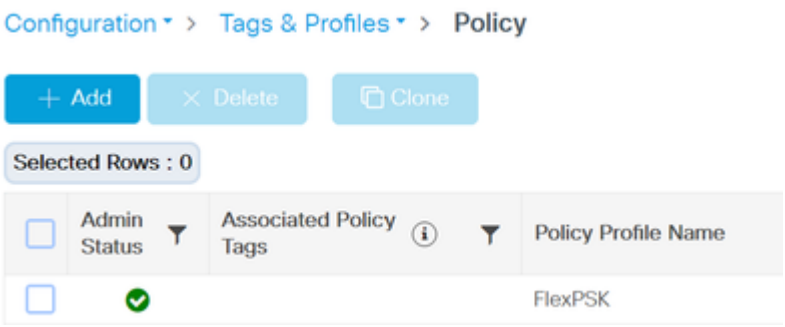


Stap 5. Blader naar het tabblad Toegangsbeleid, selecteer het VLAN:



Klik op Bijwerken en toepassen op apparaat.

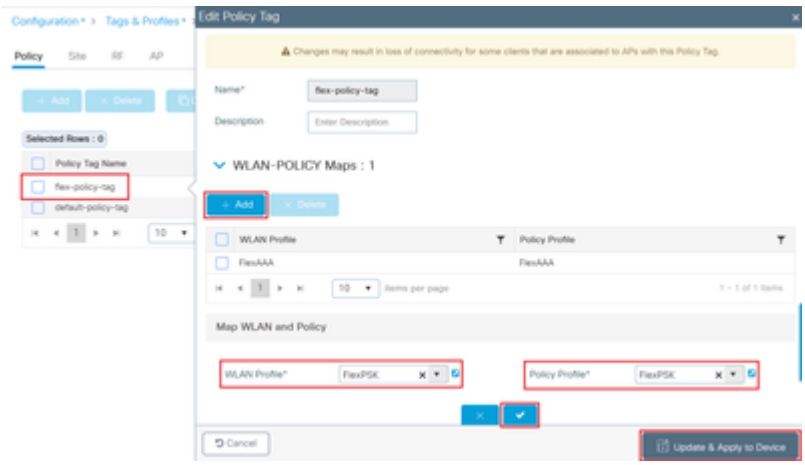
U kunt het beleidsprofiel in de lijst zien:



Stap 6. U kunt een nieuwe beleidstag maken of de bestaande tag bewerken.

Navigeer naar Configuratie > Tags & Profielen > Tags om de bestaande beleidstag te bewerken. Selecteer de tag om te bewerken.

Selecteer +Toevoegen onder WLAN-BELEIDSKAARTEN. Selecteer in het WLAN-profiel de eerder gemaakte WLAN in het keuzemenu. Selecteer in Beleidsprofiel het eerder gemaakte beleidsprofiel in het vervolgkeuzemenu. Klik op de knop Controleren en vervolgens op Toepassen op apparaat:



Als de beleidstag al op het toegangspunt is toegewezen, hoeft u niets anders te doen.

Als dat niet het geval is, wijst u de beleidstag toe op de tag AP's. Navigeer naar Configuration > Wireless > Access Points. Selecteer het toegangspunt om de beleidstag te wijzigen en klik op "Bijwerken en toepassen op apparaat".

Het toegangspunt wordt losgekoppeld en voegt zich weer bij de nieuwe beleidstag.

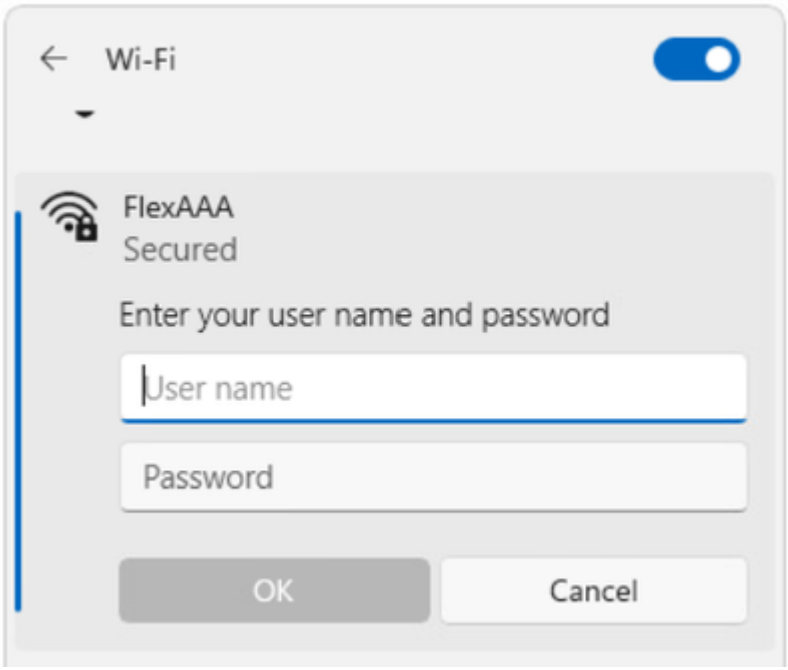
Wanneer het toegangspunt zich weer aanmeldt, kunt u de lijst met toegangspunten controleren, controleren of het toegangspunt in de Flex-modus staat en of de juiste toegewezen tags aanwezig zijn.

