802.1X-verificatie configureren met PEAP, ISE 2.1 en WLC 8.3

Inhoud

Inleiding

Dit document beschrijft hoe u een Wireless Local Area Network (WLAN) kunt instellen met 802.1x-beveiliging en Virtual Local Area Network (VLAN)-opheffing.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- 802.1x
- Protected Extensible Verification Protocol (PEAP)
- Certificeringsinstantie (CA)
- Certificaten

Gebruikte componenten

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

- WLC v8.3.102.0

- Identity Service Engine (ISE) v2.1
- Windows 10-laptop

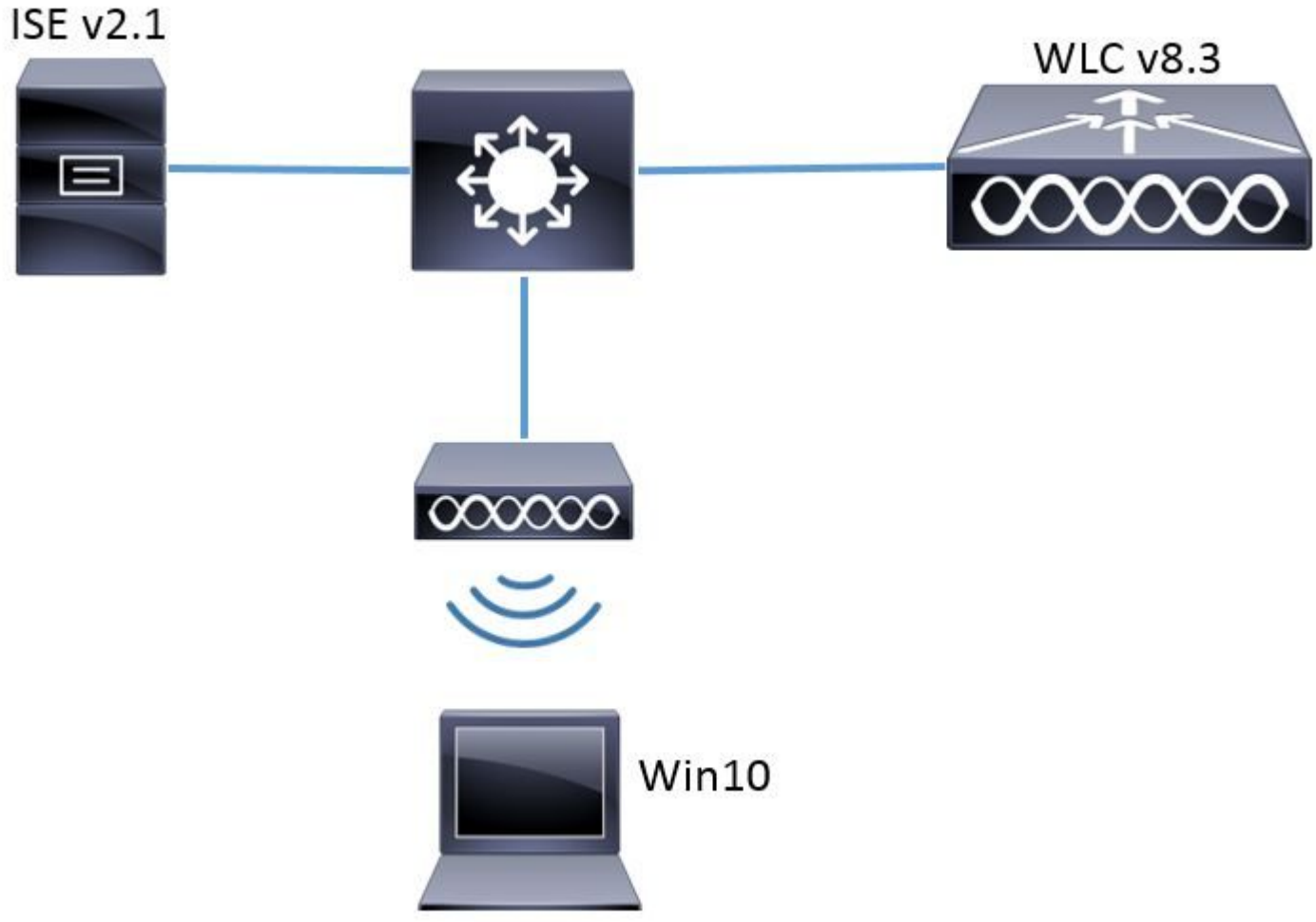
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Wanneer u een WLAN met 802.1x-beveiliging en VLAN instelt, kunt u met Protected Extensible Verification Protocol (EAP) overschrijven.

Configureren

Netwerkdiagram



Configuratie

De algemene stappen zijn:

1. Verklaar de Server van de RADIUS op WLC en vice versa om communicatie met elkaar toe te staan.
2. Maak de Service Set Identifier (SSID) aan in de WLC.
3. Maak de verificatieregel op ISE.
4. Maak het autorisatieprofiel op ISE.

5. Maak de autorisatieregel op ISE aan.
6. Configureer het eindpunt.

RADIUS-server op WLC verklaren

Om communicatie tussen RADIUS-server en WLC mogelijk te maken, moet u RADIUS-server op WLC registreren en omgekeerd.

GUI:

Stap 1. Open de GUI van de WLC en navigeer naar **SECURITY > RADIUS > Verificatie > Nieuw** zoals in de afbeelding.

Stap 2. Voer de RADIUS-serverinformatie in zoals in de afbeelding.

CLI:

```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
```

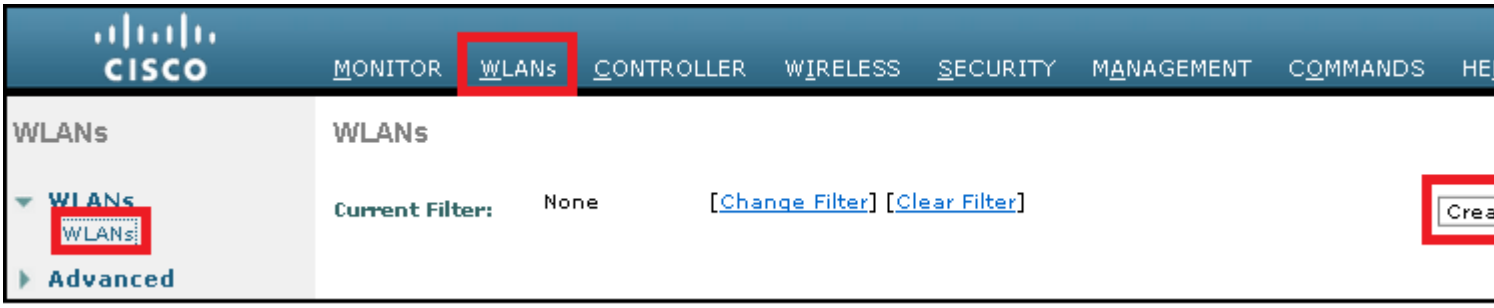
```
> config radius auth enable <index>
```

<a.b.c.d> komt overeen met de RADIUS-server.

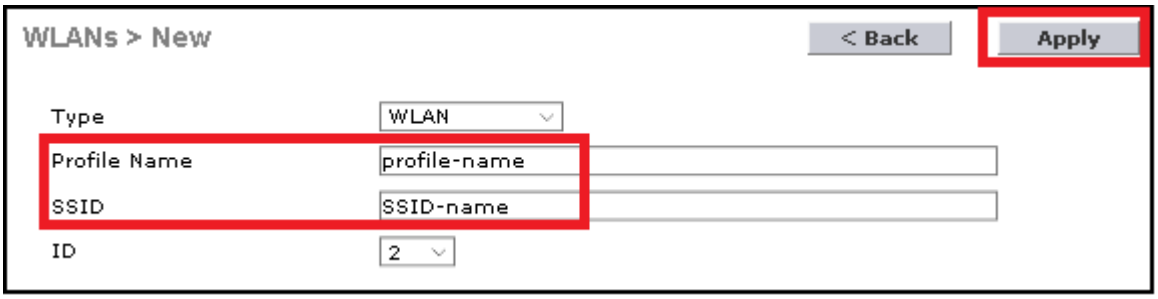
SSID maken

GUI:

Stap 1. Open de GUI van de WLC en navigeer naar **WLANâ€™s > Nieuw maken > Ga** zoals in de afbeelding.



Stap 2. Kies een naam voor de SSID en het profiel en klik vervolgens op **Toepassen** zoals in de afbeelding.



CLI:

```
> config wlan create <id> <profile-name> <ssid-name>
```

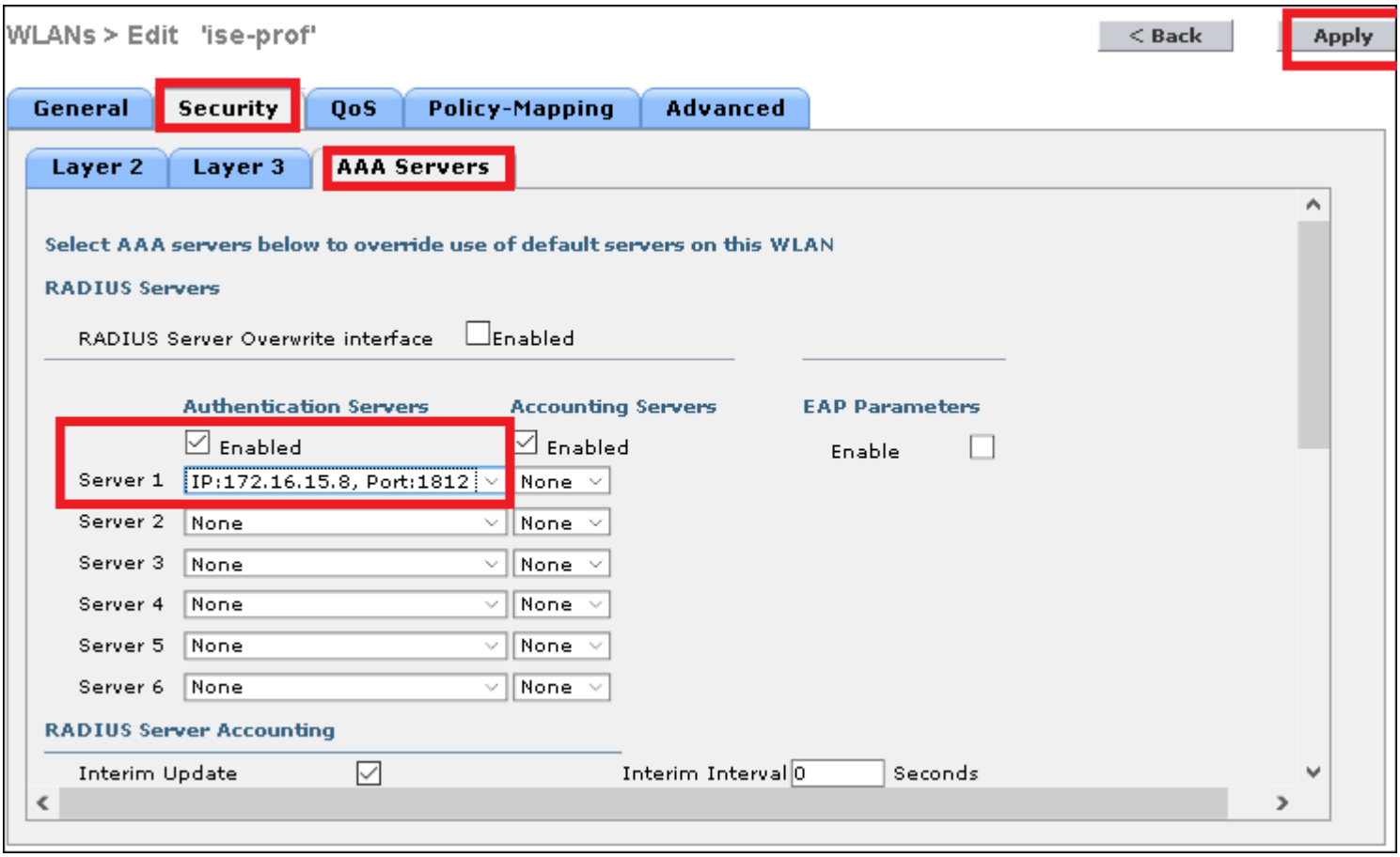
Stap 3. Wijs de RADIUS-server toe aan het WLAN.

CLI:

```
> config wlan radius_server auth add <wlan-id> <radius-index>
```

GUI:

Navigeer naar **Security > AAA-servers** en kies de gewenste RADIUS-server. Klik vervolgens op **Toepassen** zoals in de afbeelding.



