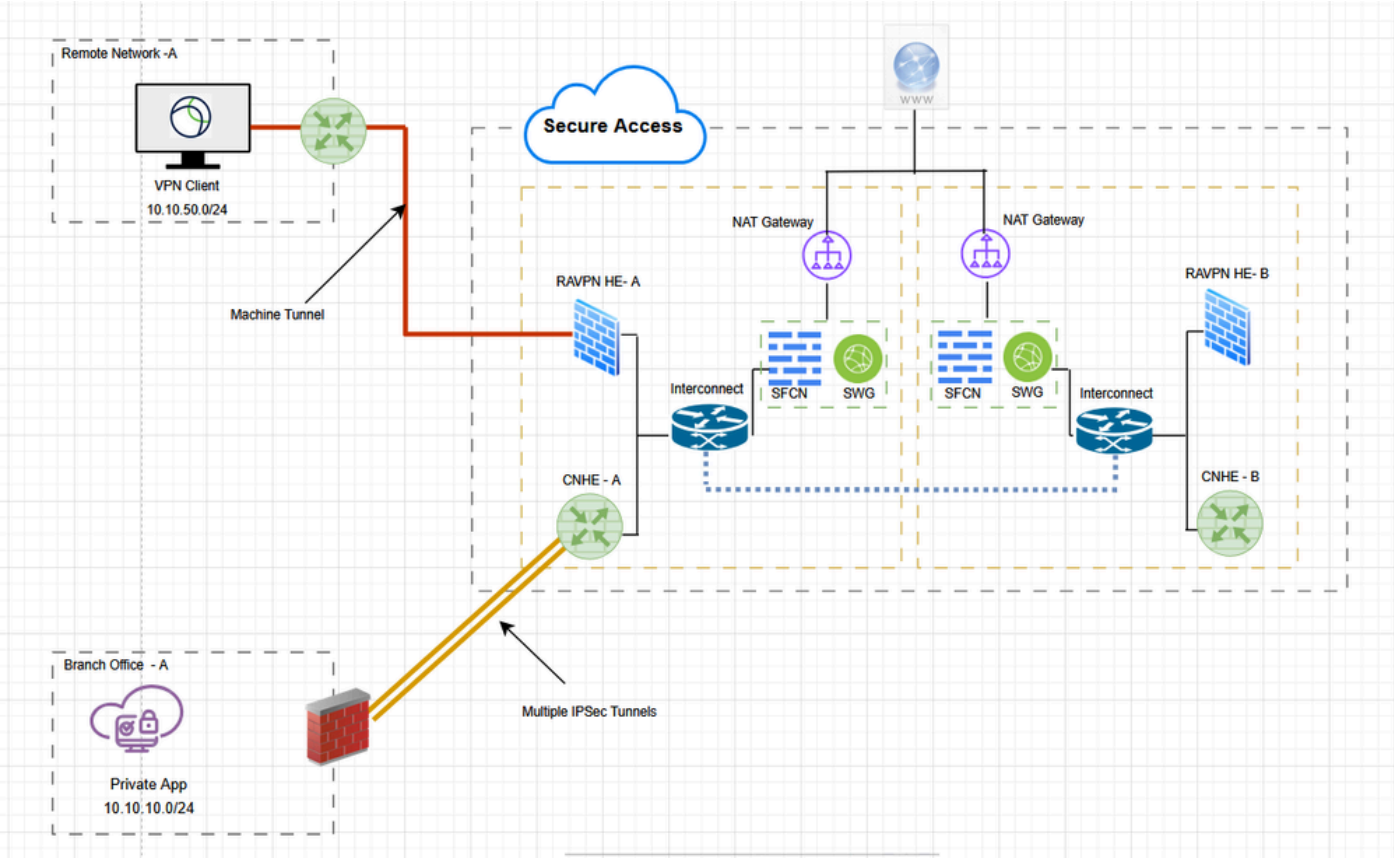
Machinetunnel configureren op Cisco Secure Access

Inhoud

Inleiding

In dit document wordt beschreven hoe u Secure Access kunt configureren als de VPN-gateway en hoe u verbindingen kunt accepteren van de Secure Client via de VPN-machinetunnel.

Netwerkdiagram



Voorwaarden

- Volledige beheerdersrol in beveiligde toegang.
- Minstens één VPN-gebruikersprofiel geconfigureerd voor Cisco Secure Access
- IP-pool van gebruiker op Cisco Secure Access

Vereisten

Het is aan te raden om kennis te hebben van deze onderwerpen:

- 509 Certificaten
- OpenSSL

Gebruikte componenten

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

- Cisco Secure Access
- Cisco Secure Client 5.1.10
- Windows 11
- Windows Server 2019 - CA

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

Een Secure Access VPN-machinetunnel zorgt voor connectiviteit met het bedrijfsnetwerk wanneer het clientsysteem wordt ingeschakeld, niet alleen wanneer de eindgebruiker een VPN-verbinding tot stand brengt. U kunt patchbeheer uitvoeren op externe eindpunten, met name apparaten die zelden door de gebruiker via VPN met het kantoornetwerk zijn verbonden. Endpoint OS-aanmeldingsscripts waarvoor netwerkconnectiviteit van het bedrijf vereist is, profiteren ook van deze functie. Om deze tunnel zonder gebruikersinteractie te maken, wordt op certificaten gebaseerde authenticatie gebruikt.

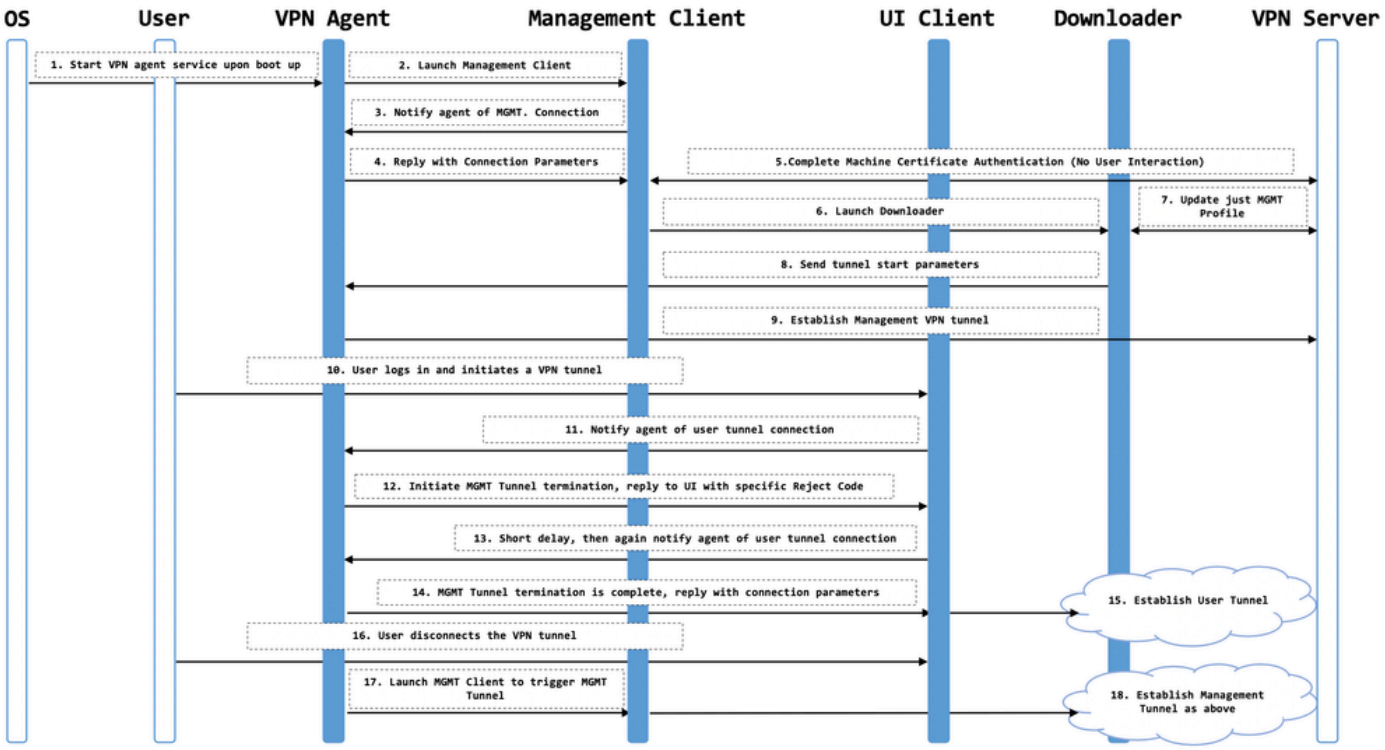
De Secure Access-machinetunnel stelt beheerders in staat om de Cisco Secure Client zonder tussenkomst van de gebruiker te laten aansluiten voordat de gebruiker zich aanmeldt. De Secure Access-machinetunnel wordt geactiveerd wanneer het eindpunt buiten het bedrijf is en de verbinding met een door de gebruiker geïnitieerde VPN is verbroken. De Secure Access VPN-machinetunnel is transparant voor de eindgebruiker en verbreekt automatisch de verbinding wanneer de gebruiker VPN start.

Werken bij Machine Tunnel

De Secure Client VPN-agentservice wordt automatisch gestart bij het opstarten van het systeem. De Secure Client VPN-agent gebruikt het VPN-profiel om te detecteren dat de functie Machinetunnel is ingeschakeld. Als de functie Machinetunnel is ingeschakeld, start de agent de beheerclienttoepassing om een verbinding met de Machinetunnel te starten. De beheerclienttoepassing gebruikt de hostvermelding van het VPN-profiel om de verbinding te starten. Vervolgens wordt de VPN-tunnel zoals gewoonlijk ingesteld, met één uitzondering: er wordt geen software-update uitgevoerd tijdens een verbinding met een machinetunnel, omdat de machinetunnel bedoeld is om transparant te zijn voor de gebruiker.

De gebruiker initieert een VPN-tunnel via de Secure Client, die de beëindiging van de machinetunnel activeert. Na beëindiging van de machinetunnel gaat de gebruikstunnel verder zoals gebruikelijk.

De gebruiker verbreekt de VPN-tunnel, waardoor de automatische herstelling van de machinetunnel wordt geactiveerd.



Beperkingen

- Gebruikersinteractie wordt niet ondersteund.
- Verificatie op basis van certificaten via Machine Certificate Store (Windows) wordt alleen ondersteund.
- Strenge controle van servercertificaten wordt afgedwongen.
- Een private proxy wordt niet ondersteund.
- Een publieke proxy wordt niet ondersteund (de waarde van ProxyNative wordt ondersteund op platforms waar Native Proxy-instellingen niet worden opgehaald uit de browser).
- Secure Client Customization Scripts worden niet ondersteund

Configureren

Methode 1 - Machinetunnel configureren met gebruiker machine@sse.com

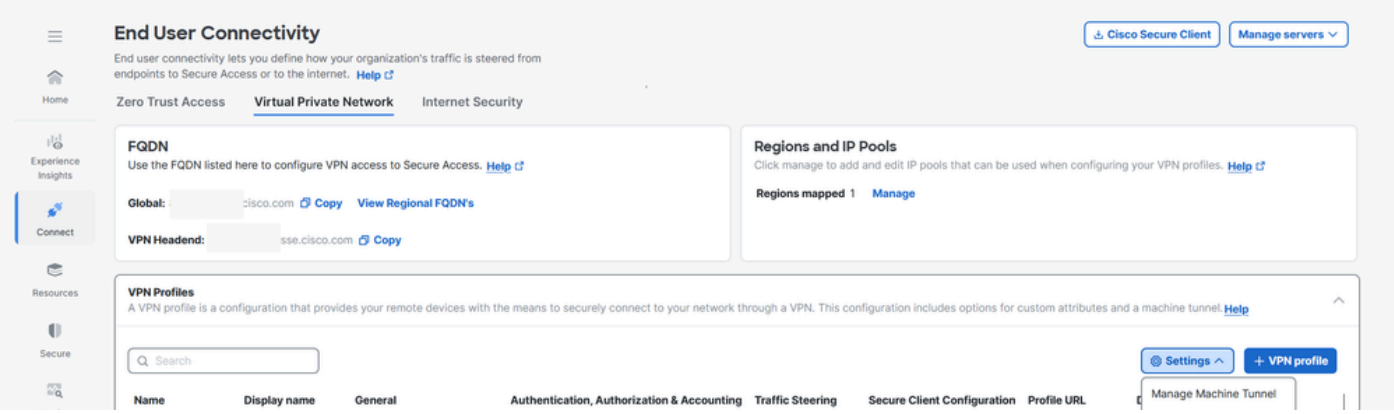
Stap 1 - Algemene instellingen

Configureer de algemene instellingen, inclusief het domein en de protocollen die deze machinetunnel gebruikt.

1. Navigeer naar Verbinden > Eindgebruikersconnectiviteit > Virtueel privé-netwerk.

2. Navigeer naar VPN-profielen en configureer de instellingen voor de machinetunnel.

    a. Klik op Instellingen en kies vervolgens Machinetunnel beheren in de vervolgkeuzelijst.

