EAP en RLAN op Catalyst 9800 WLC configureren

Inhoud

Inleiding

Dit document legt uit hoe u het Cisco OfficeExtend access point (OEAP) en het Remote Local Area Network (RLAN) op 9800 WLC kunt configureren.

Een Cisco OfficeExtend access point (OEAP) biedt beveiligde communicatie van een controller naar een Cisco AP op een externe locatie, waardoor de WLAN-vestiging van de onderneming via het internet naadloos wordt uitgebreid naar de verblijfplaats van een werknemer. De ervaring van een gebruiker op het thuiskantoor is precies dezelfde als bij het hoofdkantoor. Datagram Transport Layer Security (DTLS)-encryptie tussen een access point en de controller zorgt ervoor dat alle communicatie het hoogste beveiligingsniveau heeft.

Een Remote LAN (RLAN) wordt gebruikt voor het authenticeren van bekabelde clients met de controller. Nadat de bekabelde client zich met succes bij de controller heeft aangesloten, schakelen de LAN-poorten het verkeer tussen de centrale of lokale switching-modi in. Het verkeer van de bekabelde klanten wordt behandeld als draadloos clientverkeer. RLAN in Access Point (AP) verstuurt de authenticatieaanvraag om de bekabelde client te authenticeren. De authenticatie van de bekabelde klanten in RLAN is vergelijkbaar met de centrale geauthentiseerde draadloze client.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- 9800 WLC
- Opdracht-line Interface (CLI) toegang tot de draadloze controllers en access points

Gebruikte componenten

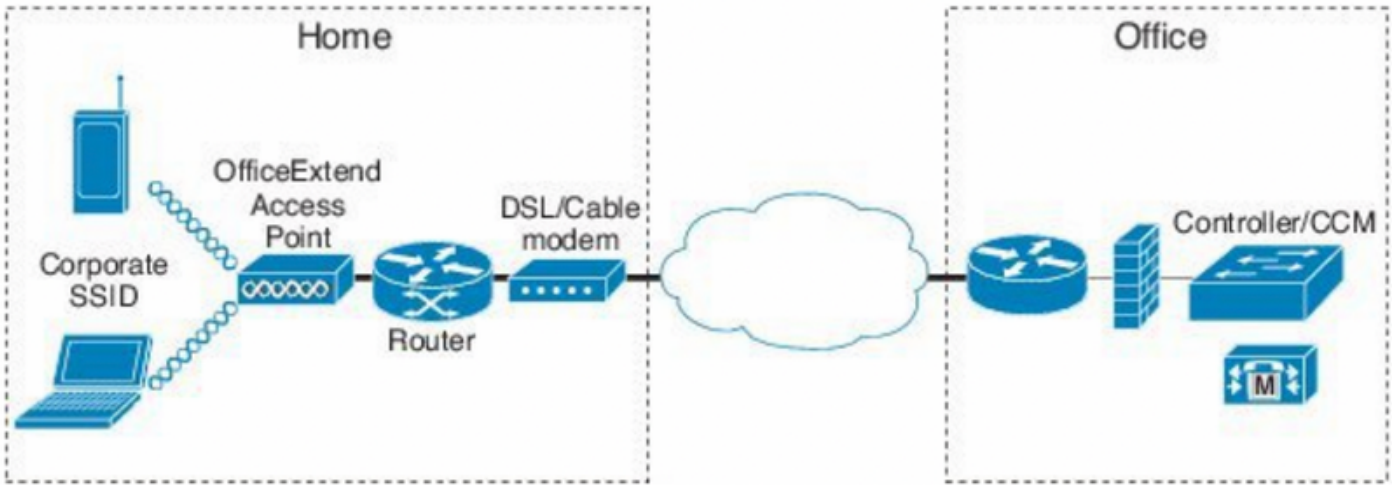
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 9800 WLC versie 17.02.01
- 1815/1810 Series AP

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Netwerkdiagram

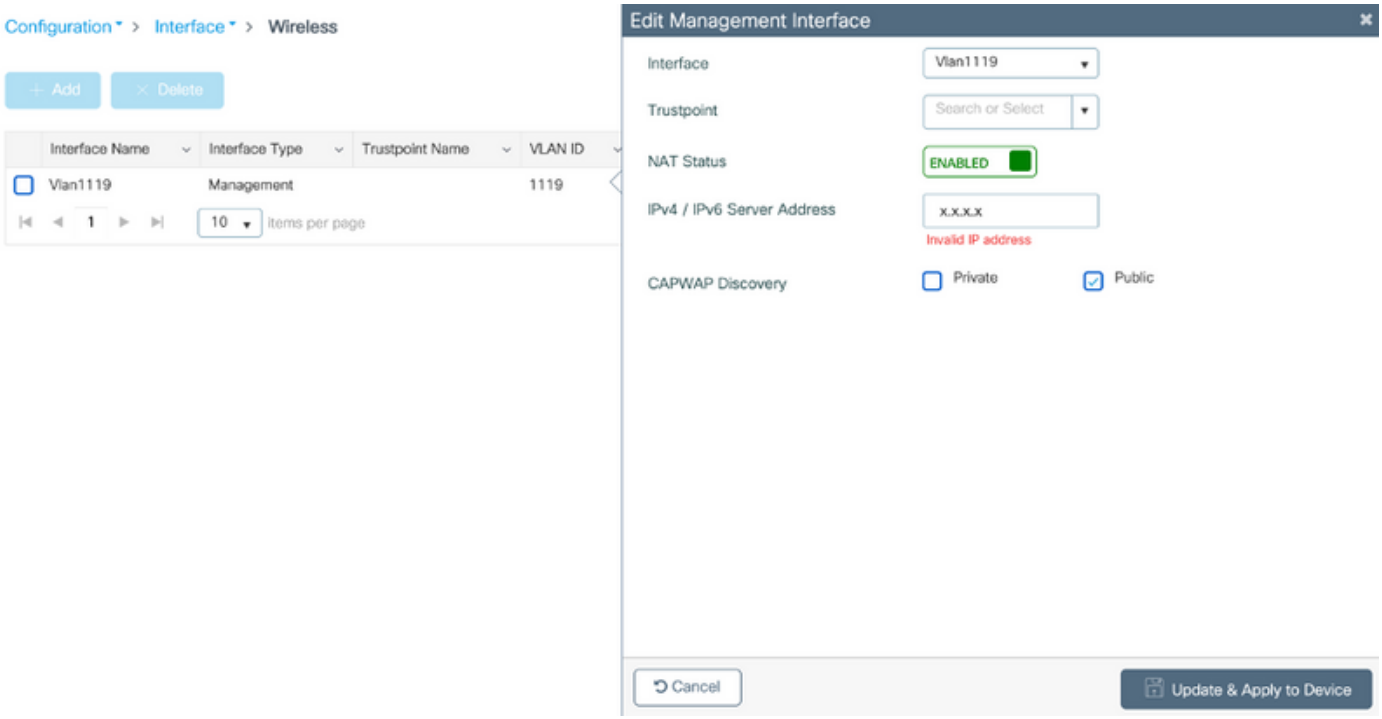


AP toetreden achter NAT

In 16.12.x codes, moet u NAT IP adres van de CLI configureren. Er is geen GUI-optie beschikbaar. U kunt ook de CAPWAP-ontdekking selecteren via openbare of particuliere IP.

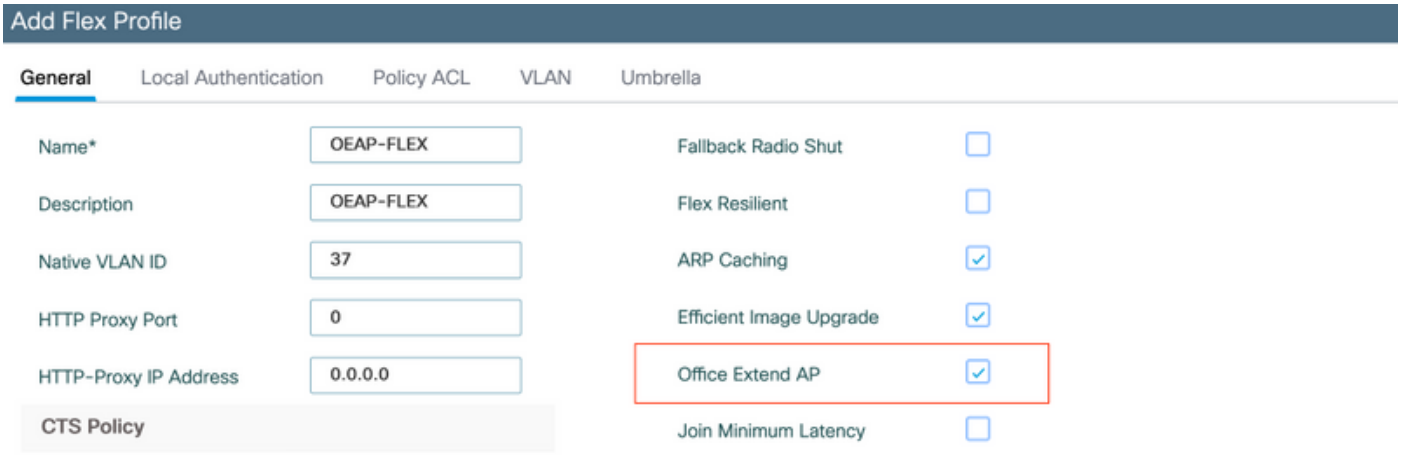
```
(config)#wireless management interface vlan 1114 nat public-ip x.x.x.x
(config-nat-interface)#capwap-discovery ?
  private  Include private IP in CAPWAP Discovery Response

  public   Include public IP in CAPWAP Discovery Response
```

In 17.x-codes, navigeer naar **Configuration > Interface > Wireless** en klik vervolgens op **Wireless Management Interface**, om NAT IP en CAPWAP-discovery type vanuit de GUI te configureren.

