Configureer ISE BYOD met enkele en dubbele SSID in ISE 3.3

Inhoud

Inleiding

Het document beschrijft hoe u BYOD-problemen op ISE kunt configureren en oplossen.

Achtergrond

BYOD is een functie waarmee gebruikers hun persoonlijke apparaten op ISE aan boord kunnen nemen, zodat de gebruiker de netwerkbron op de omgeving kan gebruiken. Het helpt de netwerkbeheerder ook om te voorkomen dat de gebruiker toegang heeft tot de kritieke bron van de persoonlijke apparaten.

In tegenstelling tot de gaststroom waarbij het apparaat is geverifieerd met de Gastpagina met behulp van de interne Store of Active directory op ISE. Met de BYOD kan de netwerkbeheerder een eindpuntprofiel op het eindpunt installeren om het type EAP-methode te kiezen. In scenario's zoals EAP-TLS wordt het clientcertificaat door de ISE zelf ondertekend om een vertrouwen te creëren tussen het eindpunt en ISE.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- WLC-controller
- Basiskennis over ISE

Gebruikte componenten

Deze gebruikte apparaten zijn niet beperkt tot één bepaalde versie voor de BYOD-stroom:

- Catalyst 9800-CL draadloze controller (17.12.3)
- ISE virtuele machine (3.3)

Wat is Single SSID en Dual SSID BYOD op ISE?

Single SSID BYOD

In een Single SSID BYOD-installatie verbinden gebruikers hun persoonlijke apparaten rechtstreeks met het draadloze bedrijfsnetwerk. Het onboarding proces vindt plaats op dezelfde SSID, waar ISE de registratie, levering en handhaving van het apparaat vergemakkelijkt. Deze benadering vereenvoudigt de gebruikerservaring, maar vereist veilige onboarding en juiste verificatiemethoden om de netwerkbeveiliging te garanderen.

Dual SSID BYOD

In een dubbele opstelling van SSID BYOD, worden twee afzonderlijke SSIDs gebruikt: een voor onboarding (onbeveiligde of beperkte toegang) en een ander voor toegang tot het bedrijfsnetwerk. Gebruikers maken eerst verbinding met de onboarding SSID, voltooien apparaatregistratie en

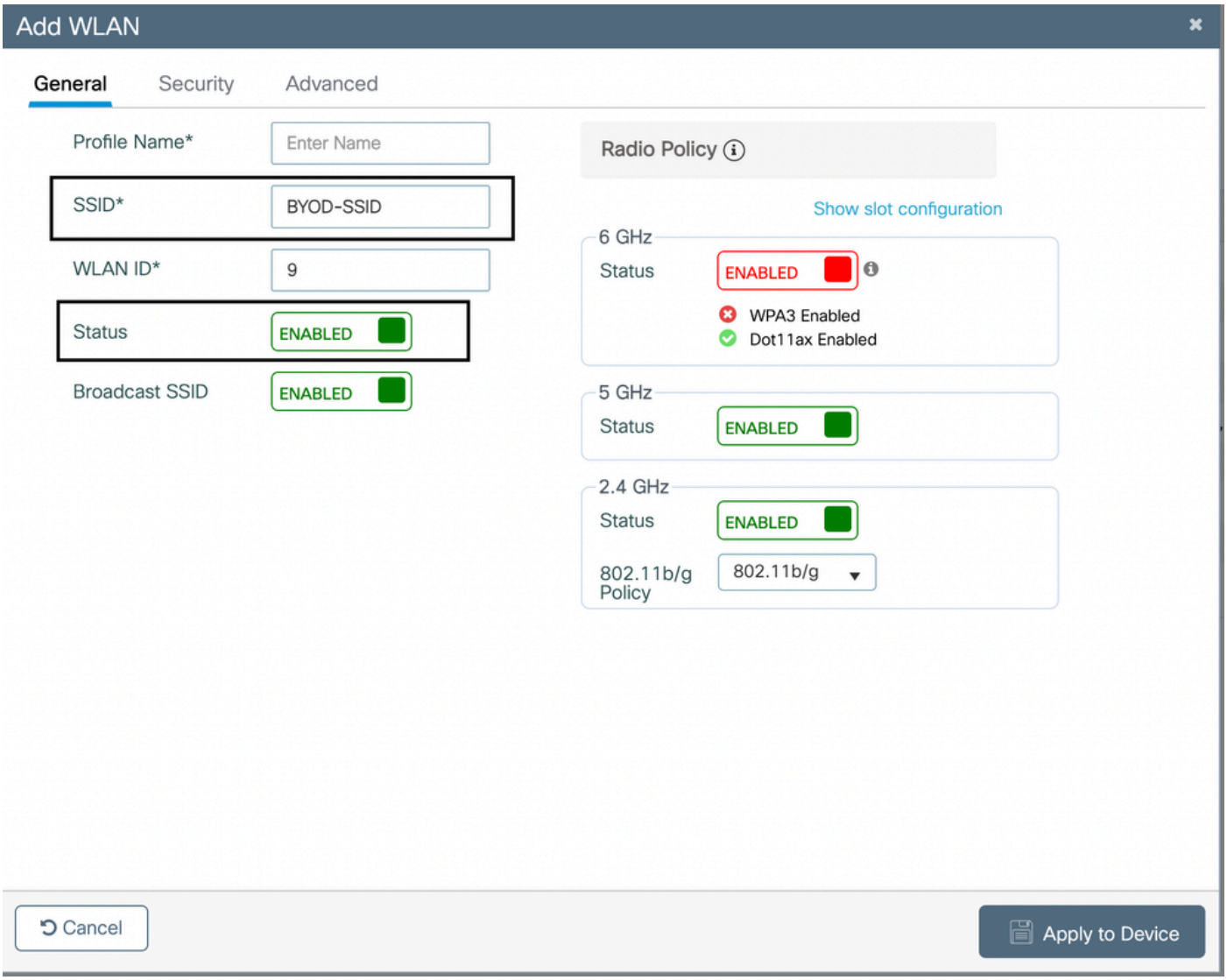
provisioning via ISE, en vervolgens switches naar de beveiligde zakelijke SSID voor netwerktoegang. Dit biedt een extra beveiligingslaag door onboarding van verkeer te scheiden van productieverkeer.

WLC-configuratie

Een WLAN voor CWA maken

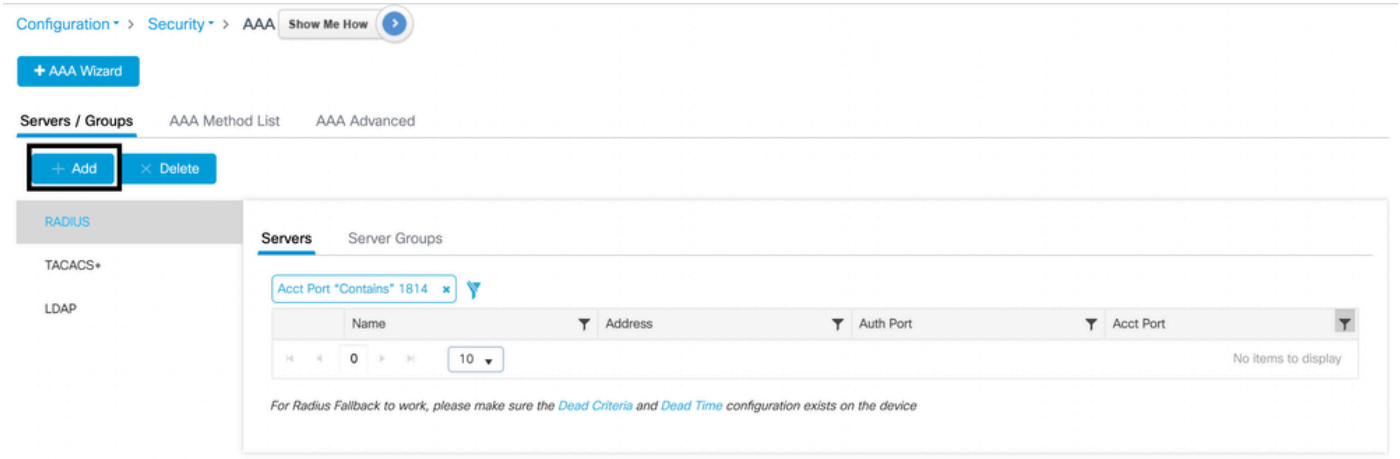
1. Ga naar Configuratie > Tags & profielen > WLAN's.
2. Klik op Add om een nieuw WLAN te maken.

    - Stel een WLAN-naam en SSID in (bijvoorbeeld BYOD-WiFi).
    - Schakel het WLAN in.

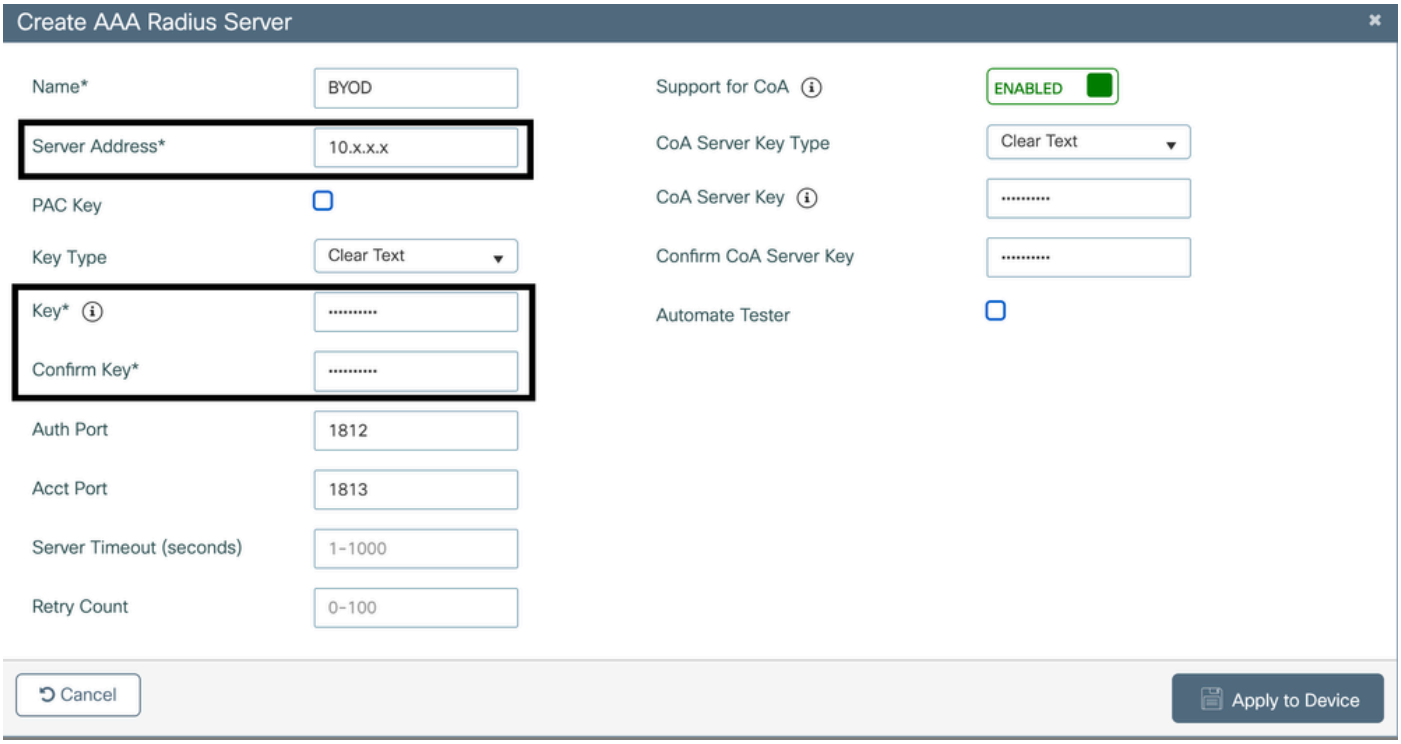


RADIUS-servers configureren

1. Navigeer naar Configuratie > Beveiliging > AAA > RADIUS > Servers.

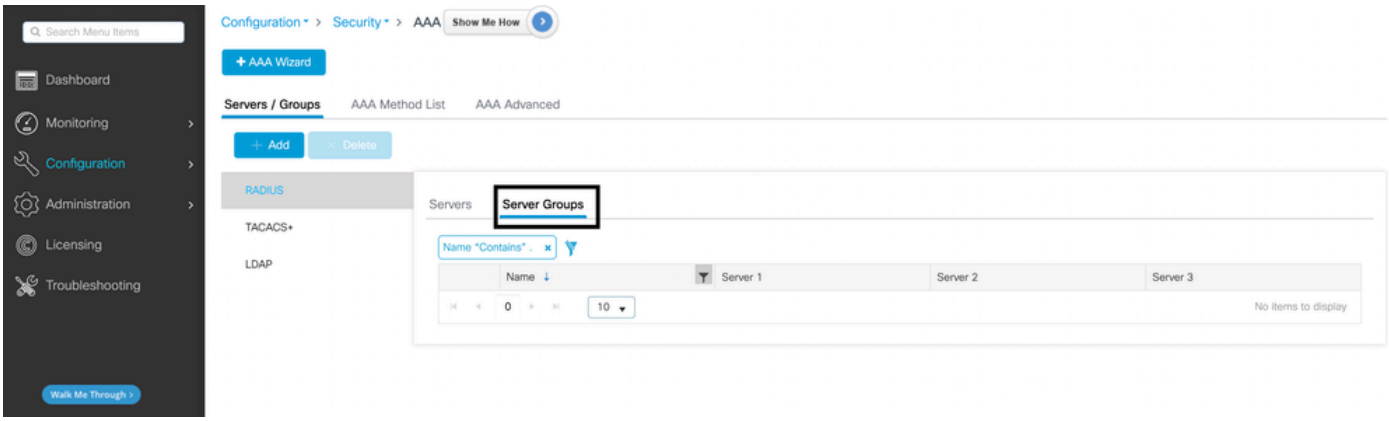


2. Klik op Add om ISE te configureren als een RADIUS-server:
    - IP-server: IP-adres van ISE.
    - Gedeeld geheim: Stem het gedeelde geheim af op ISE.

