EAP-TLS op 9800 WLC configureren met ISE-interne CA

Inhoud

Inleiding

Dit document beschrijft EAP-TLS-verificatie met behulp van de Certificate Authority of Identity

Services Engine om gebruikers te verifiëren.

Voorwaarden

Gebruikte componenten

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

- Draadloze controller: C9800-40-K9 met 17.09.04a
- Cisco ISE-lijnkaart: Patch 4 uitvoeren, versie 3
- AP-model: C9130AXI-D router
- Switch: NCS 920-L-24P

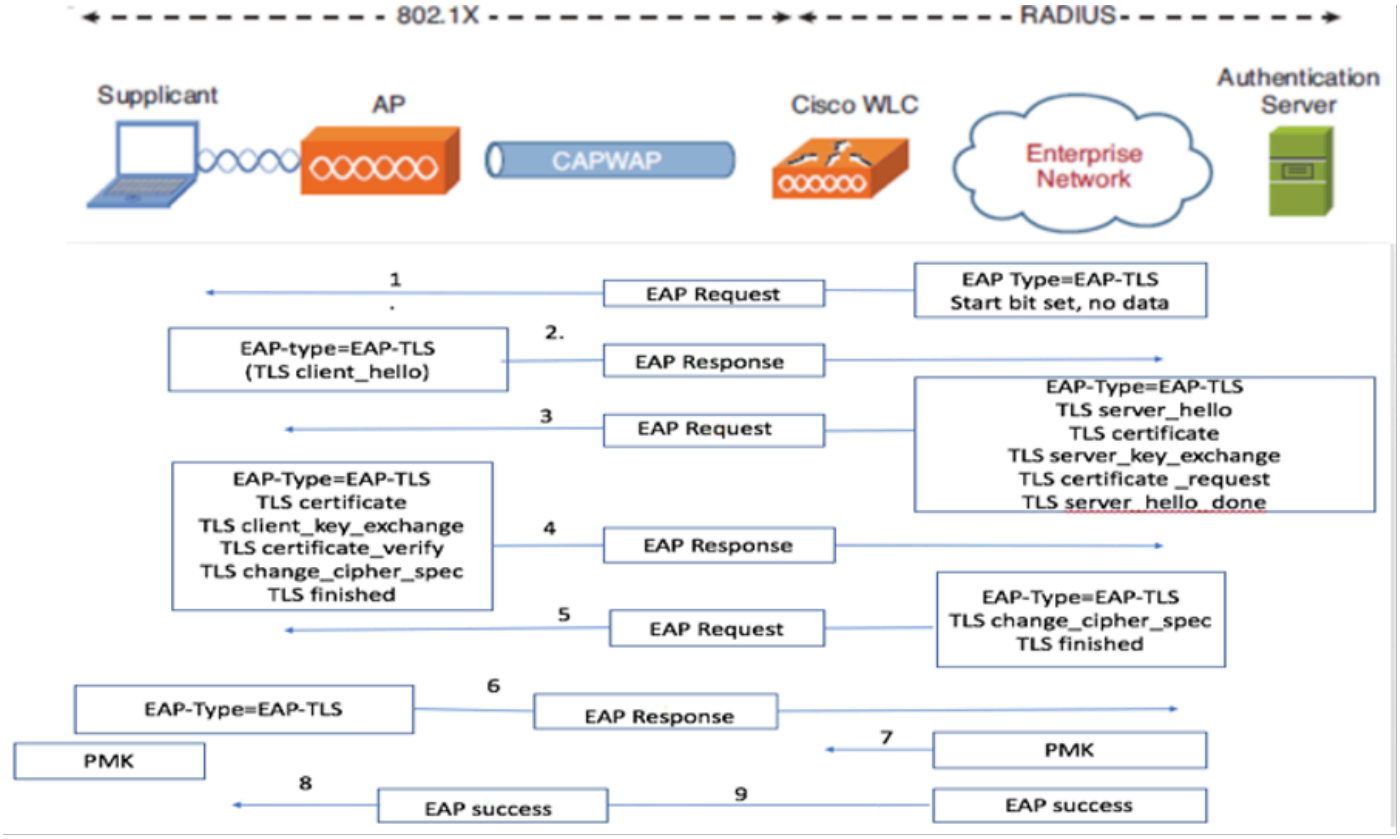
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De meeste organisaties hebben hun eigen CA die certificaten afgeeft aan eindgebruikers voor EAP-TLS-verificatie. ISE omvat een ingebouwde certificeringsinstantie die kan worden gebruikt om certificaten te genereren voor gebruikers die kunnen worden gebruikt voor EAP-TLS-verificatie. In scenario's waarin het gebruik van een volwaardige CA niet mogelijk is, wordt het gebruik van de ISE CA voor gebruikersverificatie voordelig.

Dit document beschrijft de configuratie stappen die nodig zijn om de ISE-certificeringsinstantie effectief te kunnen gebruiken om draadloze gebruikers te verifiëren. EAP-TLS-verificatiestroom

EAP-TLS-verificatiestroom



EAP-TLS-verificatiestroom

Stappen in de EAP-TLS-stroom

1. De draadloze client is gekoppeld aan het access point (AP).
2. In dit stadium staat het toegangspunt geen gegevensoverdracht toe en wordt een verificatieaanvraag verzonden.
3. De client, handelend als de aanvrager, reageert met een EAP-Response-identiteit.
4. De draadloze LAN-controller (WLC) stuurt de informatie over de gebruikers-id naar de verificatieserver.
5. De RADIUS-server reageert op de client met een EAP-TLS-startpakket.
6. Het EAP-TLS-gesprek begint vanaf dit punt.
7. De client stuurt een EAP-Response terug naar de verificatieserver, inclusief een client_hello handshake-bericht met een algoritme dat op NULL is ingesteld.
8. De verificatieserver reageert met een Access-Challenge-pakket dat het volgende bevat:

```
TLS server_hello
Handshake message
Certificate
Server_key_exchange
Certificate request
Server_hello_done
```

9. De client antwoordt met een EAP-Response-bericht met:

```
Certificate (for server validation)
Client_key_exchange
Certificate_verify (to verify server trust)
Change_cipher_spec
TLS finished
```

10. Op succesvolle clientverificatie stuurt de RADIUS-server een Access-Challenge met:

```
Change_cipher_spec
Handshake finished message
```

1. De client verifieert de hash om de RADIUS-server te verifiëren.

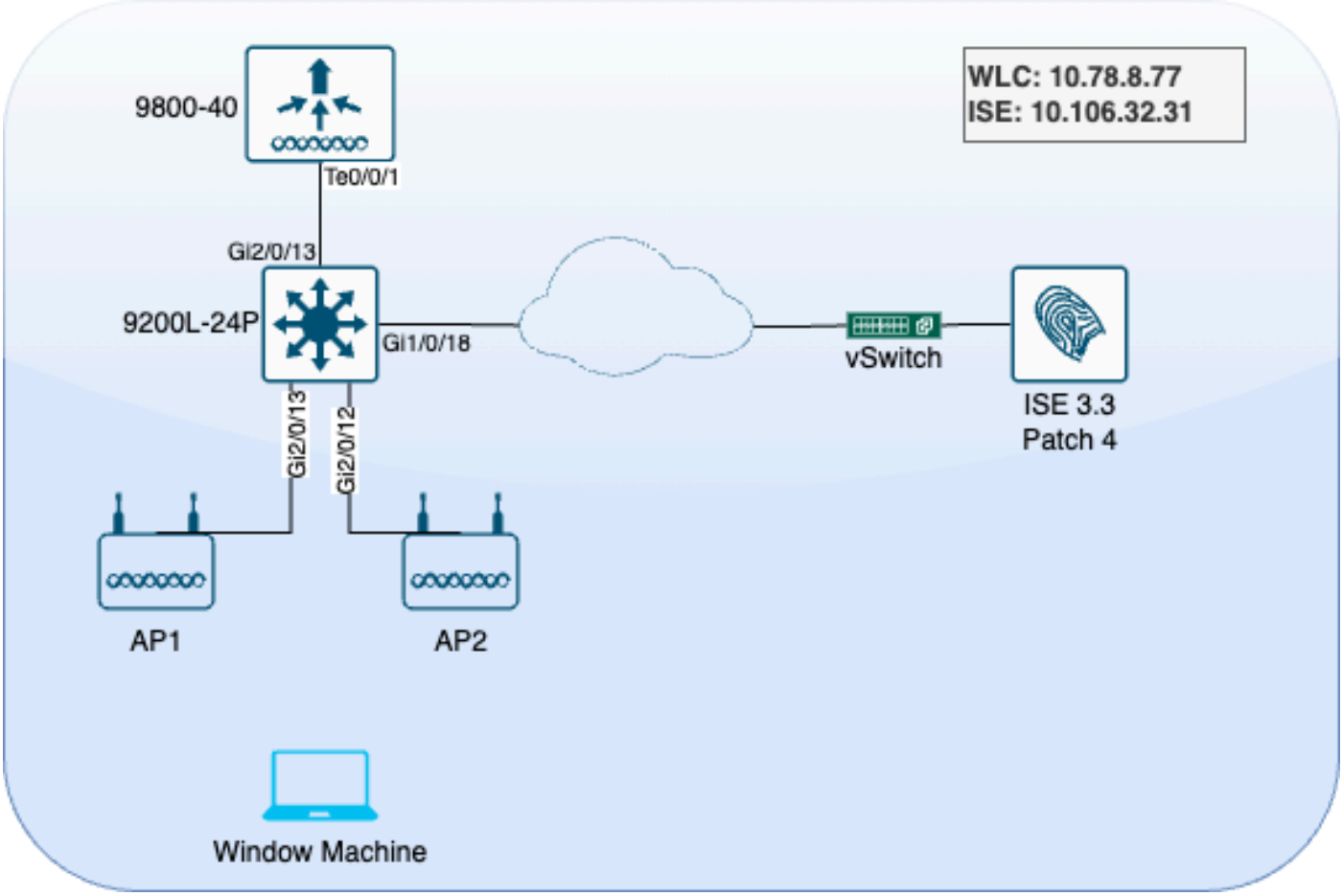
12. Een nieuwe encryptiesleutel wordt dynamisch afgeleid van het geheim tijdens de TLS handdruk.

13. Van de server wordt een EAP-Success-bericht naar de verificator en vervolgens naar de aanvrager verzonden.

14. De draadloze client met EAP-TLS-enabled kan nu toegang krijgen tot het draadloze netwerk.

Configureren

Netwerkdiagram



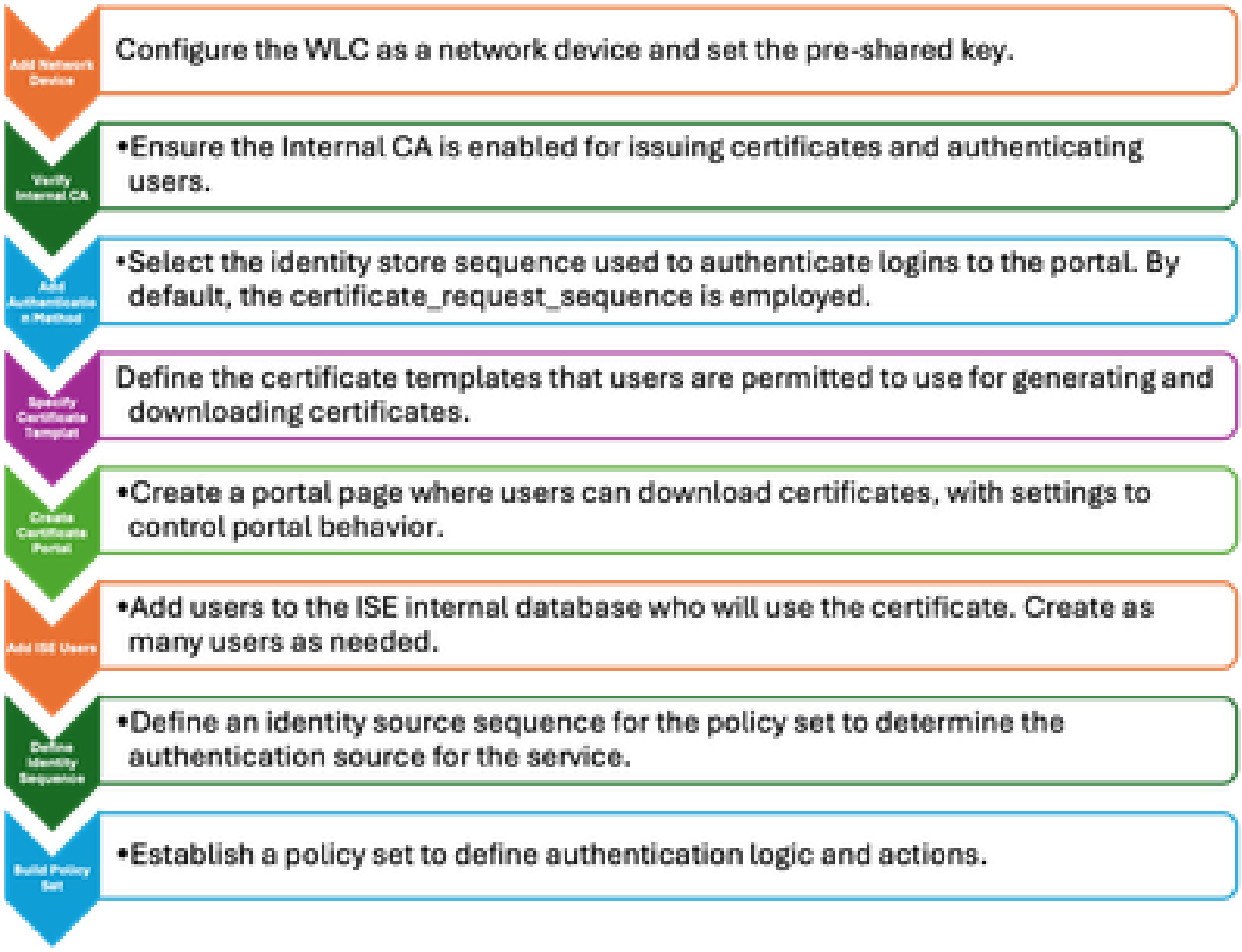
LAB-topologie

Configuraties

In dit gedeelte configureren we twee componenten: ISE en 9800 WLC.

ISE-configuratie

Hier volgen de configuratiestappen voor de ISE-server. Elke stap wordt vergezeld door screenshots in deze sectie om visuele richtlijnen te geven.

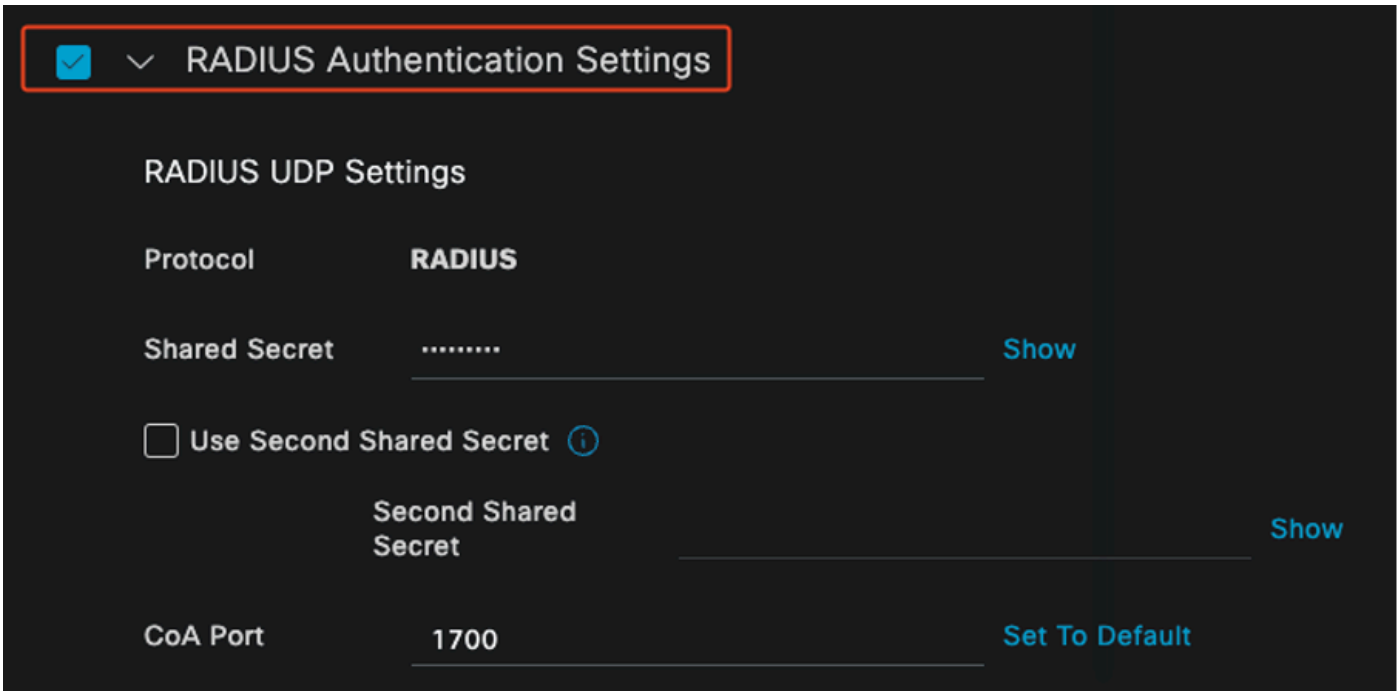


Configuratiestappen voor ISE-servers

Een netwerkapparaat toevoegen

Gebruik deze instructies om de draadloze LAN-controller (WLC) als netwerkapparaat toe te voegen:

1. Ga naar Beheer > Netwerkbronnen > Netwerkapparaten.
2. Klik op het pictogram +Add om het proces voor het toevoegen van de WLC te starten.
3. Zorg ervoor dat de pre-gedeelde sleutel zowel WLC als de server van ISE aanpast om juiste communicatie toe te laten.
4. Nadat alle details correct zijn ingevoerd, klikt u op Indienen linksonder om de configuratie op te slaan

