Secure Client NAM voor Dot1x configureren met Windows en ISE 3.2

Inhoud

Inleiding

Dit document beschrijft hoe u de Secure Client Network Analysis Module (NAM) in Windows kunt configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van wat een RADIUS-supplicant is
- Dot1x
- PEAP
- PKI

Gebruikte componenten

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

- Windows 10 Pro versie 22H2 Built 19045.3930
- ISE-lijnkaart 3.2
- Cisco C117 Cisco IOS® XE-software, versie 17.12.02
- Active Directory 2016

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

Dit document beschrijft hoe u Secure Client NAM in Windows kunt configureren. Er worden een optie voor het vooraf implementeren en een profieleditor gebruikt voor het uitvoeren van dot1x-verificatie. Er worden ook enkele voorbeelden gegeven van hoe dit wordt bereikt.

In netwerken is een supplicant een entiteit aan de ene kant van een point-to-point LAN-segment dat wil worden geverifieerd door een verificator die aan de andere kant van die link is gekoppeld. De standaard IEEE 802.1X gebruikt de term supplicant om te verwijzen naar hardware of software. In de praktijk is een supplicant een softwaretoepassing die op een eindgebruikerscomputer is geïnstalleerd. De gebruiker haalt de aanvrager aan en dient de referenties in om de computer aan te sluiten op een beveiligd netwerk. Als de verificatie slaagt, stelt de verificator de computer doorgaans in staat verbinding te maken met het netwerk.

Over Network Access Manager

Network Access Manager is clientsoftware die een beveiligd Layer 2-netwerk biedt in overeenstemming met het bijbehorende beleid. Het detecteert en selecteert het optimale Layer 2-toegangsnetwerk en voert apparaatverificatie uit voor toegang tot zowel bekabelde als draadloze netwerken. Network Access Manager beheert de gebruikers- en apparaatidentiteit en de netwerktoegangsprotocollen die nodig zijn voor beveiligde toegang. Het werkt op een intelligente manier om te voorkomen dat eindgebruikers verbindingen maken die in strijd zijn met door de beheerder gedefinieerde beleidsregels.

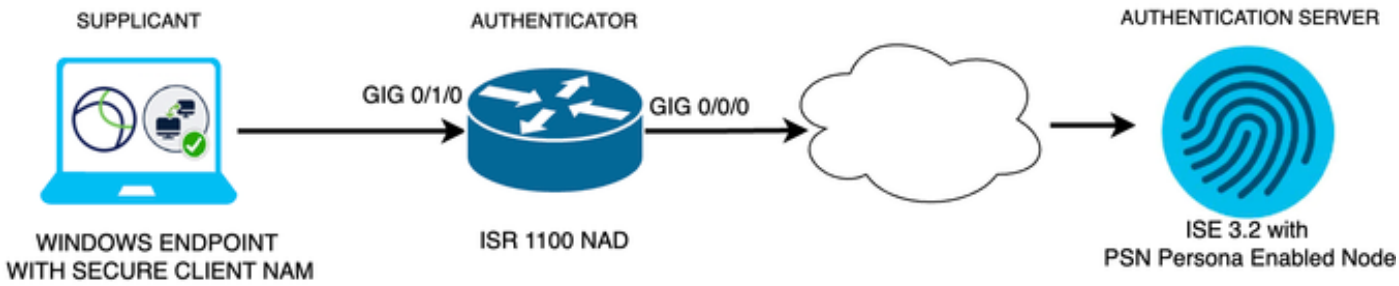
De Network Access Manager is ontworpen voor enkelvoudig calibreren, zodat u slechts één netwerkverbinding tegelijk kunt maken. Ook bekabelde verbindingen hebben een hogere prioriteit dan draadloze verbindingen, dus als u wordt aangesloten op het netwerk met een bekabelde verbinding, wordt de draadloze adapter uitgeschakeld zonder IP-adres.

Configureren

Netwerkdiagram

Het is van cruciaal belang om te begrijpen dat voor dot1x-authenticaties 3 onderdelen nodig zijn; de aanvrager die dot1x kan doen, de authenticator ook bekend als NAS/NAD die fungeert als een proxy die het dot1x-verkeer in RADIUS inkapselt, en de authenticatieserver.

In dit voorbeeld is de supplicant geïnstalleerd en geconfigureerd op verschillende manieren. Later wordt een scenario met de netwerkapparaatconfiguratie en de verificatieserver weergegeven.



Netwerkdiagram

Configuraties

1. Download en installeer Secure Client NAM (Network Access Manager).

2. Download en installeer de Secure Client NAM profieleditor.
3. Algemene standaardconfiguraties
4. Scenario 1: Configureer de Secure Client NAM Supplicant voor PEAP (MS-CHAPv2)-gebruikersverificatie.
5. Scenario 2: De Secure Client NAM Supplicant voor EAP-FAST tegelijk configureren als de gebruikers- en de machineverificatie zijn geconfigureerd.
6. Scenario 3 Part 1: Configureer de Secure Client NAM Supplicant voor EAP-TLS.
7. Scenario 3, deel 2: De NAD- en ISE-demonstratie configureren.

1. Secure Client NAM (Network Access Manager) downloaden en installeren

Cisco-softwaredownloads

Type Secure Client 5 in de zoekbalk voor productnamen.

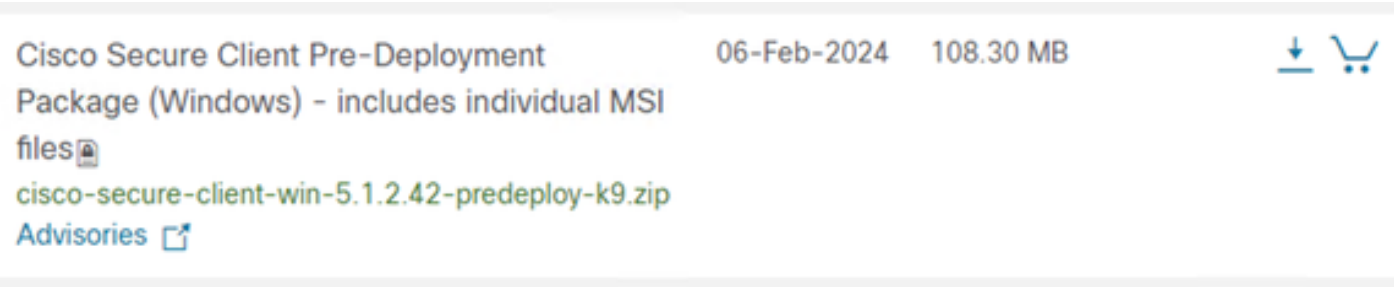
Downloads - Home > Beveiliging > Clients voor VPN- en endpointbeveiliging > Beveiligde client (inclusief AnyConnect) > Beveiligde client 5 > AnyConnect VPN-clientsoftware.

In dit configuratievoorbeeld wordt versie 5.1.2.42 gebruikt.

Er zijn meerdere manieren om Secure Client te implementeren op Windows-apparaten; vanaf SCM, vanaf de Identity Service Engine en vanaf de VPN-head-end. In dit artikel wordt echter de

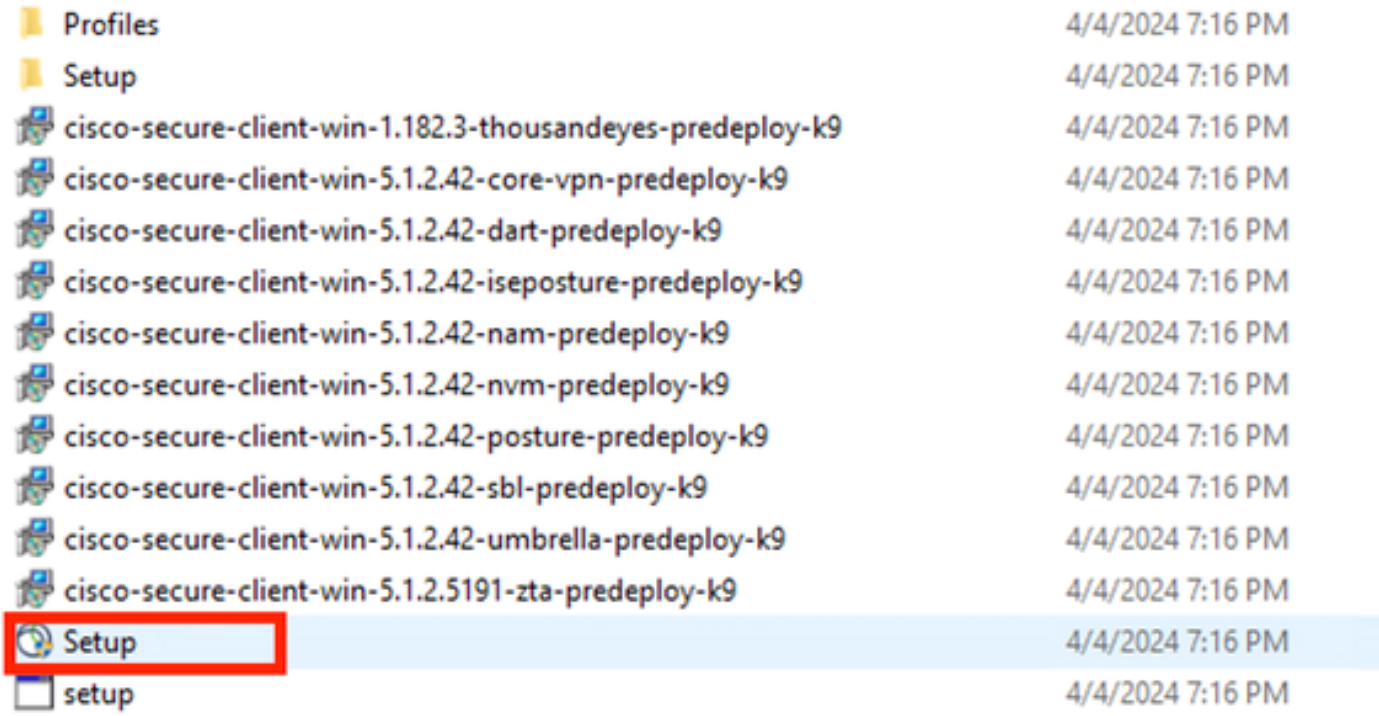
voorimplementatiemethode gebruikt.

Zoek op de pagina naar het bestand Cisco Secure Client Head-end implementatiepakket (Windows).



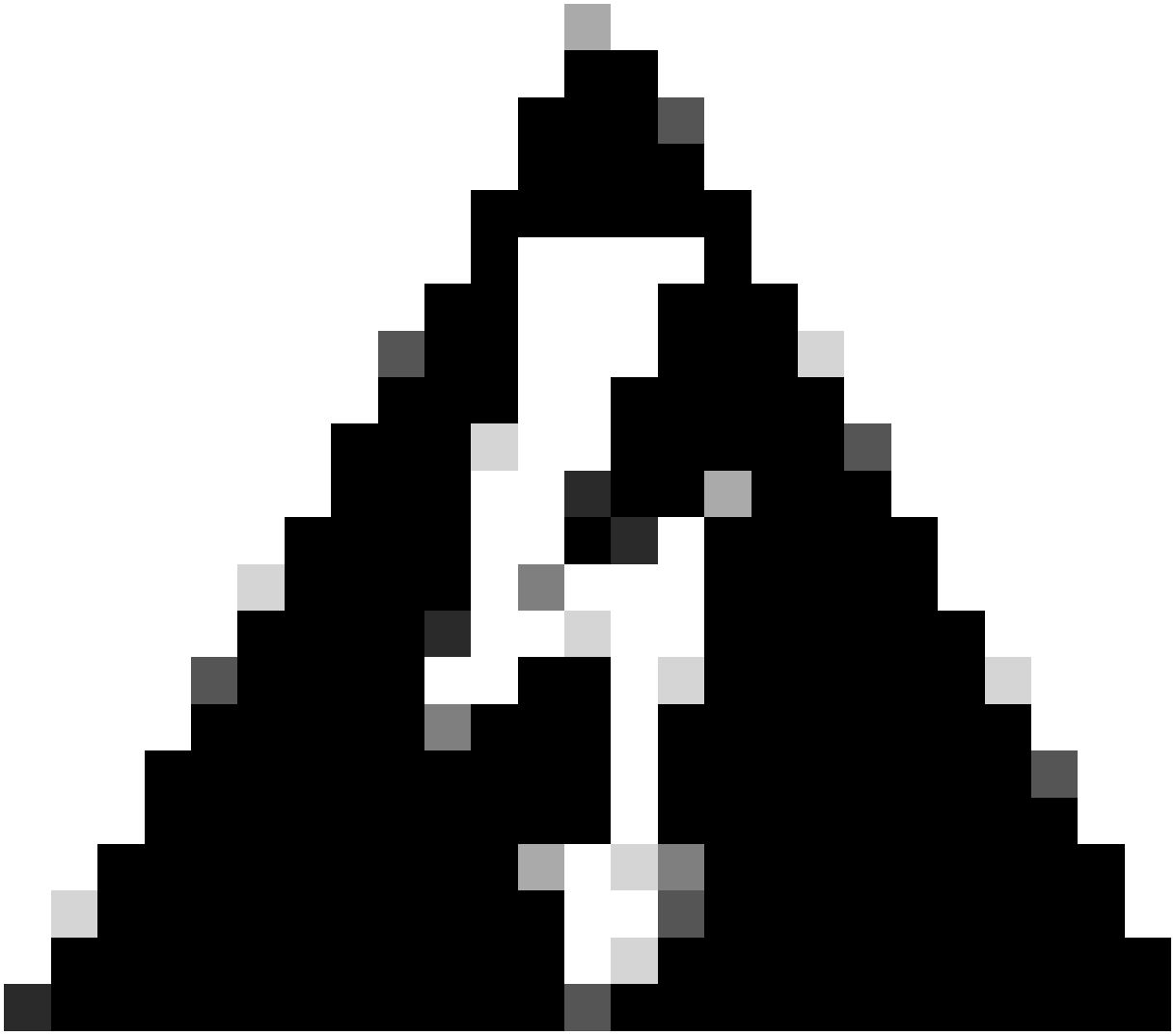
Msi-zipbestand

Klik op Setup als u het bestand hebt gedownload en geëxtraheerd.

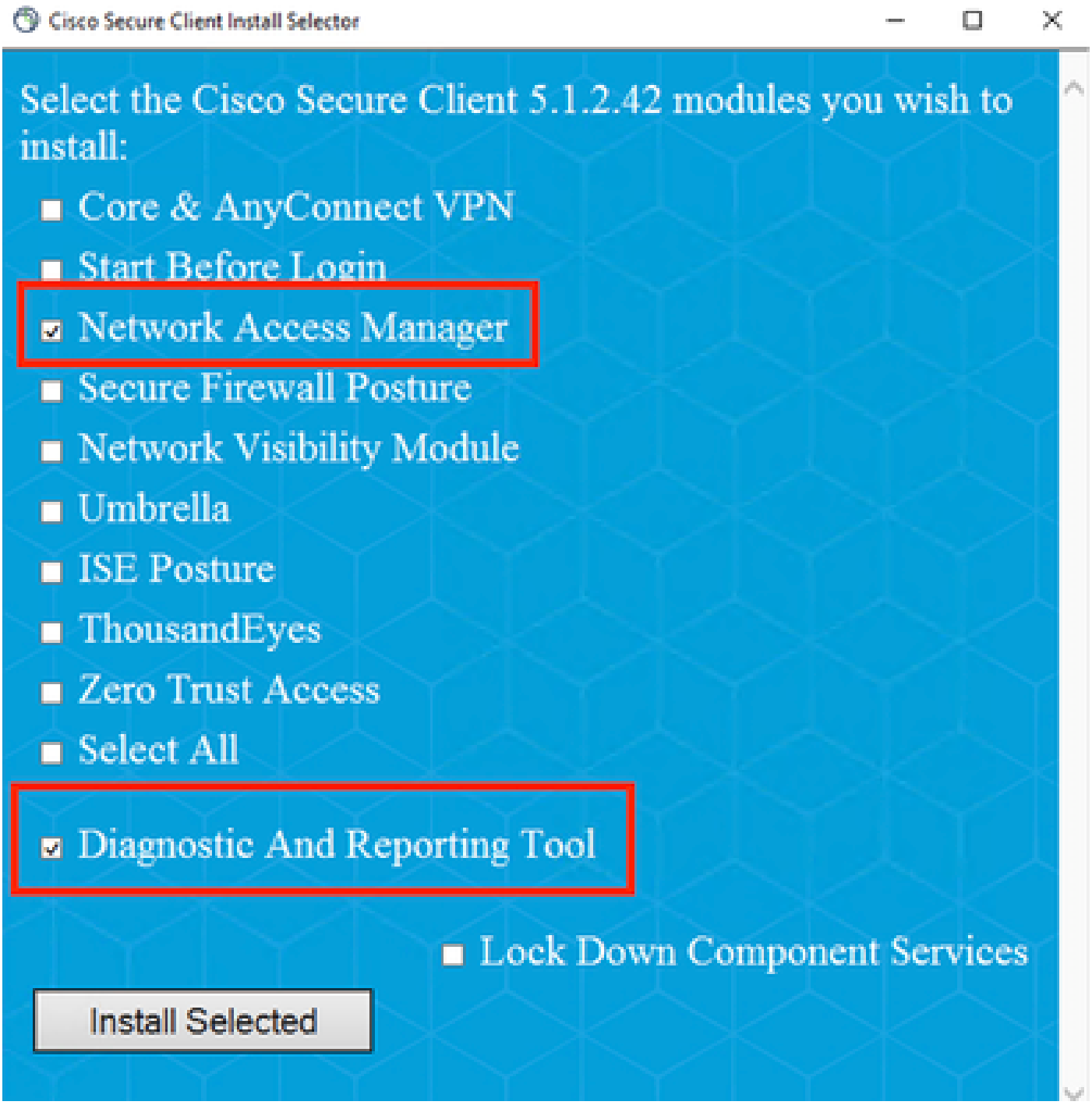


Beveiligde clientbestanden

Installeer de Network Access Manager en de modules van de Diagnostics and Reporting Tool.



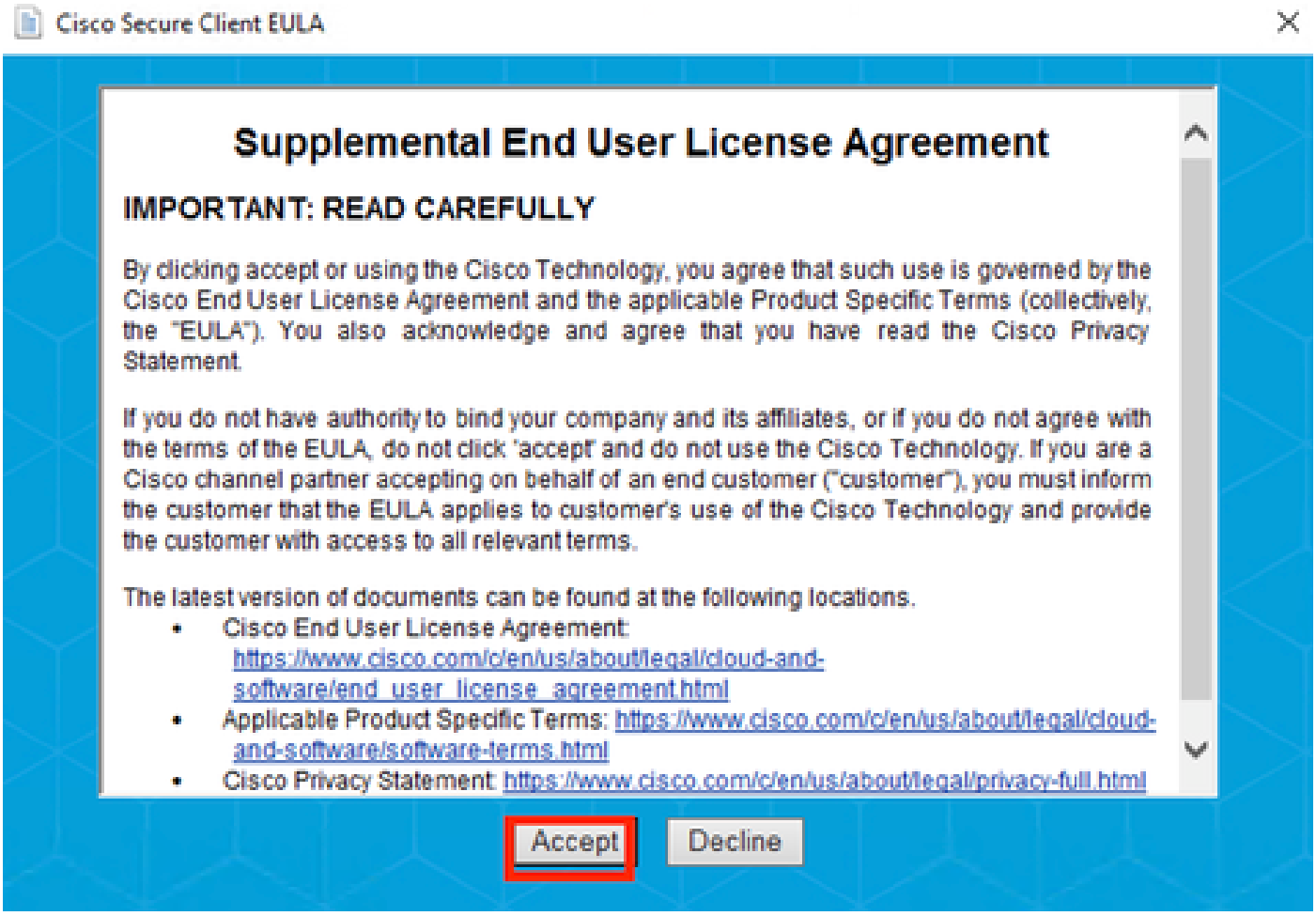
Waarschuwing: als u de Secure Client Wizard van Cisco gebruikt, wordt de VPN-module automatisch geïnstalleerd en in de GUI verborgen. NAM werkt niet als de VPN module niet geïnstalleerd is. Als u individuele MSI-bestanden of een andere installatiemethode gebruikt, zorg er dan voor dat u de VPN-module installeert.



Installatieselector

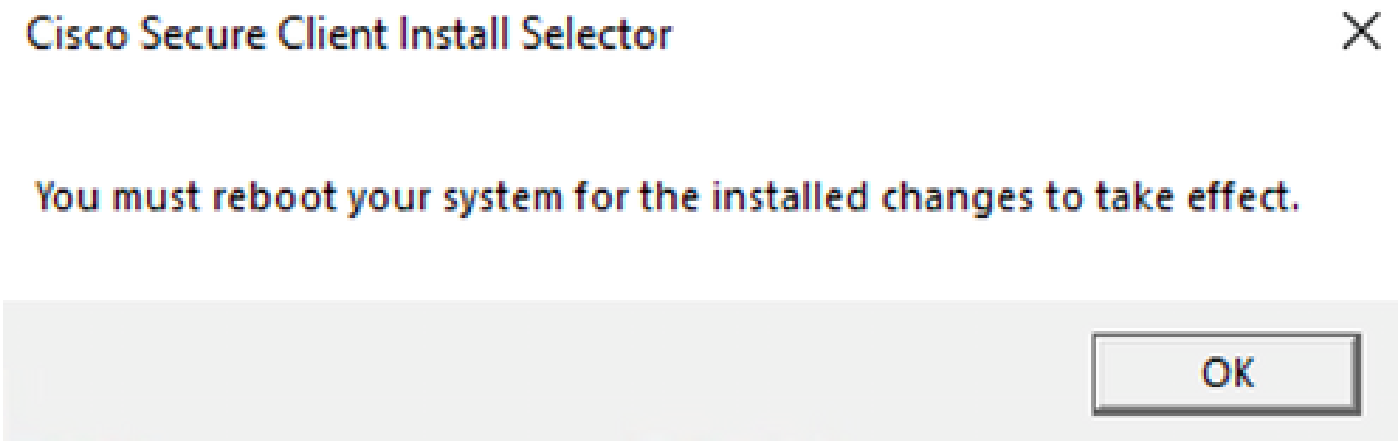
Klik op Install Selected (Selectie installeren).

Accepteer de EULA.



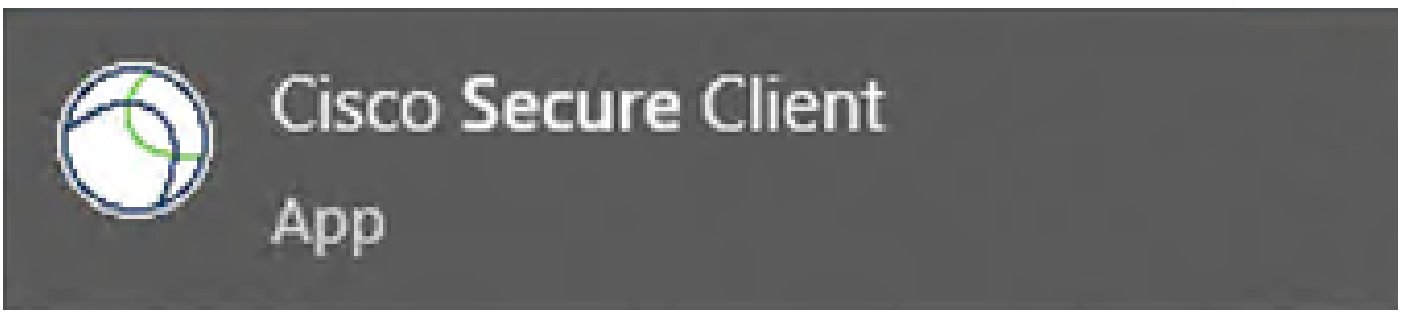
EULA-venster

Na de NAM-installatie moet opnieuw worden gestart.



Reboot Requirement Window

Eenmaal geïnstalleerd kan het worden gevonden en geopend vanuit de Windows Search bar.



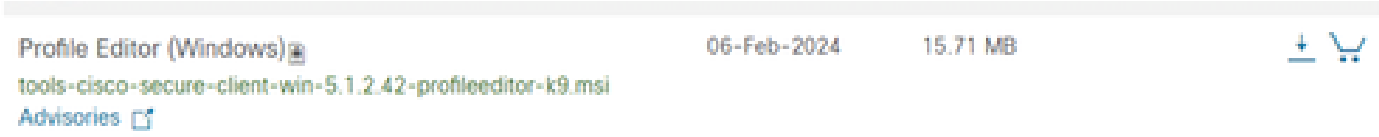
Secure-clientprogramma

2. Download en installeer de Secure Client NAM Profile Editor.

De Cisco Network Access Manager Profile Editor is vereist voor het configureren van de Dot1x-voorkeuren.

De optie Profieleditor is gevonden op dezelfde pagina waarop Secure Client is gedownload.

Dit voorbeeld gebruikt de optie met versie 5.1.2.42.



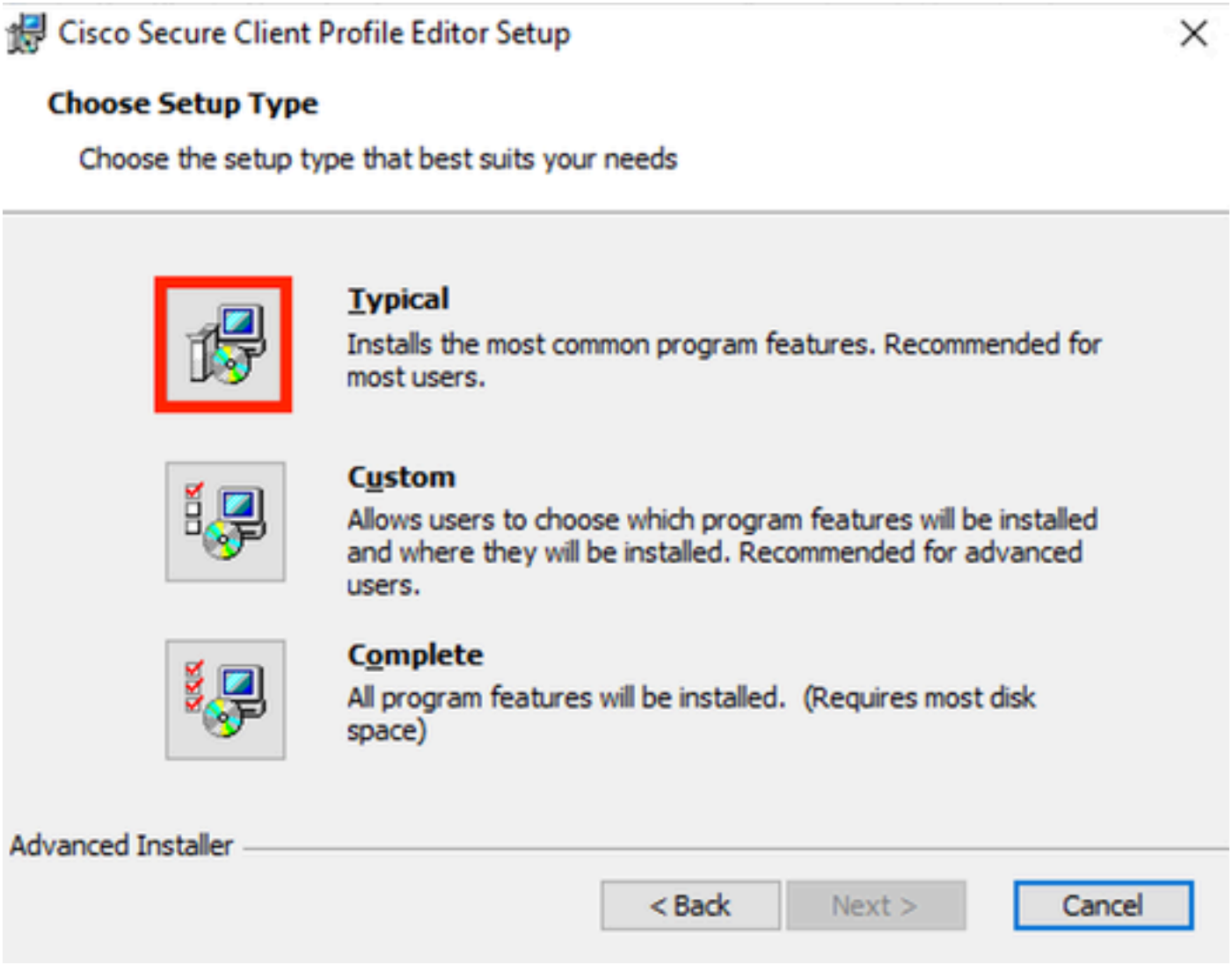
Profieleditor

Zodra het is gedownload, gaat u verder met de installatie.

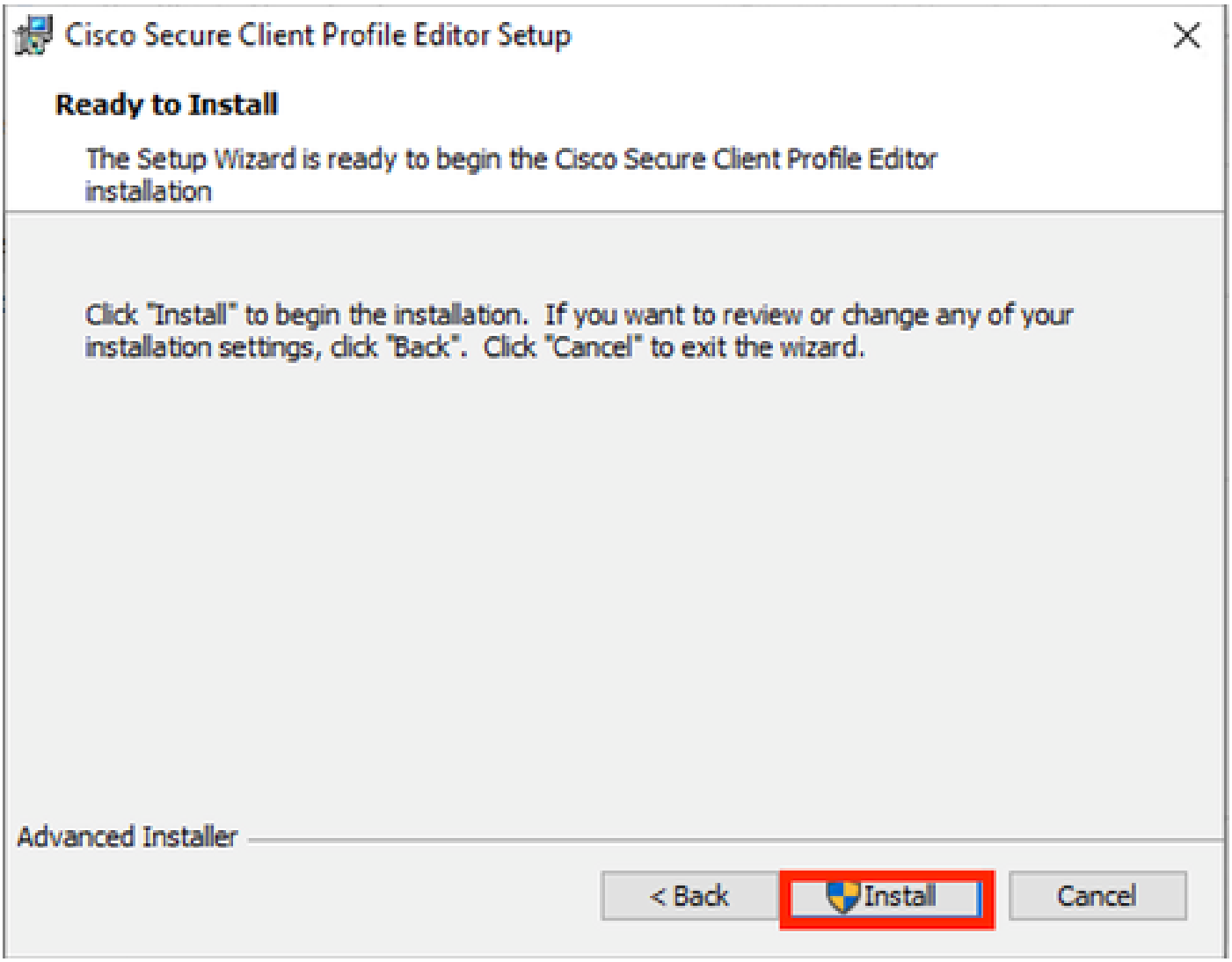
Start het MSI-bestand.

Venster Profieleditor instellen

Gebruik de optie Typische installatie.

