EAP-TLS begrijpen en configureren met een WLC en een ISE

Inhoud

Inleiding

In dit document wordt beschreven hoe u een Wireless Local Area Network (WLAN) kunt instellen met 802.1X en Extensible Verification Protocol EAP-TLS

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- 802.1X-verificatieproces
- Certificaten

Gebruikte componenten

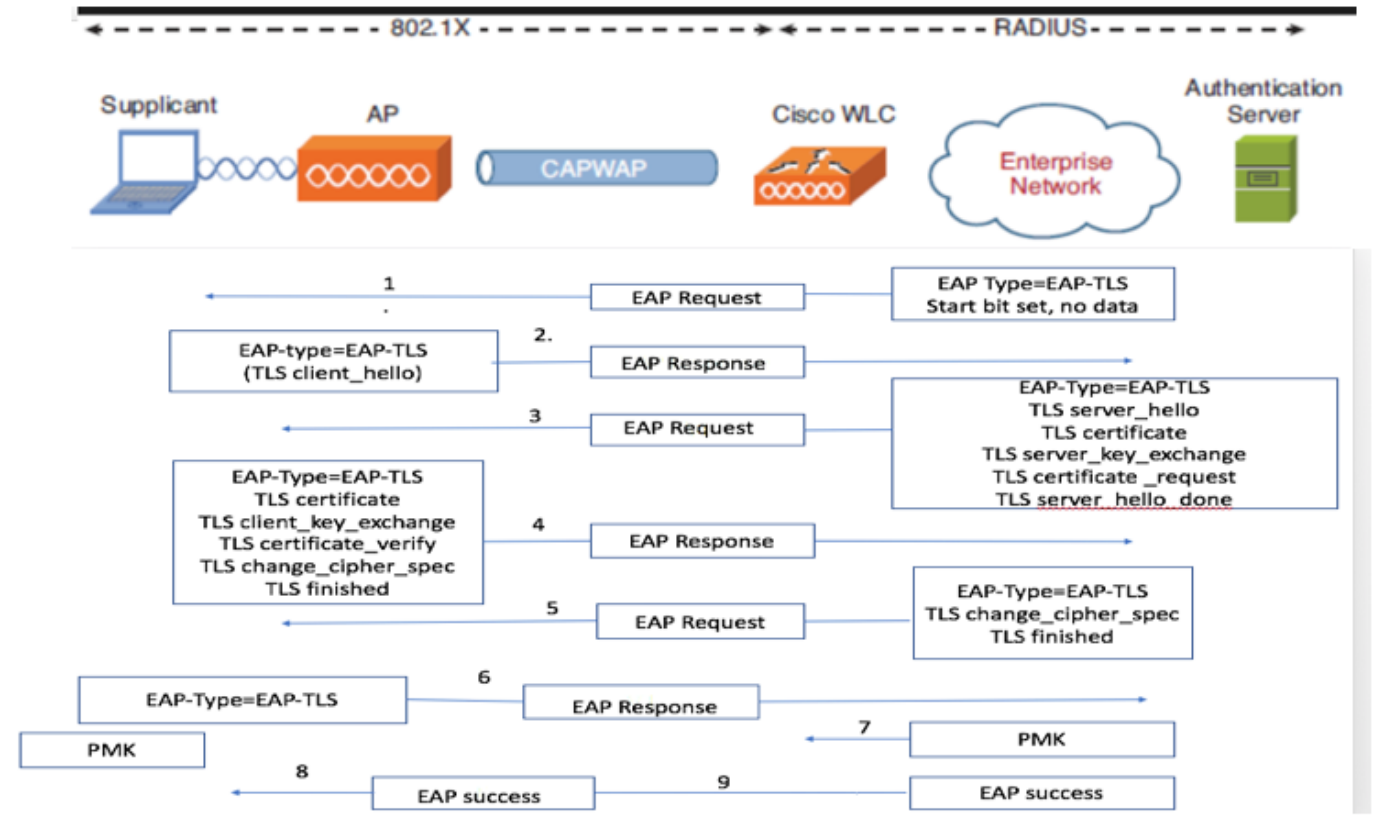
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- WLC 3504 versie 8.10
- Identity Services Engine (ISE) versie 2.7

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

EAP-TLS-stroom



Stappen in EAP-TLS-stroom

1. Draadloze client wordt gekoppeld aan het access point (AP). AP staat de client niet toe om op dit punt gegevens te verzenden en stuurt een verificatieaanvraag.De aanvrager reageert dan met een EAP-Response Identity. De WLC communiceert vervolgens de gebruiker-id informatie naar de verificatieserver. RADIUS-server reageert weer op de client met een EAP-TLS Start-pakket. Het EAP-TLS-gesprek begint op dit punt.
2. De peer stuurt een EAP-Response terug naar de verificatieserver die een "client_hello" handshake-bericht bevat, een algoritme dat voor NULL is ingesteld
3. 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.
```

4. De client reageert met een EAP-responsbericht dat het volgende bevat:

```
Certificate ¬ Server can validate to verify that it is trusted.