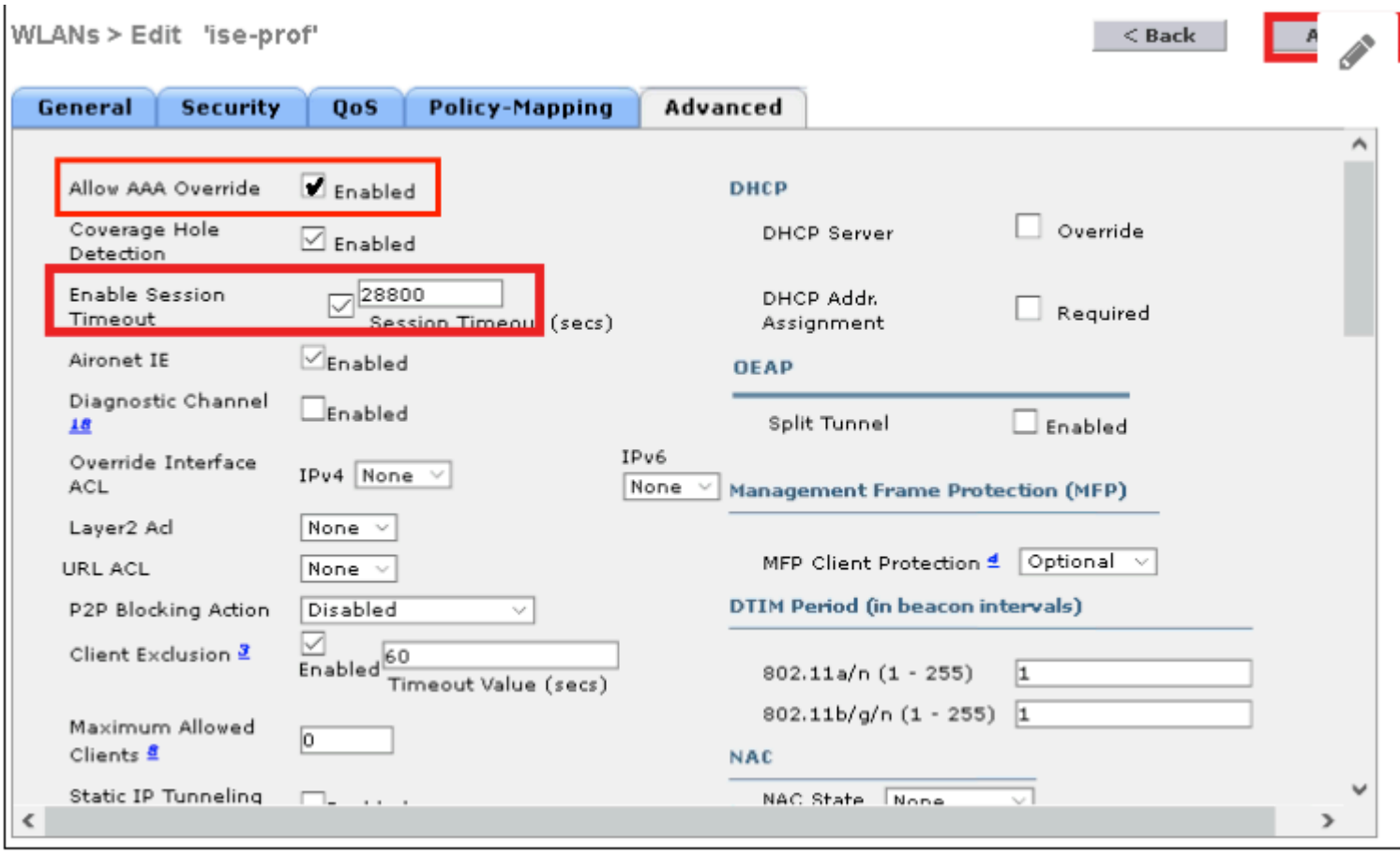
Stap 4. **AAA negeren** en optioneel de sessietime-out inschakelen

CLI:

```
> config wlan aaa-override enable <wlan-id>
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI:

Navigeer naar **WLANâ€™s > WLAN-id > Geavanceerd** en schakel **AAA-opheffing in**. Specificeer optioneel de Session Time-out zoals in de afbeelding.



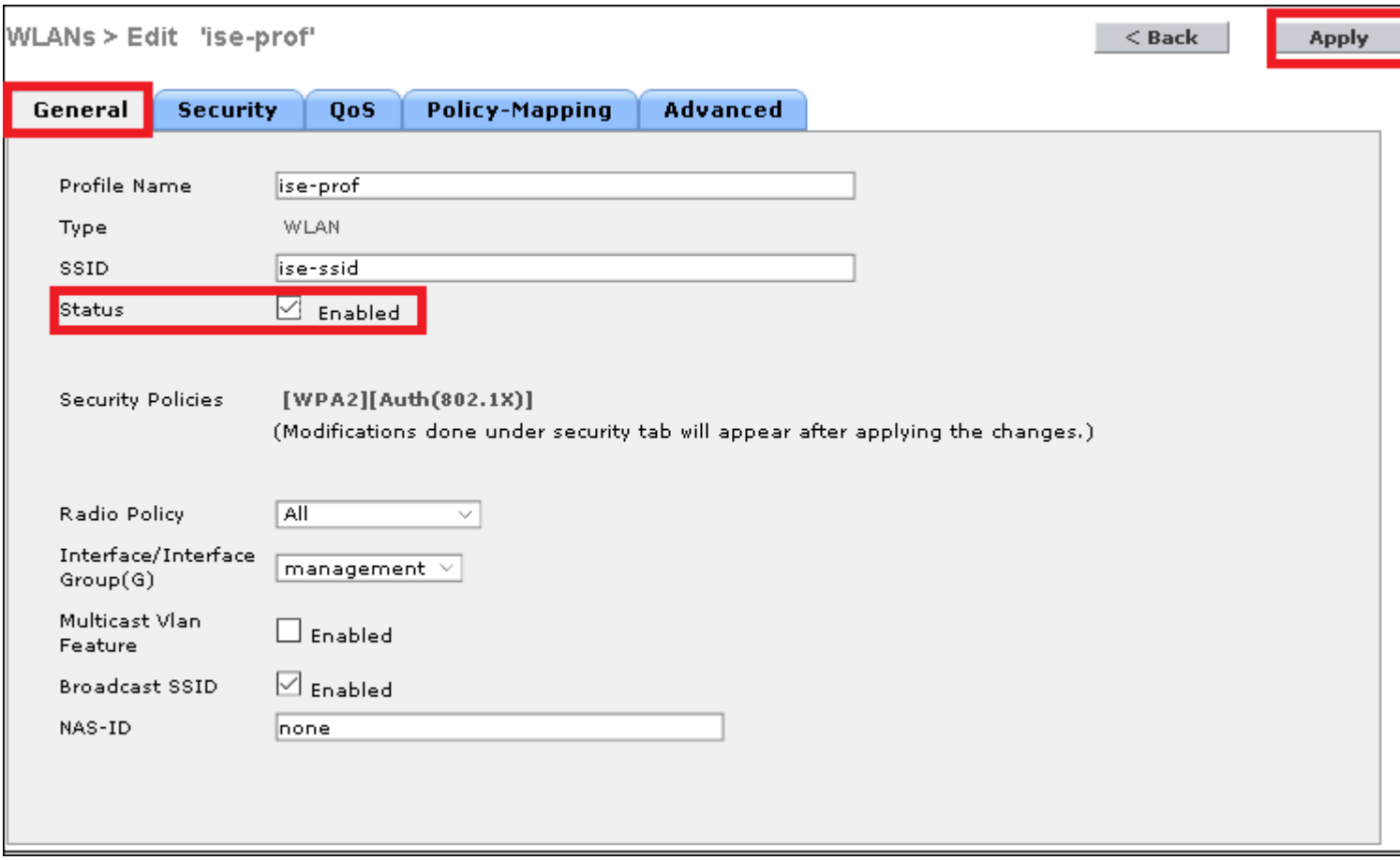
Stap 5. Schakel het WLAN in.

CLI:

```
> config wlan enable <wlan-id>
```

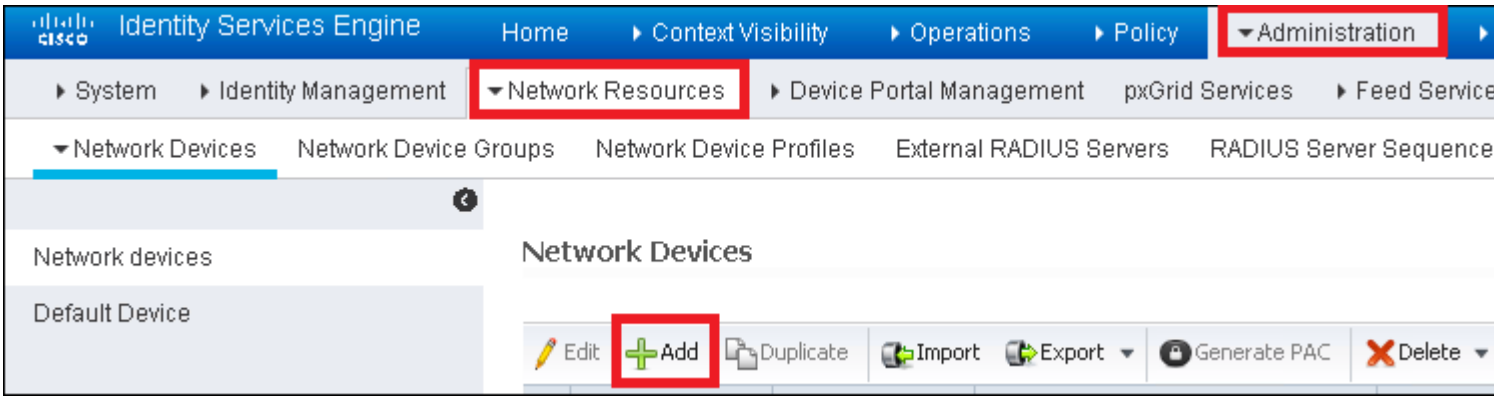
GUI:

Navigeer naar **WLANâ€™s > WLAN-id > Algemeen** en schakel de SSID in zoals in het beeld.



WLC declareren op ISE

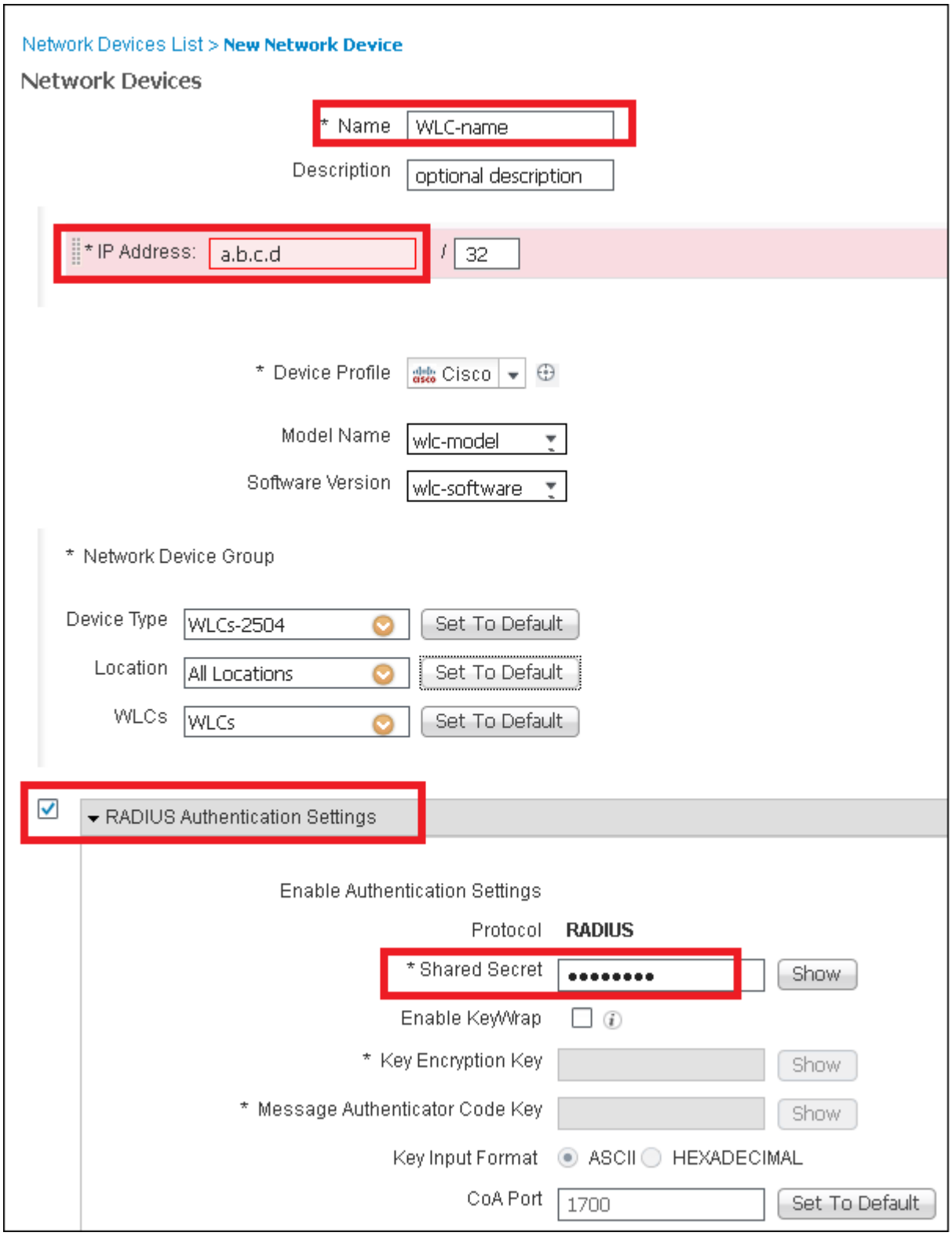
Stap 1. Open de ISE-console en navigeer naar **Beheer > Netwerkbronnen > Netwerkapparaten > Toevoegen** zoals in de afbeelding.



Stap 2. Voer de waarden in.

Optioneel kan het een opgegeven Modelnaam, softwareversie, beschrijving zijn en netwerkapparaatgroepen toewijzen op basis van apparaattypen, locatie of WLC's.

a.b.c.d komt overeen met de WLC-interface die de gevraagde verificatie verstuurt. Standaard is het de beheerinterface zoals in het beeld.

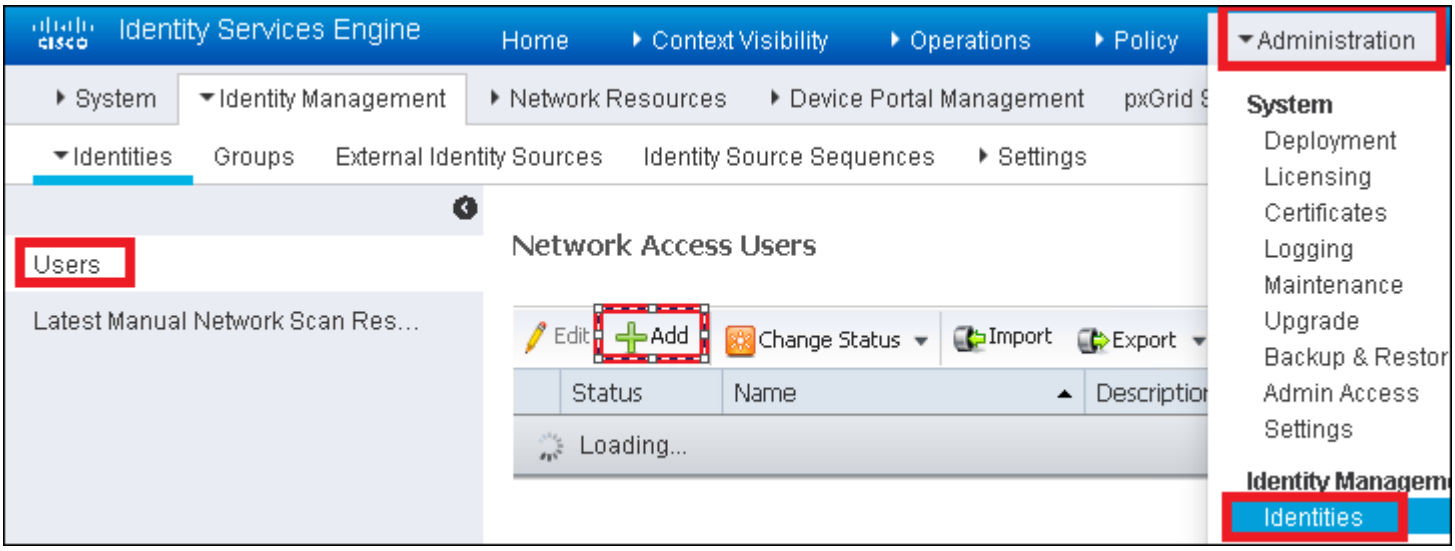


Voor meer informatie over Netwerkapparaatgroepen:

ISE - Apparaatgroepen voor netwerk

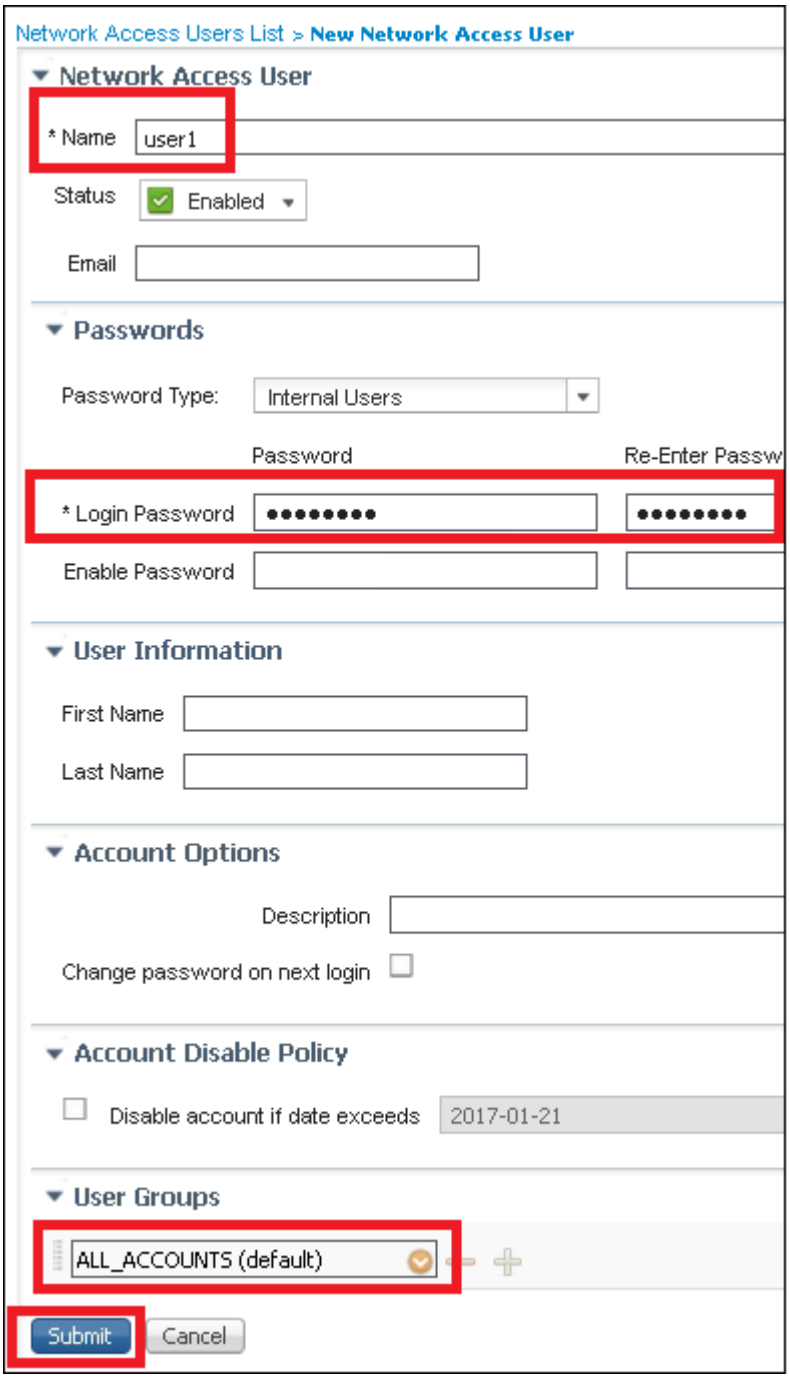
Nieuwe gebruiker maken op ISE

Stap 1. Ga naar **Beheer > Identiteitsbeheer > Identiteiten > Gebruikers > Toevoegen** zoals in de afbeelding.



Stap 2. Voer de informatie in.

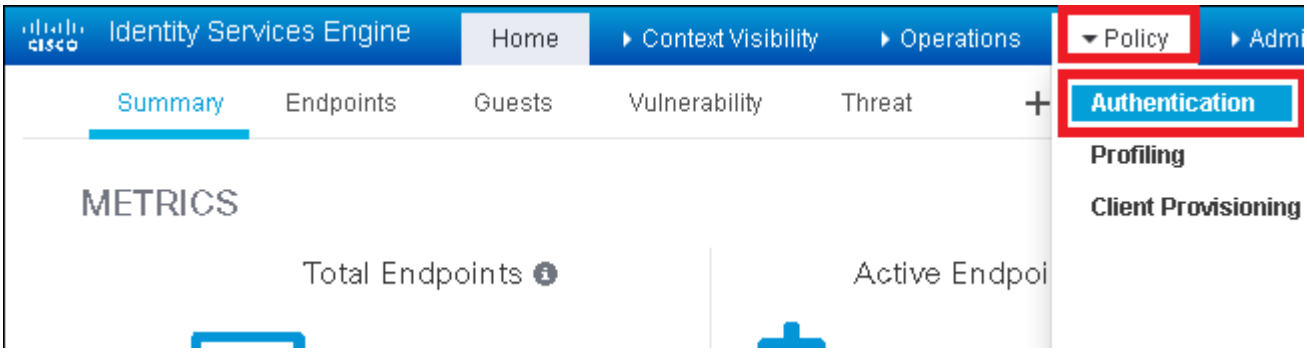
In dit voorbeeld behoort deze gebruiker tot de groep ALL_ACCOUNTANTS, maar hij kan naar behoefte worden aangepast, zoals in de afbeelding wordt getoond.



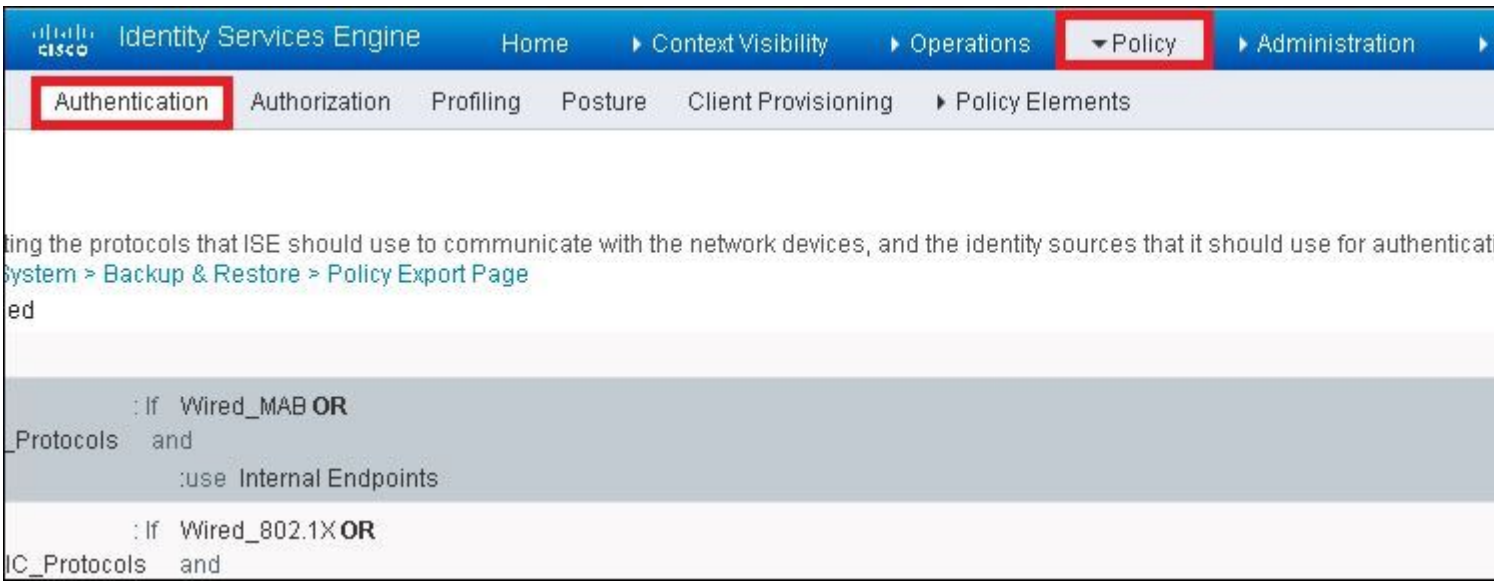
Verificatieregel maken

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

Stap 1. Navigeer naar **Beleid > Verificatie** zoals in de afbeelding.

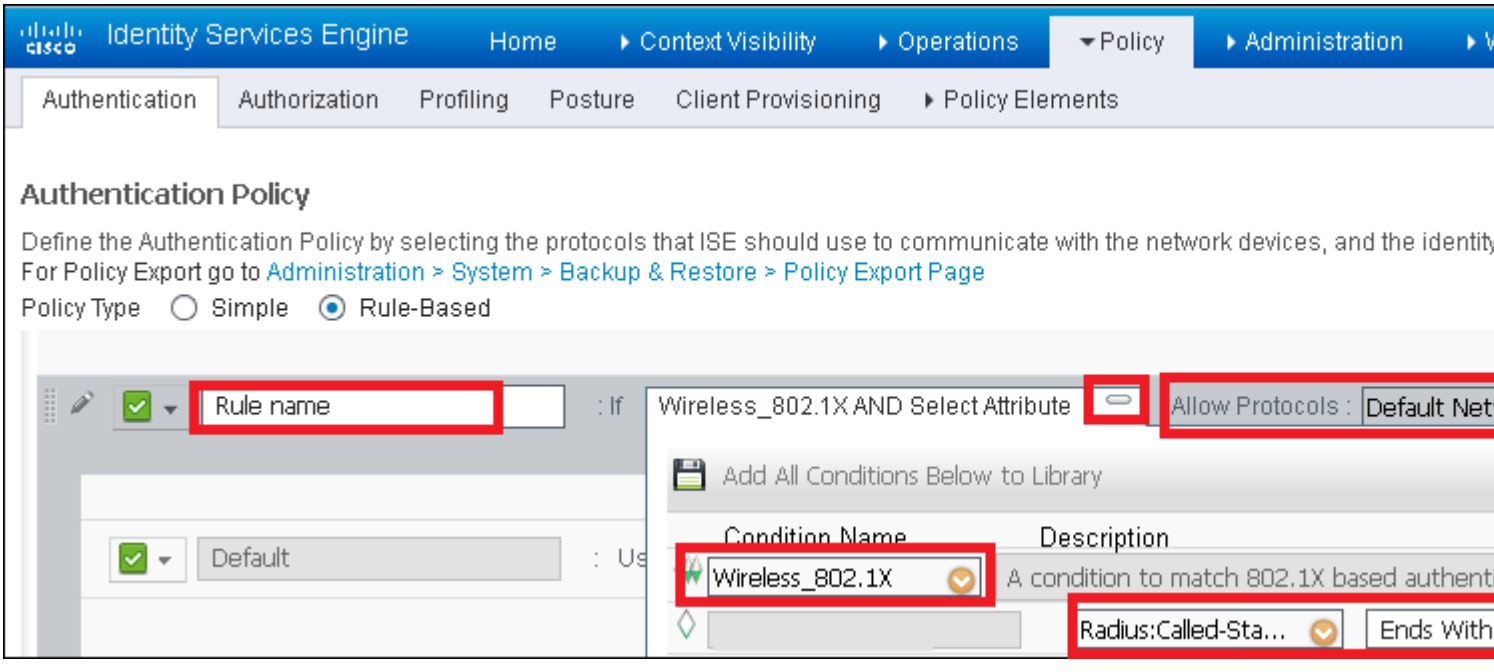


Stap 2. Plaats een nieuwe verificatieregel zoals in de afbeelding.

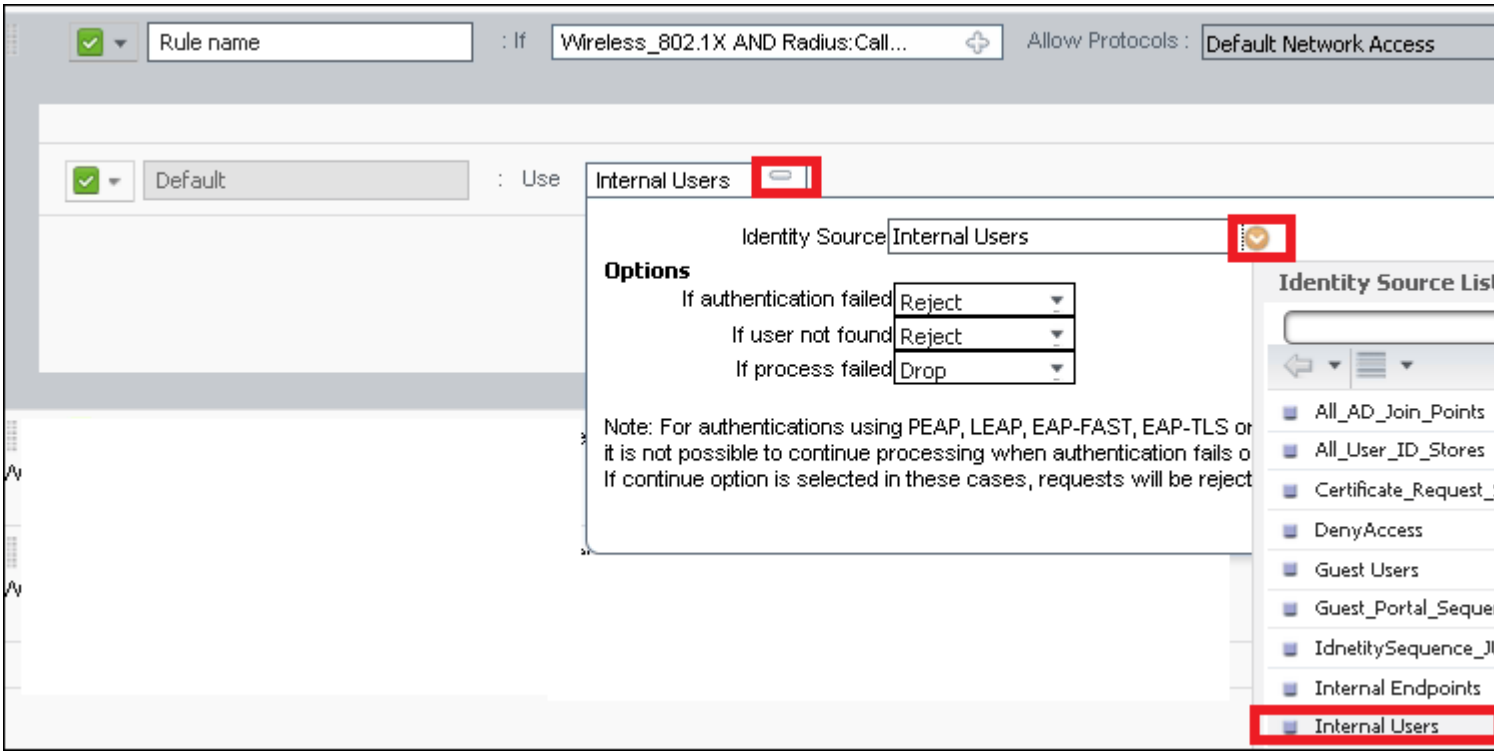


Stap 3. Voer de waarden in.

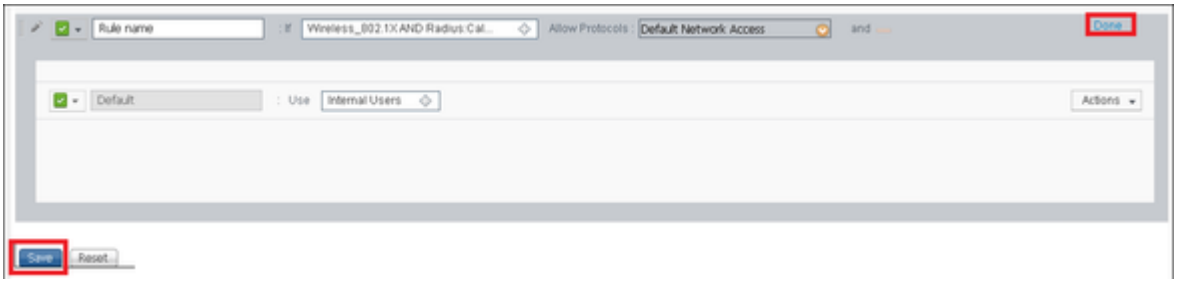
Deze verificatieregel staat alle protocollen toe die worden vermeld in de lijst Standaard netwerktoegang. Dit is van toepassing op het verificatieverzoek voor draadloze 802.1x-clients, en met Call-Station-ID, en eindigt met een stijgende lijn zoals in de afbeelding.



