

Machinetunnel configureren op Cisco Secure Access

Inhoud

[Inleiding](#)

[Netwerkdigram](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Werken bij Machine Tunnel](#)

[Beperkingen](#)

[Configureren](#)

[Methode 1 - Machinetunnel configureren met gebruiker machine@sse.com](#)

[Stap 1 - Algemene instellingen](#)

[Stap 2 - Verificatie voor machinecertificaat](#)

[Stap 3 – Verkeerssturing \(splittunnel\)](#)

[Stap 4 – Cisco Secure Client Configuration](#)

[Stap 5 - Controleer of de machine@sse.com user aanwezig is in de Cisco Secure Access](#)

[Stap 6 - Een CA-ondertekend certificaat genereren voor machine@sse.com](#)

[Stap 7 - Het machinecertificaat importeren op een testmachine](#)

[Stap 8 - Verbinding maken met de machinetunnel](#)

[Methode 2 - Machinetunnel configureren met Eindpuntcertificaat](#)

[Stap 5 - AD-connector configureren om eindpunten te kunnen importeren op de Cisco Secure Access.](#)

[Stap 6 - Verificatie van eindpuntapparaten configureren](#)

[Stap 7 - Eindpuntcertificaat genereren en importeren](#)

[Stap 8 - Verbinding maken met de machinetunnel](#)

[Methode 3 - Machinetunnel configureren met behulp van gebruikerscertificaat](#)

[Stap 5 - AD-connector configureren om gebruikers te kunnen importeren op de Cisco Secure Access.](#)

[Stap 6 - Gebruikersverificatie configureren](#)

[Stap 7 - Eindpuntcertificaat genereren en importeren](#)

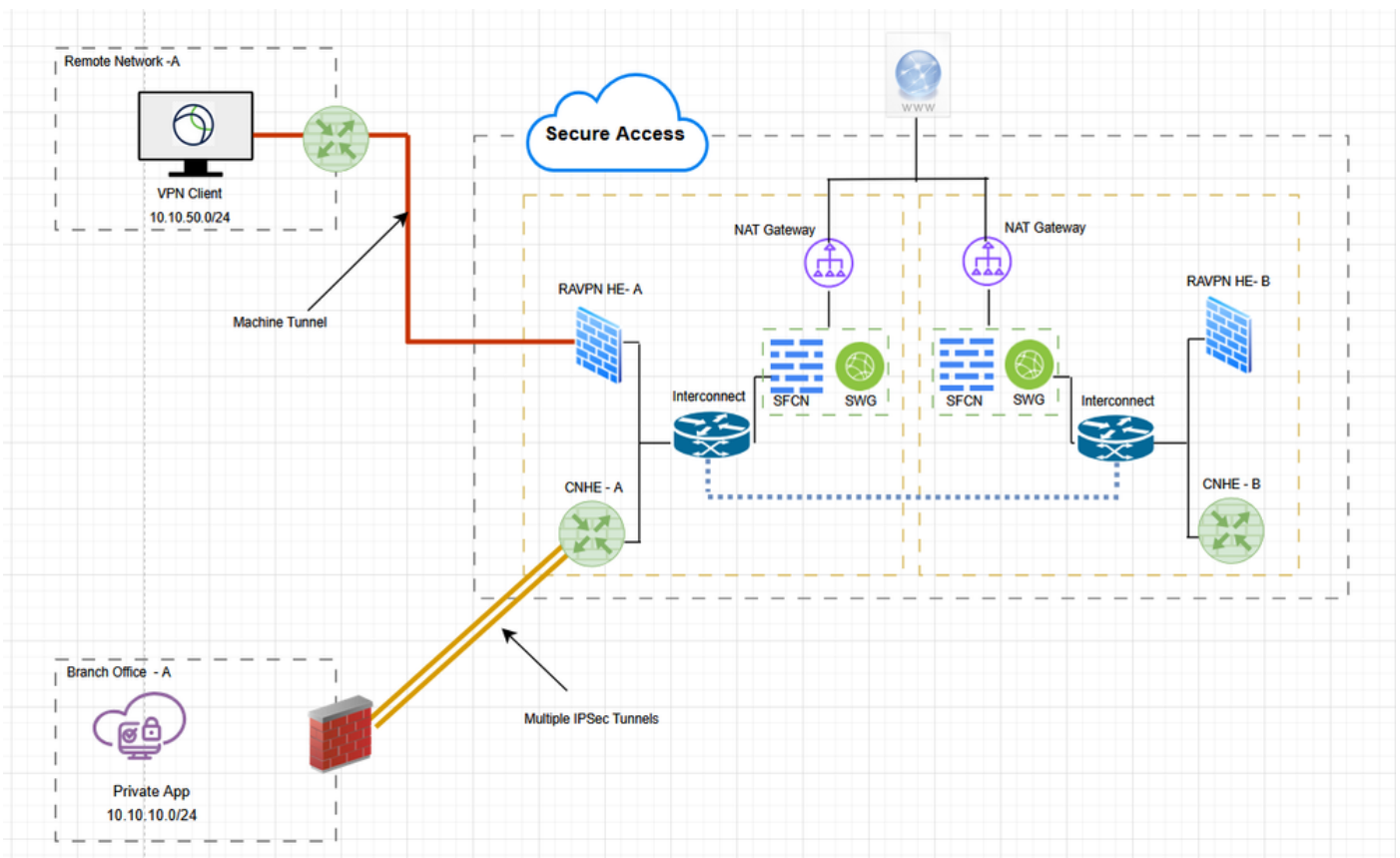
[Stap 8 - Verbinding maken met de machinetunnel](#)

[Problemen oplossen](#)

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.

Netwerkdigram



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.

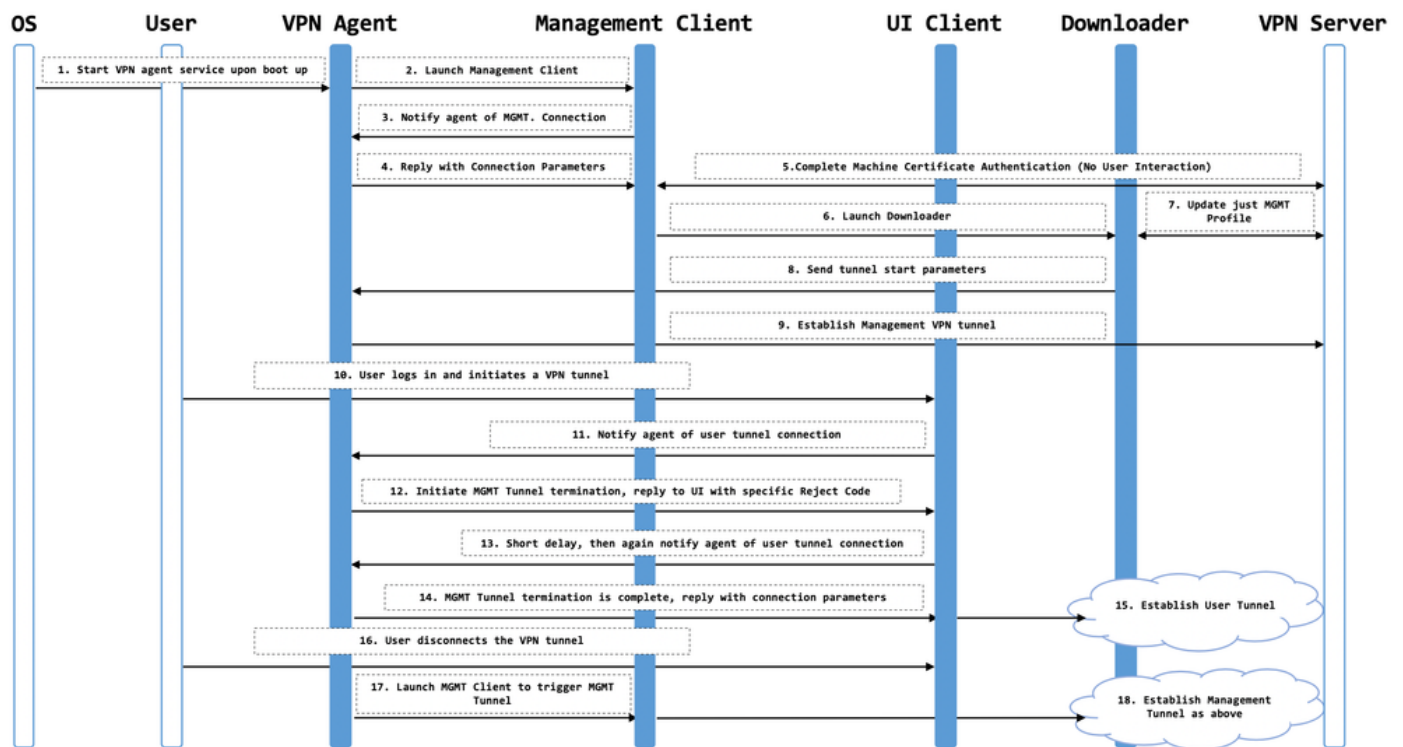
De Secure Access-machinetunnel stelt beheerders in staat om de Cisco Secure Client zonder tussenkomst van de gebruiker te laten aansluiten voordat de gebruiker zich aanmeldt. De Secure Access-machinetunnel wordt geactiveerd wanneer het eindpunt buiten het bedrijf is en de verbinding met een door de gebruiker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

