

# Secure Client NAM voor Dot1x configureren met Windows en ISE 3.2

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

- [1. Secure Client NAM \(Network Access Manager\) downloaden en installeren](#)
- [2. Download en installeer de Secure Client NAM Profile Editor.](#)
- [3. Algemene standaardconfiguraties](#)
- [4. Scenario 1: Secure Client NAM Supplicant voor PEAP \(MS-CHAPv2\)-gebruikersverificatie configureren](#)
- [5. Scenario 2: Secure Client NAM Supplicant voor EAP-FAST simultane gebruikers- en machineverificatie configureren](#)
- [6. Scenario 3: Secure Client NAM Supplicant voor EAP TLS-gebruikerscertificaatverificatie configureren](#)
- [7. Configureer ISR 1100 en ISE om verificaties toe te staan op basis van scenario 1 PEAP MSCHAPv2](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Probleem: het NAM-profiel wordt niet gebruikt door Secure Client.](#)

[Probleem 2: Logbestanden moeten worden verzameld voor verdere analyse.](#)

- [1. Uitgebreide NAM-vastlegging inschakelen](#)
- [2. Neem het probleem over.](#)
- [3. Verzamel de beveiligde bundel van het clientpijlje.](#)

[Gerelateerde informatie](#)

---

## 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 profieeditor 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 verifactor 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 verifactor 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.

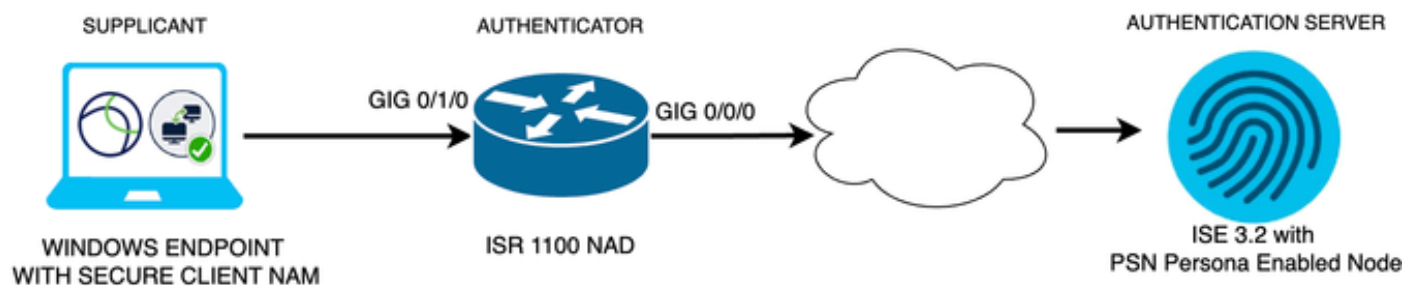
De Network Access Manager is ontworpen voor enkelvoudig calibreren, zodat u slechts één netwerkverbinding tegelijk kunt maken. Ook bekabelde verbindingen hebben een hogere prioriteit dan draadloze verbindingen, dus als u wordt aangesloten op het netwerk met een bekabelde verbinding, wordt de draadloze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

# Configureren

## Netwerkdigram

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.



Netwerkdigram

## Configuraties

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

---

Cisco Secure Client Pre-Deployment Package (Windows) - includes individual MSI files	06-Feb-2024	108.30 MB	
<a href="#">cisco-secure-client-win-5.1.2.42-predeploy-k9.zip</a>			
<a href="#">Advisories</a>			

---

Msi-zipbestand

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

Profiles	4/4/2024 7:16 PM
Setup	4/4/2024 7:16 PM
cisco-secure-client-win-1.182.3-thousandeyes-predeploy-k9	4/4/2024 7:16 PM
cisco-secure-client-win-5.1.2.42-core-vpn-predeploy-k9	4/4/2024 7:16 PM
cisco-secure-client-win-5.1.2.42-dart-predeploy-k9	4/4/2024 7:16 PM
cisco-secure-client-win-5.1.2.42-iseposture-predeploy-k9	4/4/2024 7:16 PM
cisco-secure-client-win-5.1.2.42-nam-predeploy-k9	4/4/2024 7:16 PM
cisco-secure-client-win-5.1.2.42-nvm-predeploy-k9	4/4/2024 7:16 PM
cisco-secure-client-win-5.1.2.42-posture-predeploy-k9	4/4/2024 7:16 PM
cisco-secure-client-win-5.1.2.42-sbl-predeploy-k9	4/4/2024 7:16 PM
cisco-secure-client-win-5.1.2.42-umbrella-predeploy-k9	4/4/2024 7:16 PM
cisco-secure-client-win-5.1.2.5191-zta-predeploy-k9	4/4/2024 7:16 PM
<b>Setup</b>	4/4/2024 7:16 PM
setup	4/4/2024 7:16 PM

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.

---

Select the Cisco Secure Client 5.1.2.42 modules you wish to install:

- Core & AnyConnect VPN
- Start Before Login
- Network Access Manager
- Secure Firewall Posture
- Network Visibility Module
- Umbrella
- ISE Posture
- ThousandEyes
- Zero Trust Access
- Select All
- Diagnostic And Reporting Tool
- Lock Down Component Services

Install Selected

Installatieselector

Klik op Install Selected (Selectie installeren).

Accepteer de EULA.

**Supplemental End User License Agreement**

**IMPORTANT: READ CAREFULLY**

By clicking accept or using the Cisco Technology, you agree that such use is governed by the Cisco End User License Agreement and the applicable Product Specific Terms (collectively, the "EULA"). You also acknowledge and agree that you have read the Cisco Privacy Statement.

If you do not have authority to bind your company and its affiliates, or if you do not agree with the terms of the EULA, do not click 'accept' and do not use the Cisco Technology. If you are a Cisco channel partner accepting on behalf of an end customer ("customer"), you must inform the customer that the EULA applies to customer's use of the Cisco Technology and provide the customer with access to all relevant terms.

The latest version of documents can be found at the following locations.

- Cisco End User License Agreement: [https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end\\_user\\_license\\_agreement.html](https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html)
- Applicable Product Specific Terms: <https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>
- Cisco Privacy Statement: <https://www.cisco.com/c/en/us/about/legal/privacy-full.html>

EULA-venster

Na de NAM-installatie moet opnieuw worden gestart.

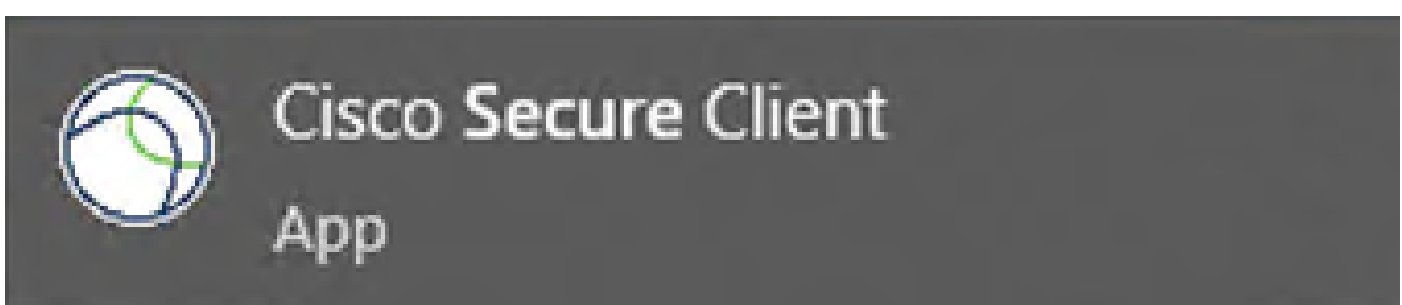
## Cisco Secure Client Install Selector

**You must reboot your system for the installed changes to take effect.**

OK

Reboot Requirement Window

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

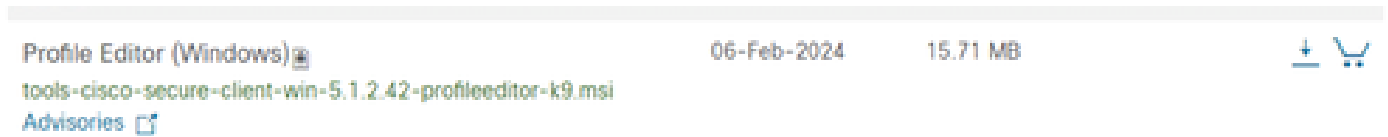


2. Download en installeer de Secure Client NAM Profile Editor.

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

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

Dit voorbeeld gebruikt de optie met versie 5.1.2.42.



Profieeditor

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

Start het MSI-bestand.



Venster Profieeditor instellen






Gebruik de optie Typische installatie.

Cisco Secure Client Profile Editor Setup

### Choose Setup Type

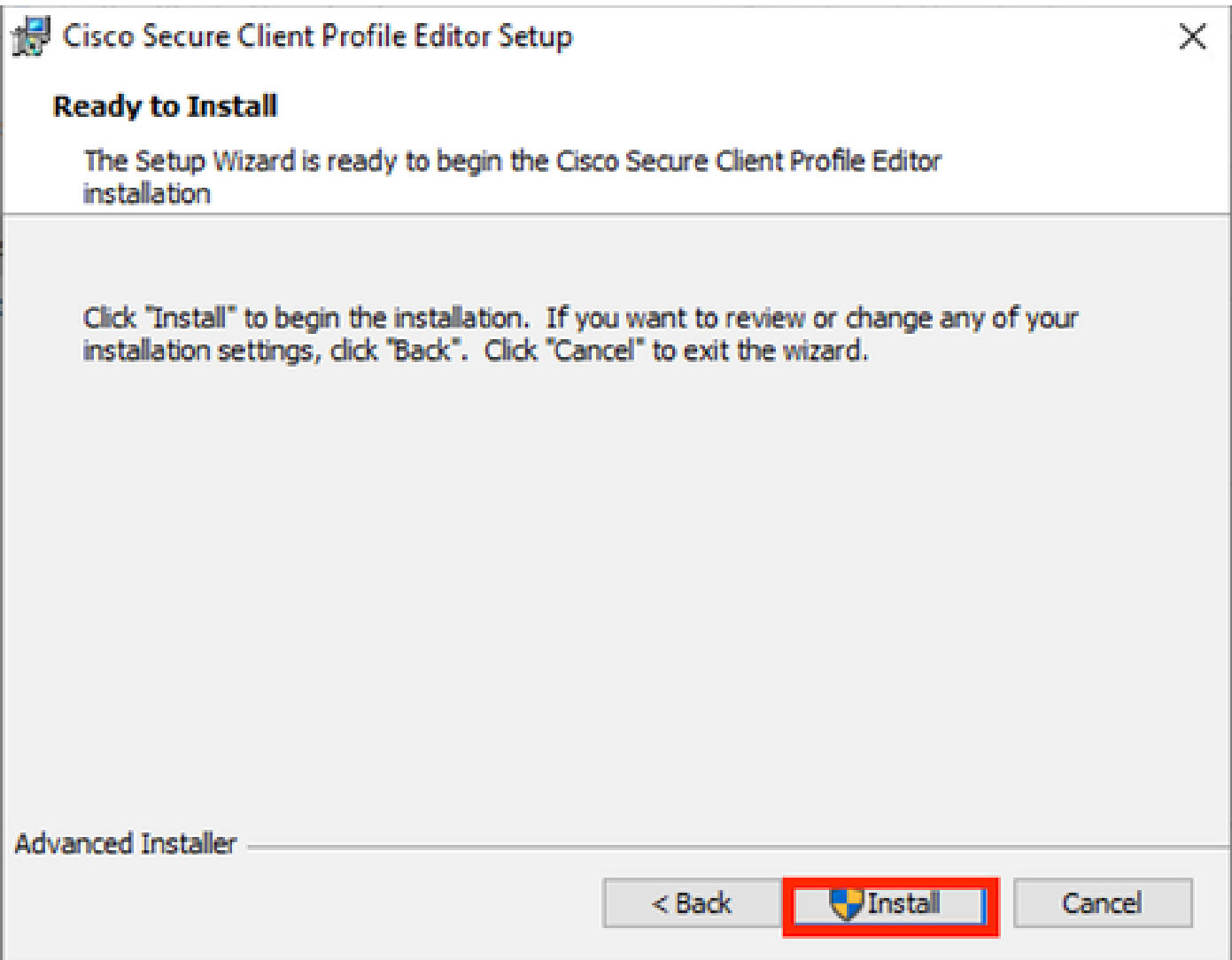
Choose the setup type that best suits your needs

	<b>Typical</b> Installs the most common program features. Recommended for most users.
	<b>Custom</b> Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.
	<b>Complete</b> All program features will be installed. (Requires most disk space)

Advanced Installer

< Back    Next >    Cancel

Profiel editor instellen



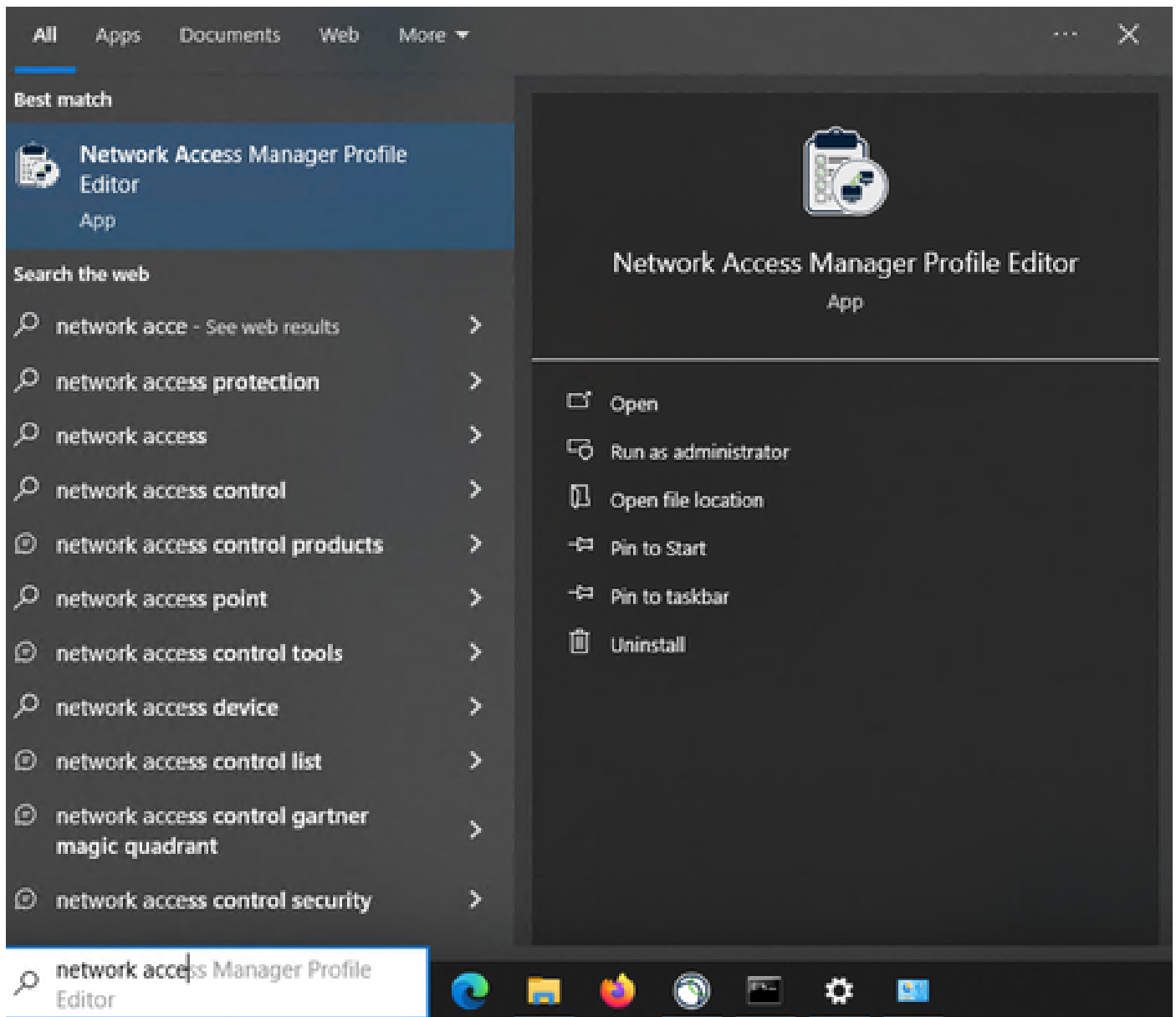
Installatievenster

Klik op Finish (Voltooien).