Kies ook de identiteitsbron voor de clients die aan deze verificatieregel voldoen. In dit voorbeeld wordt de bronlijst van interne gebruikers gebruikt zoals in de afbeelding wordt getoond.



Als u klaar bent, klikt u op **Gereed** en **Opslaan** zoals in de afbeelding.



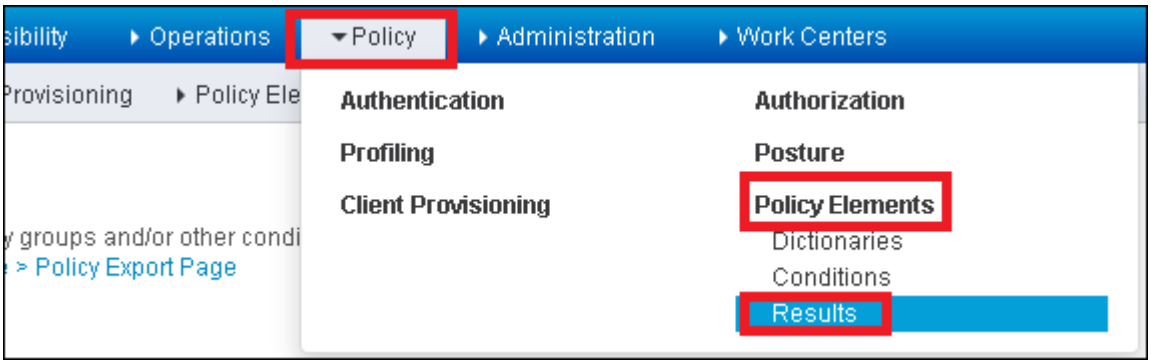
Zie voor meer informatie over Identiteitsbronnen deze link:

Een gebruikersgroep maken

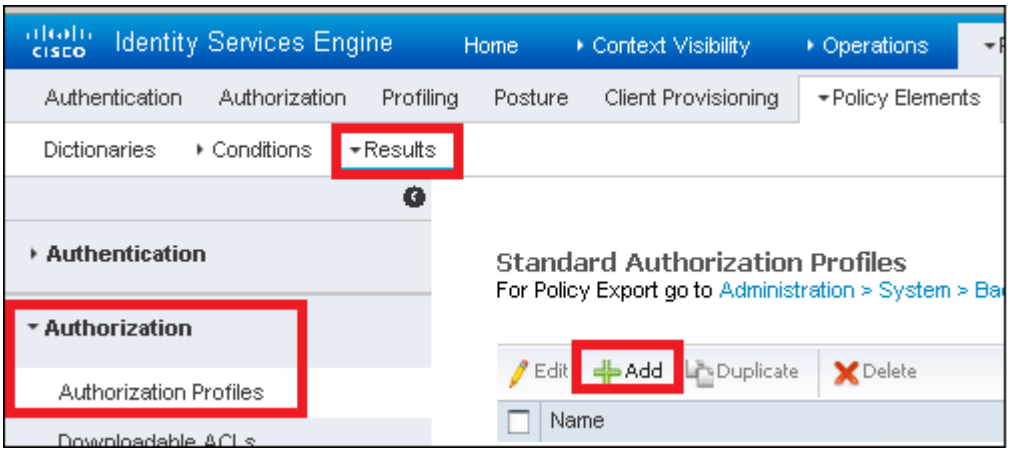
Autorisatieprofiel maken

Het autorisatieprofiel bepaalt of u al dan niet toegang hebt tot het netwerk. Druk op ACLâ€™s (Access Control Lists), VLAN-overschrijving of een andere parameter. Het in dit voorbeeld getoonde autorisatieprofiel stuurt een toegangsgoedkeuring naar u en wijst VLAN 2404 toe.

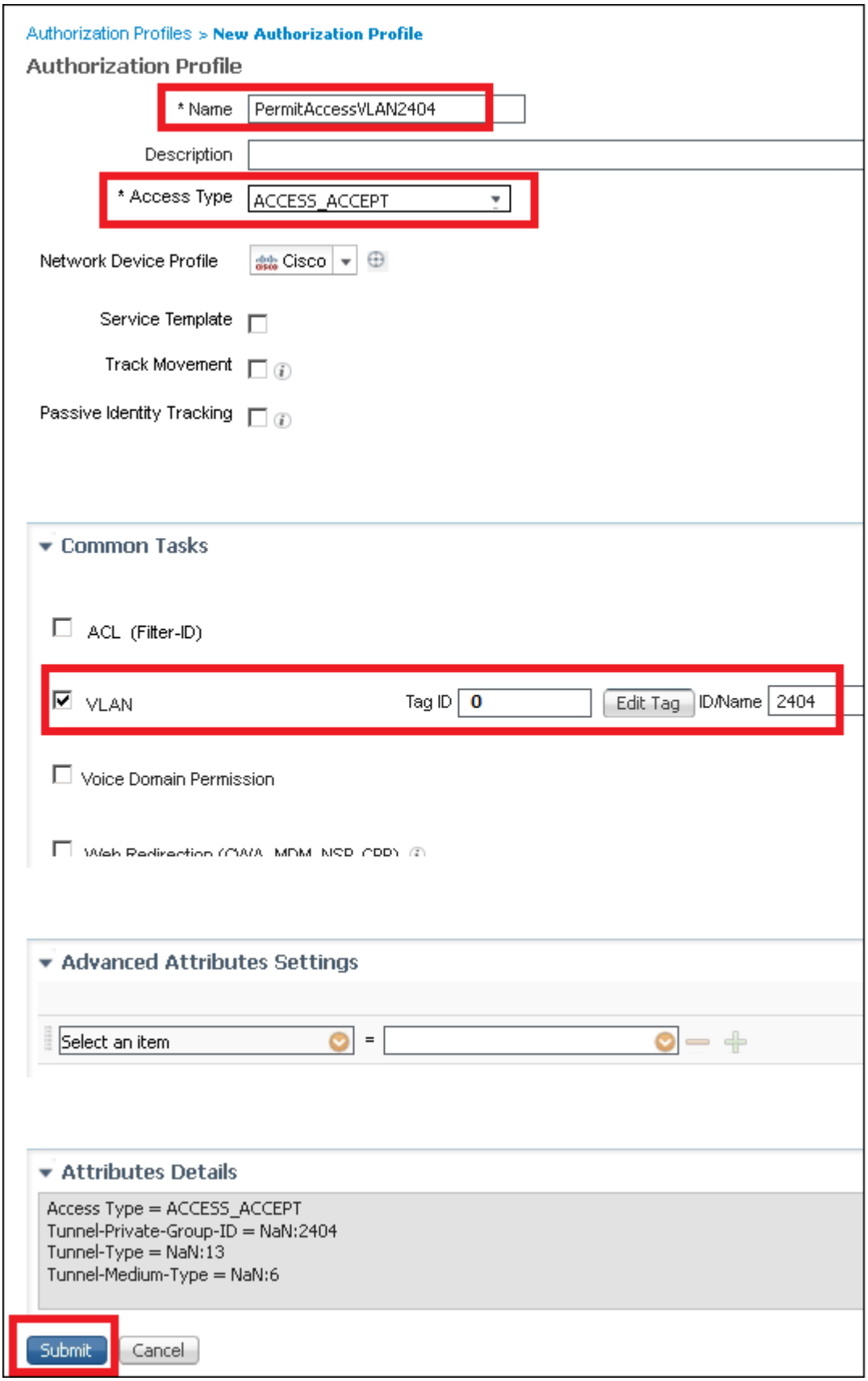
Stap 1. Navigeer naar **Beleid > Beleidselementen > Resultaten** zoals in de afbeelding.



Stap 2. Voeg een nieuw autorisatieprofiel toe. Navigeer naar **autorisatie > autorisatieprofielen > Toevoegen** zoals in de afbeelding.



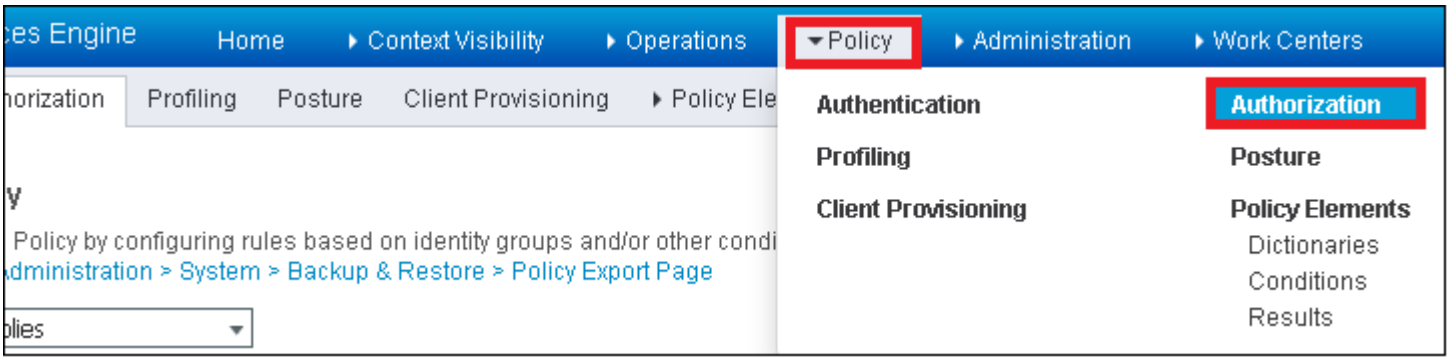
Stap 3. Voer de waarden in zoals in de afbeelding.



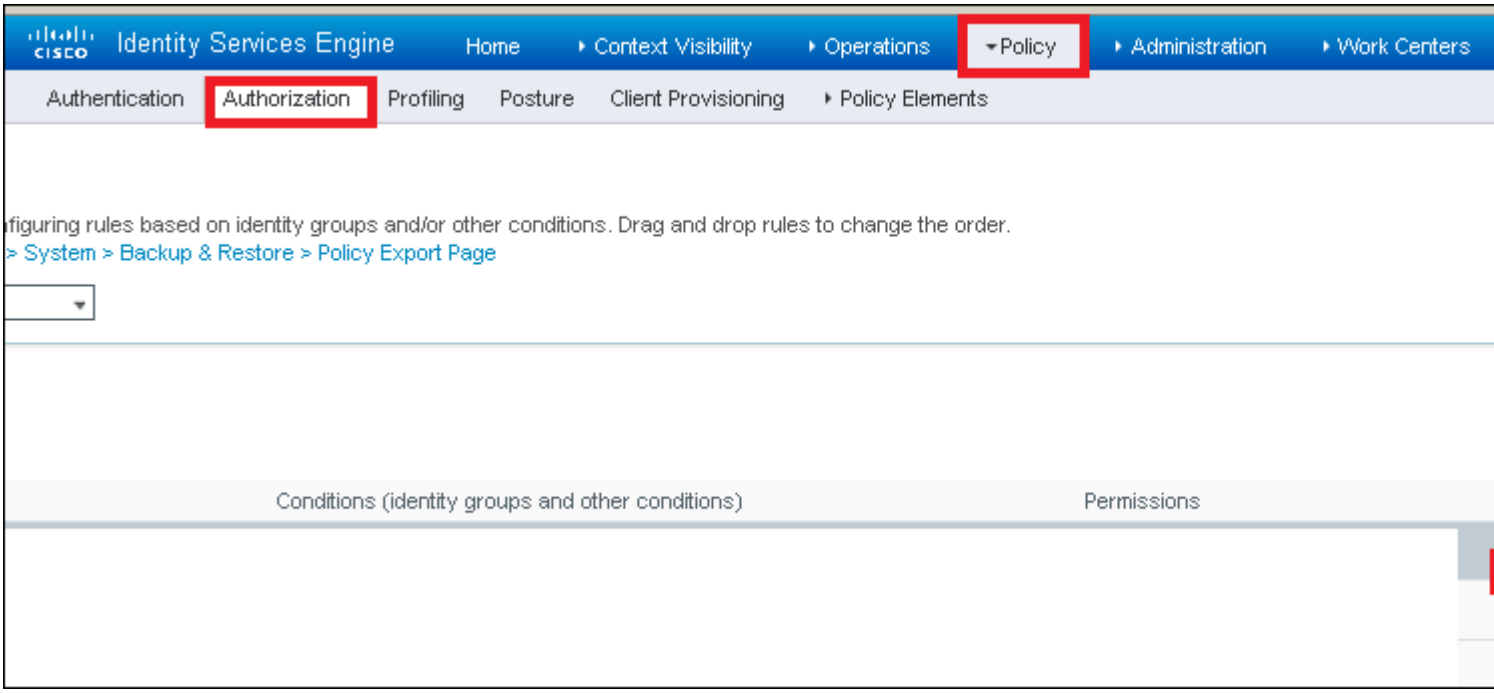
Autorisatieregel aanmaken

De autorisatieregel is degene die bepaalt welke permissies (welk autorisatieprofiel) op u worden toegepast.

Stap 1. Navigeer naar **Beleid > Autorisatie** zoals in de afbeelding.

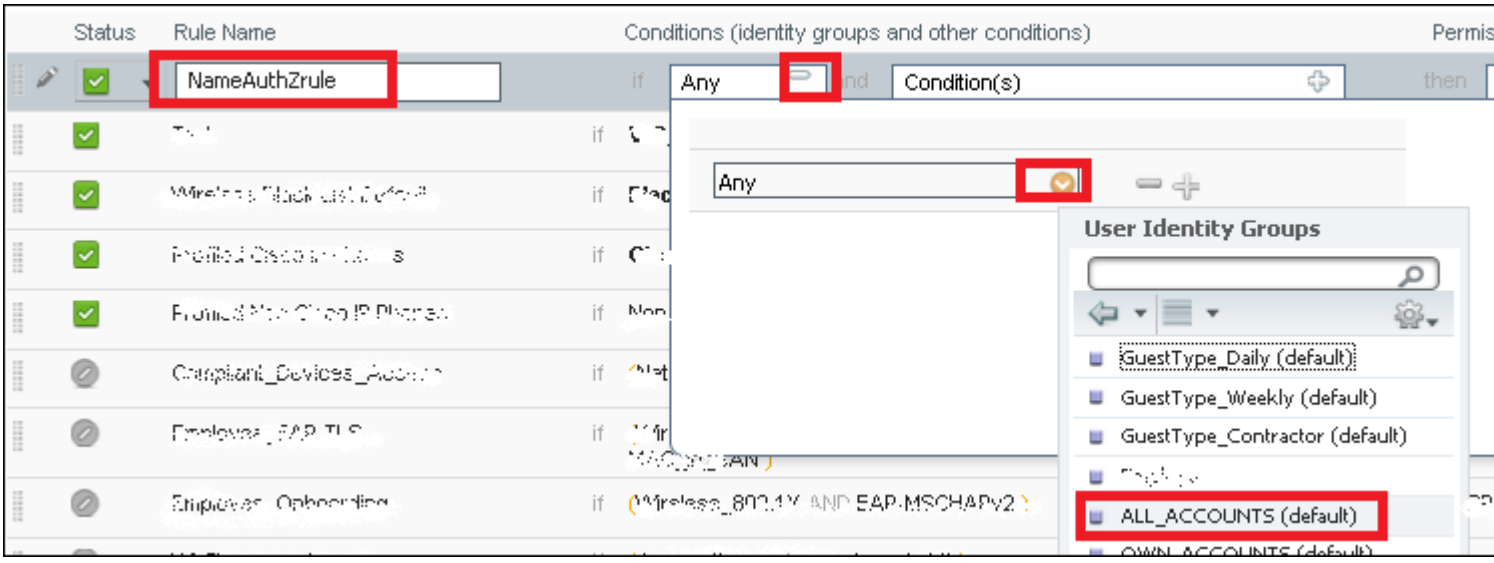


Stap 2. Plaats een nieuwe regel zoals in de afbeelding.

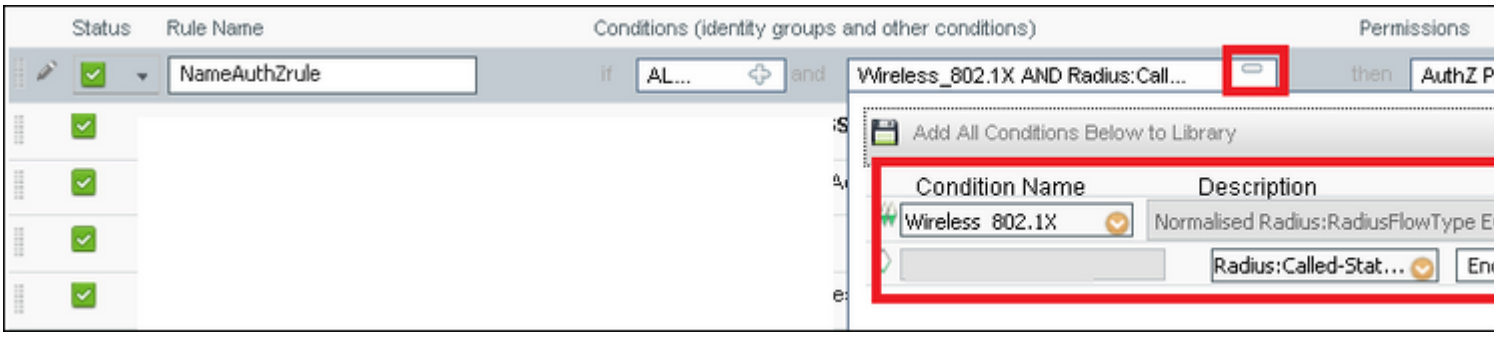


Stap 3. Voer de waarden in.

Selecteer eerst een naam voor de regel en de identiteitsgroep waarin de gebruiker is opgeslagen (ALL_ACCOUNT), zoals in de afbeelding.



