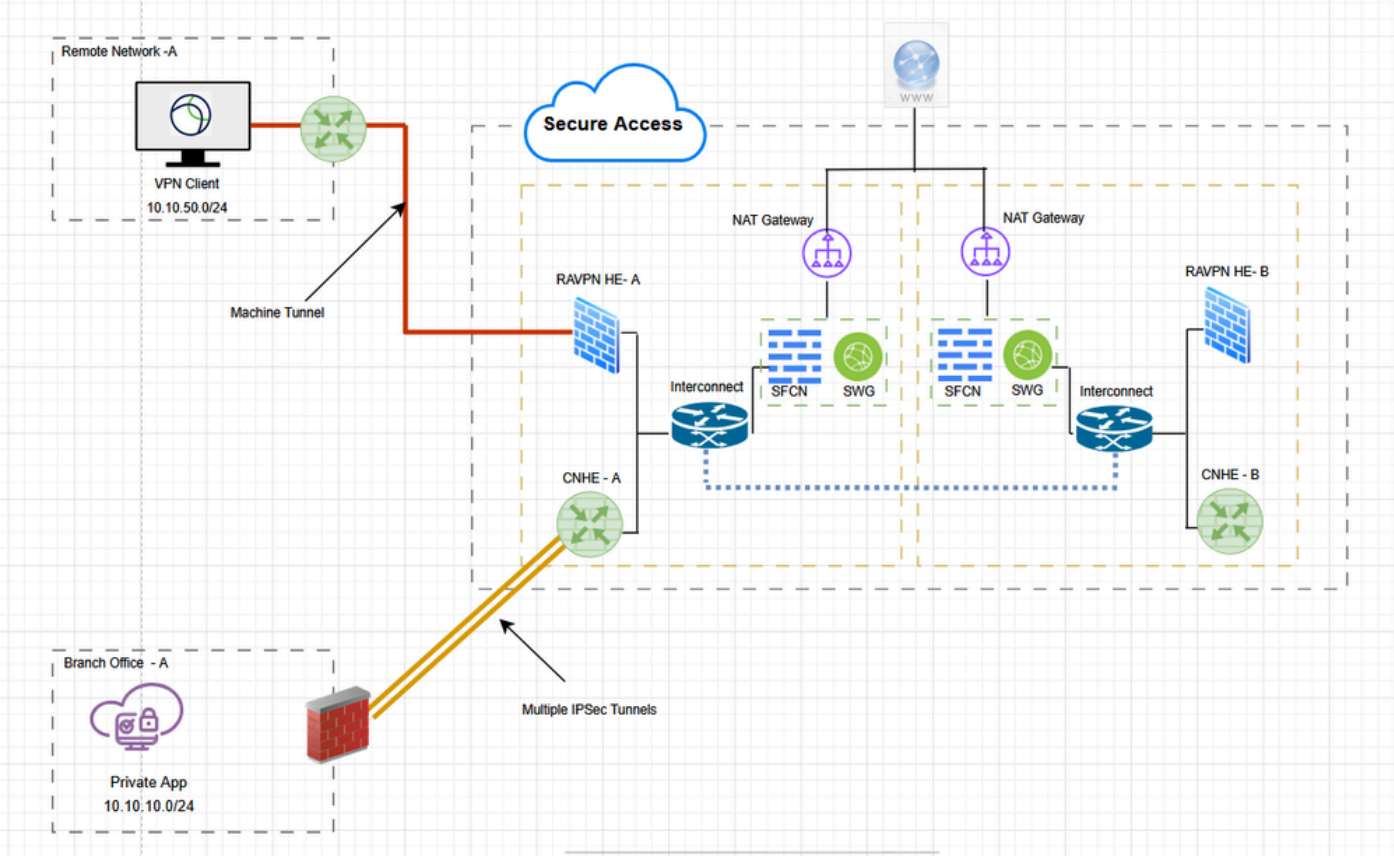
Konfigurieren von Maschinentunnel auf Cisco Secure Access

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Secure Access als VPN-Gateway konfigurieren und Verbindungen vom Secure Client über den VPN-Maschinentunnel akzeptieren.

Netzwerkdiagramm



Voraussetzungen

- Vollständige Administratorrolle in Secure Access.
- Mindestens ein in Cisco Secure Access konfiguriertes Benutzer-VPN-Profil
- Benutzer-IP-Pool in Cisco Secure Access

Anforderungen

Es wird empfohlen, dass Sie über Kenntnisse in den folgenden Themen verfügen:

- 509 Zertifikate
- OpenSSL

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Sicherer Zugriff von Cisco
- Cisco Secure Client 5.1.10
- Windows 11
- Windows Server 2019 - CA

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Ein Secure Access VPN-Maschinentunnel stellt die Verbindung zum Unternehmensnetzwerk sicher, wenn das Client-System hochgefahren wird, nicht nur, wenn der Endbenutzer eine VPN-Verbindung herstellt. Sie können das Patch-Management auf Endgeräten außerhalb des Büros durchführen, insbesondere auf Geräten, die vom Benutzer nur selten über VPN mit dem Büronetzwerk verbunden werden. Auch Betriebssystem-Anmeldeskripts für Endgeräte, die eine Verbindung mit dem Unternehmensnetzwerk benötigen, profitieren von dieser Funktion. Damit dieser Tunnel ohne Benutzereingriff erstellt werden kann, wird eine zertifikatbasierte Authentifizierung verwendet.

