EAP-FAST-verificatie met draadloze LAN-controllers en Identity Services Engine

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Conventies](#)
[Achtergrondinformatie](#)
[PAC](#)
[PAC-provisioningmodules](#)
[Configureren](#)
[Netwerkdiagram](#)
[Configuraties](#)
[De WLC configureren voor EAP-FAST-verificatie](#)
[Configureer de WLC voor RADIUS-verificatie met een externe RADIUS-server](#)
[De WLAN-verificatie configureren voor EAP-FAST](#)
[De RADIUS-server configureren voor EAP-FAST-verificatie](#)
[Een gebruikersdatabase maken om EAP-FAST-clients te certificeren](#)
[Voeg WLC als AAA-client toe aan de RADIUS-server](#)
[EAP-FAST-verificatie op de RADIUS-server configureren met anonieme Inband-PAC-provisioning](#)
[EAP-FAST-verificatie op de RADIUS-server configureren met geverificeerde in-band PAC-provisioning](#)
[Verifiëren](#)
[NAM-profielconfiguratie](#)
[Test connectiviteit op SSID met behulp van EAP-FAST-verificatie.](#)
[ISE-authenticatielogs](#)
[WLC-zijde debug in succesvolle EAP-FAST-stroom](#)
[Problemen oplossen](#)

Inleiding

Dit document legt uit hoe u de draadloze LAN-controller (WLC) voor Extensible Authentication Protocol (EAP) kunt configureren - Flexibele verificatie via Secure Tunneling (FAST)-verificatie met behulp van een externe RADIUS-server. Dit configuratievoorbeeld gebruikt de Identity Services Engine (ISE) als de externe RADIUS-server om de draadloze client te authenticeren.

Dit document concentreert zich op de manier om de ISE voor Anonymous en Geautomatiseerde In-Band (Automatic) Protected Access Credentials (PAC) voorziening aan de draadloze klanten te configureren.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Basiskennis van de configuratie van lichtgewicht access points (LAP's) en Cisco WLC's
- Basiskennis van het CAPWAP-protocol
- Kennis van het configureren van een externe RADIUS-server, zoals Cisco ISE
- Functionele kennis van het algemene MAP-kader
- Basiskennis over veiligheidsprotocollen, zoals MS-CHAPv2 en EAP-GTC, en kennis over digitale certificaten

Gebruikte componenten

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

- Cisco 5520 Series WLC-software met firmware release 8.8.11.0Cisco 4800 Series AP-switchesAnyConnect NAM.Cisco Secure ISE versie 2.3.0.29Cisco Catalyst 3560-CX Series switch met versie 15.2(4)E1

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 de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Het EAP-FAST-protocol is een voor het publiek toegankelijk type IEEE 802.1X MAP dat Cisco ontwikkelde om klanten te ondersteunen die geen sterk wachtwoordbeleid kunnen afdwingen en een MAP 802.1X willen inzetten dat geen digitale certificaten vereist.

Het EAP-FAST-protocol is een client-server security architectuur die EAP-transacties versleutelt met een TLS-tunnel (Transport Level Security). De totstandbrenging van de EAP-FAST-tunnel is gebaseerd op sterke geheimen die uniek zijn voor de gebruikers. Deze sterke geheimen worden PAC's genoemd, die de ISE genereert door gebruik te maken van een hoofdtoets die alleen bekend staat bij de ISE.

EAP-FAST vindt in drie fasen plaats:

- **Fase nul (automatische PAC-provisioningfase)**—EAP-FAST fase nul, een optionele fase is een tunnelveilig middel om een EAP-FAST eindgebruikerclient een PAC te bieden voor de gebruiker die netwerktoegang wenst. **Het verstrekken van een PAC aan de eindgebruiker-cliënt is het enige doel van fase nul**.**Opmerking:** Fase nul is optioneel omdat PAC's ook handmatig aan klanten kunnen worden geleverd in plaats van fase nul.Zie het gedeelte PAC-provisioningmodellen van dit document voor meer informatie.
- **Fase één**—In fase één zetten de ISE en de eindgebruiker client een TLS-tunnel op basis van de PAC-gecrediteerd van de gebruiker. Deze fase vereist dat de eindgebruiker client een PAC

is verstrekt voor de gebruiker die probeert toegang tot het netwerk te verkrijgen, en dat de PAC gebaseerd is op een hoofdtoets die niet is verlopen. Geen netwerkservice is mogelijk door fase één van EAP-FAST.
- **Fase twee**—In fase twee worden gebruikersverificatiegeloofsbrieven veilig doorgegeven met behulp van een interne MAP-methode die wordt ondersteund door EAP-FAST binnen de TLS-tunnel naar de RADIUS die wordt gecreëerd met behulp van de PAC tussen de client en de RADIUS-server. EAP-GTC, TLS en MS-CHAP worden ondersteund als innerlijke MAP-methoden. Voor EAP-FAST worden geen andere MAP-typen ondersteund.

Raadpleeg Hoe EAP-FAST werkt voor meer informatie.

PAC

PAC's zijn sterke gedeelde geheimen die de ISE en een MAP-FAST eindgebruiker-cliënt in staat stellen elkaar te authenticeren en een TLS-tunnel op te zetten voor gebruik in EAP-FAST fase twee. ISE genereert PAC's met behulp van de actieve hoofdtoets en een gebruikersnaam.

PAC omvat:

- **PAC-Key**-Gedeeld geheim gebonden aan een client (en client-apparaat) en server-identiteit.
- **PAC ondoorzichtig**-ondoorzichtig veld dat de client caches geeft en naar de server doorgeeft. De server herstelt de PAC-Key en de client-identiteit om deze wederzijds te bevestigen met de client.
- **PAC-Info** - Op z'n minst omvat de identiteit van de server om de client in staat te stellen om verschillende PAC's te casten. Optioneel bevat het andere informatie zoals de vervaltijd van de PAC.

PAC-provisioningmodules

Zoals eerder vermeld is fase nul een optionele fase.

EAP-FAST biedt twee opties om een klant een PAC te verschaffen:

- **Automatische PAC-provisioning (EAP-FAST fase 0 of Inband PAC-provisioning)**
- **Handmatige (out-of-band) PAC-provisioning**

In-band/automatische PAC-voorziening verstuurt een nieuwe PAC naar een eindgebruiker-client via een beveiligde netwerkverbinding. Automatische PAC-provisioning vereist geen interventie van de netwerkgebruiker of een ISE-beheerder, mits u de ISE en de eindgebruiker client configureren ter ondersteuning van automatische provisioning.

De nieuwste EAP-FAST-versie ondersteunt twee verschillende in-band PAC-provisioningopties:

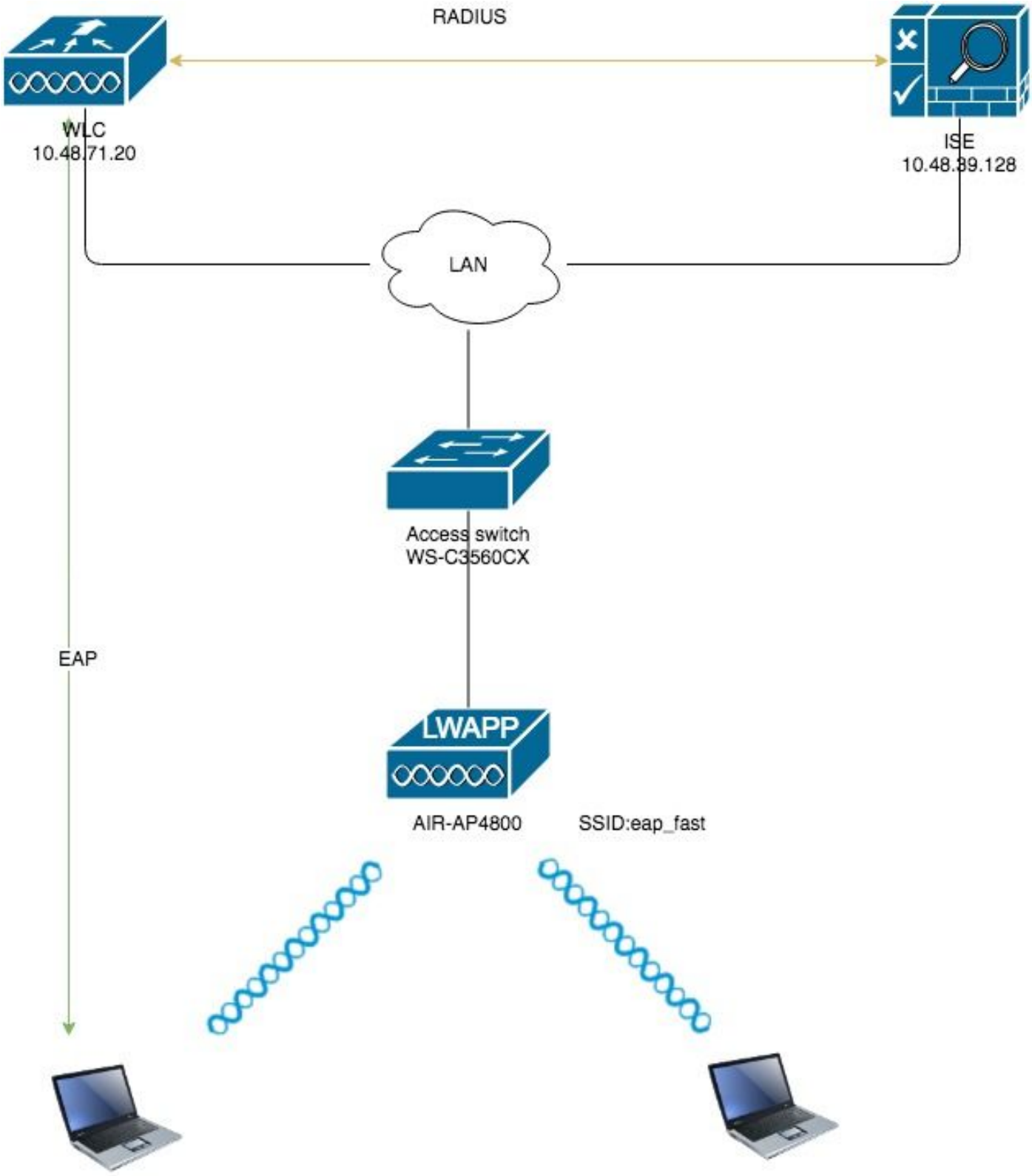
- **Anoniem in-band PAC-provisioning**
- **Geautomatiseerde in-band PAC-provisioning**

Opmerking: Dit document behandelt deze in-band PAC-provisioningmethoden en de manier waarop u deze kunt configureren.

Voor out-of-band/handmatige PAC-provisioning is een ISE-beheerder nodig om PAC-bestanden te genereren, die dan moeten worden gedistribueerd naar de toepasbare netwerkgebruikers. De gebruikers moeten de eindgebruikerscliënten met hun PAC-bestanden configureren.