client_key_exchange

certificate_verify ¬ Verifies the server is trusted

change_cipher_spec

TLS finished
```

5. Nadat de client met succes is geverifieerd, reageert de RADIUS-server met een Access-challenge, die het bericht "change_cipher_spec" en handshake voltooid bevat.

6.Wanneer het dit ontvangt, verifieert de client de hash om de radius server te verifiëren.

7.A nieuwe encryptie sleutel wordt dynamisch afgeleid uit het geheim tijdens de handdruk van TLS

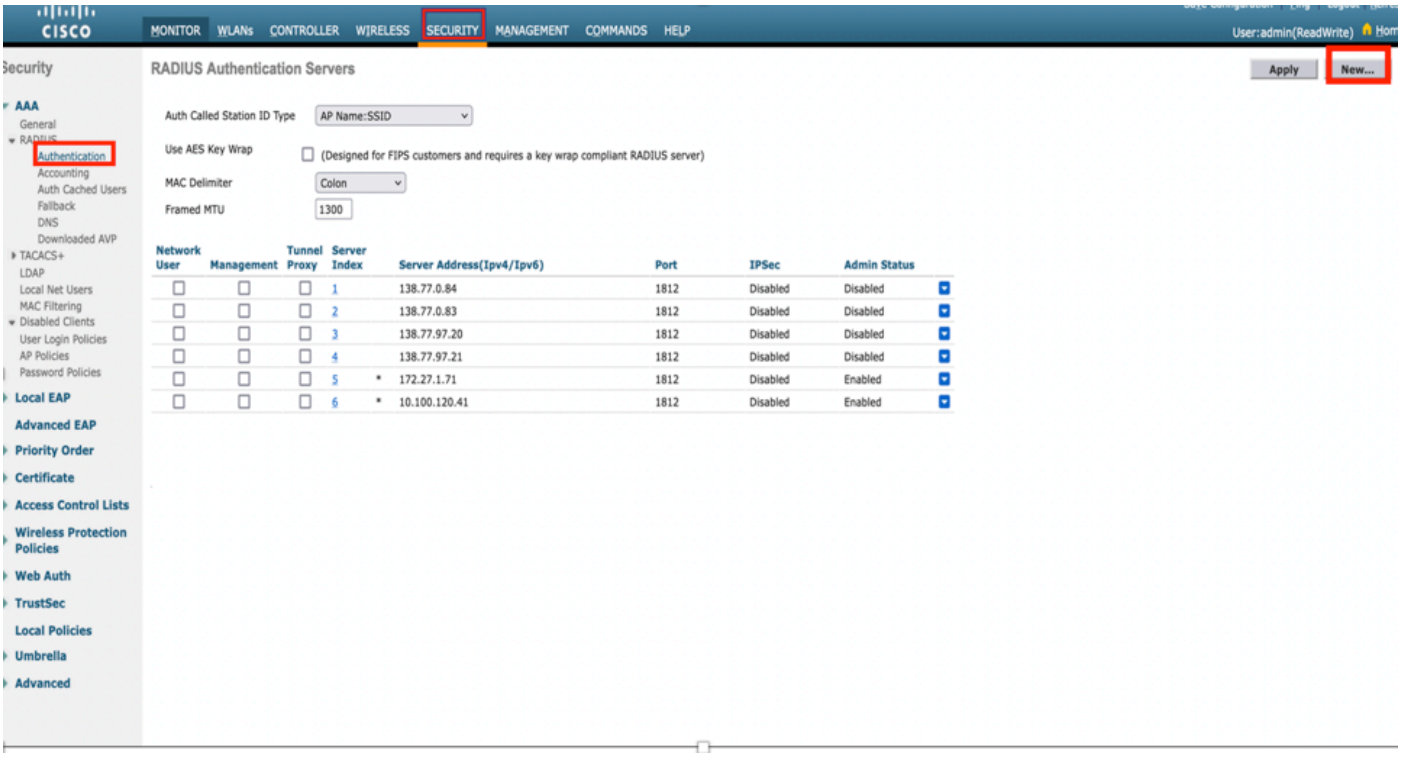
8/9.EAP-Success wordt uiteindelijk verzonden van server naar authenticator die dan wordt geplakt op de aanvrager.

Op dit punt heeft de draadloze client met EAP-TLS-enabled toegang tot het draadloze netwerk.

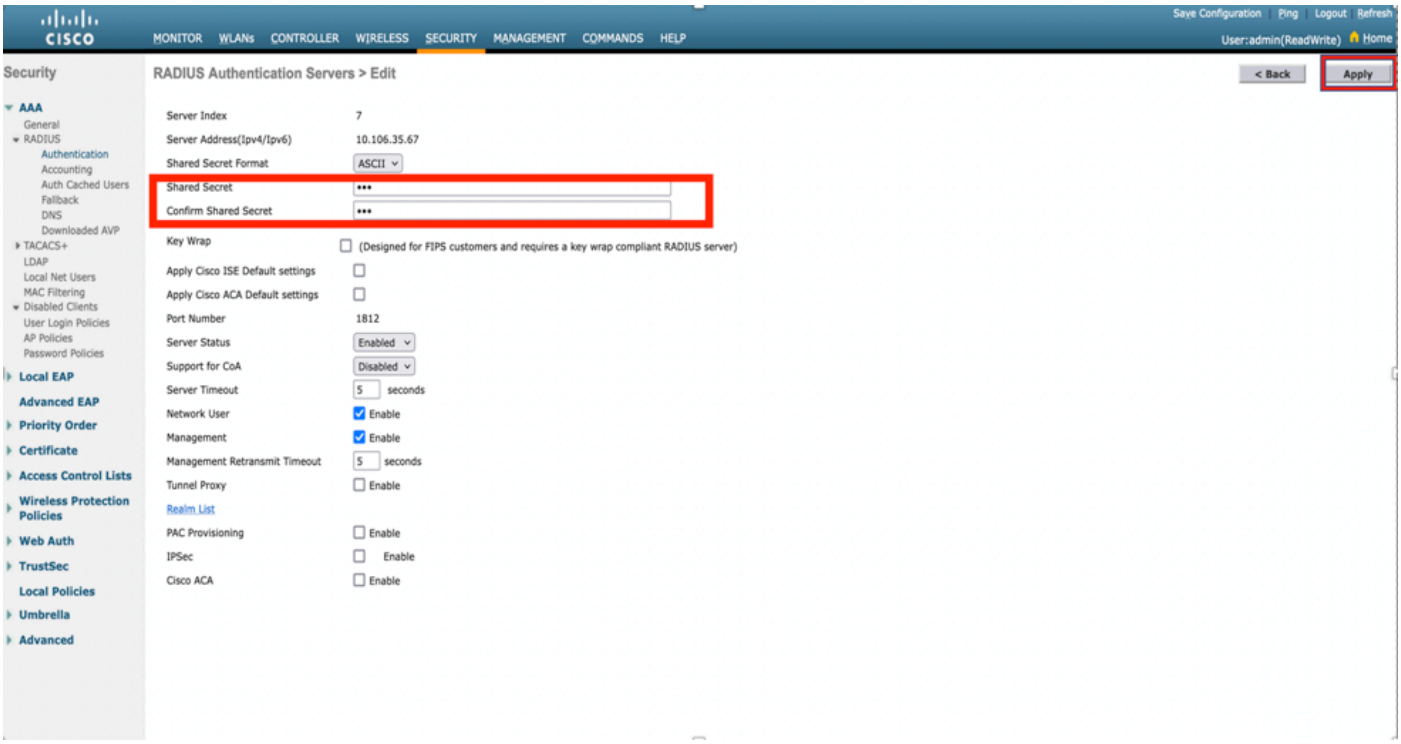
Configureren

Cisco draadloze LAN-controller

Stap 1. De eerste stap is de RADIUS-server op Cisco WLC te configureren. Als u een RADIUS-server wilt toevoegen, navigeert u naar **Security > RADIUS > Verificatie**. Klik op **Nieuw** zoals in de afbeelding.



Stap 2. Hier moet u het IP-adres en het gedeelde geheim invoeren <wachtwoord> dat wordt gebruikt om de WLC op de ISE te valideren. Klik op **Toepassen** om verder te gaan zoals in de afbeelding.

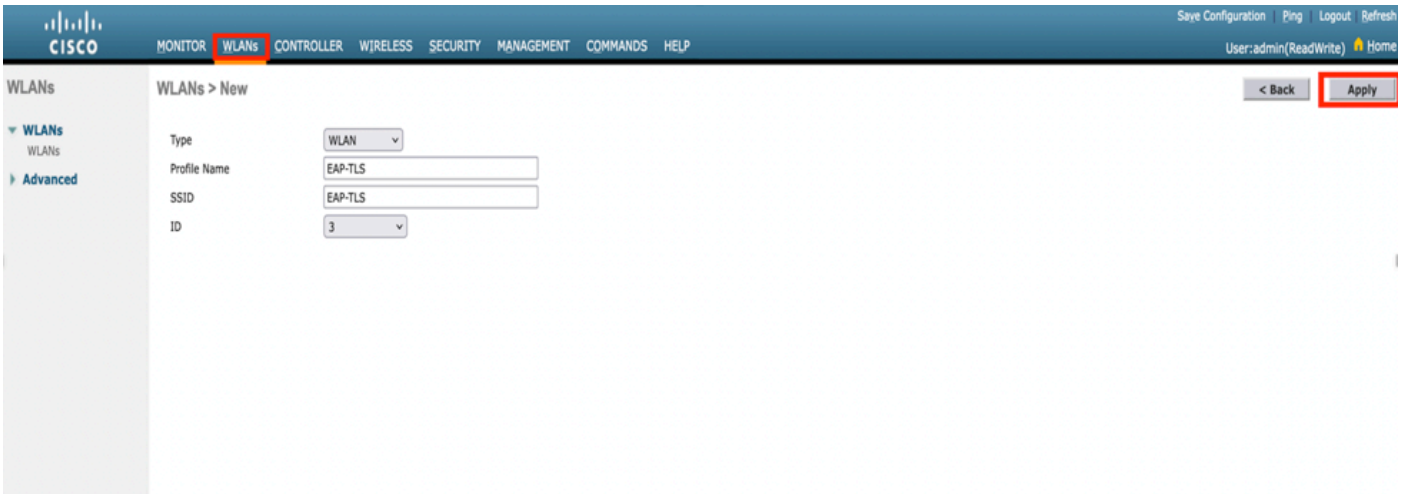


Stap 3. Maak WLAN voor RADIUS-verificatie.

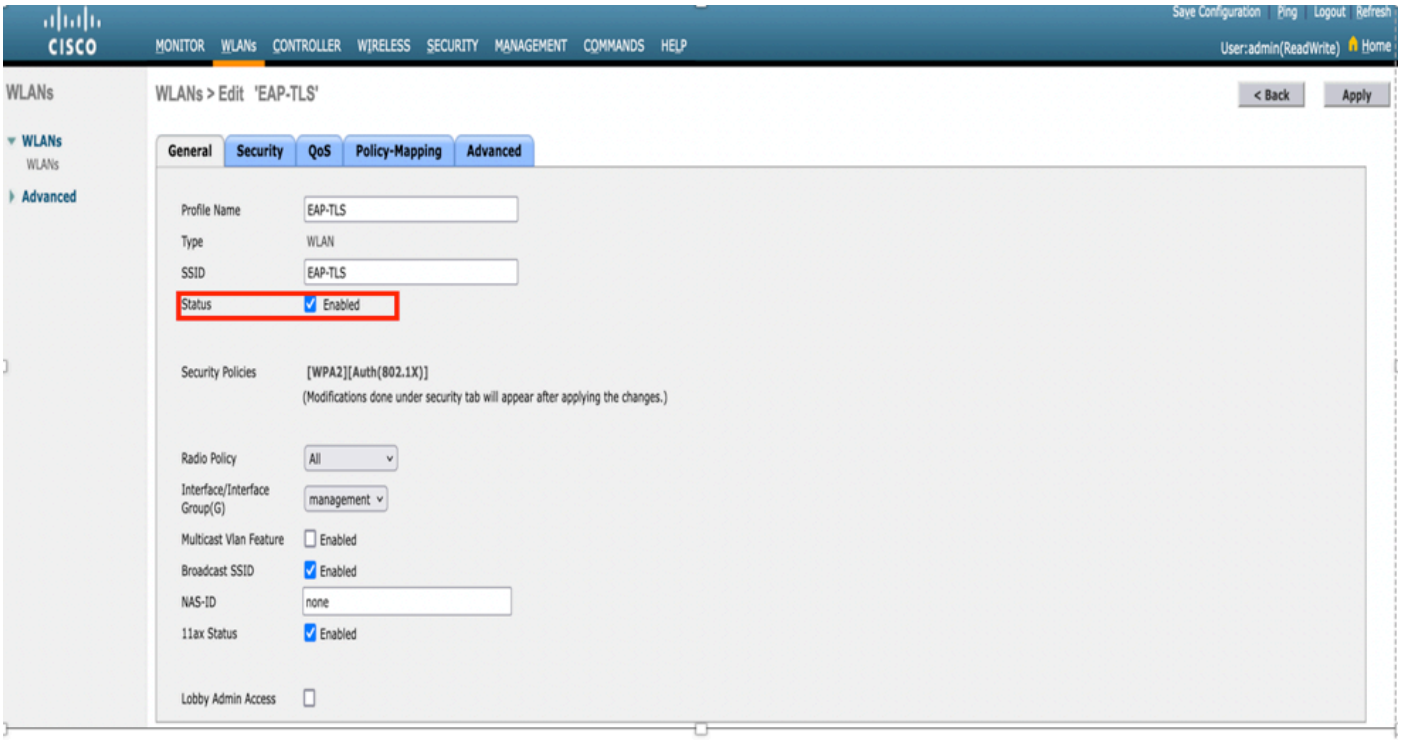
U kunt nu een nieuw WLAN maken en configureren om de WPA-enterprise-modus te gebruiken, zodat u RADIUS kunt gebruiken voor verificatie.

Stap 4. Selecteer **WLAN's** in het hoofdmenu, kies **Nieuw maken** en klik op **Ga** zoals in de afbeelding.

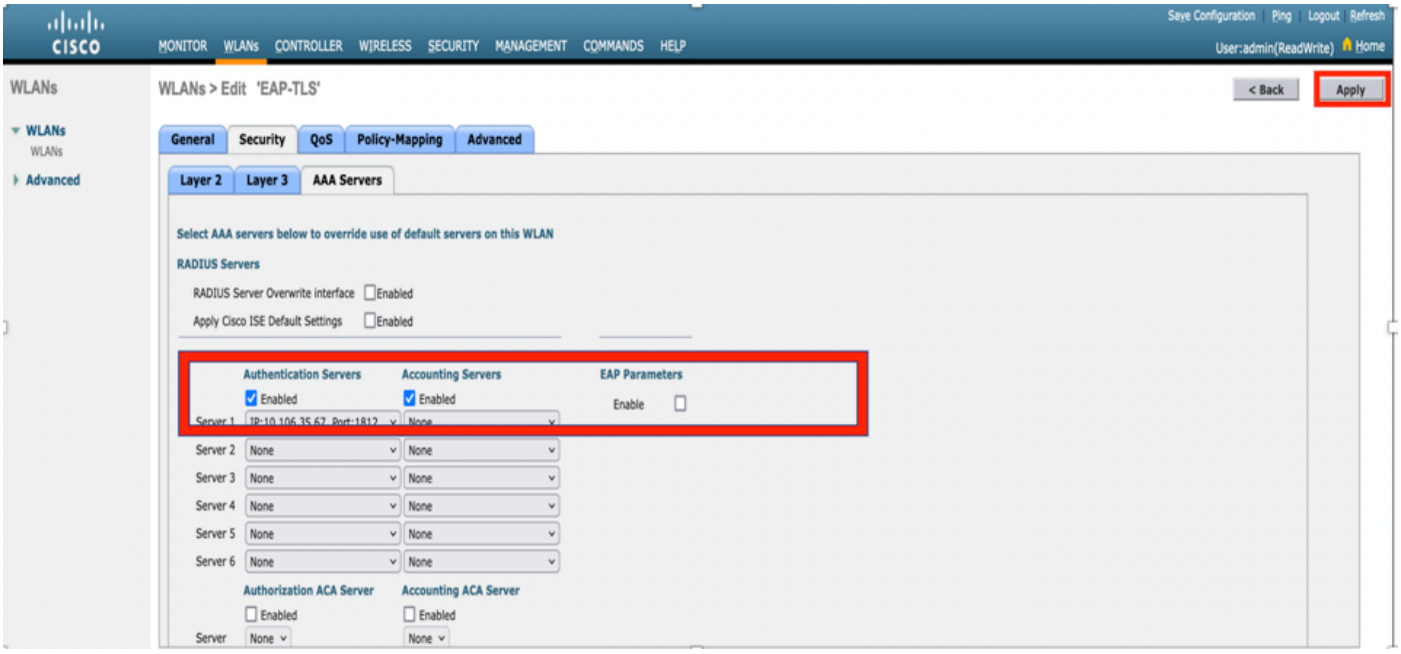
Stap 5. Geef het nieuwe WLAN **EAP-TLS een naam**. Klik op **Toepassen** om verder te gaan zoals in de afbeelding.



