EAP-TLS begrijpen en configureren met Mobility Express en ISE

Inhoud

Inleiding

Deze documenten beschrijft hoe u een Wireless Local Area Network (WLAN) kunt instellen met 802.1x-beveiliging in een Mobility Express controller. In dit document wordt ook het gebruik van Extensible Authentication Protocol (EAP) - Transport Layer Security (TLS) specifiek uitgelegd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Eerste instelling voor Mobility Express
- 802.1x-authenticatieproces
- Certificaten

Gebruikte componenten

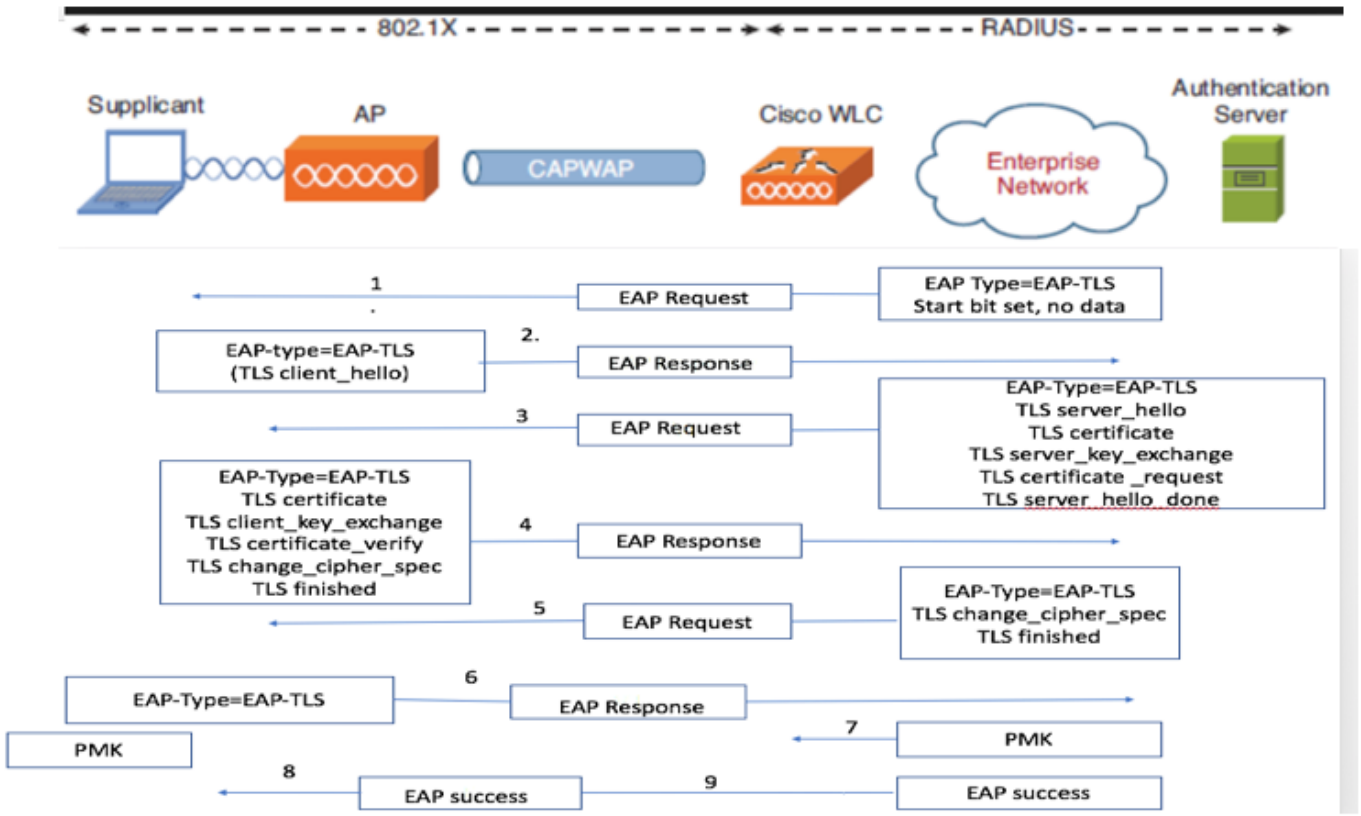
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- WLC 5508 versie 8.5
- Identity Services Engine (ISE) versie 2.1

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

EAP-TLS-stroom



Stappen in EAP-TLS-stroom

1. Draadloze client wordt gekoppeld aan het access point (AP).
2. AP staat de cliënt niet toe om op dit punt gegevens te verzenden en een authentificatieverzoek te versturen.
3. De aanvrager reageert daarop met een MAP-antwoordidentiteit. De WLC geeft vervolgens de gebruiker-id informatie door aan de verificatieserver.
4. RADIUS-server reageert weer op de client met een EAP-TLS Start-pakket. De EAP-TLS-discussie begint nu.
5. De peer stuurt een EAP-Response terug naar de authenticatieserver die een "client_hallo" handdruk bericht bevat, een algoritme dat voor NULL is ingesteld.
6. De authenticatieserver reageert met een Access-challenge pakket dat bestaat uit:

```
TLS server_hello
handshake message
certificate
server_key_exchange
certificate request
server_hello_done.
```