Selecteer vervolgens andere voorwaarden waardoor het autorisatieproces onder deze regel valt. In dit voorbeeld, het vergunningsproces raakt deze regel als het draadloze 802.1x en zijn geroepen station ID eindigt met ise-side zoals getoond in het beeld gebruikt.



Selecteer tot slot het autorisatieprofiel dat aan u is toegewezen en dat deze regel raakt. Klik op **Gereed** en **Opslaan** zoals in de afbeelding.

Configuratie van eindapparaat

Configureer een laptop Windows 10-machine om verbinding te maken met een SSID met 802.1x-verificatie en PEAP/MS-CHAPv2 (Microsoft-versie van het Challenge-Handshake-verificatieprotocol) versie 2.

In dit configuratievoorbeeld gebruikt ISE zijn zelfondertekende certificaat om de verificatie uit te voeren.

Om het WLAN-profiel op de Windows-machine te maken, zijn er twee opties:

1. Installeer het zelfondertekende certificaat op de machine om te valideren en vertrouw op de ISE-server om de verificatie te voltooien.
2. Omzeilt de validatie van de RADIUS-server en vertrouw op elke RADIUS-server die wordt gebruikt om de verificatie uit te voeren (niet aanbevolen, omdat dit een beveiligingsprobleem kan worden).

De configuratie van deze opties wordt toegelicht in de instructies voor de configuratie van het eindapparaat -

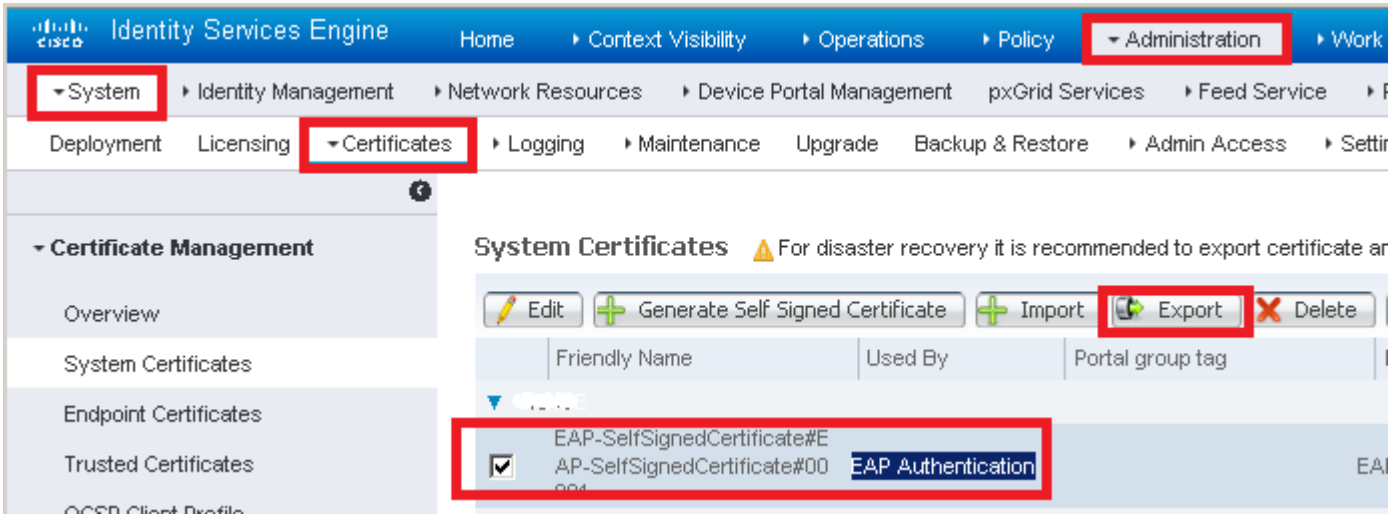
Het WLAN-profiel maken - Stap 7.

Configuratie van eindapparaat - Installeer ISE-zelfondertekend certificaat

Stap 1. Zelfondertekend certificaat voor uitvoer.

Log in op ISE en navigeer naar **Beheer > Systeem > Certificaten > Systeemcertificaten**.

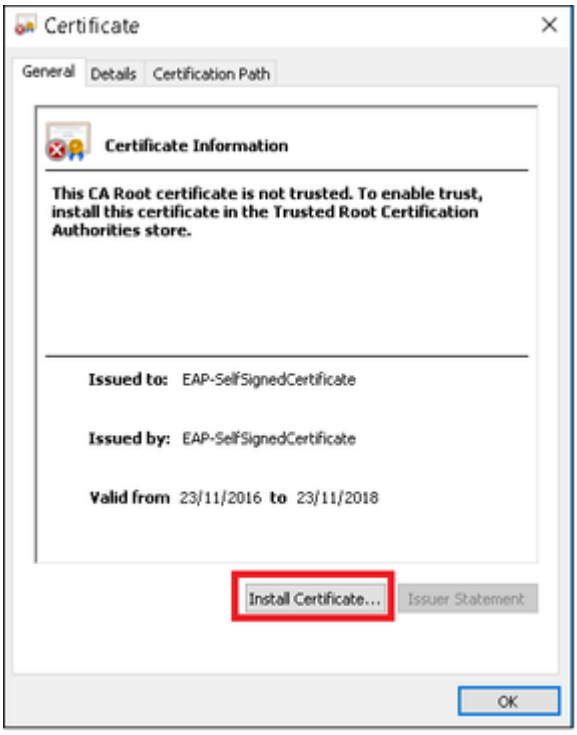
Kies vervolgens het certificaat dat wordt gebruikt voor **EAP-verificatie** en klik op **Exporteren** zoals in de afbeelding.



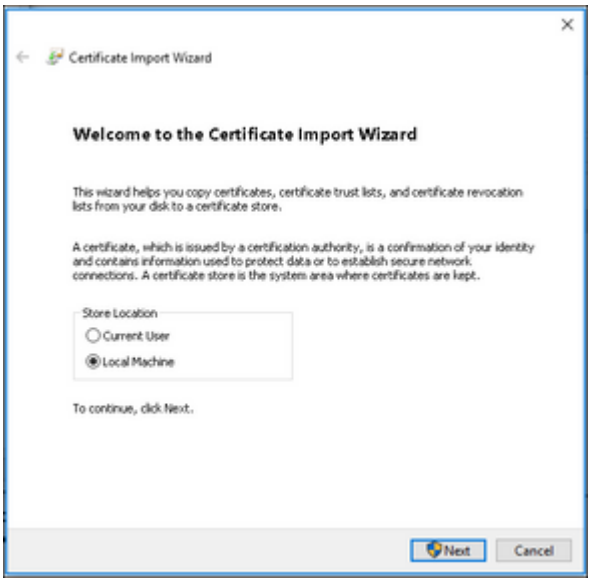
Sla het certificaat op de gewenste locatie op. Dat certificaat moet op de Windows-machine worden geïnstalleerd zoals in het beeld wordt weergegeven.