Stap 6. Klik op **Algemeen** en zorg ervoor dat de status **Ingeschakeld** is. Het standaardbeveiligingsbeleid is 802.1X-verificatie en WPA2 zoals in de afbeelding.



Stap 7. Navigeer nu naar het tabblad **Security > AAA-servers** en selecteer de RADIUS-server die u zojuist hebt geconfigureerd en zoals in de afbeelding.



Opmerking: Het is een goed idee om te verifiëren dat u de RADIUS-server van de WLC kunt bereiken voordat u doorgaat. RADIUS gebruikt UDP-poort 1812 (voor verificatie), zodat u er zeker van kunt zijn dat dit verkeer niet ergens in het netwerk wordt geblokkeerd.

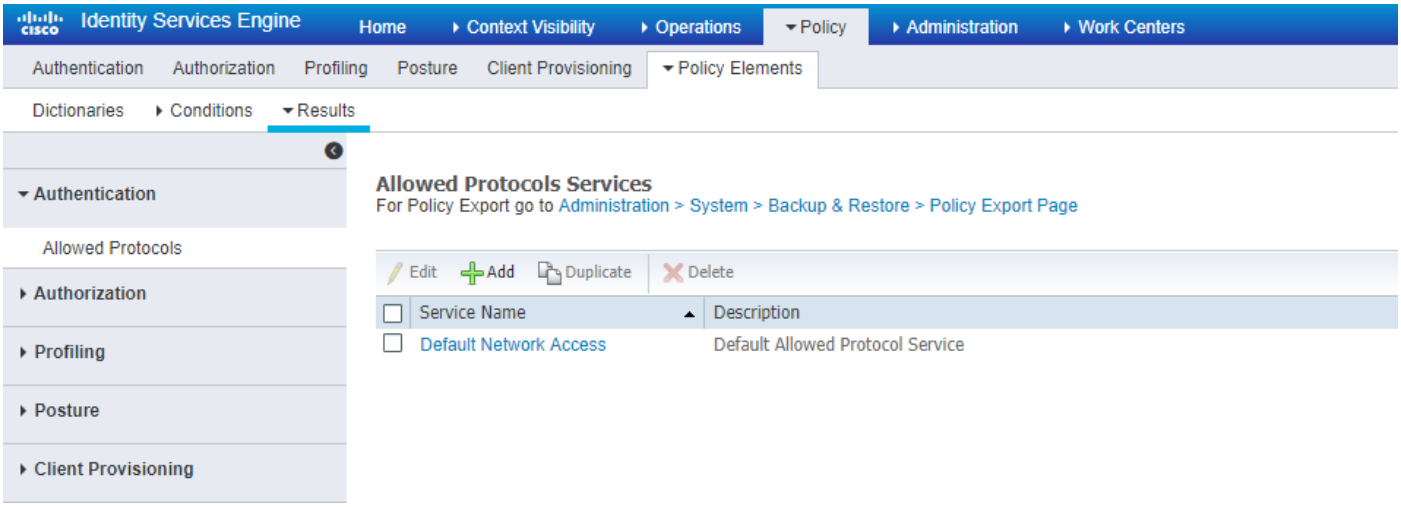
ISE-lijnkaart met Cisco WLC

EAP-TLS-instellingen

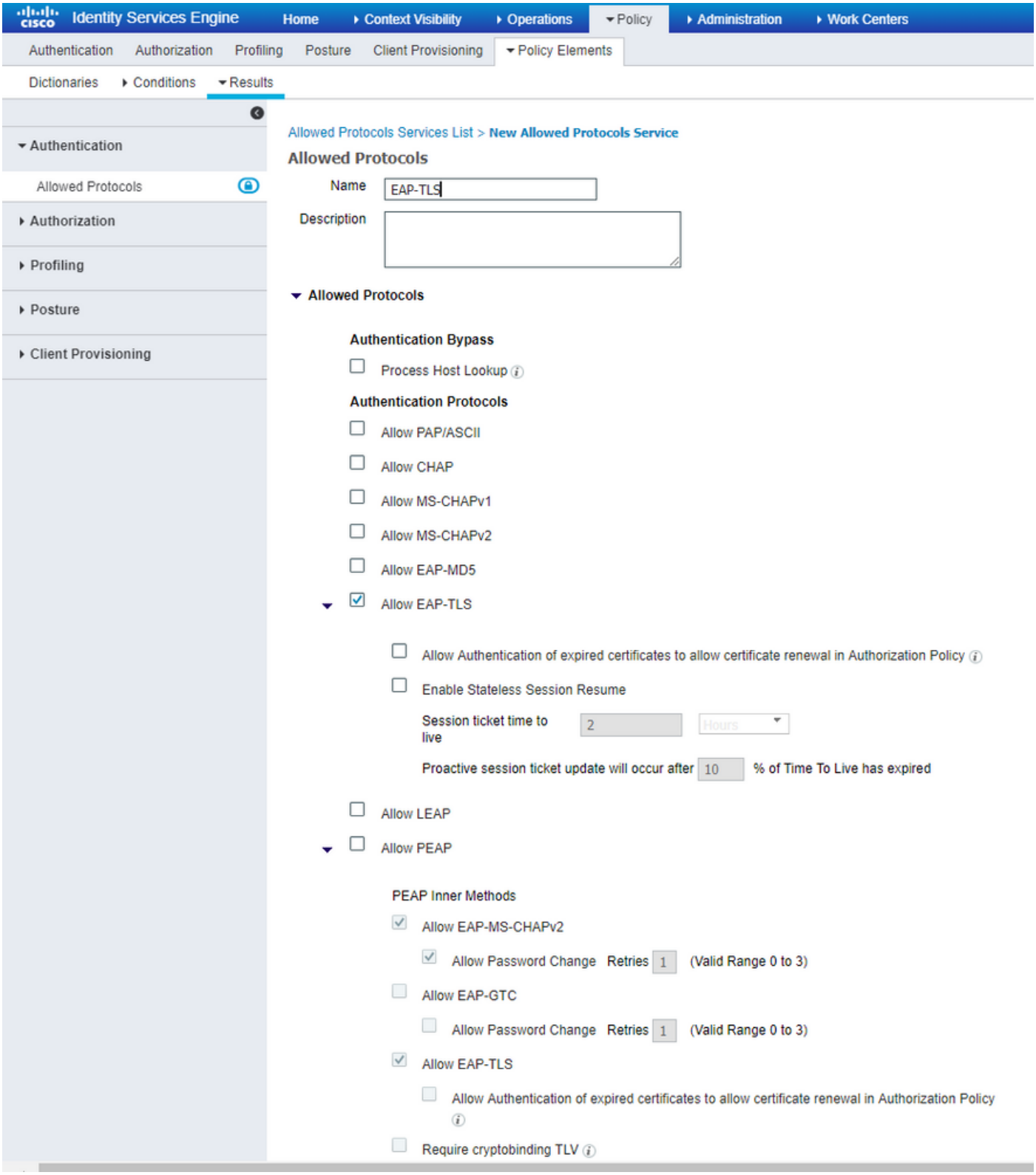
Om het beleid op te bouwen, moet u de toegestane protocollijst maken om te gebruiken in ons beleid. Aangezien een dot1x-beleid wordt geschreven, specificeert u het toegestane EAP-type op basis van de manier waarop het beleid is geconfigureerd.

Als u de standaardinstelling gebruikt, staat u de meeste EAP-typen toe voor verificatie die niet de voorkeur genieten als u de toegang tot een specifiek EAP-type moet vergrendelen.

Stap 1. Navigeer **naar Beleid > Beleidselementen > Resultaten > Verificatie > Toegestane** protocollen en **klik** op **Toevoegen** zoals in de afbeelding.

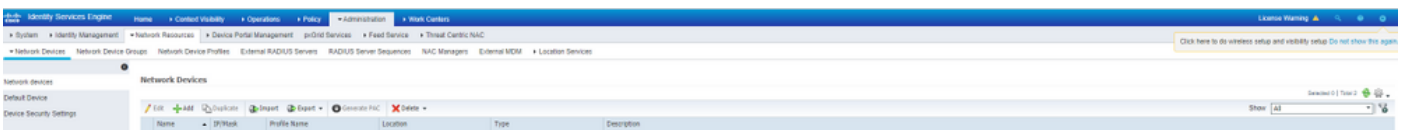


Stap 2. U kunt in deze lijst met toegestane protocollen de naam voor de lijst invoeren. In dit geval is **het** vakje **EAP-TLS toestaan** ingeschakeld en worden andere vakjes niet ingeschakeld zoals in de afbeelding.

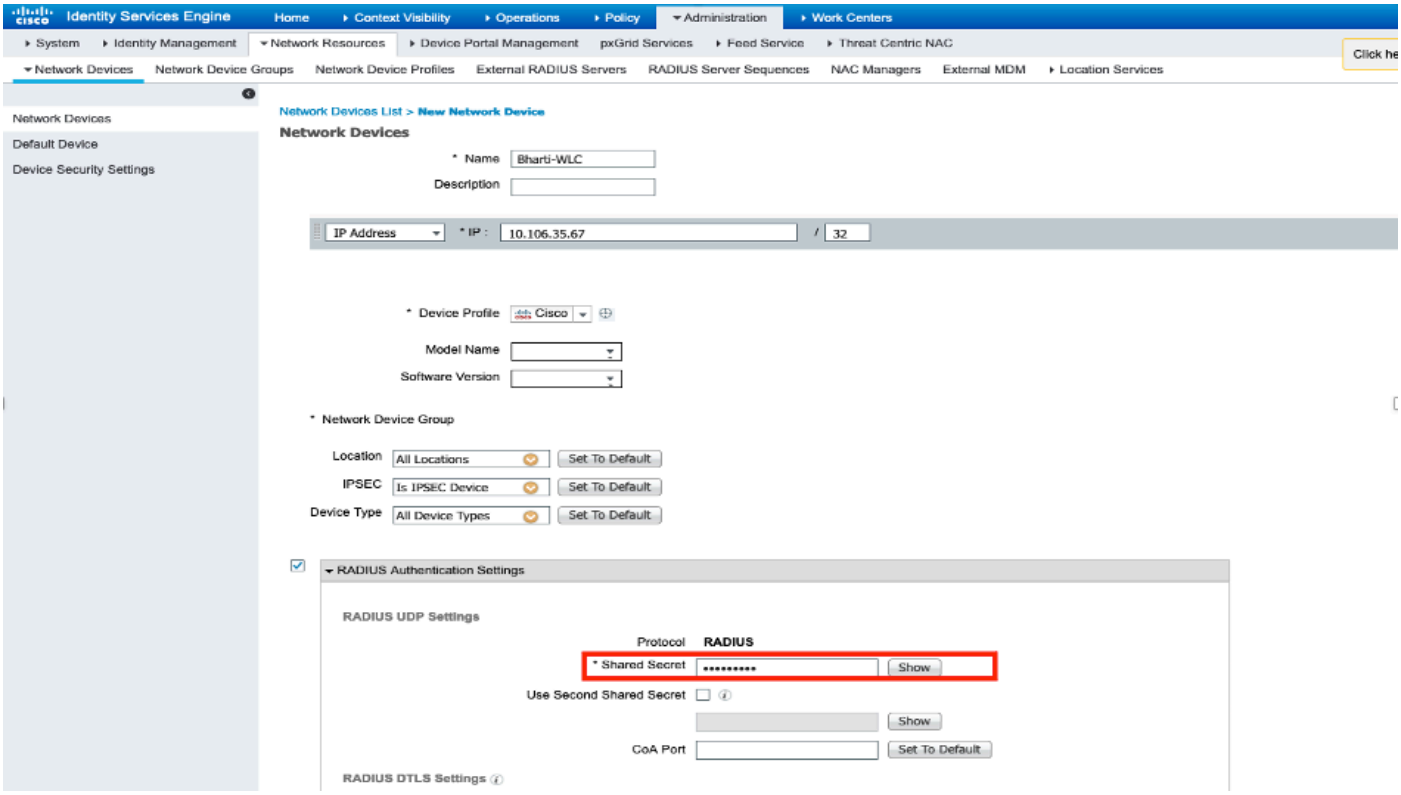


WLC-instellingen op ISE

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

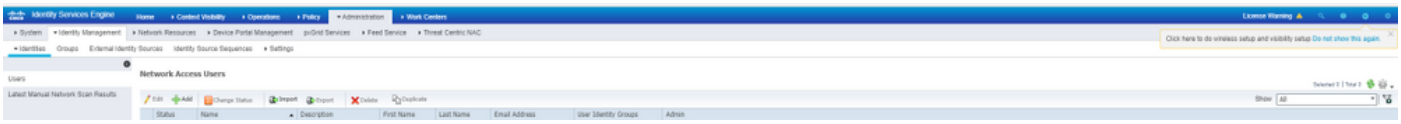