Configureren

Netwerkdiagram



Configuraties

De WLC configureren voor EAP-FAST-verificatie

Voer deze stappen uit om de WLC voor EAP-FAST-verificatie te configureren:

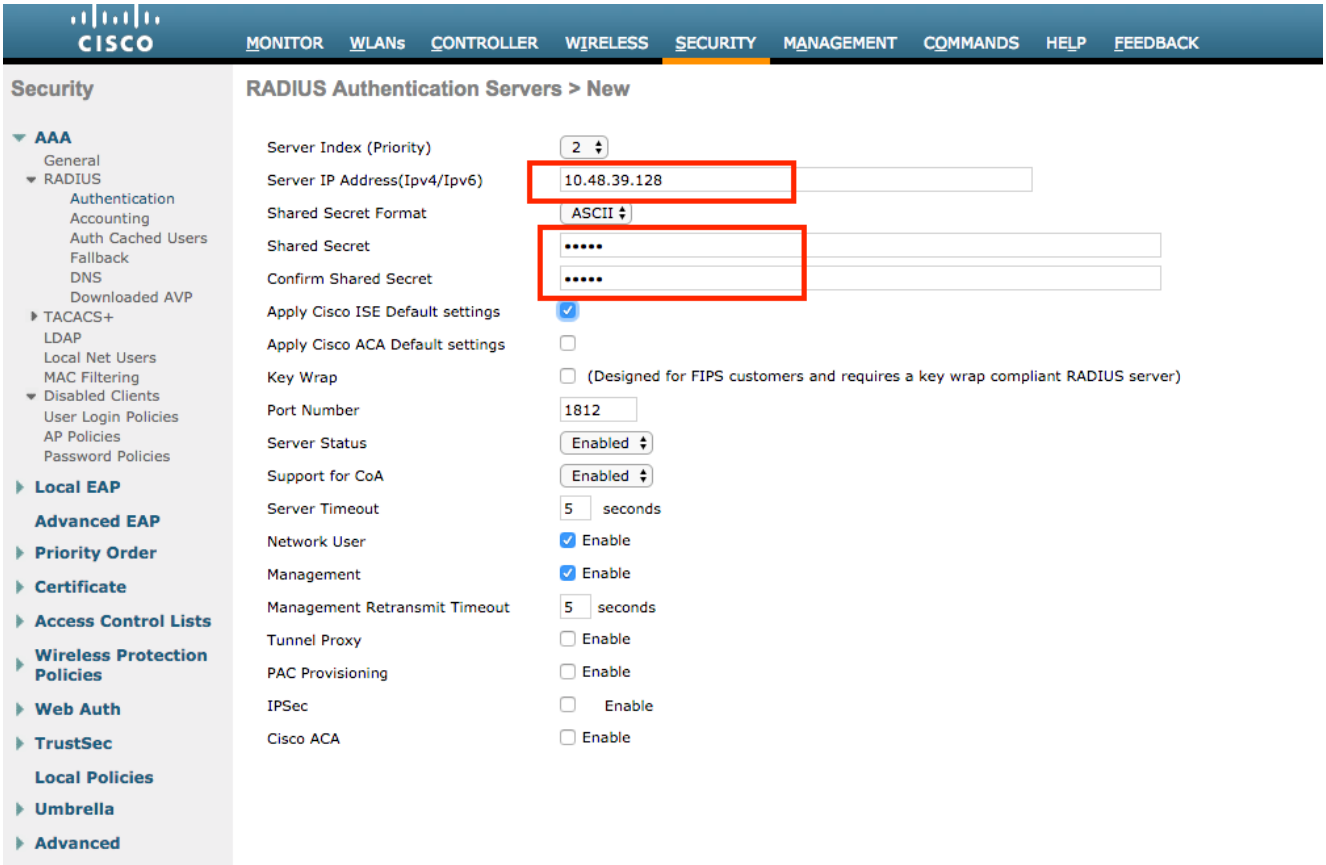
1. Configureer de WLC voor RADIUS-verificatie met een externe RADIUS-server
2. De WLAN-verificatie configureren voor EAP-FAST

Configureer de WLC voor RADIUS-verificatie met een externe RADIUS-server

De WLC moet worden geconfigureerd om de gebruikersreferenties naar een externe RADIUS-server te kunnen doorsturen. De externe RADIUS-server bevestigt vervolgens de gebruikersreferenties met EAP-FAST en geeft toegang tot de draadloze klanten.

Voltooi deze stappen om de WLC te configureren voor een externe RADIUS-server:

1. Kies **Security** en **RADIUS-verificatie** van de controller GUI om de pagina RADIUS-verificatieservers weer te geven. Klik vervolgens op **New** om een RADIUS-server te definiëren.
2. Defineert de parameters van de RADIUS-server op de **RADIUS-verificatieservers > Nieuwe** pagina. Deze parameters omvatten:IP-adres voor RADIUS-serversGedeeld geheimPoortnummerServerstatusDit document gebruikt de ISE-server met een IP-adres van 10.48.39.128.



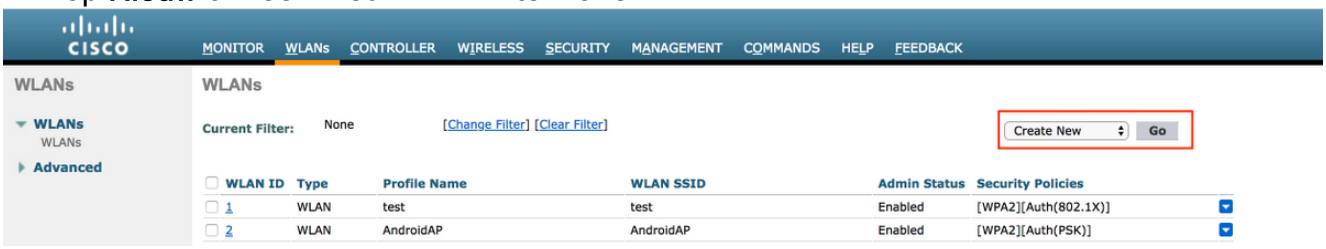
3. Klik **Toepassen**.

De WLAN-verificatie configureren voor EAP-FAST

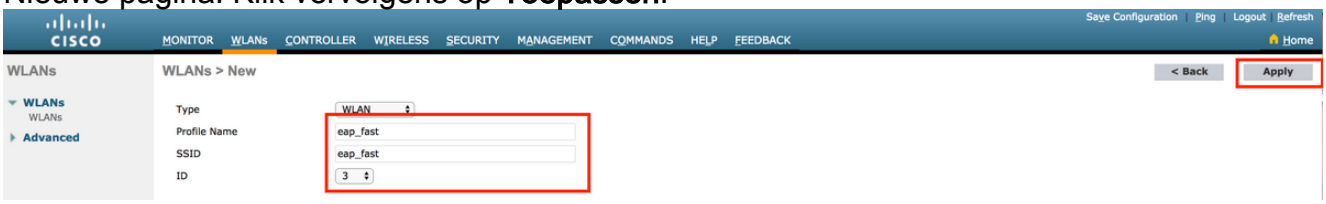
Daarna moet u de WLAN-functie configureren die de clients gebruiken om verbinding te maken met het draadloze netwerk voor EAP-FAST-verificatie en een dynamische interface toewijzen. De WLAN-naam die in dit voorbeeld wordt ingesteld, is **eenvoudig**. Dit voorbeeld wijst dit WLAN aan de beheerinterface toe.

Voltooi deze stappen om de **snelle** WLAN-functie en de bijbehorende parameters te configureren:

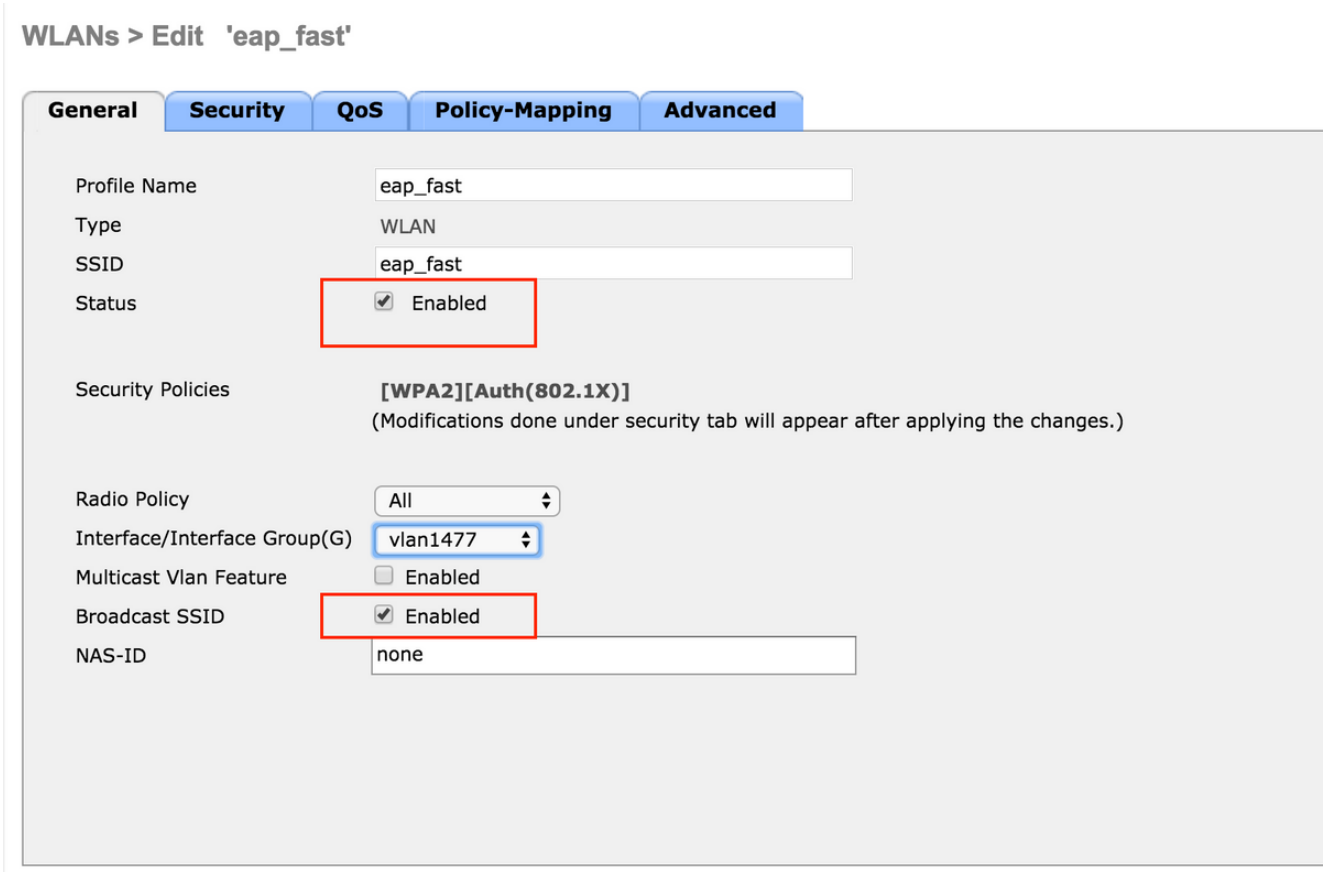
1. Klik op **WLAN's** vanuit de GUI van de controller om de WLAN's pagina weer te geven.Deze pagina toont de WLAN's die op de controller bestaan.
2. Klik op **Nieuw** om een nieuw WLAN te maken.



3. Configureer de naam **eap_fast** WLAN SSID, profielnaam en WLAN-id op de WLAN's **>** Nieuwe pagina. Klik vervolgens op **Toepassen**.