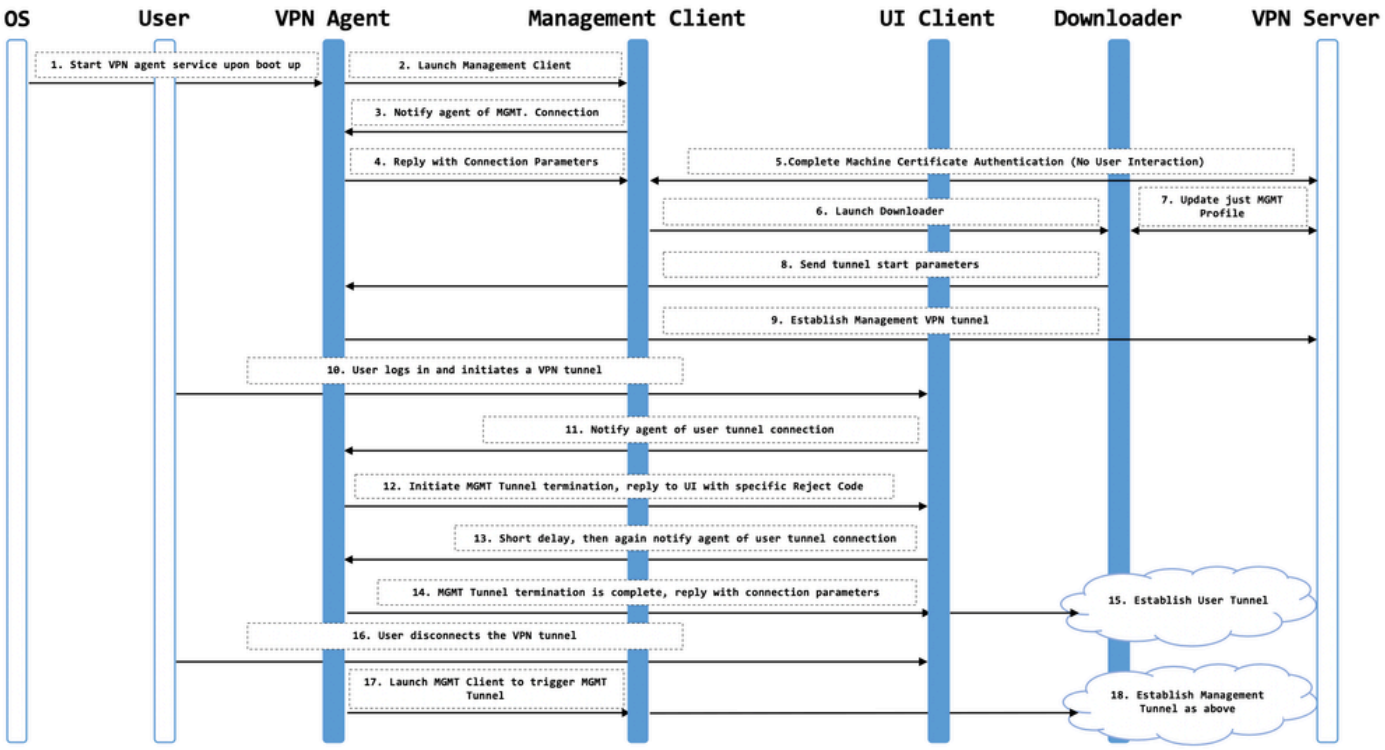
Der Secure Access-Maschinentunnel ermöglicht es Administratoren, den Cisco Secure Client ohne Benutzereingriff anzuschließen, bevor sich der Benutzer anmeldet. Der Maschinentunnel für sicheren Zugriff wird ausgelöst, wenn sich das Endgerät außerhalb des Firmengeländes befindet und nicht mit einem benutzerinitiierten VPN verbunden ist. Der Secure Access VPN-Maschinentunnel ist für den Endbenutzer transparent und trennt die Verbindung automatisch, wenn der Benutzer das VPN initiiert.

Arbeiten am Maschinentunnel

Der Secure Client VPN Agent-Dienst wird beim Systemstart automatisch gestartet. Der Secure Client VPN-Agent verwendet das VPN-Profil, um zu erkennen, dass die Maschinentunnel-Funktion aktiviert ist. Wenn die Maschinentunnel-Funktion aktiviert ist, startet der Agent die Verwaltungs-Client-Anwendung, um eine Maschinentunnel-Verbindung zu initiieren. Die Management-Client-Anwendung verwendet den Hosteintrag aus dem VPN-Profil, um die Verbindung zu initiieren. Dann wird der VPN-Tunnel wie üblich eingerichtet, mit einer Ausnahme: Während einer Maschinentunnelverbindung wird kein Software-Update durchgeführt, da der Maschinentunnel für den Benutzer transparent sein soll.

Der Benutzer initiiert über den Secure Client einen VPN-Tunnel, der die Terminierung des Maschinentunnels auslöst. Nach Abschluss des Maschinentunnels wird der Benutzertunnel wie gewohnt eingerichtet.

Der Benutzer trennt den VPN-Tunnel, was die automatische Wiederherstellung des Maschinentunnels auslöst.



Einschränkungen

- Es wird keine Benutzerinteraktion unterstützt.
- Es wird nur die zertifikatbasierte Authentifizierung über den Machine Certificate Store (Windows) unterstützt.
- Die strenge Überprüfung des Serverzertifikats wird erzwungen.
- Ein privater Proxy wird nicht unterstützt.
- Ein öffentlicher Proxy wird nicht unterstützt (ProxyNative-Wert wird auf Plattformen unterstützt, auf denen keine nativen Proxy-Einstellungen aus dem Browser abgerufen werden).
- Skripts für die sichere Client-Anpassung werden nicht unterstützt