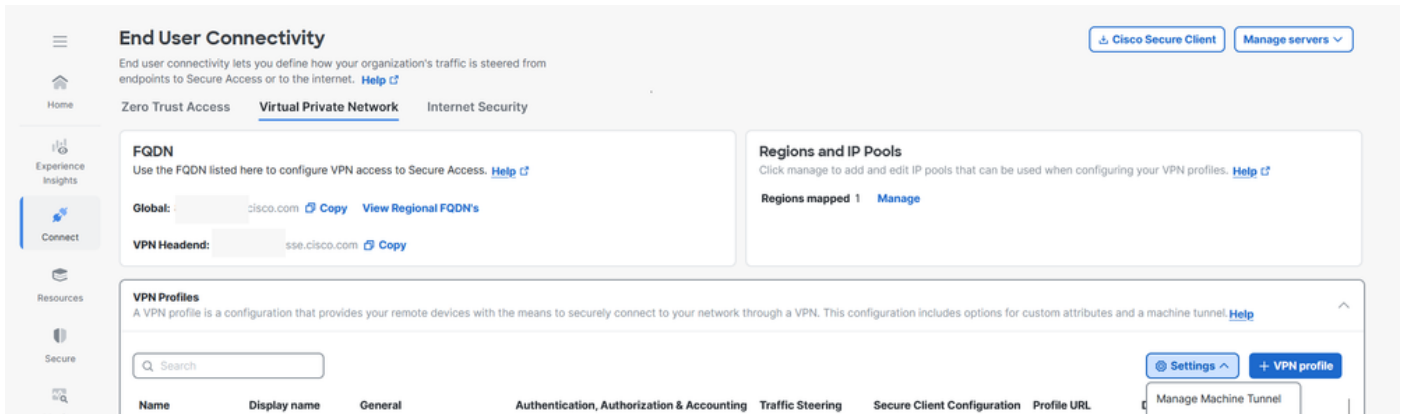
Configureren

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.

← End User Connectivity

Machine tunnel

A machine tunnel establishes a secure session to a device when the user is not signed in. This allows for the mapping of drives and secure connections at startup before a user signs into the system. [Help](#)

- 1 General settings
- 2 Authentication for Machine Certificate
- 3 Traffic Steering (Split Tunnel)
- 4 Cisco Secure Client Configuration

General settings

Select and configure the network and protocol that this Machine tunnel will use.

Default Domain

taclab.com

DNS Server

MyDNS (192.168.1.20, 10.10.10.20) [+ Add](#)

DNS servers mapped to regions [View more](#)

IP Pools

[Edit assigned IP pools](#)

Tunnel Protocol

☒ TLS / DTLS

☐ IPSec (IKEv2)

Client Bypass Protocol

☒ Include protocol

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

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

← End User Connectivity

Machine tunnel

A machine tunnel establishes a secure session to a device when the user is not signed in. This allows for the mapping of drives and secure connections at startup before a user signs into the system. [Help](#)

- 1 General settings
- 2 Authentication for Machine Certificate
- 3 Traffic Steering (Split Tunnel)
- 4 Cisco Secure Client Configuration

Authentication for Machine Certificate

Upload a CA certificate which can then be used by this machine tunnel as a machine certificate to authenticate devices.

CA Certificates

[View 1 CA certificate](#) [Upload CA Certificate](#)

Primary field to authenticate

Common Name

Secondary field to authenticate

Email

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

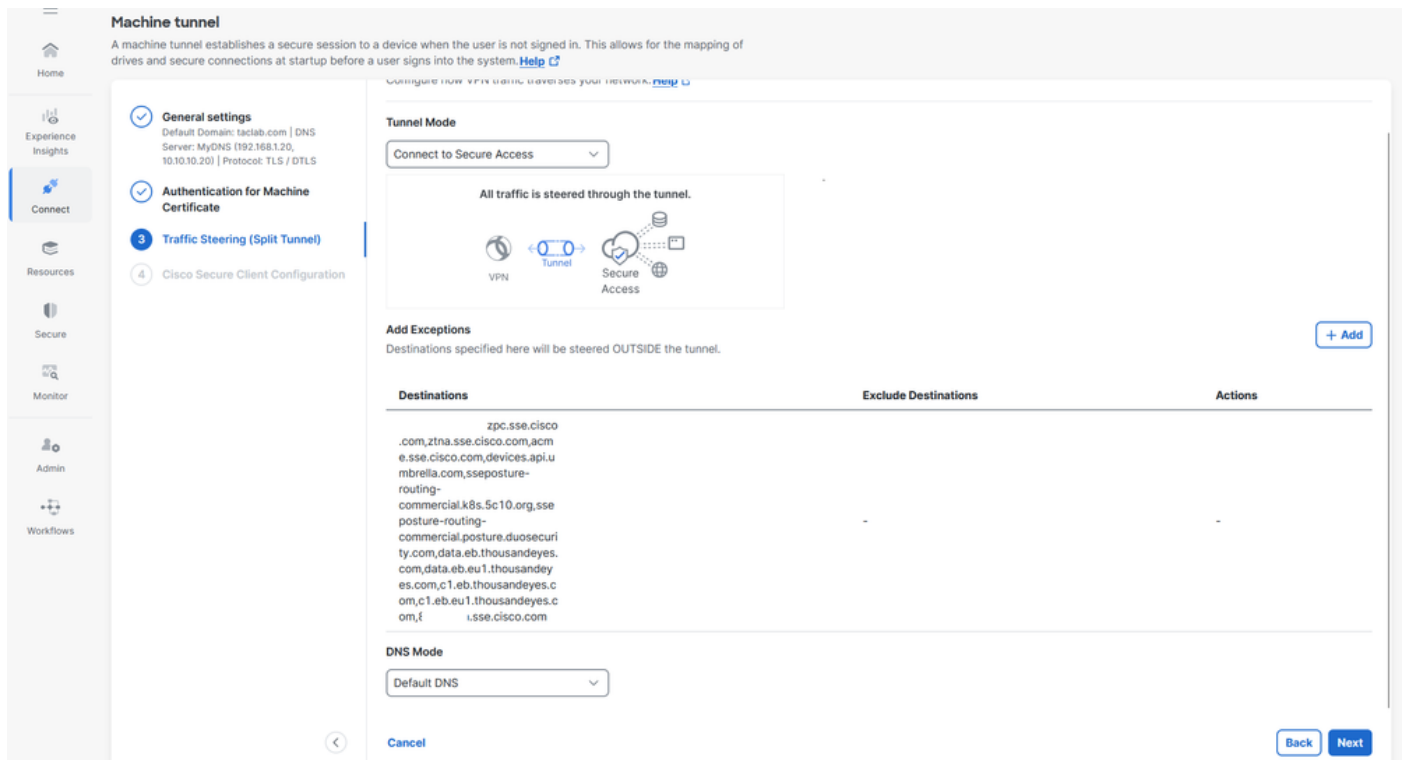
3. Klik op Volgende

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

← End User Connectivity

Machine tunnel

A machine tunnel establishes a secure session to a device when the user is not signed in. This allows for the mapping of drives and secure connections at startup before a user signs into the system. [Help](#)

- General settings
Default Domain: taclab.com | DNS Server: MyDNS (192.168.1.20, 10.10.10.20) | Protocol: TLS / DTLS
- Authentication for Machine Certificate
- Traffic Steering (Split Tunnel)
Connect to Secure Access | 1 Exceptions
- 4 Cisco Secure Client Configuration**

Cisco Secure Client Configuration

Configure how the Cisco Secure Client operates for this machine tunnel.

Session Settings **1** Client Settings **10** Client Certificate Settings **5** [Download XML](#)

Maximum Transmission Unit

[Cancel](#) [Back](#) [Save](#)

2. Clientinstellingen, raadpleeg de [clientinstellingen van Machine Tunnel](#) voor meer informatie

← End User Connectivity

Machine tunnel

A machine tunnel establishes a secure session to a device when the user is not signed in. This allows for the mapping of drives and secure connections at startup before a user signs into the system. [Help](#)

- General settings
Default Domain: taclab.com | DNS Server: MyDNS (192.168.1.20, 10.10.10.20) | Protocol: TLS / DTLS
- Authentication for Machine Certificate
- Traffic Steering (Split Tunnel)
Connect to Secure Access | 1 Exceptions
- 4 Cisco Secure Client Configuration**

Cisco Secure Client Configuration

Configure how the Cisco Secure Client operates for this machine tunnel.

Session Settings **1** **Client Settings 10** Client Certificate Settings **5** [Download XML](#)

- ☐ Local LAN Access
- ☐ Disable Captive Portal Detection
- ☐ Suspend Secure Client during suspended standby
- ☐ Captive Portal Remediation Browser Failover
- ☒ Allow local proxy connections
- ☒ Automatic VPN Policy (Windows and macOS only)

Trusted Network Policy

Untrusted Network Policy

Trusted DNS Domains

Trusted DNS Servers

Adding all DNS servers in use is recommended with Trusted Network Detection

[Cancel](#) [Back](#) [Save](#)

3. Clientcertificaatinstellingen, selecteert u de desbetreffende opties

- 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.
- Automatische certificaatselectie - Wanneer meerdere certificaatverificatie is geconfigureerd op de beveiligde gateway
- Certificaatvastlegging - CA-certificaat dat door de machinetunnel kan worden gebruikt als machinecertificaat om apparaten te verifiëren
- 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