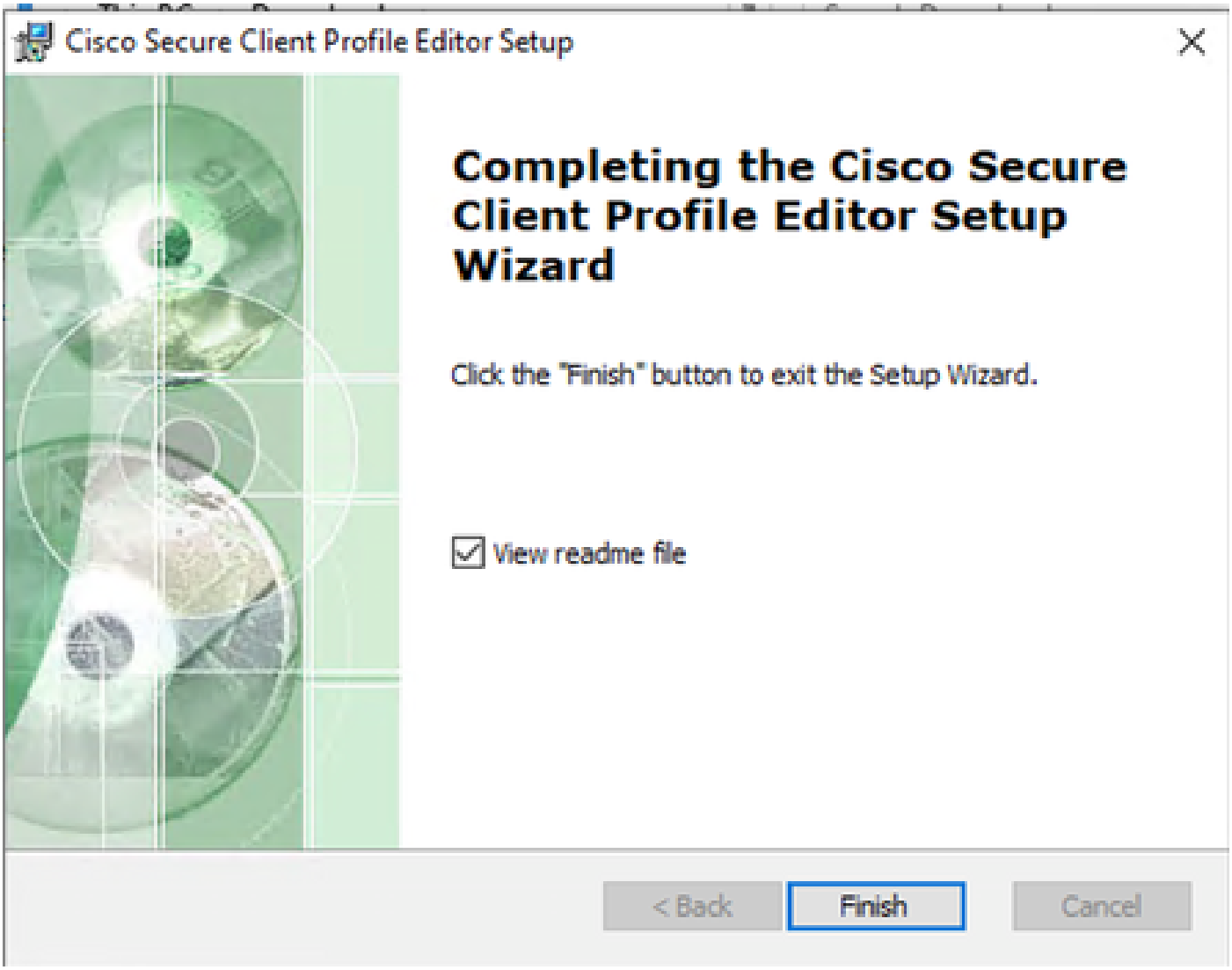


Profieleditor instellen



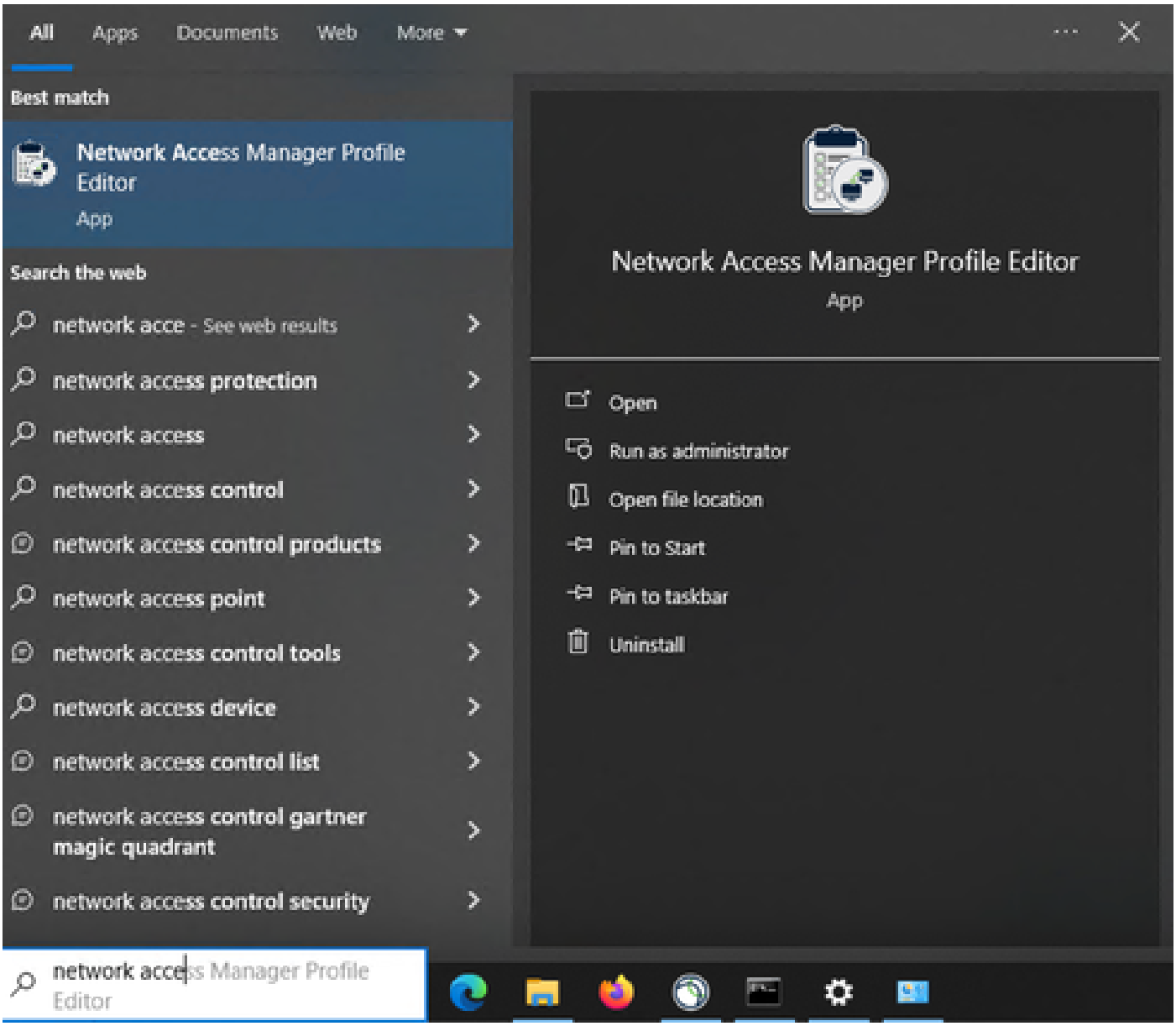
Installatievenster

Klik op Finish (Voltooien).



Einde profieleditor instellen

Open na installatie de profieleditor van Network Access Manager vanuit de zoekbalk.



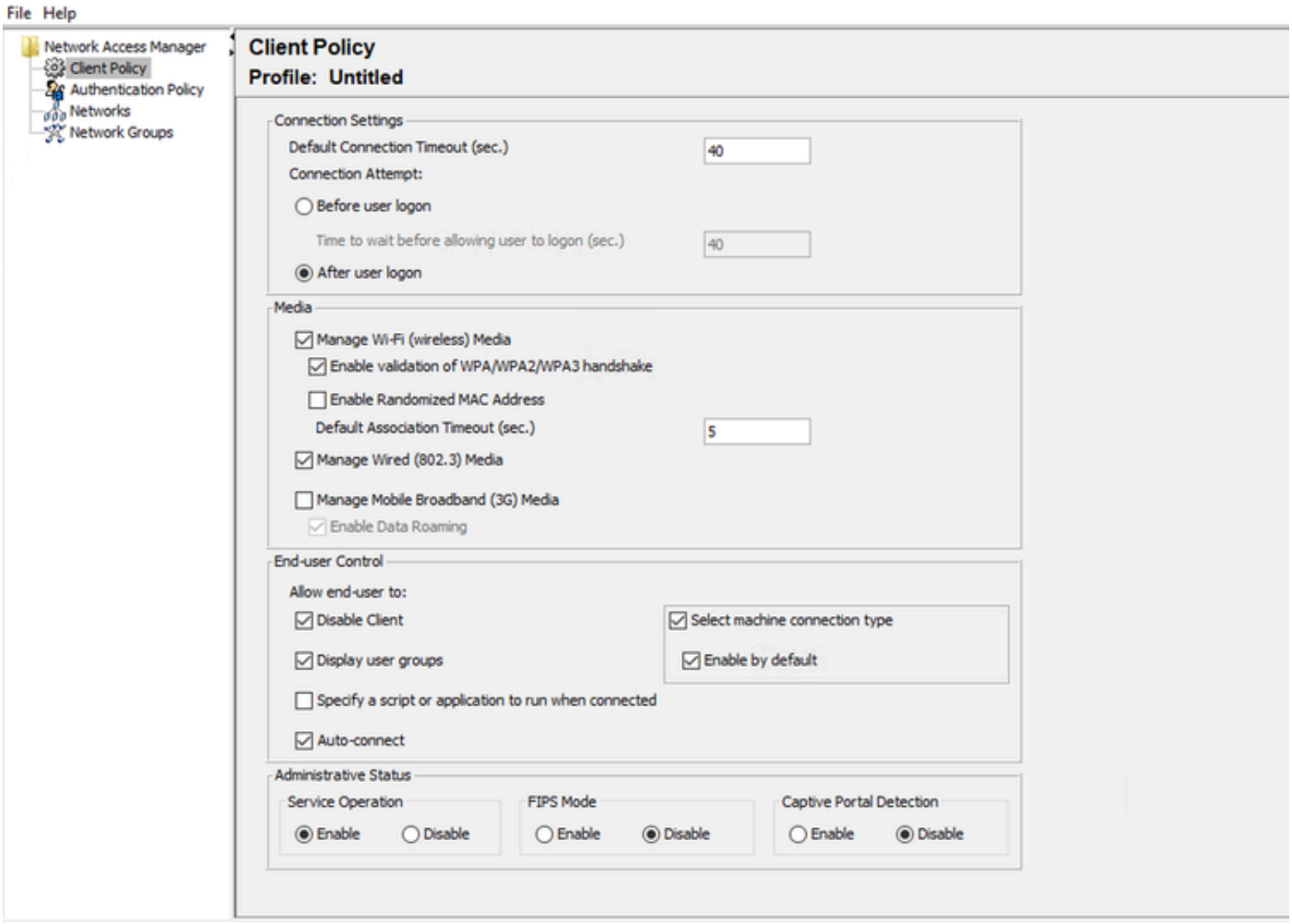
Profieleditor voor NAM in zoekbalk

De installatie van Network Access Manager en Profile Editor is voltooid.

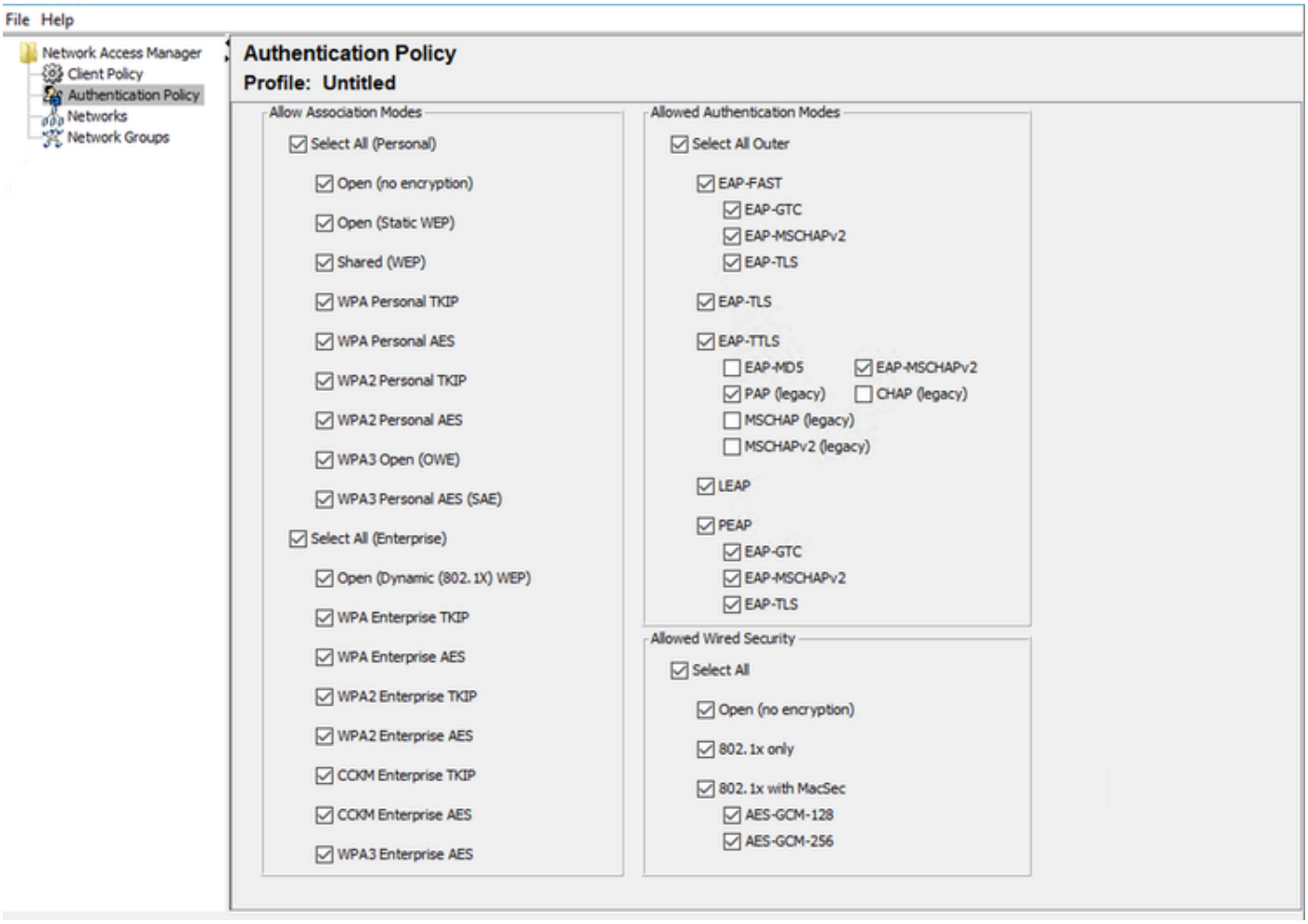
3. Algemene standaardconfiguraties

Alle scenario's in dit artikel bevatten configuraties voor:

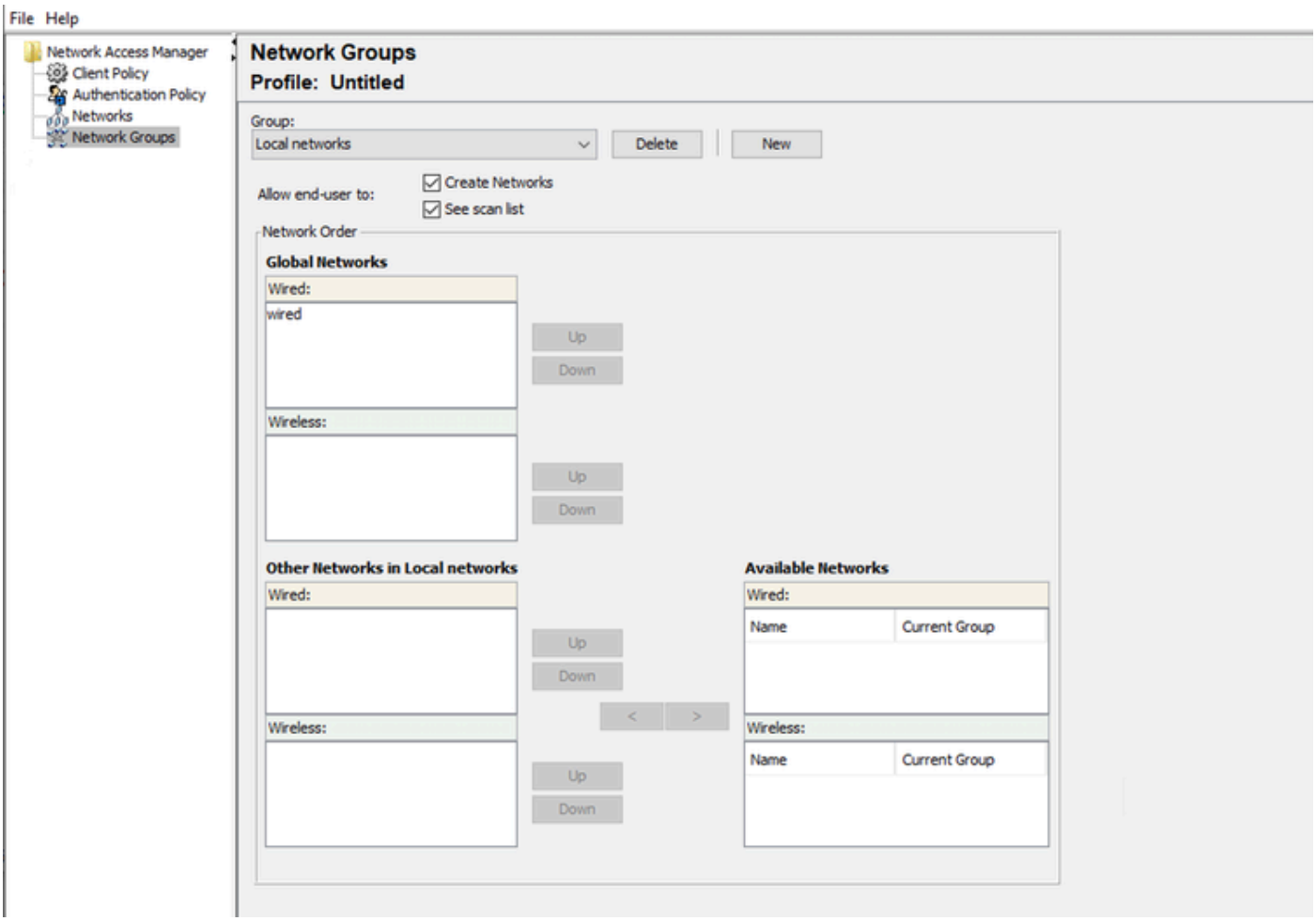
- Clientbeleid
- Verificatiebeleid
- Netwerkgroepen



Clientbeleid voor NAM Profile Editor



Verificatiebeleid voor NAM Profile Editor



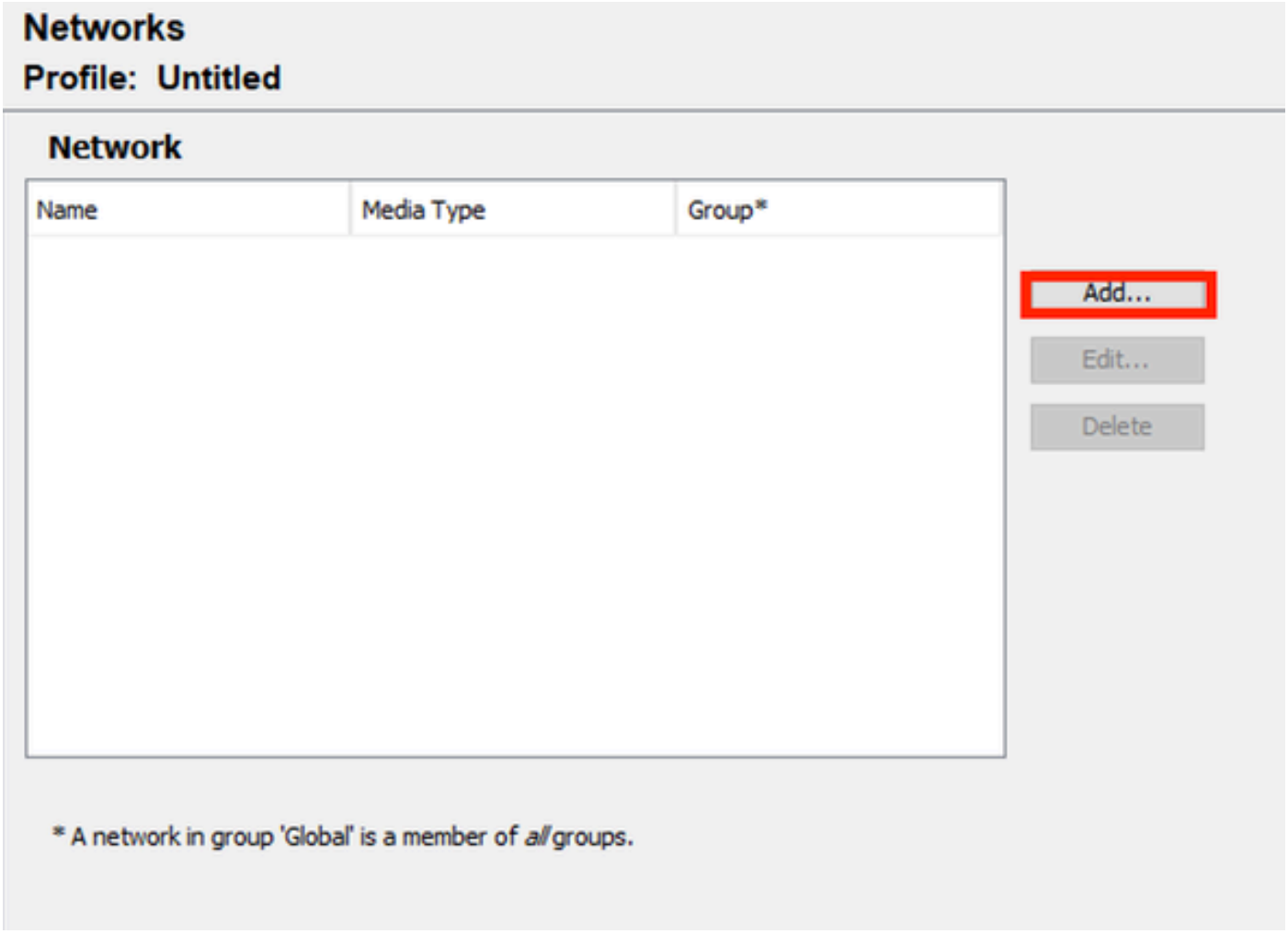
Tabblad Netwerkgroepen

4. Scenario 1: Secure Client NAM Supplicant voor PEAP (MS-CHAPv2)-gebruikersverificatie configureren

Ga naar het gedeelte Netwerken.

Het standaard netwerkprofiel kan worden verwijderd.

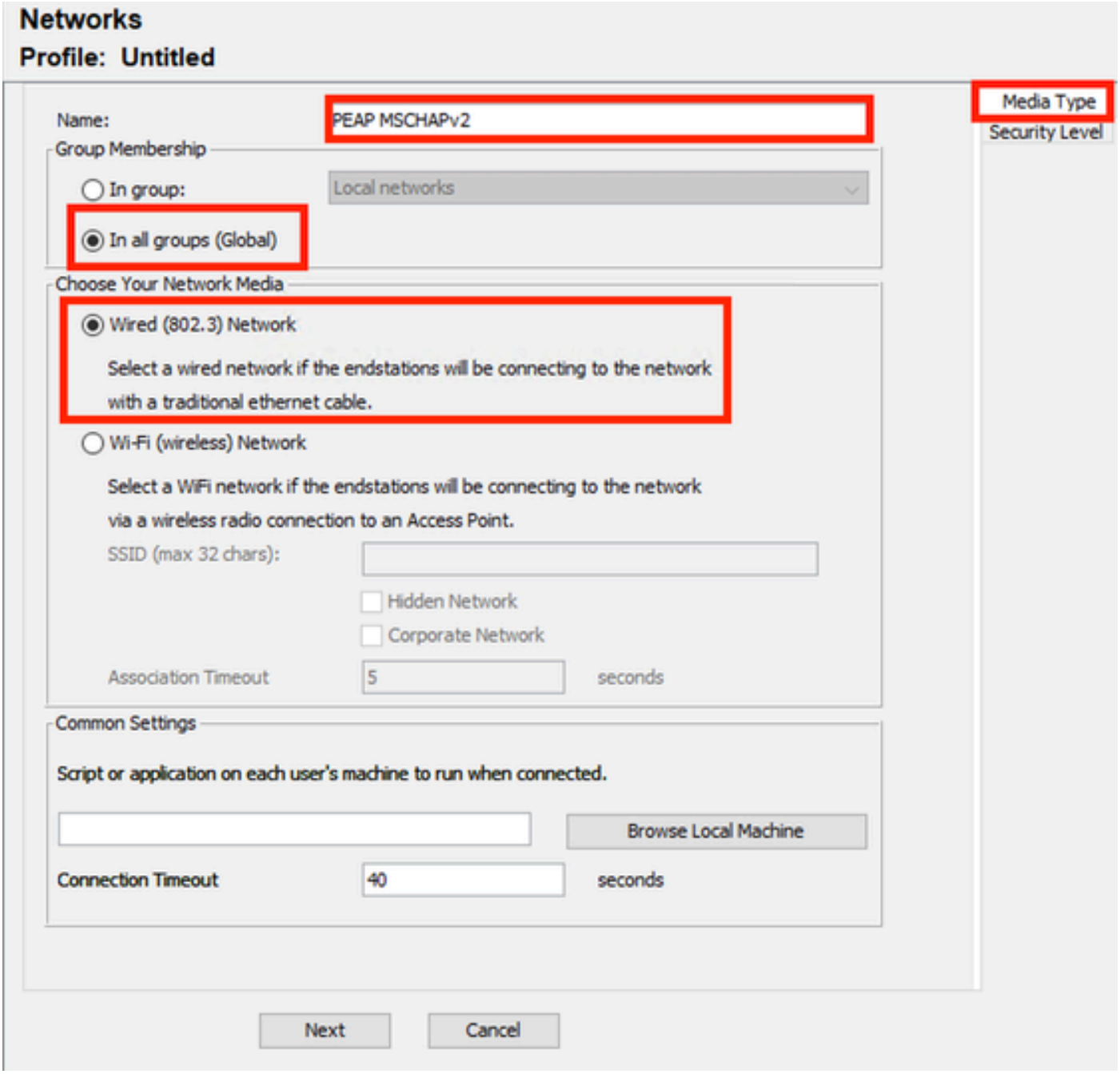
Klik op Add (Toevoegen).



Creatie van netwerkprofiel

Geef het netwerkprofiel een naam.

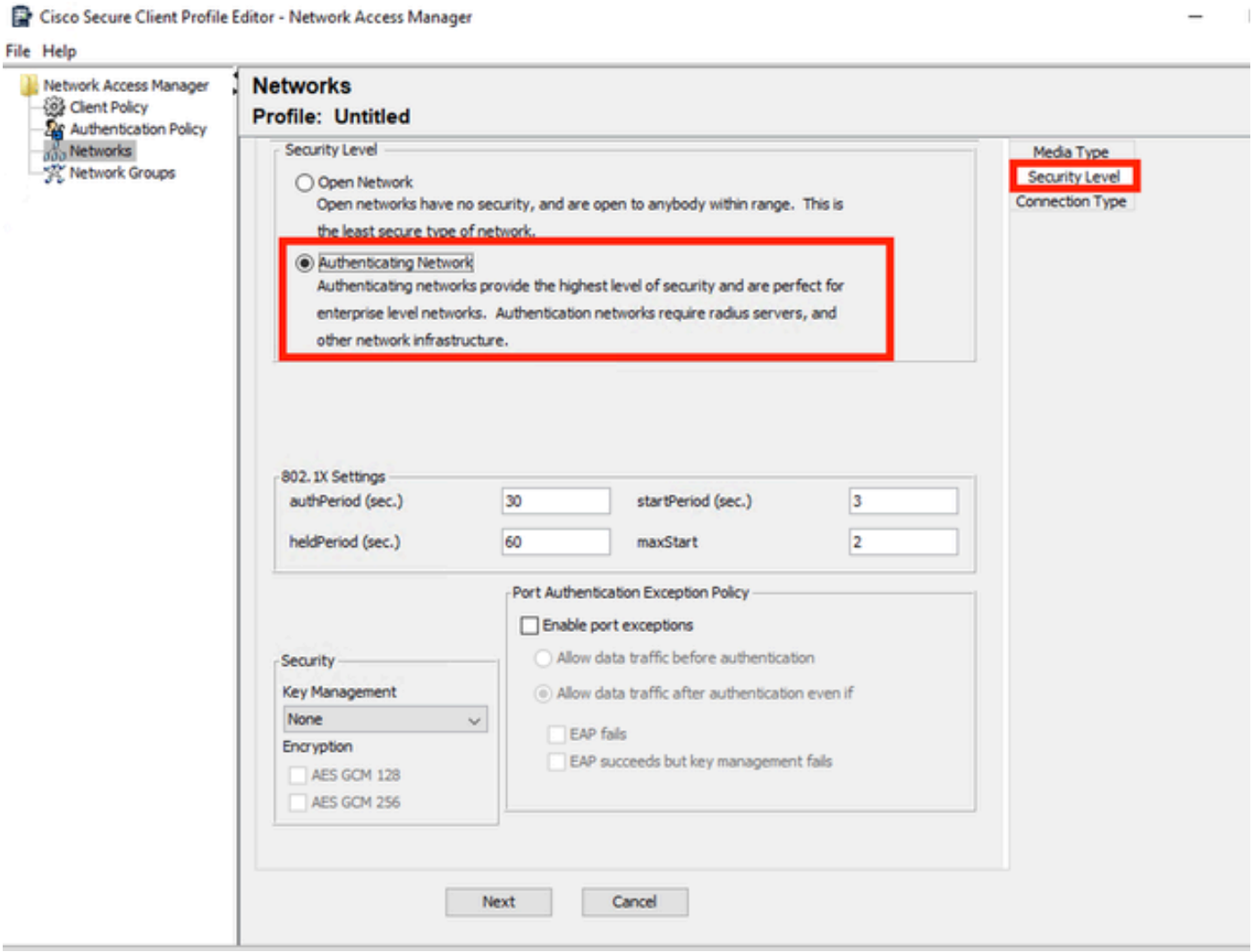
Selecteer Global for Group Membership. Selecteer de media voor bekabeld netwerk.



Sectie Netwerkprofiel voor mediatype

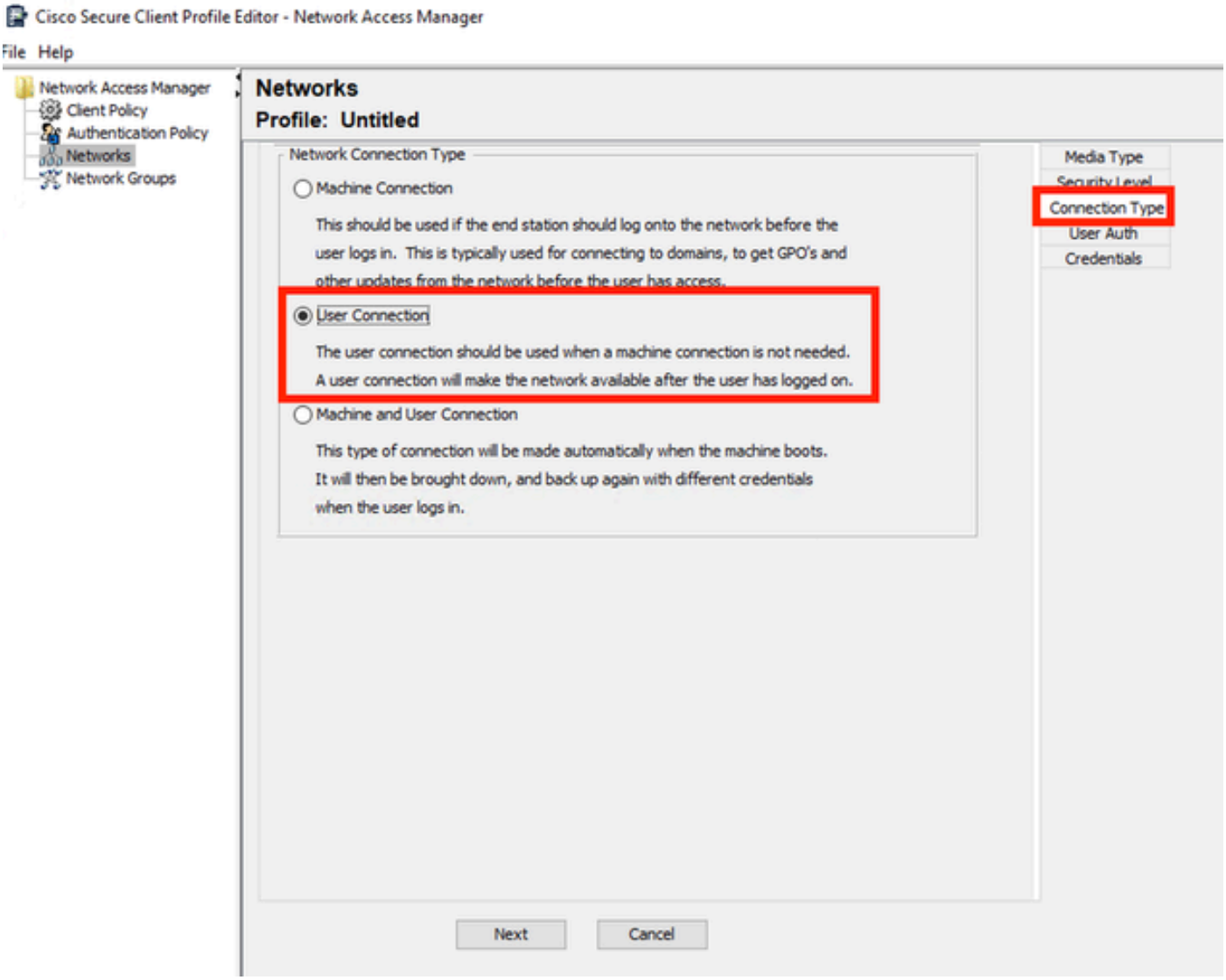
Klik op Next (Volgende).

Selecteer Netwerk verifiëren en gebruik de standaardinstelling voor de rest van de opties in het gedeelte Beveiligingsniveau.



Beveiligingsniveau van netwerkprofiel

Klik op Volgende om door te gaan met het gedeelte Verbindingstype.