Konfigurieren

Methode 1: Konfigurieren eines Maschinentunnels mit dem Benutzer machine@sse.com

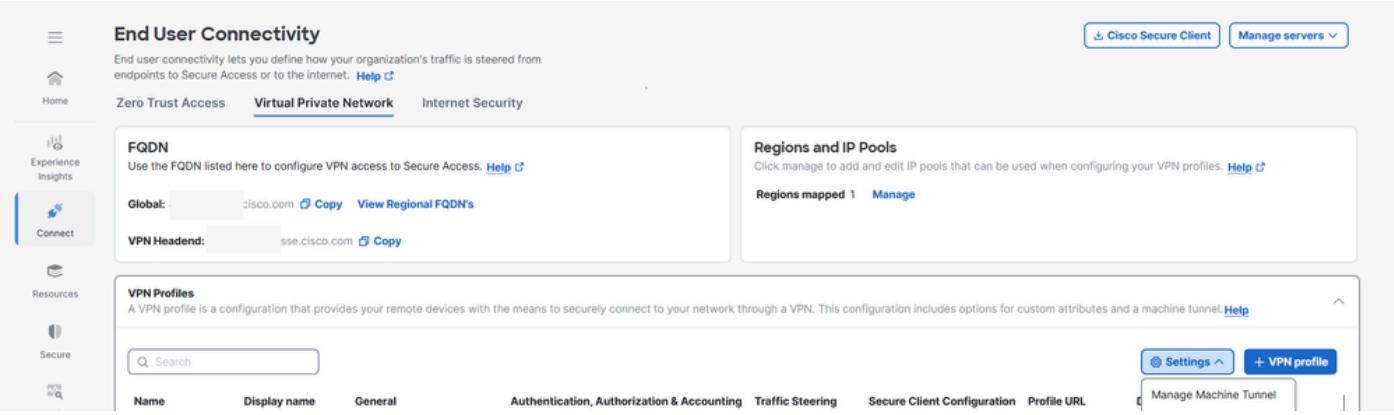
Schritt 1 - Allgemeine Einstellungen

Konfigurieren Sie die allgemeinen Einstellungen, einschließlich der Domäne und der Protokolle, die dieser Maschinentunnel verwendet.

1. Navigieren Sie zu Verbinden > Endbenutzerverbindung > Virtuelles privates Netzwerk.

2. Navigieren Sie zu VPN Profiles (VPN-Profile), und konfigurieren Sie die Einstellungen für den Maschinentunnel.

antwort: Klicken Sie auf Einstellungen, und wählen Sie dann Manage Machine Tunnel aus dem Dropdown-Menü aus.

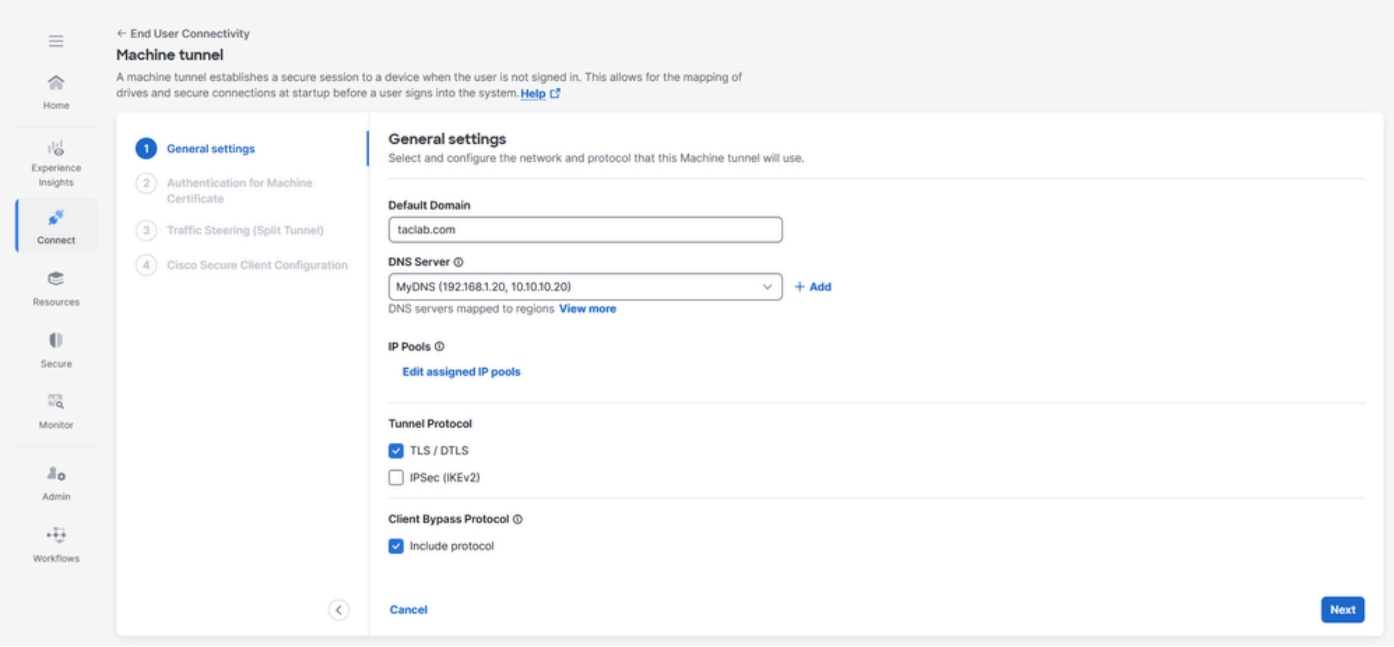


3. Geben Sie die Standarddomäne ein.
4. Der DNS-Server, der über die Seite Regionen und IP-Pools verwalten zugeordnet ist, wird als Standardserver festgelegt. Sie können den Standard-DNS-Server akzeptieren, einen anderen DNS-Server aus dem Dropdown-Menü auswählen oder auf + Hinzufügen klicken, um ein neues DNS-Serverpaar hinzuzufügen. Wenn Sie einen anderen DNS-Server auswählen oder einen neuen DNS-Server hinzufügen, wird dieser Standardserver überschrieben.
5. Wählen Sie aus dem Dropdown-Menü IP-Pools einen IP-Pool pro Region aus. Den VPN-Profilen muss mindestens ein IP-Pool in jeder Region zugewiesen sein, damit eine gültige Konfiguration möglich ist.
6. Wählen Sie das Tunnelprotokoll aus, das dieser Maschinentunnel verwendet:
   - TLS/DTLS
   - IPSec (IKEv2)