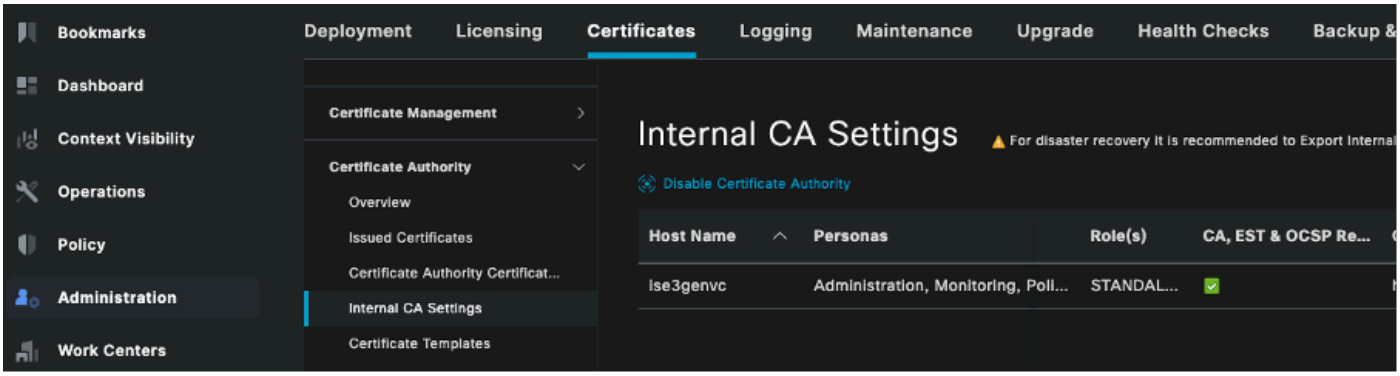


Een netwerkapparaat toevoegen

Verifiëren van interne CA

Gebruik de volgende stappen om de instellingen van de interne certificeringsinstantie (CA) te controleren:

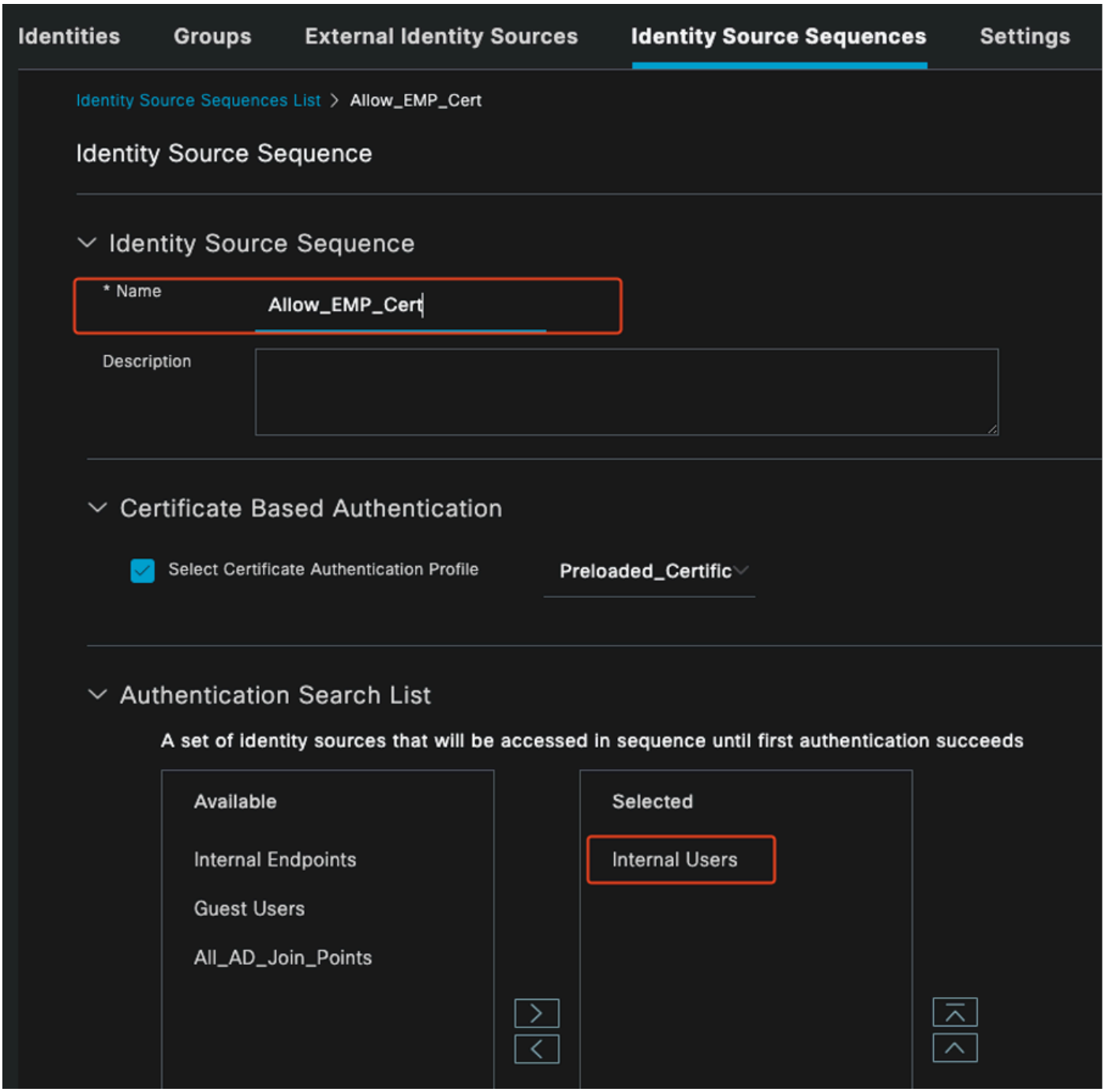
1. Ga naar Beheer > Systeem > Certificaten > Certificaatautoriteit > Interne CA-instellingen.
2. Zorg ervoor dat de kolom CA is ingeschakeld om te bevestigen dat de interne CA actief is.



Verifiëren van interne CA

Verificatiemethode toevoegen

Ga naar Beheer > Identity Management > Identity Source Sequences. Voeg een aangepaste identiteitssequentie toe om de poortinlogbron te controleren.



Verificatiemethode

Certificaatsjabloon opgeven

U kunt als volgt een certificaatsjabloon instellen:

Stap 1. Navigeer naar Beheer > Systeem > Certificaten > Certificaatautoriteit > Certificaatsjablonen.

Stap 2. Klik op het pictogram +Add om een nieuwe certificaatsjabloon te maken:

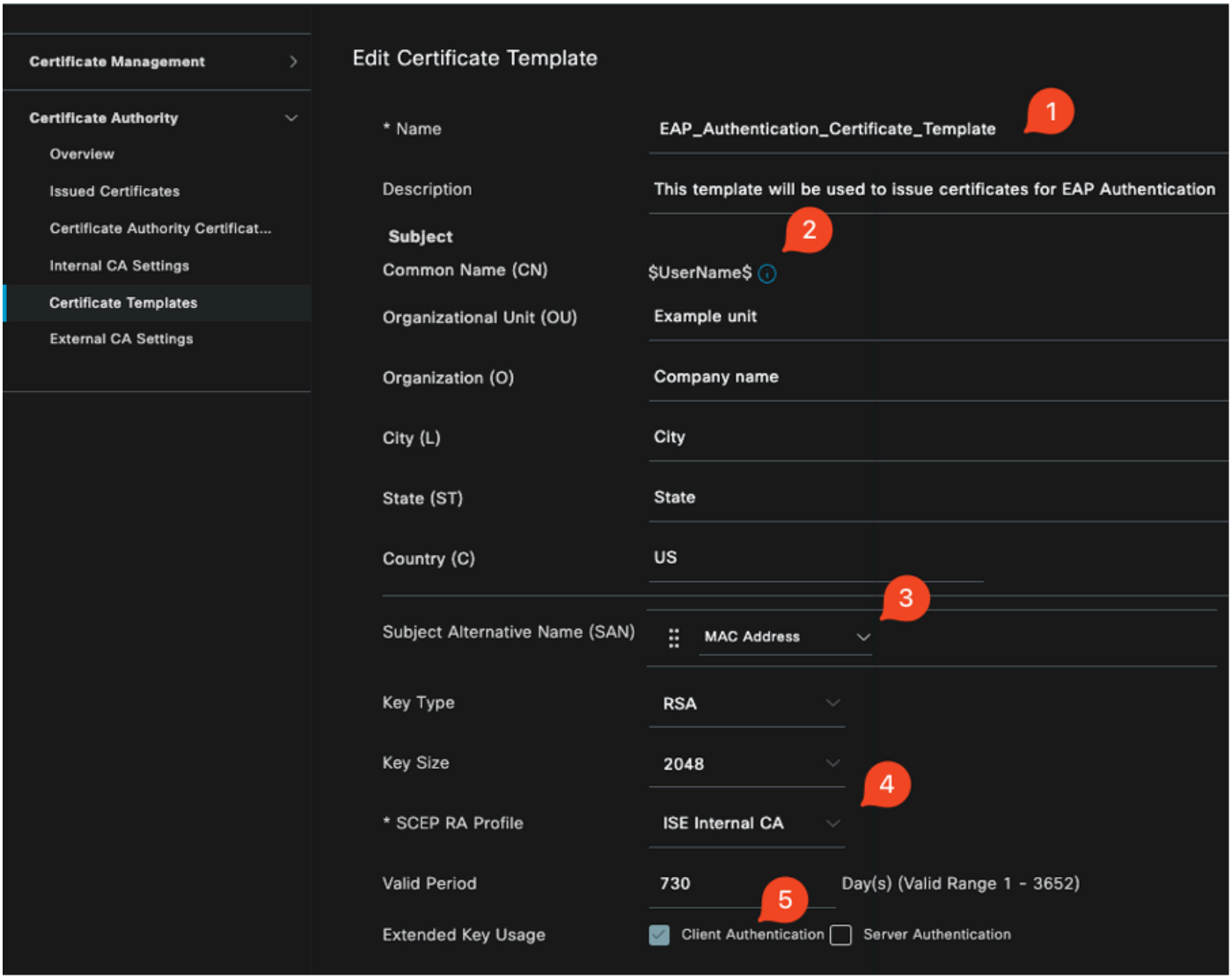
2.1 Een unieke naam opgeven die lokaal is voor de ISE-server voor de sjabloon.

2.2 Zorg ervoor dat de algemene naam (CN) is ingesteld op $UserName$.

2.3 Controleer of de alternatieve onderwerpnaam (SAN) is toegewezen aan het MAC-adres.

2.4 Stel het SCEP RA-profiel in op ISE Internal CA.

2.5 Schakel clientverificatie in in het gedeelte Extended Key Use.



Sjabloon voor certificaat

Certificaatportal maken

Gebruik de volgende stappen om een certificaatportal voor het genereren van clientcertificaten te maken:

Stap 1. Navigeer naar Beheer > Apparaatbeheer > Certificaatprovisioning.

Stap 2. Klik op Maken om een nieuwe portaalpagina in te stellen.

Stap 3. Verstrek een unieke naam voor het portaal om het gemakkelijk te identificeren.

3.1. Kies het poortnummer waarop de portaalsite actief moet zijn; Zet dit op 8443.

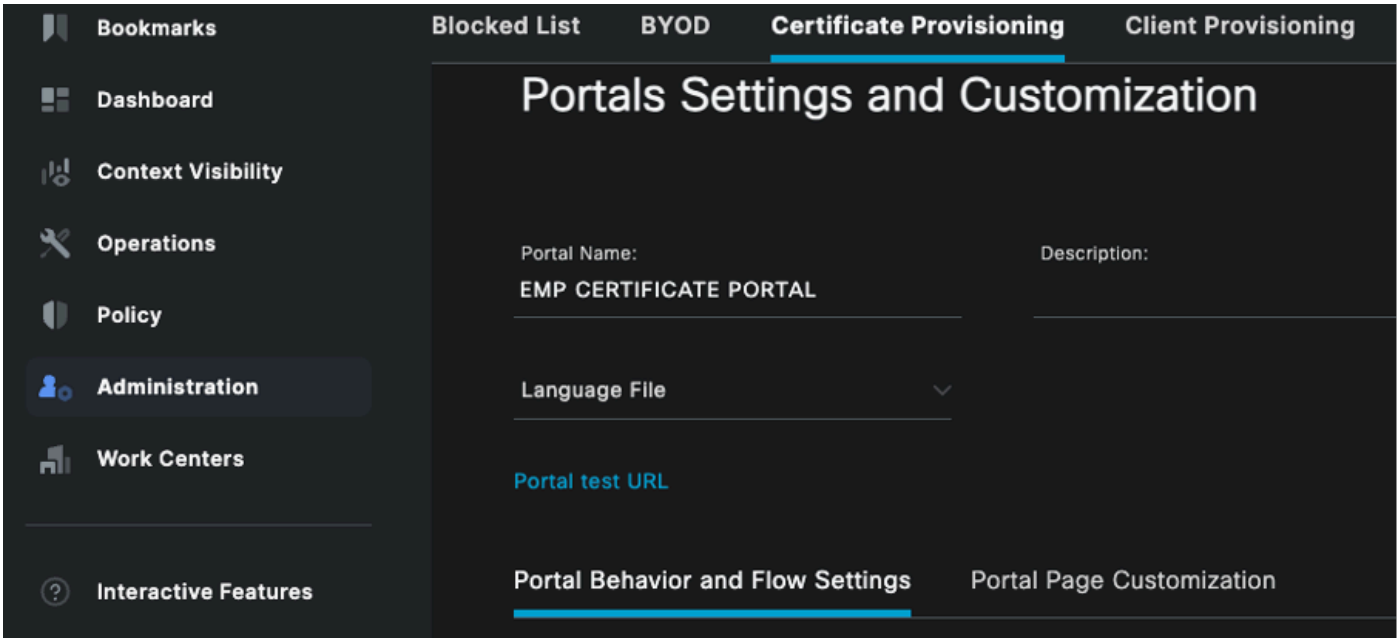
3.2. Specificeer de interfaces waarop ISE naar deze portal luistert.

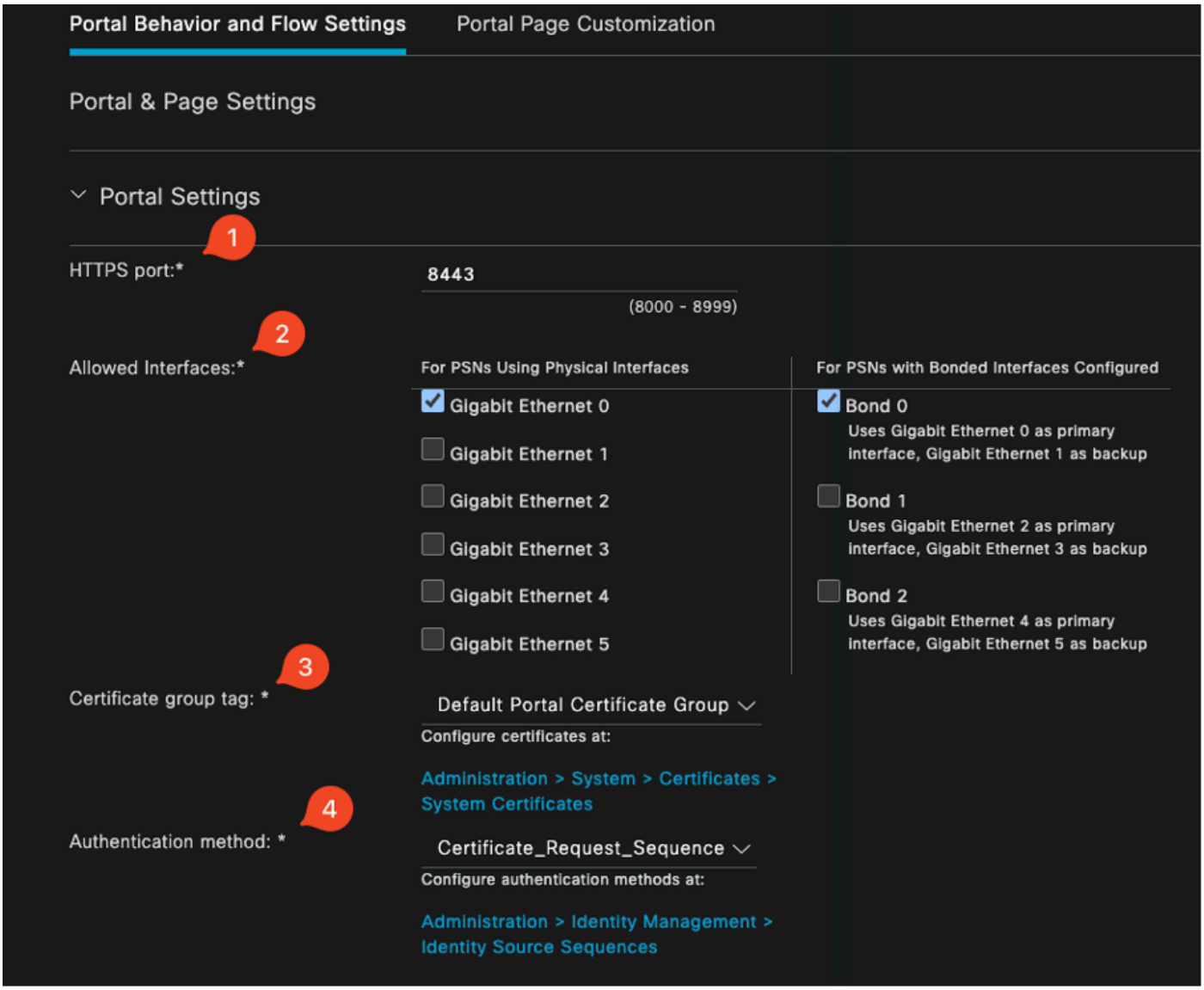
3.3. Selecteer de certificaatgroepmarkering als de standaardportalcertificaatgroep.