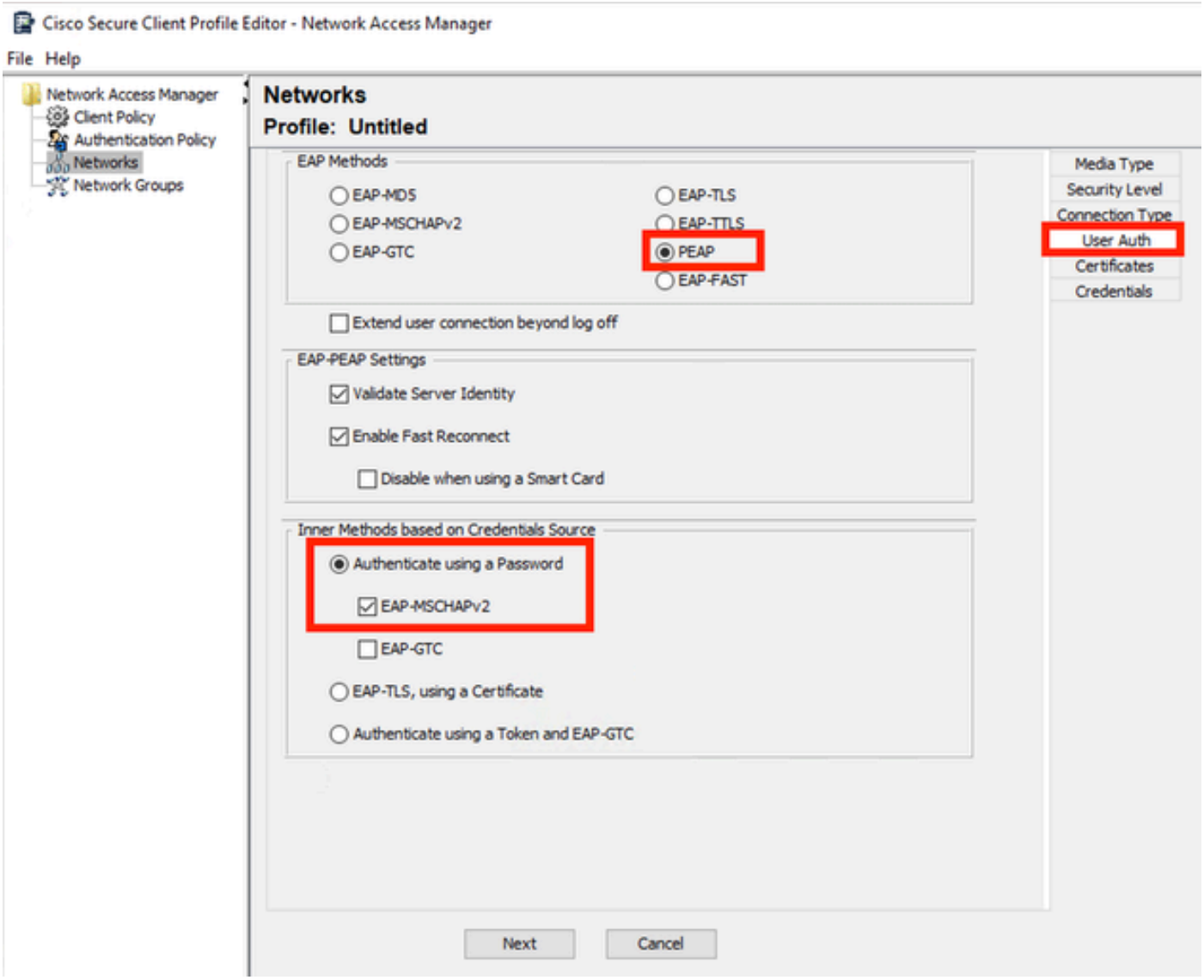


Type netwerkprofiel

Selecteer het type gebruikersverbinding.

Klik op Volgende om door te gaan met de sectie Gebruikersautorisatie die nu beschikbaar is.

Selecteer PEAP als de algemene EAP-methode.



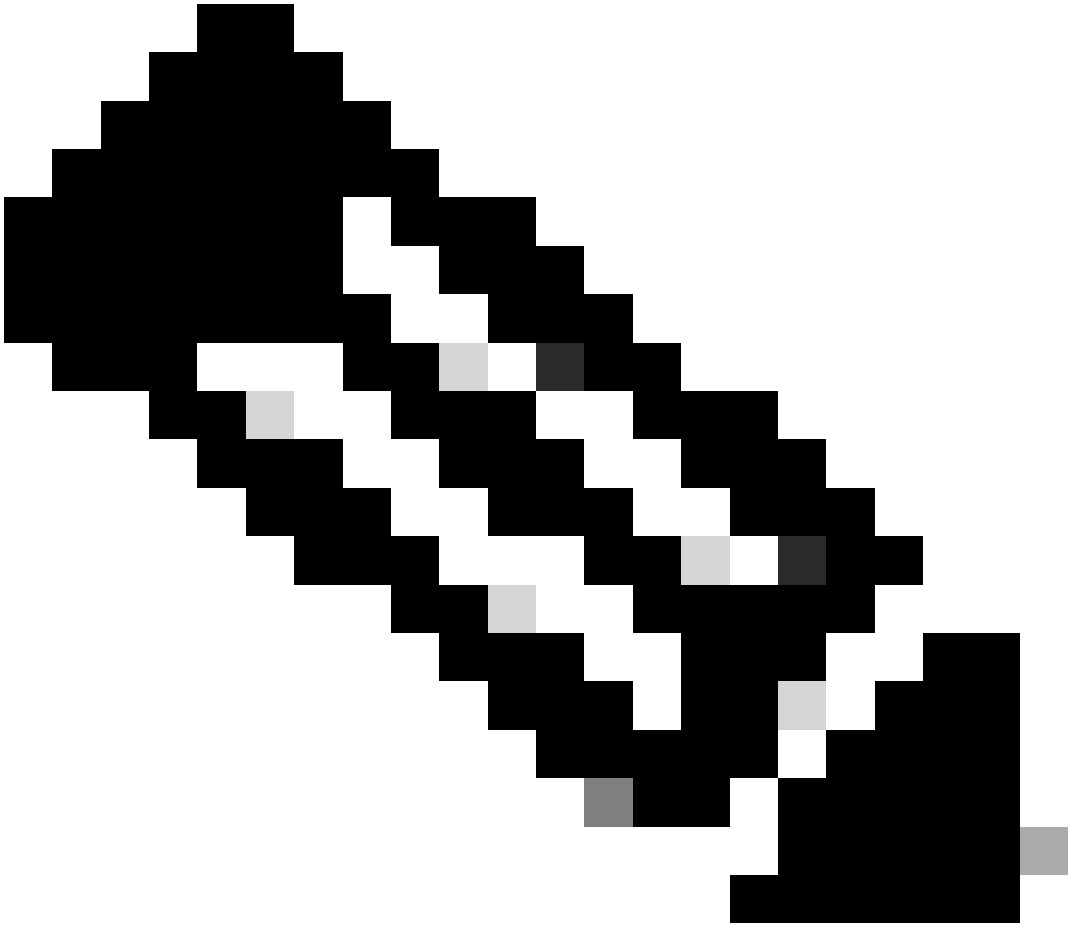
Gebruikersautorisatie Netwerkprofiel

Wijzig de standaardwaarden in de EAP-PEAP-instellingen niet.

Ga verder met de Innerlijke Methodes die op Credentials Bron sectie worden gebaseerd.

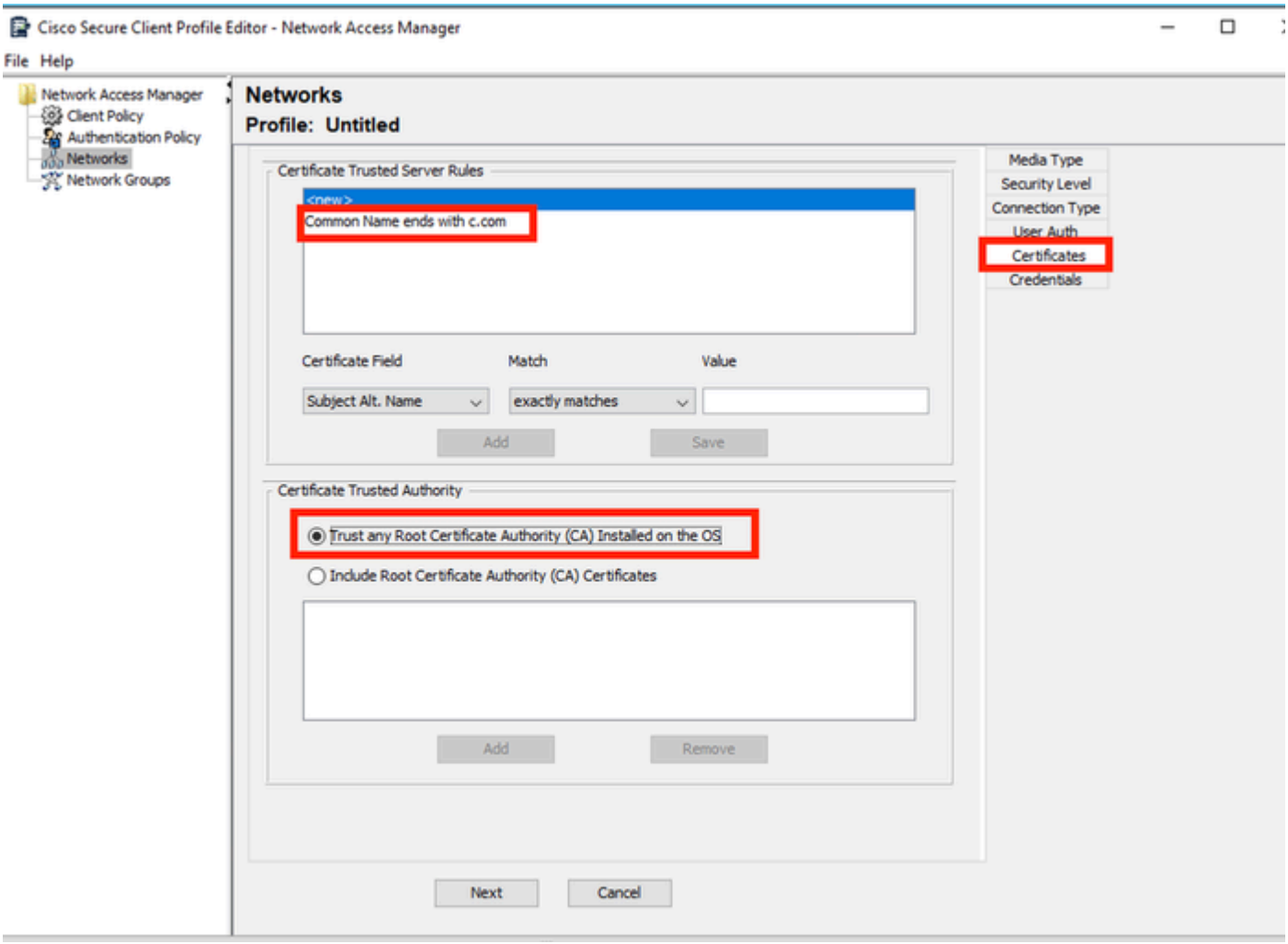
Selecteer Verifiëren met een wachtwoord en selecteer EAP-MSCHAPv2 vanuit de meerdere innerlijke methoden die bestaan voor EAP PEAP.

Klik op Volgende om verder te gaan naar het gedeelte Certificaat.



Opmerking: het gedeelte Certificaat wordt weergegeven omdat de optie Serveridentiteit valideren in EAP-PEAP-instellingen is geselecteerd. Voor EAP PEAP wordt de insluiting uitgevoerd met behulp van het servercertificaat.

In het gedeelte Certificaten wordt in de Certificate Trusted Server-regels de regel Common Name end met c.com gebruikt. Dit deel van de configuratie verwijst naar het certificaat dat de server gebruikt tijdens de EAP PEAP-stroom. Als Identity Service Engine (ISE) in uw omgeving wordt gebruikt, kunt u de algemene naam van het EAP-certificaat voor Policy Server Node gebruiken.

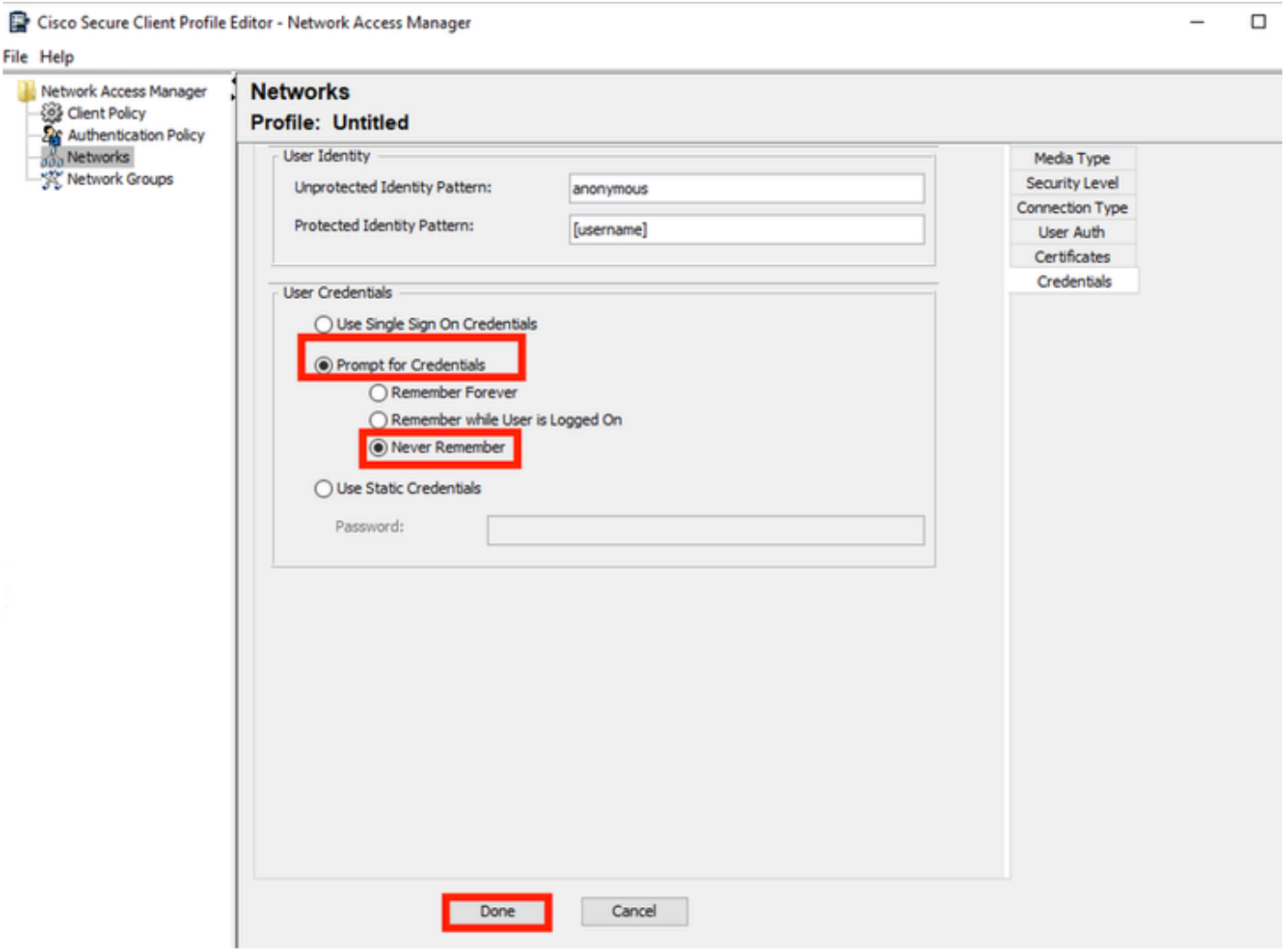


Sectie Netwerkprofiel

Er kunnen twee opties worden geselecteerd in Certificate Trusted Authority. In dit scenario wordt in plaats van een specifiek CA-certificaat dat het EAP-certificaat van RADIUS heeft ondertekend, de optie Vertrouwen elke Root Certificate Authority (CA) die op het besturingssysteem is geïnstalleerd, gebruikt.

Met deze optie vertrouwt het Windows-apparaat op een EAP cert die is ondertekend door een cert die is opgenomen in het programma Gebruikerscertificaten beheren — Huidige gebruiker > Trusted Root Certification Authorities > Certificates.

Klik op Next (Volgende).



Sectie Netwerkprofiel referenties

In het gedeelte Credentials wordt alleen het gedeelte Gebruikersreferenties gewijzigd.

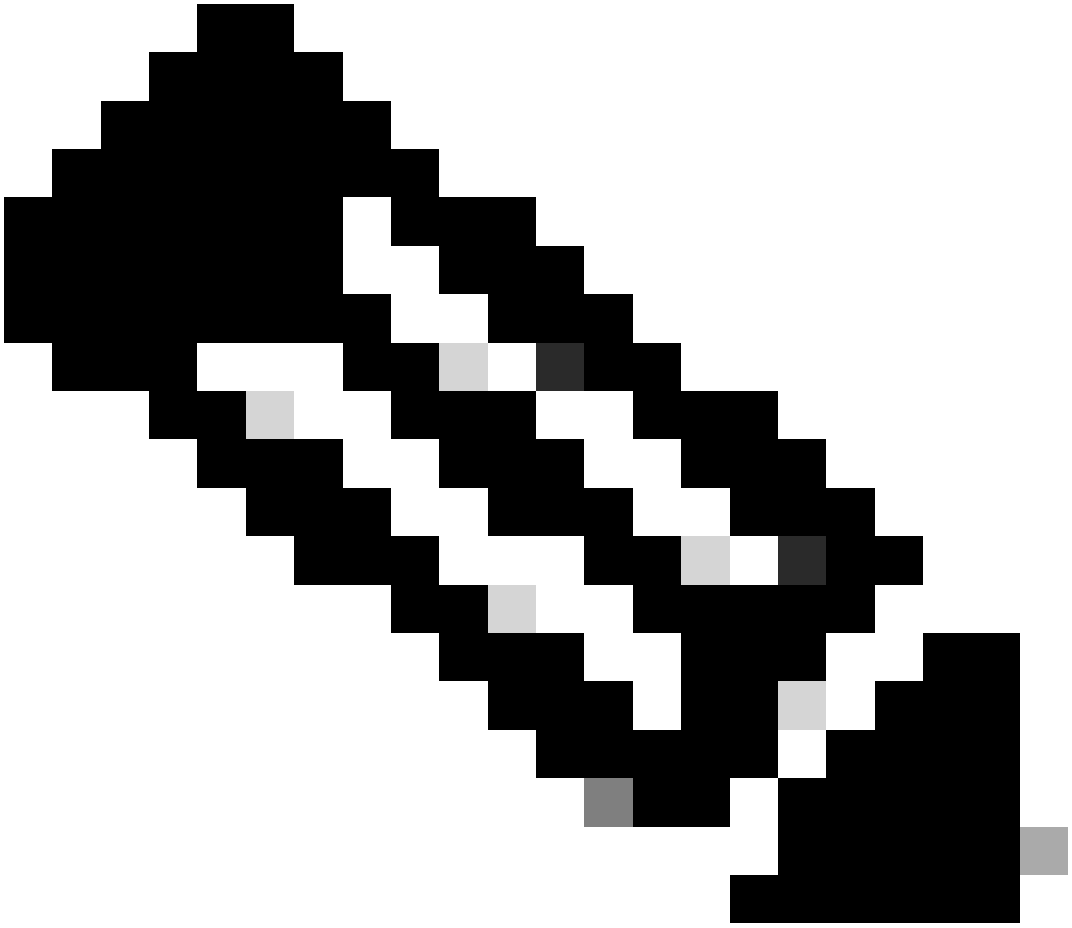
De optie Vragen om referenties > Nooit herinneren is geselecteerd, dus bij elke verificatie moet de gebruiker die de verificatie uitvoert, zijn referenties invoeren.

Klik op Gereed.

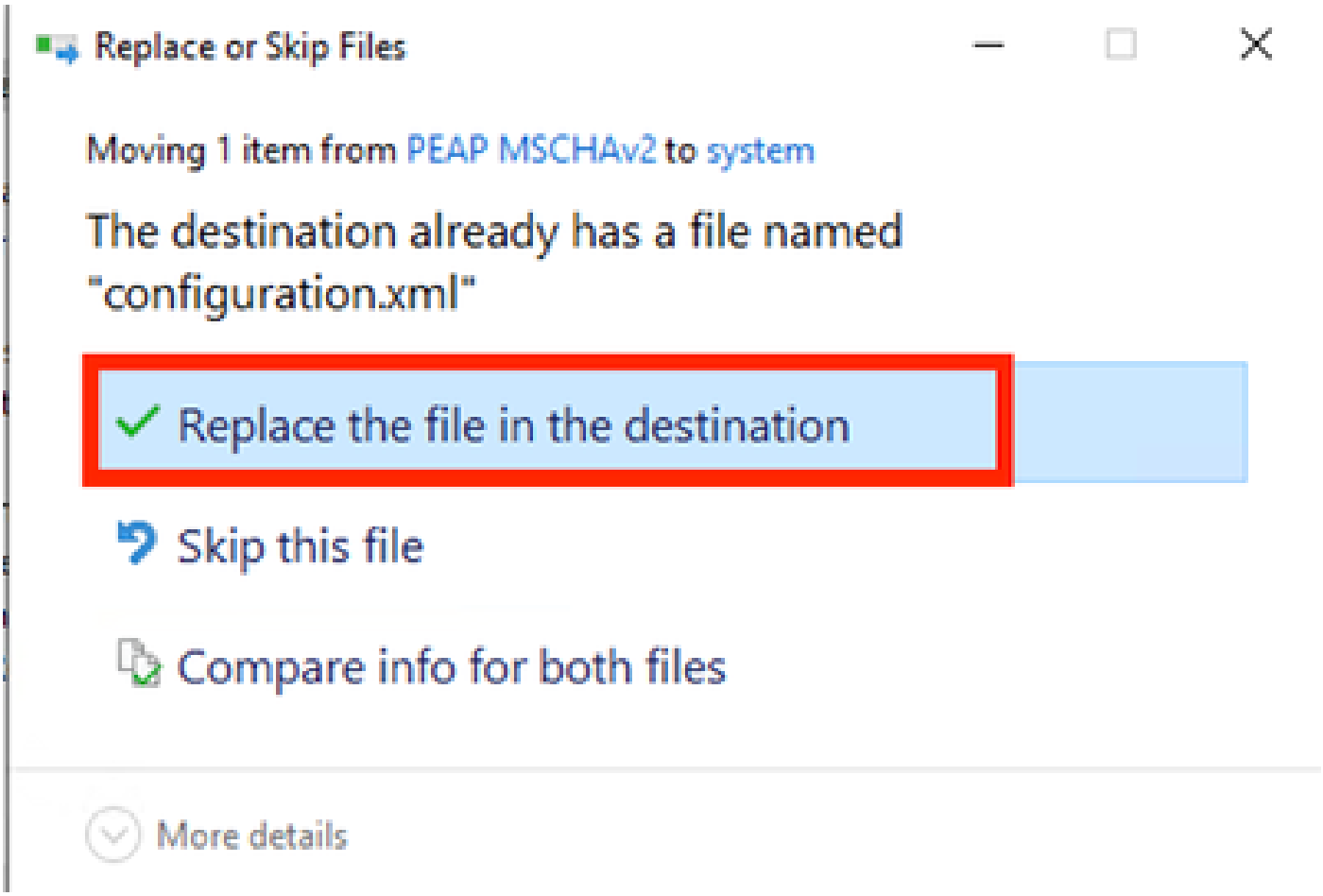
Sla het profiel voor Secure Client Network Access Manager op als configuratie.xml met de optie Bestand > Opslaan als.

Als u Secure Client Network Access Manager wilt gebruiken voor het profiel dat zojuist is gemaakt, vervangt u het bestand Configuration.xml in de volgende map door het nieuwe:

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager/systeem



Opmerking: het bestand moet Configuration.xml worden genoemd, anders werkt het niet.

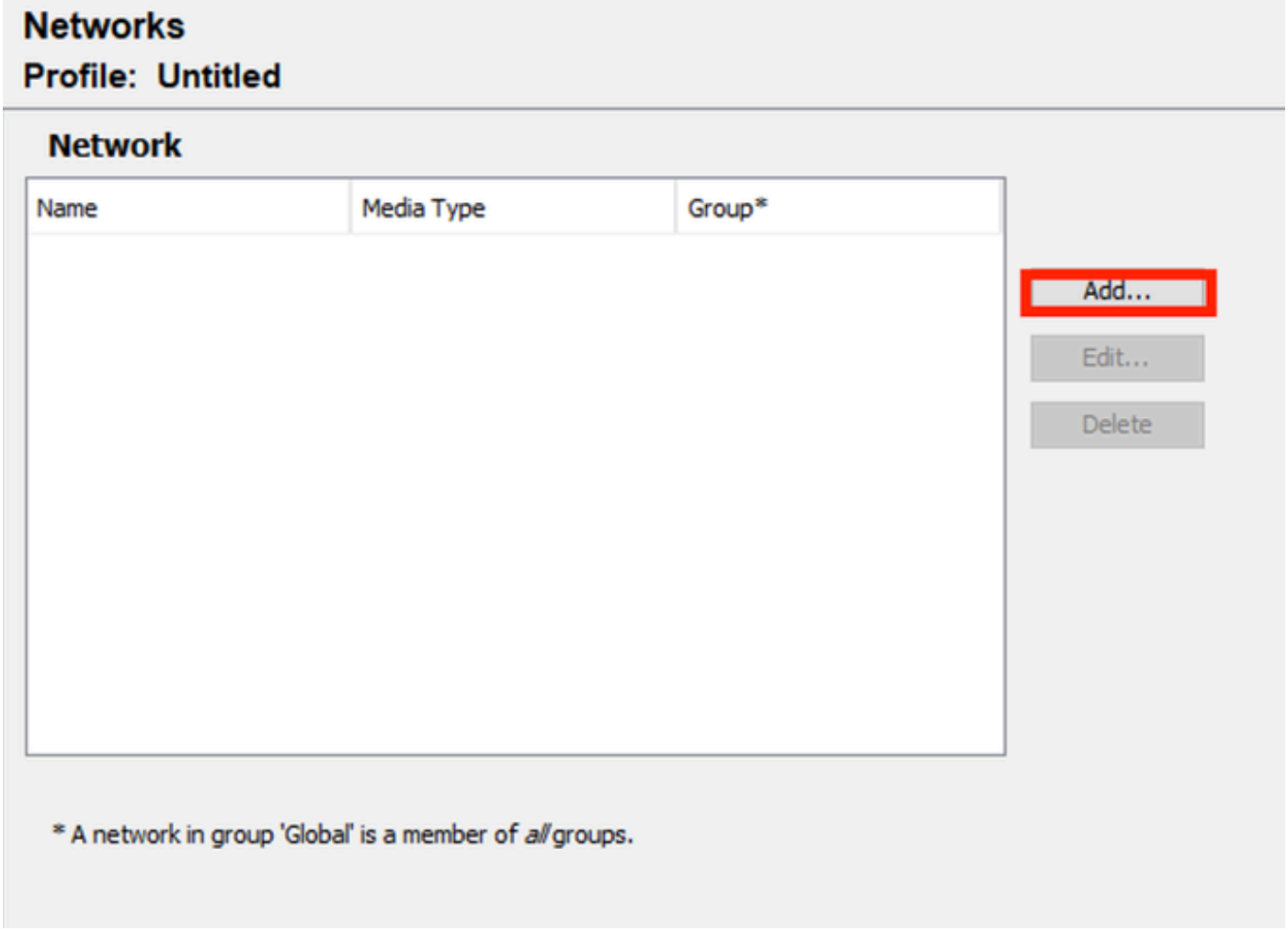


Sectie Bestand vervangen

5. Scenario 2: Secure Client NAM Supplicant voor EAP-FAST simultane gebruikers- en machineverificatie configureren

Open de NAM Profile Editor en navigeer naar de Networks sectie.

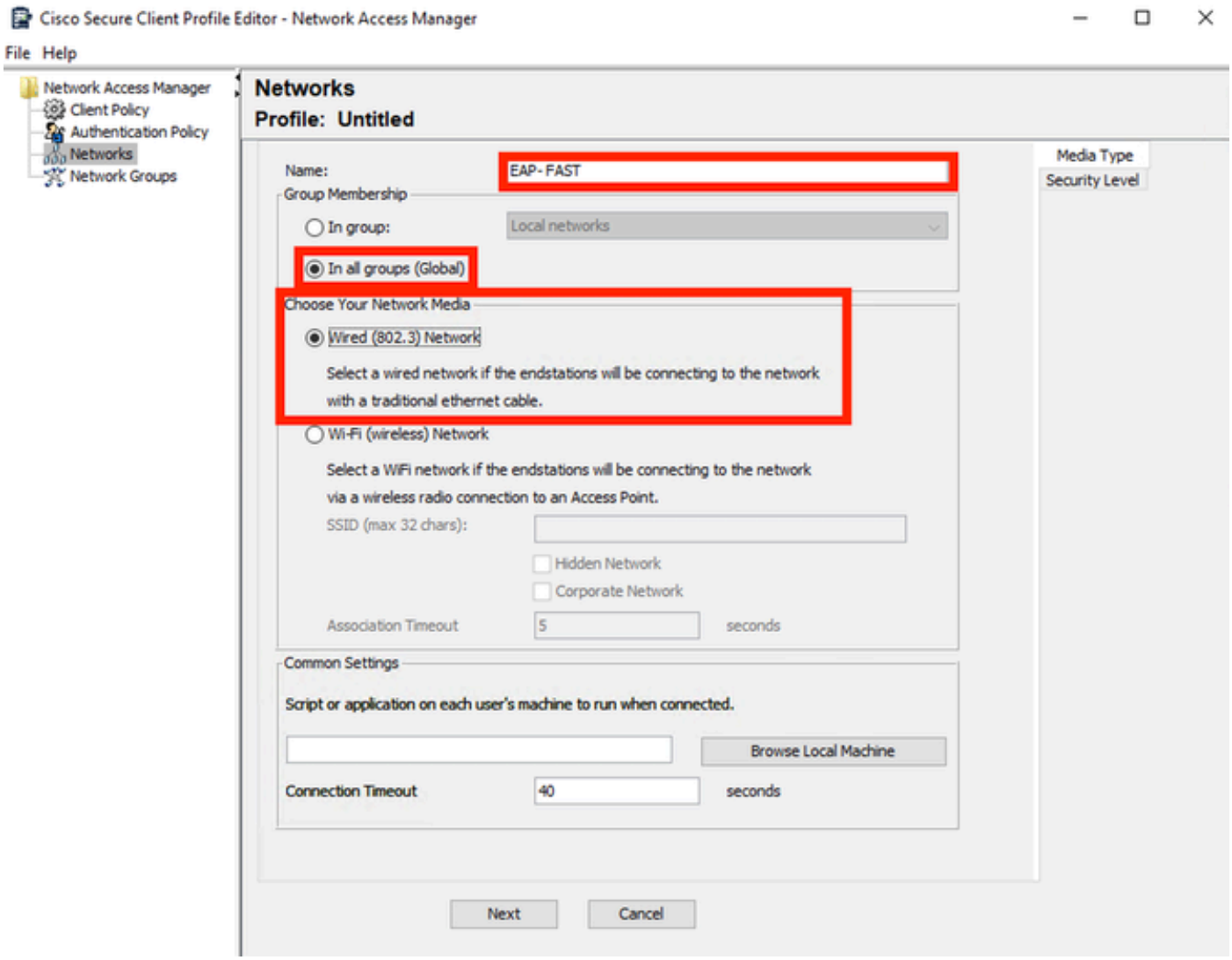
Klik op Add (Toevoegen).



Tabblad Netwerk van NAM Profile Editor

Geef een naam op in het netwerkprofiel.

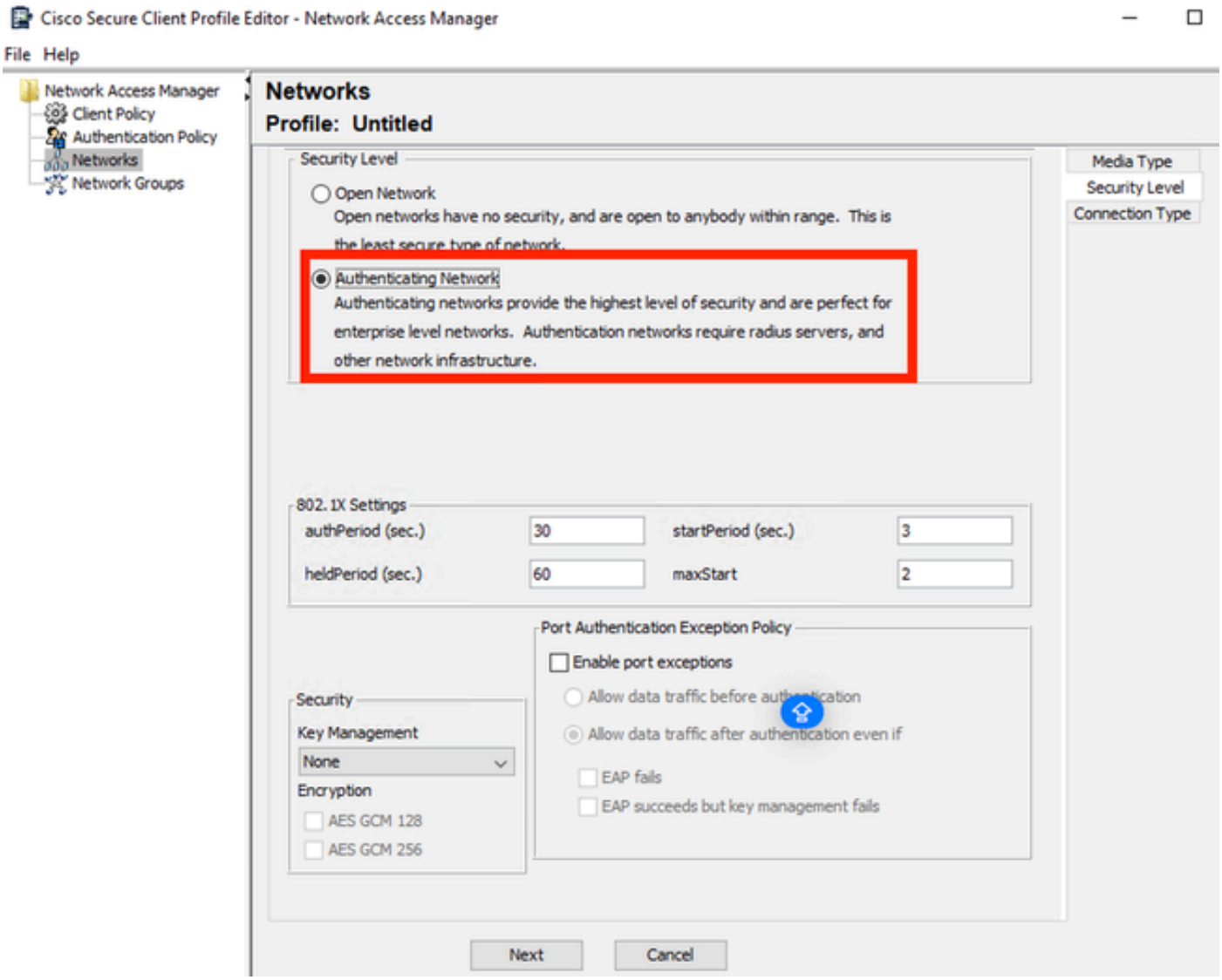
Selecteer Global for Group Membership. Selecteer de media voor bekabeld netwerk.