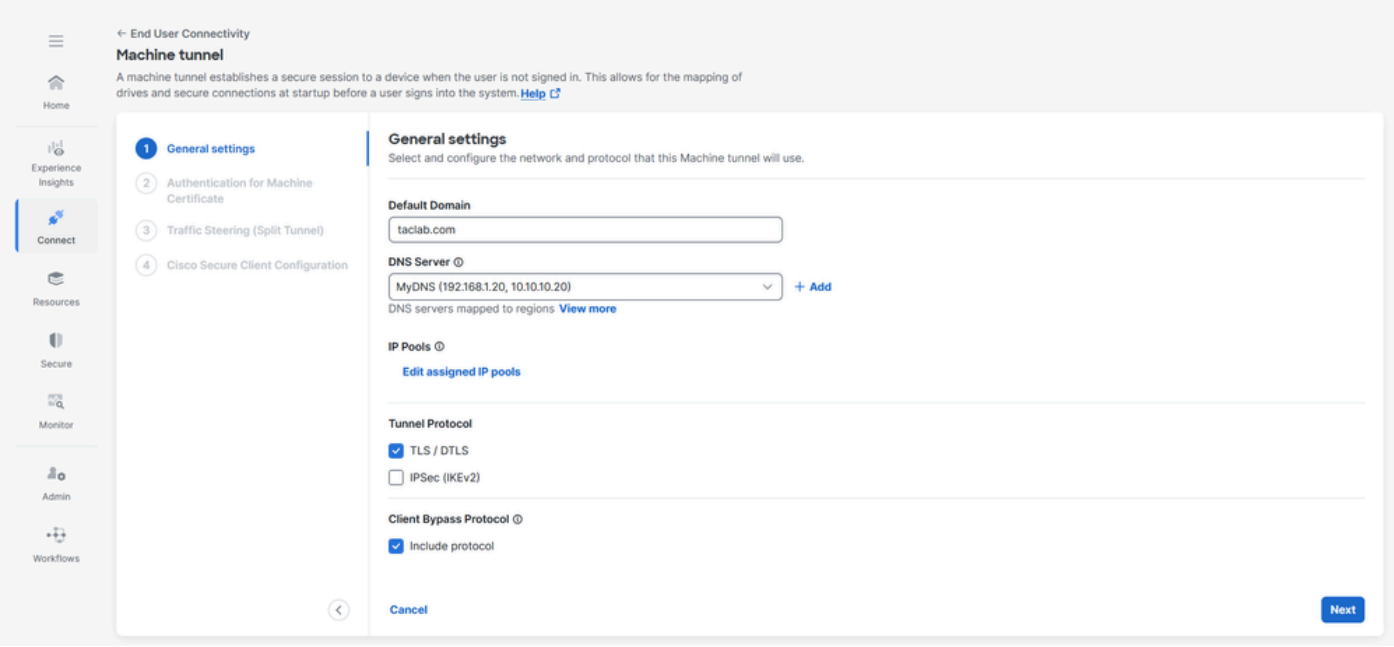


3. Voer het standaarddomein in.
4. De DNS-server die is toegewezen via de pagina Regio's en IP-groepen beheren, is ingesteld als standaardserver. U kunt de standaard DNS-server accepteren, een andere DNS-server kiezen in de vervolgkeuzelijst of op + Toevoegen klikken om een nieuw DNS-serverpaar toe te voegen. Als u een andere DNS-server selecteert of een nieuwe DNS-server toevoegt, wordt deze standaardserver overschreven.
5. Selecteer één IP-pool per regio in de vervolgkeuzelijst IP-groepen. VPN-profielen moeten ten minste één IP-pool hebben toegewezen in elke regio voor een geldige configuratie.
6. Selecteer het tunnelprotocol dat deze machinetunnel gebruikt:
   - TLS/DTLS
   - IPSec (IKEv2)

   Ten minste één protocol moet worden geselecteerd.
7. Selecteer Optioneel Inclusief protocol om het clientbypassprotocol af te dwingen.

   a. Als Client Bypass Protocol is ingeschakeld voor een IP-protocol en een adresgroep niet is geconfigureerd voor dat protocol (met andere woorden, geen IP-adres voor dat protocol is toegewezen aan de client door de ASA), wordt geen IP-verkeer met behulp van dat protocol verzonden via de VPN-tunnel. Het moet buiten de tunnel worden gebracht.

   b. Als het Client Bypass Protocol is uitgeschakeld en voor dat protocol geen adresgroep is geconfigureerd, laat de client al het verkeer voor dat IP-protocol vallen zodra de VPN-tunnel is ingesteld.



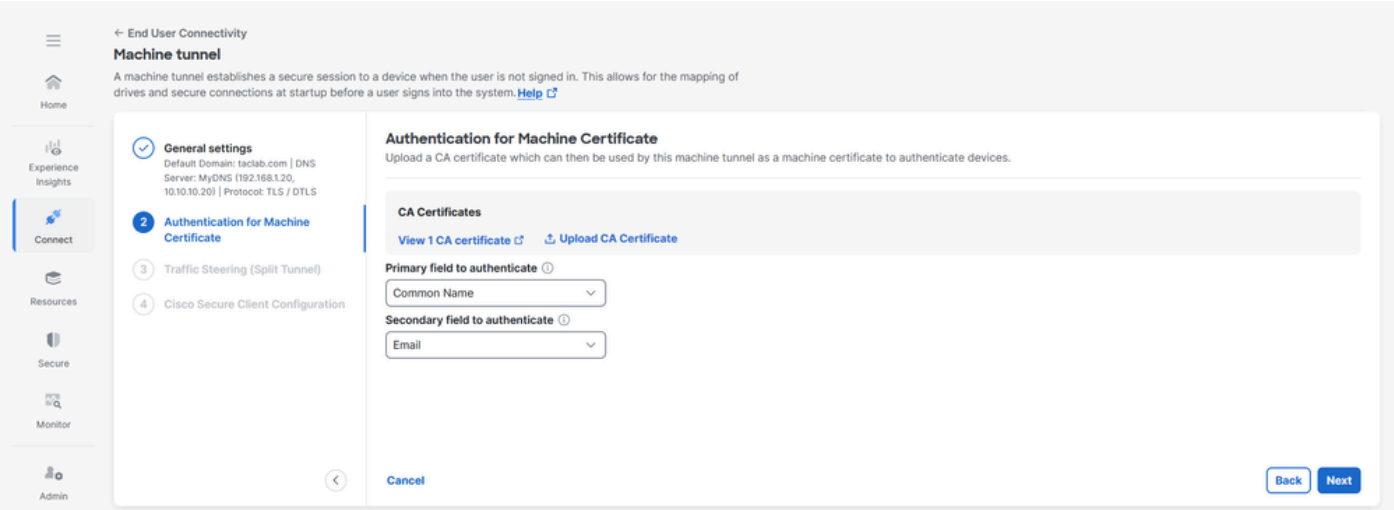
8. Klik op Volgende

Stap 2 - Verificatie voor machinecertificaat

De machinetunnel is transparant voor de eindgebruiker en verbreekt automatisch de verbinding wanneer de gebruiker een VPN-sessie start. Om deze tunnel zonder gebruikersinteractie te maken, wordt op certificaten gebaseerde authenticatie gebruikt.

1. Kies CA-certificaten in de lijst of klik op CA-certificaten uploaden

2. Selecteer de verificatievelden op basis van certificaten. Zie verificatievelden op basis van certificaten voor meer informatie



3. Klik op Volgende

Stap 3 – Verkeerssturing (splittunnel)

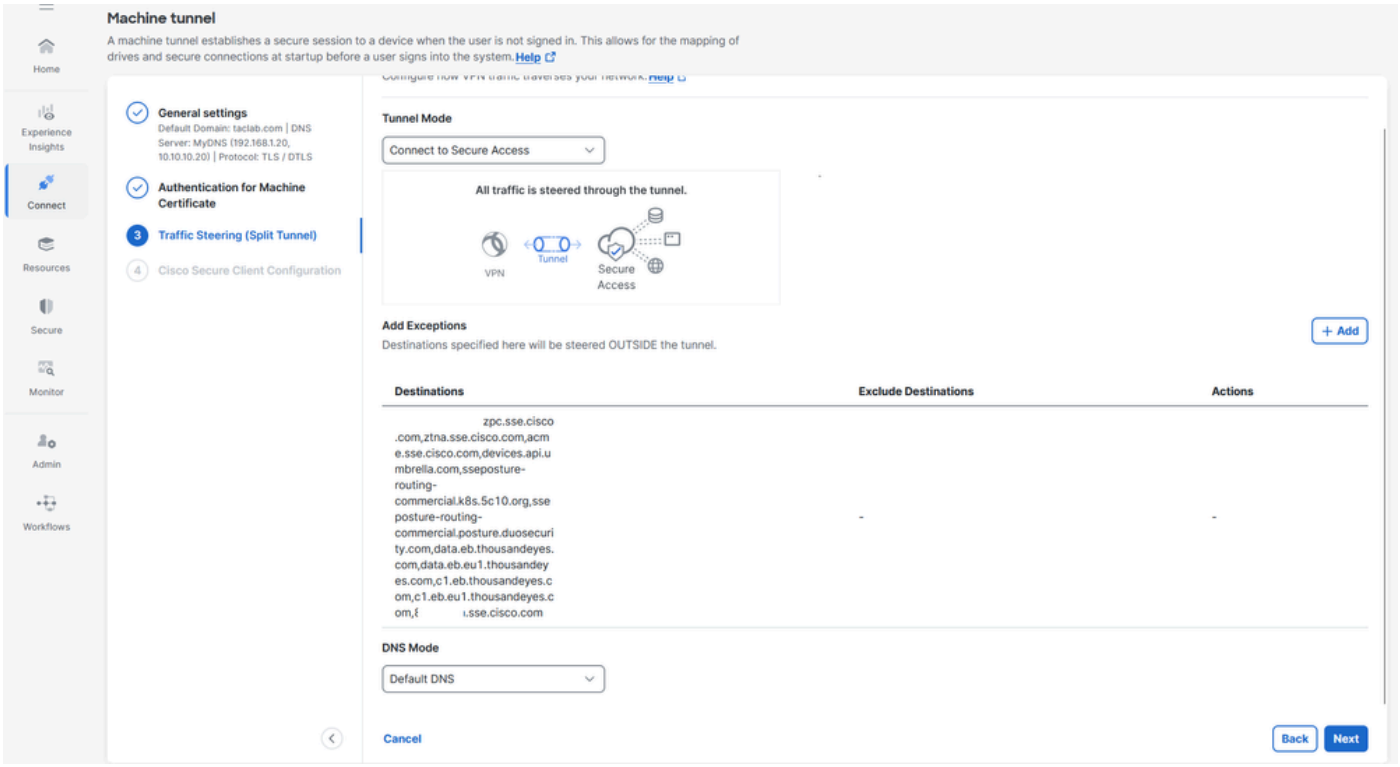
Voor Traffic Steering (Split Tunnel), kunt u een machinetunnel configureren om een volledige

tunnelverbinding met Secure Access te behouden, of configureren om een gesplitste tunnelverbinding te gebruiken om alleen verkeer door de VPN te leiden als dat nodig is.Voor meer informatie zie Machine Tunnel verkeerssturing

1. Selecteer de tunnelmodus

2. Afhankelijk van de selectie van de tunnelmodus kunt u uitzonderingen toevoegen

3. Selecteer DNS-modus

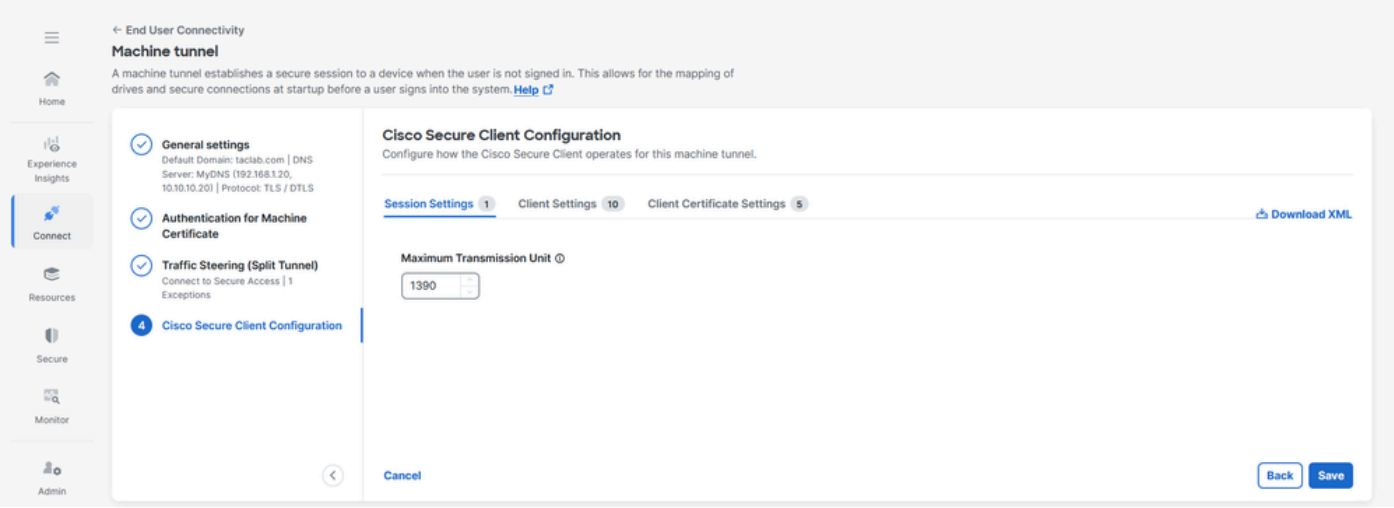


4. Klik op Volgende

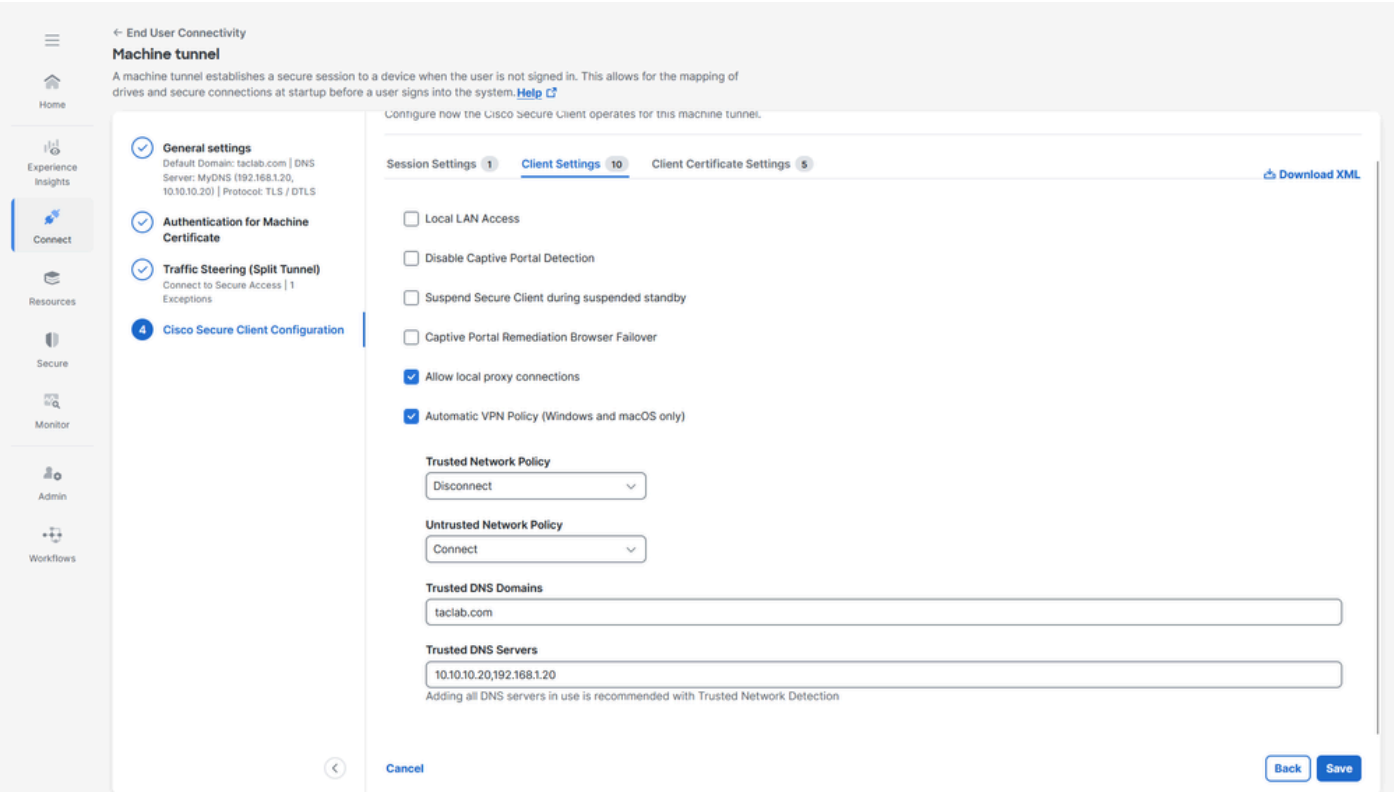
Stap 4 – Cisco Secure Client Configuration