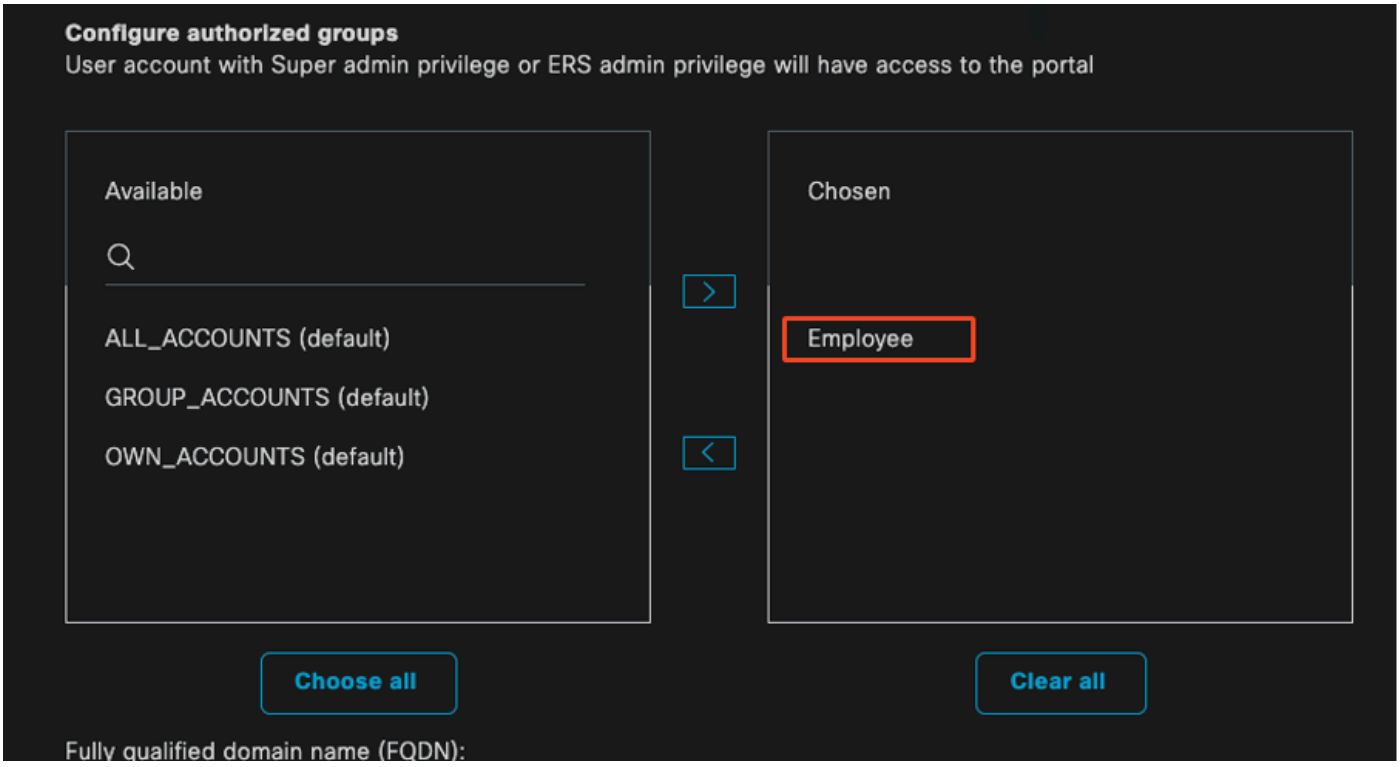
3.4. Selecteer de verificatiemethode, die de sequentie van het identiteitsarchief aangeeft die wordt gebruikt om de aanmelding bij dit portal te verifiëren.

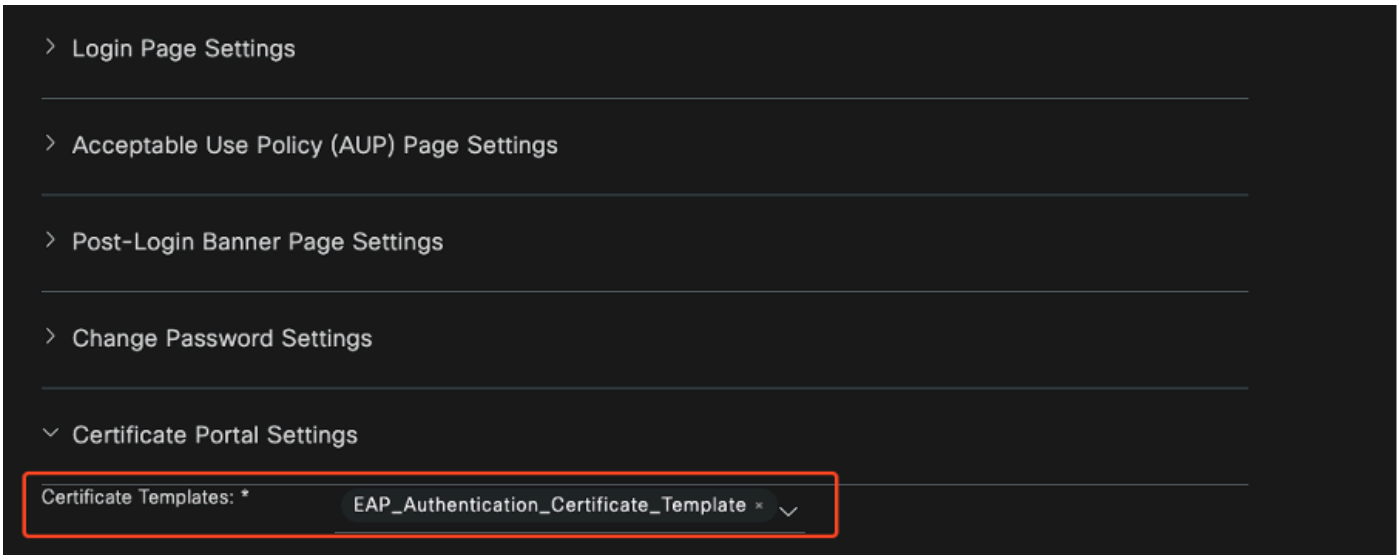
3.5. Omvat de gemachtigde groepen waarvan de leden toegang hebben tot het portaal. Selecteer bijvoorbeeld de gebruikersgroep Werknemers als uw gebruikers tot deze groep behoren.

3.6. Bepaal de certificaatsjablonen die zijn toegestaan onder de instellingen voor certificaatprovisioning.



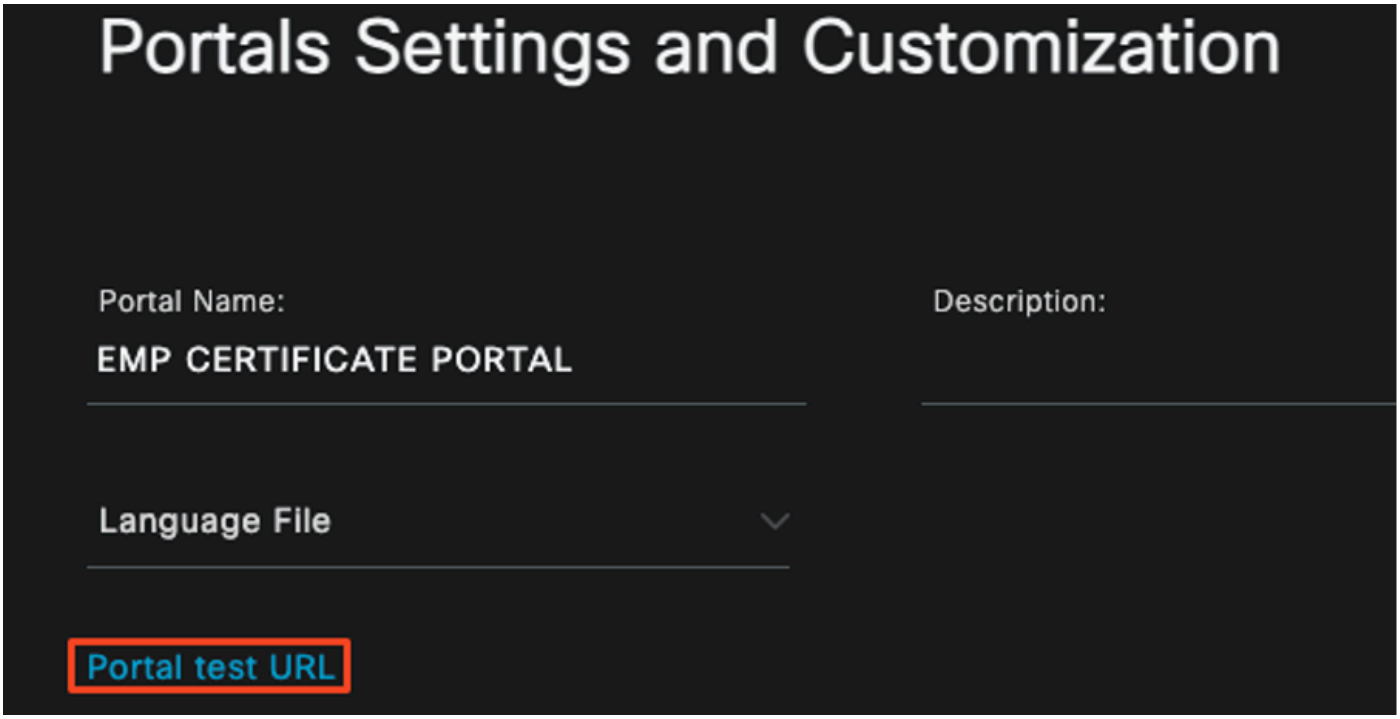

Portal Behavior and Flow Settings
Portal Page Customization
Portal & Page Settings
Portal Settings
1
HTTPS port:*
8443
(8000 - 8999)
2
Allowed Interfaces:*
For PSNs Using Physical Interfaces
Gigabit Ethernet 0
Gigabit Ethernet 1
Gigabit Ethernet 2
Gigabit Ethernet 3
Gigabit Ethernet 4
Gigabit Ethernet 5
For PSNs with Bonded Interfaces Configured
Bond 0
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
Bond 1
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
Bond 2
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup
3
Certificate group tag: *
Default Portal Certificate Group
Configure certificates at:
Administration > System > Certificates > System Certificates
4
Authentication method: *
Certificate_Request_Sequence
Configure authentication methods at:
Administration > Identity Management > Identity Source Sequences


Configure authorized groups
User account with Super admin privilege or ERS admin privilege will have access to the portal
Available
ALL_ACCOUNTS (default)
GROUP_ACCOUNTS (default)
OWN_ACCOUNTS (default)
Chosen
Employee
Choose all
Clear all
Fully qualified domain name (FQDN):

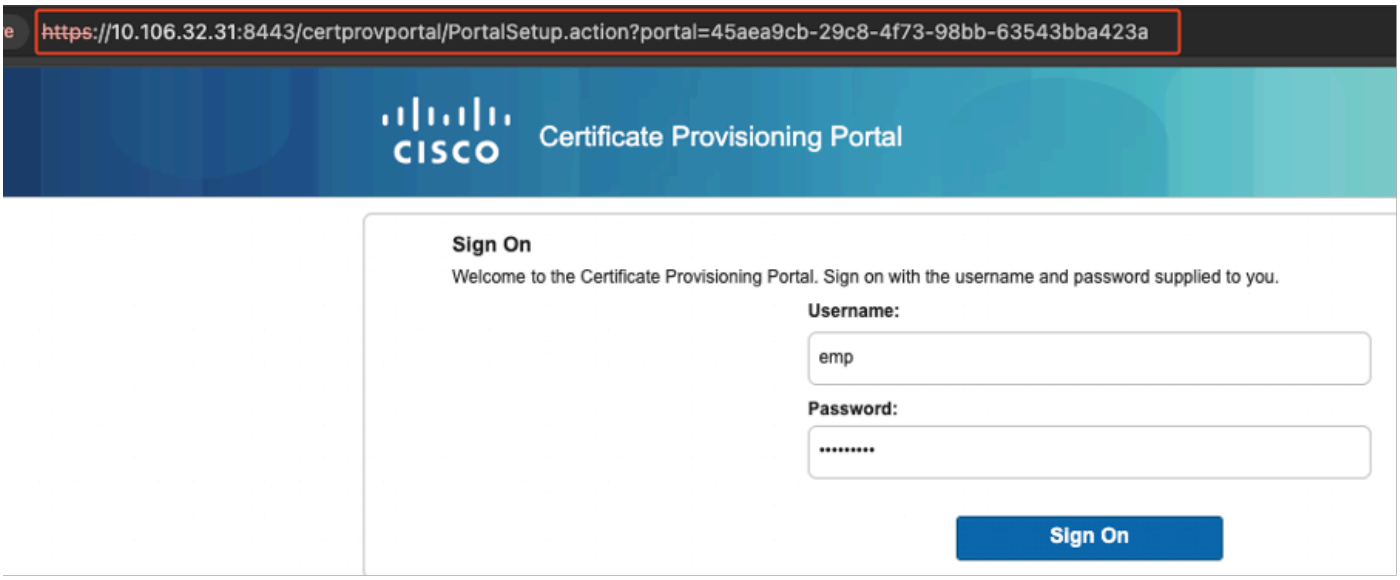


Configuratie van certificaatportal

Zodra deze installatie is voltooid, kunt u de portal testen door op de Portal Test URL te klikken. Deze actie opent de portaalpagina.



URL voor testportal

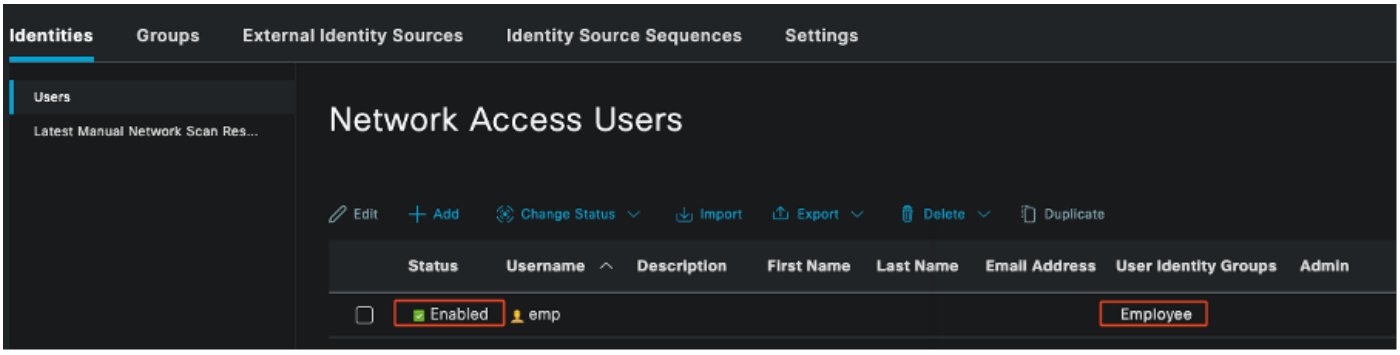


Poortpagina

Interne gebruiker toevoegen

Gebruik de volgende stappen om een gebruiker te maken voor verificatie via het certificaatportal:

1. Ga naar Administratie > Identiteitsbeheer > Identiteiten > Gebruikers.
2. Klik op de optie om een gebruiker aan het systeem toe te voegen.
3. Selecteer de Gebruikersidentiteitsgroepen waartoe de gebruiker behoort. Wijs bij dit voorbeeld de gebruiker toe aan de groep Werknemers.



Interne gebruiker toevoegen

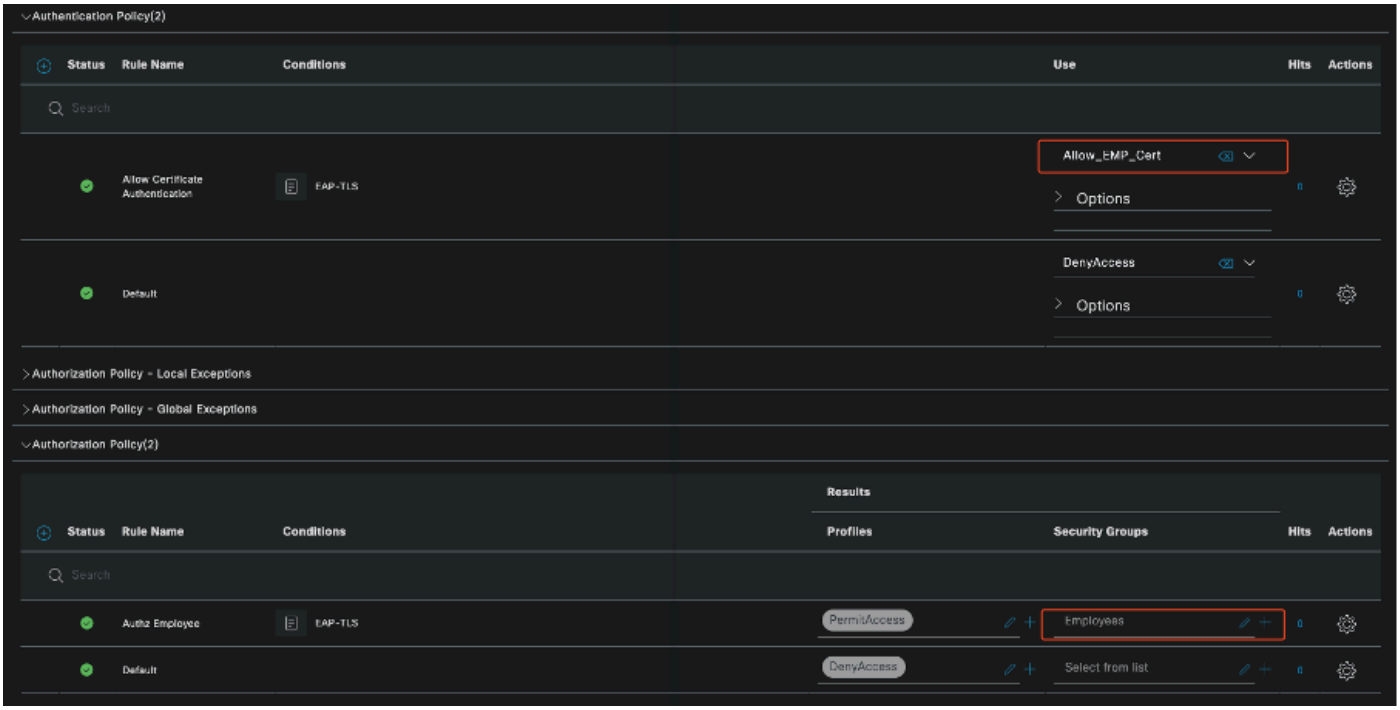
ISE-certificaatprovisioningportal en RADIUS-beleidsconfiguratie

In het vorige gedeelte werd de opzet van het ISE-portal voor certificaatprovisioning besproken. Nu, configureren wij de ISE RADIUS-beleidssets om gebruikersverificatie toe te staan.