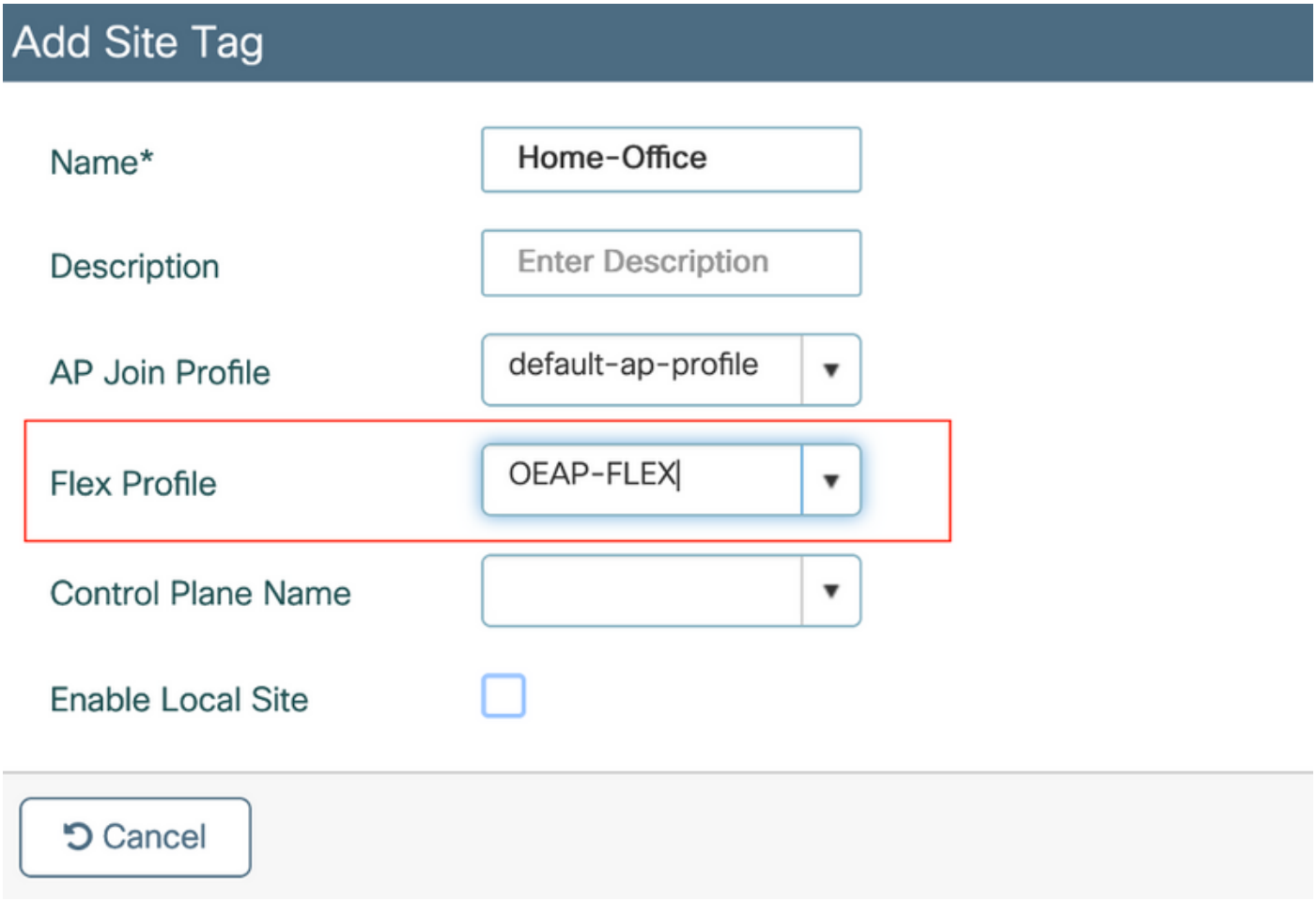


Configuratie

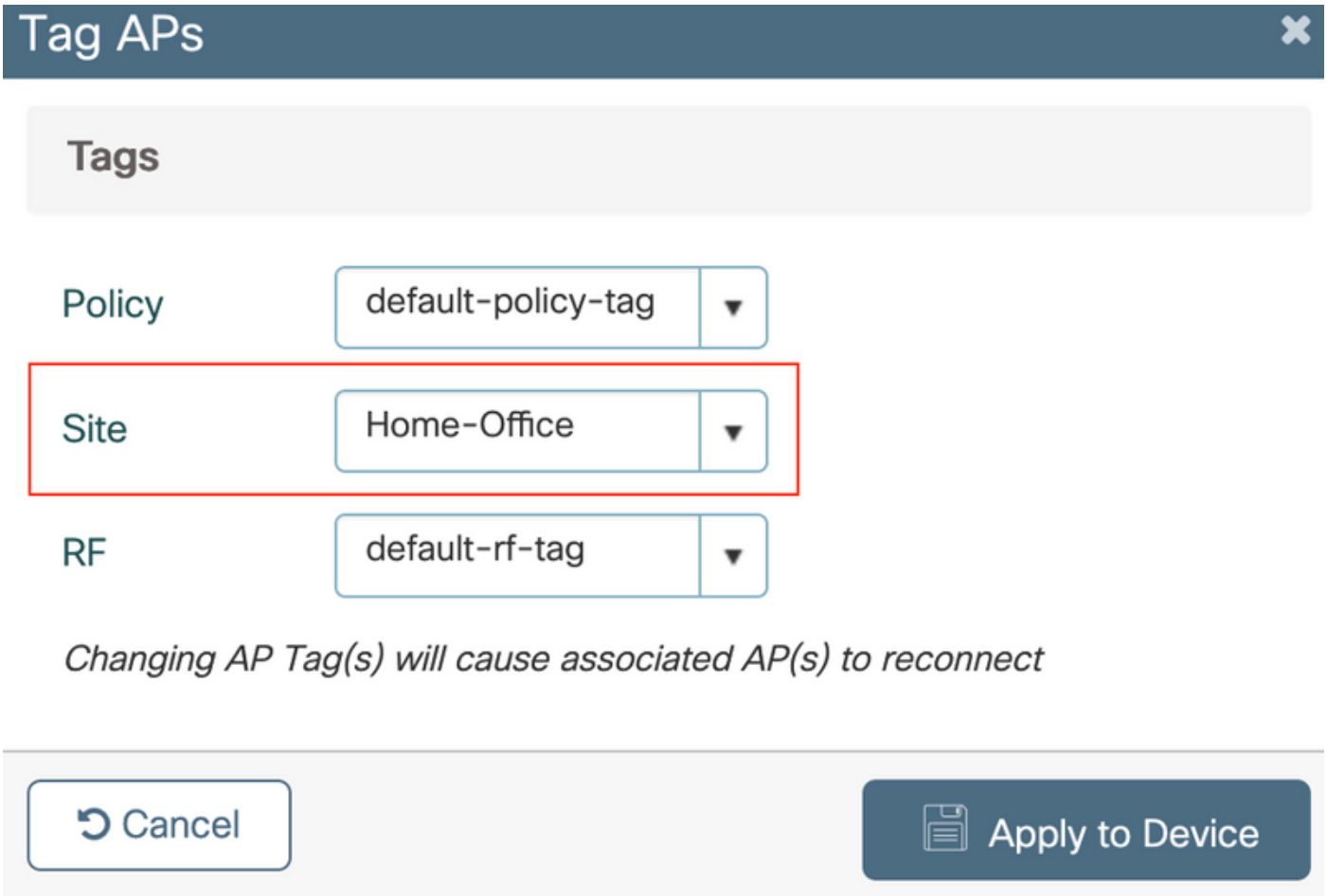
1. Om een Flex profiel te maken, stelt u **Office Extend AP in** en navigeer naar **Configuration > Tags & Profiles > Flex.**