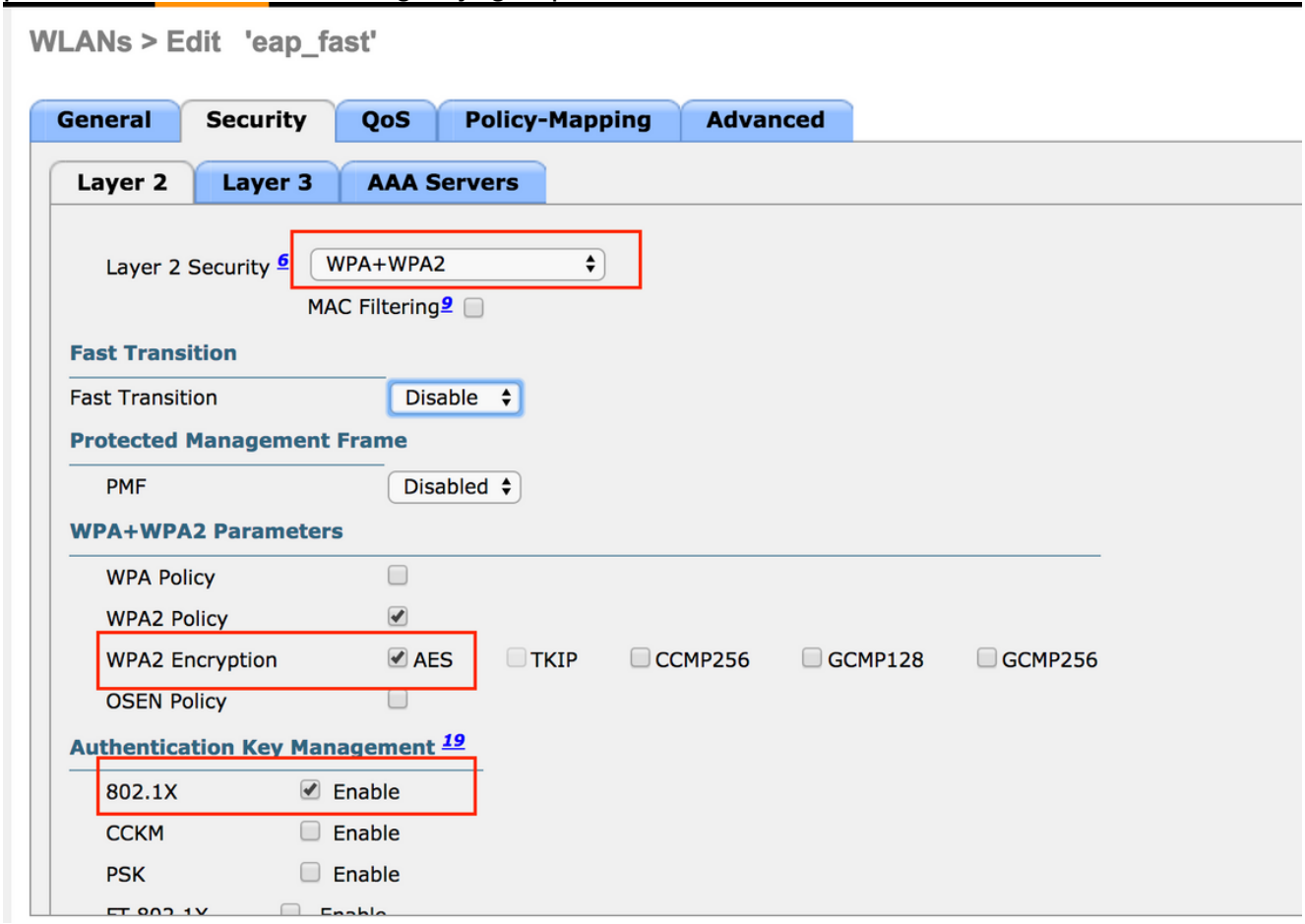


4. Zodra u een nieuw WLAN hebt gemaakt, wordt de **WLAN >** pagina **bewerken** voor de nieuwe WLAN weergegeven. Op deze pagina kunt u verschillende parameters definiëren die specifiek zijn voor dit WLAN. Dit omvat algemeen beleid, RADIUS-servers, beveiligingsbeleid en 802.1x-parameters.
5. Controleer het aanvinkvakje **Admin Status** onder het **tabblad Algemeen** beleid om het WLAN in te schakelen. Als u wilt dat AP de SSID in zijn beacon kaders uitzendt, controleer het aanvinkvakje **Broadcast SSID**.

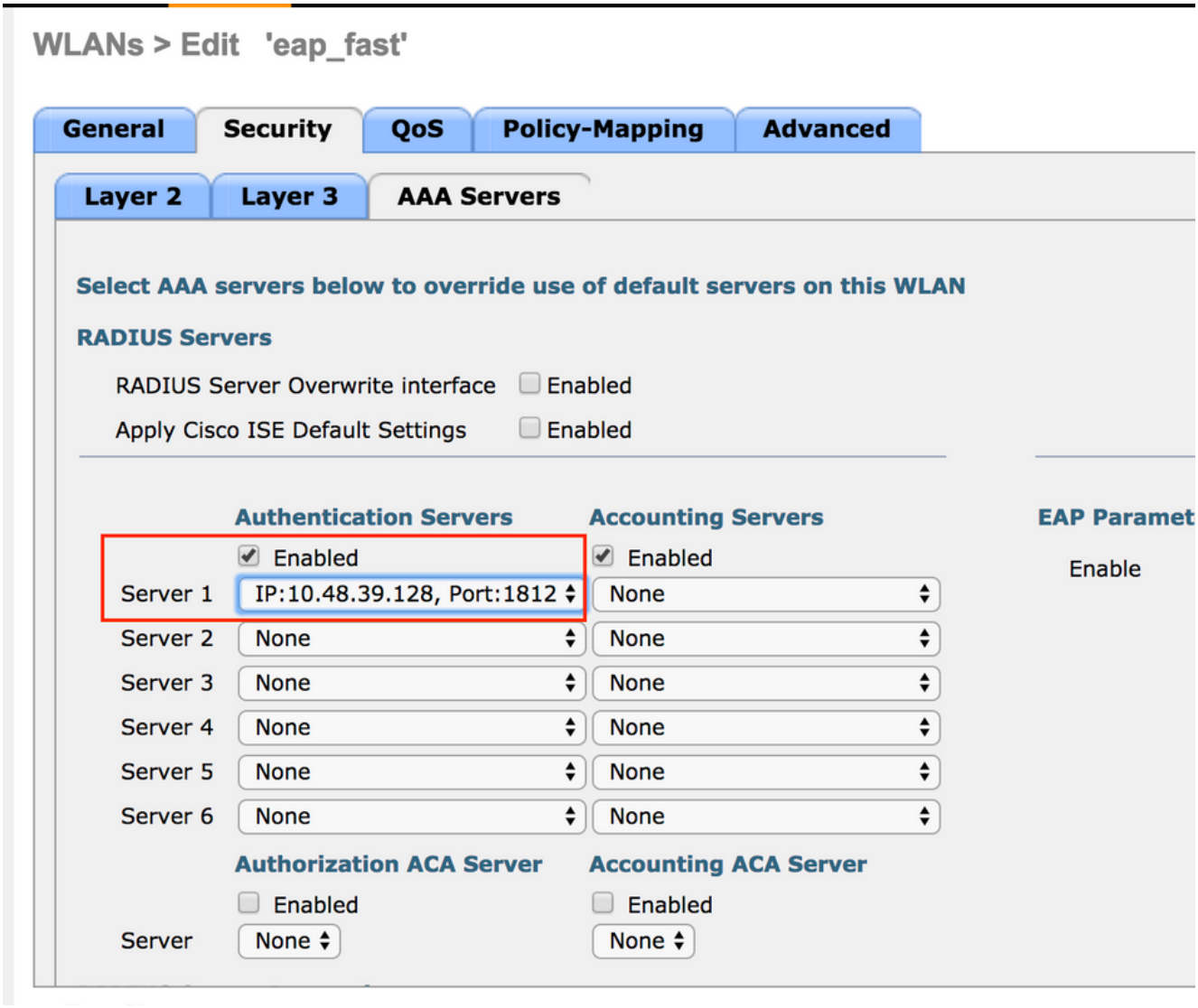


6. Onder **"WLAN -> Bewerken -> Beveiliging -> Layer 2"** Kies het tabblad WAP/WAP2-parameters en selecteer de optie punt1x voor AKM.

Dit voorbeeld gebruikt WAP2/AES + dot1x als Layer 2 beveiliging voor dit WLAN. De andere parameters kunnen worden gewijzigd op basis van de vereisten van het WLAN-netwerk.



7. Onder "**WLAN -> Bewerken -> Beveiliging -> AAA-servers**" kiest u de juiste RADIUS-server uit het keuzemenu onder RADIUS-servers.



8. Klik op **Toepassen**.**Toelichting:** Dit is de enige MAP-instelling die op de controller moet worden ingesteld voor MAP-verificatie. Alle andere configuraties die specifiek zijn voor EAP-FAST moeten worden uitgevoerd op de RADIUS-server en de klanten die geauthentiseerd moeten worden.

De RADIUS-server configureren voor EAP-FAST-verificatie

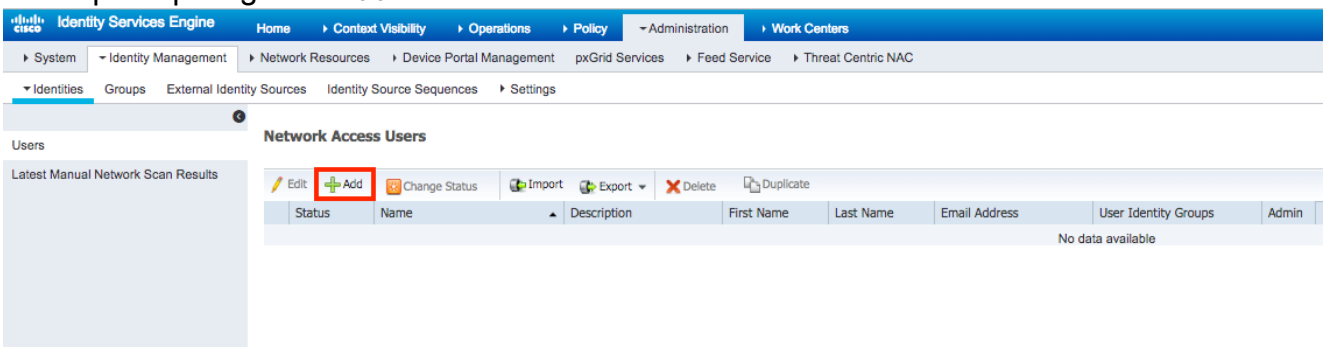
Voer deze stappen uit om de RADIUS-server voor EAP-FAST-verificatie te configureren:

1. Een gebruikersdatabase maken om EAP-FAST-clients te certificeren
2. Voeg WLC als AAA-client toe aan de RADIUS-server
3. EAP-FAST-verificatie op de RADIUS-server configureren met anonieme Inband-PAC-provisioning
4. EAP-FAST-verificatie op de RADIUS-server configureren met geverificeerde in-band PAC-provisioning

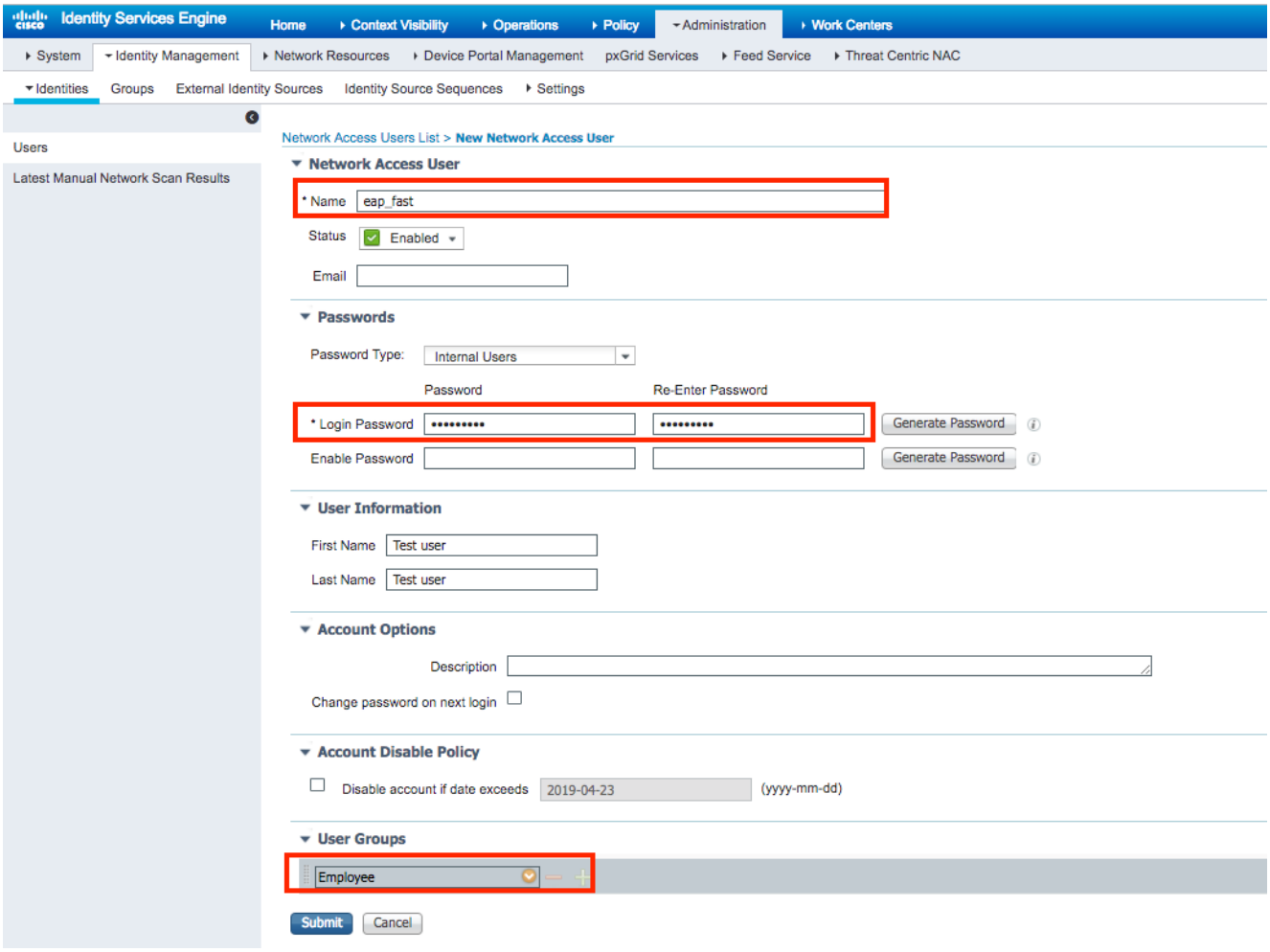
Een gebruikersdatabase maken om EAP-FAST-clients te certificeren

In dit voorbeeld worden de gebruikersnaam en het wachtwoord van de EAP-FAST-client ingesteld als respectievelijk <*eap_fast*> en <*EAP-fast1*>.