7. De client reageert met een MAP-antwoordbericht dat 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
```

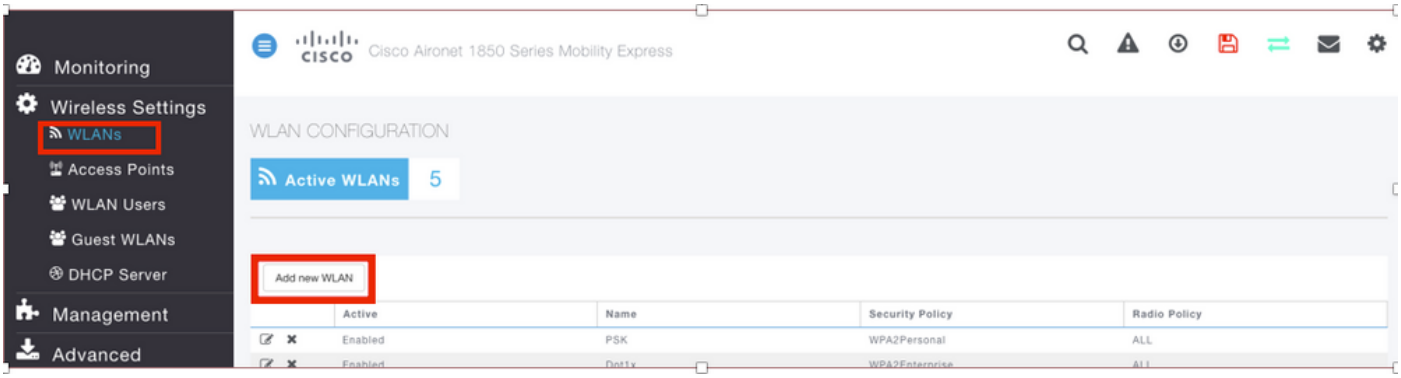
8. Nadat de client is geauthentiseerd, reageert de RADIUS-server met een Access-challenge, die het afgewerkte bericht "change_algoritme_spec" en de handdruk bevat. Na ontvangst verifieert de client de hash om de RADIUS-server voor echt te maken. Een nieuwe encryptiesleutel wordt dynamisch afgeleid van het geheim tijdens de TLS-handdruk.

9. Op dit punt kan de EAP-TLS-enabled draadloze client toegang krijgen tot het draadloze netwerk.

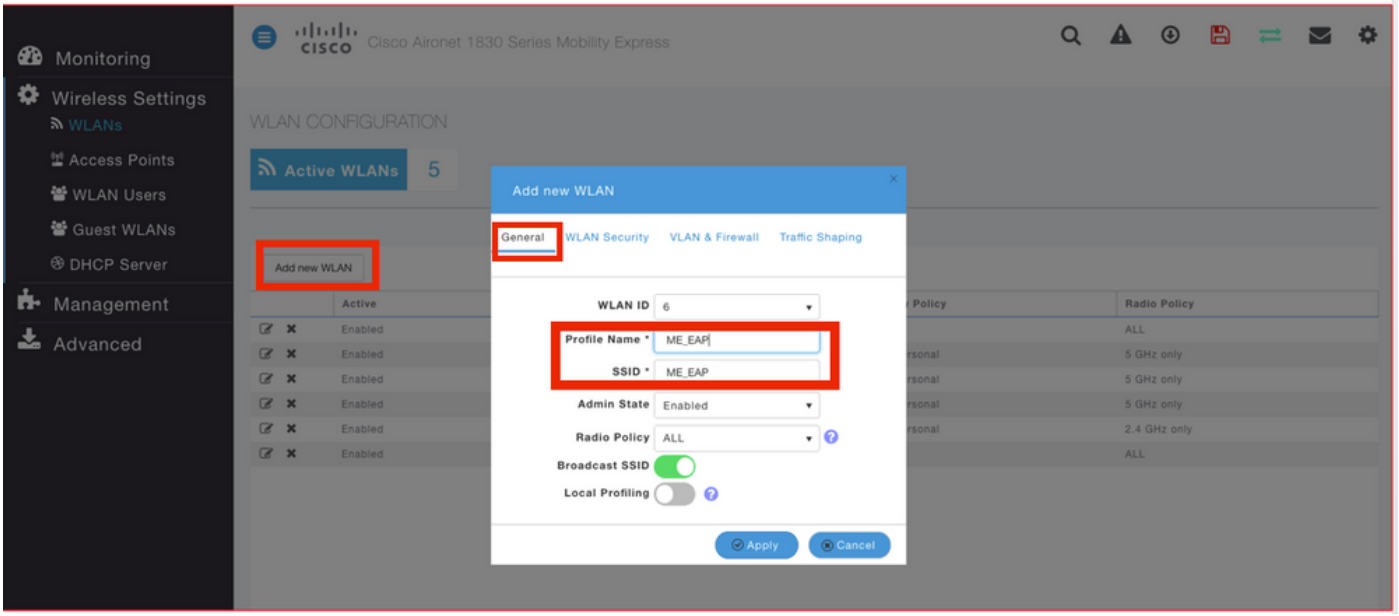
Configureren

Cisco Mobility Express

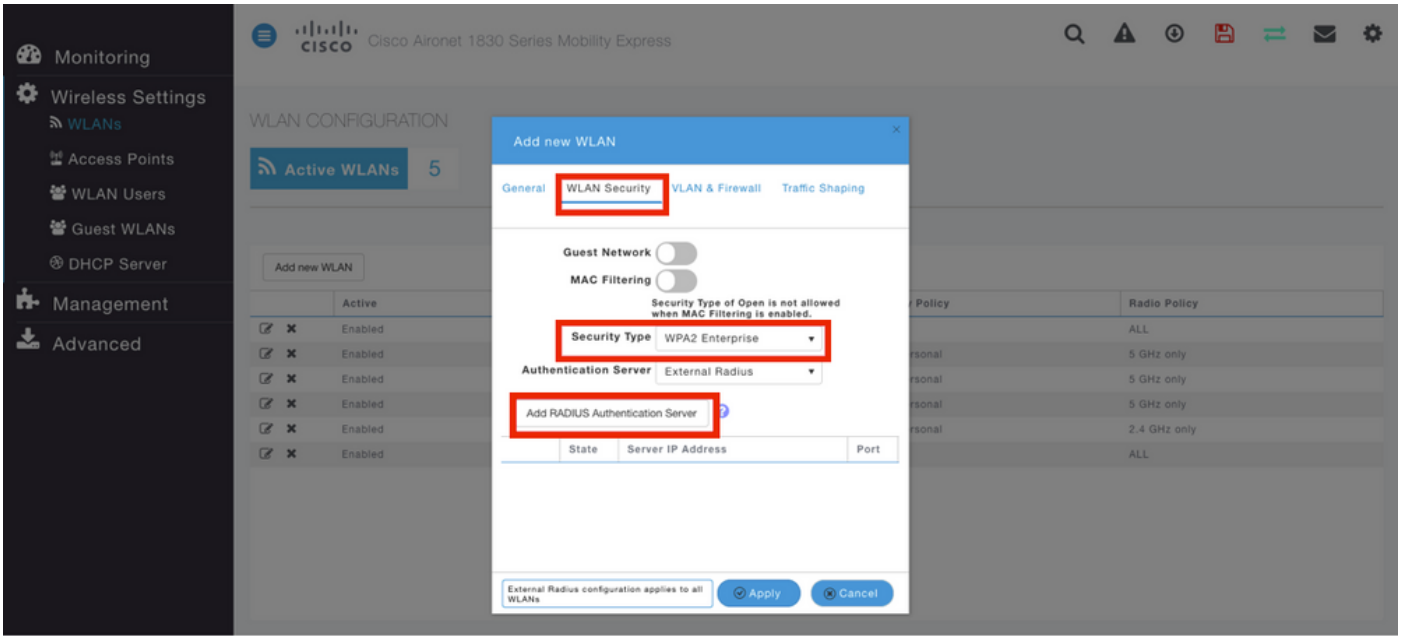
Stap 1. De eerste stap is het maken van een WLAN-functie bij Mobility Express. Om een WLAN te maken, navigeer dan naar **WLAN > Voeg nieuwe WLAN toe** zoals in de afbeelding.



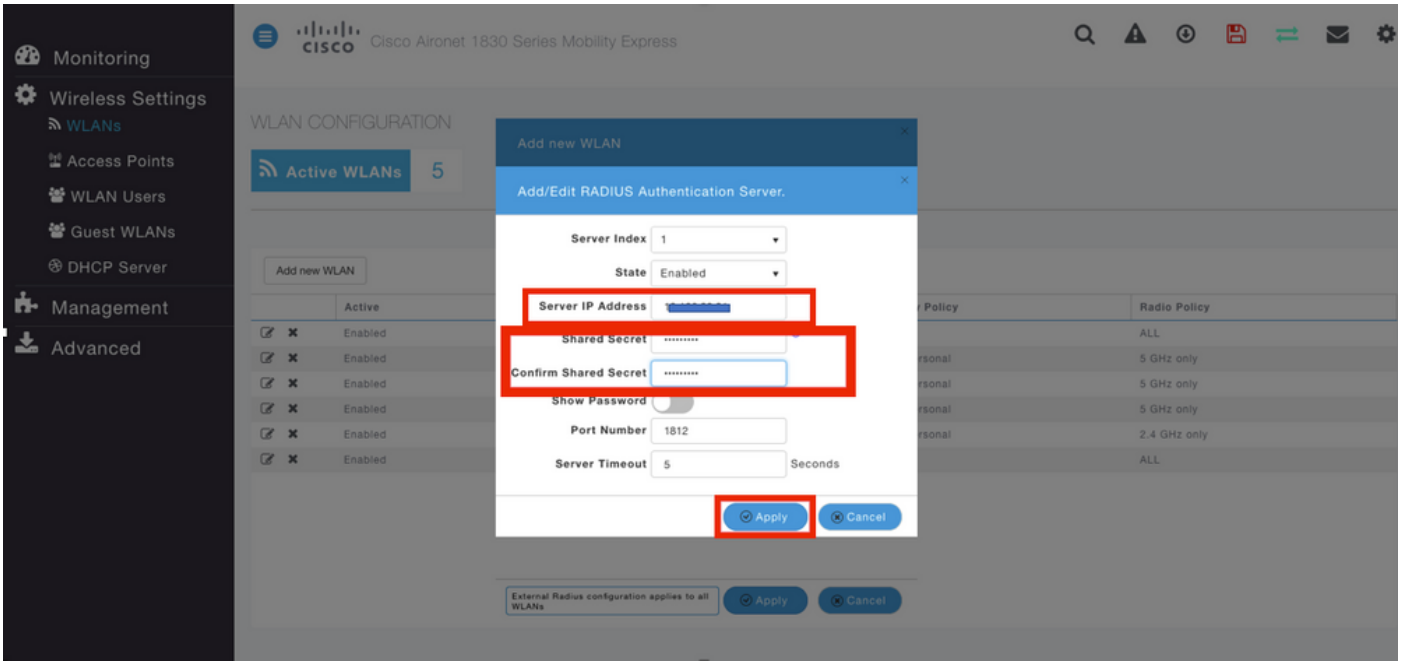
Stap 2. Er verschijnt een nieuw pop-upvenster nadat u op **Add new WLAN** klikt. Als u een Profile name wilt maken, navigeer u om **nieuwe WLAN > General** toe te **voegen** zoals in de afbeelding.



Stap 3. Configureer het verificatietype als WAP Enterprise voor 802.1x en stel RADIUS-server in onder **Add new WLAN > WLAN-beveiliging** zoals in de afbeelding.



Stap 4. Klik op **RADIUS-verificatieserver toevoegen** en geef het IP-adres op van de RADIUS-server en het gedeelde geheim dat precies overeenkomt met wat op ISE is ingesteld en klik vervolgens op **Toepassen** zoals in de afbeelding.



