Dynamische VLAN-toewijzing met WLC's configureren op basis van ISE naar Active Directory Group Map

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten
- Conventies

Dynamische VLAN-toewijzing met RADIUS-server

Configureren

- Netwerkdiagram
- Configuraties
- ISE-naar-AD-integratie en configuratie van verificatie- en autorisatiebeleid voor gebruikers op ISE
- WLC-configuratie naar Support Dot1x-verificatie en AAA-overschrijding voor SSID 'office_hq'

Verifiëren

Problemen oplossen

Inleiding

Dit document beschrijft het concept van de dynamische VLAN-toewijzing.

Voorwaarden

Het document beschrijft hoe u de Wireless LAN controller (WLC)- en Identity Services Engine (ISE)-server moet configureren om draadloze LAN (WLAN)-clients dynamisch in een specifiek VLAN toe te wijzen.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van draadloze LAN-controllers (WLC's) en lichtgewicht access points (LAP's)
- Functionele kennis van een AAA-server (Verificatie, autorisatie en accounting) zoals een ISE
- Grondige kennis van draadloze netwerken en problemen met draadloze beveiliging
- Functionele en configureerbare kennis van dynamische VLAN-toewijzing
- Basiskennis van Microsoft Windows AD-services, evenals een domeincontroller en DNS-

concepten
- Basiskennis hebben van Control and Provisioning of Access Point Protocol (CAPWAP)

Gebruikte componenten

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

- Cisco 5520 Series WLC die firmware-release 8.8.11.0 uitvoert
- Cisco 4800 Series access point
- Native Windows-applicatie en AnyConnect NAM
- Cisco Secure ISE-versie 2.3.0.298
- Microsoft Windows 2016 Server geconfigureerd als domeincontroller
- Cisco 3560-CX Series-Switch waarop versie 15.2(4)E1 wordt uitgevoerd

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.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Dynamische VLAN-toewijzing met RADIUS-server

In de meeste WLAN-systemen heeft elk WLAN een statisch beleid dat van toepassing is op alle clients die zijn gekoppeld aan een Service Set Identifier (SSID) of WLAN in de controllerterminologie. Hoewel krachtig, heeft deze methode beperkingen omdat het cliënten vereist om met verschillende SSIDs te associëren om verschillend QoS en veiligheidsbeleid te erven.

Cisco WLAN-oplossing biedt een oplossing voor deze beperking door ondersteuning van identiteitsnetwerken. Hiermee kan het netwerk één SSID adverteren, maar kunnen specifieke gebruikers verschillende QoS, VLAN-kenmerken en/of beveiligingsbeleid erven op basis van de gebruikersreferenties.

Dynamische VLAN-toewijzing is zo'n functie die een draadloze gebruiker in een specifiek VLAN plaatst op basis van de referenties die door de gebruiker worden geleverd. Deze taak om gebruikers toe te wijzen aan een specifiek VLAN wordt uitgevoerd door een RADIUS-verificatieserver, zoals Cisco ISE. Dit kan bijvoorbeeld worden gebruikt om de draadloze host in

staat te stellen op hetzelfde VLAN te blijven als het binnen een campusnetwerk beweegt.

De Cisco ISE-server verifieert draadloze gebruikers aan de hand van een van de verschillende mogelijke databases, waaronder de interne database. Voorbeeld:

- Interne DB
- Active Directory
- Generic Lichtgewicht Directory Access Protocol (LDAP)
- Open Database Connectivity (ODBC)-conforme relationele databases
- Rivest, Shamir en Adelman (RSA) SecurityID-token servers
- RADIUS-conforme token-servers

Cisco ISE-verificatieprotocollen en ondersteunde externe identiteitsbronnen maken een lijst van de verschillende verificatieprotocollen die worden ondersteund door interne en externe ISE-databases.

Dit document concentreert zich op het verifiëren van draadloze gebruikers die externe database van Windows Active Directory gebruiken.

Na een succesvolle verificatie haalt ISE de groepsinformatie van die gebruiker uit de Windows-database en koppelt de gebruiker aan het betreffende autorisatieprofiel.

Wanneer een client probeert te associëren met een LAP die is geregistreerd bij een controller, geeft de LAP de referenties van de gebruiker door aan de WLC met behulp van de betreffende EAP-methode.

WLC stuurt deze referenties naar ISE met behulp van het RADIUS-protocol (dat het EAP inkapselt) en ISE geeft de referenties van gebruikers door aan AD voor validatie met behulp van het KERBEROS-protocol.

AD valideert de gebruikersreferenties en informeert de ISE wanneer de verificatie is geslaagd.

Zodra de verificatie succesvol is, geeft de ISE-server bepaalde Internet Engineering Task Force (IETF)-kenmerken door aan WLC. Deze RADIUS-kenmerken bepalen welke VLAN-id aan de draadloze client moet worden toegewezen. De SSID (WLAN, in termen van WLC) van de client is niet van belang, omdat de gebruiker altijd wordt toegewezen aan deze vooraf bepaalde VLAN-id.

De RADIUS-gebruikerskenmerken die voor de VLAN-id-toewijzing worden gebruikt, zijn:

- IETF 64 (tunneltype)—Dit instellen op VLAN
- IETF 65 (tunnel van middelgroot type)—Dit instellen op 802
- IETF 81 (Tunnel Private Group ID)—Dit instellen op VLAN-id

De VLAN-id is 12 bits en neemt een waarde tussen 1 en 4094, inclusief. Omdat de Tunnel-

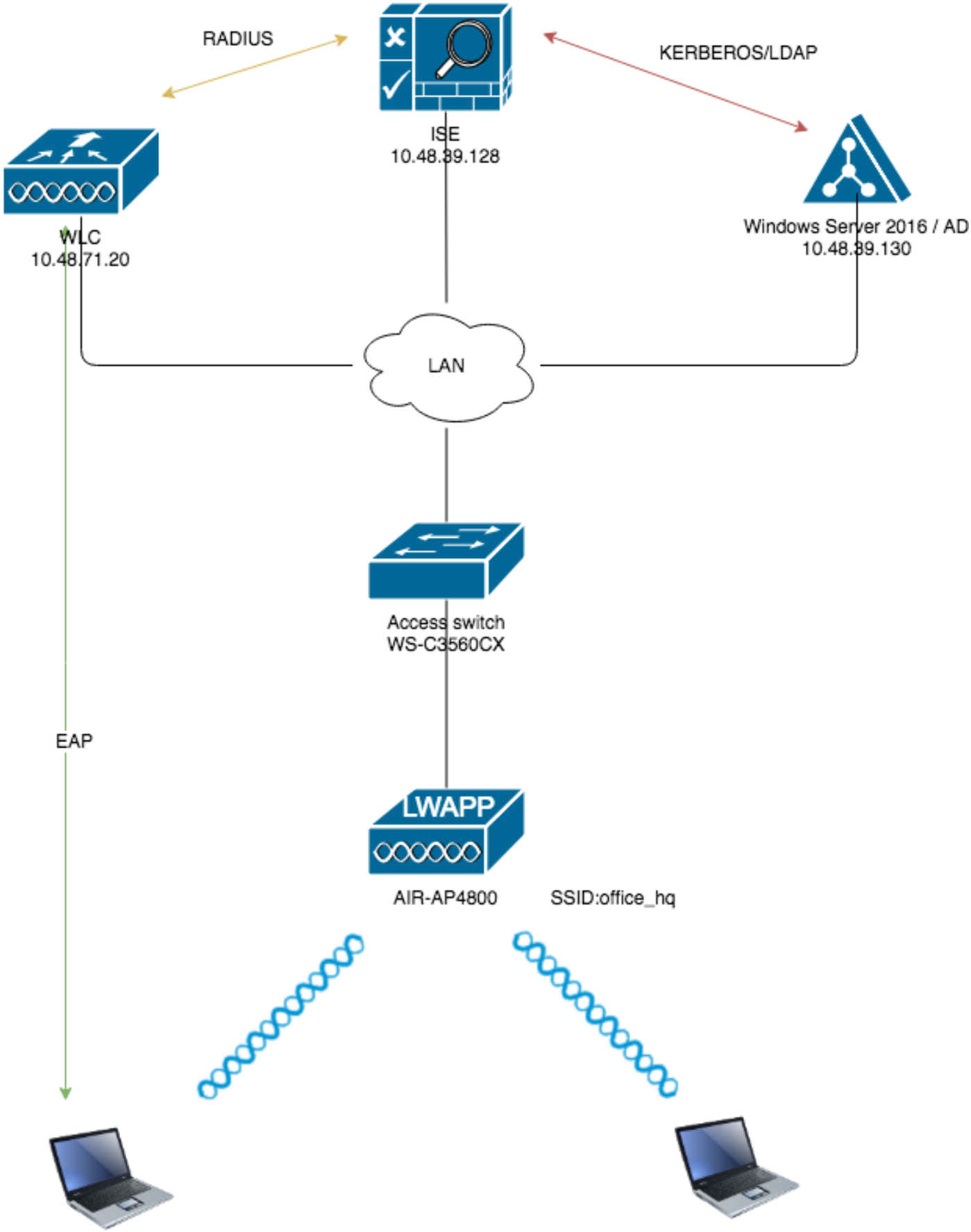
Private-Group-ID van het type-string is, zoals gedefinieerd in RFC2868 voor gebruik met IEEE 802.1X, wordt de waarde van het VLAN-ID-integer gecodeerd als een string. Wanneer deze tunnelkenmerken worden verzonden, is het noodzakelijk om het veld Tag in te vullen.

Zoals opgemerkt in RFC 2868, paragraaf 3.1: het Tag-veld is één octet in lengte en is bedoeld om een middel te bieden om attributen in hetzelfde pakket te groeperen die naar dezelfde tunnel verwijzen. De geldige waarden voor dit veld zijn 0x01 tot 0x1F, inclusief. Als het veld Tag niet wordt gebruikt, moet deze nul zijn (0x00). Raadpleeg RFC 2868 voor meer informatie over alle RADIUS-kenmerken.

Configureren

Deze sectie verschaft de informatie die nodig is om de beschreven functies in het document te kunnen configureren.

Netwerkdiagram

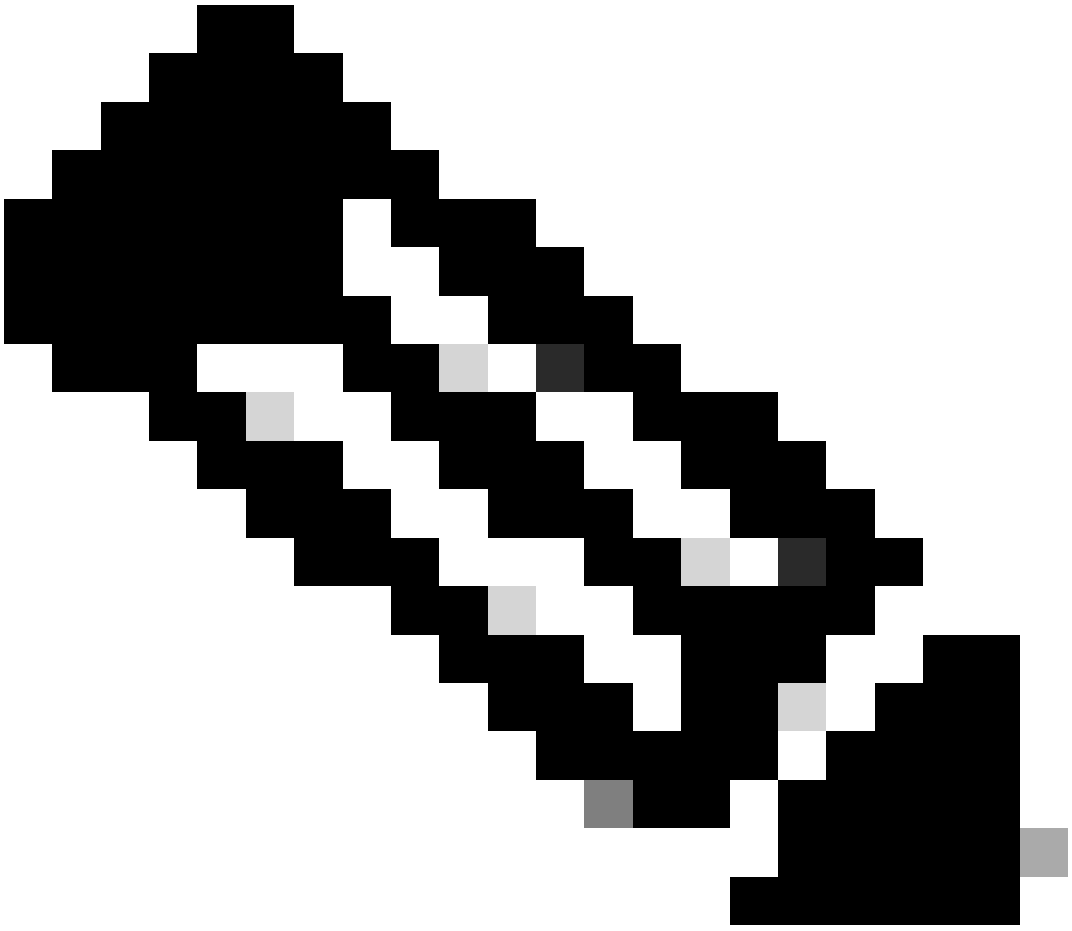


Configuraties

Dit zijn de configuratiedetails van de componenten die in dit diagram worden gebruikt:

- Het IP-adres van de ISE (RADIUS)-server is 10.48.39.128.
- Het beheer en AP-manager interfaceadres van de WLC is 10.48.71.20.
- DHCP-server bevindt zich in het LAN-netwerk en is geconfigureerd voor de desbetreffende clientpools; dit wordt niet in het diagram weergegeven.
- VLAN1477 en VLAN1478 worden gebruikt in deze configuratie. Gebruikers van de Marketing afdeling zijn geconfigureerd om in de VLAN1477 te worden geplaatst en gebruikers van de HR afdeling zijn geconfigureerd om in VLAN1478 te worden geplaatst door de RADIUS-server wanneer beide gebruikers verbinding maken met dezelfde SSID — office_hq.

  VLAN1477: 192.168.77.0/24 Gateway: 192.168.77.1 VLAN1478: 192.168.78.0/24. Gateway: 192.168.78.1
- In dit document wordt 802.1x gebruiktPEAP-mschapv2als beveiligingsmechanisme.



Opmerking: Cisco raadt u aan geavanceerde verificatiemethoden te gebruiken, zoals EAP-FAST- en EAP-TLS-verificatie, om het WLAN te beveiligen.

Deze veronderstellingen worden gemaakt alvorens u deze configuratie uitvoert:

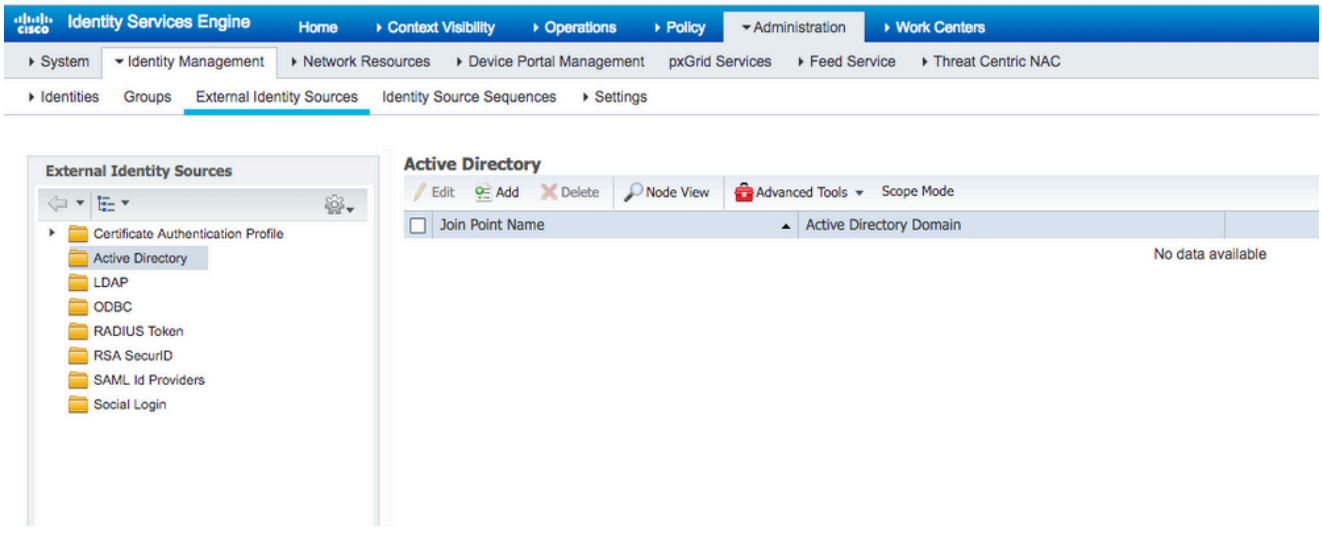
- De LAP is al geregistreerd bij de WLC
- De DHCP-server is een DHCP-scope toegewezen
- Layer 3-connectiviteit bestaat tussen alle apparaten in het netwerk
- Het document bespreekt de configuratie die aan de draadloze kant is vereist en gaat ervan uit dat het bekabelde netwerk is geïnstalleerd
- De respectieve gebruikers en groepen zijn ingesteld op AD

Om dynamische VLAN-toewijzing met WLC's op basis van ISE-naar-AD-groepstoewijzing te realiseren, moeten deze stappen worden uitgevoerd:

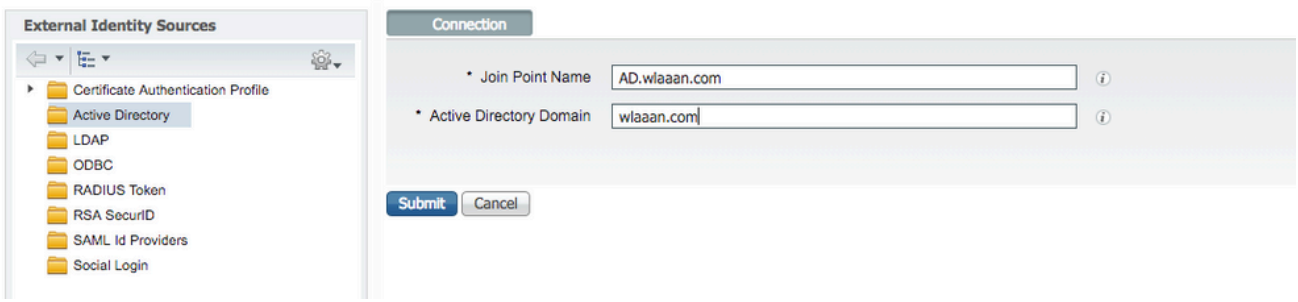
1. ISE-naar-AD-integratie en configuratie van verificatie- en autorisatiebeleid voor gebruikers op ISE.
2. WLC-configuratie ter ondersteuning van dot1x-verificatie en AAA-opheffing voor SSID 'office_hq'.
3. Configuratie van endclient-aanvrager.

ISE-naar-AD-integratie en configuratie van verificatie- en autorisatiebeleid voor gebruikers op ISE

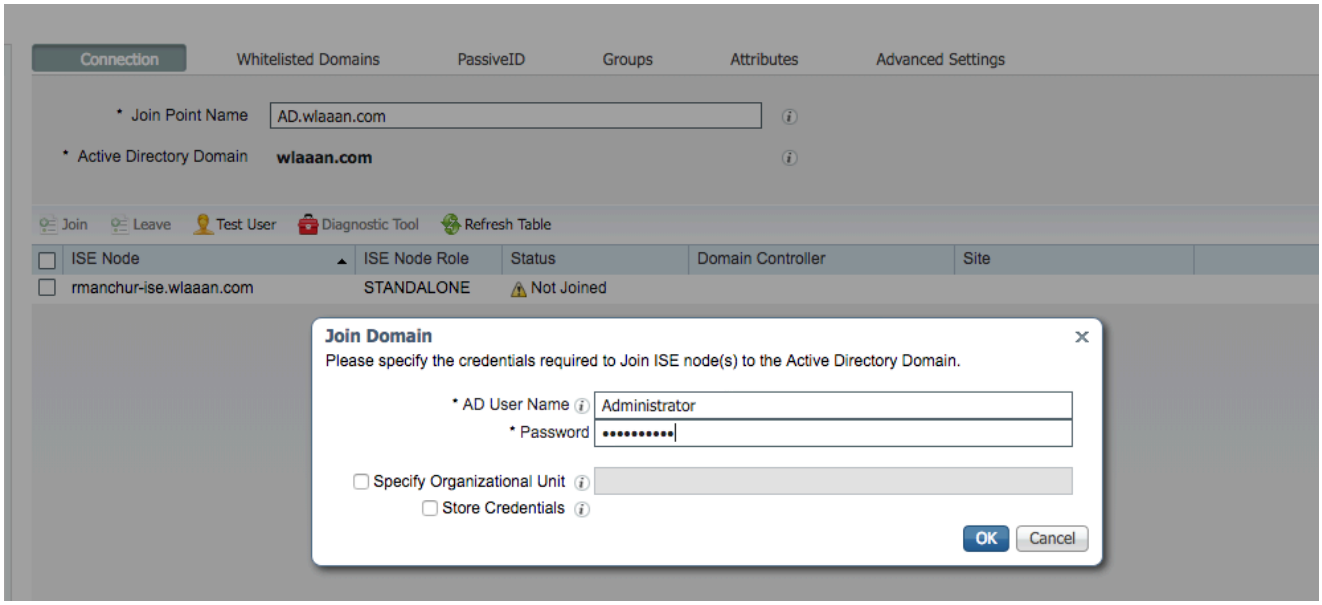
1. Login aan de interface van het Web UI van ISE met behulp van een admin- rekening.
2. Navigeer naarAdministration > Identity management > External Identity Sources > Active directory.



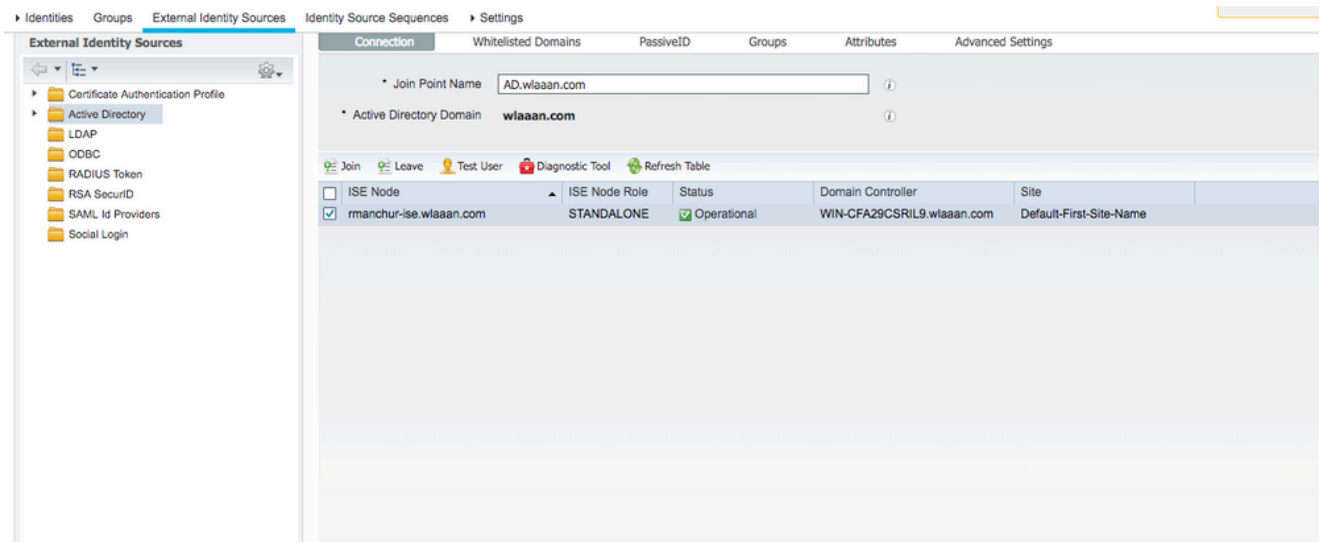
3. Klik op Add en voer de domeinnaam en de naam van de identiteitsopslag in vanuit de Active Directory Join Point Name instellingen. In het voorbeeld wordt ISE geregistreerd voor het domeinwlaaan.comen is aanspreekpunt aangegeven alsAD.wlaaan.com- plaatselijk belangrijke naam voor ISE.