Stap 2. Installeer het certificaat in de Windows-machine.

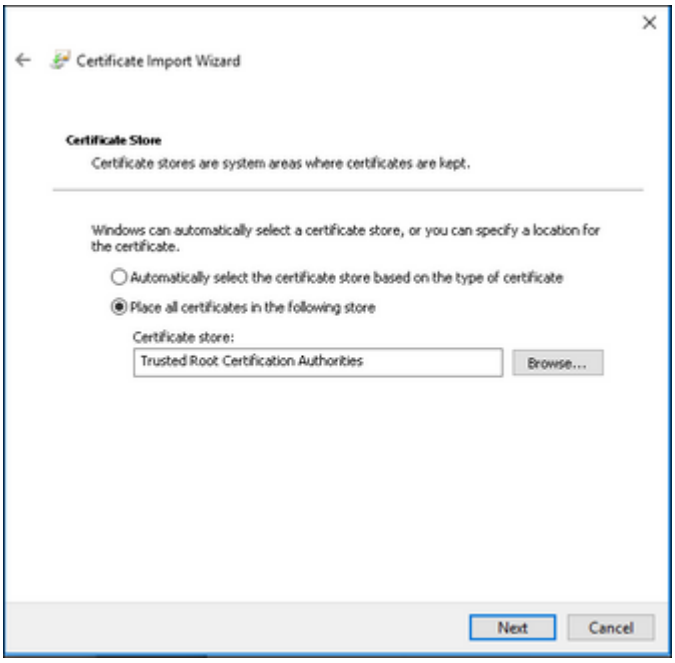
Kopieer het certificaat dat uit ISE naar de Windows-machine is geëxporteerd, wijzig de extensie van het bestand van .pem naar .crt en dubbelklik daarna om het te installeren zoals in de afbeelding.



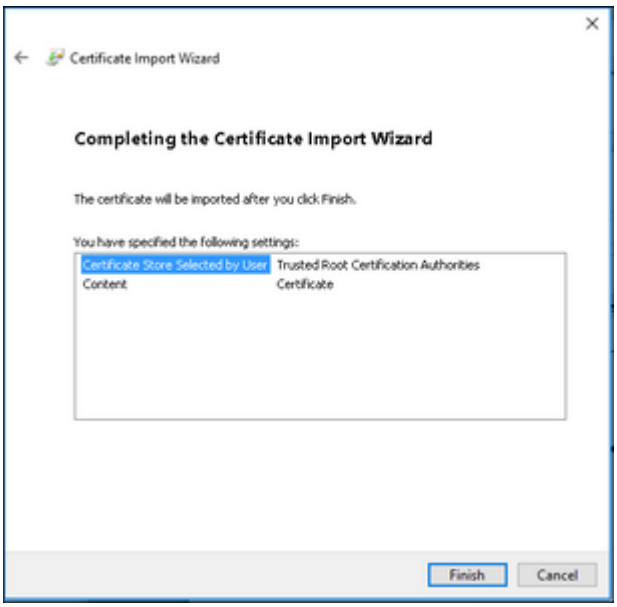
Stap 3. Selecteer de optie in **Lokale machine** installeren en klik op **Volgende** zoals in de afbeelding.



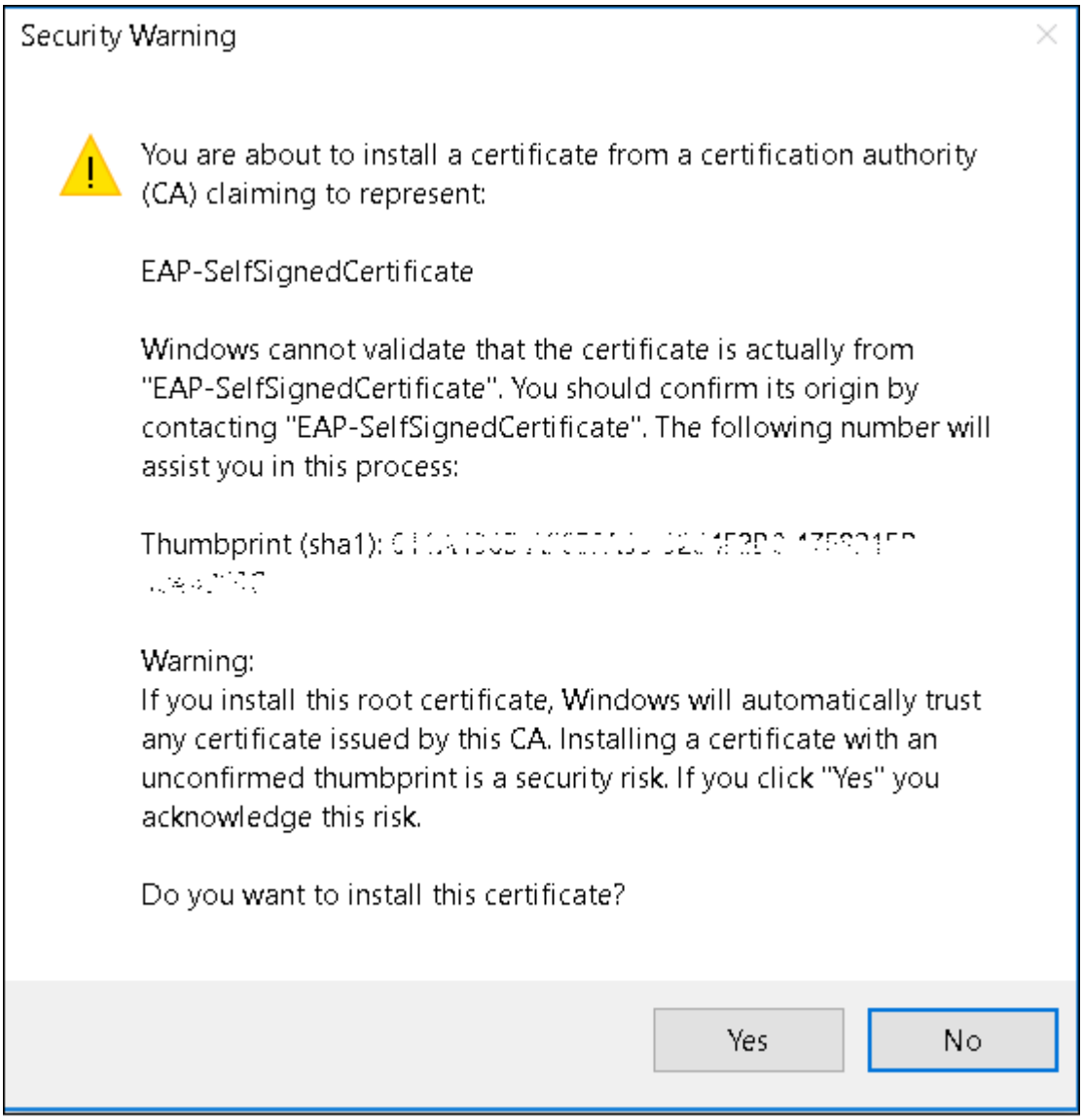
Stap 4. Selecteer **Alle certificaten in deze winkel plaatsen**, blader en selecteer vervolgens **Trusted Root Certification Authorities.** Klik vervolgens op **Volgende** zoals in de afbeelding.



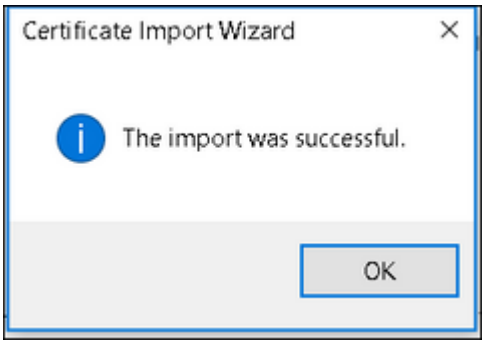
Stap 5. Klik vervolgens op **Voltooien** zoals in de afbeelding.



Stap 6. Bevestig de installatie van het certificaat. Klik op **Ja** zoals in de afbeelding.

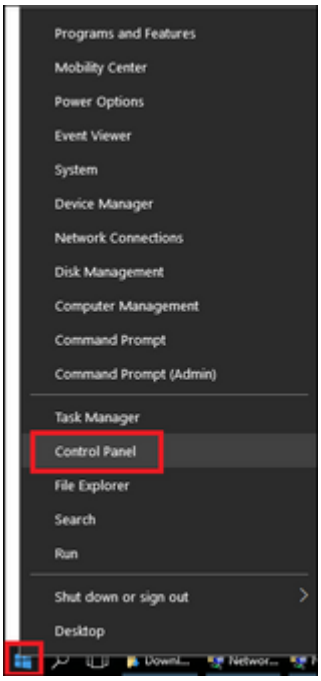


Stap 7. Klik tot slot op **OK** zoals in de afbeelding.

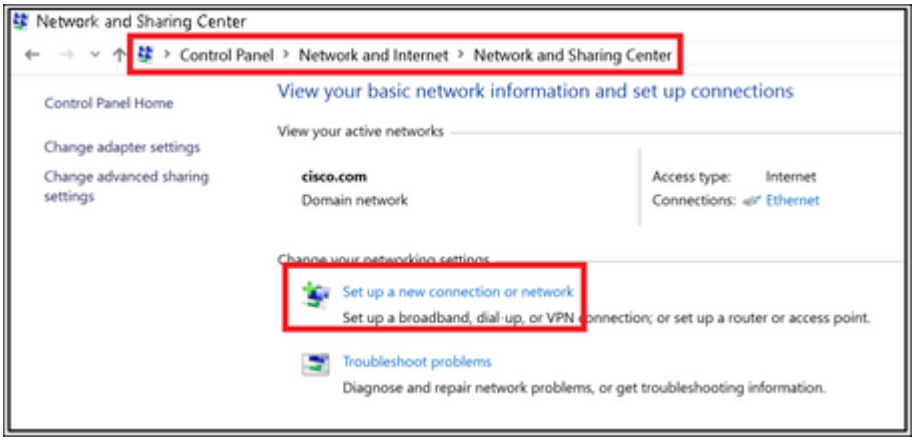


Configuratie van eindapparaat - Het WLAN-profiel maken

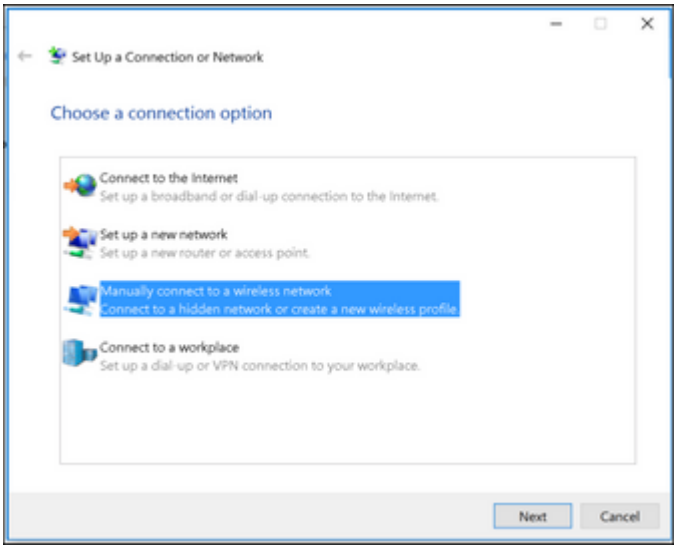
Stap 1. Klik met de rechtermuisknop op het pictogram **Start** en selecteer **Configuratiescherm** zoals in de afbeelding.



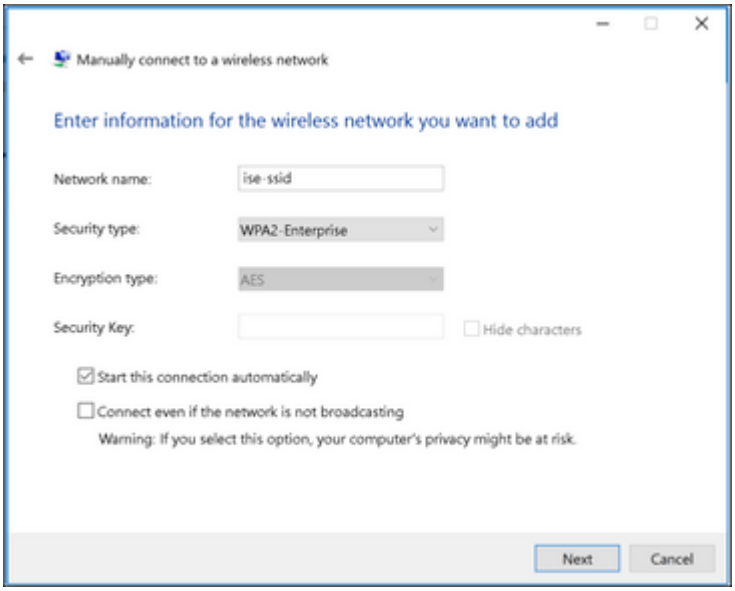
Stap 2. Navigeer naar **Netwerk en Internet**, navigeer vervolgens naar **Netwerkcentrum** en klik op **Een nieuwe verbinding of netwerk instellen** zoals in de afbeelding.



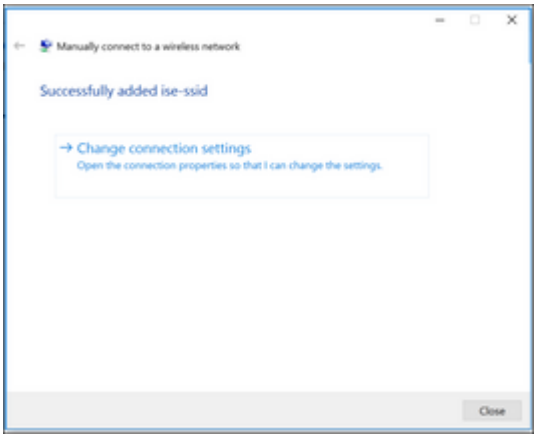
Stap 3. Selecteer **Handmatig verbinding maken met een draadloos netwerk** en klik op **Volgende** zoals in de afbeelding.



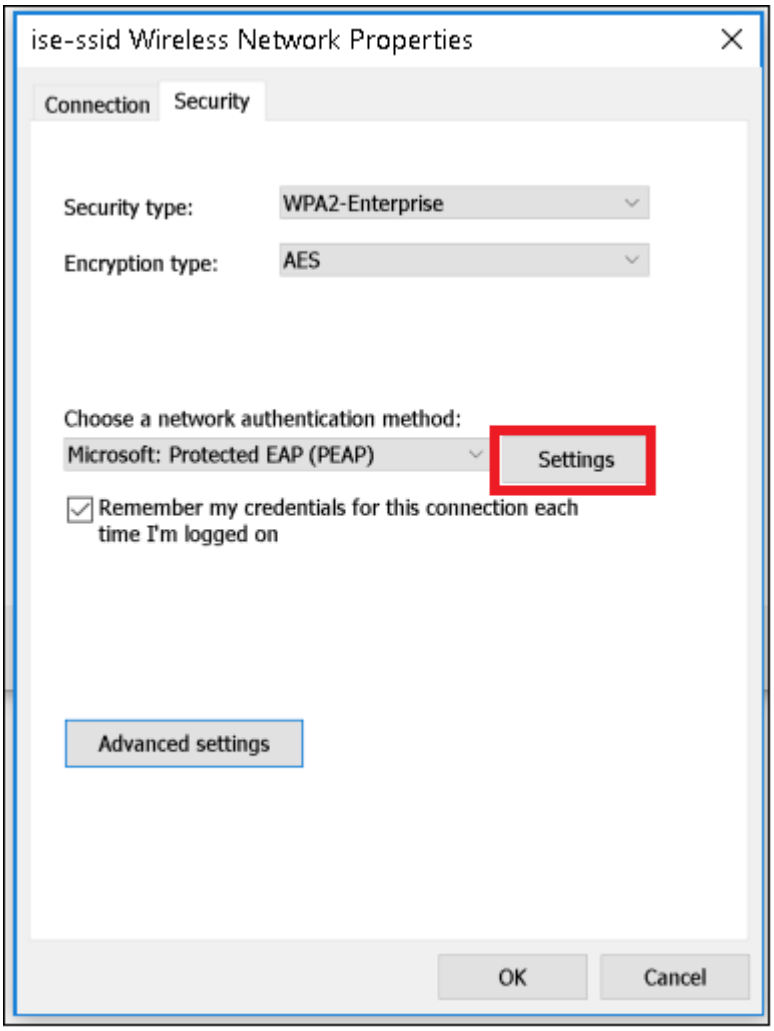
Stap 4. Voer de informatie in met de naam van de SSID en het beveiligingstype WPA2-Enterprise en klik op **Volgende** zoals in de afbeelding.