Stap 2. Voer de waarden in zoals in de afbeelding.

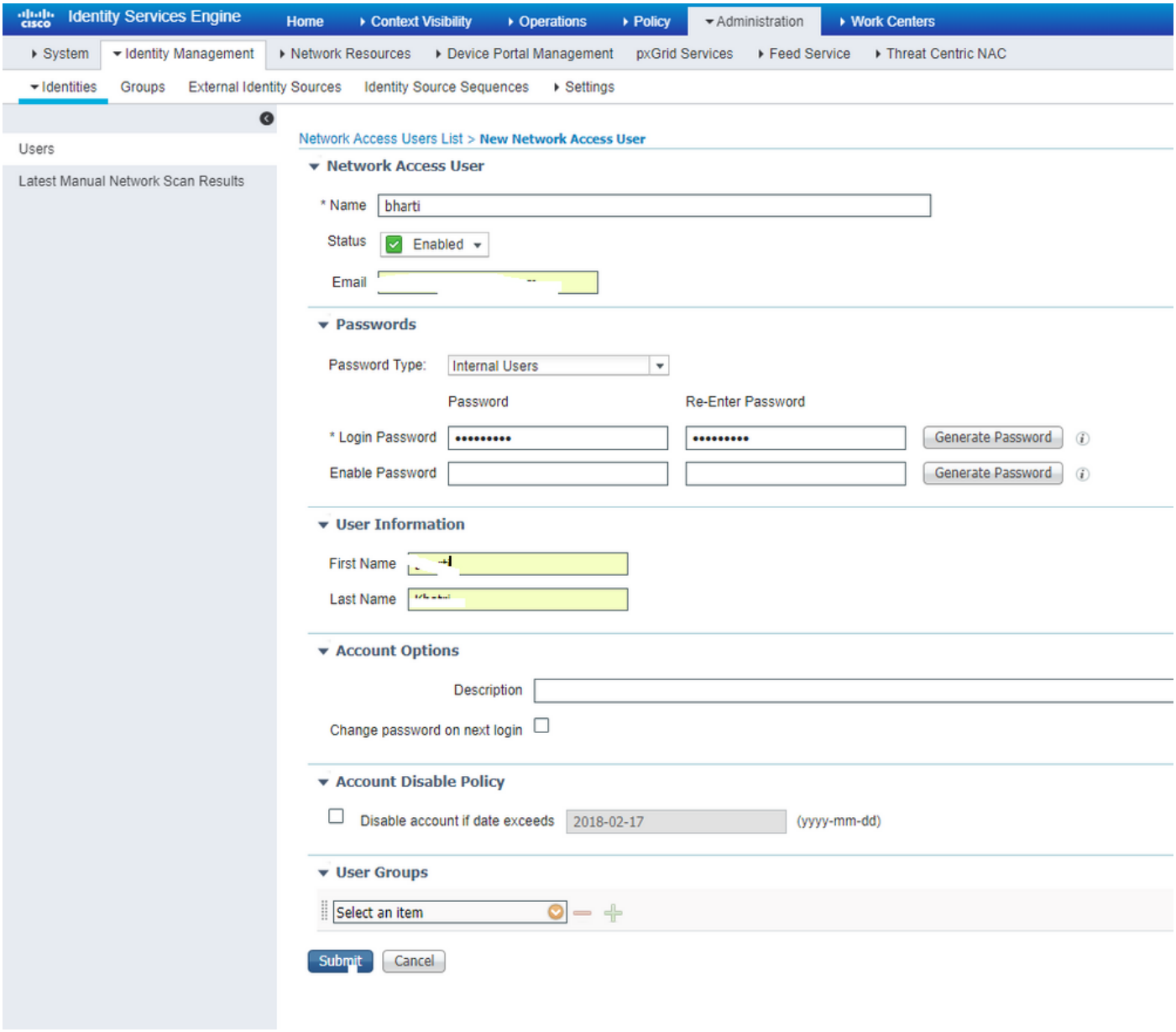


Nieuwe gebruiker maken op ISE

Stap 1. Navigeer naar **Beheer > Identity Management > Identiteiten > Gebruikers > Toevoegen** zoals in de afbeelding.



Stap 2. Voer de informatie in zoals in de afbeelding.

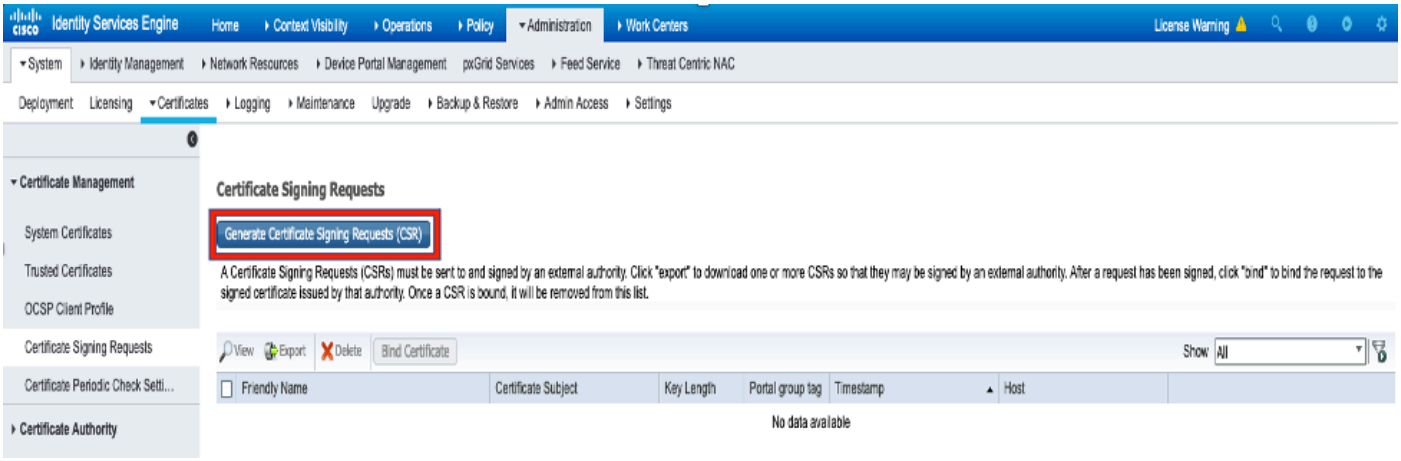


Trust Certificate op ISE

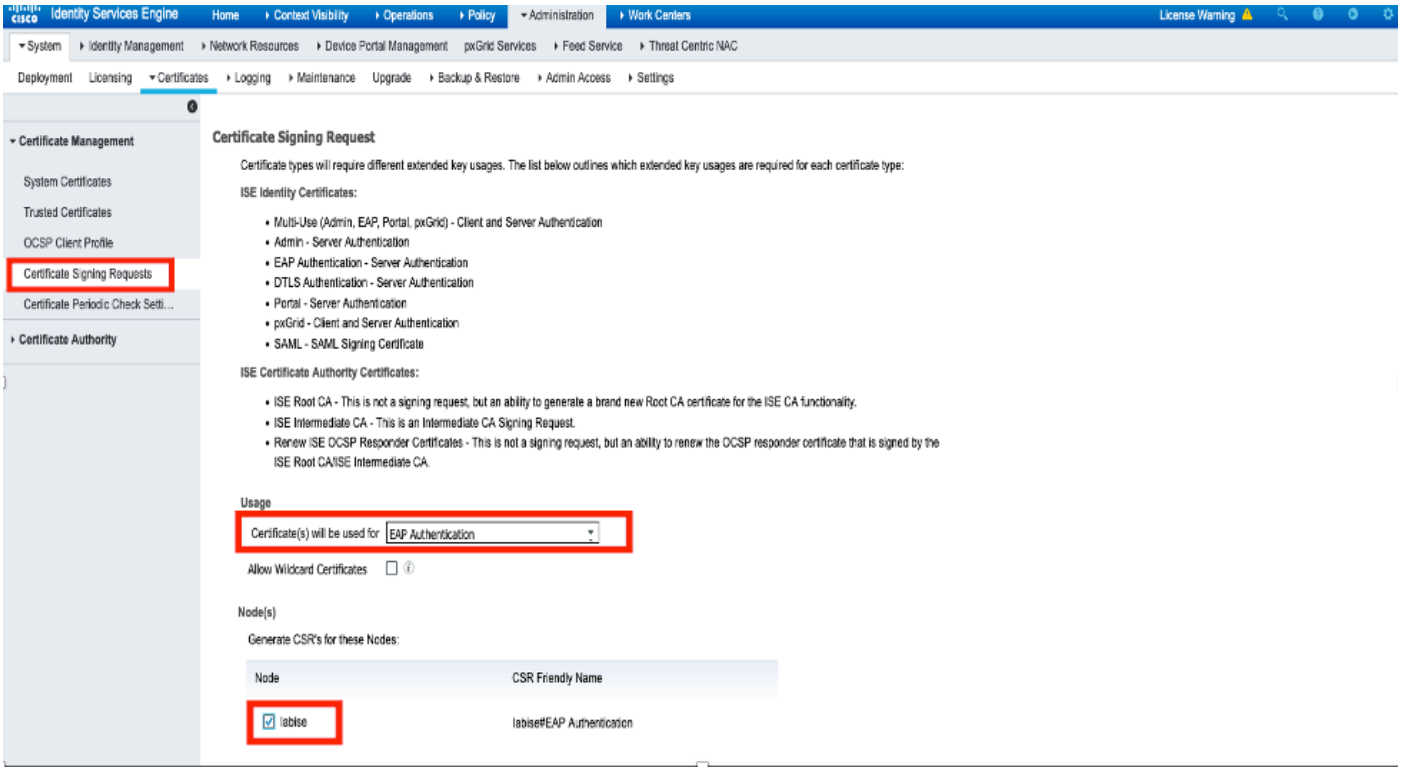
Stap 1. Navigeer naar **Beheer > Systeem > Certificaten > Certificaatbeheer > Betrouwbare certificaten**.

Klik op **Importeren** om een certificaat te importeren naar ISE. Zodra u een WLC toevoegt en een gebruiker aanmaakt op ISE, moet u het belangrijkste deel van EAP-TLS doen dat is het vertrouwen op het certificaat op ISE. Daarvoor moeten we MVO ontwikkelen.

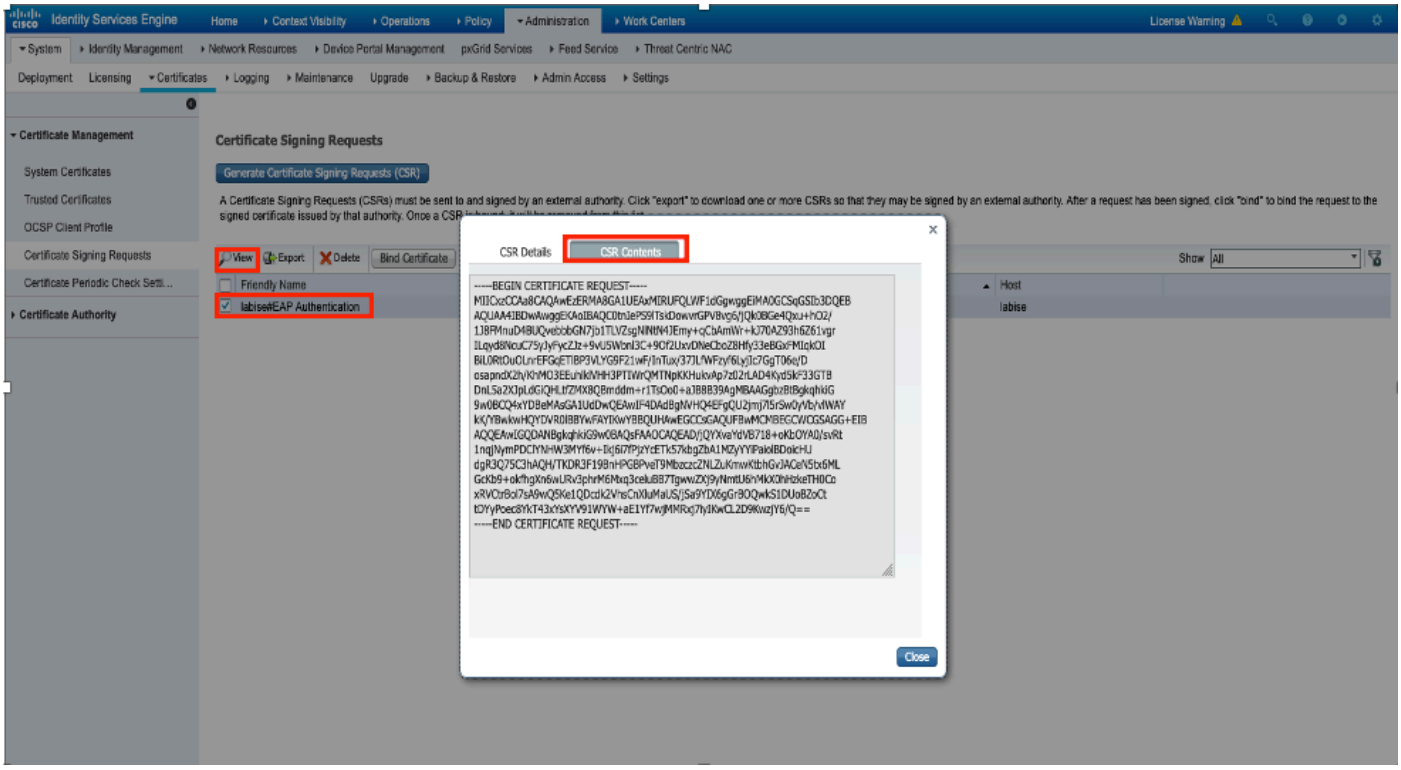
Stap 2. Navigeer naar **Beheer > Certificaten > Verzoeken voor certificaatondertekening > Verzoeken voor certificaatondertekening genereren (CSR)** zoals in de afbeelding.



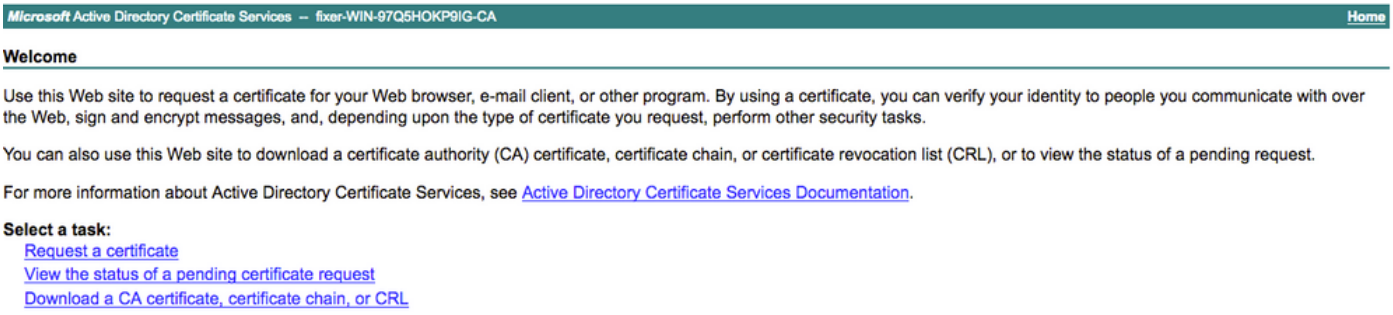
Stap 3. Om MVO te genereren, navigeer naar **Gebruik** en selecteer **EAP-verificatie** zoals in de afbeelding **wordt gebruikt voor** uitrolopties.



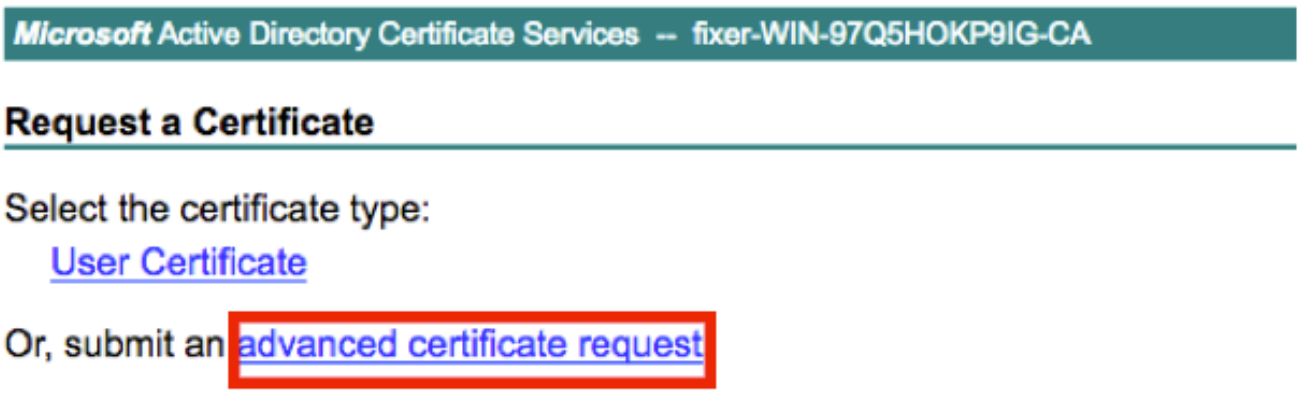
Stap 4. De op ISE gegenereerde MVO kan worden bekeken. Klik op **Weergeven** zoals in de afbeelding.



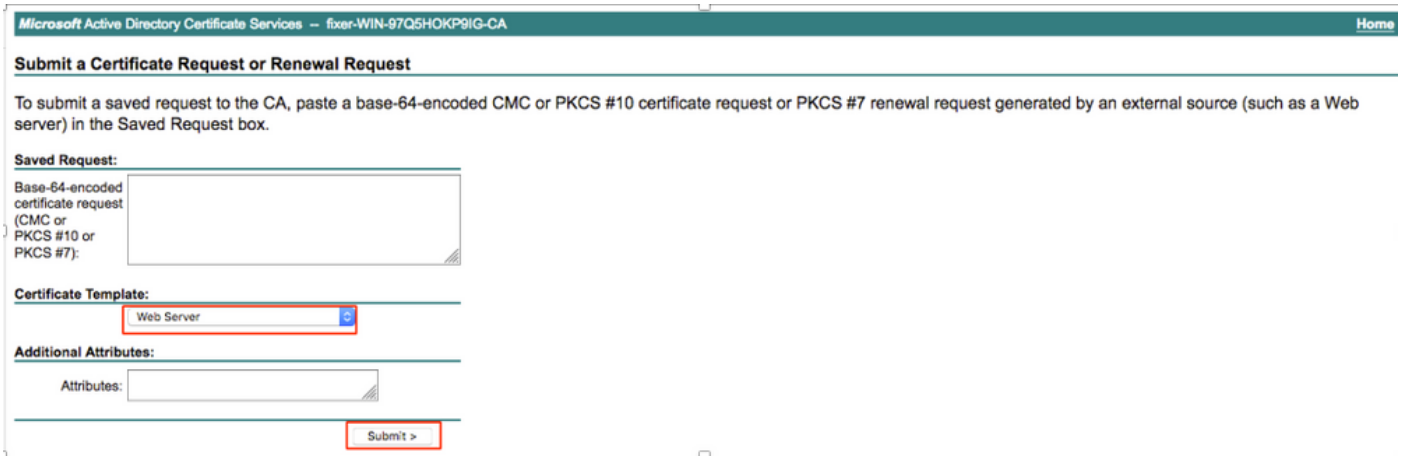
Stap 5. Nadat CSR is gegenereerd, bladert u naar de CA-server en klikt u op **Certificaat aanvragen** zoals in de afbeelding:



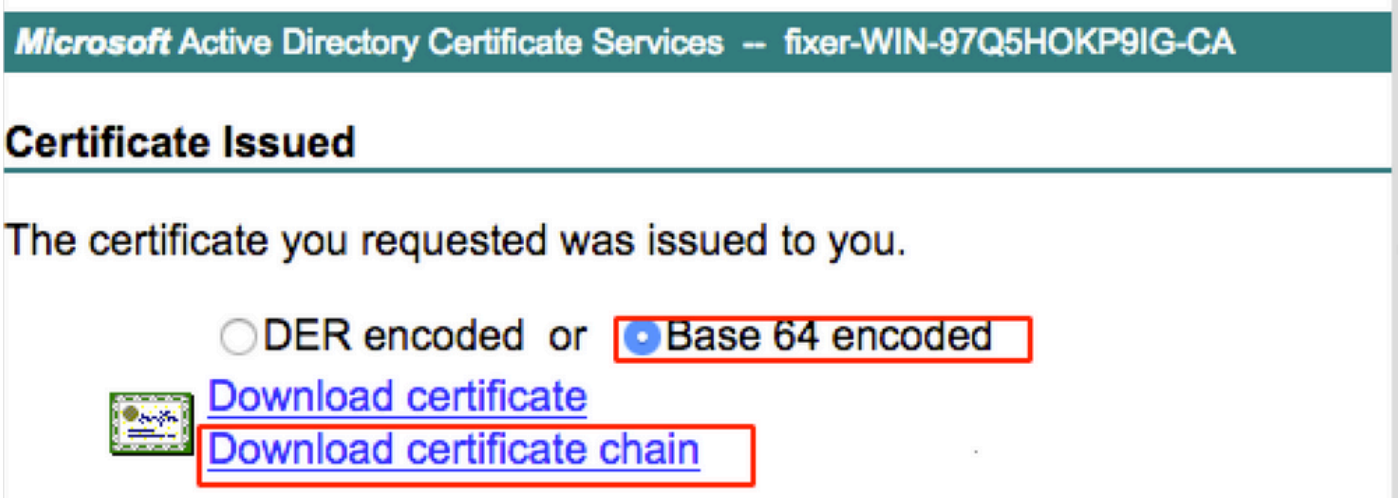
Stap 6. Zodra u een certificaat aanvraagt, krijgt u opties voor **gebruikerscertificaat** en **geavanceerde certificaataanvraag**, klikt u op **Geavanceerd certificaatverzoek** zoals in de afbeelding.



