&Configuratie van de 9800 WLC-integratie met Aruba ClearPass - Dot1x FlexConnect voor implementatie van vestigingen

Inhoud

Inleiding

Dit document beschrijft de integratie van de Catalyst 9800 draadloze controller met Aruba ClearPass Policy Manager (CPPM) en Microsoft Active Directory (AD) om dot1x-verificatie te leveren aan draadloze clients in een Flexconnect-implementatie.

Voorwaarden

Vereisten

Cisco raadt aan dat u kennis hebt van deze onderwerpen en dat deze zijn geconfigureerd en geverifieerd:

- Catalyst 9800 draadloze controller
- Aruba ClearPass Server (vereist platformlicentie, toegangslicentie, on-board licentie)
- Operationele Windows AD
- Optionele certificeringsinstantie (CA)
- Operationele DHCP-server
- Operationele DNS-server (vereist voor certificaat-CRL-validatie)
- ESX.i
- Alle relevante componenten worden gesynchroniseerd met NTP en geverifieerd om de juiste tijd te hebben (vereist voor certificaatvalidatie)
- Kennis van onderwerpen: C9800 implementatie- en nieuwe Config-modelFlexConnect-handeling op C980 Dot1x-verificatie

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

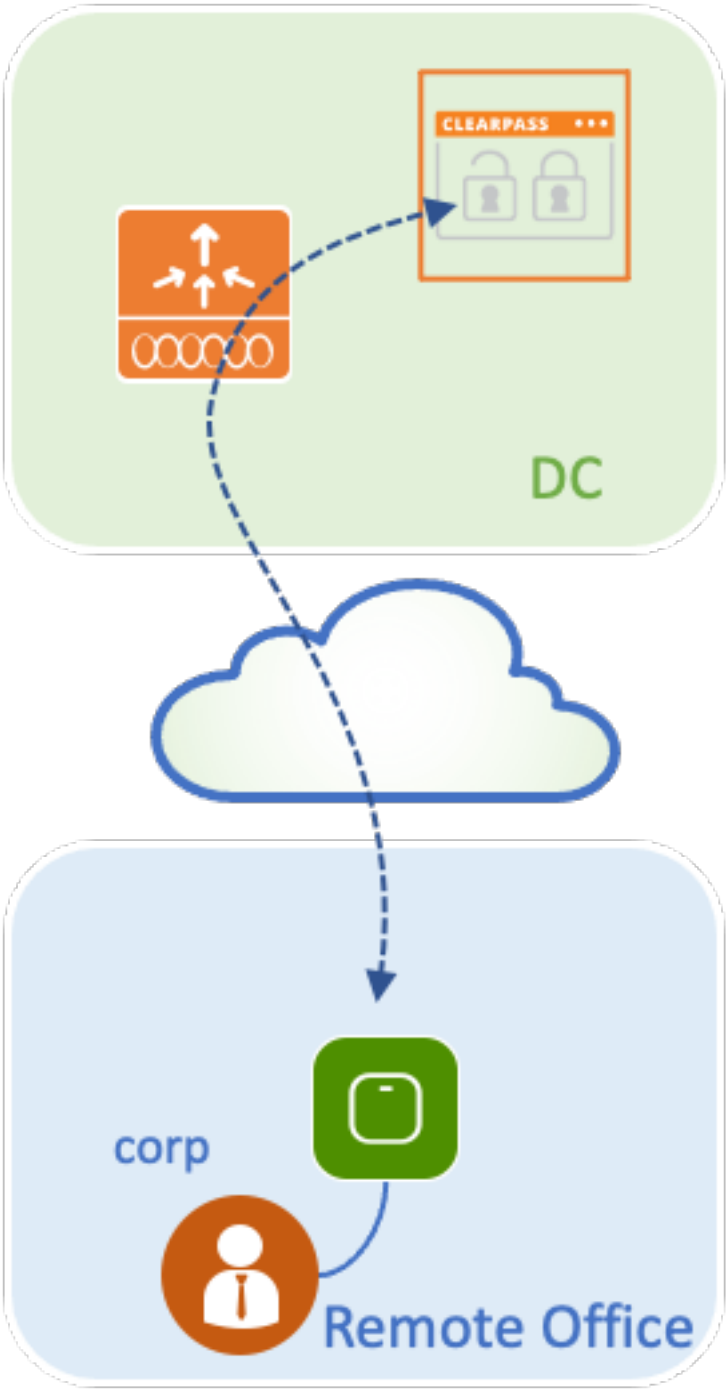
- C980-L-C Cisco IOS-XE 17.3.3
- C9130AXE, 4800 access points
- Aruba ClearPass, 6-8-0-109592 en 6.8-3 patch
- MS Windows-server Active Directory (GP geconfigureerd voor geautomatiseerde op machine gebaseerde afgifte van cert naar beheerde endpoints)DHCP-server met optie 43 en optie 60DNS-serverNTP-server om alle componenten te synchroniserenCA

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.

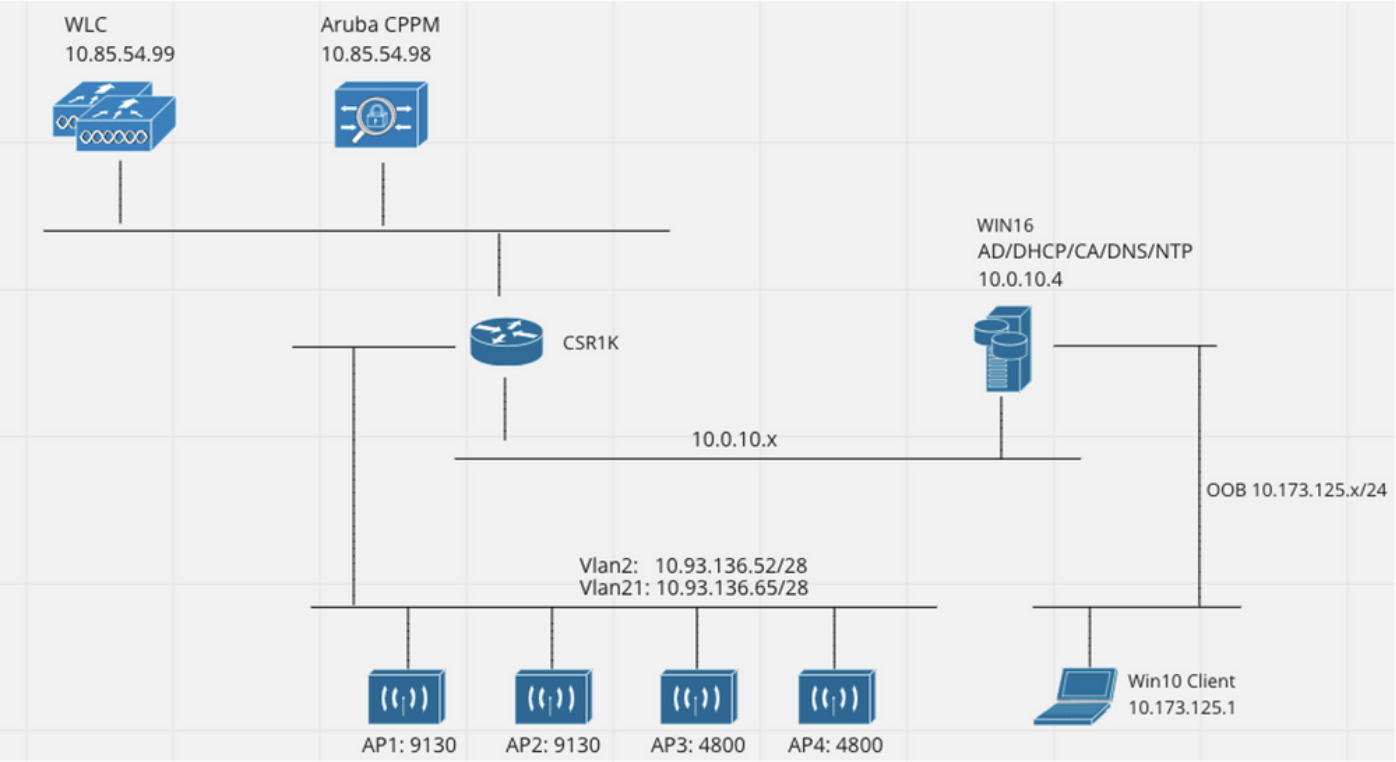
Achtergrondinformatie

Traffic Flow

In een typische bedrijfsplaatsing met meerdere bijkantoren, wordt elk bijkantoor opgericht om dot1x toegang tot de collectieve werknemers te verlenen. In dit configuratievoorbeeld wordt PEAP gebruikt om zakelijke gebruikers via een ClearPass-instantie in het centrale datacenter (DC) dot1x-toegang te bieden. Machinecertificaten worden gebruikt in combinatie met een onderzoek van de werknemersreferenties ten aanzien van een Microsoft AD server.

