Configureer de MAC-verificatie SSID op Catalyst 9800 draadloze controllers

Inhoud

Inleiding

Dit document beschrijft hoe u een Wireless Local Area Network (WLAN) kunt instellen met MAC-verificatiebeveiliging op Cisco Catalyst 9800 WLC.

Voorwaarden

Vereiste

Cisco raadt kennis van de volgende onderwerpen aan:

- MAC-adres
- Cisco Catalyst 9800 Series wireless controllers
- Identity Service Engine (ISE)

Gebruikte componenten

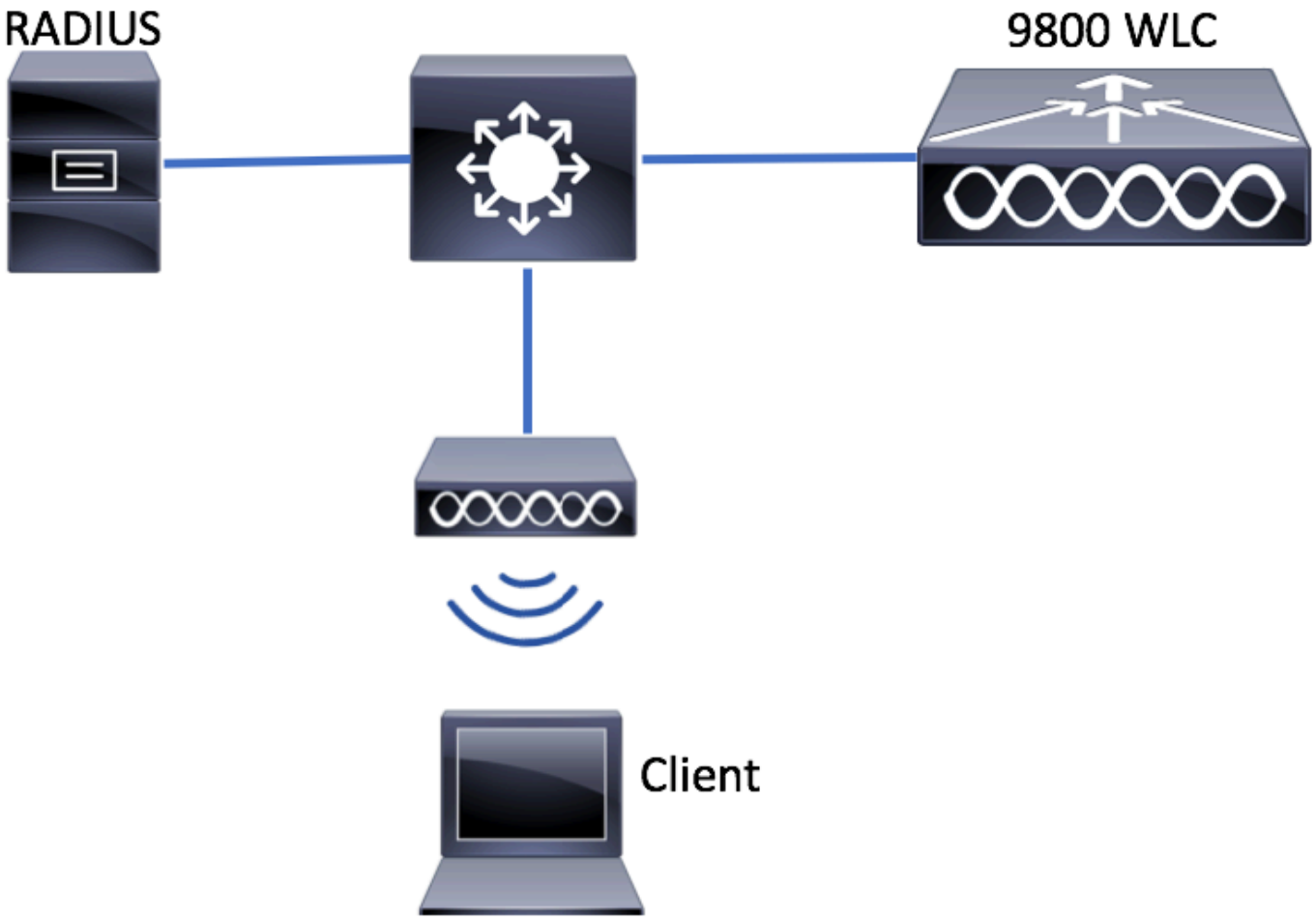
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS® XE Gibraltar v16.12
- ISE v2.2

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



AAA-configuratie op 9800 WLC

Clients met externe server verifiëren

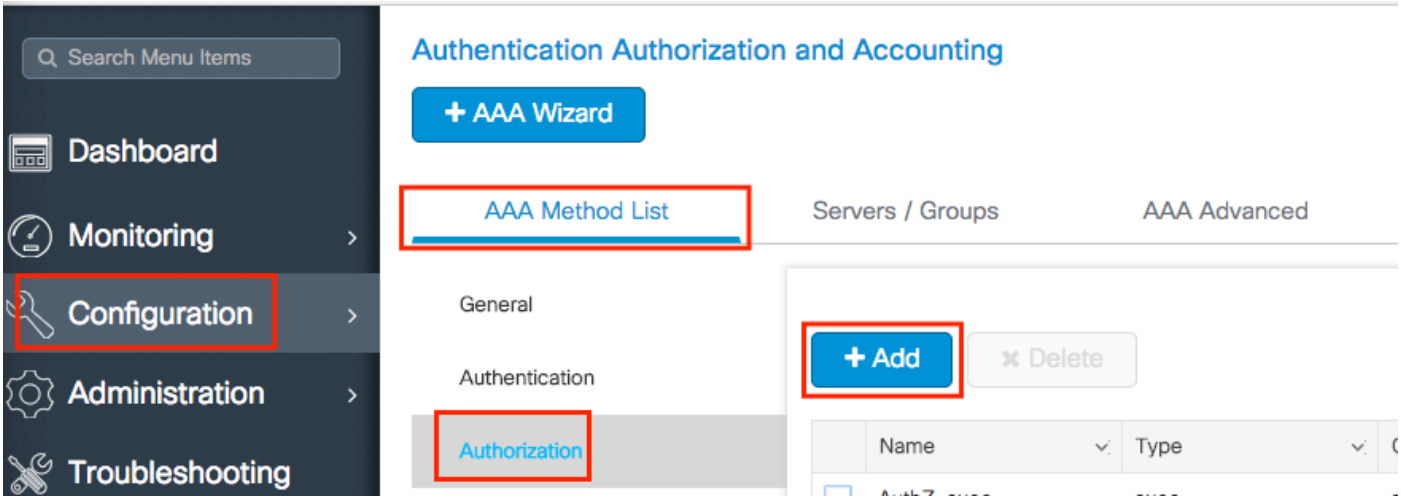
GUI:

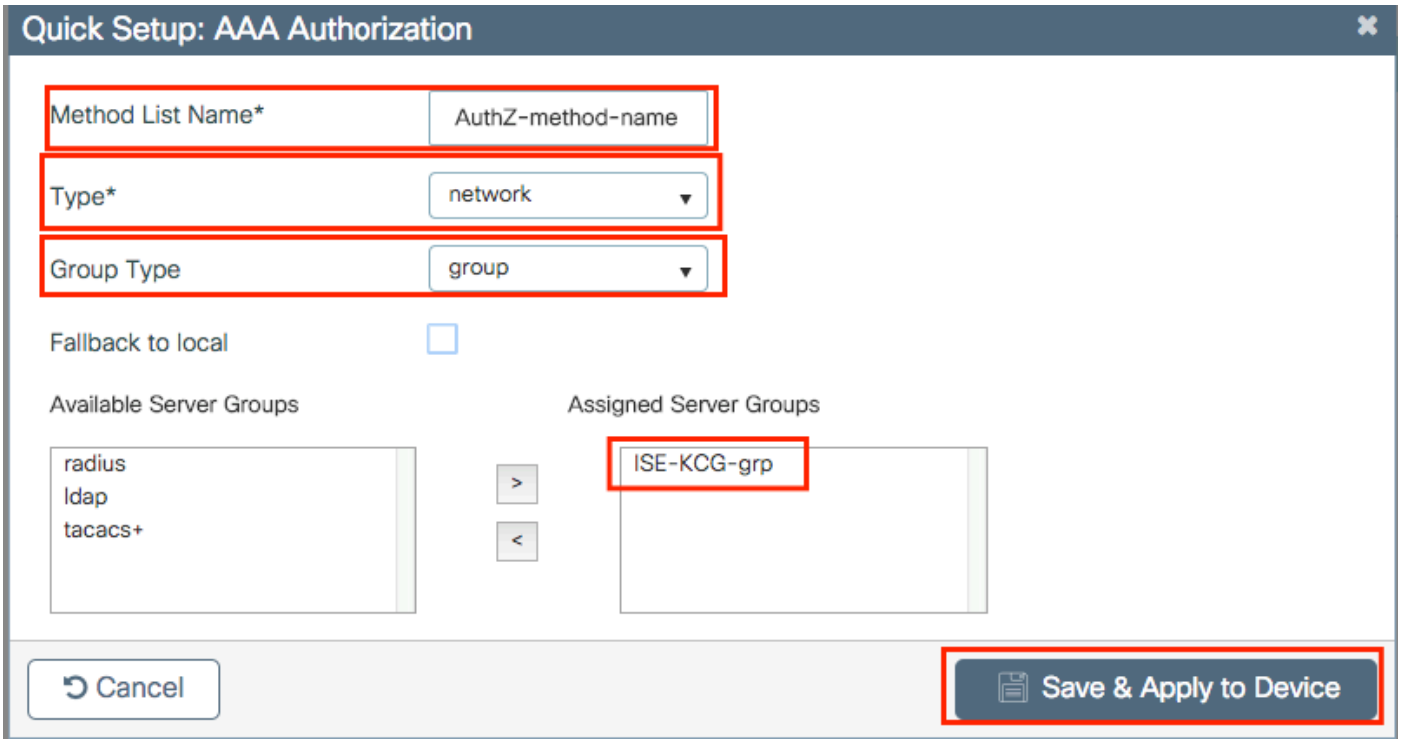
Lees stap 1-3 van de sectie 'AAA Configuration on 9800 WLCs' via deze link:

AAA-configuratie op 9800 Series WLC

Stap 4. Maak een autorisatienetwerkmethode aan.

Naar navigeren Configuration > Security > AAA > AAA Method List > Authorization > + Add en creëer het.





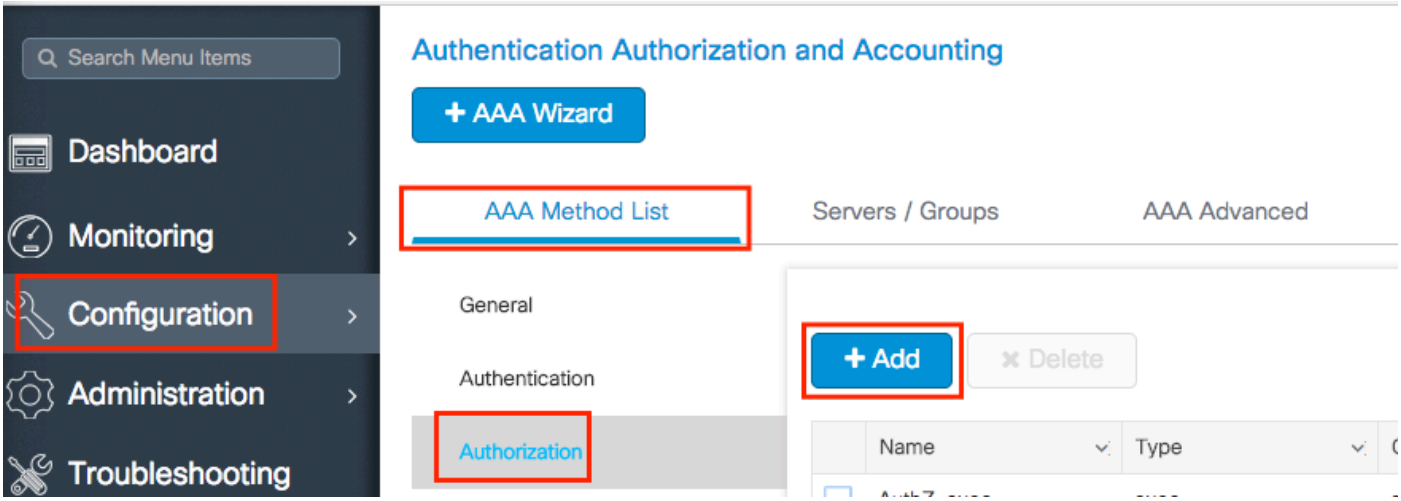
CLI:

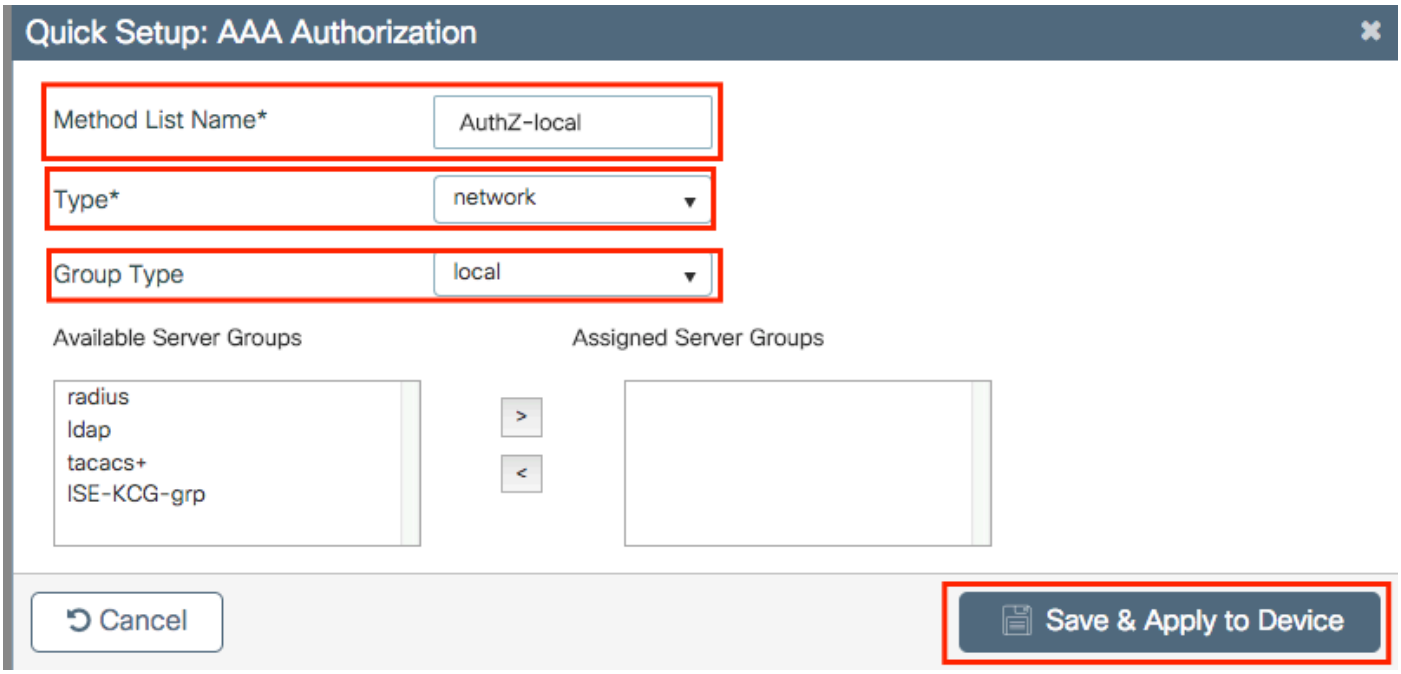
```
# config t
# aaa new-model

# 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 authorization network <AuthZ-method-name> group <radius-grp-name>
```

Clients lokaal verifiëren

Maak een lokale autorisatienetwerkmethode aan.

Naar navigeren Configuration > Security > AAA > AAA Method List > Authorization > + Add en creëer het.





CLI:

```
# config t
# aaa new-model
# aaa authorization network AuthZ-local local
```

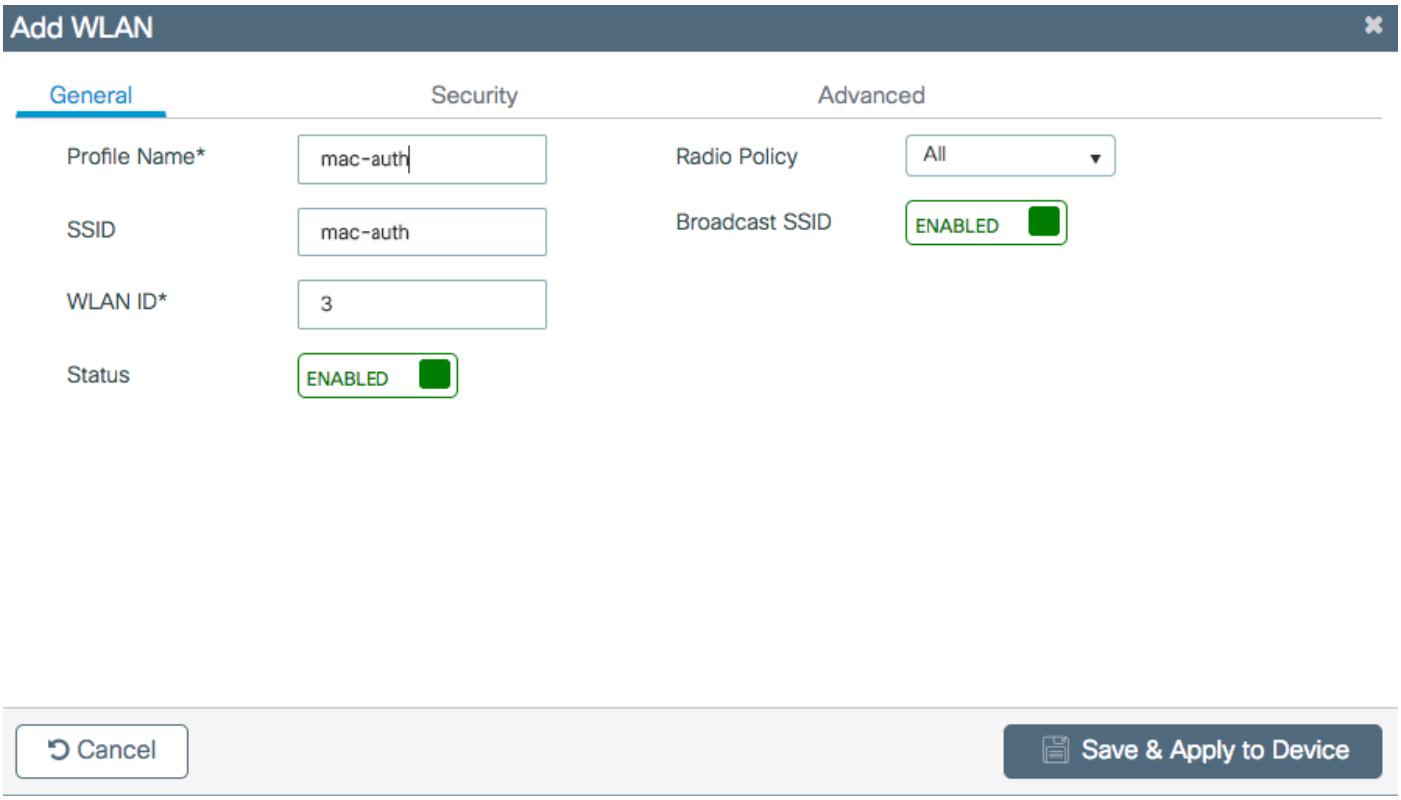
WLAN-configuratie

GUI:

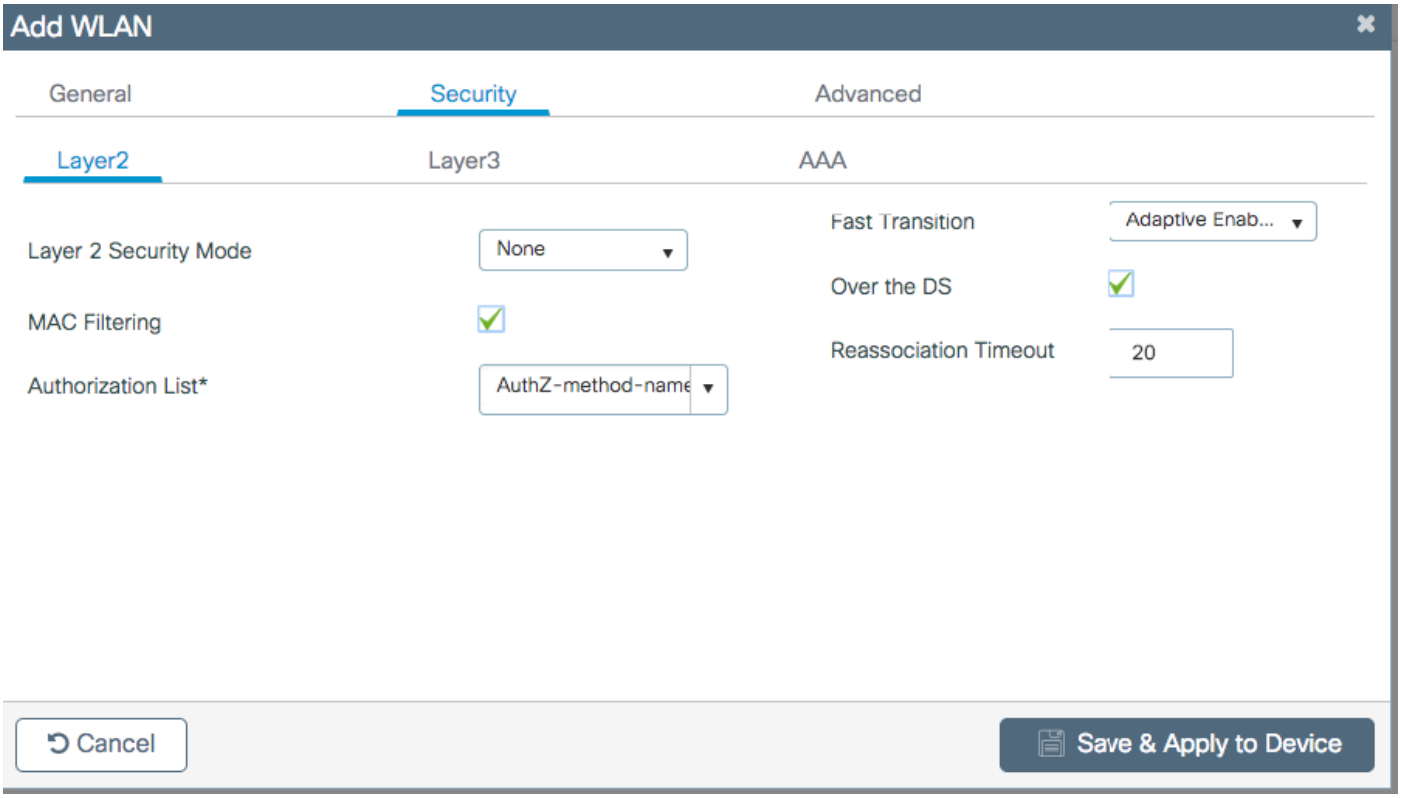
Stap 1. Maak het WLAN.

Naar navigeren Configuration > Wireless > WLANs > + Add en configureer het netwerk naar wens.

Stap 2. Voer de WLAN-informatie in.



Stap 3. Naar het Security tabblad en uitschakelen Layer 2 Security Mode en MAC Filtering. Van Authorization List, kies de autorisatiemethode die in de vorige stap is gemaakt. Klik vervolgens op Save & Apply to Device.



CLI:

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# mac-filtering <authZ-network-method>
# no security wpa akm dot1x
# no security wpa wpa2 ciphers aes
# no shutdown
```

Configuratie van beleidsprofiel

U moet aaa-override in het beleidsprofiel om ervoor te zorgen dat de mac-filtering per SSID werkt prima.

Configuratie van beleidsprofiel op 9800 WLC

Configuratie van beleidstag

Policy Tag op 9800 WLC

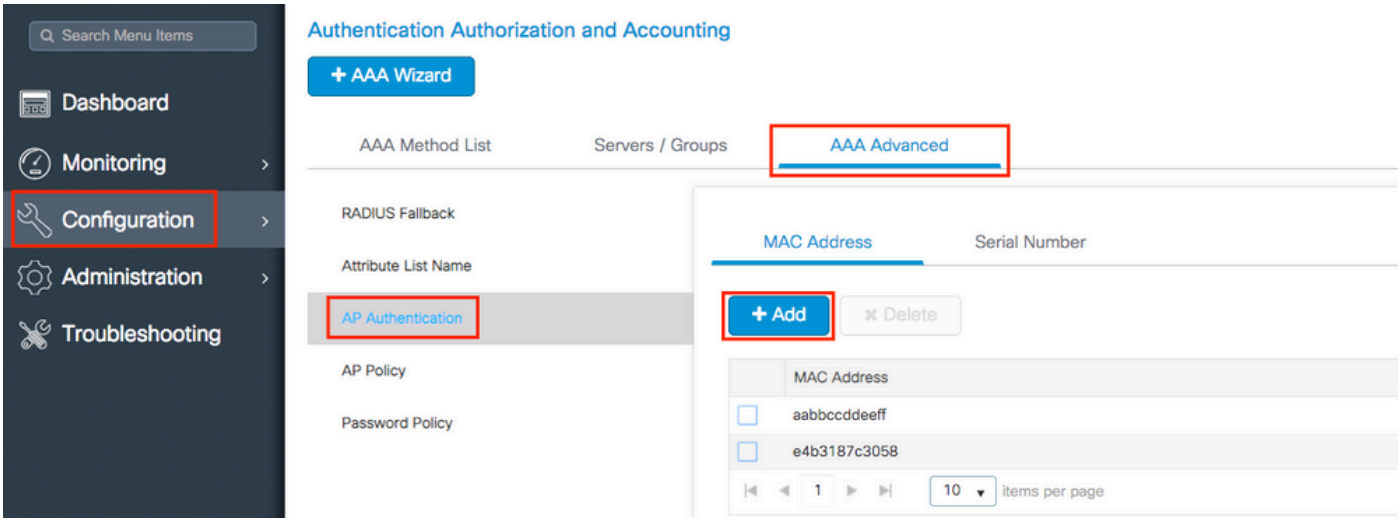
Toewijzing van beleidstags

Policy Tag-toewijzing op 9800 WLC

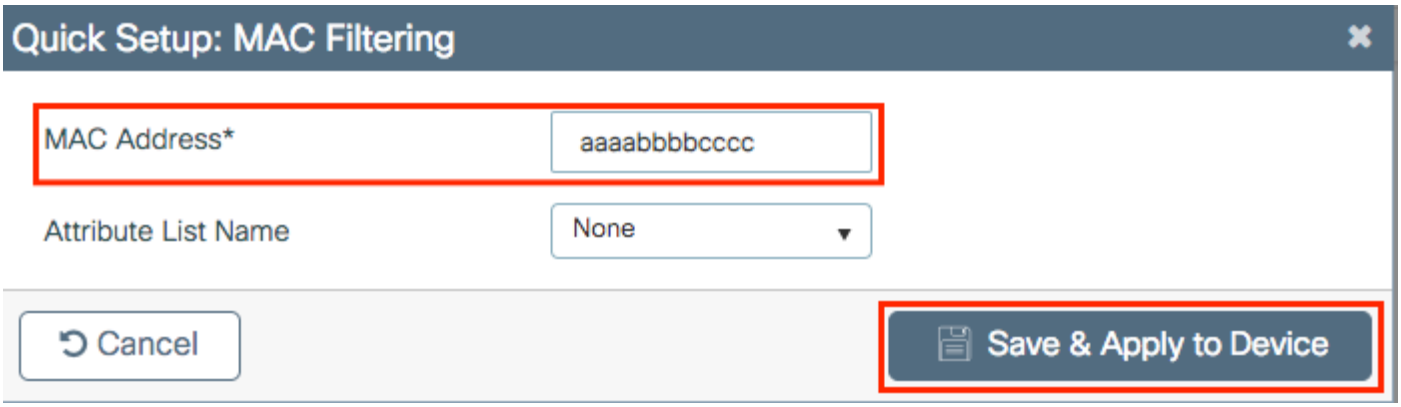
Registreer het toegestane MAC-adres.

Registreer lokaal het MAC-adres op de WLC voor lokale verificatie

Naar navigeren Configuration > Security > AAA > AAA Advanced > AP Authentication > + Add.



Schrijf het MAC-adres in alle kleine letters zonder scheidingsteken en klik op Save & Apply to Device.



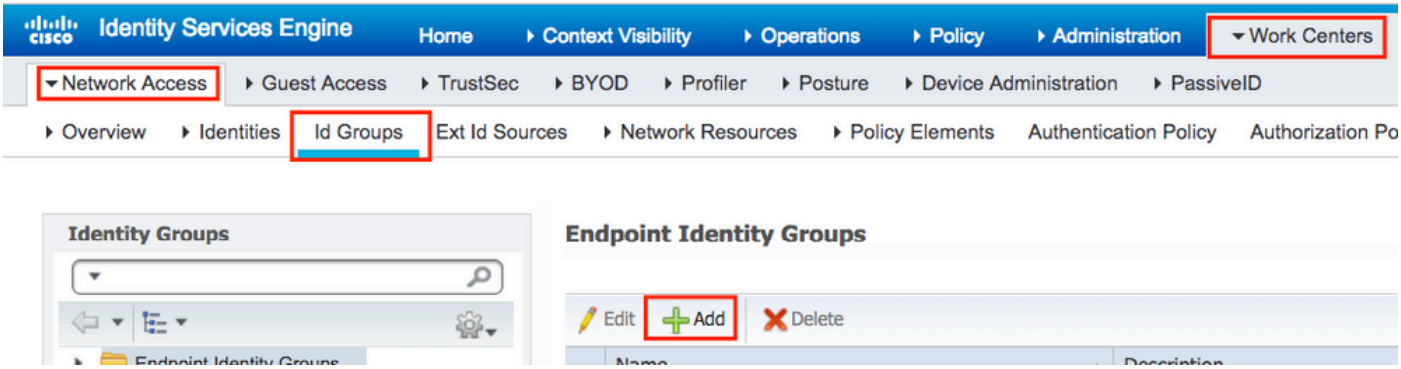
> **Opmerking**: In versies eerder dan 17.3, veranderde de web UI elke MAC-indeling die u hebt getypt in de 'no separator'-indeling die in de afbeelding wordt weergegeven. In 17.3 en later respecteert de web UI elk ontwerp dat u invoert en het is daarom essentieel om geen scheidingsteken in te voeren. Cisco bug-id CSCv43870 van de verbeteringsbug volgt de ondersteuning van verschillende formaten voor MAC-verificatie.

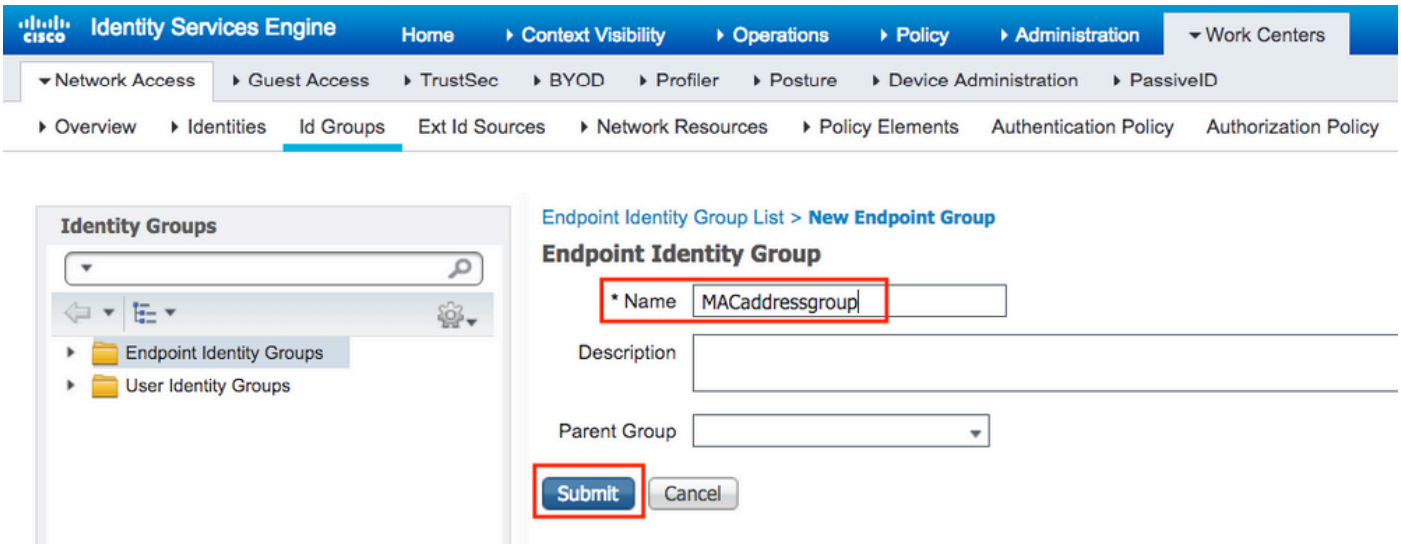
CLI:

```
# config t
# username <aabbccddeeff> mac
```

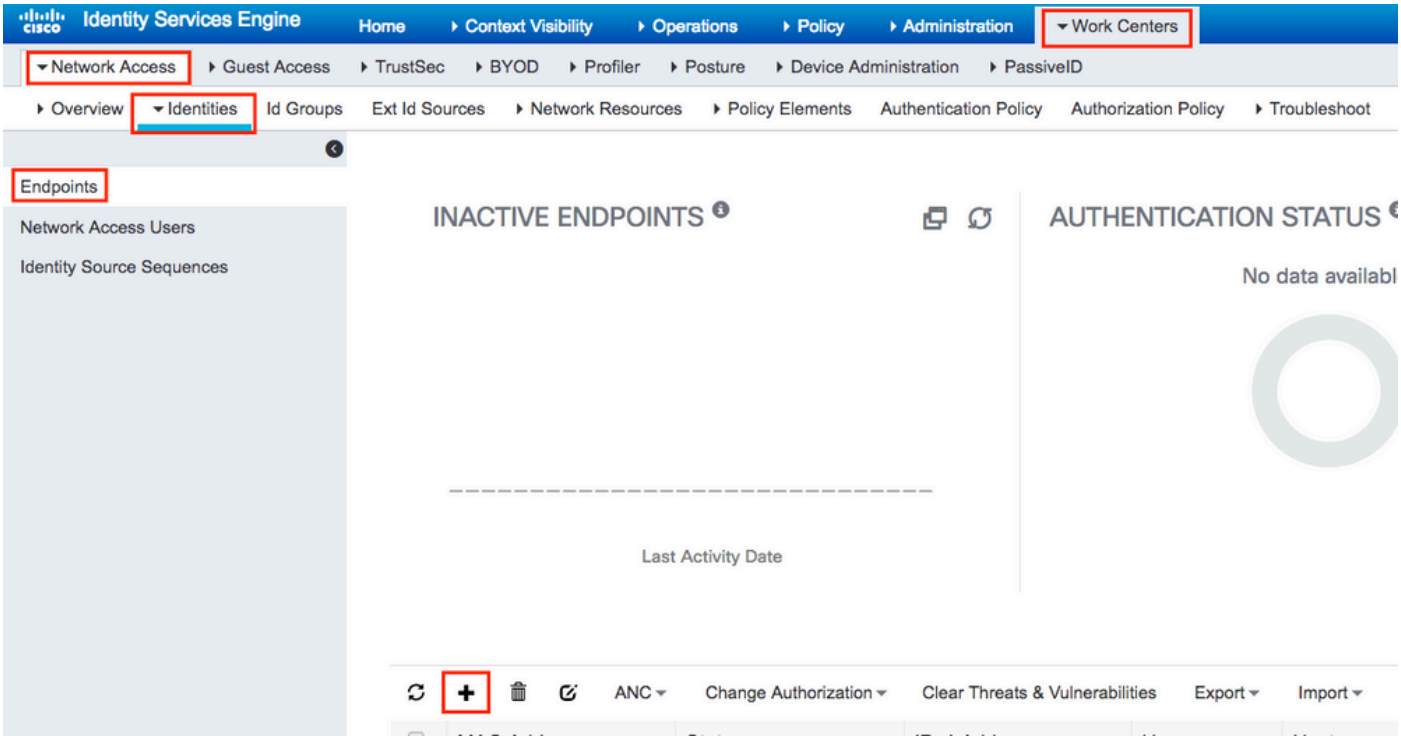
Voer het MAC-adres in in de ISE-endpointdatabase

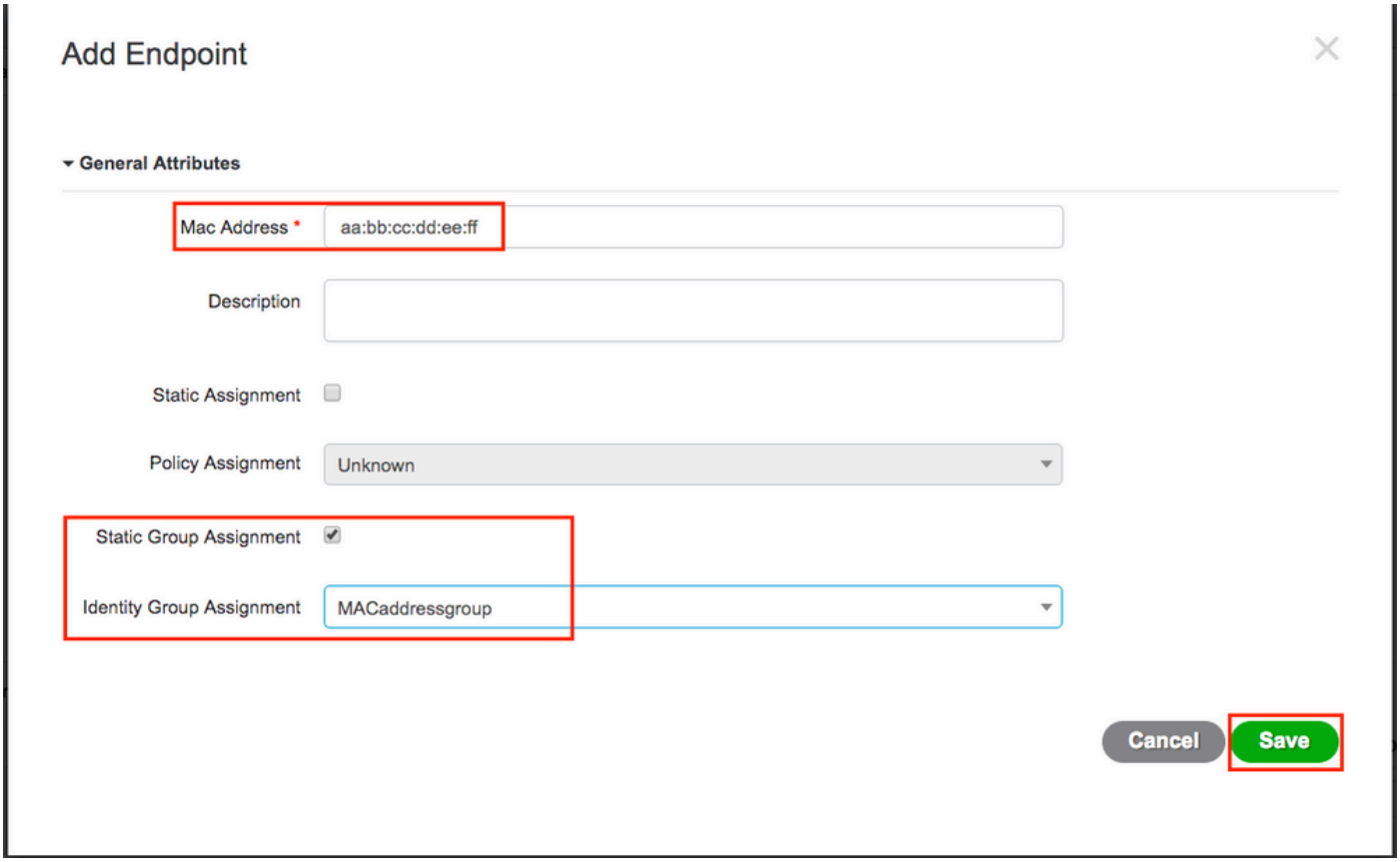
Stap 1. (optioneel) Maak een nieuwe endpointgroep.
Naar navigeren Work Centers > Network Access > Id Groups > Endpoint Identity Groups > + Add.





Stap 2. Naar navigeren Work Centers > Network Access > Identities > Endpoints > +Add.





ISE-configuratie

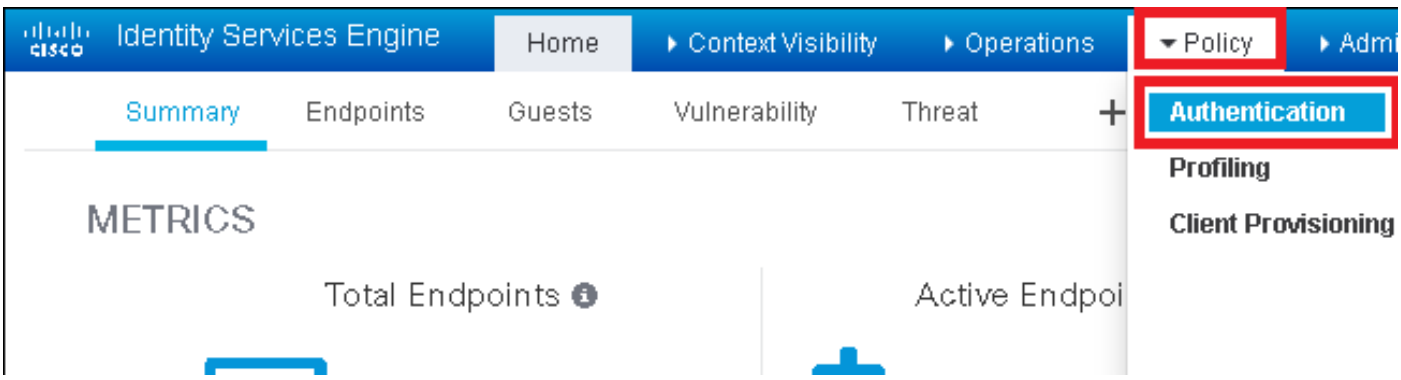
Voeg 9800 WLC toe aan ISE.

Lees de instructies in deze link: Vermeld WLC aan ISE.

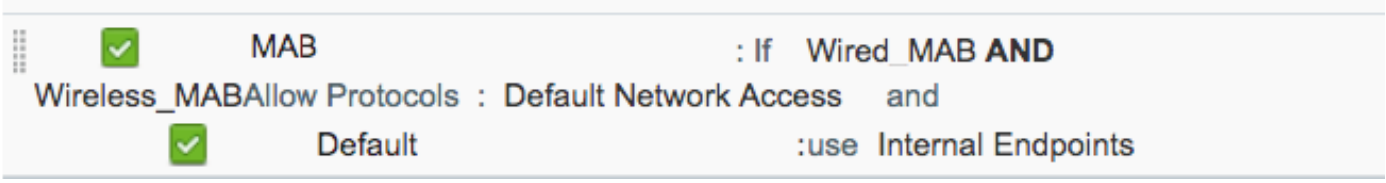
Een verificatieregel maken

Verificatieregels worden gebruikt om te verifiëren of de referenties van de gebruikers juist zijn (verifiëren of de gebruiker echt is wie het zegt dat het is) en om de verificatiemethoden te beperken die door hem mogen worden gebruikt.

Stap 1. Naar navigeren Policy > Authentication zoals in de afbeelding.
Bevestig dat de standaard MAB-regel op uw ISE bestaat.



Stap 2. Controleer of de standaardverificatieregel voor MAB reeds bestaat:

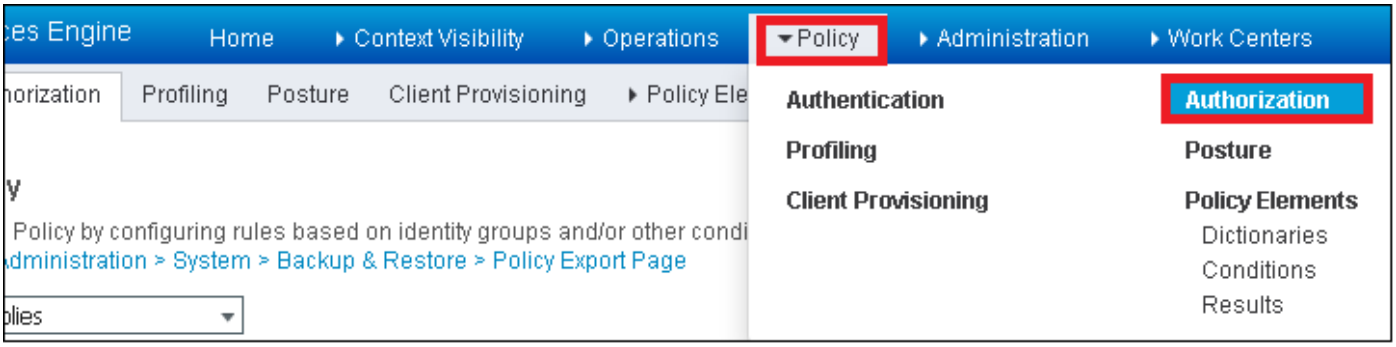


