FlexConnect met verificatie configureren op Catalyst 9800 WLC

Inhoud

Inleiding

Dit document beschrijft hoe u FlexConnect met centrale of lokale verificatie kunt configureren op Catalyst 9800 draadloze LAN-controller.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Catalyst draadloze 9800 configuratiemodel
- FlexConnect
- 802.1x

Gebruikte componenten

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

- C980-CL, Cisco IOS-XE® 17.3.4

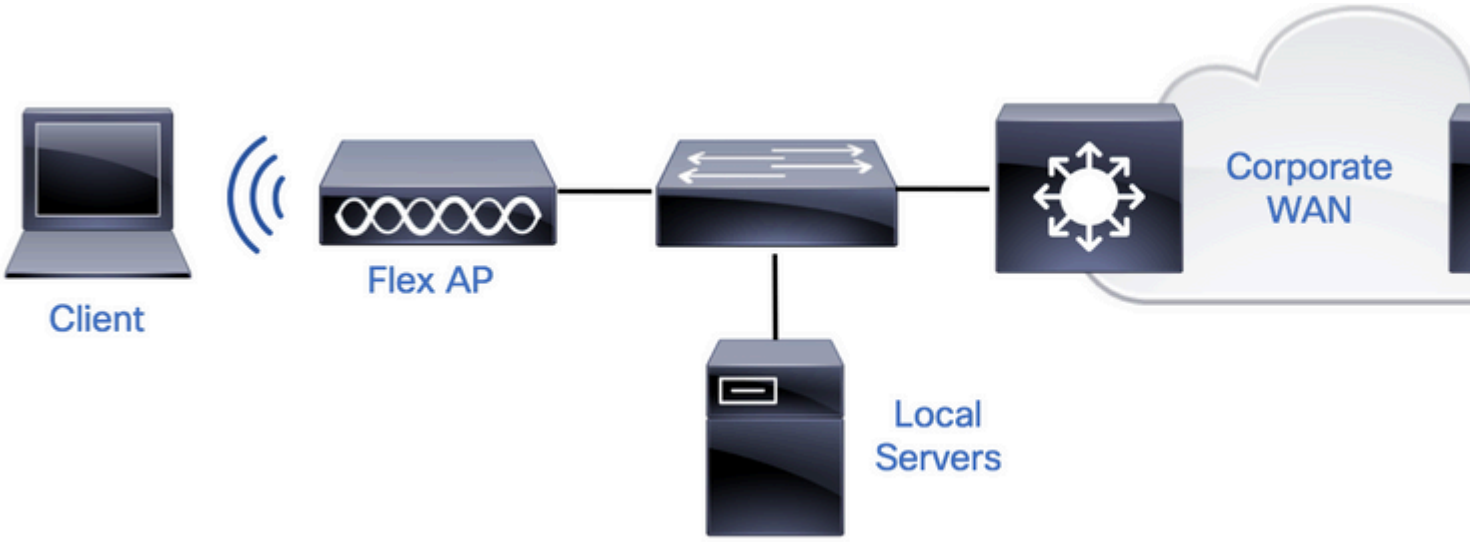
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

FlexConnect is een draadloze oplossing voor implementatie in externe vestigingen. Hiermee kunt u access points (APâ€™s) configureren op externe locaties vanuit het kantoor van het bedrijf via een Wide Area Network (WAN)-link zonder dat u in elke locatie een controller hoeft te implementeren. De FlexConnect APâ€™s kunnen het clientgegevensverkeer lokaal switches en de clientverificatie lokaal uitvoeren wanneer de verbinding met de controller verloren gaat. In de verbonden modus kunnen de FlexConnect AP's ook lokale verificatie uitvoeren.

Configureren

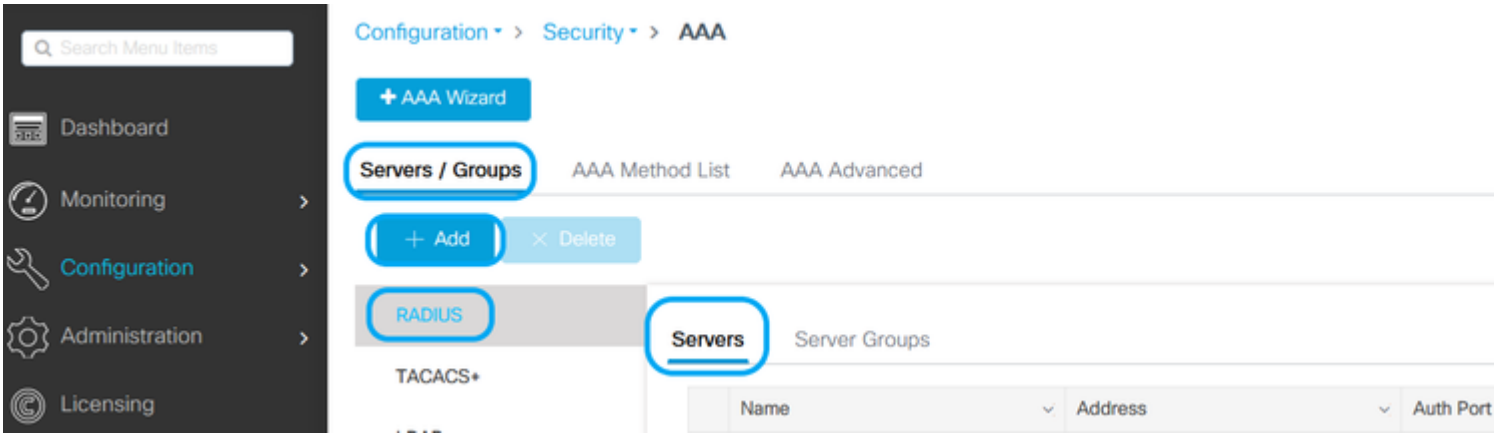
Netwerkdiagram



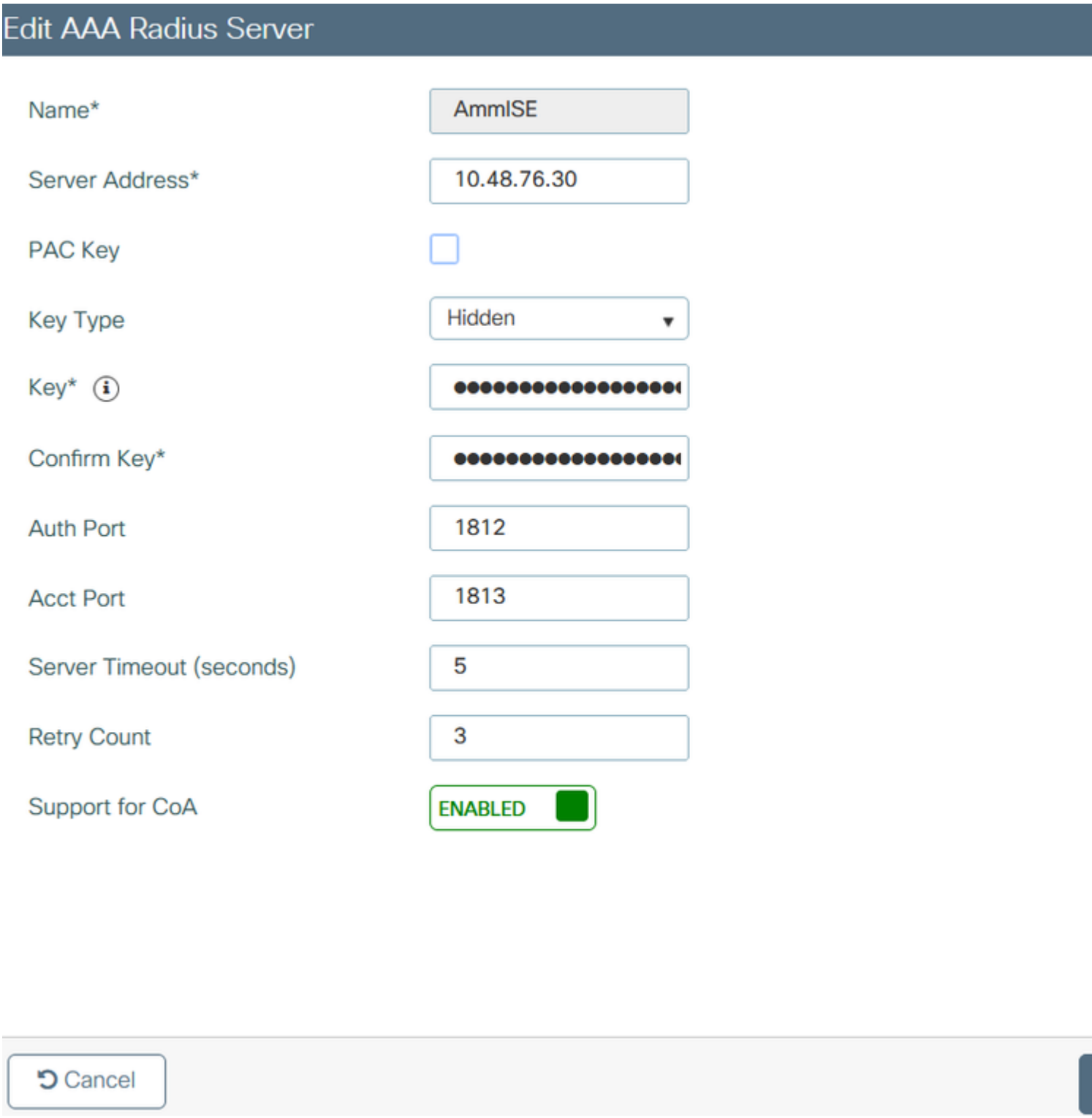
Configuraties

AAA-configuratie op 9800 WLCâ€™s

Stap 1. RADIUS-server declareren. **Van GUI:** Navigeer naar Configuratie > Beveiliging > AAA > Servers / Groepen > RADIUS > Servers > + Voeg de RADIUS-serverinformatie toe en voer deze in.