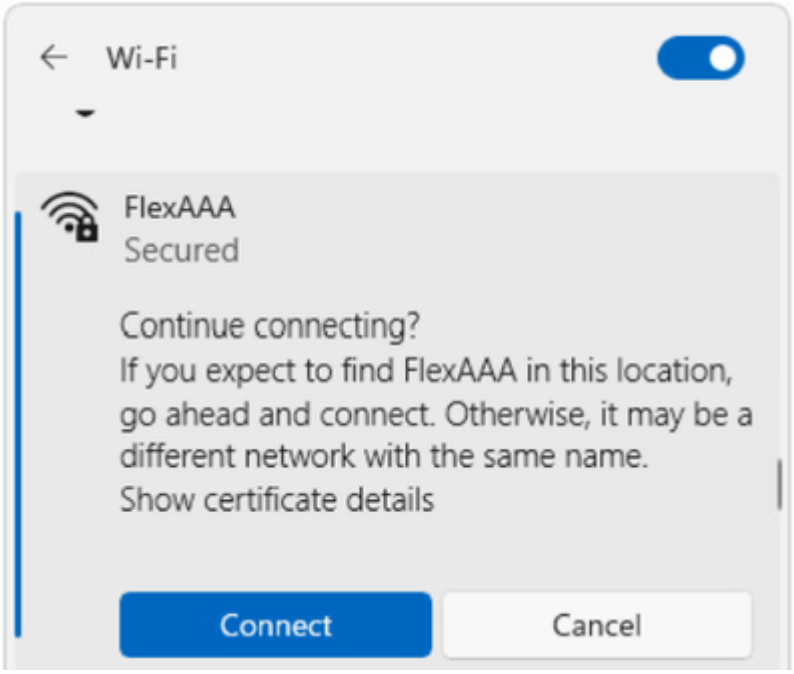
CLI:

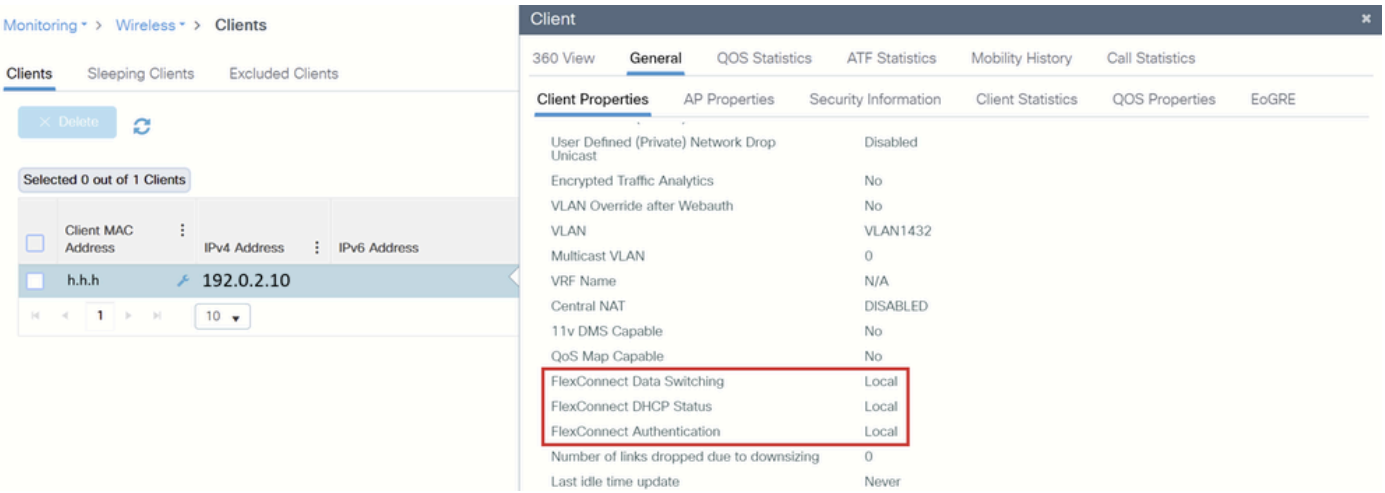
```
wlan FlexPSK 5 FlexPSK
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa psk set-key ascii 0 Password123
no security wpa akm dot1x
security wpa akm ft psk
security wpa akm psk
no shutdown
!
wireless profile policy FlexPSK
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
wlan FlexPSK policy FlexPSK
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

Verifiëren

Voor 802.1x WLAN:


Wi-Fi
FlexAAA
Secured
Enter your user name and password
User name
Password
OK
Cancel


Wi-Fi
FlexAAA
Secured
Continue connecting?
If you expect to find FlexAAA in this location, go ahead and connect. Otherwise, it may be a different network with the same name.
Show certificate details
Connect
Cancel


Monitoring > Wireless > Clients
Clients
Sleeping Clients
Excluded Clients
Delete
Selected 0 out of 1 Clients
Client MAC Address
IPv4 Address
IPv6 Address
h.h.h
192.0.2.10
1
10
Client
360 View
General
QOS Statistics
ATF Statistics
Mobility History
Call Statistics
Client Properties
AP Properties
Security Information
Client Statistics
QOS Properties
EoGRE
User Defined (Private) Network Drop Unicast
Disabled
Encrypted Traffic Analytics
No
VLAN Override after Webauth
No
VLAN
VLAN1432
Multicast VLAN
0
VRF Name
N/A
Central NAT
DISABLED
11v DMS Capable
No
QoS Map Capable
No
FlexConnect Data Switching
Local
FlexConnect DHCP Status
Local
FlexConnect Authentication
Local
Number of links dropped due to downsizing
0
Last idle time update
Never

CLI:

```
C9800-1#show wireless client mac-address      h.h.h        detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :192.0.2.10
Client IPv6 Addresses :
Client Username : test
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexAAA
Flex Profile : Flex
Wireless LAN Id: 4
WLAN Profile Name: FlexAAA
Wireless LAN Network Name (SSID): FlexAAA
BSSID :
Connected For : 134 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

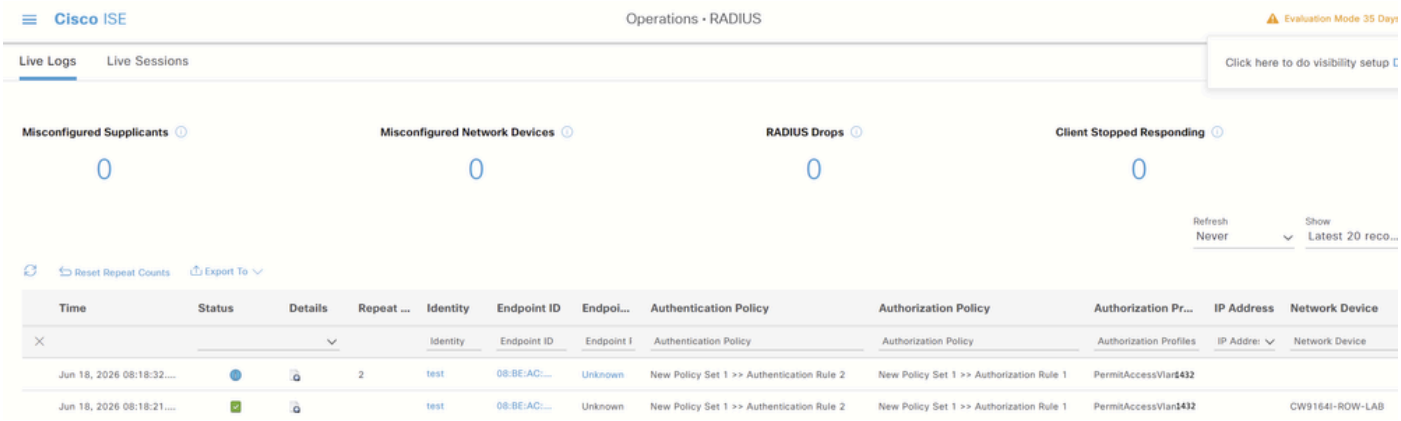
```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

Over de AP CLI:

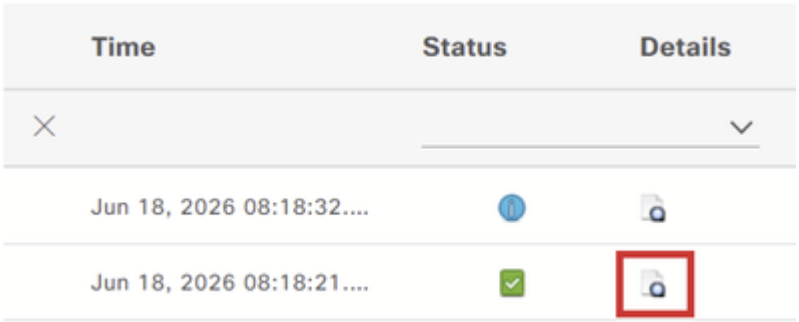
```
CW9164I-ROW-LAB#show dot11 clients