4. Er verschijnt een pop-upvenster nadat Submit op de knop is gedrukt die u vraagt of u zich onmiddellijk bij ISE wilt aanmelden voor AD. Druk op Yes en geef Active Directory gebruikersreferenties met beheerdersrechten om een nieuwe host aan het domein toe te voegen.



5. Na dit punt moet ISE zijn geregistreerd bij AD.



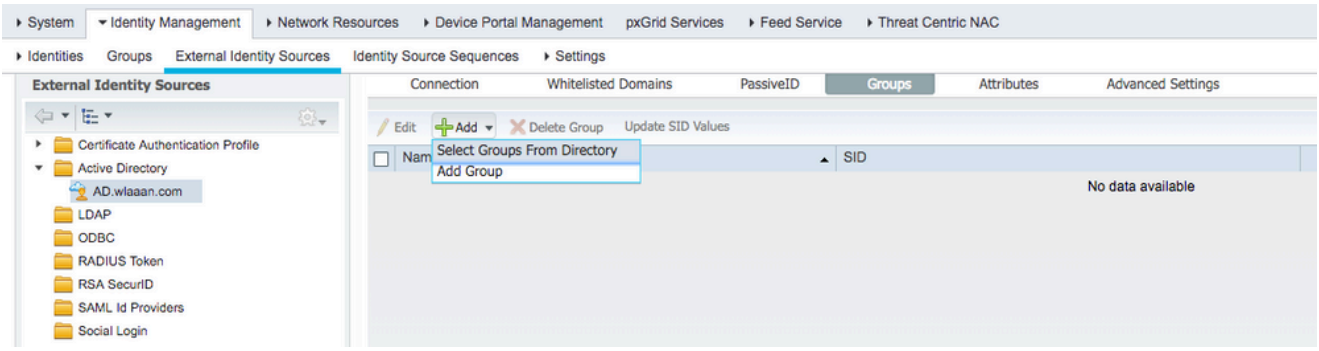
Als u problemen hebt met het registratieproces, kunt u deze gebruiken om Diagnostic Tool de

tests uit te voeren die vereist zijn voor verbinding met de AD.

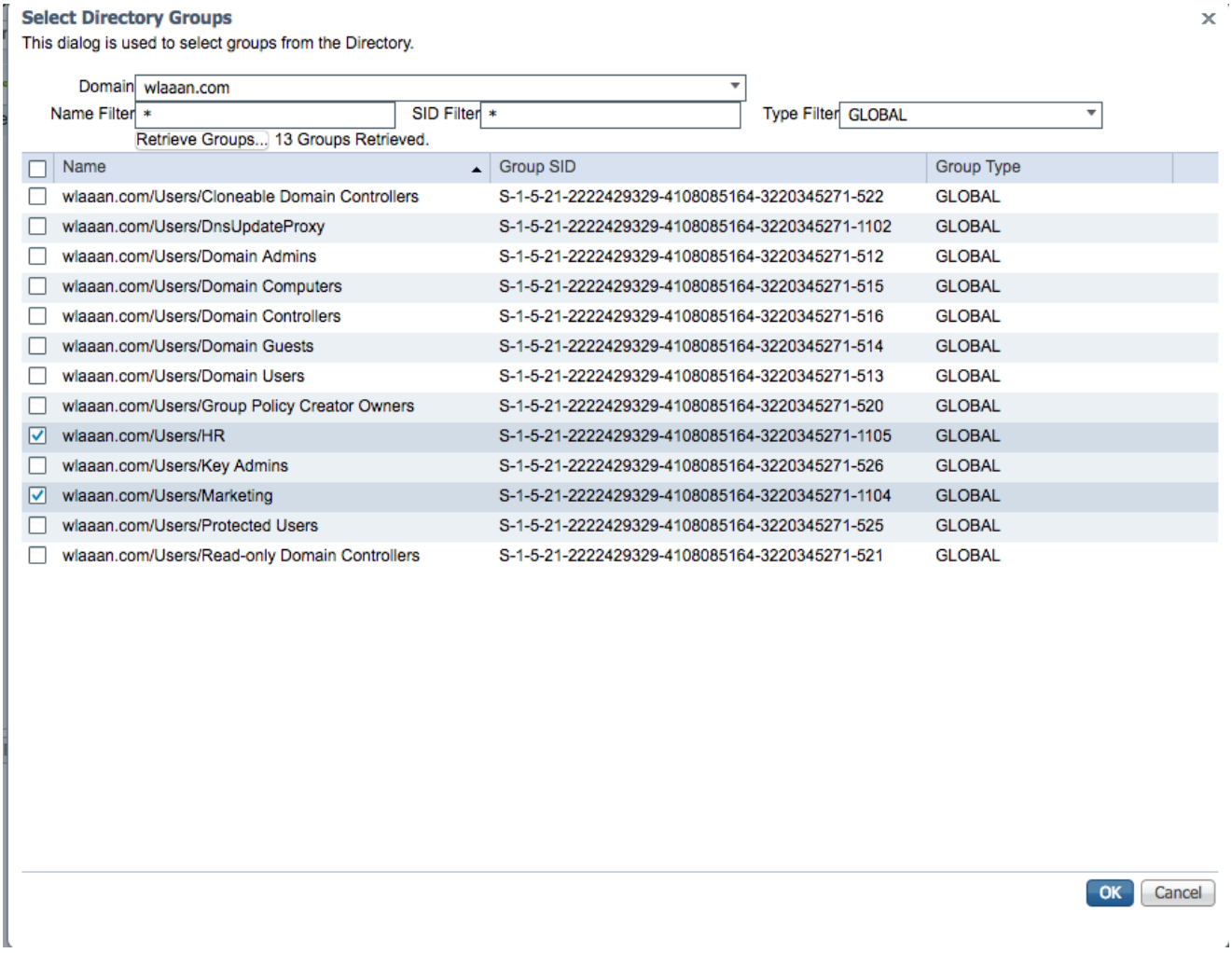
6. U moet groepen ophalen voor de actieve directory's die worden gebruikt om respectievelijke autorisatieprofielen toe te wijzen. Navigeer naarAdministration > Identity management > External Identity Sources > Active directory >

   > Groups

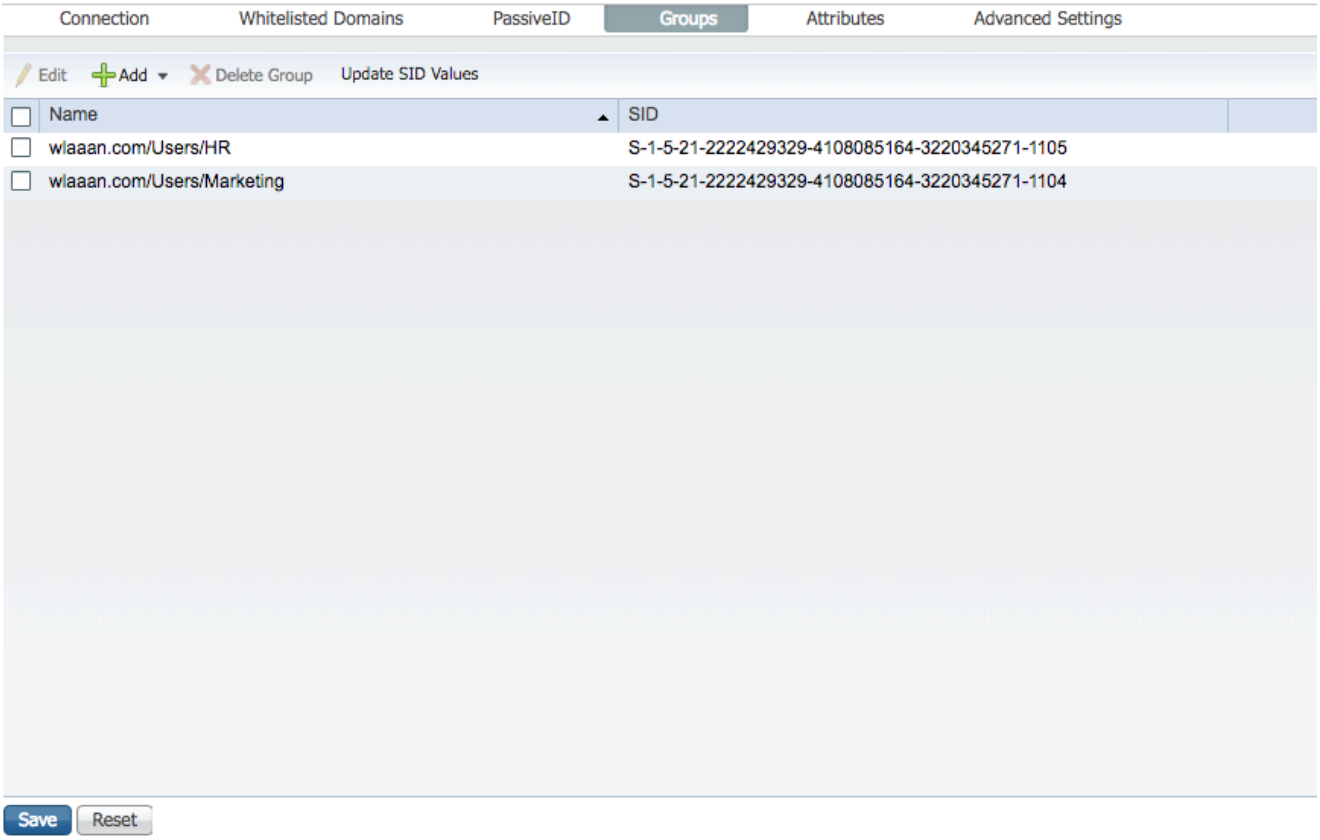
   , klik vervolgens opAddenkiesSelect Groups from Active Directory.