U kunt een subset van Cisco Secure Client-instellingen wijzigen op basis van de behoeften van een bepaalde VPN-machinetunnel. Zie Beveiligde clientconfiguratie voor meer informatie

1. Verifieer de maximale transmissie-eenheid, de grootste grootte van het pakket dat zonder fragmentatie in de VPN-tunnel kan worden verzonden



2. Clientinstellingen, raadpleeg de clientinstellingen van Machine Tunnel voor meer informatie



3. Clientcertificaatinstellingen, selecteert u de desbetreffende opties

a. Windows Certificate Store Override — Hiermee kan een beheerder Secure Client opdracht geven om certificaten te gebruiken in het certificaatarchief van het Windows-systeem (Lokaal systeem) voor clientcertificaatverificatie.

b. Automatische certificaatselectie - Wanneer meerdere certificaatverificatie is geconfigureerd op de beveiligde gateway

c. Certificaatvastlegging - CA-certificaat dat door de machinetunnel kan worden gebruikt als machinecertificaat om apparaten te verifiëren

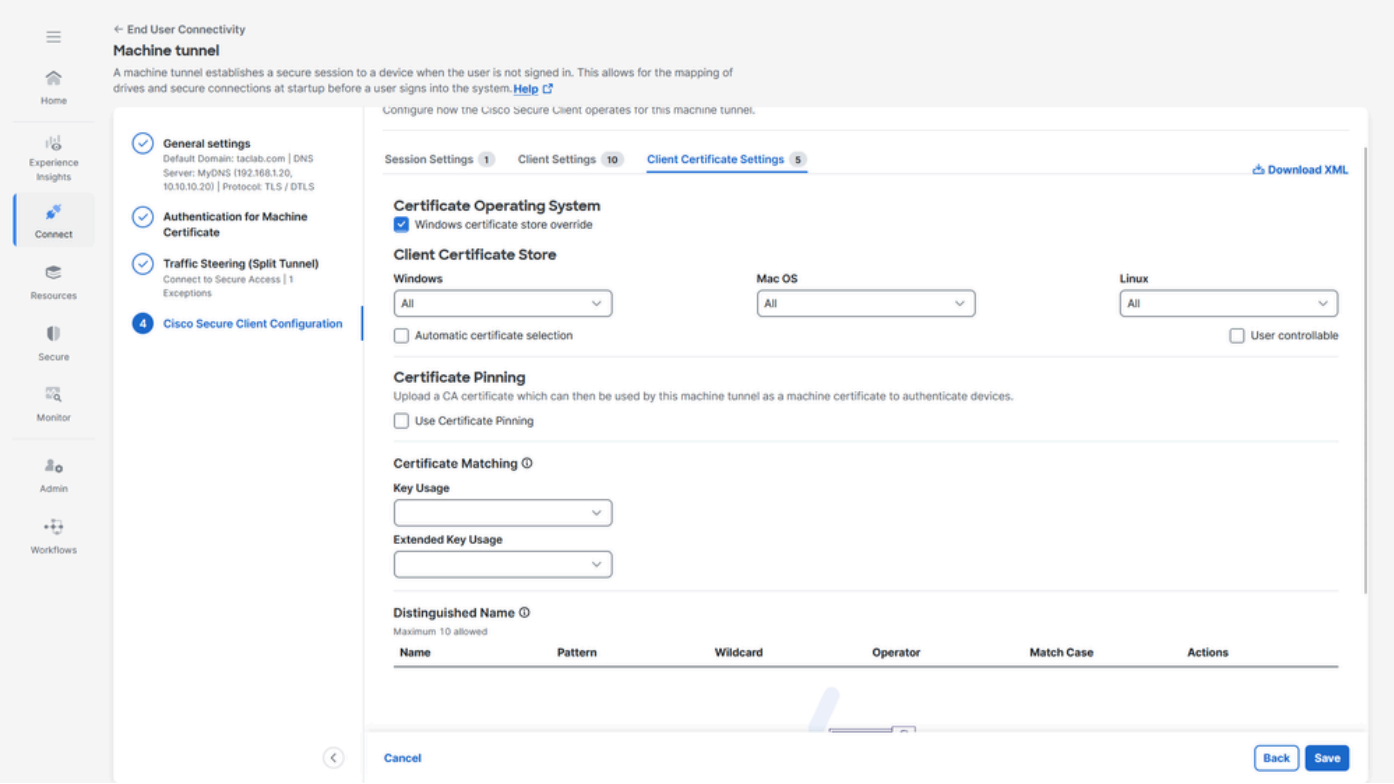
d. Overeenstemming van certificaten - Als er geen criteria voor overeenkomende certificaten

zijn opgegeven, past Cisco Secure Client de regels voor overeenkomende certificaten toe

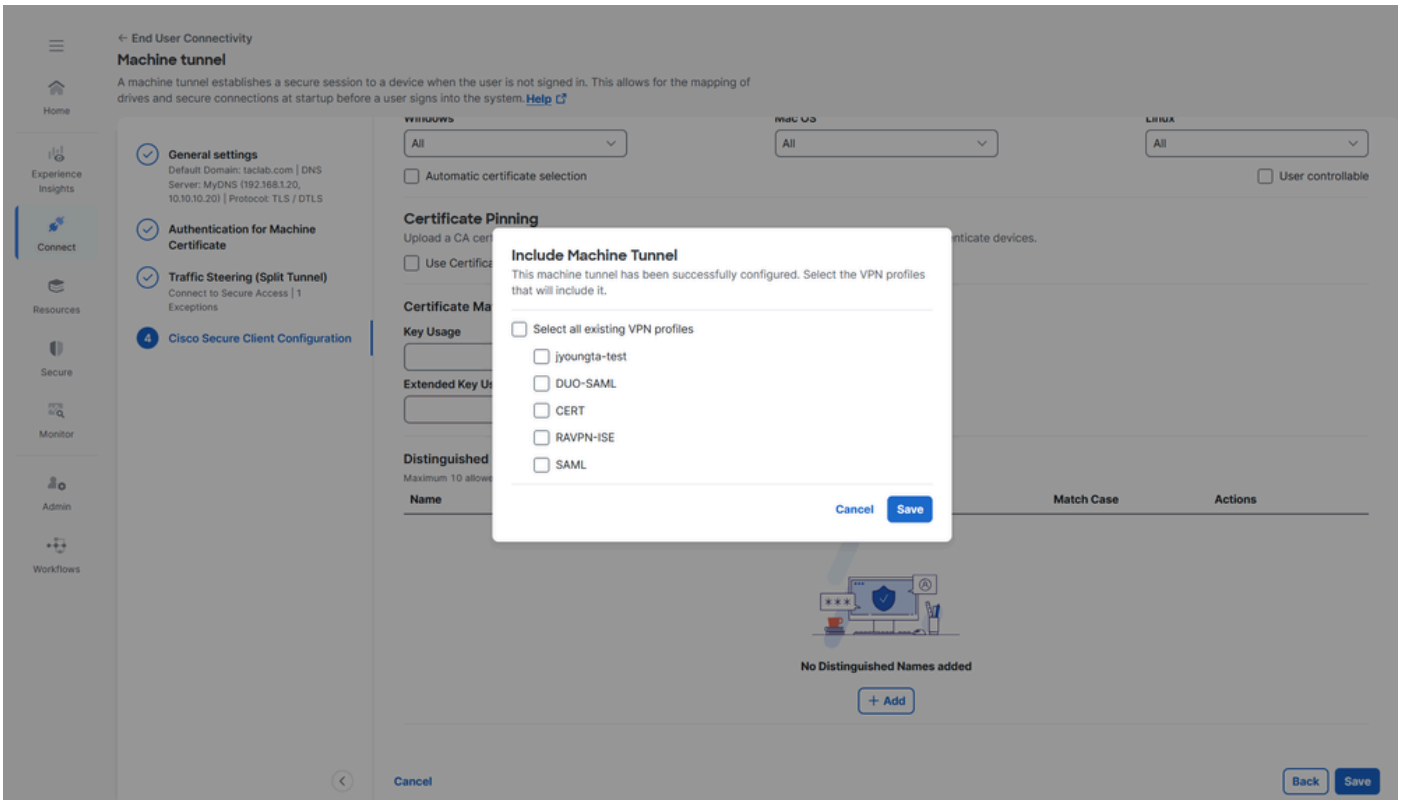
i. Hoofdgebruik: Digital_Signature

ii. Uitgebreid sleutelgebruik: clientauteur

e. Voorkeursnaam - Hiermee geeft u voorkeursnamen (DN's) op voor exacte overeenkomende criteria bij het kiezen van aanvaardbare clientcertificaten. Wanneer u meerdere Distinguished Names toevoegt, wordt elk certificaat gecontroleerd aan de hand van alle vermeldingen en moeten ze allemaal overeenkomen.

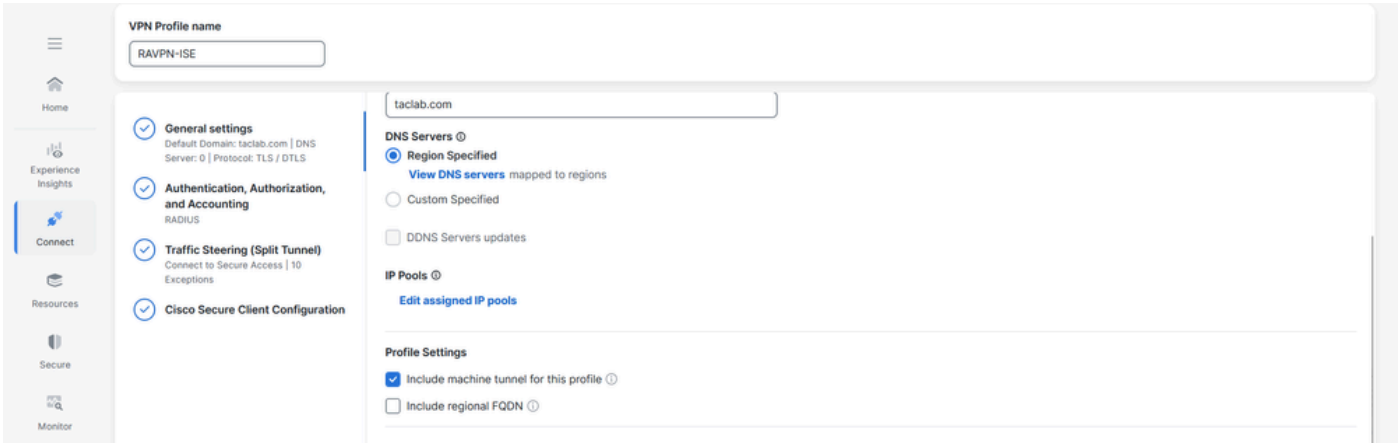


4. Wijs het Machine Tunnel profiel toe aan een User VPN profiel, klik op Opslaan en dan is er een optie om de User VPN profielen te selecteren



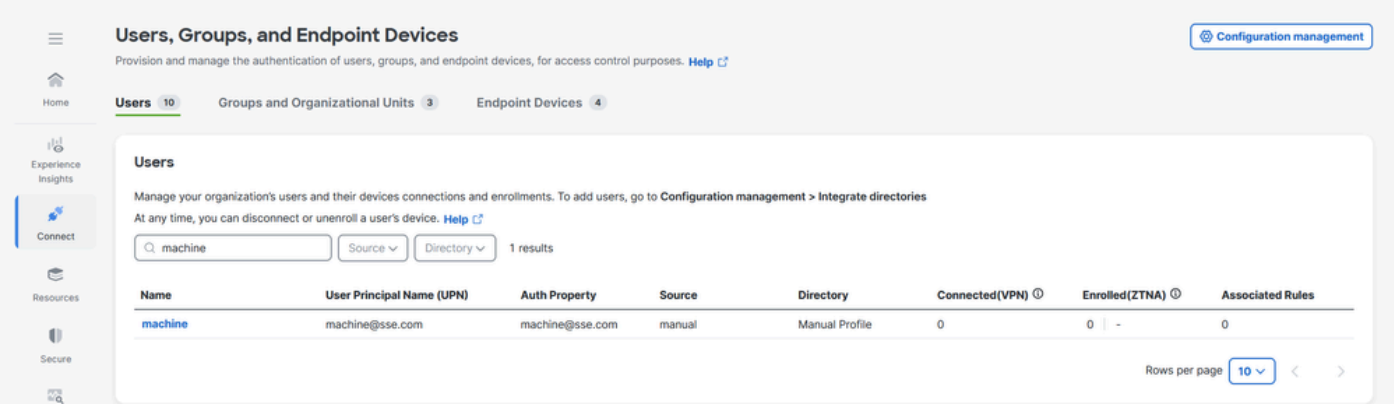
5. Klik op Opslaan

6. Controleer of het Machinetunnelprofiel is gekoppeld aan een VPN-gebruikersprofiel



Stap 5 - Controleer of de machine@sse.com-gebruiker aanwezig is in de Cisco Secure Access

1. Navigeer naar Verbinden > Gebruikers, groepen en eindpuntapparaten > Gebruikers



2. Als de gebruiker van machine@sse.com niet handmatig aanwezig is bij het importeren. Zie Handmatig gebruikers en groepen importeren voor meer informatie