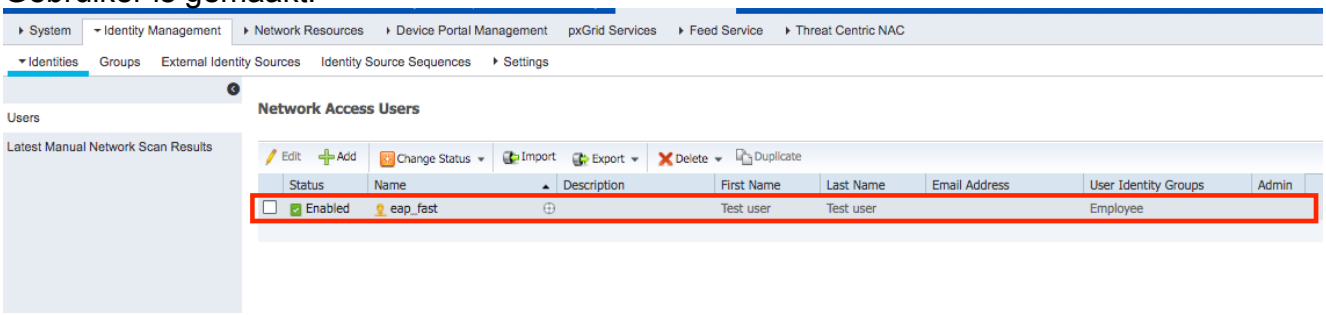
1. In ISE Web admin UI navigeren onder **"Beheer -> Identity Management -> Gebruikers"** en druk op het pictogram **"Add"**.



2. Vul vereiste formulieren in zodat de gebruiker kan worden gemaakt - **"Naam"** en **"Wachtwoord voor loggen"** en selecteer **"Gebruikersgroep"** uit de vervolgkeuzelijst.[Opties dat u andere informatie voor de gebruikersaccount kunt invullen]
Druk op **"Sumbit"**



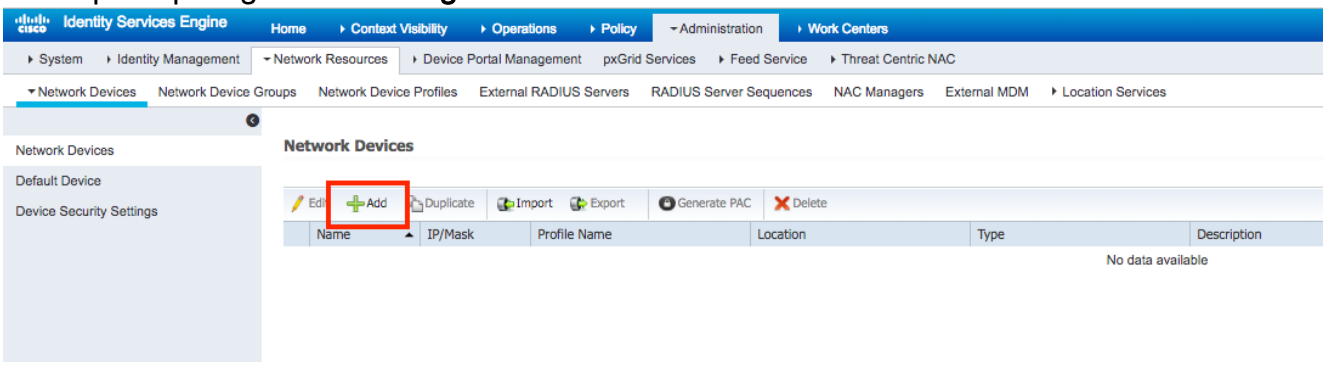
3. Gebruiker is gemaakt.



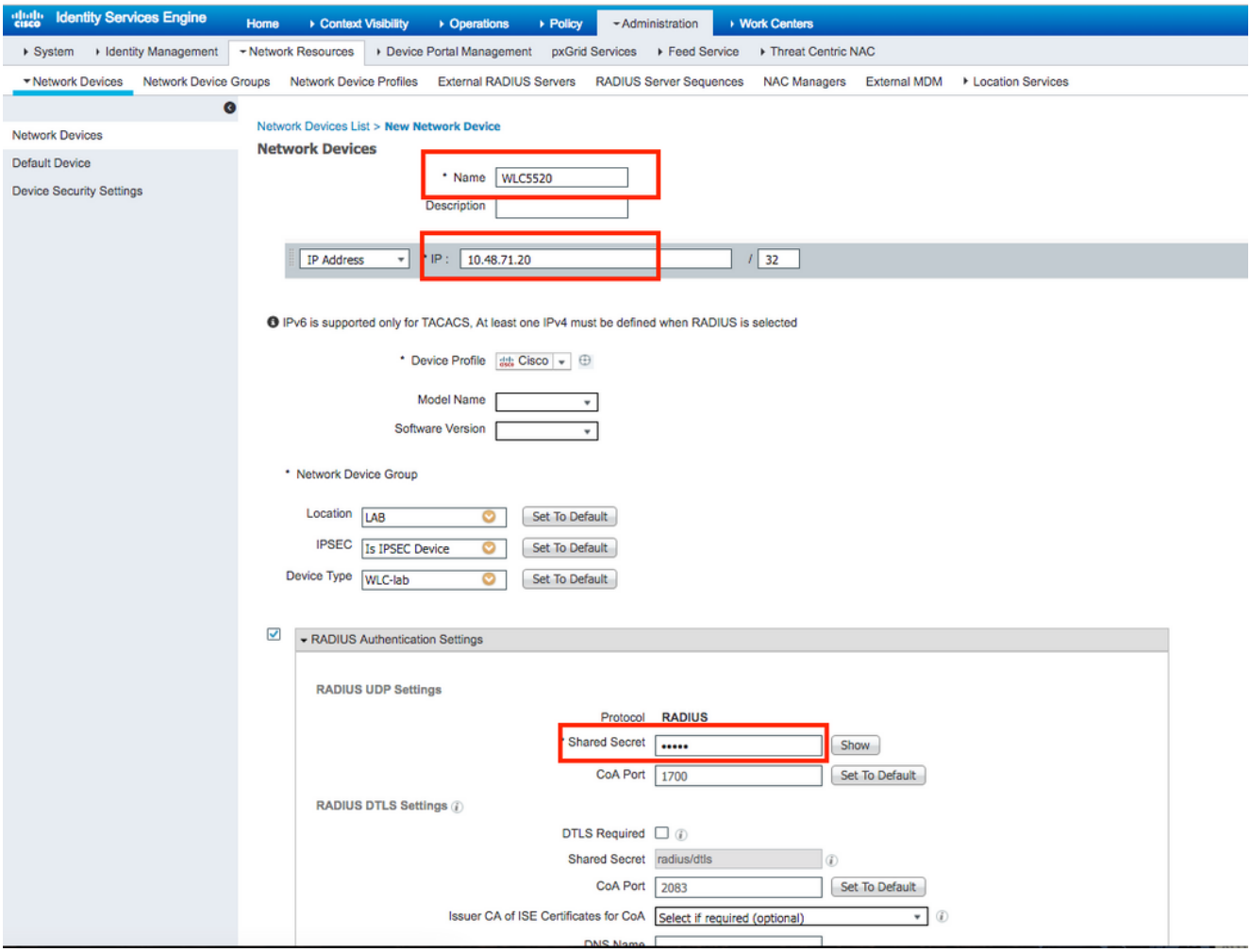
Voeg WLC als AAA-client toe aan de RADIUS-server

Voltooi deze stappen om de controller te definiëren als een AAA-client op de ACS-server:

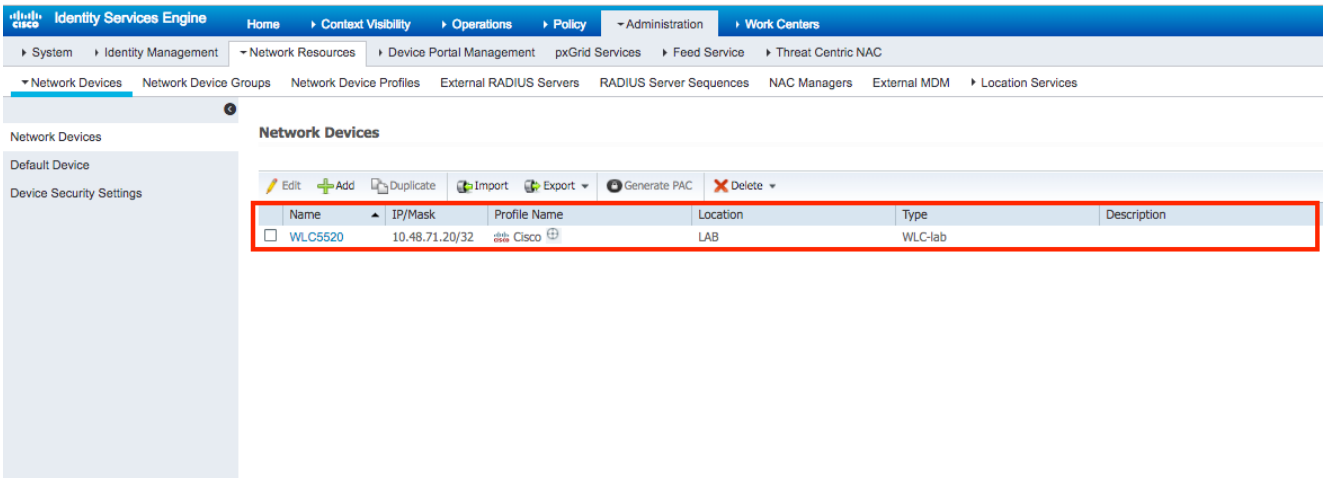
1. In ISE Web admin UI navigeer onder **"Beheer -> Netwerkbronnen -> Netwerkapparaten"** en druk op het pictogram **"Toevoegen"**.