   Es muss mindestens ein Protokoll ausgewählt werden.
7. Aktivieren Sie optional das Kontrollkästchen Include protocol, um das Client-Umgehungsprotokoll durchzusetzen.

   antwort: Wenn das Client Bypass Protocol für ein IP-Protokoll aktiviert und kein Adresspool für dieses Protokoll konfiguriert ist (d. h., dass dem Client von der ASA keine IP-Adresse für dieses Protokoll zugewiesen wurde), wird kein IP-Datenverkehr, der dieses Protokoll verwendet, über den VPN-Tunnel gesendet. Es soll aus dem Tunnel heraus geschickt werden.

   b. Wenn das Client Bypass Protocol deaktiviert und kein Adresspool für dieses Protokoll konfiguriert ist, verwirft der Client nach Einrichtung des VPN-Tunnels den gesamten Datenverkehr für dieses IP-Protokoll.



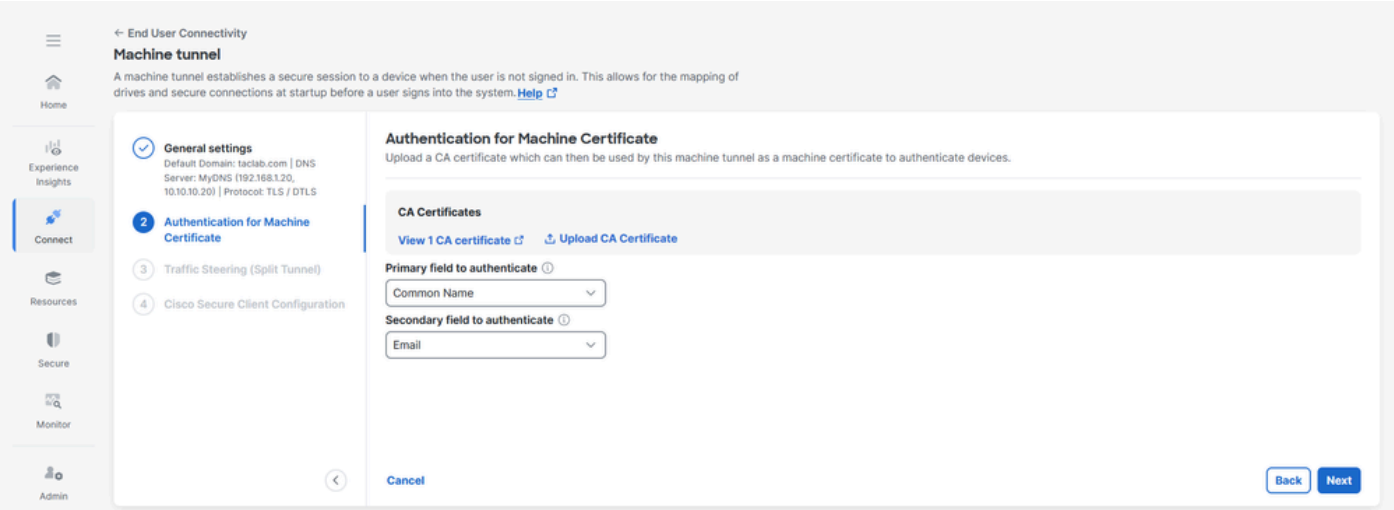
8. Klicken Sie auf Weiter

Schritt 2 - Authentifizierung für Computerzertifikat

Der Maschinentunnel ist für den Endbenutzer transparent und trennt die Verbindung automatisch, wenn der Benutzer eine VPN-Sitzung initiiert. Damit dieser Tunnel ohne Benutzereingriff erstellt werden kann, wird eine zertifikatbasierte Authentifizierung verwendet.

1. Wählen Sie CA-Zertifikate aus der Liste aus, oder klicken Sie auf CA-Zertifikate hochladen

2. Wählen Sie die zertifikatbasierten Authentifizierungsfelder aus. Weitere Informationen finden Sie unter [Zertifikatbasierte Authentifizierungsfelder.]



3. Klicken Sie auf Weiter

Schritt 3 - Verkehrssteuerung (Split-Tunnel)