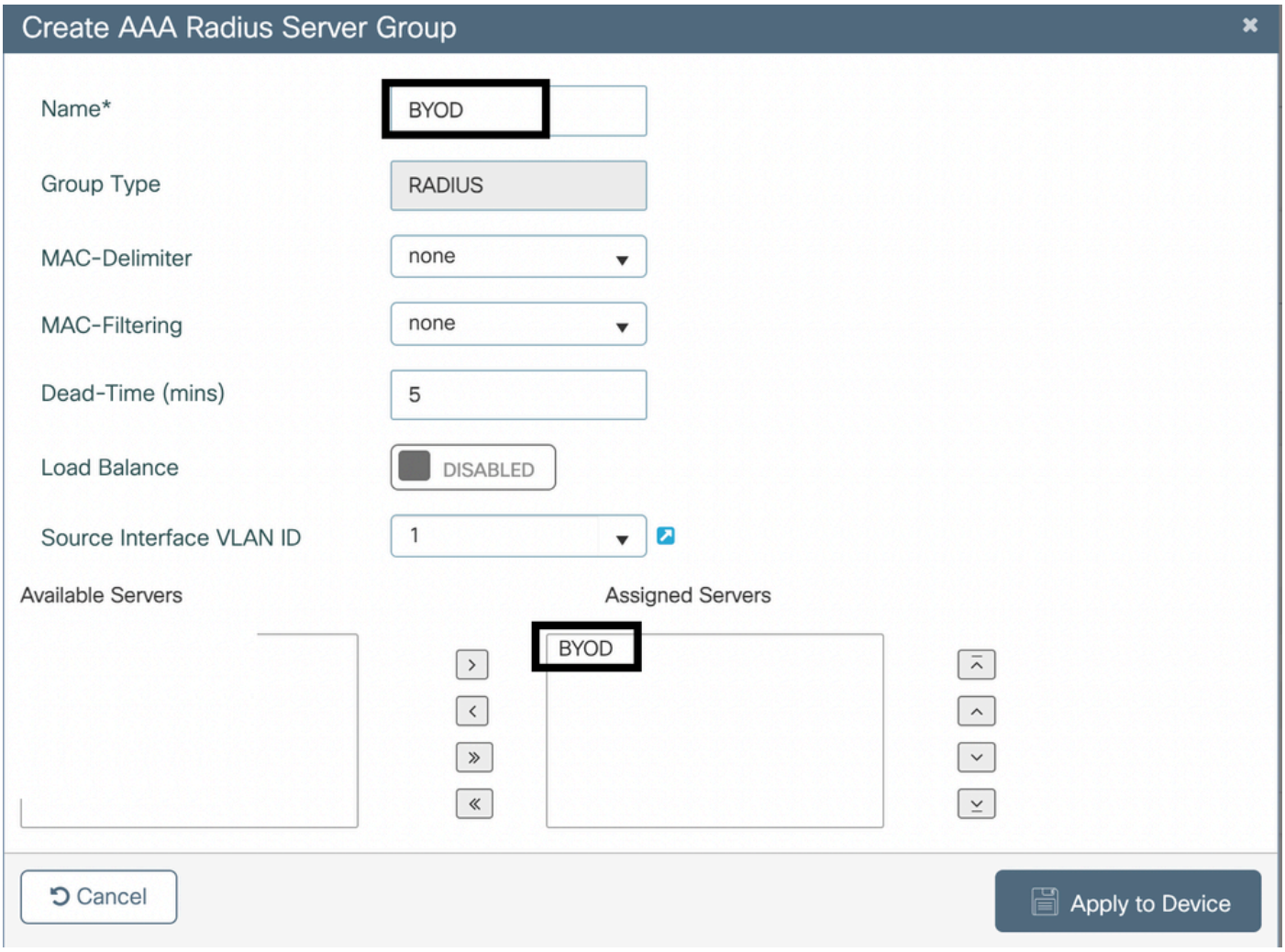


AAA-servers configureren

1. Ga naar Configuratie > Beveiliging > AAA > Servers/groepen.



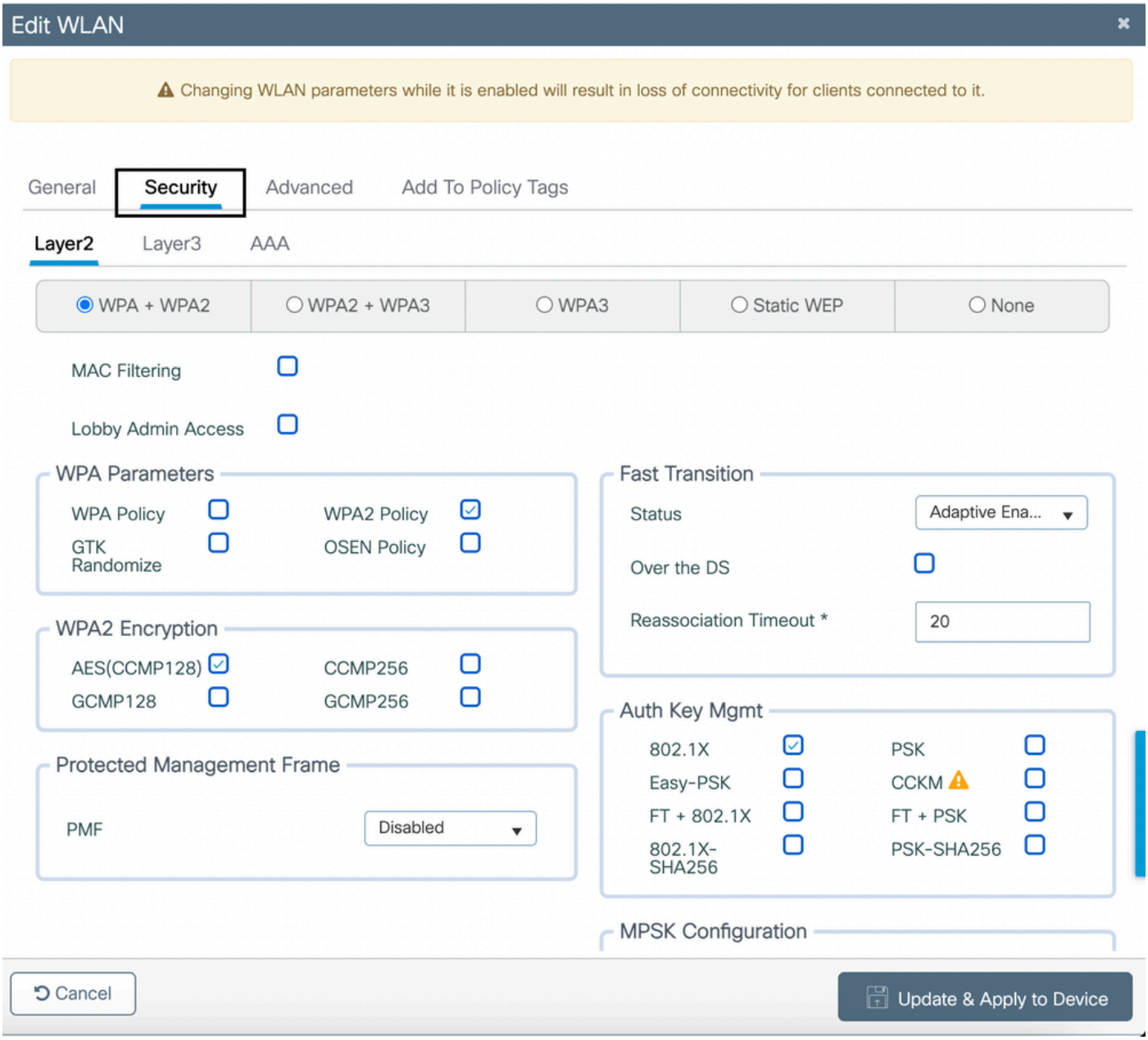
2. Wijs de RADIUS-server toe aan een nieuwe of bestaande servergroep.



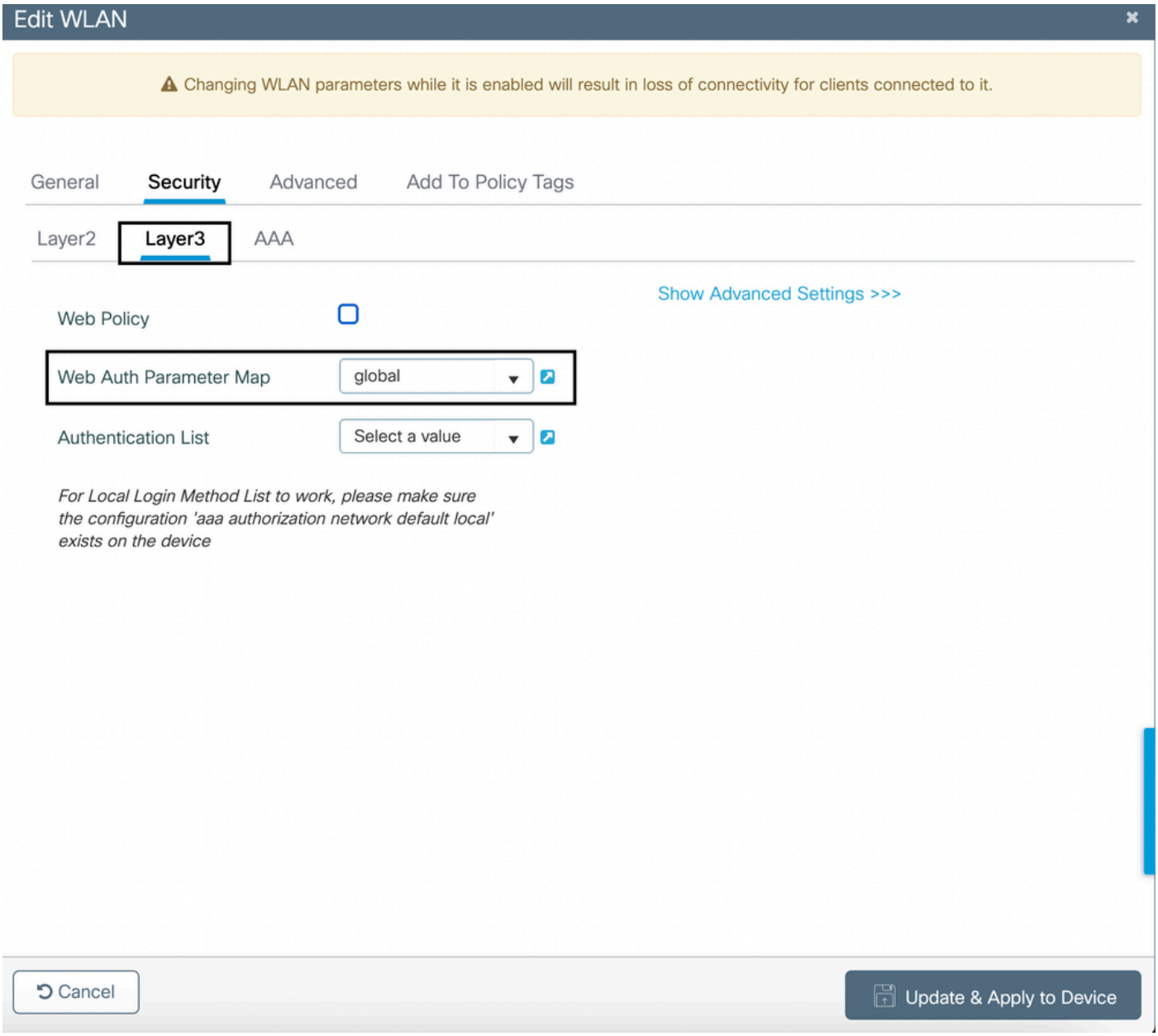
Beveiligingsbeleid voor het WLAN configureren

1. Navigeer naar Configuratie > Tags en profielen > WLAN's. Bewerk het eerder gemaakte WLAN.

2. Onder het tabblad Security > Layer 2:
   - WPA+WPA2 inschakelen
   - AES (CCMP128) instellen onder WPA2-encryptie
   - Beheer autosleutel als 802.1x



3. Selecteer onder het tabblad Security > Layer 3 de optie global uit de vervolgkeuzelijst voor Web Auth Parameter Map.



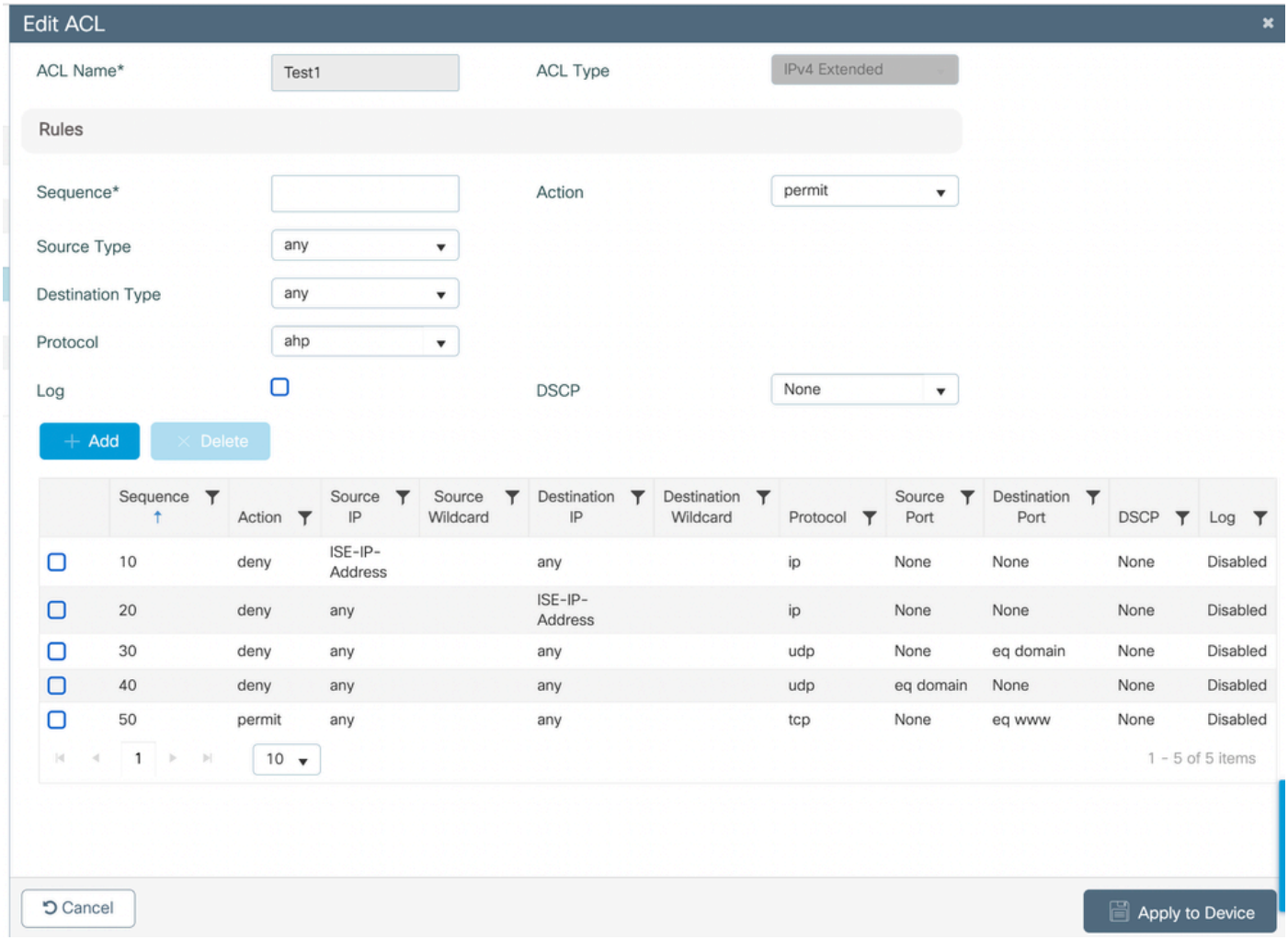
Voorafgaande verificatie-ACL configureren

Maak een ACL om dezie omleidingsacties:

- DNS-verkeer.
- HTTP/HTTPS naar het ISE-portal.
- Alle vereiste back-end services.

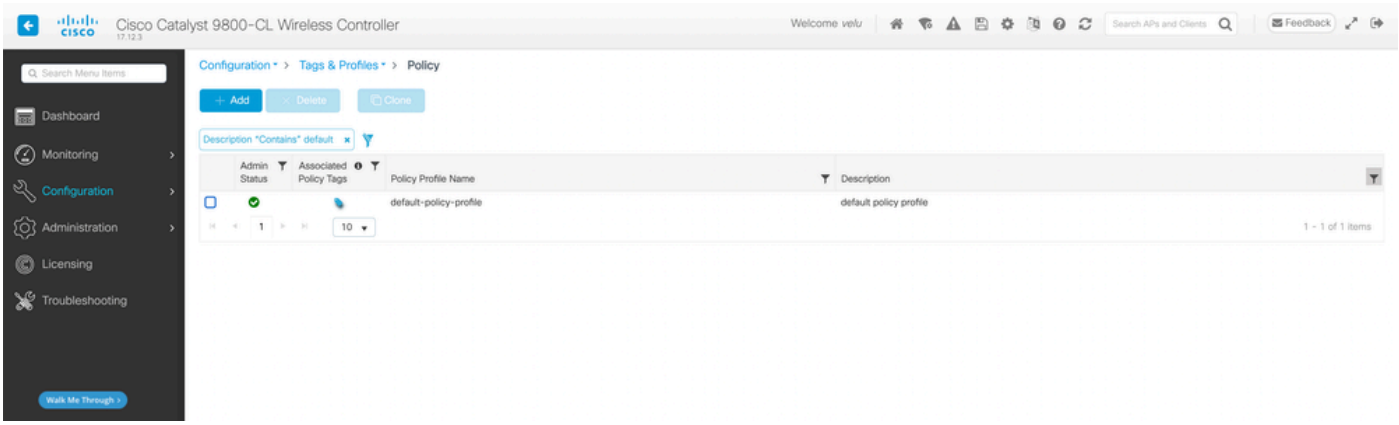
Dit doet u zo:

1. Ga naar Configuratie > Beveiliging > ACL's > Toegangscontrolelijsten.
2. Maak een nieuwe ACL met regels om noodzakelijk verkeer toe te staan.

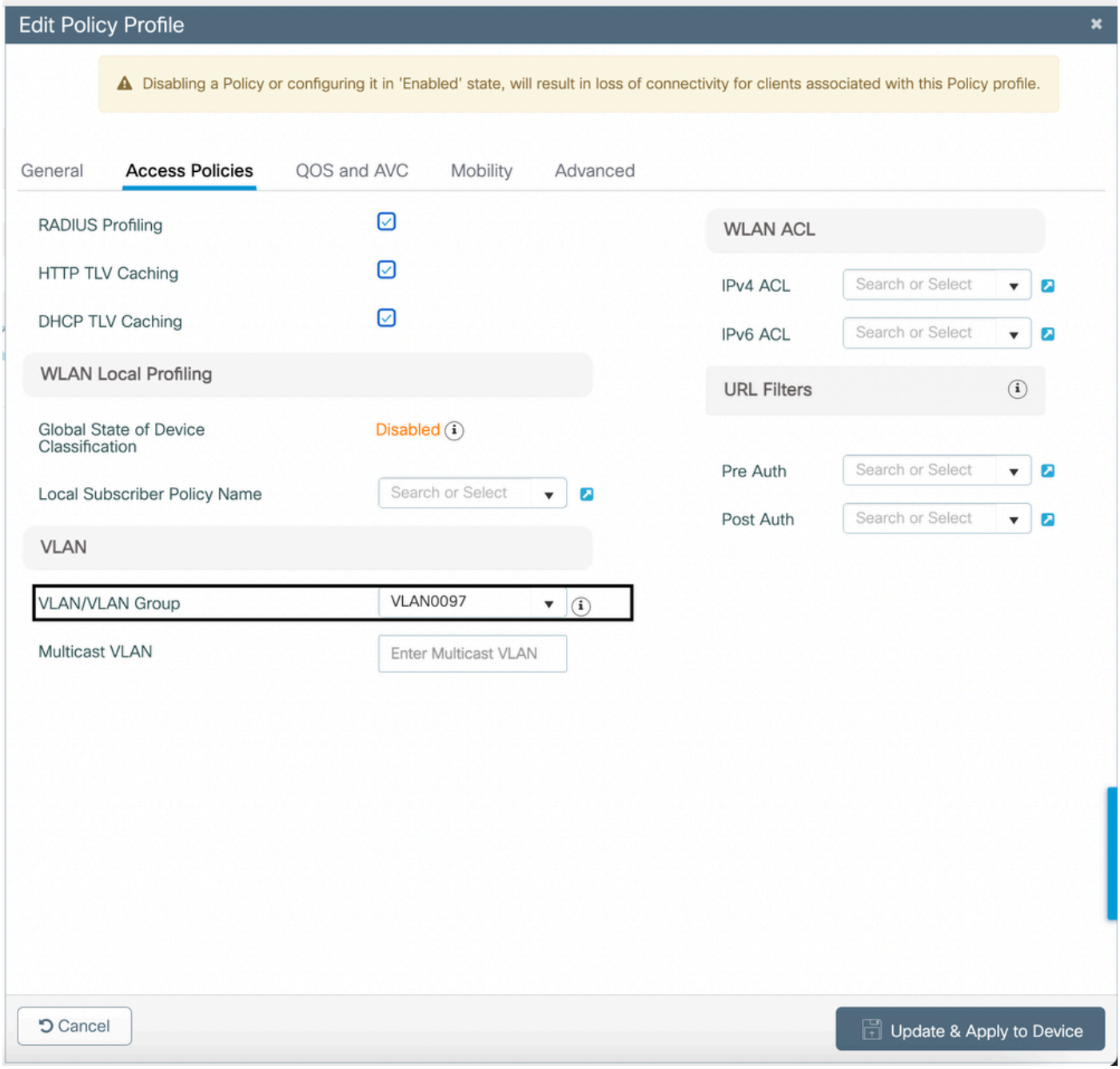


Beleidsprofiel configureren

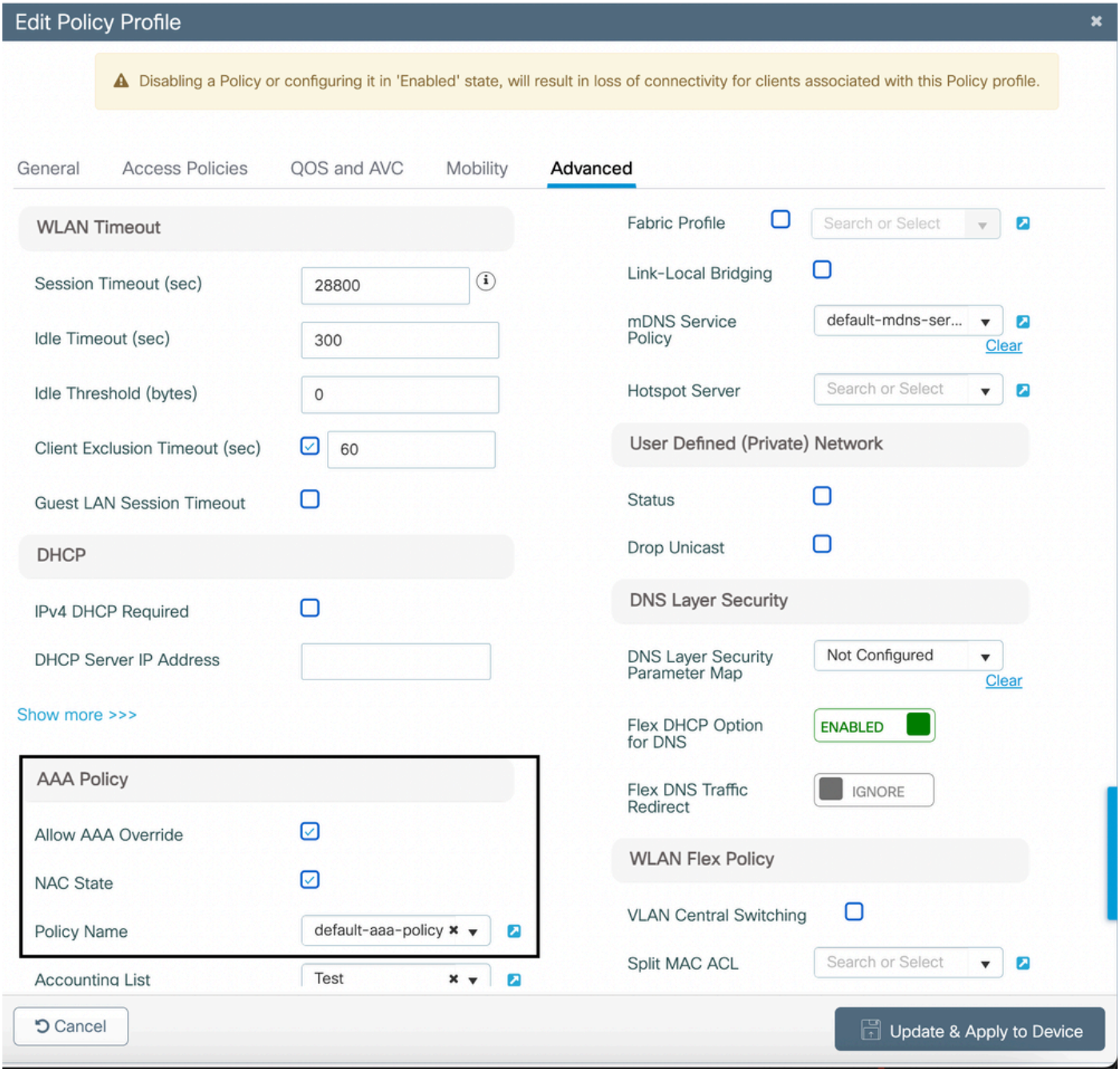
1. Ga naar Configuration > Tags & profielen > Policy. U kunt het standaardbeleid maken of gebruiken