2. Om een Site Tag en map Flex Profile te maken, navigeer dan naar **Configuration > Tags en profielen > Tags.**



3. navigeren om het AP uit 1815 te taggen met de Site Tag gemaakt door **Configuration > Wireless Setup > Advanced > Tag AP's.**



Verifiëren

Controleer deze uitvoer zodra AP uit 1815 opnieuw aan WLC deelneemt:

```
vk-9800-1#show ap name AP1815 config general

Cisco AP Name   : AP1815
================================================

Cisco AP Identifier                             : 002c.c8de.3460

Country Code                                    : Multiple Countries : IN,US

Regulatory Domain Allowed by Country            : 802.11bg:-A   802.11a:-ABDN

AP Country Code                                 : US  - United States

Site Tag Name                                   : Home-Office

RF Tag Name                                     : default-rf-tag

Policy Tag Name                                 : default-policy-tag

AP join Profile                                 : default-ap-profile

Flex Profile                                    : OEAP-FLEX

Administrative State                            : Enabled

Operation State                                 : Registered

AP Mode                                         : FlexConnect

AP VLAN tagging state                           : Disabled

AP VLAN tag                                     : 0

CAPWAP Preferred mode                           : IPv4

CAPWAP UDP-Lite                                 : Not Configured

AP Submode                                      : Not Configured

Office Extend Mode                              : Enabled

Dhcp Server                                     : Disabled

Remote AP Debug                                 : Disabled


vk-9800-1#show ap link-encryption

                          Encryption      Dnstream    Upstream     Last

AP Name                   State           Count       Count        Update

---------------------------------------------------------------------------

N2                         Disabled       0           0           06/08/20 00:47:33
```

```
AP1815                          Enabled         43          865         06/08/20 00:46:56
```

```
when you enable the OfficeExtend mode for an access point DTLS data encryption is enabled
automatically.
```

```
AP1815#show capwap client config

AdminState                          : ADMIN_ENABLED(1)

Name                                : AP1815

Location                            : default location

Primary controller name             : vk-9800-1

ssh status                          : Enabled

ApMode                              : FlexConnect

ApSubMode                           : Not Configured

Link-Encryption                     : Enabled

OfficeExtend AP                     : Enabled

Discovery Timer                     : 10

Heartbeat Timer                     : 30

Syslog server                       : 255.255.255.255

Syslog Facility                     : 0

Syslog level                        : informational
```

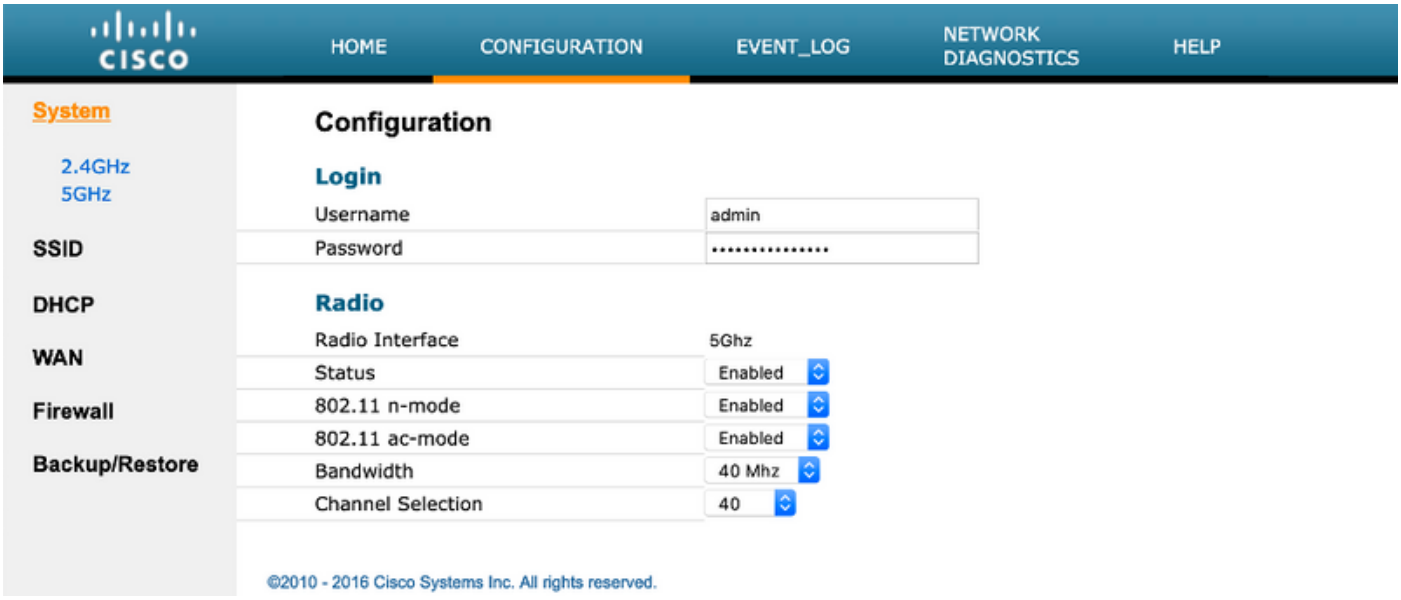
Opmerking: U kunt DTLS-gegevensencryptie voor een specifiek access point of voor alle access points in- of uitschakelen met behulp van de opdracht Plaink-encryptie

```
vk-9800-1(config)#ap profile default-ap-profile

vk-9800-1(config-ap-profile)#no link-encryption

Disabling link-encryption globally will reboot the APs with link-encryption.

Are you sure you want to continue? (y/n)[y]:y
```

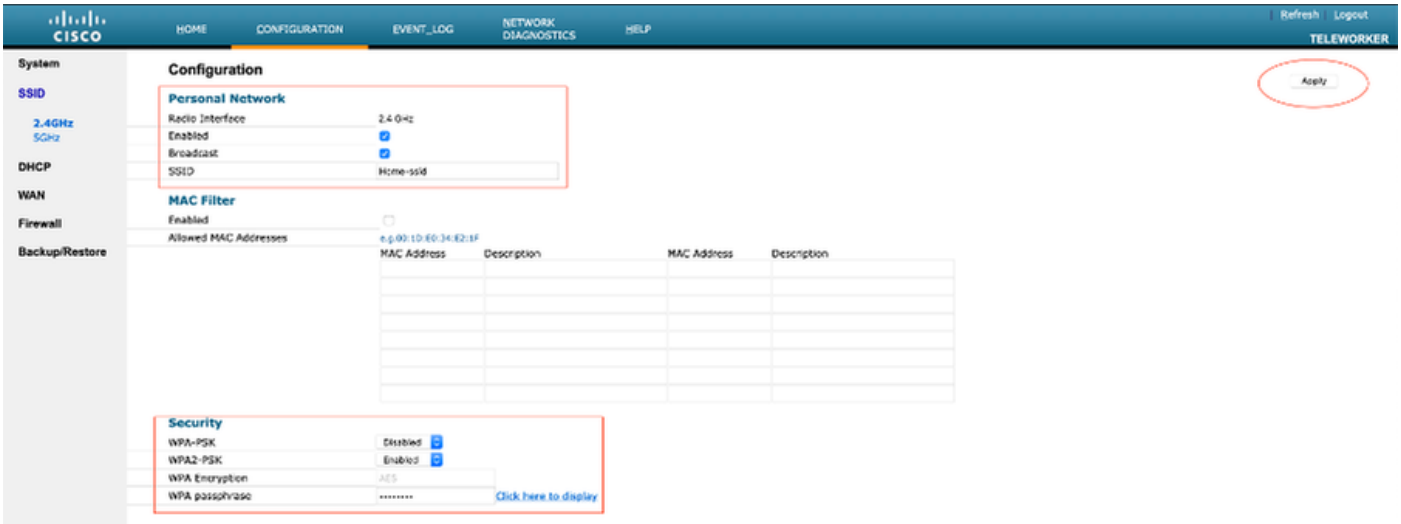
Inloggen op OEAP en Persoonlijke SSID configureren

1. U hebt toegang tot de webinterface van het OEAP met het IP-adres. De standaard inlogreferenties zijn **admin** en **admin**.