1. Configureer ISE-beleidssets
2. Ga naar Beleidssets > Beleidssets.
3. Klik op het plusteken (+) om een nieuwe beleidsset te maken.

In dit voorbeeld, opstelling een eenvoudige beleidsreeks die wordt ontworpen om gebruikers voor authentiek te verklaren die hun certificaten gebruiken.

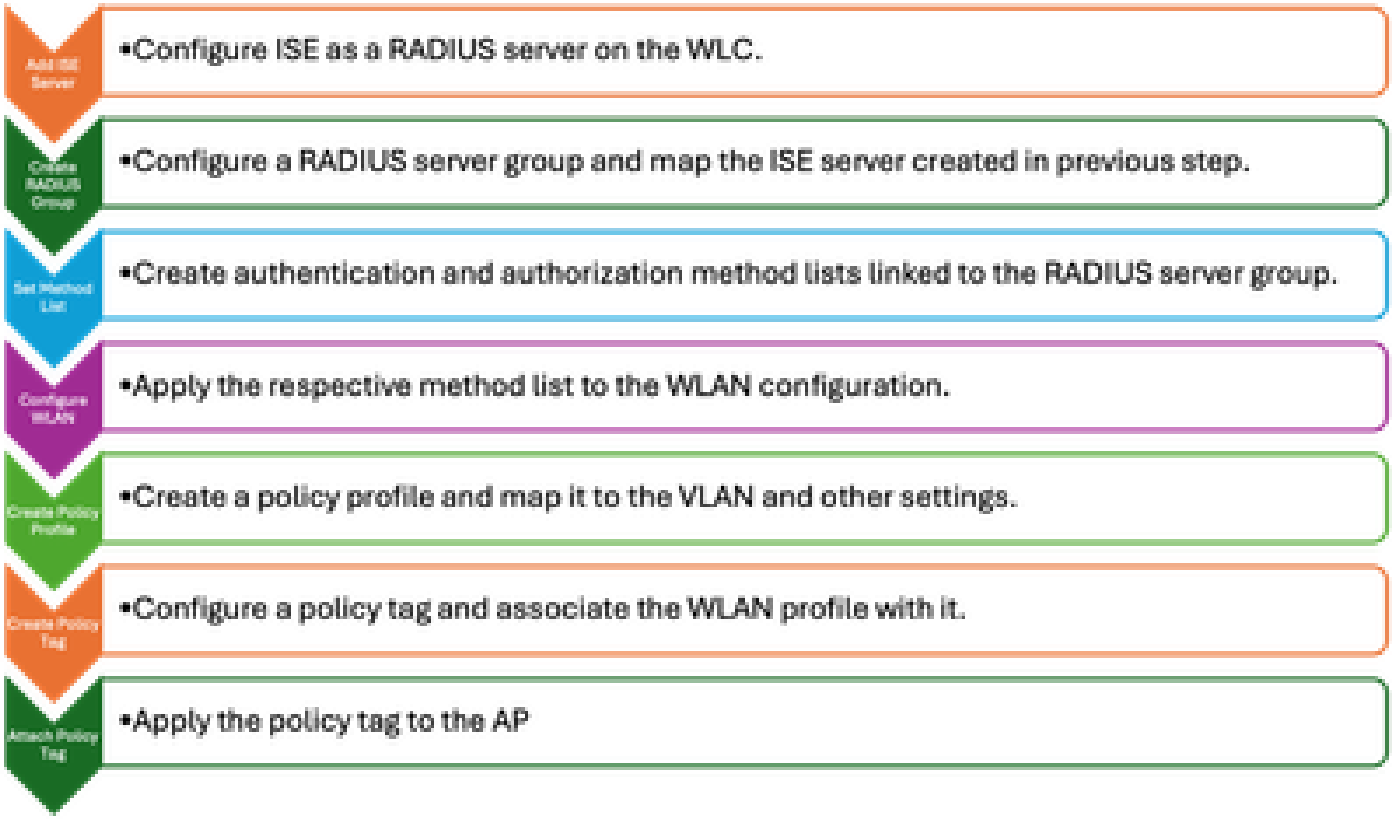
Beleidsset



Beleidsset voor verificatie en autorisatie

9800 WLC-configuratie

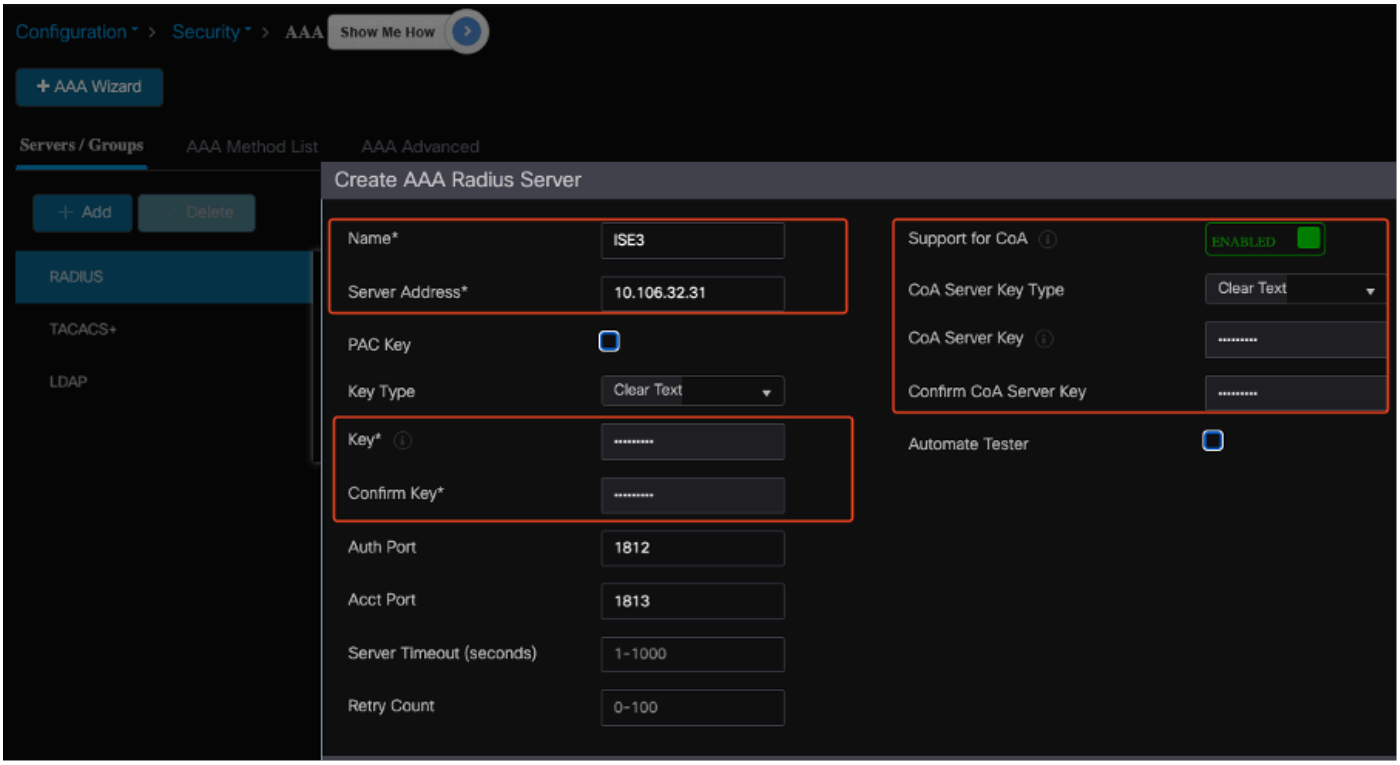
Hier zijn de configuratiestappen voor de 9800 WLC. Elke stap wordt begeleid door screenshots in deze sectie om visuele begeleiding te bieden.



WLC-configuratiestappen

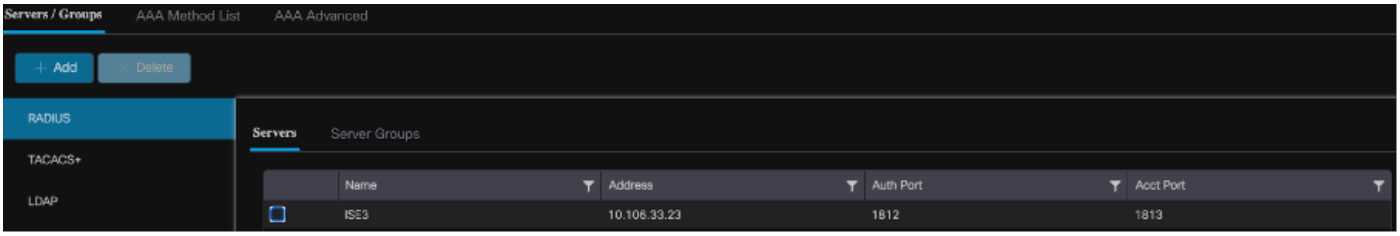
ISE-server toevoegen aan 9800 WLC

1. Gebruik de volgende stappen om de ISE-server te integreren met de 9800 draadloze LAN-controller (WLC):
2. Ga naar Configuratie > Beveiliging > AAA.
3. Klik op de knop Add om de ISE-server op te nemen in de WLC-configuratie.



ISE-server toevoegen in de WLC

Zodra de server is toegevoegd, wordt deze weergegeven in de lijst met servers.

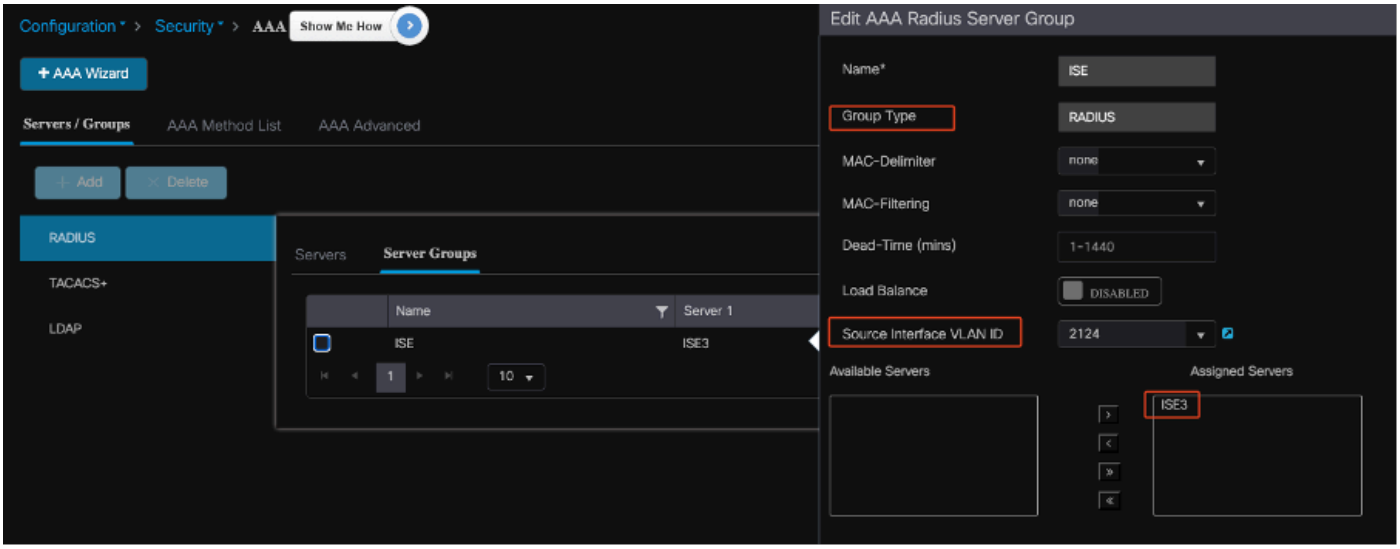


Radiusservers weergeven

Add Server Group op 9800 WLC

Voltooi de volgende stappen om een servergroep toe te voegen aan de 9800 draadloze LAN-controller:

1. Ga naar Configuratie > Beveiliging > AAA.
2. Klik op het tabblad Servergroep en klik vervolgens op Toevoegen om een nieuwe servergroep te maken.

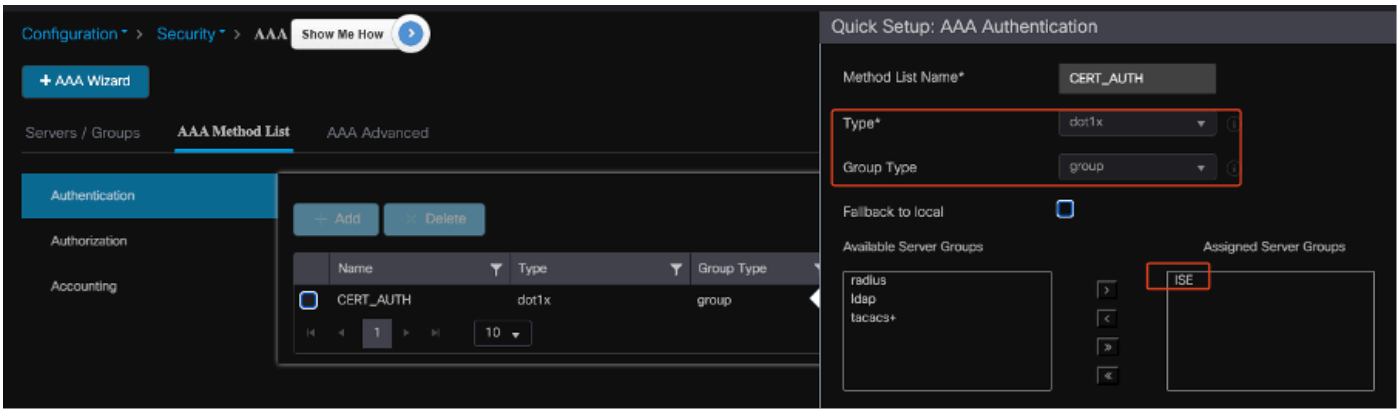


ISE-servers toewijzen aan een RADIUS-servergroep

Configureer de AAA-methodelijst op 9800 WLC

Nadat u de servergroep hebt gemaakt, configureert u de lijst met verificatiemethoden in de volgende stappen:

1. Blader naar Configuratie > Beveiliging > AAA > AAA-methodelijst.
2. Voeg op het tabblad Verificatie een nieuwe lijst van verificatiemethoden toe.
3. Stel het type in op dot1x.
4. Selecteer groep als groepstype.
5. Omvat de ISE-servergroepen die u eerder als servergroepen hebt gemaakt.

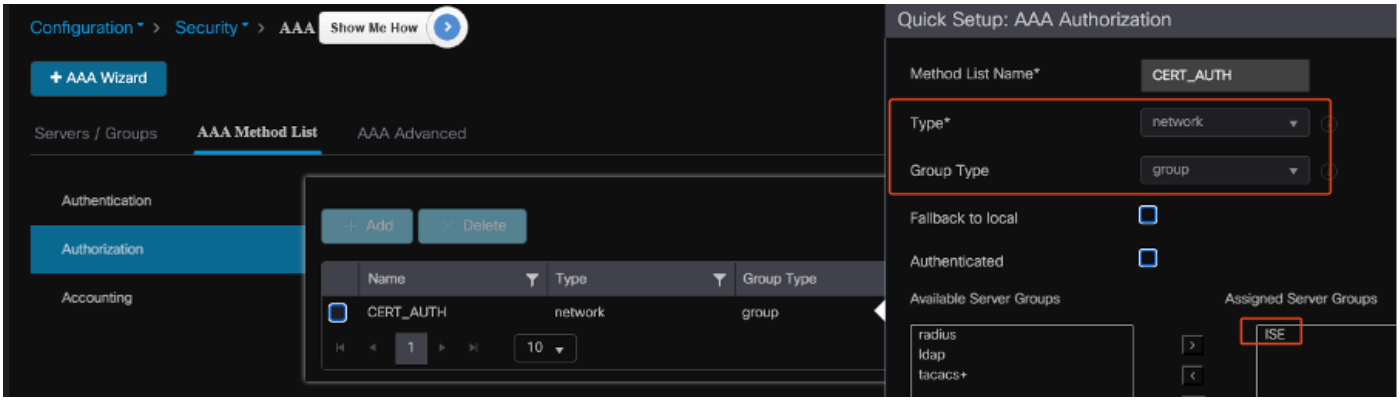


Verificatiemethodelijsten maken

Configureer de autorisatiemethode op de 9800 WLC

Gebruik de volgende stappen om de lijst met autorisatiemethoden in te stellen:

1. Navigeer naar het tabblad Autorisatie in het gedeelte AAA-methodelijst.
2. Klik op Add om een nieuwe lijst met autorisatiemethoden te maken.
3. Kies netwerk als type.
4. Selecteer groep als groepstype.
5. De ISE-servergroep als servergroep opnemen.