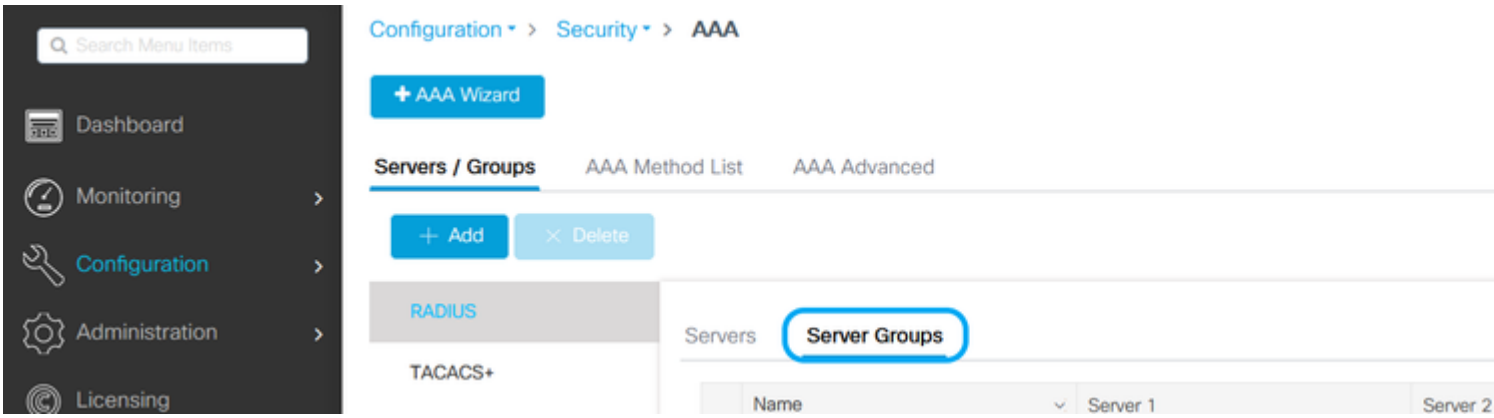


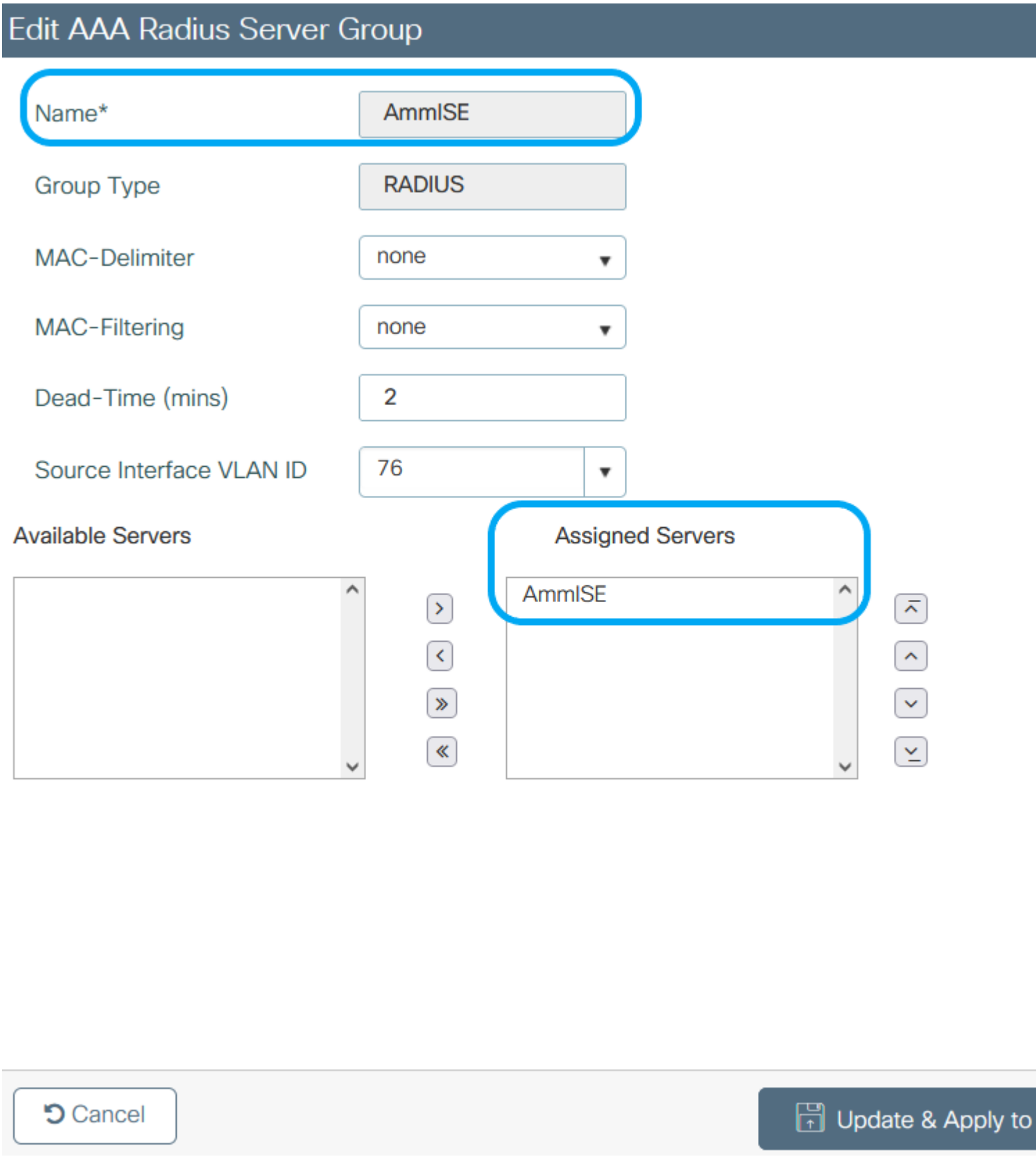
Zorg ervoor dat ondersteuning voor CoA is ingeschakeld als u van plan bent om in de toekomst elke vorm van beveiliging te gebruiken die CoA vereist.



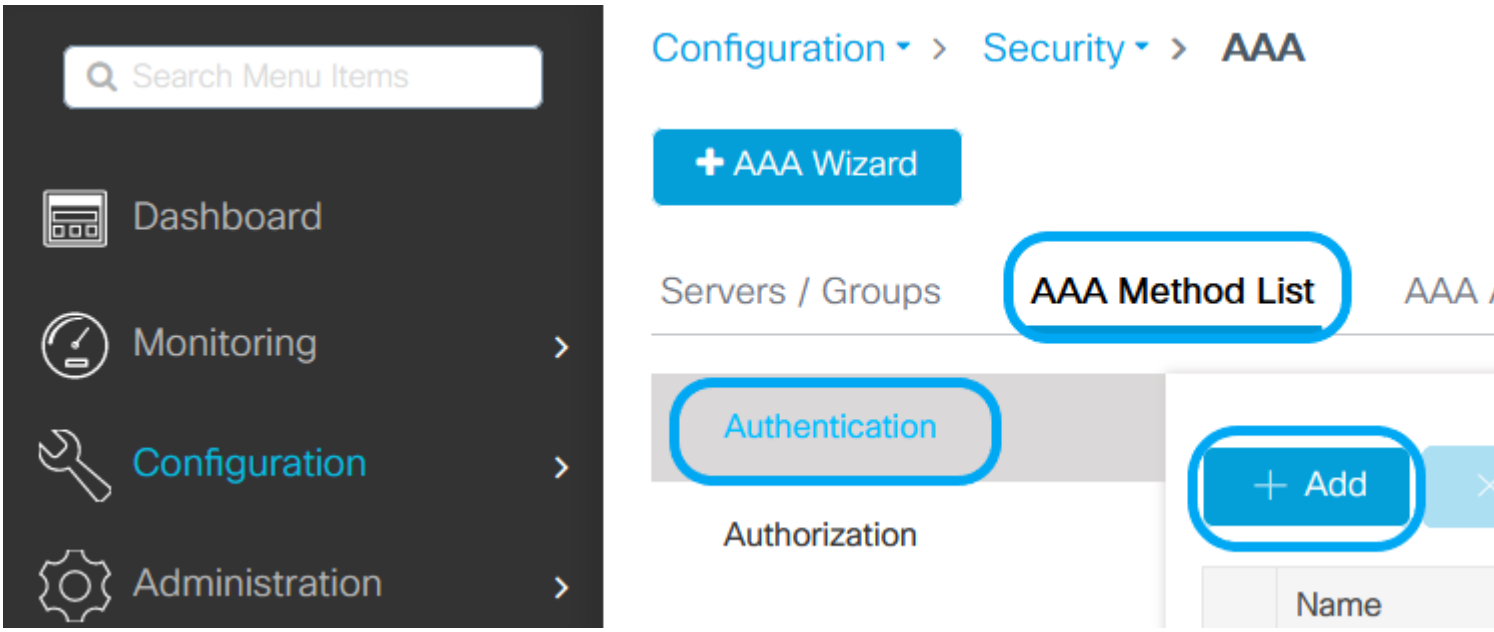
Opmerking: Radius CoA wordt niet ondersteund in Flex Connect-implementatie van lokale audits. .

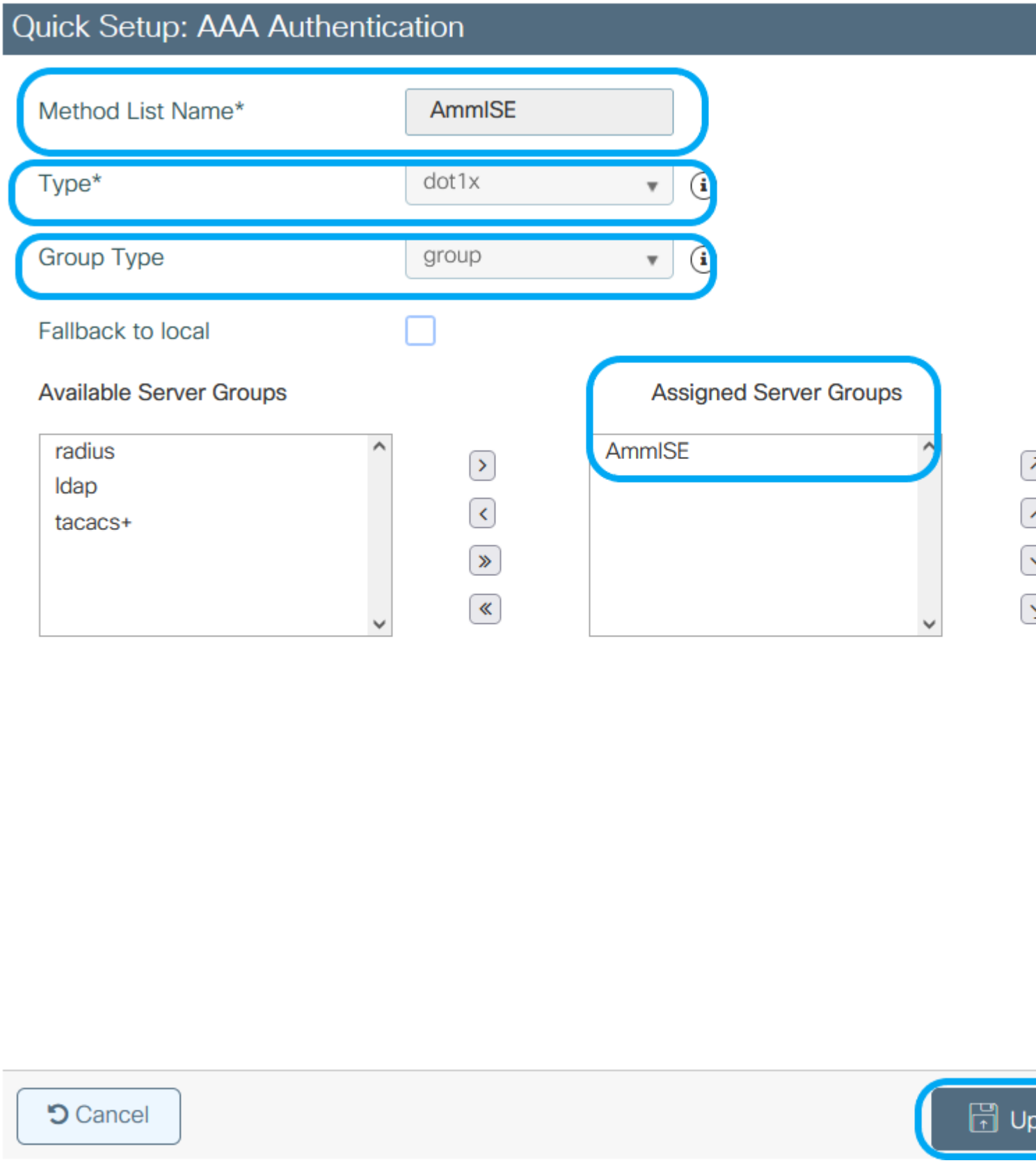
Stap 2. Voeg de RADIUS-server toe aan een RADIUS-groep. **Van GUI:** Navigeer naar Configuratie > Beveiliging > AAA > Servers / Groepen > RADIUS > Servergroepen > + Add.


Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Licensing
Configuration > Security > AAA
+ AAA Wizard
Servers / Groups
AAA Method List
AAA Advanced
+ Add
Delete
RADIUS
TACACS+
Servers
Server Groups
Name
Server 1
Server 2



Stap 3. Maak een lijst met verificatiemethoden. **Van GUI:** Navigeer naar Configuratie > Beveiliging > AAA > AAA-methodelijst > Verificatie > + Toevoegen


Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Configuration > Security > AAA
+ AAA Wizard
Servers / Groups
AAA Method List
Authentication
Authorization
+ Add
Name



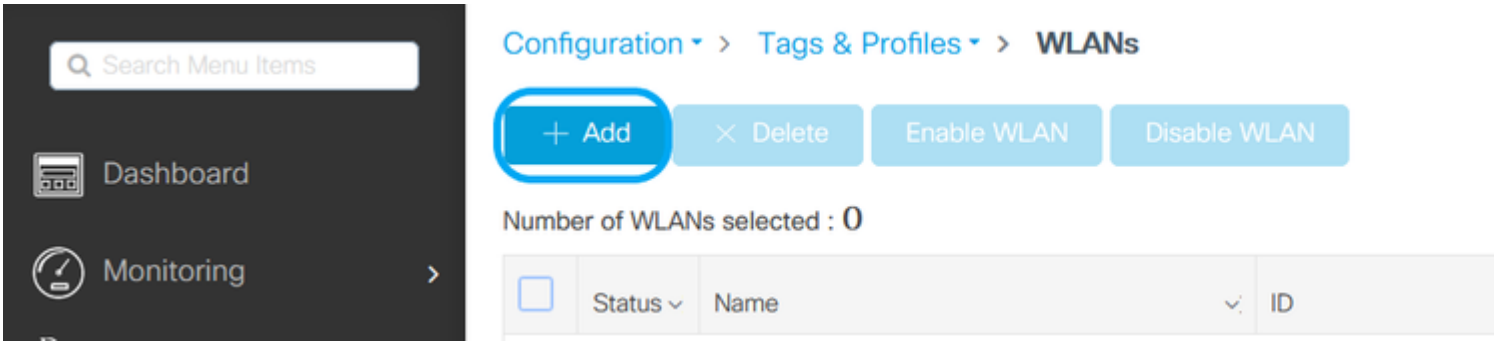
Van CLI:

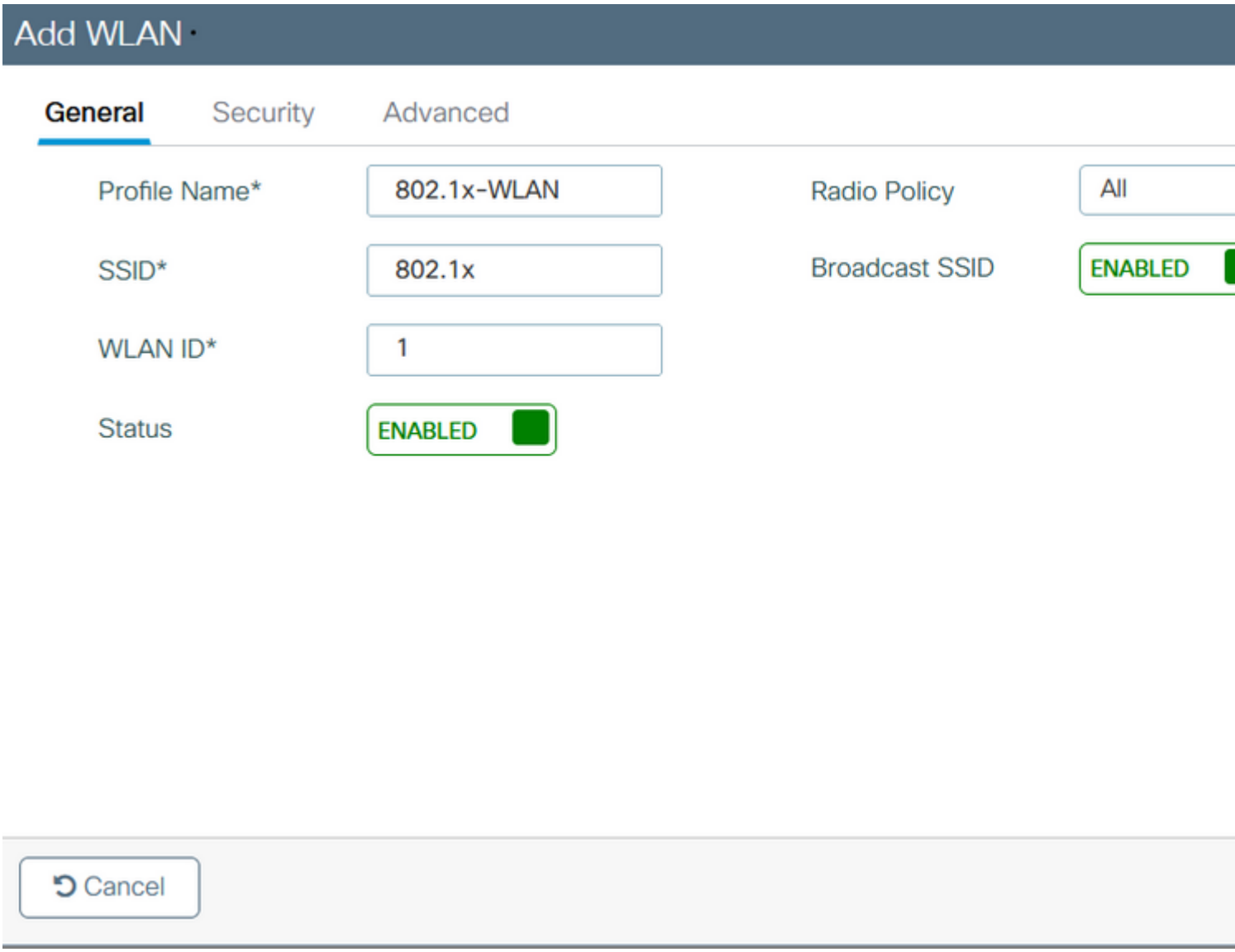
```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
```

```
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

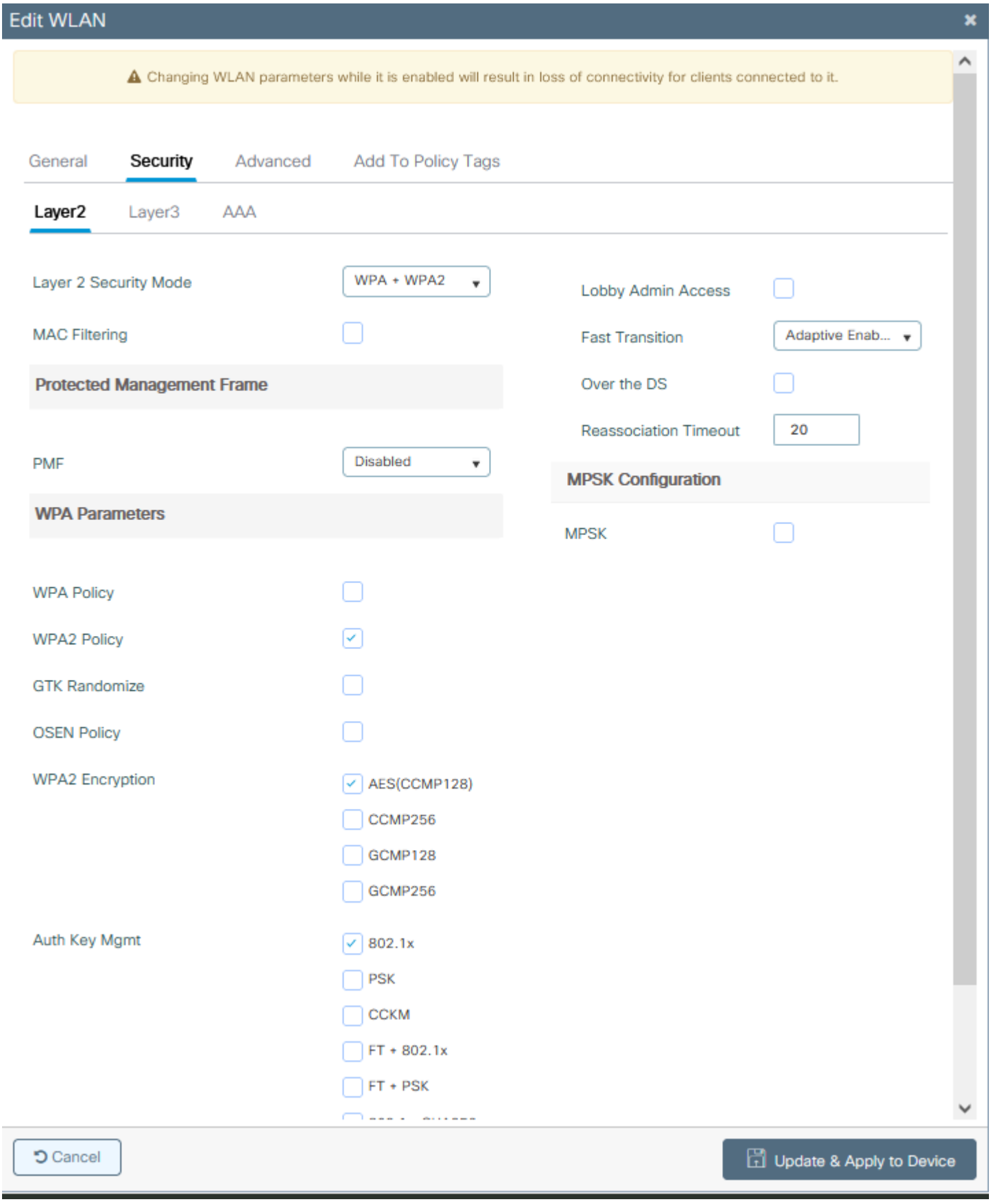
WLAN-configuratie

Stap 1. **Van GUI:** Navigeer naar Configuration > Wireless > WLANâ€™s en klik op +Add om een nieuw WLAN te maken en voer de WLAN-informatie in. Klik vervolgens op Toepassen op apparaat.



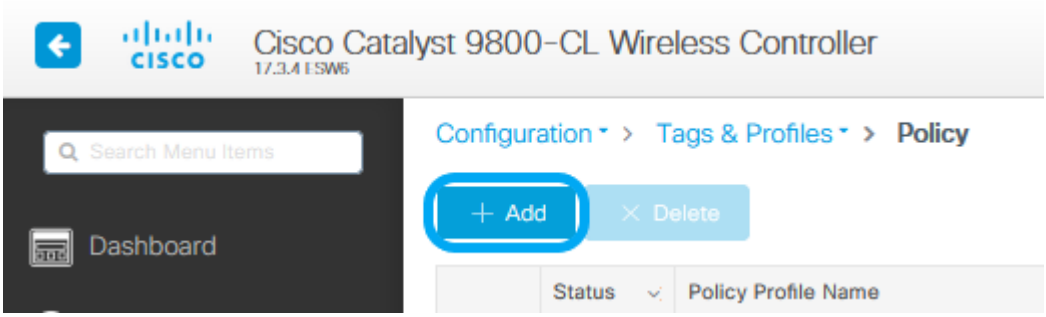


Stap 2. **Van GUI:** Navigeer aan het tabblad Security om de Layer 2/Layer 3-beveiligingsmodus te configureren zolang de coderingsmethode en de verificatielijst in het geval 802.1x in gebruik is. Klik vervolgens op Bijwerken en toepassen op apparaat.

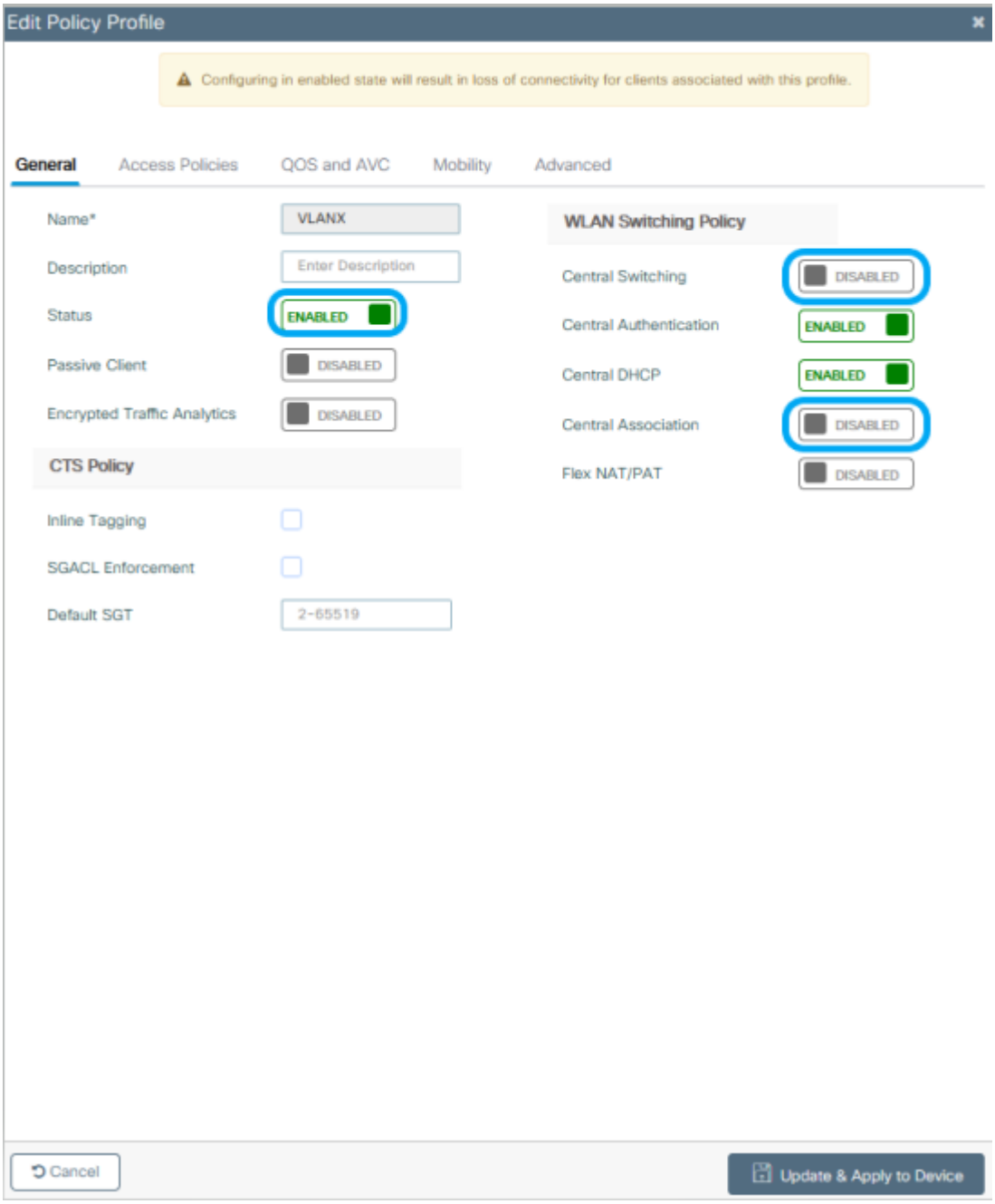


Configuratie van beleidsprofiel

Stap 1. **Van GUI:** Navigeer aan Configuratie > Markeringen & Profielen > Beleid en klik +Add om een Beleidsprofiel te creëren.



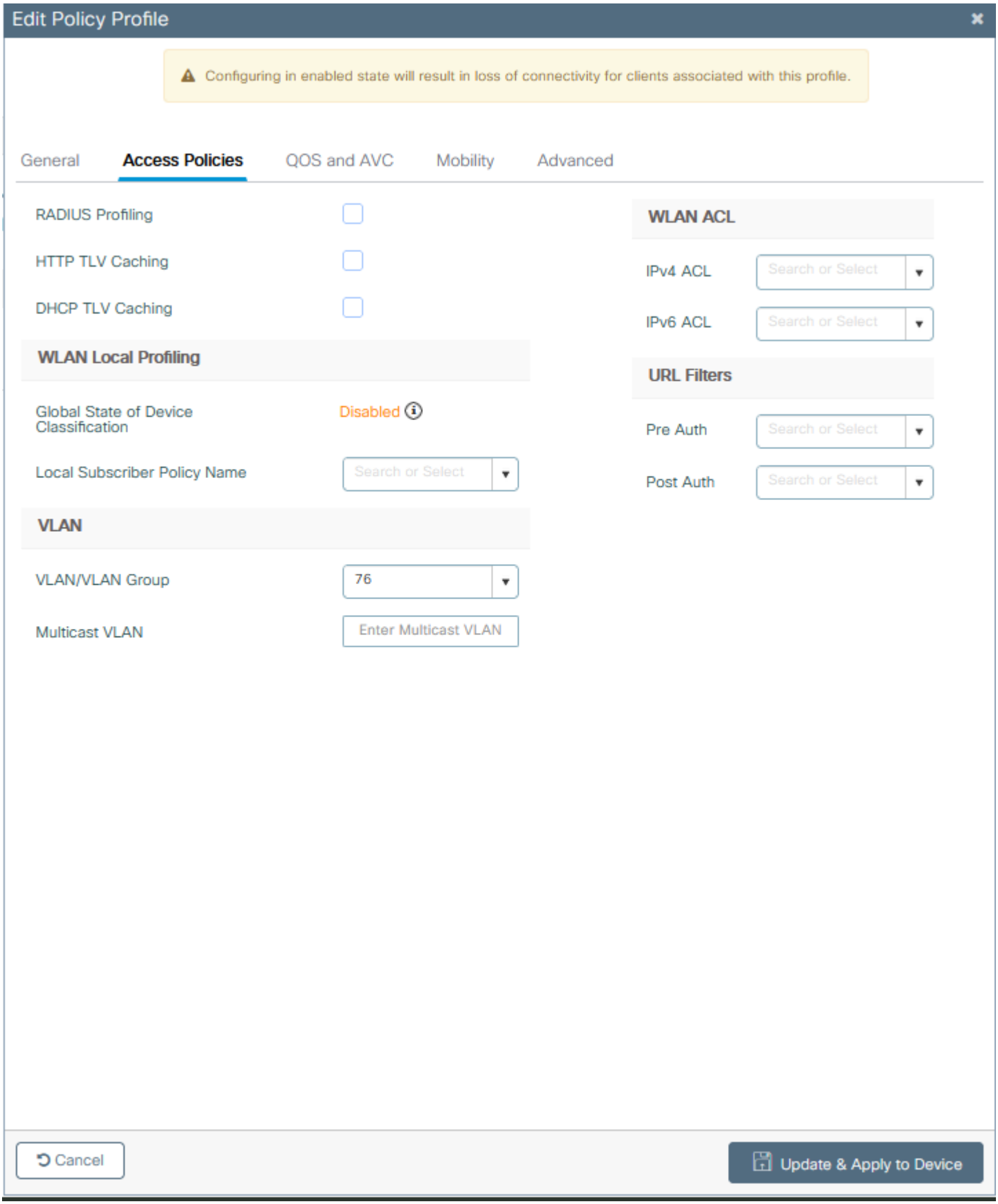
Stap 2. Voeg de naam toe en vink het vakje Central Switching uit. Bij deze installatie wordt de clientverificatie door de controller verwerkt en worden de clientgegevenspakketten van FlexConnect Access Point switches lokaal verwerkt.



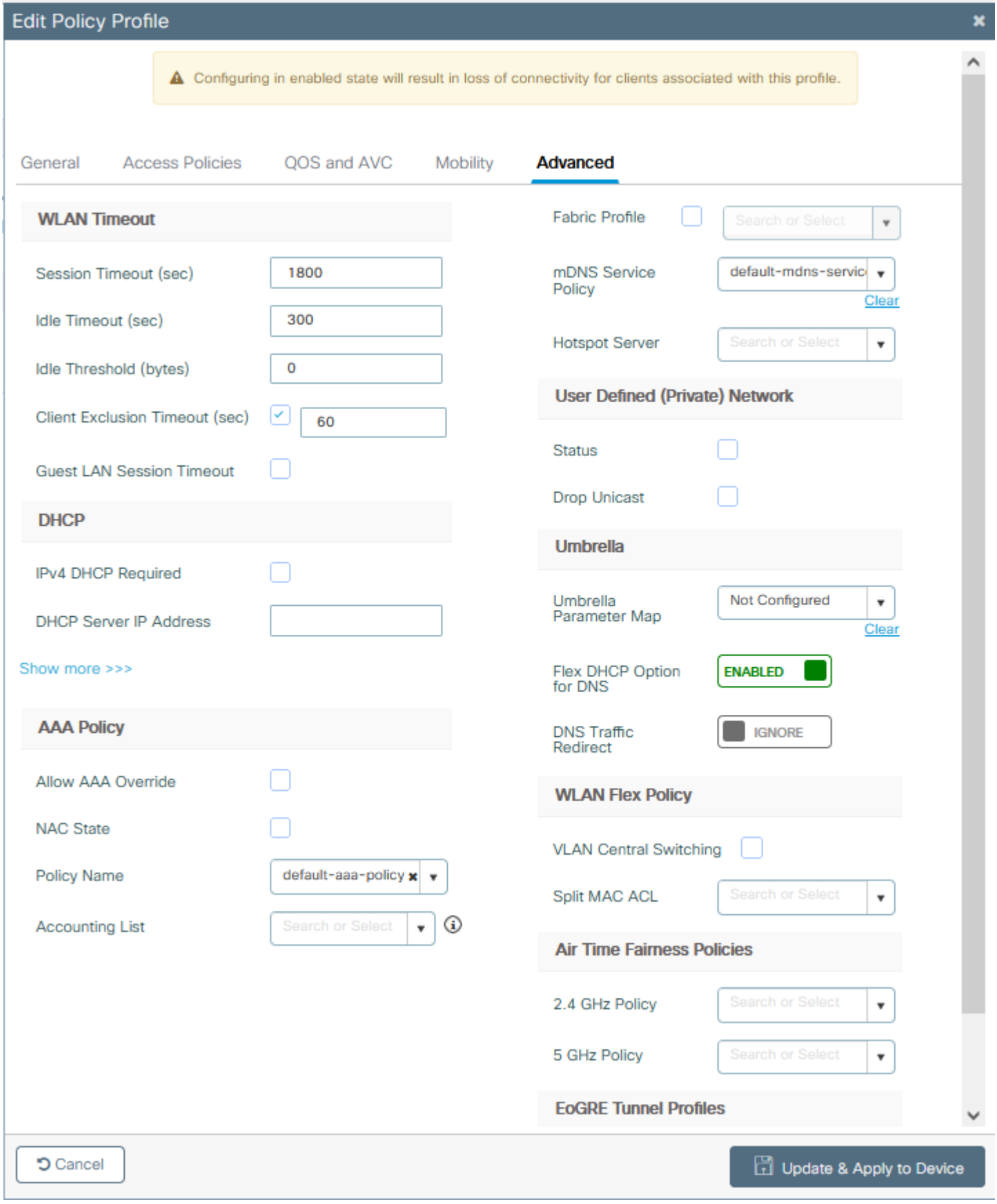
Opmerking: associatie en switching moeten altijd gekoppeld zijn, als centrale switching uitgeschakeld is moet centrale associatie ook uitgeschakeld worden op alle beleidsprofielen wanneer Flexconnect AP's worden gebruikt.

Stap 3. **Van GUI:** Navigeer naar het tabblad Toegangsbeleid om het VLAN toe te wijzen waaraan de draadloze clients kunnen