2. Vul vereiste formulieren in zodat een apparaat kan worden toegevoegd - **"Naam"**, **"IP"** en stel hetzelfde gedeelde geheime wachtwoord in zoals we in eerder vak op WLC hebben ingesteld in het formulier **"Gedeeld geheim"** [optioneel: u kunt andere informatie voor het apparaat invullen zoals locatie, groep, enzovoort].
Druk op "**Sumbit**"



3. Het apparaat wordt toegevoegd aan de lijst met ISE-toegangsapparaat. (NAD)

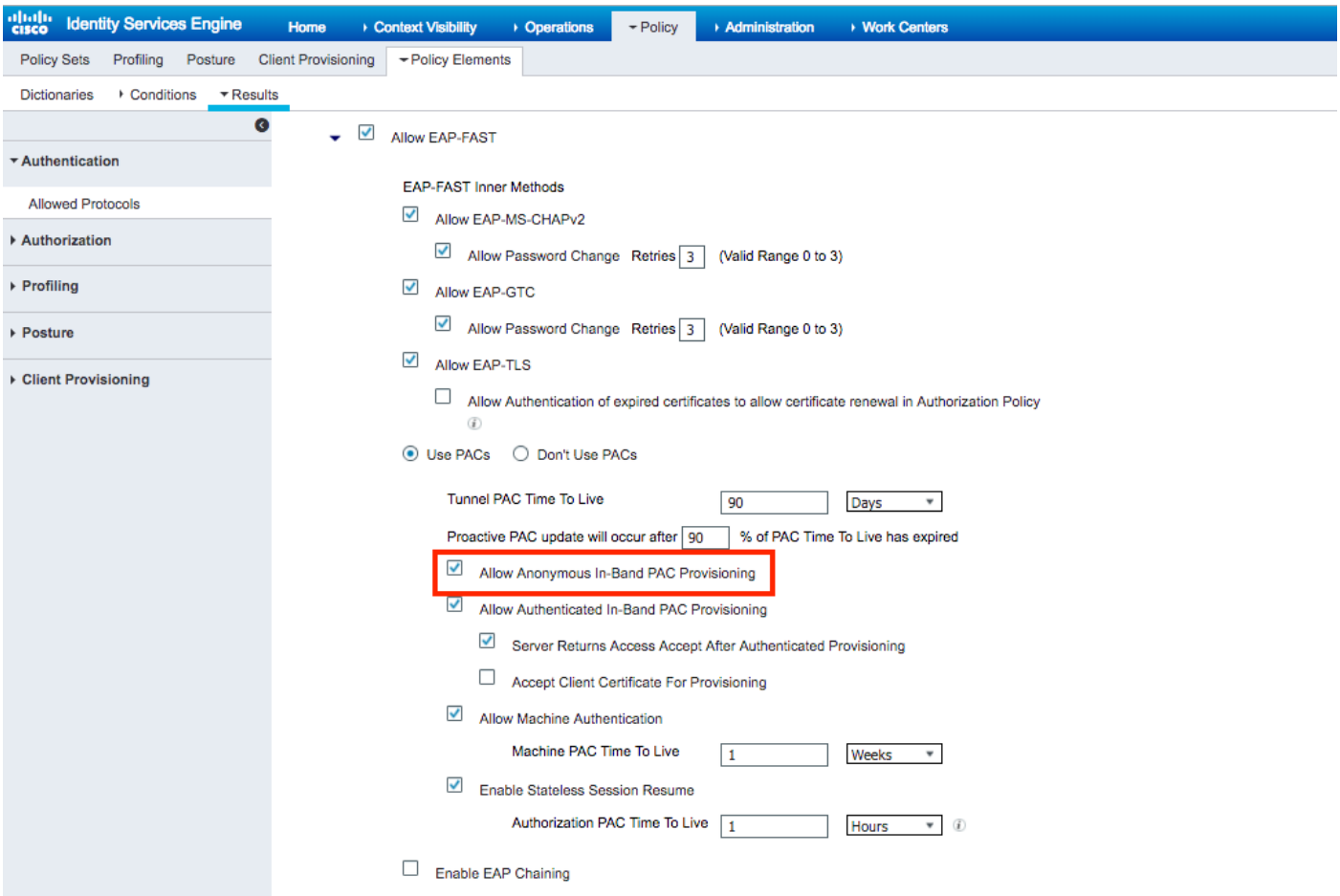


EAP-FAST-verificatie op de RADIUS-server configureren met anonieme Inband-PAC-provisioning

Over het algemeen wil je dit type methode gebruiken voor het geval dat ze geen PKI-infrastructuur hebben in hun implementatie.

Deze methode werkt binnen een Authenticated Diffie-Hellman Key Agreement Protocol (ADHP)-tunnel voordat de peer de ISE-server authentiek verklaart.

Om deze methode te ondersteunen moeten we "**Laat anonieme In-band PAC Provisioning**" op ISE mogelijk maken onder de "**Verificatie toegestaan protocollen**":



Opmerking: Zorg ervoor dat u een wachtwoord type autorisatie hebt toegestaan, zoals EAP-MS-CHAPv2 voor EAP-FAST binnenmethode, omdat we natuurlijk met Anonymous In-band

Provisioning geen certificaten kunnen gebruiken.

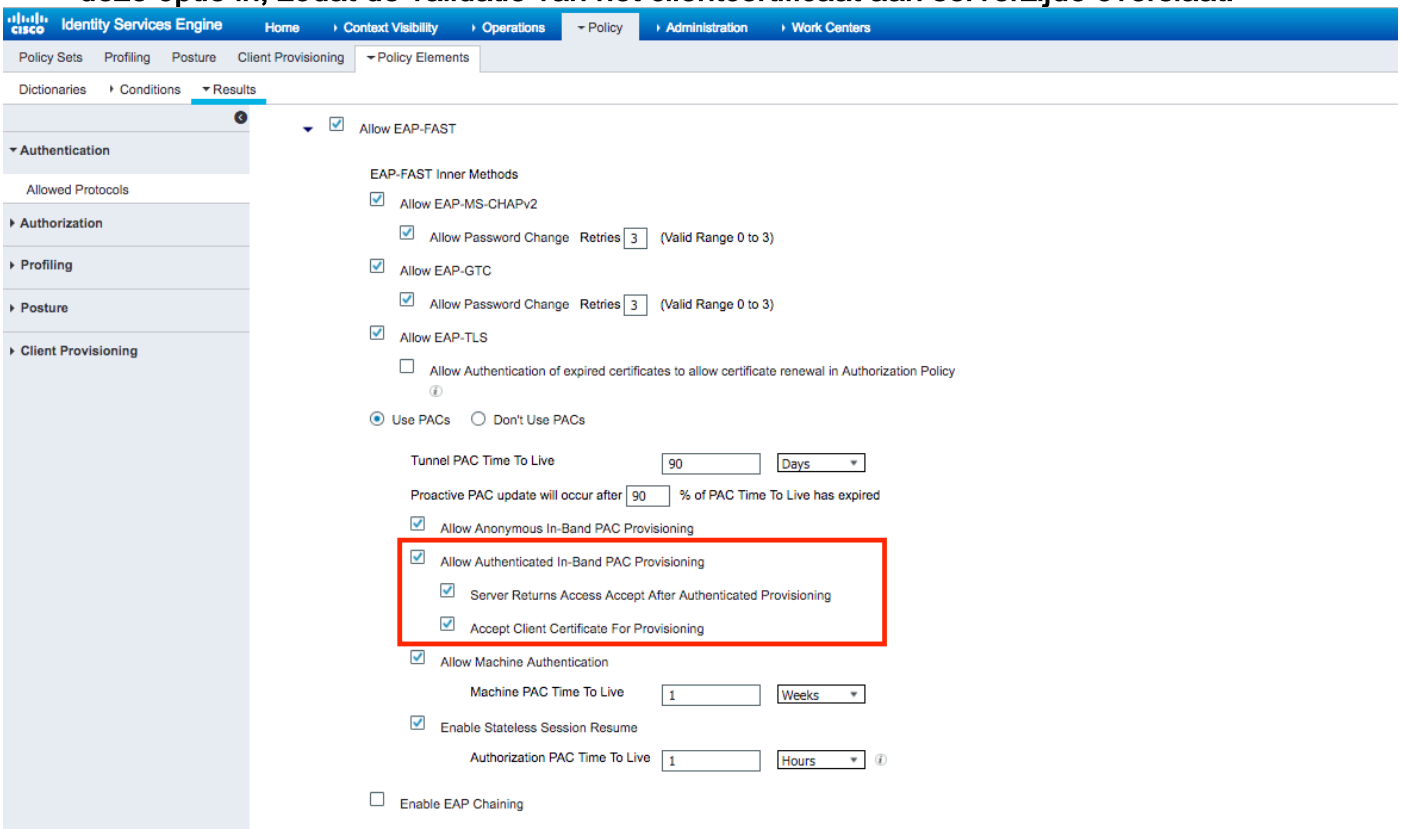
EAP-FAST-verificatie op de RADIUS-server configureren met geverificeerde in-band PAC-provisioning

Dit is de best beveiligde en aanbevolen optie. De TLS-tunnel is gebouwd op basis van het servercertificaat dat is gevalideerd door het leveringscertificaat en het certificaat van scheiding is gevalideerd door ISE (standaard).

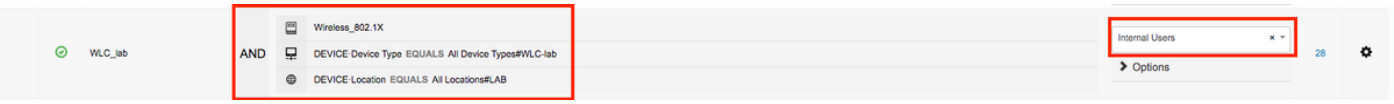
Voor die optie is een PKI-infrastructuur nodig voor client en server, hoewel de PKI-infrastructuur alleen aan serverkant is toegestaan of aan beide kanten is overgeslagen.

Op ISE zijn er twee extra opties voor Voor Verifieerde In-band provisioning:

1. **"Server Retourenaccess accepteren na geauthentiseerde provisioning"** - Normaal gesproken, na PAC-provisioning, dient een toegangsverwerp te worden verzonden, waarbij de aanvrager wordt gedwongen om het gebruik van PAC's te reauthentiseren. Maar omdat PAC-provisioning wordt uitgevoerd in geauthenticeerde TLS-tunnels kunnen we onmiddellijk reageren met Access-Accept om de authenticatietijd te minimaliseren. (in dat geval moet u ervoor zorgen dat u de certificaten aan de kant plint en de server hebt vertrouwd).
2. **"Accept Client certificaatcertificaat for Provisioning" - indien men geen PKI-infrastructuur aan clientapparaten wil leveren en alleen een betrouwbaar certificaat op ISE heeft, schakelt u deze optie in, zodat de validatie van het clientcertificaat aan serverzijde overslaat.**



Op ISE definiëren we ook eenvoudig authentificatiebeleid dat voor draadloze gebruikers is ingesteld. Hieronder wordt bijvoorbeeld gebruikt als parameter van het type en locatie en authenticatie type, dan wordt authenticatie flow matching die voorwaarde gevalideerd aan de hand van interne gebruikersdatabase.



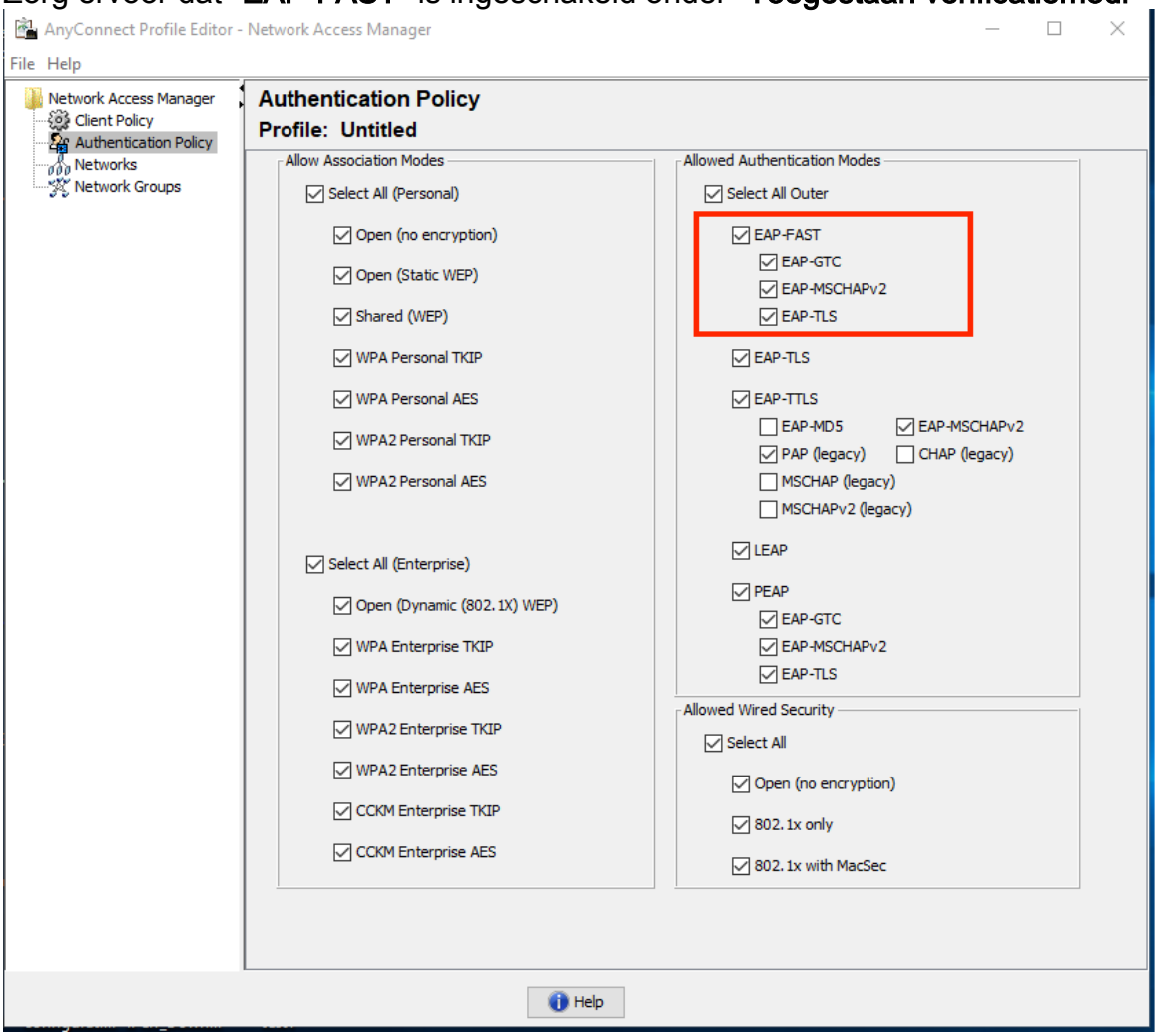
Verifiëren

Dit voorbeeld zal de geauthentiseerde In-band PAC Provisioning Flow en de configuratie van het Netwerk Access Manager (NAM) samen met respectieve WLC-debugs tonen.