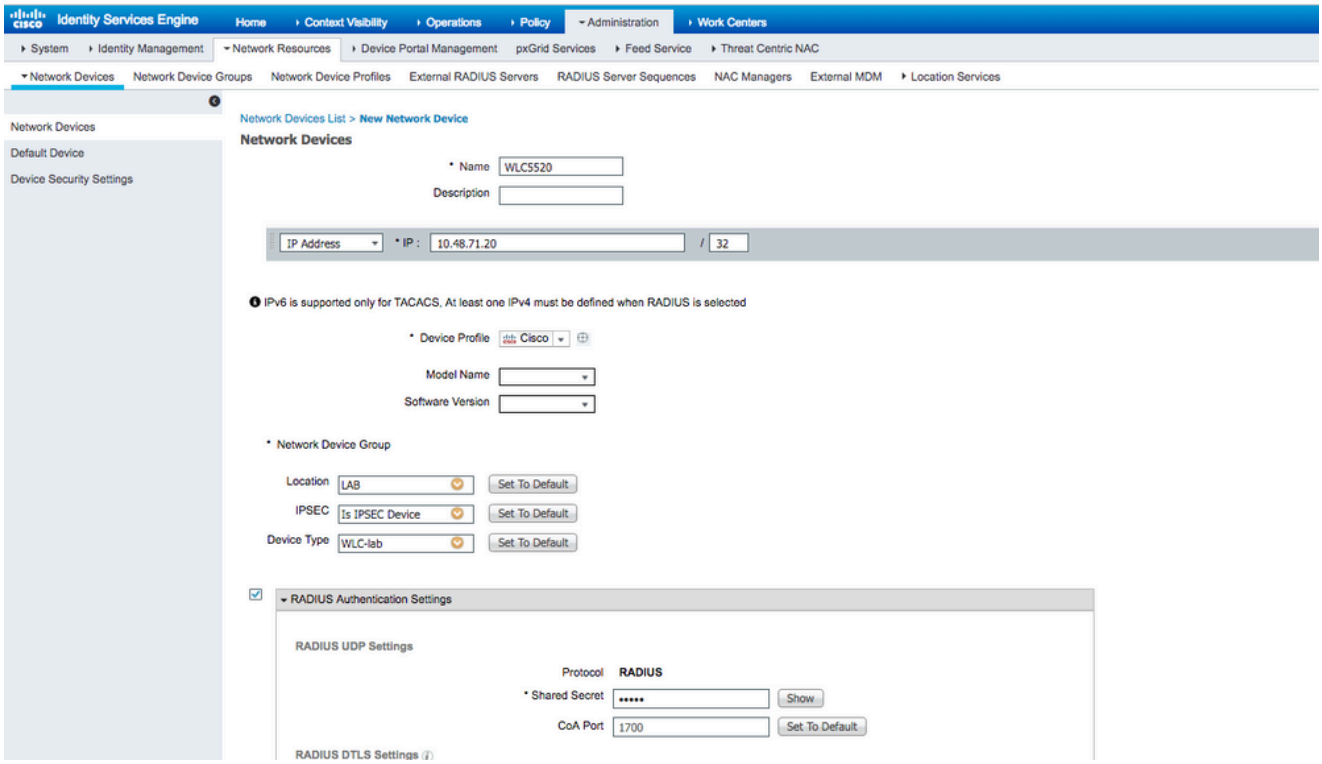
7. Er wordt een nieuw pop-upvenster geopend waarin u een filter kunt instellen om specifieke groepen op te halen of alle groepen uit de AD kunt ophalen.
   Kies de betreffende groepen in de lijst AD-groepen en druk opOK.



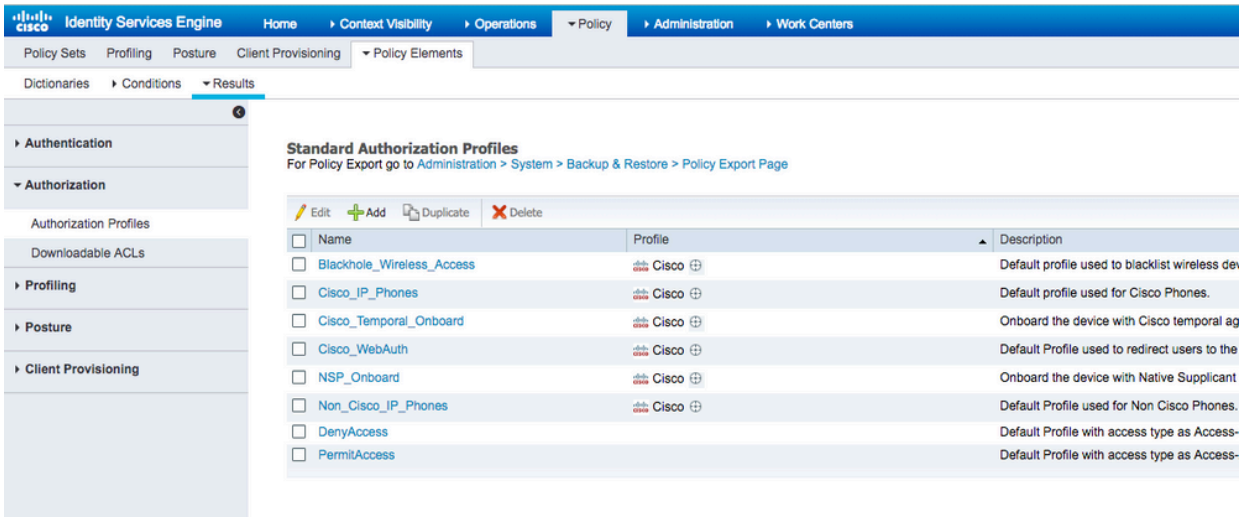
8. Respectieve groepen worden toegevoegd aan ISE en kunnen worden opgeslagen. Druk opSave.



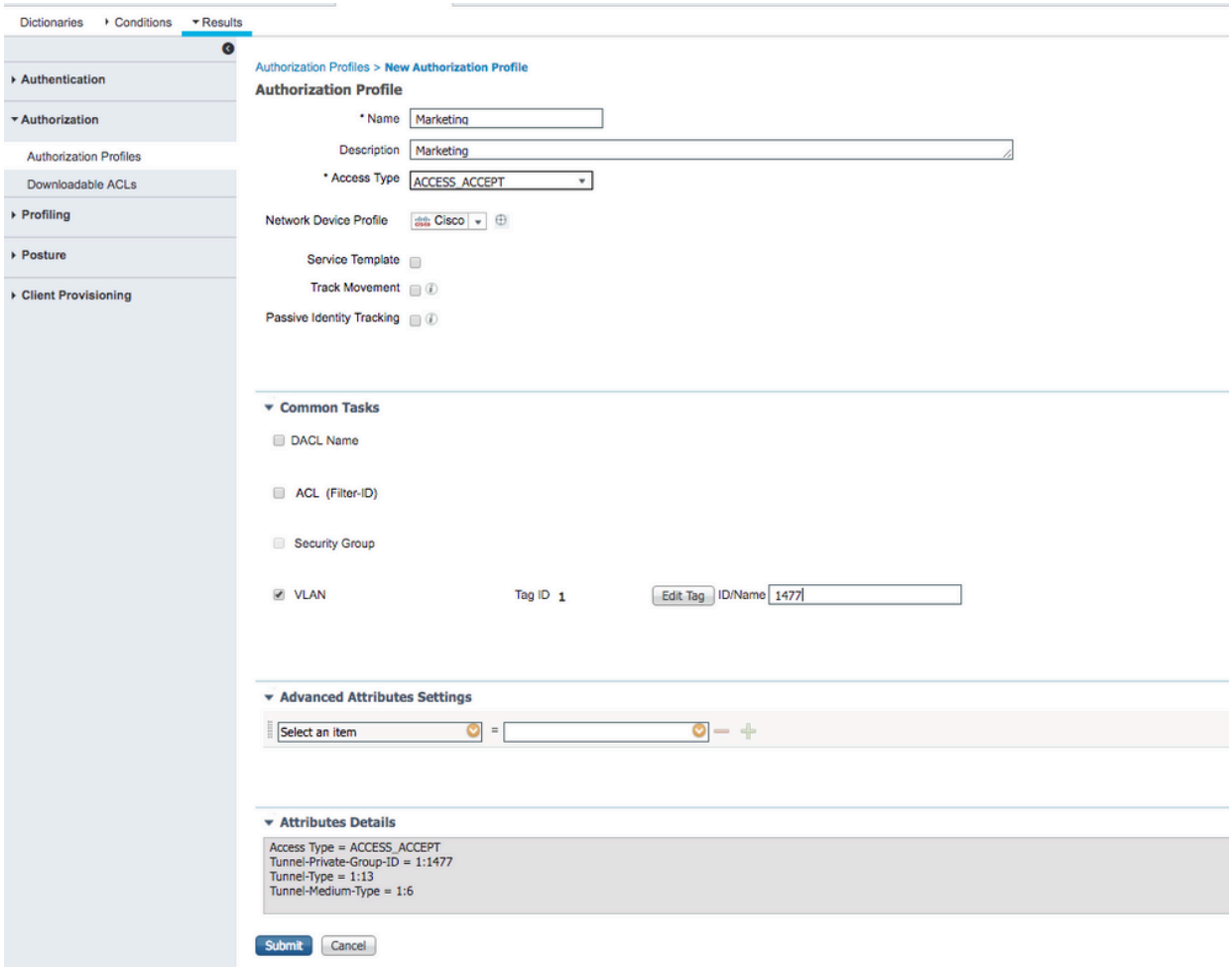
9. Voeg WLC toe aan de lijst met ISE-netwerkapparaten - navigeer naarAdministration > Network Resources > Network Devicesen druk opAdd.
   Volledige configuratie, door WLC beheer IP adres en RADIUS gedeeld geheim tussen WLC en ISE te verstrekken.



10. Nadat u zich hebt aangesloten bij ISE naar AD en de WLC hebt toegevoegd aan de lijst met apparaten, kunt u de configuratie van verificatie- en autorisatiebeleid voor gebruikers starten.
    - Maak een autorisatieprofiel om gebruikers van Marketing aan VLAN1477 toe te wijzen en van de HR-groep aan VLAN1478.
      Navigeer naarPolicy > Policy Elements > Results > Authorization > Authorization profilesen klik op de knopAddom een nieuw profiel te maken.

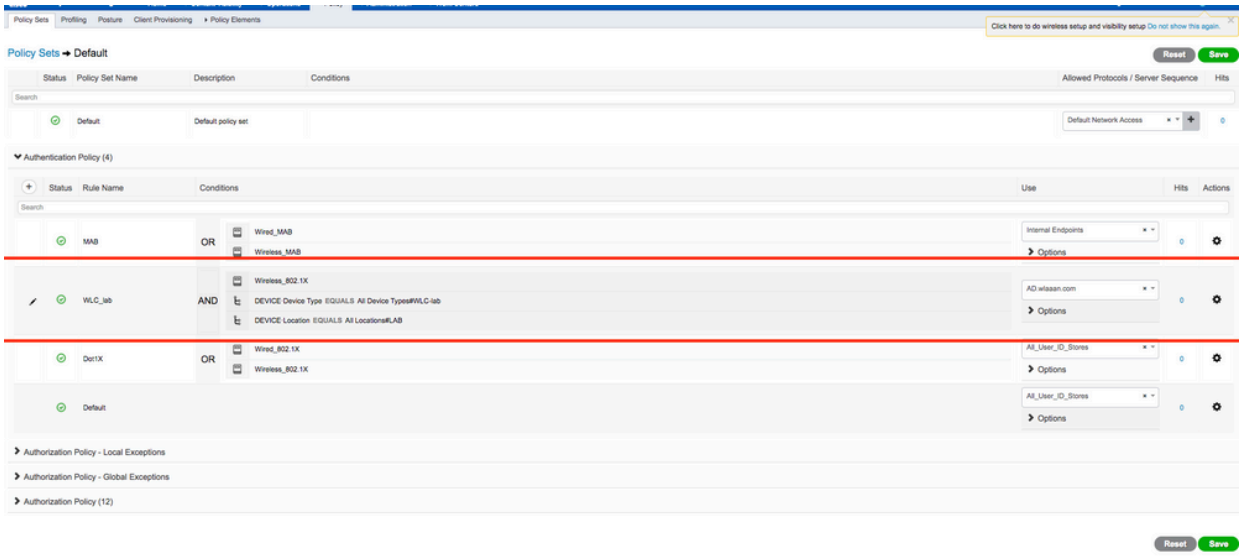


    - Voltooi de configuratie van het vergunningsprofiel met de informatie van VLAN voor de respectieve groep; het voorbeeld toont de instellingen van de groepsconfiguratieMarketing.