worden toegewezen wanneer zij standaard verbinding maken met dit WLAN.
U kunt één VLAN-naam in de vervolgkeuzelijst selecteren of als beste praktijk handmatig een VLAN-id typen.

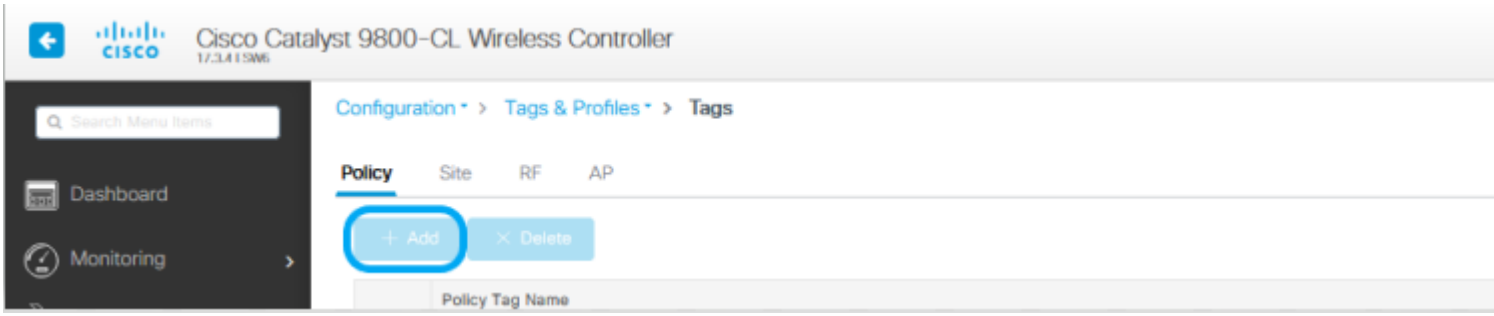


Stap 4. **Van GUI:** Navigeer naar het tabblad Advanced om de WLAN-timeouts, DHCP, WLAN Flex Policy en AAA-beleid te configureren voor het geval ze in gebruik zijn. Klik vervolgens op Bijwerken en toepassen op apparaat.

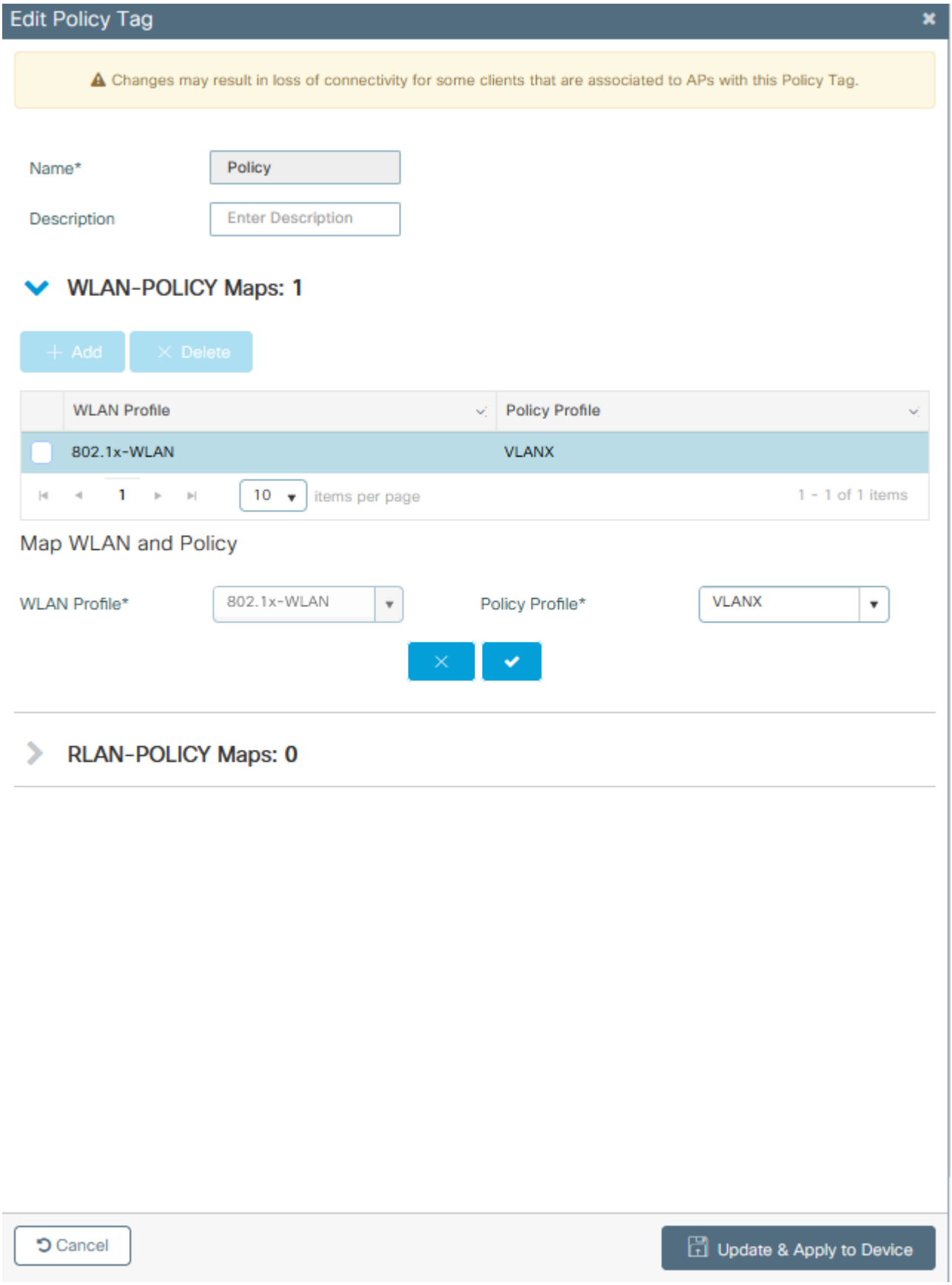


Configuratie van beleidstag

Stap 1. **Van GUI:** Navigeer aan Configuratie > Markeringen & Profielen > Markeringen > Beleid > +Add.

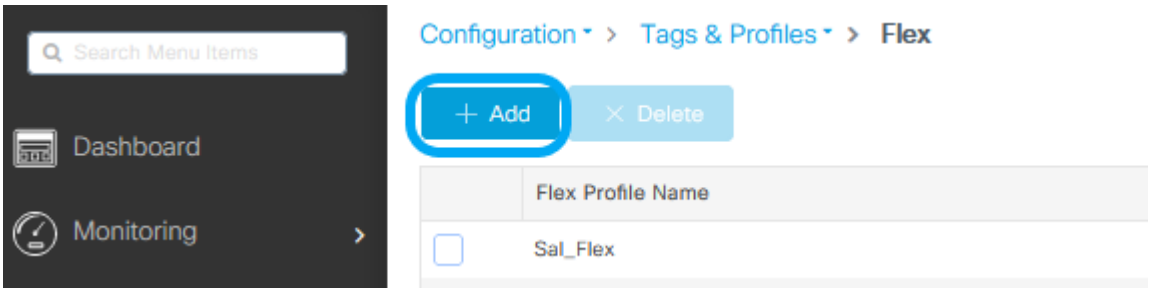


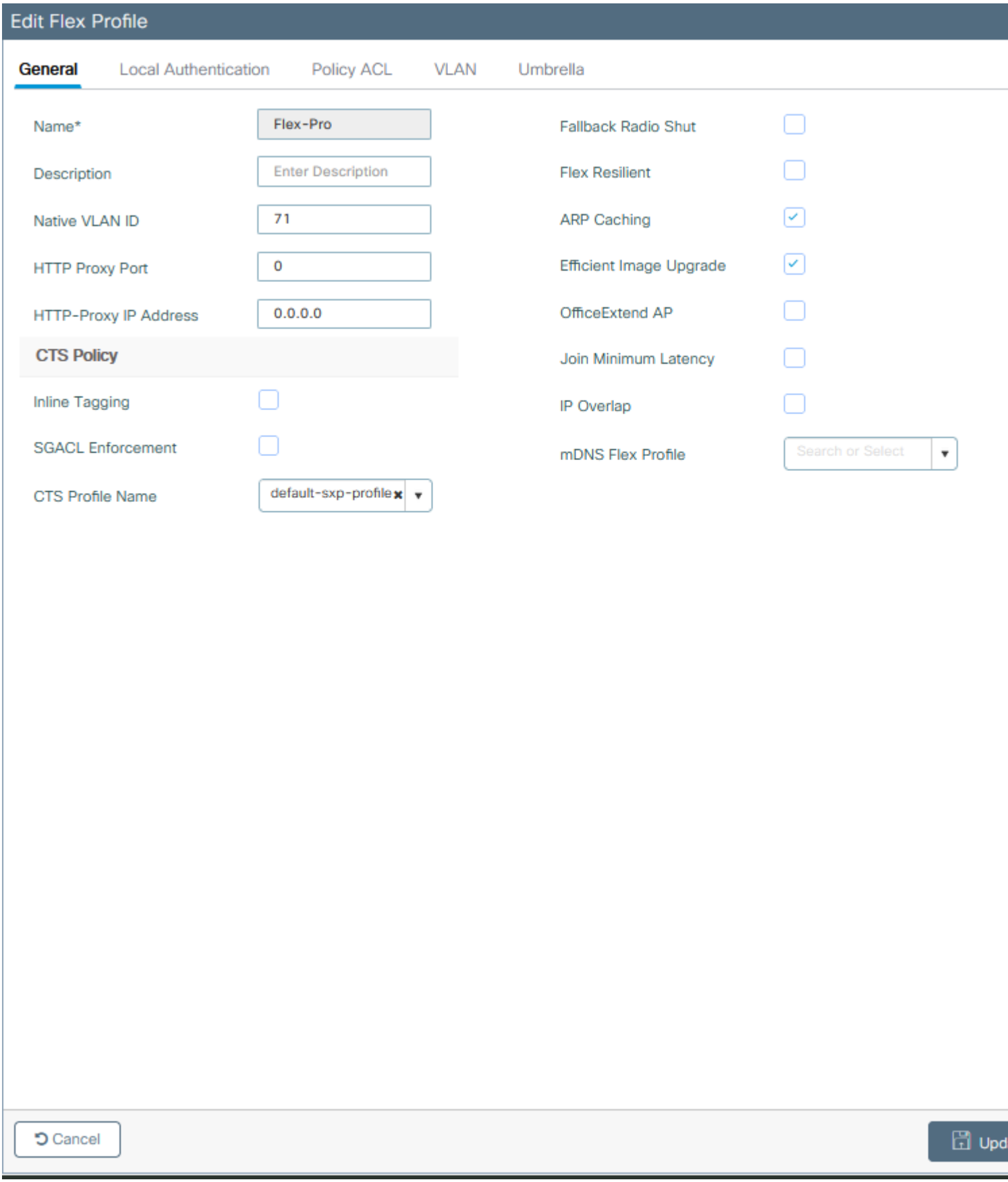
Stap 2. Wijs een naam toe en geef het beleidsprofiel en het WLAN-profiel dat u eerder hebt gemaakt, in kaart.



Flex-profielconfiguratie

Stap 1. **Van GUI:** Navigeer aan Configuratie > Markeringen & Profielen > Flex en klik +Add om nieuwe te creëren.

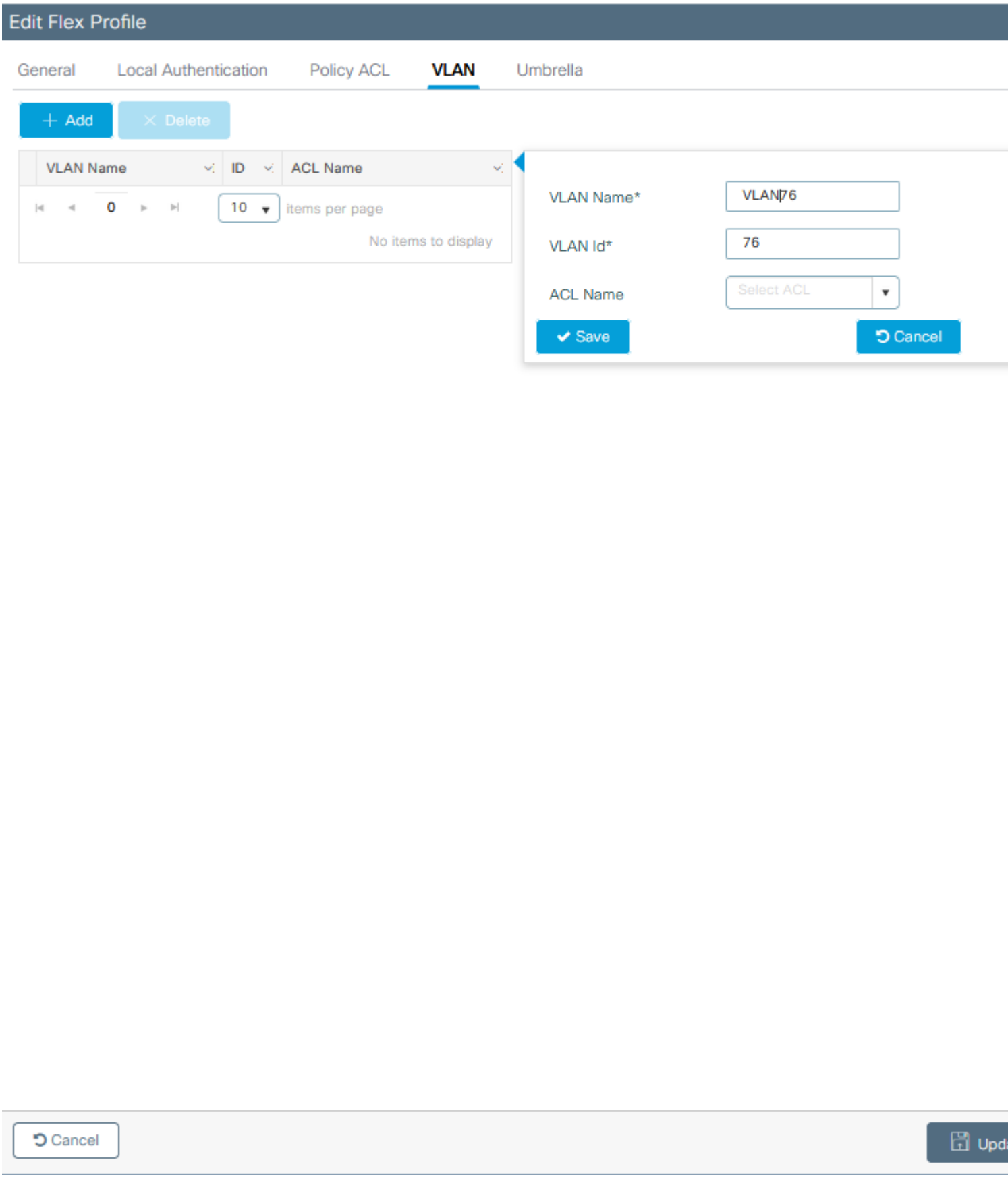

Search Menu Items
Dashboard
Monitoring
Configuration
Tags & Profiles
Flex
Add
Delete
Flex Profile Name
Sal_Flex



Opmerking: Native VLAN-id verwijst naar het VLAN dat wordt gebruikt door de APâ€™s die dit Flex Profile kunnen toewijzen, en het moet dezelfde VLAN-id zijn die is geconfigureerd als native op de switch-poort waarop de APâ€™s zijn aangesloten.

Stap 2. Voeg onder het tabblad VLAN de benodigde VLANâ€™s toe, de VLANâ€™s die standaard aan het WLAN zijn toegewezen via een beleidsprofiel of de VLANâ€™s die door een RADIUS-server worden gedrukt. Klik vervolgens op Bijwerken