2. Wijs het juiste VLAN toe onder Toegangsbeleid

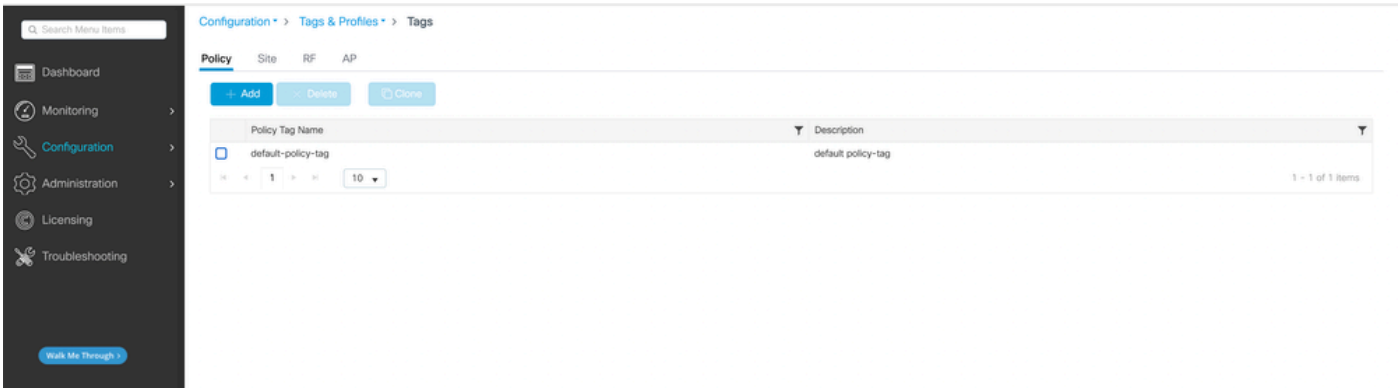


3. Schakel ook AAA en NAC status toestaan in onder Advanced in het beleid.



Tags toepassen en implementeren

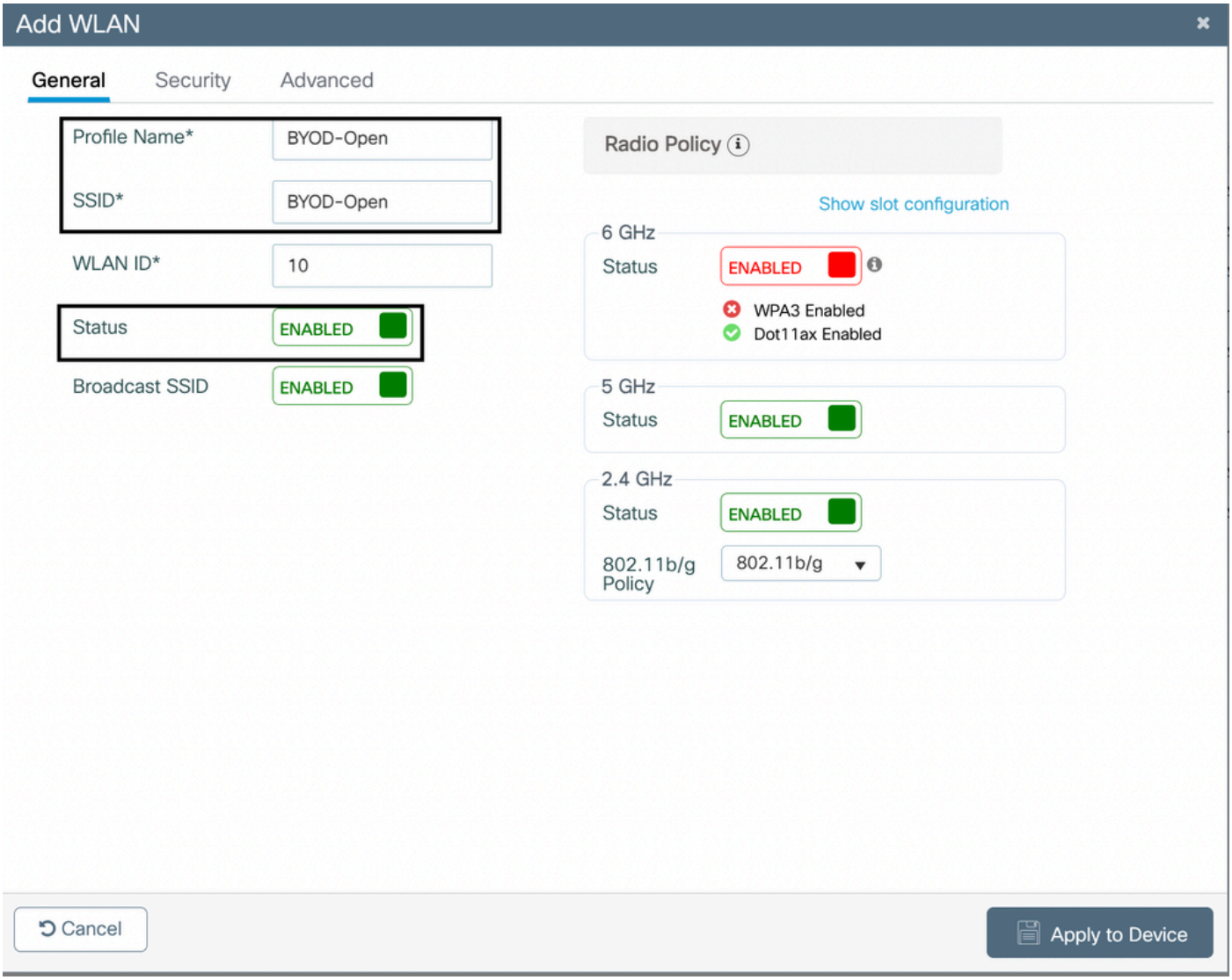
- Ga naar Configuration > Tags & profielen > Tags.
- Maak of bewerk een tag om het WLAN- en beleidsprofiel op te nemen.
- Wijs de tag toe aan de access points.



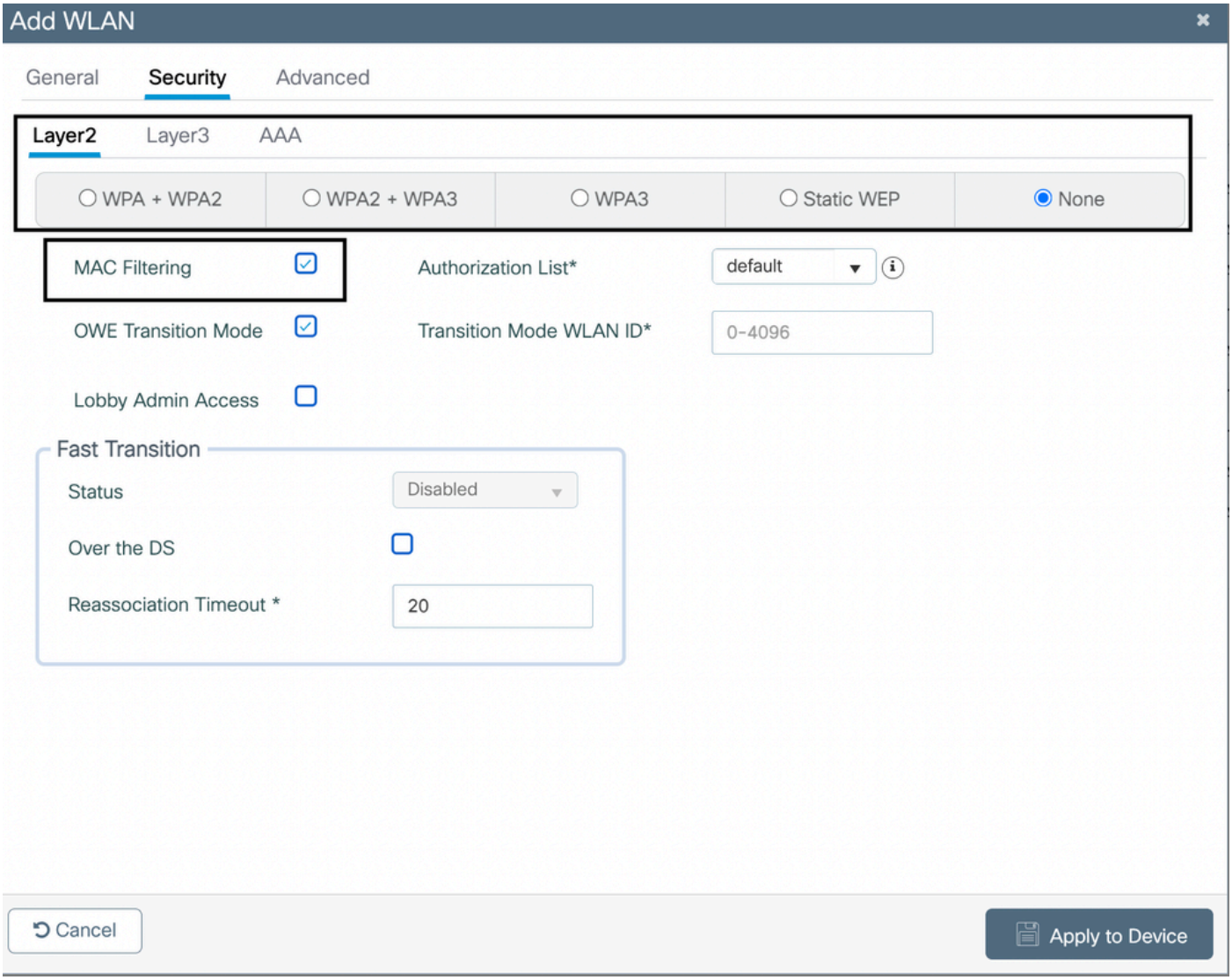
Een open/onbeveiligde SSID configureren

De Open SSID wordt alleen gemaakt wanneer u besluit om een Dual SSID BYOD-configuratie op uw omgeving te hebben.

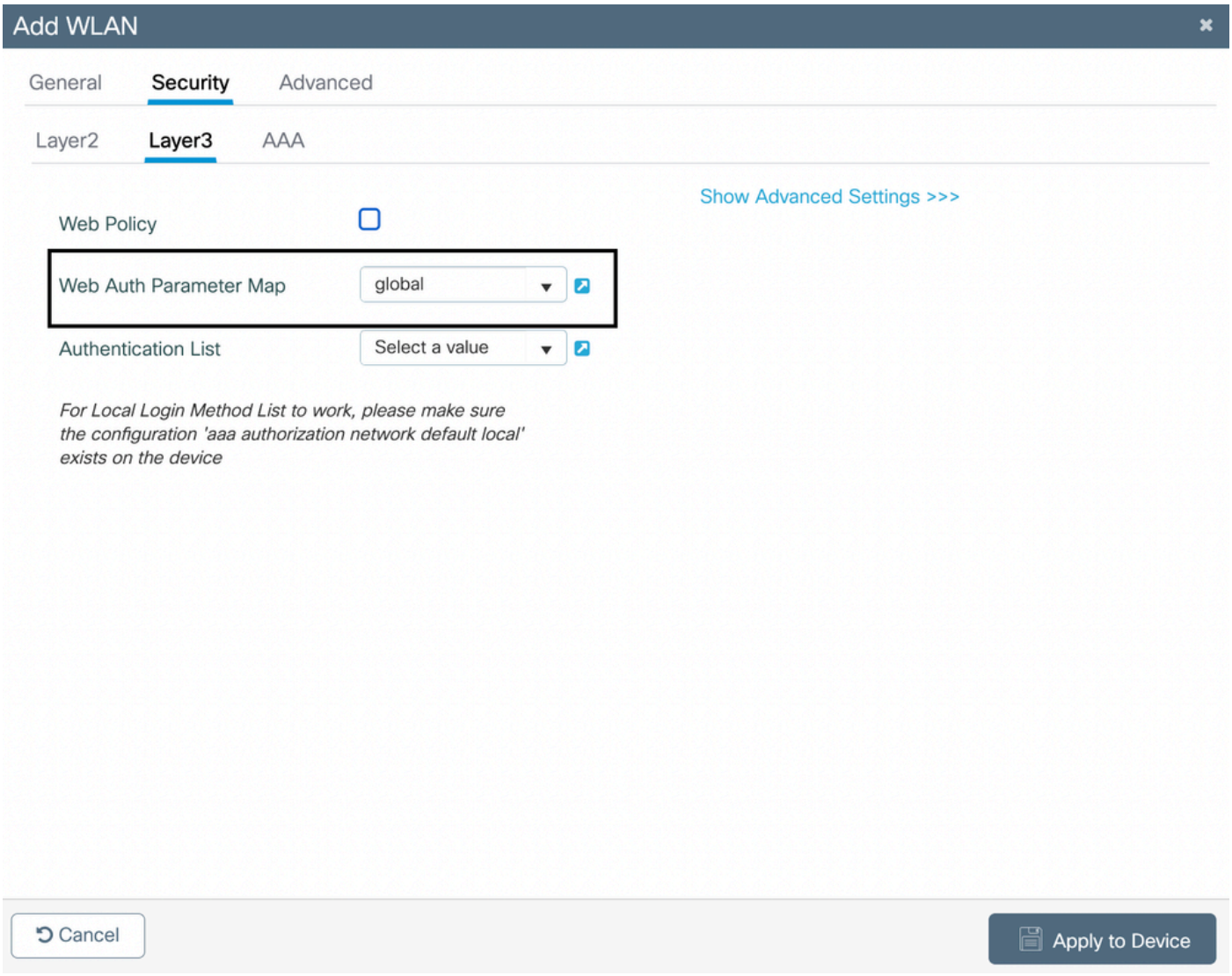
1. Navigeren naar Configuratie > Tags en profielen > WLAN's. Klik op de knop Toevoegen.
2. Geef een SSID-naam op onder het tabblad Algemeen en schakel de WLAN-knop in.



3. Klik in hetzelfde venster op het tabblad Beveiliging. Selecteer het keuzerondje Geen en schakel Mac-filtering in.



4. In Layer 3 onder Security selecteert u de wereldwijde instelling voor Web Auth Parameter Map. Als u een ander web auth profiel geconfigureerd op de WLC, kunt u het hier ook in kaart brengen:



ISE-configuratie

Voorwaarden

- Zorg ervoor dat Cisco ISE is geïnstalleerd en gelicentieerd voor BYOD-functionaliteit.
- Voeg uw WLC toe aan ISE als netwerkapparaat met het gedeelde RADIUS-geheim.

Certificaten

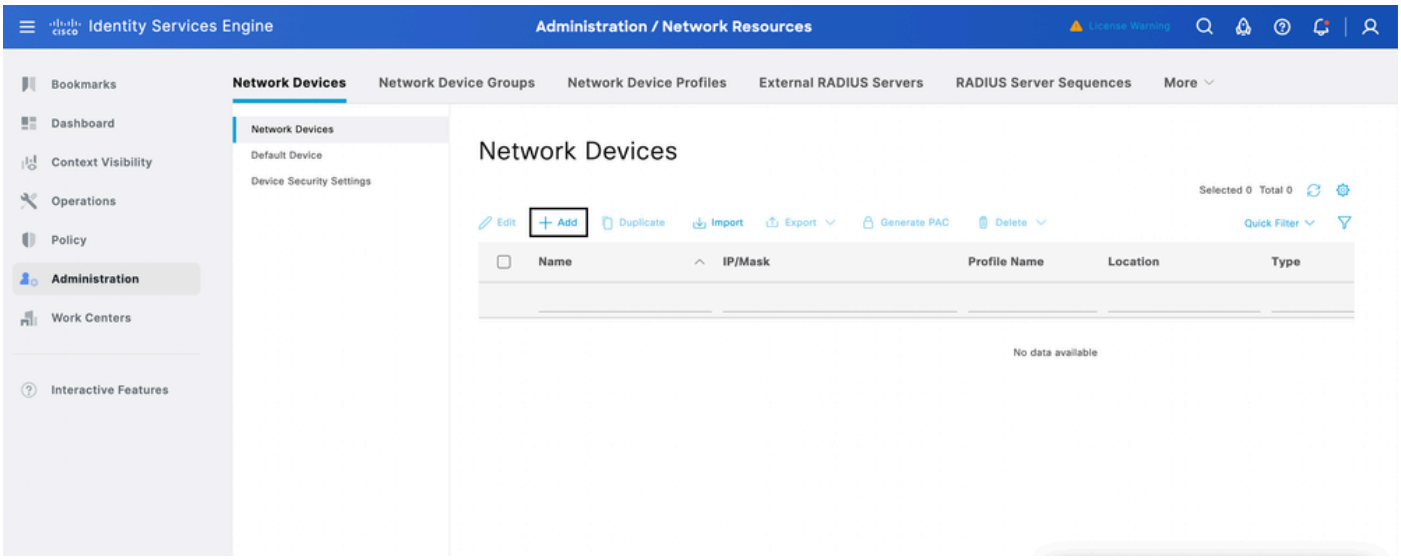
- Installeer een geldig servercertificaat op ISE om beveiligingswaarschuwingen voor de browser te voorkomen.
- Zorg ervoor dat het certificaat wordt vertrouwd door eindpunten (ondertekend door een bekende CA of een interne CA met vertrouwde basis).