Total dot11 clients: 1
      Client MAC   Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH          1       1  33   FlexAAA  -45 MCS9ISS           No         No
```

Op ISE



IP Address	Network Device	Device Port	Identity Group	Posture ...	Server
IP Addre:	Network Device	Device Port	Identity Group	Posture Sta	Server
		Radio:1Wlan:1			ISE1
	CW9164I-ROW-LAB	Radio:1Wlan:1	User Identity Groups:ALL_ACCOUNTS (default),Unknown		ISE1



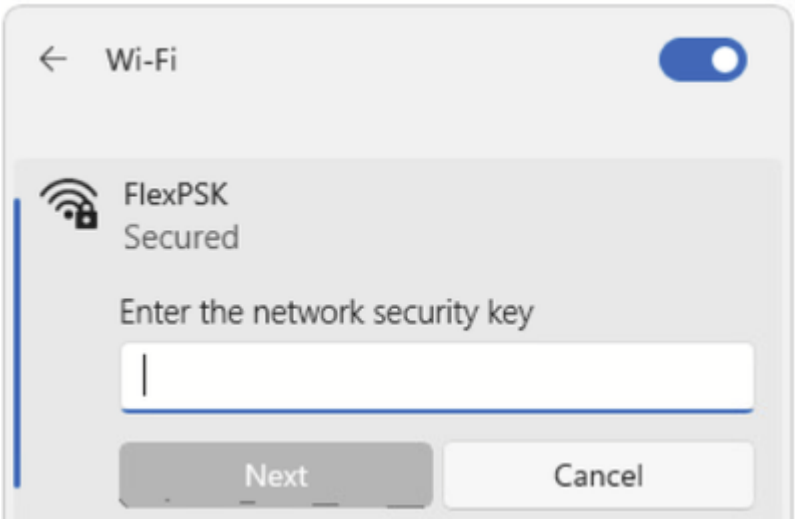
Cisco ISE

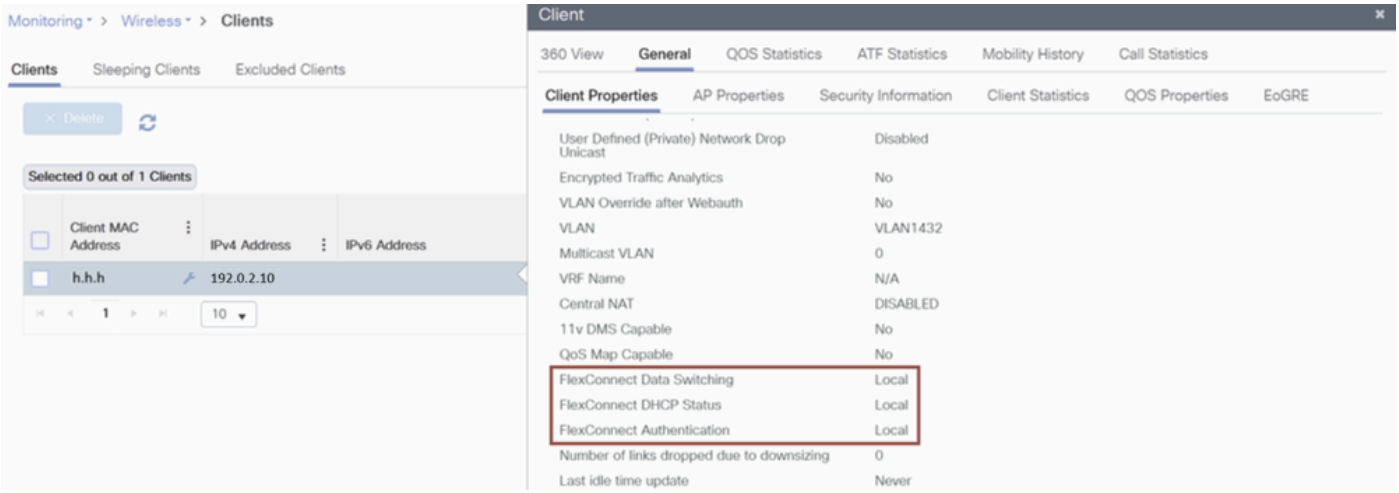
Overview

Event	5200 Authentication succeeded
Username	test
Endpoint Id	HH:HH:HH:HH:HH:HH
Endpoint Profile	Unknown
Authentication Policy	New Policy Set 1 >> Authentication Rule 2
Authorization Policy	New Policy Set 1 >> Authorization Rule 1
Authorization Result	PermitAccessVlan1432

Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:ALL_ACCOUNTS (default),Unknown
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	CW9164I-ROW-LAB
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.0.2.40
NAS Port Id	Radio:1Wlan:1
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccessVlan1432
Response Time	64 milliseconds

Voor PSK WLAN:





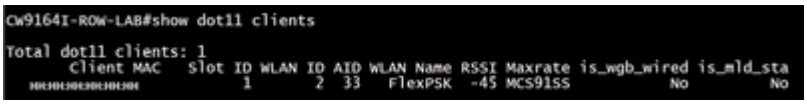
CLI:

```
C9800-1#show wireless client mac-address h.h.h detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 192.0.2.10
Client IPv6 Addresses :
Client Username: N/A
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexPSK
Flex Profile : Flex
Wireless LAN Id: 5
WLAN Profile Name: FlexPSK
Wireless LAN Network Name (SSID): FlexPSK
BSSID :
Connected For : 116 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

Over AP CLI:



Problemen oplossen

Schakel AP-foutopsporing en RA-tracering in met het client-mac-adres, gesynchroniseerd.

Schakel op het toegangspunt de volgende foutopsporing in:

Foutopsporingsgebeurtenis FlexConnect
Foutopsporing FlexConnect PMK
Foutopsporing FlexConnect Dot11R
Beheergegevens debug Dot11-client
Foutopsporing Dot11 Client Management Critical
Fouten in het beheer van Dot11-client debuggen
Gebeurtenissen voor debugbeheer van Dot11-client

Voor 802.1x WLAN:

AP-foutopsporingslogboeken met succesvolle verificatie:

Het toegangspunt regelt het 802.11-statussysteem en het beheer van de lokale sleutel.
Het toegangspunt verwerkt de koppeling en bereidt de client voor op verificatie.

```
[*06/19/2026 06:49:00.1836] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*06/19/2026 06:49:00.1890] wcp/flex_roam_st :: Flexconnect 11r enabled for client HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1908] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*06/19/2026 06:49:00.1909] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1931] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
```

Het toegangspunt verwerkt de autorisatie, past de VLAN-overschrijving toe en verplaatst de client naar de FWD-status (Forwarding).

```
[*06/19/2026 06:49:20.3601] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*06/19/2026 06:49:20.3601] CLSM[HH:HH:HH:HH:HH:HH]: WCP_EVENT_CLIENT_AUTHORIZE : Plumbing key info to
[*06/19/2026 06:49:20.3612] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
```

```
[*06/19/2026 06:49:20.3625] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*06/19/2026 06:49:20.3627] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Retrieved key for FT+FT_DOT1X algono: 8, vlanId: 1
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Local auth (Add) on radio 1 Vap 0 reported to WLC
[*06/19/2026 06:49:20.3701] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*06/19/2026 06:49:20.4313] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr1v0
[*06/19/2026 06:49:20.4317] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 1 Vap 0 IP 192.0.2.10 updatere
[*06/19/2026 06:49:20.4318] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

RA trace logs voor dezelfde succesvolle authenticatie:

De RA registreert de orkestratie van de sessie door de WLC. De WLC valideert de identiteit en het beleid van de klant.
WLC erkent de FlexConnect-associatie.

```
2026/06/19 06:49:20.934325580 {wncd_x_R0-1}{1}: [client-orch-sm] [18318]: (note): MAC: hhhh.hhhh.hhhh H
2026/06/19 06:49:20.936543415 {wncd_x_R0-1}{1}: [dot1x] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040000
2026/06/19 06:49:20.936579730 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936600851 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936654791 {wncd_x_R0-1}{1}: [ewlc-infra-evq] [18318]: (note): Authentication Succes
2026/06/19 06:49:20.936769433 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

WLC duwt het beleid naar de AP.

```
2026/06/19 06:49:20.937447786 {wncd_x_R0-1}{1}: [svm] [18318]: (info): [hhhh.hhhh.hhhh] Applied User Pr
2026/06/19 06:49:20.937451734 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: c
2026/06/19 06:49:20.937452534 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937455590 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: v
2026/06/19 06:49:20.937456177 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: m
2026/06/19 06:49:20.937458436 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: u
2026/06/19 06:49:20.937462127 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile:tu
2026/06/19 06:49:20.937462755 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937463426 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937464035 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
```