Stap 6 - Een CA-ondertekend certificaat genereren voor machine@sse.com

1. Een aanvraag voor de ondertekening van een certificaat genereren

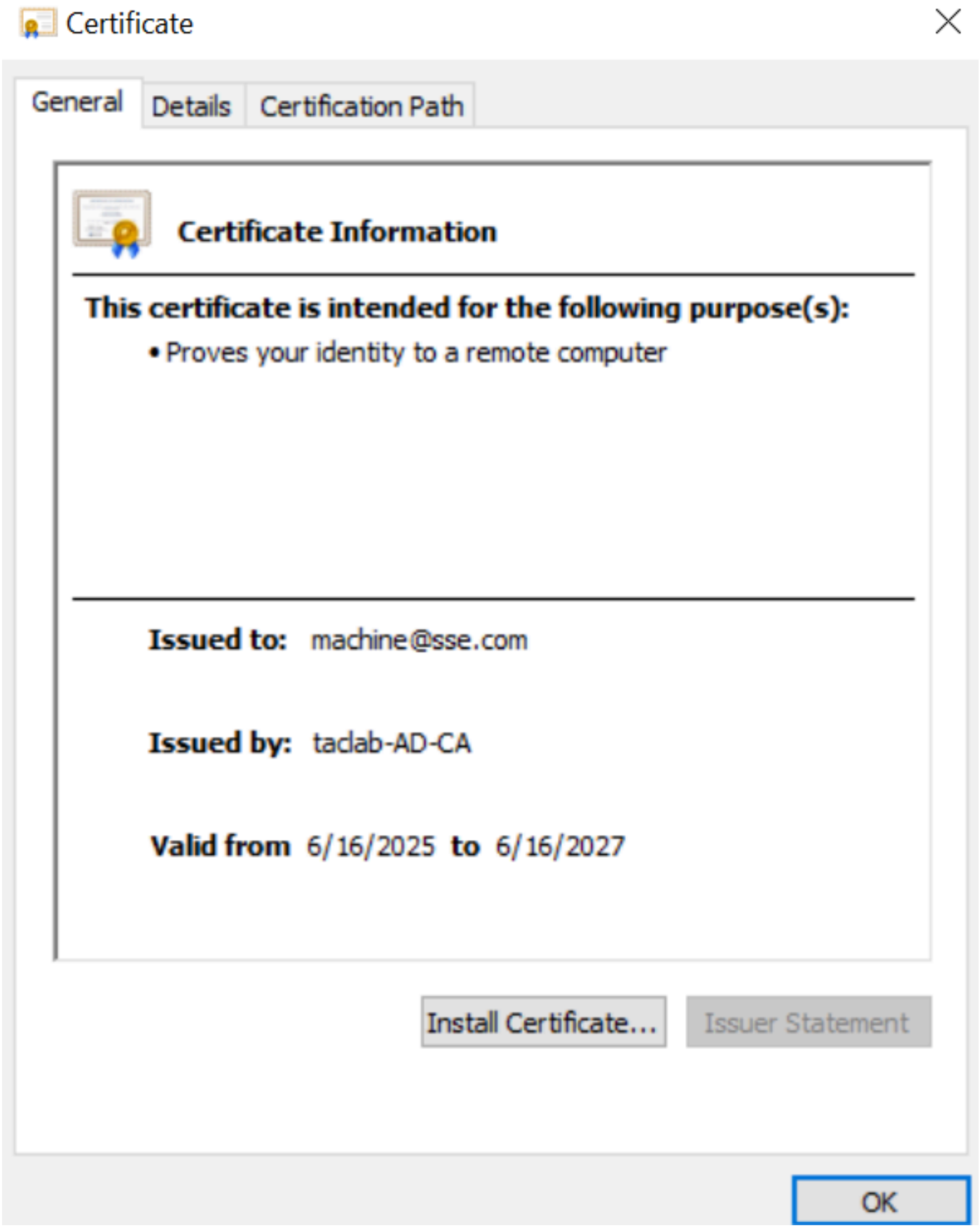
   a. We kunnen elke online CSR-generatorsoftware gebruiken CSR Generator of een openssl CLI

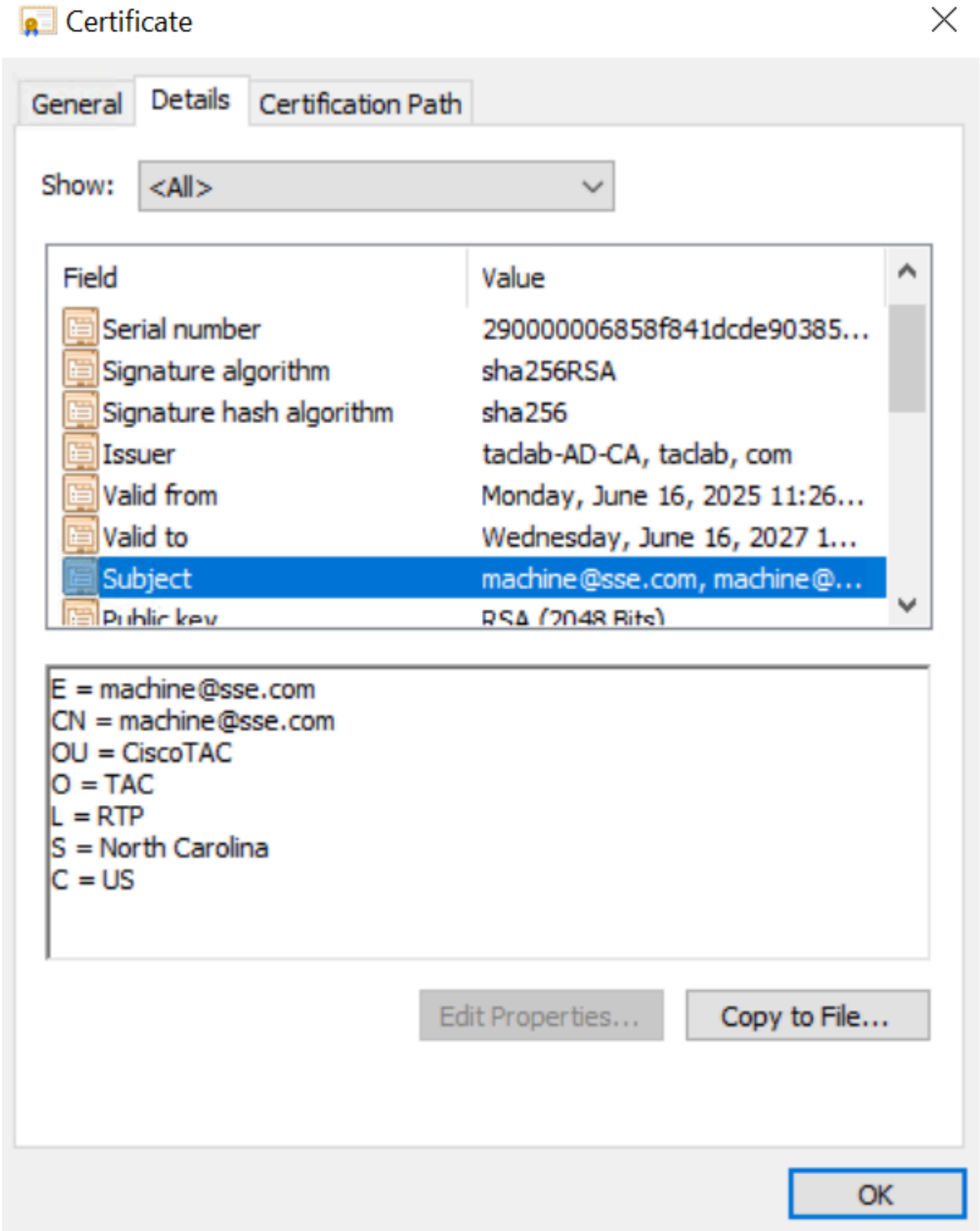
OpenSSL REQ -NewKey RSA:2048 -Nodes -Keyout CERT.Key -Out CERT.CSR

```
root@ftd1:/home/admin# openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr
Generating a RSA private key
.....................................................................................+++++
.....................................................................+++++
writing new private key to 'cert.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:North Carolina
Locality Name (eg, city) []:RTP
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TAC
Organizational Unit Name (eg, section) []:CiscoTAC
Common Name (e.g. server FQDN or YOUR name) []:machine@sse.com
Email Address []:machine@sse.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

2. Kopieer de CSR en genereer een machinecertificaat


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
Issued to: machine@sse.com
Issued by: tadab-AD-CA
Valid from 6/16/2025 to 6/16/2027
Install Certificate...
Issuer Statement
OK



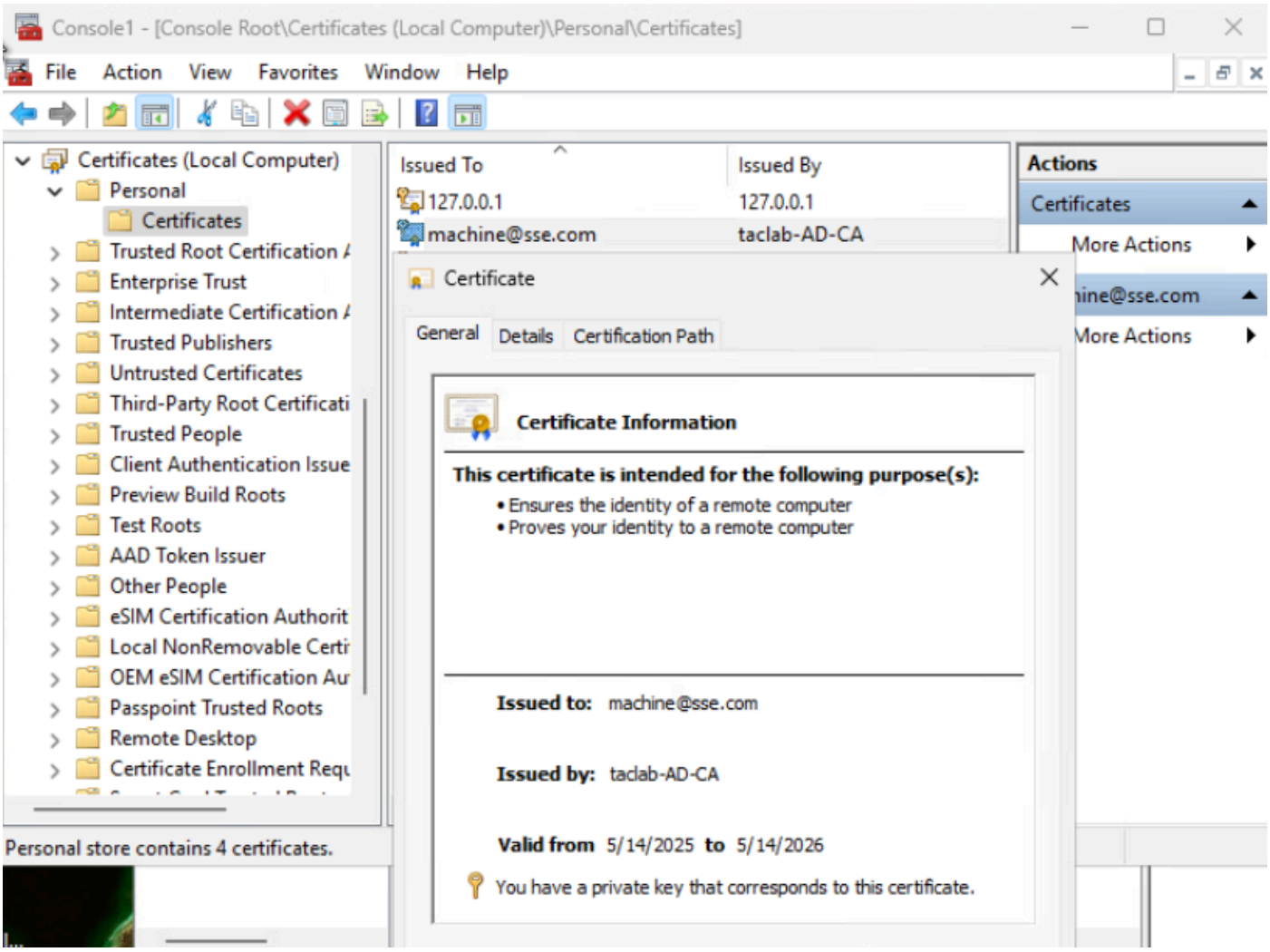
3. Converteer het machinecertificaat in PKCS12-indeling met behulp van de sleutel en cert die in de vorige stappen (stap 1 en 2) zijn gegenereerd

openssl pkcs12 -export -out Machine.p12 -in machine.crt -inkey cert.key