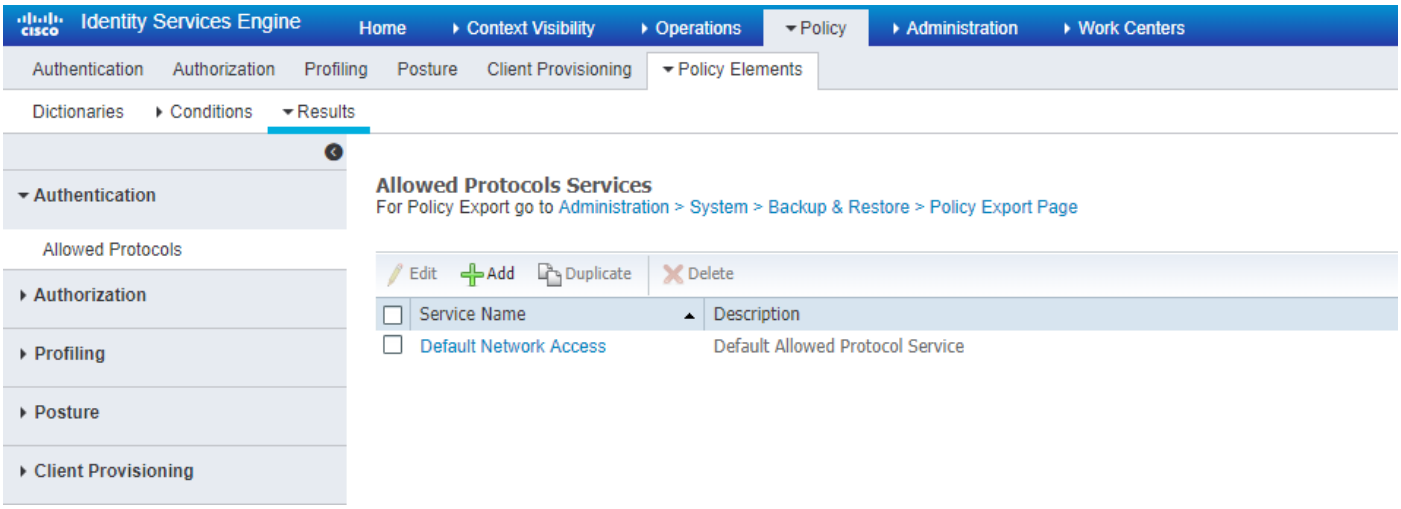
ISE met Cisco Mobility Express

EAP-TLS-instellingen

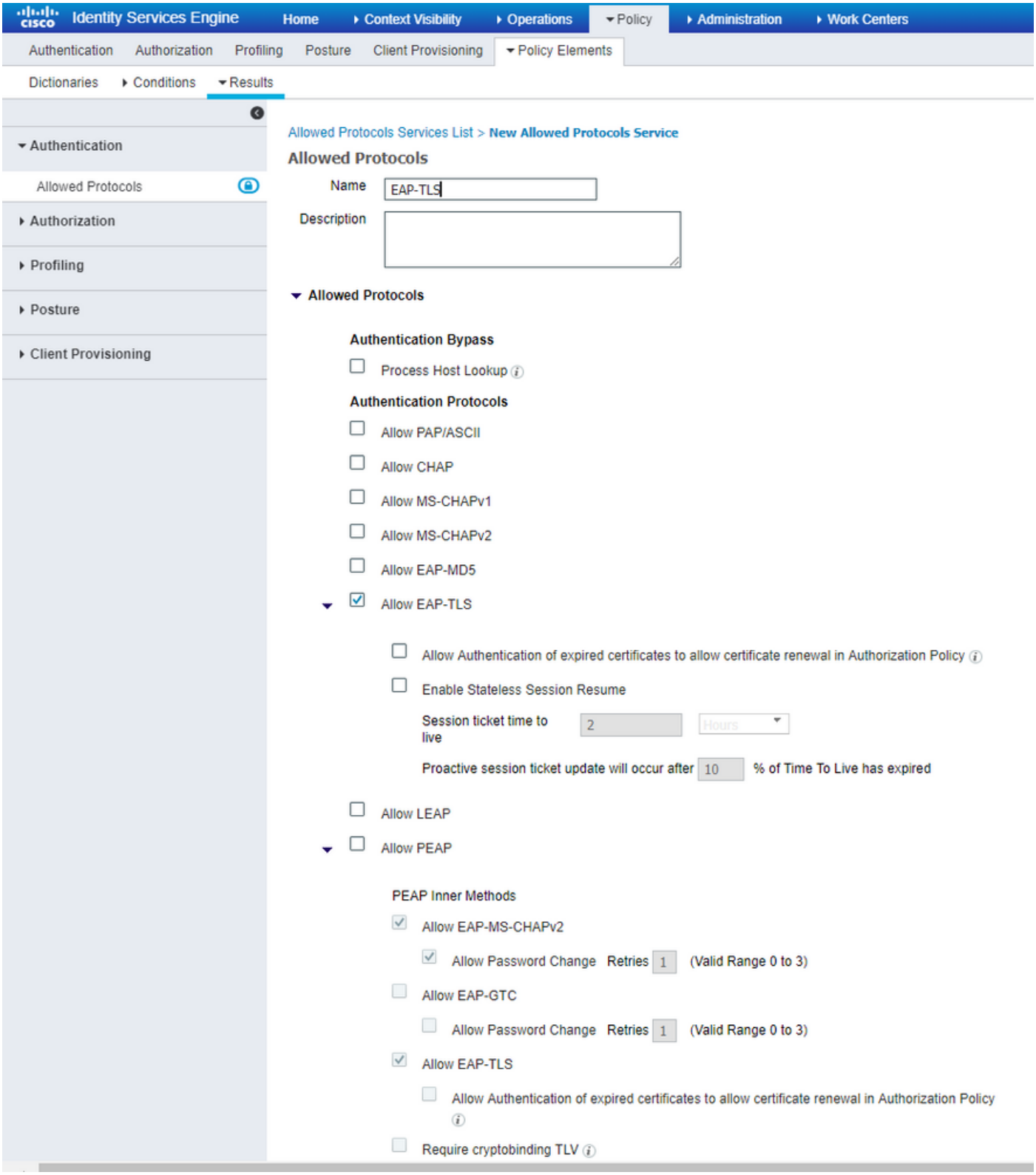
Om het beleid te kunnen bouwen, moet u de toegestane protocollijst maken die in uw beleid moet worden gebruikt. Aangezien er een dot1x-beleid is geschreven, moet u het toegestane MAP-type specificeren op basis van de manier waarop het beleid wordt ingesteld.

Als u de standaardinstelling gebruikt, staat u de meeste MAP-typen toe voor authenticatie die wellicht niet de voorkeur genieten als u de toegang tot een specifiek MAP-type moet afsluiten.

Stap 1. Navigeer in op **Policy > Policy Elementen > Resultaten > Verificatie > Toegestane protocollen** en klik op **Add** zoals in de afbeelding.

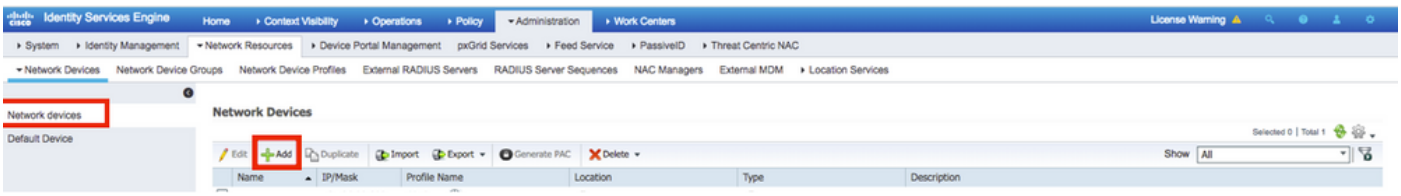


Stap 2. Op deze toegestane protocollijst kunt u de naam voor de lijst invoeren. In dit geval is **het** vakje **EAP-TLS toestaan** ingeschakeld en zijn andere vakjes niet ingeschakeld zoals in de afbeelding wordt weergegeven.

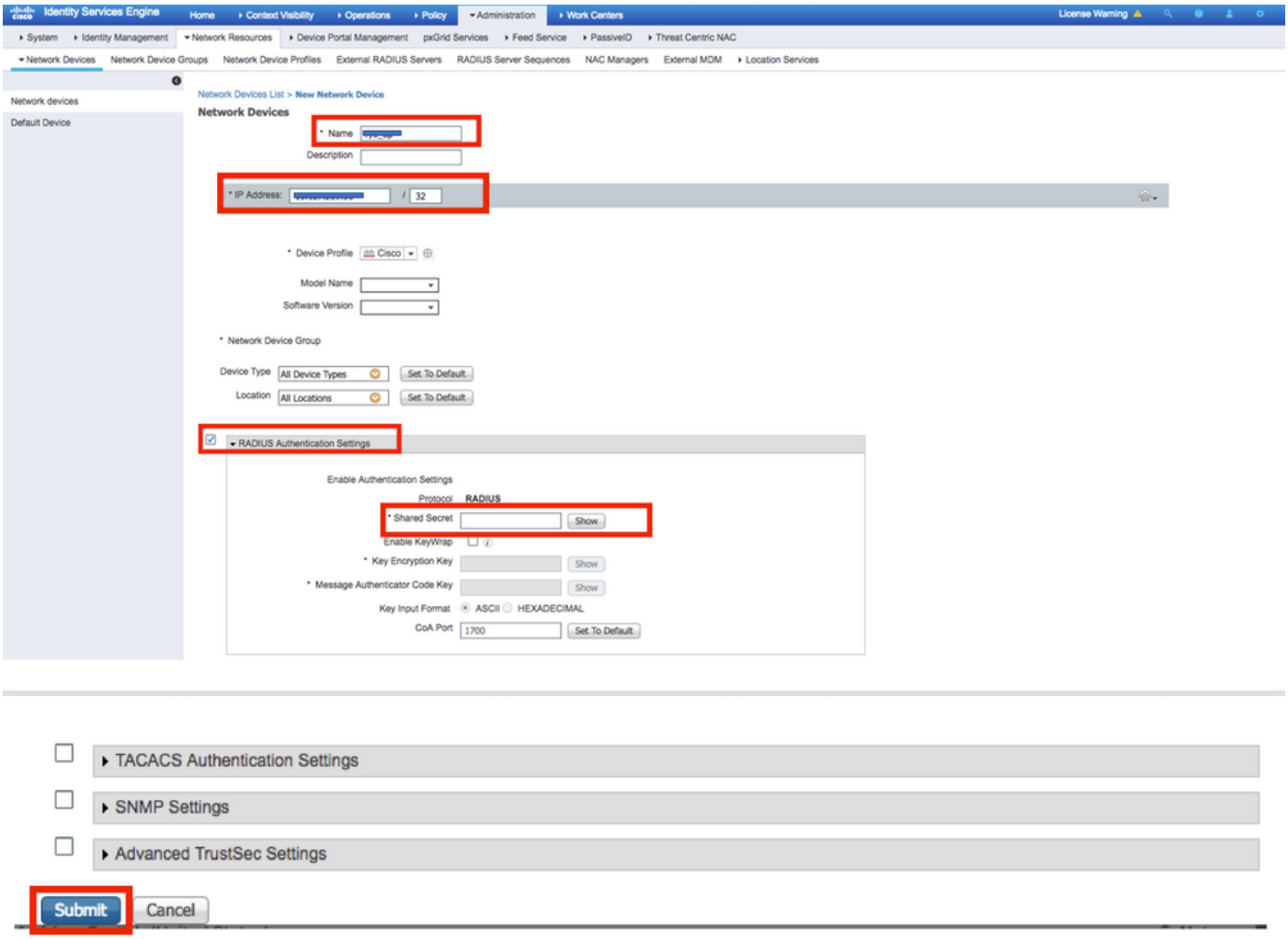


Mobility Express-instellingen voor ISE

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



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

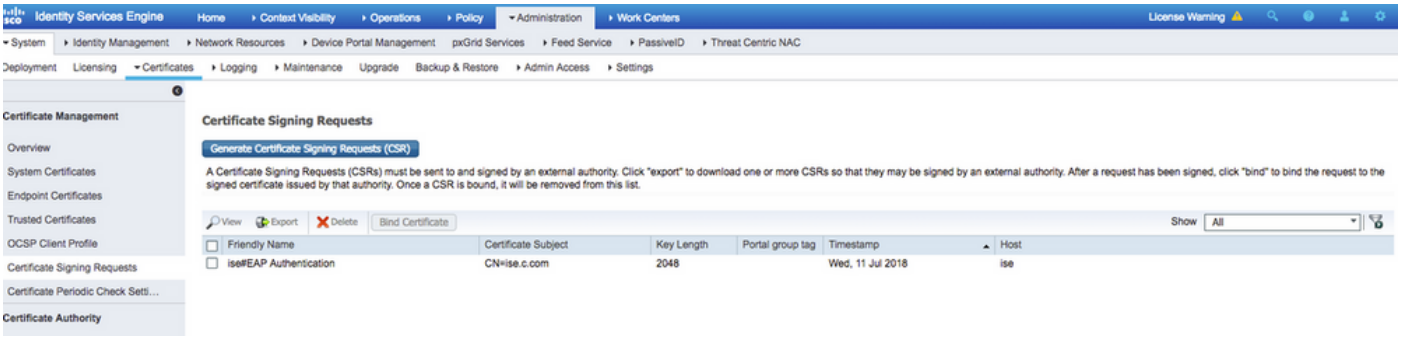


Trustcertificaat op ISE

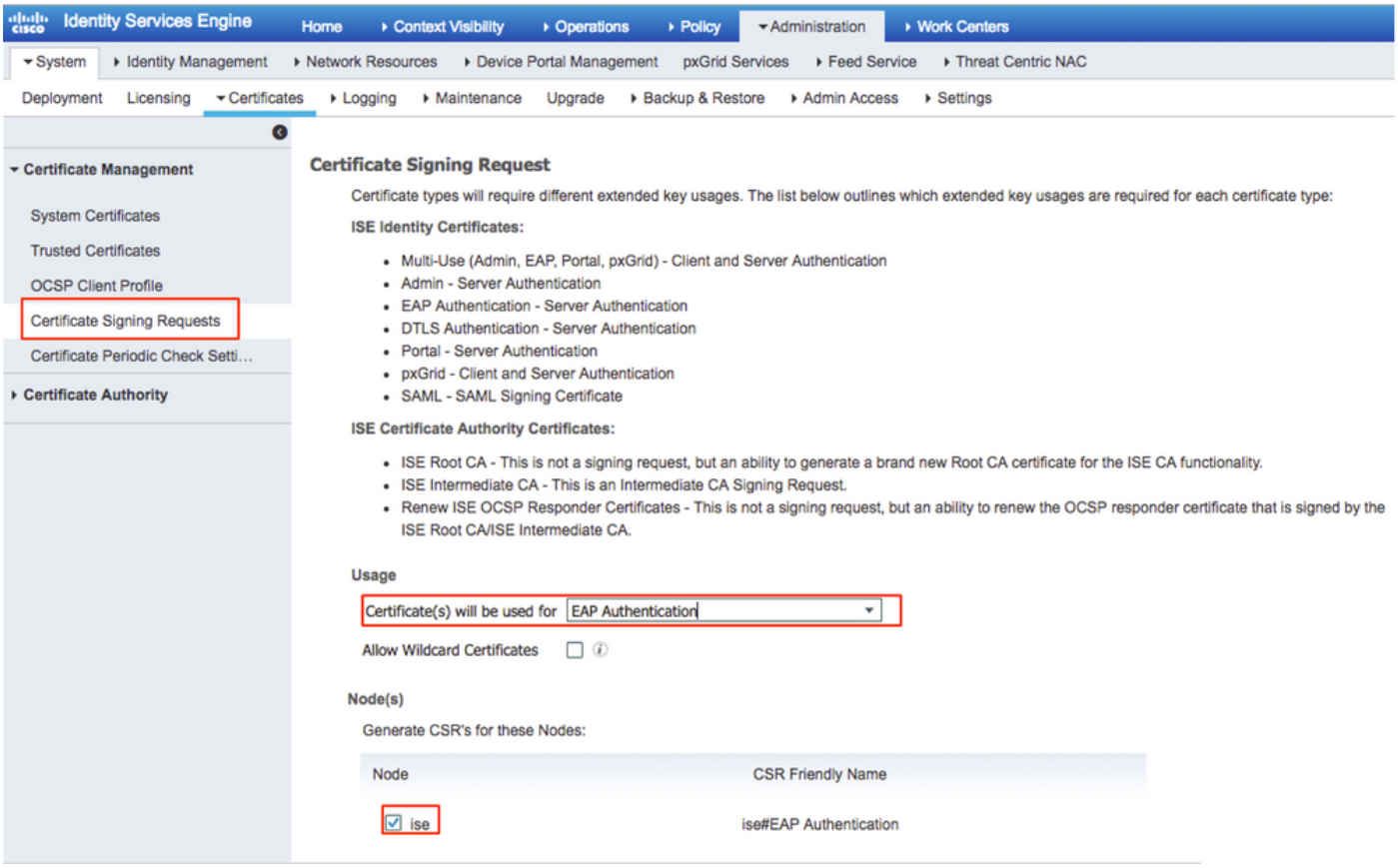
Stap 1. Navigeer naar **Administratie > Systeem > Certificaten > certificaatbeheer > Vertrouwde certificaten**.