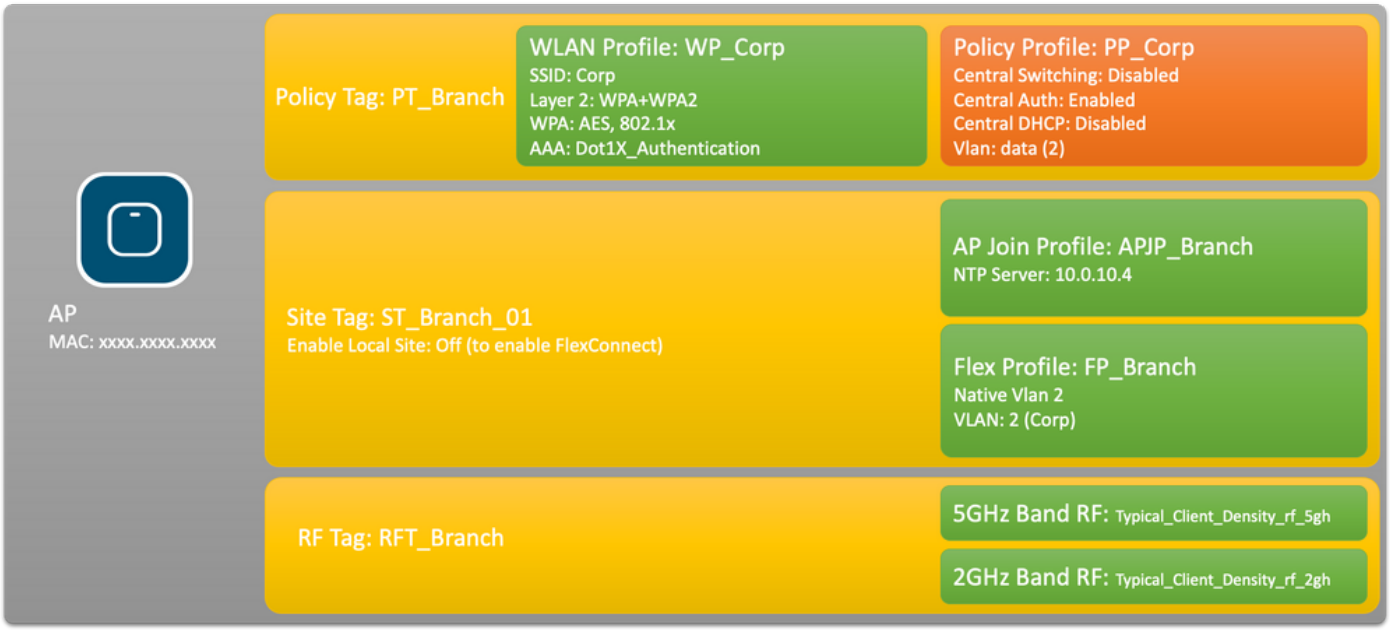


Netwerkdiagram



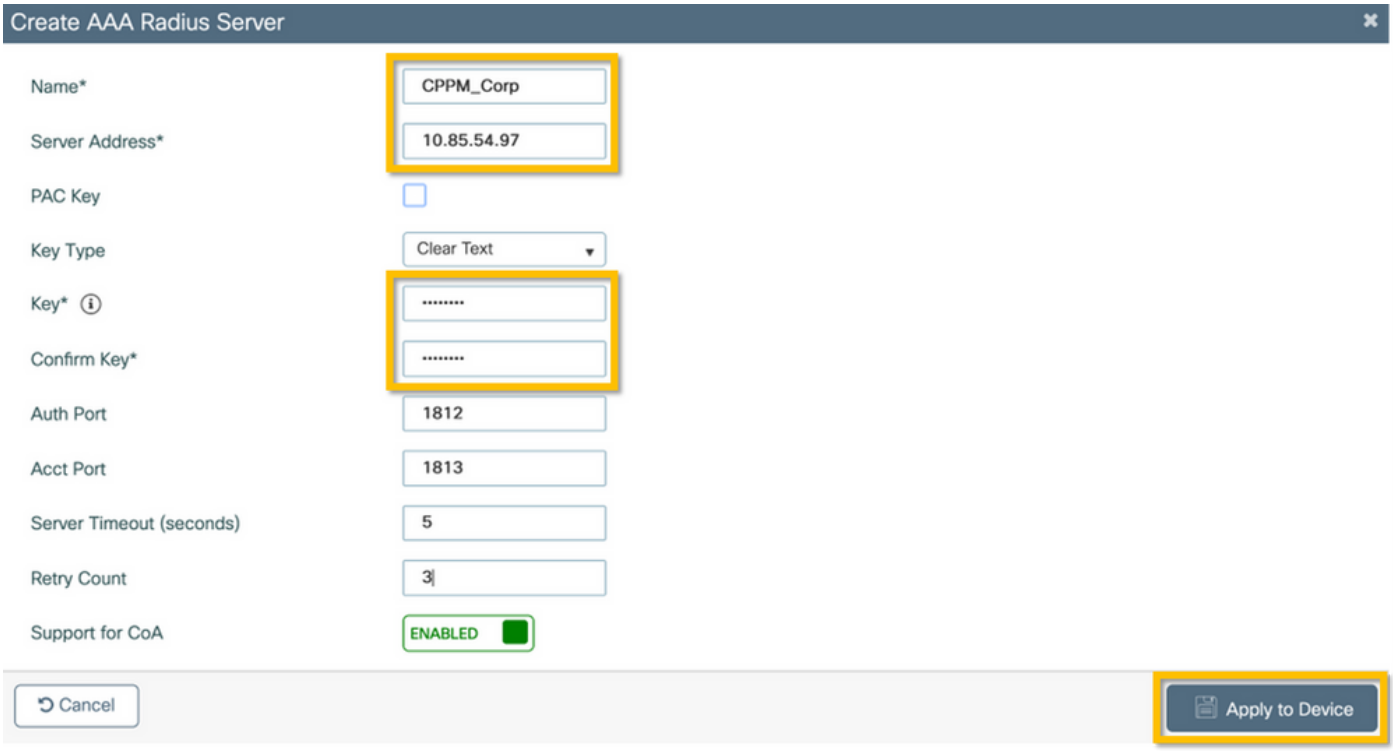
De Catalyst 9800 draadloze controller configureren

In dit configuratievoorbeeld wordt het nieuwe configuratiemodel op C9800 gebruikt om de benodigde profielen en tags te maken voor dot1x Corporate Access naar de bedrijfsonderdelen. De resulterende configuratie wordt in het diagram samengevat.

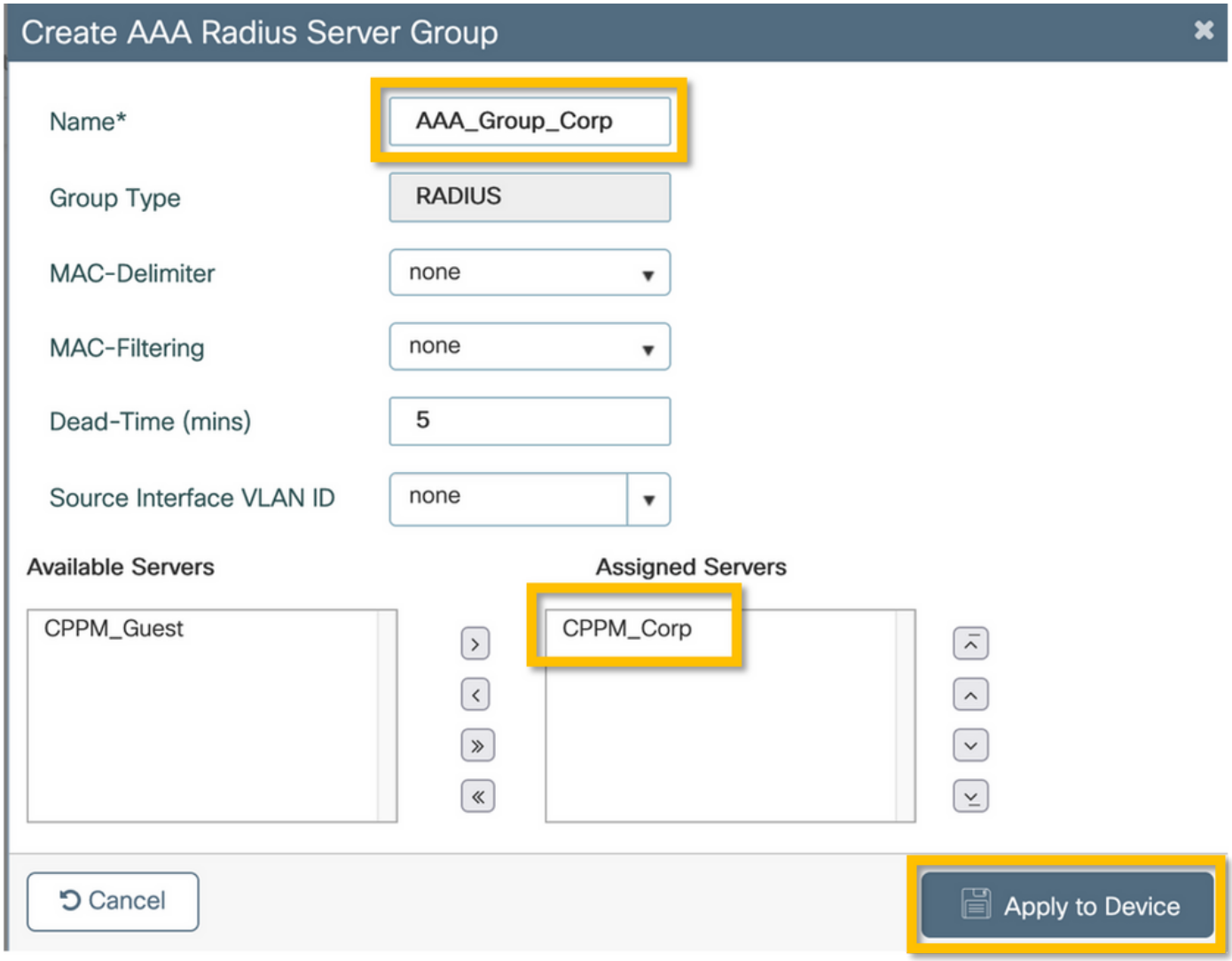


C9800 - AAA-parameters configureren voor dot1x

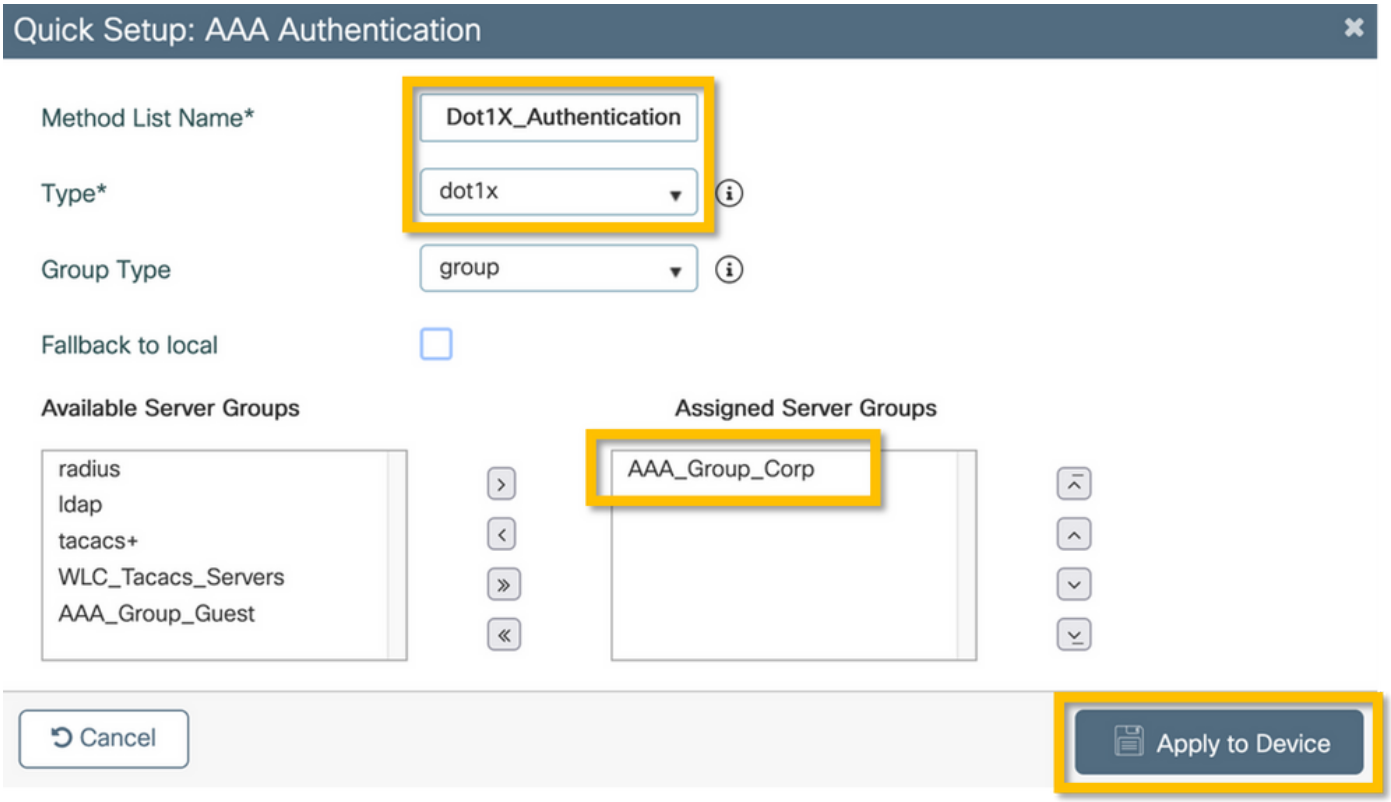
Stap 1. Voeg de Aruba ClearPass Policy Manager 'Corp'-server toe aan de 9800 WLC-configuratie. Navigeer naar **Configuratie > Beveiliging > AAA > servers/groepen > RADIUS > servers.** Klik op **+Add** en voer de RADIUS-serverinformatie in. Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.