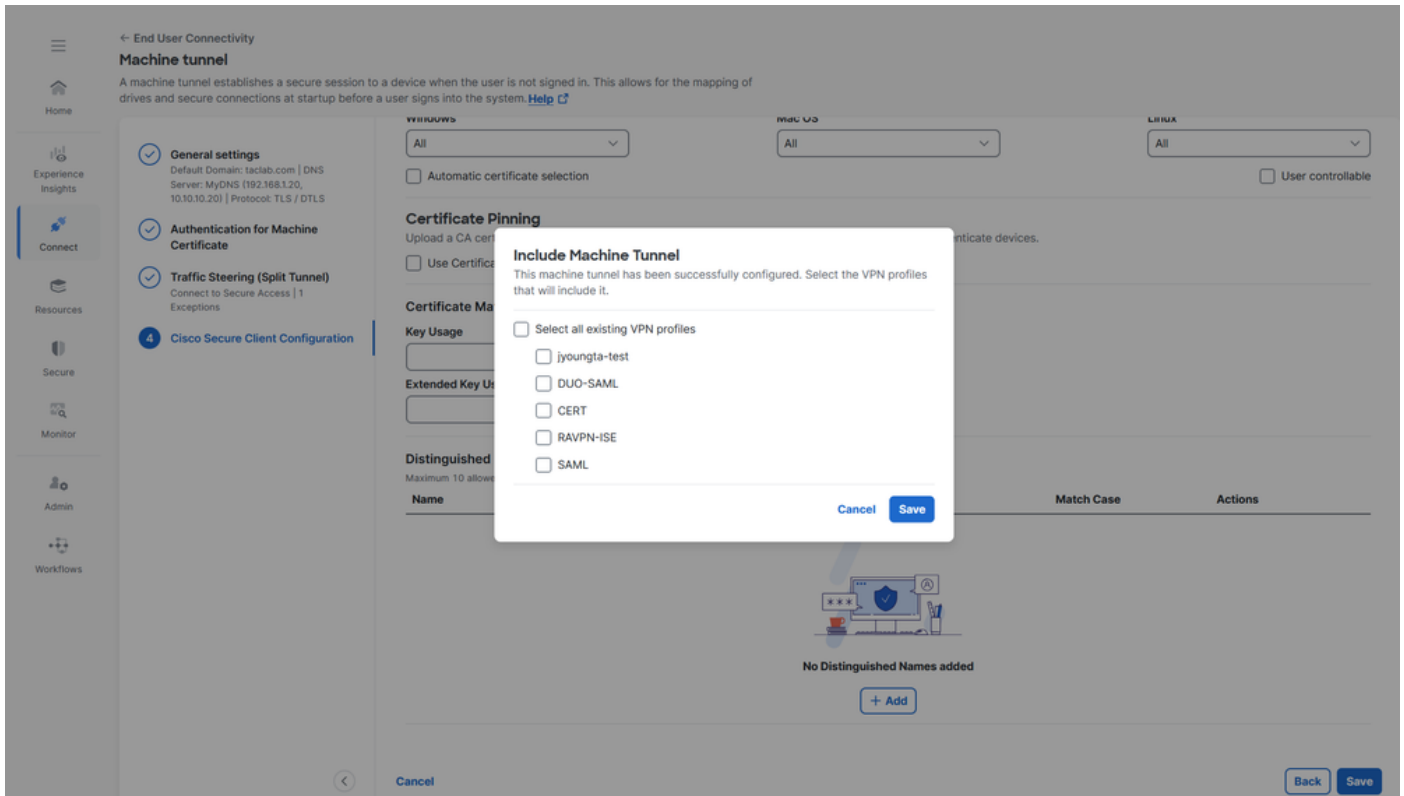
ii. Uitgebreid sleutelgebruik: clientauteur

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.

The screenshot shows the Cisco Secure Client configuration interface for Machine Tunnel settings. The left sidebar contains navigation options: Home, Experience Insights, Connect, Resources, Secure, Monitor, Admin, and Workflows. The main content area is titled 'Machine tunnel' and includes a description: 'A machine tunnel establishes a secure session to a device when the user is not signed in. This allows for the mapping of drives and secure connections at startup before a user signs into the system. [Help](#)'. Below this, there are tabs for 'Session Settings', 'Client Settings', and 'Client Certificate Settings' (which is selected). The 'Client Certificate Settings' tab has a 'Download XML' link. The settings are organized into sections: 'General settings' (Default Domain: tacitlab.com | DNS Server: MyDNS (192.168.1.20, 10.10.10.20) | Protocol: TLS / DTLS), 'Authentication for Machine Certificate', 'Traffic Steering (Split Tunnel)' (Connect to Secure Access | 1 Exceptions), and 'Cisco Secure Client Configuration'. The 'Client Certificate Settings' section includes: 'Certificate Operating System' (Windows certificate store override checked), 'Client Certificate Store' (Windows, Mac OS, Linux dropdowns, All selected), 'Automatic certificate selection' (unchecked), 'User controllable' (unchecked), 'Certificate Pinning' (Upload a CA certificate which can then be used by this machine tunnel as a machine certificate to authenticate devices. Use Certificate Pinning unchecked), 'Certificate Matching' (Key Usage, Extended Key Usage dropdowns), and 'Distinguished Name' (Maximum 10 allowed). The 'Distinguished Name' section has a table with columns: Name, Pattern, Wildcard, Operator, Match Case, and Actions.

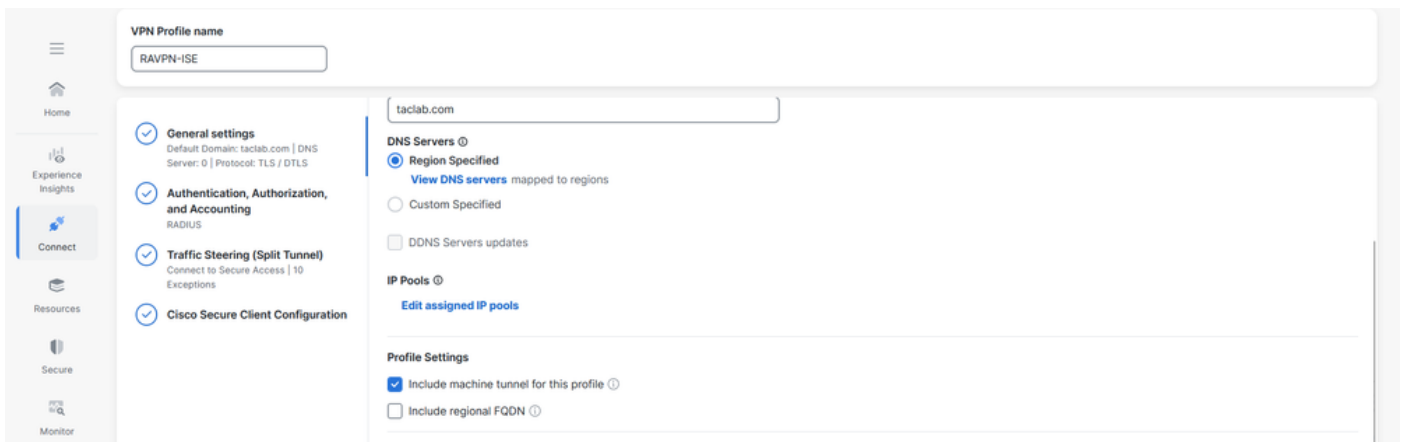
Name	Pattern	Wildcard	Operator	Match Case	Actions
------	---------	----------	----------	------------	---------