Sectie Mediatype

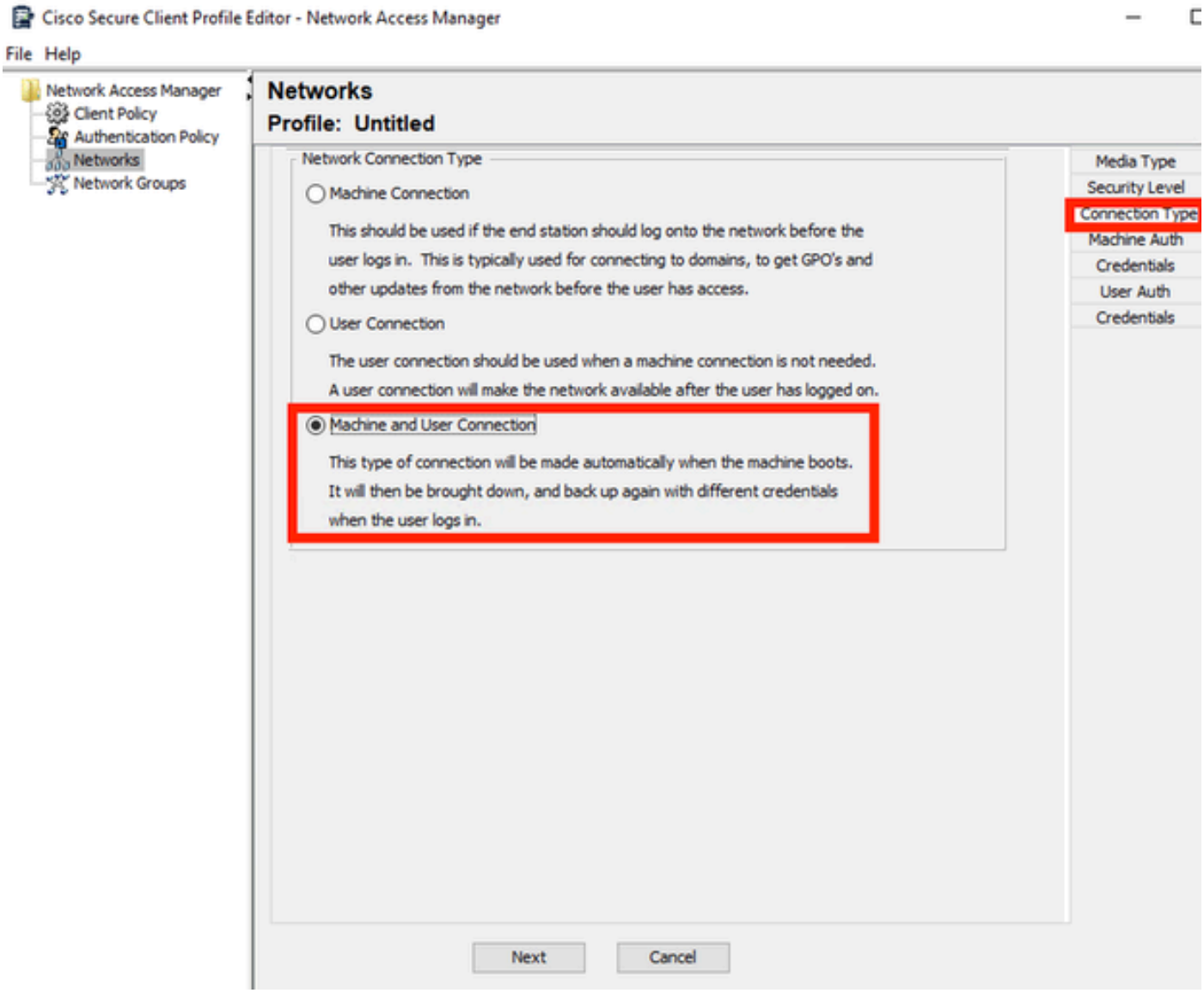
Klik op Next (Volgende).

Selecteer Netwerk verifiëren en wijzig de standaardwaarden voor de rest van de opties in deze sectie niet.



Sectie Security Level Profile Editor

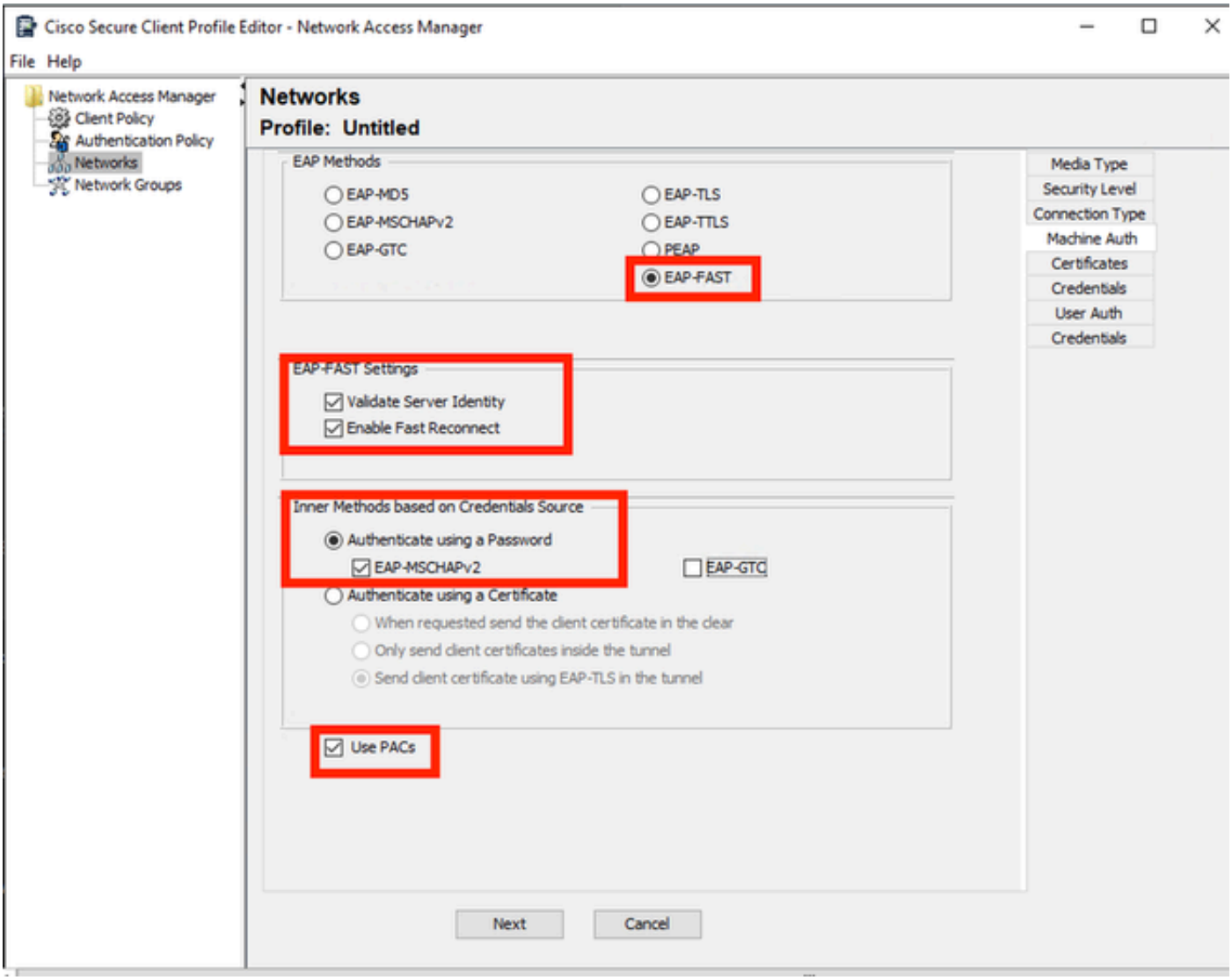
Klik op Volgende om door te gaan met het gedeelte Verbindingstype.



Sectie Verbindingstype

Configureer de gebruiker- en machine-verificatie tegelijkertijd door de derde optie te selecteren.

Klik op Next (Volgende).

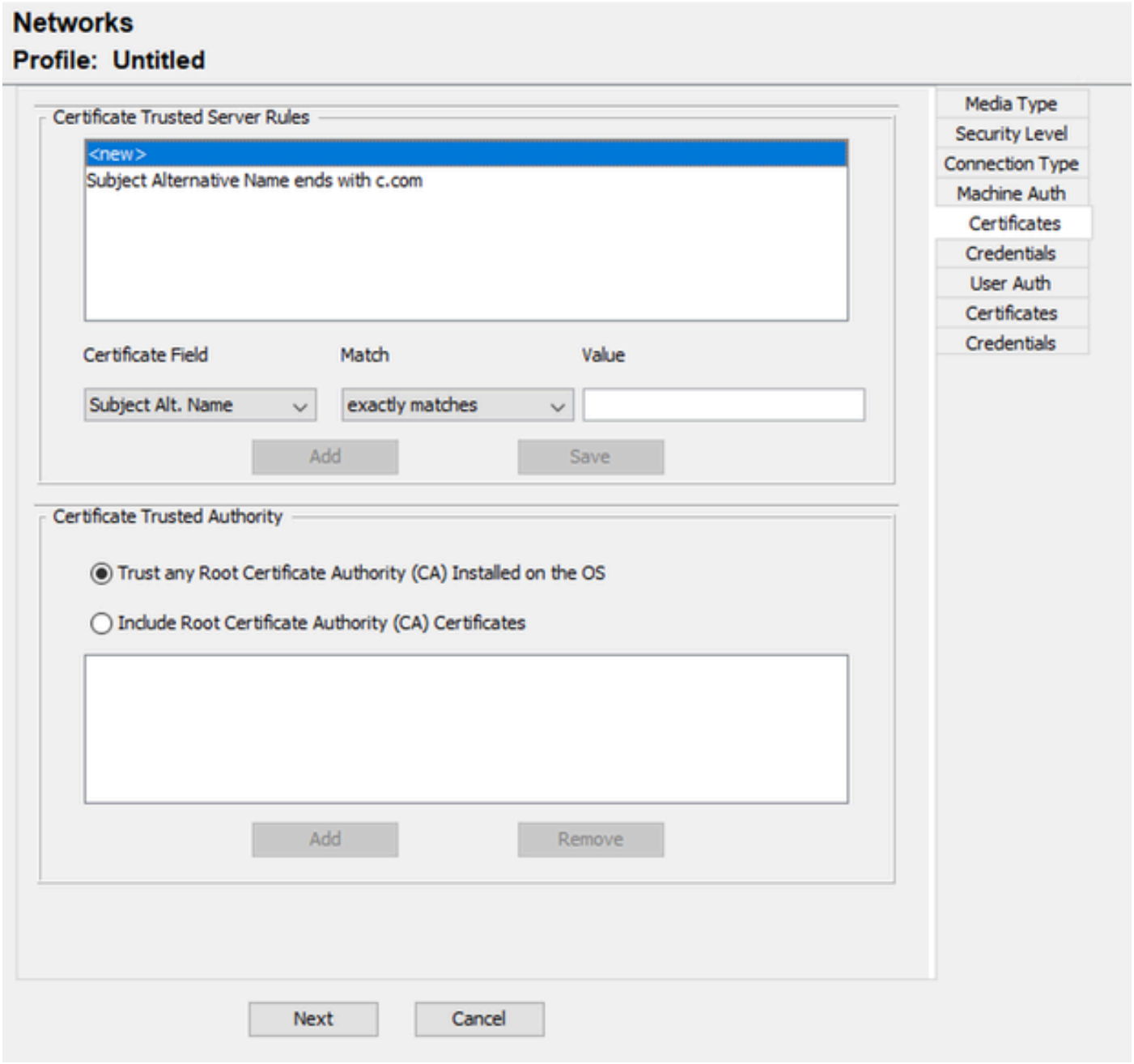


Machinesectie

Selecteer in het gedeelte Machinemachine EAP-FAST als de EAP-methode. Wijzig de standaardwaarden van de EAP FAST-instellingen niet. Voor de Innerlijke methodes die op Credentials Bron sectie worden gebaseerd selecteer Verifiëren met een Wachtwoord en EAP-MSCHAPv2 als de methode. Selecteer vervolgens de optie PAC's gebruiken.

Klik op Next (Volgende).

In de sectie Certificaten, in Certificate Trusted Server Rules eindigt de regel gemeenschappelijke naam met c.com. Dit deel verwijst naar het certificaat dat de server gebruikt tijdens de EAP PEAP-stroom. Als Identity Service Engine (ISE) in uw omgeving wordt gebruikt, kan de algemene naam van het EAP-certificaat van het Policy Server-knooppunt worden gebruikt.

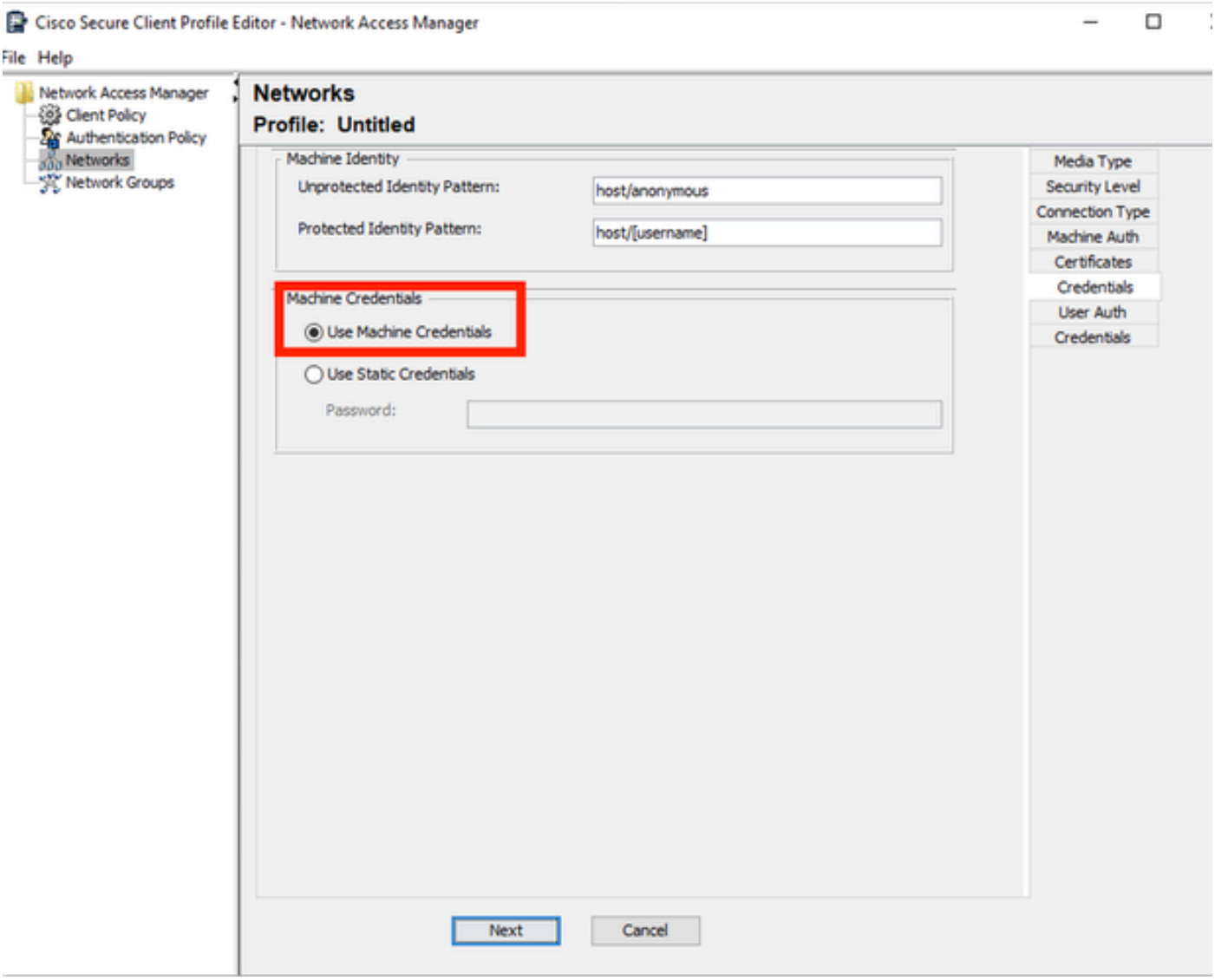


Sectie Machineserver Certificaat van vertrouwen

Er kunnen twee opties worden geselecteerd in Certificate Trusted Authority. Voor dit scenario in plaats van een specifiek CA-certificaat toe te voegen dat het EAP-certificaat van RADIUS heeft ondertekend, gebruikt u de optie Vertrouwen op elke Root Certificate Authority (CA) die op het besturingssysteem is geïnstalleerd.

Met deze optie vertrouwt Windows op elke EAP cert die is ondertekend door een cert die is opgenomen in het programma Gebruikerscertificaten beheren (huidige gebruiker > Trusted Root Certification Authorities > Certificates).

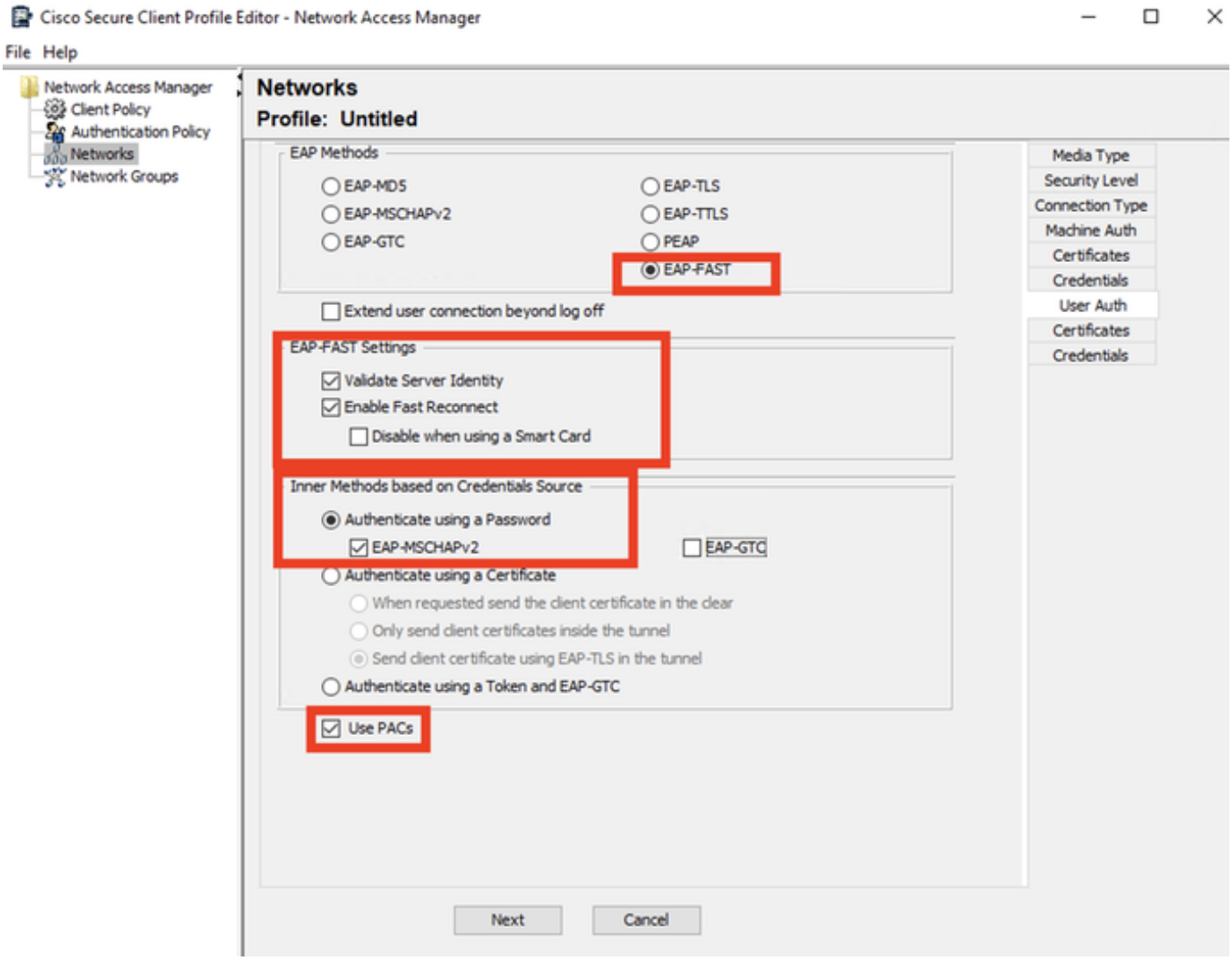
Klik op Next (Volgende).



Sectie Automatische referenties

Selecteer Machine-referenties gebruiken in het gedeelte Machine-referenties.

Klik op Next (Volgende).



Sectie Gebruikersverificatie

Selecteer voor Gebruikersautorisatie EAP-FAST als de EAP-methode.

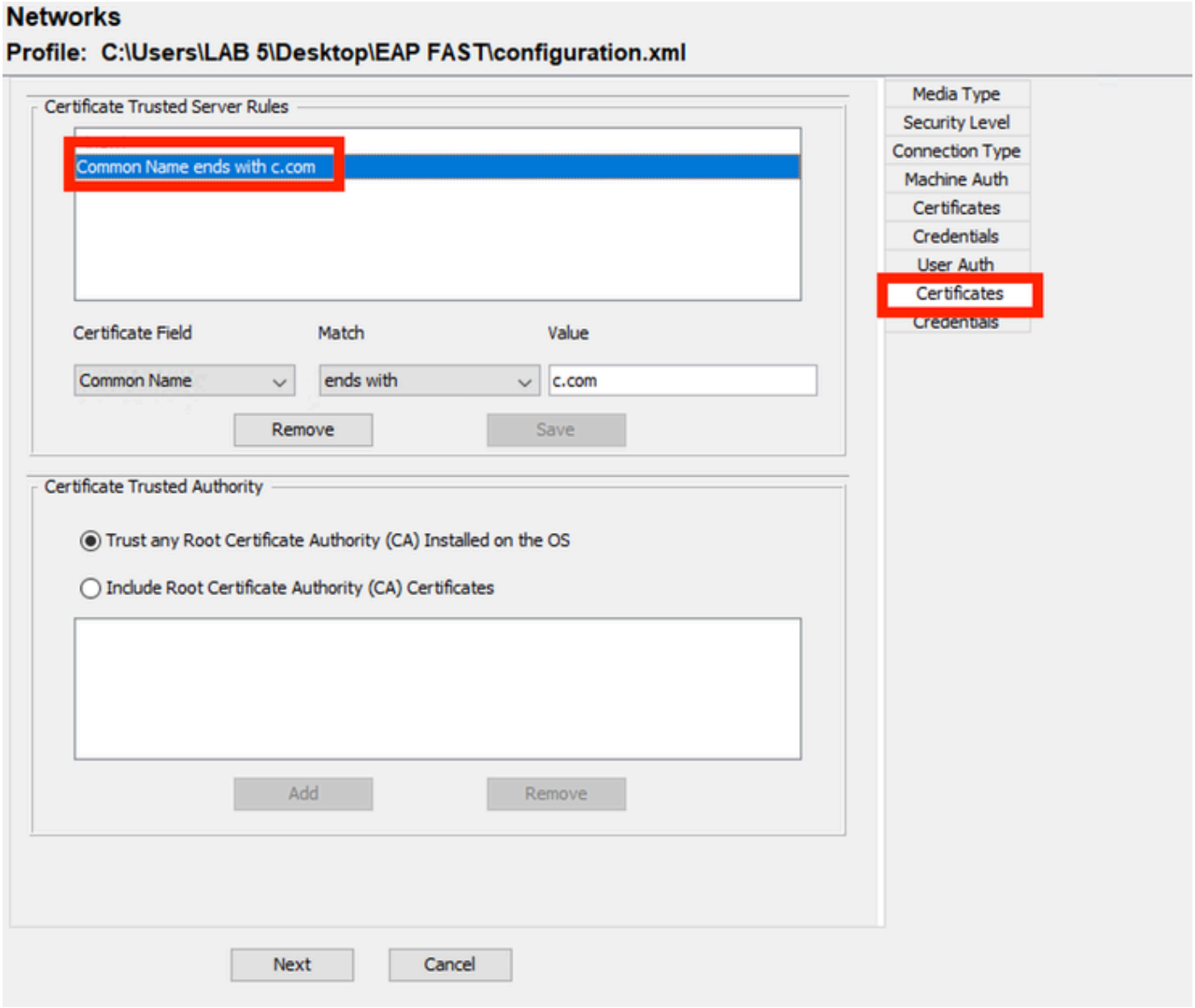
Wijzig de standaardwaarden niet in het gedeelte EAP-FAST-instellingen.

Selecteer in het gedeelte Inner Method gebaseerd op aanmeldingsbron de optie Verifiëren met een wachtwoord en EAP-MSCHAPv2 als methode.

Selecteer PAC's gebruiken.

Klik op Next (Volgende).

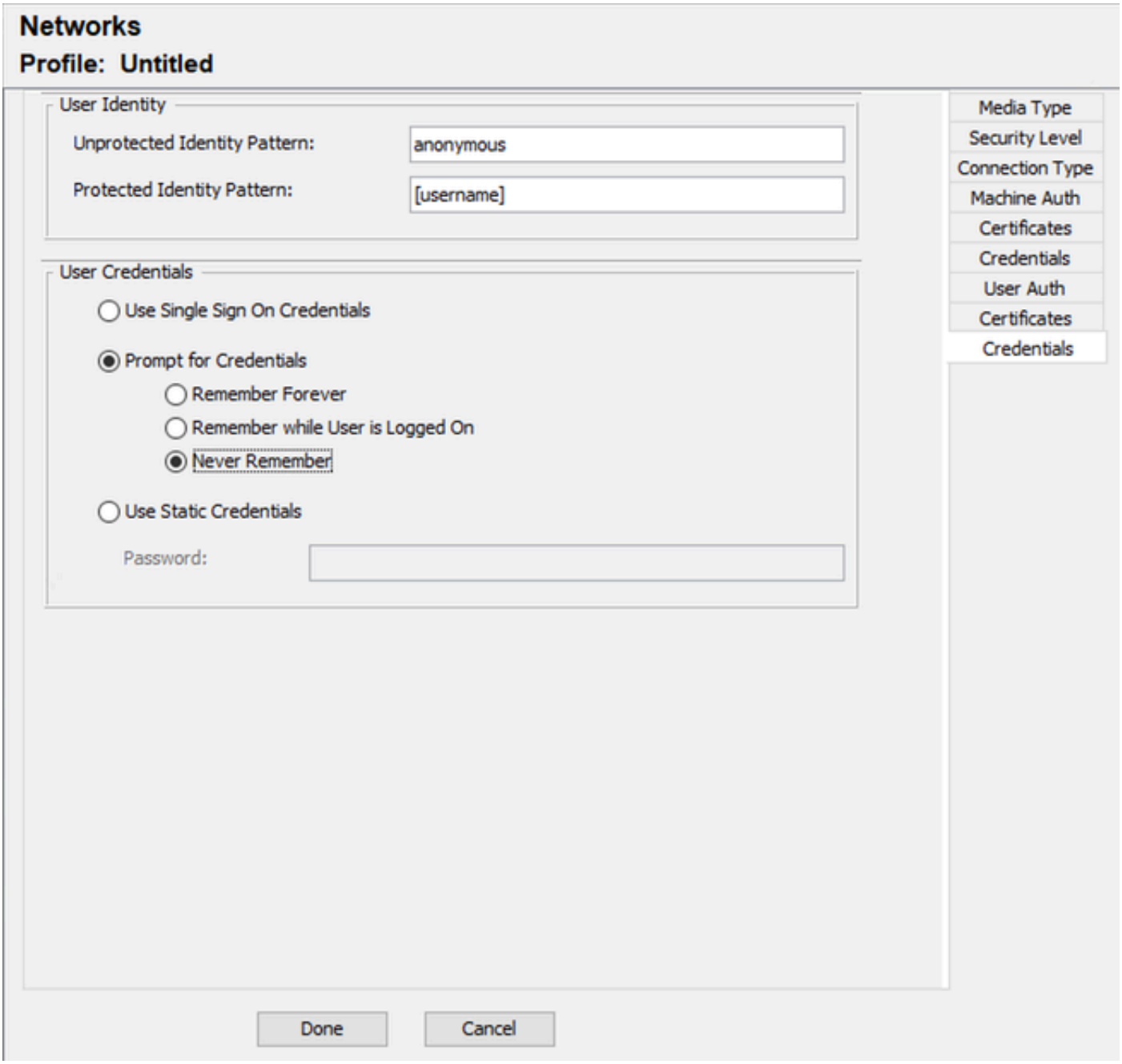
In de sectie Certificaten, in Certificate Trusted Server Regels, is de regel Common Name eindigt met c.com. Deze configuraties dienen voor het certificaat dat de server gebruikt tijdens de EAP PEAP-stroom. Als ISE in uw omgeving wordt gebruikt, kan de algemene naam van het EAP-certificaat voor de beleidsserverknooppunt worden gebruikt.



Sectie Gebruikersautorisatieserver - Certificaat van vertrouwen

Er kunnen twee opties worden geselecteerd in Certificate Trusted Authority. In dit scenario wordt in plaats van een specifiek CA-certificaat dat het EAP-certificaat van RADIUS heeft ondertekend, de optie Vertrouwen elke Root Certificate Authority (CA) die op het besturingssysteem is geïnstalleerd, gebruikt.

Klik op Next (Volgende).



Credentials gebruikersautorisatie

In het gedeelte Credentials wordt alleen het gedeelte Gebruikersreferenties gewijzigd.

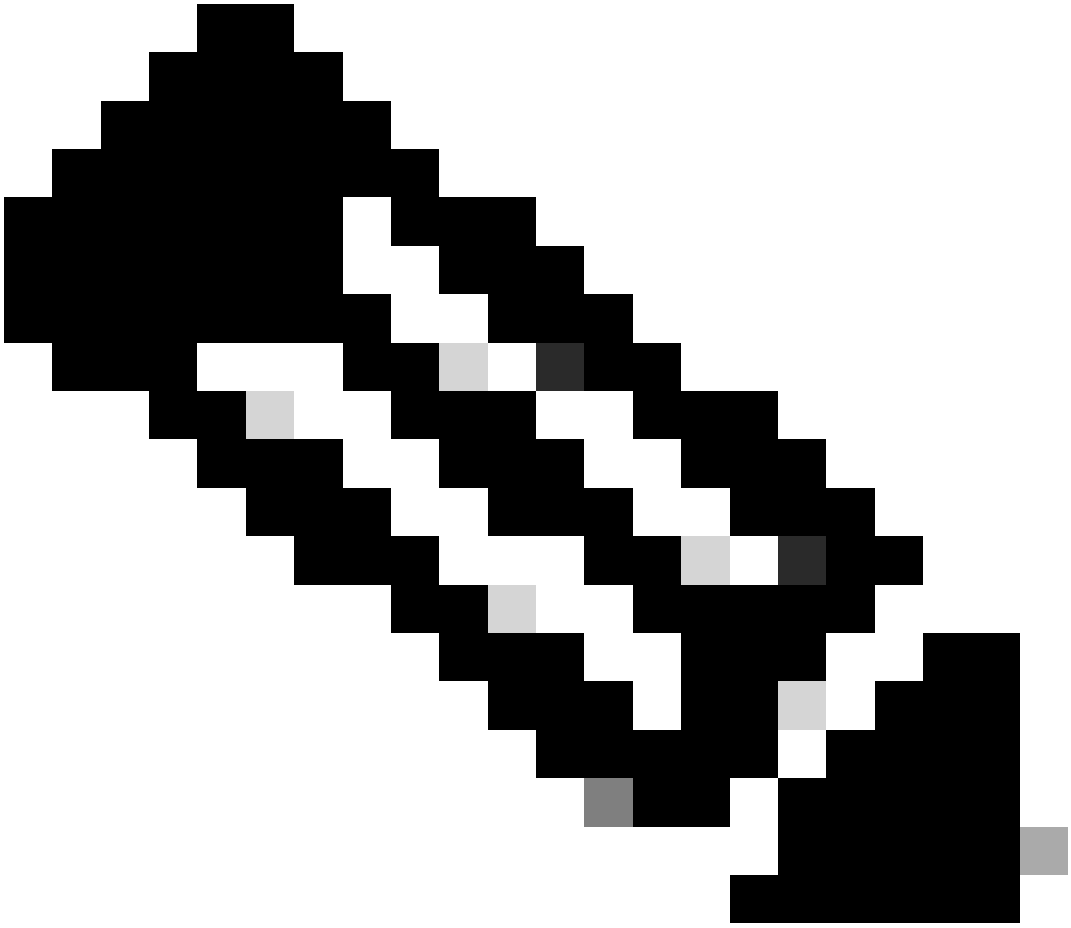
De optie Vragen om referenties > Niet onthouden is geselecteerd. Bij elke verificatie moet de gebruiker die de verificatie uitvoert dus zijn referenties invoeren.

Klik op de knop Gereed.

Selecteer Bestand > Opslaan als en sla het profiel voor Secure Client Network Access Manager op als configuratie.xml.