*Einde profieeditor instellen*

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



Profiel editor 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

Network Access Manager

- Client Policy
- Authentication Policy
- Networks
- Network Groups

### Client Policy

Profile: Untitled

**Connection Settings**

Default Connection Timeout (sec.)

Connection Attempt:

Before user logon

Time to wait before allowing user to logon (sec.)

After user logon

**Media**

Manage Wi-Fi (wireless) Media

- Enable validation of WPA/WPA2/WPA3 handshake
- Enable Randomized MAC Address

Default Association Timeout (sec.)

Manage Wired (802.3) Media

Manage Mobile Broadband (3G) Media

- Enable Data Roaming

**End-user Control**

Allow end-user to:

- Disable Client
- Display user groups
- Specify a script or application to run when connected
- Auto-connect

Select machine connection type

Enable by default

**Administrative Status**

Service Operation:  Enable  Disable

FIPS Mode:  Enable  Disable

Captive Portal Detection:  Enable  Disable

Clientbeleid voor NAM Profile Editor

- Network Access Manager
  - Client Policy
  - Authentication Policy**
  - Networks
  - Network Groups

### Authentication Policy

Profile: **Untitled**

#### Allow Association Modes

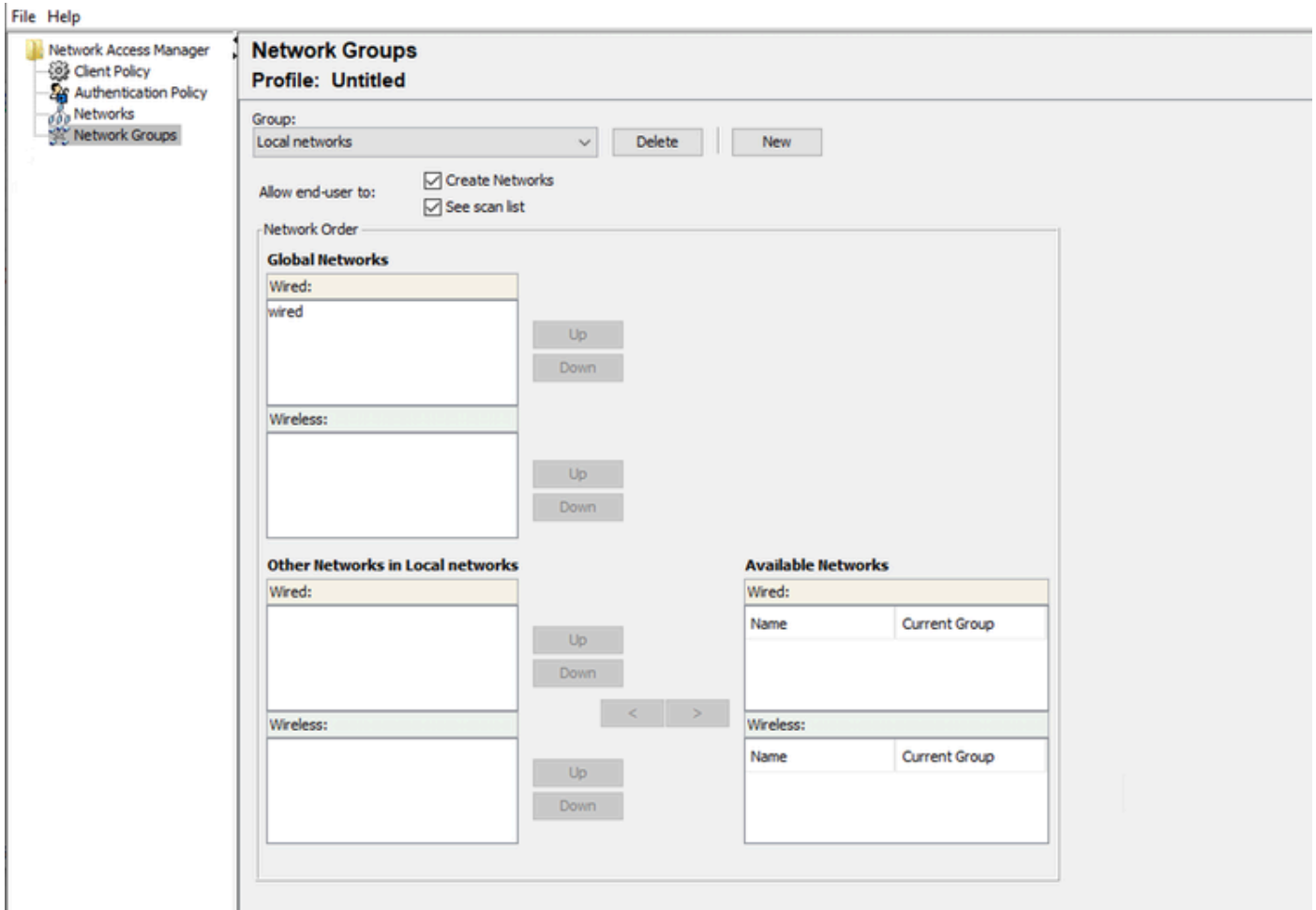
- Select All (Personal)
  - Open (no encryption)
  - Open (Static WEP)
  - Shared (WEP)
  - WPA Personal TKIP
  - WPA Personal AES
  - WPA2 Personal TKIP
  - WPA2 Personal AES
  - WPA3 Open (OWE)
  - WPA3 Personal AES (SAE)
- Select All (Enterprise)
  - Open (Dynamic (802.1X) WEP)
  - WPA Enterprise TKIP
  - WPA Enterprise AES
  - WPA2 Enterprise TKIP
  - WPA2 Enterprise AES
  - CKM Enterprise TKIP
  - CKM Enterprise AES
  - WPA3 Enterprise AES

#### Allowed Authentication Modes

- Select All Outer
  - EAP-FAST
    - EAP-GTC
    - EAP-MSCHAPv2
    - EAP-TLS
  - EAP-TLS
  - EAP-TTLS
    - EAP-MD5
    - EAP-MSCHAPv2
    - PAP (legacy)
    - CHAP (legacy)
    - MSCHAP (legacy)
    - MSCHAPv2 (legacy)
  - LEAP
  - PEAP
    - EAP-GTC
    - EAP-MSCHAPv2
    - EAP-TLS

#### Allowed Wired Security

- Select All
  - Open (no encryption)
  - 802.1x only
  - 802.1x with MacSec
    - AES-GCM-128
    - AES-GCM-256



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).

## Networks

Profile: Untitled

### Network

Name	Media Type	Group*
------	------------	--------

Add...

Edit...

Delete

\* A network in group 'Global' is a member of *all* groups.

*Creatie van netwerkprofiel*

Geef het netwerkprofiel een naam.

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



## Networks

Profile: Untitled

Name:	<input type="text" value="PEAP MSCHAPv2"/>	Media Type
Group Membership	<input type="radio"/> In group: <input type="text" value="Local networks"/>	Security Level
	<input checked="" type="radio"/> In all groups (Global)	
Choose Your Network Media	<input checked="" type="radio"/> <b>Wired (802.3) Network</b> Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.	
	<input type="radio"/> Wi-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.	
	SSID (max 32 chars): <input type="text"/>	
	<input type="checkbox"/> Hidden Network	
	<input type="checkbox"/> Corporate Network	
Association Timeout	<input type="text" value="5"/> seconds	
Common Settings	Script or application on each user's machine to run when connected. <input type="text"/>	
	<input type="button" value="Browse Local Machine"/>	
Connection Timeout	<input type="text" value="40"/> seconds	
	<input type="button" value="Next"/> <input type="button" value="Cancel"/>	

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.

**Networks**  
Profile: Untitled

Security Level

Open Network  
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

**Authenticating Network**  
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

Media Type  
**Security Level**  
Connection Type

802.1X Settings

authPeriod (sec.)	30	startPeriod (sec.)	3
heldPeriod (sec.)	60	maxStart	2

Security

Key Management  
None

Encryption

AES GCM 128  
 AES GCM 256

Port Authentication Exception Policy

Enable port exceptions

Allow data traffic before authentication  
 Allow data traffic after authentication even if

EAP fails  
 EAP succeeds but key management fails

Next Cancel

Beveiligingsniveau van netwerkprofiel

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

**Networks**  
**Profile: Untitled**

Network Connection Type

Machine Connection

This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

**User Connection**

The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.

Machine and User Connection

This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

Media Type  
Security Level  
**Connection Type**  
User Auth  
Credentials

Next Cancel

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.

**Networks**  
Profile: Untitled

**EAP Methods**

- EAP-MD5
- EAP-MSCHAPv2
- EAP-GTC
- EAP-TLS
- EAP-TTLS
- PEAP
- EAP-FAST

Extend user connection beyond log off

**EAP-PEAP Settings**

- Validate Server Identity
- Enable Fast Reconnect
- Disable when using a Smart Card

**Inner Methods based on Credentials Source**

- Authenticate using a Password
  - EAP-MSCHAPv2
  - EAP-GTC
- EAP-TLS, using a Certificate
- Authenticate using a Token and EAP-GTC

Media Type  
Security Level  
Connection Type  
User Auth  
Certificates  
Credentials

Next Cancel

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.

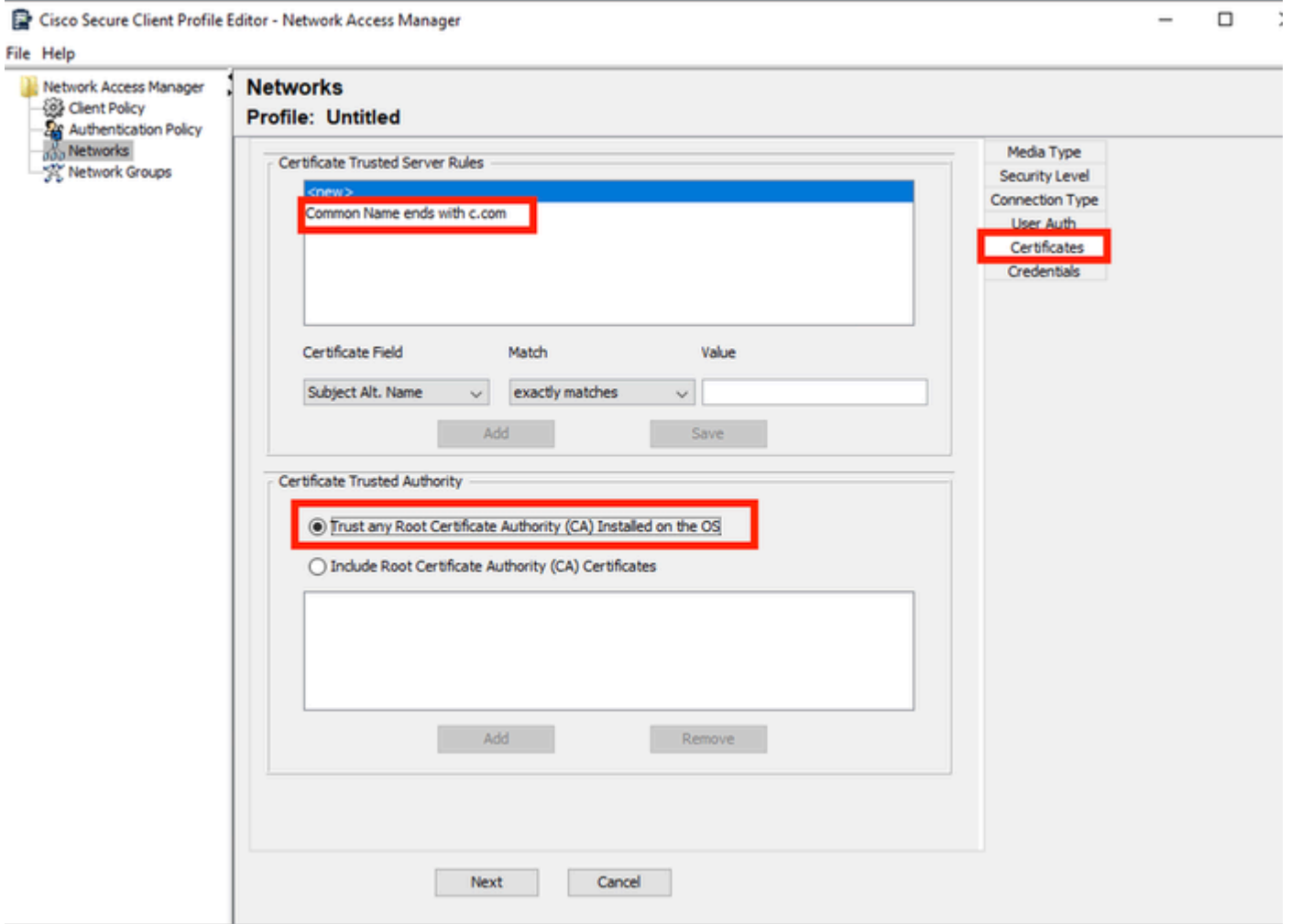
Klik op Volgende om verder te gaan naar het gedeelte Certificaat.



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.

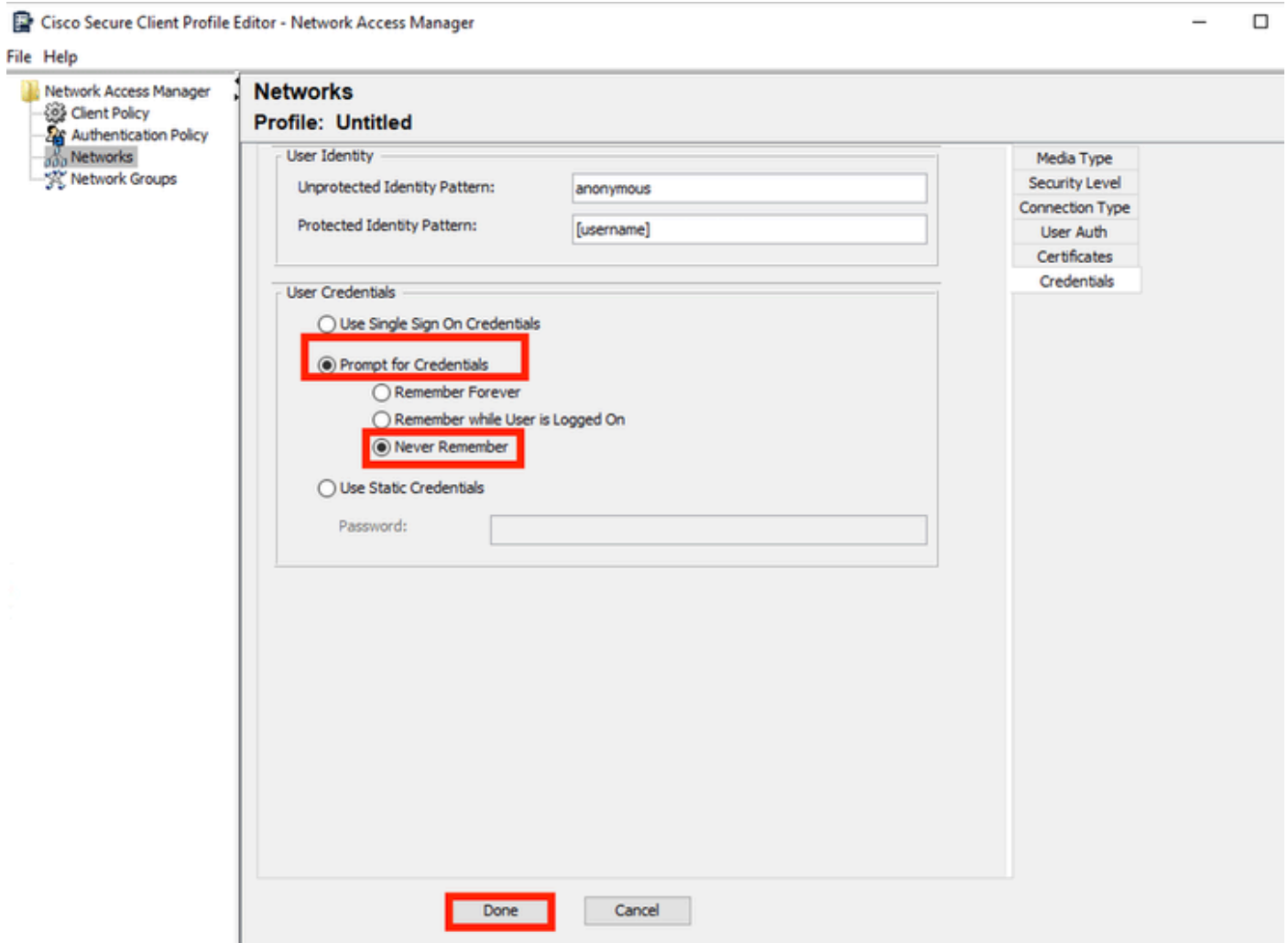


#### Sectie Netwerkprofiel

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.