DNS-configuratie

- Zorg ervoor dat DNS de ISE-hostnaam voor het BYOD-portal oplost.

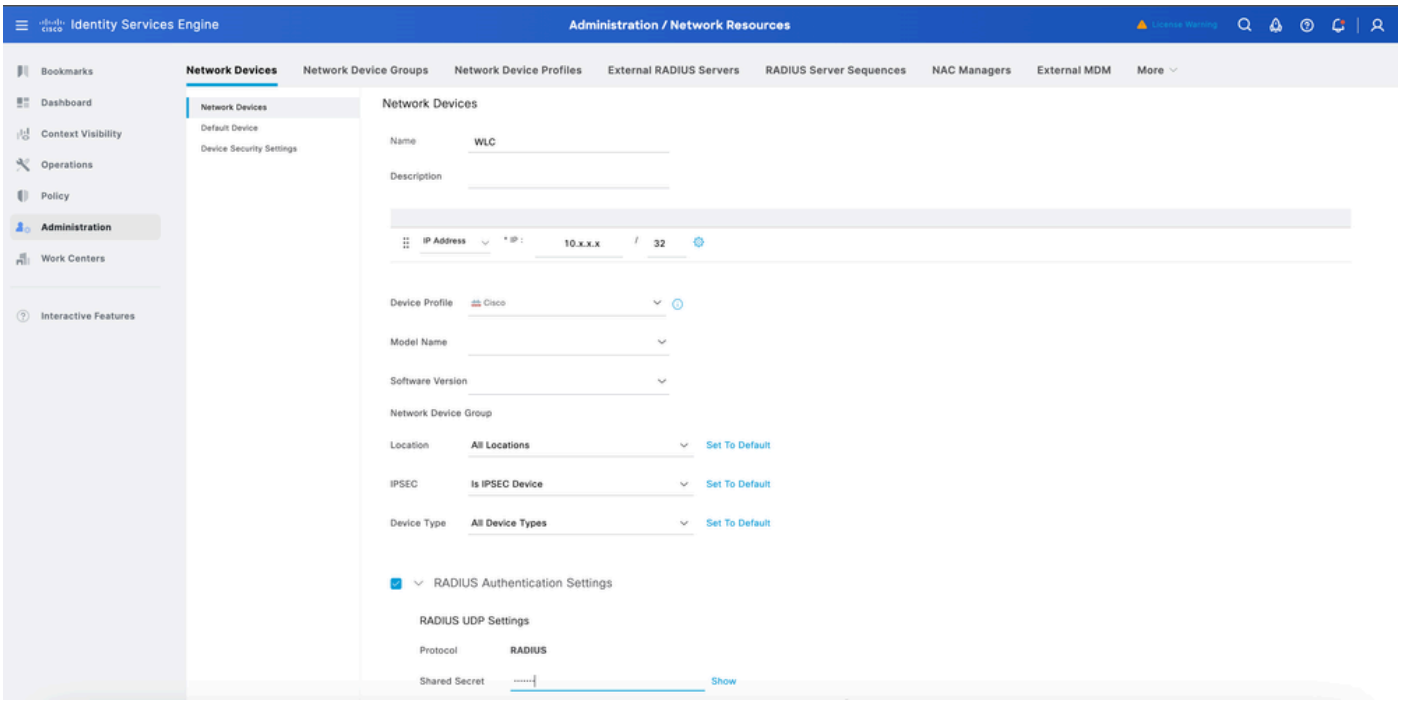
ISE-netwerkapparaat configureren

1. Log in op de ISE web UI.
2. Ga naar Beheer > Netwerkbronnen > Netwerkapparaten.



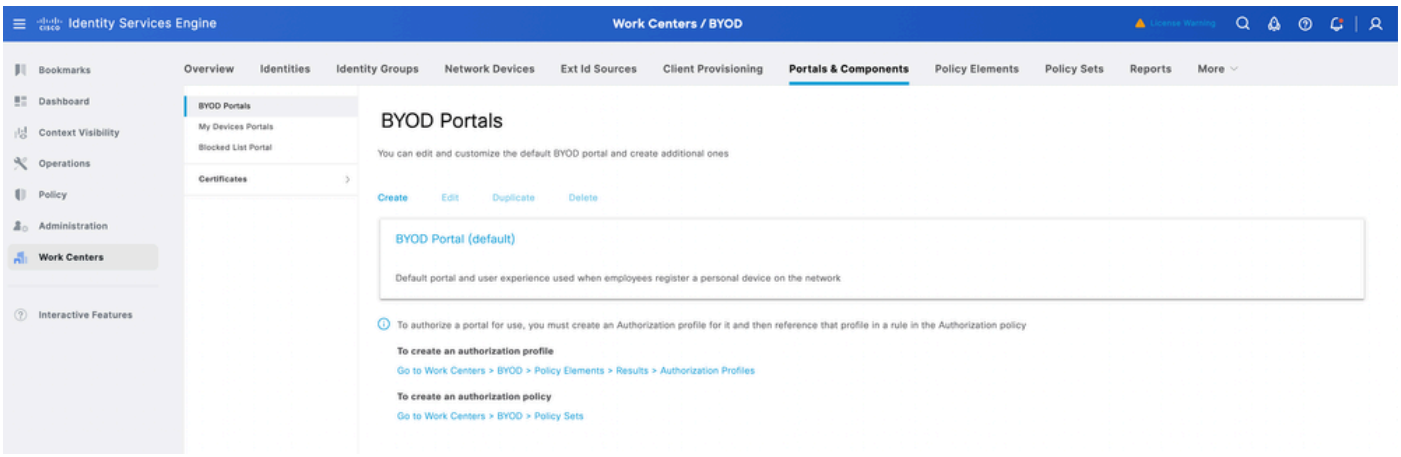
3.Add uw WLC als netwerkapparaat:

- Naam: Voer een naam in voor de WLC.
- IP-adres: Voer het WLC-beheer IP in.
- RADIUS gedeeld geheim: Voer hetzelfde gedeelde geheim in als geconfigureerd op de WLC.
- Klik op Verzenden.



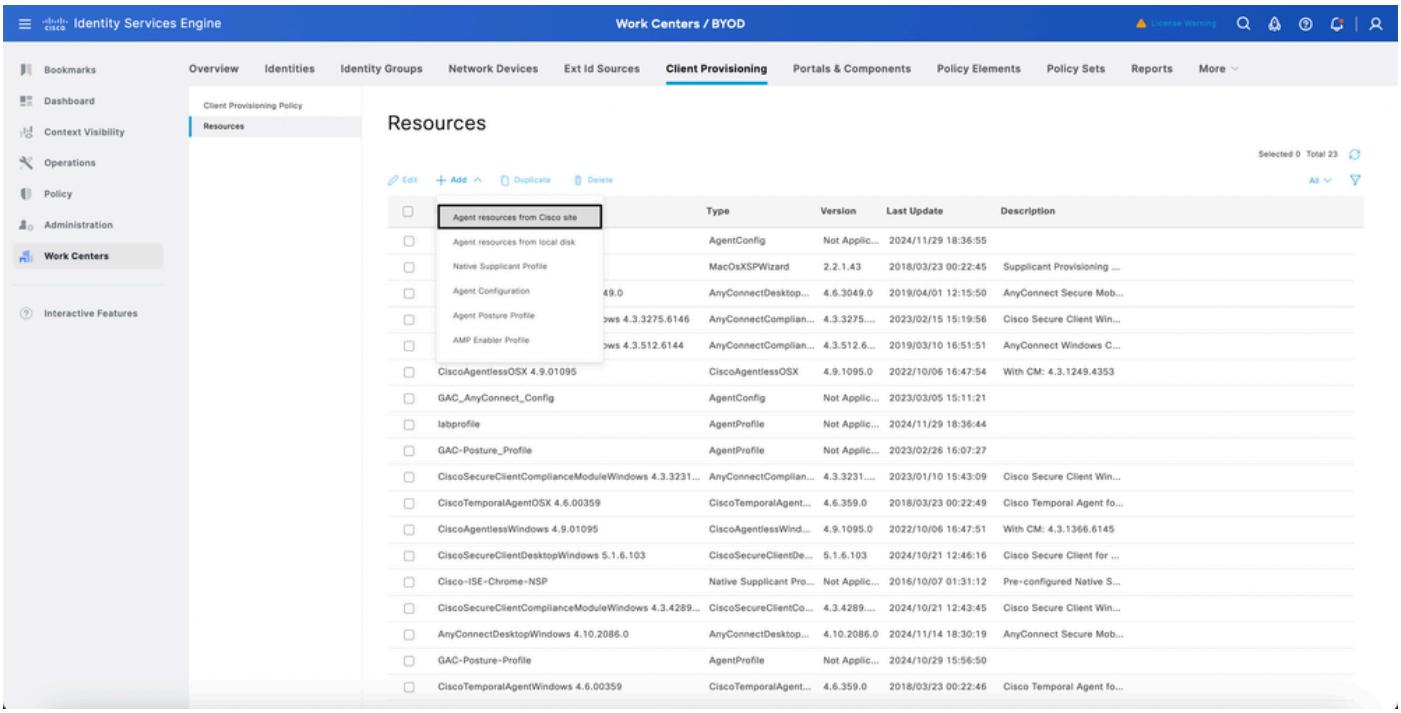
Een BYOD-portal maken

1. Navigeren naar werkcentra > BYOD > Instellingen > Portals & Components > BYOD Portals.
2. Klik op Add om een BYOD-portal te maken of u kunt het bestaande standaardportal op ISE gebruiken.



Nieuwste versie Cisco IOS® downloaden

1. Navigeren naar werkcentra > BYOD > Clientprovisioning > Resources.
2. Klik op de knop Add en selecteer agent resources uit de Cisco-site.



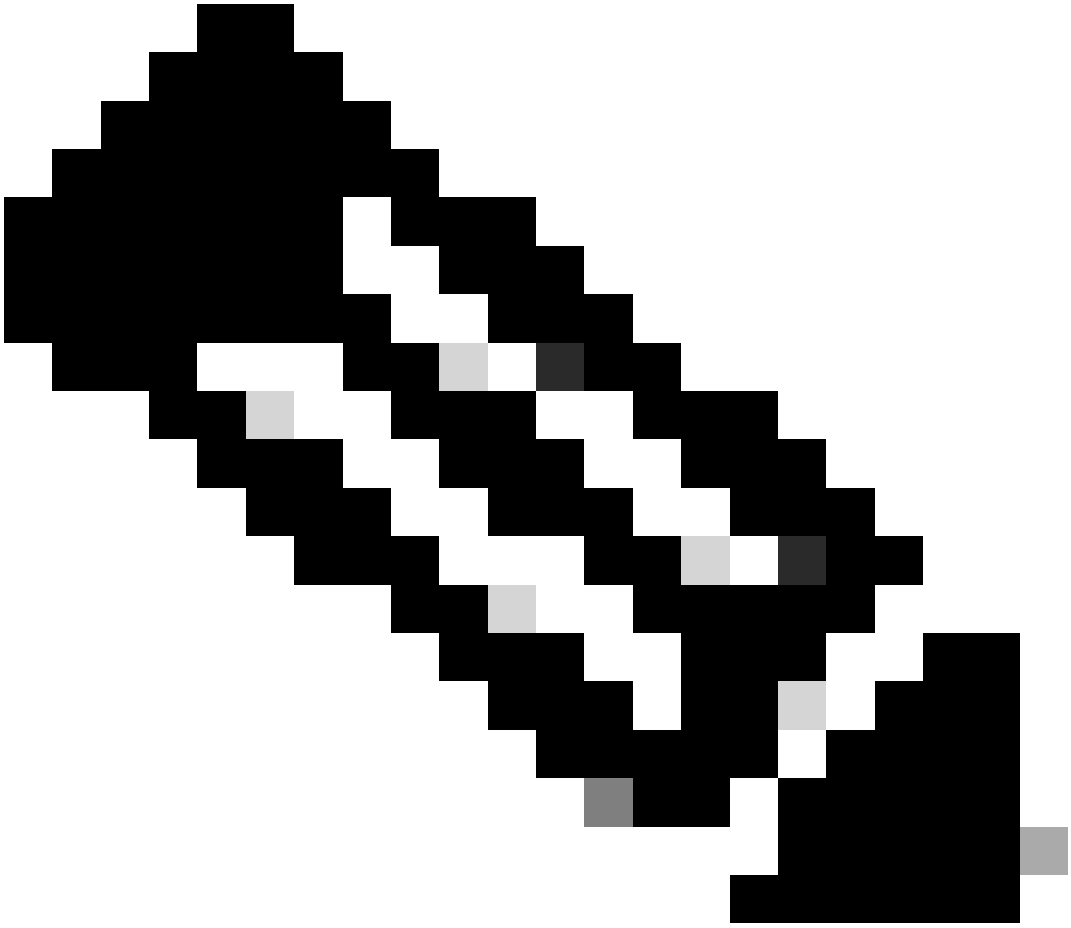
3. Selecteer in de softwarelijst de nieuwste Cisco IOS-versie die u wilt downloaden.

Download Remote Resources

	Name	Description
☐	MacOsXSPWizard 2.7.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.1.0.1	Supplicant Provisioning Wizard for MAC OSX Version 3.1.0.1
☐	MacOsXSPWizard 3.1.0.2	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.2.0.1	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	MacOsXSPWizard 3.4.0.0	Supplicant Provisioning Wizard for Mac OsX (ISE 2.2 and above releases)
☐	WinSPWizard 3.0.0.2	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)
☑	WinSPWizard 3.0.0.3	Supplicant Provisioning Wizard for Windows (ISE 2.x and Above)

For Agent software, please download from http://cisco.com/go/ciscosecureclient. Use the "Agent resource from local disk" add option, to import into ISE

Cancel Save

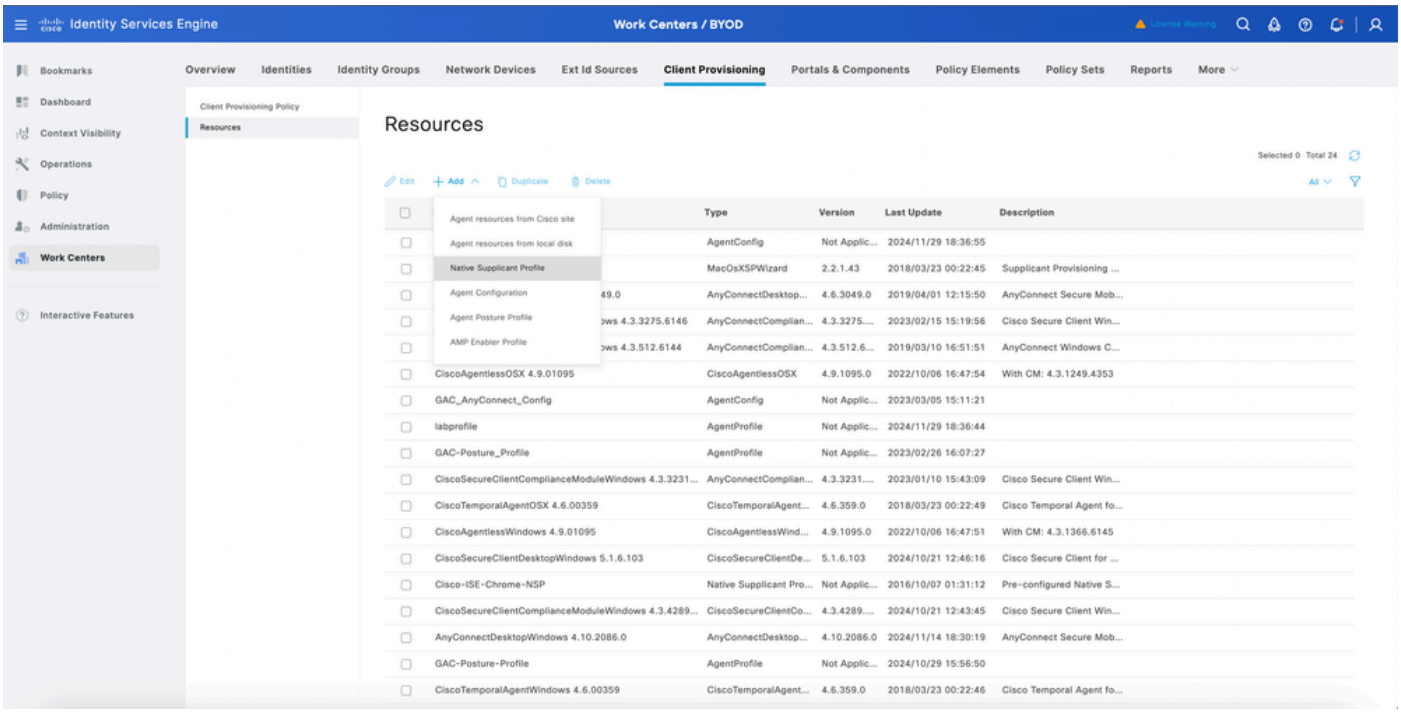


Opmerking: Cisco IOS-software wordt gedownload op de ISE voor Windows- en MacOS-endpoints. Voor Apple iPhone IOS, het gebruikt een native supplicant om het apparaat te provisioneren en voor Android-apparaat, je hebt Network setup assistent die moet worden gedownload van Play Store.