2. Om veiligheidsredenen wordt het aanbevolen de standaardaanmeldingsgegevens te wijzigen.



3. Navigeer naar **Configuration> SSID> 2.4 GHz/5 GHz** om de persoonlijke SSID te configureren.



4. Schakel de radio in.

5. Voer de SSID's in en schakelt Broadcast in

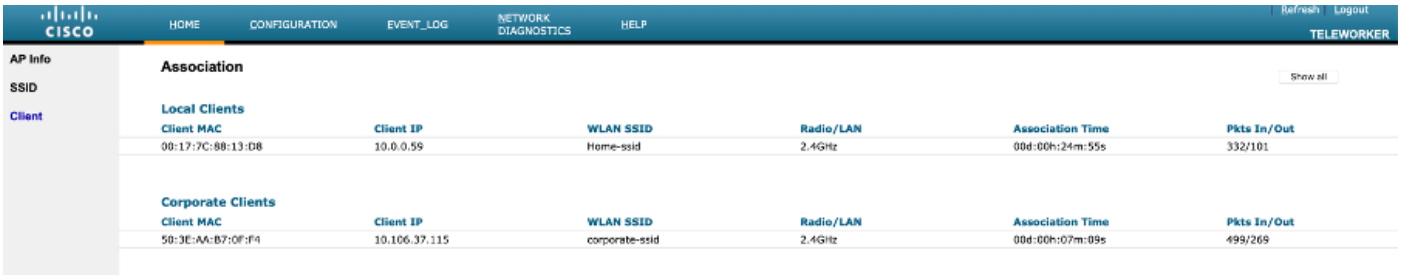
6. Voor encryptie, kies **WAP-PSK** of **WAP2-PSK** en voer het wachtwoord voor het corresponderende beveiligingstype in.

7. Klik op Toepassen om de instellingen te laten uitvoeren.

8. Clients die verbinding maken met de persoonlijke SSID's krijgen het IP-adres standaard vanaf het 10.0.0.1/24 netwerk.

9. Thuisgebruikers kunnen dezelfde AP gebruiken om verbinding te maken voor hun thuisgebruik en dat verkeer niet via de DTLS-tunnel wordt doorgegeven.

10. Om de cliëntenverenigingen op de OEAP te controleren, navigeer naar **startpunt > client**. U kunt de lokale klanten en zakelijke klanten die bij het OEAP betrokken zijn, zien.




```
To clear personal ssidfrom office-extend ap

ewlc#ap name cisco-ap clear-personalssid-config

clear-personalssid-config Clears the Personal SSID config on an OfficeExtend AP
```

LAN op 9800 WLC configureren

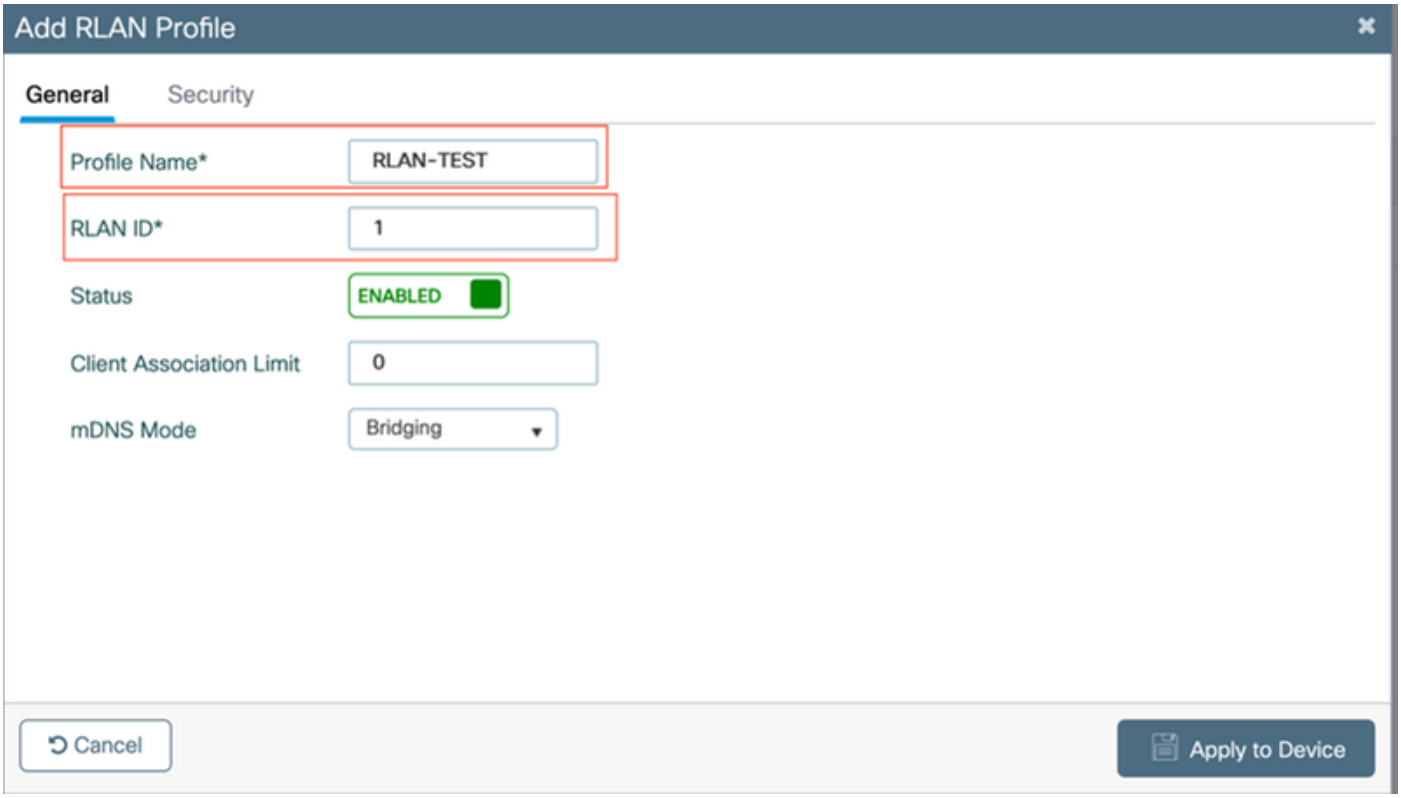
Een Remote LAN (RLAN) wordt gebruikt voor het authenticeren van bekabelde clients met de controller. Nadat de bekabelde client zich met succes bij de controller heeft aangesloten, schakelen de LAN-poorten het verkeer tussen de centrale of lokale switching-modi in. Het verkeer van de bekabelde klanten wordt behandeld als draadloos clientverkeer. RLAN in Access Point (AP) verstuurt de authenticatieaanvraag om de bekabelde client te authenticeren. Het

De authenticatie van de bekabelde klanten in RLAN is vergelijkbaar met de centrale geauthentiseerde draadloze client.

> Opmerking: Lokale EAP wordt gebruikt voor RLAN-clientverificatie in dit voorbeeld. Plaatselijke MAP-configuratie moet op de WLC aanwezig zijn om de volgende stappen te kunnen uitvoeren. Het omvat een authenticatie - en autorisatiemethoden, een lokaal MAP - profiel en lokale geloofsbrieven.

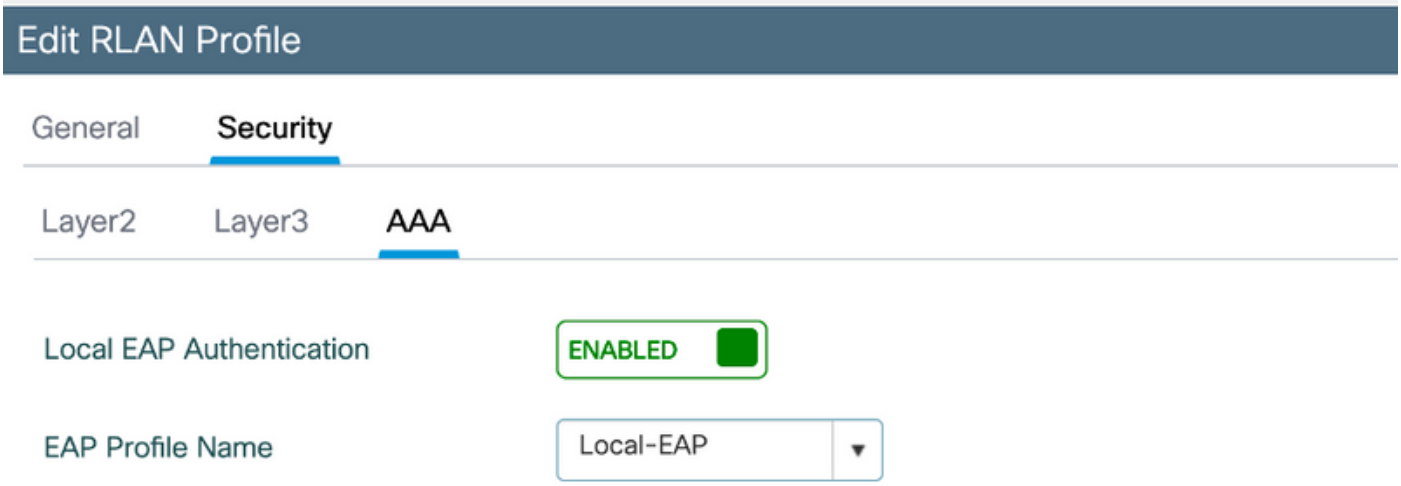
Lokale MAP-verificatie op Catalyst 9800 WLC-configuratievoorbeeld

1. Om een RLAN-profiel te maken, navigeer dan naar **Configuration > Wireless > Remote LAN** en voer een naam en RLAN-ID in voor het RLAN-profiel, zoals in deze afbeelding wordt weergegeven.