Klik op **Importeren** om een certificaat te importeren naar ISE. Zodra u een WLC hebt toegevoegd en een gebruiker op ISE hebt gemaakt, moet u het belangrijkste onderdeel van EAP-TLS doen dat is om het certificaat op ISE te vertrouwen. Daarvoor moet je CSR genereren.

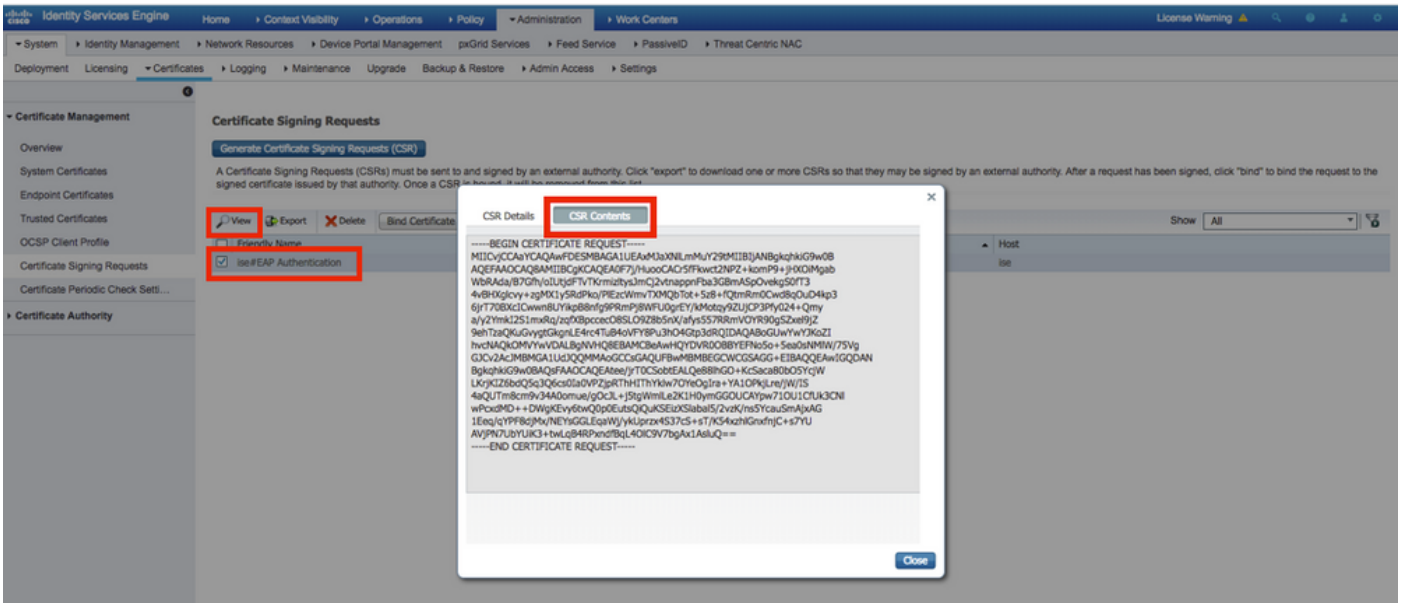
Stap 2. Navigeer naar **Advisering > Certificaten > Verzoeken voor certificatie > Generate certificaatsignalering (CSR)** zoals in de afbeelding getoond.



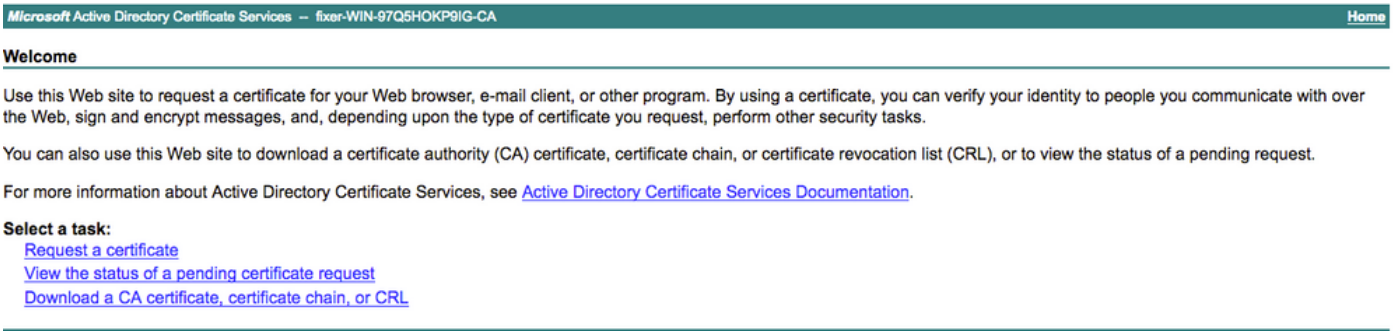
Stap 3. Om CSR te genereren, navigeer dan naar **Gebruik** en **van** het**(de) Certificaat(en) wordt (worden) gebruikt voor** uitrolopties, selecteer **EAP-verificatie** zoals in de afbeelding.



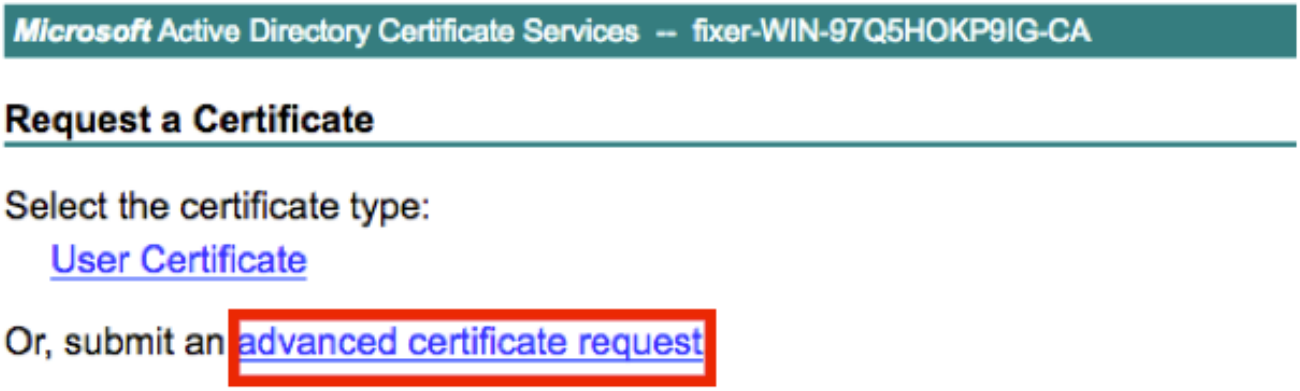
Stap 4. Het CSR dat op ISE is gegenereerd, kan worden bekeken. Klik op **Weergeven** zoals in de afbeelding.



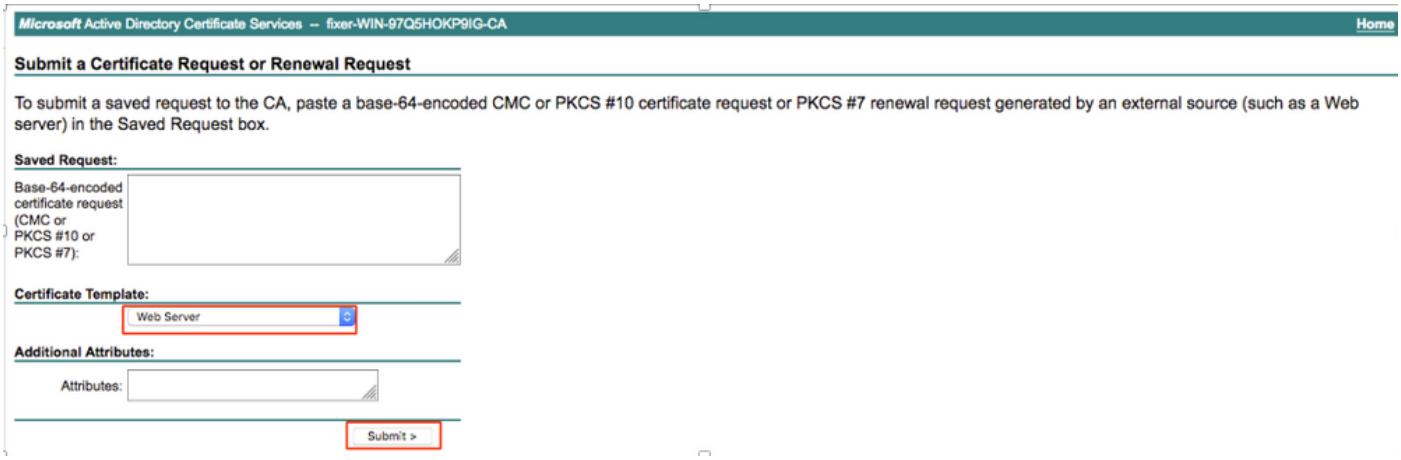
Stap 5. Wanneer CSR gegenereerd is, bladert u naar een CA-server en klikt u op **Een certificaat aanvragen** zoals in de afbeelding:



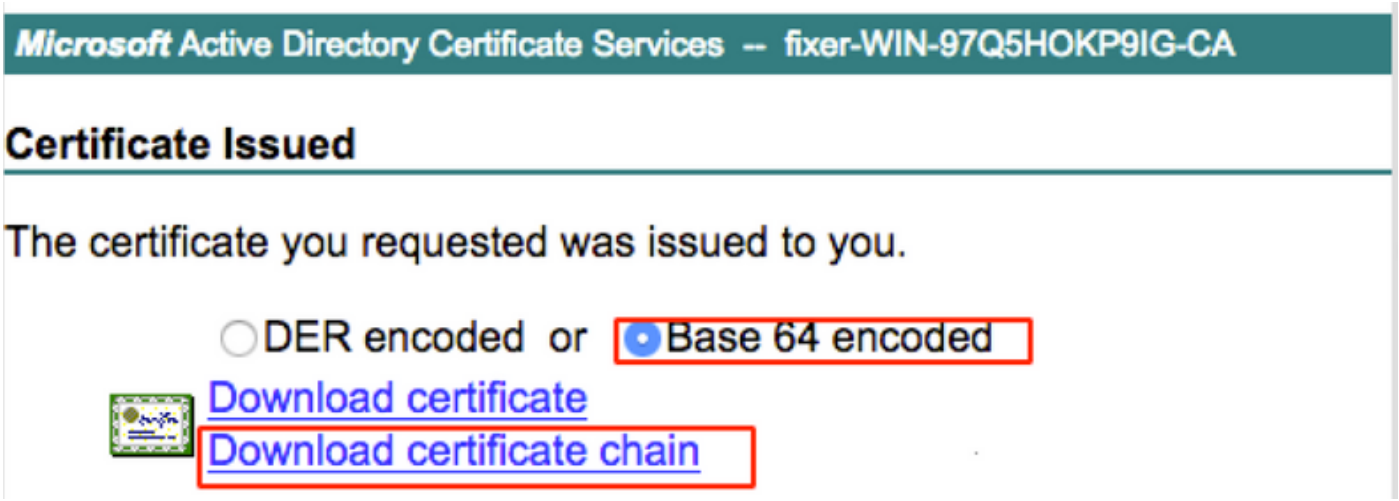
Stap 6. Nadat u een certificaat hebt aangevraagd, krijgt u opties voor **Gebruikerscertificaat** en **geavanceerde certificaataanvraag**, klikt u op **geavanceerde certificaataanvraag** zoals in de afbeelding.



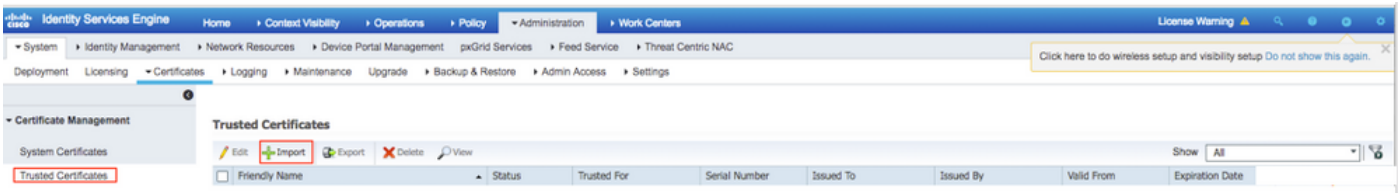
Stap 7. Plakt de CSR die in **Base-64 gecodeerd certificaatverzoek** is gegenereerd. Selecteer de optie **Webserver** selecteren in **de** vervolgkeuzelijst**:** klik op **Webserver** en klik op **Inzenden** zoals in de afbeelding.