Als u de Secure Client Network Access Manager wilt laten gebruiken van het profiel dat zojuist is gemaakt, vervangt u het bestand Configuration.xml in de volgende map door het nieuwe:

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager/systeem



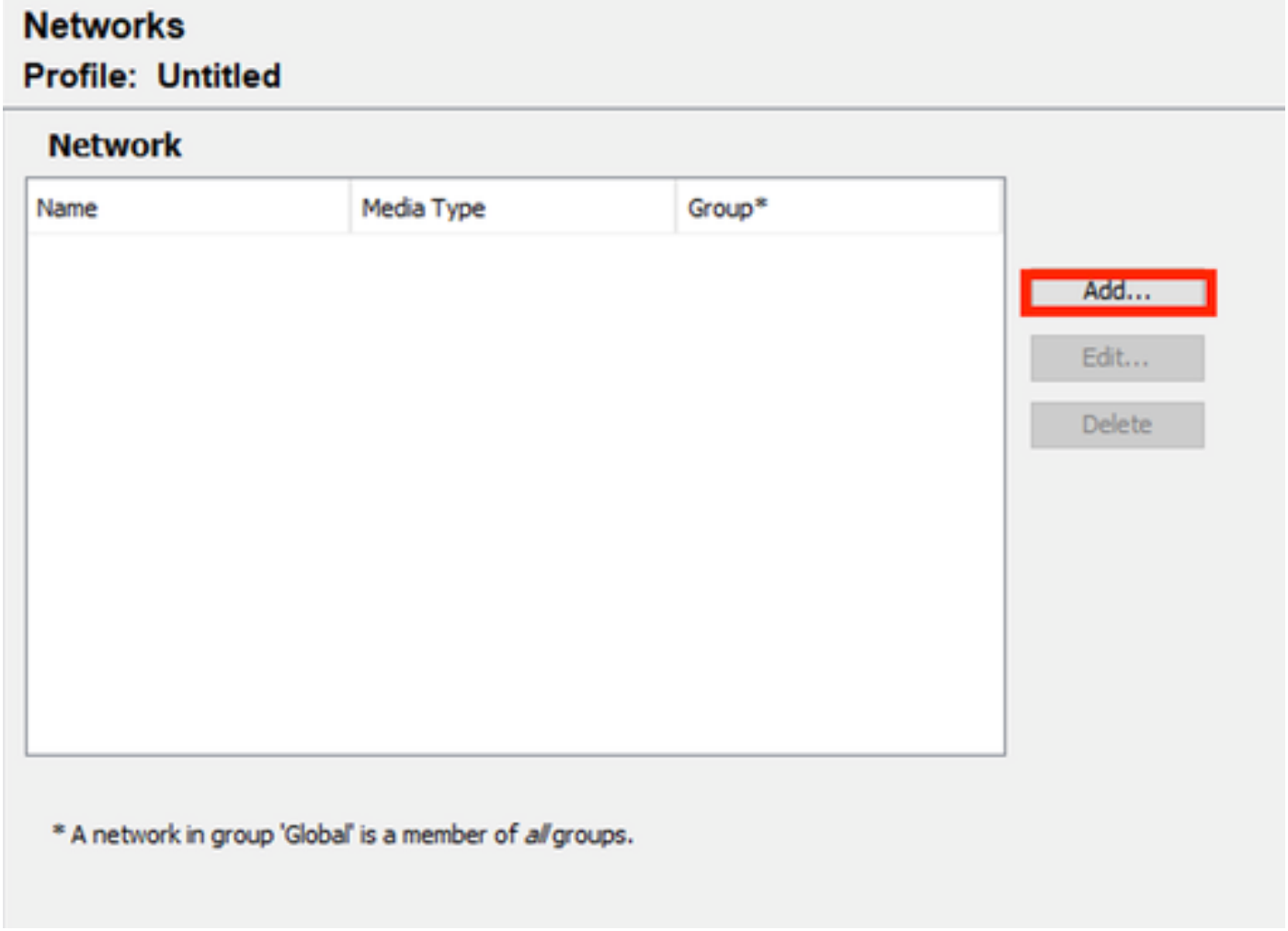
Opmerking: het bestand moet Configuration.xml worden genoemd, anders werkt het niet.

---

6. Scenario 3: Secure Client NAM Supplicant voor EAP TLS-gebruikerscertificaatverificatie configureren

Open de NAM Profile Editor en navigeer naar de sectie Networks.

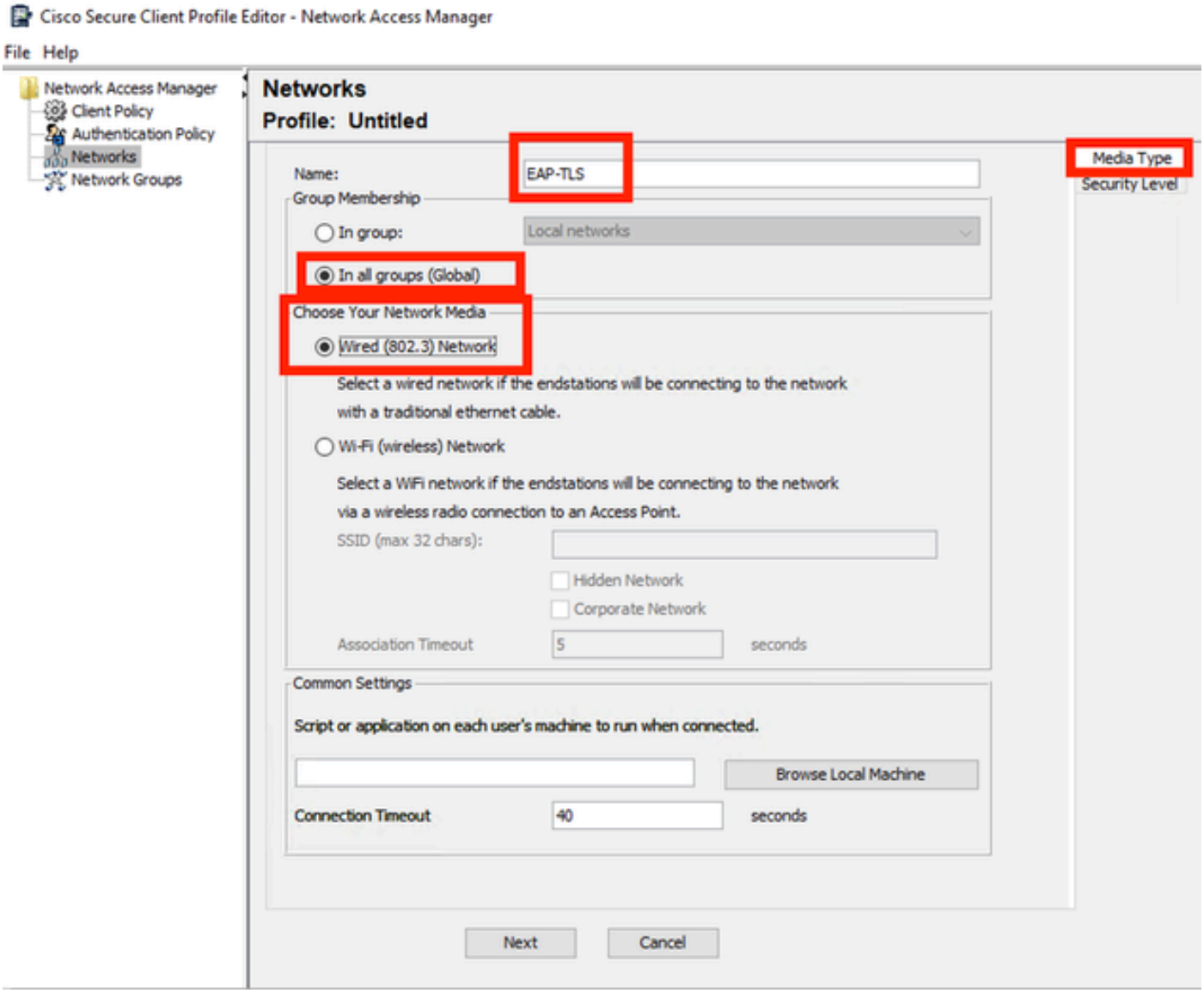
Klik op Add (Toevoegen).



Sectie Netwerkmaken

Geef het netwerkprofiel een naam, in dit geval is de naam gelijk aan het EAP-protocol dat voor dit scenario wordt gebruikt.

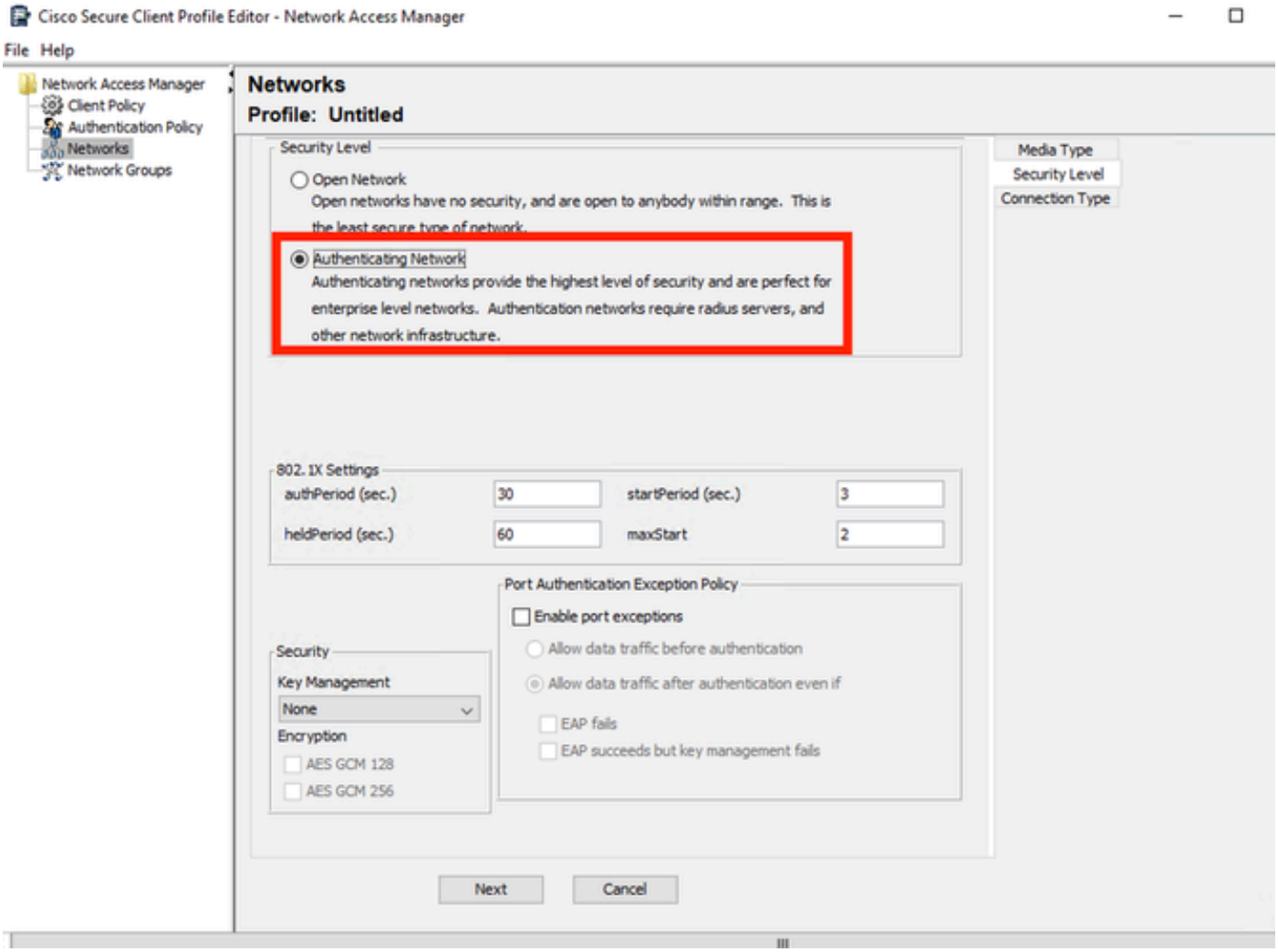
Selecteer Global for Group Membership. en bekabelde netwerkmedia.



Sectie Mediatype

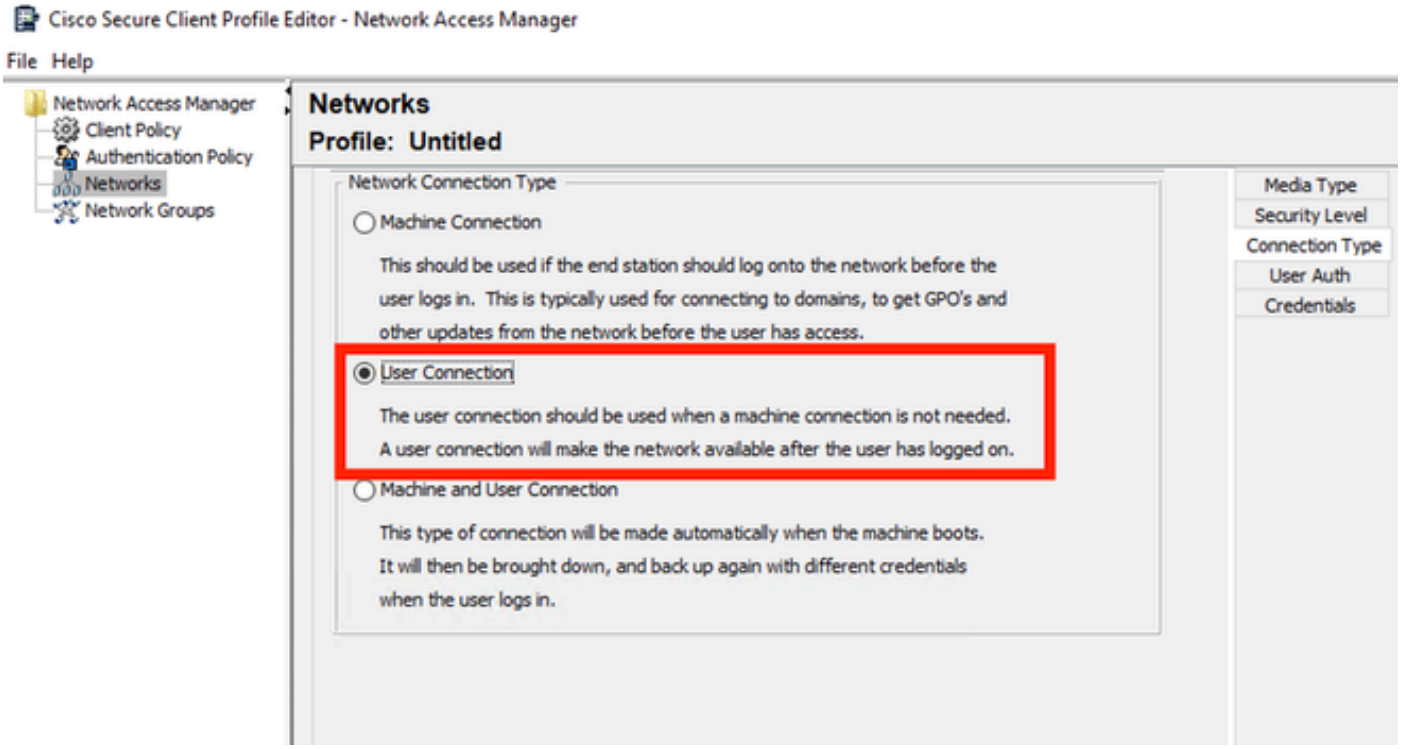
Klik op Next (Volgende).

Selecteer Netwerk verifiëren en wijzig de standaardwaarden voor de rest van de opties in de sectie Beveiligingsniveau niet.



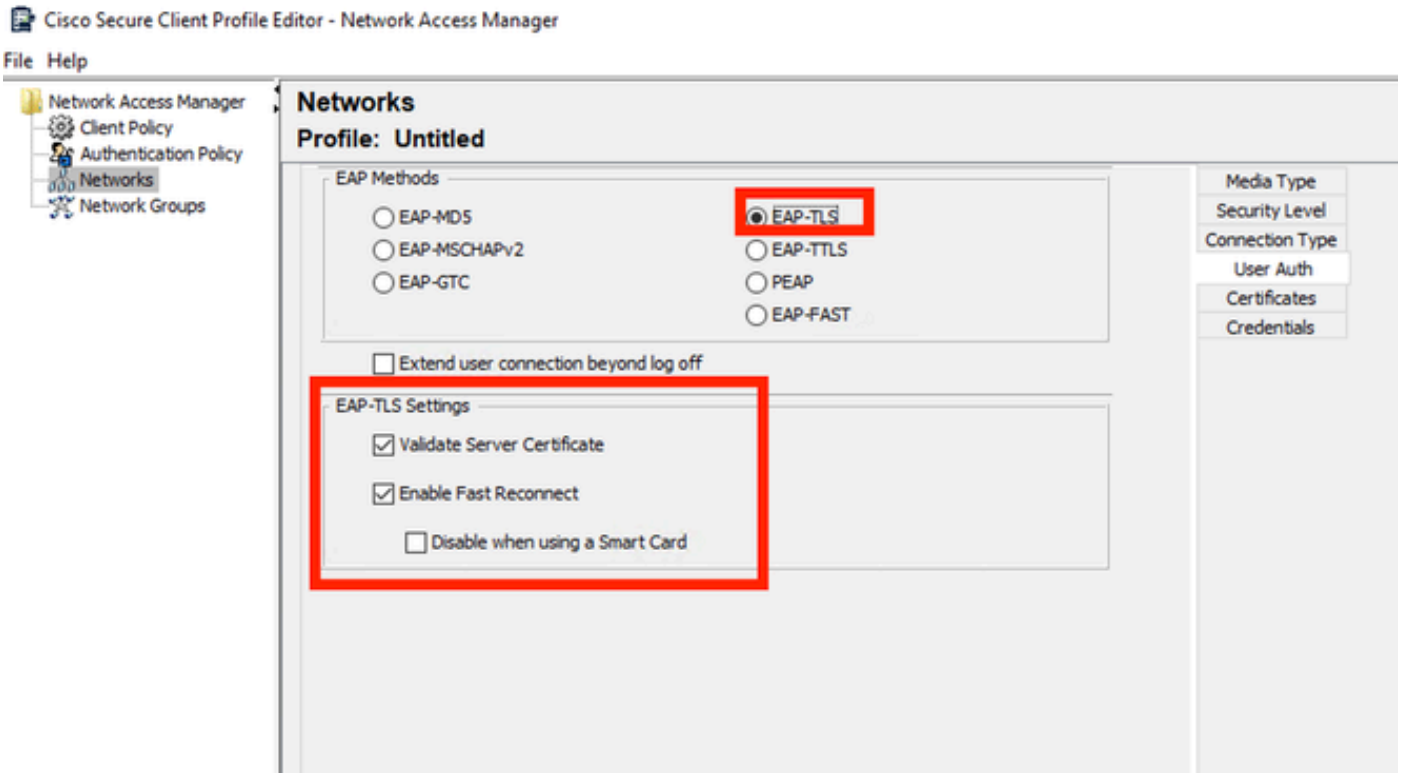
Beveiligingsniveau

Dit scenario is voor gebruikersverificatie met behulp van een certificaat. Daarom wordt de optie Gebruikersverbinding gebruikt.



Verbindingstype

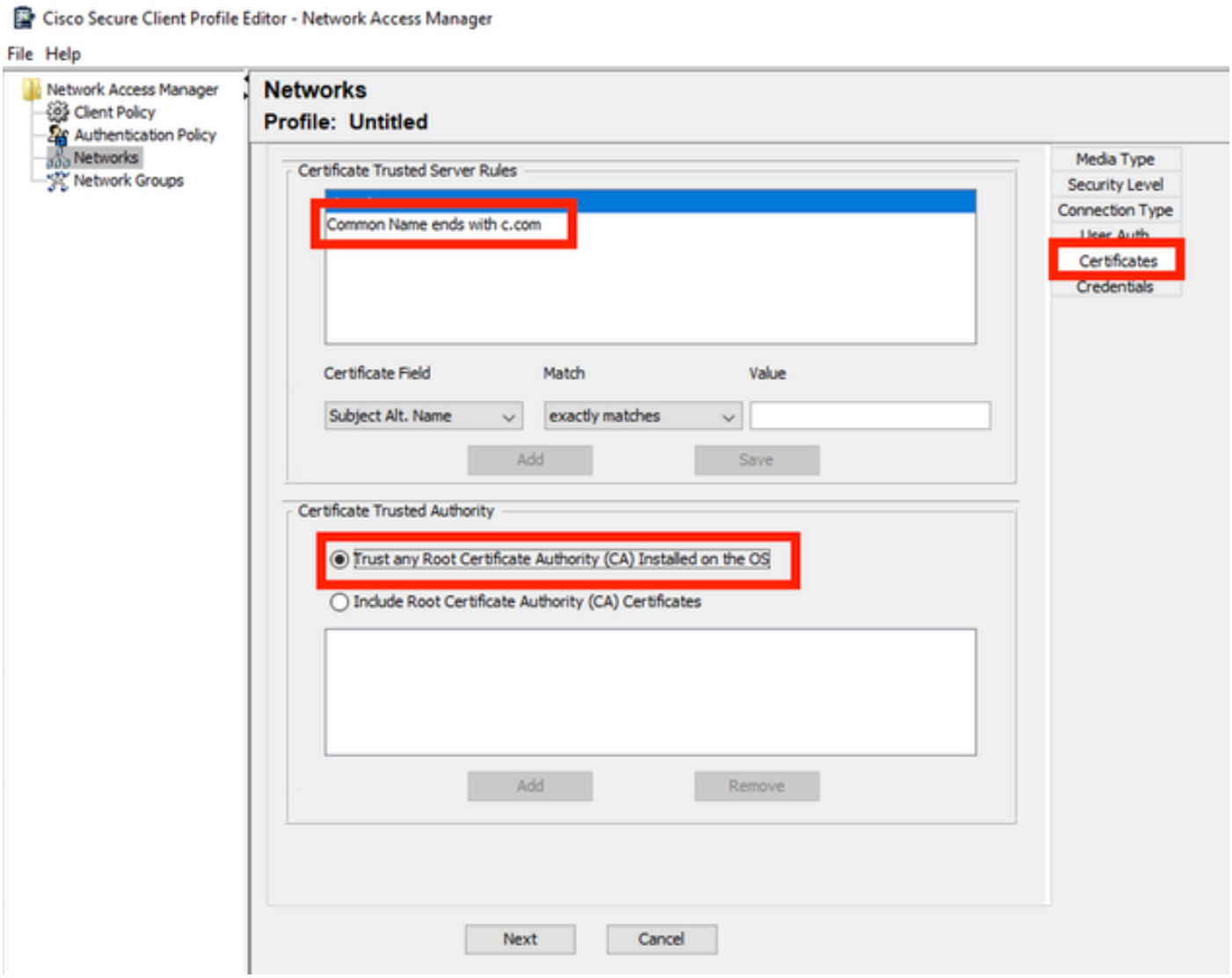
Configureer EAP-TLS als de EAP-methode. Wijzig de standaardwaarden in het gedeelte EAP-TLS-instellingen niet.



Sectie Gebruikersautorisatie

Voer in het gedeelte Certificaten een regel in die overeenkomt met het AAA EAP-TLS-certificaat. Als u ISE gebruikt, vindt u deze regel in sectie Beheer > Systeem > Certificaten.

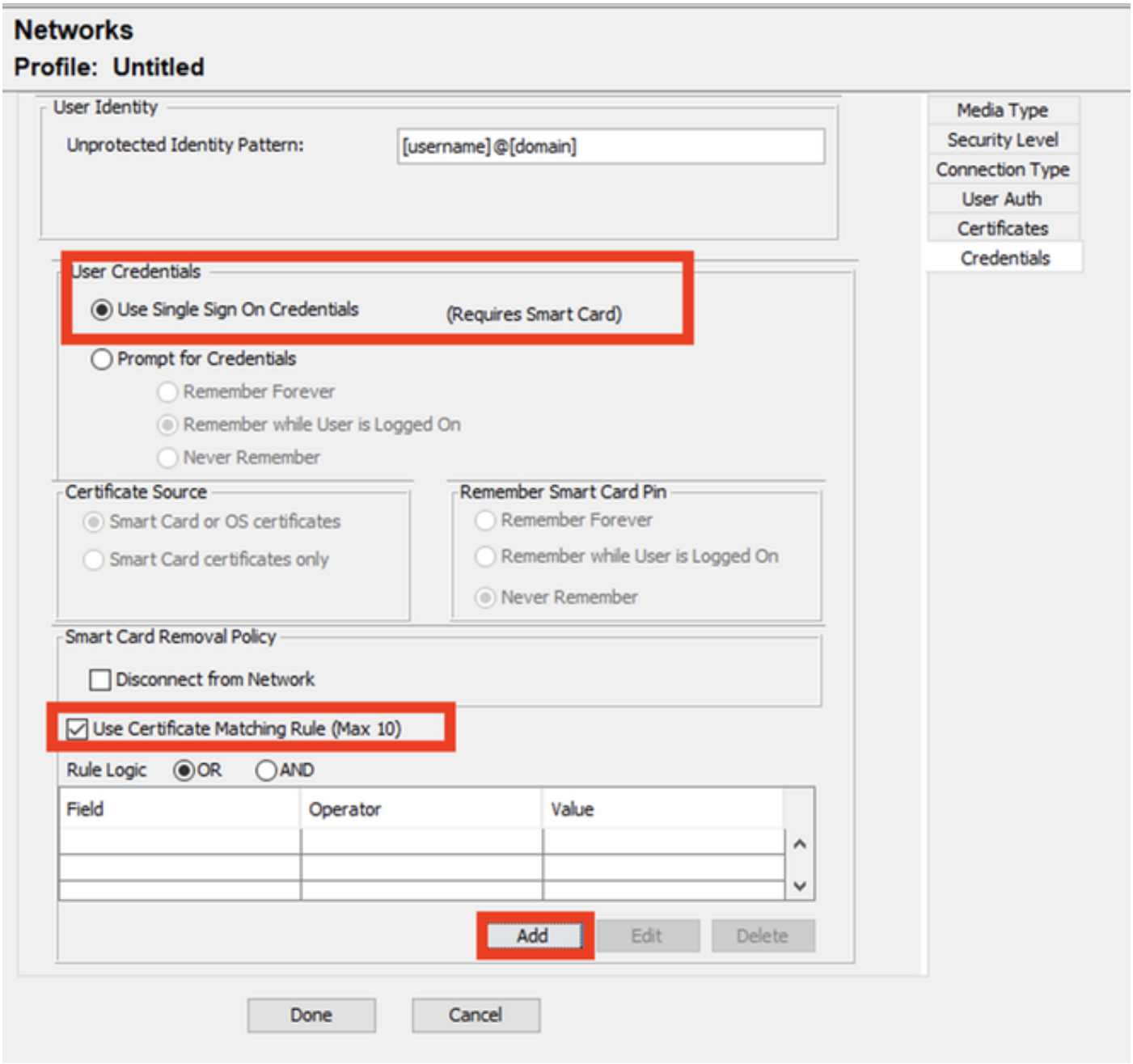
Selecteer in het gedeelte Certificate Trusted Authority de optie Trust Any Root Certificate Authority (CA) dat in het besturingssysteem is geïnstalleerd.



Instellingen voor certificaat van gebruikersautorisatie

Klik op Next (Volgende).

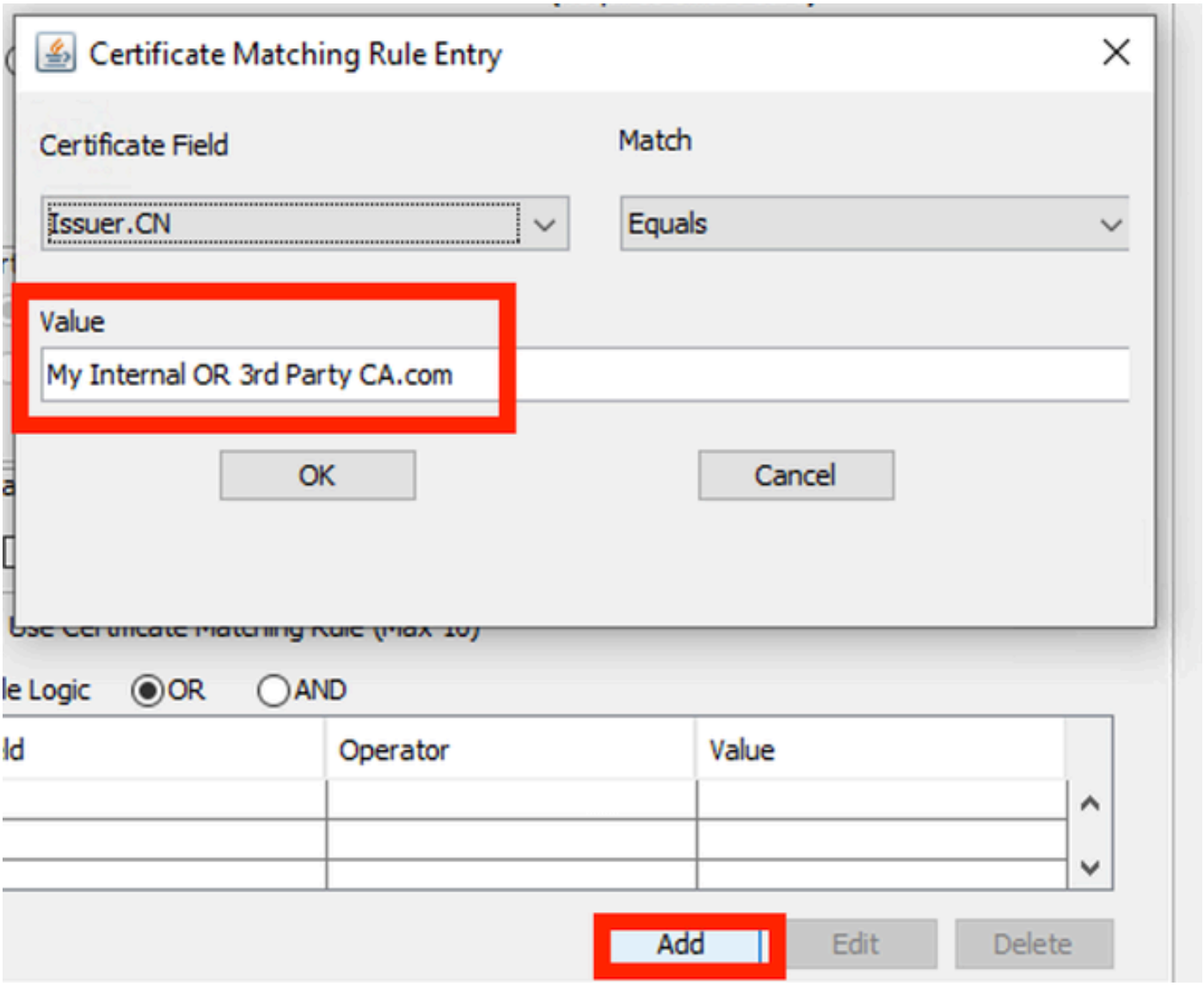
Wijzig de standaardwaarden in het eerste deel van het gedeelte Gebruikersreferenties niet.



Sectie Gebruikersautorisatie

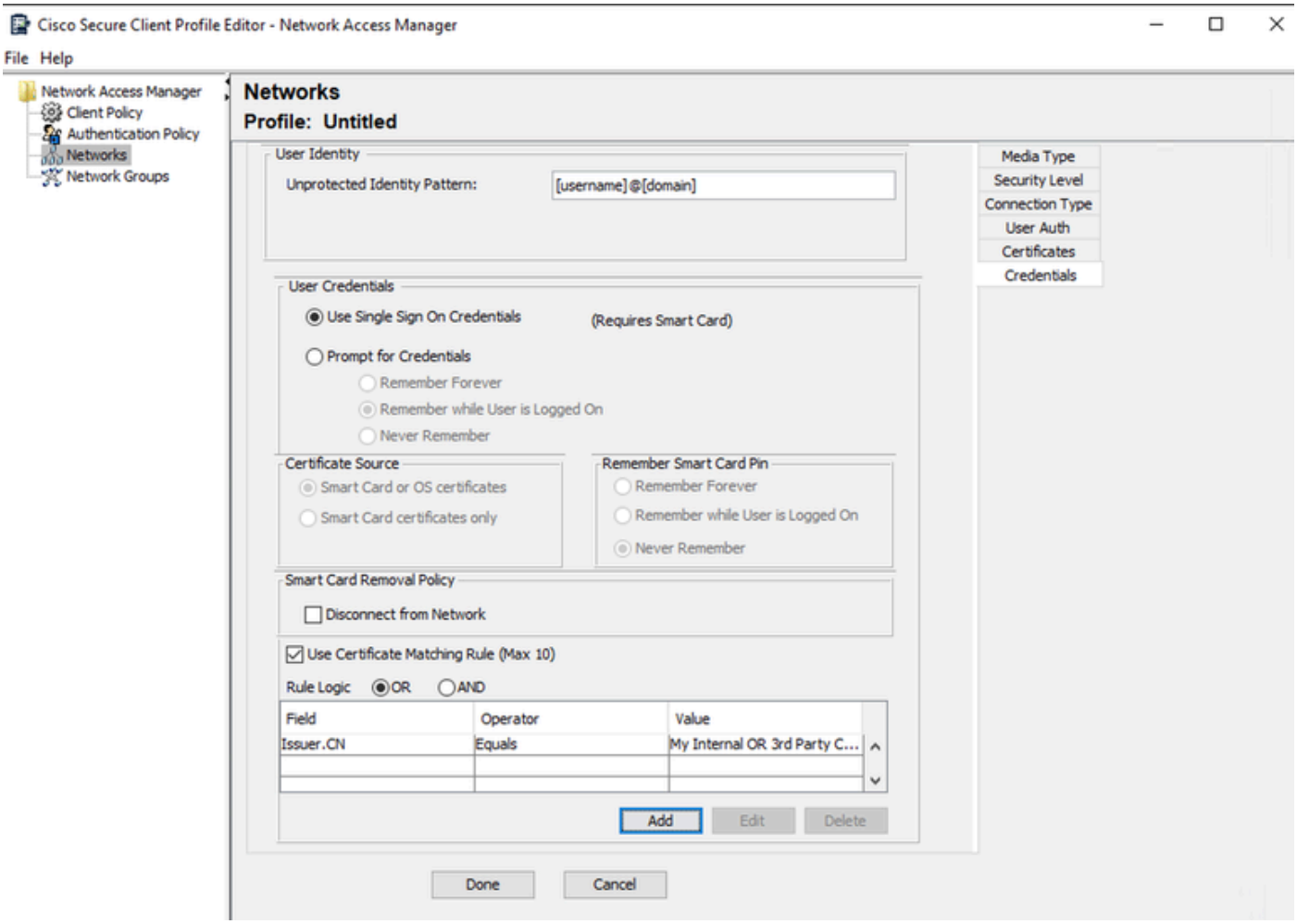
Het is belangrijk om een regel te configureren die overeenkomt met het identiteitscertificaat dat de gebruiker verstuurt tijdens het EAP TLS-proces. Om dit te doen klik op het selectievakje naast Certificaatbewerkingsregel gebruiken (max. 10).

Klik op Add (Toevoegen).



Venster Certificaat-overeenkomstregel

Vervang de waarde My Internal OR 3rd Party CA.com string door de CN van het gebruikerscertificaat.