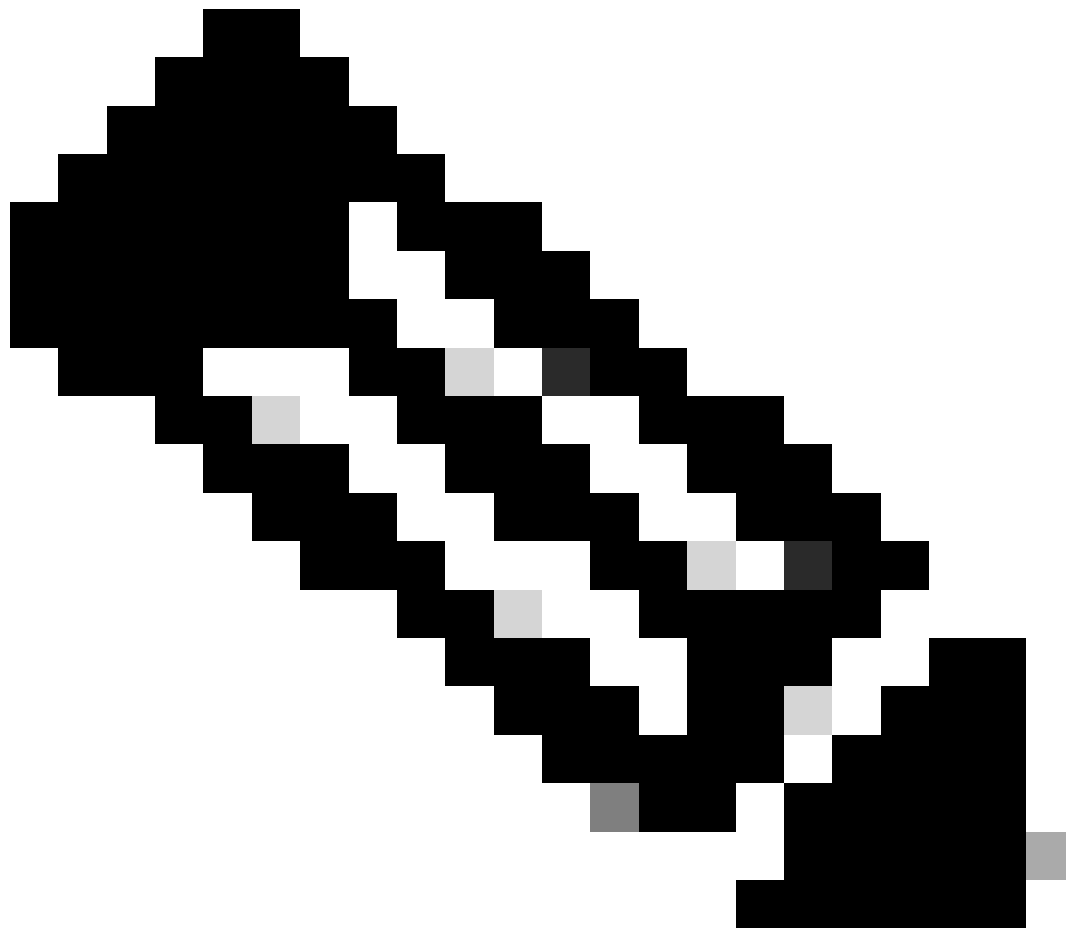
De optie Vragen om referenties > Nooit herinneren is geselecteerd, dus bij elke verificatie moet de gebruiker die de verificatie uitvoert, zijn referenties invoeren.

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:

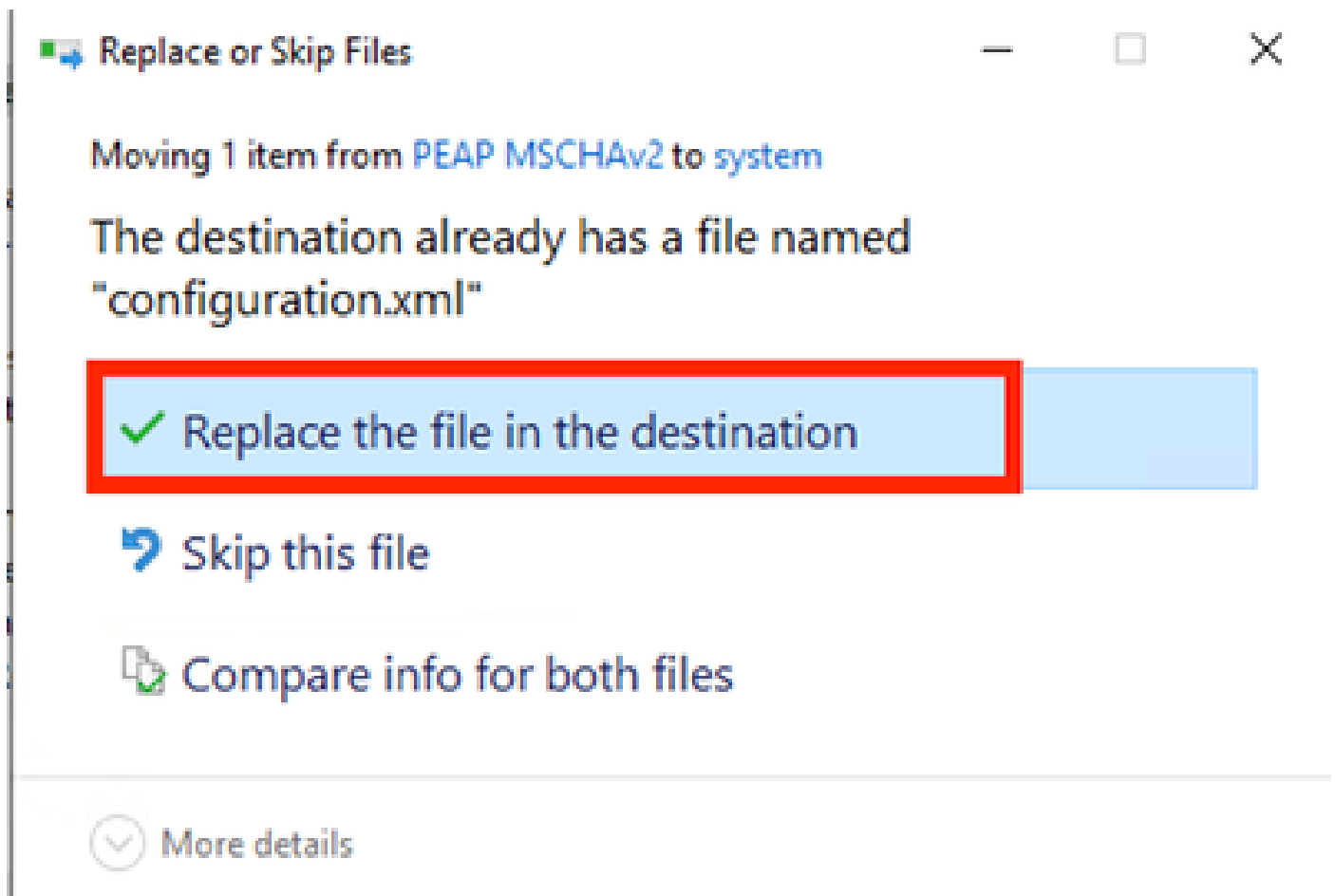
C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



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).

## Networks

Profile: Untitled

### Network

Name	Media Type	Group*
------	------------	--------

Add...

Edit...

Delete

\* A network in group 'Global' is a member of *all* groups.

Tabblad Netwerk van NAM Profile Editor

Geef een naam op in het netwerkprofiel.

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

File Help

**Networks**  
Profile: Untitled

Name:

Group Membership

In group:

In all groups (Global)

Choose Your Network Media

Wired (802.3) Network  
Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

Wi-Fi (wireless) Network  
Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

Hidden Network  
 Corporate Network

Association Timeout:  seconds

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout:  seconds

Media Type  
Security Level

*Sectie Mediatype*

Klik op Next (Volgende).

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

File Help

**Networks**  
Profile: Untitled

Security Level

Open Network  
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

**Authenticating Network**  
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.)	<input type="text" value="30"/>	startPeriod (sec.)	<input type="text" value="3"/>
heldPeriod (sec.)	<input type="text" value="60"/>	maxStart	<input type="text" value="2"/>

Security

Key Management  
None

Encryption

AES GCM 128  
 AES GCM 256

Port Authentication Exception Policy

Enable port exceptions

Allow data traffic before authentication

Allow data traffic after authentication even if

EAP fails  
 EAP succeeds but key management fails

Next Cancel

Sectie Security Level Profile Editor

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

File Help

**Networks**  
Profile: Untitled

Network Connection Type

Machine Connection

This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

User Connection

The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.

Machine and User Connection

This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

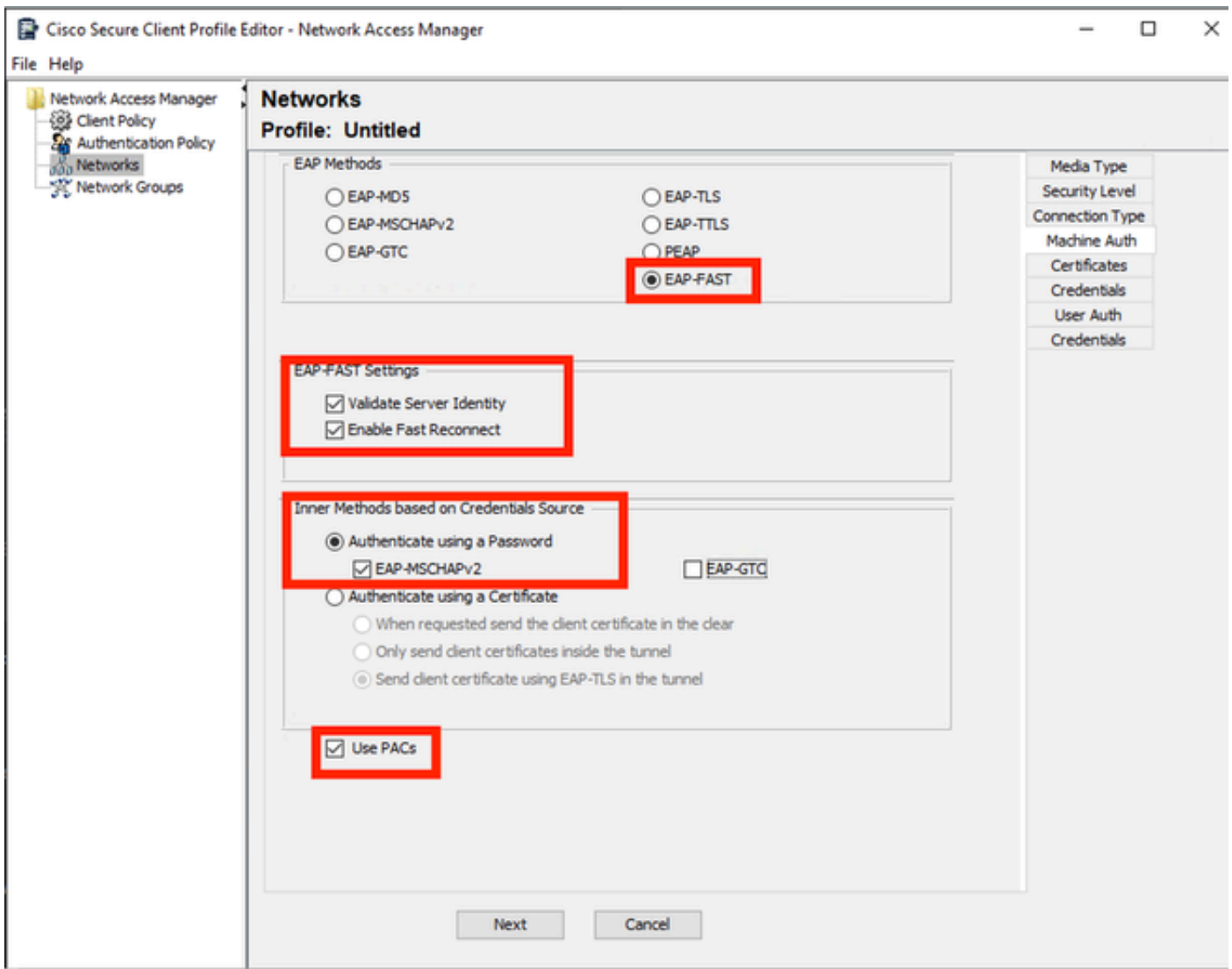
Media Type  
Security Level  
**Connection Type**  
Machine Auth  
Credentials  
User Auth  
Credentials

Next Cancel

*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.

## Networks

Profile: Untitled

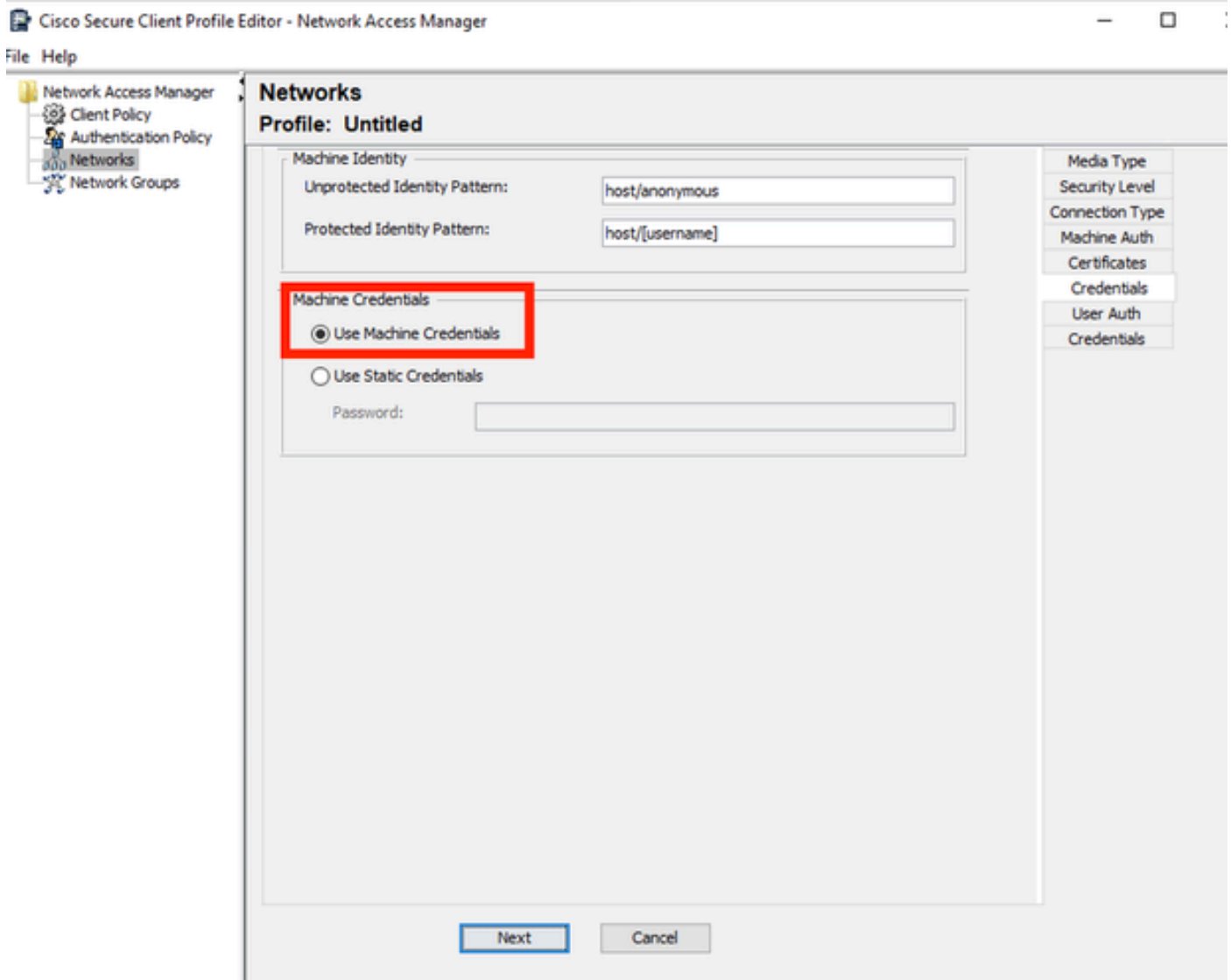
The screenshot shows the 'Certificate Trusted Server Rules' and 'Certificate Trusted Authority' sections of a network configuration wizard. The 'Certificate Trusted Server Rules' section has a list with one rule: '<new>' with the value 'Subject Alternative Name ends with c.com'. Below this is a table with columns 'Certificate Field', 'Match', and 'Value'. The 'Certificate Field' is set to 'Subject Alt. Name', the 'Match' is 'exactly matches', and the 'Value' field is empty. There are 'Add' and 'Save' buttons below the table. The 'Certificate Trusted Authority' section has two radio button options: 'Trust any Root Certificate Authority (CA) Installed on the OS' (which is selected) and 'Include Root Certificate Authority (CA) Certificates'. Below these is an empty list box with 'Add' and 'Remove' buttons. At the bottom of the wizard are 'Next' and 'Cancel' buttons. On the right side, there is a vertical menu with options: Media Type, Security Level, Connection Type, Machine Auth, Certificates (highlighted), Credentials, User Auth, Certificates, and Credentials.