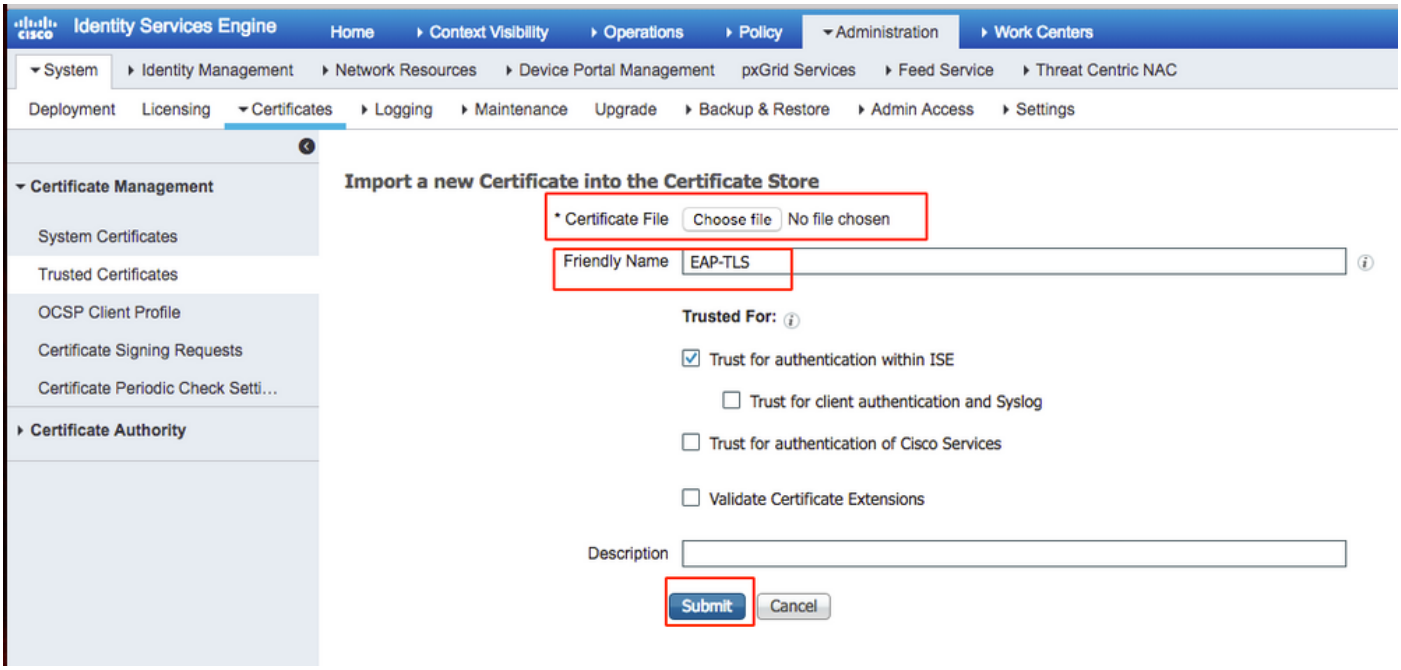


Stap 8. Zodra u op **Inzenden** klikt, krijgt u de optie om het type certificaat te selecteren, selecteert u **Base-64 gecodeerd** en klikt u op **Download certificaat** zoals in de afbeelding.

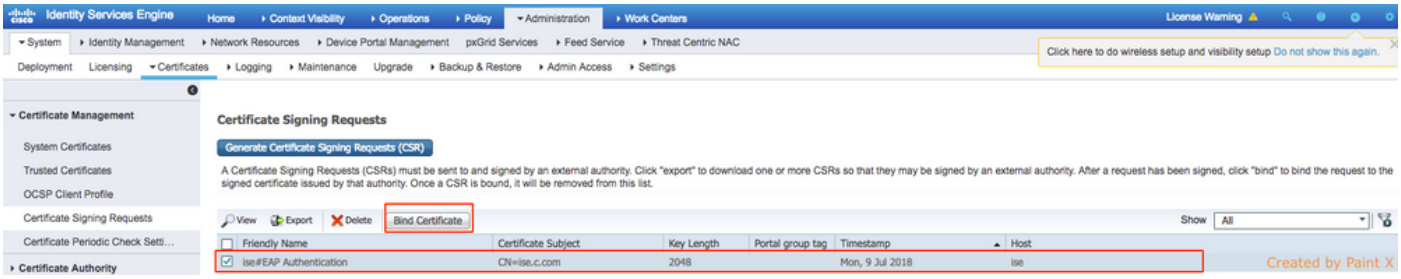


Stap 9. Het certificaat is gedownload voor de ISE-server. U kunt het certificaat opvragen, het certificaat bevat twee certificaten, één wortelcertificaat en een ander tussenproduct. Het basiscertificaat kan worden geïmporteerd onder **Beheer > Certificaten > Vertrouwde certificaten > Importeren** zoals in de afbeeldingen.

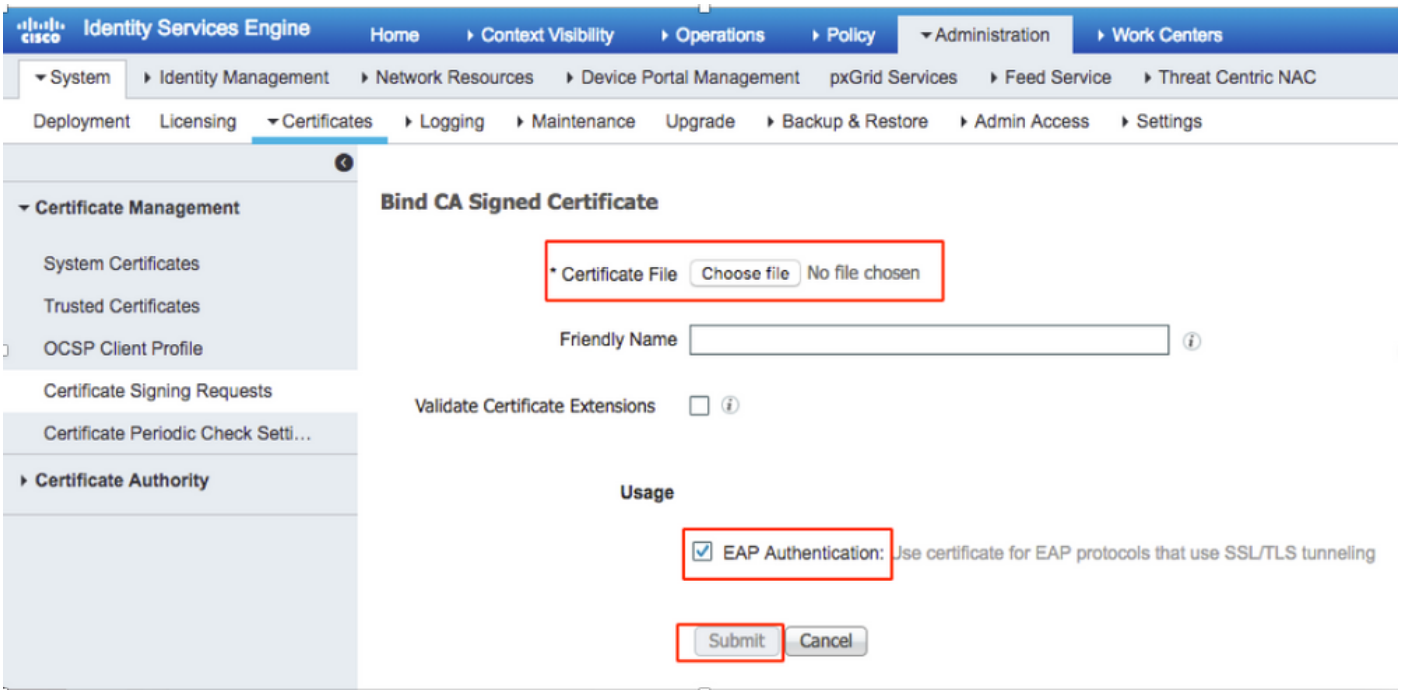




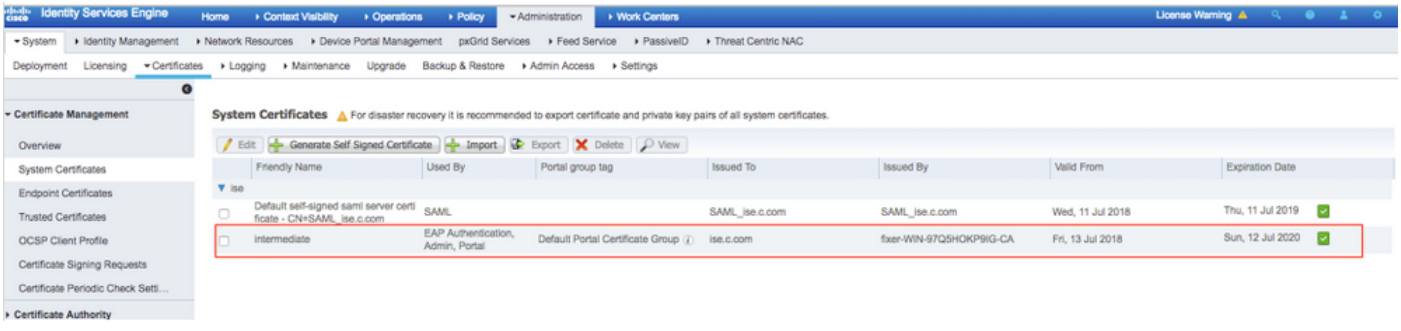
Stap 10. Zodra u op **Inzenden** klikt, wordt het certificaat toegevoegd aan de lijst met vertrouwde certificaten. Bovendien is het intermediaire certificaat nodig om aan CSR te binden zoals in de afbeelding.



Stap 1. Zodra u op **Bind certificaat** klikt, kunt u het certificaatbestand kiezen dat in uw bureaublad is opgeslagen. Bladeren naar het intermediaire certificaat en klik op **Inzenden** zoals in de afbeelding.



Stap 12. Om het certificaat te kunnen weergeven, navigeer dan naar **Administratie > Certificaten > Systeemcertificaten** zoals in de afbeelding.



Cliënt voor EAP-TLS

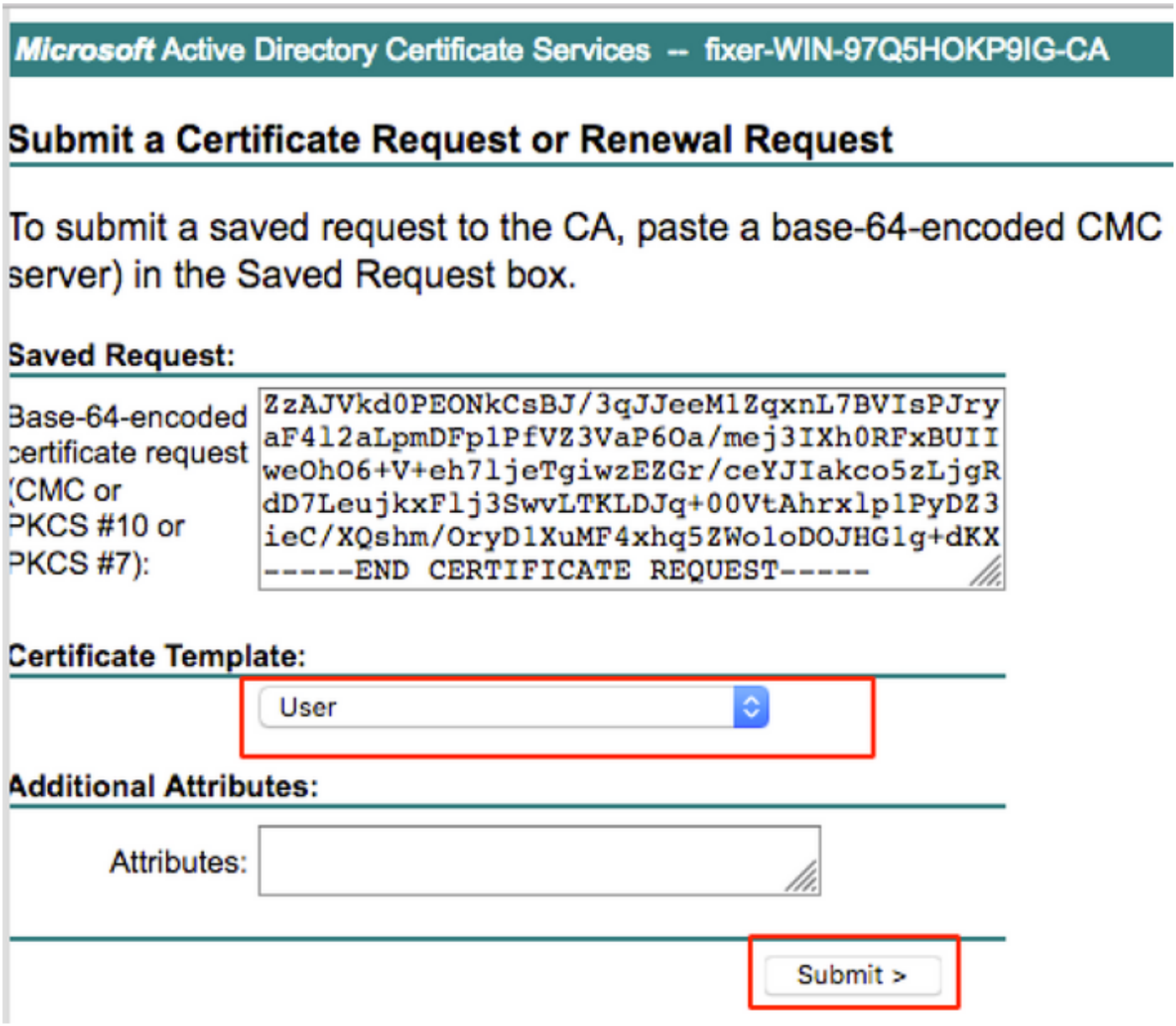
Gebruikershandleiding downloaden op clientmachine (Windows bureaublad)

Stap 1. Om een draadloze gebruiker via EAP-TLS te authentiseren, moet u een client certificaat 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 adr./certsrv