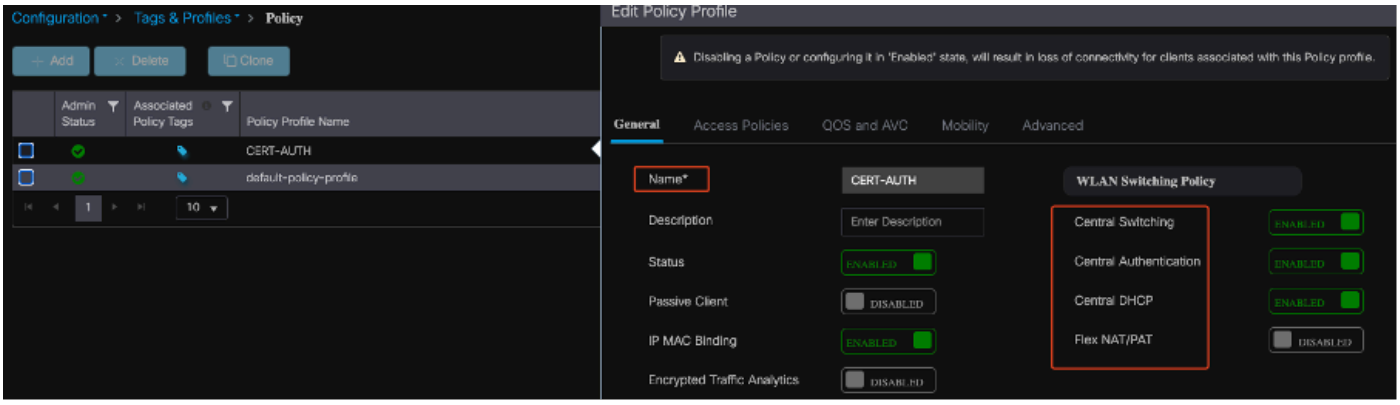


Toevoeging van een autorisatiemethode

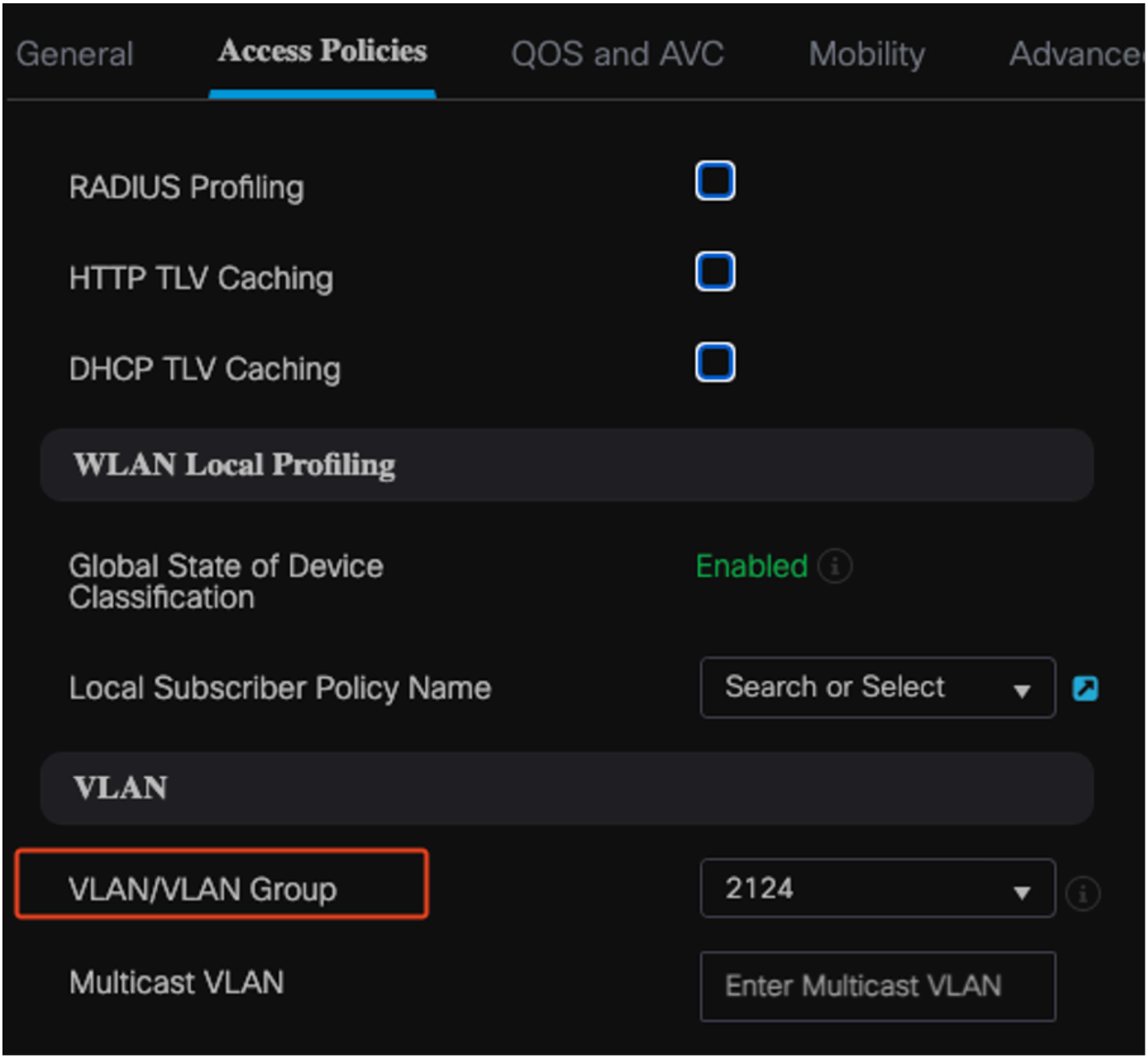
Een beleidsprofiel op 9800 WLC maken

Als de RADIUS-groepsconfiguratie is voltooid, gaat u verder met het maken van een beleidsprofiel:

1. Ga naar Configuration > Tags & profielen > Policy.
2. Klik op Add om een nieuw beleidsprofiel te maken.
3. Kies de juiste parameters voor uw beleidsprofiel. In dit voorbeeld is alles centraal en LAB VLAN wordt gebruikt als client-VLAN.



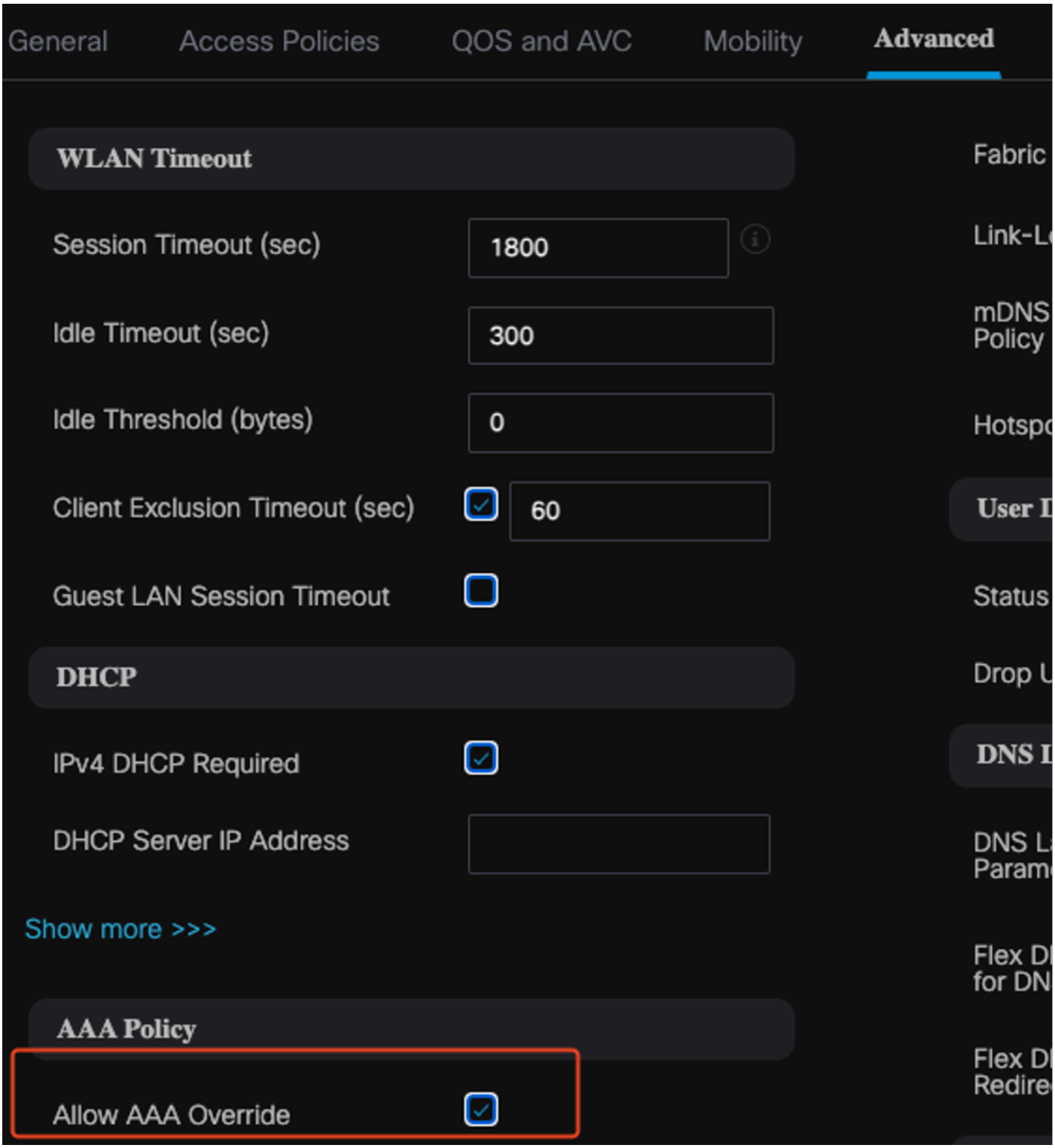
Beleidsprofiel configureren



Toewijzing van VLAN-naar-beleid

Zorg er bij het configureren van RADIUS-autorisatie voor dat de optie AAA Override is ingeschakeld in het tabblad Geavanceerd van de instellingen van het beleidsprofiel. Deze

instelling maakt het mogelijk dat de draadloze LAN-controller op RADIUS gebaseerde autorisatiebeleid toepast op gebruikers en apparaten.



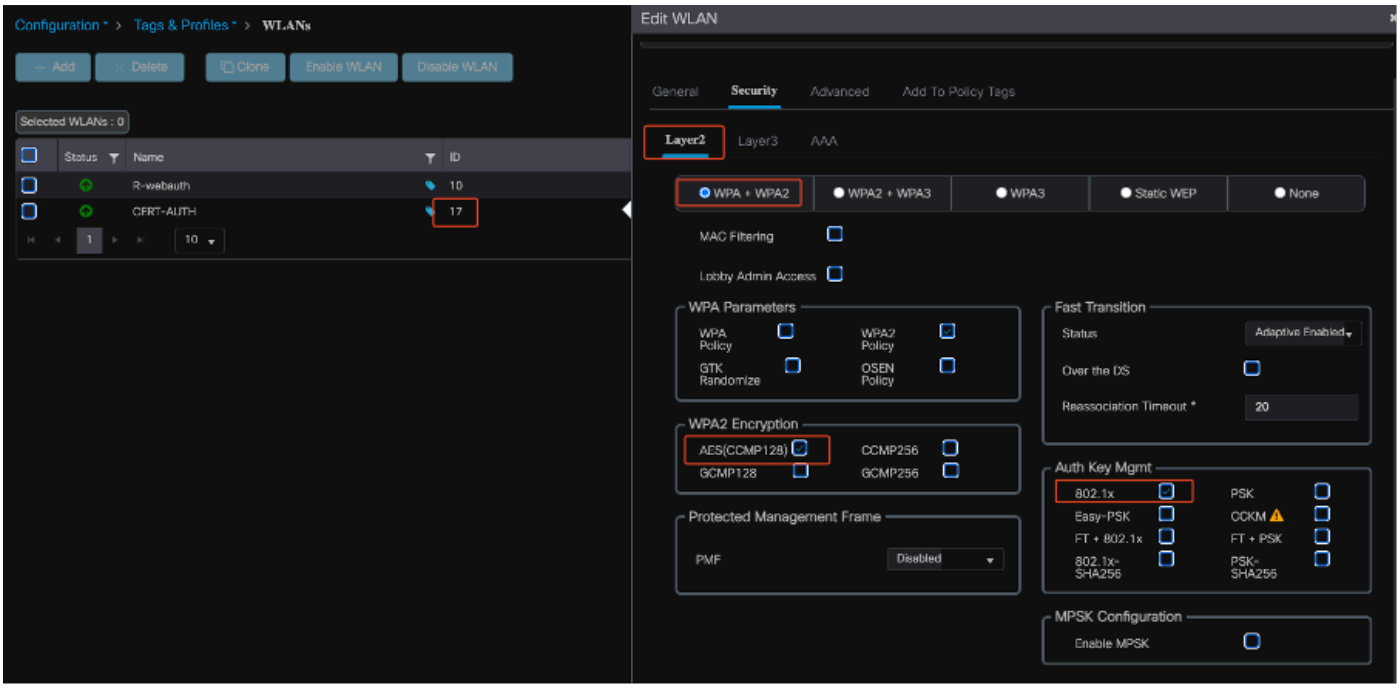
AAA-opheffing

WLAN's maken op 9800 WLC

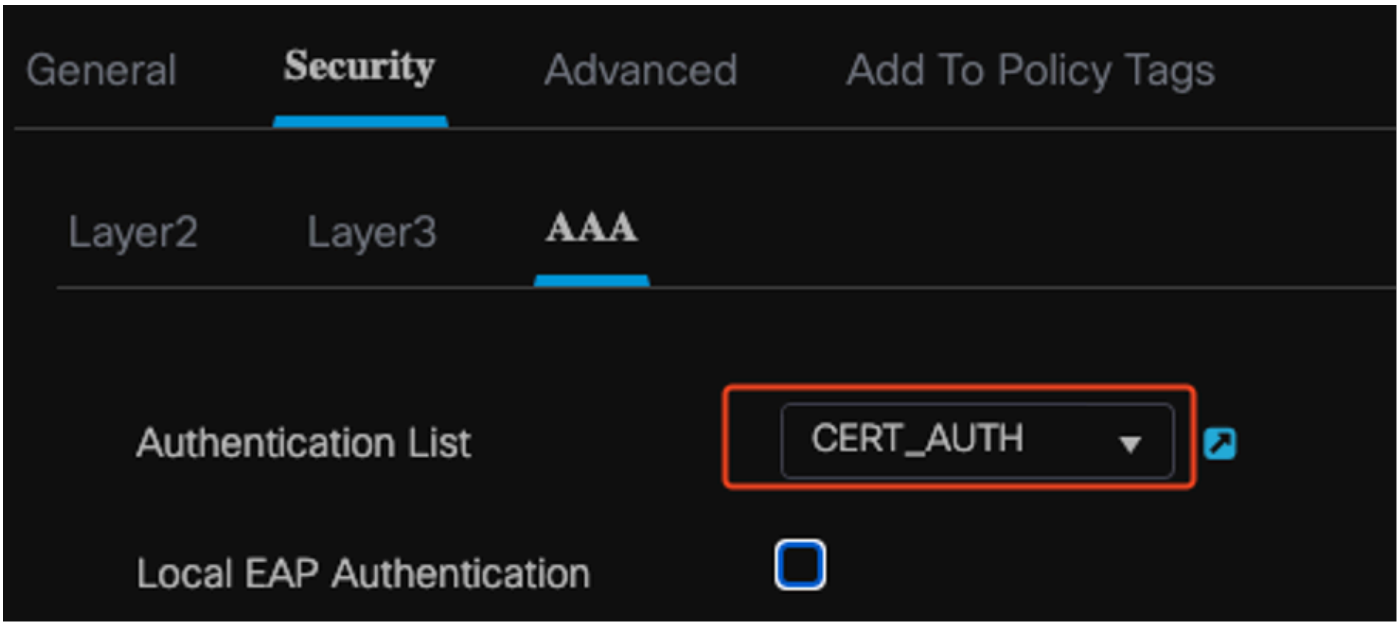
Gebruik de volgende stappen om een nieuw WLAN met 802.1x-verificatie in te stellen:

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

3. Selecteer de Layer 2-verificatie-instellingen en schakel de 802.1x-verificatie in.



WLAN-profielconfiguratie

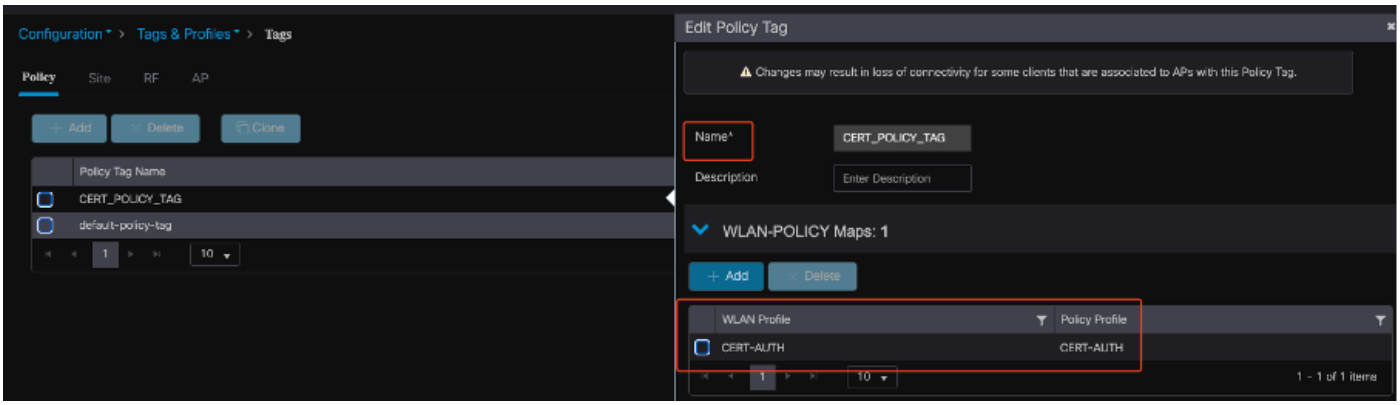


WLAN-profiel naar methodelijstkaart

WLAN-kaart met beleidsprofiel op 9800 WLC

Gebruik de volgende stappen om uw WLAN aan een beleidsprofiel te koppelen:

1. Navigeren naar Configuratie > Tags & profielen > Tags.
2. Klik op Add om een nieuwe tag toe te voegen.
3. In het gedeelte WLAN-BELEID koppelt u het nieuwe WLAN aan het juiste beleidsprofiel.