```
root@ftd1:/home/admin# openssl pkcs12 -export -out Machine.p12 -in machine.crt -inkey cert.key
Enter Export Password:
Verifying - Enter Export Password:
root@ftd1:/home/admin#
```

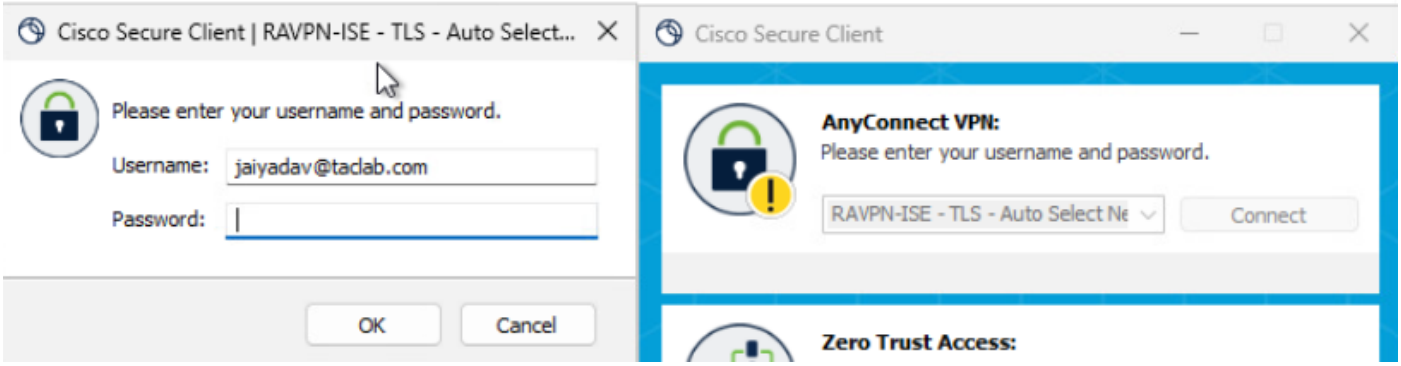
Stap 7 - Het machinecertificaat importeren op een testmachine

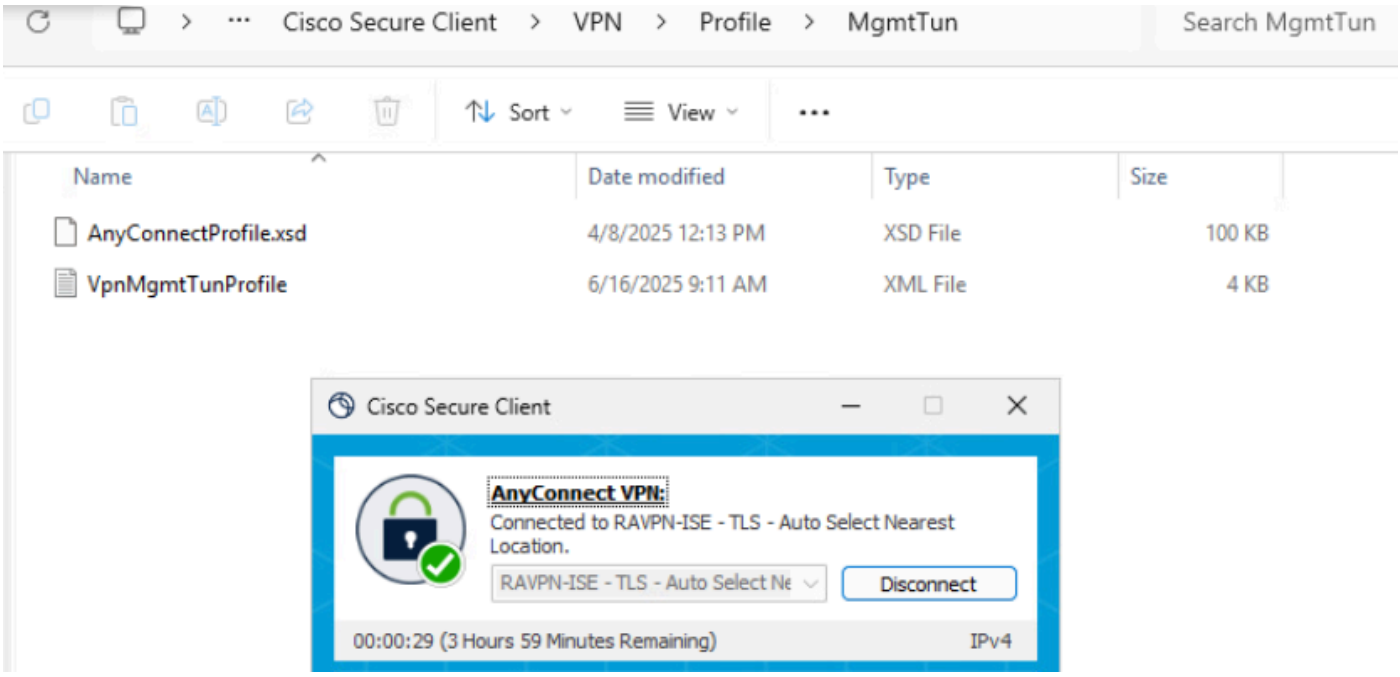
a. Importeer het PKCS12-machinecertificaat onder lokaal of machineopslag



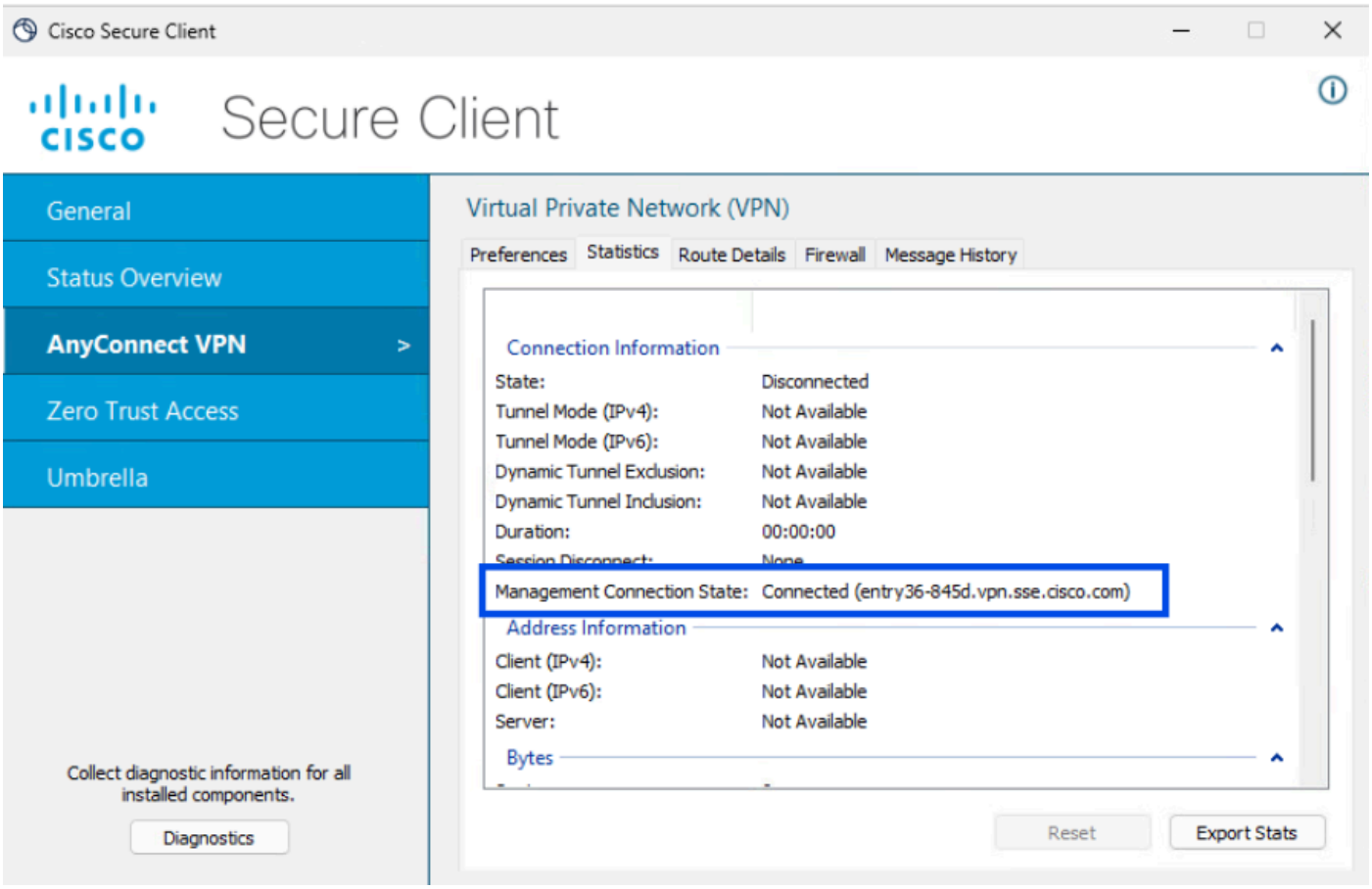
Stap 8 - Verbinding maken met de machinetunnel

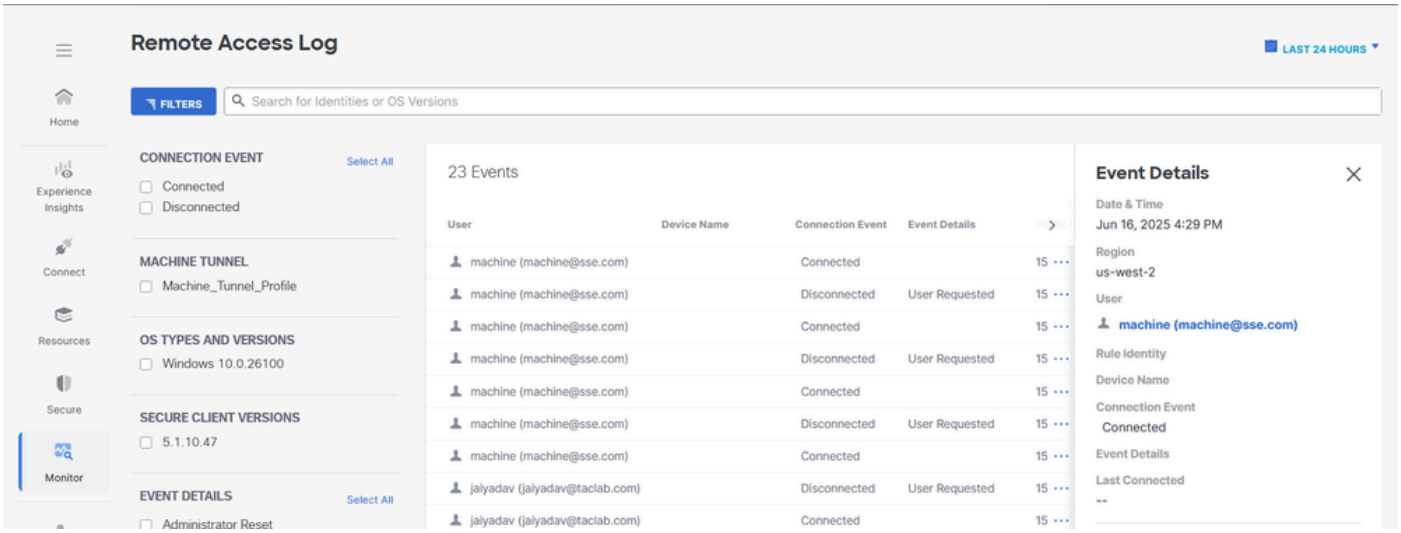
a. Verbinding maken met een gebruikerstunnel, wordt het XML-profiel van het systeem geactiveerd om te worden gedownload.





b. De connectiviteit van de machinetunnel controleren





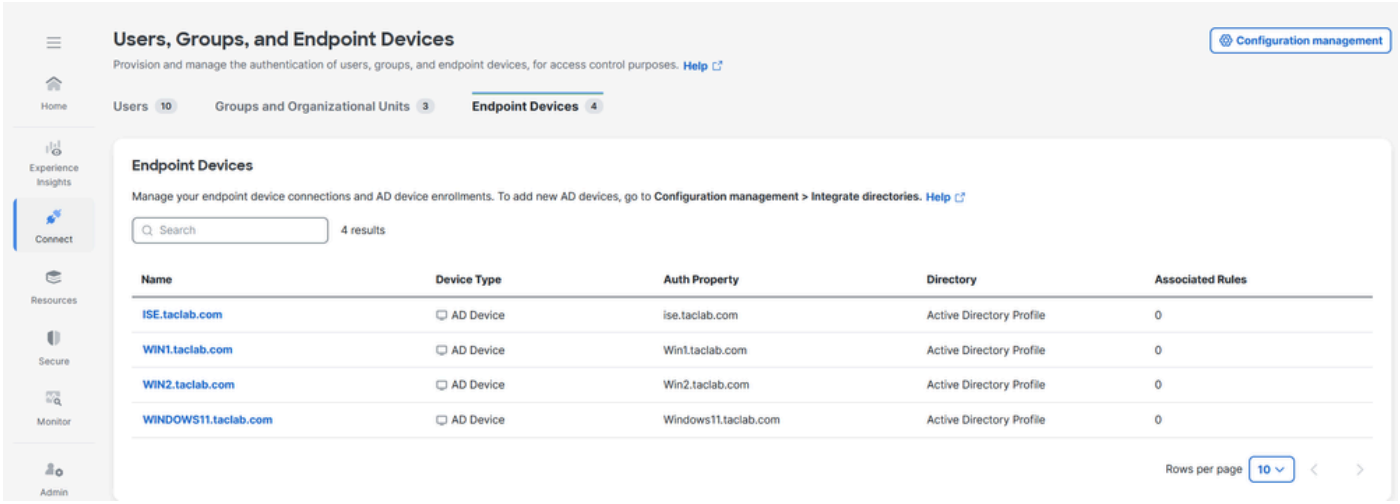
Methode 2 - Machinetunnel configureren met Eindpuntcertificaat

In dit geval kiest u het certificaatveld met de apparaatnaam (computernaam) om het primaire veld te verifiëren. Secure Access gebruikt de apparaatnaam als de machine-tunnelidentificatie. Het formaat van de computernaam moet overeenkomen met het formaat van de gekozen apparaat-id

Ga door stap 1 naar stap 4 voor machinetunnelconfiguratie