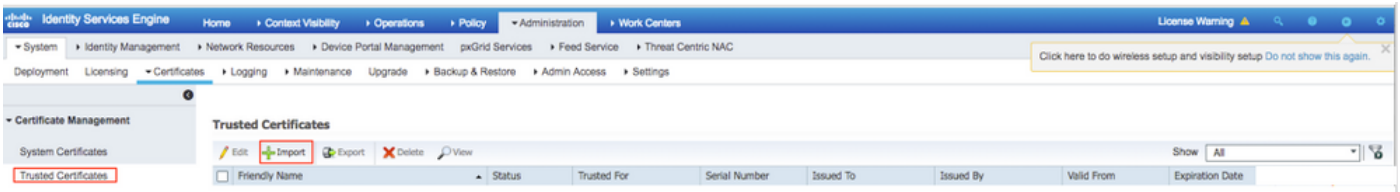
Stap 7. Plakt de CSR die in **Base-64 gecodeerde certificaataanvraag is** gegenereerd. Van de **certificaatsjabloon:** Kies **Webserver** en klik op **Indienen** zoals in de afbeelding.

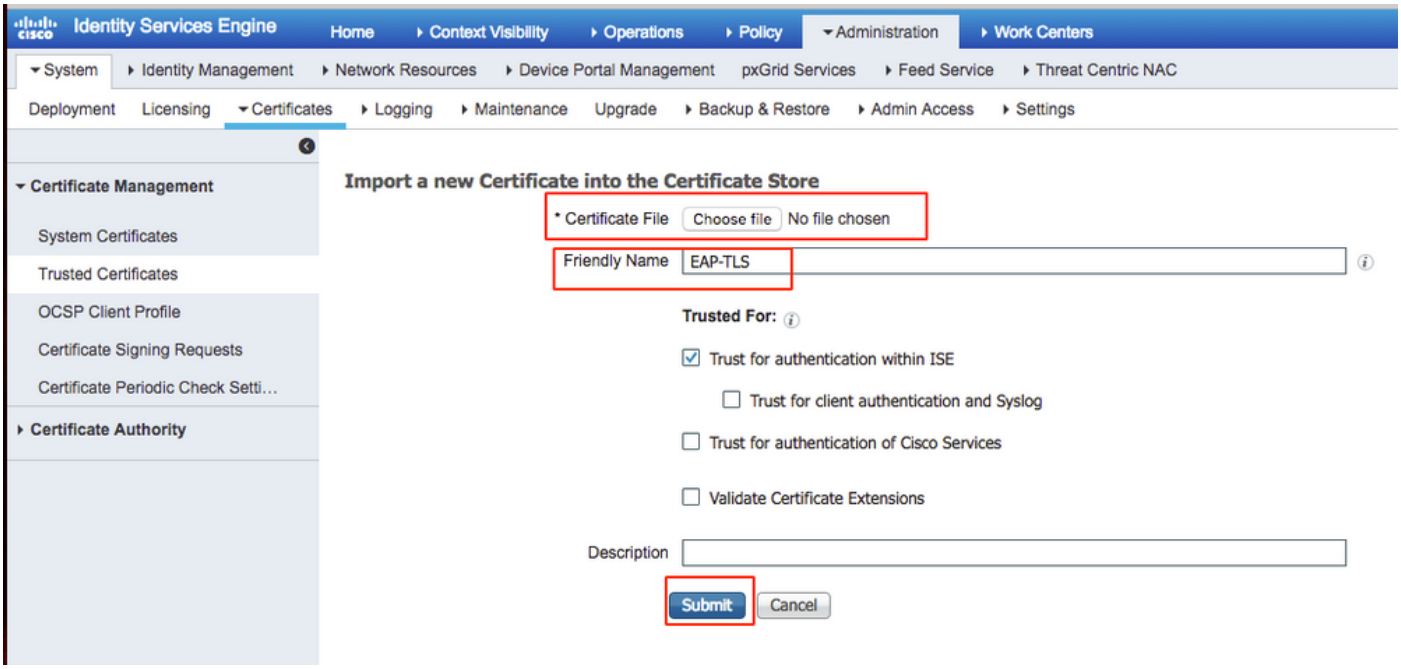


Stap 8. Zodra u op **Indienen** klikt, krijgt u de optie om het type certificaat te selecteren, **Base-64 encoded** te selecteren en te klikken op **Certificaatketen downloaden** zoals in de afbeelding.

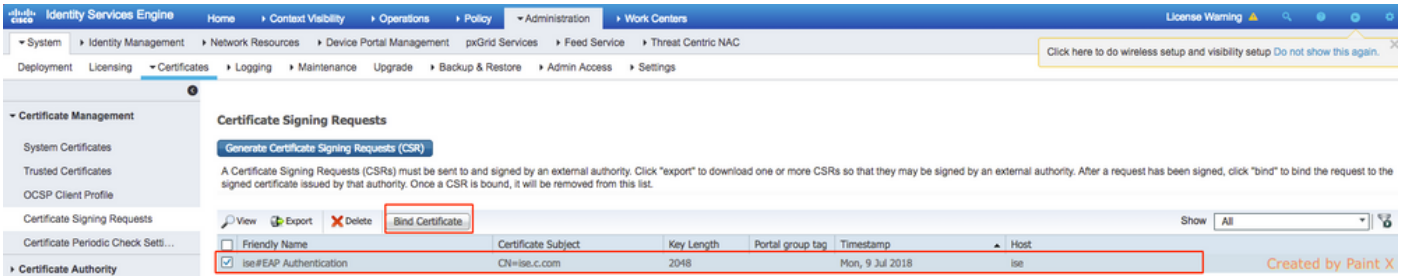


Stap 9. De certificaatdownload is voltooid voor de ISE-server. U kunt het certificaat halen, het certificaat bevat twee certificaten, een wortelcertificaat en ander tussenproduct. Het basiscertificaat kan worden geïmporteerd onder **Beheer > Certificaten > Betrouwbare certificaten > Importeren** zoals in de afbeeldingen wordt getoond.

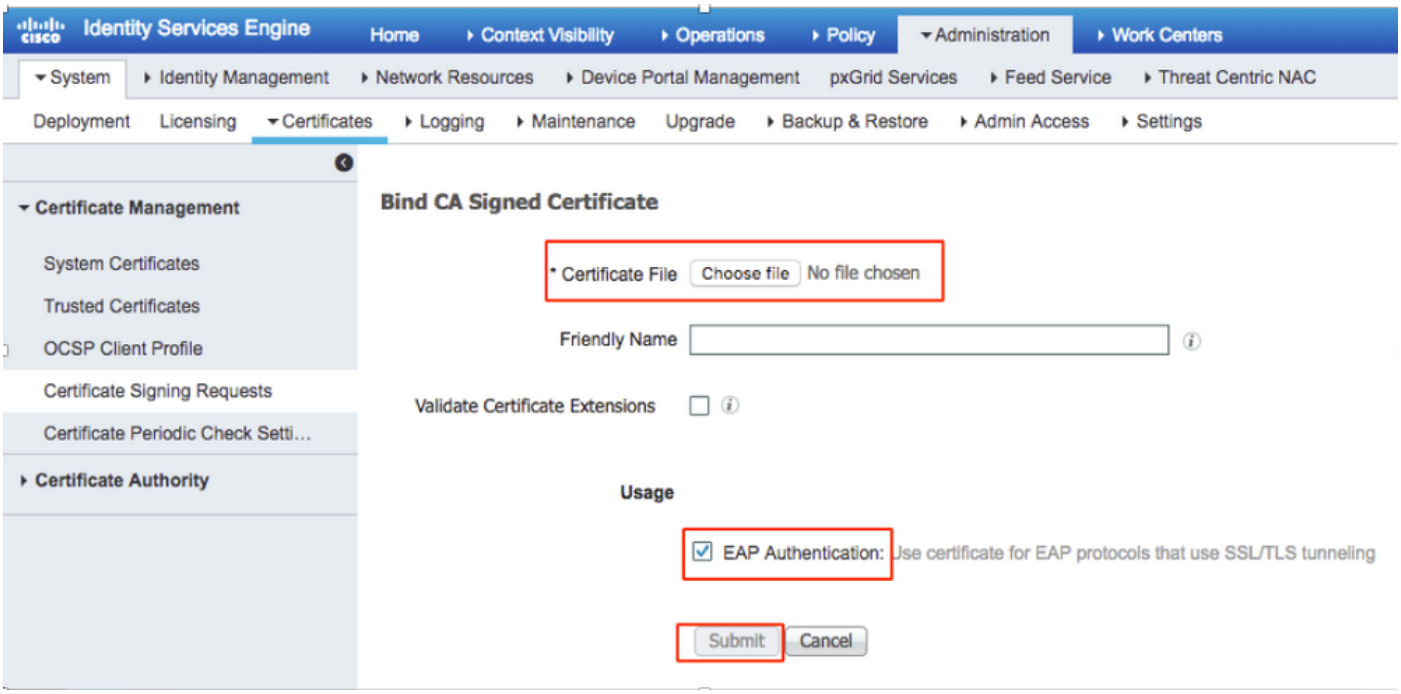




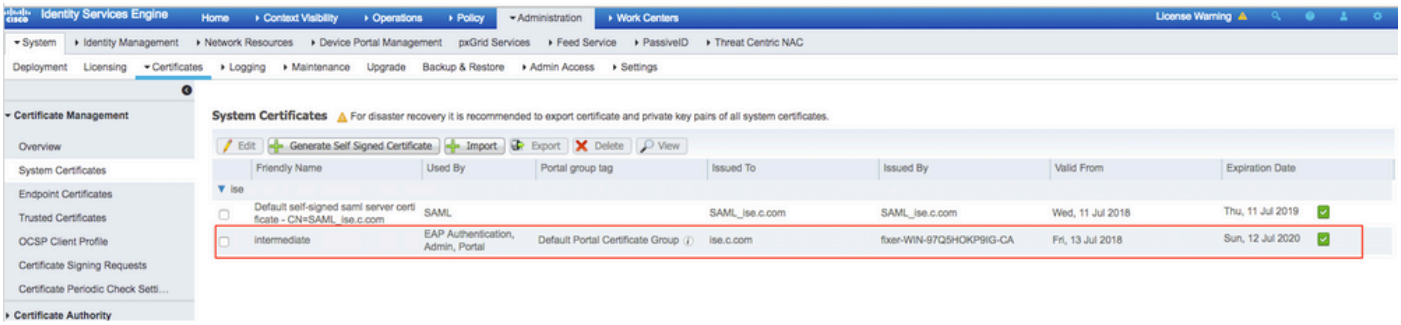
Stap 10. Zodra u op **Indienen** klikt, wordt het certificaat toegevoegd aan de lijst met vertrouwde certificaten. Ook is het tussentijds certificaat nodig om te kunnen binden met MVO zoals weergegeven in de afbeelding.



Stap 11. Zodra u op **Bind certificaat** klikt, is er een optie om het certificaatbestand te kiezen dat op uw bureaublad is opgeslagen. Blader naar het tussenliggende certificaat en klik op **Indienen** zoals in de afbeelding.



Stap 12. Ga om het certificaat te bekijken naar **Beheer > Certificaten > Systeemcertificaten** zoals in de afbeelding.



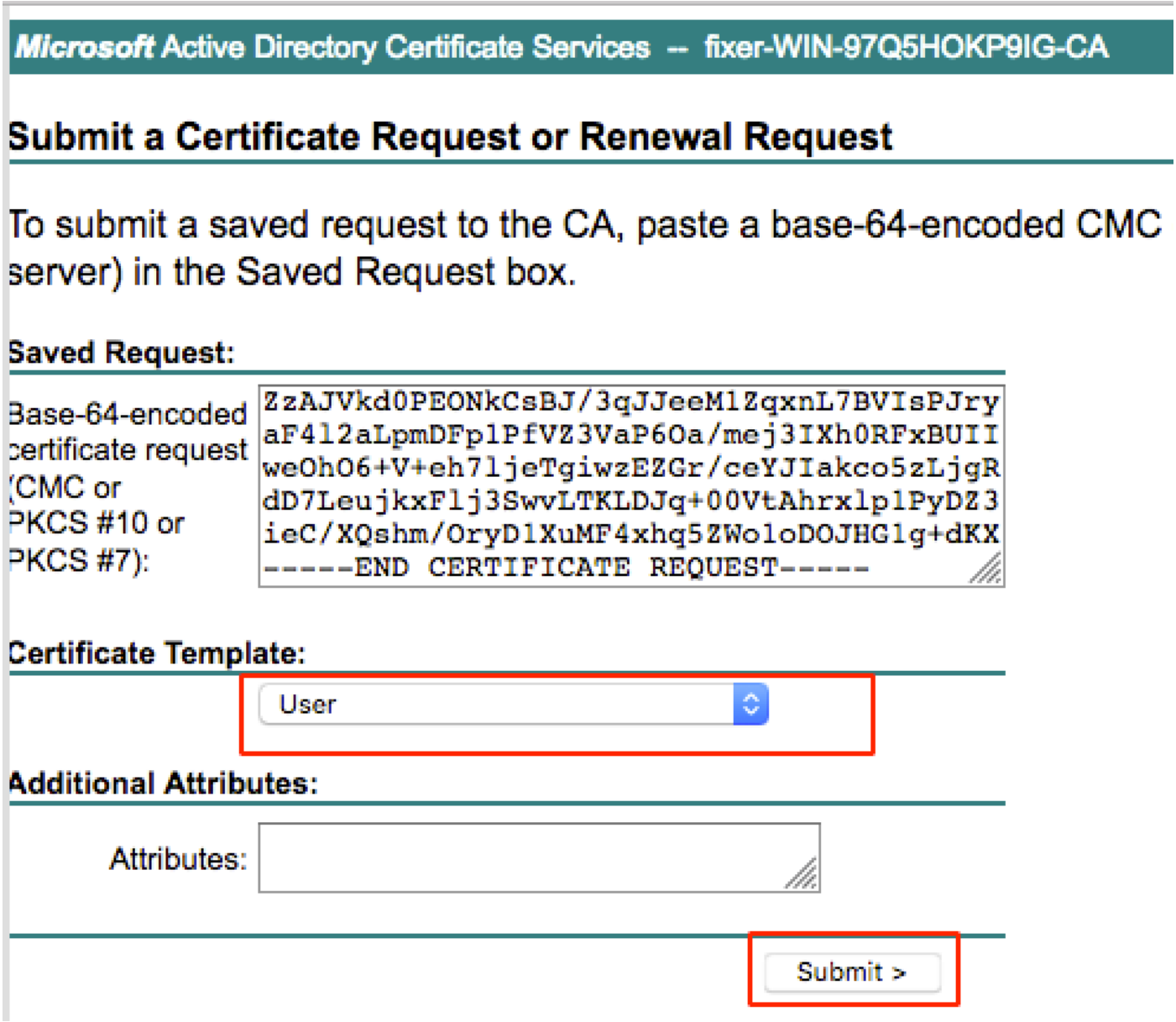
Client voor EAP-TLS

Gebruikerscertificaat downloaden op clientmachine (Windows bureaublad)