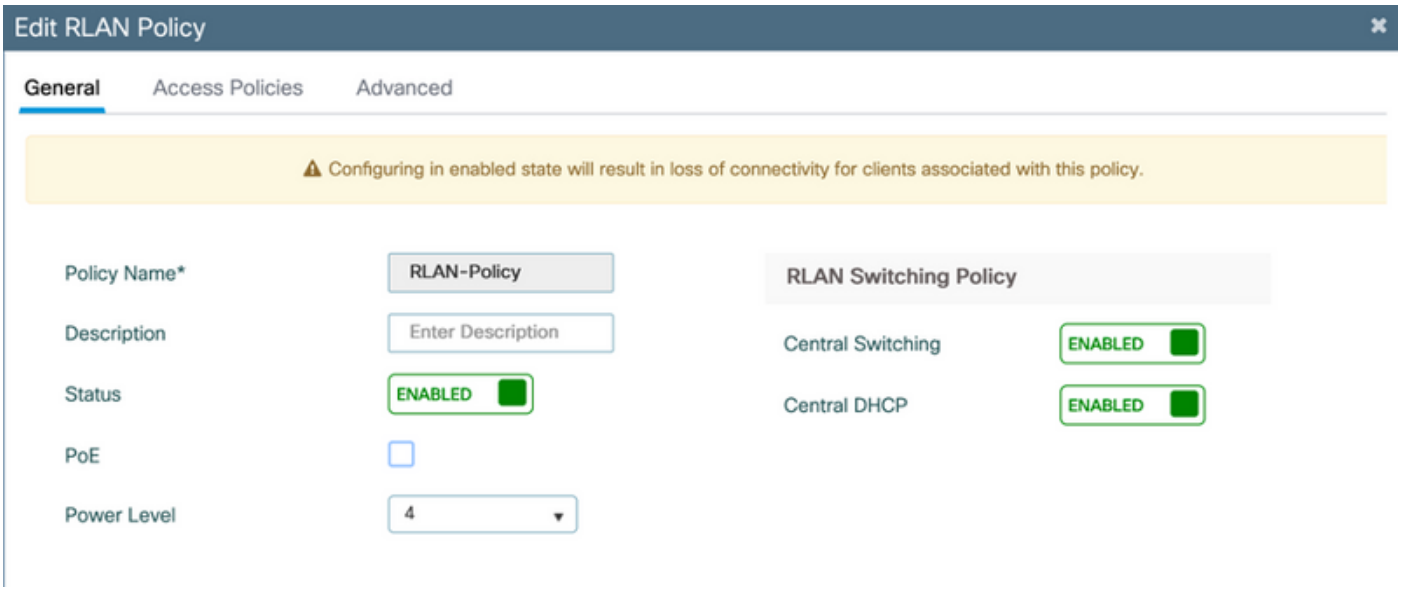


2. Navigeer naar **Security > Layer 2**, om 802.1x voor een netwerk in te schakelen, stel de 802.1x status in als Enabled, zoals in deze afbeelding wordt getoond.

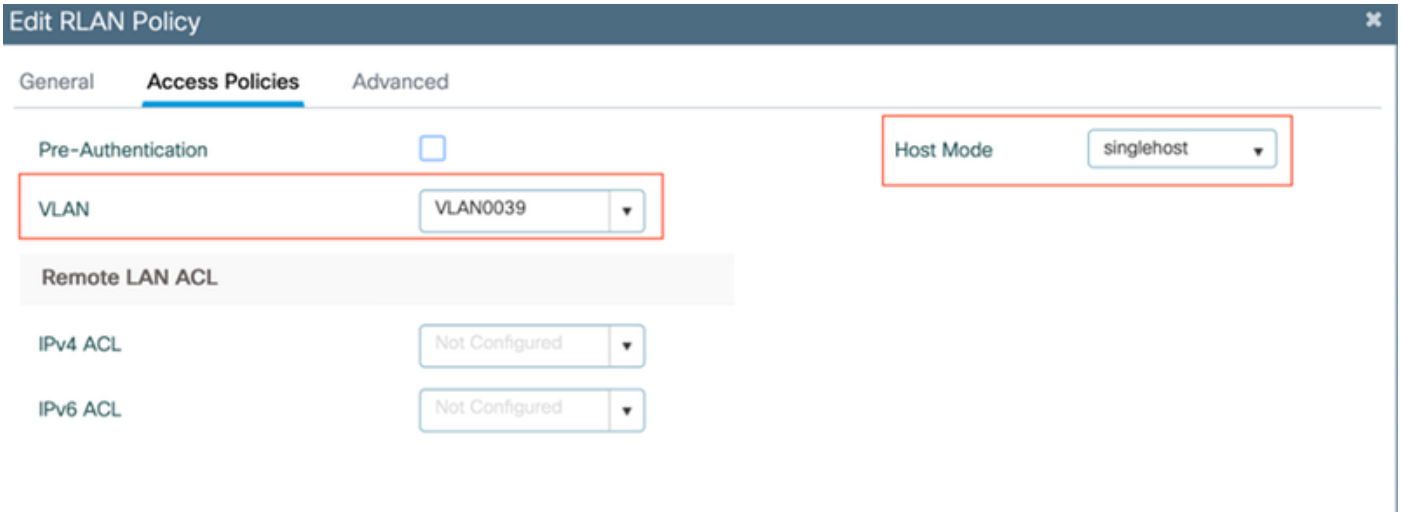
3. Navigeer naar **Beveiliging > AAA**, stel de lokale MAP-verificatie in om deze in te schakelen en kies de gewenste EAP-profielnaam in de vervolgkeuzelijst, zoals in deze afbeelding wordt weergegeven.



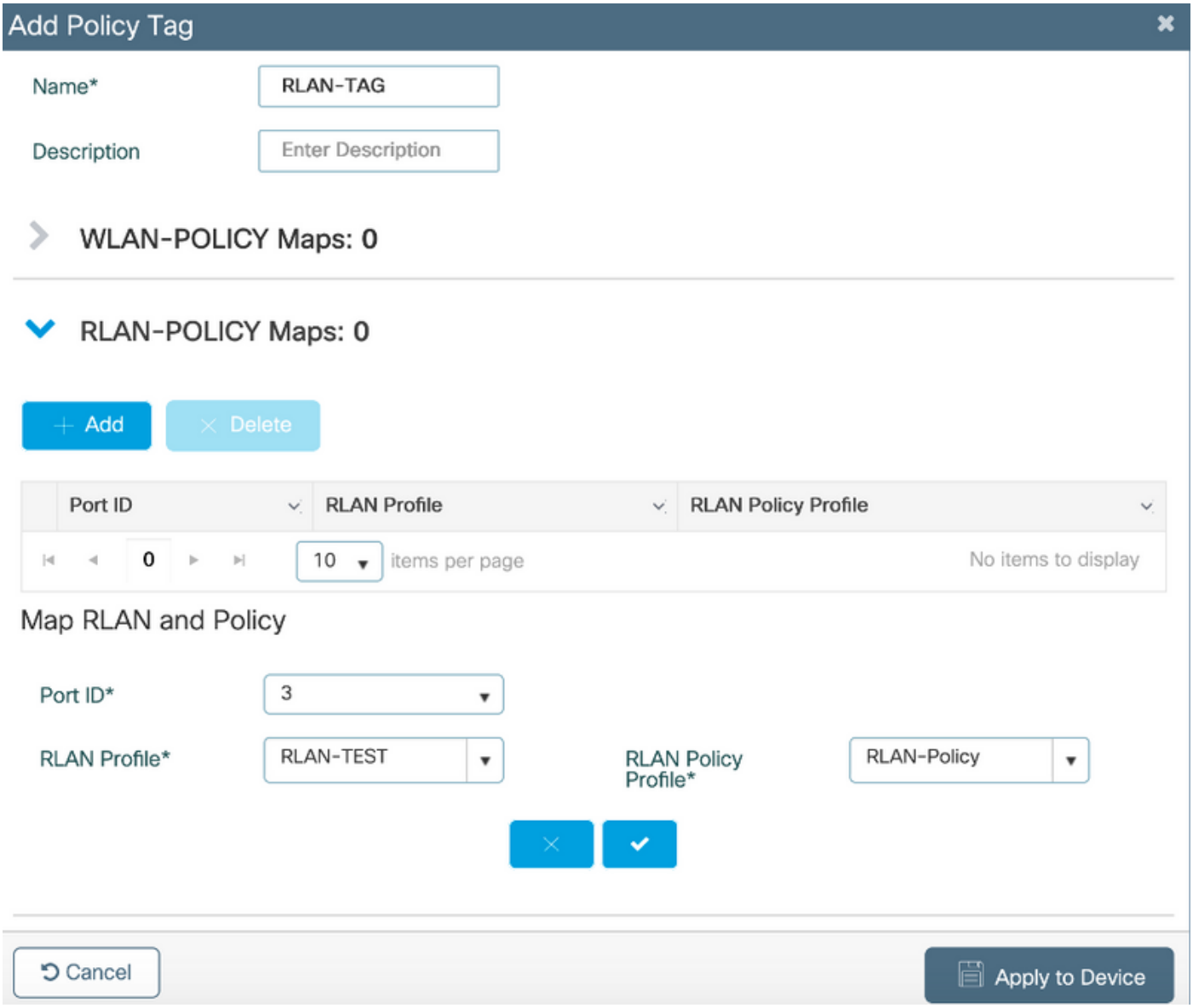
4. Als u het LAN-beleid wilt maken, navigeer dan naar **Configuration > Wireless > Remote LAN** en klik op het tabblad **RLAN**, zoals in deze afbeelding weergegeven.