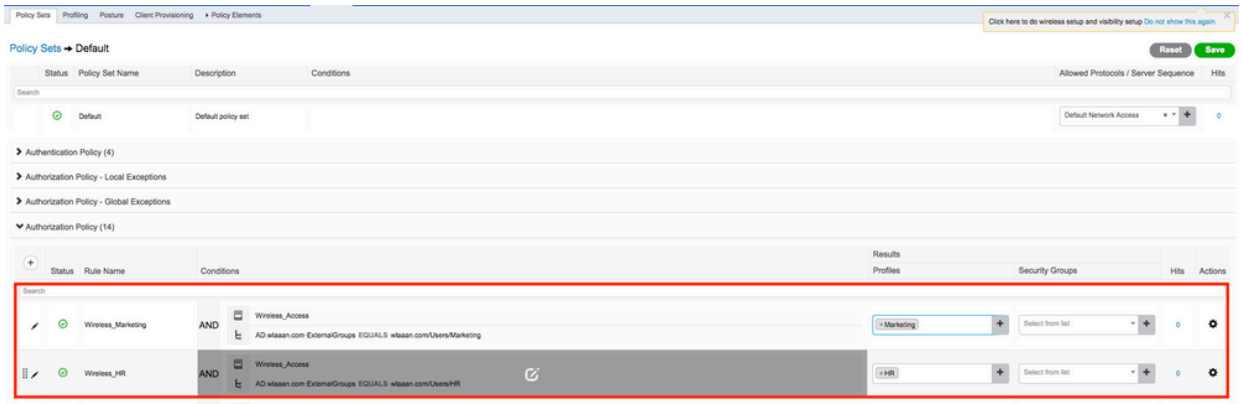


Een soortgelijke configuratie moet worden uitgevoerd voor andere groepen en de bijbehorende VLAN-tagkenmerken moeten worden geconfigureerd.

- Nadat de autorisatieprofielen zijn geconfigureerd, kunt u een verificatiebeleid voor draadloze gebruikers definiëren. CustomDit kan worden gedaan door deDefaultbeleidsset te configureren of aan te passen. In dit voorbeeld wordt de Standaardbeleidsset gewijzigd. Navigeer naarPolicy > Policy Sets > Default. Standaard voordot1xverificatietype zal ISE worden gebruiktAll_User_ID_Stores, hoewel het werkt zelfs met de huidige standaardinstellingen omdat AD deel uitmaakt van de lijst met identiteitsbronnen vanAll_User_ID_Stores, dit voorbeeld gebruikt een specifiekere regelWLC_labvoor die betreffende LAB-controller en gebruikt AD als de enige bron voor verificatie.

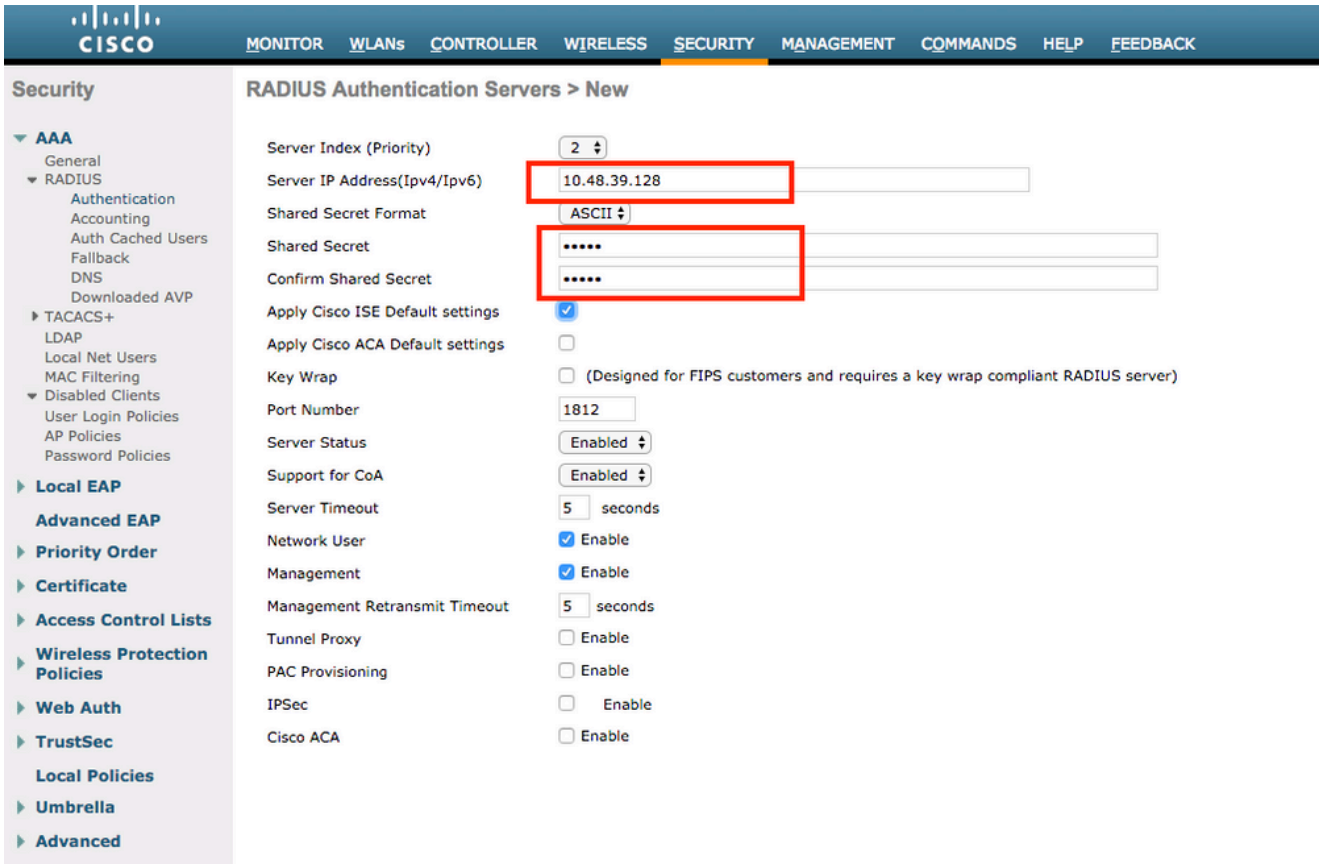


- Nu moet u autorisatiebeleid maken voor gebruikers die respectievelijke autorisatieprofielen toekennen op basis van groepslidmaatschap. Navigeer naarAuthorization policysectie en maak beleid om dat vereiste te realiseren.

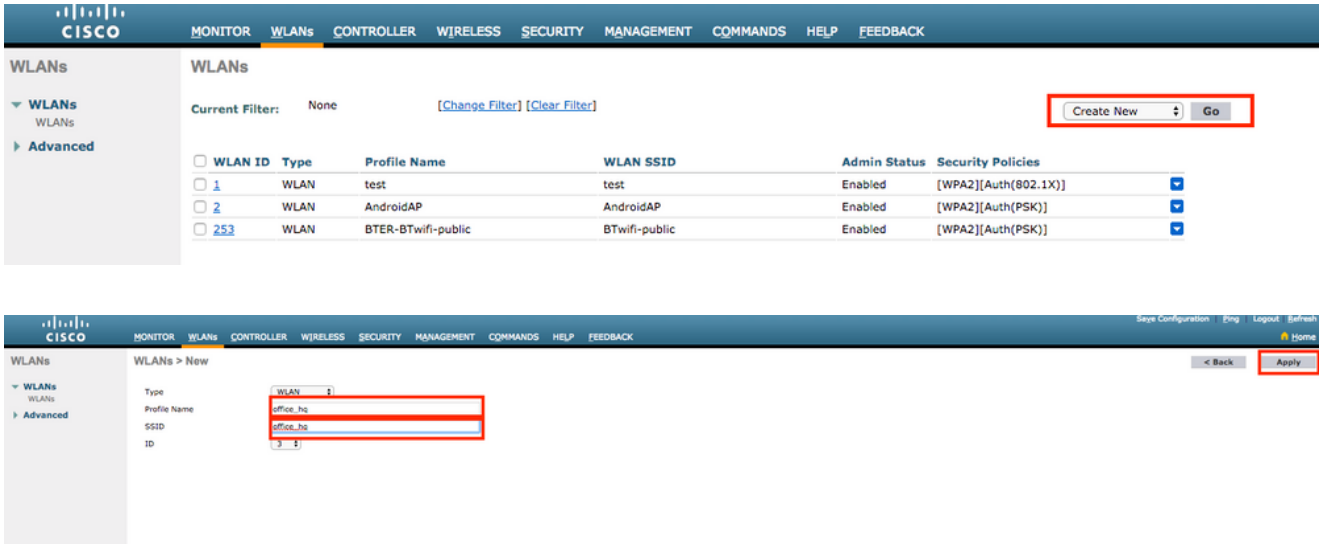


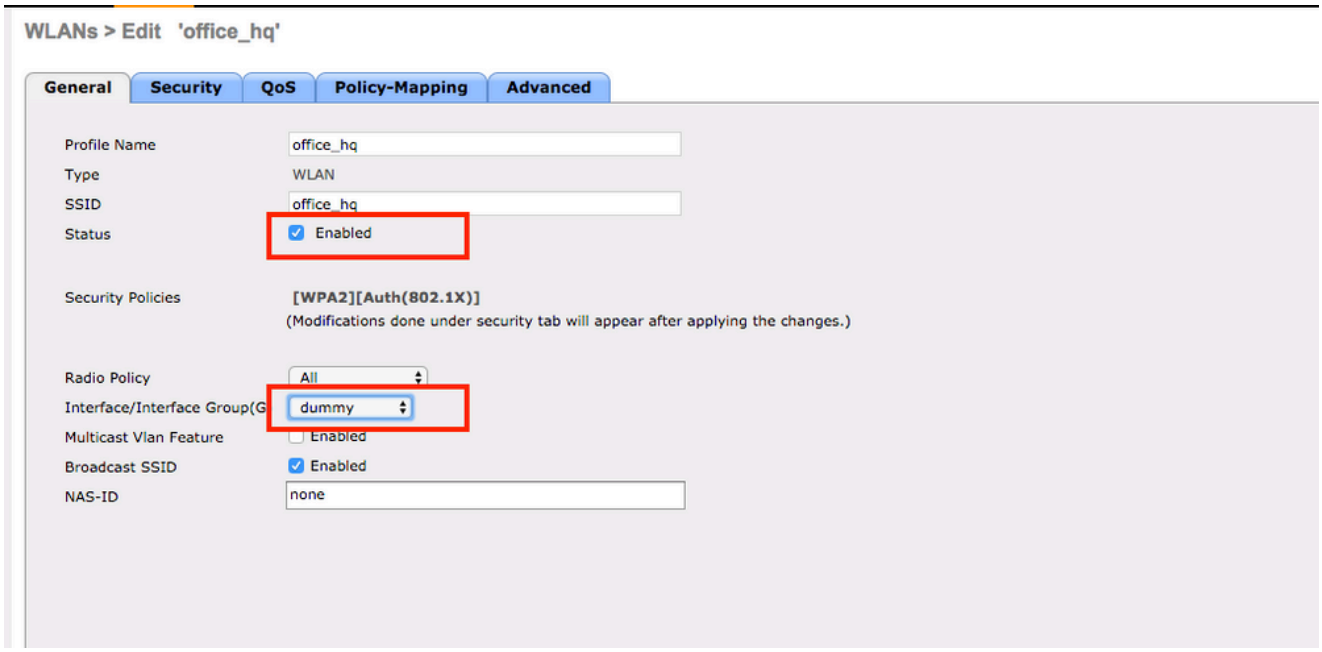
WLC-configuratie ter ondersteuning van dot1x-verificatie en AAA-overschrijding voor SSID 'office_hq'