Stap 1. Om een draadloze gebruiker te authenticeren via EAP-TLS, moet u een clientcertificaat genereren. Sluit uw Windows-computer aan op het netwerk zodat u toegang hebt tot de server. Open een webbrowser en voer dit adres in: https://sever IP-adres/certsrv—

Stap 2. Merk op dat CA het zelfde moet zijn waarmee het certificaat voor ISE werd gedownload.

Hiervoor moet u bladeren naar dezelfde CA-server die u hebt gebruikt om het certificaat voor de server te downloaden. Op dezelfde CA, klik op **Certificaat aanvragen** zoals eerder gedaan, maar deze keer moet u **Gebruiker** als Certificaatsjabloon selecteren zoals in de afbeelding.



Stap 3. Klik vervolgens op **de certificaatketen downloaden**, zoals eerder voor de server is gedaan.

Zodra u de certificaten krijgt, volg deze stappen om het certificaat op Windows laptop te importeren:

Stap 4. U moet het certificaat openen vanuit de Microsoft Management Console (MMC) om het te kunnen importeren.

1. Om de MMC te openen, navigeert u naar **Start > Uitvoeren > MMC**.
2. Naar **bestand** navigeren **> Magnetisch toevoegen / verwijderen**
3. Dubbelklik op **Certificaten**.
4. **Selecteer Computeraccount**.
5. Selecteer **Lokale computer > Voltooien**
6. Klik op **OK** om het venster Snap-In te verlaten.
7. Klik op **[+]** naast **Certificaten > Persoonlijk > Certificaten**.
8. Klik met de rechtermuisknop op **Certificaten** en selecteer **Alle taken > Importeren**.
9. Klik op **Next** (Volgende).
10. Klik op **Bladeren**.
11. Selecteer de **.cer, .crt of .pfx** die u wilt importeren.

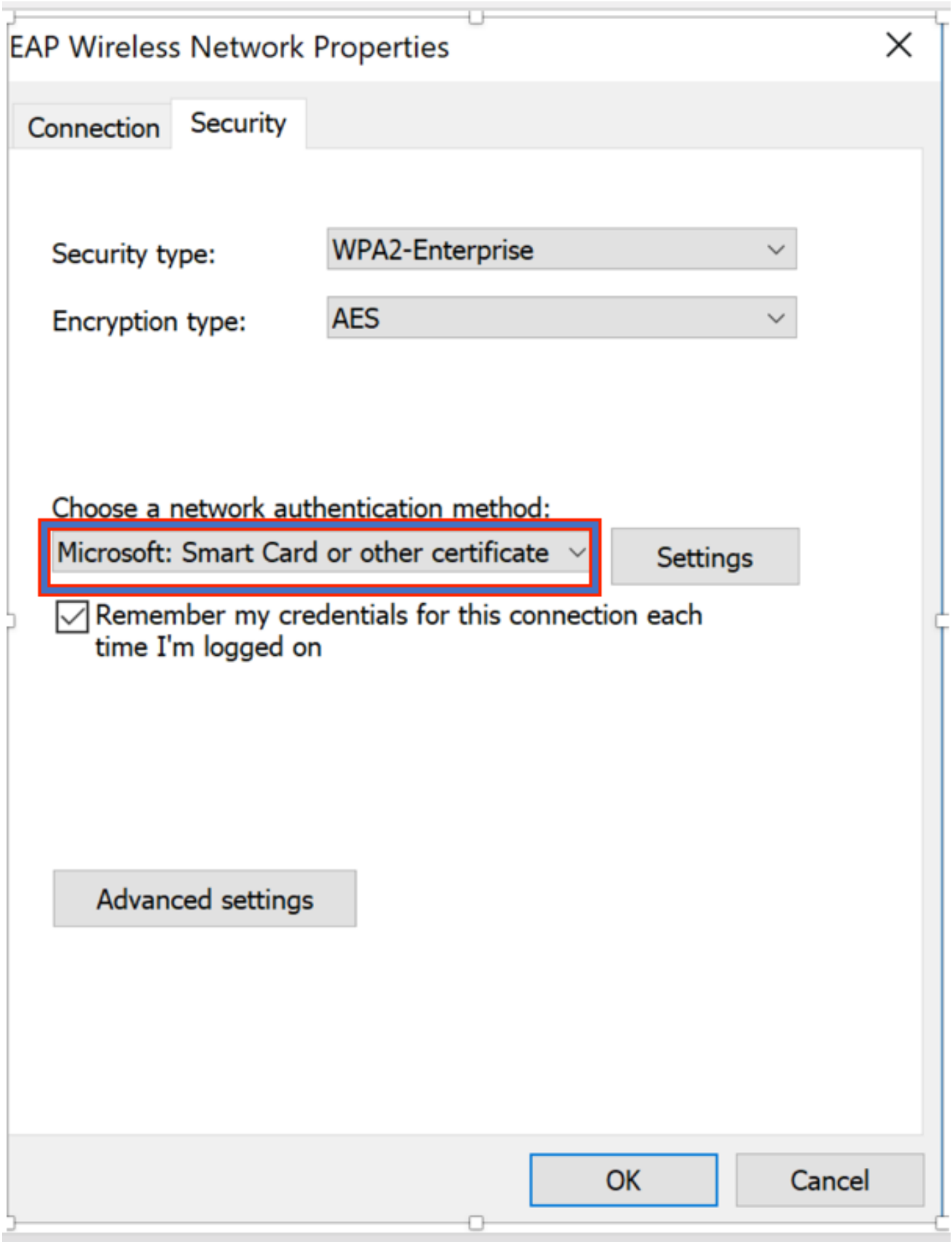
12. Klik op **Openen**.
13. Klik op **Next** (Volgende).
14. Selecteer **Automatisch het certificaatarchief selecteren op basis van het type certificaat**.
15. Klik op **Voltooien & OK**