Stap 2. Definieer AAA-servergroep voor zakelijke gebruikers. Navigeer naar **Configuratie > Beveiliging > AAA > Servers/groepen > RADIUS > Groepen** en klik op **+Add,** voer de naam van de RADIUS-servergroep in en wijs de RADIUS-serverinformatie toe. Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.

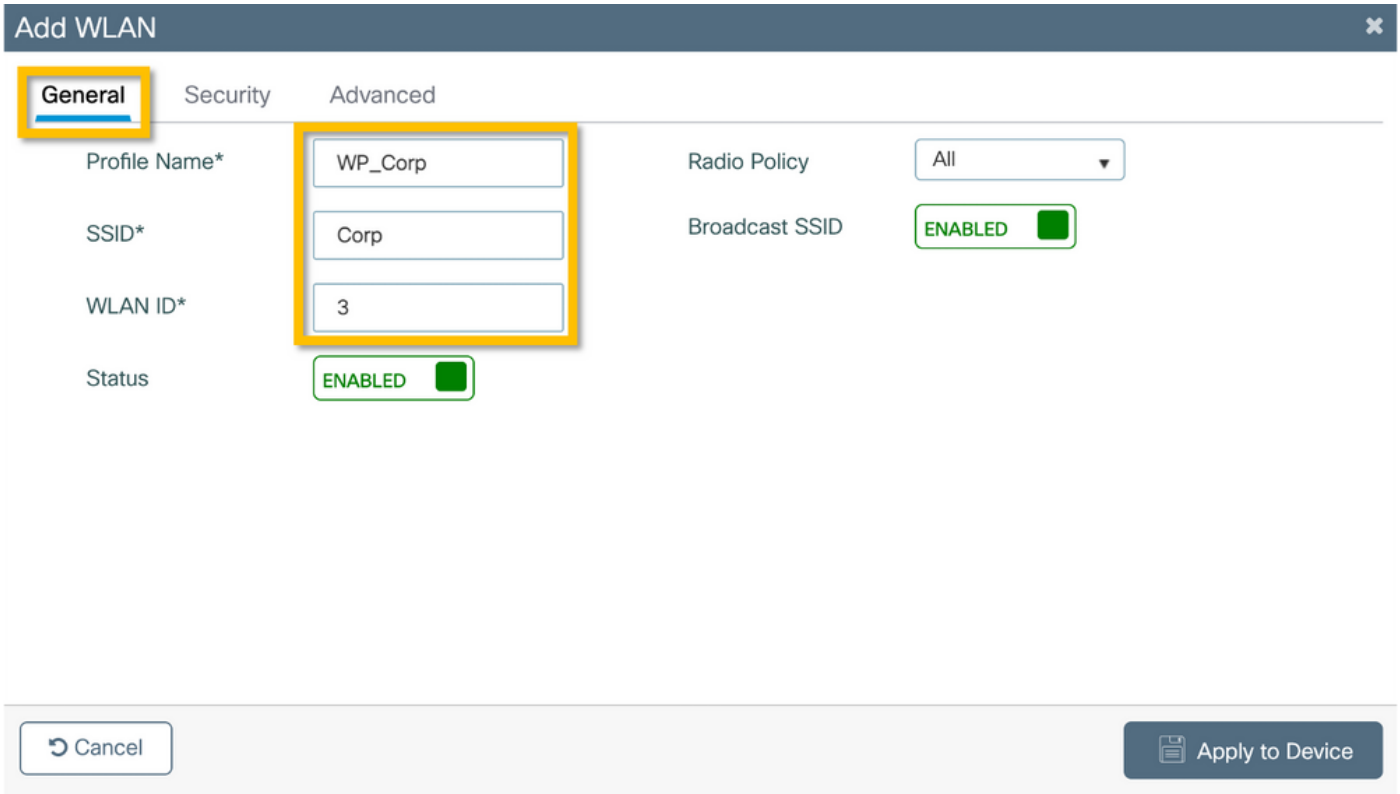


Stap 3. Definieer de dot1x-verificatiemethode voor zakelijke gebruikers. Navigeer naar **Configuratie > Beveiliging > AAA > AAA-methodelijst > Verificatie** en klik op **+Add**. Selecteer **Type dot1x** in het vervolgkeuzemenu. Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.

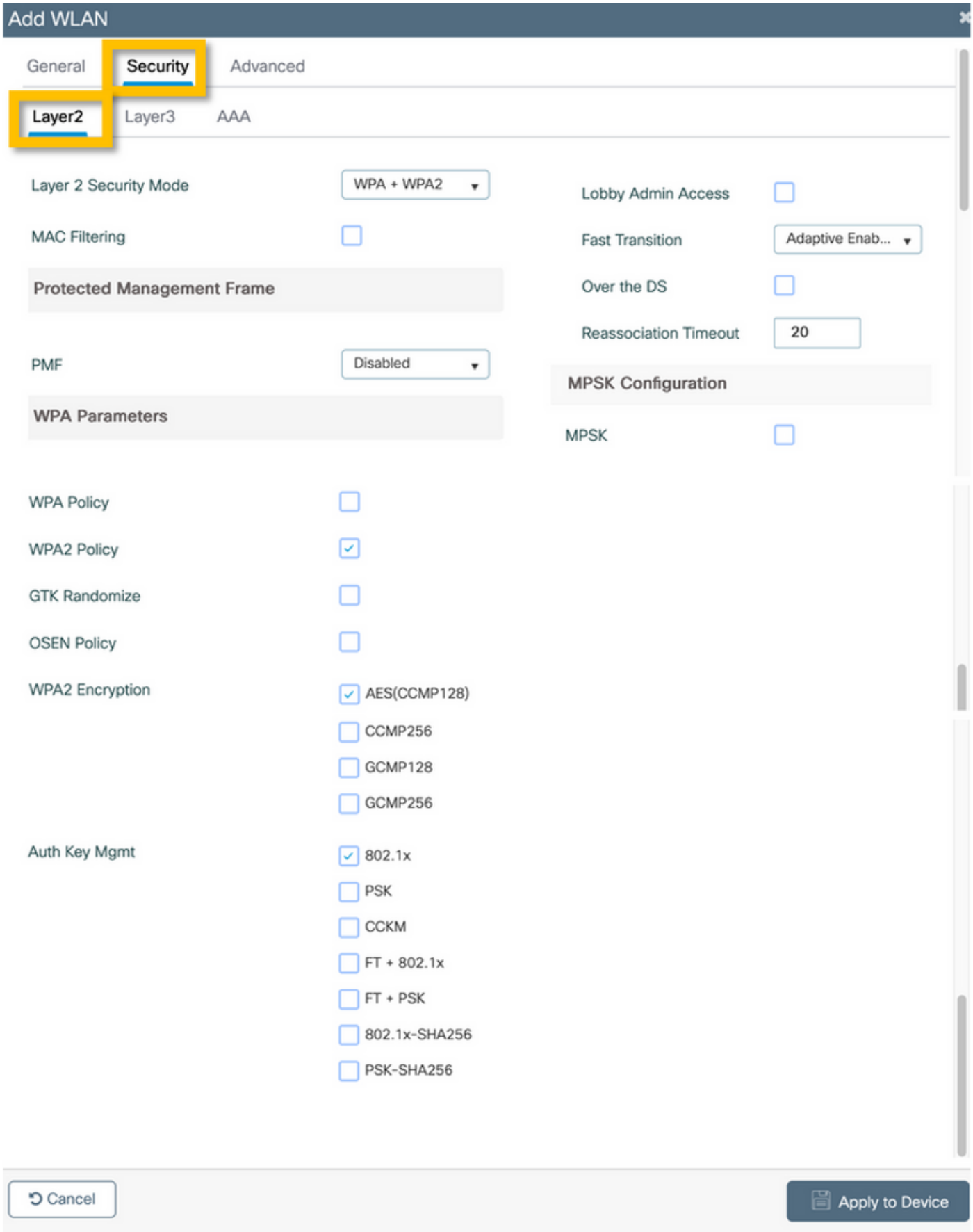


C9800 - Het 'Corp' WLAN-profiel configureren

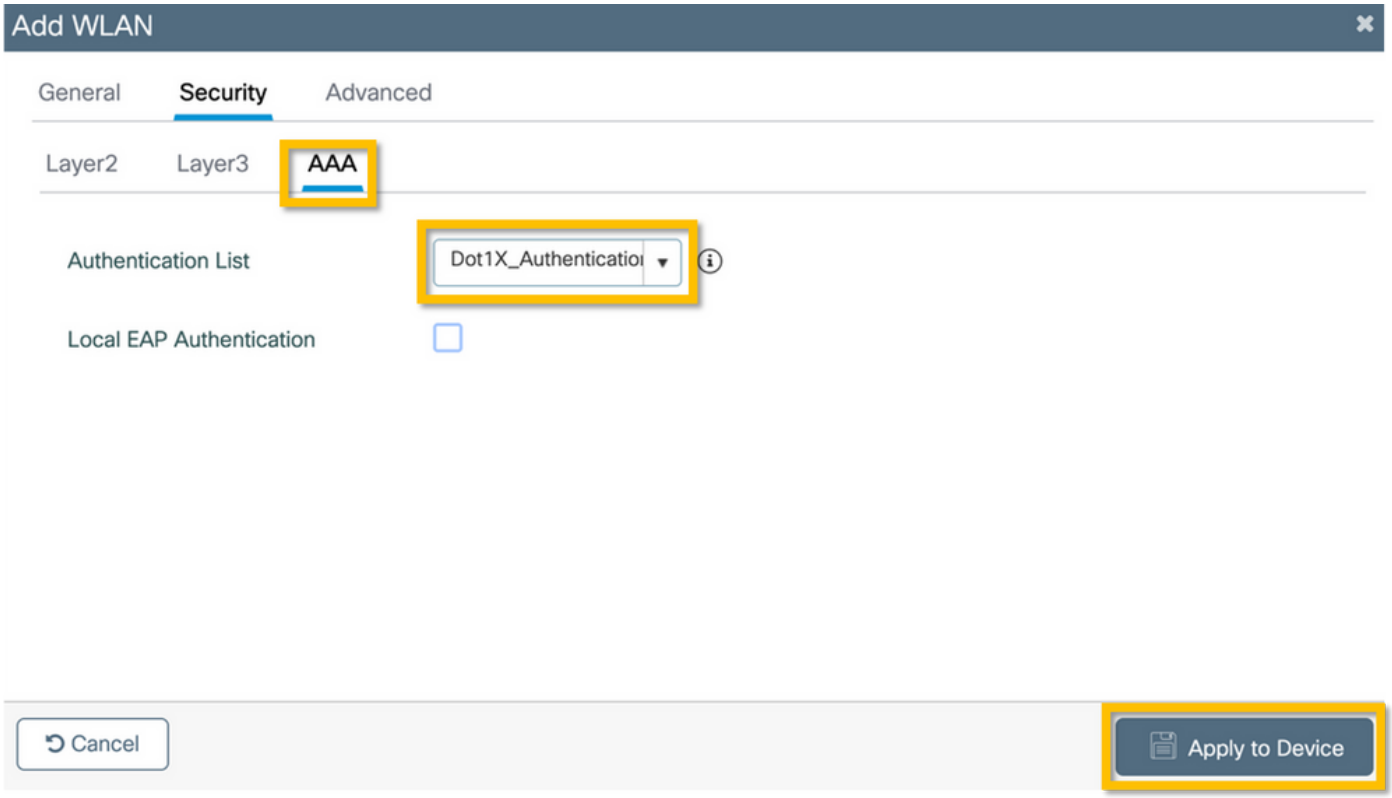
Stap 1. Navigeer naar **Configuration > Tags en profielen > Draadloos** en klik op **+Add**. Voer een profielnaam, de SSID 'Corp' en een WLAN-id in die nog niet in gebruik is.