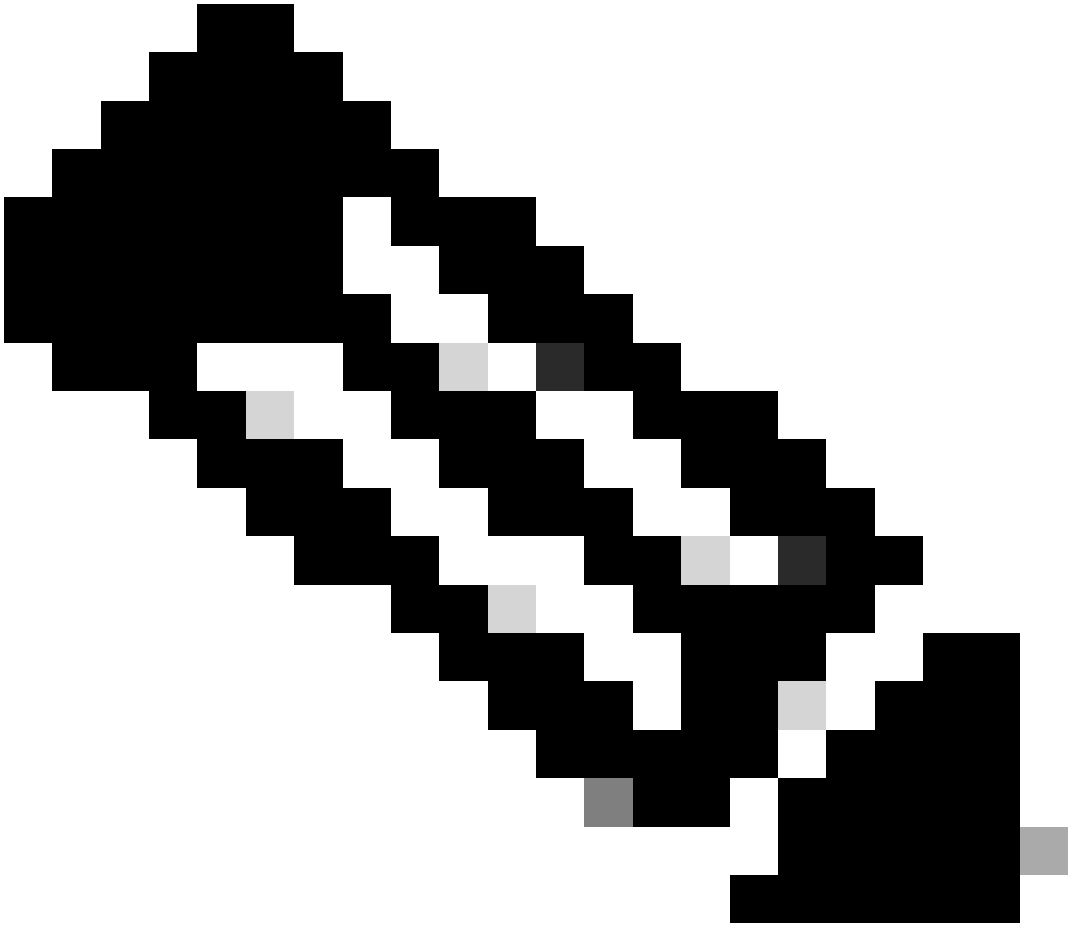
Sectie Gebruikersautorisatiecertificaat referenties

Klik op Gereed om de configuratie te voltooien.

Selecteer Bestand > Opslaan als om het profiel voor Secure Client Network Access Manager op te slaan als configuratie.xml.

Als u de Secure Client Network Access Manager wilt laten gebruiken van het profiel dat zojuist is gemaakt, vervangt u het bestand Configuration.xml in de volgende map door het nieuwe:

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager/systeem



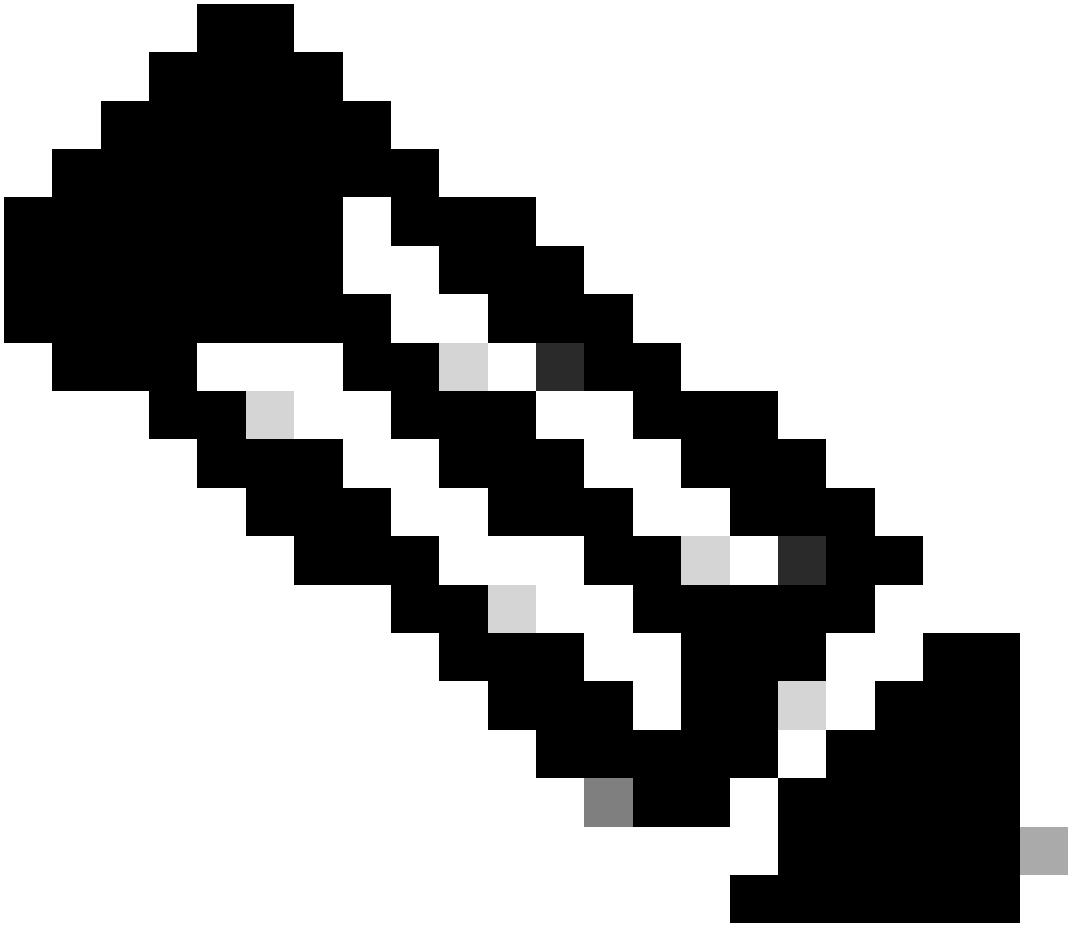
Opmerking: het bestand moet Configuration.xml worden genoemd, anders werkt het niet.

---

7. Configureer ISR 1100 en ISE om verificaties toe te staan op basis van scenario 1 PEAP MSCHAPv2

Configureer de ISR 1100 router.

In dit hoofdstuk wordt ingegaan op de basisconfiguratie die de NAD moet hebben om dot1x te laten werken.



Opmerking: voor de implementatie van ISE voor meerdere knooppunten, wijs naar elk knooppunt dat de Policy Server Node-persoonlijkheid heeft ingeschakeld. Dit kan worden gecontroleerd door naar ISE te navigeren in het tabblad Beheer > Systeem > Installatie.

```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
 client A.B.C.D server-key  <Your shared secret>
!
!
radius server  ISE-PSN-1
 address ipv4 A.B.C.D auth-port 1645 acct-port 1646
 timeout 15
 key <Your shared secret>
```

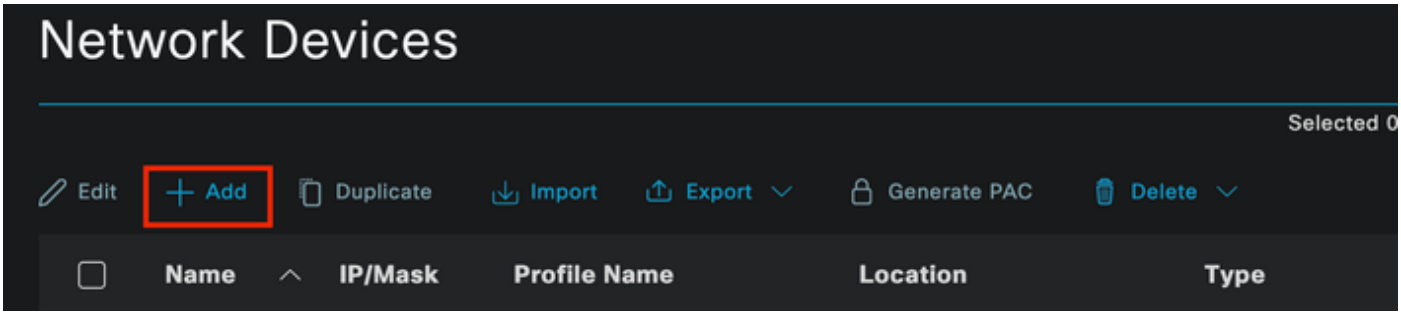
```
!
!
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
```

Identity Service Engine configureren 3.2.

Configureer het netwerkapparaat.

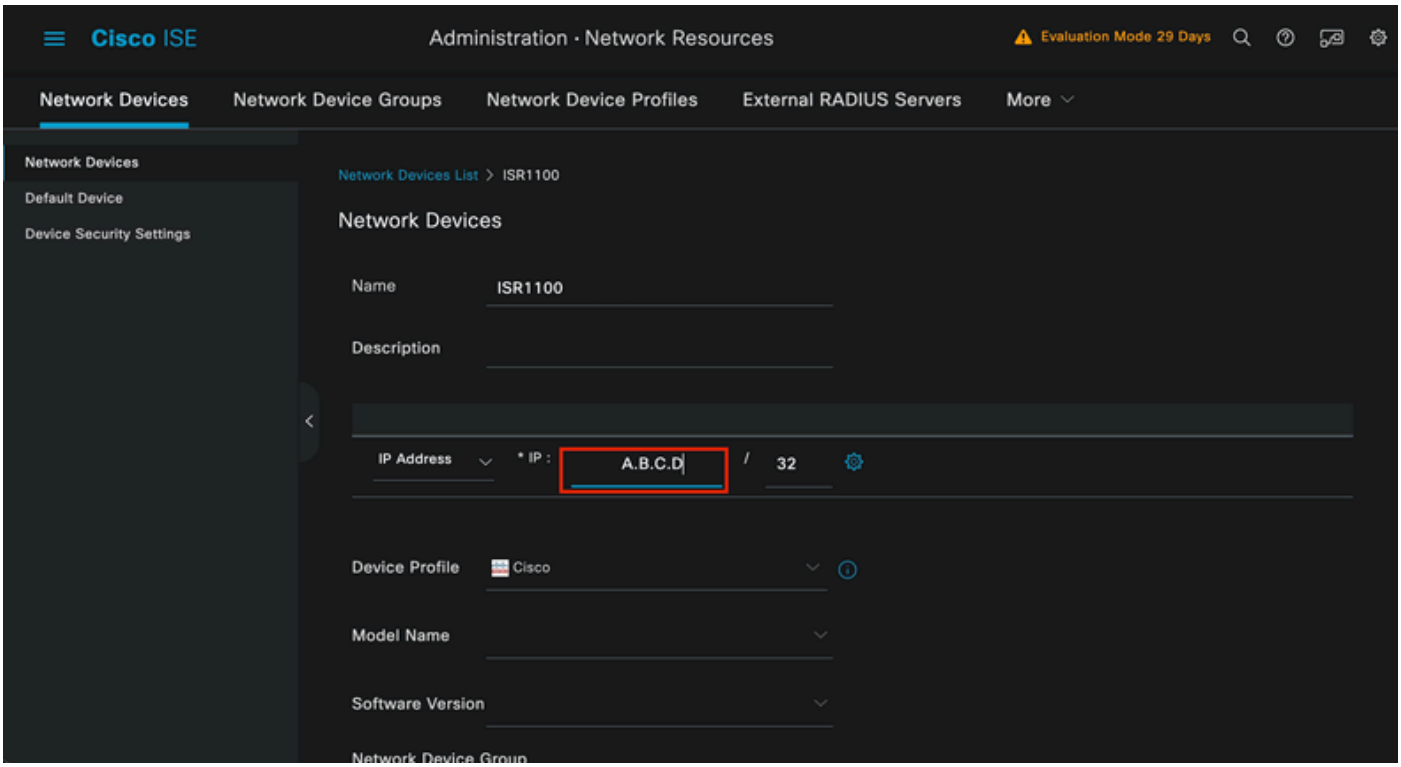
Voeg de ISR en de ISE toe aan ISE-beheer > Netwerkbronnen > Netwerkapparaten.

Klik op Add (Toevoegen).



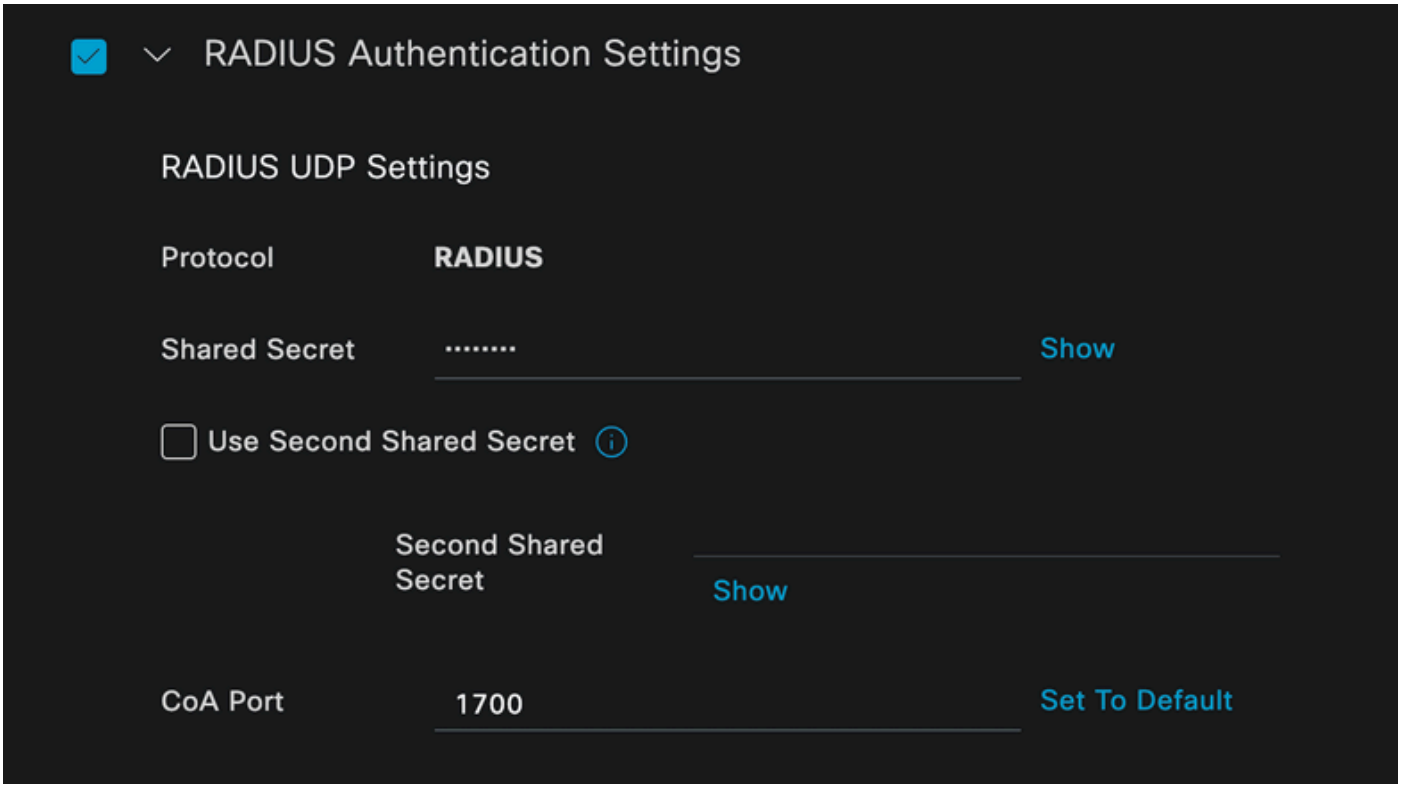
Sectie Netwerkapparaat

Wijs een naam toe aan de NAD die u maakt. Voeg het IP-netwerkapparaat toe.



Creatie van netwerkapparaat

Onderaan dezelfde pagina voegt u hetzelfde gedeelde geheim toe dat u in uw netwerkapparaatconfiguratie hebt gebruikt.



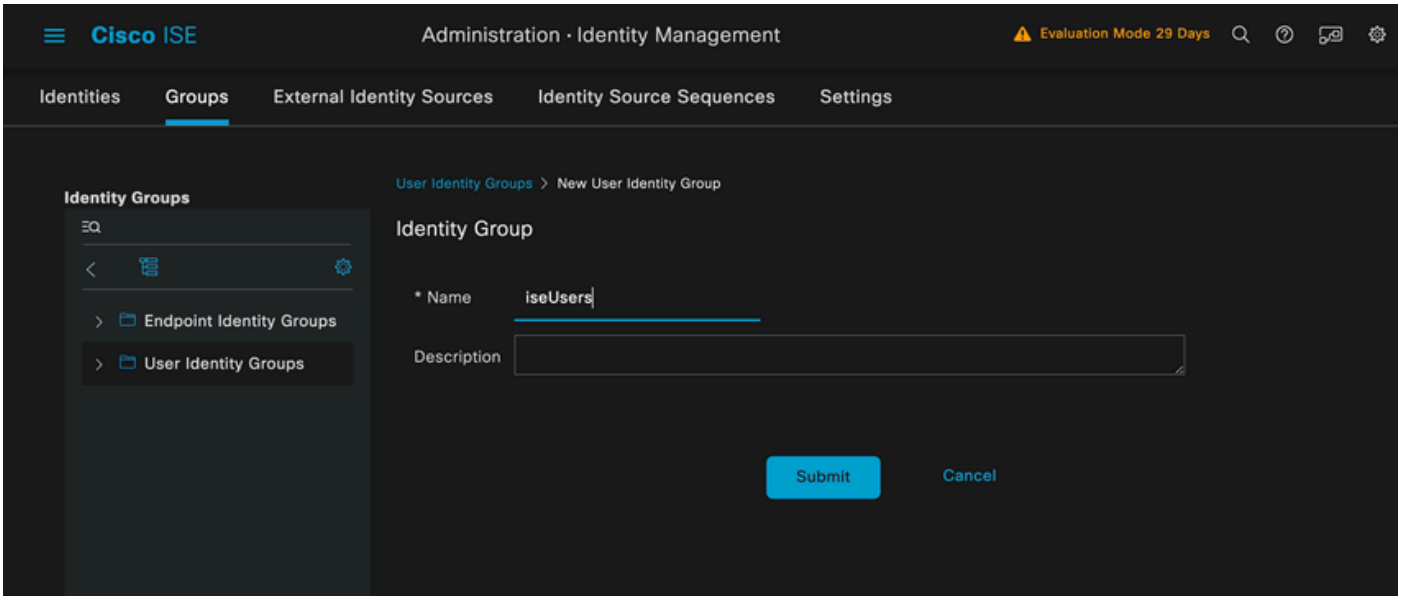
Instellingen straal netwerkapparaat

Sla de wijzigingen op.

Configureer de identiteit die wordt gebruikt voor de verificatie van het eindpunt.

Lokale verificatie met ISE wordt gebruikt. De externe authentificatie van ISE wordt niet verklaard in dit artikel.

Navigeer naar het tabblad Beheer > Identity Management > Groepen en maak de groep aan waar de gebruiker deel van uitmaakt. De identiteitsgroep die voor deze demonstratie werd gecreëerd is iseUser.

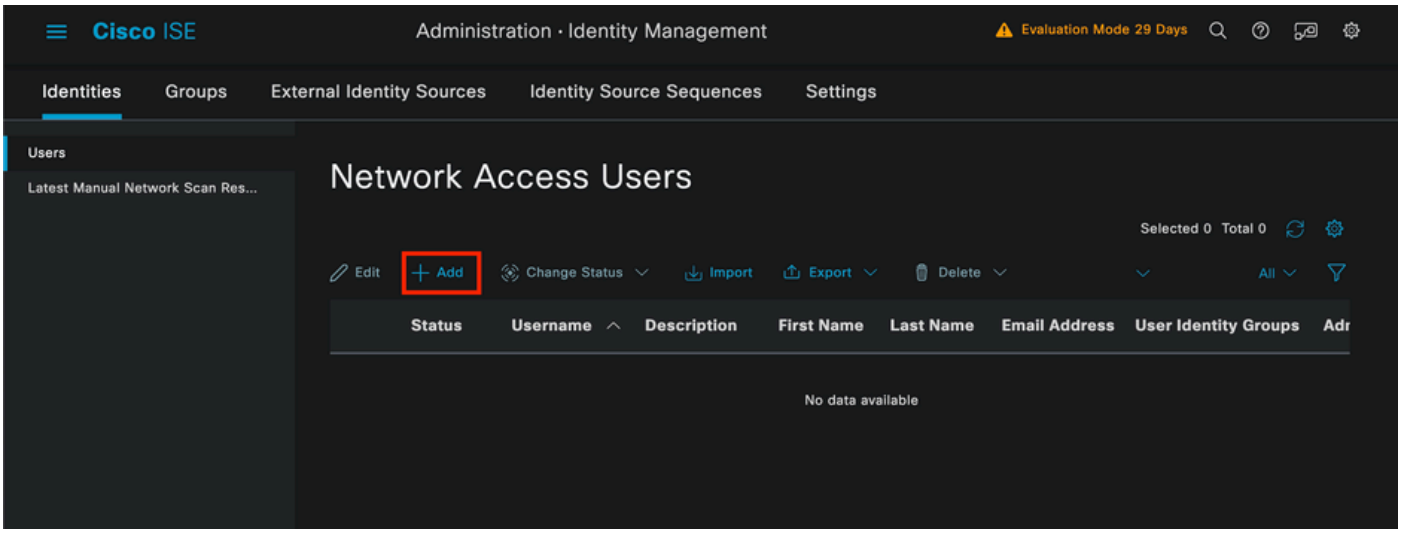


Creatie van identiteitsgroep

Klik op Verzenden.

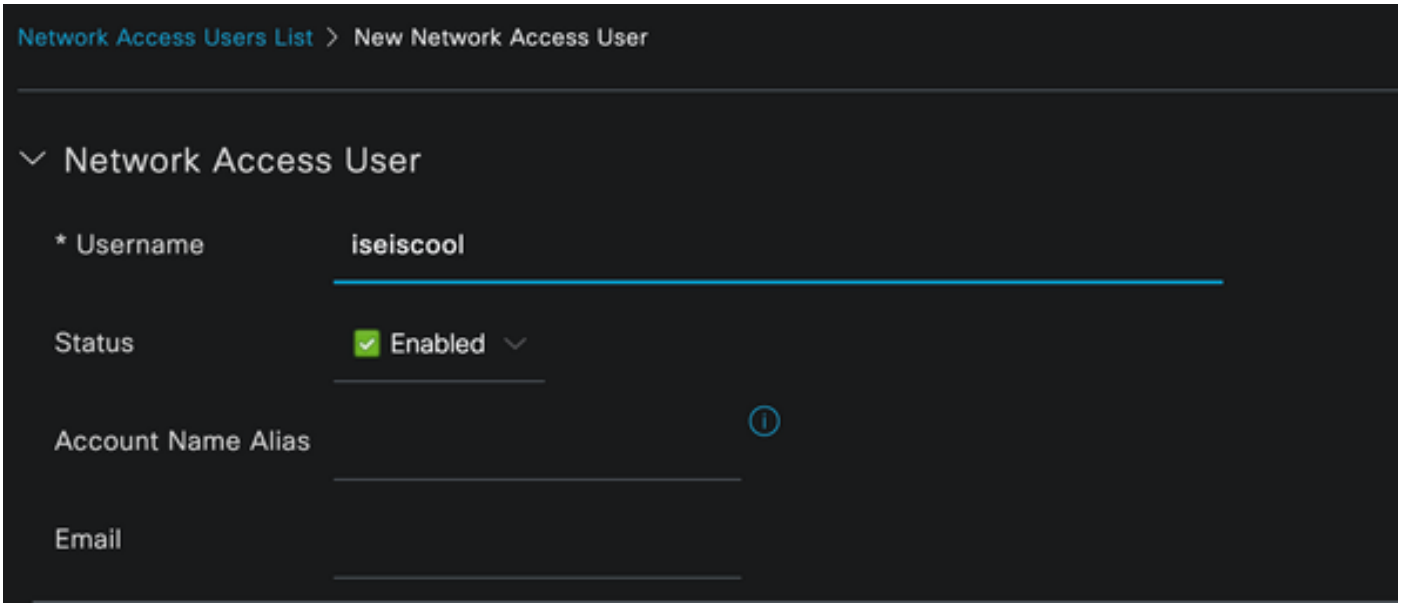
Navigeer naar Beheer > Identity Management > tabblad Identity.

Klik op Add (Toevoegen).



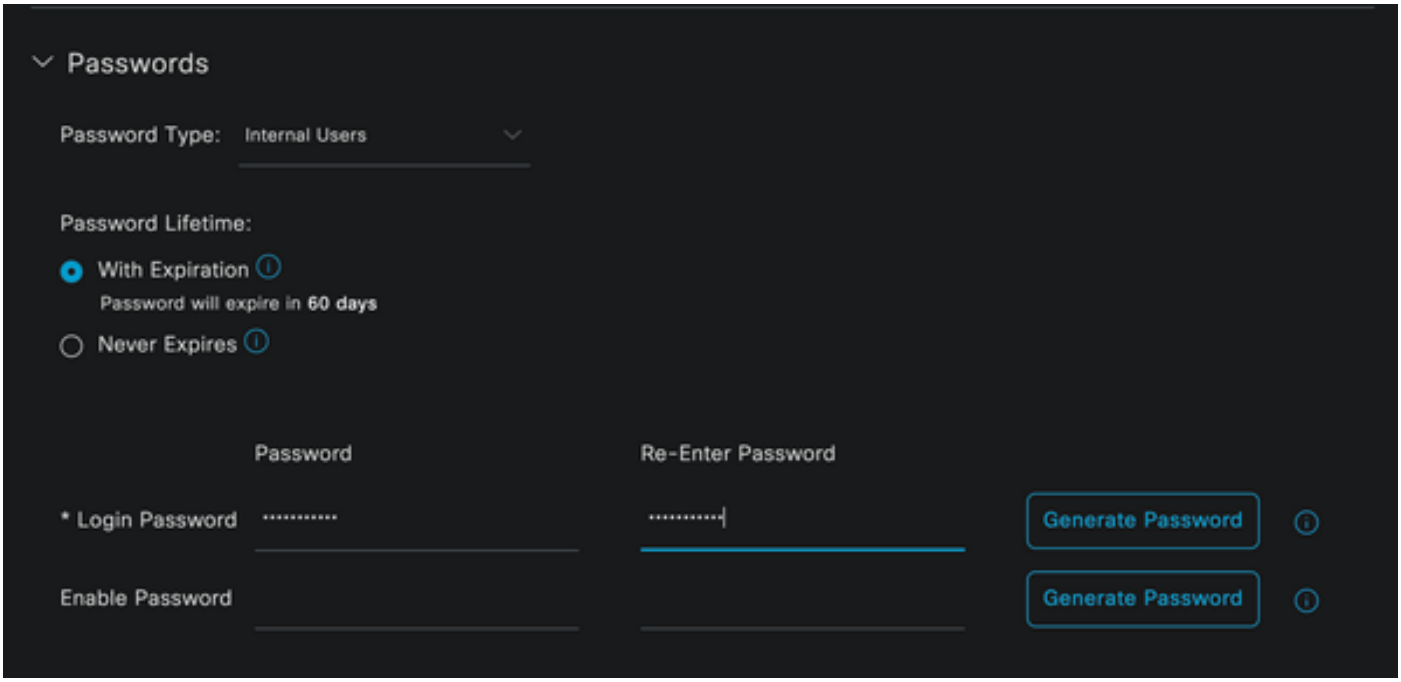
Sectie Netwerktoegangsgebruikers

Als onderdeel van de verplichte velden begint de naam van de gebruiker. De gebruikersnaam isisisecool wordt in dit voorbeeld gebruikt.



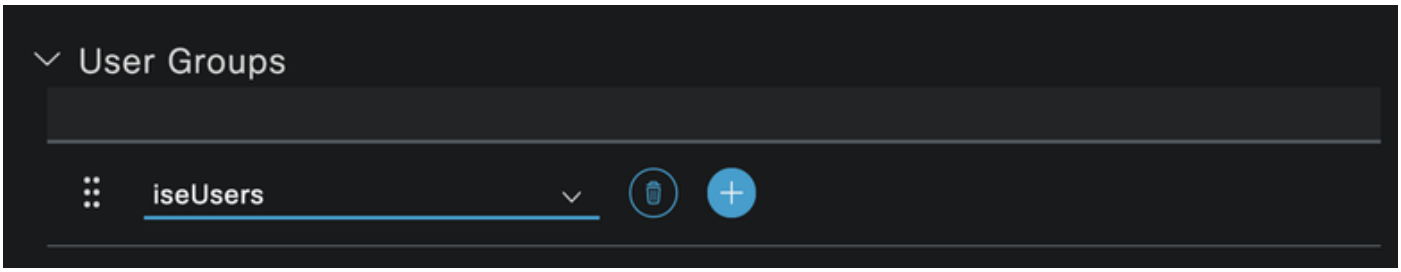
Creatie van gebruiker voor netwerktoegang

Wijs een wachtwoord toe aan de gebruiker. Er wordt een Vainilla ISE97 gebruikt.



Gedeelte Wachtwoord voor maken van gebruiker

Wijs de gebruiker toe aan de groep ISEusers.

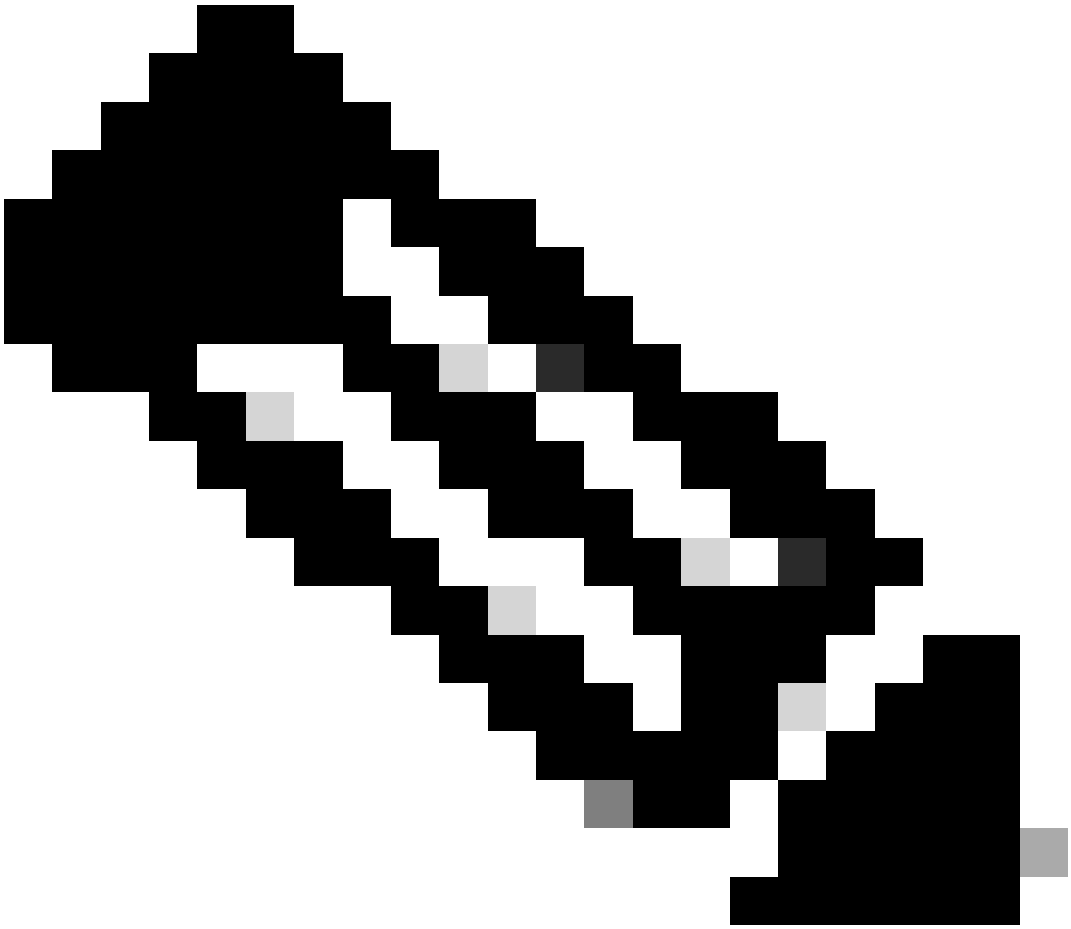


Toewijzing van gebruikersgroep

Configureer de beleidsset.

Navigeer naar het ISE-menu > Beleidssets > Beleidssets.

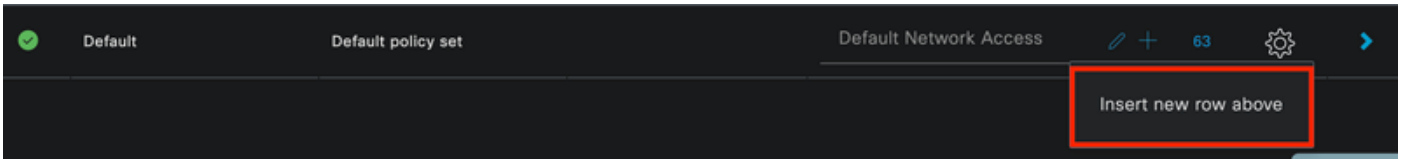
De standaard Beleidsset kan worden gebruikt. Er is echter een met de naam Wired aangemaakt voor dit voorbeeld.