Zodra de invoer van certificaat is gedaan, moet u uw draadloze client (Windows-bureaublad in dit voorbeeld) configureren voor EAP-TLS.

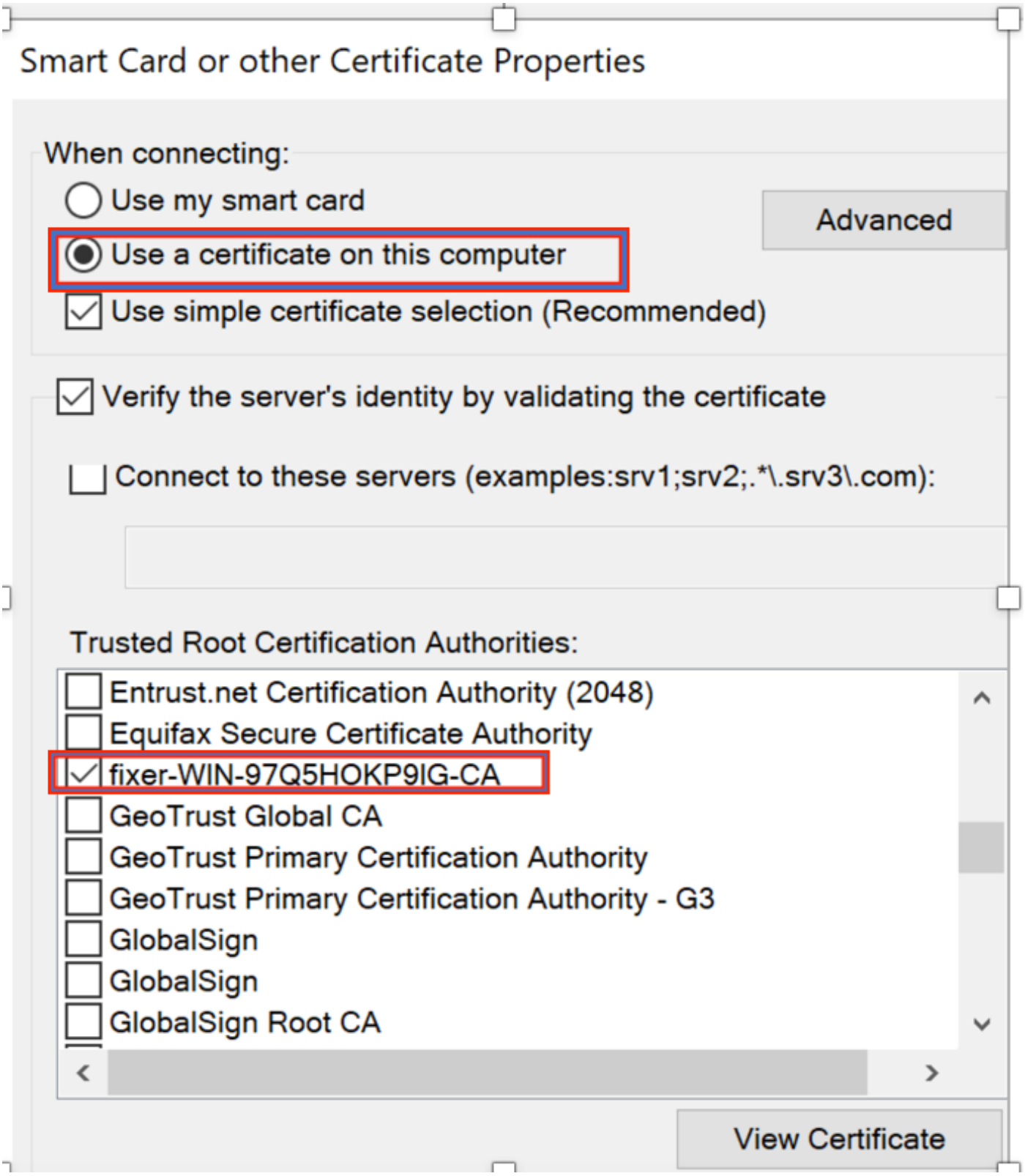
Draadloos profiel voor EAP-TLS

Stap 1. Wijzig het draadloze profiel dat eerder voor Protected Extensible Verification Protocol (PEAP) is gemaakt om in plaats daarvan de EAP-TLS te gebruiken. Klik op **EAP Wireless-profiel**.

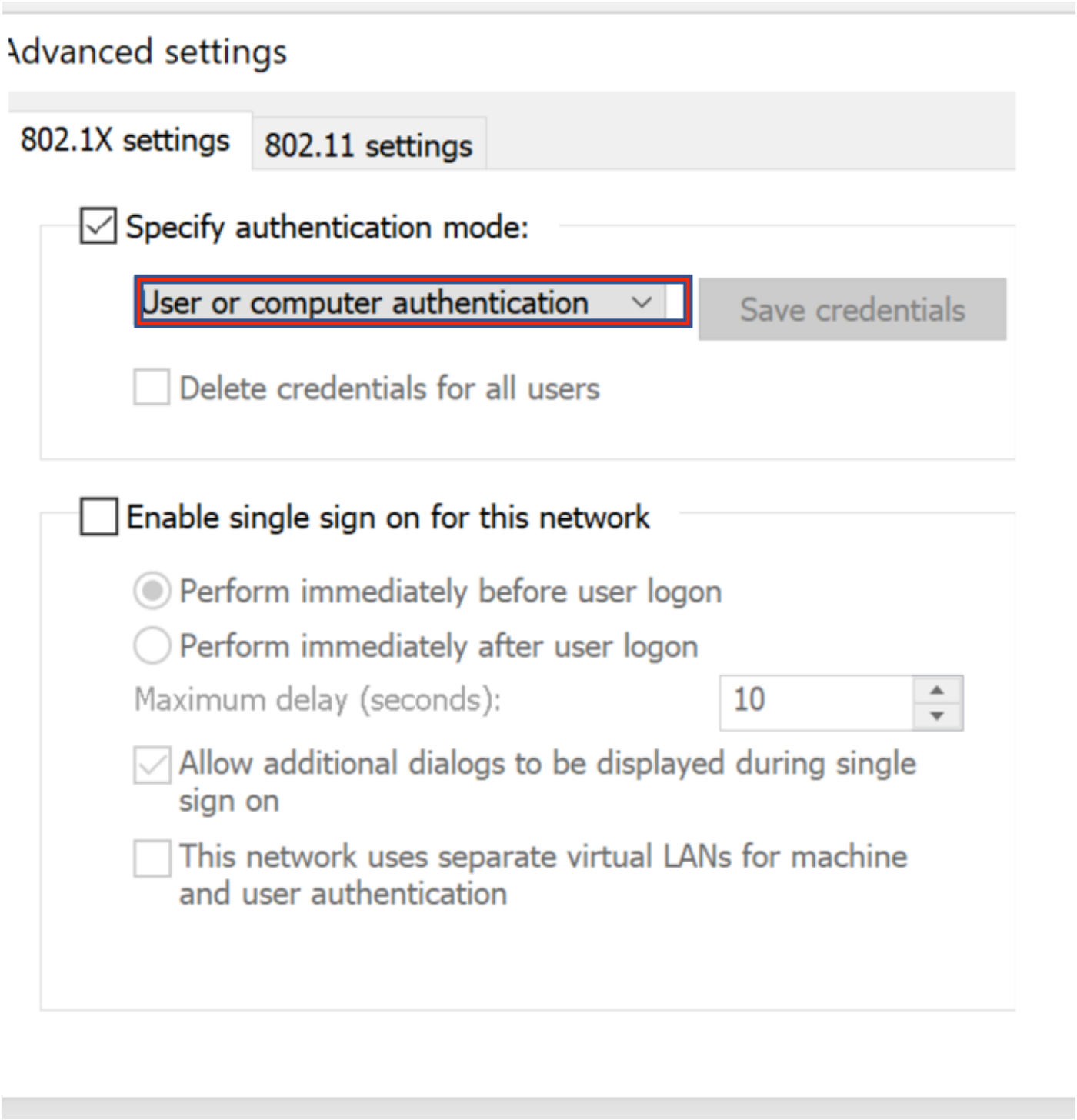
Stap 2. Selecteer **Microsoft: Slimme kaart of ander certificaat** en klik op **OK** in de afbeelding.



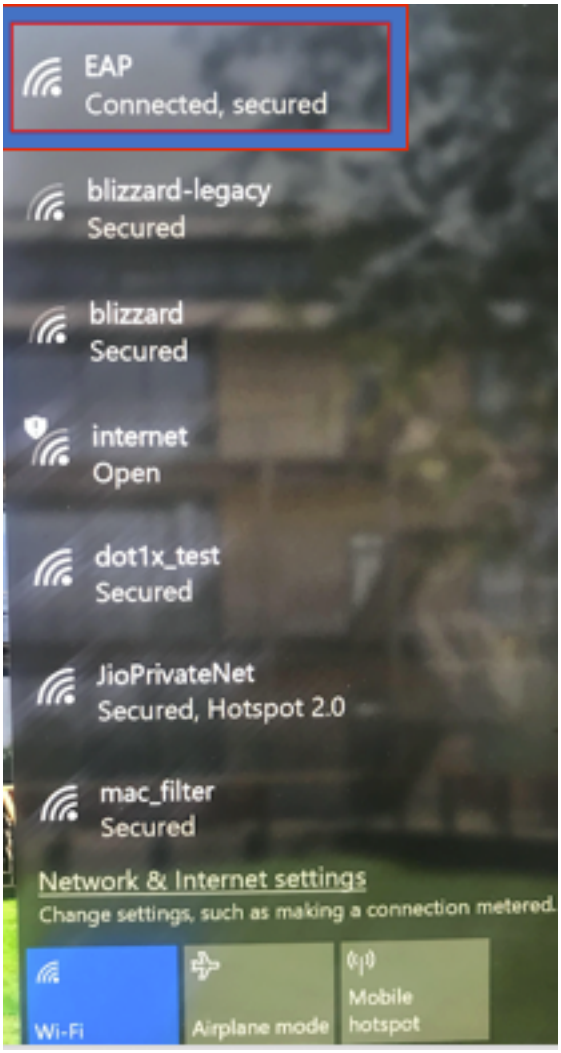
Stap 3. Klik op **instellingen** en selecteer het basiscertificaat dat is afgegeven vanaf een CA-server zoals in de afbeelding.



Stap 4. Klik op **Geavanceerde instellingen** en selecteer **Gebruiker- of computerverificatie** op het tabblad 802.1x-instellingen zoals in de afbeelding.



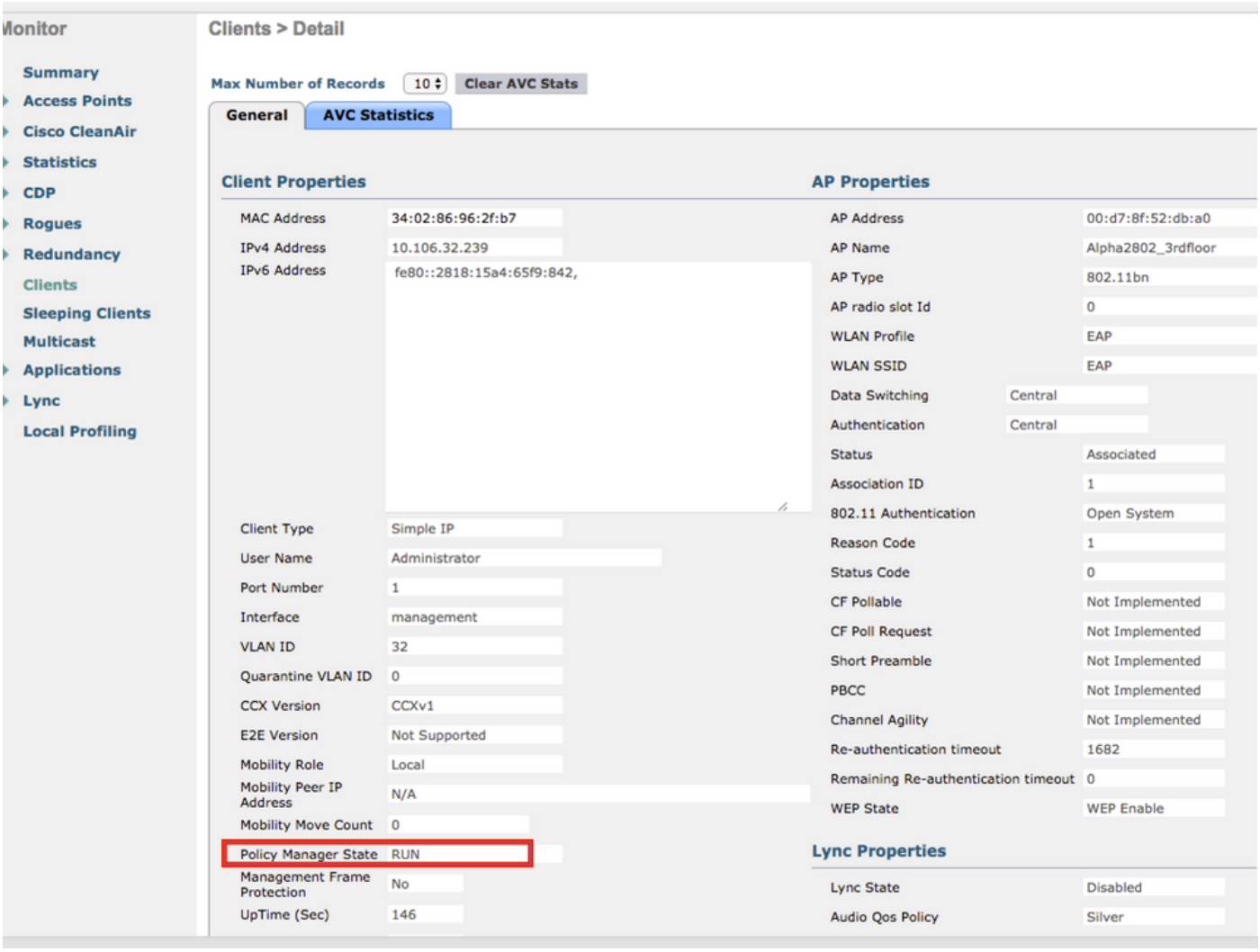
Stap 5. Probeer nu opnieuw verbinding te maken met het draadloze netwerk, selecteer het juiste profiel (EAP in dit voorbeeld) en **Verbind**. U bent verbonden met het draadloze netwerk zoals in de afbeelding wordt weergegeven.



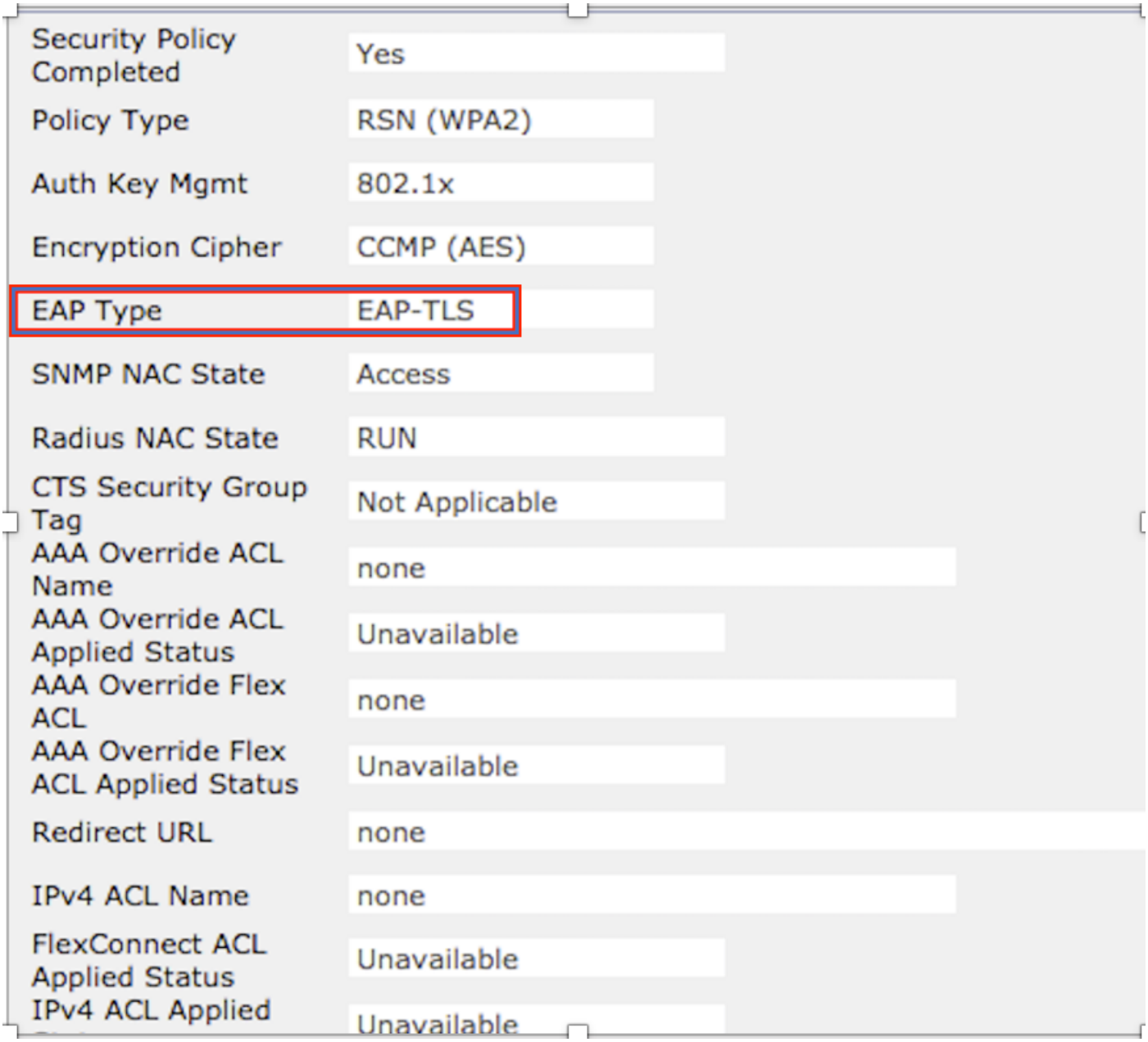
Verifiëren

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

Stap 1. De status van de client policy manager moet worden weergegeven als **RUN**. Dit betekent dat de client de verificatie heeft voltooid, IP-adres heeft verkregen en klaar is om het verkeer door te geven dat in de afbeelding wordt weergegeven.



Stap 2. Controleer ook de juiste EAP-methode op WLC op de pagina met clientdetails zoals in de afbeelding.

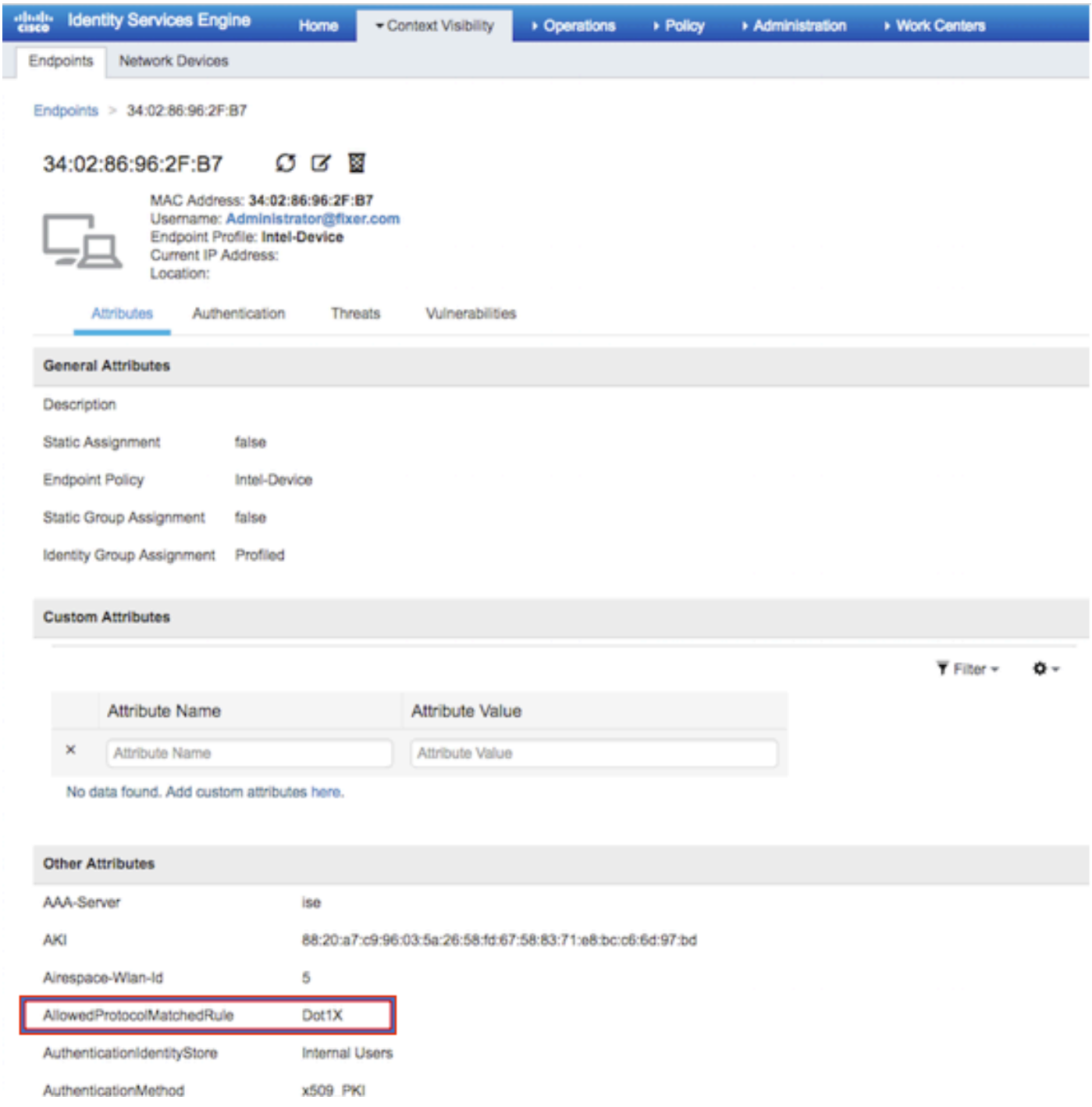


Stap 3. Hier zijn de cliëntdetails van CLI van het controlemechanisme (geknipte output):