Stap 2. Navigeer naar het tabblad **Beveiliging** en het subtabblad **Layer 2**. U hoeft de standaardparameters voor dit configuratievoorbeeld niet te wijzigen.

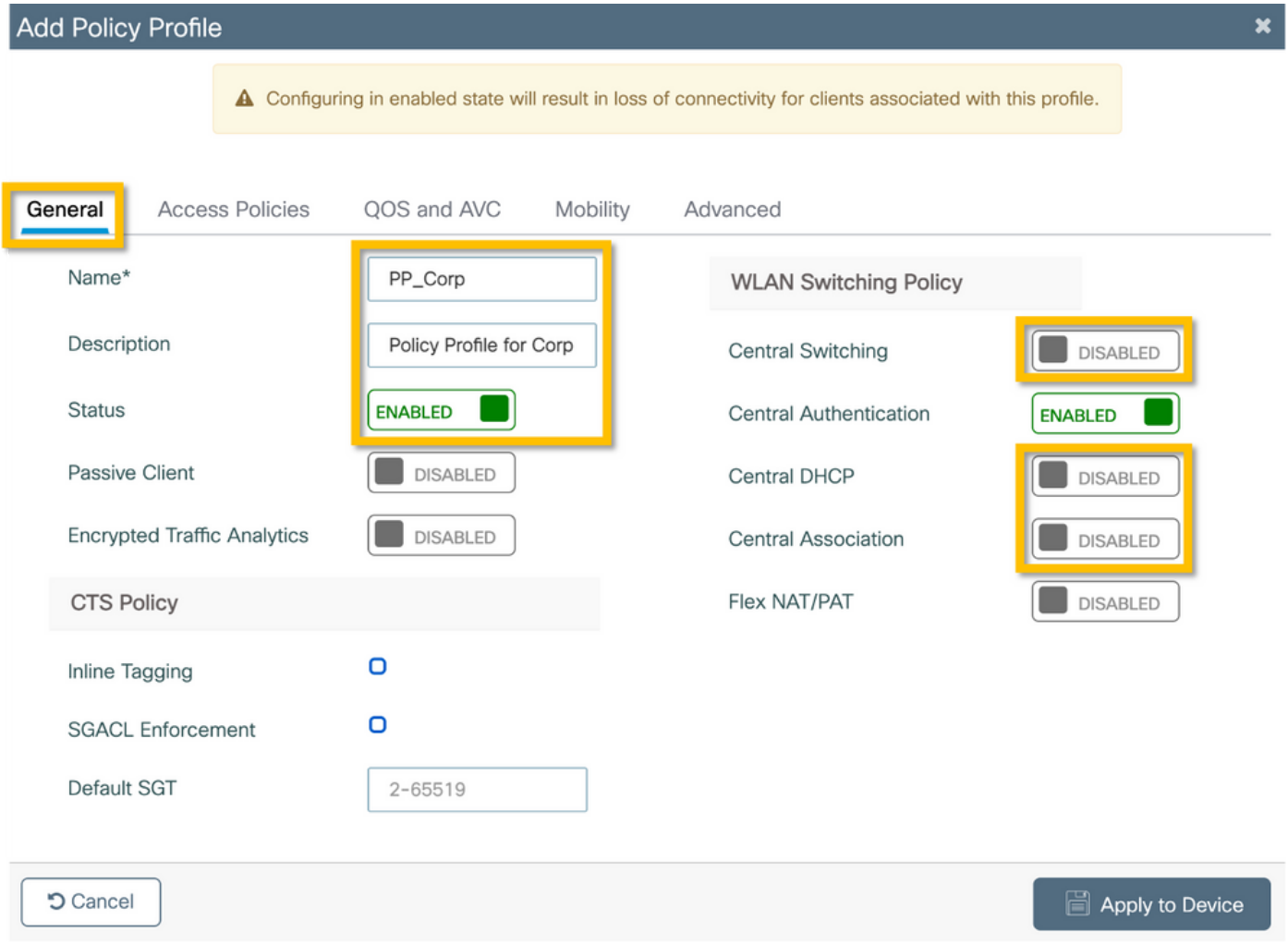


Stap 3. Navigeer naar het subtabblad **AAA** en selecteer de Lijst met verificatiemethoden die eerder is geconfigureerd. Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.

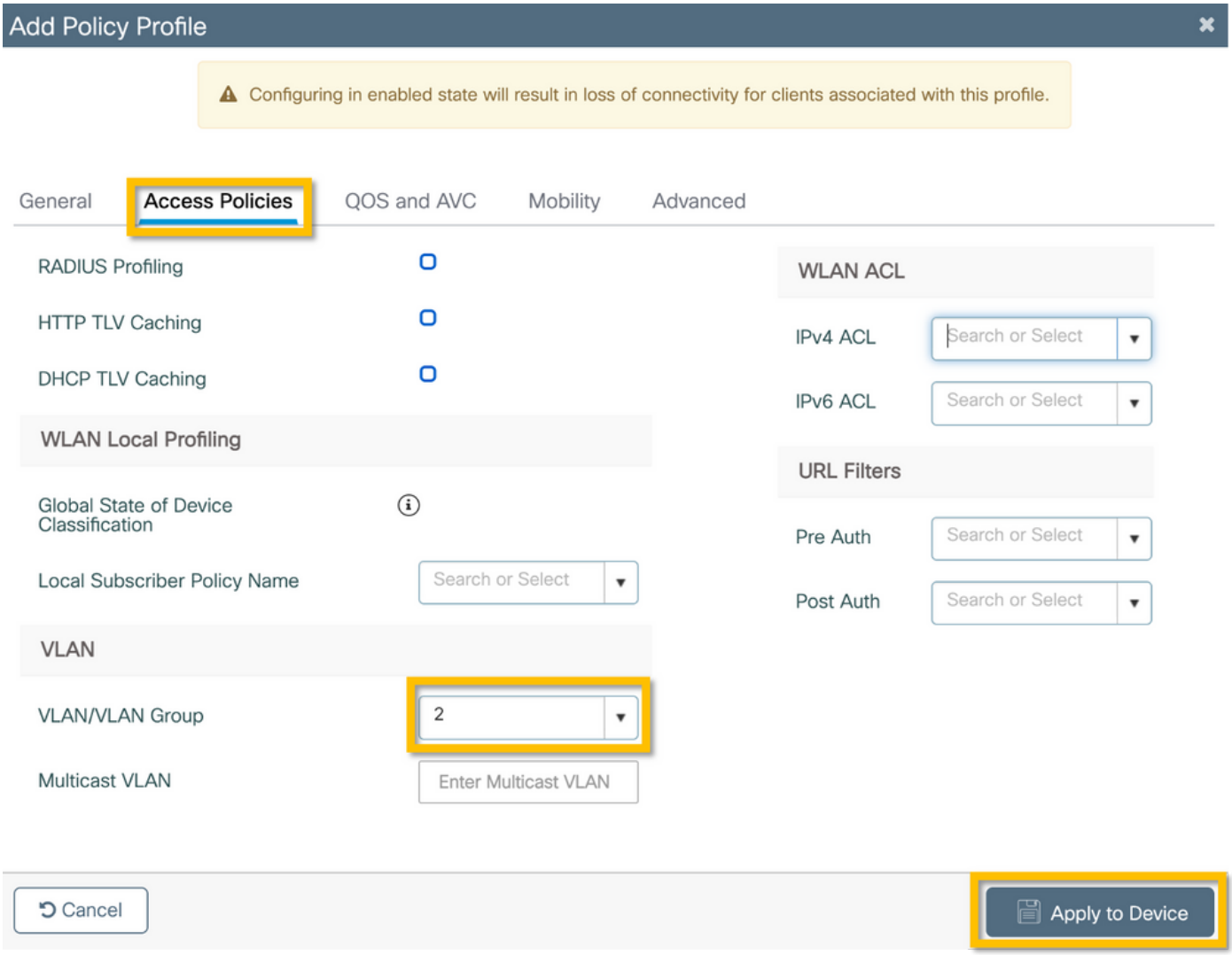


C9800 - Beleidsprofiel configureren

Stap 1. Navigeer naar **Configuration > Tags & profielen > Beleid** en klik op **+Add** en voer een naam en beschrijving van het beleidsprofiel in. Schakel het beleid in en schakel de centrale switching, DHCP en associatie uit, aangezien het bedrijfsgebruikersverkeer lokaal is ingeschakeld op het toegangspunt zoals in het afbeelding wordt getoond.