*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).



File Help

**Networks**  
Profile: Untitled

EAP Methods

EAP-MD5                       EAP-TLS  
 EAP-MSCHAPv2               EAP-TTLS  
 EAP-GTC                         PEAP  
 **EAP-FAST**

Extend user connection beyond log off

EAP-FAST Settings

Validate Server Identity  
 Enable Fast Reconnect  
 Disable when using a Smart Card

Inner Methods based on Credentials Source

Authenticate using a Password  
 EAP-MSCHAPv2               EAP-GTC  
 Authenticate using a Certificate  
 When requested send the client certificate in the clear  
 Only send client certificates inside the tunnel  
 Send client certificate using EAP-TLS in the tunnel  
 Authenticate using a Token and EAP-GTC

Use PACs

Next      Cancel

Media Type  
Security Level  
Connection Type  
Machine Auth  
Certificates  
Credentials  
User Auth  
Certificates  
Credentials

*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 beleidserverknooppunt worden gebruikt.

## Networks

Profile: C:\Users\LAB 5\Desktop\EAP FAST\configuration.xml

The screenshot shows the 'Certificate Trusted Server Rules' section of a network configuration wizard. A rule is defined with the following details:

Certificate Field	Match	Value
Common Name	ends with	c.com

Below the table are 'Remove' and 'Save' buttons. The 'Certificate Trusted Authority' section below it has two radio button options:

- Trust any Root Certificate Authority (CA) Installed on the OS
- Include Root Certificate Authority (CA) Certificates

Below these options is an empty list box with 'Add' and 'Remove' buttons. At the bottom of the wizard are 'Next' and 'Cancel' buttons. On the right side, a vertical menu contains the following items: Media Type, Security Level, Connection Type, Machine Auth, Certificates, Credentials, User Auth, Certificates, and Credentials. The second 'Certificates' item is highlighted with a red box.

*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).

## Networks

### Profile: Untitled

**User Identity**

Unprotected Identity Pattern:

Protected Identity Pattern:

**User Credentials**

Use Single Sign On Credentials

Prompt for Credentials

Remember Forever

Remember while User is Logged On

Never Remember

Use Static Credentials

Password:

Media Type

Security Level

Connection Type

Machine Auth

Certificates

Credentials

User Auth

Certificates

Credentials

*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\system



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).

## Networks

Profile: Untitled

### Network

Name	Media Type	Group*
------	------------	--------

Add...

Edit...

Delete

\* A network in group 'Global' is a member of *all* groups.

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.

**Networks**  
Profile: Untitled

Name:

Group Membership

In group:

In all groups (Global)

Choose Your Network Media

Wired (802.3) Network

Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

Wi-Fi (wireless) Network

Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

Hidden Network

Corporate Network

Association Timeout  seconds

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout  seconds

Media Type Security Level

*Sectie Mediatype*

Klik op Next (Volgende).

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

Network Access Manager

- Client Policy
- Authentication Policy
- Networks**
- Network Groups

## Networks

Profile: Untitled

Security Level

Open Network  
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

**Authenticating Network**  
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.)  startPeriod (sec.)

heldPeriod (sec.)  maxStart

Port Authentication Exception Policy

Enable port exceptions

Allow data traffic before authentication

Allow data traffic after authentication even if

EAP fails

EAP succeeds but key management fails

Security

Key Management

None

Encryption

AES GCM 128

AES GCM 256

Media Type

Security Level

Connection Type

Next Cancel

Beveiligingsniveau

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

Network Access Manager

- Client Policy
- Authentication Policy
- Networks**
- Network Groups

## Networks

Profile: Untitled

Network Connection Type

Machine Connection  
This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

**User Connection**  
The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.

Machine and User Connection  
This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

Media Type

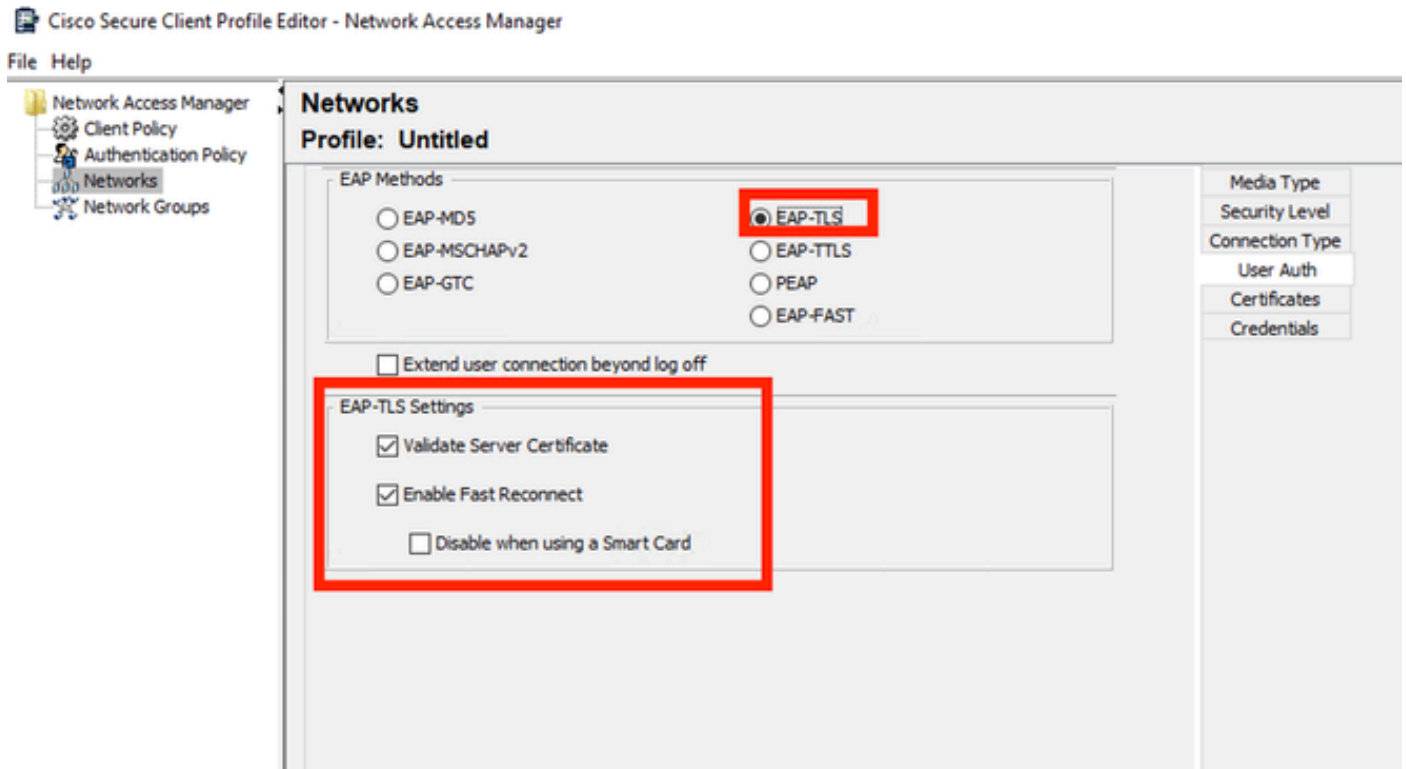
Security Level

Connection Type

User Auth

Credentials

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.



The screenshot shows the 'Networks' section of the Cisco Secure Client Profile Editor. The main window is titled 'Profile: Untitled'. On the left, a navigation pane shows 'Network Access Manager', 'Client Policy', 'Authentication Policy', 'Networks', and 'Network Groups'. The 'Networks' section is active, displaying two main configuration areas:

- Certificate Trusted Server Rules:** A list box contains one rule: 'Common Name ends with c.com'. Below this is a table for defining rules:

Certificate Field	Match	Value
Subject Alt. Name	exactly matches	

Buttons for 'Add' and 'Save' are located below the table.

- Certificate Trusted Authority:** Two radio button options are present:

- Trust any Root Certificate Authority (CA) Installed on the OS
- Include Root Certificate Authority (CA) Certificates

A list box is empty below these options, with 'Add' and 'Remove' buttons at the bottom.

At the bottom of the main window are 'Next' and 'Cancel' buttons. On the right side, a vertical menu shows 'Media Type', 'Security Level', 'Connection Type', 'User Auth', 'Certificates', and 'Credentials', with 'Certificates' highlighted.

*Instellingen voor certificaat van gebruikersautorisatie*

Klik op Next (Volgende).

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

## Networks

Profile: Untitled

User Identity

Unprotected Identity Pattern:

User Credentials

Use Single Sign On Credentials (Requires Smart Card)

Prompt for Credentials

- Remember Forever
- Remember while User is Logged On
- Never Remember

Certificate Source

Smart Card or OS certificates

Smart Card certificates only

Remember Smart Card Pin

Remember Forever

Remember while User is Logged On

Never Remember

Smart Card Removal Policy

Disconnect from Network

Use Certificate Matching Rule (Max 10)

Rule Logic  OR  AND

Field	Operator	Value

Media Type

Security Level

Connection Type

User Auth

Certificates

Credentials

Done Cancel

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).

**Certificate Matching Rule Entry** [X]

Certificate Field: Issuer.CN      Match: Equals

Value: My Internal OR 3rd Party CA.com

OK      Cancel

Use Certificate Matching Rule (Max 10)

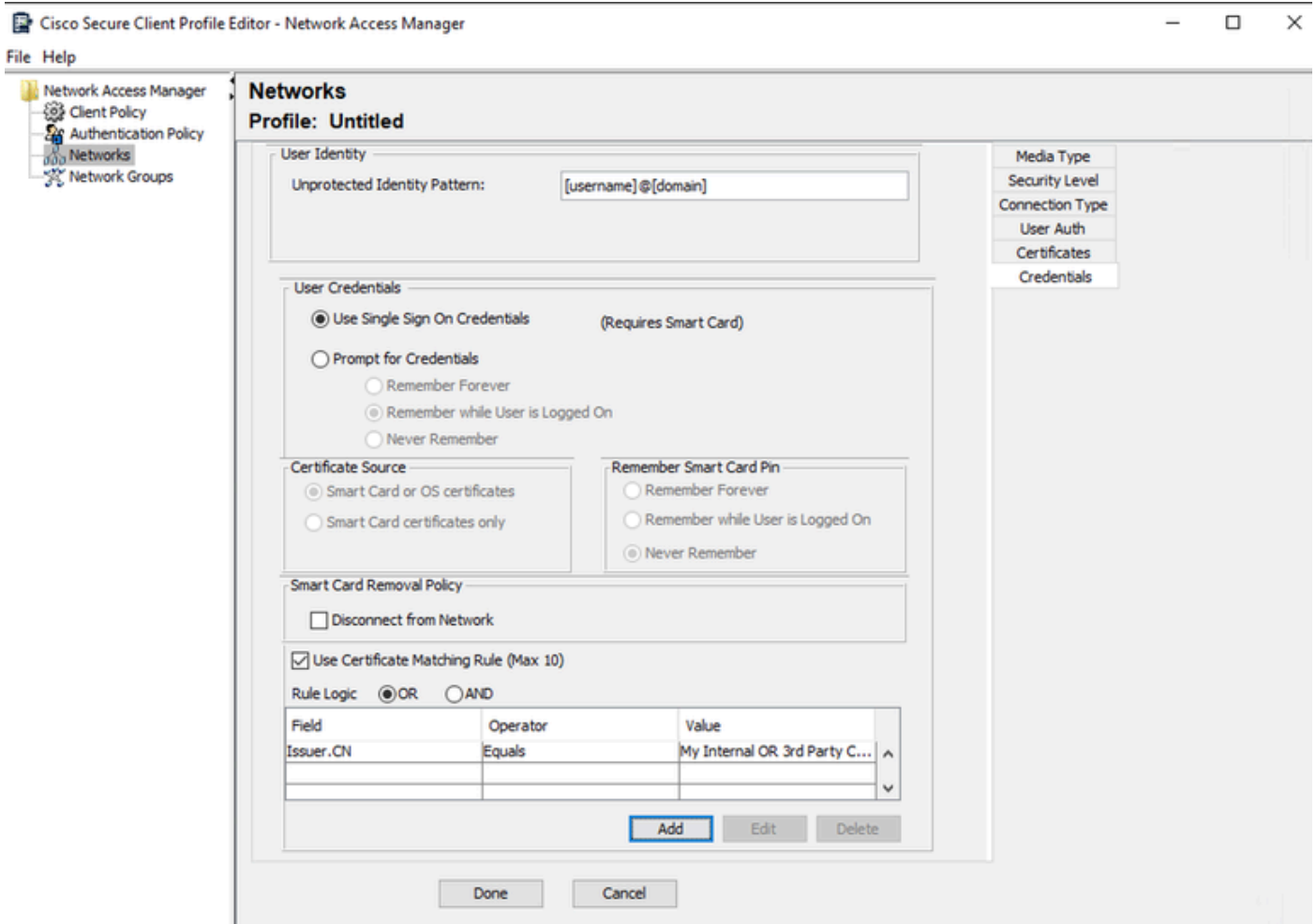
Logic:  OR     AND

Id	Operator	Value

Add    Edit    Delete

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\system



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>
```

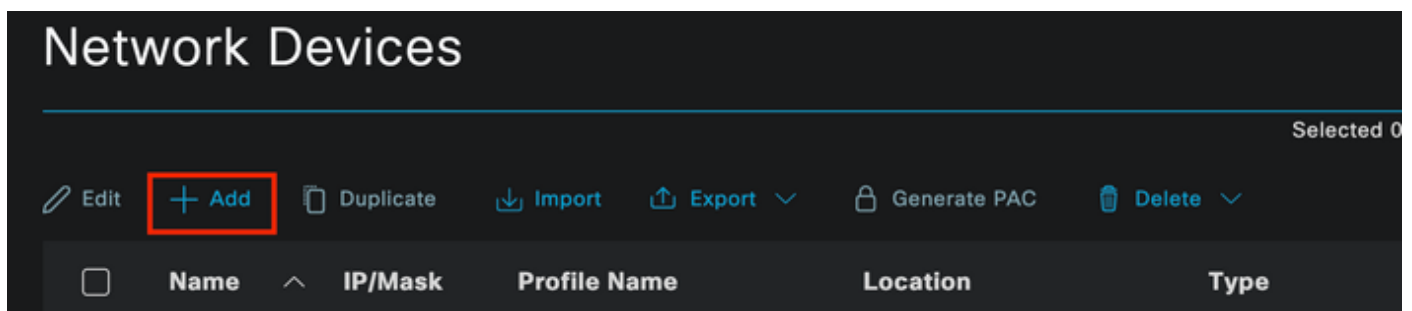
```
!  
!  
aaa group server radius ISE-CLUSTER  
  server name ISE-PSN-1  
!  
interface GigabitEthernet0/1/0  
  description "Endpoint that supports dot1x"  
  switchport access vlan 15  
  switchport mode access  
  authentication host-mode multi-auth  
  authentication order dot1x mab  
  authentication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

### Identity Service Engine configureren 3.2.

Configureer het netwerkapparaat.