Stap 5. Selecteer **Verbindingsinstellingen wijzigen** om de configuratie van het WLAN-profiel aan te passen zoals in de afbeelding.



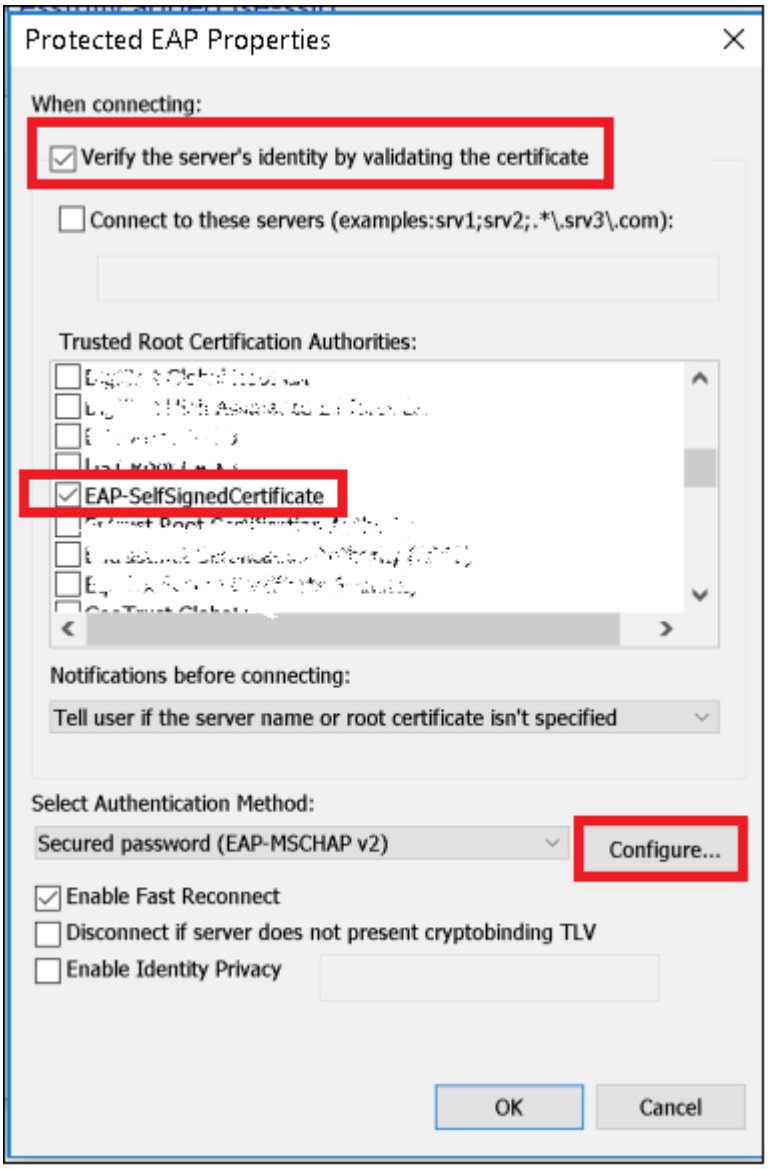
Stap 6. Navigeer naar het tabblad **Beveiliging** en klik op **Instellingen** zoals in de afbeelding.

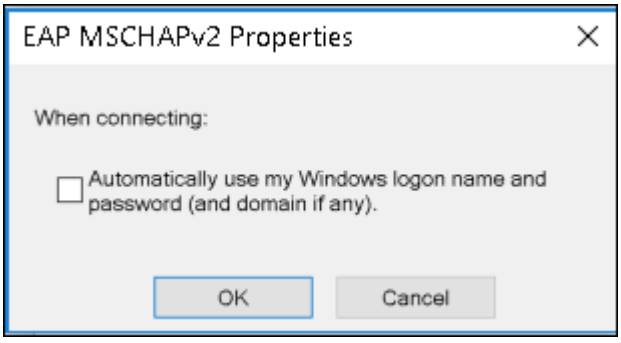


Stap 7. Selecteer deze optie als RADIUS-server al dan niet is gevalideerd.

Indien ja, **controleer de serveridentiteit door het certificaat te valideren** en van **Trusted Root Certification Authorities:** list selecteer het zelfondertekende certificaat van ISE.

Daarna selecteert u **Configureren** en uitschakelen **Automatisch mijn Windows-aanmeldingsnaam en wachtwoord gebruiken...** en klikt u vervolgens op **OK** zoals in de afbeeldingen.

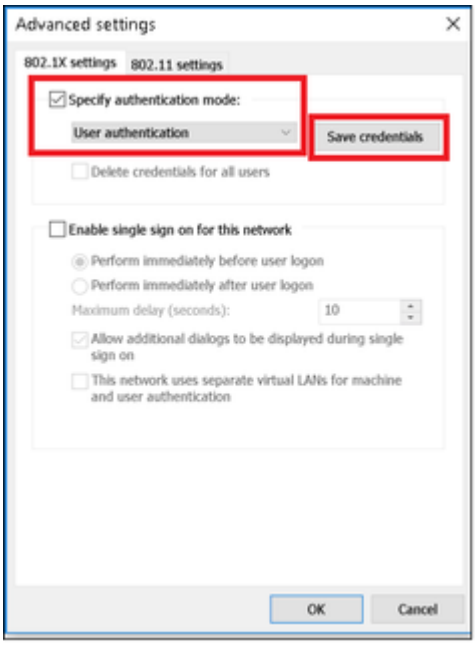


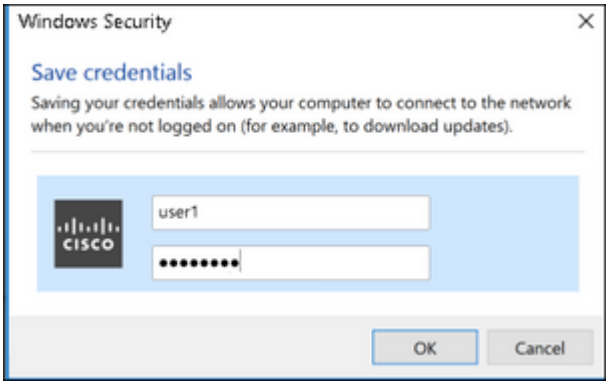


Stap 8. Configureer de gebruikersreferenties.

Terug naar het tabblad **Beveiliging** selecteert u **Geavanceerde instellingen**, specificeert u de verificatiemodus als gebruikersverificatie en **slaat u** de referenties op die op ISE zijn ingesteld om de gebruiker te verifiëren zoals in de afbeeldingen.


ise-ssid Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel


Advanced settings
802.1X settings
802.11 settings
Specify authentication mode:
User authentication
Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel


Windows Security
Save credentials
Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).
user1
OK
Cancel

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

De verificatiestroom kan worden geverifieerd vanuit WLC of ISE-perspectief.

Verificatieproces op WLC

Voer de volgende opdrachten uit om het verificatieproces voor een specifieke gebruiker te bewaken:

```
> debug client <mac-add-client>
> debug dot1x event enable
> debug dot1x aaa enable
```

Voorbeeld van een succesvolle verificatie (een of andere uitvoer is weggelaten):

<#root>

```
*apfMsConnTask_1: Nov 24 04:30:44.317:

e4:b3:18:7c:30:58 Processing assoc-req station:e4:b3:18:7c:30:58 AP:00:c8:8b:26:2c:d0-00

 thread:1a5cc288
*apfMsConnTask_1: Nov 24 04:30:44.317: e4:b3:18:7c:30:58 Reassociation received from mobile on BSSID 00:
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mobile
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying site-specific Local Bridging override
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Local Bridging Interface Policy for st
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 RSN Capabilities:  60
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Marking Mobile as non-

e4:b3:18:7c:30:58 Received 802.11i 802.1X key management suite, enabling dot1x Authentication

11w Capable
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Received RSN IE with 1 PMKIDs from mobile e4:b3
*apfMsConnTask_1: Nov 24 04:30:44.319: Received PMKID:  (16)
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Searching for PMKID in MSCB PMKID cache for mob
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 No valid PMKID found in the MSCB PMKID cache fo
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 START (0) Initializing policy
*apfMsConnTask_1: Nov 24 04:30:44.319:

e4:b3:18:7c:30:58 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state START (0)

*apfMsConnTask_1: Nov 24 04:30:44.319:

e4:b3:18:7c:30:58 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)

*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP rul
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfMsAssoStateInc
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2 (apf_policy.c:437) Changing stat
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2:session timeout forstation e4:b3
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Stopping deletion of Mobile Station: (callerId:
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Func: apfPemAddUser2, Ms Timeout = 0, Session T
*apfMsConnTask_1: Nov 24 04:30:44.320: e4:b3:18:7c:30:58 Sending Assoc Response to station on BSSID 00:c
*spamApTask2: Nov 24 04:30:44.323: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP 0
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58 Received ADD_MOBILE ack - Initiating 1x to STA e4:b
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58

Sent dot1x auth initiate message for mobile e4:b3:18:7c:30:58

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 reauth_sm state transition 0 ---> 1 for mobi
```

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 EAP-PARAM Debug - eap-params for Wlan-Id :2
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x reau
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:5
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326:
```

e4:b3:18:7c:30:58 Sending EAP-Request/Identity to mobile e4:b3:18:7c:30:58 (EAP Id 1)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received Identity Response (count=1) from mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Resetting reauth count 1 to 0 for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 EAP State update from Connecting to Authenti
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Created Acct-Session-ID (58366cf4/e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.386: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=215) for
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 WARNING: updated EAP-Identifier 1 ===> 215 f
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Allocating EAP Pkt for retransmission to mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAP Response from mobile e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Resetting reauth count 0 to 0 for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=216) for
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for re
.
.
.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:
```

e4:b3:18:7c:30:58 Processing Access-Accept for mobile e4:b3:18:7c:30:58

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 acl from 255 to 255
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 Flex acl from 65535 to 65
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:
```

e4:b3:18:7c:30:58 Username entry (user1) created for mobile, length = 253

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:
```

e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name received: vlan2404

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 override for default ap group, marking intgr
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Re-applying interface policy for client
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 apfApplyWlanPolicy: Apply WLAN Policy over P
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531:
```

e4:b3:18:7c:30:58 Inserting AAA Override struct for mobile

```
        MAC: e4:b3:18:7c:30:58, source 4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying override policy from source Overrid
*Dot1x_NW_MsgTask_0: Nov 24
```

04:30:44.531: e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name receive

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying Interface(vlan2404) policy on Mobil
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Re-applying interface policy for client
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Setting re-auth timeout to 0 seconds, got fr
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x reau
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:5
```

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Creating a PKC PMKID Cache entry for station
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Resetting MSCB PMK Cache Entry 0 for station
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding BSSID 00:c8:8b:26:2c:d1 to PMKID cach
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: New PMKID: (16)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531:      [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 unsetting PmkIdValidatedByAp
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Updating AAA Overrides from local for static
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding Audit session ID payload in Mobility
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 0 PMK-update groupcast messages sent
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 PMK sent to mobility group
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Disabling re-auth since PMK lifetime can tak
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Sending EAP-Success to mobile e4:b3:18:7c:30
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Freeing AAACB from Dot1xCB as AAA auth is do
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Found an cache entry for BSSID 00:c8:8b:26:2
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: Including PMKID in M1  (16)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: M1 - Key Data: (22)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0000] dd 14 00 0f ac 04 cc 3a 3d 26 80 17 8b f1 2d c5
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0016] cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:
```

e4:b3:18:7c:30:58 Starting key exchange to mobile e4:b3:18:7c:30:58, data packets will be dropped

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:
```

e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18:7c:30:58

```
state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for re
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Entering Backend Auth Success state (id=223)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Received Auth Success while in Authenticatin
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL-
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547:
```

e4:b3:18:7c:30:58 Received EAPOL-key in PTK_START state (message 2) from mobile

```
 e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Successfully computed PTK from PMK!!!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Received valid MIC in EAPOL Key Message M2!!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Not Flex client. Do not distribute PMK Key c
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for re
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL-
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:
```

e4:b3:18:7c:30:58 Received EAPOL-key in PTKINITNEGOTIATING state (message 4)

```
 from mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Freeing EAP Retransmit Bufer for mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMs1xStateInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqSuccessCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:
```

e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Mobility query, PEM State: L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58   Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Vlan Ip: 172.16.0.134, Vlan mask
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Virtual Ip: 10.10.10.10
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58   Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Not Using WMM Compliance code qosCap 00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LW
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556:
```

e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6677,
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
  type = Airespace AP - Learn IP address
  on AP 00:c8:8b:26:2c:d0, slot 0, interface = 1, QOS = 0
  IPv4 ACL ID = 255, IPv
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed m
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successfully Plumbed PTK session Keysfor mob
*spamApTask2: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP 0
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update reque
  Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.3
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) State Update from Mobility
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6315, Add
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
  IPv4 ACL ID = 255,
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobil
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 Sent an XID frame
*dtlArpTask: Nov 24 04:30:47.932: e4:b3:18:7c:30:58 Static IP client associated to interface vlan2404 wh
*dtlArpTask: Nov 24 04:30:47.933: e4:b3:18:7c:30:58 apfMsRunStateInc
*dtlArpTask: Nov 24 04:30:47.933:
```

e4:b3:18:7c:30:58 172.16.0.151 DHCP_REQD (7) Change state to RUN (20)

```
 last state DHCP_REQD (7)
```

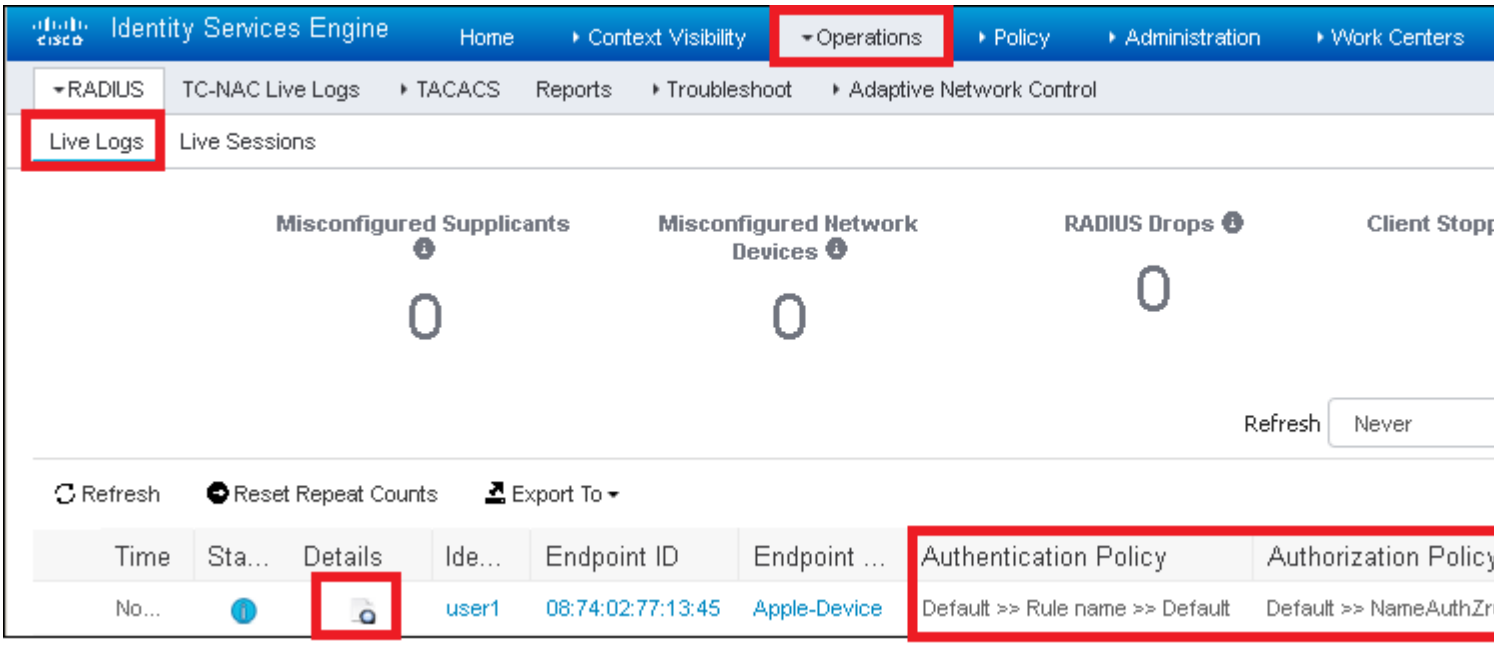
Voor een eenvoudige manier om te lezen debug client outputs, gebruik de draadloze debug analyzer tool:

Wireless Debug Analyzer

Verificatieproces op ISE

Navigeer naar **Operations > RADIUS > Live Logs** om te zien welk verificatiebeleid, autorisatiebeleid en autorisatieprofiel aan de gebruiker is toegewezen.

Klik voor meer informatie op **Details** om een meer gedetailleerd verificatieproces te zien, zoals in de afbeelding.



Problemen oplossen

Er is momenteel geen specifieke informatie beschikbaar om deze configuratie problemen op te lossen.

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.