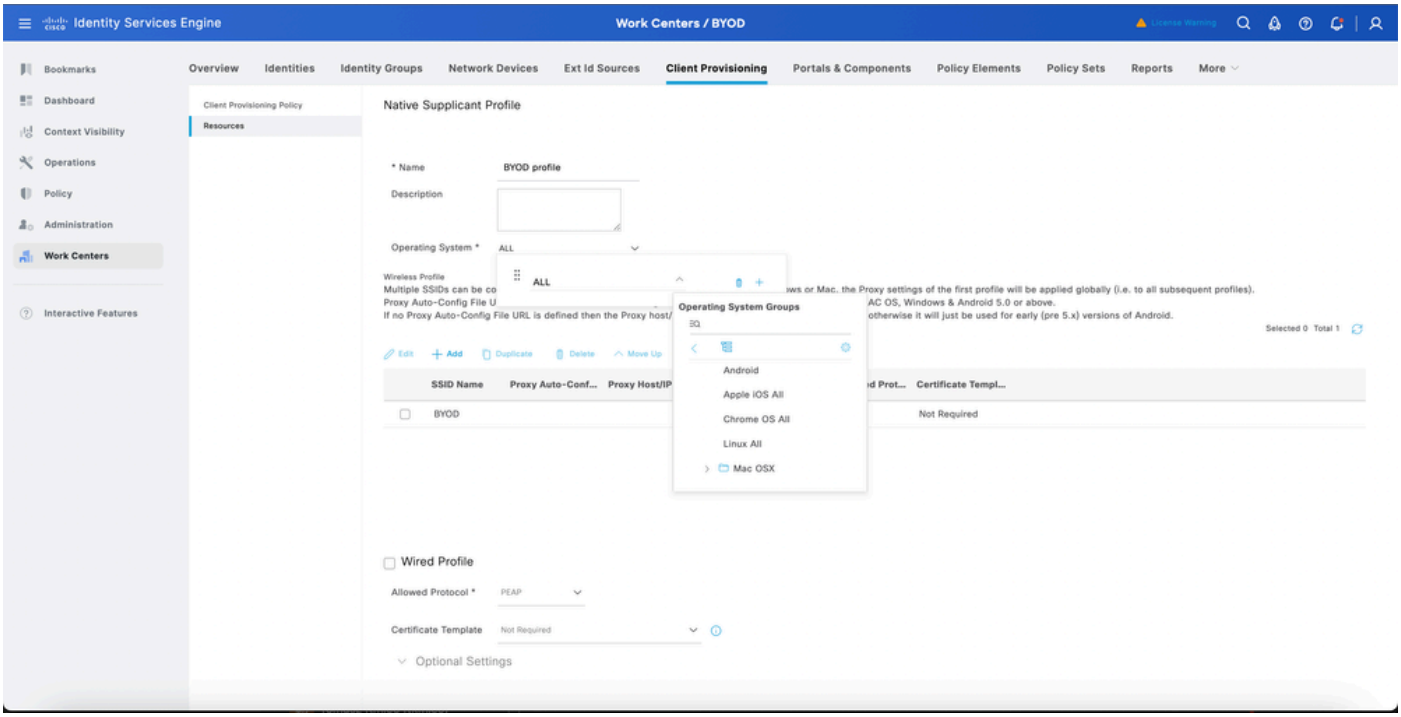
Een endpointprofiel maken

1. Navigeren naar werkcentra > BYOD > Clientprovisioning > Resources.

2. Klik op Add, selecteer Native Supplicant-profiel in het keuzemenu.



3. Selecteer in de uitrollijst van het besturingssysteem het gewenste besturingssysteem op het apparaat of stel het in op ALL voor alle eindpunten in uw omgeving:



4. Klik op Add op de pagina om het eindpuntprofiel te maken om 802.1X te configureren voor het eindpunt:

Wireless Profile(s)

SSID Name * BYOD

Proxy Auto-Config File URL

Proxy Host/IP

Proxy Port

Security * WPA2 Enterprise

Allowed Protocol * PEAP

Certificate Template Not Required

Optional Settings

Windows Settings

Authentication Mode User or Computer

- [ ] Automatically use logon name and password (and domain if any)
- [x] Enable fast reconnect
- [ ] Enable quarantine checks
- [ ] Disconnect if server does not present cryptobinding TLV
- [ ] Do not prompt user to authorize new servers or trusted certification authorities
- [x] Connect even if the network is not broadcasting its name (SSID)

iOS Settings

- [ ] Enable if target network is hidden

Android Settings

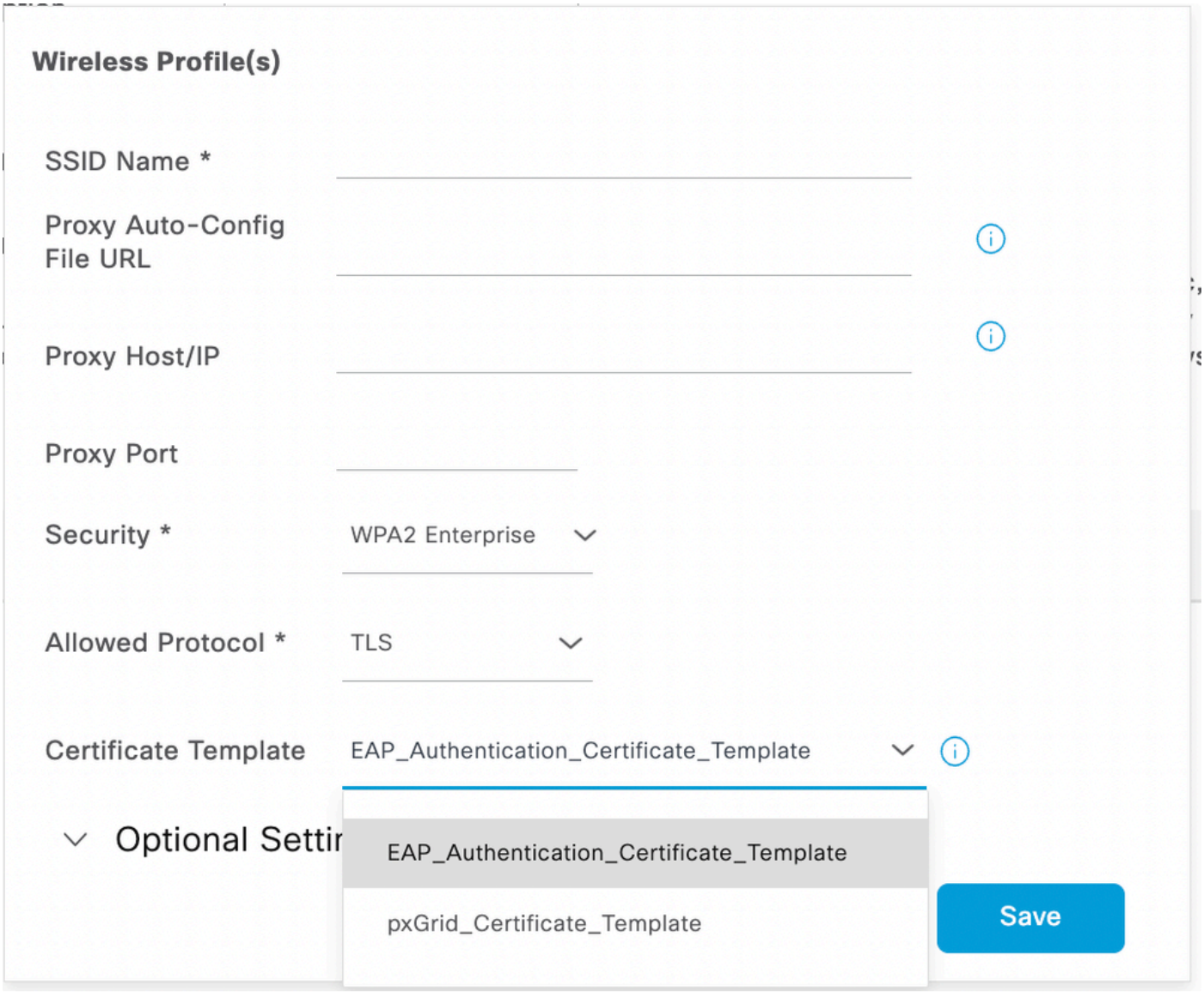
Certificate Enrollment Protocol:

Afhankelijk van uw vereiste dient u het eindpuntprofiel voor het eindpunt in uw omgeving te configureren. Met het profiel voor endpoints kunnen we EAP-PEAP, EAP-TLS configureren.

5. Klik op Opslaan en vervolgens op Indienen in het eindpuntprofiel.

Sjabloon voor certificaat

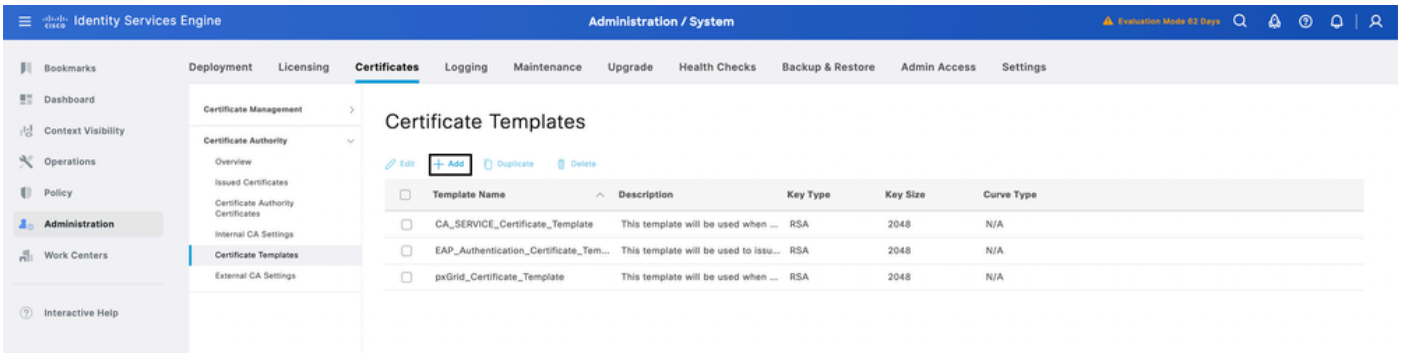
Het eindpuntprofiel is vooraf geconfigureerd om EAP-TLS uit te voeren. Er moet een certificaatsjabloon aan het profiel worden toegevoegd. Standaard heeft ISE twee vooraf gedefinieerde sjablonen die uit de vervolgkeuzelijst kunnen worden gekozen.



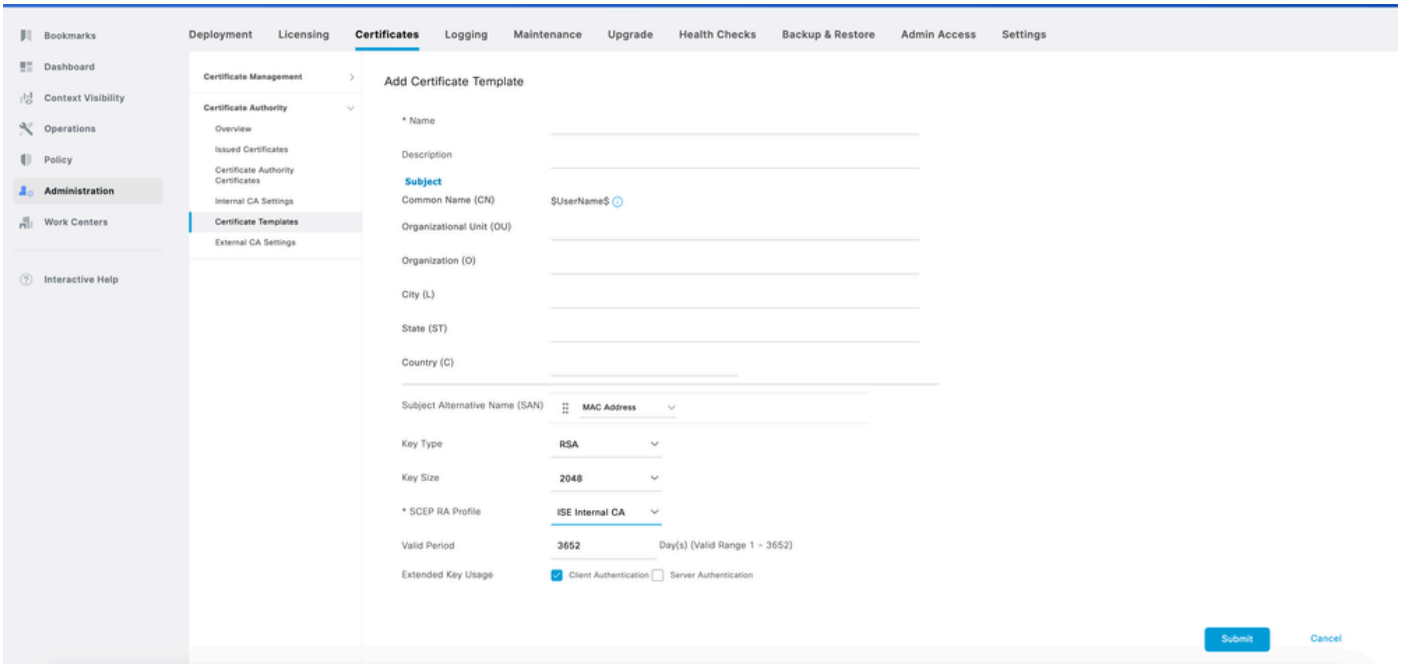
Voer de volgende stappen uit om een nieuwe certificaatsjabloon te maken:

1. Ga naar Beheer > Systeem > Certificaten > Certificaatautoriteit > Certificaatsjablonen.

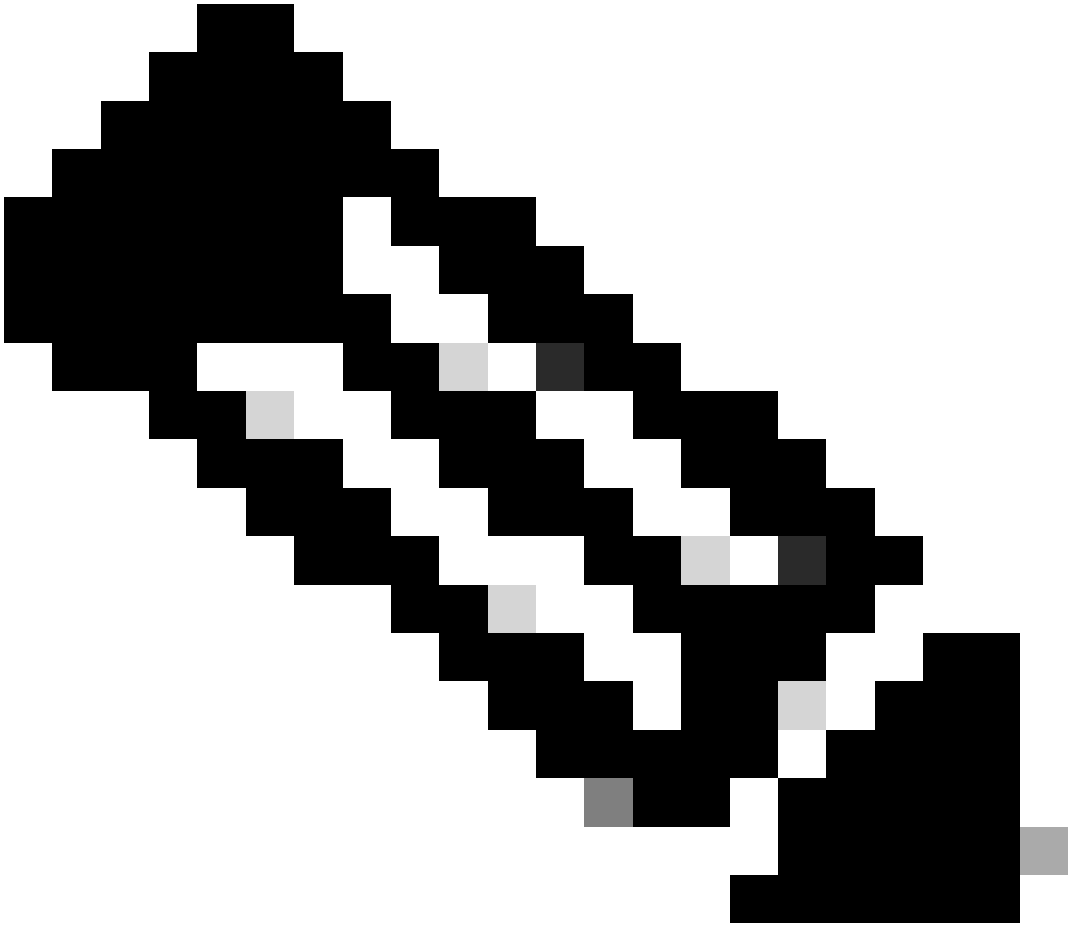
2. Klik op de knop Toevoegen op de pagina.



3. Vul de gegevens in die zijn afgestemd op de specifieke behoeften van uw organisatie.



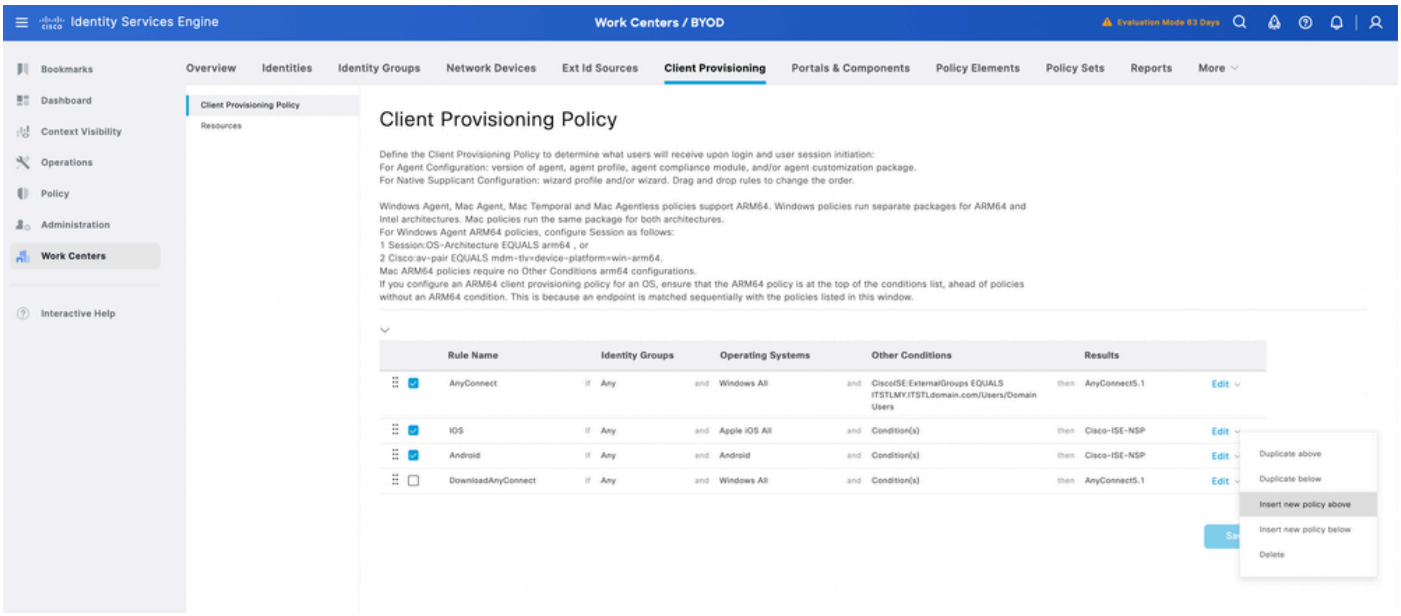
4. Klik op Indienen om de wijzigingen op te slaan.