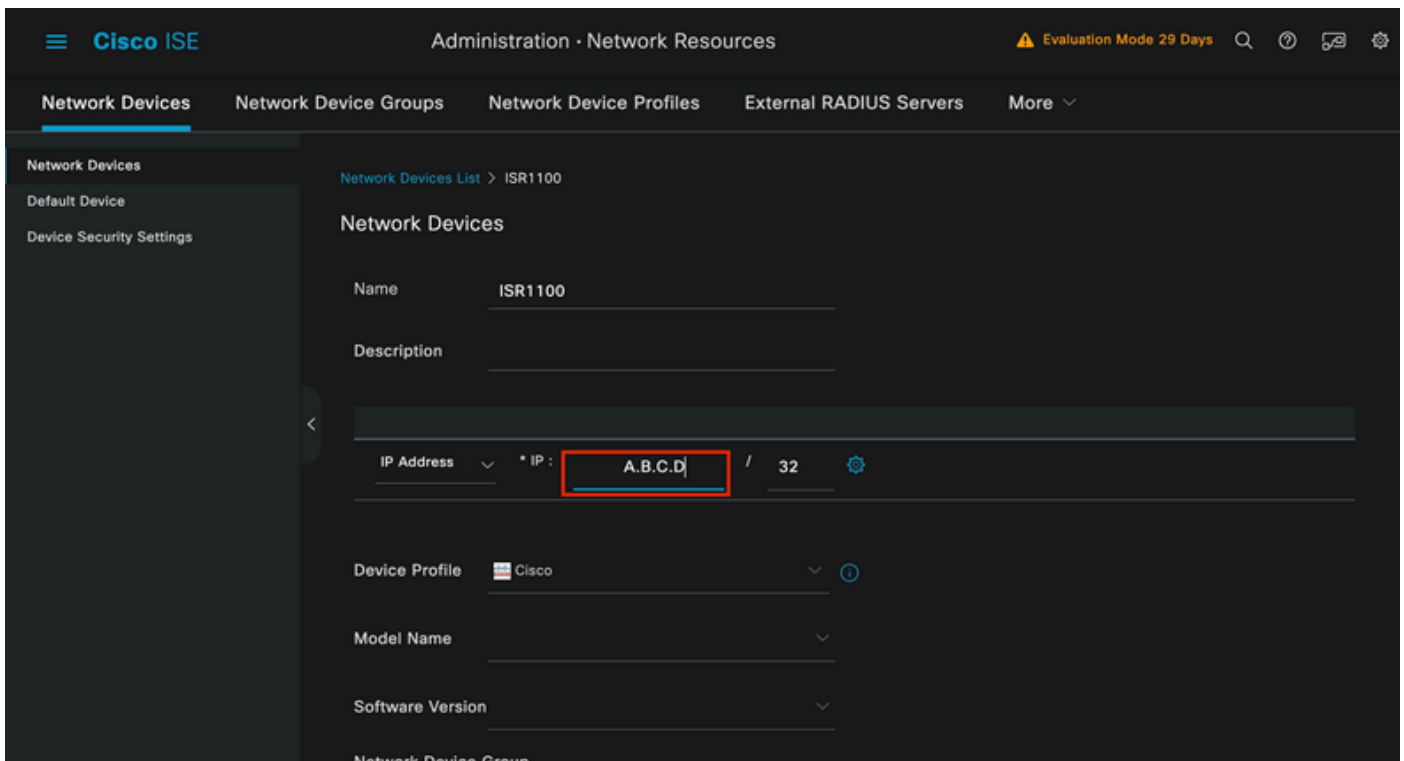
Voeg de ISR en de ISE toe aan ISE-beheer > Netwerkbronnen > Netwerkapparaten.

Klik op Add (Toevoegen).



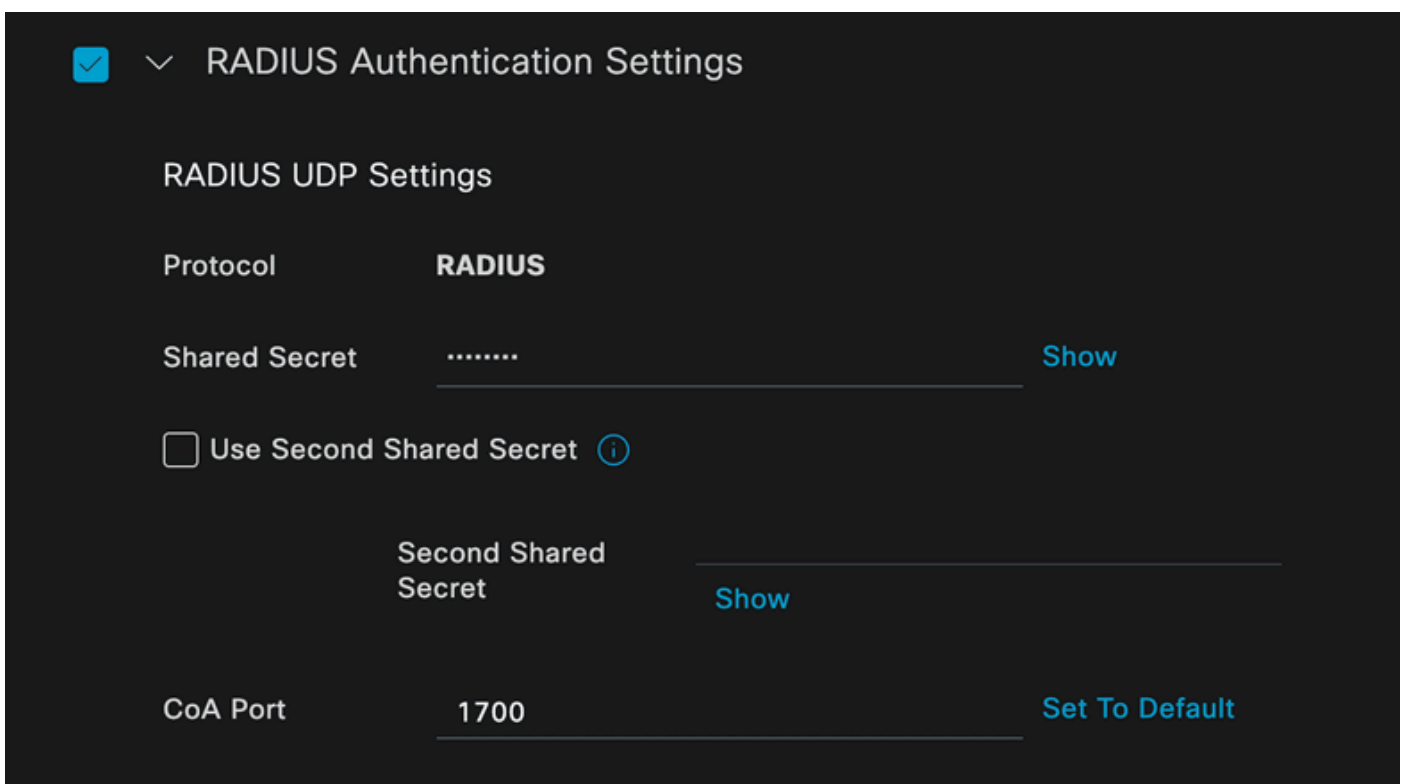
Sectie Netwerkapparaat

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



Creatie van netwerkkapparaat

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



Instellingen straal netwerkkapparaat

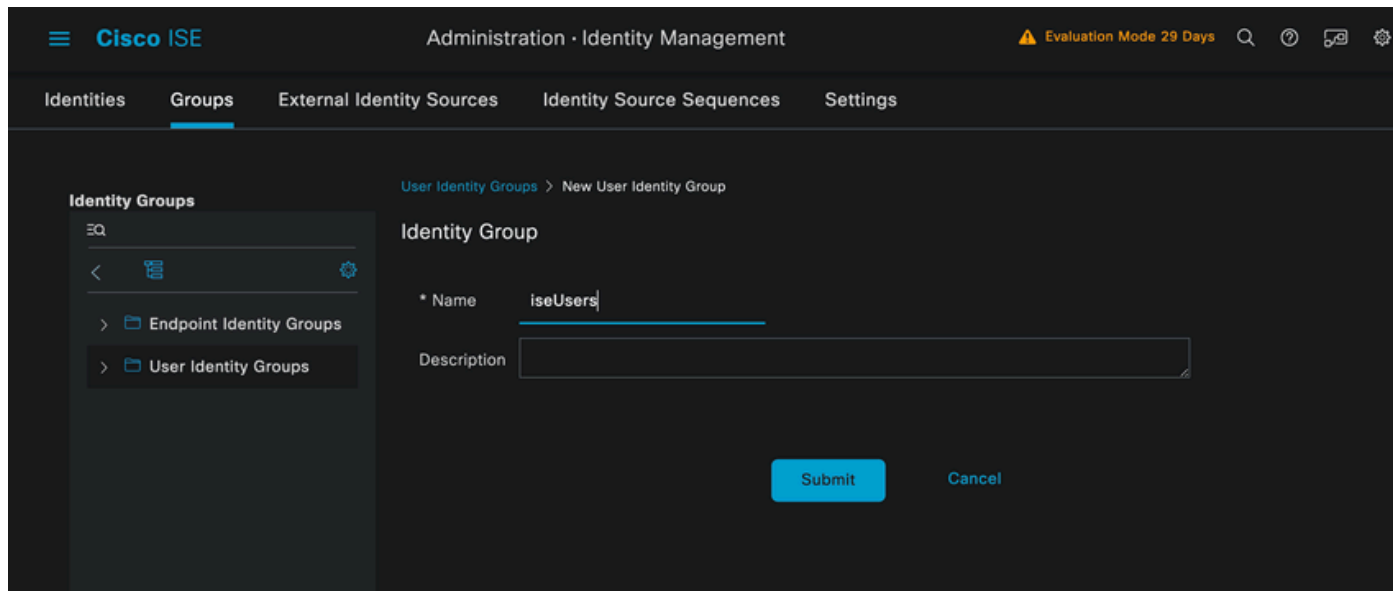
Sla de wijzigingen op.

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



Lokale verificatie met ISE wordt gebruikt. De externe authenticatie 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.

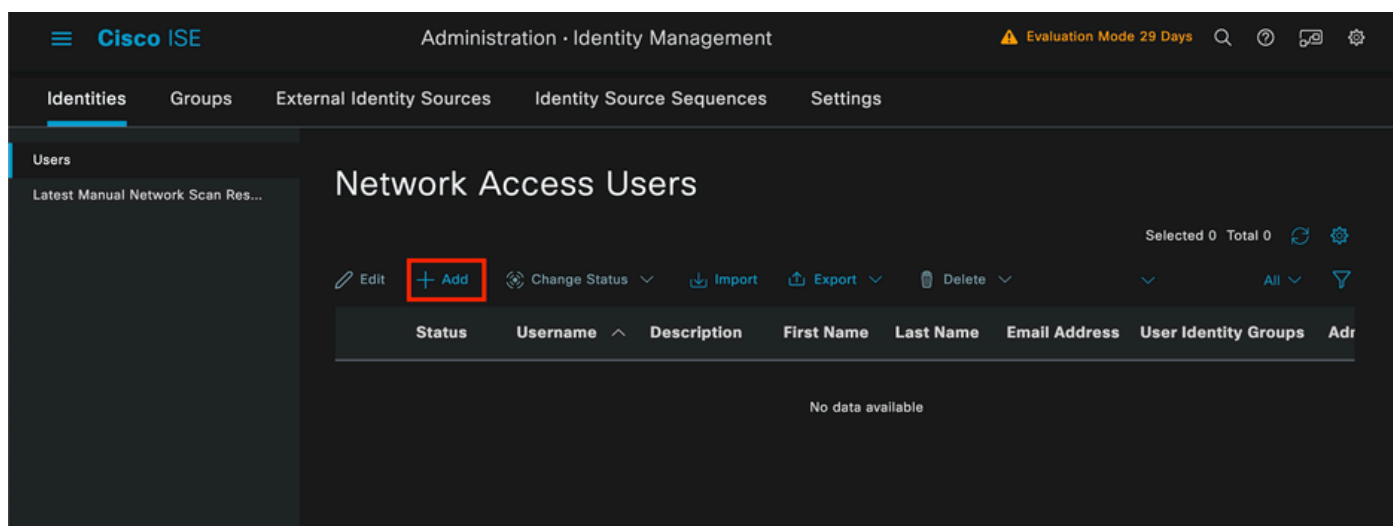


*Creatie van identiteitsgroep*

Klik op Verzenden.

Navigeer naar Beheer > Identity Management > tabblad Identity.

Klik op Add (Toevoegen).



*Sectie Netwerkttoegangsgebruikers*

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

### Network Access User

\* Username

Status  Enabled

Account Name Alias

Email

Creatie van gebruiker voor netwerktoegang

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

### Passwords

Password Type:

Password Lifetime:

- With Expiration  
Password will expire in 60 days
- Never Expires

Password

Re-Enter Password

\* Login Password

Generate Password

Enable Password

Generate Password

Gedeelte Wachtwoord voor maken van gebruiker

Wijs de gebruiker toe aan de groep ISEusers.

### User Groups



iseUsers



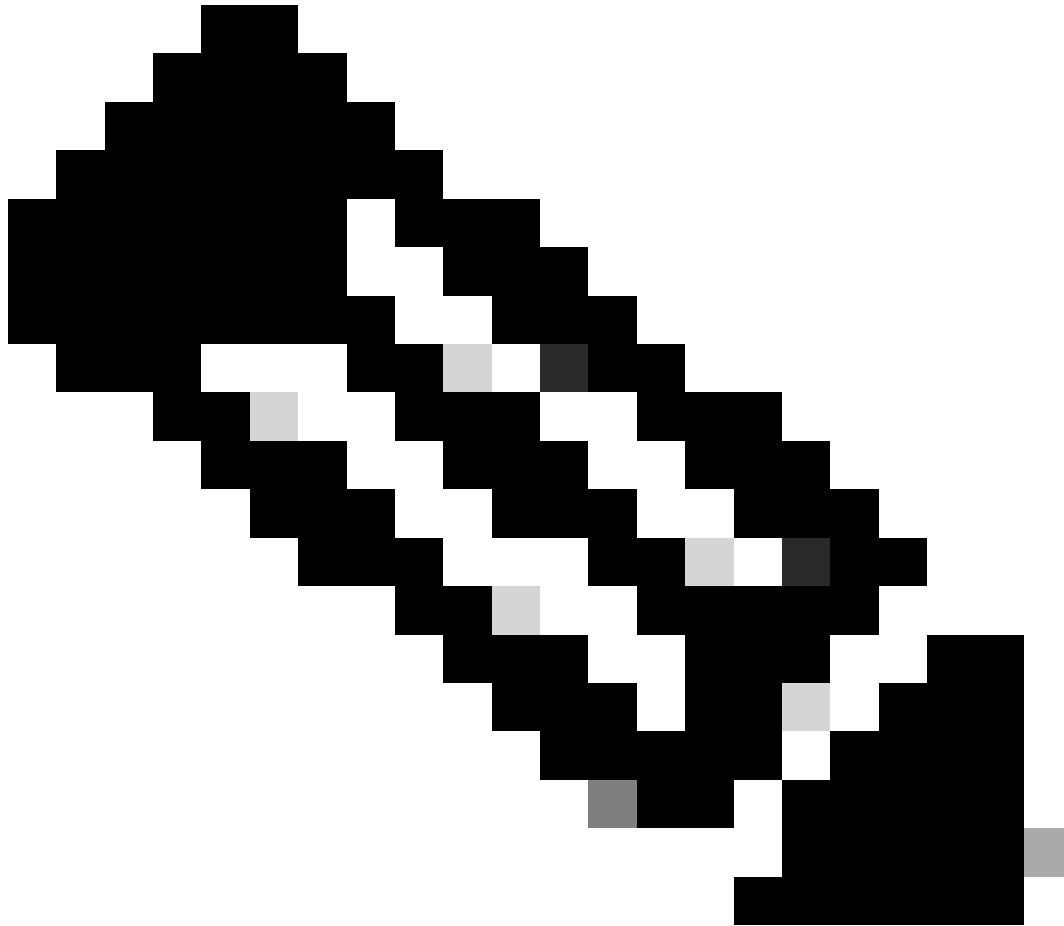
Toewijzing van gebruikersgroep

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.