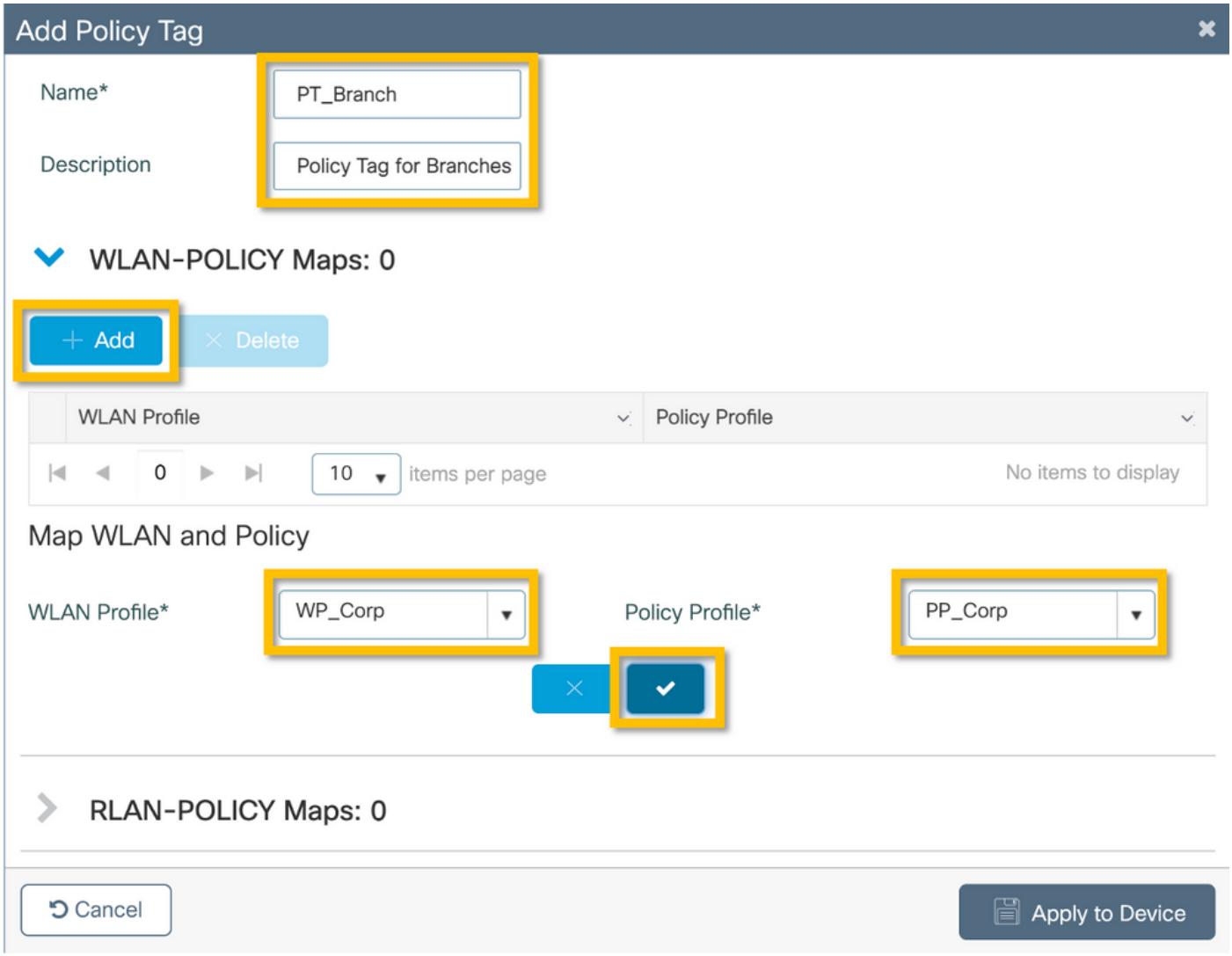
Stap 2. Navigeer naar het tabblad **Toegangsbeleid** en voer handmatig de ID van het VLAN in die moet worden gebruikt in de aftakking voor het bedrijfsgebruikersverkeer. Dit VLAN hoeft niet te worden geconfigureerd op de C9800 zelf. Het moet worden geconfigureerd in het Flex Profile, zoals verder uitgewerkt. Selecteer een VLAN-naam niet in de vervolgkeuzelijst (zie Cisco bug-id CSCvn48234 voor meer informatie). Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.



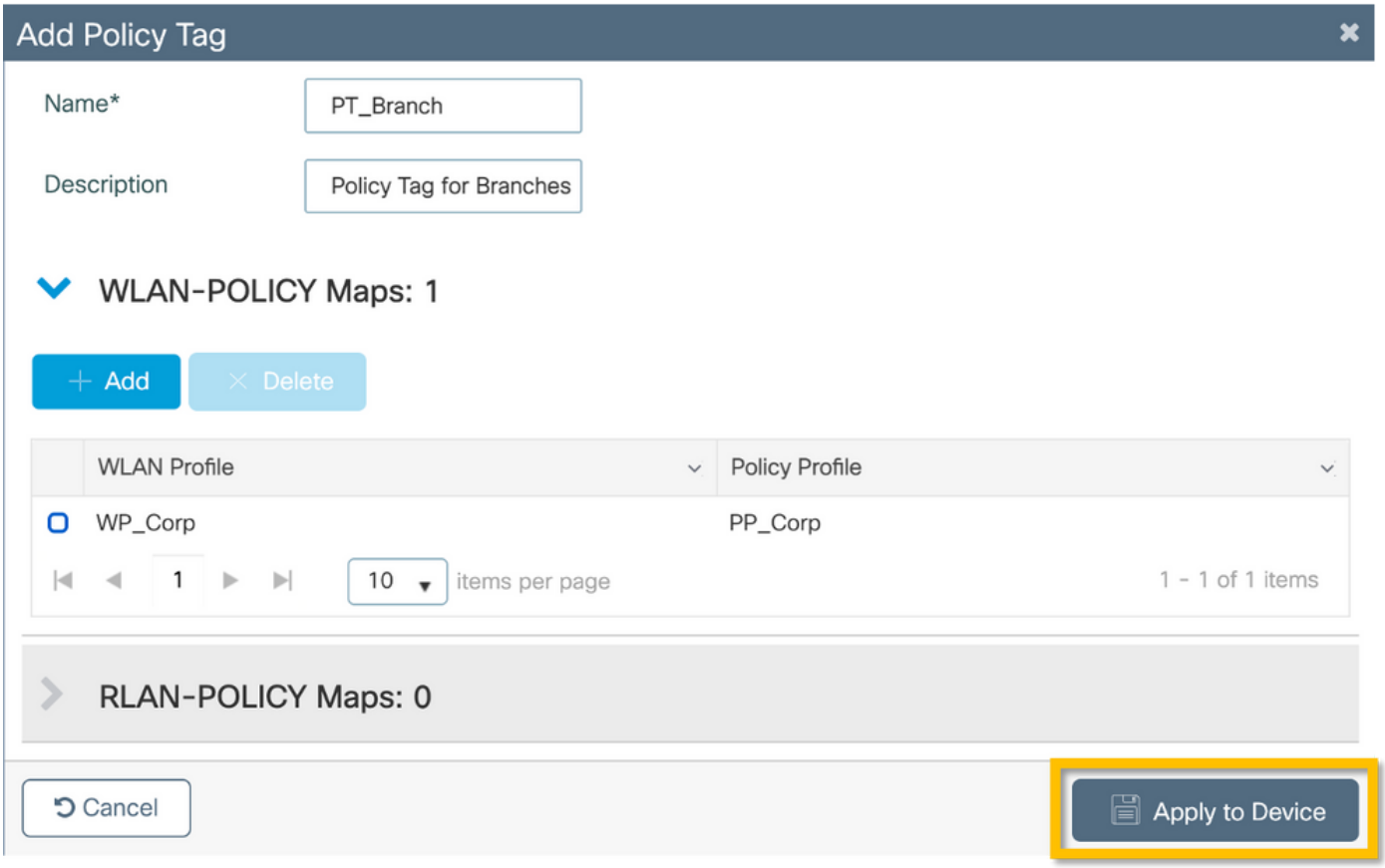
C9800 - Beleidsmarkering configureren

Zodra het WLAN-profiel (WP_Corp) en het beleidsprofiel (PP_Corp) zijn gemaakt, moet er een beleidstag worden gemaakt om deze WLAN- en beleidsprofielen samen te binden. Deze beleidsmarkering wordt toegepast op access points. Wijs deze beleidstag toe aan access points om de configuratie van deze toegangspunten te activeren om de geselecteerde SSID's op deze toegangspunten in te schakelen.

Stap 1. Navigeer naar **Configuration > Tags & profielen > Tags**, selecteer het tabblad **Policy** en klik op **+Add**. Voer de naam en beschrijving van de beleidstag in. Klik op **+Add** onder **WLAN-POLICY Maps**. Selecteer het eerder gemaakte WLAN-profiel en -beleidsprofiel en klik vervolgens op de knop voor het selectieteken zoals in deze afbeelding.



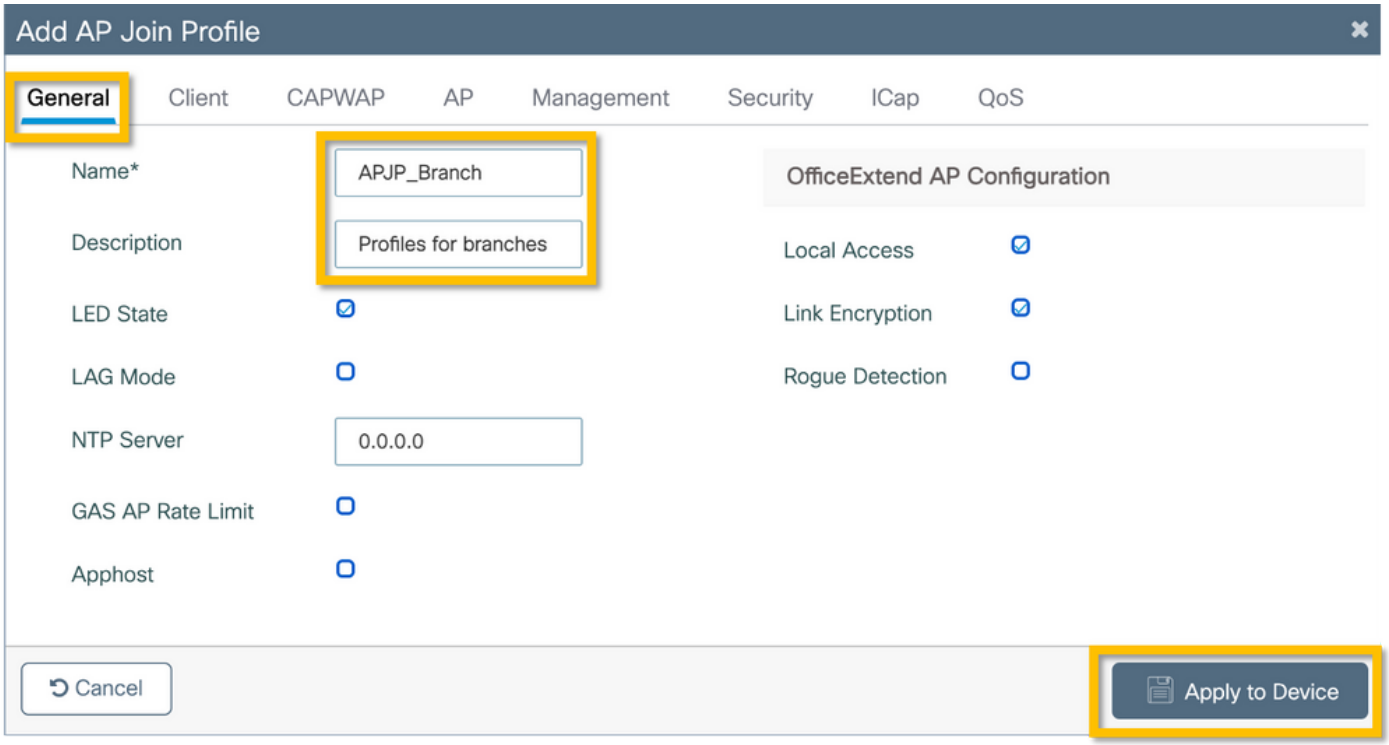
Stap 2. Controleer en klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.