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



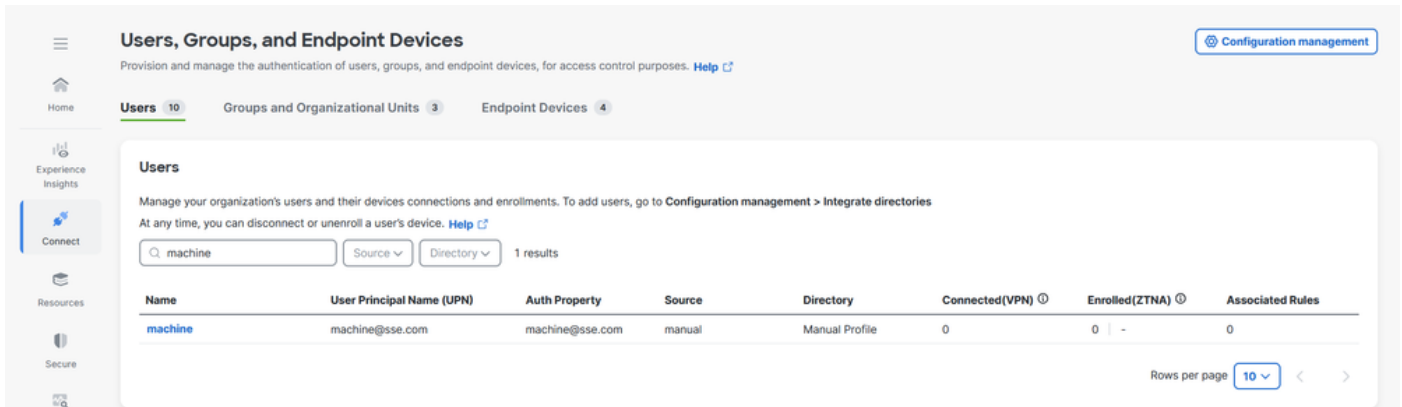
5. Klik op Opslaan

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

General

Details

Certification Path

**Certificate Information****This certificate is intended for the following purpose(s):**

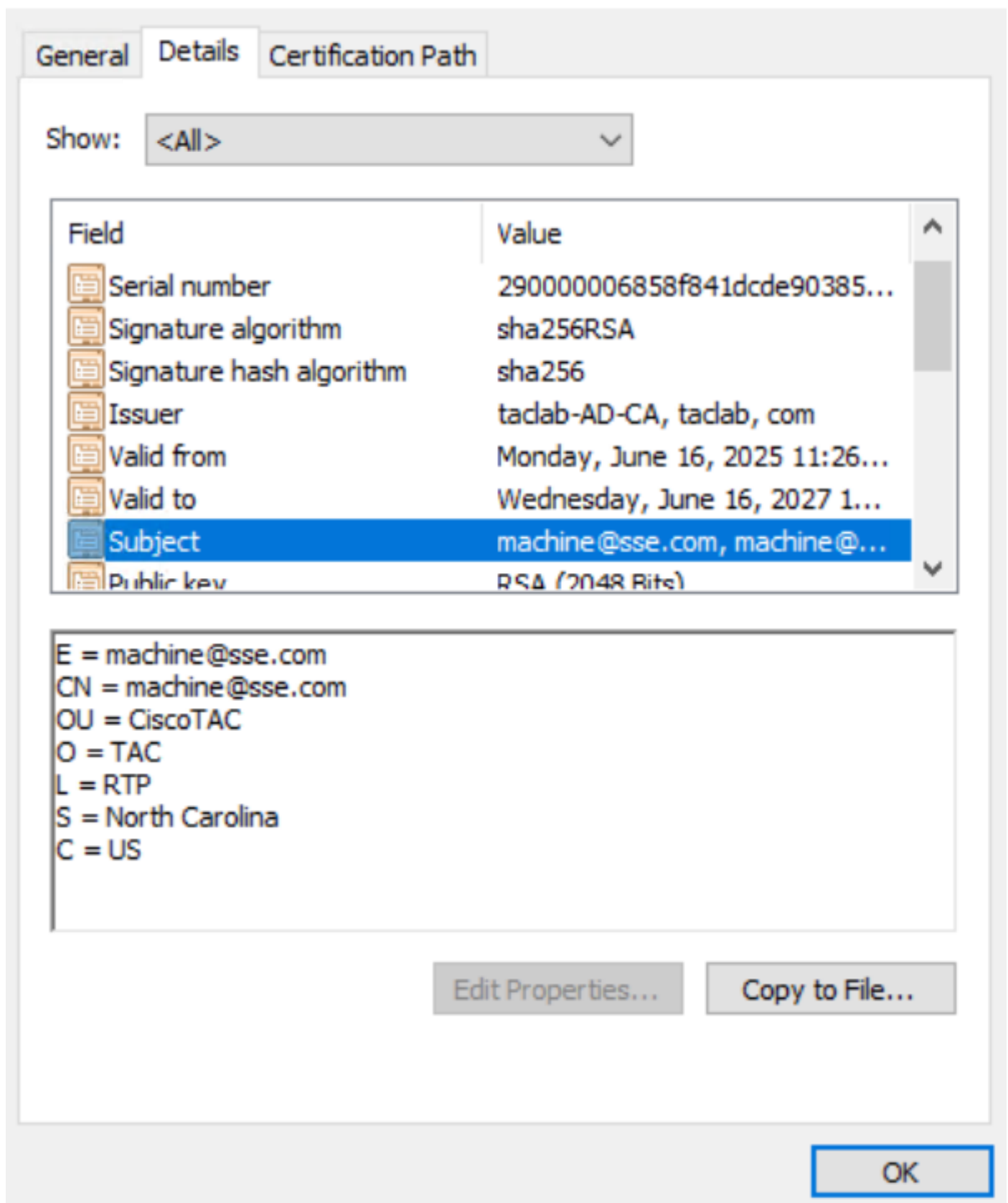
- Proves your identity to a remote computer

Issued to: machine@sse.com**Issued by:** tadab-AD-CA**Valid from** 6/16/2025 **to** 6/16/2027

Install Certificate...

Issuer Statement

OK



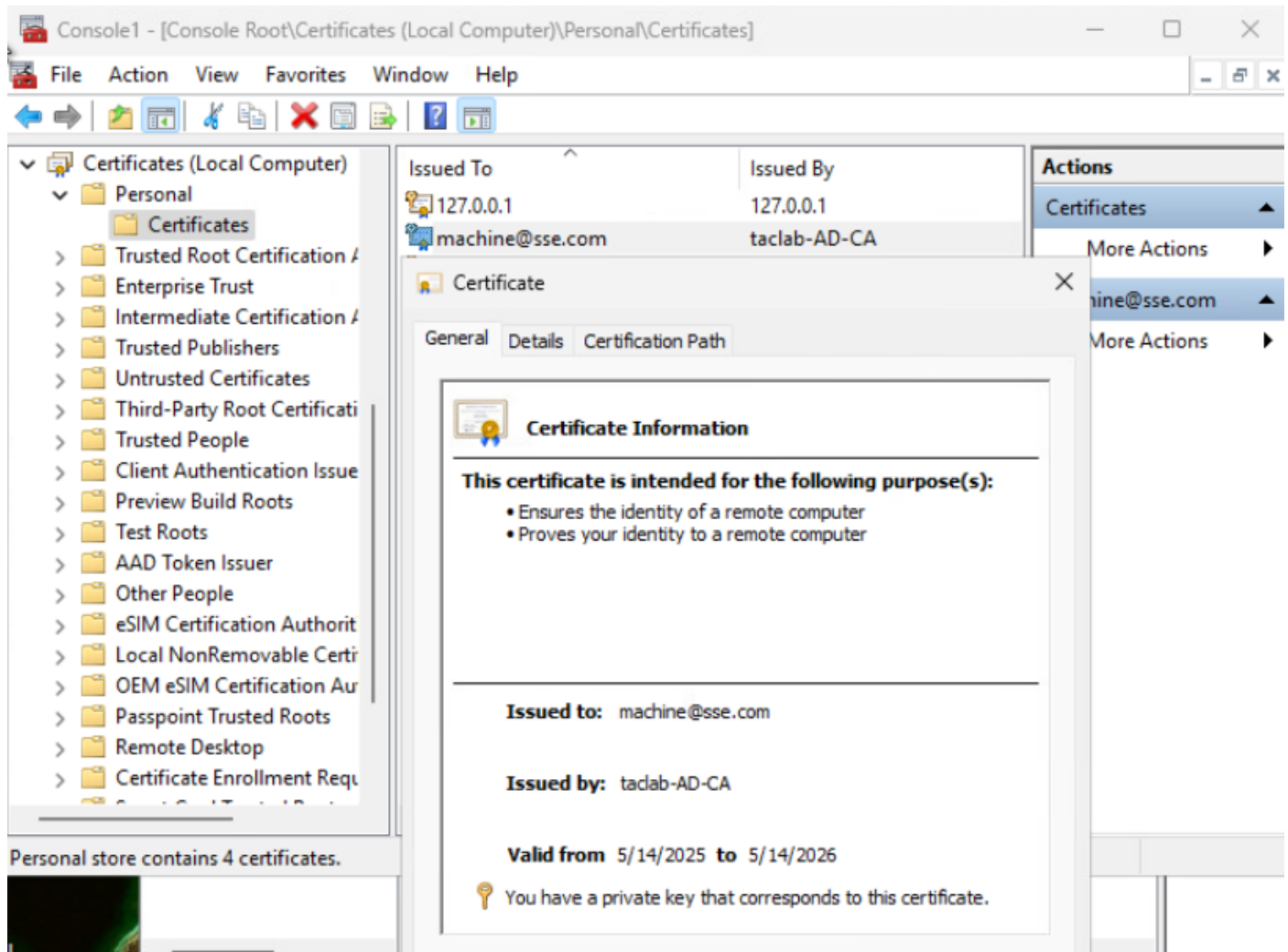
3. Converteer het machinecertificaat in PKCS12-indeling met behulp van de sleutel en cert die in de vorige stappen (stap 1 en 2) zijn gegenereerd

```
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#
```

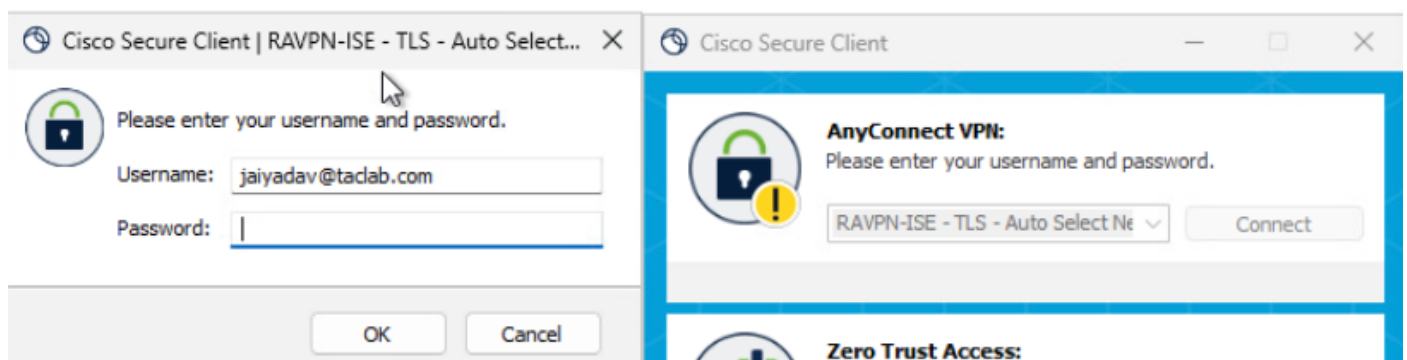
Stap 7 - Het machinecertificaat importeren op een testmachine

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.



Cisco Secure Client > VPN > Profile > MgmtTun Search MgmtTun

Name	Date modified	Type	Size
AnyConnectProfile.xsd	4/8/2025 12:13 PM	XSD File	100 KB
VpnMgmtTunProfile	6/16/2025 9:11 AM	XML File	4 KB

Cisco Secure Client

AnyConnect VPN:
Connected to RAVPN-ISE - TLS - Auto Select Nearest Location.