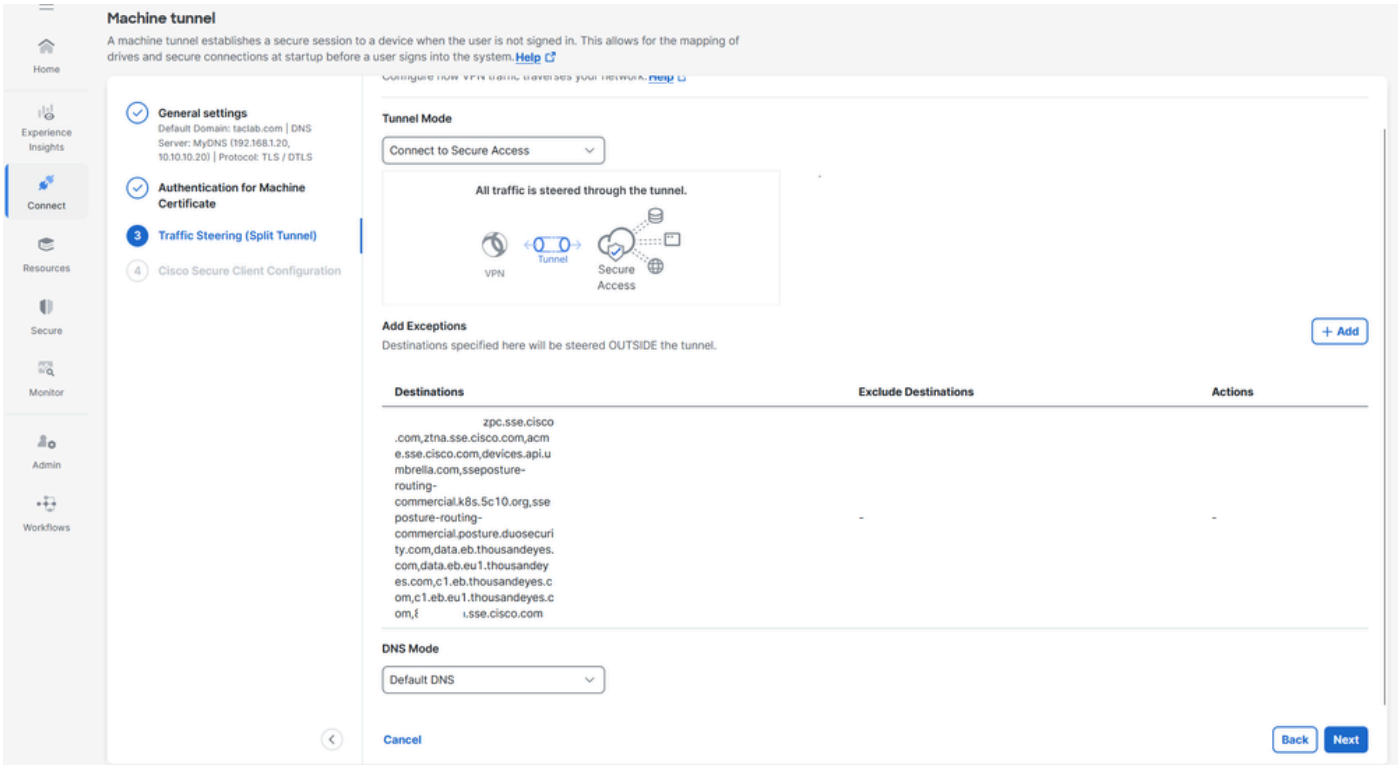
Für die Verkehrssteuerung (Split-Tunnel) können Sie einen Maschinentunnel so konfigurieren,

dass er eine vollständige Tunnelverbindung zu Secure Access aufrechterhält, oder ihn so konfigurieren, dass er eine Split-Tunnelverbindung verwendet, um den Verkehr nur bei Bedarf durch das VPN zu leiten.Weitere Informationen finden Sie unter Maschinentunnel-Verkehrssteuerung