en toepassen op apparaat.

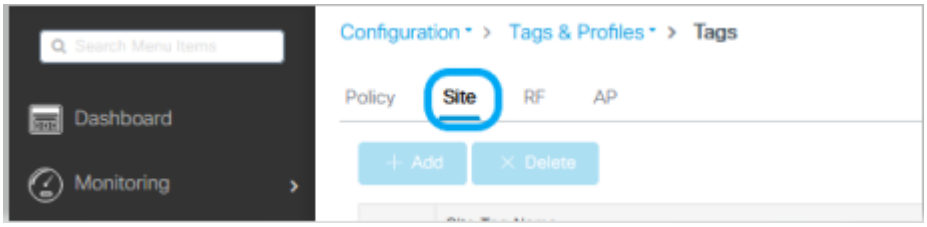


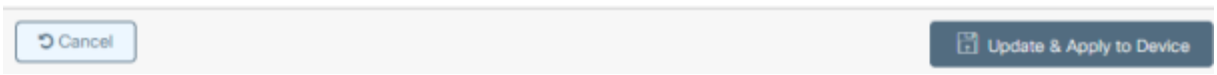
Opmerking: voor beleidsprofiel, wanneer u het standaard VLAN selecteert dat aan de SSID is toegewezen. Als u een VLAN-naam in die stap gebruikt, zorg er dan voor dat u dezelfde VLAN-naam gebruikt in de Flex Profile Configuration, anders kunnen clients geen verbinding maken met het WLAN.

Opmerking: om een ACL voor flexConnect met AAA-opheffing te configureren, moet u deze alleen configureren op "beleids-ACL". Als ACL is toegewezen aan een specifiek VLAN, moet u ACL toevoegen wanneer u VLAN toevoegt en vervolgens ACL toevoegen op "beleid-ACL".

Configuratie van sitetag

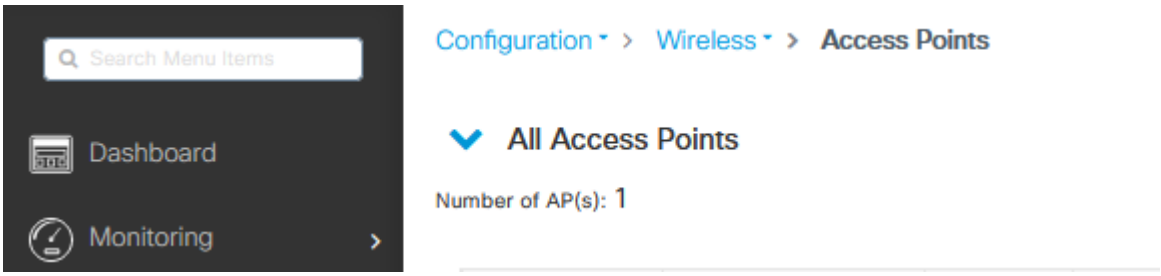
Stap 1. **Van GUI:** Navigeren naar Configuratie > Tags & profielen > Tags > Site en klik op +Add om een nieuwe Site tag te maken. Schakel het vakje Local Site inschakelen uit om AP's toe te staan lokaal switch te maken van het clientgegevensverkeer en het eerder gemaakte Flex Profile toe te voegen.

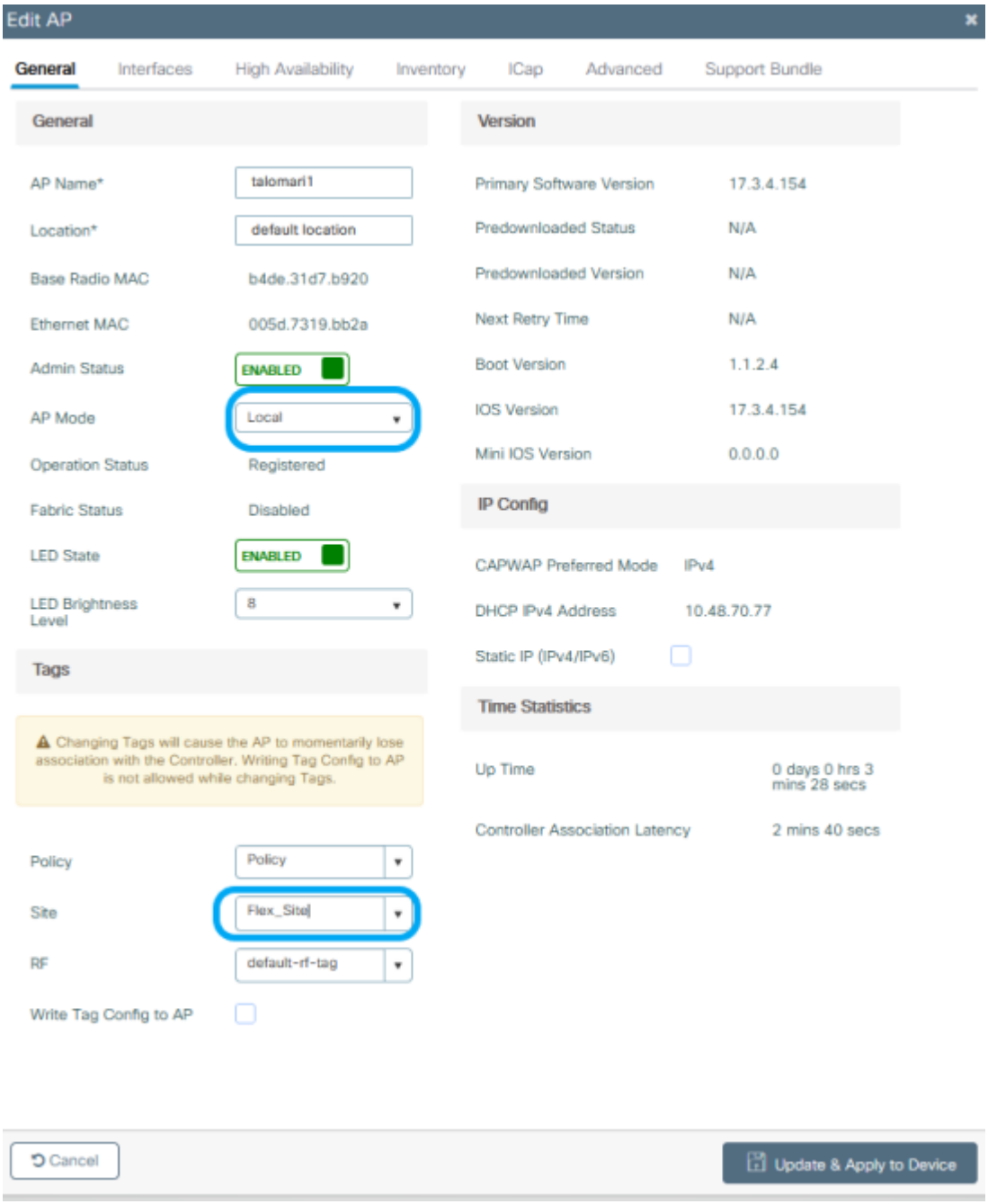




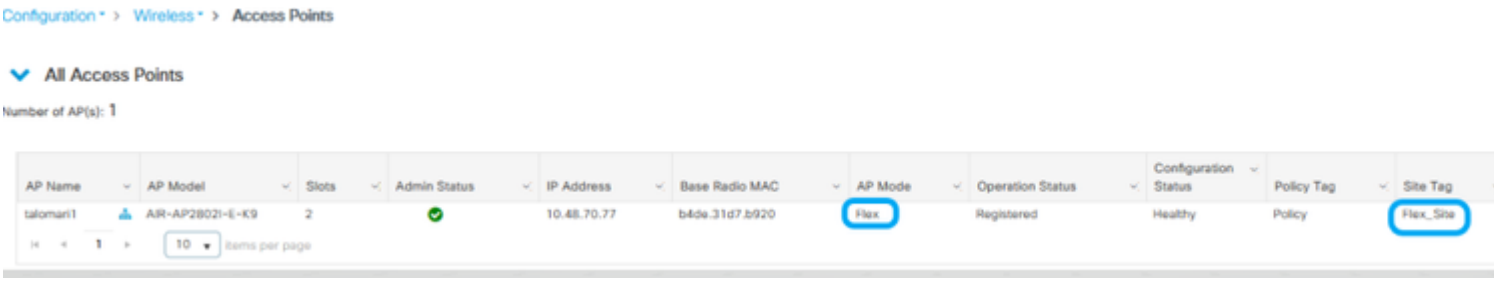
Opmerking: aangezien de optie Local Site inschakelen is uitgeschakeld, kunnen de toegangspunten die deze sitetag toegewezen krijgen, worden geconfigureerd als FlexConnect-modus.

Stap 2. **Van GUI:** Navigeer naar Configuration > Wireless > Access points > AP-naam om de Site Tag en Policy Tag aan een gekoppeld AP toe te voegen. Dit kan de AP ertoe bewegen zijn CAPWAP-tunnel opnieuw te starten en terug te keren naar de 9800 WLC.



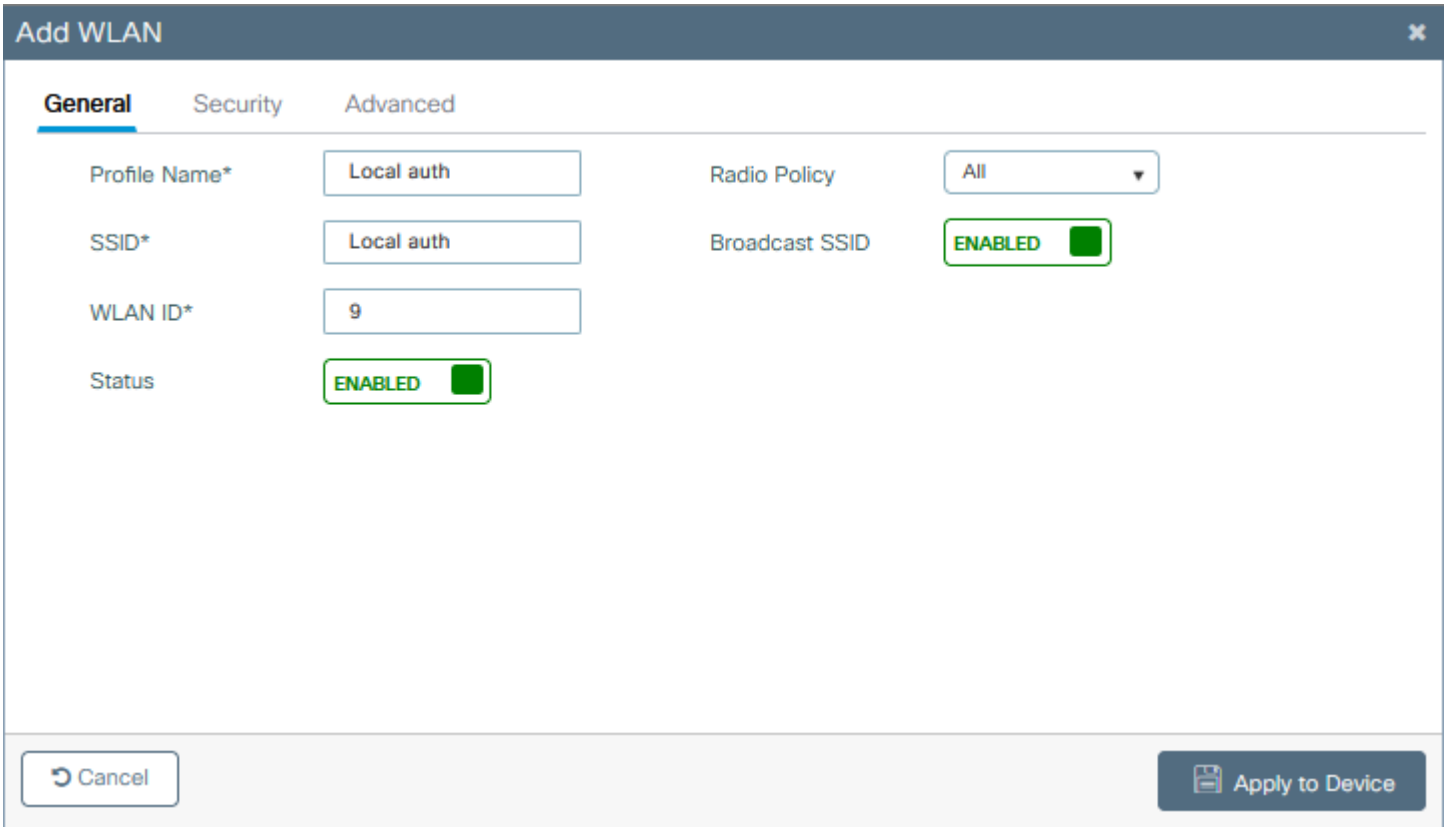