Opmerking: De certificaatsjabloon kan nuttig zijn in een scenario wanneer u verschillende domeinen hebt en de gebruiker segmenteert door een andere waarde toe te voegen in de OE van het certificaat.

Een endpointprofiel toewijzen aan de client-provisioningportal

1. Navigeren naar werkcentra > BYOD > Clientprovisioning > Clientprovisioningbeleid.
2. Klik op v.n van de regels om een nieuwe regel voor clientprovisioning te maken.

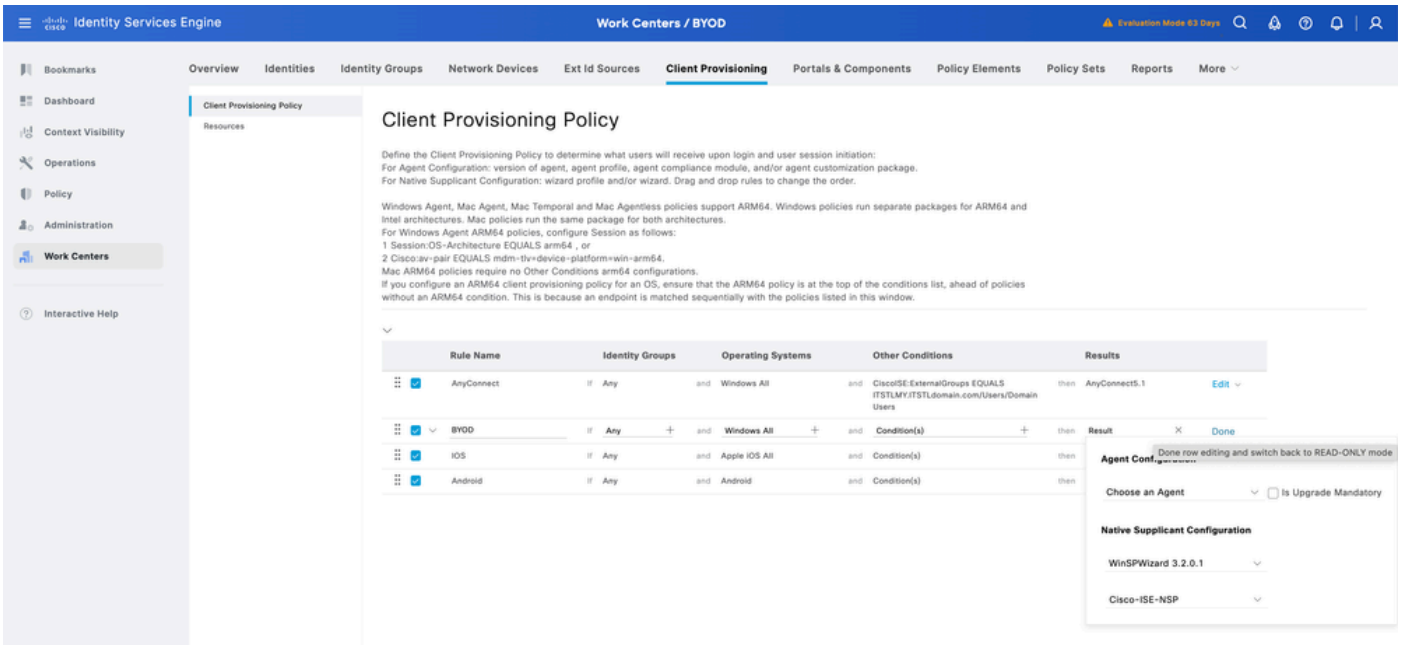


3. Plaats de nieuwe regel op de pagina

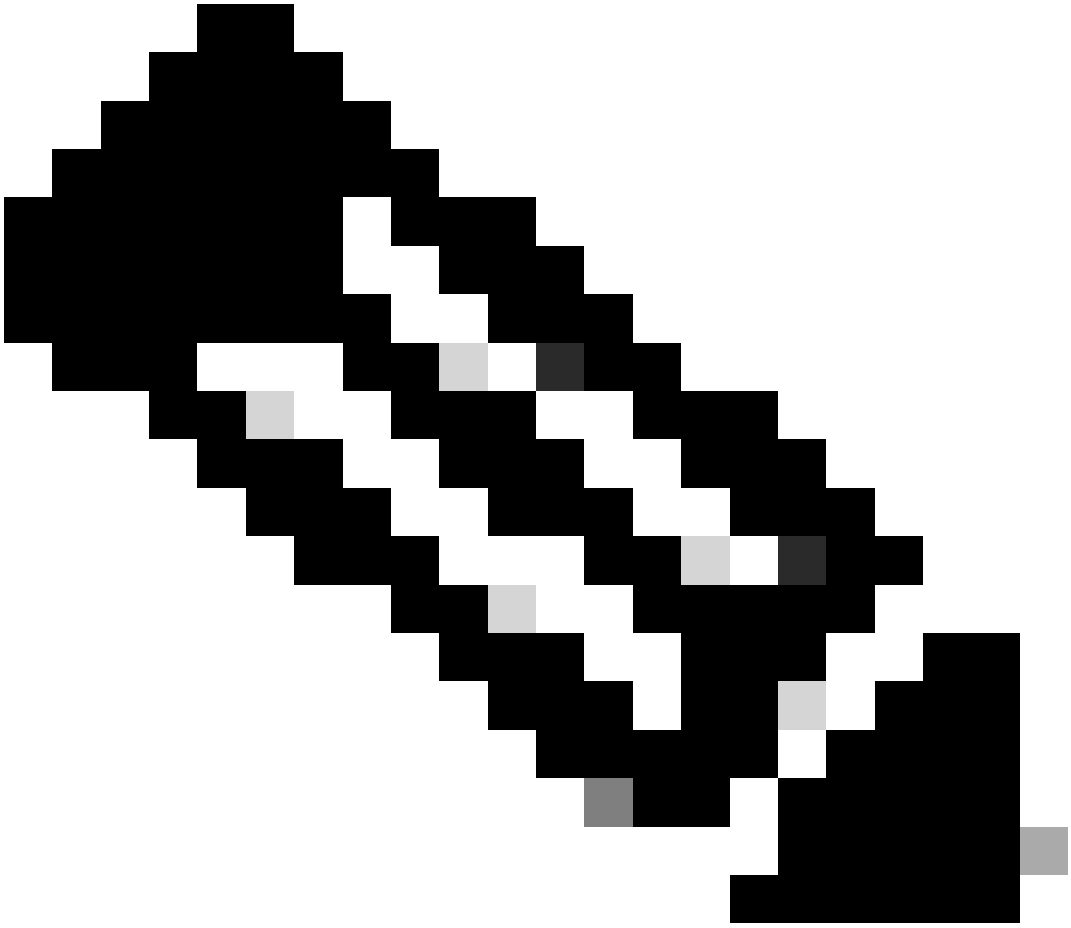
4. Voeg de identiteitsgroep toe als u bepaalde gebruikers wilt beperken om het BYOD-portaal te gebruiken

5. Voeg het besturingssysteem toe dat u toegang wilt hebben tot het BYOD-portal

6. Breng de Cisco IOS-versie uit de vervolgkeuzelijst in kaart en selecteer ook het eindpuntprofiel dat u op basis van het resultaat hebt gemaakt



7. Klik op Gereed en vervolgens op de knop Opslaan.

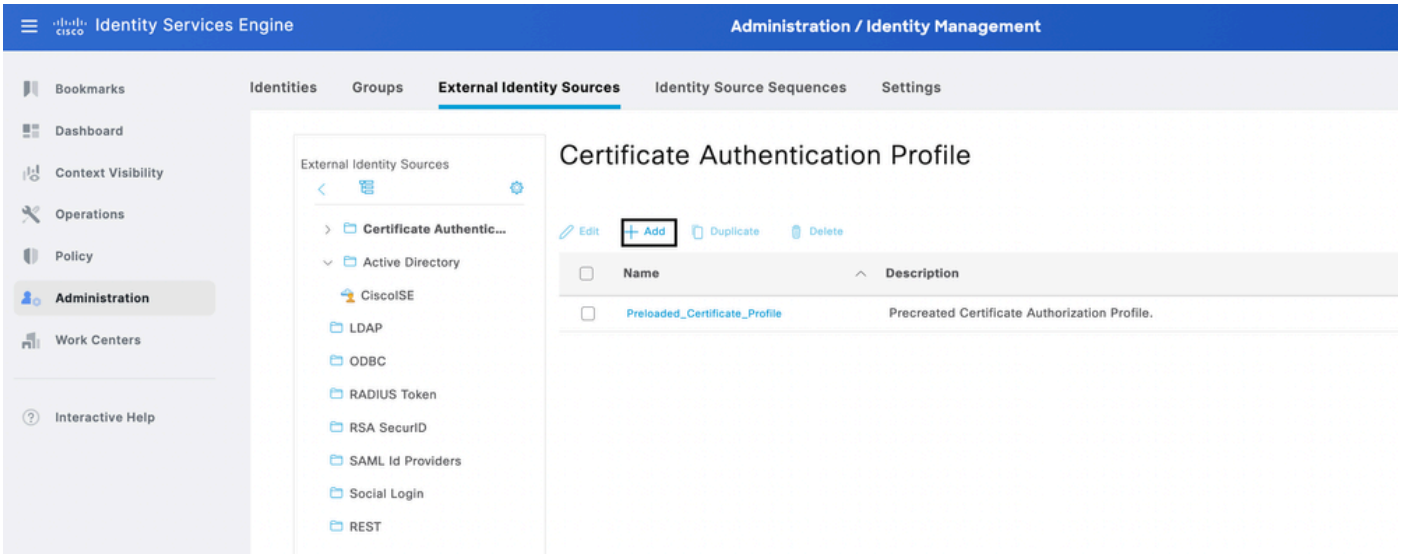


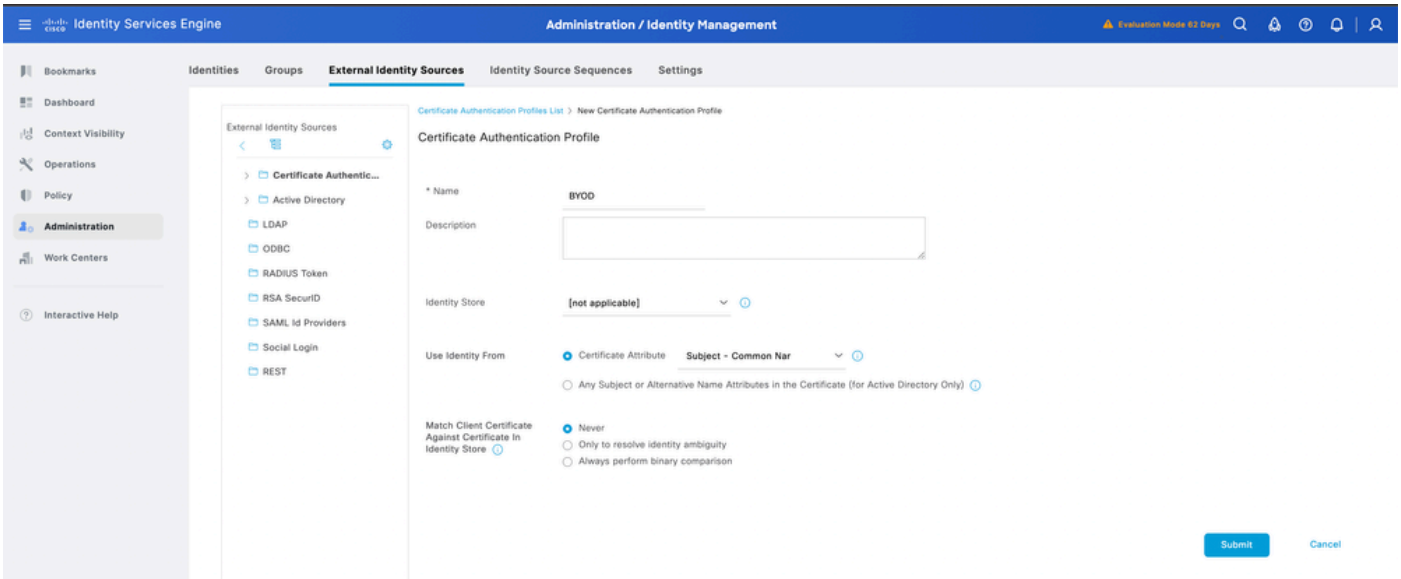
Opmerking: Dit beleid heeft invloed op zowel postuur client provisioning en BYOD provisioning, waar de Agent Configuration sectie bepaalt de postuur agent en compliance module afgedwongen voor postuur controles, terwijl de Native Supplicant Configuration sectie instellingen beheert voor BYOD provisioning stromen

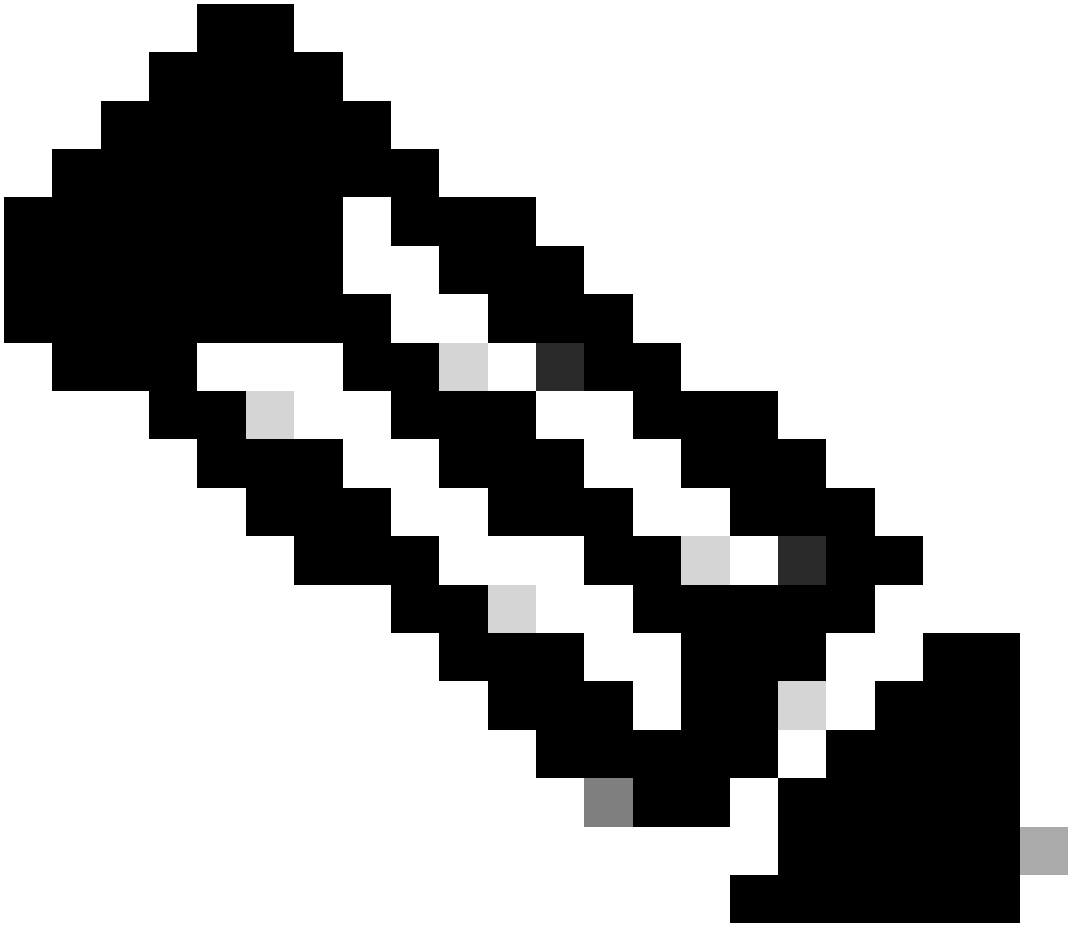
Configureer ISE-beleidssets voor één SSID-BYOD

1. Navigeren naar Policy > Policy Set en een beleid maken voor BYOD flow op ISE:

2. Navigeer vervolgens naar Beheer > Identity Management > Externe Identiteitsbronnen > Certificaatverificatieprofiel. Klik op de knop Add om het certificaatprofiel te maken:

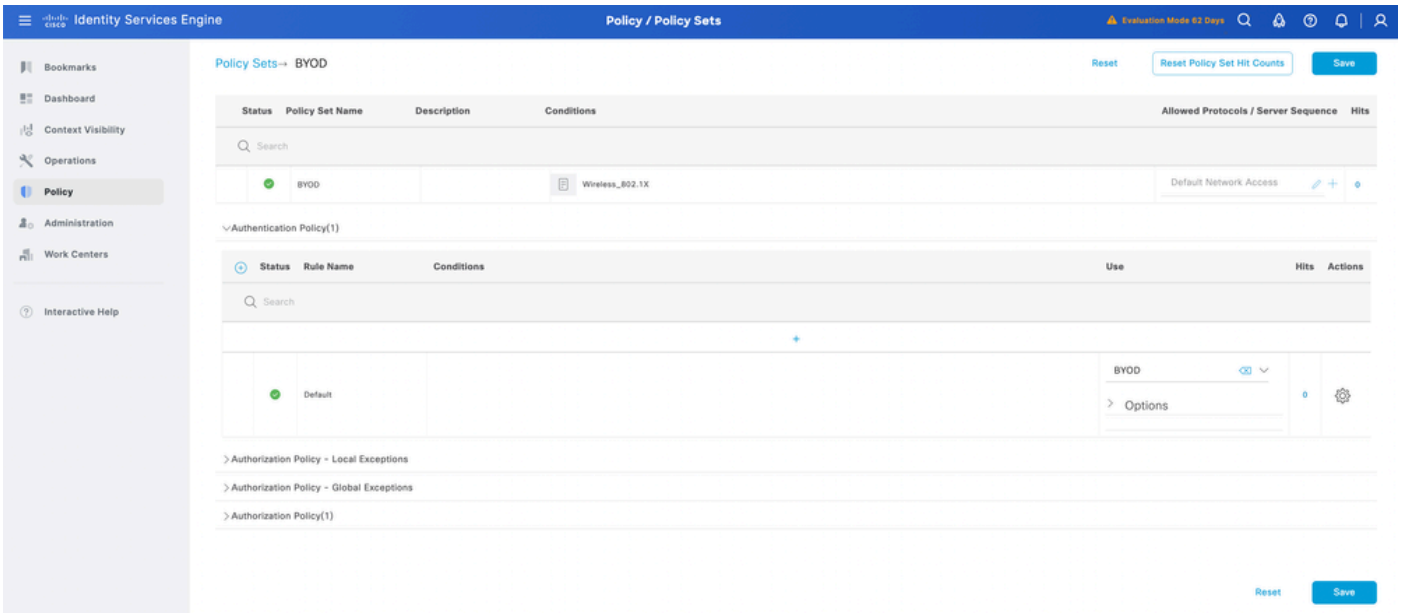






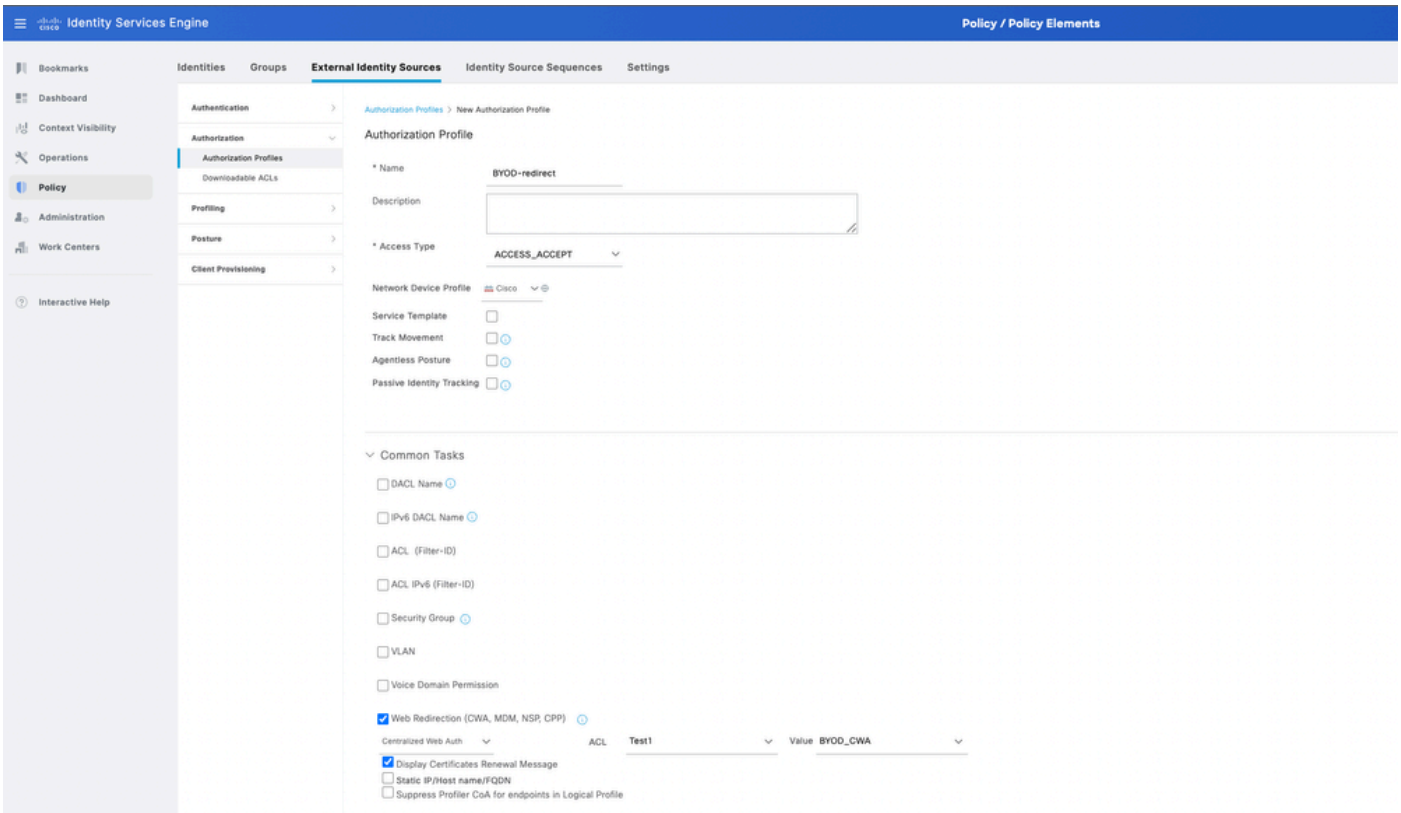
Opmerking: In de Identity Store kunt u altijd uw Active Directory selecteren die is geïntegreerd in ISE om een gebruikersraadpleging uit te voeren vanuit het certificaat voor extra beveiliging.

3. Klik op Indienen om de configuratie op te slaan. Vervolgens brengt u het certificaatprofiel in kaart met de beleidsset voor BYOD:

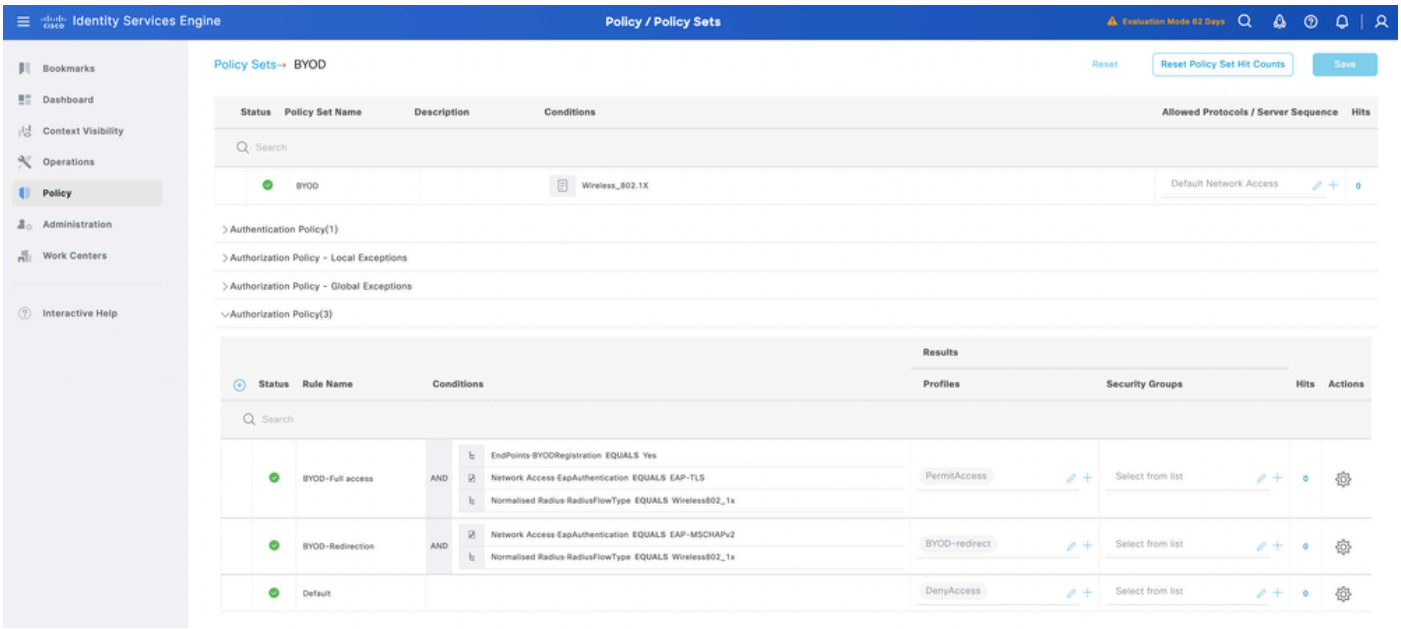


4. Het autorisatieprofiel voor BYOD-omleiding en volledige toegang na de BYOD-stroom configureren. Navigeer naar Beleid > Beleidselementen > Resultaten > Vergunning > Vergunningsprofielen.

5. Klik op Add en maak een autorisatieprofiel aan. Controleer de webomleiding (CWA, MDM, NSP, CPP) en breng de pagina van het BYOD-portaal in kaart. Voeg ook de Redirectie ACL-naam van WLC toe aan het profiel. Voor het volledige toegangsprofiel configureer je een vergunningstoegang met het betreffende zakelijke VLAN in het profiel.



6. Het autorisatieprofiel in kaart brengen aan de autorisatieregel. De BYOD volledige toegang moet de regel EndPoints·BYOD registratie gelijk ja hebben, zodat de gebruiker volledige toegang krijgt tot het netwerk na de BYOD-stroom.

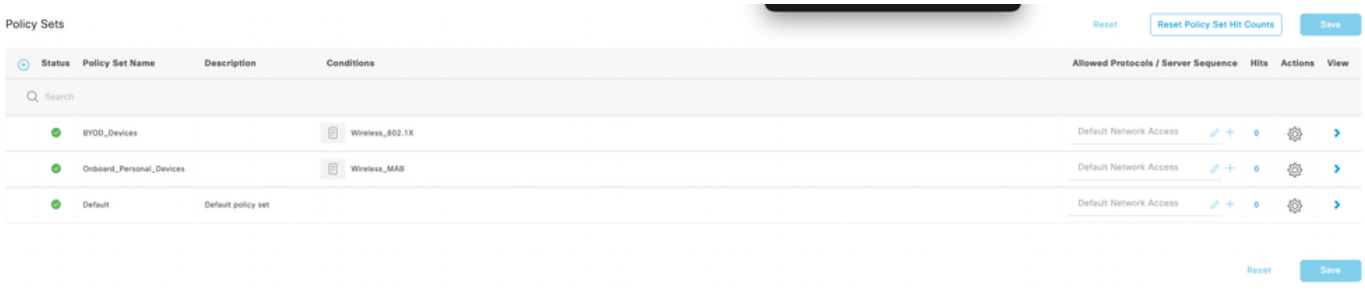


Configureer ISE-beleidssets voor Dual SSID BYOD

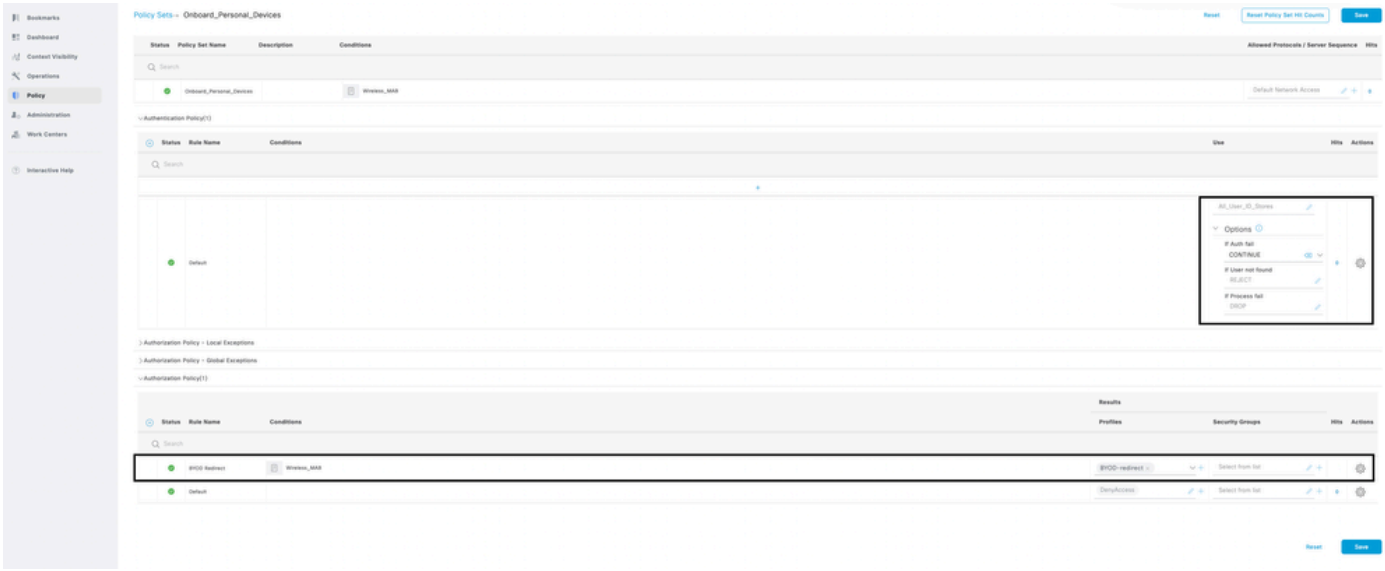
In Dual SSID BYOD configuratie, wordt de twee-beleid set geconfigureerd op ISE. De eerste beleidsset is voor de open/onbeveiligde SSID, waar de Policy Set-configuratie de gebruiker omleidt naar de BYOD-pagina bij het verbinden met de open/onbeveiligde SSID

1. Ga naar Policy > Policy Set en maak een Policy voor BYOD-flow op ISE.

2. Maak een Policy set voor de Open/Unsecure SSID en Corporate SSID die de geregistreerde BYOD-gebruiker op ISE authenticeert.

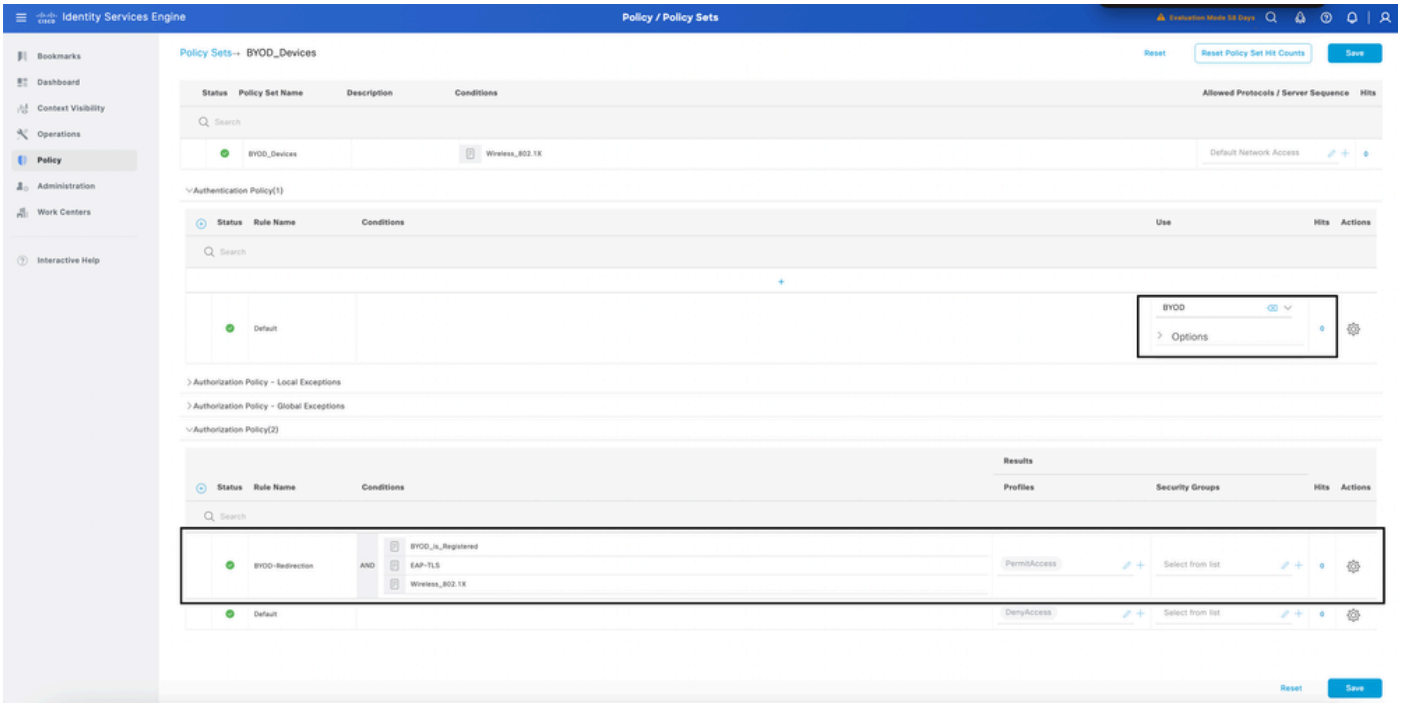


3. Zoek in de reeks Onboarding Policy de optie Doorgaan onder de opties. Voor het autorisatiebeleid moet u een voorwaarde maken en het omleidingsautorisatieprofiel toewijzen. Dezelfde stappen zijn nodig bij het opstellen van het vergunningsprofiel, dat onder punt 4 kan worden gevonden.



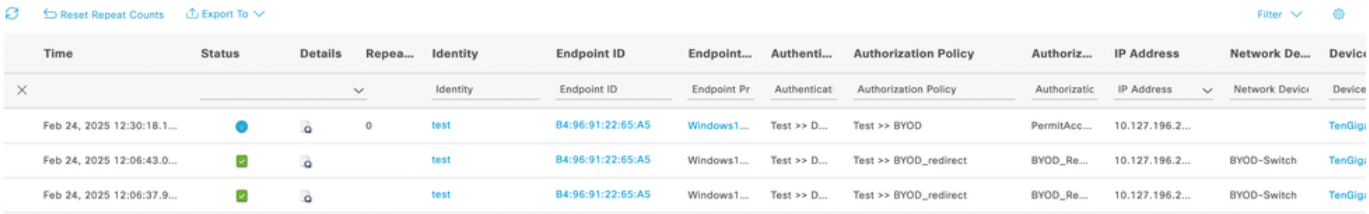
4. In de BYOD Registered Policy Set moet u het verificatiebeleid configureren met hetzelfde certificaatprofiel als u hebt gevonden.

in het configureren van ISE Policy Sets voor Single SSID BYOD in punt 2. Maak ook een voorwaarde voor autorisatiebeleid en breng het volledige toegangsprofiel in kaart met het beleid.