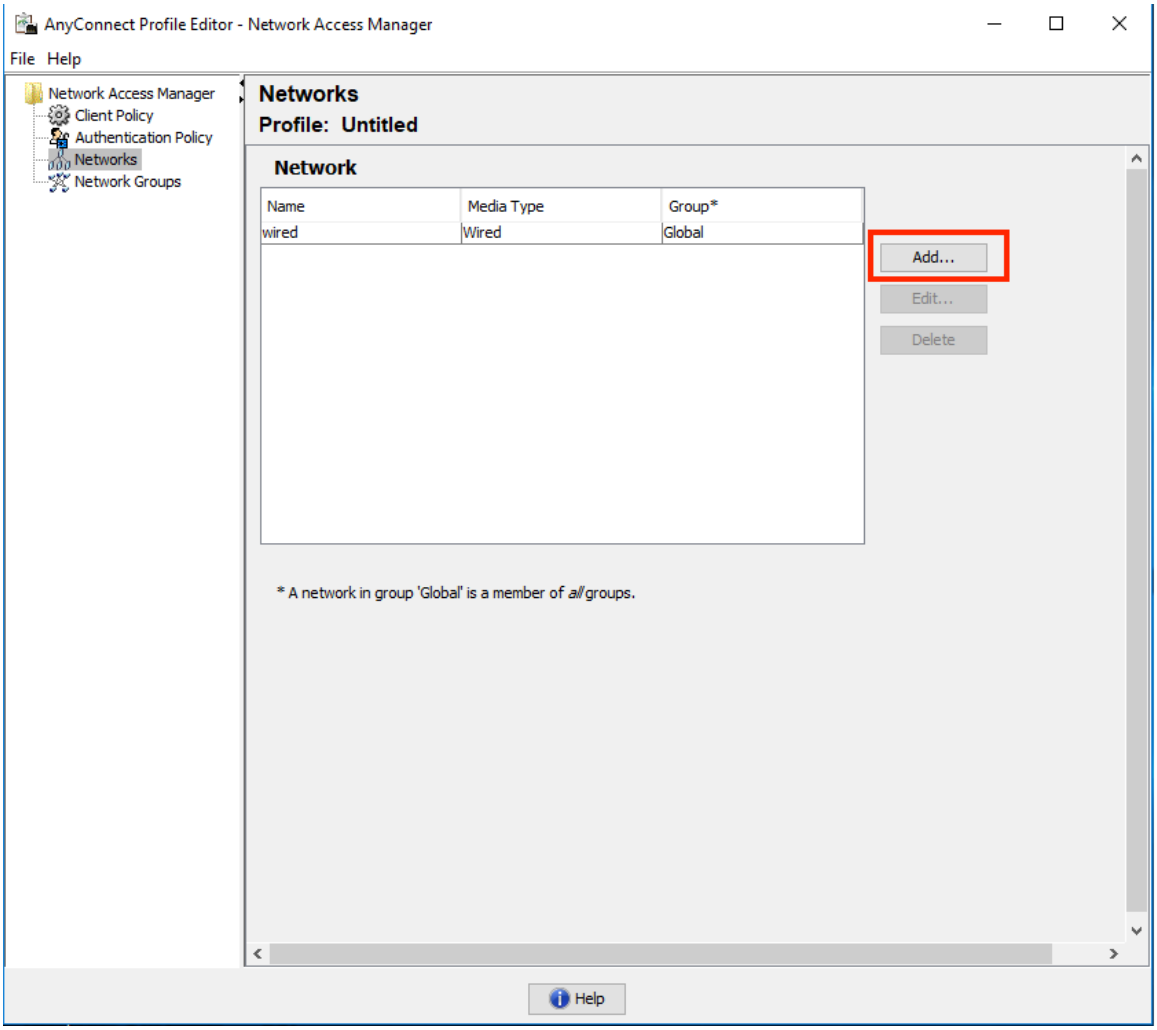
NAM-profielconfiguratie

Er moeten de volgende stappen worden gezet om het NAM-profiel van AnyConnect te configureren om gebruikerssessie tegen ISE te bevestigen met behulp van EAP-FAST:

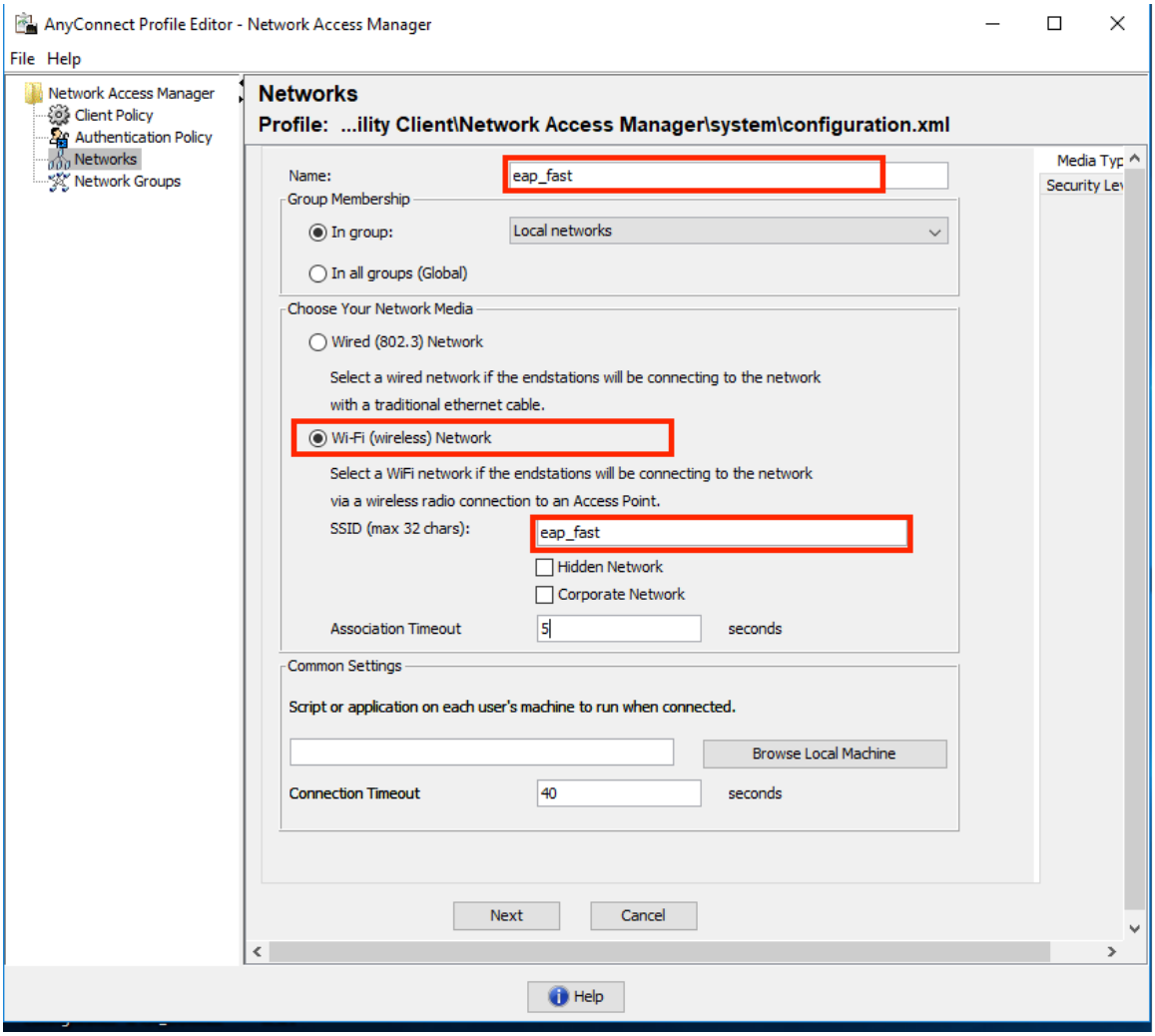
1. Profieleditor van Open Network Access Manager en laadt het huidige configuratiebestand.
2. Zorg ervoor dat "**EAP-FAST**" is ingeschakeld onder **"Toegestaan verificatiemodi"**



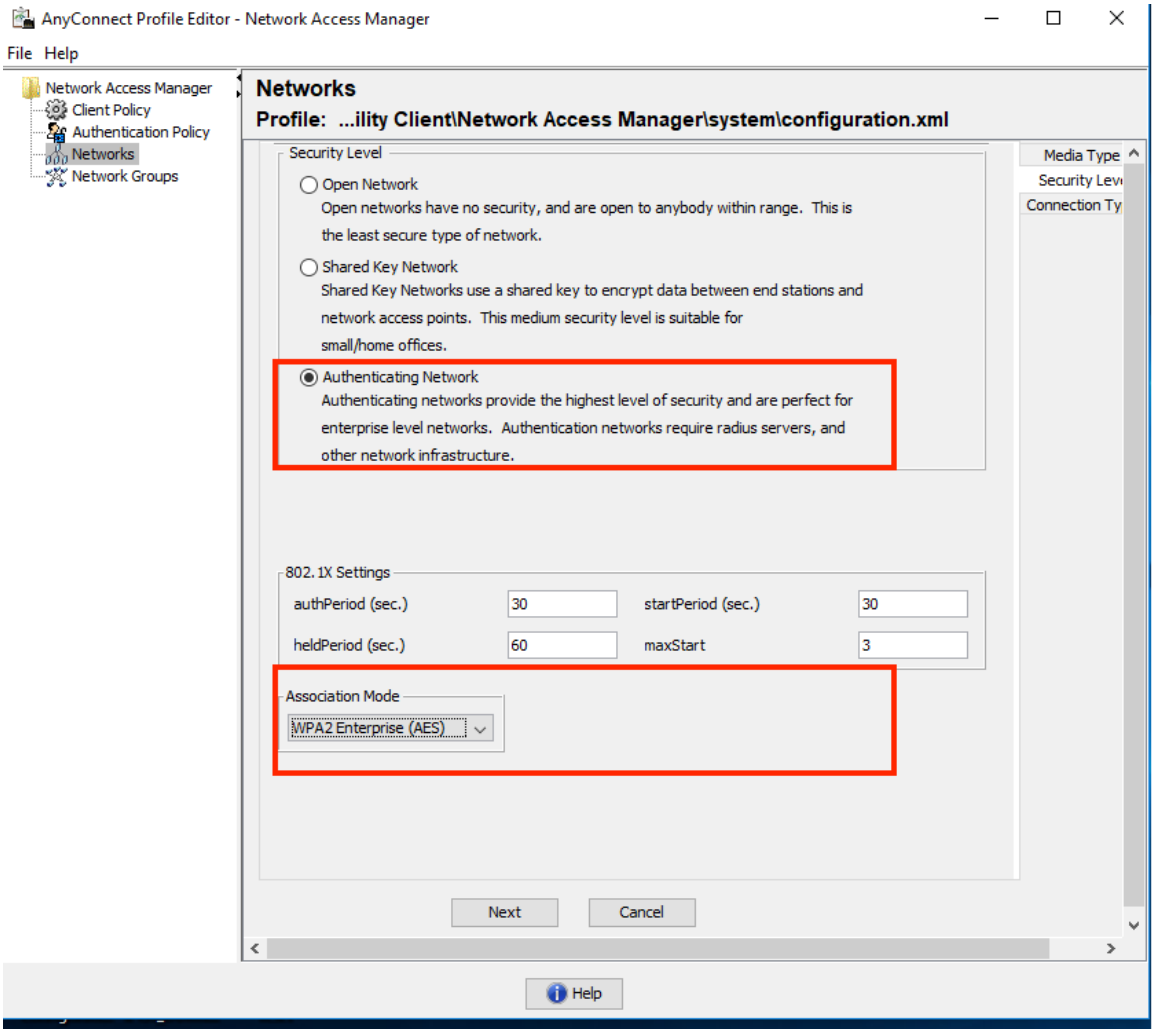
3. **"Voeg"** een nieuw netwerkprofiel toe:



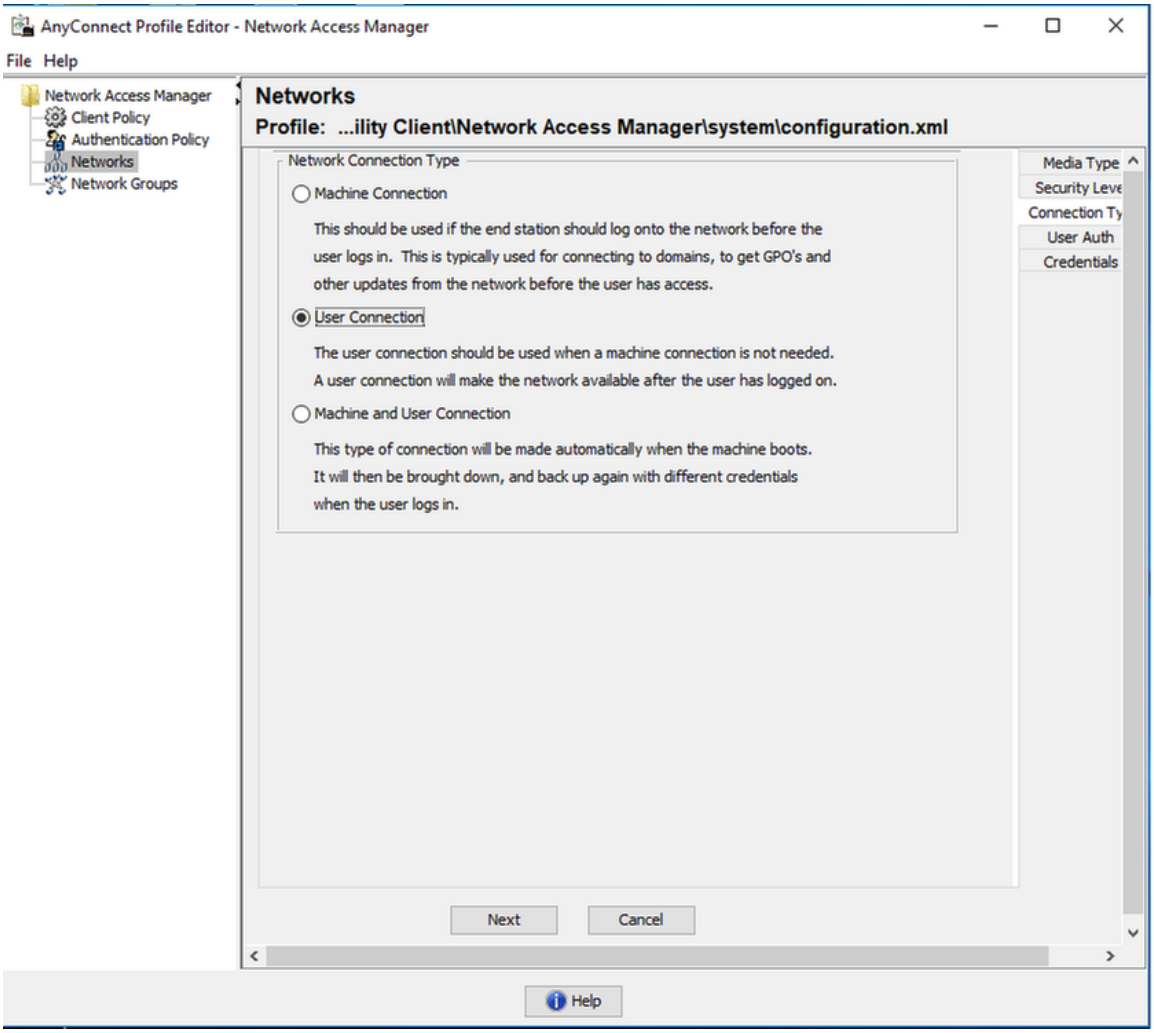
4. Onder **"Mediatype"** definieert de configuratie sectie profiel "**Naam**", draadloze verbinding als uw medianetype en specificeer de naam SSID.



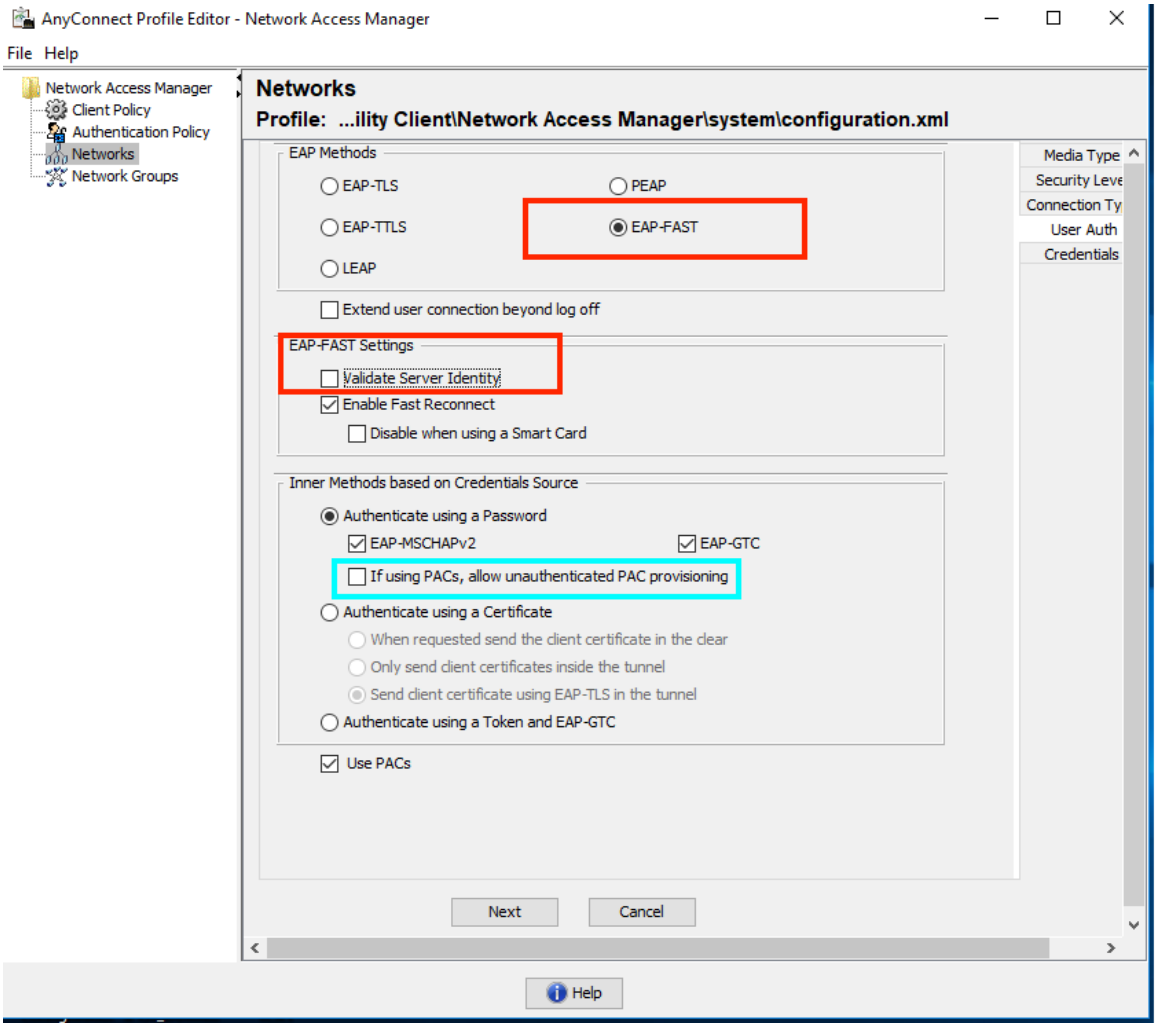
5. Selecteer onder **het** tabblad "**Security Level**" het optie "Veriating Network" en specificeer de associatiemodus als WAP2 Enterprise (AES)



6. In dit voorbeeld gebruiken we gebruikerstype authenticatie, daarom onder volgende tab "**Connection type**" selecteert u "**User Connection**"

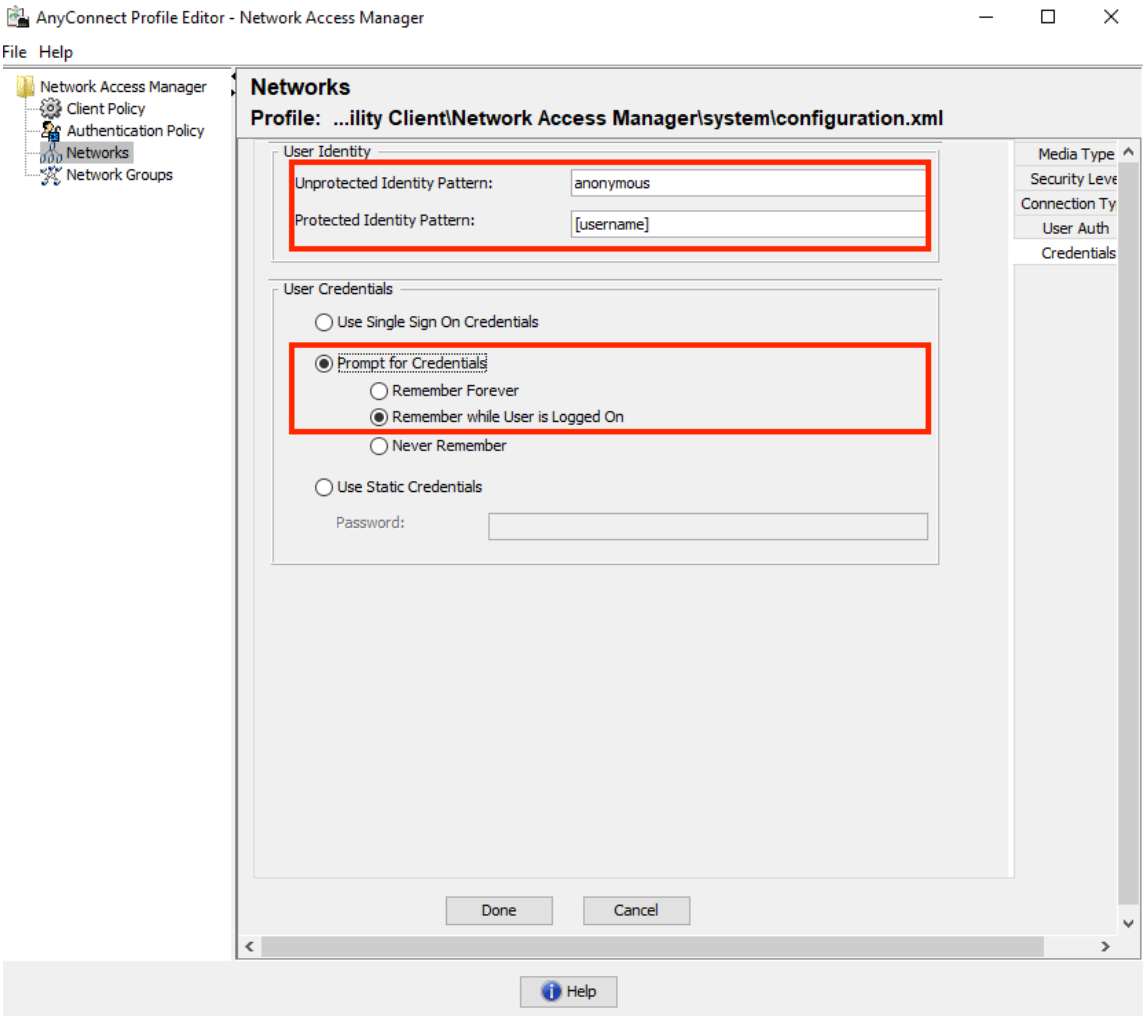


7. Specificeer onder "**User Auth**"-tabblad EAP-FAST als toegestane authenticatiemethode en verlaag de validatie van servercertificaten omdat we in dit voorbeeld geen vertrouwde certificaten gebruiken.