RAVPN-ISE - TLS - Auto Select Nearest Location

Disconnect

00:00:29 (3 Hours 59 Minutes Remaining) IPv4

b. De connectiviteit van de machinetunnel controleren

Cisco Secure Client

Secure Client

- General
- Status Overview
- AnyConnect VPN**
- Zero Trust Access
- Umbrella

Collect diagnostic information for all installed components. [Diagnostics](#)

Virtual Private Network (VPN)

Preferences Statistics Route Details Firewall Message History

Connection Information

State: Disconnected

Tunnel Mode (IPv4): Not Available

Tunnel Mode (IPv6): Not Available

Dynamic Tunnel Exclusion: Not Available

Dynamic Tunnel Inclusion: Not Available

Duration: 00:00:00

Session Disconnect: None

Management Connection State: Connected (entry36-845d.vpn.sse.cisco.com)

Address Information

Client (IPv4): Not Available

Client (IPv6): Not Available

Server: Not Available

Bytes

Reset Export Stats

Remote Access Log LAST 24 HOURS

Filters: Search for Identities or OS Versions

Left Sidebar:

- Home
- Experience Insights
- Connect
- Resources
- Secure
- Monitor**
- Admin

CONNECTION EVENT [Select All](#)

☐ Connected
☐ Disconnected

MACHINE TUNNEL

☐ Machine_Tunnel_Profile

OS TYPES AND VERSIONS

☐ Windows 10.0.26100

SECURE CLIENT VERSIONS

☐ 5.1.10.47

EVENT DETAILS [Select All](#)

☐ Administrator Reset

23 Events

User	Device Name	Connection Event	Event Details	
machine (machine@sse.com)		Connected		15 ...
machine (machine@sse.com)		Disconnected	User Requested	15 ...
machine (machine@sse.com)		Connected		15 ...
machine (machine@sse.com)		Disconnected	User Requested	15 ...
machine (machine@sse.com)		Connected		15 ...
machine (machine@sse.com)		Disconnected	User Requested	15 ...
machine (machine@sse.com)		Connected		15 ...
jaiyadav (jaiyadav@taclab.com)		Disconnected	User Requested	15 ...
jaiyadav (jaiyadav@taclab.com)		Connected		15 ...

Event Details ×

Date & Time
Jun 16, 2025 4:29 PM

Region
us-west-2

User
machine (machine@sse.com)

Rule Identity

Device Name

Connection Event
Connected

Event Details

Last Connected
--

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

Users, Groups, and Endpoint Devices Configuration management

Provision and manage the authentication of users, groups, and endpoint devices, for access control purposes. [Help](#)

Users 10 **Groups and Organizational Units** 3 **Endpoint Devices** 4

Endpoint Devices

Manage your endpoint device connections and AD device enrollments. To add new AD devices, go to [Configuration management > Integrate directories](#). [Help](#)

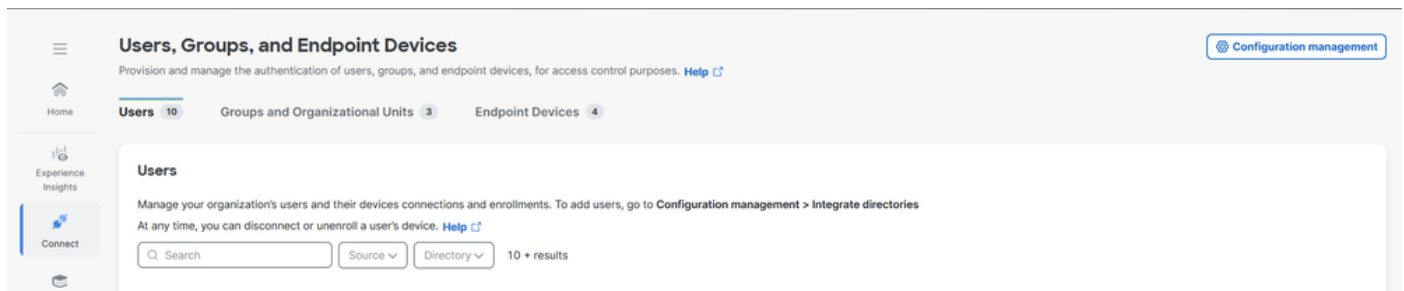
Search 4 results

Name	Device Type	Auth Property	Directory	Associated Rules
ISE.taclab.com	AD Device	ise.taclab.com	Active Directory Profile	0
WIN1.taclab.com	AD Device	Win1.taclab.com	Active Directory Profile	0
WIN2.taclab.com	AD Device	Win2.taclab.com	Active Directory Profile	0
WINDOWS11.taclab.com	AD Device	Windows11.taclab.com	Active Directory Profile	0

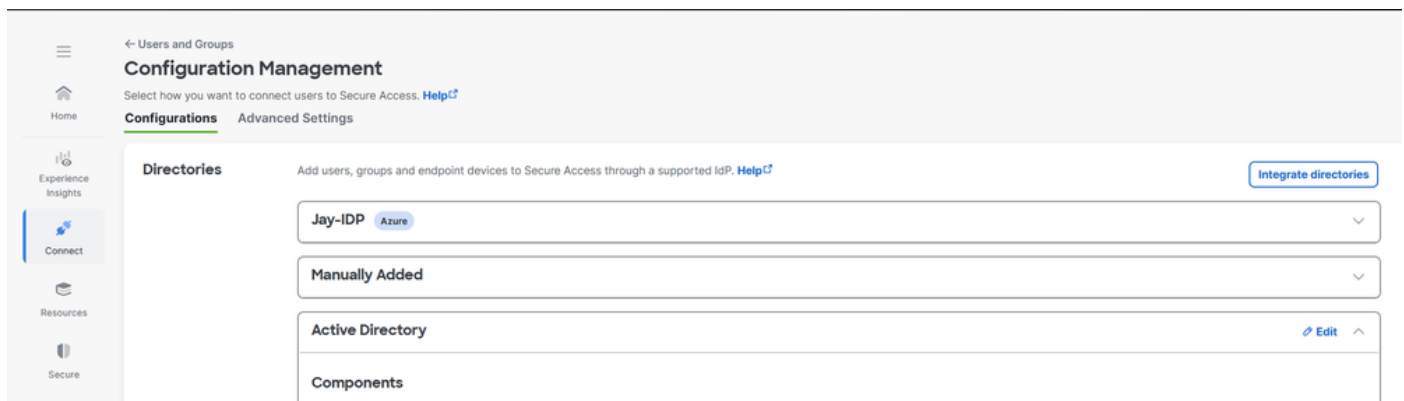
Rows per page 10 < >

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

Endpoint Devices Authentication

Select the Authentication Property that will be used to authenticate AD endpoint devices when connected via RA-VPN. [Help](#)

Authentication Property

Hostname

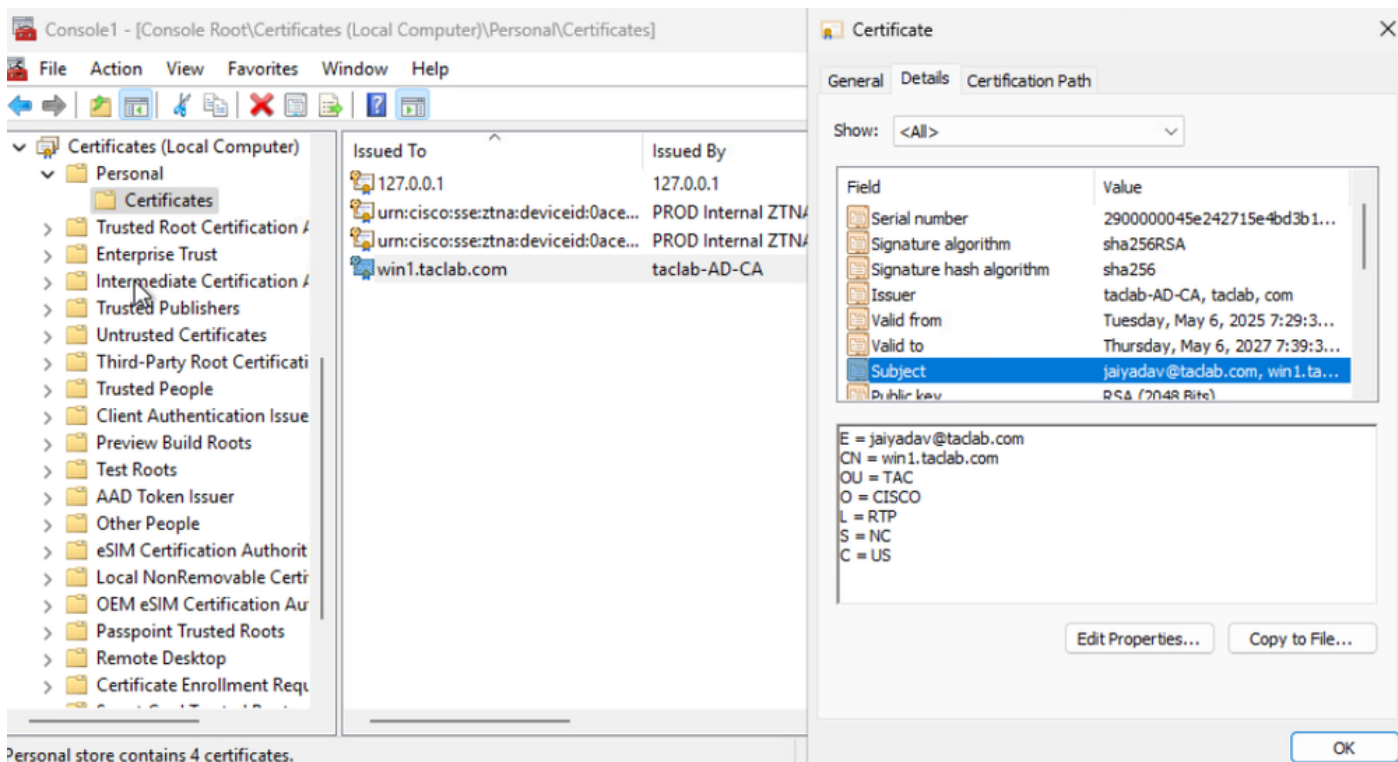
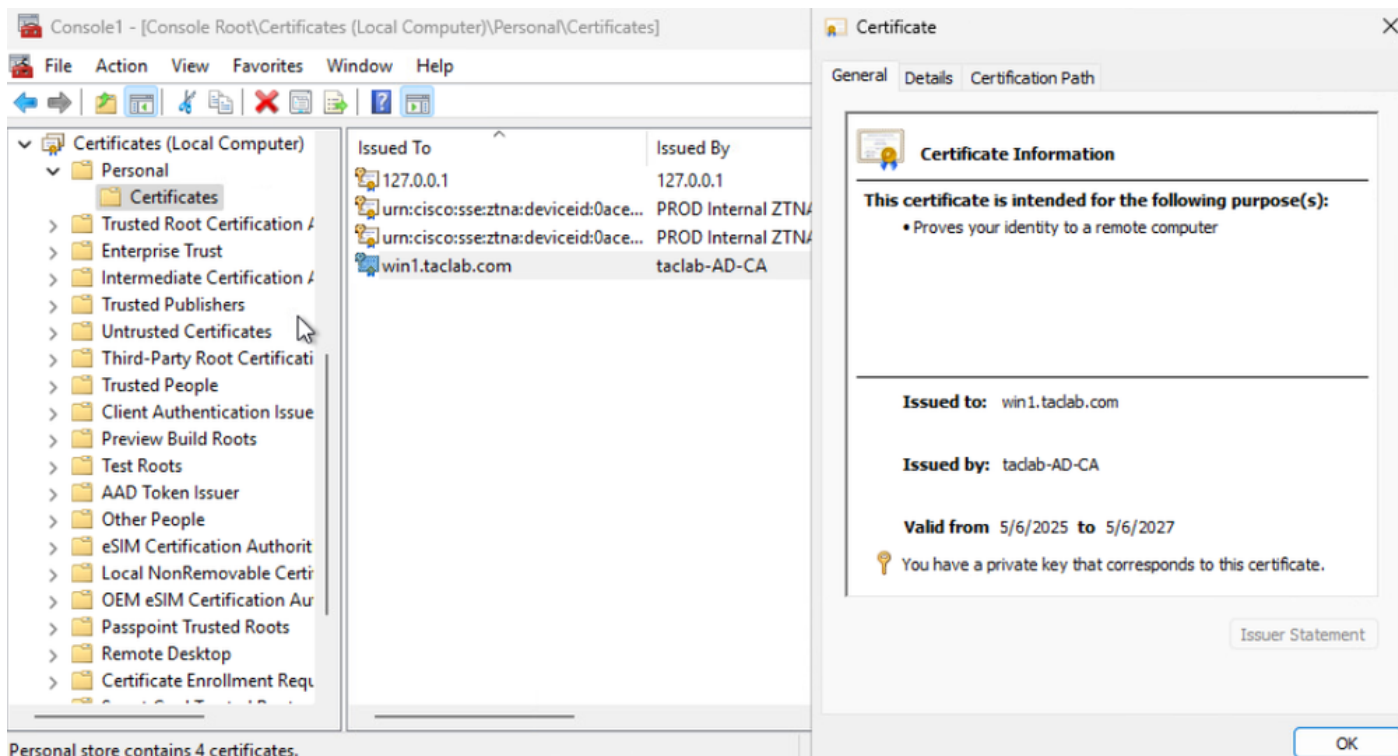
You must re-sync AD identities when you update this Authentication Property.