---

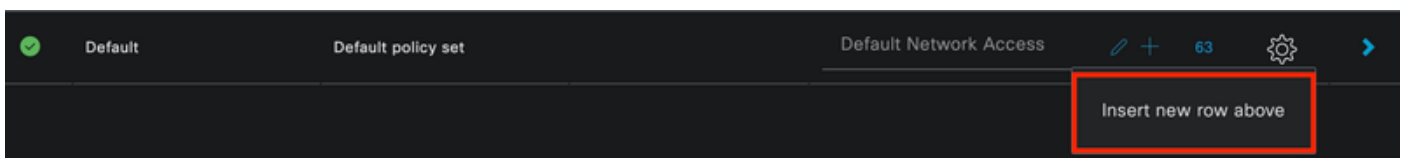


Opmerking: het classificeren en differentiëren van de beleidssets helpt bij het oplossen van problemen,

---

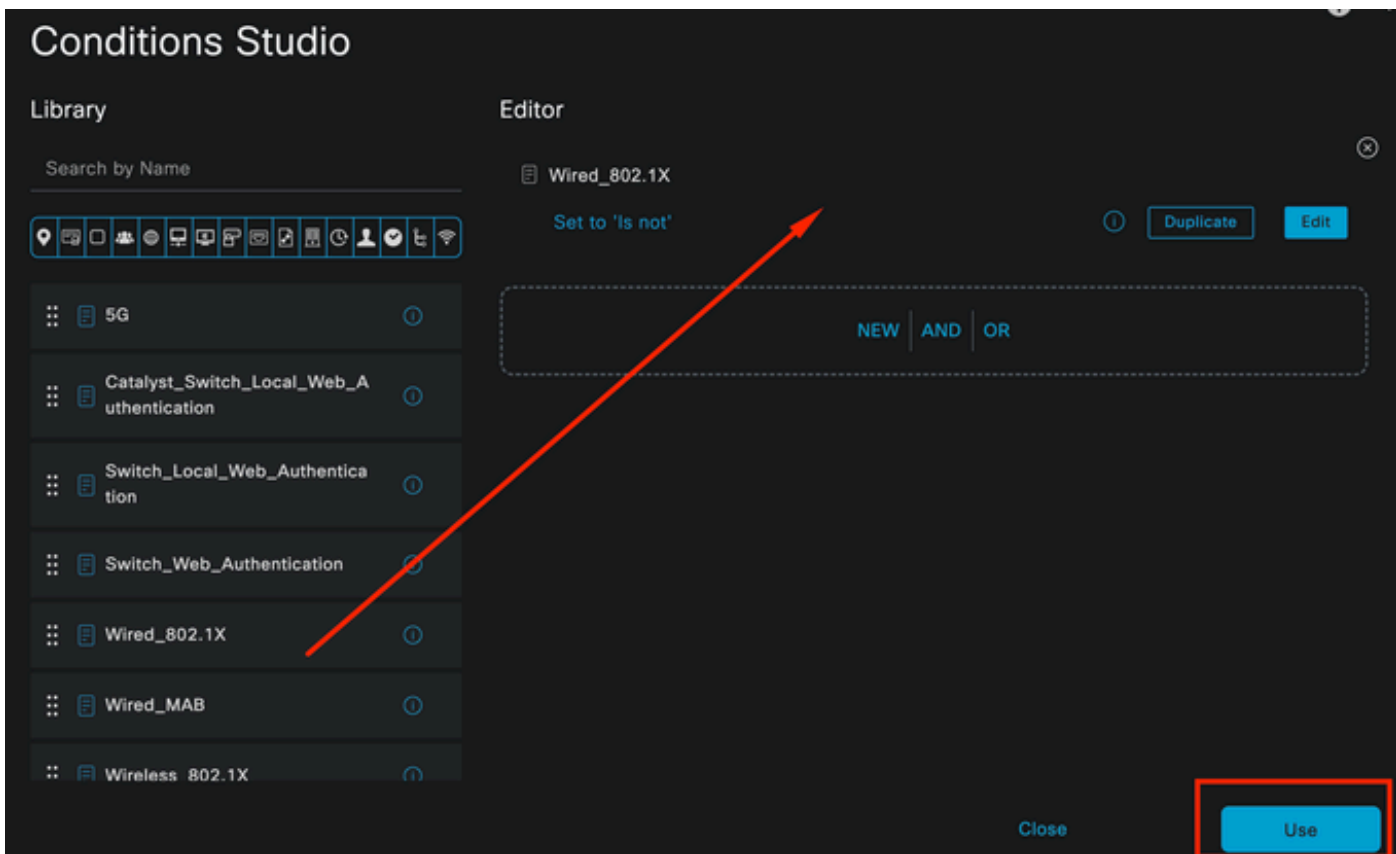


Opmerking: Als het pictogram add of plus niet zichtbaar is, kan het versnellingspictogram van elke beleidsset worden geklikt en selecteer vervolgens Nieuwe rij invoegen hierboven.



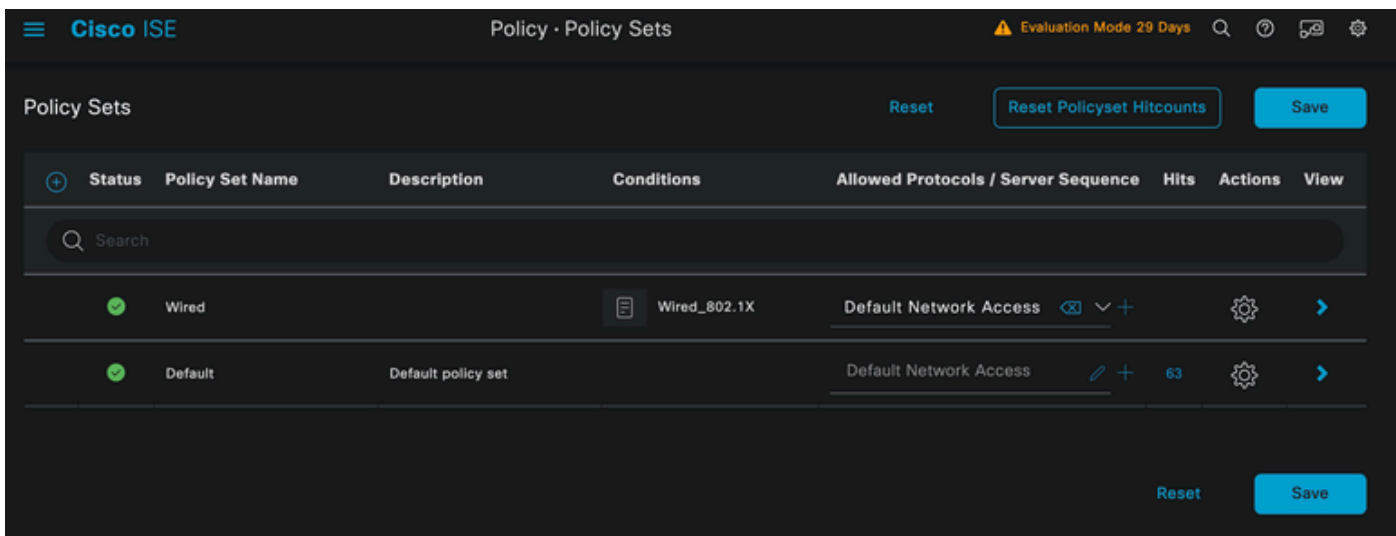
*Pictogramopties tandwiel*

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.

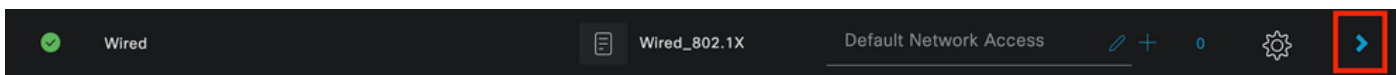


Algemene weergave van beleidssets

Klik op Save (Opslaan).

2. Configureer het verificatie- en autorisatiebeleid.

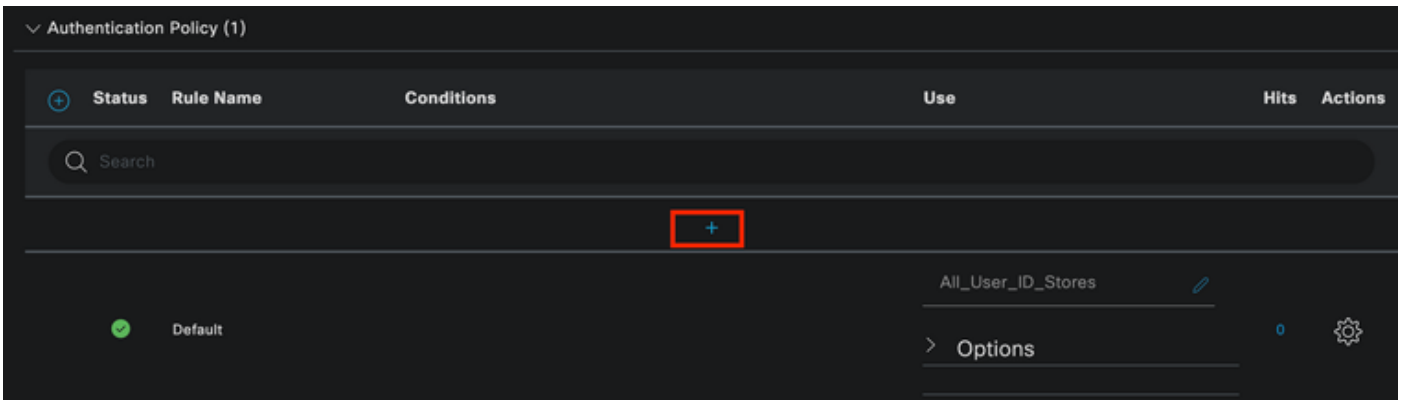
Klik op het >pictogram.



Bedrade beleidsset

Breid het gedeelte Verificatiebeleid uit.

Klik op het pictogram +.



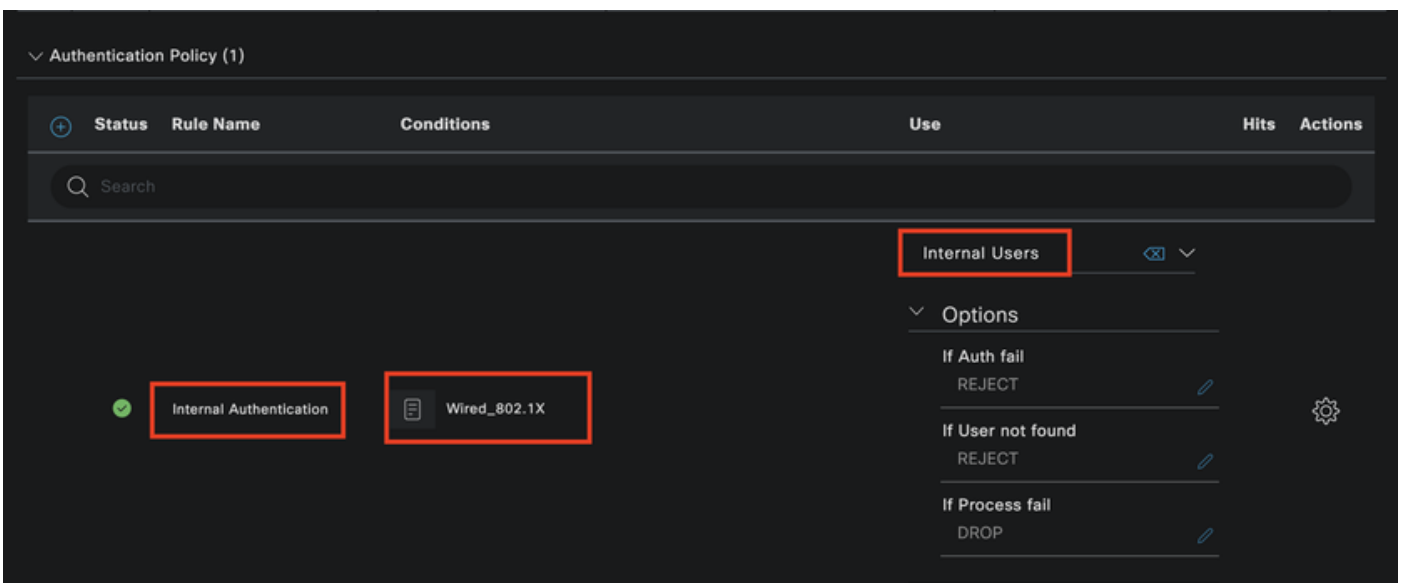
*Verificatiebeleid*

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.

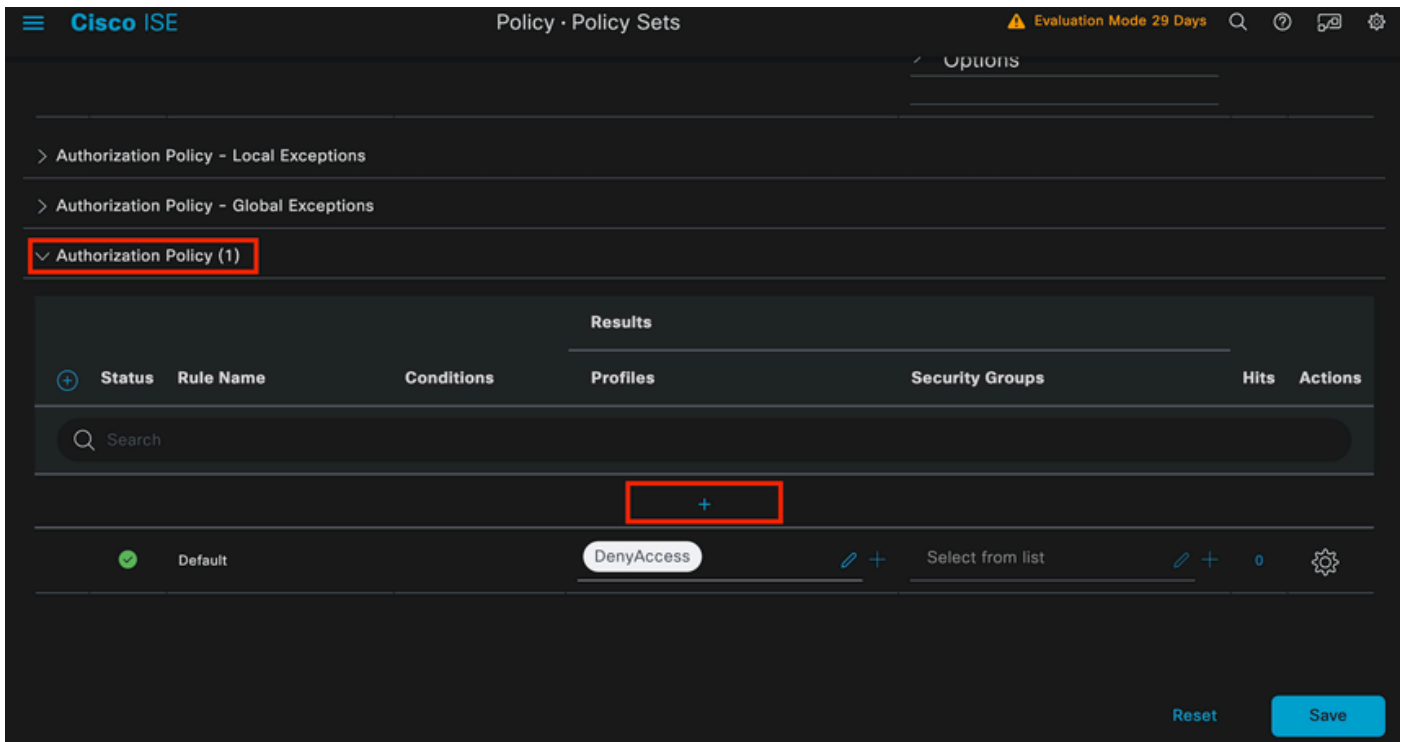
Selecteer in de kolom Gebruik tot slot de optie Interne gebruikers.