> Opmerking: het classificeren en differentiëren van de beleidssets helpt bij het oplossen van problemen,

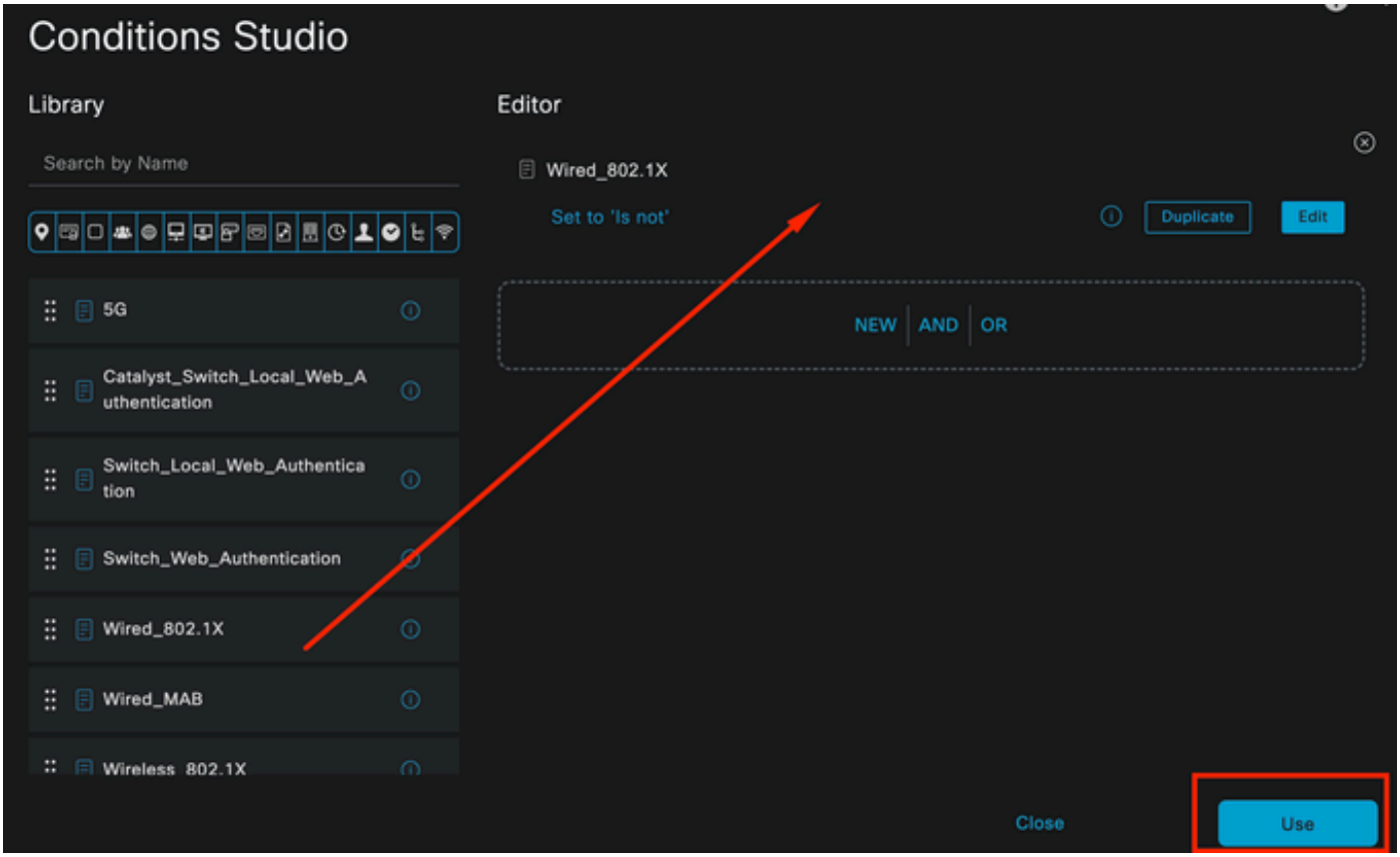
---

Opmerking: Als het pictogram add of plus niet zichtbaar is, kan het versnellingspictogram van elke beleidsset worden geklikt en selecteer vervolgens Nieuwe rij invoegen hierboven.



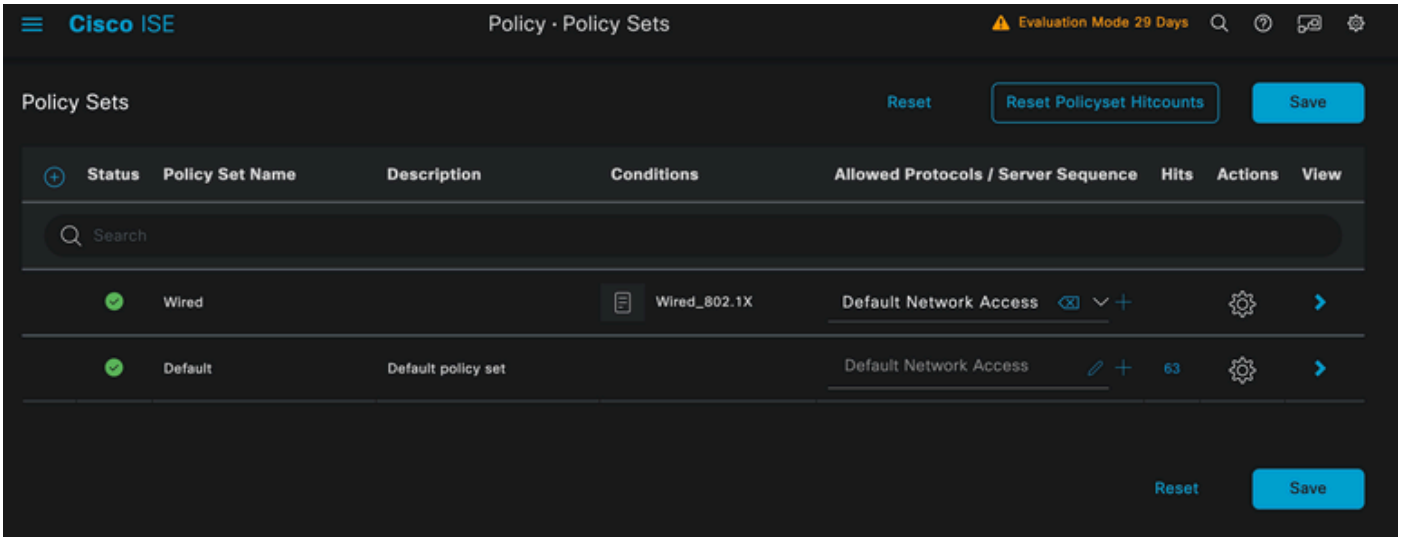
Pictogramopties tandwiel

De gebruikte voorwaarde is Wired 8021x. Sleep het bestand en klik op Gebruik.



Verificatiebeleidsvoorwaarde Studio

Selecteer in het gedeelte Toegestane protocollen de optie Standaard netwerktoegang.

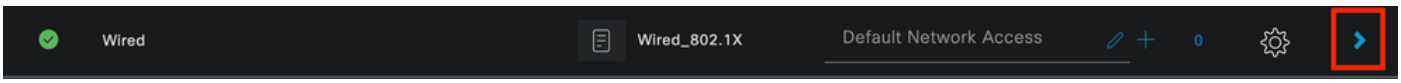


Algemene weergave van beleidssets

Klik op Save (Opslaan).

2. Configureer het verificatie- en autorisatiebeleid.

Klik op het >pictogram.



Bedrade beleidsset

Breid het gedeelte Verificatiebeleid uit.

Klik op het pictogram +.

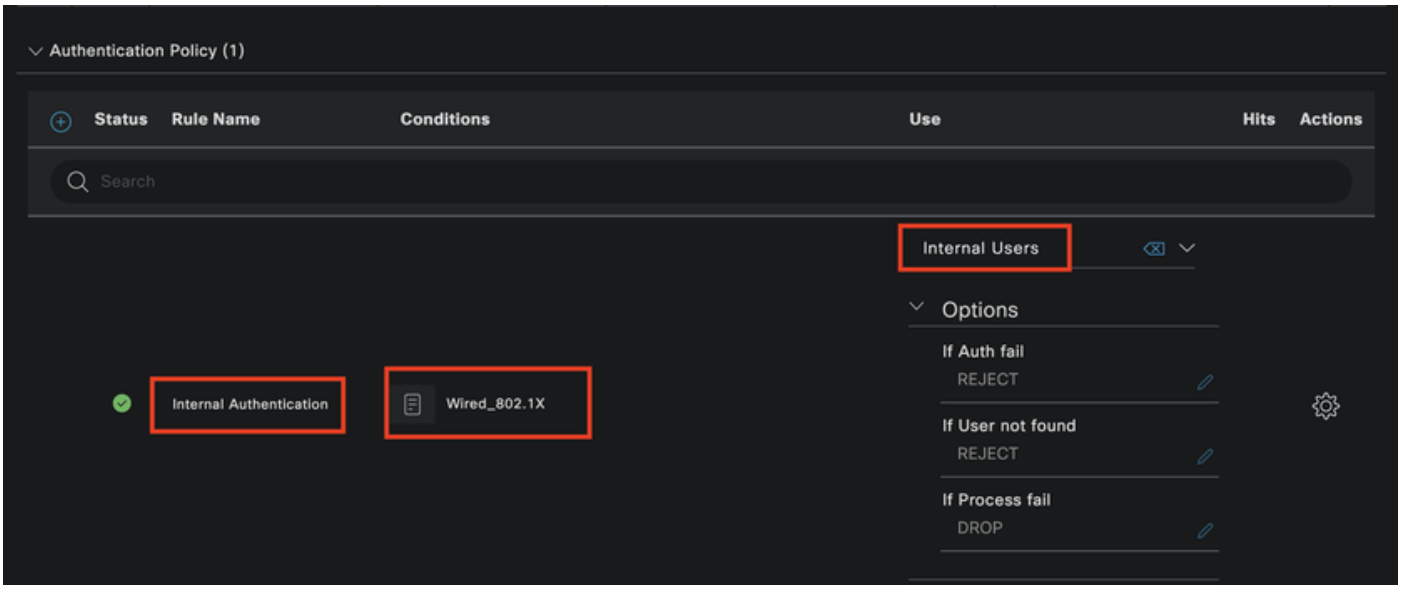
Verificatiebeleid

Wijs een naam toe aan het verificatiebeleid. Interne verificatie wordt in dit voorbeeld gebruikt.

Klik op het +-pictogram in de kolom Voorwaarden voor dit nieuwe verificatiebeleid.

De bekabelde Dot1x-verbinding wordt gebruikt in de vooraf geconfigureerde toestand.

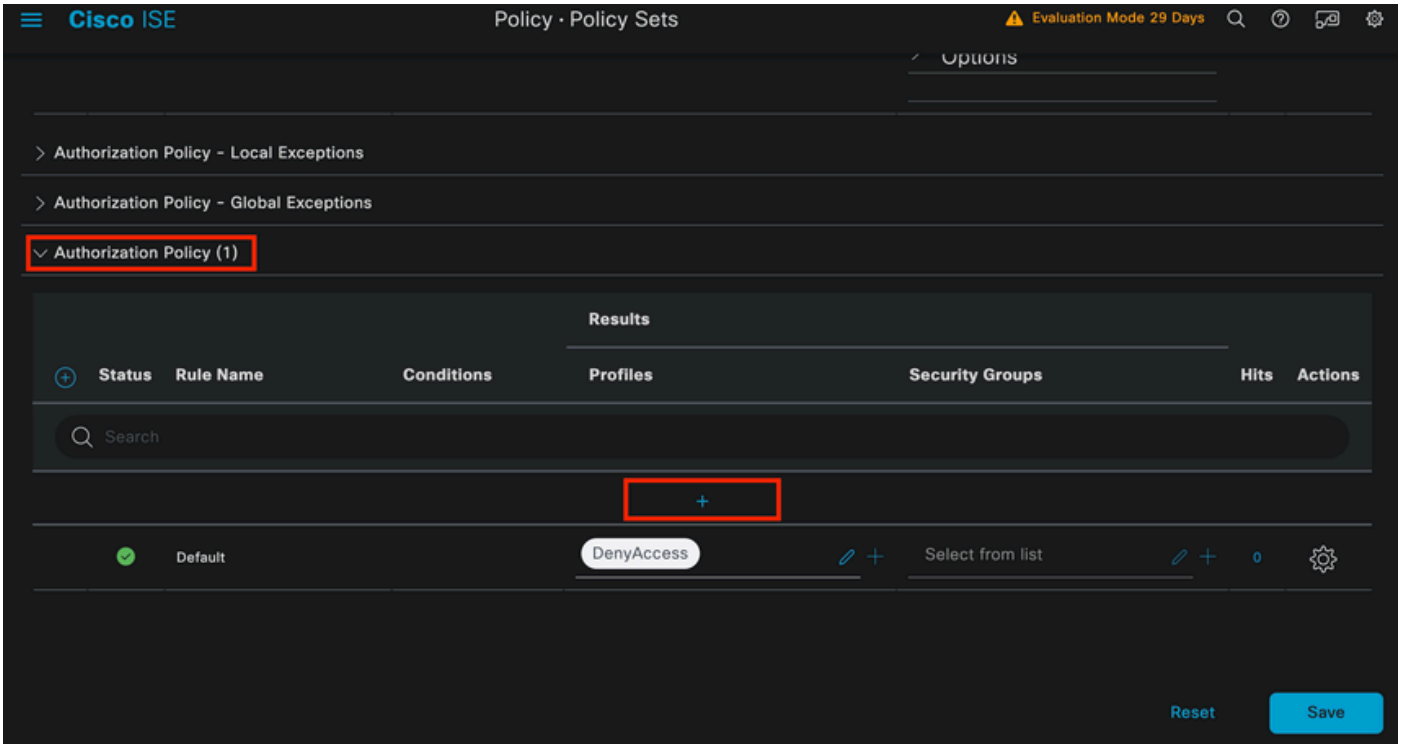
Selecteer in de kolom Gebruik tot slot de optie Interne gebruikers.



Verificatiebeleid

Vergunningsbeleid.

De sectie Autorisatiebeleid staat onderaan de pagina. Breid het uit en klik op het + pictogram.



Vergunningsbeleid

Geef het recent gemaakte autorisatiebeleid een naam. In dit configuratievoorbeeld wordt de naam Interne ISE-gebruikers gebruikt.

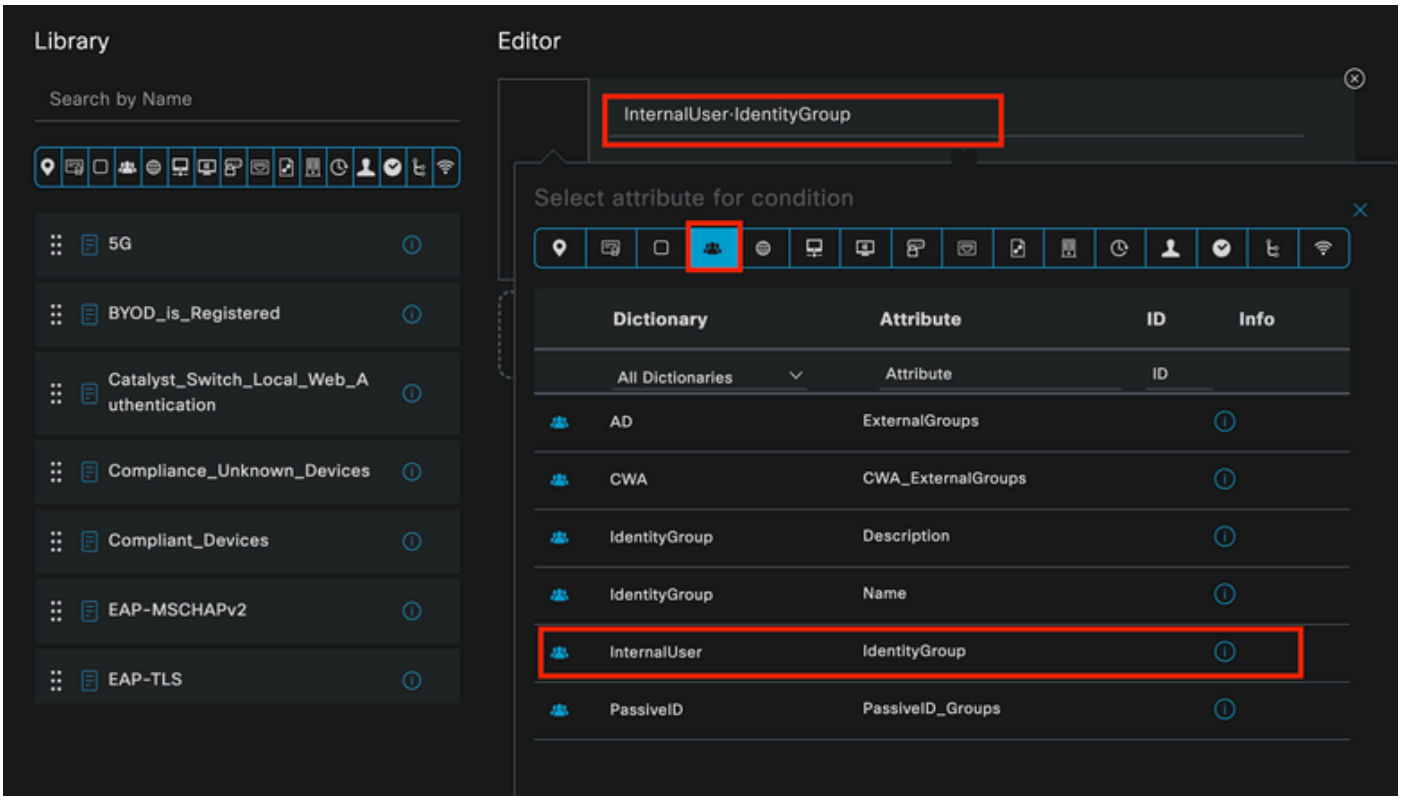
Als u een voorwaarde voor dit autorisatiebeleid wilt maken, klikt u op het +-pictogram in de kolom Voorwaarden.

De groep IseGebruikers wordt gebruikt.

Klik op de sectie Kenmerken.

Selecteer het pictogram IdentityGroup.

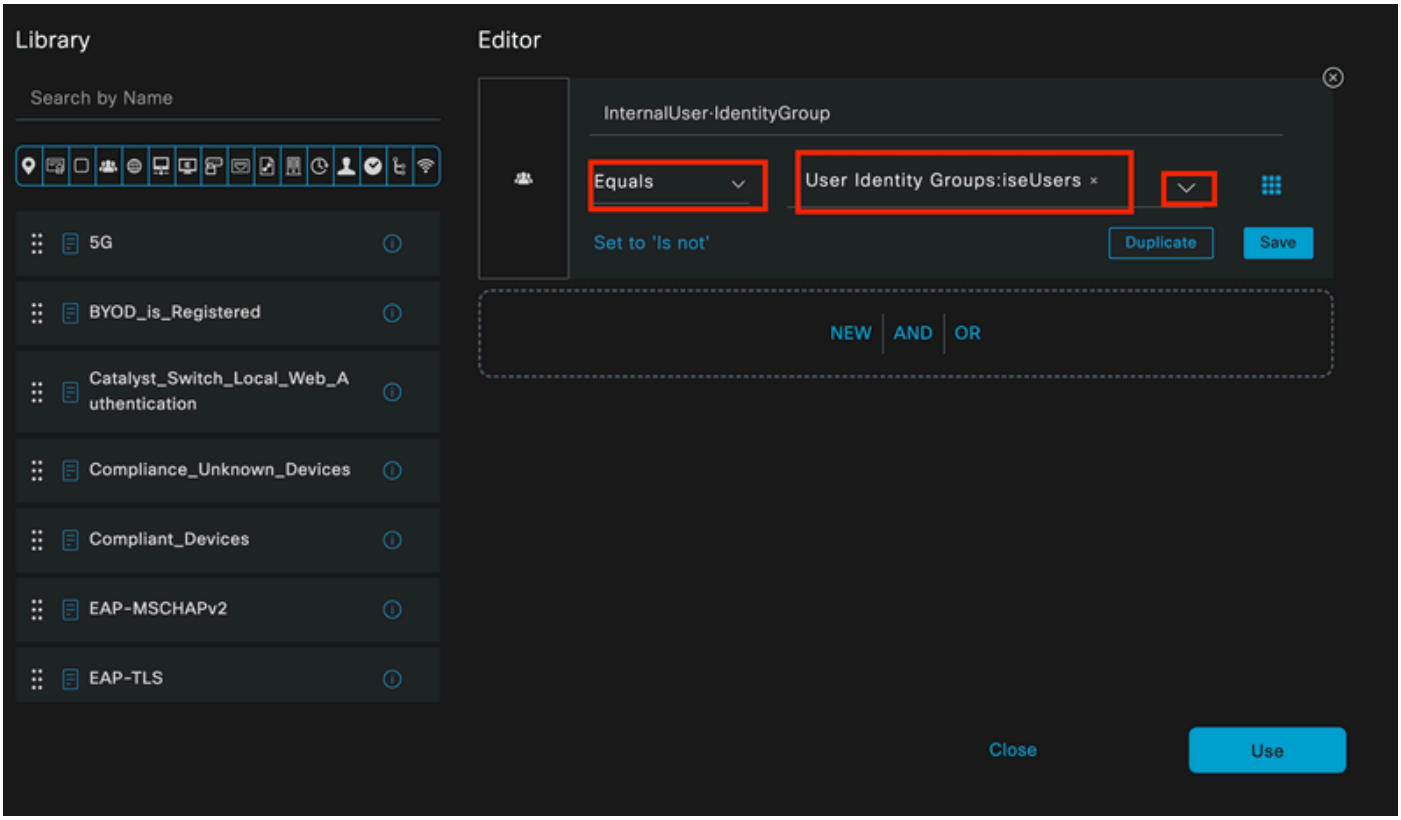
Selecteer in het woordenboek het interne gebruikerswoordenboek dat bij het kenmerk IdentityGroup wordt geleverd.



Conditie maken

Selecteer de operator Gelijk.

Selecteer vanuit Gebruikersidentiteitsgroepen de groep IseGebruikers.

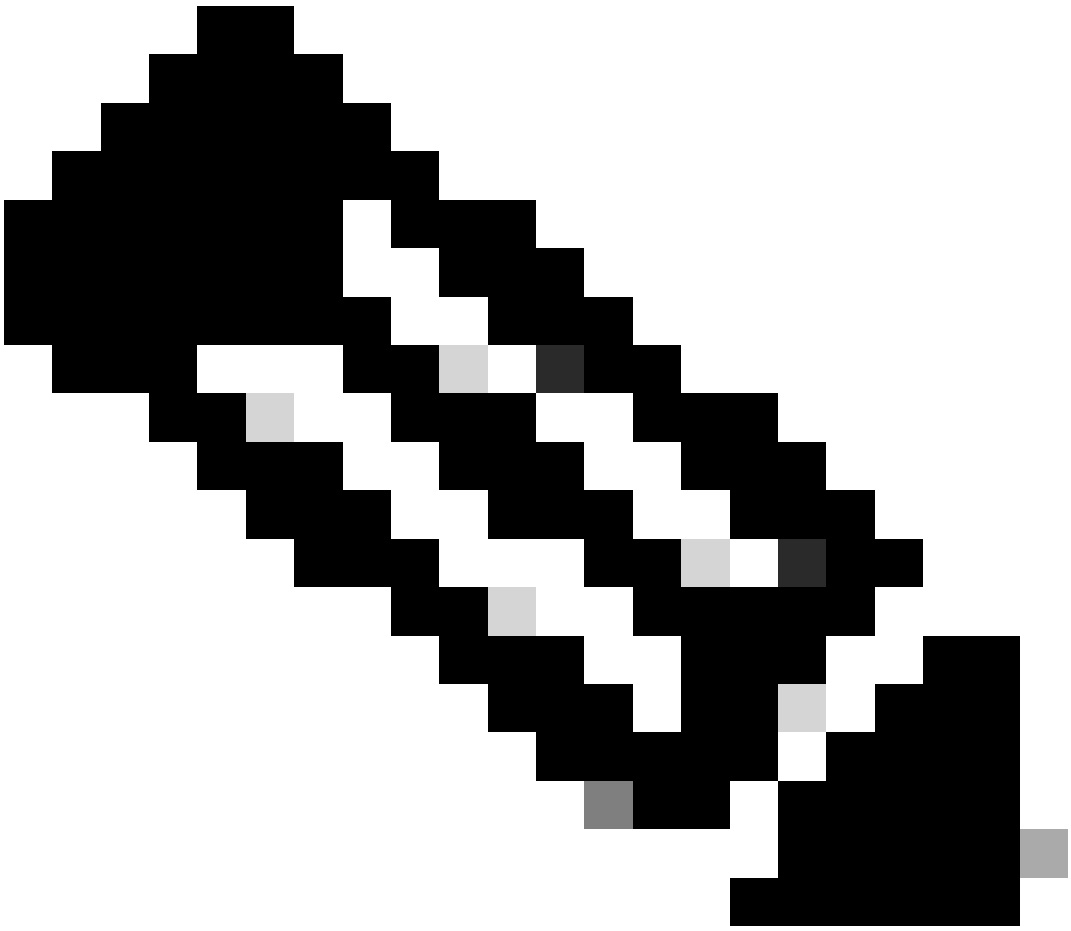


Conditie maken

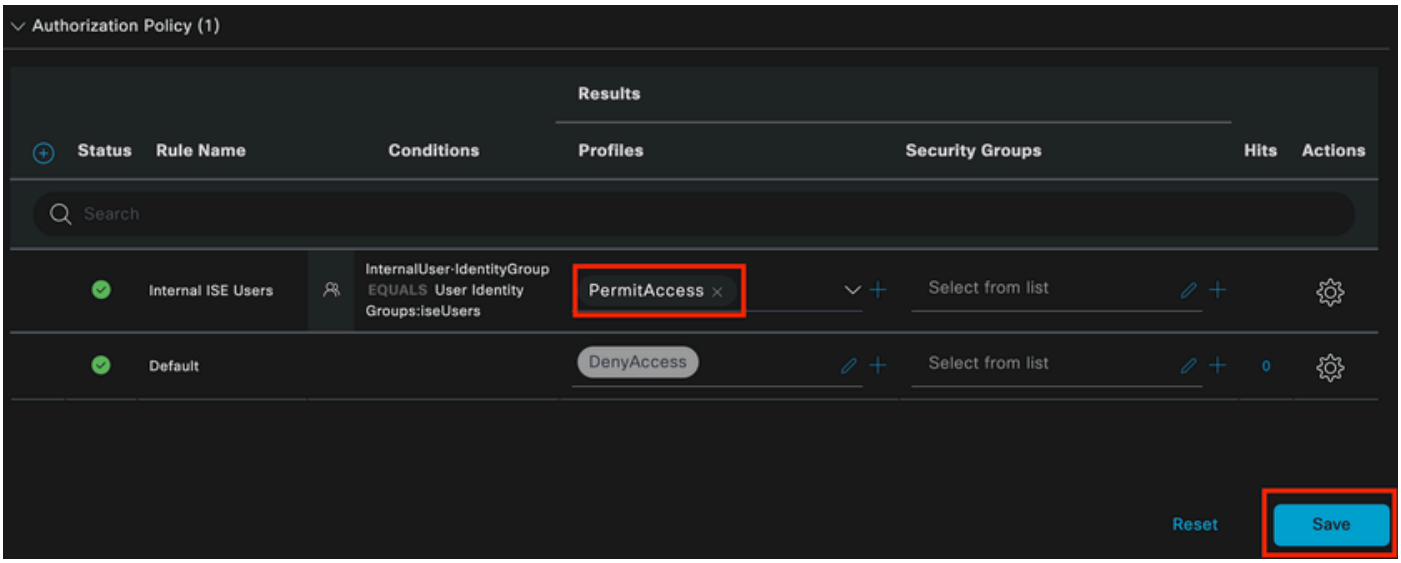
Klik op Gebruik.

Voeg het resultaat autorisatieprofiel toe.

Er wordt gebruikgemaakt van het vooraf ingestelde profiel Permit Access.



Opmerking: Merk op dat de authenticaties die naar ISE komen op deze Wired Dot1x Policy-set die geen deel uitmaken van de User Identity Group ISEU-gebruikers, het standaard autorisatiebeleid raken, wat het resultaat DenyAccess heeft.



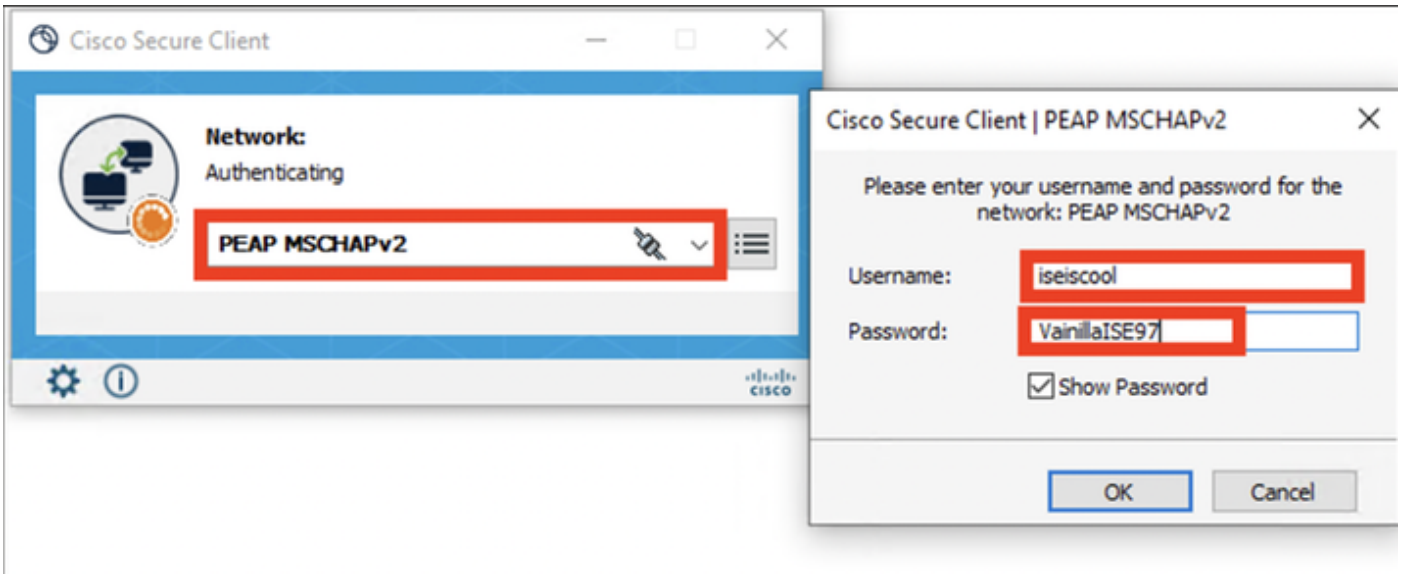
Vergunningsbeleid

Klik op Save (Opslaan).

Verifiëren

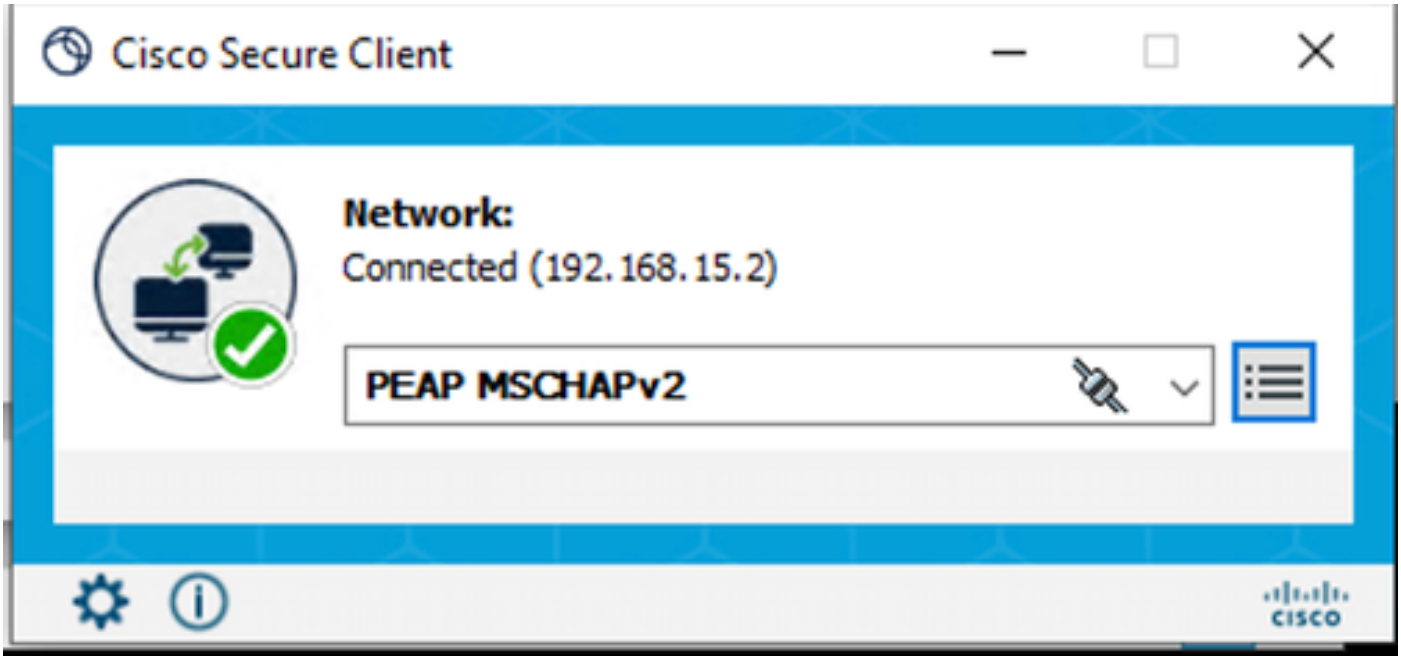
Nadat de configuratie is voltooid, wordt Secure Client gevraagd om de referenties en wordt het gebruik van het PEAP MSCHAPv2-profiel gespecificeerd.

De eerder gemaakte referenties worden ingevoerd.



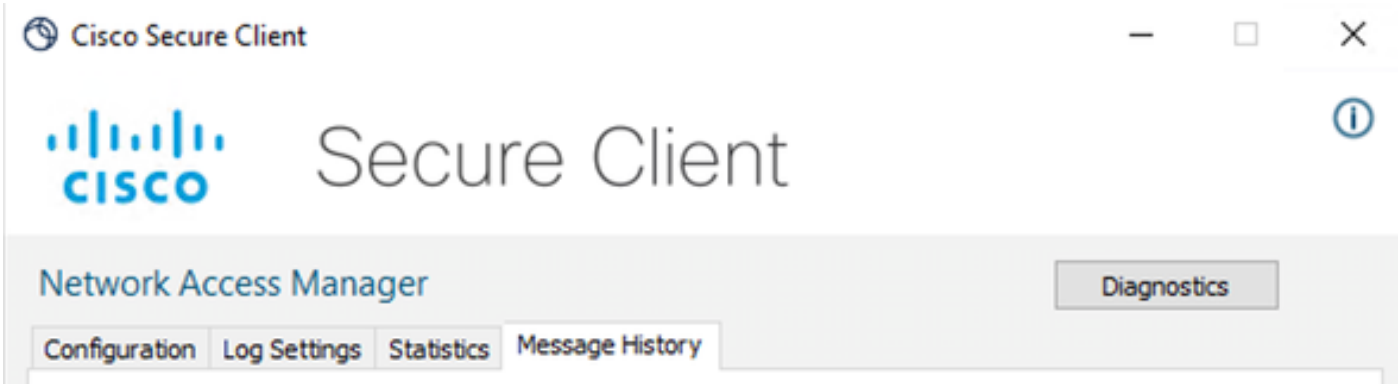
Secure-clientnaam

Als het eindpunt op de juiste manier wordt geverifieerd,. NAM toont dat het verbonden is.