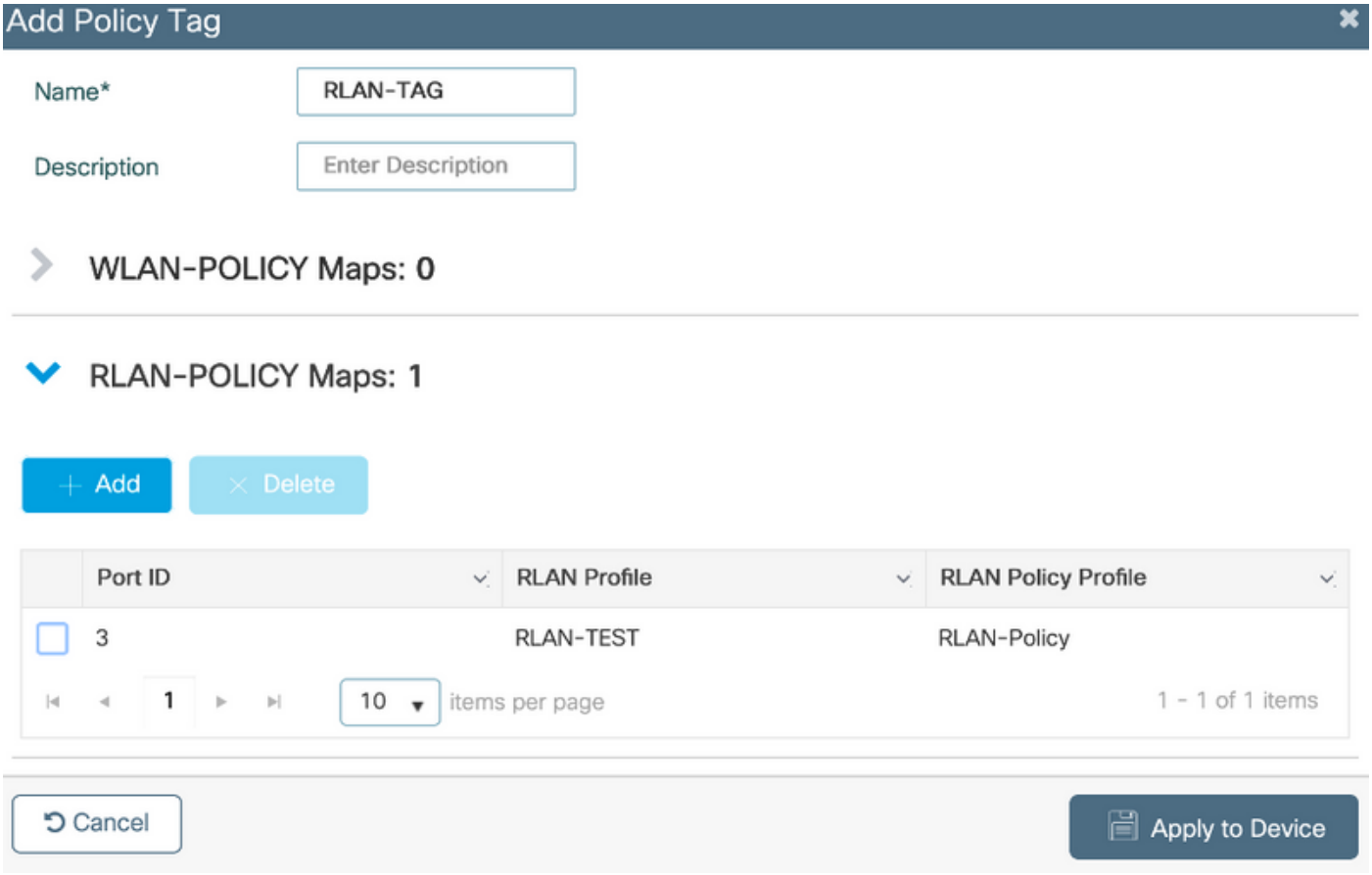


Navigeren in op toegangsbeleid en configureren VLAN en hostmodus en passen de instellingen toe.

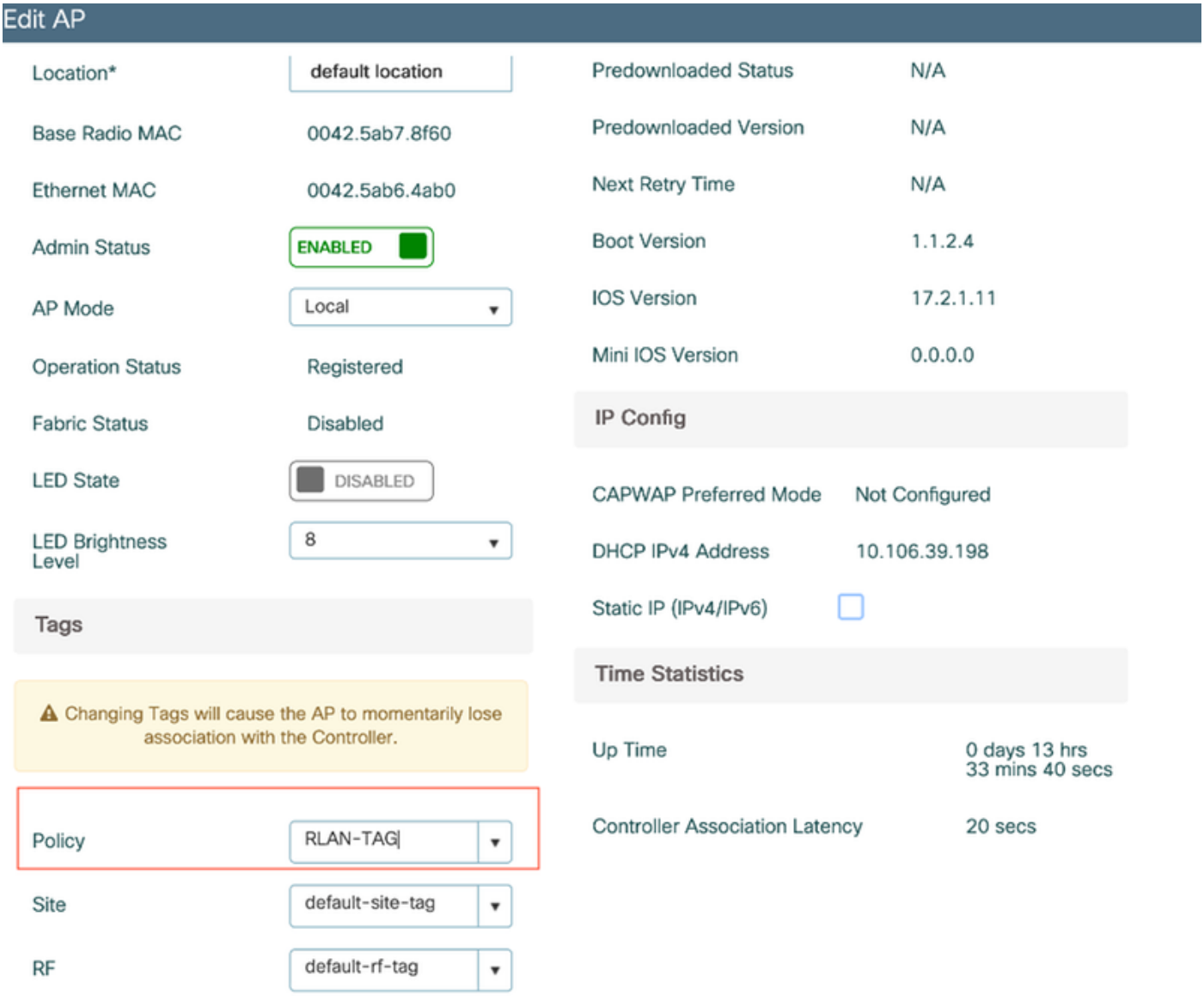


5. Als u een beleidslabel en een profiel voor LAN-programma wilt maken, navigeer dan naar **Configuratie > Tags en profielen > Tags.**