1. Wählen Sie den Tunnelmodus

2. Je nach Auswahl des Tunnelmodus können Sie Ausnahmen hinzufügen.

3. DNS-Modus auswählen

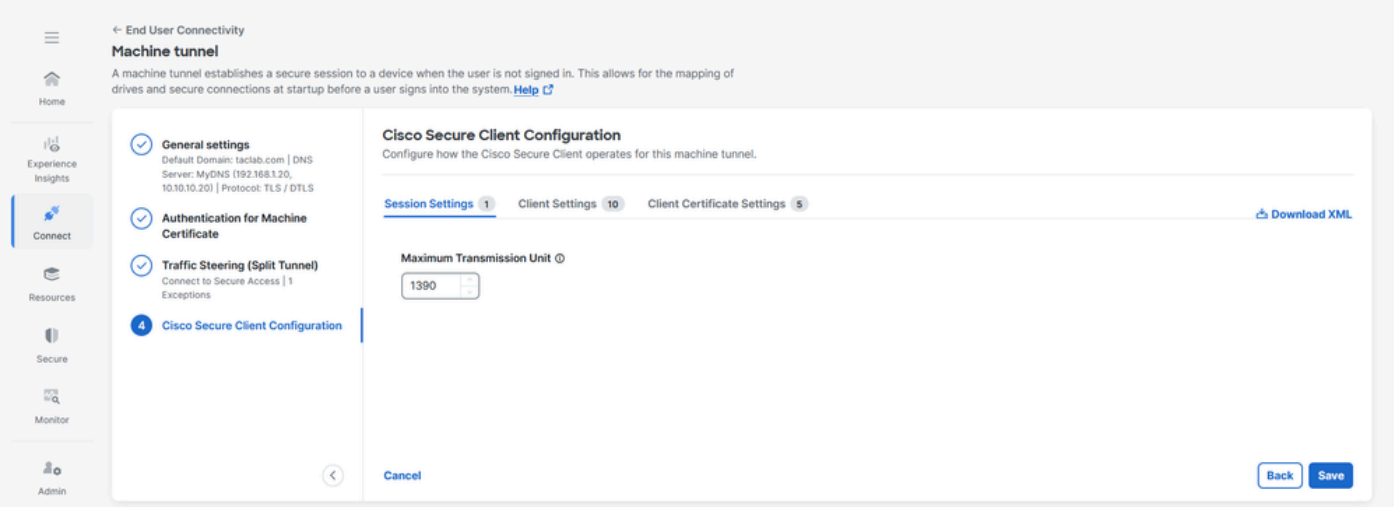


4. Klicken Sie auf Weiter

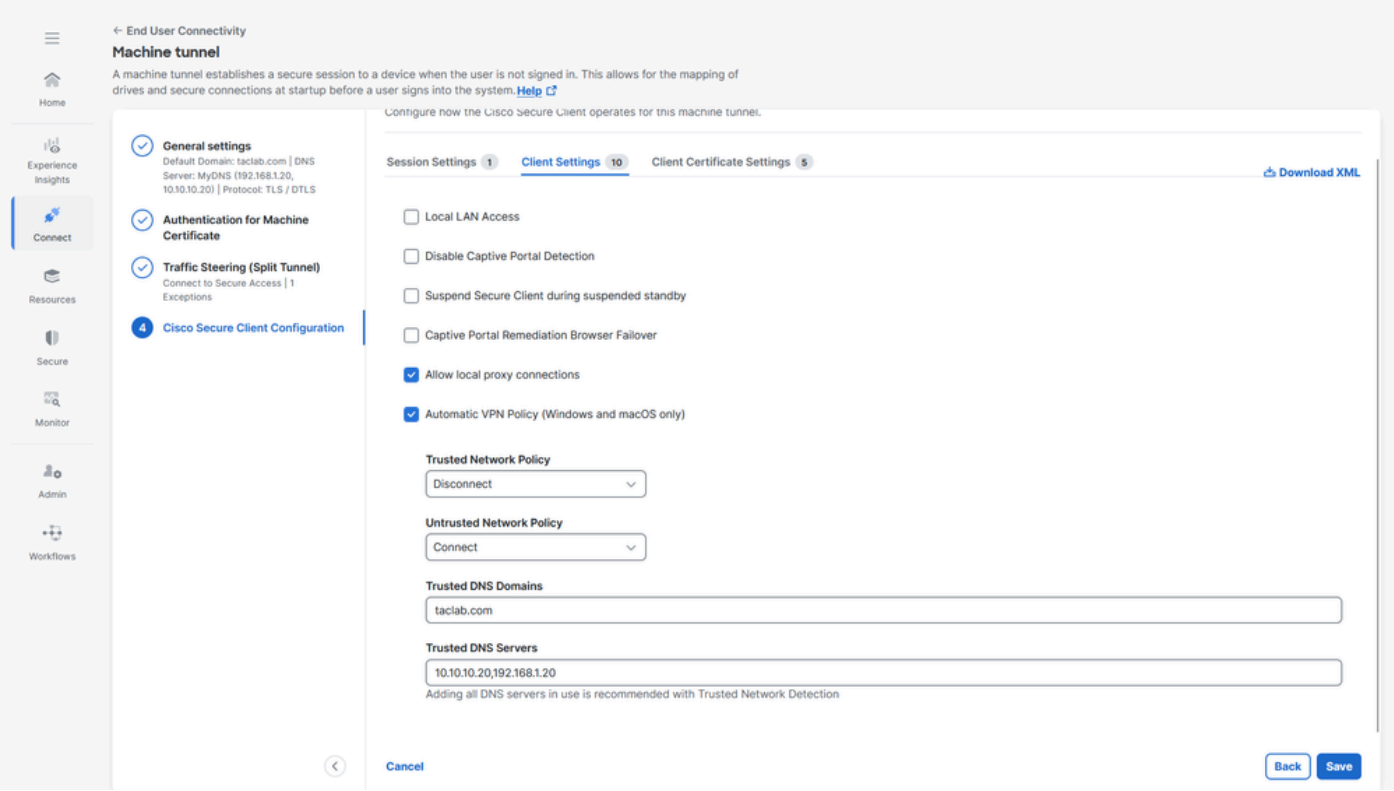
Schritt 4: Konfiguration des Cisco Secure Client

Sie können eine Teilmenge der Cisco Secure Client-Einstellungen je nach den Anforderungen eines bestimmten VPN-Maschinentunnels ändern. Weitere Informationen finden Sie unter Sichere Client-Konfiguration

1. Überprüfen Sie die maximale Übertragungseinheit, die größte Paketgröße, die im VPN-Tunnel ohne Fragmentierung gesendet werden kann.



2. Client-Einstellungen finden Sie weitere Informationen in den Einstellungen für den Maschinentunnel-Client



3. Client-Zertifikateinstellungen, wählen Sie die Optionen entsprechend

a. Überschreiben des Windows-Zertifikatspeichers - Ermöglicht es einem Administrator, Secure Client anzuweisen, Zertifikate im Zertifikatspeicher des Windows-Computers (lokales System) für die Clientzertifikatauthentifizierung zu verwenden.

b. Automatische Zertifikatauswahl - Wenn auf dem sicheren Gateway mehrere Zertifikatauthentifizierungen konfiguriert sind