C9800 - Profiel voor AP Join

AP Join Profiles en Flex Profiles moeten worden geconfigureerd en toegewezen aan access points met Site Tags. Voor elke tak moet een andere Site Tag worden gebruikt om 802.11r Fast Transition (FT) binnen een tak te ondersteunen, maar de distributie van de client PMK alleen tussen de AP's van die tak te beperken. Het is belangrijk om niet dezelfde site tag over meerdere takken te gebruiken. Configureer een AP Join Profile. U kunt één enkel AP Join Profiel gebruiken als alle takken gelijkaardig zijn, of tot meerdere profielen leiden als sommige van de gevormde parameters verschillend moeten zijn.

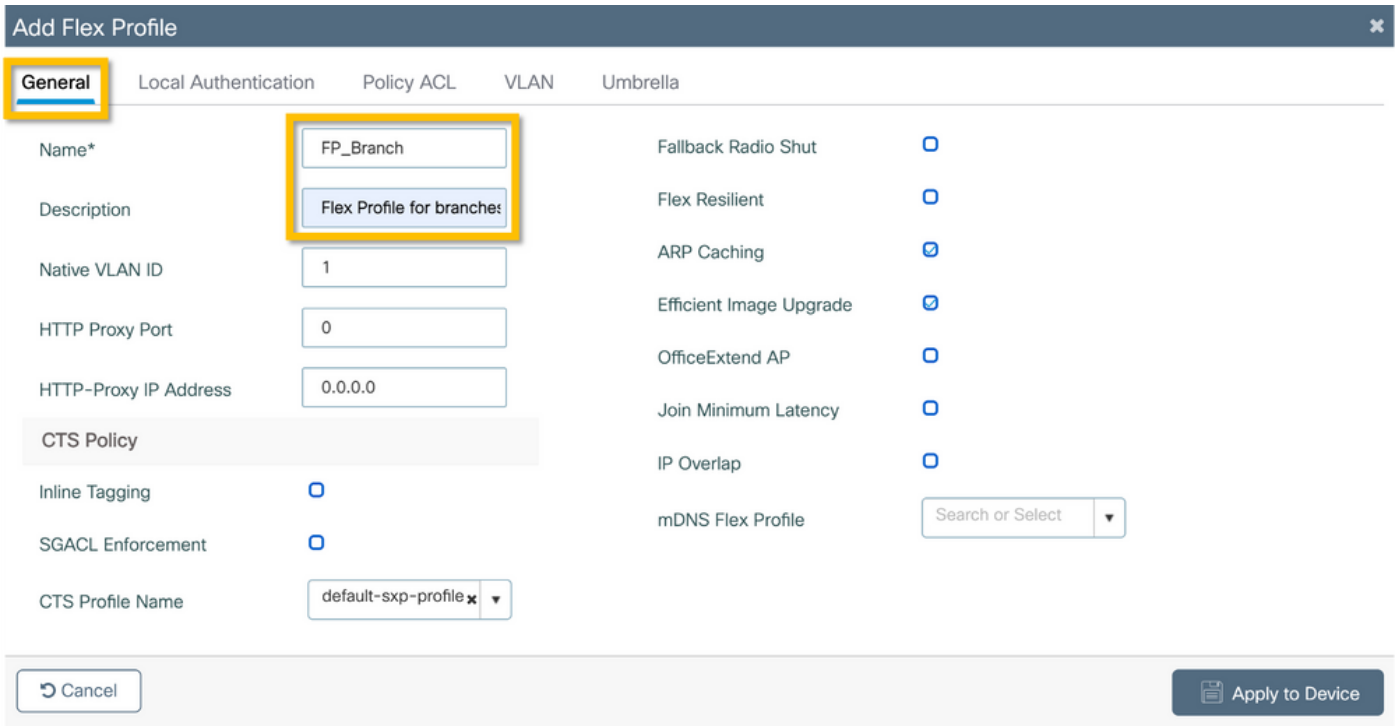
Stap 1. Navigeer naar **Configuration > Tags en profielen > AP Join** en klik op **+Add**. Voer de naam en beschrijving van het AP Join Profile in. Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.



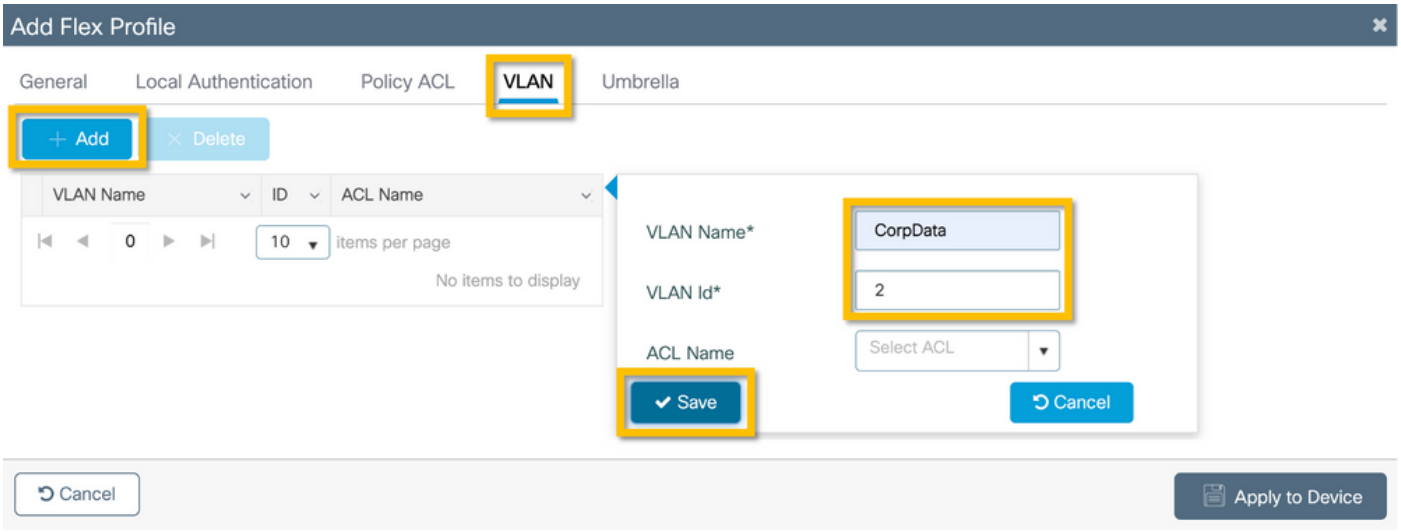
C9800 - Flex profiel

Configureer nu een Flex-profiel. Opnieuw kunt u één profiel gebruiken voor alle vertakkingen als deze gelijk zijn en dezelfde VLAN/SSID-toewijzing hebben. U kunt ook meerdere profielen maken als bepaalde ingestelde parameters, zoals de VLAN-toewijzingen, anders zijn.

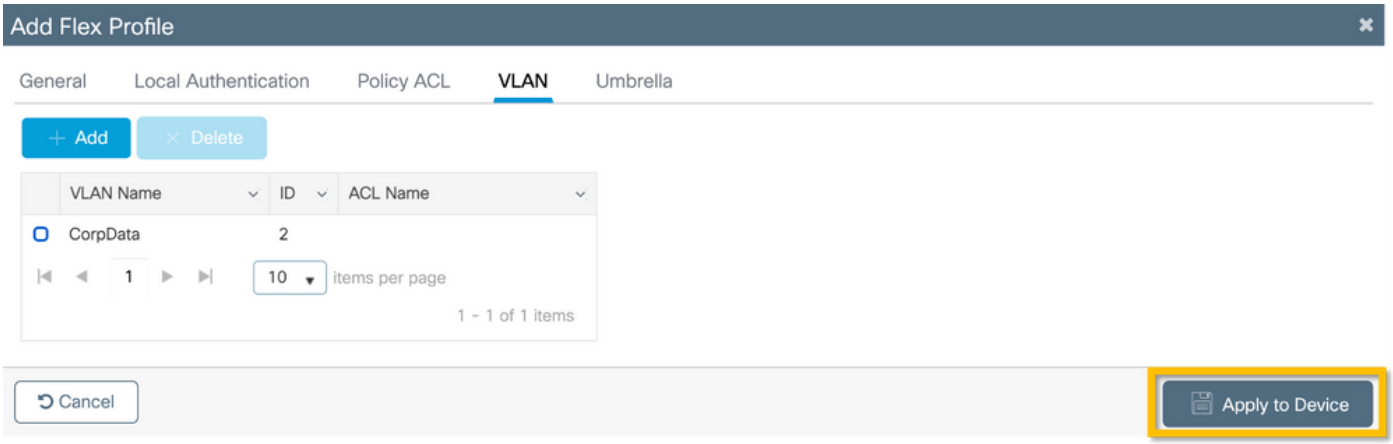
Stap 1. Navigeer naar **Configuration > Tags en profielen > Flex** en klik op **+Add**. Voer de naam en beschrijving van Flex Profile in.



Stap 2. Navigeer naar het tabblad **VLAN** en klik op **+Add**. Voer de VLAN-naam en -id in van het lokale VLAN bij de aftakking die het toegangspunt moet gebruiken om het bedrijfsgebruikersverkeer lokaal te switches. Klik op de knop **Opslaan** zoals in deze afbeelding.



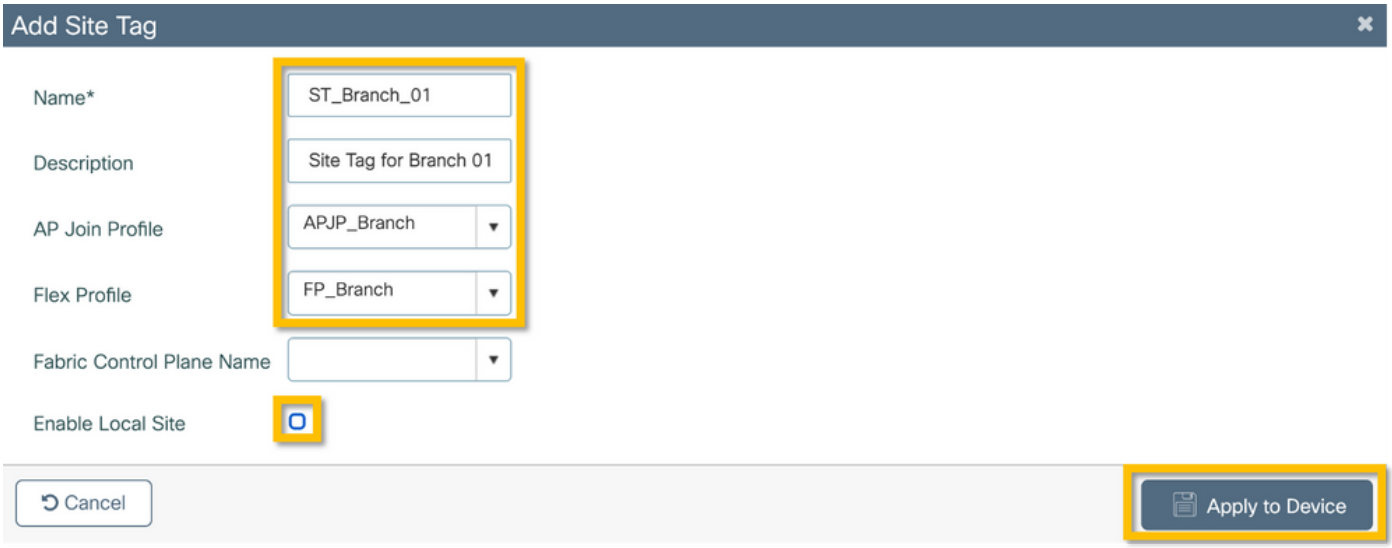
Stap 3. Controleer en klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.