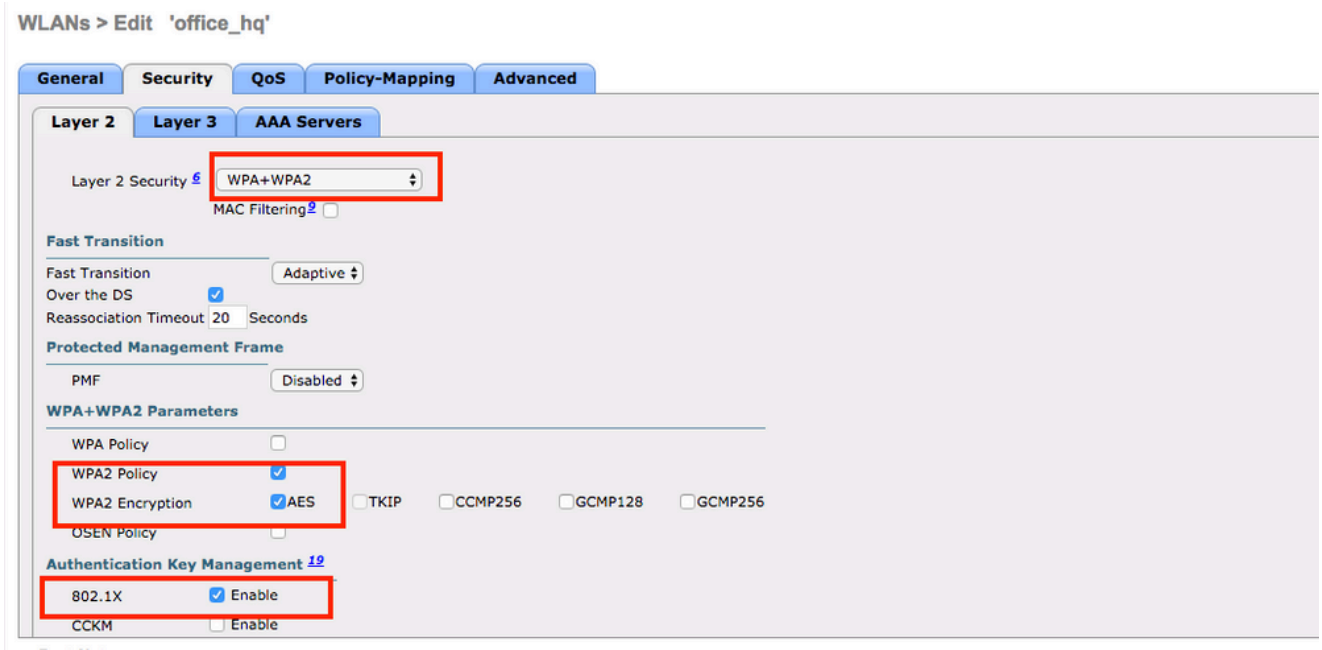
1. Configureer ISE als een RADIUS-verificatieserver op WLC. Navigeer naarSecurity > AAA > RADIUS > Authenticationsectie in de web UI-interface en geef het ISE IP-adres en gedeelde geheime informatie.

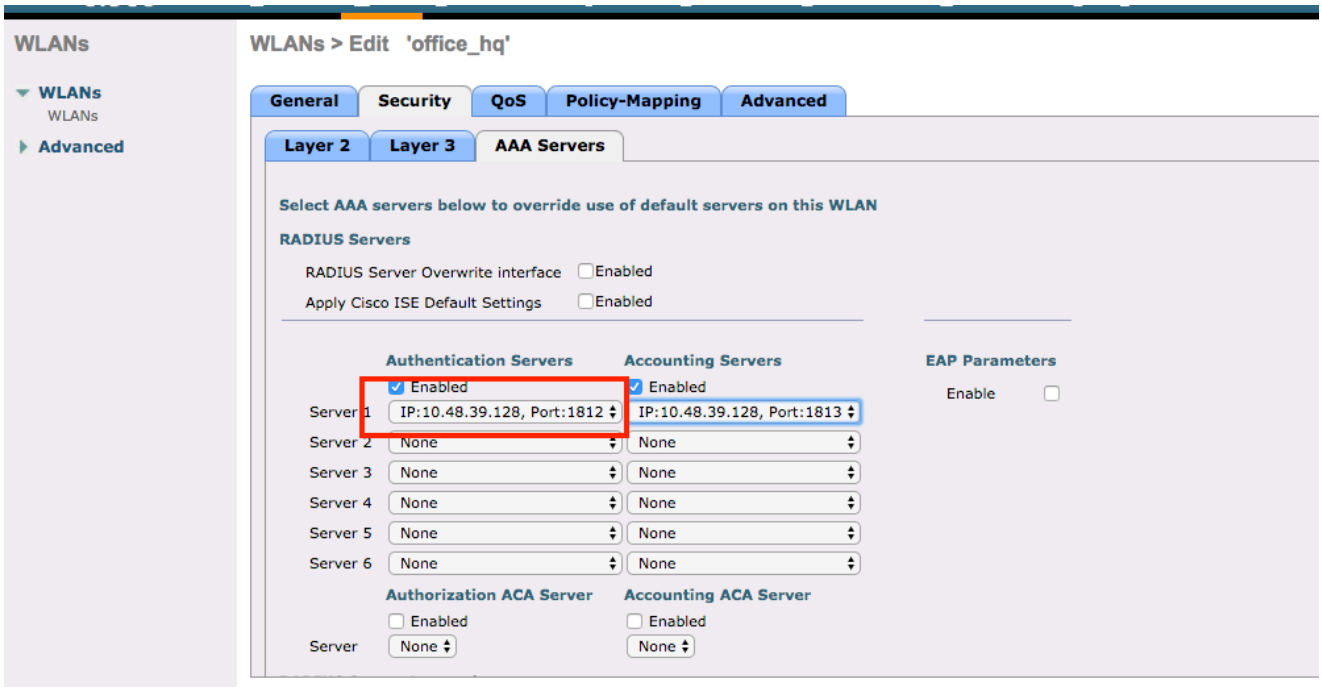


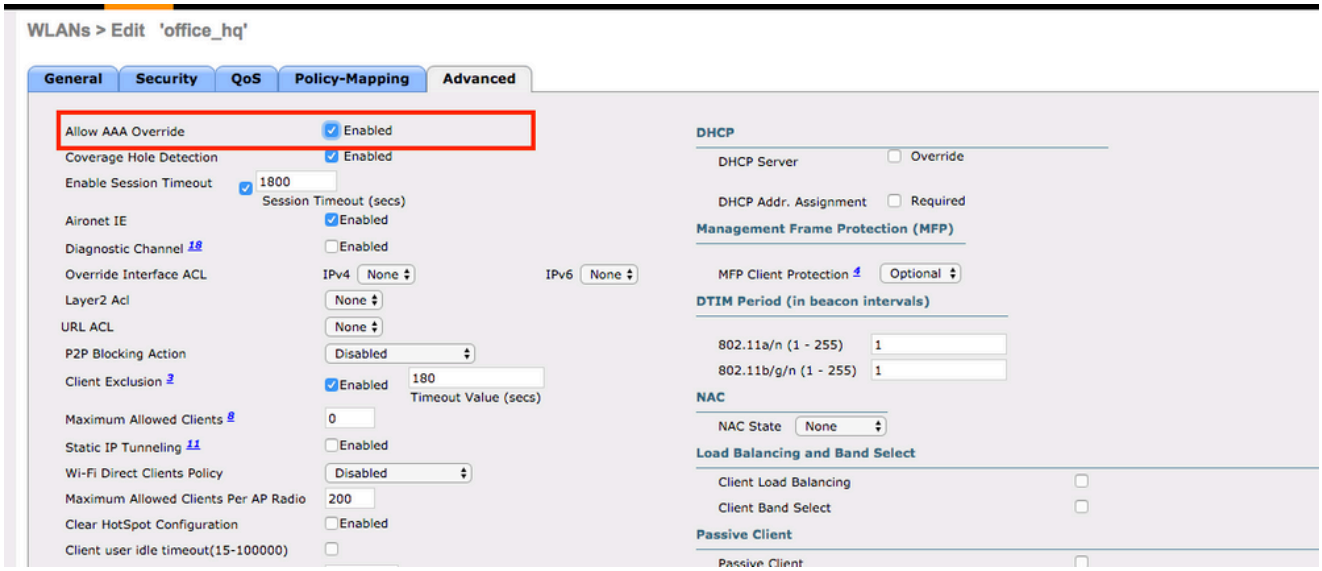
2. Configureer SSIDoffice_hqonder de sectieWLANsWLC; in dit voorbeeld worden SSID metWPA2/AES+dot1xen AAA-override geconfigureerd. De interfaceDummywordt gekozen voor het WLAN omdat het juiste VLAN hoe dan ook via RADIUS wordt toegewezen. Deze dummy interface moet worden gemaakt op de WLC en moet een IP-adres krijgen, maar het IP-adres hoeft niet geldig te zijn en het VLAN waarin het wordt gezet kan niet worden gemaakt in de uplink-switch, zodat als er geen VLAN wordt toegewezen, de client nergens kan gaan.



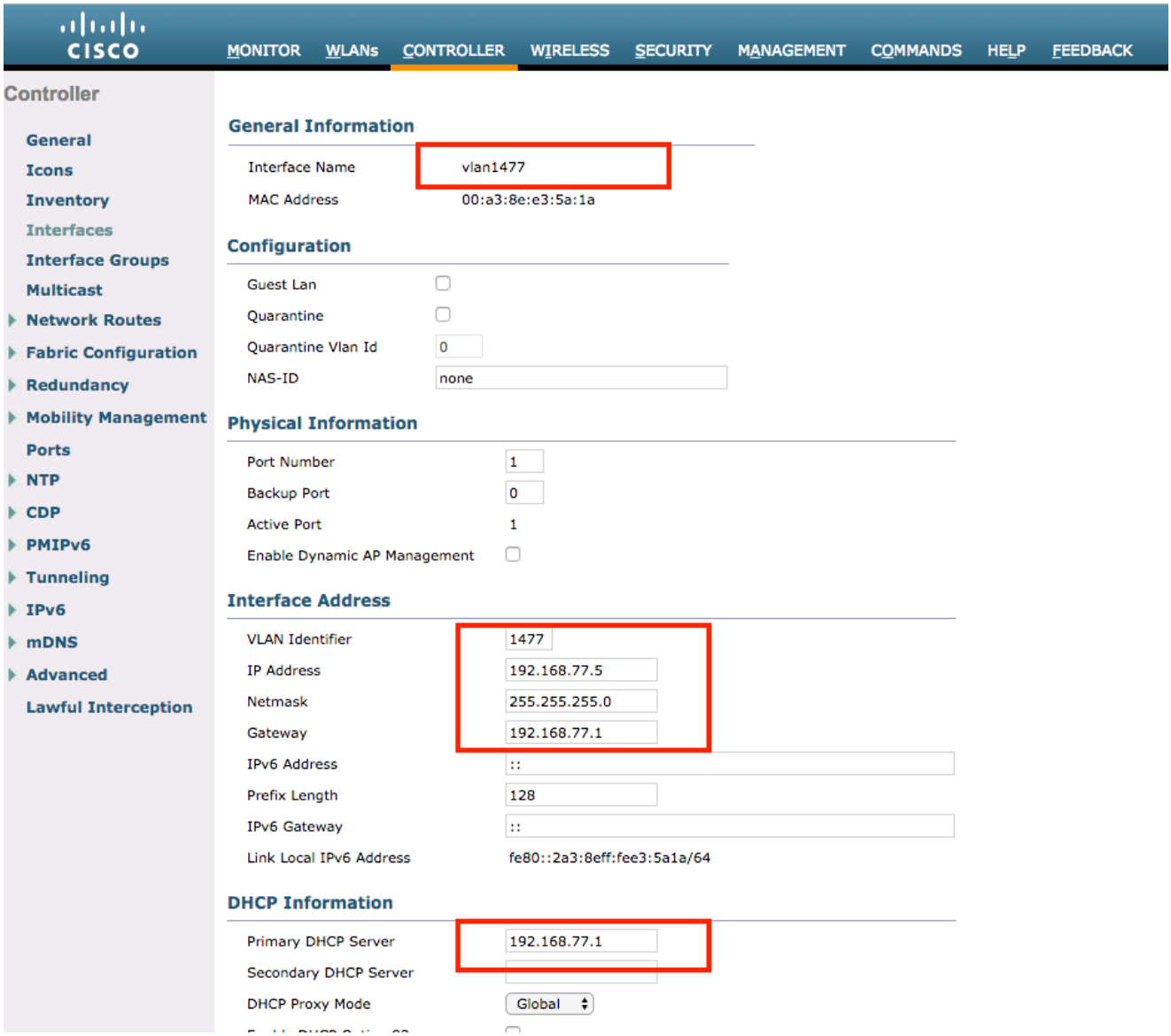

WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Profile Name
office_hq
Type
WLAN
SSID
office_hq
Status
Enabled
Security Policies
[WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy
All
Interface/Interface Group(G
dummy
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled
NAS-ID
none


WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
Fast Transition
Fast Transition
Adaptive
Over the DS
Reassociation Timeout
20
Seconds
Protected Management Frame
PMF
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
CCMP256
GCMP128
GCMP256
OSEN Policy
Authentication Key Management
802.1X
Enable
CCKM
Enable





3. U moet ook dynamische interfaces op de WLC voor gebruikers-VLAN's maken. Navigeer naarController > Interfaceshet UI-menu. De WLC kan de VLAN-toewijzing die via AAA wordt ontvangen alleen honoreren als er een dynamische interface in dat VLAN is.