*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.

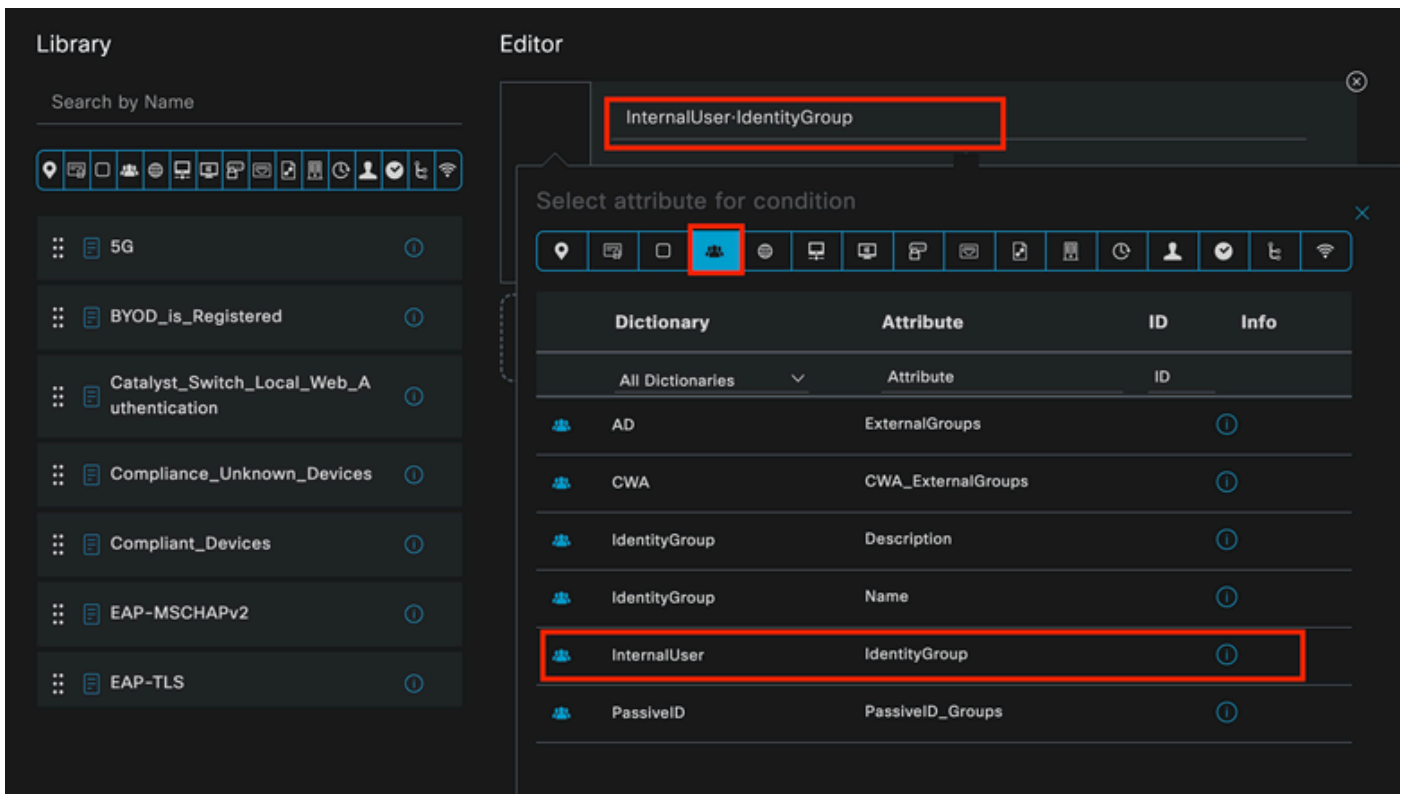
Als u een voorwaarde voor dit autorisatiebeleid wilt maken, klikt u op het +-pictogram in de kolom Voorwaarden.

De groep IseGebruikers wordt gebruikt.

Klik op de sectie Kenmerken.

Selecteer het pictogram IdentityGroup.

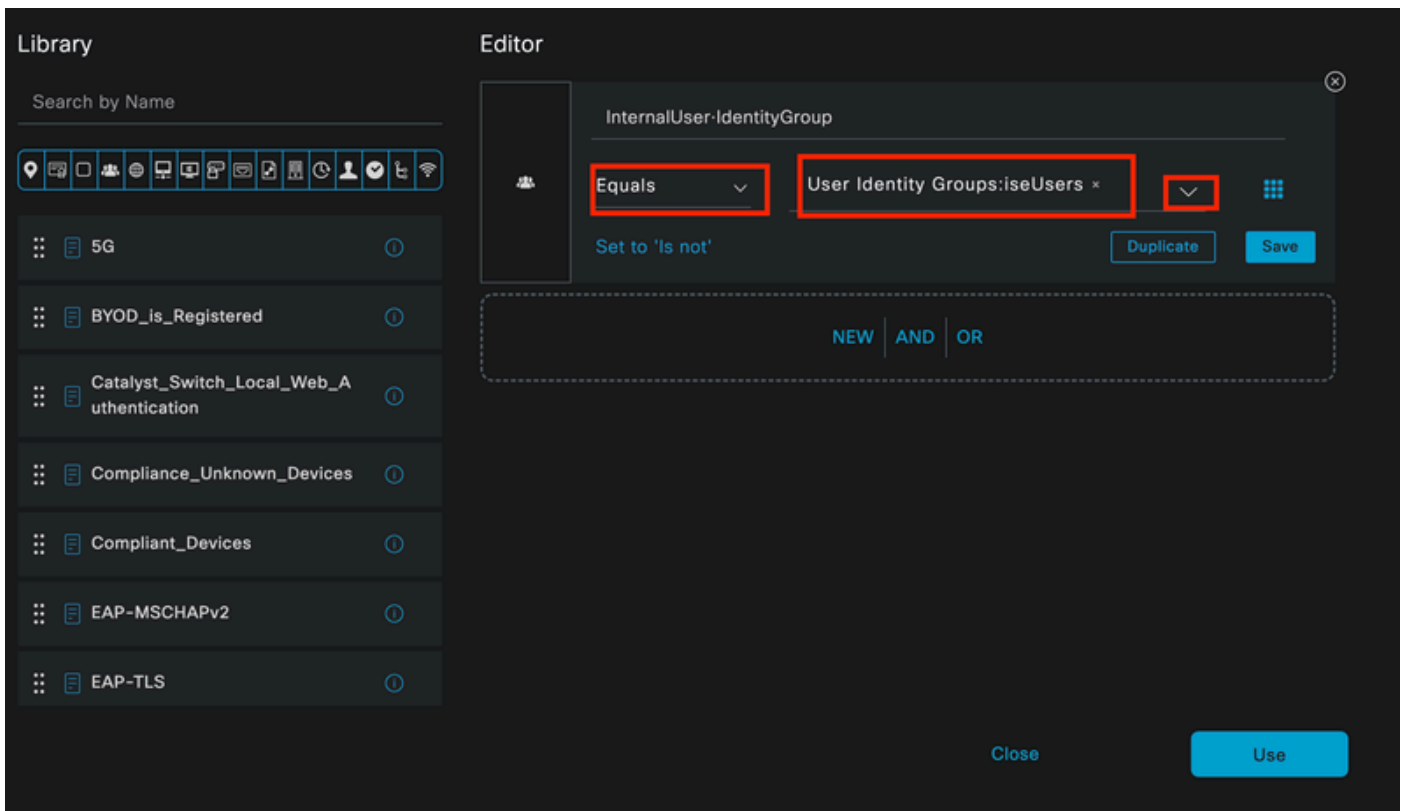
Selecteer in het woordenboek het interne gebruikerswoordenboek dat bij het kenmerk IdentityGroup wordt geleverd.



Conditie maken

Selecteer de operator Gelijk.

Selecteer vanuit Gebruikersidentiteitsgroepen de groep IseGebruikers.



Conditie maken

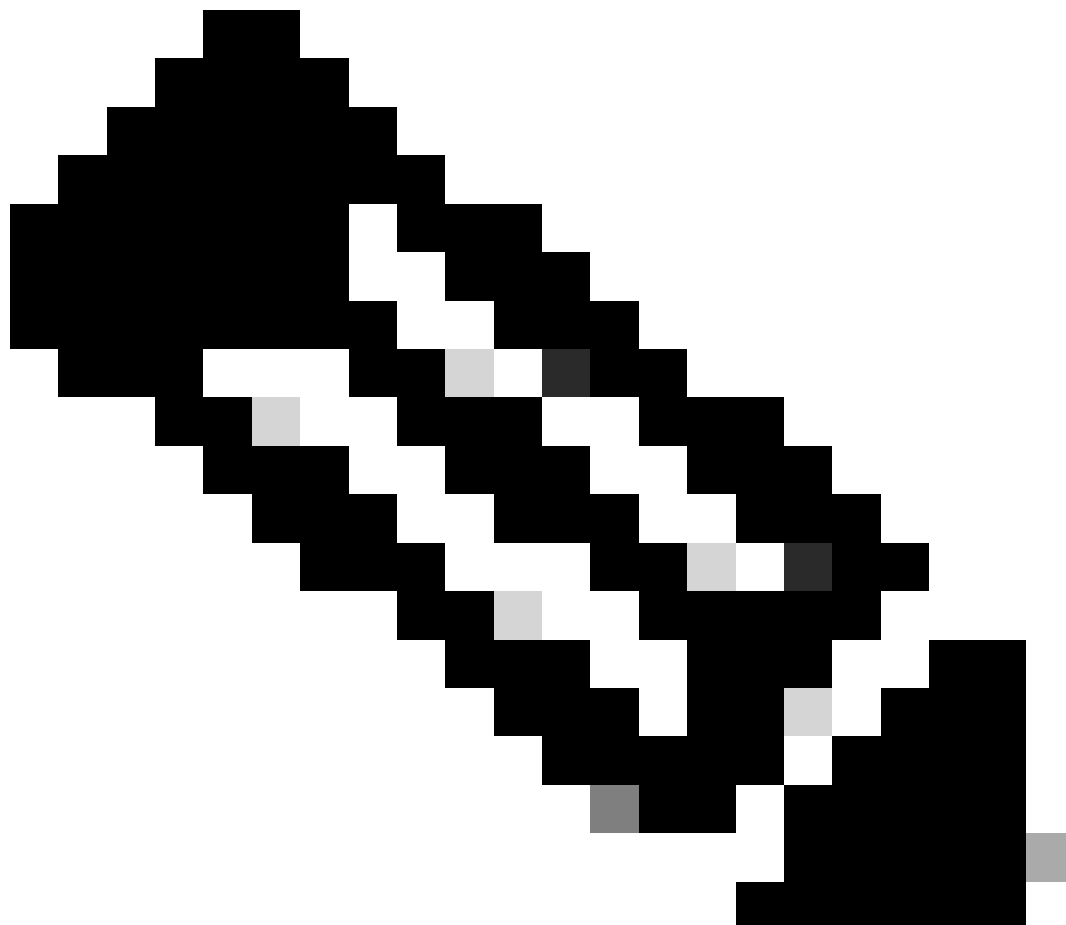


Klik op Gebruik.

Voeg het resultaat autorisatieprofiel toe.

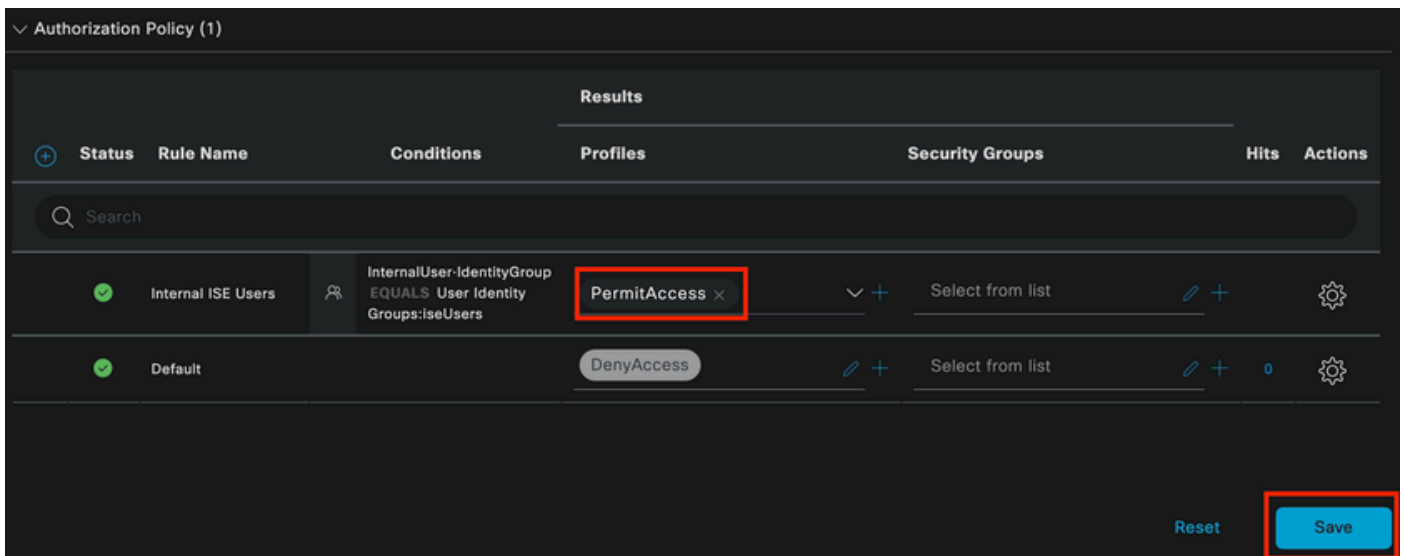
Er wordt gebruikgemaakt van het vooraf ingestelde profiel Permit Access.

---



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.

---



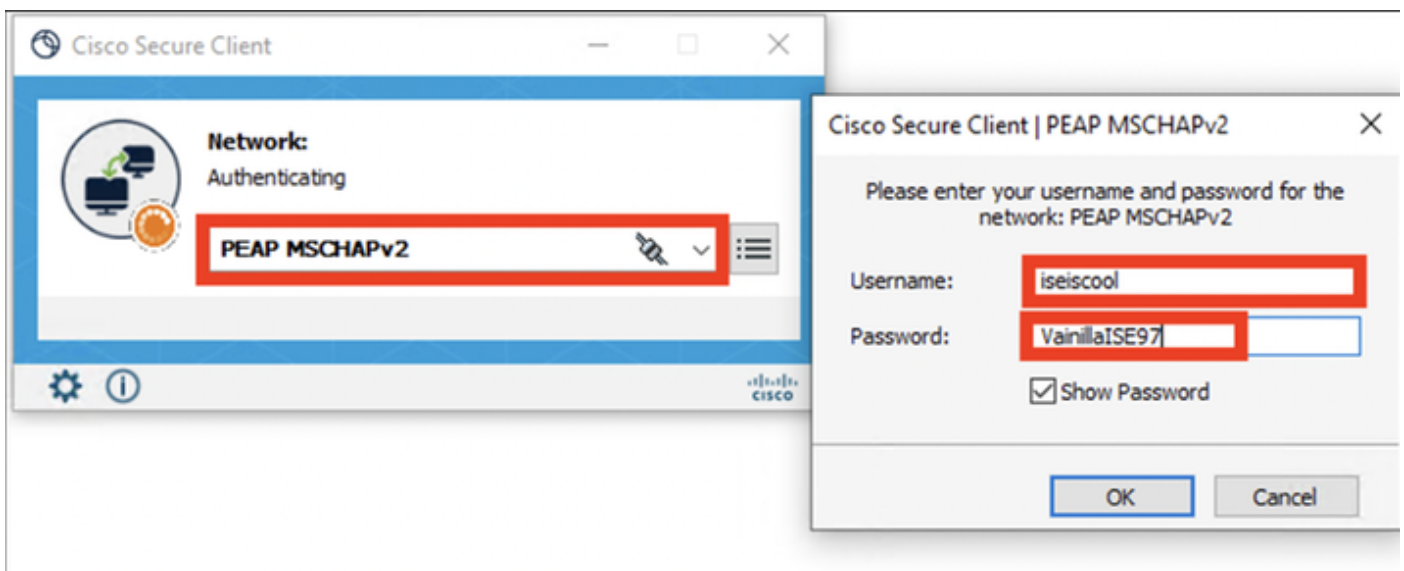
Vergunningsbeleid

Klik op Save (Opslaan).