C9800 - Sitetag

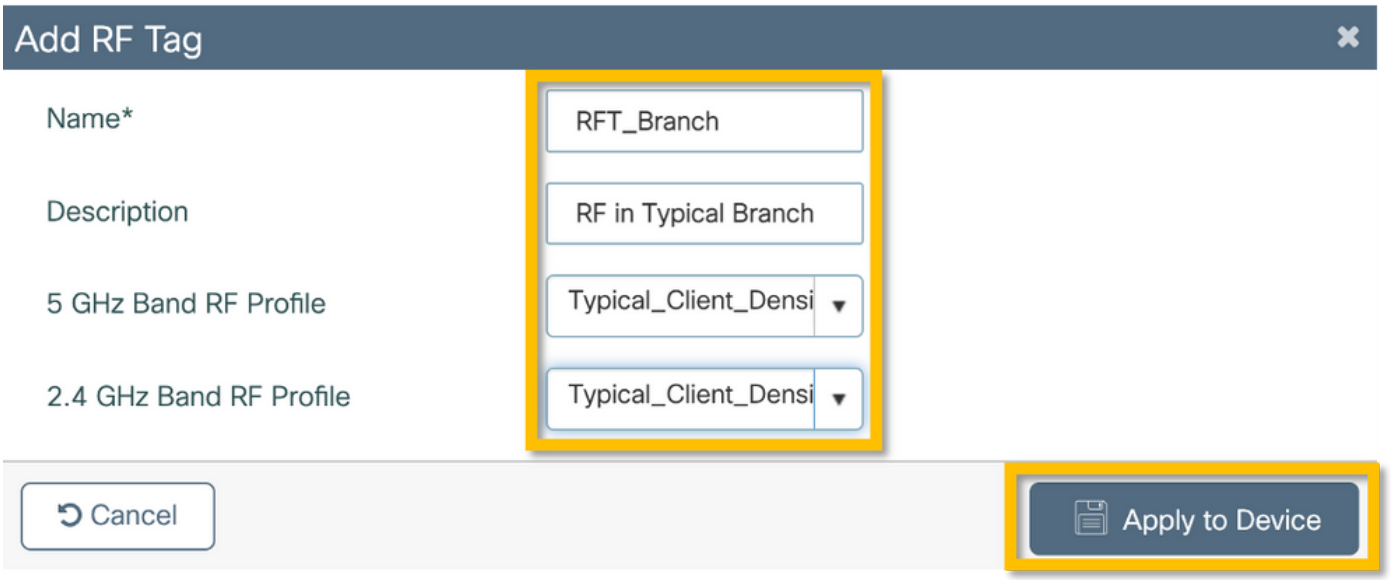
Site-tags worden gebruikt om Join Profiles en Flex Profiles toe te wijzen aan access points. Zoals eerder vermeld, moet voor elke tak een andere Site-tag worden gebruikt om 802.11r Fast Transition (FT) binnen een tak te ondersteunen, maar de verdeling van de client-PMK over alleen de AP's van die tak te beperken. Het is belangrijk om dezelfde site-tag niet opnieuw te gebruiken over meerdere takken.

Stap 1. Navigeer naar **Configuration > Tags & profielen > Tags**, selecteer het tabblad **Site** en klik op **+Add**. Voer een naam en beschrijving van de sitetag in, selecteer het profiel samenvoegen met het toegangspunt, deselecteer het vakje **Lokale site inschakelen** en selecteer ten slotte het eerder gemaakte Flex-profiel. Schakel het vakje **Local Site inschakelen uit** om het toegangspunt van **Local Mode** in **FlexConnect** te wijzigen. Klik tot slot op de knop **Toepassen op apparaat** zoals in dit beeld.



C9800 - RF-tag

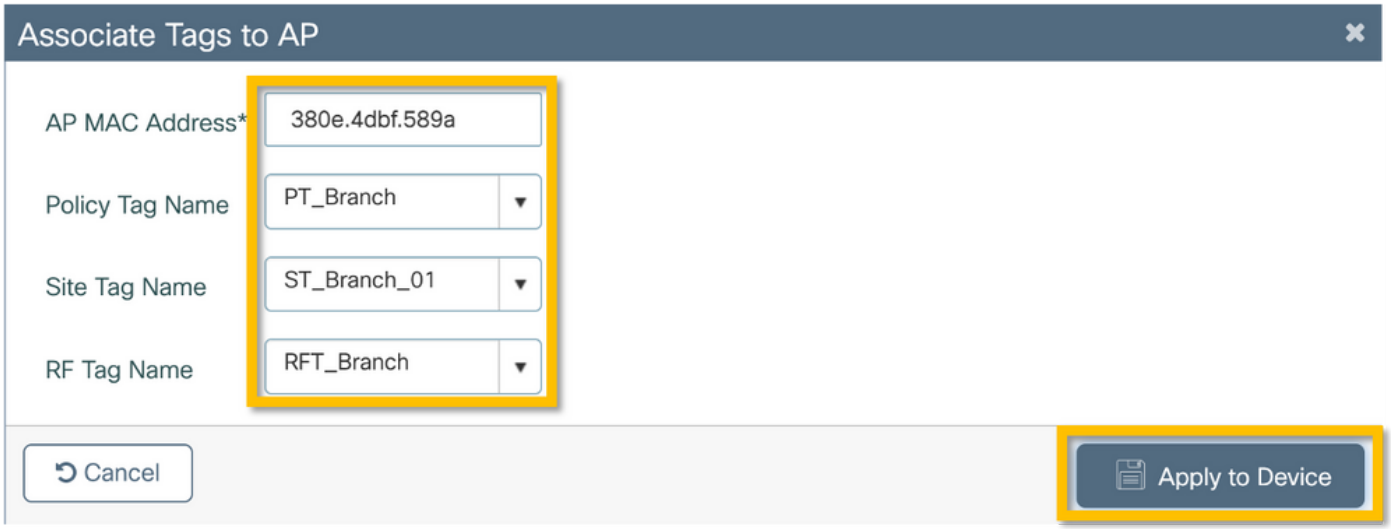
Stap 1. Navigeer naar **Configuration > Tags & profielen > tags**, selecteer het **tabblad RF** en klik op **+Add.** Voer een naam en beschrijving in voor de RF-tag.Selecteer de door het systeem gedefinieerde **RF-profielen in het vervolgkeuzemenu**. Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.



C9800 - Tags toewijzen aan AP

Nu de tags worden gecreëerd die de verschillende beleidslijnen en profielen bevatten die nodig zijn om de access points te configureren, moeten we ze toewijzen aan de access points. Deze paragraaf laat zien hoe u een statische tag kunt uitvoeren die handmatig aan een access point wordt toegewezen, op basis van het Ethernet MAC-adres. Voor productproductieomgevingen wordt aanbevolen de Cisco DNA Center AP PNP Workflow te gebruiken, of een statische, bulk-CSV-uploadmethode te gebruiken die beschikbaar is in 9800.

Stap 1. Navigeer om te **configureren > Tags & profielen > tags**, selecteer het **AP-**tabblad en vervolgens het **tabblad Statisch**. Klik op **+Add** en voer het MAC-adres van het AP in en selecteer de eerder gedefinieerde Policy Tag, Site Tag en RF-tag. Klik op de knop **Toepassen op apparaat** zoals in deze afbeelding.



Aruba CPPM configureren

Eerste configuratie van Aruba ClearPass Policy Manager-server

Aruba clearpass wordt via OVF-sjabloon op ESXi-server ingezet met deze bronnen:

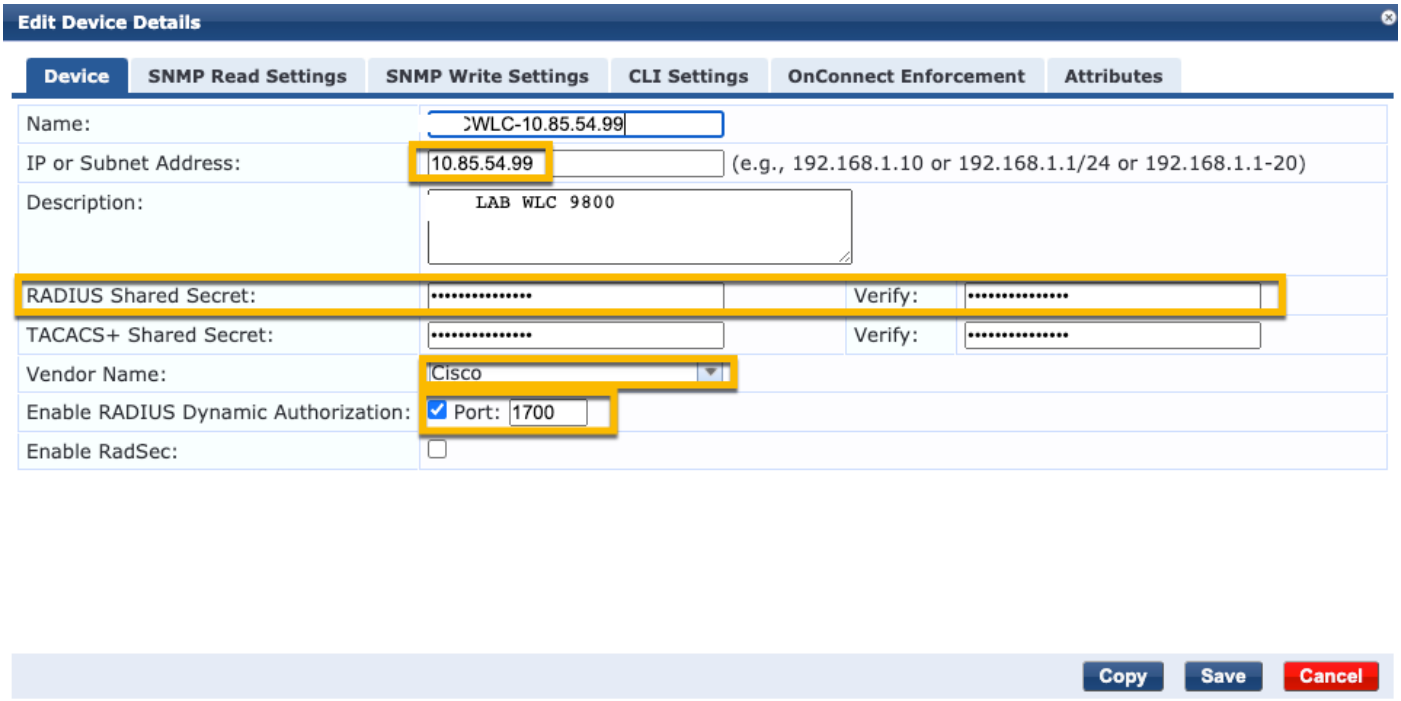
- 2 gereserveerde virtuele CPU's
- 6 GB RAM
- 80 GB schijf (moet handmatig worden toegevoegd na eerste VM-implementatie voordat de machine wordt ingeschakeld)