Wanneer het toegangspunt weer is aangesloten, ziet u dat het toegangspunt zich nu in de FlexConnect-modus bevindt.

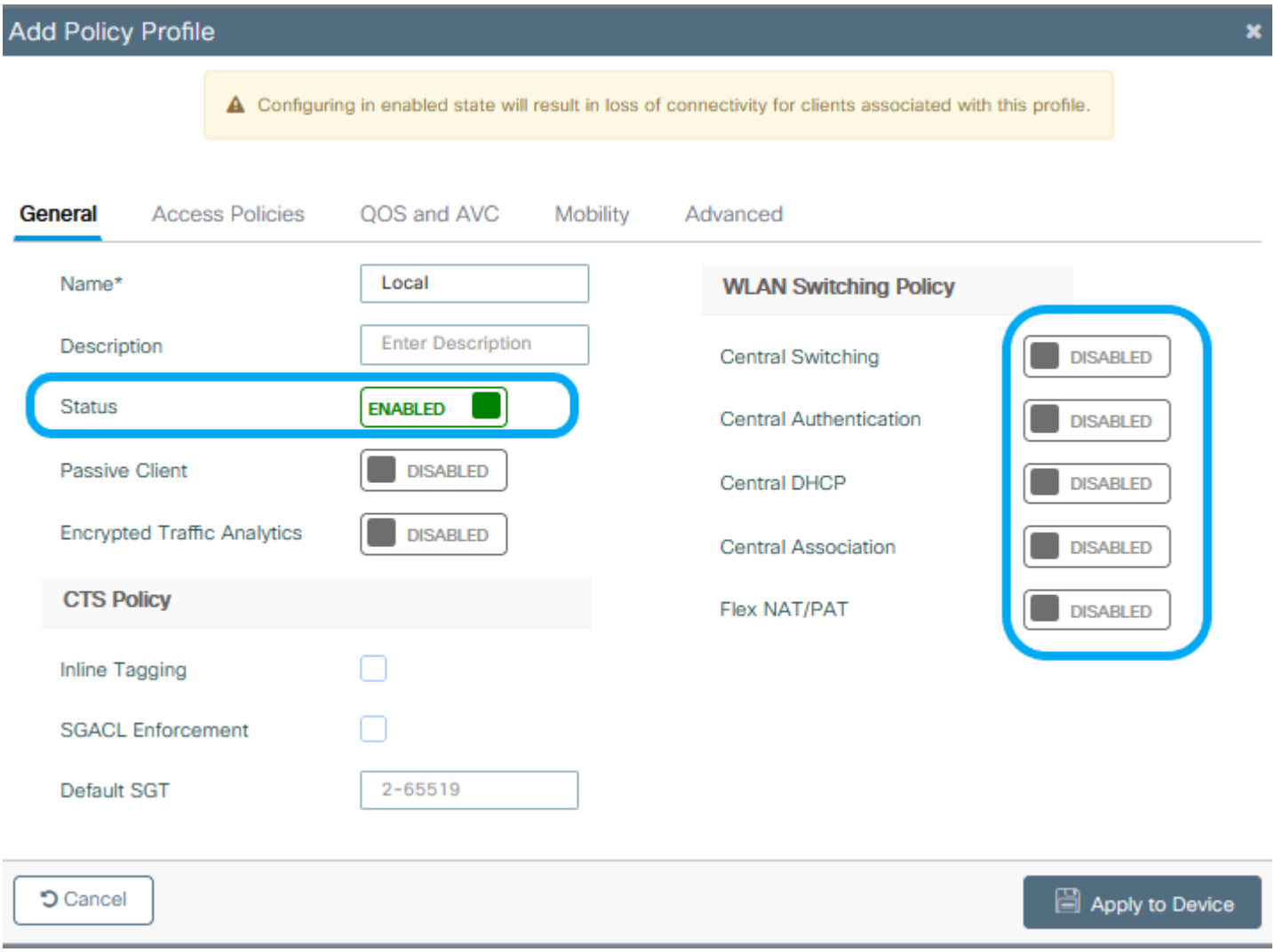


Lokale verificatie met externe RADIUS-server

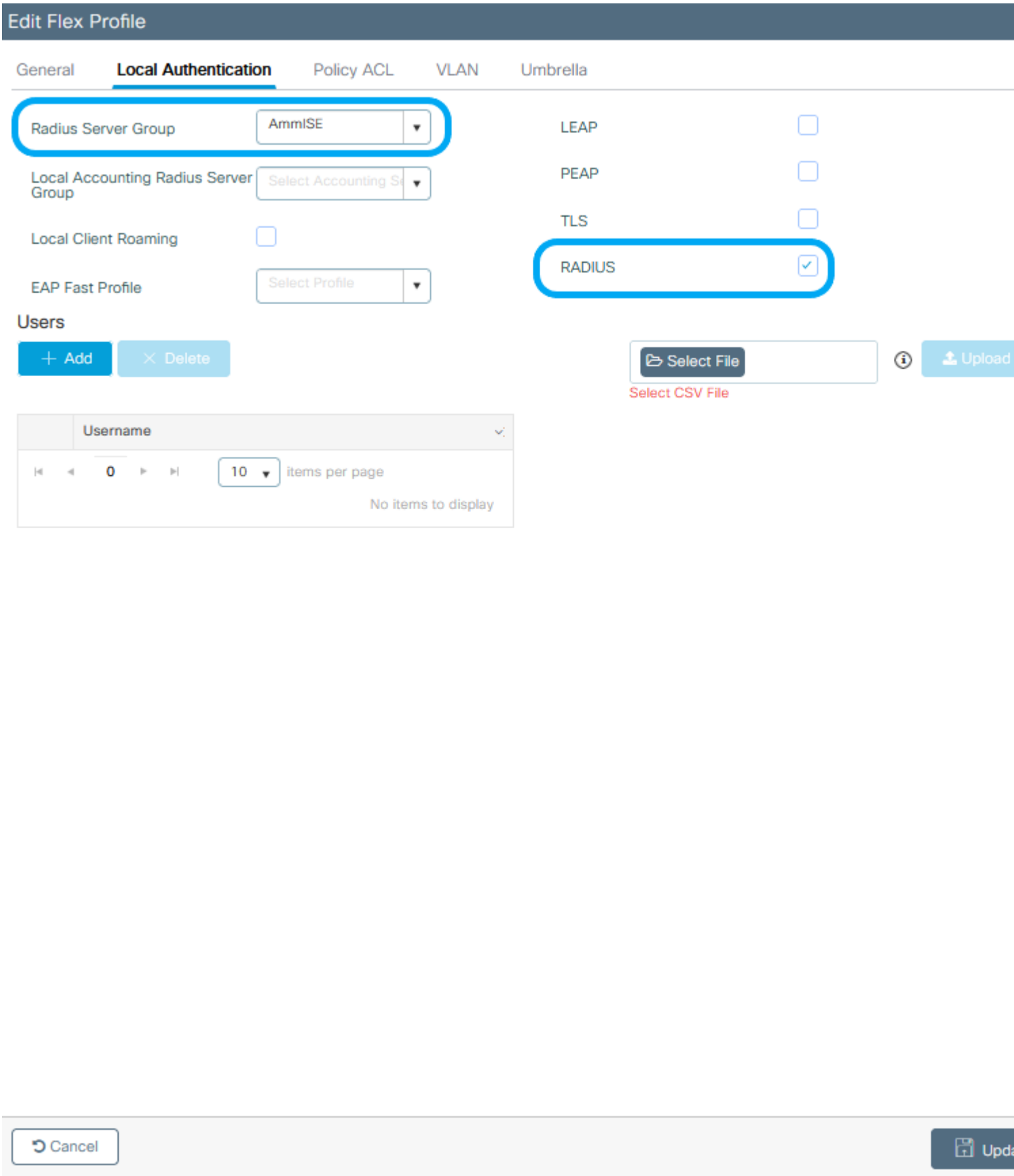
Stap 1. Voeg het toegangspunt als netwerkapparaat toe aan de RADIUS-server. Raadpleeg bijvoorbeeld Hoe u Identity Service Engine (ISE) gebruikt als RADIUS-server
Stap 2. Maak een WLAN.
De configuratie kan hetzelfde zijn als de configuratie die eerder is geconfigureerd.



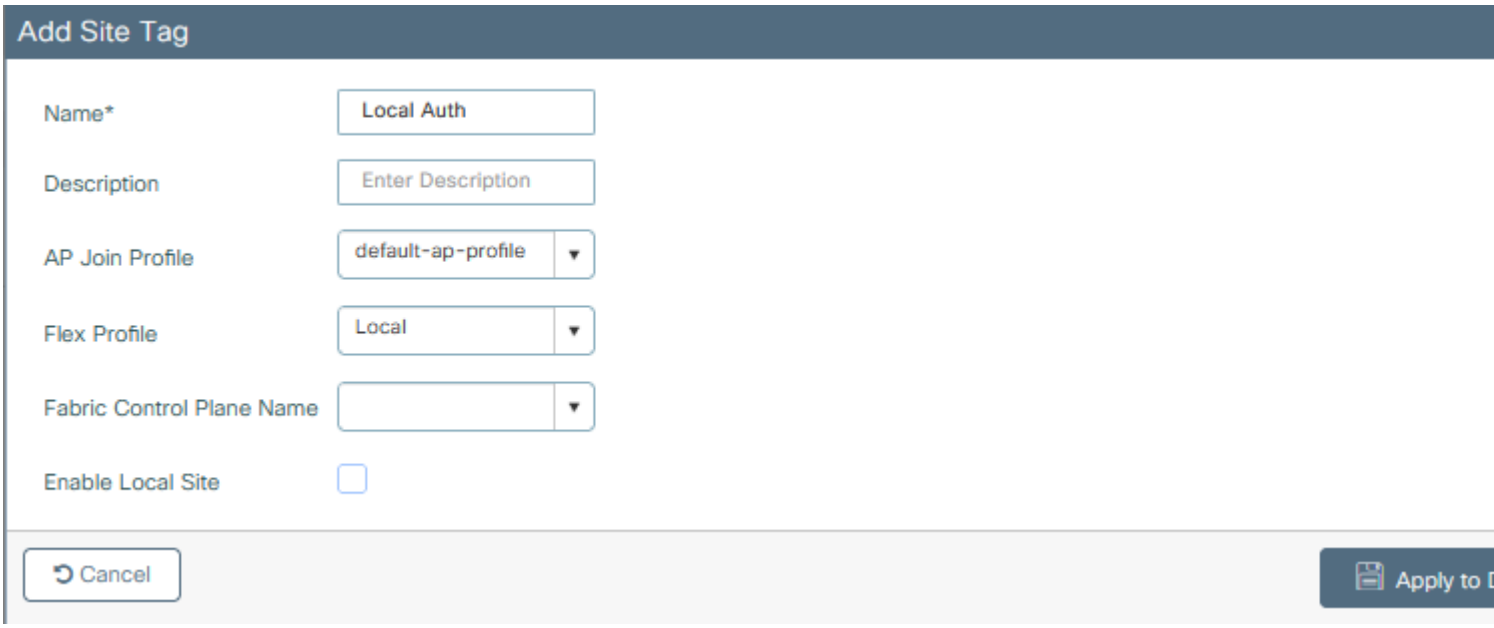
Stap 3. Configuratie beleidsprofiel.
U kunt een nieuwe maken of de eerder geconfigureerde software gebruiken. Schakel deze keer de selectievakjes Central Switching, Central Verification, Central DHCP en Central Association Enable uit.



Stap 4. Configuratie van beleidstags.
Associeer het geconfigureerde WLAN en het gemaakte beleidsprofiel.
Stap 5. Configuratie Flex-profiel.
Maak een Flex Profile, navigeer naar het tabblad Local Authentication, configureer de Radius Server Group en controleer het vakje RADIUS.



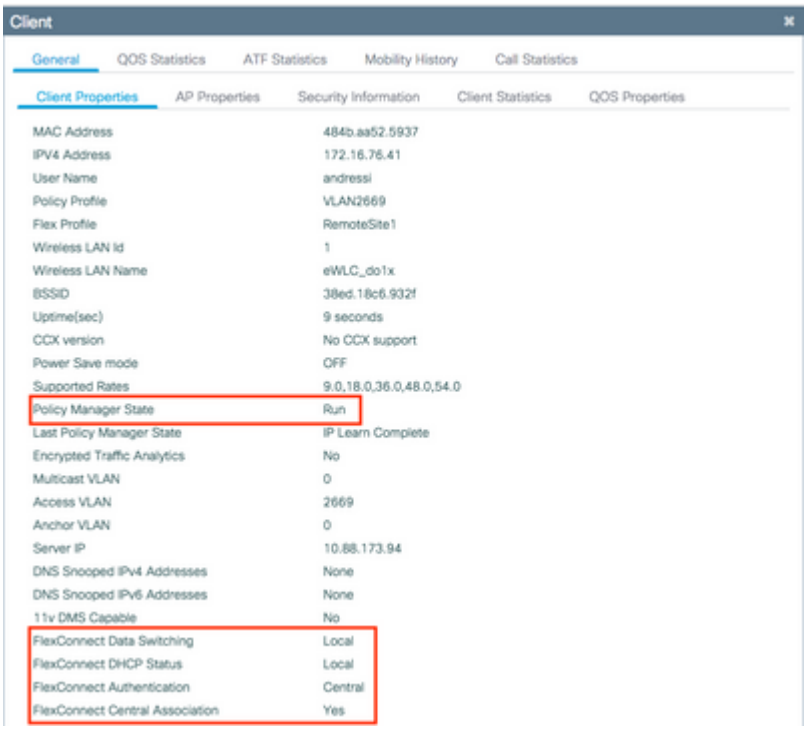
Stap 6. Configuratie van sitetag.
Configureer het Flex Profile dat in stap 5 is geconfigureerd en schakel het vakje Local Site inschakelen uit.



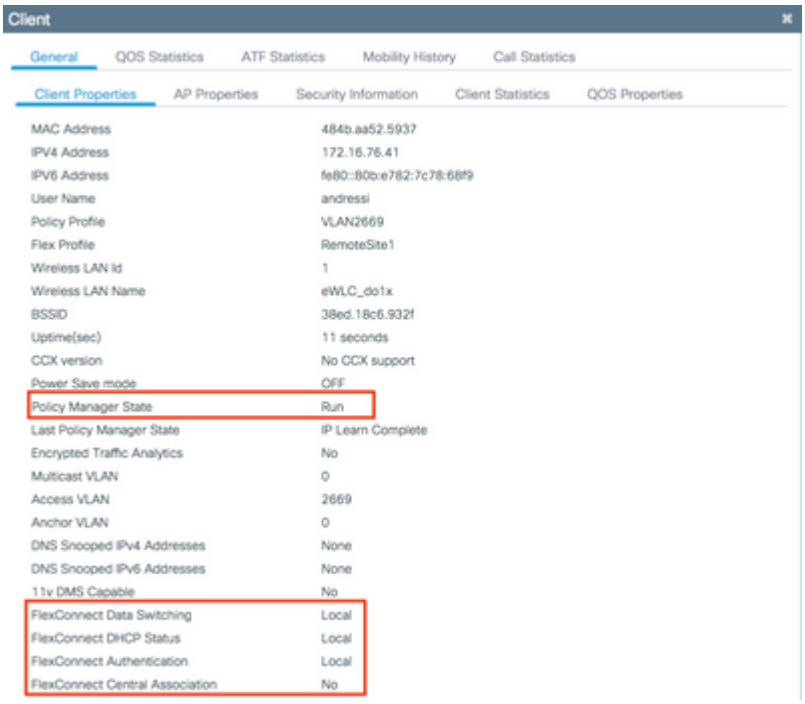
Verifiëren

Van GUI: Navigeer naar **Monitoring** > **Wireless** > **Clients** en bevestig de **Policy Manager-status** en de FlexConnect-parameters.

Centrale verificatie:



Lokale verificatie:



U kunt deze opdrachten gebruiken om de huidige configuratie te verifiëren:

Van CLI:

```
# show wlan { summary | id | name | all }
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

Problemen oplossen

WLC 9800 biedt ALTIJD-ON traceermogelijkheden. Dit zorgt ervoor dat alle aan de client gerelateerde fouten, waarschuwingen en meldingen op het niveau constant worden vastgelegd en u kunt logbestanden bekijken voor een incident of storing nadat het is opgetreden.

> **Opmerking**: op basis van het volume van de gegenereerde logbestanden kunt u enkele uren teruggaan naar meerdere dagen.

Om de sporen te bekijken die 9800 WLC standaard heeft verzameld, kunt u via SSH/Telnet verbinding maken met de 9800 WLC en deze stappen doorlopen (zorg ervoor dat u de sessie aan een tekstbestand registreert).

Stap 1. Controleer de huidige controllertijd zodat u de logbestanden kunt volgen in de tijd terug naar toen het probleem zich voordeed.

Van CLI:

```
# show clock
```

Stap 2. Verzamel syslogs van de controllerbuffer of externe syslog zoals die door de systeemconfiguratie wordt gedicteerd. Dit geeft een snel overzicht van de systeemstatus en eventuele fouten.

Van CLI:

```
# show logging
```

Stap 3. Controleer of de debug-voorwaarden zijn ingeschakeld.

Van CLI:

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:


Packet Infra debugs:

Ip Address                                              Port
------------------------------------------------------|----------
```

> **Opmerking**: Als u een voorwaarde vermeld vindt, betekent het dat de sporen zijn ingelogd om het debug-niveau voor alle processen die de ingeschakelde voorwaarden (mac-adres, ip-adres enzovoort) tegenkomen. Dit zou het volume van de boomstammen doen toenemen. Daarom wordt aanbevolen alle voorwaarden te wissen wanneer niet actief debuggen

---

Stap 4. Als u aanneemt dat het mac-adres dat wordt getest niet als voorwaarde in Stap 3 is vermeld, verzamelt u de altijd beschikbare meldingen op het niveau voor het specifieke mac-adres.

Van CLI:

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<
```

U kunt de inhoud op de sessie weergeven of u kunt het bestand kopiëren naar een externe TFTP-server.

Van CLI:

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Voorwaardelijke debug en radio actief spoor

Als de altijd-on sporen u niet genoeg informatie geven om de trigger voor het probleem dat wordt onderzocht te bepalen, kunt u voorwaardelijke debugging inschakelen en Radio Active (RA)-spoor opnemen, dat debug level traces kan bieden voor alle processen die interacteren met de gespecificeerde voorwaarde (client mac-adres in dit geval). Om het voorwaardelijke zuiveren toe te laten, ga door deze stappen.

Stap 5. Zorg ervoor dat de debug-voorwaarden niet zijn ingeschakeld.

Van CLI:

```
# clear platform condition all
```

Stap 6. Schakel de debug-voorwaarde in voor het draadloze client-MAC-adres dat u wilt controleren.

Met deze opdracht wordt het opgegeven MAC-adres gedurende 30 minuten (1800 seconden) bewaakt. U kunt deze tijd optioneel tot 2085978494 seconden verlengen.

Van CLI:

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

Opmerking: als u meer dan één client tegelijk wilt bewaken, voert u de opdracht debug wireless mac <aaaa.bbbb.ccc> per mac-adres uit.

Opmerking: U ziet de output van de client activiteit niet op de terminal sessie, omdat alles intern wordt gebufferd om later bekeken te worden.

Stap 7. Reproduceer het probleem of gedrag dat u wilt controleren.

Stap 8. Stop de debugs als het probleem wordt gereproduceerd voordat de standaard of de ingestelde monitortijd is ingesteld.

Van CLI:

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Zodra de monitor-tijd is verstreken of de debug-radio is gestopt, genereert de 9800 WLC een lokaal bestand met de naam:

ra_trace_MAC_aabbcccc_HMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Stap 9. Verzamel het bestand van de mac-adresactiviteit. U kunt het spoor .log naar een externe server kopiëren of de uitvoer direct op het scherm weergeven.

Controleer de naam van het RA traces bestand

Van CLI:

```
# dir bootflash: | inc ra_trace
```

Kopieert het bestand naar een externe server:

Van CLI:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d
```

Geef de inhoud weer:

Van CLI:

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Stap 10. Als de worteloorzaak nog niet duidelijk is, verzamel de interne logboeken die een meer breedsprakige mening van debug niveaulogboeken zijn. U hoeft de client niet opnieuw te debuggen omdat u een gedetailleerde kijk hebt genomen op debug-logbestanden die al zijn verzameld en intern zijn opgeslagen.

Van CLI:

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra
```

> **Opmerking**: deze opdrachtoutput geeft sporen voor alle registratieniveaus voor alle processen en is vrij omvangrijk. Neem contact op met Cisco TAC om te helpen bij het doorlopen van deze sporen.

U kunt de Ra-internal-FILENAME.txt kopiëren naar een externe server of de uitvoer rechtstreeks op het

scherm weergeven.

Kopieert het bestand naar een externe server:

Van CLI:

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Geef de inhoud weer:

Van CLI:

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Stap 11. Verwijder de debug-voorwaarden.

Van CLI:

```
# clear platform condition all
```

Opmerking: Zorg ervoor dat u altijd de debug-voorwaarden verwijdert na een probleemoplossing sessie.

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.