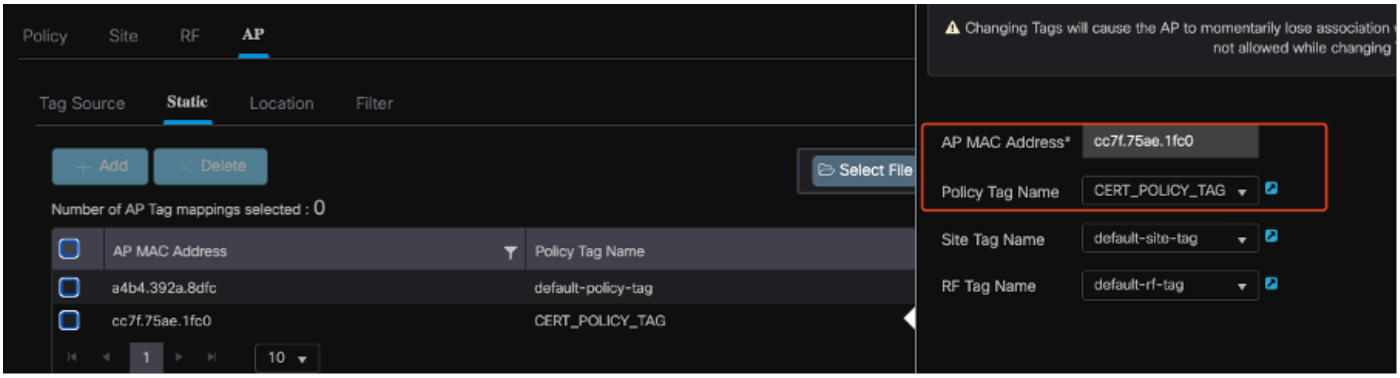


Configuratie beleidslabel

Toewijzing van beleidstag aan access point op 9800 WLC

Voltooi de volgende stappen om de beleidstag aan een access point (AP) toe te wijzen:

1. Ga naar Configuration > Tags & profielen > Tags > AP.
2. Ga naar het Statische gedeelte binnen de AP-configuratie.
3. Klik op het specifieke toegangspunt dat u wilt configureren.
4. Wijs de beleidsmarkering die u aan geselecteerde AP hebt gemaakt toe.



Toewijzing AP-TAG

Lopende Configuratie van WLC na de Voltooiing van de Opstelling

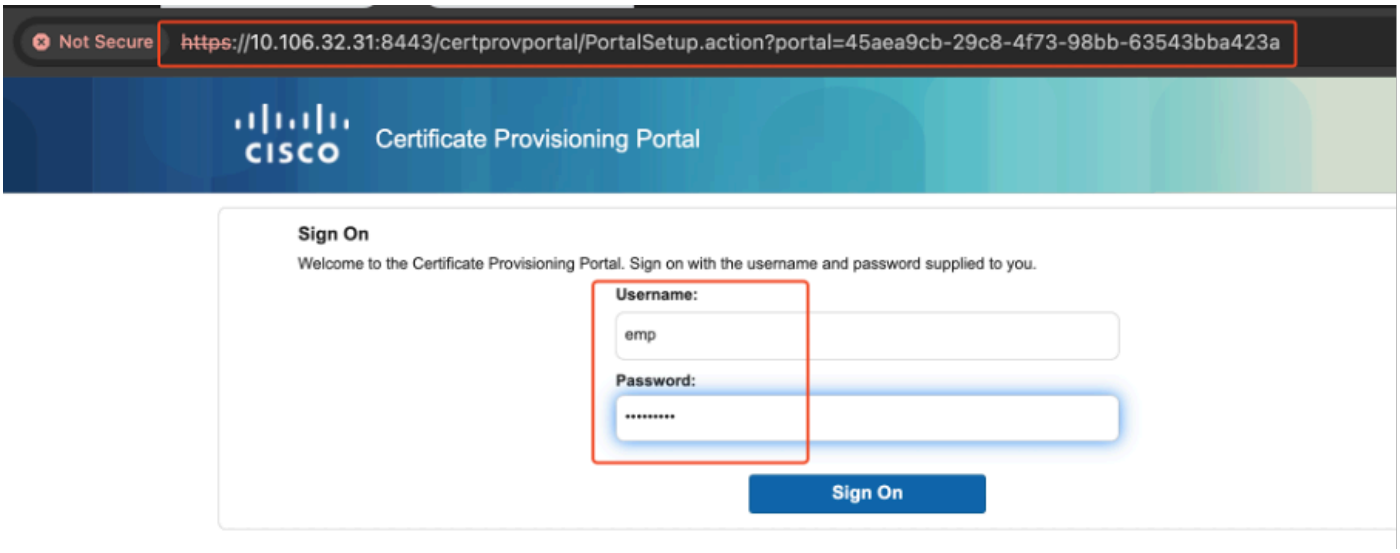
```
aaa group server radius ISE
 server name ISE3
 ip radius source-interface Vlan2124
aaa authentication dot1x CERT_AUTH group ISE
aaa authorization network CERT_AUTH group ISE
aaa server radius dynamic-author
 client 10.106.32.31 server-key Cisco!123
!

wireless profile policy CERT-AUTH
 aaa-override
 ipv4 dhcp required
 vlan 2124
 no shutdown
 wlan CERT-AUTH policy CERT-AUTH
wlan CERT-AUTH 17 CERT-AUTH
```

```
 security dot1x authentication-list CERT_AUTH
 no shutdown
!
wireless tag policy CERT_POLICY_TAG
 wlan CERT-AUTH policy CERT-AUTH
```

Certificaat voor de gebruiker maken en downloaden

Voer de volgende stappen uit om een certificaat voor een gebruiker te maken en te downloaden:

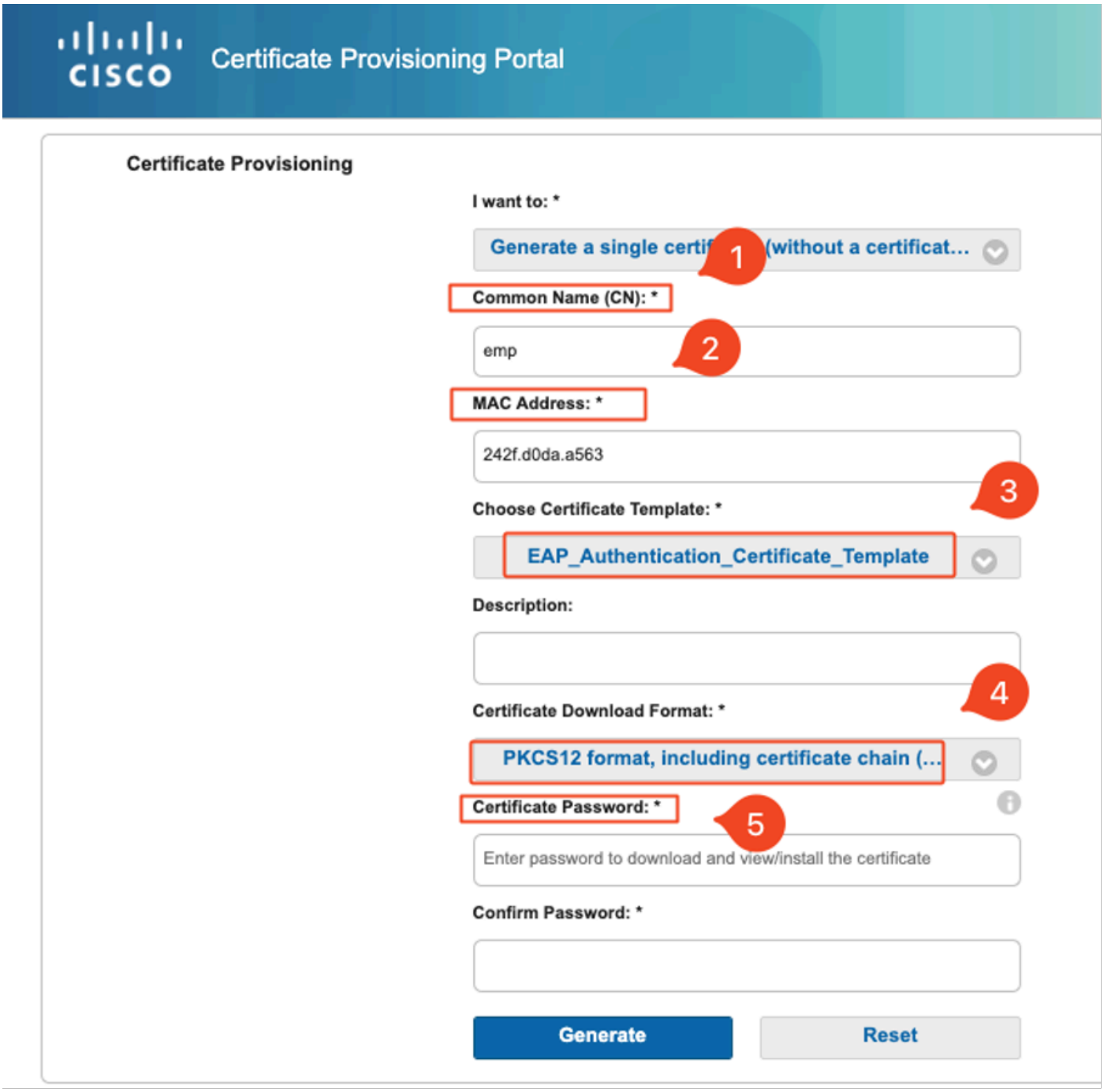
1. Laat de gebruiker inloggen op het certificaatportal dat eerder is ingesteld.



Certificaatportal gebruiken

2. Accepteer het beleid voor acceptabel gebruik (AUP). De ISE presenteert vervolgens een pagina voor het genereren van certificaten.

3. Selecteer Generate a single certificate (zonder certificaat dat verzoek ondertekent).



Certificaat genereren

Zorg ervoor dat deze verplichte velden zijn ingevuld om een certificaat te genereren via het Certificate Provisioning Portal:

- GN: De verificatieserver gebruikt de waarde die in het veld Gemeenschappelijke naam op het clientcertificaat wordt weergegeven voor de verificatie van een gebruiker. Voer in het veld algemene naam de gebruikersnaam in (waarmee u zich hebt aangemeld bij het portal Certificaatprovisioning).
- MAC-adres: Onderwerp Alternative Names (SAN) is een X.509 extensie waarmee verschillende waarden kunnen worden gekoppeld aan een beveiligingscertificaat. Cisco ISE, release 2.0 ondersteunt alleen MAC-adres. Vandaar in het veld SAN/MAC-adres.
    - Sjabloon voor certificaat: De certificaatsjabloon definieert een reeks velden die de CA gebruikt bij het valideren van een verzoek en het afgeven van een certificaat. Velden

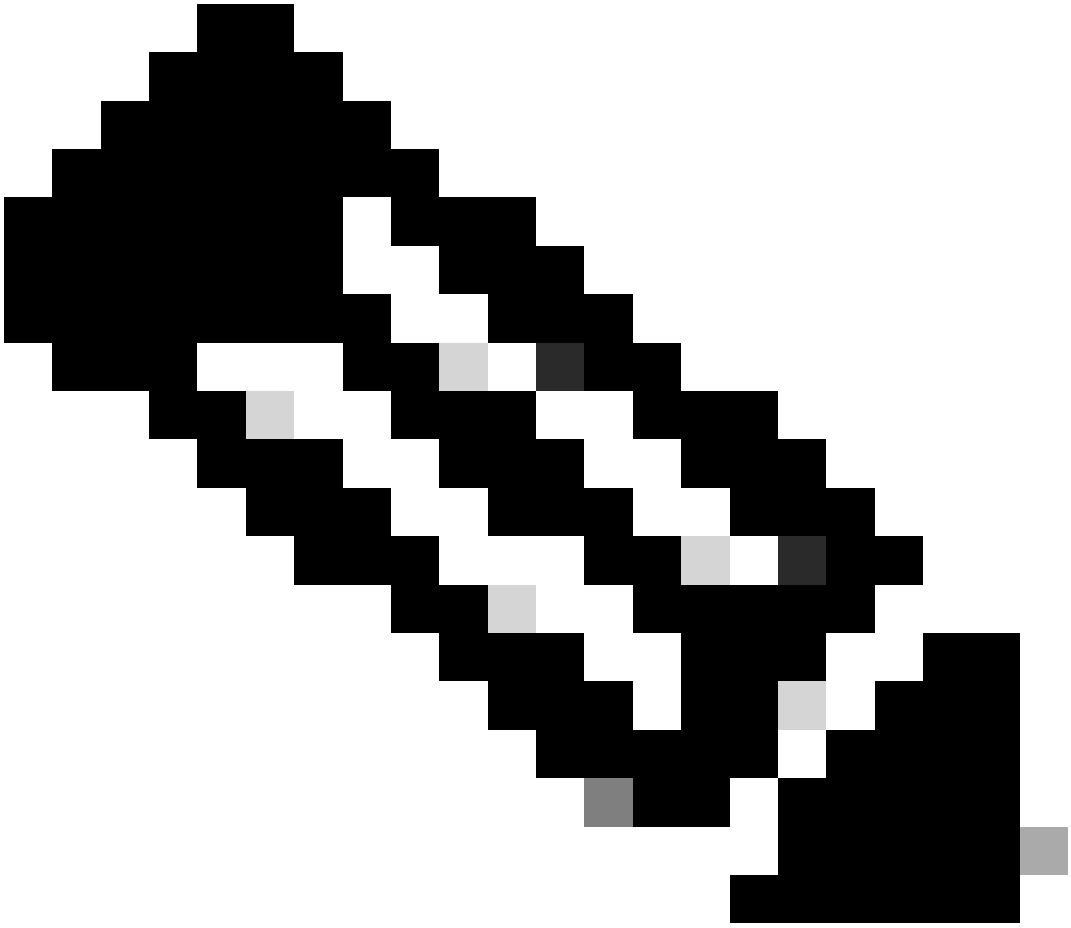
zoals de algemene naam (CN) worden gebruikt om het verzoek te valideren (CN moet overeenkomen met de gebruikersnaam). Andere velden worden door de CA gebruikt bij het afgeven van het certificaat.

- Wachtwoord voor certificaat: U hebt een certificaatwachtwoord nodig om uw certificaat te beveiligen. U moet het certificaatwachtwoord opgeven om de inhoud van het certificaat te kunnen bekijken en het certificaat op een apparaat te kunnen importeren.
- Uw wachtwoord moet aan deze regels voldoen:
- Het wachtwoord moet minimaal 1 hoofdletter, 1 kleine letter en 1 cijfer bevatten
    - Wachtwoord moet tussen 8 en 15 tekens lang zijn
    - Toegestane tekens zijn A-Z, a-z, 0-9, _, #

Nadat alle velden zijn ingevuld, selecteert u Generate om het certificaat te maken en te downloaden.

Certificaatinstallatie op een Windows 10-machine

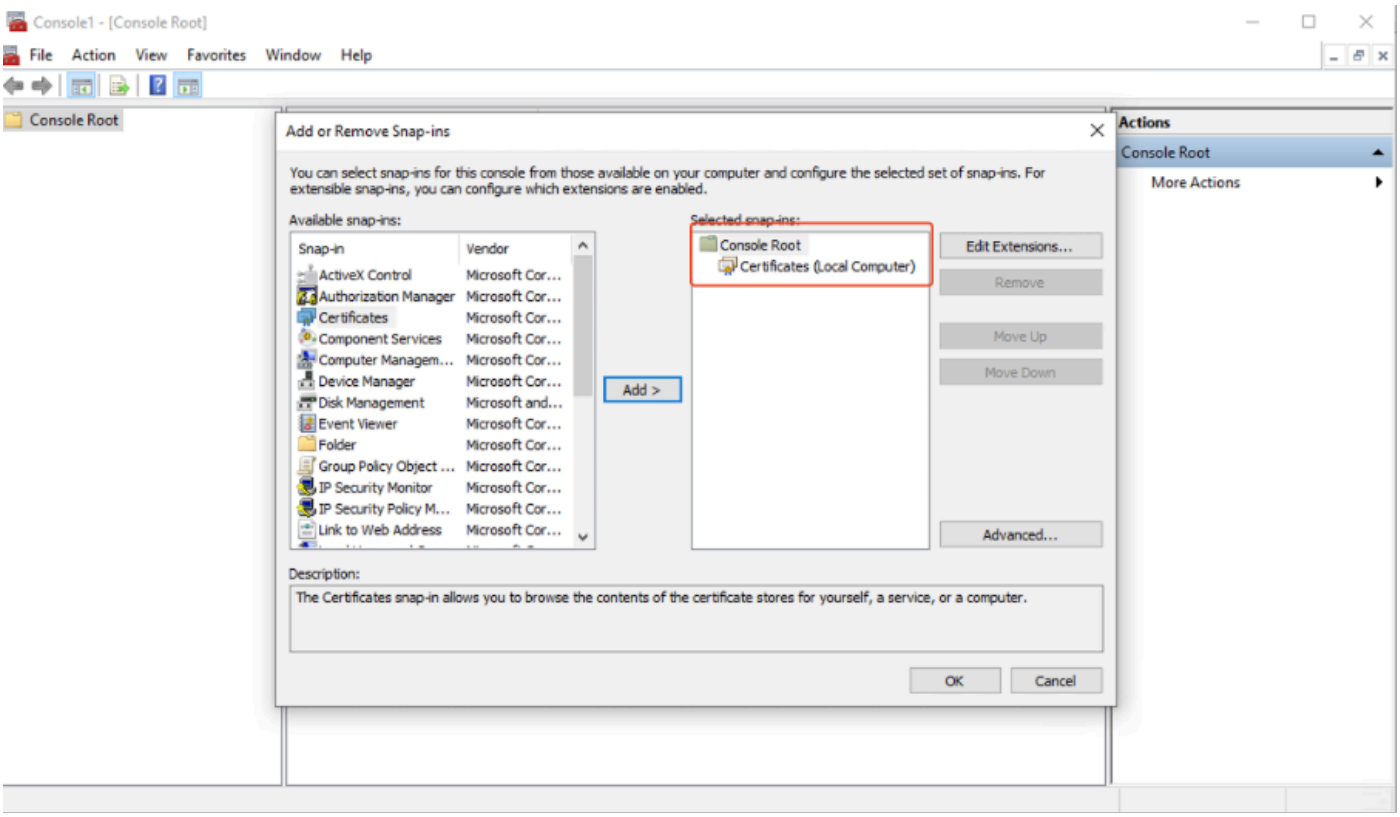
Als u een certificaat op een Windows 10-machine wilt installeren, opent u de Microsoft Management Console (MMC) met de volgende stappen:



Opmerking: Deze instructies kunnen afwijken, afhankelijk van uw Windows-installatie. Het wordt daarom aanbevolen om de Microsoft-documentatie te raadplegen voor specifieke informatie.