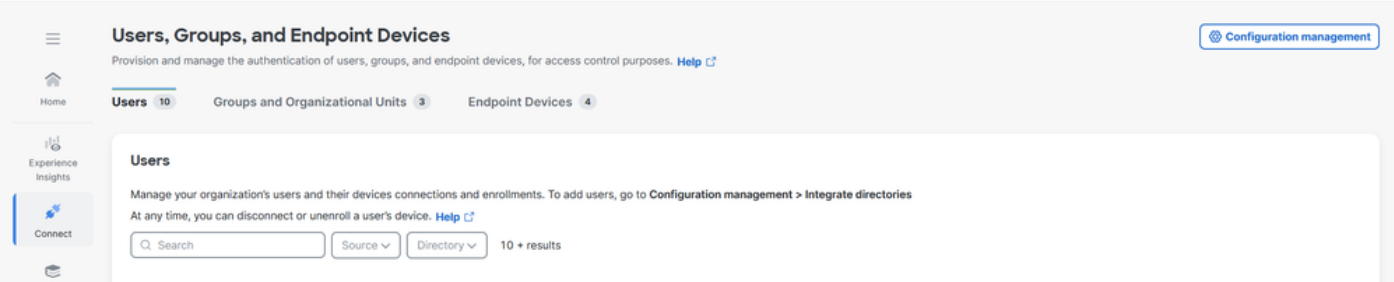
Stap 5 - AD-connector configureren om Eindpunten te kunnen importeren op de Cisco Secure Access.

Zie On-Perm Active Directory Integration voor meer informatie

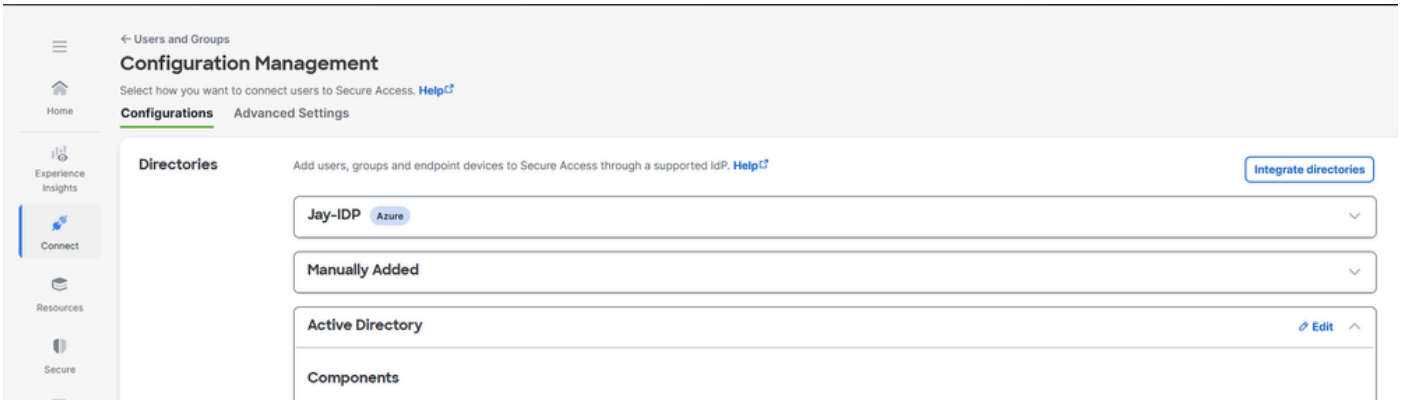


Stap 6 - Eindpuntapparaatverificatie configureren

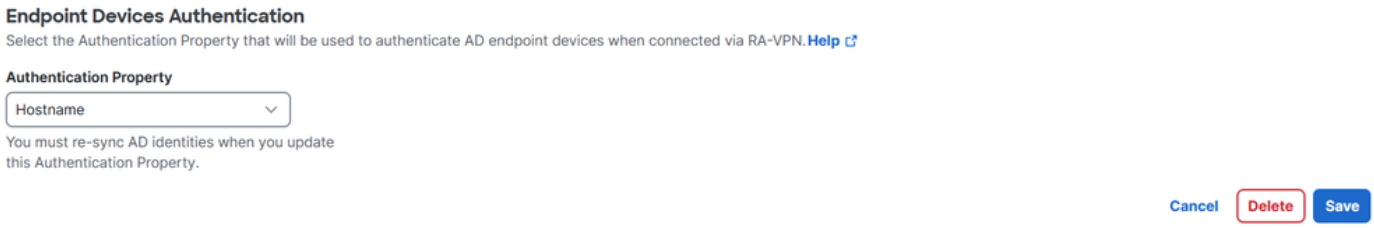
1. Navigeer naar Verbinden > Gebruikers, groepen en eindpuntapparaten.
2. Klik op Configuratiebeheer



3. Bewerk Active Directory onder Configurations



4. De eigenschap Endpoint Devices Authentication instellen op Hostname



5. Klik op Opslaan en herstart AD Connector-services op de servers waarop de adapter is geïnstalleerd

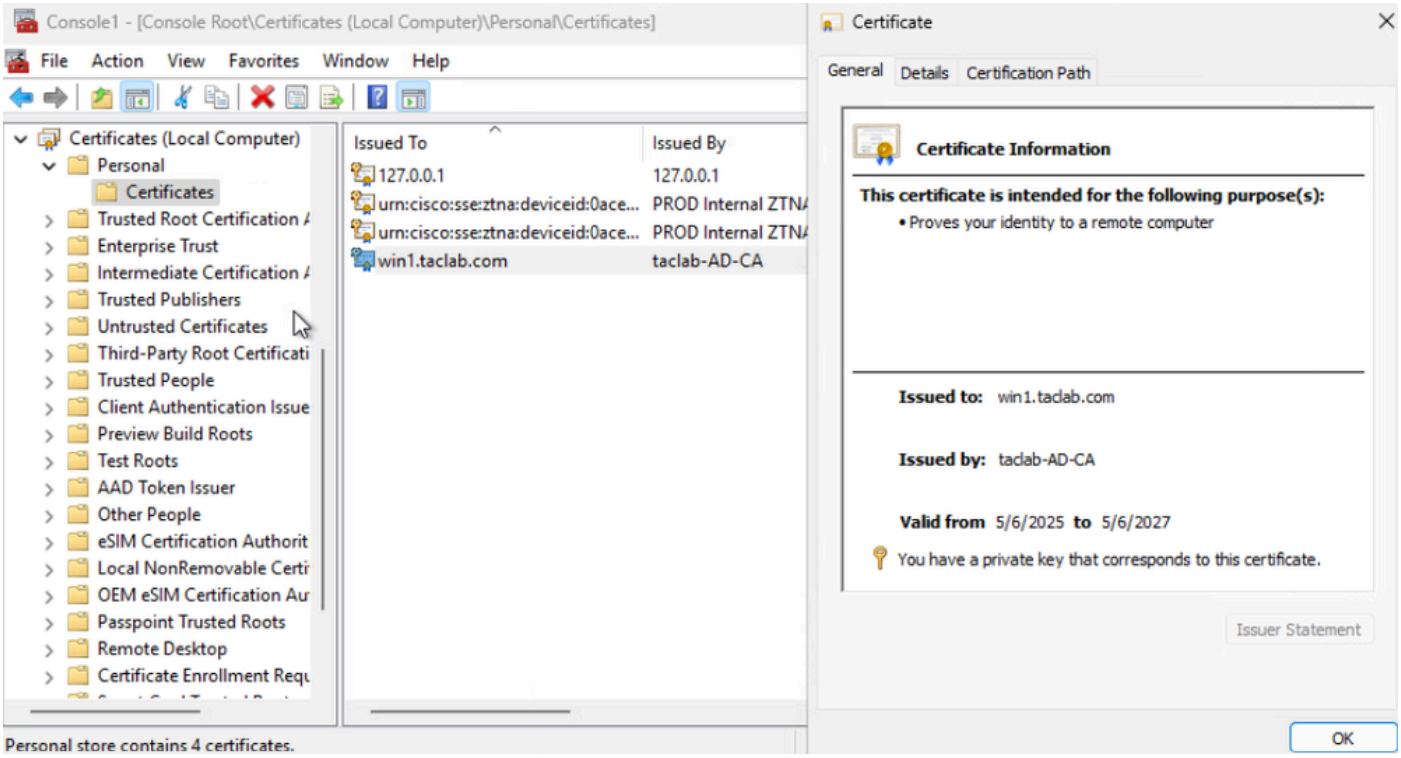
Stap 7 - Eindpuntcertificaat genereren en importeren

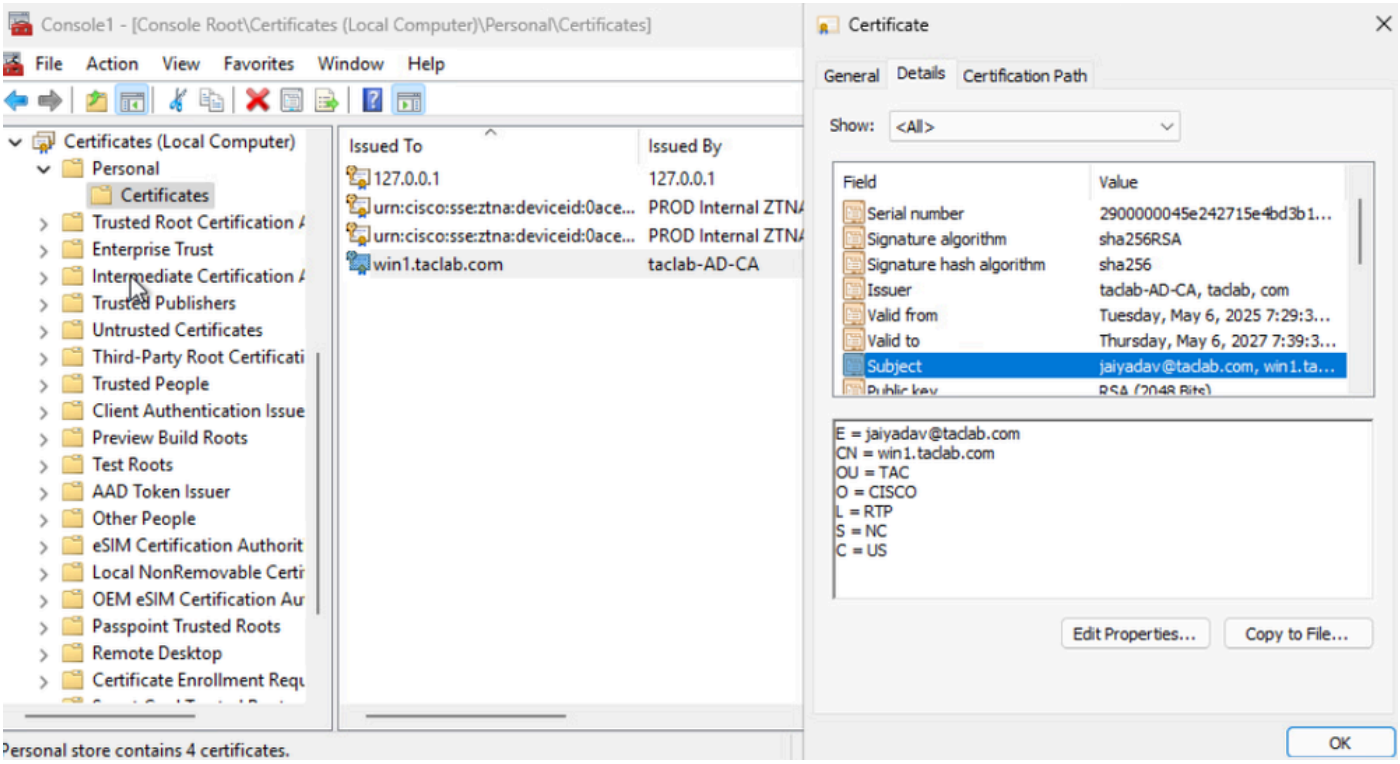
a. MVO genereren, een MVO-generator of OpenSSL-tool openen

b. Een eindpuntcertificaat genereren van CA

c. Converteer het .cert bestand naar PKCS12 formaat

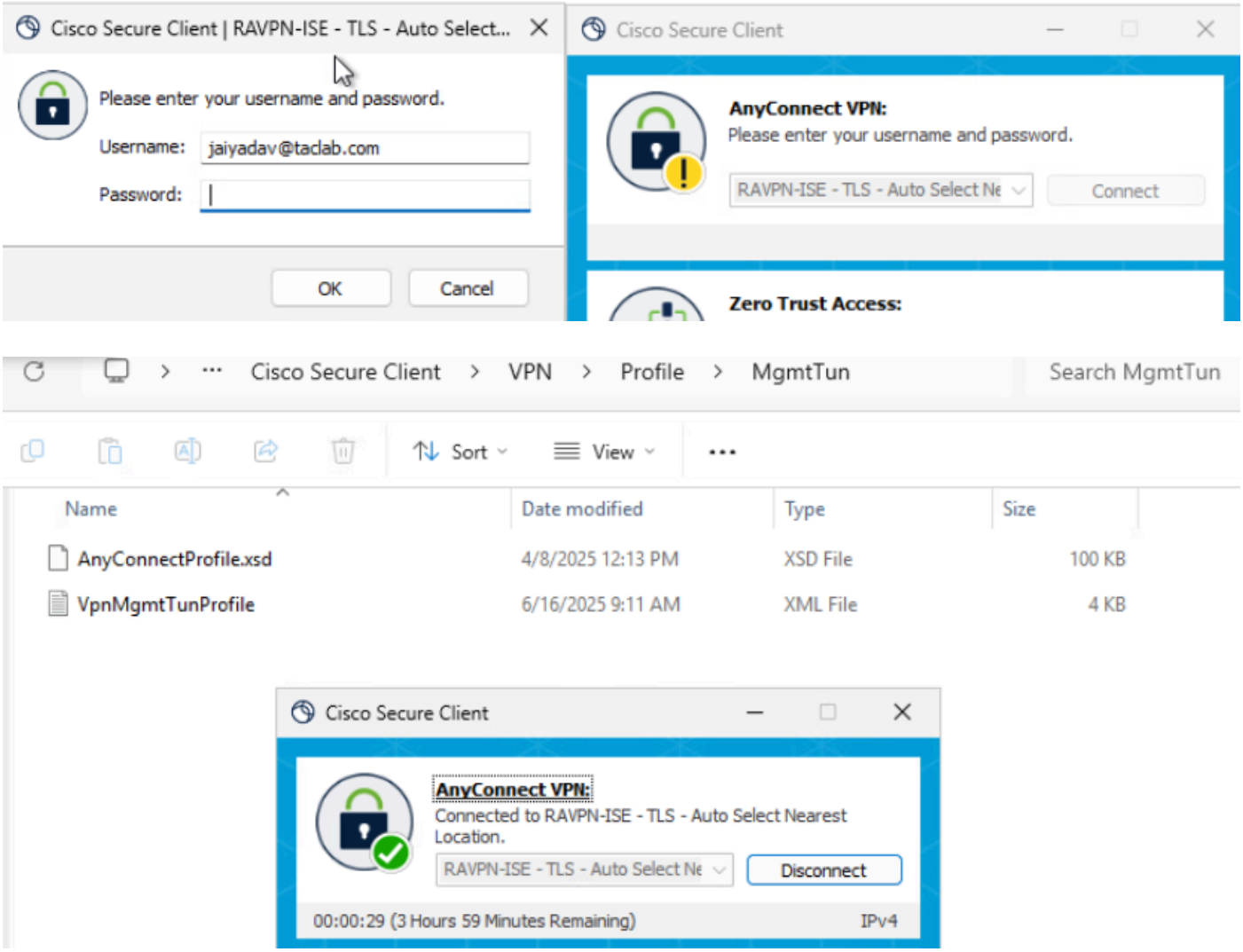
d. Het PKCS12-certificaat importeren in het endpoint-certificaatarchief



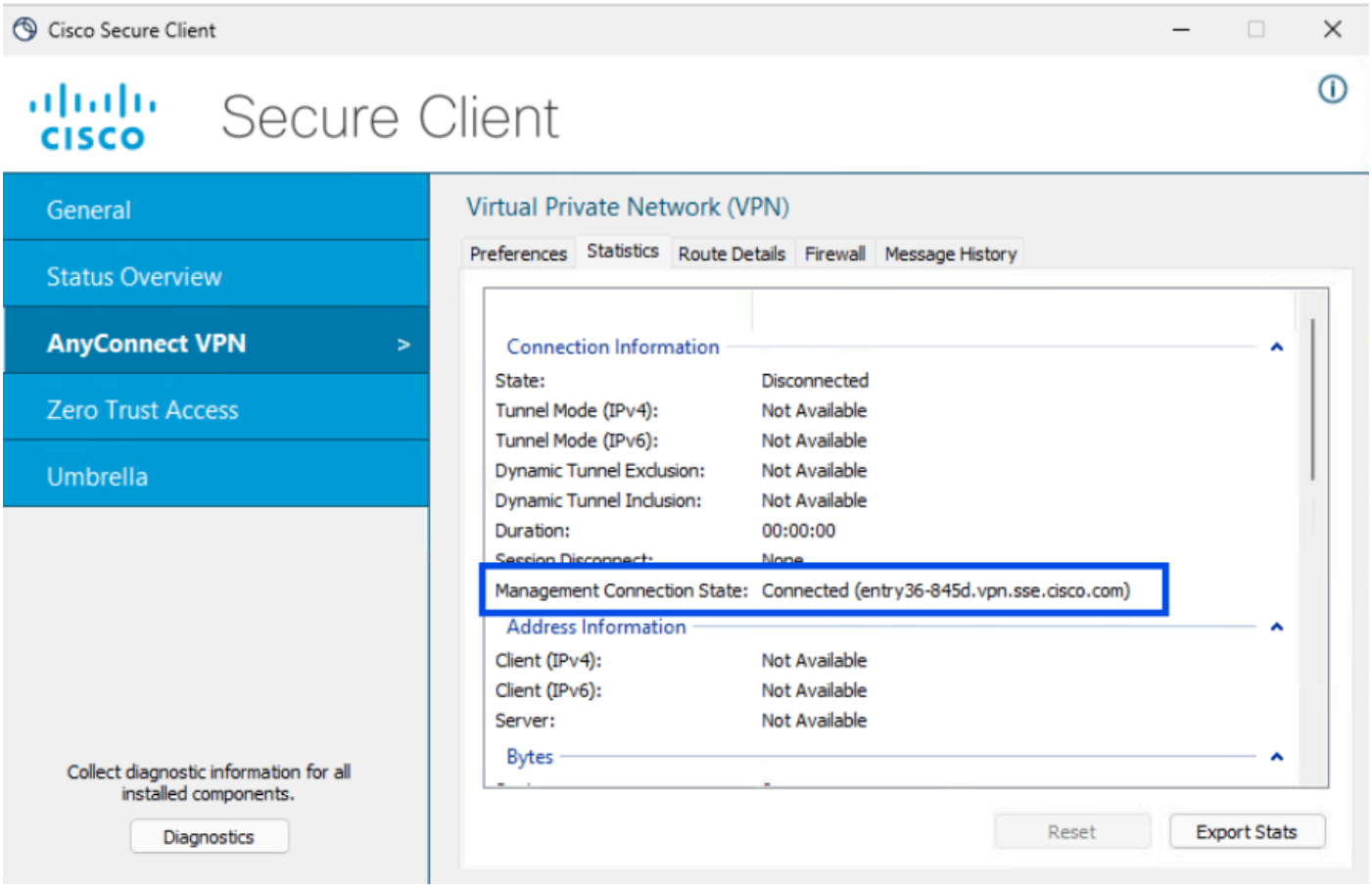


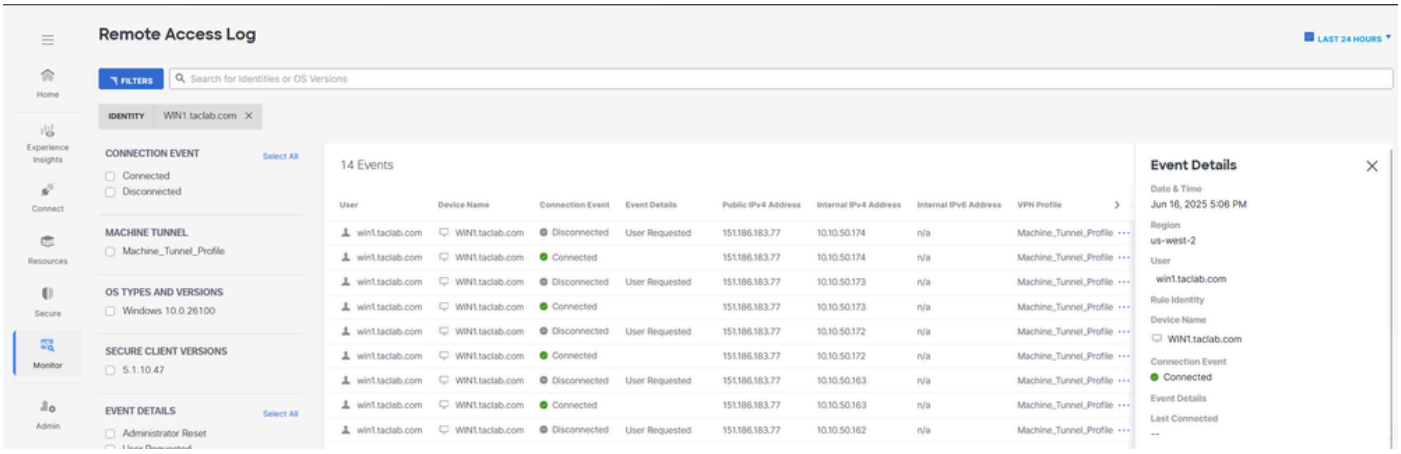