Autorisatie geslaagd.

```
2026/06/19 06:49:20.937594042 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.937597878 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

Clientparameters.
2026/06/19 06:49:20.939394217 {wncd_x_R0-1}{1}: [dot11] [18318]: (noot): MAC:

hhhhh.hhhh.hhhh Invoerparameters voor clientgegevenspaden - ssid:FlexAAA, slot_id:1 bssid ifid: 0x0, radio_ifid: 0x9040008, wlan_ifid: 0XF0400004

WLC leert het IP via lokale DHCP/ARP.
2026/06/19 06:49:21.001000218 {wncd_x_R0-1}{1}: [client-iplearn] [18318]: (noot): MAC: hhhhhh.hhhh.hhhh Client IP learn successful. Methode: IP-snooping IP: 192.0.2.10

De klant is volledig verbonden.
2026/06/19 06:49:21.002363496 {wncd_x_R0-1}{1}: [errmsg] [18318]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/1: wncd: gebruikersnaam (test) toegevoegd aan SSID (FlexAAA) voor apparaat met MAC: hhhhhh.hhhhh.hhhhh op kanaal (48)
2026/06/19 06:49:21.002795009 {wncd_x_R0-1}{1}: [client-orch-state] [18318]: (noot): MAC: hhhhhh.hhhh.hhhh Overgang van clienttoestand: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN

Standalone scenario

Gedrag tijdens het verlies van AP-WLC-connectiviteit en het daaropvolgende herstel.

De AP is aangesloten bij de WLC. De client voert een succesvolle 802.1X-verificatie uit en het toegangspunt schakelt de client over naar de FWD-status (Forwarding).

Op ISE RADIUS Live Logs zien we de clientsessie.

```
[*07/06/2026 20:26:05.8590] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 0 Vap 0 IP 192.0.2.10 updatere
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```

Het toegangspunt slaagt er niet in de WLC te bereiken, gebruikt het aantal hertransmissies en schakelt de switches naar de stand-alone modus uit. Bestaande clients blijven lokaal verbonden.

```
[*07/06/2026 20:28:47.0840] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=33, NumofPendingMsgs=4
[*07/06/2026 20:28:50.0860] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=34, NumofPendingMsgs=5
```

```
[*07/06/2026 20:28:53.0870] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:56.0990] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:59.1000] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:29:02.1010] Max retransmission count exceeded, going back to DISCOVER mode.
[*07/06/2026 20:29:02.1020] Flexconnect Switching to Standalone Mode!
[*07/06/2026 20:29:02.2170] CAPWAP State: DTLS Teardown
```

Maar de klant is nog steeds verbonden:

CW9164I-ROW-LAB2#Dot11-clients weergeven

Totaal aantal dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Naam RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 Nee Nee

Wanneer de client in de stand-alone modus naar een ander toegangspunt zwerft, mislukt de EAP-handshake omdat de RADIUS-server niet kan worden bereikt. De client wordt gedeautoriseerd en verwijderd uit het toegangspunt.

```
[*07/06/2026 20:34:44.7240] CLSM[HH:HH:HH:HH:HH:HH]: Session timeout
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-RETRANSMIT hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-TIMEOUT-FAILURE hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: Received UNAUTHORIZE for hh:hh:hh:h
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: recv'd UNAUTH with DISCONNECT REQUE
[*07/06/2026 20:36:15.2680] CLSM[HH:HH:HH:HH:HH:HH]: Client delete initiated with timeout of 10 seconds
[*07/06/2026 20:36:15.2770] CLSM[HH:HH:HH:HH:HH:HH]: Remove success from ClientIPTable on apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Not sending DELETE to cont, reason CLIENT_DEL_EAP_
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Deauthorize succeeded to radio intf apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: client moved from FWD to DELETE_PENDING
[*07/06/2026 20:36:15.2880] CLSM[HH:HH:HH:HH:HH:HH]: Send Deauth with reason 2 force 1 - Radio 0 Vap 0
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete timeout
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete client reassoc 0 succeeded to radio intf ap
```

AP verzendt de clientsessie naar de RADIUS-back-upserver.

Het toegangspunt herwint de connectiviteit met de WLC. Het toegangspunt switch terug naar de Verbonden modus en synchroniseert de lokale clientsessiegegevens met de WLC.

De clientsessie gaat over tussen de primaire en back-up ISE-nodes op basis van de verbindingsstatus van het toegangspunt.

Het toegangspunt en de client worden weergegeven als verbonden op de WLC en de client heeft geen verbroken verbindingen of flap opgemerkt wanneer de verbinding tussen het toegangspunt

en de WLC uitviel.