## Verifiëren

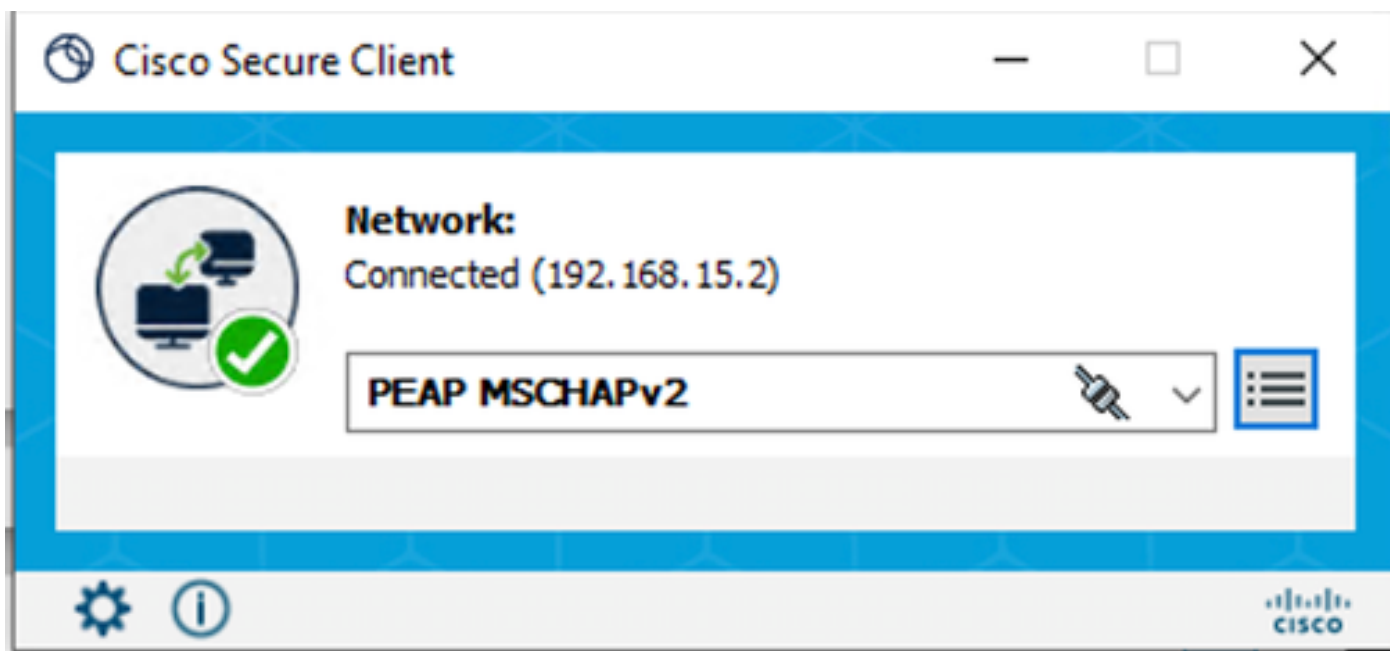
Nadat de configuratie is voltooid, wordt Secure Client gevraagd om de referenties en wordt het gebruik van het PEAP MSCHAPv2-profiel gespecificeerd.

De eerder gemaakte referenties worden ingevoerd.



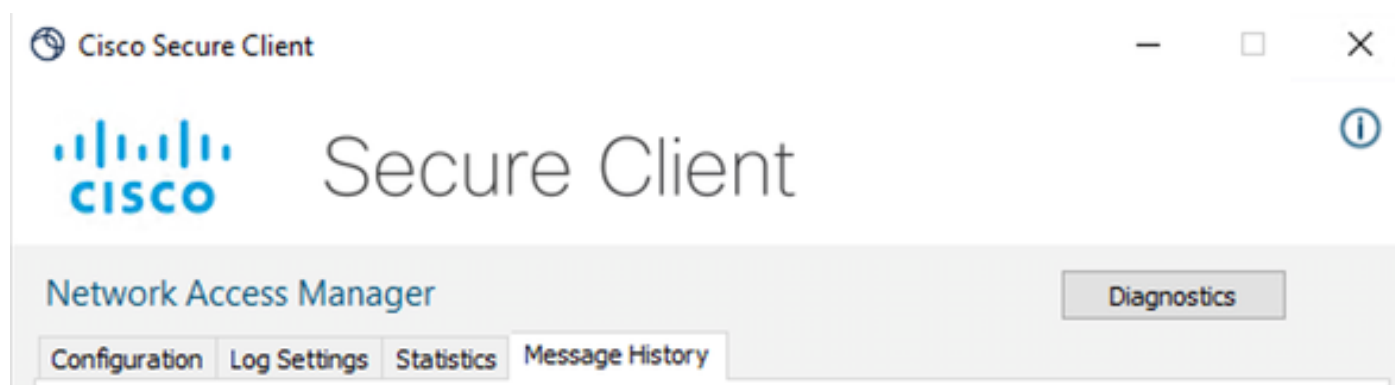
Secure-clientnaam

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

```
7:06:01 PM PEAP MSCHAPv2 : Authenticating
7:06:21 PM PEAP MSCHAPv2 : Acquiring IP Address
7:06:21 PM PEAP MSCHAPv2 : Connected
```

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.

The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are navigation tabs for 'Live Logs' and 'Live Sessions'. Below this, there are five summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (25), 'Client Stopped Responding' (0), and 'Repeat Counter' (0). Below the cards, there are controls for 'Refresh' (Never), 'Show' (Latest 20 records), and 'Within' (Last 5 minutes). A table below shows the live logs with columns: Time, Status, Details, Repea..., Identity, Endpoint ID, Endpoint..., Authentication Policy, Authorization Policy, Authoriz..., IP Address, and Network De... The table contains two rows of log entries. At the bottom, it says 'Last Updated: Tue Apr 23 2024 13:02:14 GMT-0600 (Central Standard Time)' and 'Records Shown: 2'.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Authoriz...	IP Address	Network De...
Apr 23, 2024 06:38:07.0...	●		0	isetscool	8C:16:45:00:F4...	Unknown	Wired >> Internal Authentication	Wired >> Internal ISE Users	PermitAcc...		
Apr 23, 2024 06:38:06.8...	■			isetscool	8C:16:45:00:F4...	Unknown	Wired >> Internal Authentication	Wired >> Internal ISE Users	PermitAcc...		ISR1100

ISE RADIUS live logs

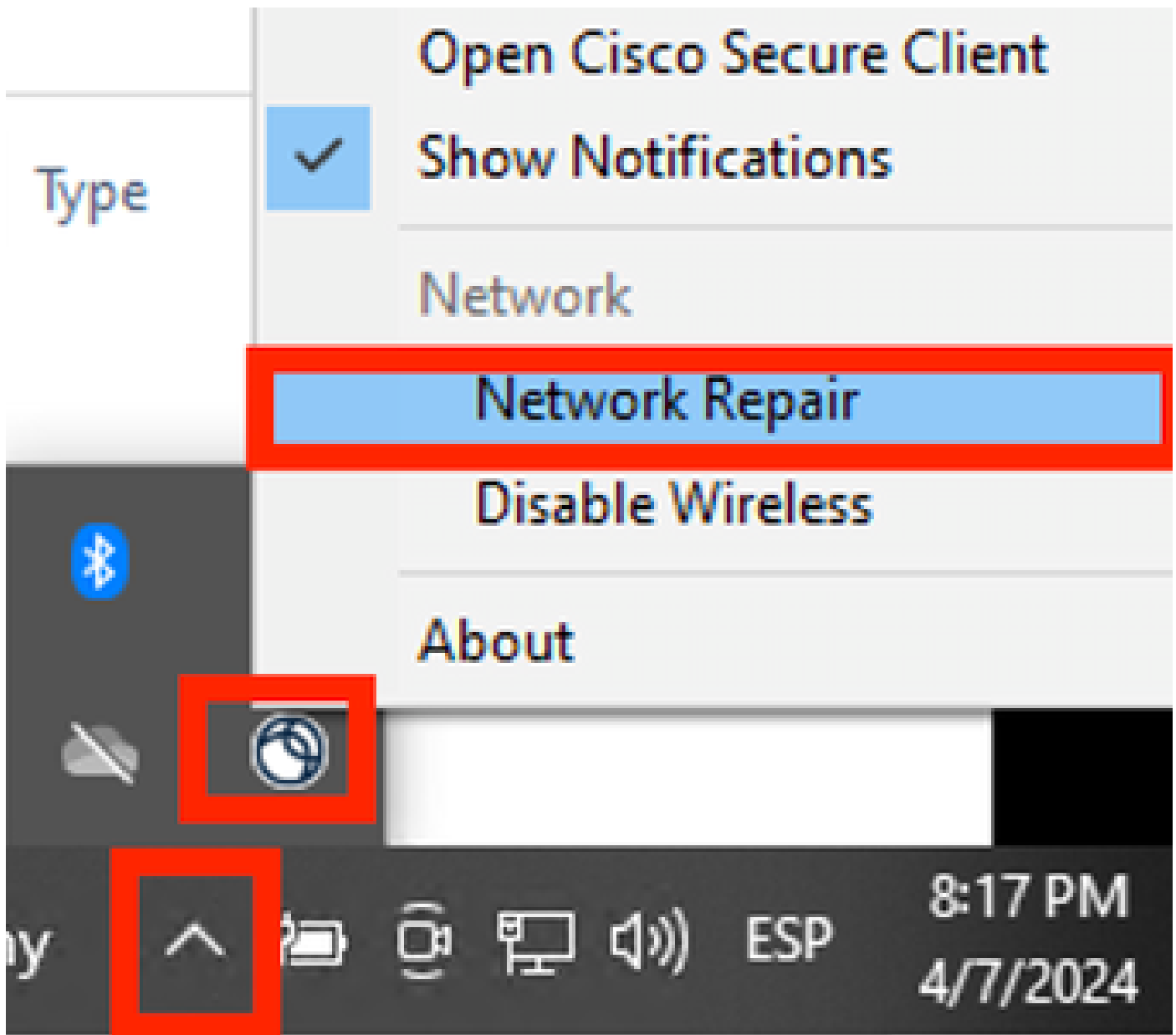
Aangezien u kunt zien dat het de juiste beleidsregels raakt en het resultaat een succesvolle verificatiestatus is, wordt geconcludeerd dat de configuratie correct is.

## 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.

Cisco Secure Client

Secure Client

Network Access Manager

Configuration Log Settings Statistics Message History

Diagnostics

Use extended logging to collect additional information about product operations.

Enable Extended Logging

IHV: Off

Filter Driver: Off

Credential Provider

Packet Capture

Maximum Packet Capture File Size (MB): 100

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 clientpijlje.

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



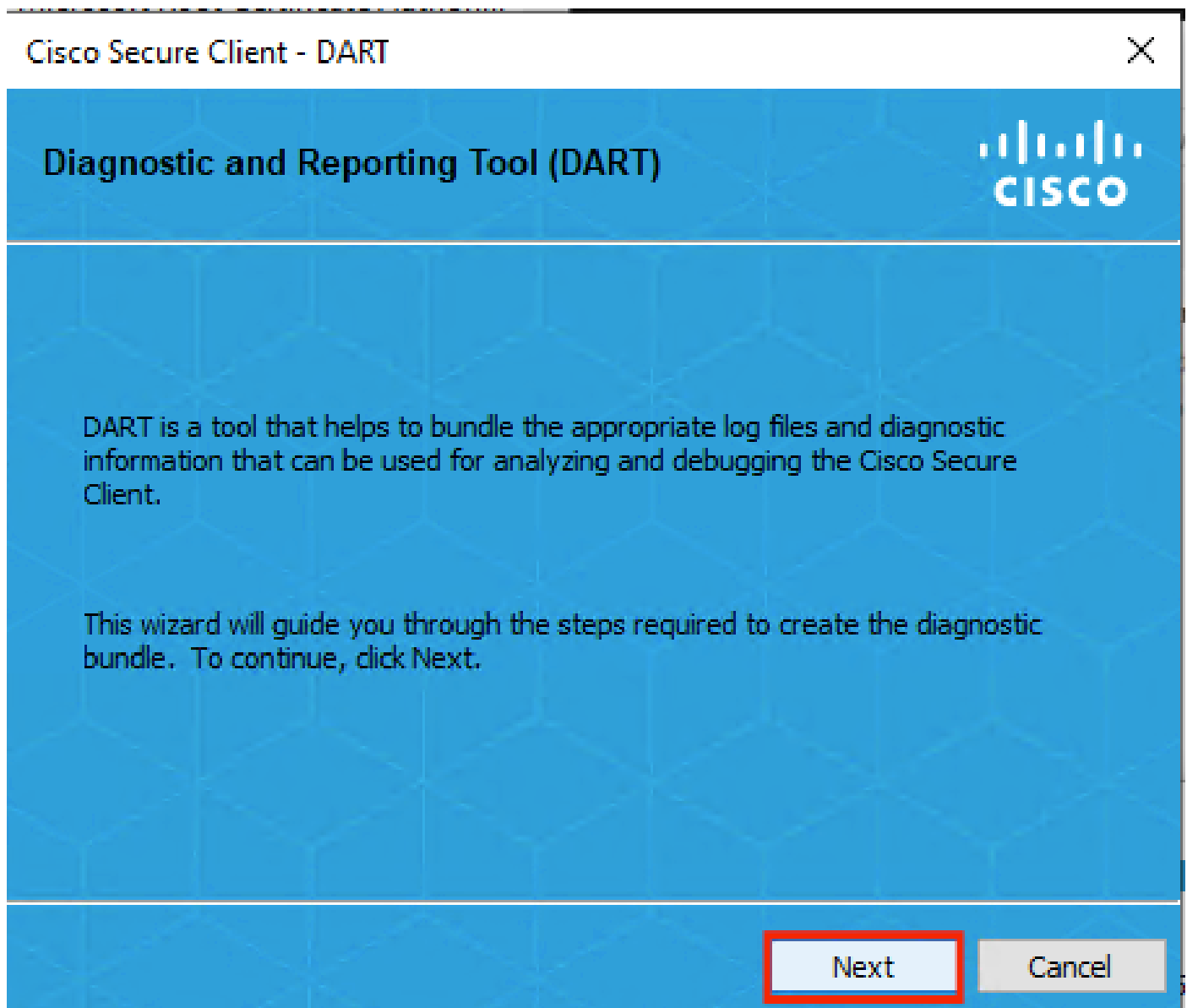
# Cisco Secure Client Diagnostics and Reporting Tool

App

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.

Cisco Secure Client - DART




**Bundle Creation Option** 

Select "Default" to include the typical log files and diagnostic information in the bundle. Select "Custom" to choose the list of log files and diagnostic information to be included in the bundle.

Default - Bundle will be saved to Desktop

Custom

 DART requires administrative privileges to clear Cisco Secure Client logs.

[Clear All Logs](#)

[Back](#) [Next](#) [Cancel](#)

DART-module

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





## Bundle Encryption Option



Enable Bundle Encryption

Mask Password

Encryption Password

Confirm Password

Back

Next

Cancel

DART-module

DART-logboekverzameling start.

Bundle Creation Progress

Processing Application logs...

Progress bar showing approximately 10% completion (green segment).

Finish Cancel

DART-logverzameling

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


**Bundle Creation Result**

The bundle was created successfully in C:\Users\LAB5\Desktop\DARTBundle\_0423\_1538.zip.

[Email Bundle](#)[Finish](#)

Resultaat van maken DART-bundel

Het DART-resultaatbestand vindt u in de desktopmap.

Name	Date modified	Type
 DARTBundle_0423_1538	4/24/2024 1:14 PM	Compressed (zipped) Folder

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.