1. Klik op Start en vervolgens op Uitvoeren.
2. Typ mmc in het vak Uitvoeren en druk op ENTER. De Microsoft Management Console wordt geopend.
3. Certificaat magnetisch toevoegen:
4. Ga naar Bestand > Magnetisch toevoegen/verwijderen.
5. Selecteer Toevoegen, kies Certificaten en klik op Toevoegen.
6. Selecteer Computeraccount, vervolgens Lokale computer en klik op Voltooien.

Met deze stappen kunt u certificaten op uw lokale computer beheren.



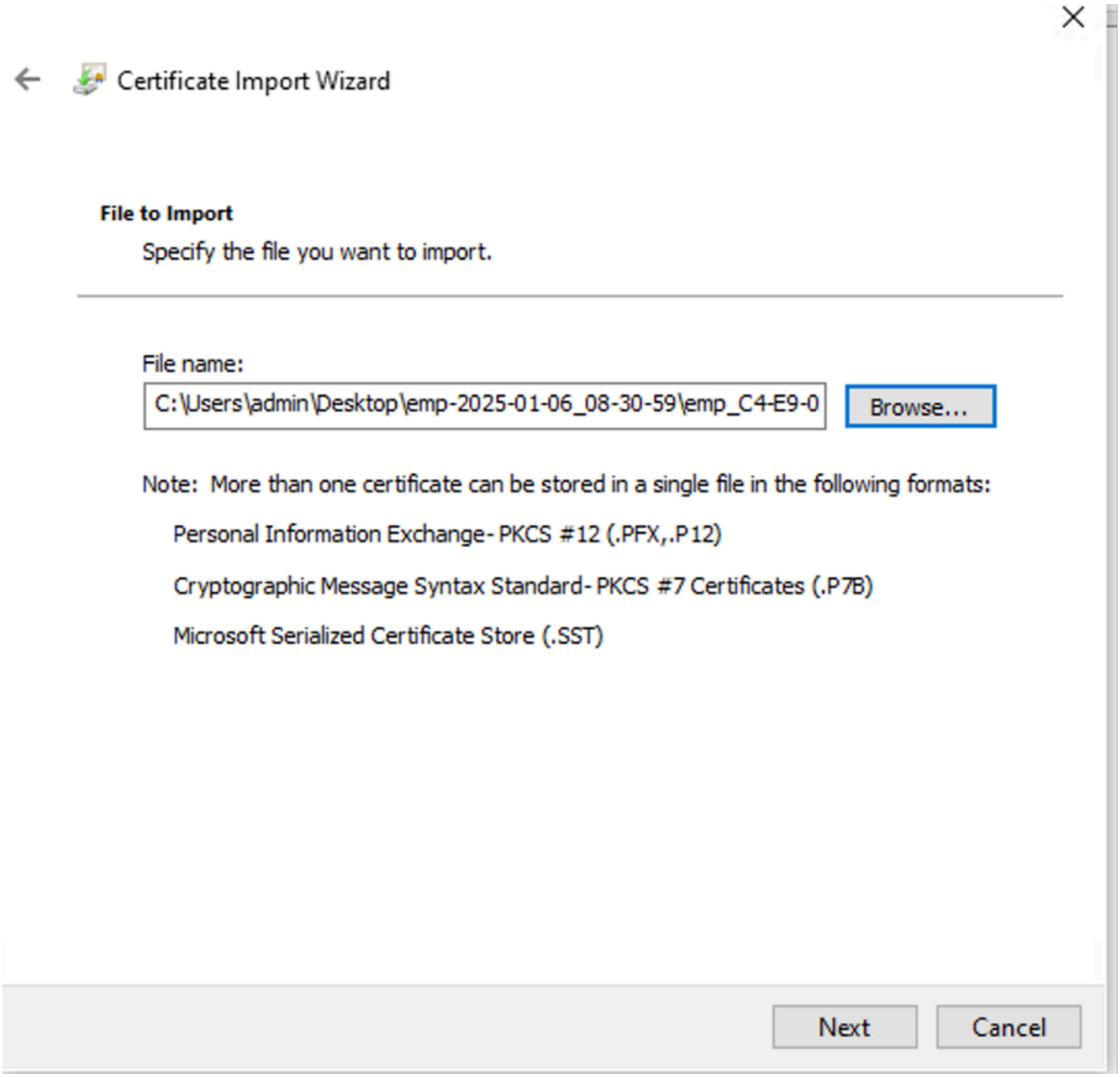
Windows MMC-console

Stap 1. Voer het certificaat in:

1.1. Klik op Actie in het menu.

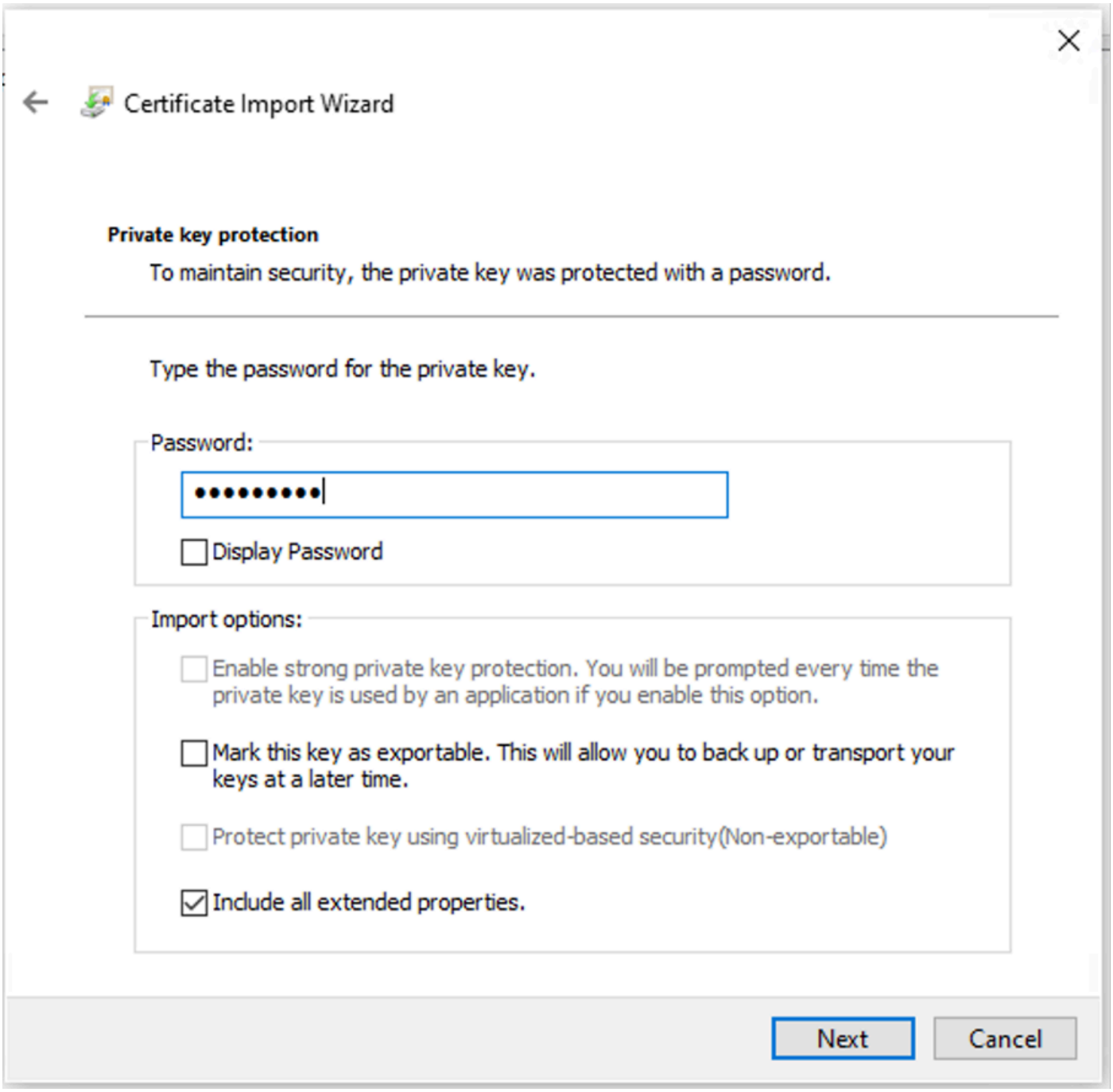
1.2. Ga naar Alle taken en selecteer vervolgens Importeren.

1.3. Ga door de aanwijzingen om het certificaatbestand op uw computer te vinden en te selecteren.



Invoercertificaat

Tijdens het proces voor het importeren van certificaten wordt u gevraagd het wachtwoord in te voeren dat u hebt aangemaakt bij het genereren van het certificaat op de portal. Zorg ervoor dat u dit wachtwoord nauwkeurig invoert om het certificaat op uw computer te kunnen importeren en installeren.



Wachtwoord voor certificaat invoeren

Stap 2. Certificaten naar de juiste mappen verplaatsen:

2.1. Open de Microsoft Management Console (MMC) en navigeer naar de Certificaten (Lokale computer) > Persoonlijke map.

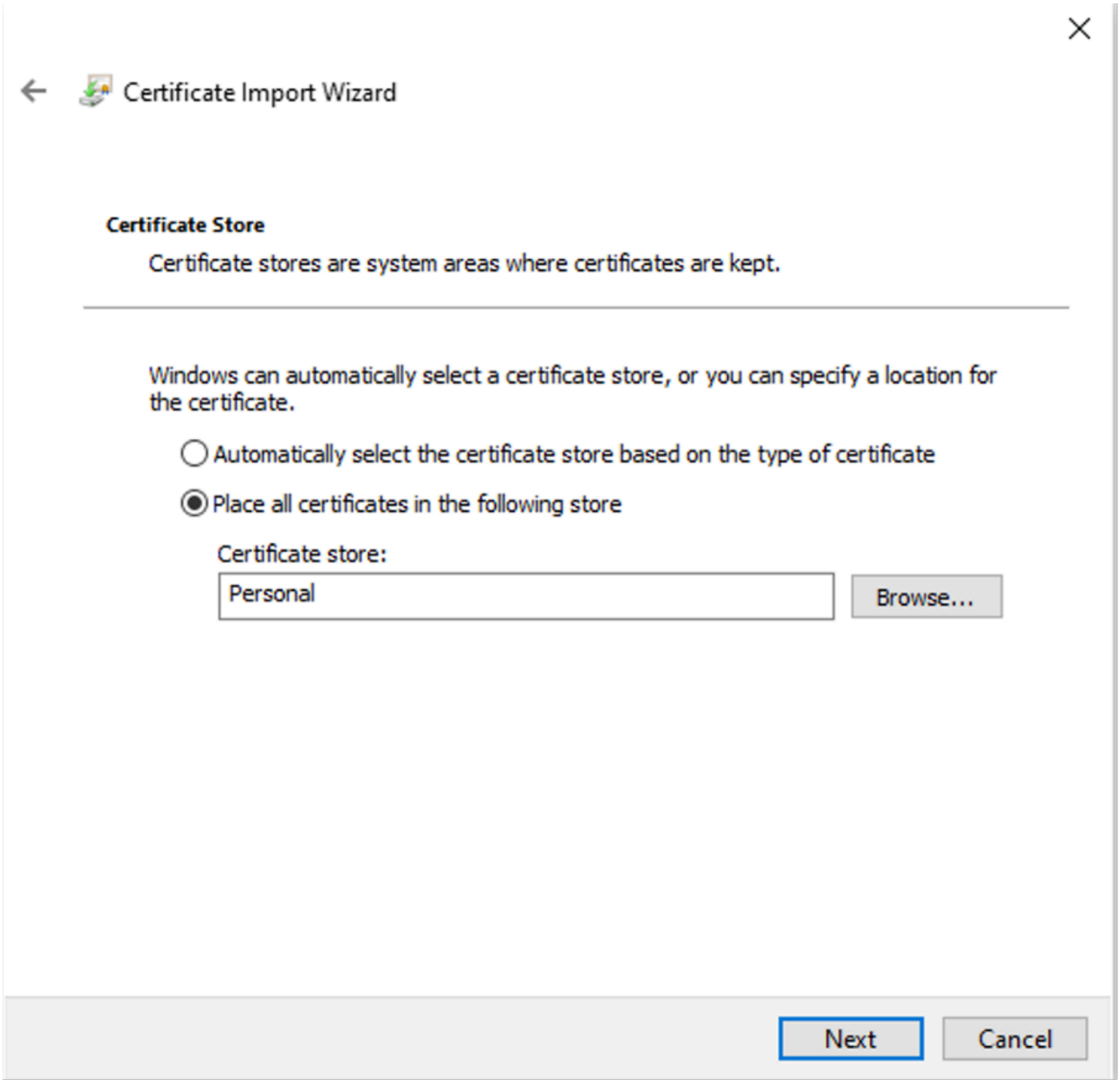
2.2. Bekijk de certificaten en bepaal de typen ervan (bijvoorbeeld Root CA, Intermediate CA of Personal).

2.3. Verplaats elk certificaat naar de daartoe bestemde opslagplaats:

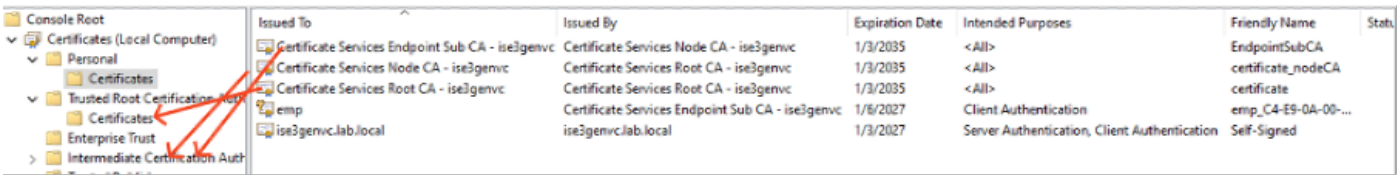
2.4. CA-basiscertificaten: Ga naar Trusted Root-certificeringsinstanties.