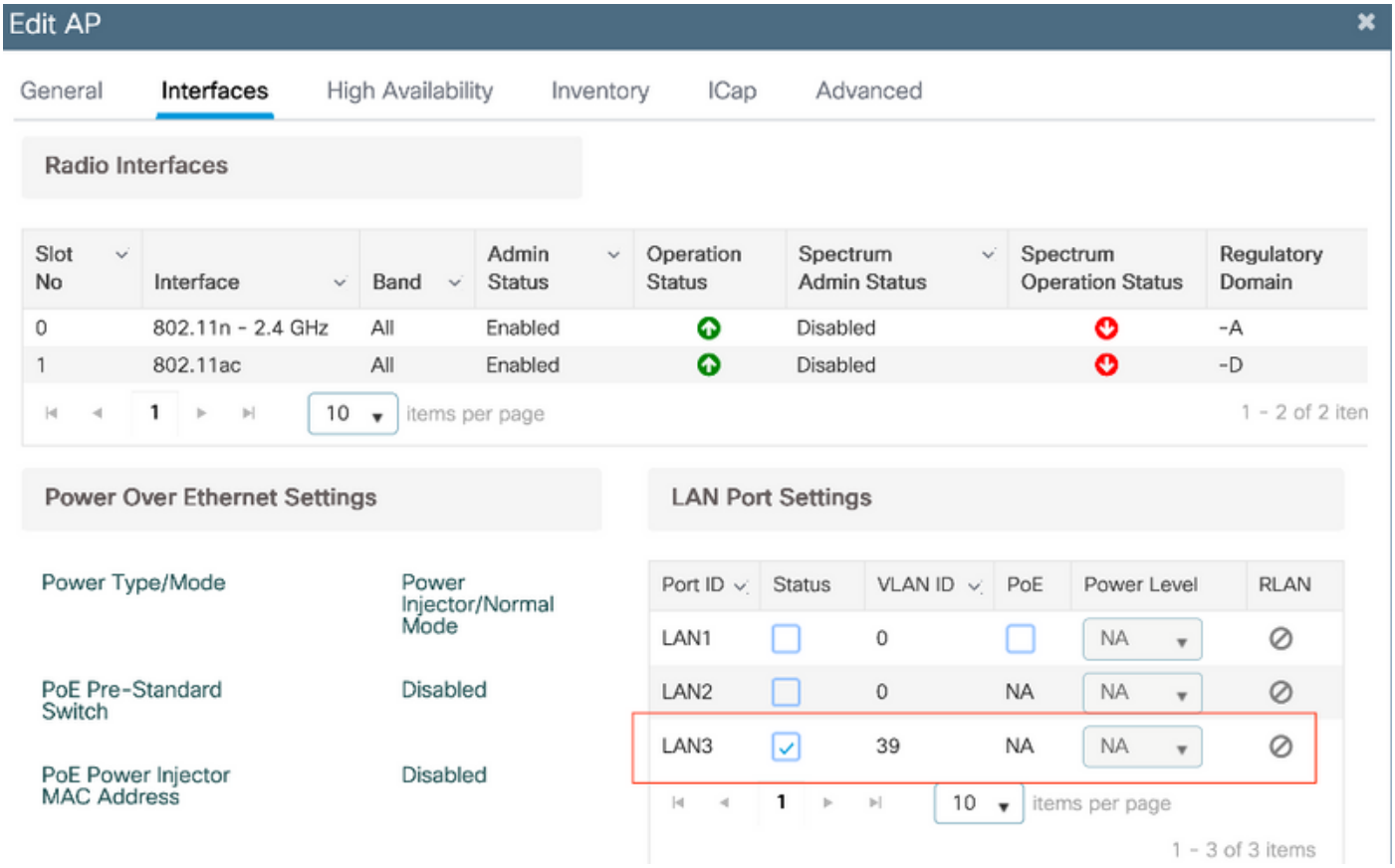

Add Policy Tag
Name*
RLAN-TAG
Description
Enter Description
WLAN-POLICY Maps: 0
RLAN-POLICY Maps: 0
Add
Delete
Port ID
RLAN Profile
RLAN Policy Profile
0
10
items per page
No items to display
Map RLAN and Policy
Port ID*
3
RLAN Profile*
RLAN-TEST
RLAN Policy Profile*
RLAN-Policy
Cancel
Apply to Device



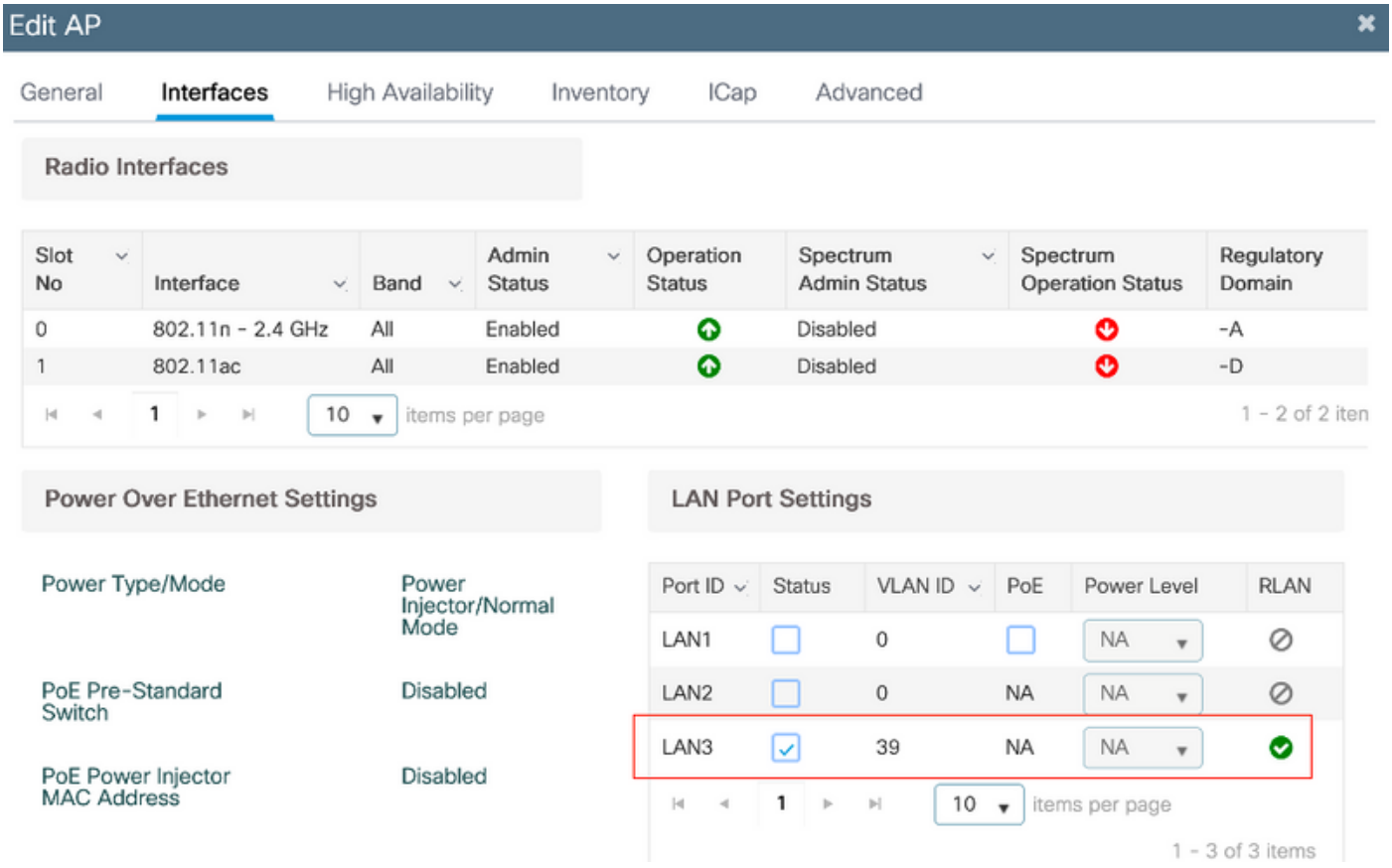
6. Schakel de LAN poort in en pas de Policy TAG op het AP toe. Navigeer naar **Configuration > Wireless > Access Point** en klik op **AP**.



Pas de instelling toe en koppel de AP opnieuw aan de WLC. Klik op **AP**, selecteer dan **Interfaces** en laat de LAN poort toe.