Stap 2. Merk op dat de CA hetzelfde moet zijn als waarmee het certificaat voor ISE is

gedownload.

Hiervoor moet u voor dezelfde CA-server bladeren die u het certificaat voor server hebt gedownload. Klik op **Aanvragen van een certificaat** zoals eerder gedaan. U moet echter deze keer **Gebruiker** selecteren als de certificaatsjabloon zoals in de afbeelding weergegeven.



Stap 3. Klik vervolgens op de **downloadcertificaatketen** zoals eerder voor de server is gedaan.

Nadat u de certificaten heeft gekregen, volgt u deze stappen om het certificaat op Windows-laptop te importeren.

Stap 4. Om het certificaat te kunnen importeren, moet u het vanaf de Microsoft Management Console (MMC) benaderen.

1. Om de MMC te openen navigeer naar **Start > Run > MMC**.
2. Navigeren in op **bestand > Magnetisch toevoegen / verwijderen**
3. Dubbelklik op **certificaten**.
4. Selecteer **Computer-account**.
5. Selecteer **Local Computer > Finish**
6. Klik op **OK** om het Magnetisch-In venster te verlaten.

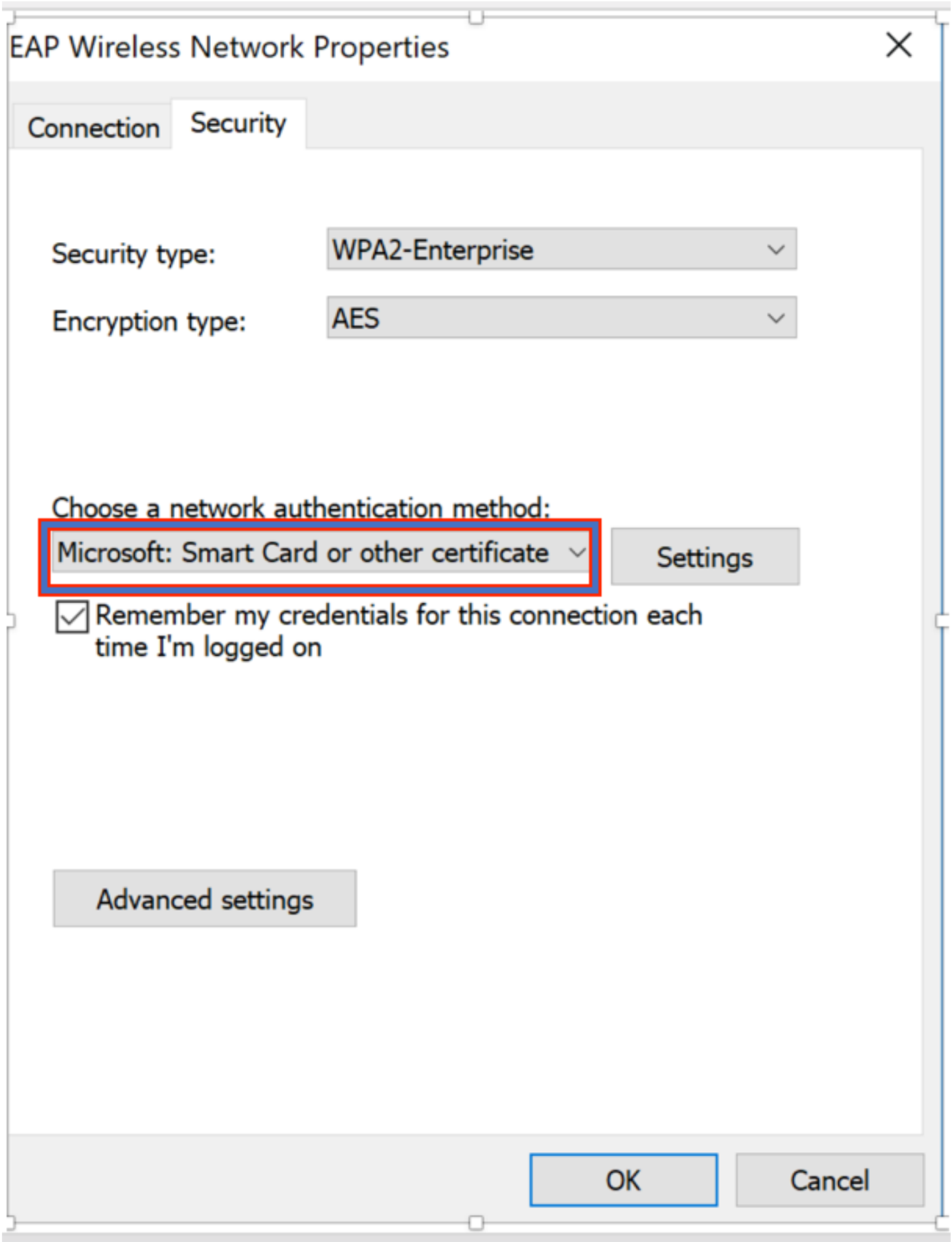
7. Klik op **[+]** naast **certificaten > Persoonlijk > Certificaten**.
8. Klik met de rechtermuisknop op **Certificaten** en selecteer **Alle taken > Importeren**.
9. Klik op **Volgende**.
10. Klik op **Bladeren**.
11. Selecteer de optie **.cer, .crt of .pfx** die u wilt importeren.
12. Klik op **Openen**.
13. Klik op **Volgende**.
14. Selecteer **Automatisch de certificaatwinkel selecteren op basis van het type certificaat**.