Opmerking: in de reële productieomgeving zorgt ervoor dat u het certificaat dat op ISE is geïnstalleerd, hebt vertrouwd en houdt u de optie voor de validering van het servercertificaat ingeschakeld in de NAM-instellingen.
Opmerking: optie "Als u PAC's gebruikt, mag u niet-gewaarmerkte PAC-provisioning" alleen toestaan in het geval van Anoniem In-band PAC-provisioning.

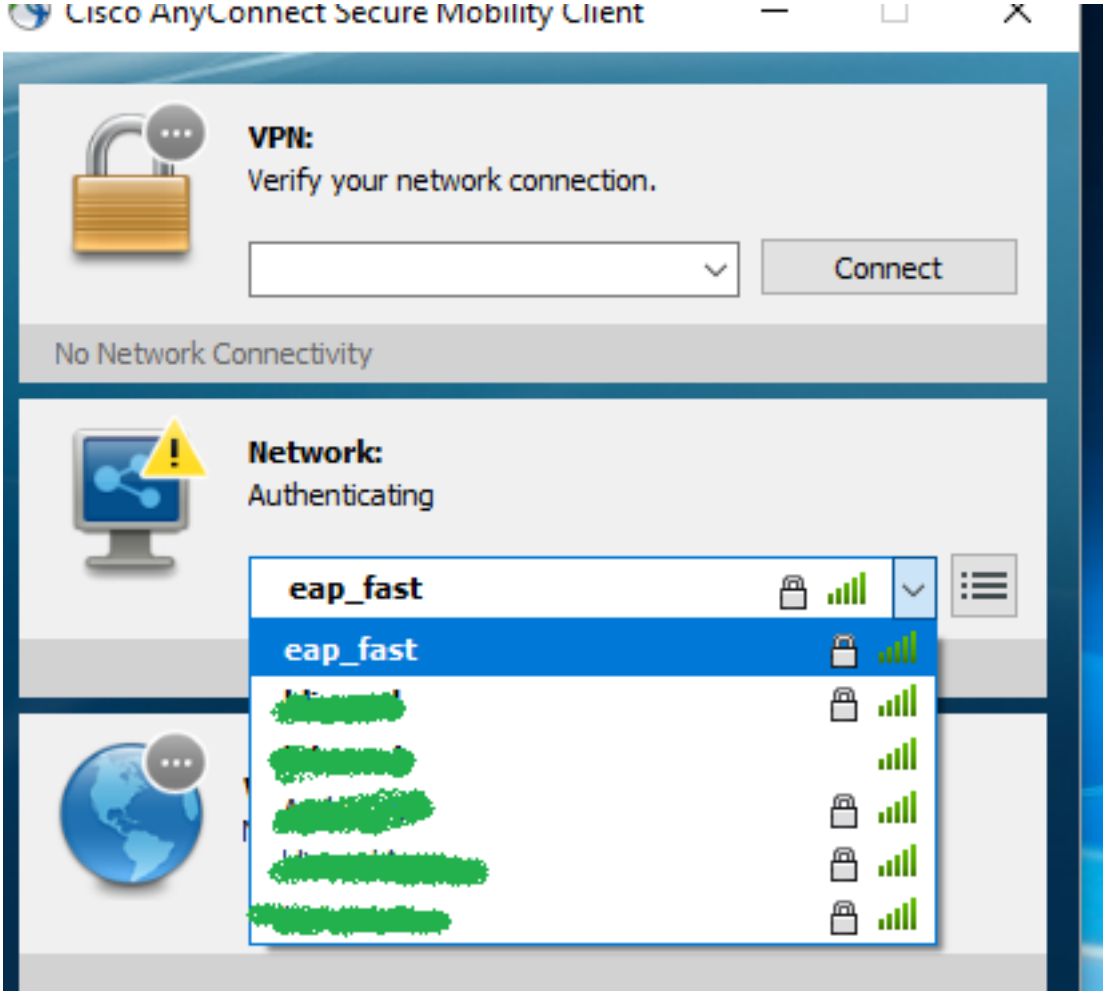
8. Defineer gebruikersreferenties, of als SSO voor het geval u dezelfde aanmeldingsgegevens wilt gebruiken als die voor inloggen worden gebruikt, of selecteer "Wachtwoord voor referenties" voor het geval u wilt dat een gebruiker om aanmeldingsgegevens wordt gevraagd tijdens het aansluiten op een netwerk, of definieer statische aanmeldingsgegevens voor dat toegangstype. In dit voorbeeld vragen we gebruikers om aanmeldingsgegevens bij een verbinding naar een netwerk.



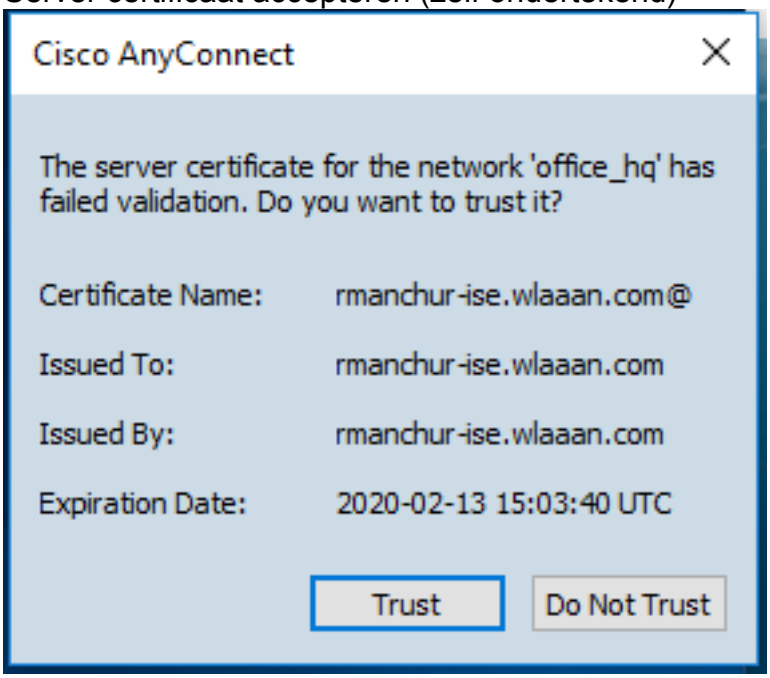
9. Opslaan van ingesteld profiel onder de desbetreffende NAM-map.

Test connectiviteit op SSID met behulp van EAP-FAST-verificatie.

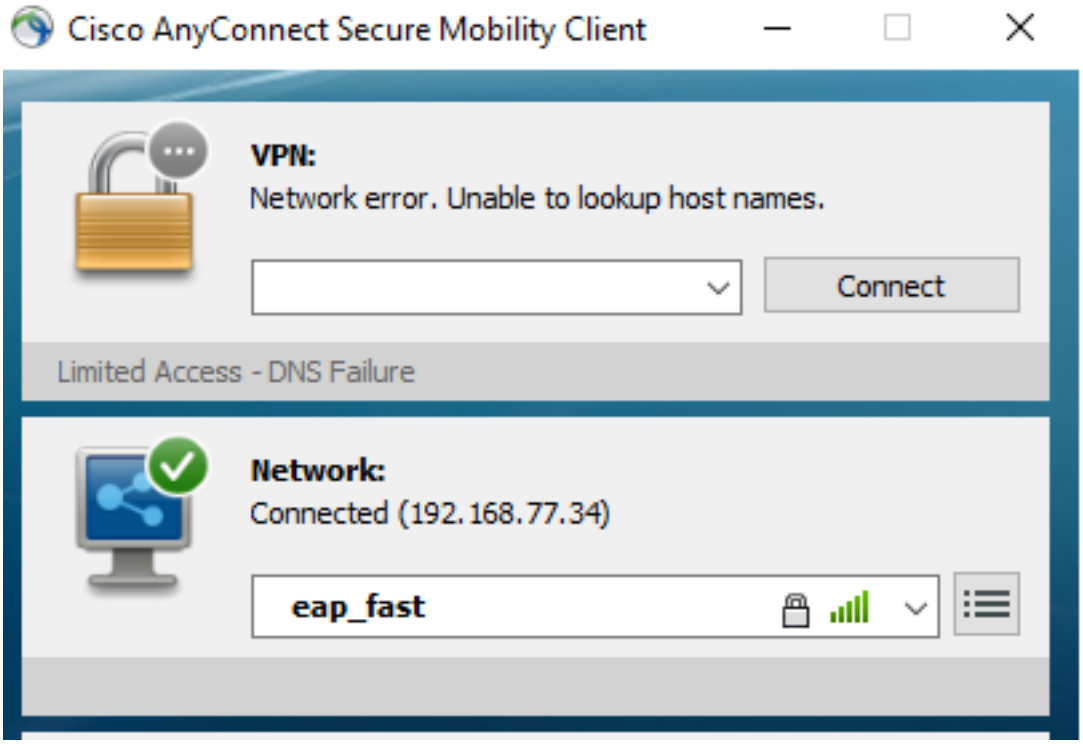
1. Selecteer respectieve profiel van AnyConnect-netwerklijst



2. Voer een gebruikersnaam en wachtwoord in dat voor verificatie vereist is
3. Server certificaat accepteren (zelf ondertekend)



4. Gereed



ISE-authenticatielogs

ISE-authenticatiebestanden die EAP-FAST en PAC-voorzieningsstroom tonen, kunnen worden gezien onder "**Operations -> RADIUS -> Live Logs**" en kunnen in meer details worden bekeken met behulp van het pictogram **Zoom**:

1. De cliënt is begonnen met authenticatie en ISE stelde EAP-TLS voor als authenticatiemethode, maar client verworpen en voorgesteld EAP-FAST, dat was de methode waarover zowel cliënt als ISE het eens waren.

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12101	Extracted EAP-Response/NAK requesting to use EAP-FAST instead
12100	Prepared EAP-Request proposing EAP-FAST with challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12102	Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

2. De TLS-handdruk is tussen client en server gestart om een beschermde omgeving te bieden voor PAC-uitwisseling en is met succes voltooid.

12800 Extracted first TLS record; TLS handshake started

12805 Extracted TLS ClientHello message

12806 Prepared TLS ServerHello message

12807 Prepared TLS Certificate message

12808 Prepared TLS ServerKeyExchange message

12810 Prepared TLS ServerDone message

12811 Extracted TLS Certificate message containing client certificate

12105 Prepared EAP-Request with another EAP-FAST challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request

11018 RADIUS is re-using an existing session

12104 Extracted EAP-Response containing EAP-FAST challenge-response

12105 Prepared EAP-Request with another EAP-FAST challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request (⏰ Step latency=13317 ms)

11018 RADIUS is re-using an existing session

12104 Extracted EAP-Response containing EAP-FAST challenge-response

12812 Extracted TLS ClientKeyExchange message

12813 Extracted TLS CertificateVerify message

12804 Extracted TLS Finished message

12801 Prepared TLS ChangeCipherSpec message

12802 Prepared TLS Finished message

12816 TLS handshake succeeded

3. Inner authenticatie gestart en gebruikersreferenties werden gevalideerd door ISE met behulp van MS-CHAPv2 (op gebruikersnaam/wachtwoord gebaseerde verificatie)