[Cancel](#) [Delete](#) [Save](#)

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

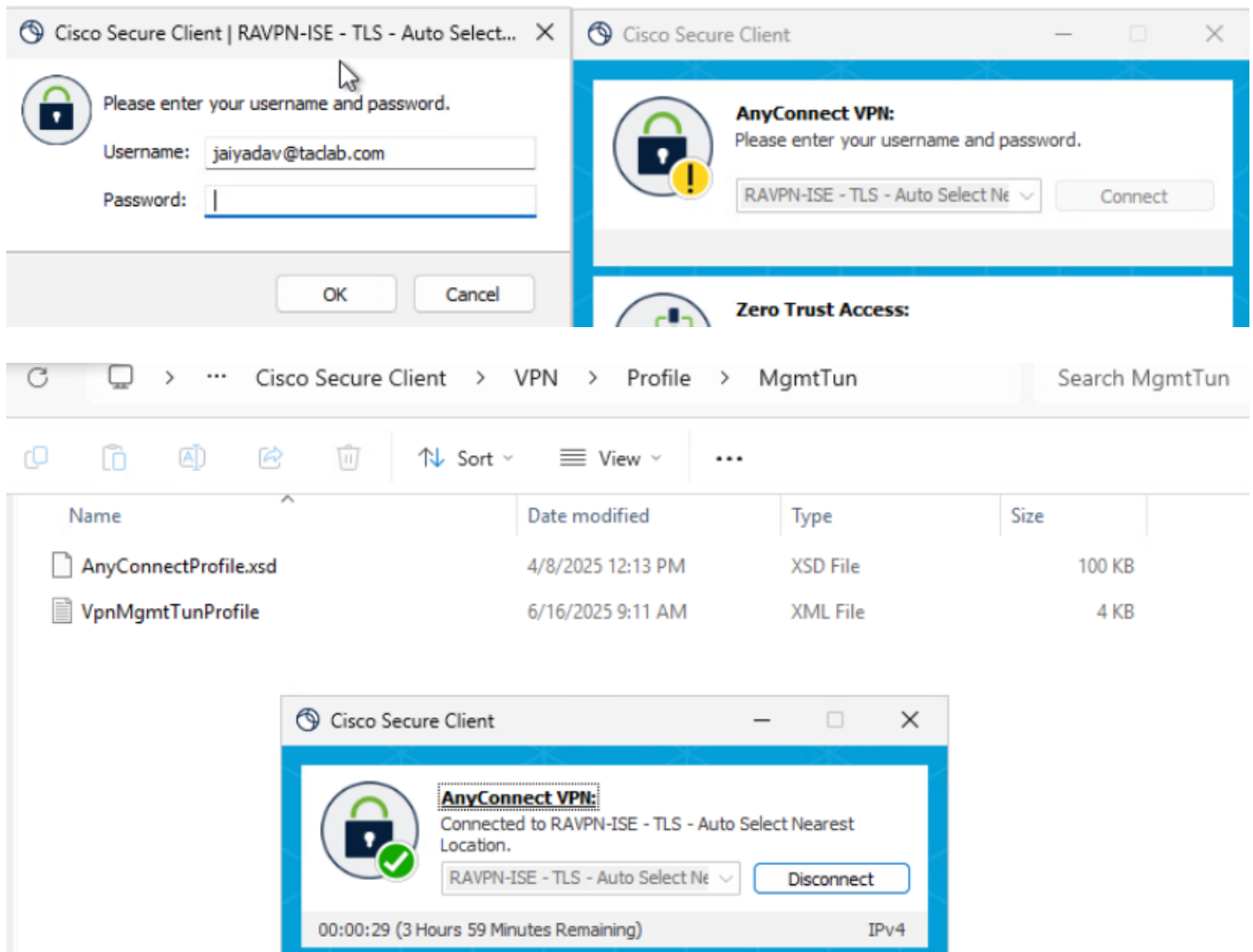
Stap 7 - Eindpuntcertificaat genereren en importeren

- MVO genereren, een MVO-generator of OpenSSL-tool openen
- Een eindpuntcertificaat genereren van CA
- Converteer het .cert bestand naar PKCS12 formaat
- Het PKCS12-certificaat importeren in het endpoint-certificaatarchief