15. Klik op **Voltooien & OK**

Nadat het certificaat is ingevoerd, moet u uw draadloze client (Windows bureaublad in dit voorbeeld) voor EAP-TLS configureren.

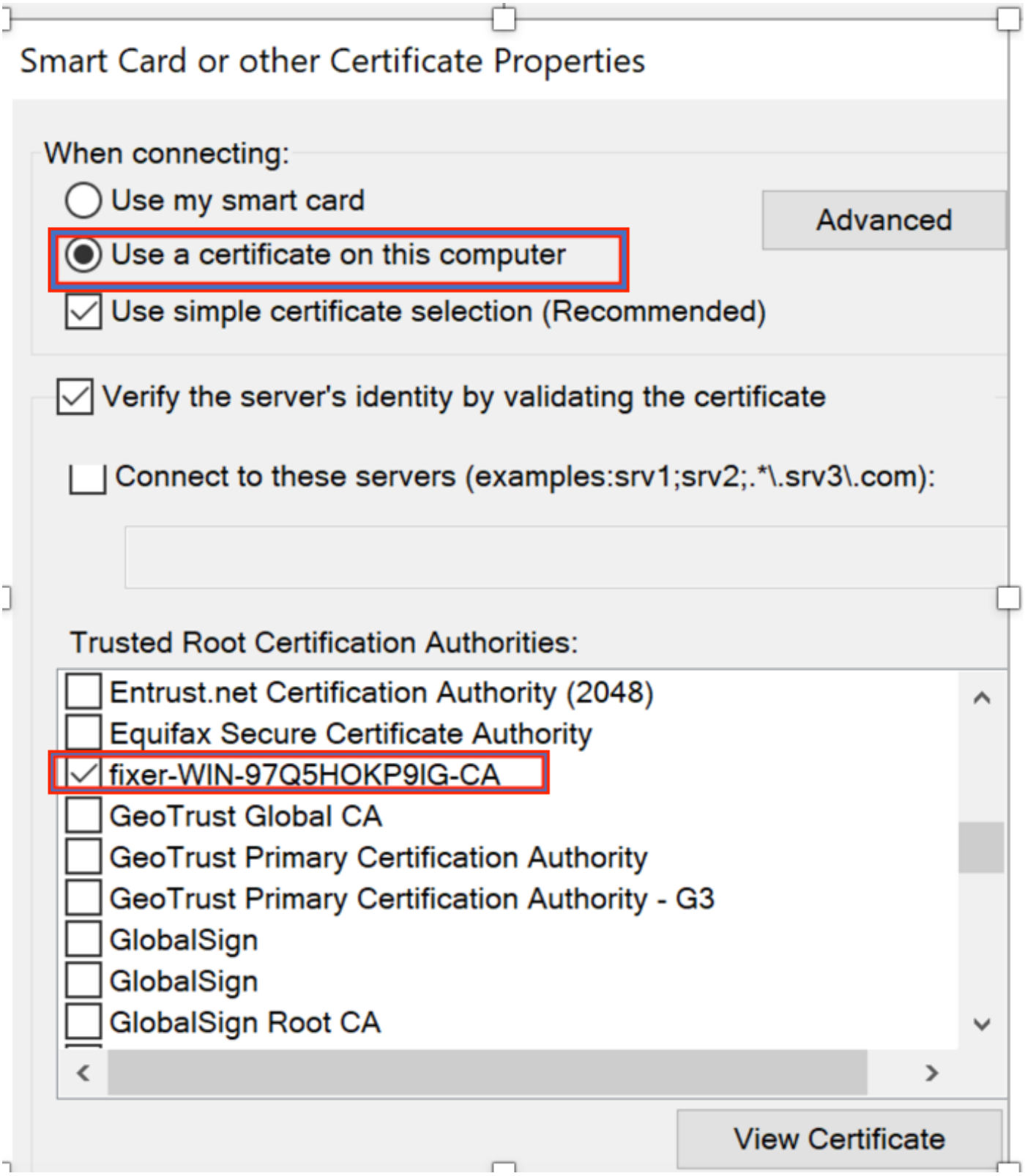
Draadloos profiel voor EAP-TLS

Stap 1. Verander het draadloze profiel dat eerder was gemaakt voor Protected Extensible Authentication Protocol (PEAP) om in plaats daarvan EAP-TLS te gebruiken. Klik op **EAP draadloos profiel**.

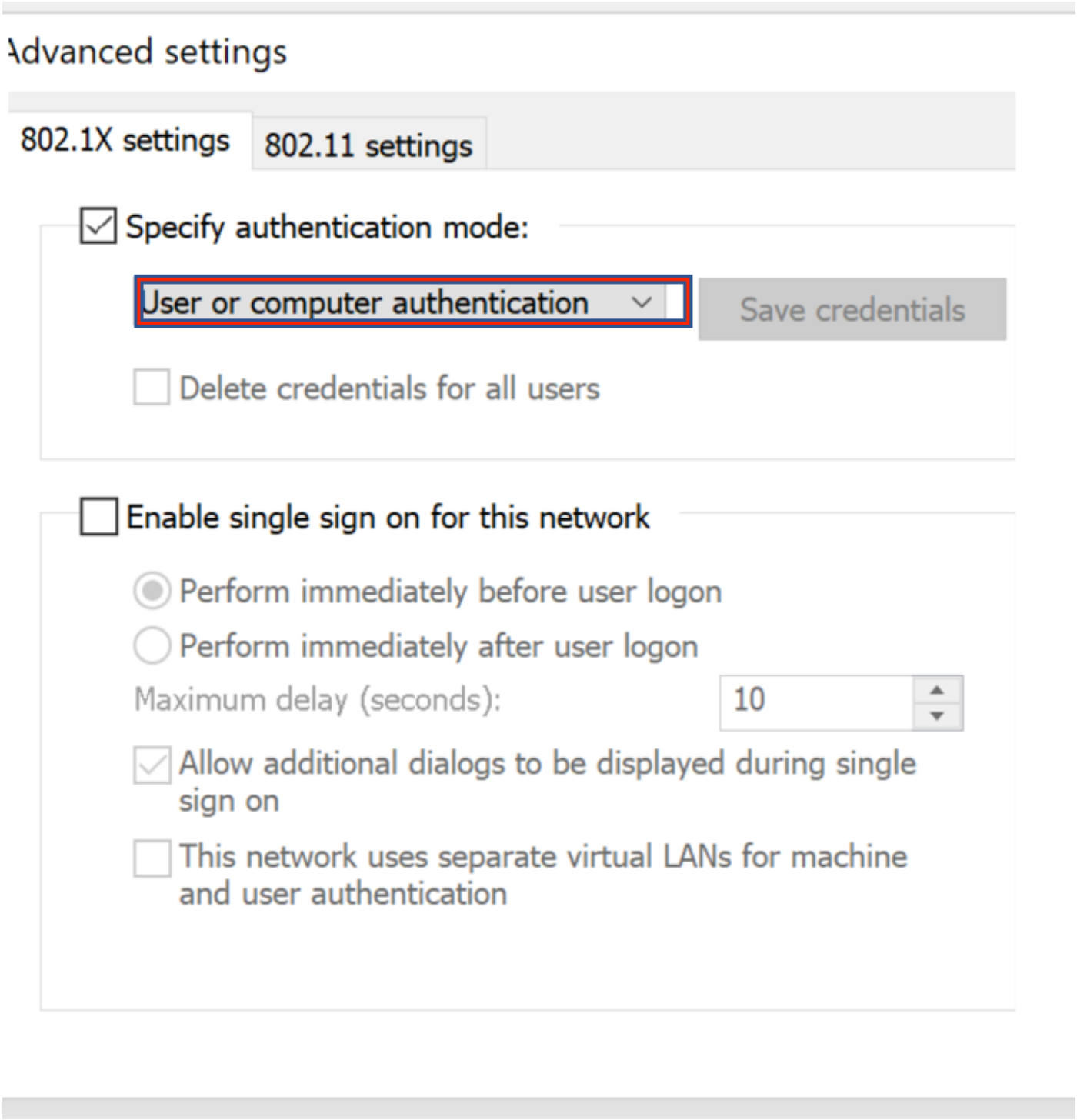
Stap 2. Selecteer **Microsoft: Smart Card of ander certificaat** en klik op **OK** zoals in de afbeelding.



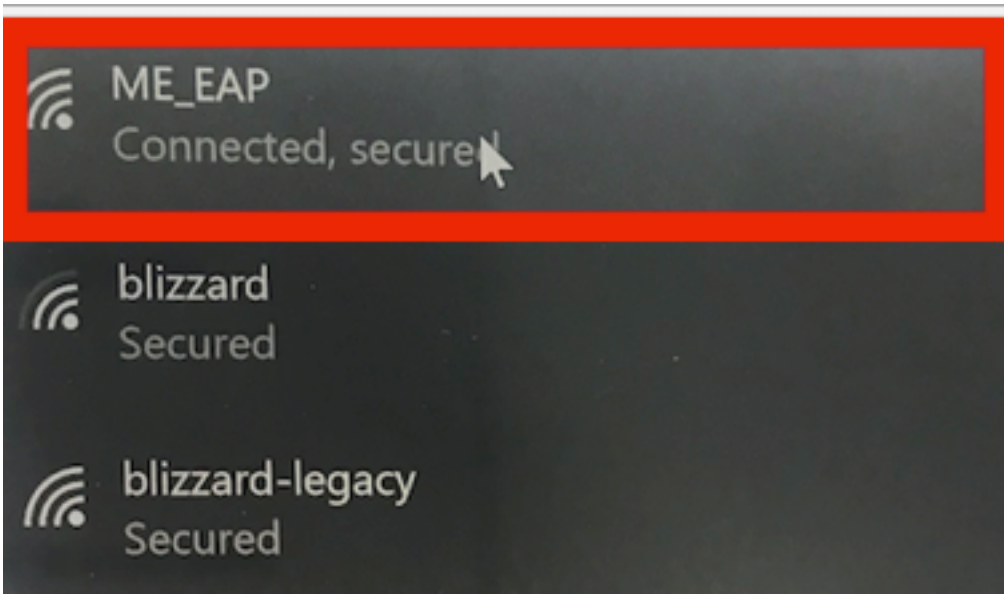
Stap 3. Klik op **Instellingen** en selecteer het basiscertificaat dat is verstrekt vanaf een CA-server zoals in de afbeelding.



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



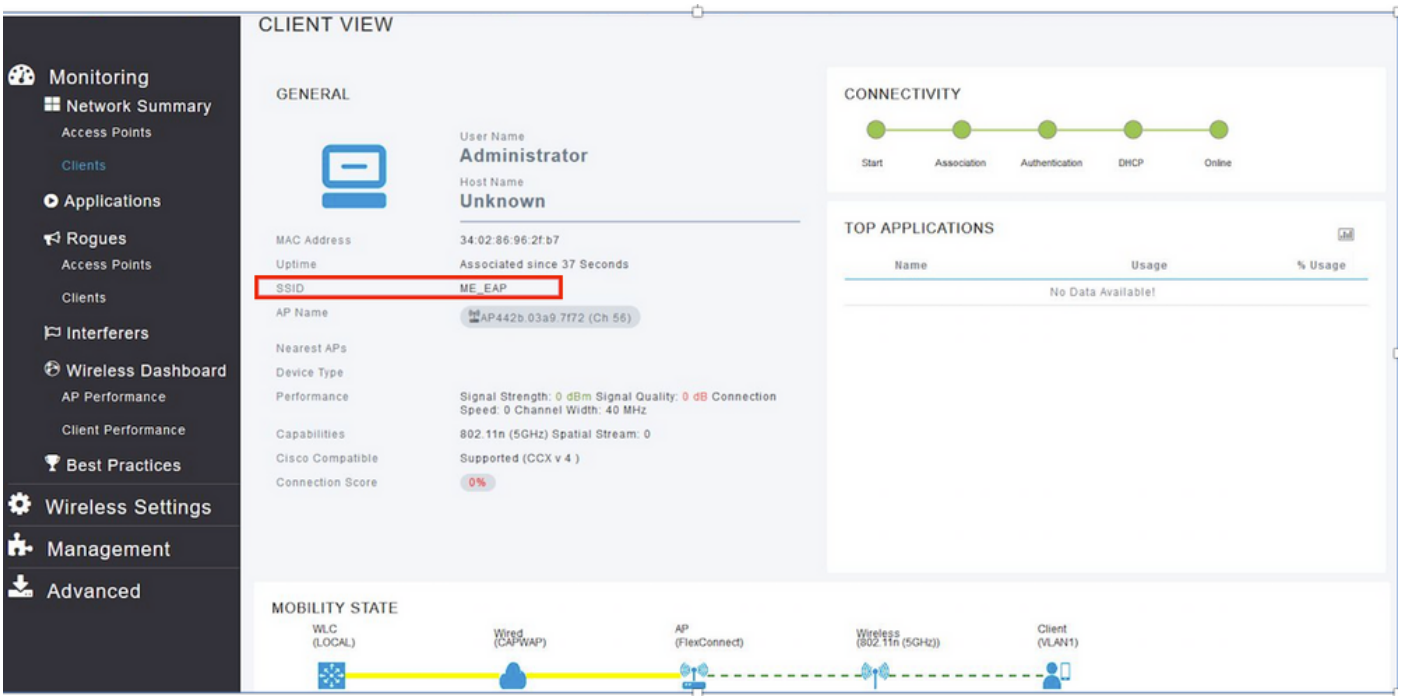
Stap 5. Probeer nu opnieuw verbinding te maken met het draadloze netwerk, selecteer het juiste profiel (EAP in dit voorbeeld) en **Connect**. U bent aangesloten op het draadloze netwerk zoals in de afbeelding wordt weergegeven.

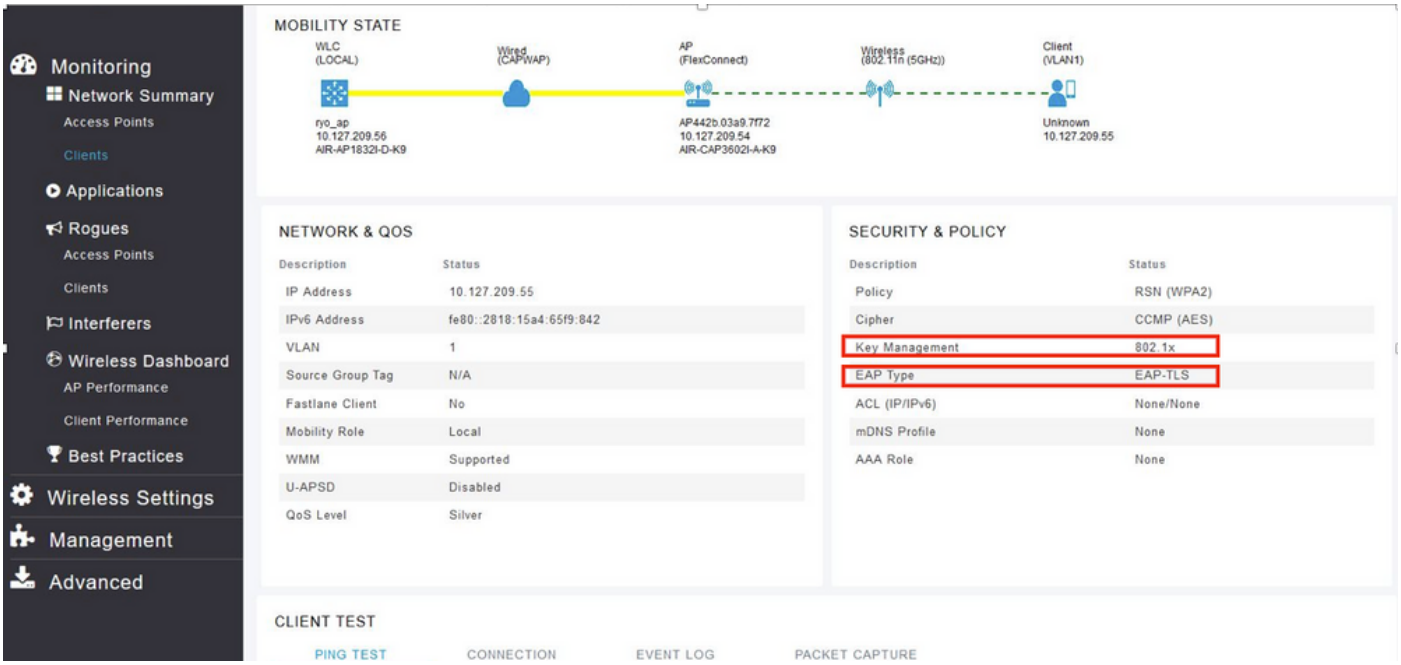


Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Stap 1. Het MAP-type van de cliënt moet een MAP-TLS zijn. Dit betekent dat de cliënt, met behulp van EAP-TLS, een IP-adres heeft verkregen en bereid is het verkeer door te geven zoals in de afbeeldingen wordt getoond.

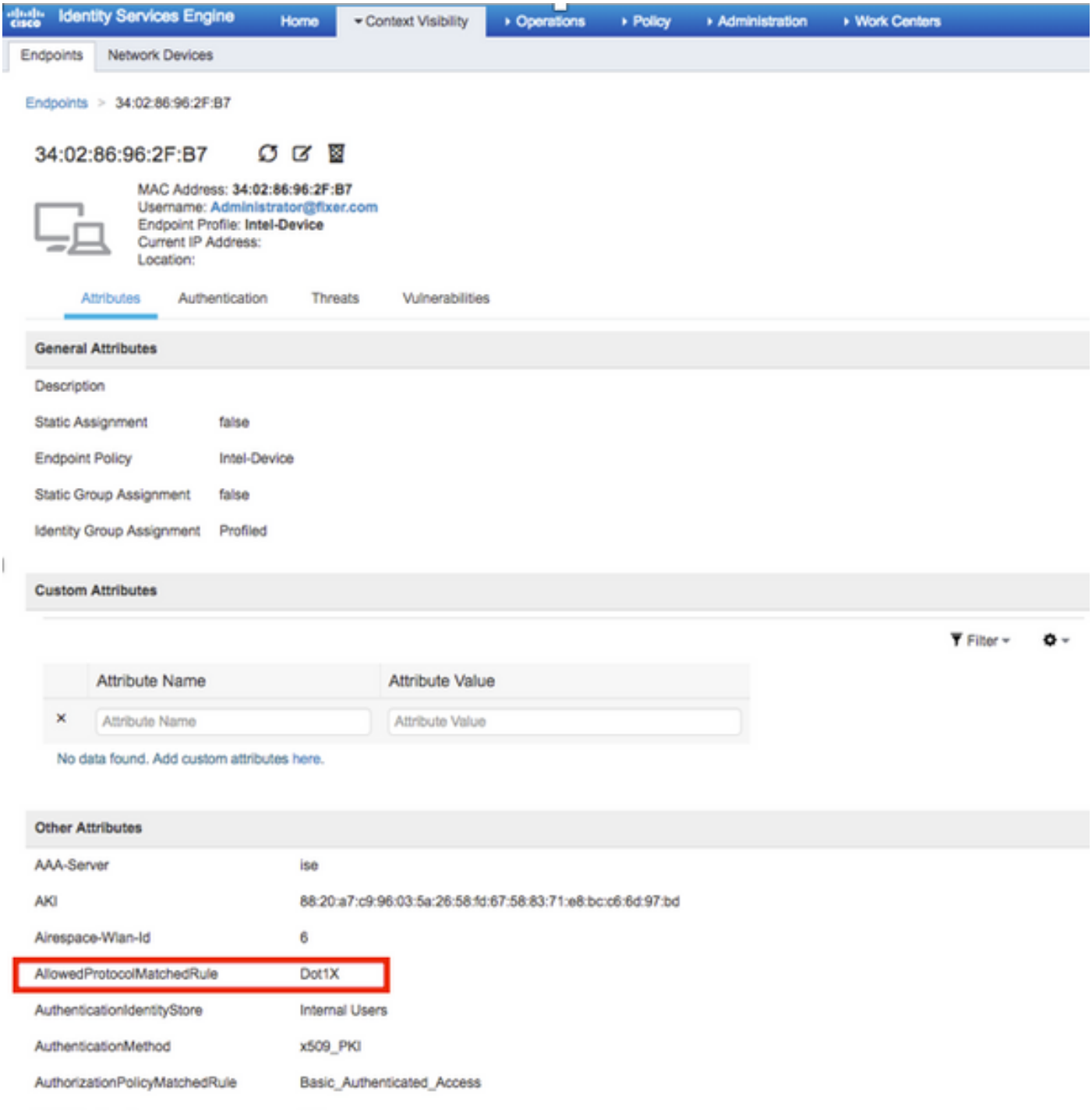




Stap 2. Dit is de clientdetails van CLI van de controller (vastgemaakt):