Als dit niet het geval is, kunt u een nieuwe toevoegen wanneer u op Insert new row above.

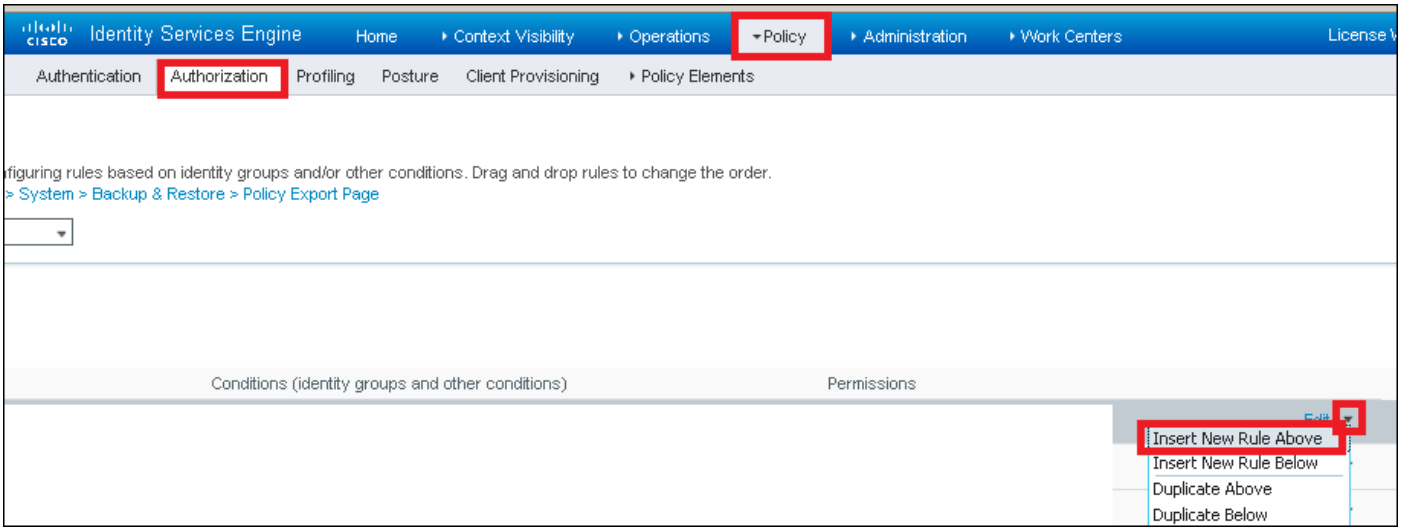
Creatie van autorisatieregel

De autorisatieregel is de regel die bepaalt welke permissies (welk autorisatieprofiel) op de client worden toegepast.

Stap 1. Naar navigeren Policy > Authorization zoals in de afbeelding.

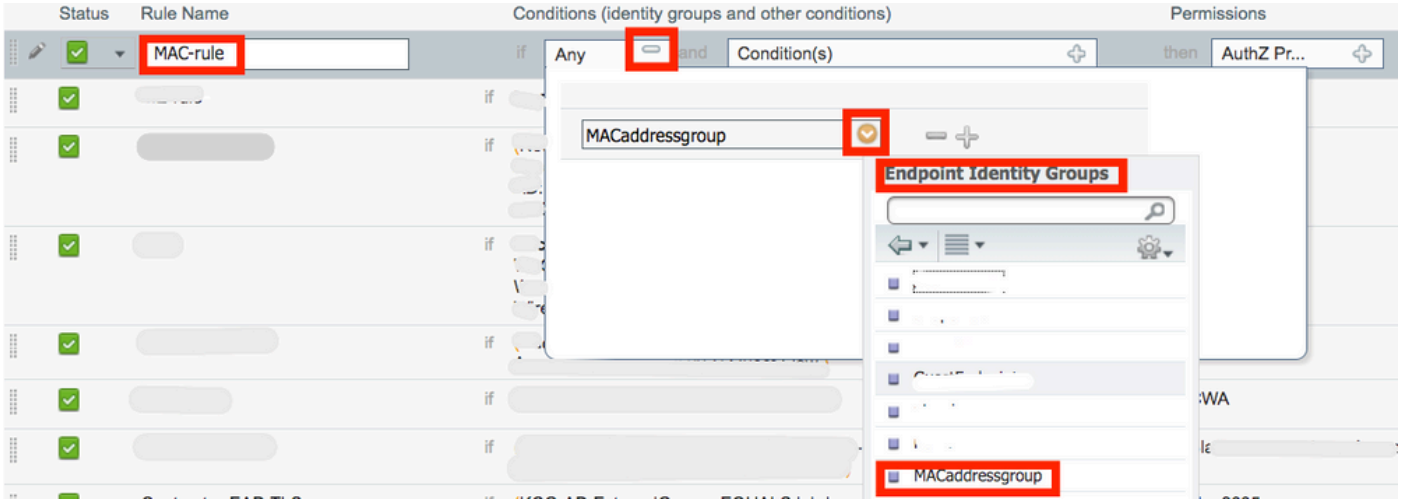


Stap 2. Plaats een nieuwe regel zoals in de afbeelding.

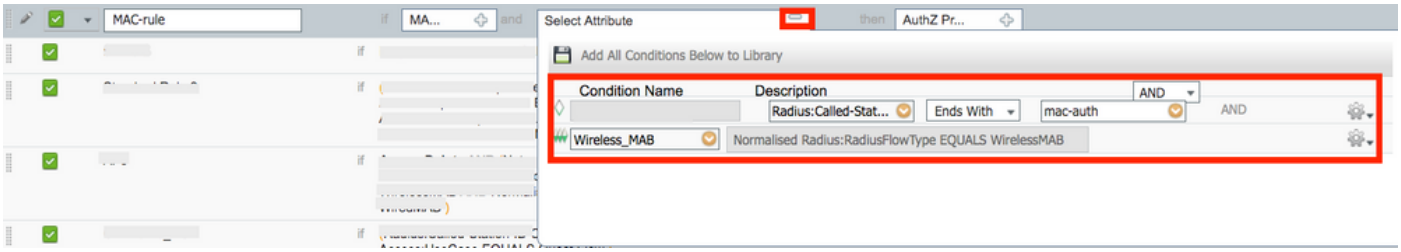


Stap 3. Voer de waarden in.

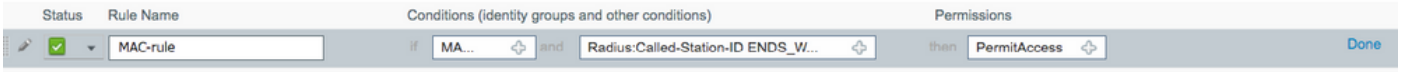
Kies eerst een naam voor de regel en de groep Identity waarin het eindpunt is opgeslagen (**MACaddressgroup**) zoals in het beeld.



Kies vervolgens andere voorwaarden die het autorisatieproces doen om onder deze regel te vallen. In dit voorbeeld, het autorisatieproces raakt deze regel als het draadloze MAB gebruikt en zijn geroepen station ID (de naam van de SSID) eindigt met mac-auth zoals in de afbeelding.



Kies tot slot het autorisatieprofiel dat is toegewezen, in dit geval: PermitAccess aan de klanten die aan die regel voldoen. Klik Done en bewaar het.



Verifiëren

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