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 0


Upon roaming back, the client undergoes local authentication. The AP processes the association and move

[*07/06/2026 20:48:49.2830] CLSM[HH:HH:HH:HH:HH:HH]: US Auth(b0) seq 2653 IF 23 slot 0 vap 0 len 30 sta
[*07/06/2026 20:48:49.2840] CLSM[HH:HH:HH:HH:HH:HH]: DS Auth len 30 slot 0 vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*07/06/2026 20:48:49.2920] CLSM[HH:HH:HH:HH:HH:HH]: US Reassoc Req(20) seq 2654 IF 23 slot 0 vap 0 len
[*07/06/2026 20:48:49.2930] CLSM[HH:HH:HH:HH:HH:HH]: AUTH TYPE RSNIE DOT1X
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: Populate client capability: cap_from_click=true, ma
[*07/06/2026 20:48:49.2940] Flexconnect local_auth 1 local_assoc 1 frame subtype 32
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio id: 0, vap id: 0, max clients for this wlan:
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio state: 1, client state: 1, max_client_per_ra
[*07/06/2026 20:48:49.2940] Adding RM Capable IE - Len = 5, RRM[0] = 73, RRM[1] = c0
[*07/06/2026 20:48:49.2940] DS [re]Assoc 1 req_len=201 resp_len=146 11r_len=0 cckm 0 qos_flag 1 status
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: DS Reassoc Resp(30) IF 0 slot 0 vap 0 state AUTH,
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*07/06/2026 20:48:49.2950] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-na
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client_
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Driver Add Client success AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Added to ClientIPTable on apr0v0
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: Added to WCP client table AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2980] wcp/flex_roam_st :: Flexconnect hapdev: client WCP_EVENT_CLIENT_ASSOC/REASSO
[*07/06/2026 20:48:49.6360] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*07/06/2026 20:48:49.6360] wcp/flex_roam_st :: Flexconnect (AUTHORIZE) received PTK thru wcp_event
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect HH:HH:HH:HH:HH:HH client ACL , Qos Profile:
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-na
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client_
[*07/06/2026 20:48:49.6370] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: check vlan override vlan 1432
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: Client ADD Encrypt Key success AID 1 Radio 0 Enc 4
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*07/06/2026 20:48:49.6390] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*07/06/2026 20:48:49.6900] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:48:49.6910] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD


CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -39 M7 No No

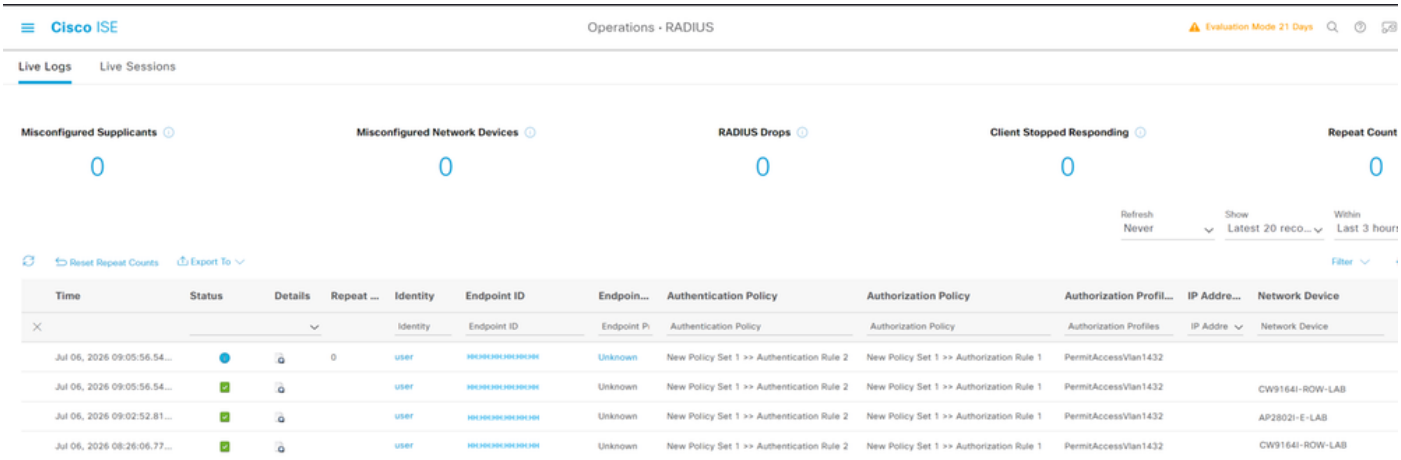



*07/06/2026 20:59:57.7690] Discovery Response from 192.0.2.20
[*07/06/2026 21:00:08.0080] CAPWAP State: DTLS Setup
```

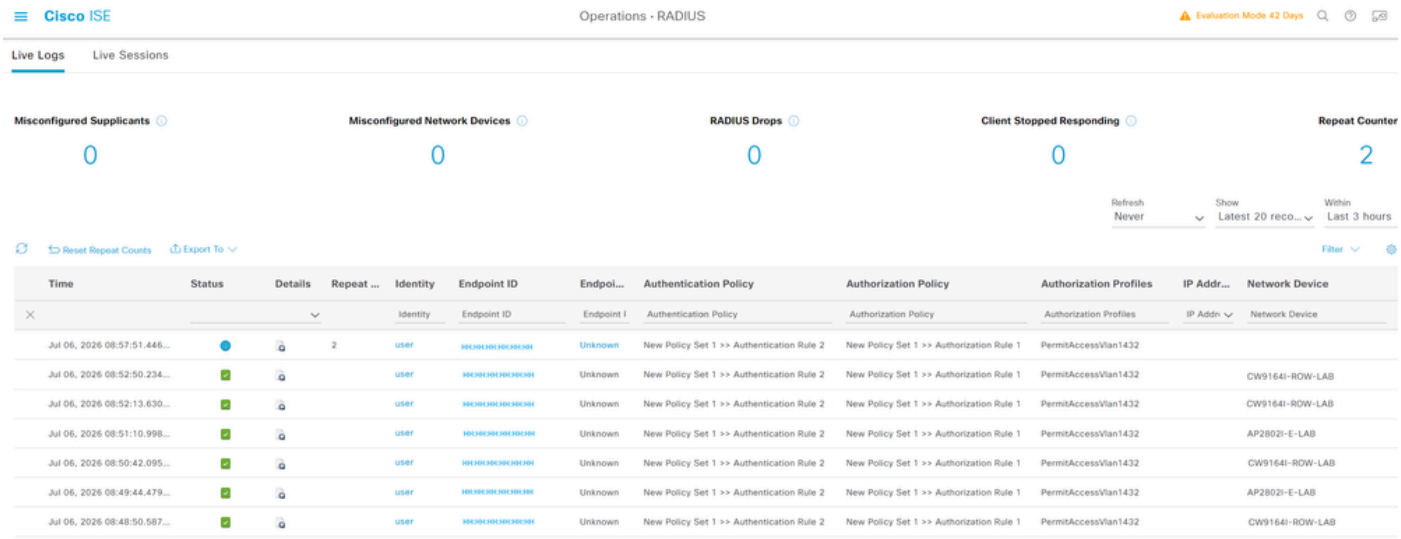
```
[*07/06/2026 21:00:08.4820] CAPWAP State: Join
[*07/06/2026 21:00:09.3740] Sending Join request to 192.0.2.20 through port 5253, packet size 1376
[*07/06/2026 21:00:09.3780] Join Response from 192.0.2.20, packet size 1397
[*07/06/2026 21:00:09.4040] CAPWAP State: Image Data
[*07/06/2026 21:00:09.5020] CAPWAP State: Configure
[*07/06/2026 21:00:12.5510] CAPWAP State: Run
[*07/06/2026 21:00:12.6480] AP has joined controller C9800-1
[*07/06/2026 21:00:12.6490] Flexconnect Switching to Connected Mode!
[*07/06/2026 21:00:12.6520] CLSM[HH:HH:HH:HH:HH:HH]: AP_REAP_CLIENT_INFO_PAYLOAD Client MAC HH:HH:HH:HH
[*07/06/2026 21:00:12.6520] AssocTimeAtAP 1783371169 clientBitmap=0x13
[*07/06/2026 21:00:12.6520] CLSM[00:00:00:00:00:00]: Numbers of Local Switching clients to report : 1
[*07/06/2026 21:00:14.8270] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8270] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
[*07/06/2026 21:00:14.8280] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8280] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
```

```
CW9164I-ROW-LAB2# show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```



Primaire ISE: registreert de eerste sessie (08:26:06) en de hervatte sessie na WLC-connectiviteitsherstel (09:02:52).



Back-up ISE: hiermee wordt de sessieactiviteit vastgelegd (08:48:50 - 08:57:51) terwijl het toegangspunt in de stand-alone modus actief was.

De eerste sessie was om 08:26:06, daarna verloor het toegangspunt de connectiviteit met de WLC en verhuisde het naar de Standalone-modus.

De sessie 09:02:52 is de eerste sessie nadat AP de verbinding met de WLC heeft hersteld.

Gerelateerde informatie

- CCNP Enterprise Wireless Design ENWLSD 300-425 en implementatie ENWLSI 300-430 Officiële CERT Guide, 2e editie
- Cisco Catalyst 9800-reeks Configuratiehandleiding voor draadloze controllersoftware, Cisco IOS XE 17.8.x - Hoofdstuk: FlexConnect
- Release Notes voor Cisco Catalyst 9800-serie draadloze controller, Cisco IOS XE Cupertino Release 17.8.x
- Feature Matrix voor Cisco Wireless Access Points
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.