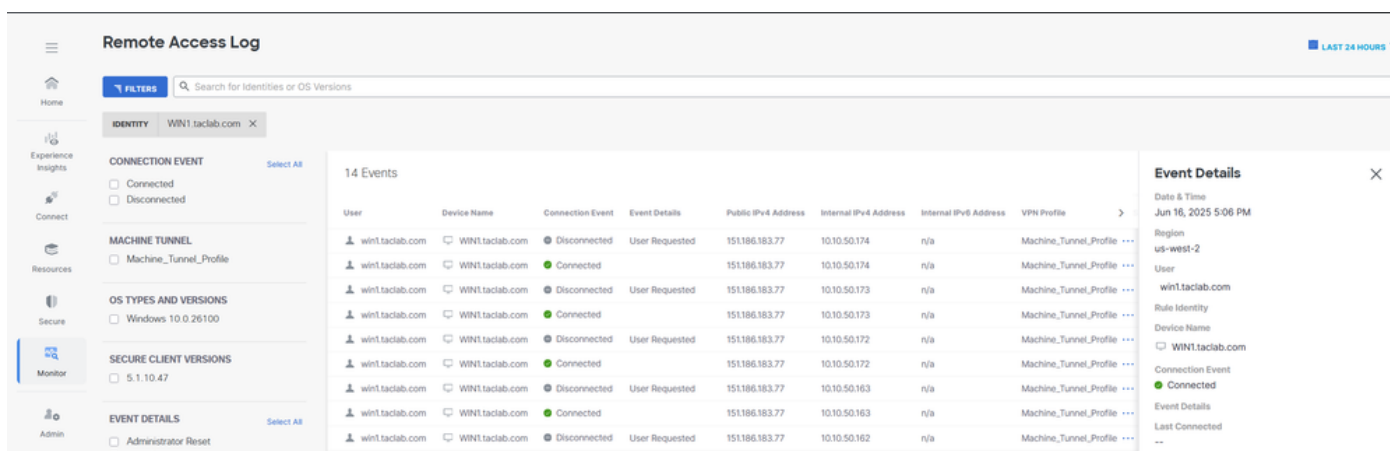
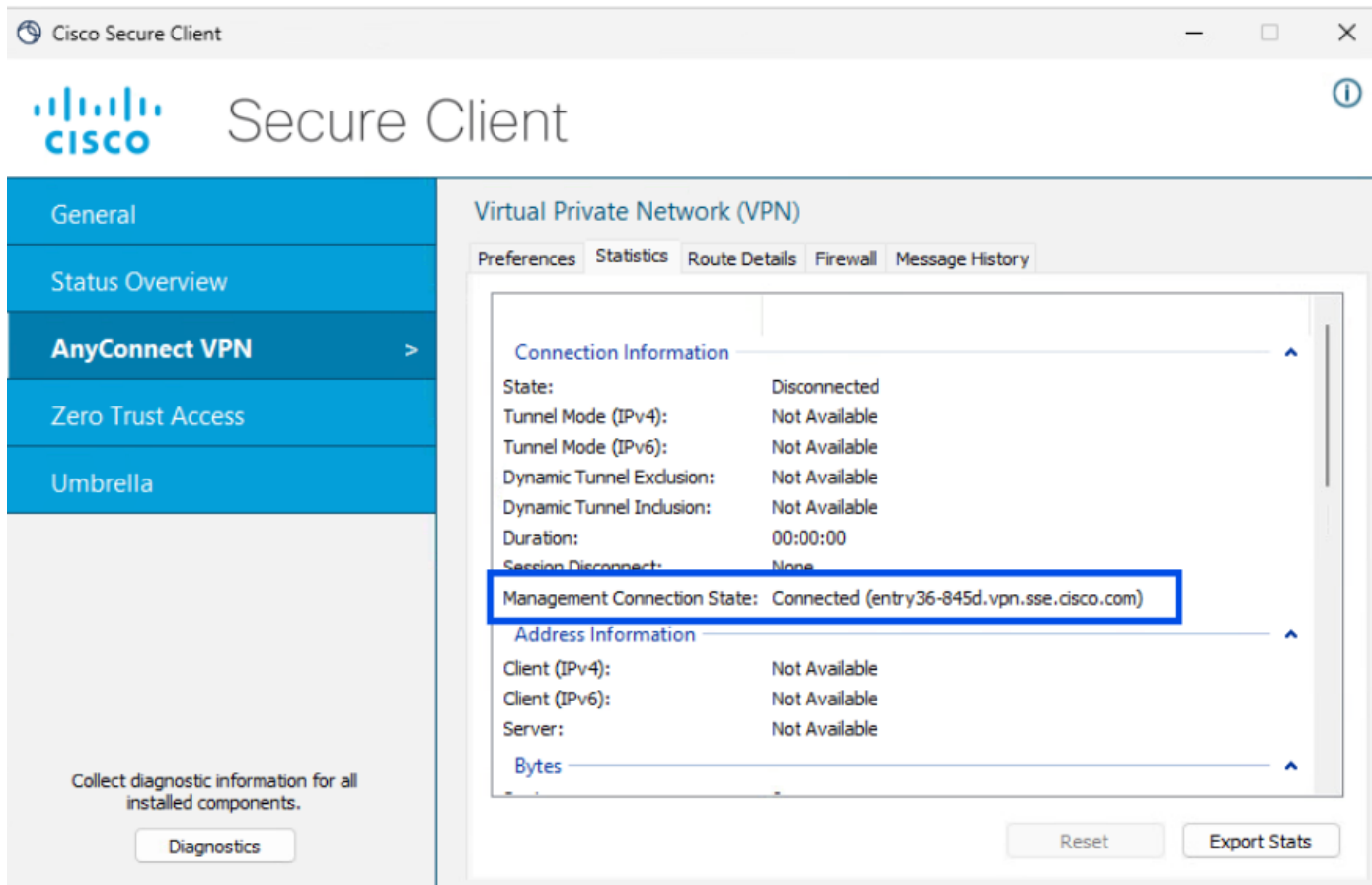


Stap 8 - Verbinding maken met de machinetunnel

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

Users, Groups, and Endpoint Devices

Provision and manage the authentication of users, groups, and endpoint devices, for access control purposes. [Help](#)

Users 10 Groups and Organizational Units 3 Endpoint Devices 4

Users

Manage your organization's users and their devices connections and enrollments. To add users, go to [Configuration management > Integrate directories](#). At any time, you can disconnect or unenroll a user's device. [Help](#)

Search: jaiyadav Source: Active Directory Directory: 1 results

Name	User Principal Name (UPN)	Auth Property	Source	Directory	Connected(VPN)	Enrolled(ZTNA)	Associated Rules
jaiyadav	jaiyadav@taclab.com	jaiyadav@taclab.com	onprem	Active Directory Profile	2	4 2 active	0

Rows per page: 10

Stap 6 - Gebruikersverificatie configureren

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

Users, Groups, and Endpoint Devices

Provision and manage the authentication of users, groups, and endpoint devices, for access control purposes. [Help](#)

Users 10 Groups and Organizational Units 3 Endpoint Devices 4

Users

Manage your organization's users and their devices connections and enrollments. To add users, go to [Configuration management > Integrate directories](#). At any time, you can disconnect or unenroll a user's device. [Help](#)

Search: Search Source: Directory 10 + results

3. Bewerk Active Directory onder Configurations

Configuration Management

Select how you want to connect users to Secure Access. [Help](#)

Configurations Advanced Settings

Directories

Add users, groups and endpoint devices to Secure Access through a supported IdP. [Help](#)

[Integrate directories](#)

Jay-IDP Azure	
Manually Added	
Active Directory	Edit
Components	

4. De eigenschap User Authentication instellen op Email

Users Authentication

Select the Authentication Property that will be used to authenticate AD Users.

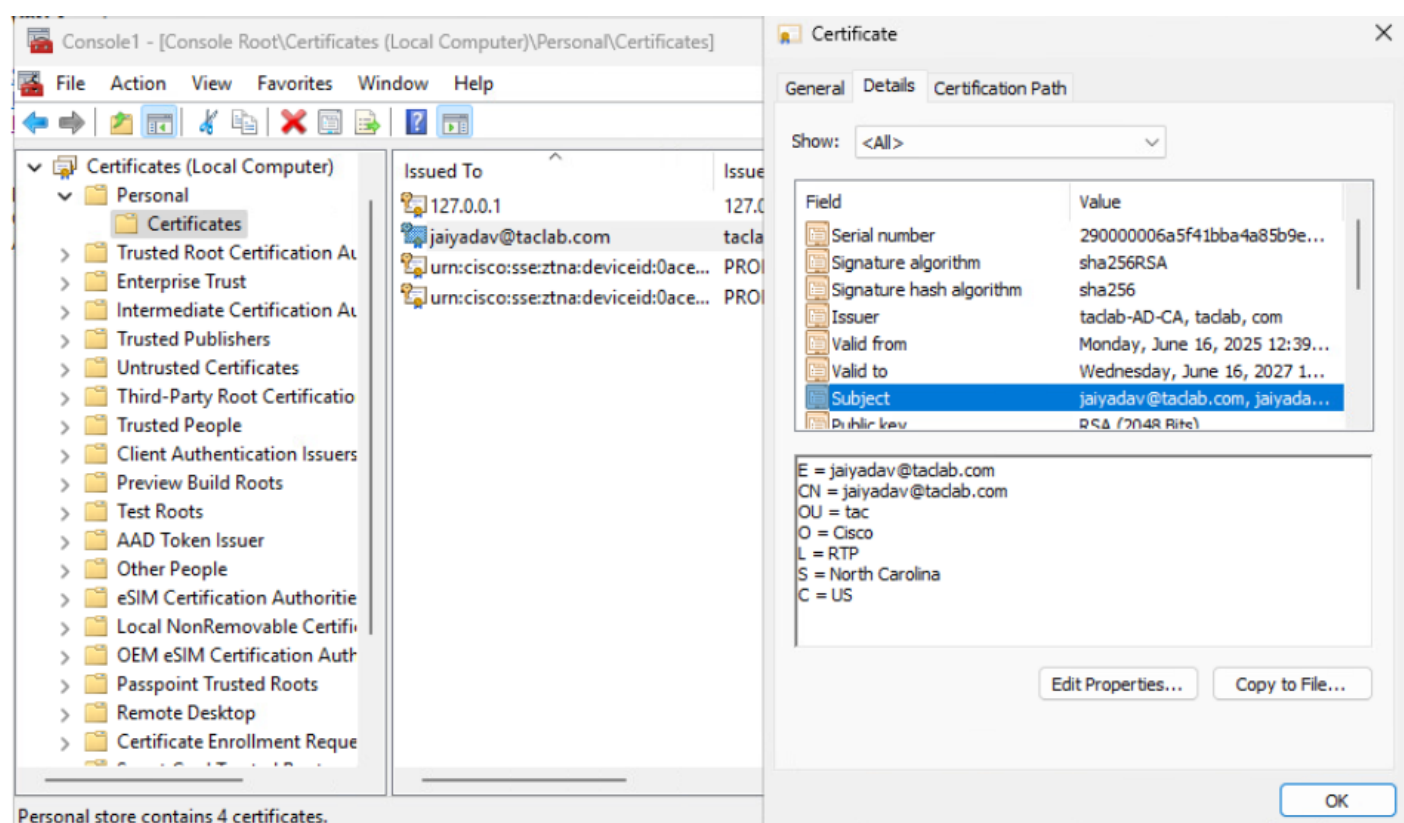
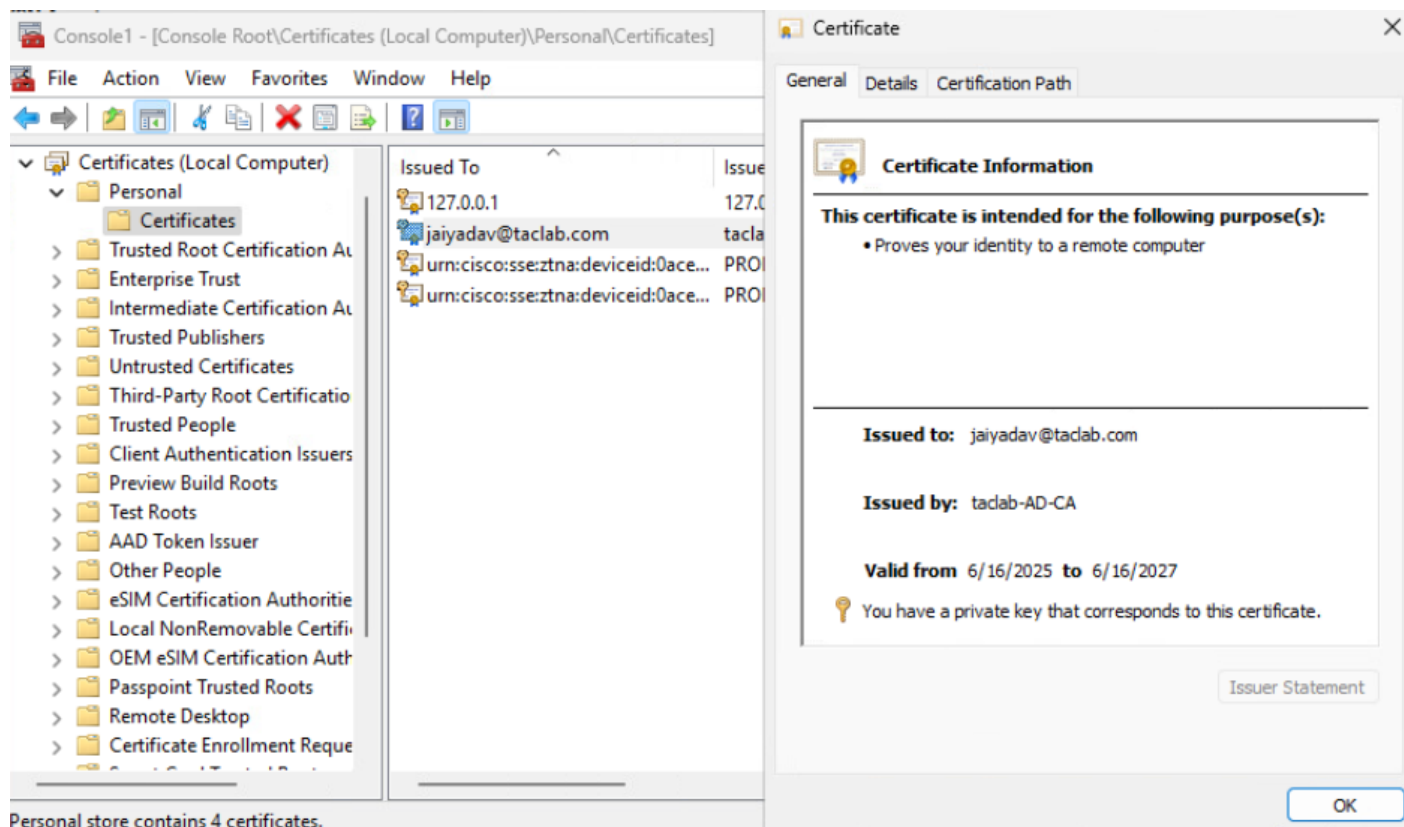
Authentication Property