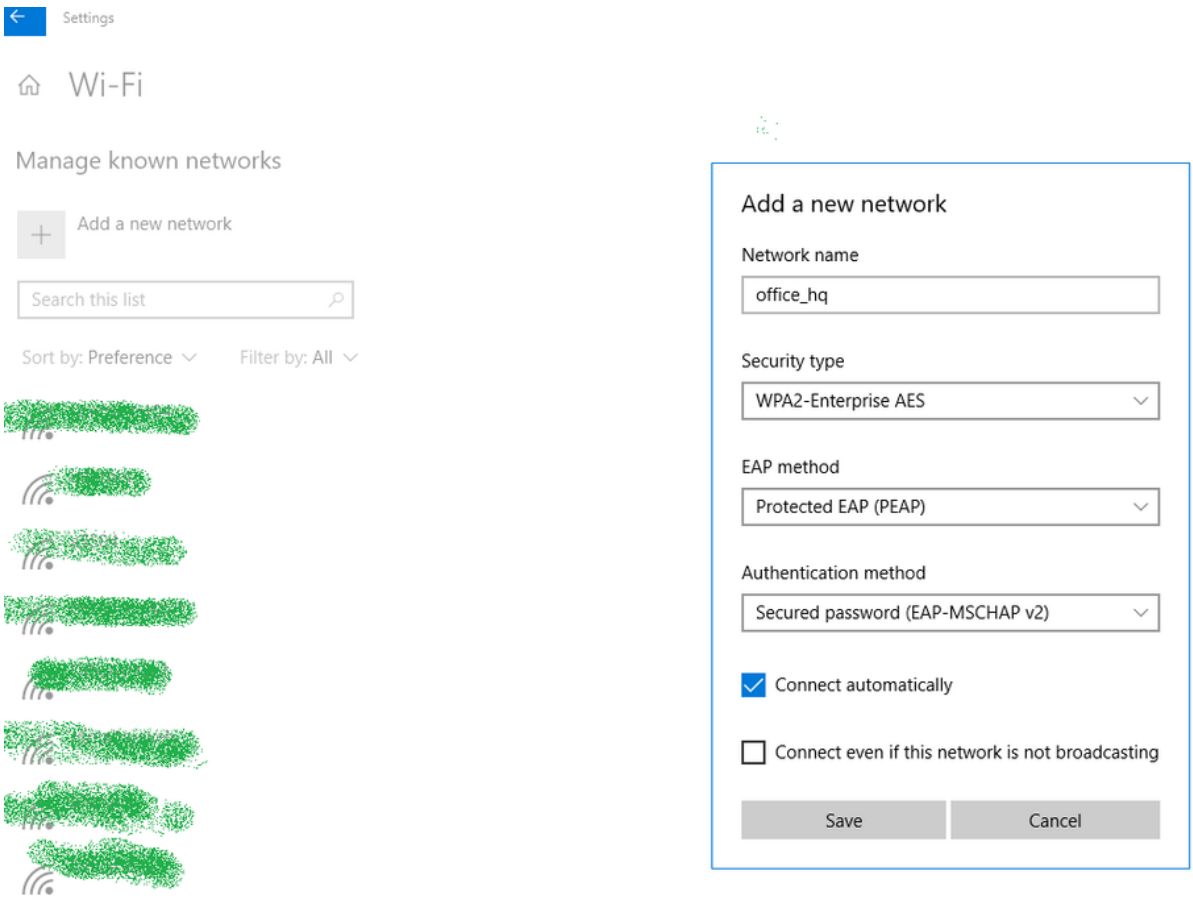
Verifiëren

Gebruik de Windows 10 native supplicant en AnyConnect NAM om verbindingen te testen.

Aangezien u EAP-PEAP-verificatie gebruikt en ISE een zelfondertekend certificaat (SSC) gebruikt, moet u akkoord gaan met een certificaatwaarschuwing of certificaatvalidatie uitschakelen. In een bedrijfsomgeving moet u een ondertekend en vertrouwd certificaat op ISE gebruiken en ervoor zorgen dat de eindgebruikerapparaten het juiste basiscertificaat hebben geïnstalleerd onder de lijst van Trusted CA.

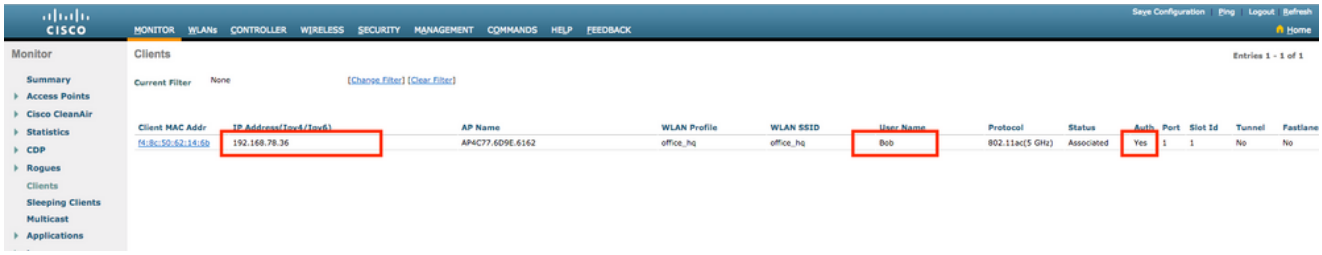
Testverbinding met Windows 10 en native aanvrager:

1. OpenNetwork & Internet settings > Wi-Fi > Manage known networksen maak een nieuw netwerkprofiel door op deAdd new networktoets te drukken;vul de gewenste informatie in.



2. Controleer het verificatielogboek op ISE en controleer of het juiste profiel voor de gebruiker is geselecteerd.

3. Controleer de client-invoer op WLC en zorg ervoor dat deze is toegewezen aan het juiste VLAN en zich in de staat RUN bevindt.



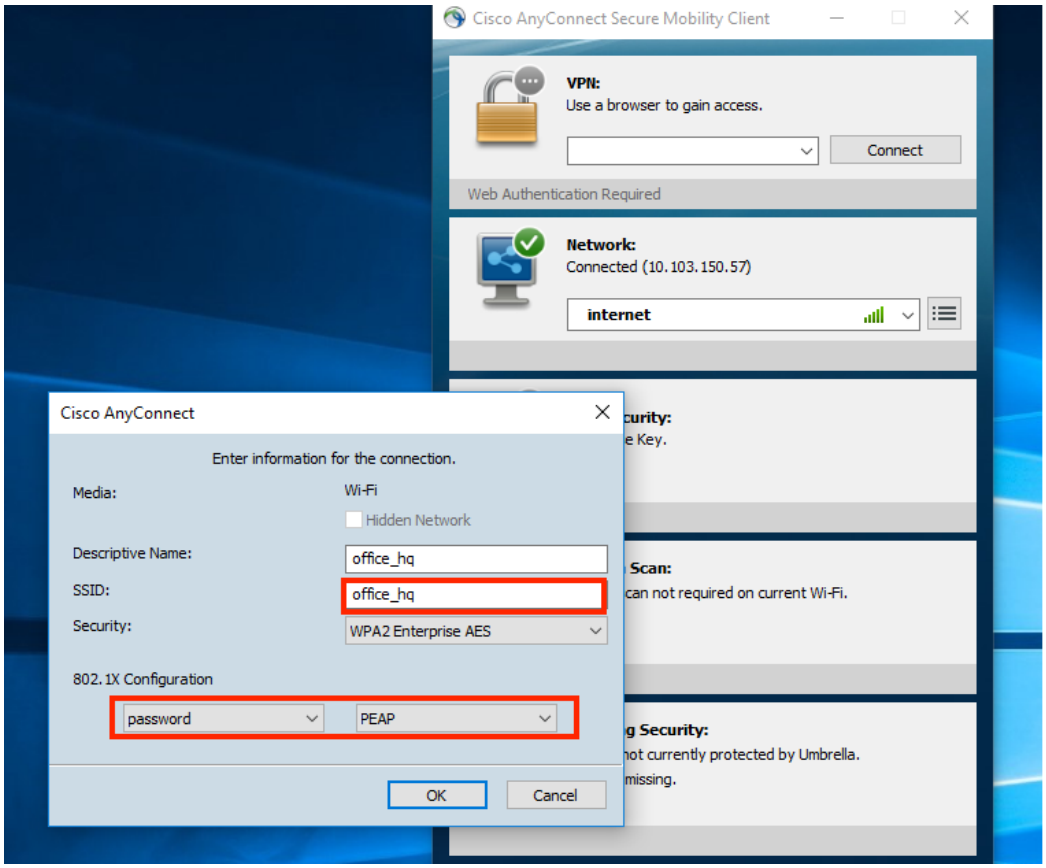
4. Van de WLC CLI, kan de cliëntstatus met worden gecontroleerd`show client dertails` :

```
show client detail f4:8c:50:62:14:6b
Client MAC Address.............................. f4:8c:50:62:14:6b
Client Username ................................ Bob
```

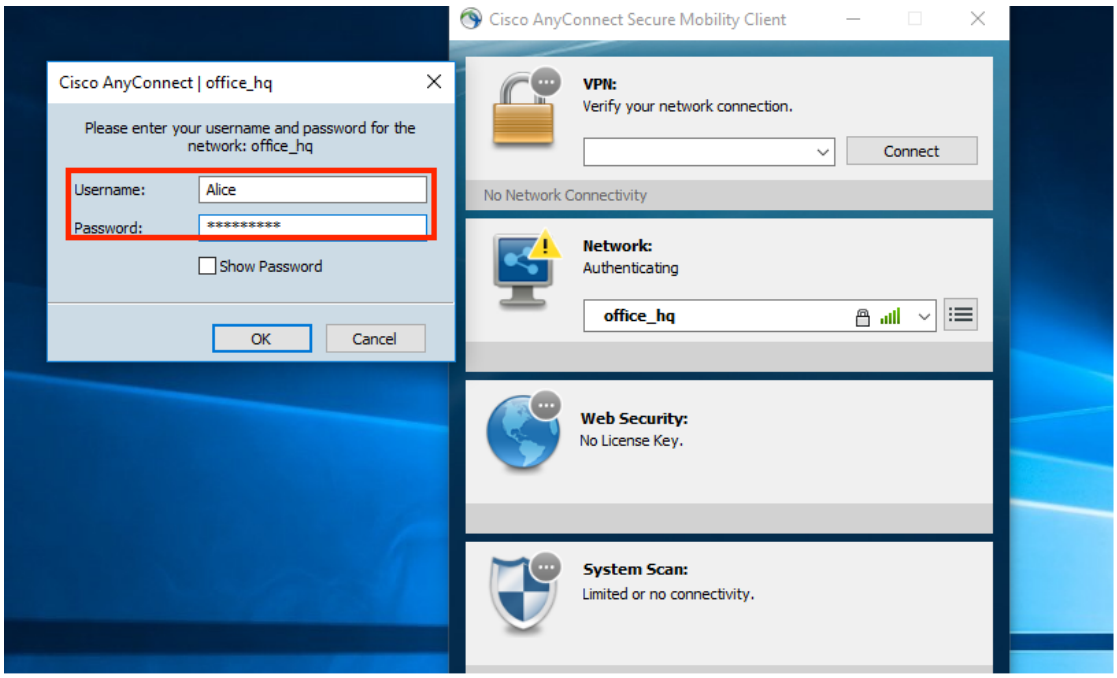
```
Client Webauth Username ..... N/A
Hostname: .....
Device Type: ..... Intel-Device
AP MAC Address..... 70:69:5a:51:4e:c0
AP Name..... AP4C77.6D9E.6162
AP radio slot Id..... 1
Client State..... Associated
User Authenticated by ..... RADIUS Server
Client User Group..... Bob
Client NAC OOB State..... Access
Wireless LAN Id..... 3
Wireless LAN Network Name (SSID)..... office_hq
Wireless LAN Profile Name..... office_hq
Hotspot (802.11u)..... Not Supported
Connected For ..... 242 secs
BSSID..... 70:69:5a:51:4e:cd
Channel..... 36
IP Address..... 192.168.78.36
Gateway Address..... 192.168.78.1
Netmask..... 255.255.255.0
...
Policy Manager State..... RUN
...
EAP Type..... PEAP
Interface..... vlan1478
VLAN..... 1478
Quarantine VLAN..... 0
Access VLAN..... 1478
```