Stap 8 - Verbinding maken met de machinetunnel

a. Verbinding maken met een gebruikerstunnel, activeert het downloaden van het XML-profiel van de machinetunnel



b. De connectiviteit van de machinetunnel controleren





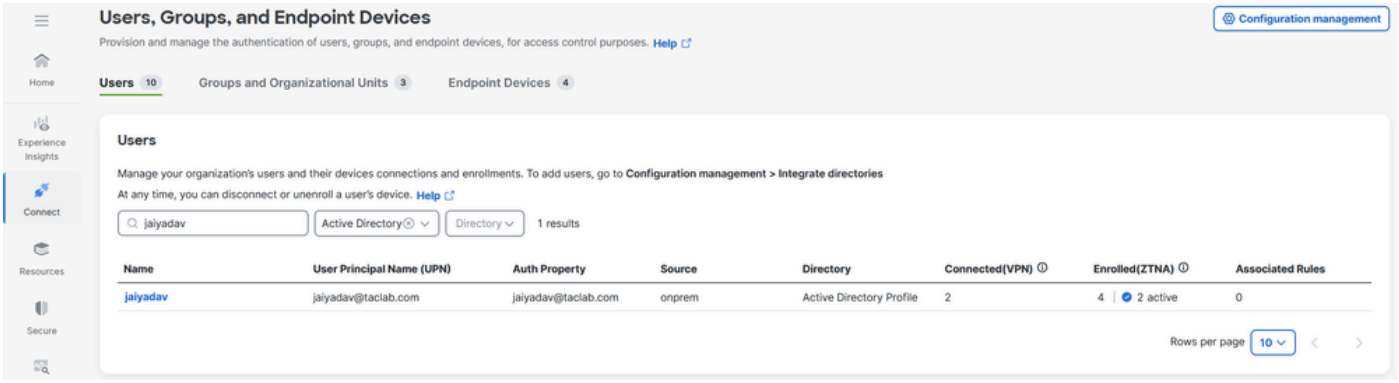
Methode 3 - Machinetunnel configureren met behulp van gebruikerscertificaat

In dit geval kiest u voor het veld Primair voor verificatie het certificaatveld dat de e-mail van de gebruiker of UPN bevat. Secure Access gebruikt de e-mail of UPN als de machine tunnel identifier. Het formaat van de e-mail of UPN moet overeenkomen met het formaat van de gekozen apparaat-ID

Doorloop de stappen 1 tot en met 4 voor de configuratie van de machinetunnel

Stap 5 - AD-connector configureren om gebruikers te kunnen importeren op de Cisco Secure Access.

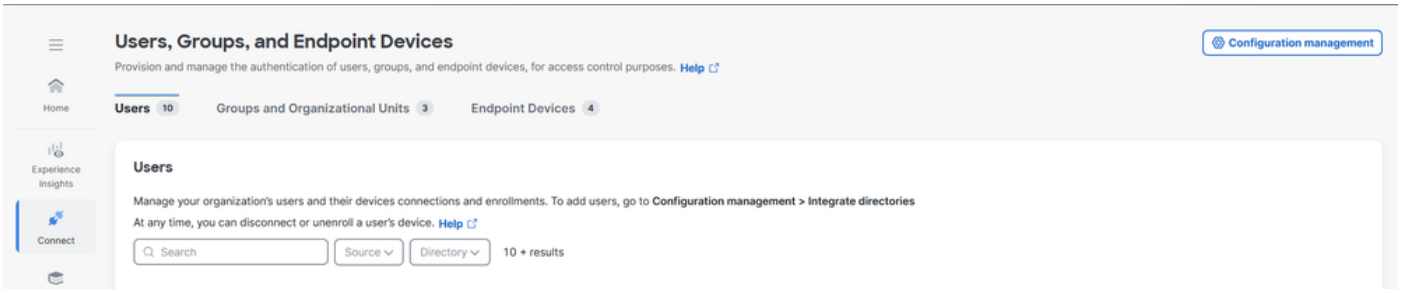
Zie On-Perm Active Directory Integration voor meer informatie



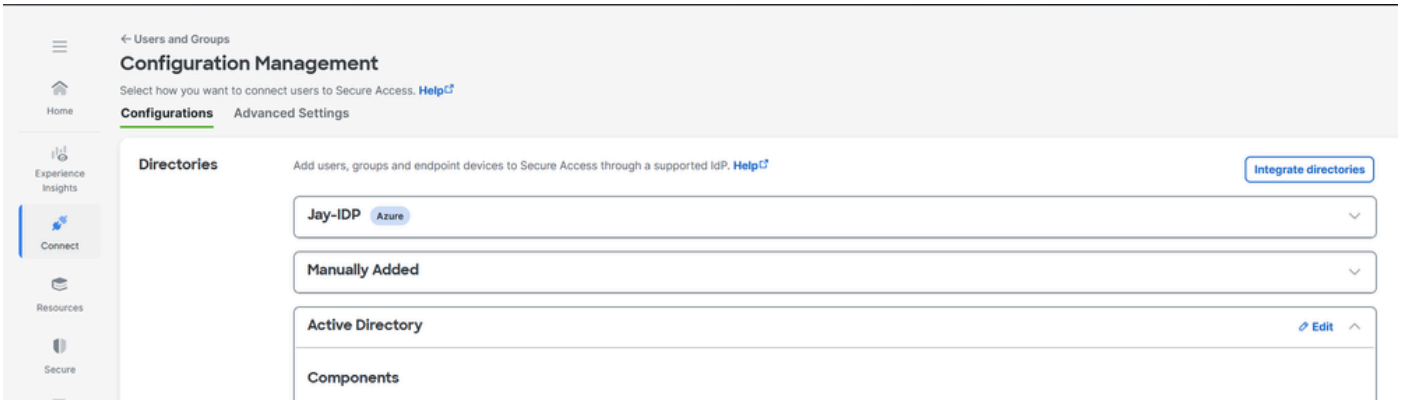
Stap 6 - Gebruikersverificatie configureren

1. Navigeer naar Verbinden > Gebruikers, groepen en eindpuntapparaten.

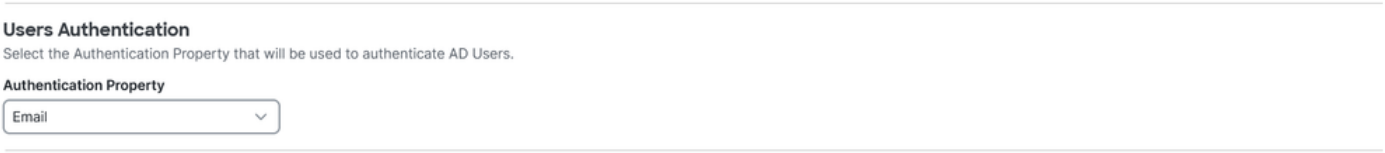
2. Klik op Configuratiebeheer