Licenties toepassen

Platformlicentie toepassen via: **Beheer > Server Manager > Licentie**. **Toegang en** ingebouwd toevoegen

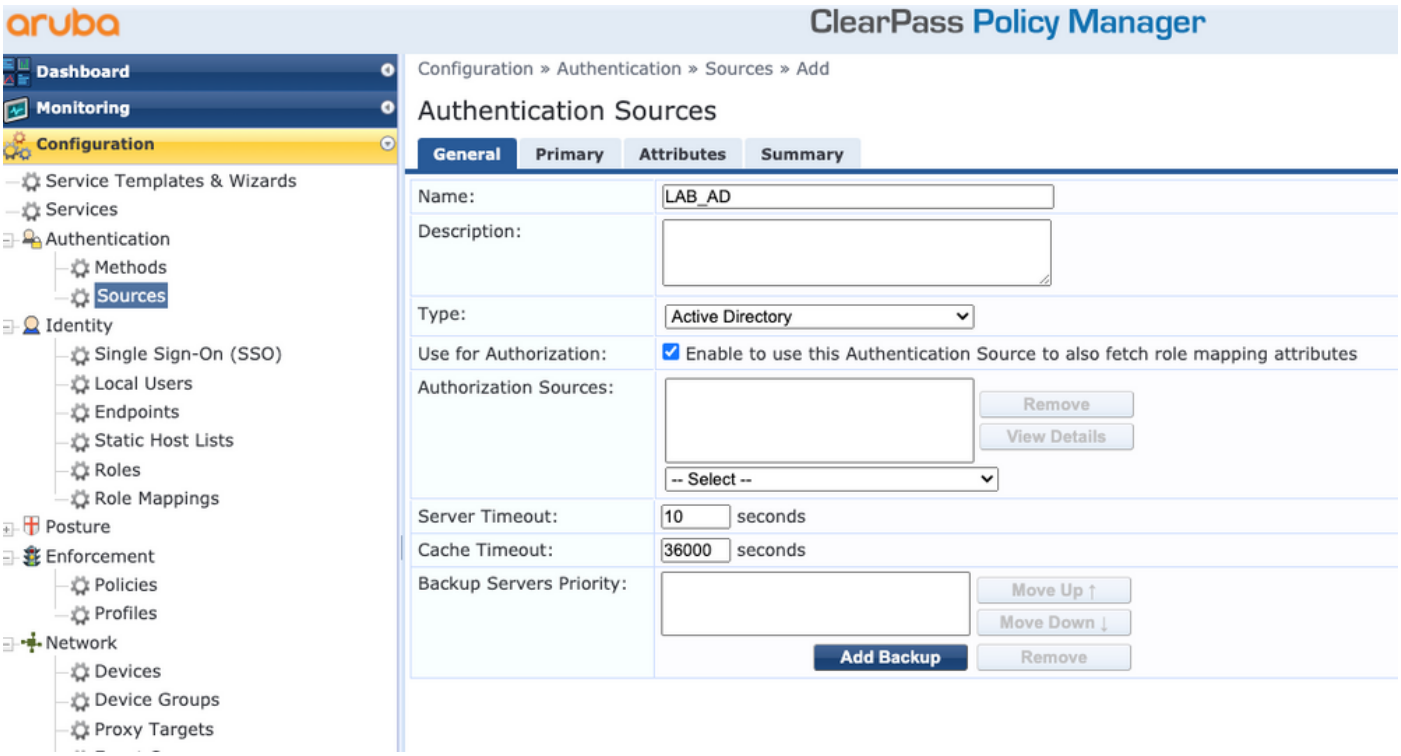
De C9800 draadloze controller toevoegen als netwerkapparaat

Ga naar **Configuratie > Netwerk > Apparaten > Toevoegen** zoals in deze afbeelding.



CPPM configureren om Windows AD als verificatiebron te gebruiken

Navigeer naar **Configuratie > Verificatie > Bronnen > Toevoegen**. Selecteer **Type: Active Directory** in het vervolgkeuzemenu zoals in deze afbeelding.



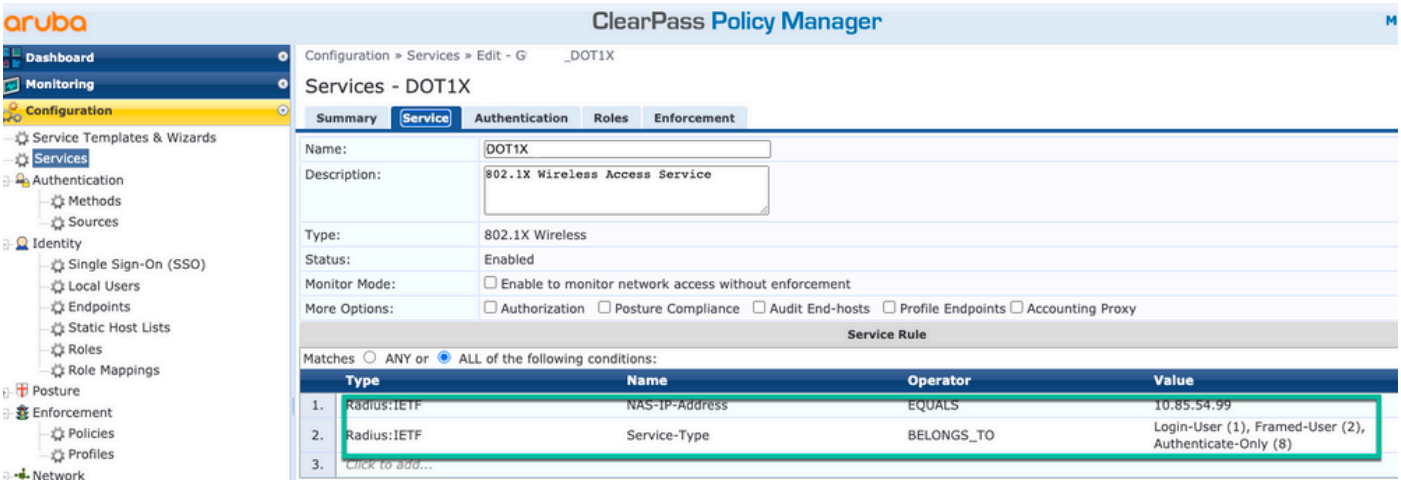
CPPM configureren Dot1X-verificatieservice

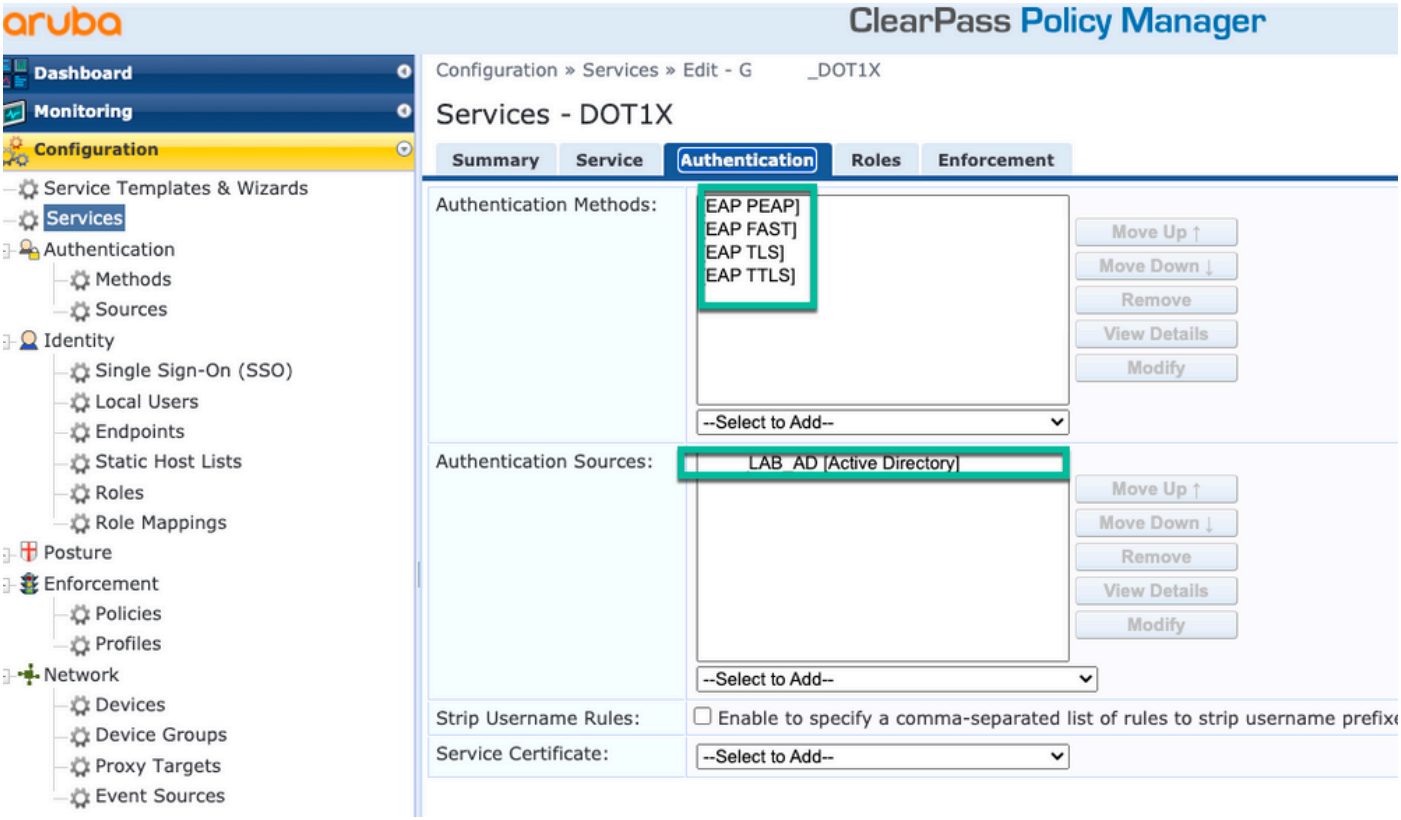
Stap 1. Maak een 'service' die overeenkomt met verschillende RADIUS-kenmerken:

- Straal:IETF | Naam: NAS-IP-adres | GELIJKHEID | <IP-ADRES>
- Straal:IETF | Naam: Service-type | GELIJKHEID | 1,2,8

Stap 2. Voor de productie wordt aanbevolen een SSID-naam te gebruiken in plaats van 'NAS-IP-

Adres', zodat één voorwaarde volstaat voor een multi-WLC-implementatie. | cisco-WLAN | Dot1XSSID





Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Handleiding voor best practices voor Cisco 9800 implementaties

- Inzicht in Catalyst 9800 configuratiemodel voor draadloze controllers
- Begrijp FlexConnect op Catalyst 9800 draadloze controller
- **Technische ondersteuning en documentatie – Cisco Systems**

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.