```
# 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 client-connectiviteit gerelateerde fouten, waarschuwingen en meldingen voortdurend worden vastgelegd en u kunt logbestanden bekijken voor een incident of storing nadat het is opgetreden.

> **Opmerking**: hoewel het afhankelijk is van het volume van de gegenereerde logbestanden, kunt u een paar uur 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 lezen (zorg ervoor dat u de sessie aan een tekstbestand registreert).

Stap 1. Controleer de huidige tijd van de controller, zodat u de logbestanden kunt volgen vanaf de tijd terug tot wanneer het probleem zich voordeed.

```
# 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 gezondheid en eventuele fouten van het systeem.

```
# show logging
```

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

```
# 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 van de vermelde voorwaarden ziet, betekent dit dat de sporen zijn aangemeld om het debug-niveau te bereiken voor alle processen die de ingeschakelde voorwaarden ervaren (mac-adres, IP-adres, enzovoort). Dit verhoogt het volume van logboeken. Daarom wordt aanbevolen om alle voorwaarden te wissen wanneer niet actief debuggen.

Stap 4. Als het MAC-adres onder de test niet als voorwaarde in Stap 3 was vermeld, verzamel dan de altijd-op meldingen niveau sporen voor het specifieke MAC-adres.

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

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

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

Voorwaardelijke debugging en radio actieve tracering

Als de altijd-op 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 sporen biedt voor alle processen die interacteren met de gespecificeerde voorwaarde (client mac-adres in dit geval). Lees deze stappen om voorwaardelijke debugging in te schakelen.

Stap 5. Zorg ervoor dat geen debug voorwaarden zijn ingeschakeld.

```
# clear platform condition all
```

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

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

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

> **Opmerking:** Als u meer dan één client tegelijk wilt bewaken, voert u debug (debug) draadloze Mac uit opdracht per mac-adres.

> **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.

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

Zodra de monitortijd is verstreken of de debug-radio is gestopt, genereert de 9800 WLC een lokaal bestand met de naam: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Stap 9. Verzamel het bestand van de mac-adresactiviteit. U kunt de ra trace .log naar een externe server of de uitvoer rechtstreeks op het scherm weergeven.

Controleer de naam van het RA traces bestand:

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

Kopieert het bestand naar een externe server:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
tftp://a.b.c.d/ra-FILENAME.txt
```

Geef de inhoud weer:

```
# 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 uitgebreide mening van debug-niveau logboeken zijn. U hoeft niet opnieuw te debuggen de client als u alleen een verdere gedetailleerde kijk op debug logbestanden die al zijn verzameld en intern opgeslagen.

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

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

U kunt de ra-internal-FILENAME.txt naar een externe server of de uitvoer rechtstreeks op het scherm weergeven.

Kopieert het bestand naar een externe server:

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

Geef de inhoud weer:

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

Stap 11. Verwijder de debug-voorwaarden.

```
# 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.