3. Bewerk Active Directory onder Configurations



4. De eigenschap User Authentication instellen op Email



5. Klik op Opslaan en herstart AD Connector-services op de servers waarop de adapter is geïnstalleerd

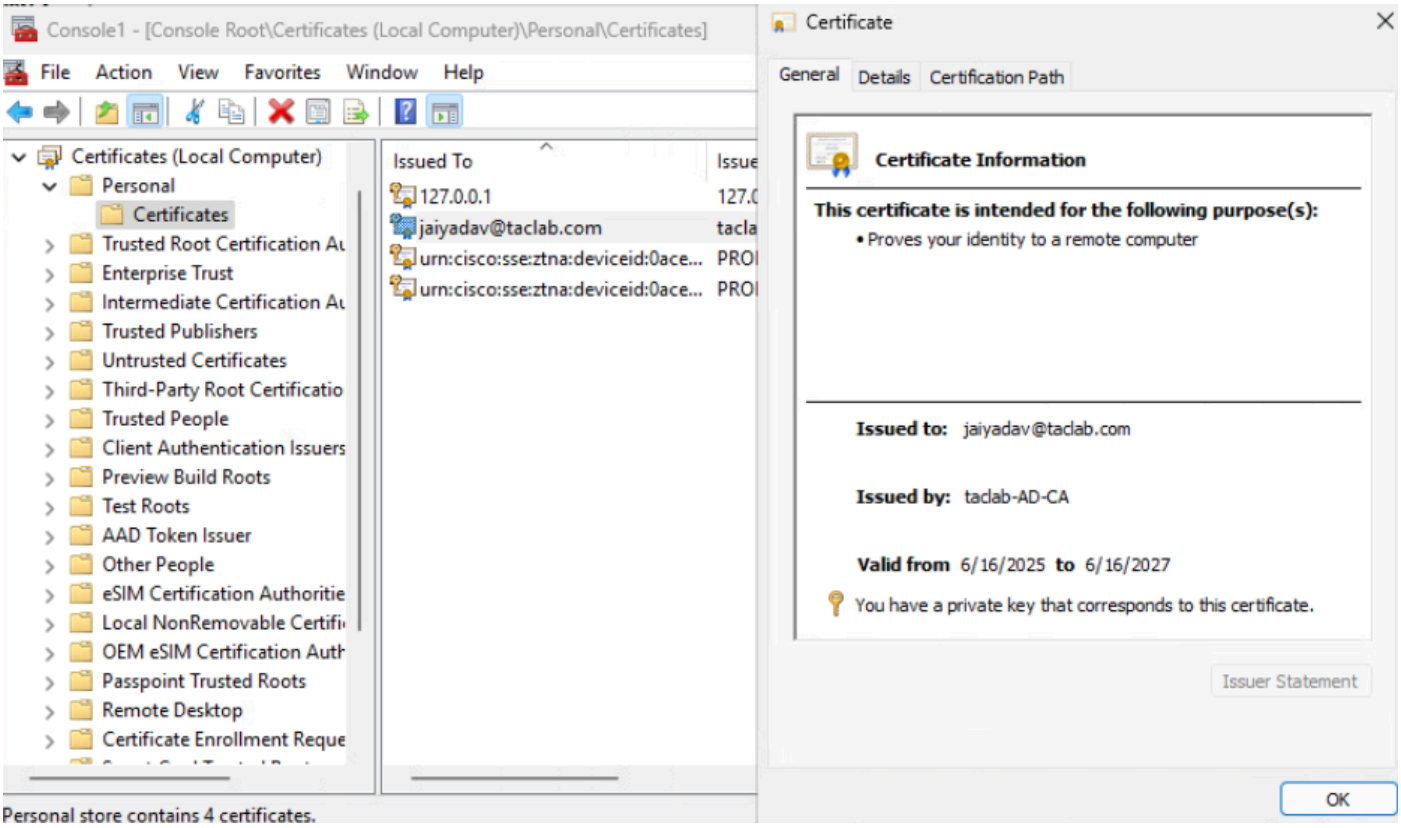
Stap 7 - Eindpuntcertificaat genereren en importeren

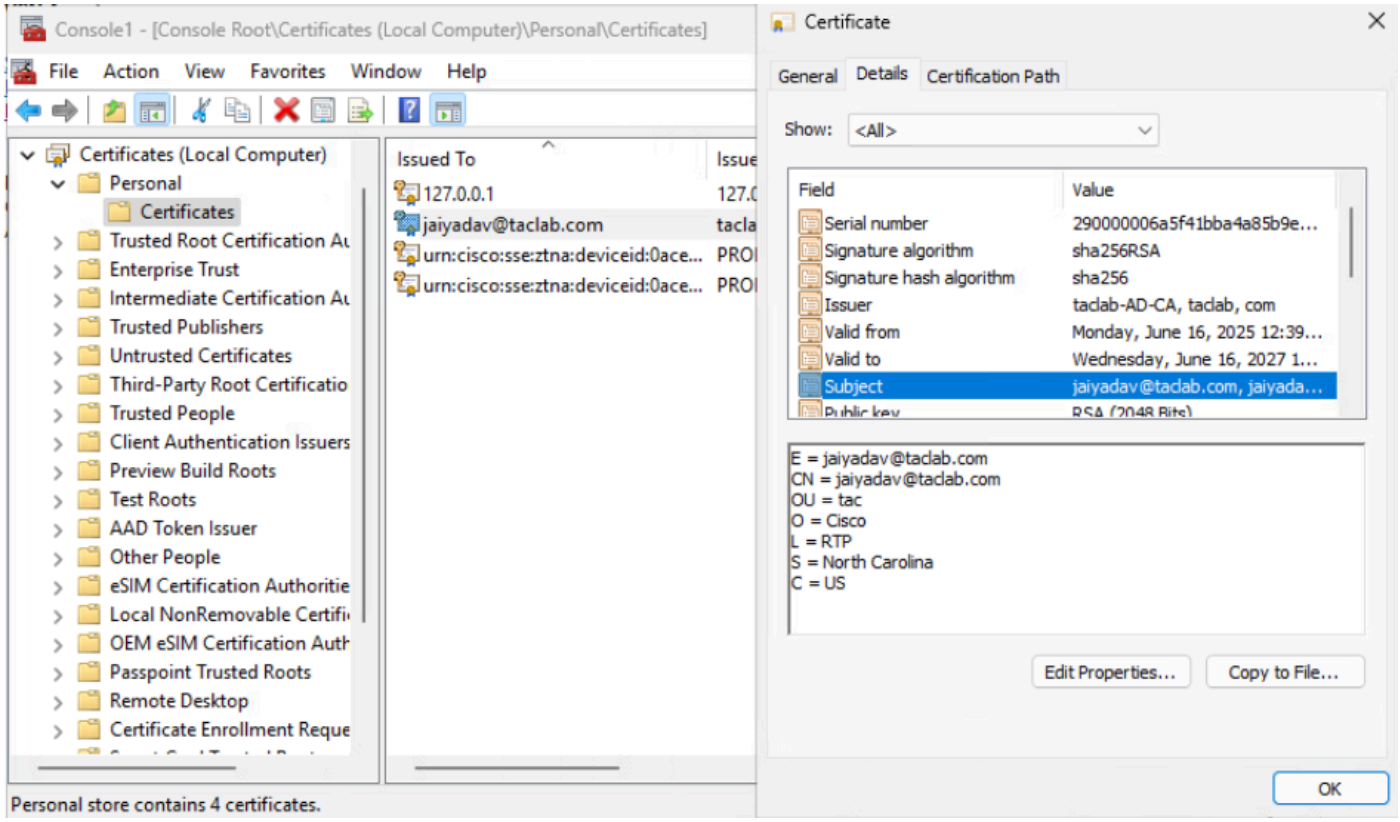
a. MVO genereren, een MVO-generator of OpenSSL-tool openen

b. Een eindpuntcertificaat genereren van CA

c. Converteer het .cert bestand naar PKCS12 formaat

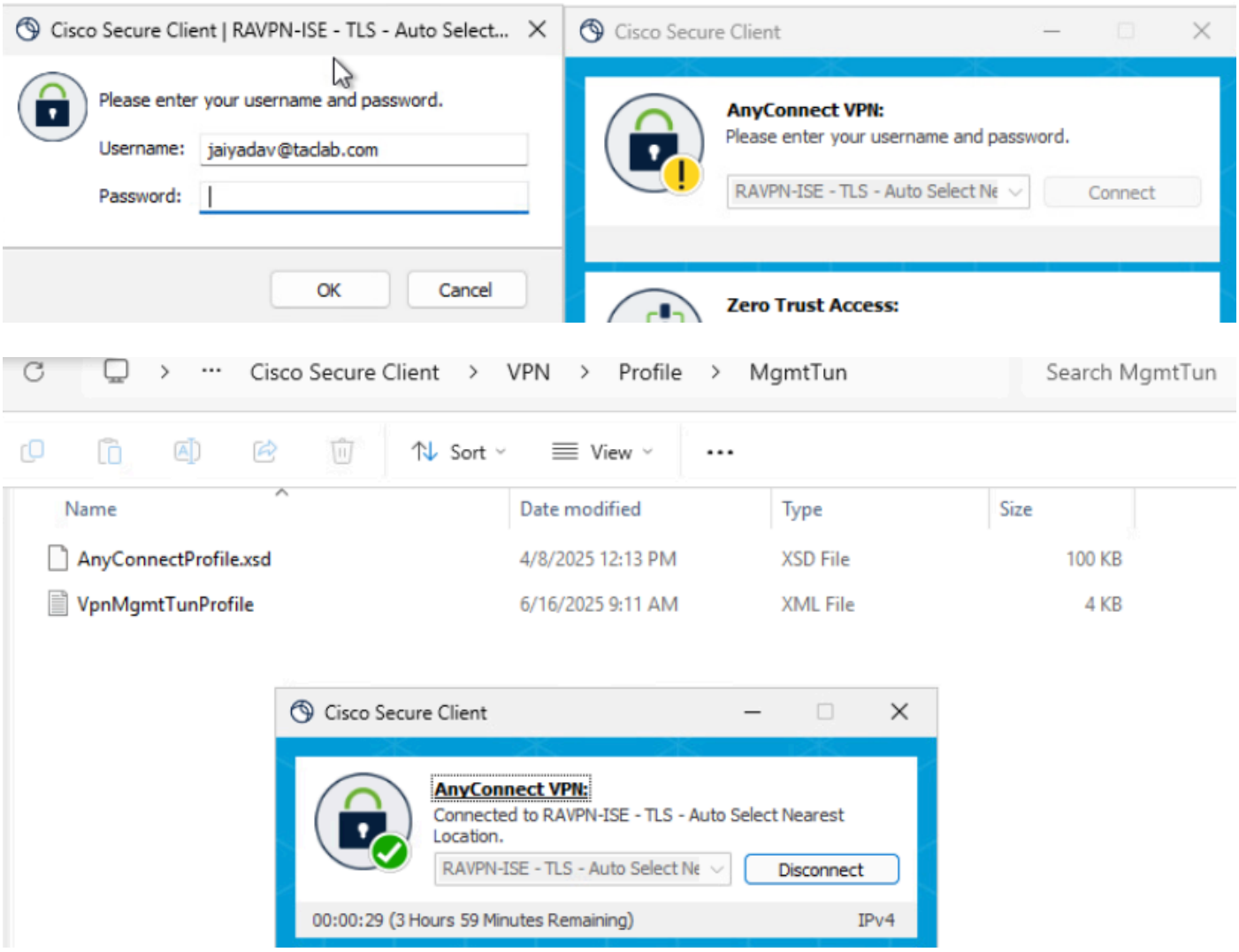
d. Het PKCS12-certificaat importeren in het endpoint-certificaatarchief



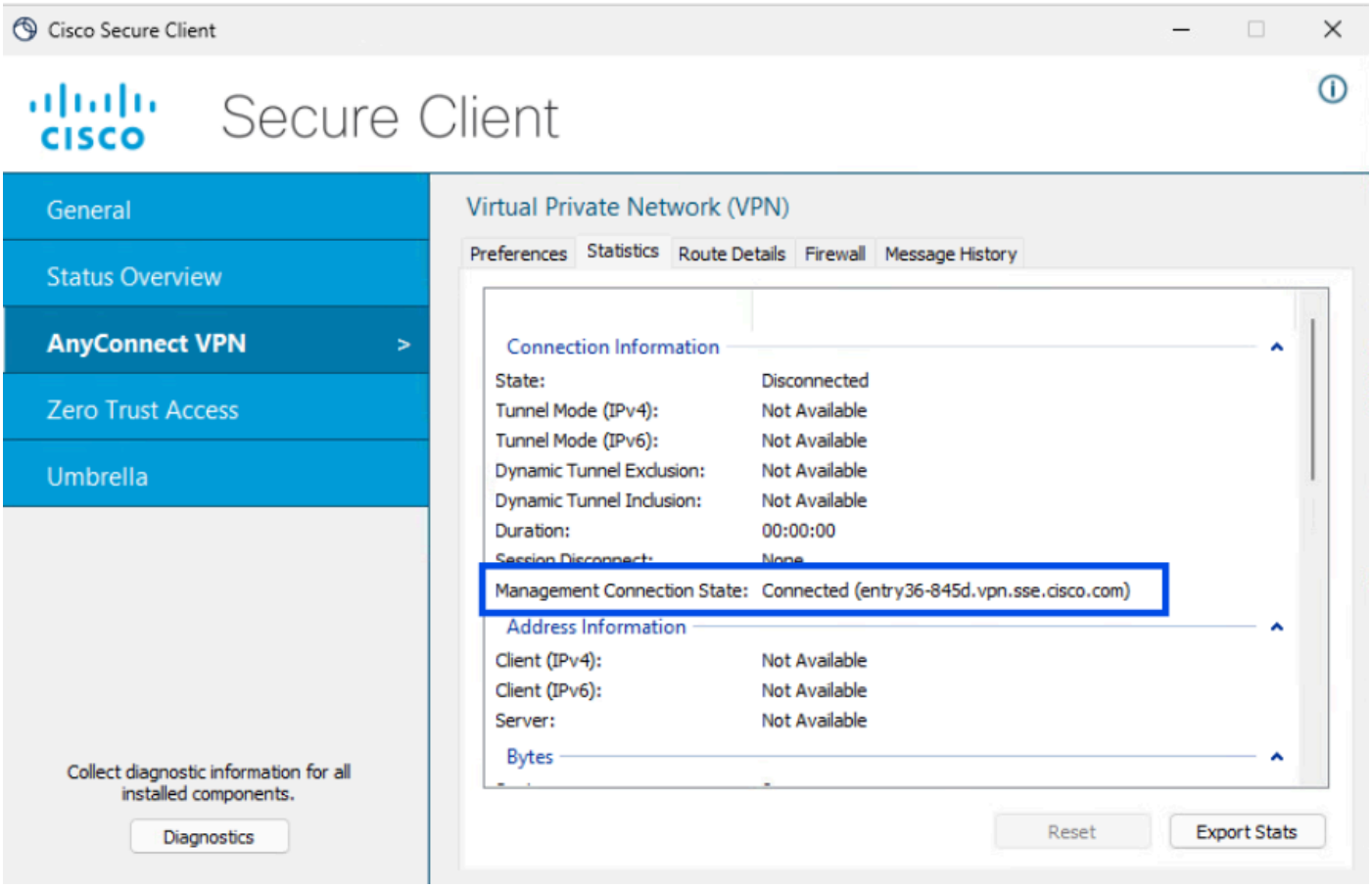


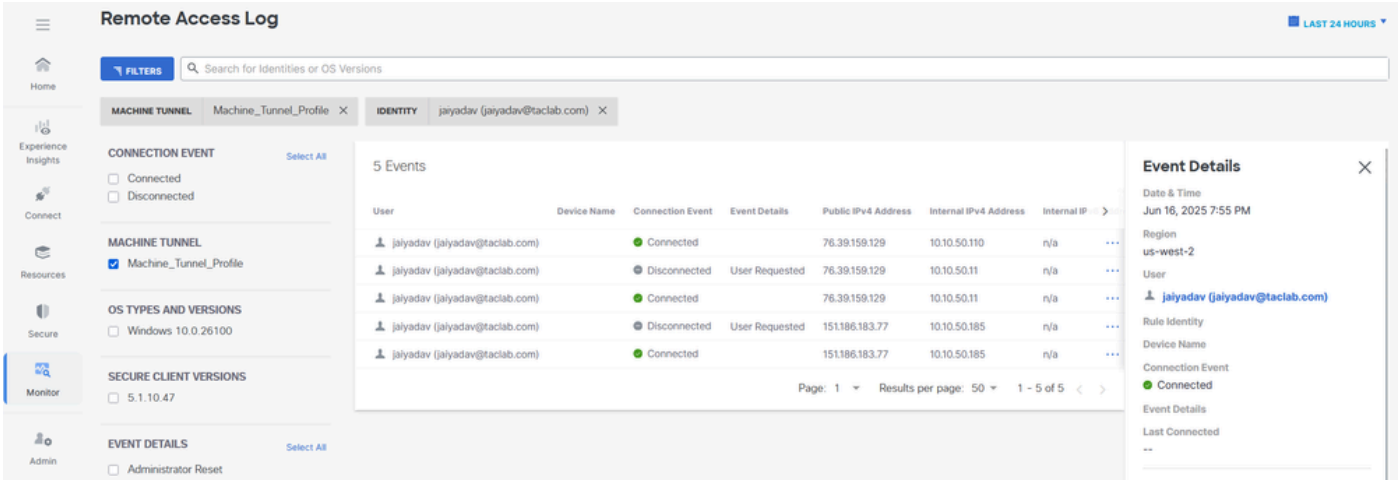
Stap 8 - Verbinding maken met de machinetunnel

a. Verbinding maken met een gebruikerstunnel, activeert het downloaden van het XML-profiel van de machinetunnel



b. De connectiviteit van de machinetunnel controleren





Problemen oplossen

Pak de DART-bundel uit en open de AnyConnectVPN-logs en analyseer voor de foutmeldingen

DARTBundle_0603_1656.zip\Cisco Secure Client\AnyConnect VPN\Logs

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.