```
(Cisco Controller) >show client detail 34:02:86:96:2f:b7
Client MAC Address.............................. 34:02:86:96:2f:b7
Client Username ................................ Administrator
AP MAC Address.................................. c8:f9:f9:83:47:b0
AP Name......................................... AP442b.03a9.7f72
AP radio slot Id................................ 1
Client State.................................... Associated
Client User Group............................... Administrator
Client NAC OOB State............................ Access
Wireless LAN Id................................. 6
Wireless LAN Network Name (SSID)................ ME_EAP
Wireless LAN Profile Name....................... ME_EAP
Hotspot (802.11u)............................... Not Supported
BSSID........................................... c8:f9:f9:83:47:ba
Connected For .................................. 18 secs
Channel......................................... 56
IP Address...................................... 10.127.209.55
Gateway Address................................. 10.127.209.49
Netmask......................................... 255.255.255.240
IPv6 Address.................................... fe80::2818:15a4:65f9:842
--More-- or (q)uit
Security Policy Completed....................... Yes
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 3. Op ISE, navigeer naar **ACHTERGROND > Eindpunten > Eigenschappen** zoals in de afbeeldingen.


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Endpoints
Network Devices
Endpoints > 34:02:86:96:2F:B7
34:02:86:96:2F:B7
MAC Address: 34:02:86:96:2F:B7
Username: Administrator@fixer.com
Endpoint Profile: Intel-Device
Current IP Address:
Location:
Attributes
Authentication
Threats
Vulnerabilities
General Attributes
Description
Static Assignment false
Endpoint Policy Intel-Device
Static Group Assignment false
Identity Group Assignment Profiled
Custom Attributes
Filter
Attribute Name
Attribute Value
Attribute Name
Attribute Value
No data found. Add custom attributes here.
Other Attributes
AAA-Server ise
AKI 88:20:a7:c9:96:03:5a:26:58:fd:67:58:83:71:e8:bc:c6:6d:97:bd
Airespace-Wlan-Id 6
AllowedProtocolMatchedRule Dot1X
AuthenticationIdentityStore Internal Users
AuthenticationMethod x509_PKI
AuthorizationPolicyMatchedRule Basic_Authenticated_Access

BYODRegistration	Unknown
Called-Station-ID	c8-f9-f9-83-47-b0:ME_EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	344
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.127.209.56
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	21
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	12935 Supplicant stopped responding to ISE during
IdentityGroup	Profiled
InactiveDays	0
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA\,DC=fixer\,DC=co
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com
Key Usage	0, 2
Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7

MatchedPolicy	Intel-Device
MessageCode	5411
NAS-IP-Address	10.127.209.56
NAS-Identifier	ryo_ap
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	ryo_ap
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	Drop
SSID	c8-f9-f9-83-47-b0:ME_EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 00 11
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
StepData	4=Dot1X

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.