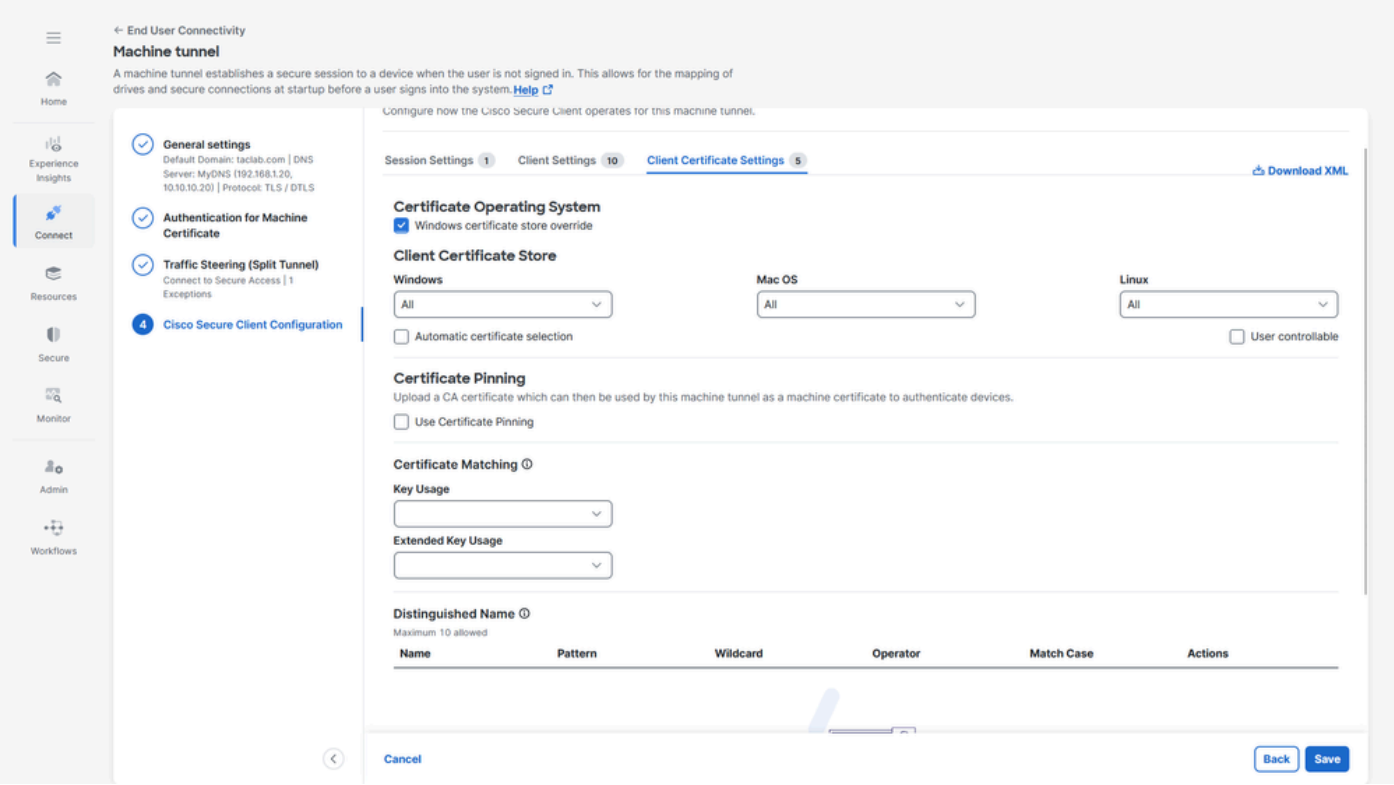
c. Certificate Pinning - CA-Zertifikat, das vom Maschinentunnel als Computerzertifikat zur Authentifizierung von Geräten verwendet werden kann

d. Zertifikatzuordnung - Wenn keine Kriterien für die Zertifikatzuordnung angegeben sind, wendet Cisco Secure Client die Regeln für die Zertifikatzuordnung an.

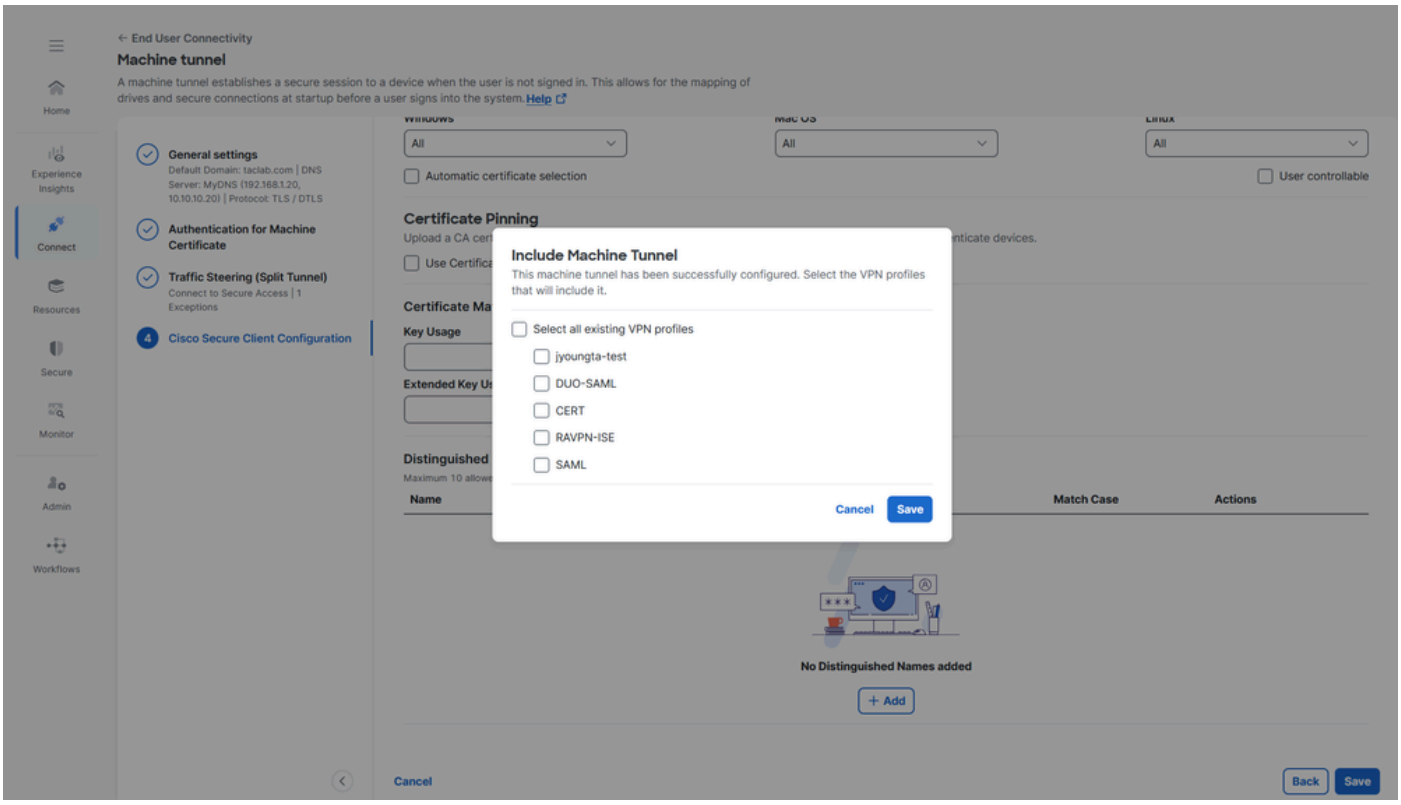
i. Schlüsselverwendung: Digitale Signatur