Email

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

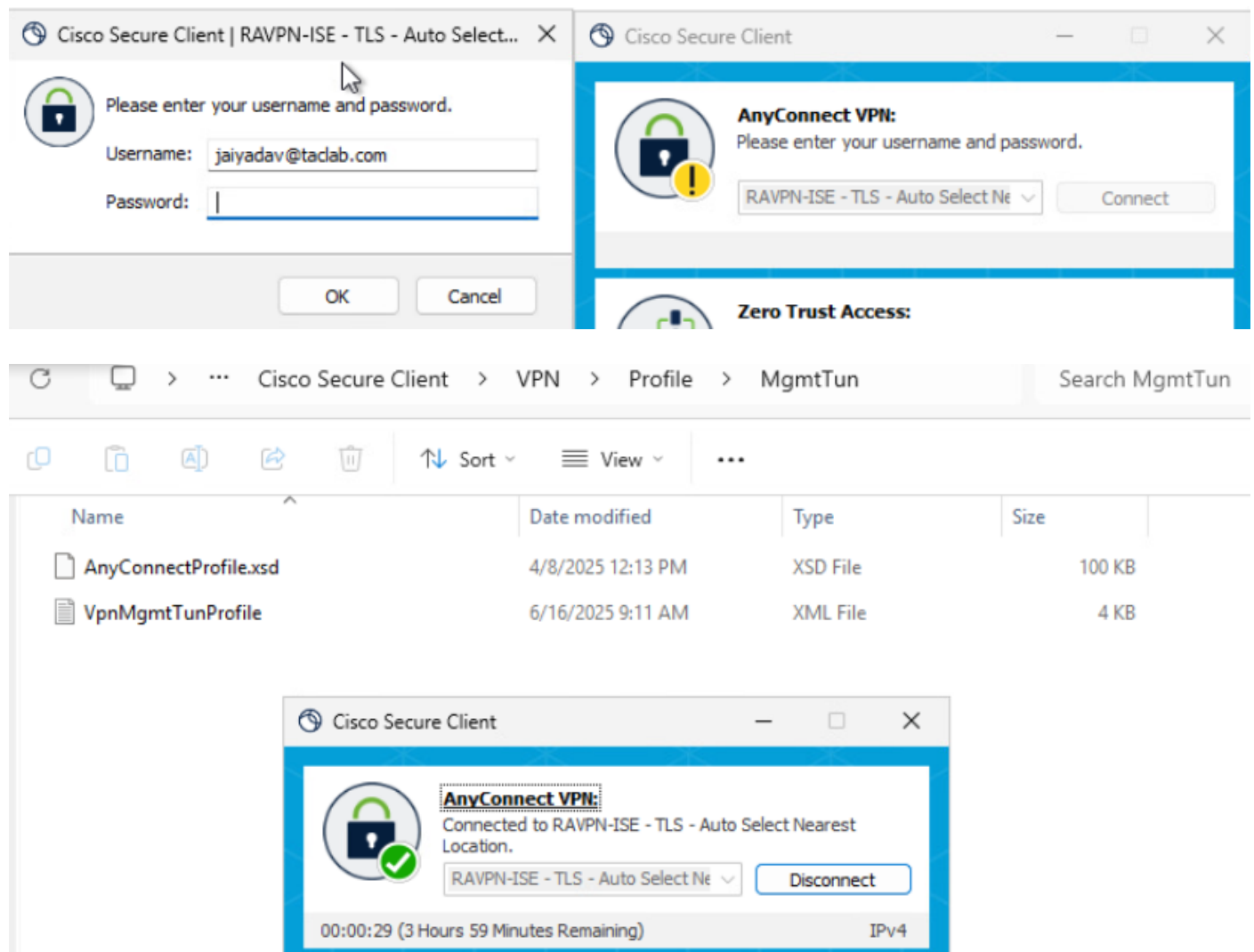
Stap 7 - Eindpuntcertificaat genereren en importeren

- MVO genereren, een MVO-generator of OpenSSL-tool openen
- Een eindpuntcertificaat genereren van CA
- Converteer het .cert bestand naar PKCS12 formaat
- 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

Secure Client

General

Status Overview

AnyConnect VPN >

Zero Trust Access

Umbrella

Collect diagnostic information for all installed components.

Diagnostics

Virtual Private Network (VPN)

Preferences

Statistics

Route Details

Firewall

Message History

Connection Information

State:

Disconnected

Tunnel Mode (IPv4):

Not Available

Tunnel Mode (IPv6):

Not Available

Dynamic Tunnel Exclusion:

Not Available

Dynamic Tunnel Inclusion:

Not Available

Duration:

00:00:00

Session Disconnect:

None

Management Connection State:

Connected (entry36-845d.vpn.sse.cisco.com)

Address Information

Client (IPv4):

Not Available

Client (IPv6):

Not Available

Server:

Not Available

Bytes

Reset

Export Stats

Remote Access Log

LAST 24 HOURS

Home

Experience Insights

Connect

Resources

Secure

Monitor

Admin

Filters

Search for Identities or OS Versions

MACHINE TUNNEL

Machine_Tunnel_Profile

IDENTITY

jaiyadav (jaiyadav@taclab.com)

CONNECTION EVENT

Connected

Disconnected

MACHINE TUNNEL

Machine_Tunnel_Profile

OS TYPES AND VERSIONS

Windows 10.0.26100

SECURE CLIENT VERSIONS

5.1.10.47

EVENT DETAILS

Administrator Reset

5 Events

User	Device Name	Connection Event	Event Details	Public IPv4 Address	Internal IPv4 Address	Internal IP
jaiyadav (jaiyadav@taclab.com)		Connected		76.39.159.129	10.10.50.110	n/a
jaiyadav (jaiyadav@taclab.com)		Disconnected	User Requested	76.39.159.129	10.10.50.11	n/a
jaiyadav (jaiyadav@taclab.com)		Connected		76.39.159.129	10.10.50.11	n/a
jaiyadav (jaiyadav@taclab.com)		Disconnected	User Requested	151.186.183.77	10.10.50.185	n/a
jaiyadav (jaiyadav@taclab.com)		Connected		151.186.183.77	10.10.50.185	n/a

Page: 1

Results per page: 50

1 - 5 of 5

Event Details

Date & Time

Jun 16, 2025 7:55 PM

Region

us-west-2

User

jaiyadav (jaiyadav@taclab.com)

Rule Identity

Device Name

Connection Event

Connected

Event Details

Last Connected

--

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.