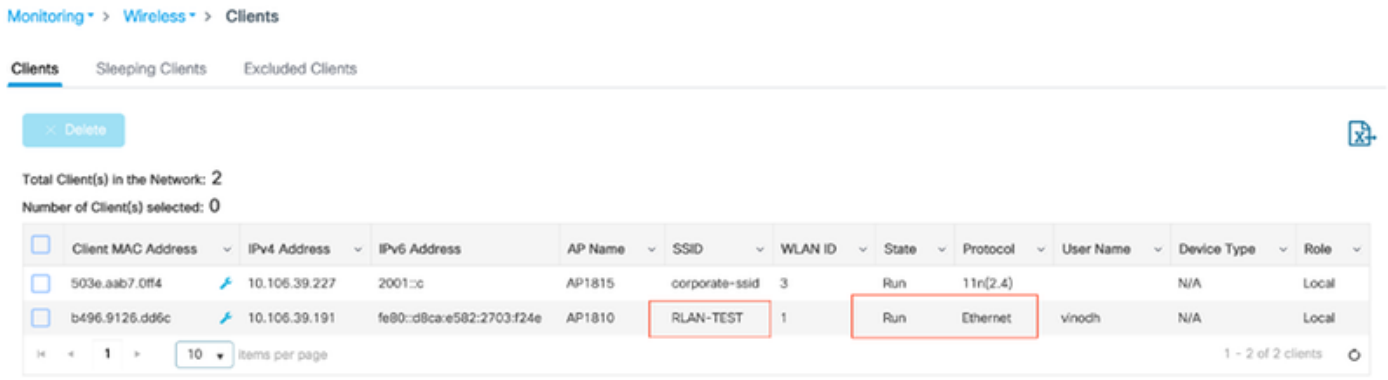


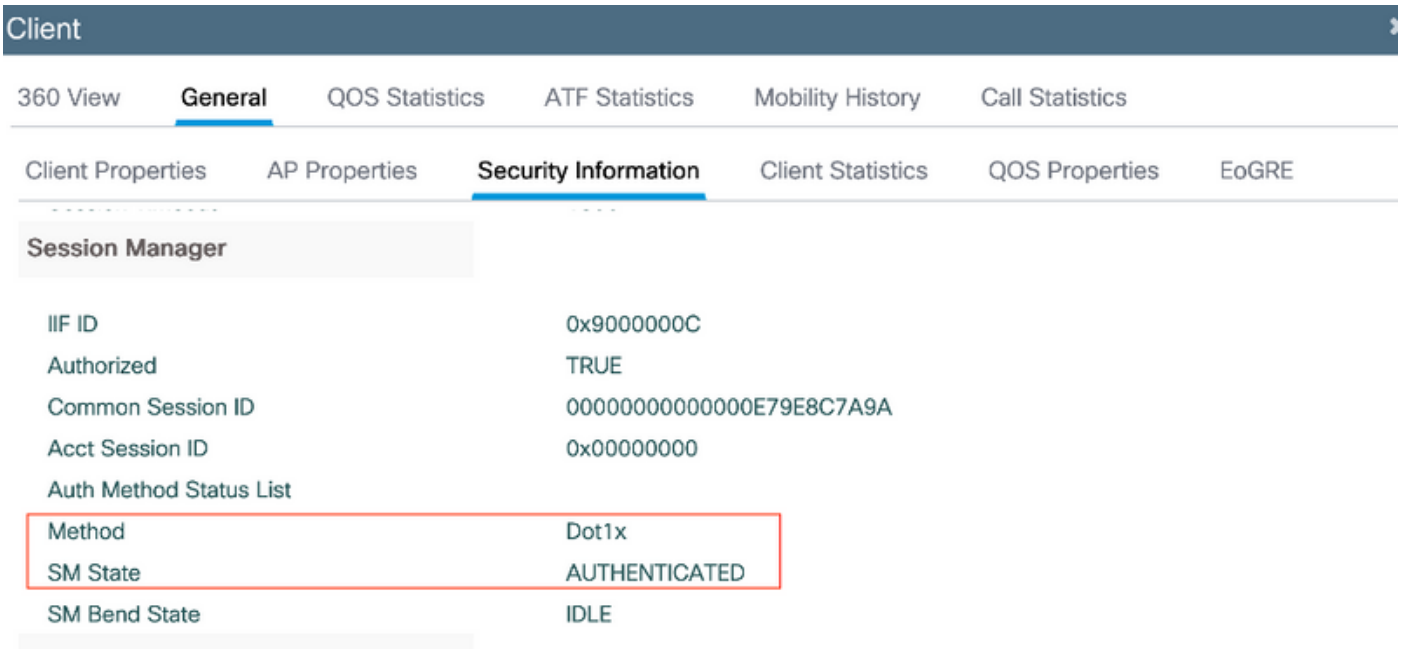
Pas de instellingen toe en controleer de status.



7. Sluit een pc in de LAN3-poort van het AP aan. PC zal worden geauthentiseerd via 802.1x en krijgt een IP adres van het geconfigureerde VLAN.

Navigeer naar **bewaking >Draadloos > Clients** om de status van de client te controleren.






```
vk-9800-1#show wireless client summary
Number of Clients: 2
MAC Address    AP Name                                          Type ID   State
Protocol Method     Role
--------------------------------------------------------------------------------------------------
-------------------------
503e.aab7.0ff4 AP1815                                           WLAN 3    Run
11n(2.4) None       Local
b496.9126.dd6c AP1810                                           RLAN 1    Run
Ethernet Dot1x      Local
Number of Excluded Clients: 0
```

Problemen oplossen

Vaak voorkomende problemen:

- Alleen het werk van lokale SSID, is SSID ingesteld op WLC dat niet wordt uitgezonden: controleer of AP zich goed bij de controller heeft aangesloten.
- Geen toegang tot de OEAP GUI: Controleer of ap IP-adres heeft en controleer bereikbaarheid (firewall, ACL, enz in netwerk)
- Centraal switched draadloze of bekabelde klanten die niet kunnen authenticeren of het IP-adres verkrijgen: Neem RA sporen, altijd op sporen, enz.

Steekproef van altijd op sporen voor de bekabelde 802.1x-client:

[client-orch-sm] [18950]: (note): MAC: <client-mac> Association received. BSSID 00b0.e187.cfc0, old BSSID 0000.0000.0000, WLAN test_rlan, Slot 2 AP 00b0.e187.cfc0, Ap_1810

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_INIT -> S_CO_ASSOCIATING

[dot11-validate] [18950]: (ERR): MAC: <client-mac> Failed to dot11 determine ms physical radio type. Invalid radio type :0 of the client.

[dot11] [18950]: (ERR): MAC: <client-mac> Failed to dot11 send association response. Encoding of assoc response failed for client reason code: 14.

[dot11] [18950]: (note): MAC: <client-mac> Association success. AID 1, Roaming = False, WGB = False, 11r = False, 11w = False AID list: 0x1| 0x0| 0x0| 0x0

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS

[client-auth] [18950]: (note): MAC: <client-mac> ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 00b0.e187.cfc0 capwap IFID: 0x90000012

[client-auth] [18950]: (note): MAC: <client-mac> L2 Authentication initiated. method DOT1X, Policy VLAN 1119,AAA override = 0 , NAC = 0

[ewlc-infra-evq] [18950]: (note): Authentication Success. Resolved Policy bitmap:11 for client <client-mac>

[client-orch-sm] [18950]: (note): MAC: <client-mac> Mobility discovery triggered. Client mode: Local

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS

[mm-client] [18950]: (note): MAC: <client-mac> Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Previous BSSID MAC: 0000.0000.0000   Client IFID: 0xa0000003, Client Role: Local PoA: 0x90000012 PoP: 0x0

[client-auth] [18950]: (note): MAC: <client-mac> ADD MOBILE sent. Client state flags: 0x72 BSSID: MAC: 00b0.e187.cfc0 capwap IFID: 0x90000012

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS

[dot11] [18950]: (note): MAC: <client-mac> Client datapath entry params - ssid:test_rlan,slot_id:2 bssid ifid: 0x0, radio_ifid: 0x90000006, wlan_ifid: 0xf0404001

[dpath_svc] [18950]: (note): MAC: <client-mac> Client datapath entry created for ifid 0xa0000003

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS

[client-iplearn] [18950]: (note): MAC: <client-mac> Client IP learn successful. Method: DHCP IP: <Cliet-IP>

[apmgr-db] [18950]: (ERR): 00b0.e187.cfc0 Get ATF policy name from WLAN profile:: Failed to get wlan profile. Searched wlan profile test_rlan

[apmgr-db] [18950]: (ERR): 00b0.e187.cfc0 Failed to get ATF policy name

[apmgr-bssid] [18950]: (ERR): 00b0.e187.cfc0 Failed to get ATF policy name from WLAN profile name: No such file or directory

```
[client-orch-sm] [18950]: (ERR): Failed to get client ATF policy name: No such file or directory

[client-orch-state] [18950]: (note): MAC: <client-mac>  Client state transition:
S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN
```