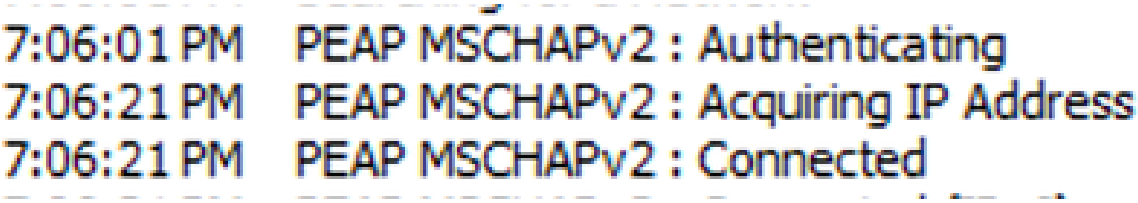


Secure-clientnaam

Door op het informatiepictogram te klikken en naar de sectie Berichtgeschiedenis te navigeren, worden de details van elke stap die de NAM heeft uitgevoerd weergegeven.



Historie voor beveiligde clientberichten



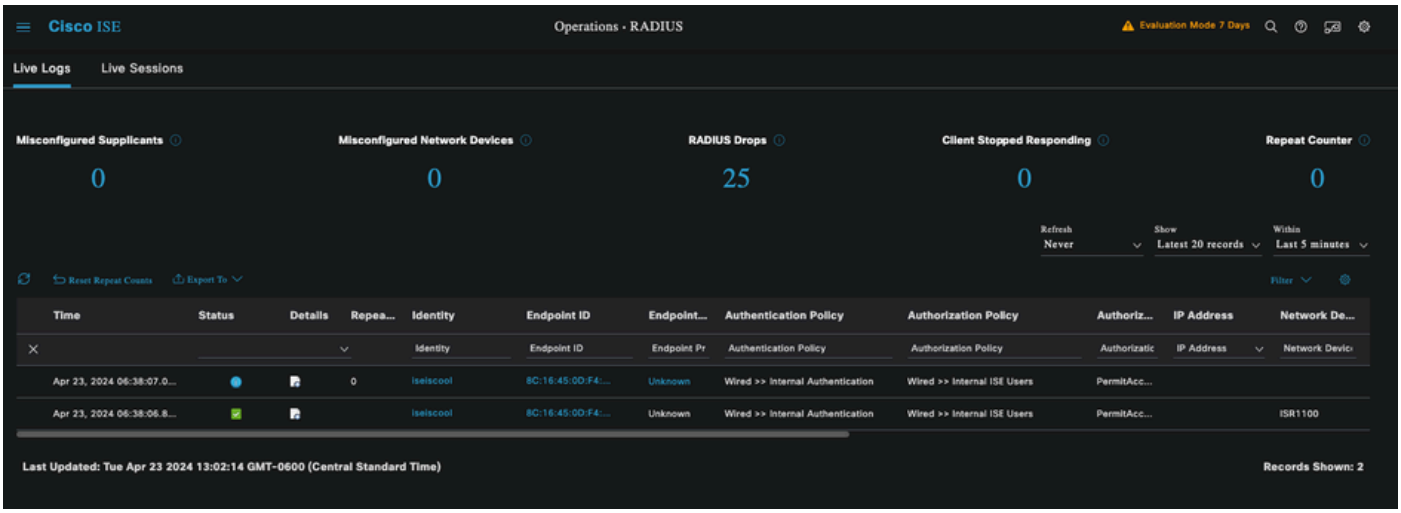
Historie voor beveiligde clientberichten

Ga van ISE naar Operations > Radius LiveLogs om de details van de verificatie te zien. Zoals in de volgende afbeelding wordt de gebruikersnaam weergegeven die is gebruikt.

Ook andere details, zoals:

- Tijdsindicatie.
- MAC-adres.
- Gebruikte beleidsset.
- Verificatiebeleid.

- Vergunningsbeleid.
- Andere relevante informatie.



ISE RADIUS live logs

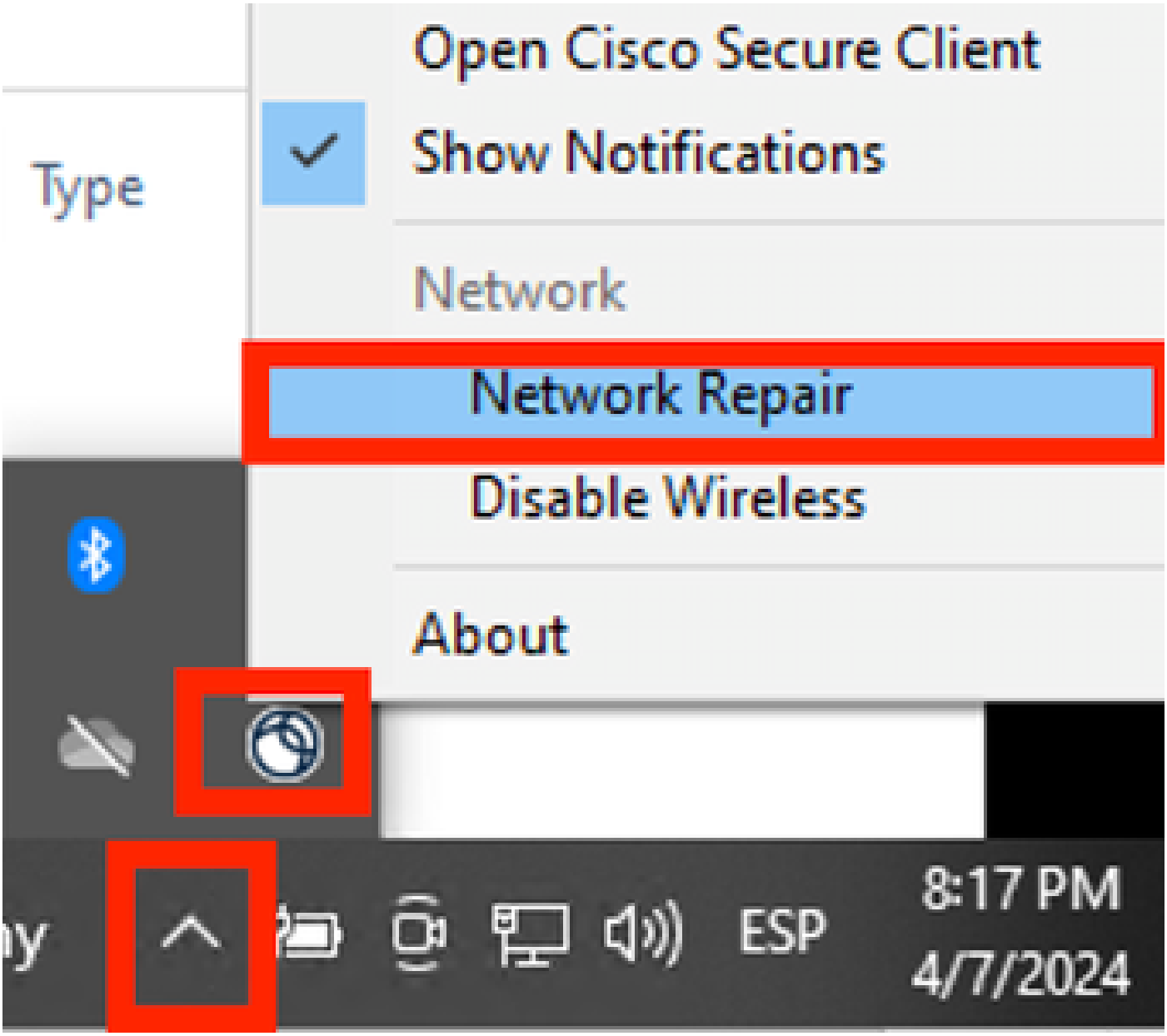
Aangezien u kunt zien dat het de juiste beleidsregels raakt en het resultaat een succesvolle verificatiestatus is, wordt geconcludeerd dat de configuratie correct is.

Problemen oplossen

Probleem: het NAM-profiel wordt niet gebruikt door Secure Client.

Als het nieuwe profiel dat is gemaakt in de profieleditor niet wordt gebruikt door NAM, gebruikt u de optie Network Repair voor Secure Client.

U kunt deze optie vinden door naar de Windows-balk te navigeren > Klik op het pictogram circumflex > Klik met de rechtermuisknop op het pictogram Secure Client > Klik op Network Repair.



Sectie Netwerkreparatie

Probleem 2: Logbestanden moeten worden verzameld voor verdere analyse.

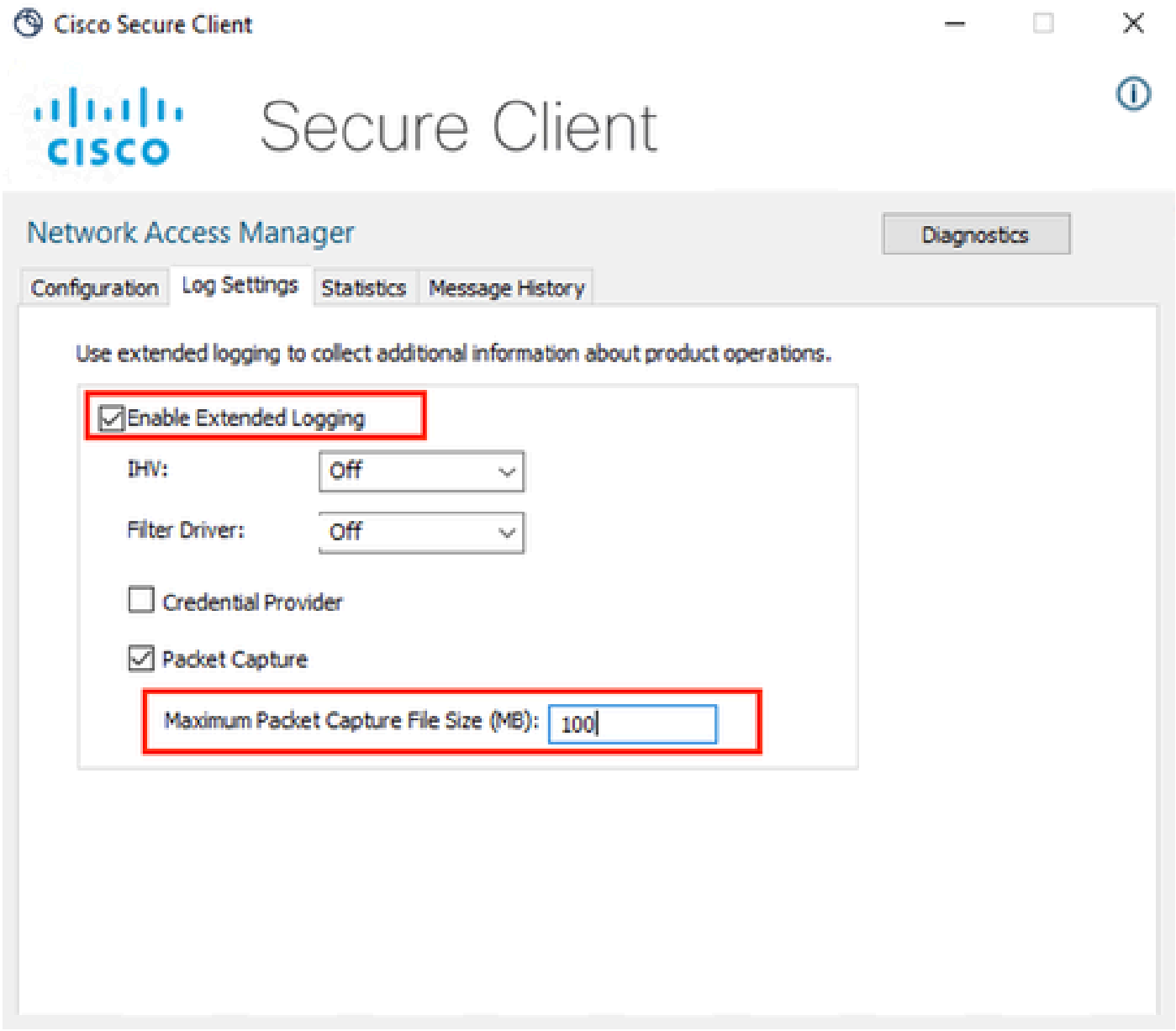
1. Uitgebreide NAM-vastlegging inschakelen

Open NAM en klik op het tandwielpictogram.

NAM Interface

Navigeer naar het tabblad Loginstellingen. Schakel het selectievakje Uitgebreid vastlegging inschakelen in.

Stel de grootte van het pakketopnamebestand in op 100 MB.



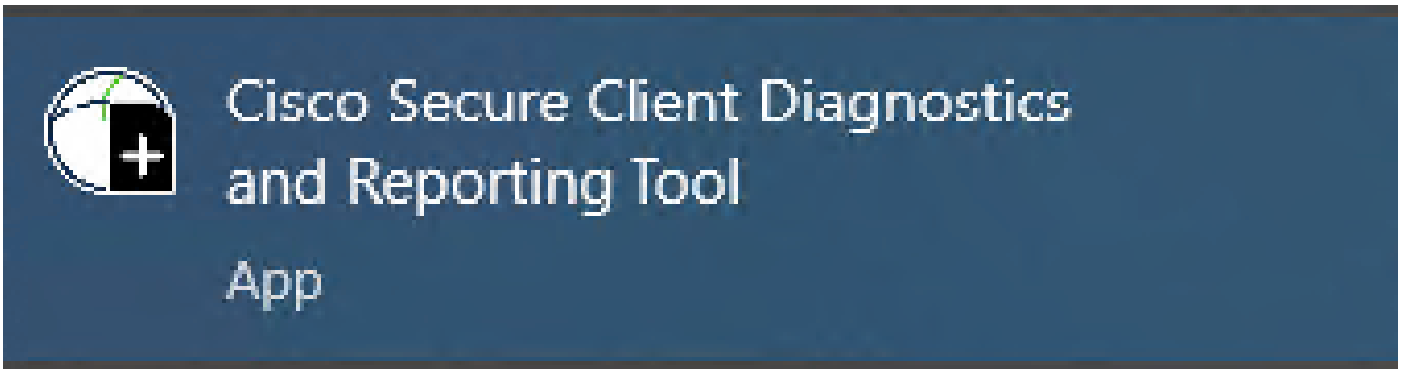
Instellingen voor beveiligde client-NAM-logbestanden

2. Neem het probleem over.

Als uitgebreide vastlegging is ingeschakeld, reproduceert u het probleem meerdere malen om er zeker van te zijn dat de logbestanden worden gegenereerd en het verkeer wordt opgenomen.

3. Verzamel de beveiligde bundel van het clientpijltje.

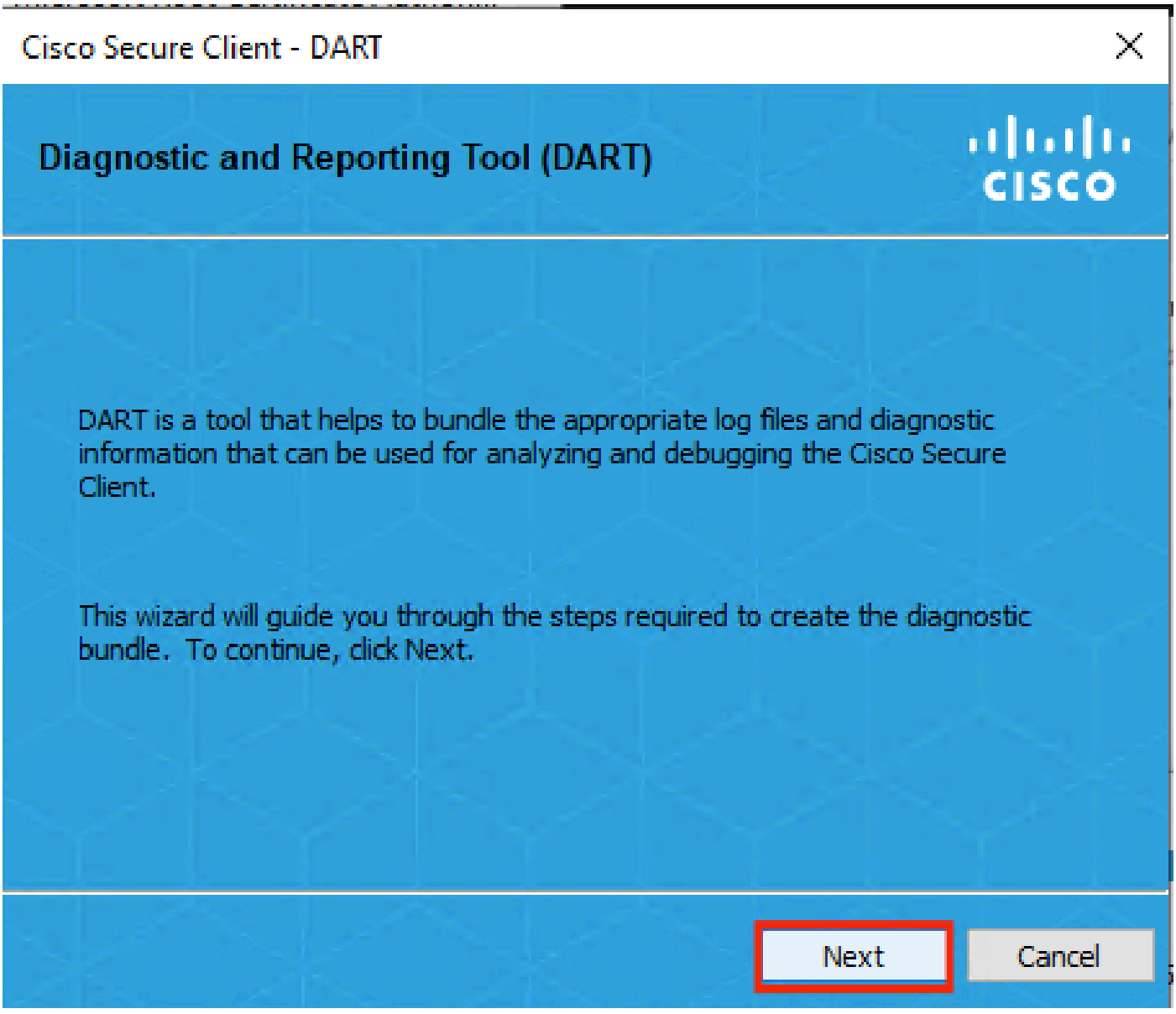
Navigeer vanuit Windows naar de zoekbalk en typ Cisco Secure Client Diagnostics and Reporting Tool.



DART-module

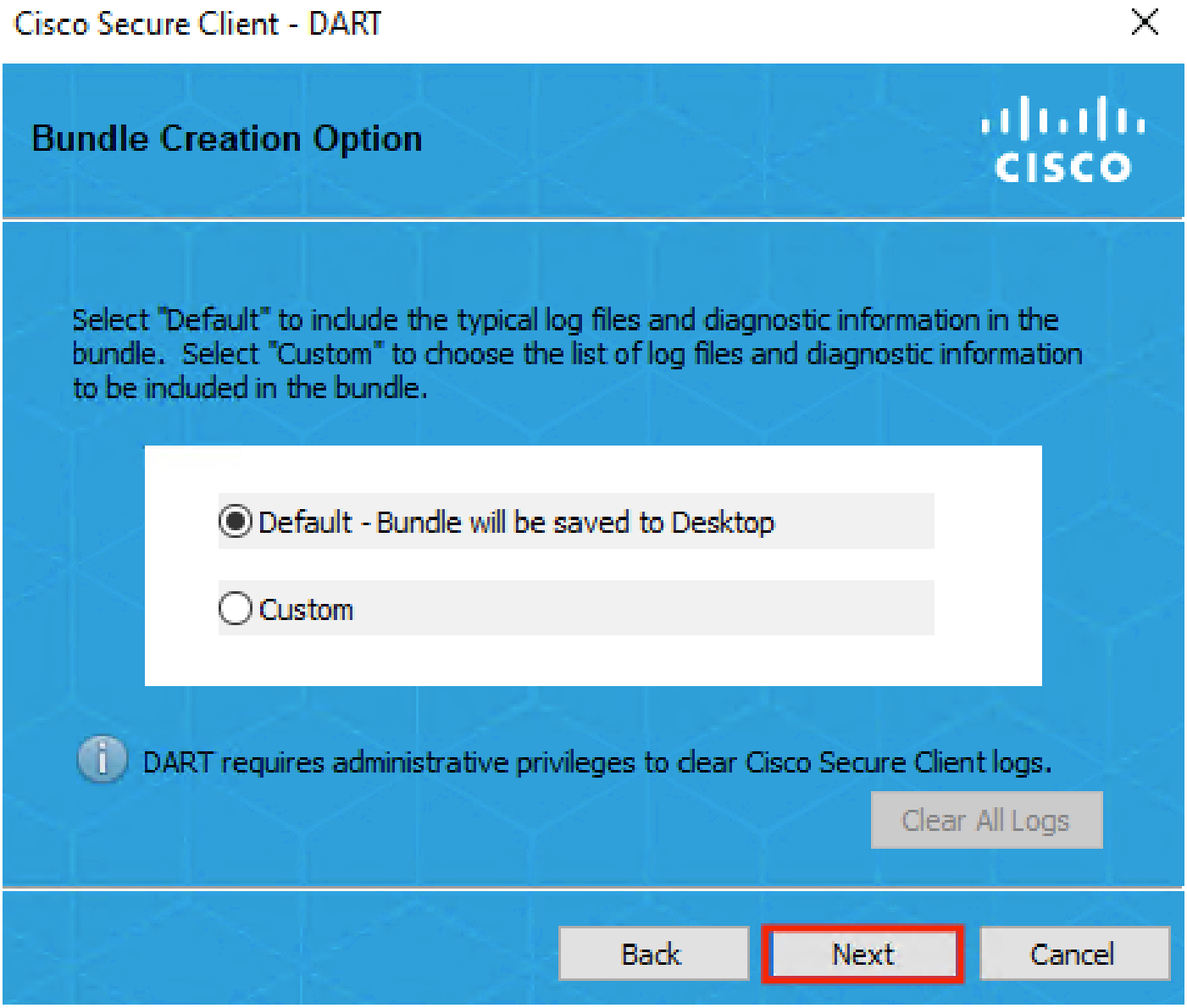
Tijdens het installatieproces, installeerde u ook deze module. Het is een hulpmiddel dat tijdens het probleemoplossingsproces helpt door logboeken en relevante dot1x-sessieinformatie te verzamelen.

Klik op Volgende in het eerste venster.



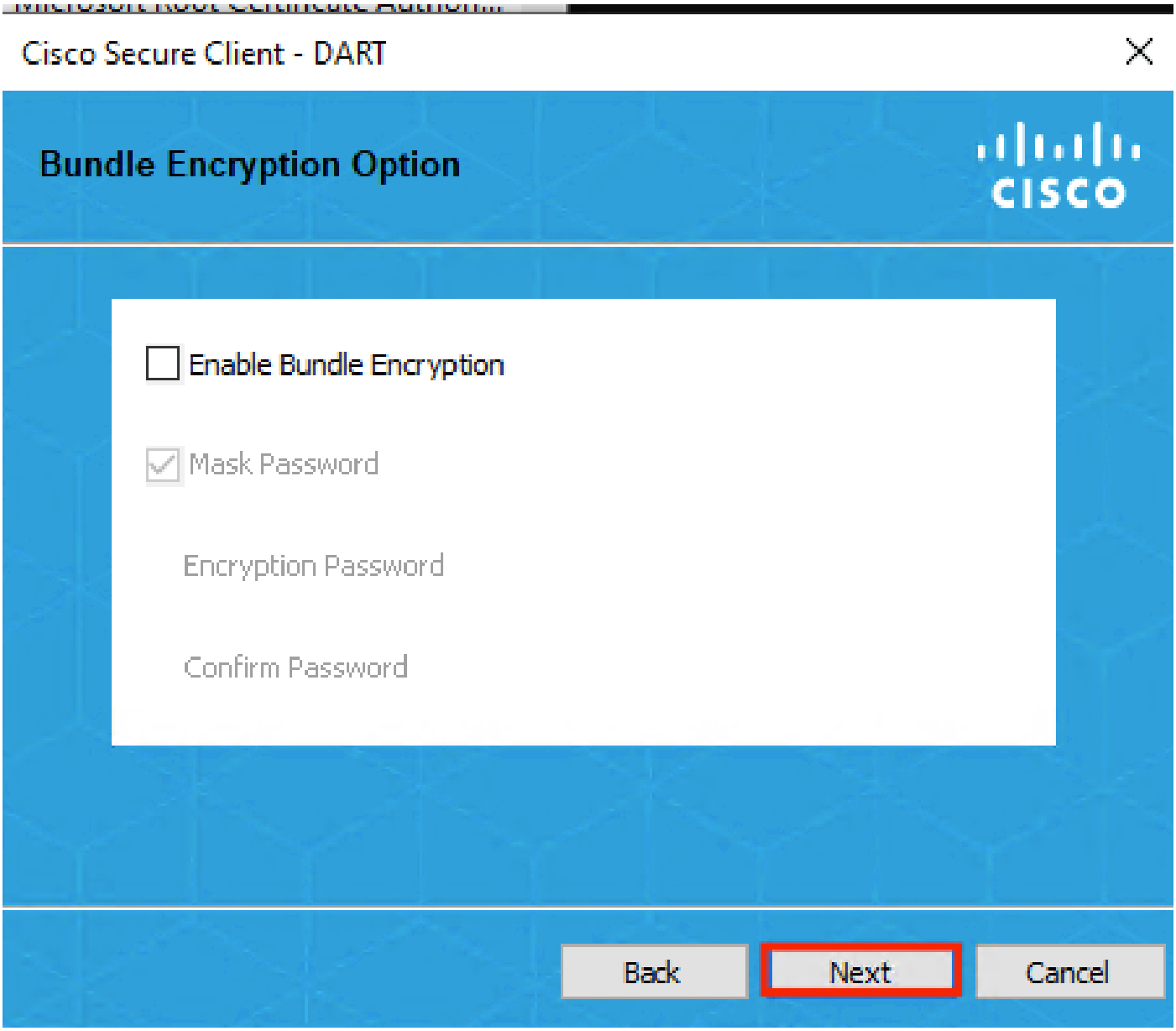
DART-module

Klik nogmaals op Volgende, zodat de logbundel kan worden opgeslagen op het bureaublad.



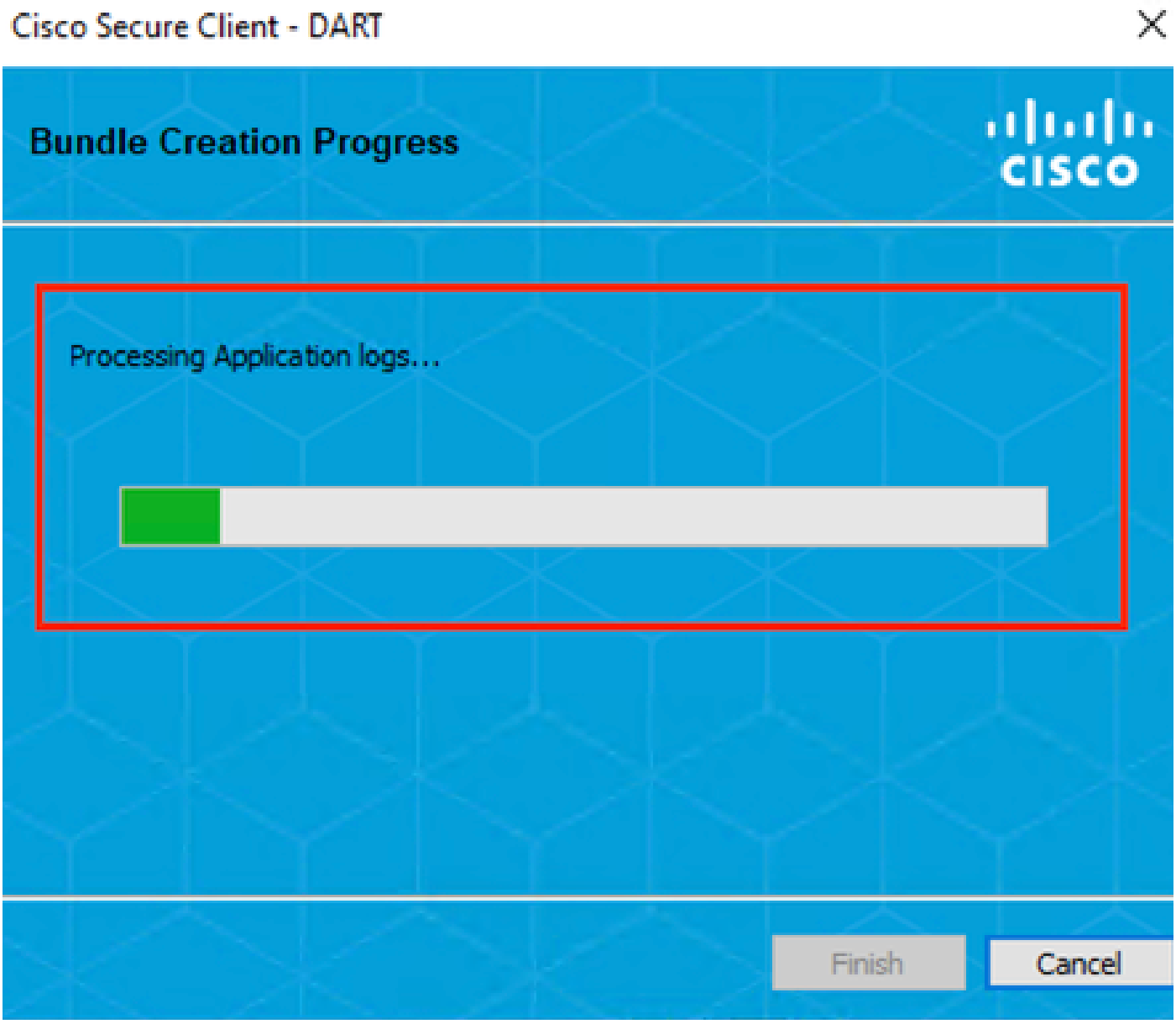
DART-module

Indien nodig vinkt u het aanvinkvakje Bundle-encryptie inschakelen aan.



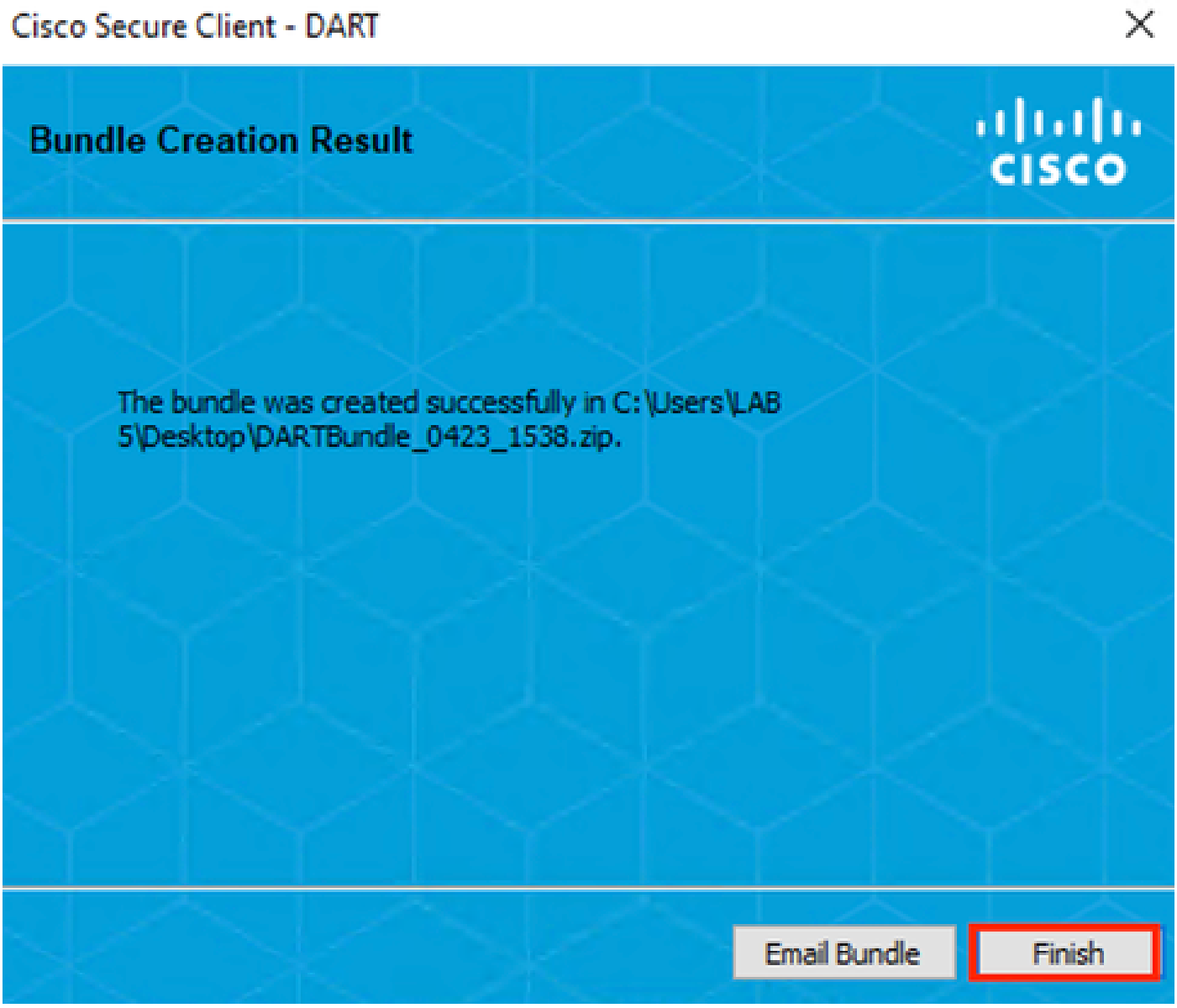
DART-module

DART-logboekverzameling start.



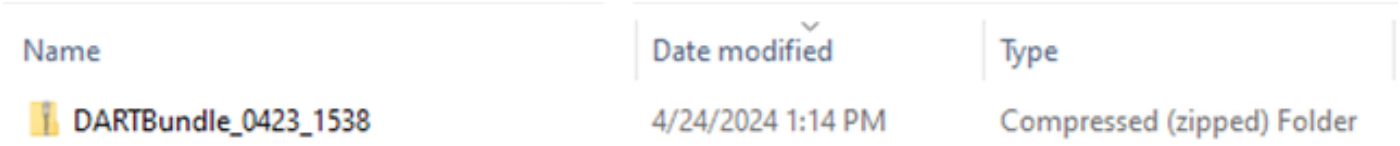
DART-logverzameling

Het kan 10 minuten of langer duren totdat het proces is voltooid.



Resultaat van maken DART-bundel

Het DART-resultaatbestand vindt u in de desktopmap.



DART-resultaatbestand

Gerelateerde informatie

- Cisco Technical Support en downloads

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.