```
(Cisco Controller-Standby) >show client detail 34:02:86:96:2f:b7
Client MAC Address.............................. 34:02:86:96:2f:b7
Client Username ................................ Administrator
AP MAC Address.................................. 00:d7:8f:52:db:a0
AP Name......................................... Alpha2802_3rdfloor
AP radio slot Id................................ 0
Client State.................................... Associated
Wireless LAN Id................................. 5
Wireless LAN Network Name (SSID)................ EAP
Wireless LAN Profile Name....................... EAP
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 00:d7:8f:52:db:a4
Connected For .................................. 48 secs
Channel......................................... 1
IP Address...................................... 10.106.32.239
Gateway Address................................. 10.106.32.1
Netmask......................................... 255.255.255.0
Policy Manager State............................ RUN
Policy Type..................................... WPA2
Authentication Key Management................... 802.1x
```

```
Encryption Cipher.............................. CCMP-128 (AES)
Protected Management Frame ..................... No
Management Frame Protection..................... No
EAP Type....................................... EAP-TLS
```

Stap 4. Ga op ISE naar **Context Visibility > End points > Attributes** zoals in de afbeeldingen.



BYODRegistration	Unknown
Called-Station-ID	00-d7-8f-52-db-a0:EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	363
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.106.32.223
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	7
EnableFlag	Enabled
EndPointMACAddress	34-02-86-96-2F-B7
EndPointPolicy	Intel-Device
EndPointProfilerServer	ise.c.com
EndPointSource	RADIUS Probe
Extended Key Usage - Name	130, 132, 138
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.4, 1.3.6.1.4.1.311.1
FailureReason	-
IdentityGroup	Profiled
InactiveDays	5
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA\,DC=fixer\,DC=c
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com

Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7
MatchedPolicy	Intel-Device
MessageCode	5200
NAS-IP-Address	10.106.32.223
NAS-Identifier	HA_Pri
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	HA_Pri
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
NetworkDeviceProfileName	Cisco
OUI	Intel Corporate
OpenSSLErrorMessage	SSL alert: code=0x230=560 \; source=local \; type=fatal \; message="Unknown CA - error unable to get issuer certificate locally"
OpenSSLErrorStack	140160653813504:error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned:s3_srvr.c:3370:
PolicyVersion	0
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
RadiusFlowType	Wireless802_1x
RadiusPacketType	AccessRequest
SSID	00-d7-8f-52-db-a0:EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 00 11

Problemen oplossen

Er is momenteel geen specifieke informatie beschikbaar voor probleemoplossing voor deze configuratie.

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.