Testverbinding met Windows 10 en AnyConnect NAM:

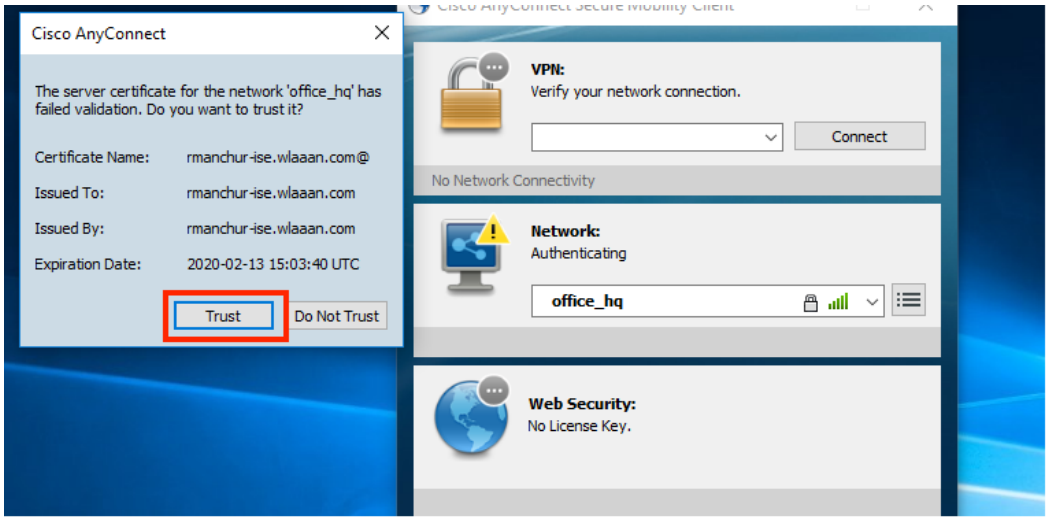
1. Kies de SSID uit de lijst van beschikbare SSID's en het respectieve EAP-verificatietype (in dit voorbeeld PEAP) en het innerlijke verificatieformulier.



2. Gebruikersnaam en wachtwoord opgeven voor gebruikersverificatie.

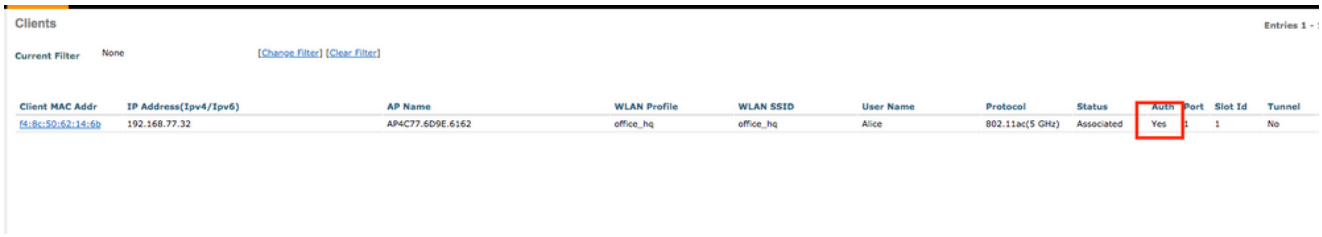


3. Aangezien ISE een SSC naar de client verzendt, moet u handmatig kiezen of u het certificaat vertrouwt (in de productieomgeving wordt het sterk aanbevolen om het vertrouwde certificaat op ISE te installeren).



4. Controleer de verificatie en logt ISE in en zorg ervoor dat het juiste autorisatieprofiel voor de gebruiker is geselecteerd.

5. Controleer de client-invoer op de WLC en zorg ervoor dat deze is toegewezen aan het juiste VLAN en zich in de RUN-status bevindt.



6. Van de WLC CLI, kan de cliëntstatus met worden gecontroleerd`show client dertails` :

```
Client MAC Address.............................. f4:8c:50:62:14:6b
Client Username ................................ Alice
Client Webauth Username ........................ N/A
Hostname: ......................................
Device Type: ................................... Intel-Device
AP MAC Address.................................. 70:69:5a:51:4e:c0
AP Name......................................... AP4C77.6D9E.6162
AP radio slot Id................................ 1
```

```
Client State..................................... Associated
User Authenticated by ........................... RADIUS Server
Client User Group................................ Alice
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 3
Wireless LAN Network Name (SSID)................. office_hq
Wireless LAN Profile Name........................ office_hq
Hotspot (802.11u)................................ Not Supported
Connected For ................................... 765 secs
BSSID............................................ 70:69:5a:51:4e:cd
Channel.......................................... 36
IP Address....................................... 192.168.77.32
Gateway Address.................................. 192.168.77.1
Netmask.......................................... 255.255.255.0
...
Policy Manager State............................. RUN
...
Policy Type...................................... WPA2
Authentication Key Management.................... 802.1x
Encryption Cipher................................ CCMP-128 (AES)
Protected Management Frame ...................... No
Management Frame Protection...................... No
EAP Type......................................... PEAP
Interface........................................ vlan1477
VLAN............................................. 1477
```

Problemen oplossen

1. Gebruik de knoptest aaa radius username

   password

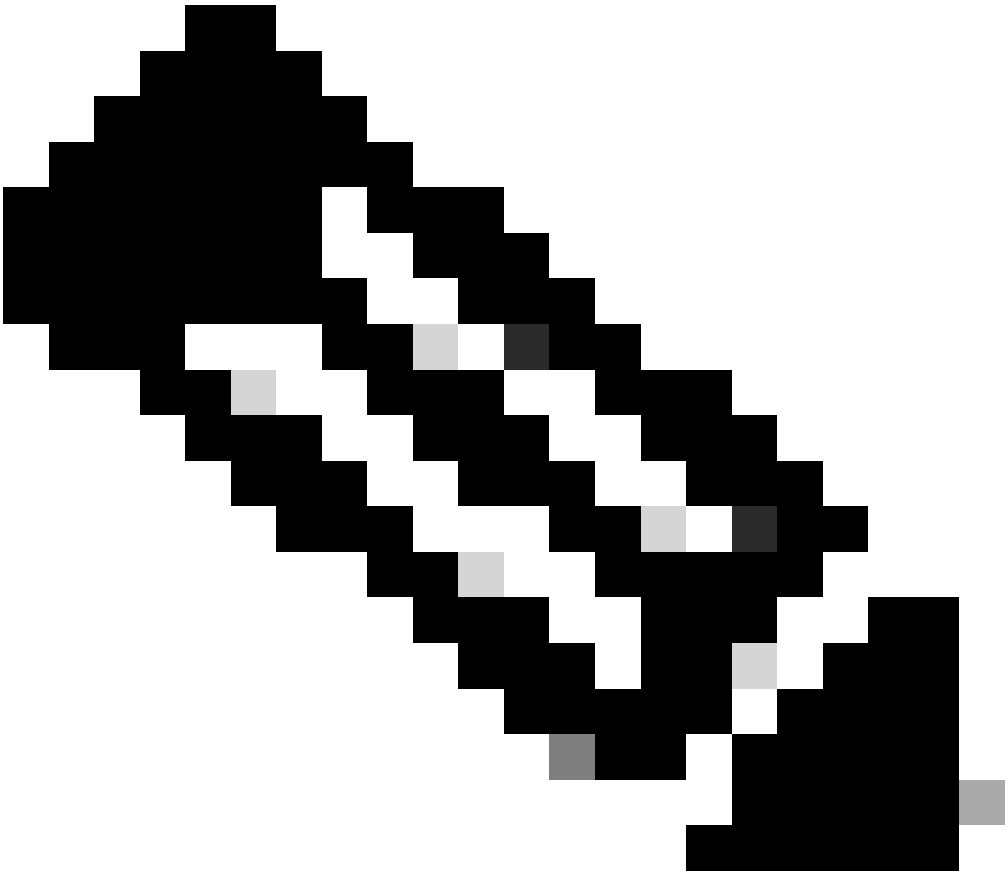
   wlan-id

   om de RADIUS-verbinding tussen WLC en ISE te testentest aaa show radiusom de resultaten weer te geven.

```
test aaa radius username Alice password <removed> wlan-id 2

Radius Test Request
  Wlan-id.......................................... 2
  ApGroup Name..................................... none

  Attributes                    Values
  ----------                    ------
  User-Name                     Alice
  Called-Station-Id             00-00-00-00-00-00:AndroidAP
  Calling-Station-Id            00-11-22-33-44-55
  Nas-Port                      0x00000001 (1)
```

```
  Nas-Ip-Address                  10.48.71.20
  NAS-Identifier                  0x6e6f (28271)
  Airespace / WLAN-Identifier     0x00000002 (2)
  User-Password                   cisco!123
  Service-Type                    0x00000008 (8)
  Framed-MTU                      0x00000514 (1300)
  Nas-Port-Type                   0x00000013 (19)
  Cisco / Audit-Session-Id        1447300a0000003041d5665c
  Acct-Session-Id                 5c66d541/00:11:22:33:44:55/743


test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) >test aaa show radius

Radius Test Request
  Wlan-id..................................... 2
  ApGroup Name................................ none
Radius Test Response

Radius Server            Retry Status
-------------            ----- ------
10.48.39.128             1     Success

Authentication Response:
  Result Code: Success

  Attributes                      Values
  ----------                      ------
  User-Name                       Alice
  State                           ReauthSession:1447300a0000003041d5665c
  Class                           CACS:1447300a0000003041d5665c:rmanchur-ise/339603379/59
  Tunnel-Type                     0x0000000d (13)
  Tunnel-Medium-Type              0x00000006 (6)
  Tunnel-Group-Id                 0x000005c5 (1477)


(Cisco Controller) >
```

2. Gebruik het debug client
   formulier om problemen met draadloze clientconnectiviteit op te lossen.
3. Gebruik hetdebug aaa all enableom problemen met verificatie en autorisatie op de WLC op te lossen.



Opmerking: gebruik deze opdracht alleen met de`debug mac addr`om de uitvoer te beperken op basis van het MAC-adres waarvoor debugging is uitgevoerd.

4. Raadpleeg de bewegende logbestanden en sessielogboeken van ISE om problemen met verificatie en problemen met AD-communicatie te identificeren.

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.