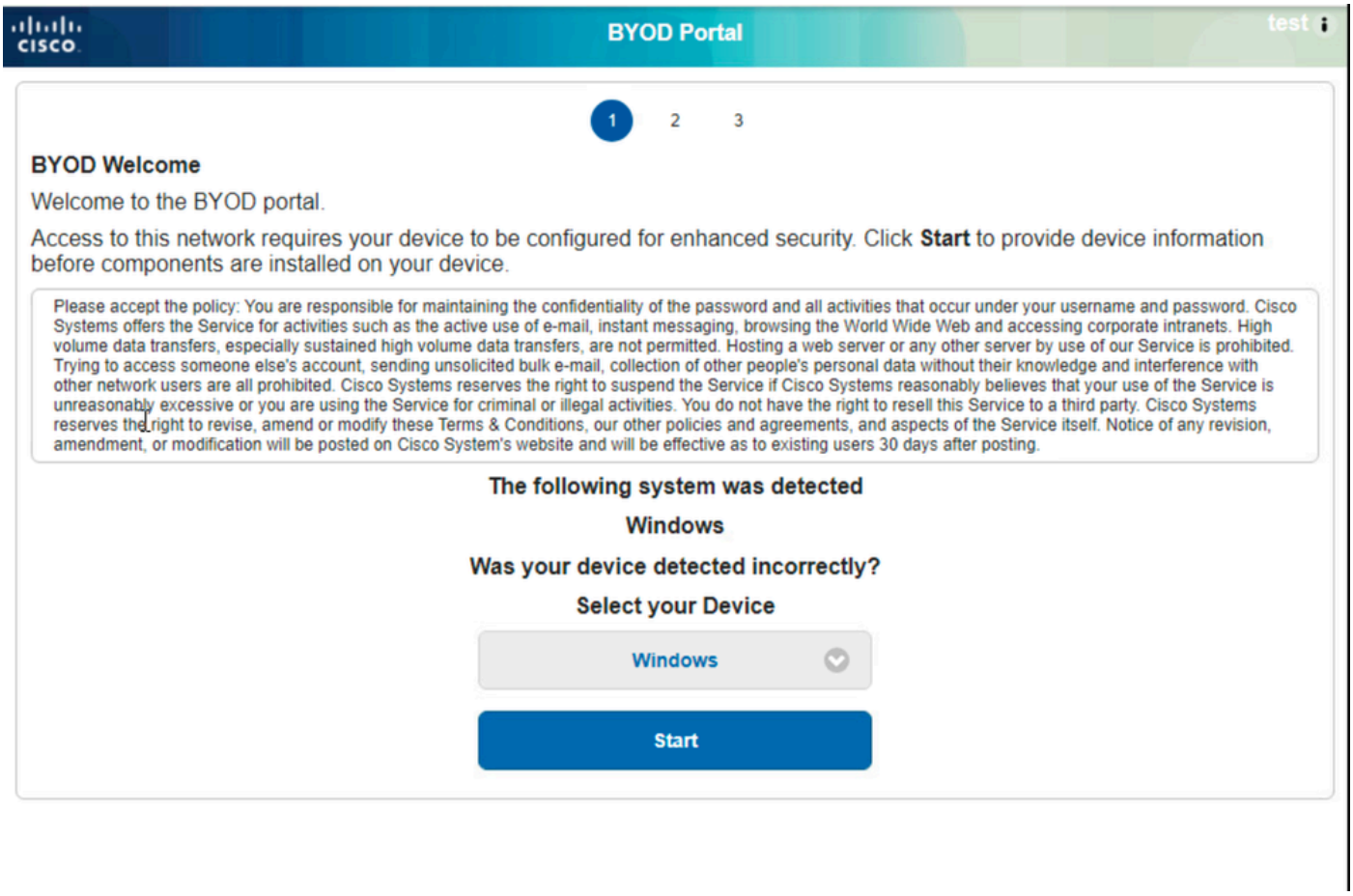


Logboekregistratie

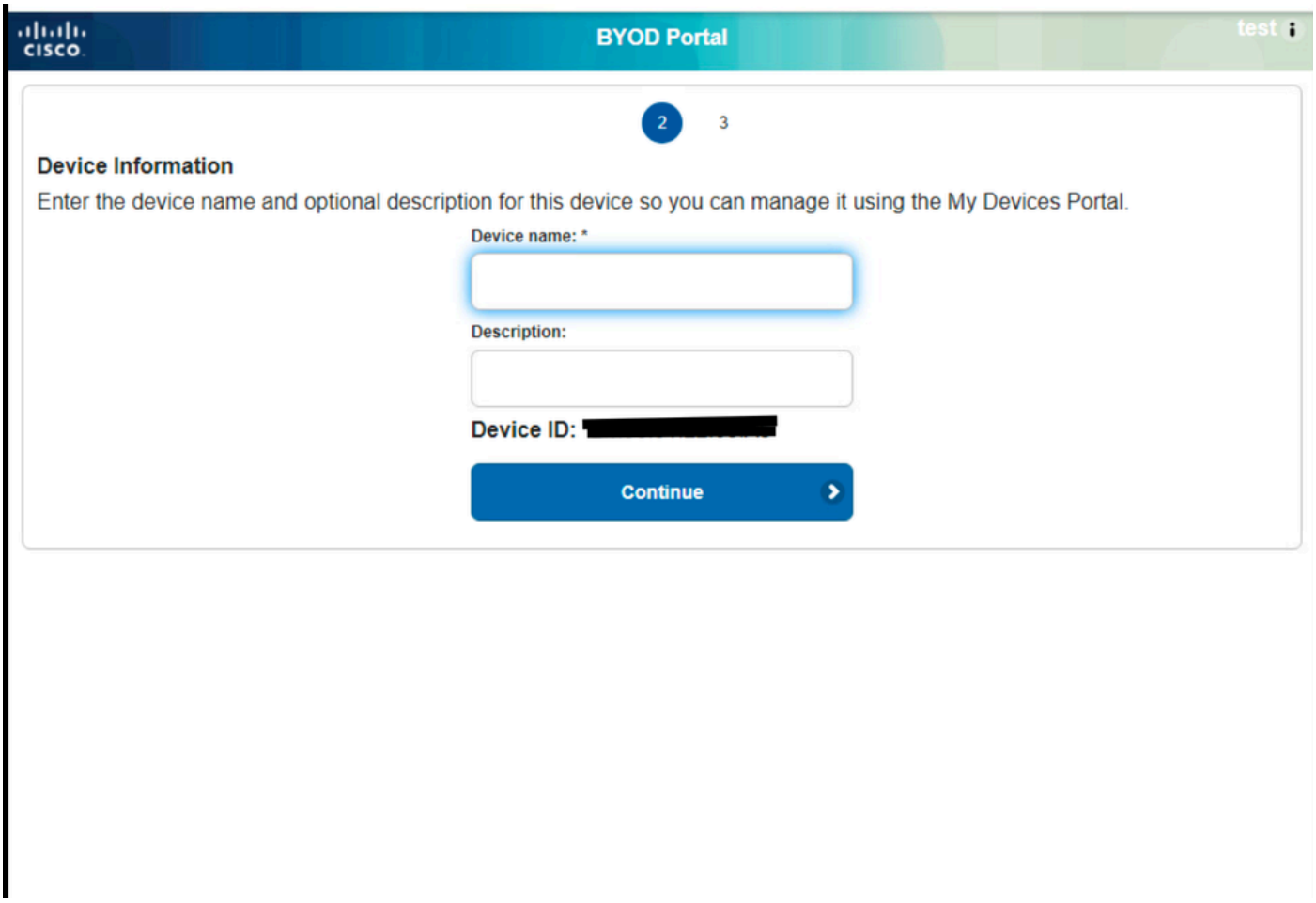
Vanuit het live-logbestand van ISE zou de gebruikersverificatie succesvol zijn en worden doorgestuurd naar de BYOD Portal-pagina. Na voltooiing van de BYOD-stroom, zou de gebruiker toegang tot het netwerk moeten verlenen



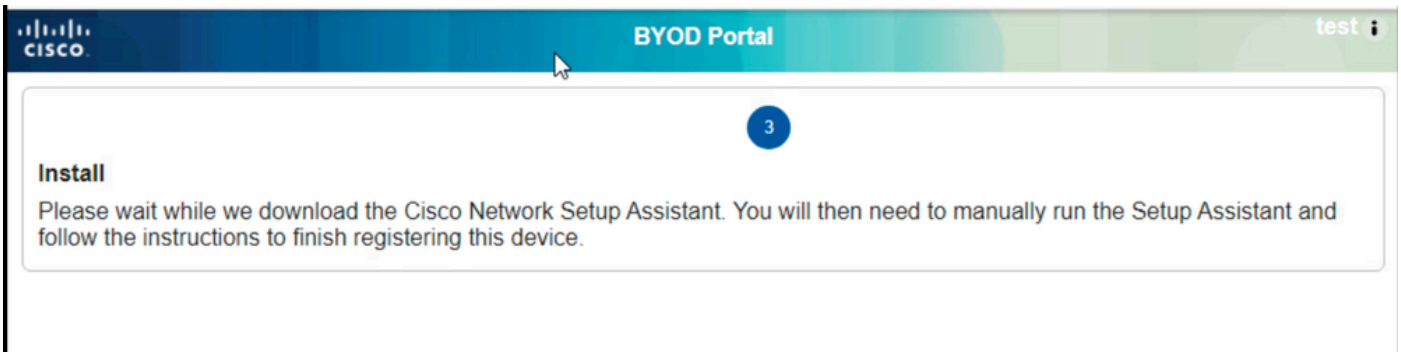
Vanuit het gebruikersperspectief worden ze eerst omgeleid naar de BYOD-pagina en moet het juiste apparaat worden geselecteerd van de webpagina. Voor het testen van een Windows 10 apparaat werd gebruikt



Nadat u op de knop Volgende hebt geklikt, wordt u naar een pagina geleid waar de gebruiker wordt gevraagd de naam van het apparaat en de beschrijving in te voeren

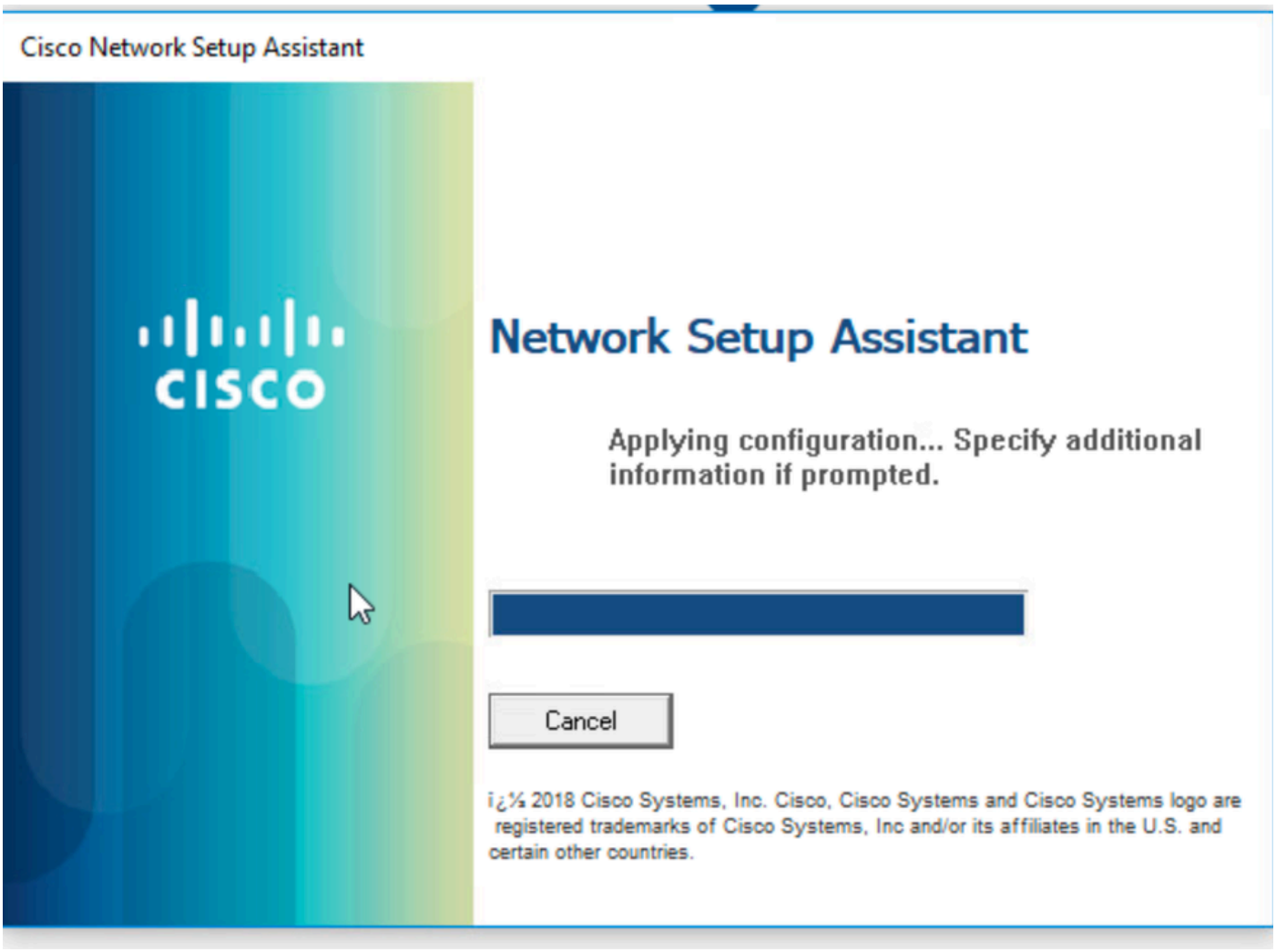


Plaats dat de gebruiker wordt gevraagd om het Network Assistant-programma te downloaden voor het downloaden van het Endpoint-profiel en het EAP TLS-certificaat voor verificatie als het profiel is geconfigureerd voor het uitvoeren van EAP-TLS-verificatie



Voer de Network Assistant-toepassing uit met beheerdersrechten en klik op de knop Start om het onboarding te starten:


Cisco Network Setup Assistant
Network Setup Assistant
This application automatically configures network settings.
Start
Quit
i¿¼ 2018 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.



De gebruiker is met succes op het netwerk met hun persoonlijk apparaat aan boord gegaan om tot de middelen toegang te hebben.

Probleemoplossing

Als u het probleem met BYOD wilt oplossen, schakelt u deze debug in op ISE

Kenmerken die moeten worden ingesteld om debug niveau:

- client (guest.log)
- client-webapp (guest.log)
- scep (ise-psc.log)
- ca-service (ise-psc.log)
- admin-ca (ise-psc.log)
- runtime-AAA (poortserver.log)
- nsf (ise-psc.log)
- nsf-sessie (ise-psc.log)
- profiler (profiler.log)

Logfragment

Gastenlogboeken

Deze logbestanden geven aan dat de gebruiker met succes naar de pagina is doorgestuurd en de Network Assistant-toepassing heeft gedownload:

2025-02-24 12:06:08,053 INFO [https-jsse-nio-10.127.196.172-8443-exec-4][[]] portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:000000000000000B30D59CC5::::- kartering gevonden in actie-forwards, doorsturen naar: pages/byodWelcome.jsp // De welkomstpagina van BYOD
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- Grootte van pTranStappen:1
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep, pTranStps:[id: d2513b7b-7249-4bc3-a423-0e7d9a0b2500]
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep, stepTran:d2513b IE-7249-4bc3-a423-0e7d9a0b2500
2025-02-24 12:06:09,979 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]] portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:000000000000000B30D59CC5::::- kartering pad gevonden in actie-forwards, doorsturen naar: pages/byodRegistration.jsp
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- Grootte van pTranStappen:1
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep, pTranStps:[id: f203b757-9e8a-473e-abdc-879d0cd37491]
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][[]] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep, stepTran:f203b7 7-9e8a-473e-abdc-879d0cd37491
2025-02-24 12:06:14,647 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][] portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:000000000000000B30D59CC5::::- kartering pad gevonden in actie-forwards, doorsturen naar: pages/byodInstall.jsp
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5:::- Session = null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::::- portalSessionID = null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5:::::- StreamingServlet URI:/auth/provisioning/download/f6b73ef8-4502-4d50-81aa-bbb91e8828da/NetworkSetupAssistant.exe // De netwerk bijstandsapplicatie is naar het netwerk verzonden

ISE-PSC-logbestanden

Aangezien de toepassing aan het eindpunt wordt gedownload, stelt de toepassing een stroom SCEP in werking om het cliëntcertificaat van ISE te krijgen.

2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::::- CertStore bevat 4 certificaat(s):
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::::- 1. "[issuer=CN=Certificate Services Root CA - iseguest; seriële=322815127387689606282525327846633020 89]'
2025-02-24 12:04:39,808 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- 2. "[issuer=CN=Certificate Services Endpoint Sub CA - iseguest; seriële=131900858749761727853768227590303808637]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- 3. "[issuer=CN=Certificate Services Root CA - iseguest; seriële=686276201605863086858498187751006982 24]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- 4. "[issuer=CN=Certificate Services Node CA - iseguest; seriële=729347676986030971539324822275488749 53]'
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::::- Selecteren van encryptie certificaat
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Certificaat selecteren met sleutelEncipherment keyGebruik
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Gevonden 1 certificaat(en) met keyEncipherment keyGebruik
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::: - Gebruik [issuer=CN=Certificate Services Endpoint Sub CA - Inguest; seriële=131900858749761727853768227590303808637] voor berichtversleuteling
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::::- Selecteren van verificateur certificaat
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Certificaat selecteren met digitaleHandtekening sleutelGebruik
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Gevonden 1 certificaat(en) met digitaleSignature sleutelGebruik
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::: - Gebruik [issuer=CN=Certificate Services Endpoint Sub CA - Inguest; seriële=131900858749761727853768227590303808637] voor berichtverificatie
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::::- Selecteren van emittentencertificaat
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::::- Certificaat selecteren met basisBeperkingen

2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::::- Gevonden 3 certificaat(s) met basisBeperkingen
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -:::: - Gebruik [issuer=CN=Certificate Services Endpoint Sub CA - Inguest; seriële=131900858749761727853768227590303808637] voor de emittent
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] com.cisco.cpm.scep.PKIServerLoadBalancer -::::- SCEP servers prestatiemaatstaven: naam[levend/dood, totale vereisten, totale mislukkingen, inflight-vereisten, gemiddelde RTT] http://127.0.0.1:9444/caservice/scep[live,96444,1,0,120]

Downloaden van endpointprofiel

Nadat het SCEP-proces is voltooid en het eindpunt het certificaat installeert, downloadt de toepassing het eindpuntprofiel voor toekomstige verificatie die door het apparaat zou worden uitgevoerd:

2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]] cisco.cpm.client.provisioning.EvaluationServlet -::::- Refferer = Windows // Het Windows-apparaat is gedetecteerd op basis van de webpagina
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]] cisco.cpm.client.provisioning.EvaluationServlet -:::- Session = 000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]] cisco.cpm.client.provisioning.EvaluationServlet -:::- Session = 000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]] cisco.cpm.client.provisioning.EvaluationServlet -::::- Voorziening nsp profiel
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -::::- Session = 000000000000000B30D59CC5
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -::::- portalSessionID = null
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -::::- StreamingServlet URI:/auth/provisioning/download/b8ce01e6-b150-4d4e-9698-40e48d5e0197/Cisco-ISE-NSP.xml//Het NSP profiel wordt gedownload naar het eindpunt
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -::::- Streaming naar ip: bestandstype: NativeSPP-bestandsnaam:Cisco-ISE-NSP.xml //The Network Assistant-toepassing
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -::::- BYODStatus:INIT_PROFILE
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -::::- userID is ingesteld om te testen
2025-02-24 12:06:26,558 DEBUG [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -::::- omleiden type is: SUCCESS_PAGE, omleiden url is: mac:

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.