2.5. Tussentijdse CA-certificaten: Verplaatsen naar intermediaire certificeringsinstanties.

2.6. Persoonlijke certificaten: Laat de persoonlijke map achter.



Certificaten opslaan in de persoonlijke map

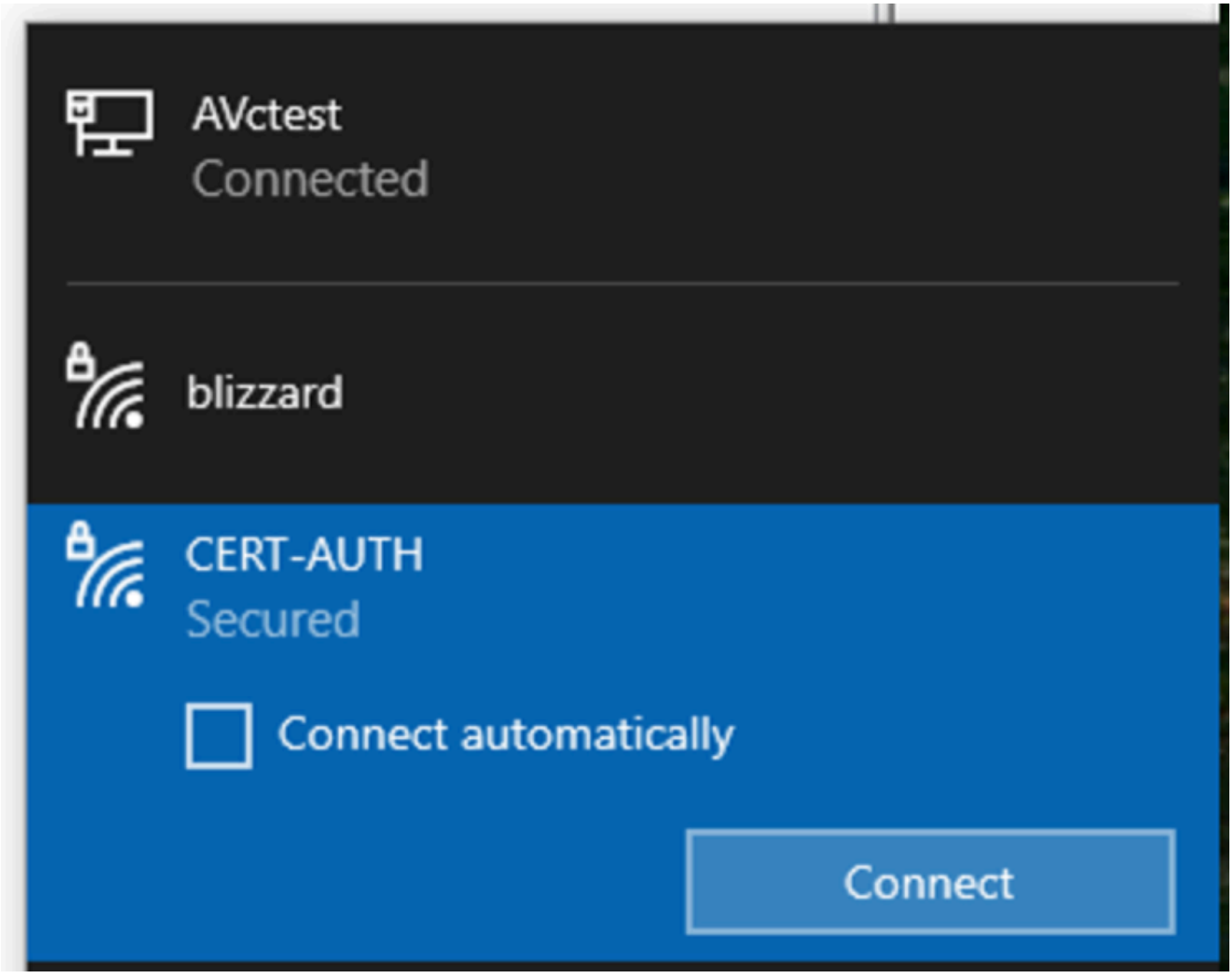


Certificaten verplaatsen in hun winkels

De Windows-machine aansluiten

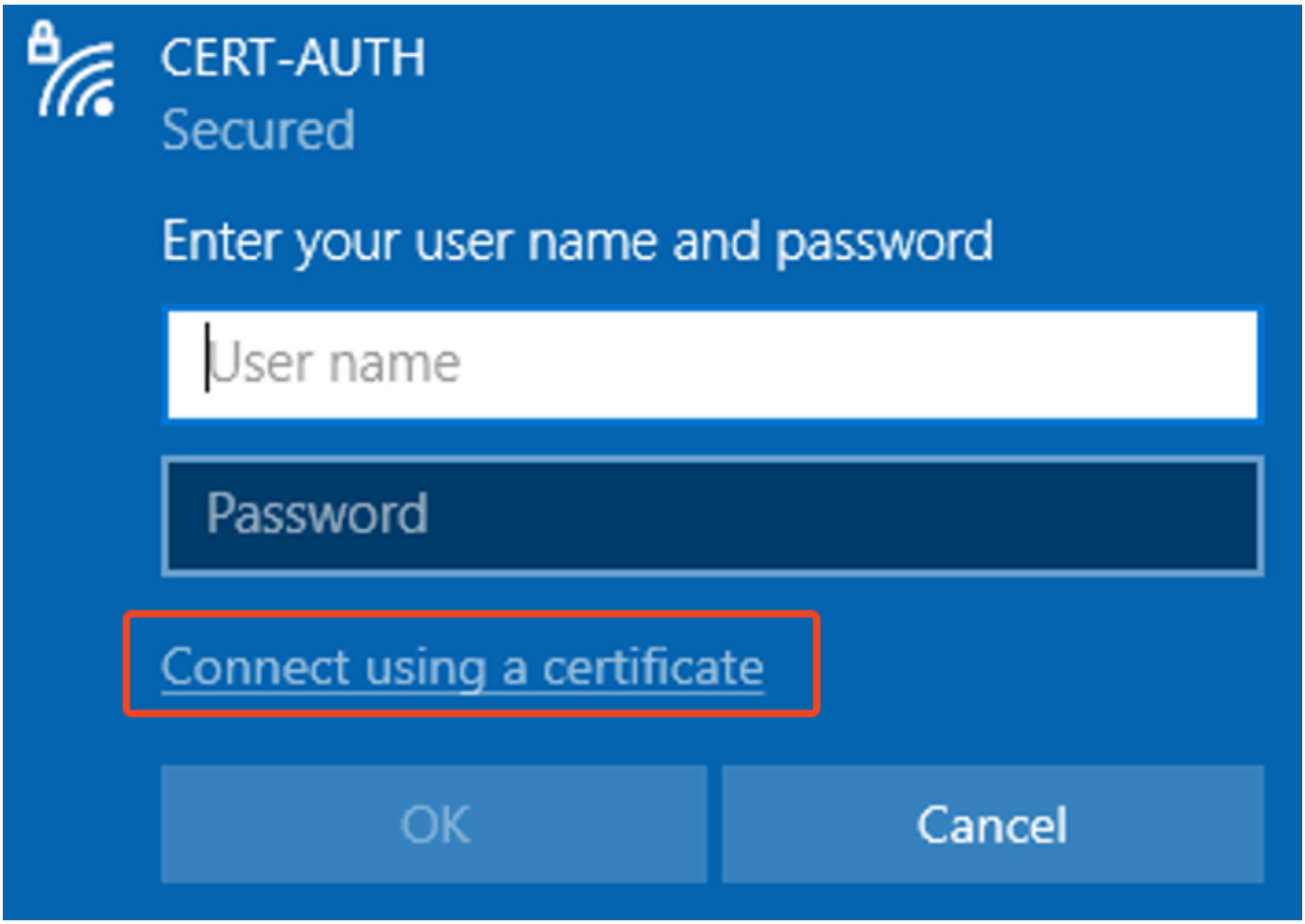
Zodra de certificaten naar de juiste winkels zijn verplaatst, gebruikt u deze stappen om verbinding te maken met het WLAN:

1. Klik op het pictogram netwerk in het systeemvak om beschikbare draadloze netwerken te bekijken.
2. Zoek en klik op de naam van het WLAN waarmee u verbinding wilt maken.
3. Klik op Verbinden en ga verder met aanvullende aanwijzingen om het verbindingsproces te voltooien met behulp van uw certificaat voor verificatie.



Verbinding maken met het draadloze netwerk

Wanneer u tijdens het verbindingsproces wordt gevraagd naar het WLAN, selecteert u de optie Verbinding maken met behulp van een certificaat.



Certificaat als referenties gebruiken

Hiermee kunt u met succes verbinding maken met het draadloze netwerk met behulp van het certificaat.

```
C:\>netsh wlan  show interface

There is 1 interface on the system:

    Name                   : Wi-Fi 3
    Description            : TP-Link Wireless USB Adapter
    GUID                   : ee5d1c47-43cc-4873-9ae6-99e2e43c39ea
    Physical address       : 24:2f:d0:da:a5:63
    State                  : connected
    SSID                   : CERT-AUTH
    BSSID                  : a4:88:73:9e:8d:af
    Network type           : Infrastructure
    Radio type             : 802.11ac
    Authentication         : WPA2-Enterprise
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 36
    Receive rate (Mbps)    : 360
    Transmit rate (Mbps)   : 360
    Signal                 : 100%
    Profile                : CERT-AUTH

    Hosted network status  : Not available


C:\>netsh wlan show profiles CERT-AUTH | find "Smart"
    EAP type               : Microsoft: Smart Card or other certificate
```

Draadloos profiel controleren

Verifiëren

Controleer dat het WLAN wordt uitgezonden door de WLC:

<#root>

```
POD6_9800#show wlan summ
Number of WLANs: 2
ID Profile Name SSID Status Security
-----------------------------------------------------------------------------------------------------------------
```

17

CERT-AUTH

CERT-AUTH

UP [WPA2][802.1x][AES]

Controleer of de AP op de WLC staat:

```
POD6_9800#show ap summ
Number of APs: 1
CC = Country Code
RD = Regulatory Domain
AP Name Slots AP Model Ethernet MAC Radio MAC CC RD IP Address State Location
-------------------------------------------------------------------------------------------------
AP1 3 C9130AXI-D cc7f.75ae.1fc0 a488.739e.8da0 IN -D 10.78.8.78 Registered default location
```

Zorg ervoor dat het toegangspunt het WLAN uitzendt:

<#root>

```
POD6_9800#show ap name AP1 wlan dot11 24ghz
Slot id : 0
WLAN ID BSSID
------------------------
17 a488.739e.8da0

POD6_9800#show ap name AP1 wlan dot11 5ghz
Slot id : 1
WLAN ID BSSID
------------------------
```

17

```
 a488.739e.8daf
```

Met client verbonden via EAP-TLS:

<#root>

```
POD6_9800#show wire cli summ
Number of Clients: 1
MAC Address AP Name Type ID State Protocol Method Role
-----------------------------------------------------------------------------------------------------
242f.d0da.a563 AP1 WLAN
```

17

```
 IP Learn 11ac
```

Dot1x

```
 Local

POD6_9800#sho wireless client mac-address 242f.d0da.a563 detail | in username|SSID|EAP|AAA|VLAN
```

Wireless LAN Network Name (SSID): CERT-AUTH

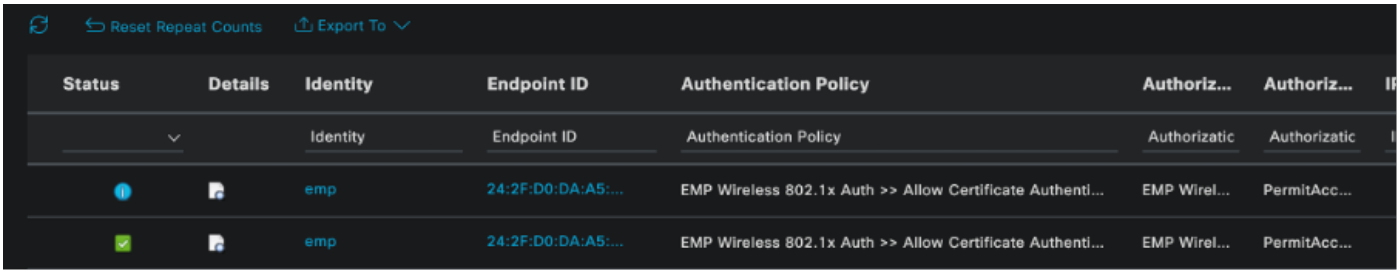
```
BSSID : a488.739e.8daf
```

EAP Type : EAP-TLS

```
VLAN : 2124
Multicast VLAN : 0
```

VLAN : 2124

Cisco Radius ISE-live logs:

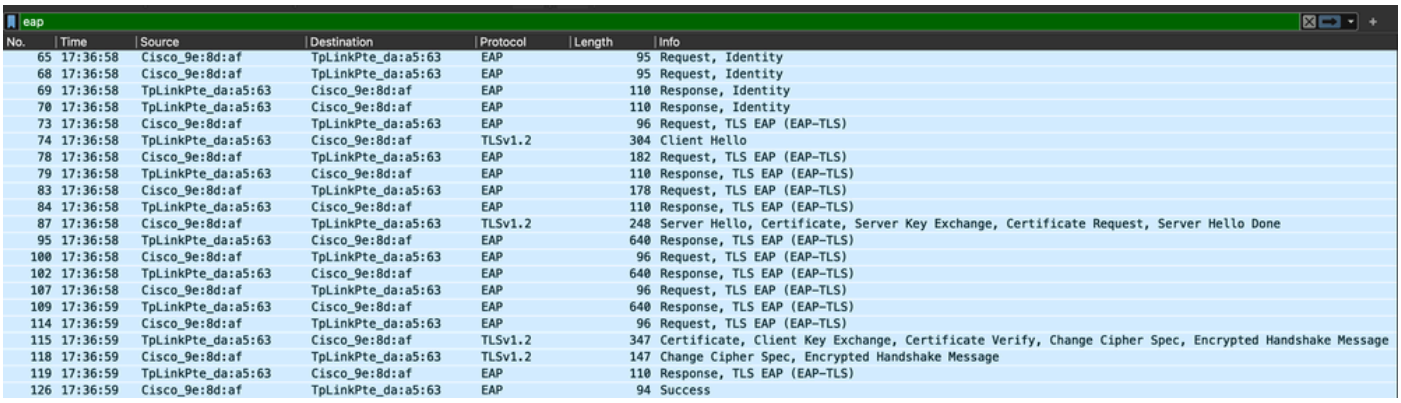


ISE-straal voor live logs

Gedetailleerd verificatietype:

Gedetailleerde ISE-logbestanden

WLC EPC Capture toont de EAP-TLS-pakketten:



eap

No.	Time	Source	Destination	Protocol	Length	Info
65	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
68	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
69	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
70	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
73	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
74	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	304	Client Hello
78	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	182	Request, TLS EAP (EAP-TLS)
79	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
83	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	178	Request, TLS EAP (EAP-TLS)
84	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
87	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	248	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
95	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
100	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
102	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
107	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
109	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
114	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
115	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	347	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
118	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	147	Change Cipher Spec, Encrypted Handshake Message
119	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
126	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	94	Success

WLC Capture toont de EAP-transactie

- Packet nummer 87 komt overeen met stap 8 in de EAP-TLS-stroom die aan het begin van het document is beschreven.
- Packet nummer 115 komt overeen met stap 9 in de EAP-TLS-stroom die aan het begin van het document is beschreven.
- Packet nummer 118 komt overeen met stap 10 in de EAP-TLS-stroom die aan het begin van het document is beschreven.

Radio actief (RA) spoor dat de verbinding van de cliënt toont: Dit RA-spoor wordt gefilterd om enkele relevante lijnen van de verificatietransactie weer te geven.

2025/01/08 11 58 20.816875191 {wncd_x_r0-2} {1} [ewlc-capwapmsg-sess] [15655] (debug) Versleuteld DTLS-bericht verzenden. Dest IP 10.78.8.78[5256], lengte 499
2025/01/08 11 58 20.851392112 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Verzend access-request naar 10.106.33.23 1812 id 0/25, len 390
2025/01/08 11 58 20.871842938 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Ontvangen van id 1812/25 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.872246323 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Verzend EAPOL-pakket - versie 3, EAPOL-type EAP, payload-lengte 6, EAP-type = EAP-TLS
2025/01/08 11 58 20.881960763 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ontvangen EAPOL-pakket - versie 1,EAPOL Type EAP, payload-lengte 204, EAP-type = EAP-TLS
2025/01/08 11 58 20.882292551 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Verzend access-request naar 10.106.33.23 1812 id 0/26, len 663
2025/01/08 11 58 20.926204990 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Ontvangen van id 1812/26 10.106.33.23 0, Access-Challenge, len 1135
2025/01/08 11 58 20.927390754 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Verzend EAPOL-pakket - versie 3, EAPOL-type EAP, payload-lengte 1012, EAP-type = EAP-TLS
2025/01/08 11 58 20.935081108 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ontvangen EAPOL-pakket - versie 1, EAPOL Type EAP, payload-lengte 6, EAP-type = EAP-TLS
2025/01/08 11 58 20.935405770 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Verzend access-request naar 10.106.33.23 1812 id 0/27, len 465
2025/01/08 11 58 20.938485635 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Ontvangen van

id 1812/27 10.106.33.23 0, Access-Challenge, len 1131
2025/01/08 11 58 20.939630108 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Verzend EAPOL-pakket - versie 3, EAPOL-type EAP, payload-lengte 1008, EAP-type = EAP-TLS
2025/01/08 11 58 20.947417061 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ontvangen EAPOL-pakket - versie 1, EAPOL Type EAP, payload-lengte 6, EAP-type = EAP-TLS
2025/01/08 11 58 20.947722851 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Verzend access-request naar 10.106.33.23 1812 id 0/28, len 465
2025/01/08 11 58 20.949913199 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Ontvangen van id 1812/28 10.106.33.23 0, Access-Challenge, len 275
2025/01/08 11 58 20.950432303 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Verzend EAPOL-pakket - versie 3,EAPOL Type EAP, payload-lengte 158, EAP-type = EAP-TLS
2025/01/08 11 58 20.966862562 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ontvangen EAPOL-pakket - versie 1,EAPOL Type EAP, payload-lengte 1492, EAP-type = EAP-TLS
2025/01/08 11 58 20.967209224 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Verzend access-request naar 10.106.33.23 1812 id 0/29, len 1961
2025/01/08 11 58 20.971337739 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Ontvangen van id 1812/29 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.971708100 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Verzend EAPOL-pakket - versie 3, EAPOL-type EAP, payload-lengte 6, EAP-type = EAP-TLS
2025/01/08 11 58 20.978742828 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ontvangen EAPOL-pakket - versie 1,EAPOL Type EAP, payload-lengte 1492, EAP-type = EAP-TLS
2025/01/08 11 58 20.979081544 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Verzend access-request naar 10.106.33.23 1812 id 0/30, len 1961
2025/01/08 11 58 20.982535977 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Ontvangen van id 1812/30 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.982907200 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Verzend EAPOL-pakket - versie 3, EAPOL-type EAP, payload-lengte 6, EAP-type = EAP-TLS
2025/01/08 11 58 20.990141062 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ontvangen EAPOL-pakket - versie 1,EAPOL Type EAP, payload-lengte 1492, EAP-type = EAP-TLS
2025/01/08 11 58 20.990472026 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Verzend access-request naar 10.106.33.23 1812 id 0/31, len 1961
2025/01/08 11 58 20.994358525 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Ontvangen van id 1812/31 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.994722151 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Verzend EAPOL-pakket - versie 3, EAPOL-type EAP, payload-lengte 6, EAP-type = EAP-TLS
2025/01/08 11 58 21.001735553 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ontvangen EAPOL-pakket - versie 1,EAPOL Type EAP, payload-lengte 247,

EAP-type = EAP-TLS
2025/01/08 11 58 21.002076369 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Verzend access-request naar 10.106.33.23 1812 id 0/32, len 706
2025/01/08 11 58 21.013571608 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Ontvangen van id 1812/32 10.106.33.23 0, Access-Challenge, len 174
2025/01/08 11 58 21.013987785 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Verzend EAPOL-pakket - versie 3,EAPOL Type EAP, payload-lengte 57, EAP-type = EAP-TLS
2025/01/08 11 58 21.024429150 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ontvangen EAPOL-pakket - versie 1,EAPOL Type EAP, payload-lengte 6, EAP-type = EAP-TLS
2025/01/08 11 58 21.024737996 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Verzend access-request naar 10.106.33.23 1812 id 0/33, len 465
2025/01/08 11 58 21.057794929 {wncd_x_r0-2}{1} [radius] [15655] (info) RADIUS Ontvangen van id 1812/33 10.106.33.23 0, access-Accept, len 324
2025/01/08 11 58 21.058149893 {wncd_x_r0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Verhoogde identiteit update gebeurtenis voor SAP methode EAP-TLS

Problemen oplossen

Er zijn geen specifieke stappen voor probleemoplossing bij dit probleem buiten de gebruikelijke procedures voor draadloze 802.1x-probleemoplossing:

1. Neem client-RA-debugs om het verificatieproces te controleren.
2. Voer een WLC EPC-opname uit om de pakketten tussen de client, WLC en RADIUS-server te onderzoeken.
3. Controleer de live logs van ISE om te controleren of het verzoek overeenkomt met het juiste beleid.
4. Controleer op het Windows-eindpunt dat het certificaat correct is geïnstalleerd en dat de gehele vertrouwensketen aanwezig is.

Referenties

- Veelgestelde vragen over certificaatprovisioningportal, release 3.2
- Interne certificeringsinstantie van ISE begrijpen
- EAP-TLS begrijpen en configureren met een WLC en een ISE

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.