ii) Erweiterte Schlüsselverwendung: Client-Authentifizierung

e. Distinguished Name: Definiert Distinguished Names (DNs) für exakte Übereinstimmungskriterien bei der Auswahl akzeptabler Clientzertifikate. Wenn Sie mehrere Distinguished Names hinzufügen, wird jedes Zertifikat mit allen Einträgen abgeglichen, und alle müssen übereinstimmen.

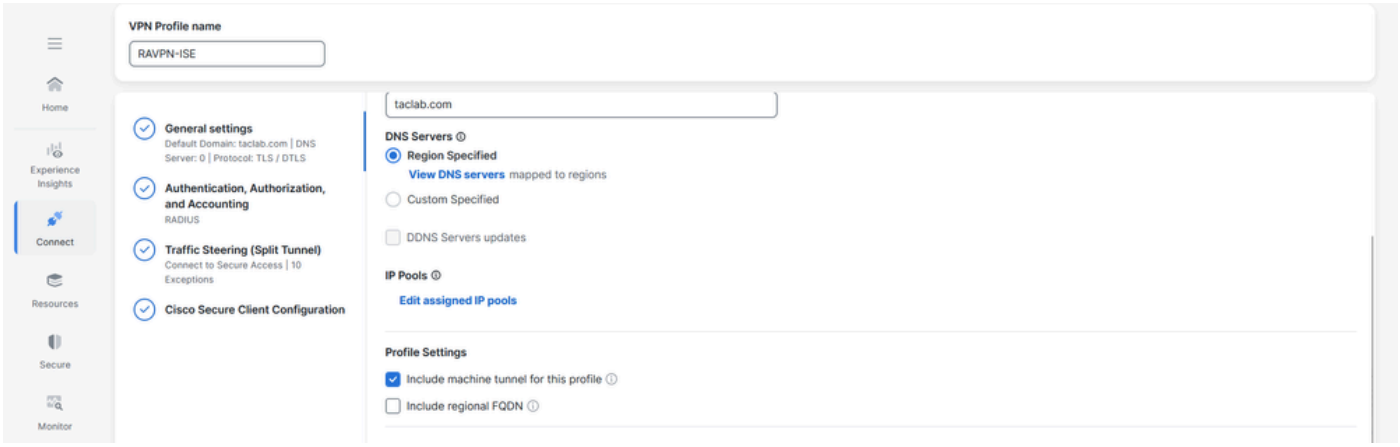


4. Weisen Sie einem Benutzer-VPN-Profil ein Computertunnelprofil zu, klicken Sie auf Speichern, und wählen Sie anschließend die Benutzer-VPN-Profile aus.



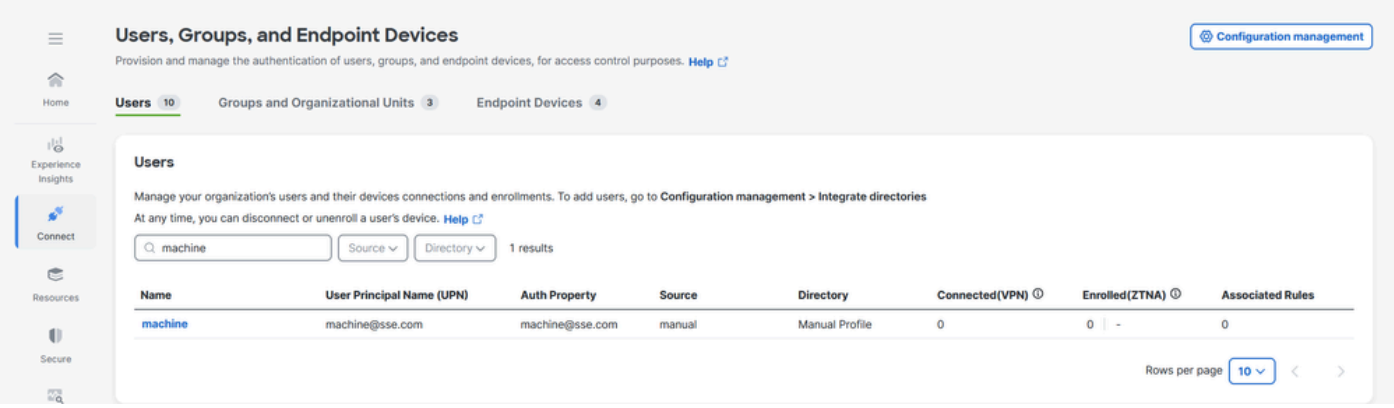
5. Klicken Sie auf Speichern

6. Überprüfen Sie, ob das Maschinentunnelprofil mit einem Benutzer-VPN-Profil verbunden ist.



Schritt 5: Überprüfen, ob der Benutzer machine@sse.com im Cisco Secure Access-System vorhanden ist

1. Navigieren Sie zu Verbinden > Benutzer, Gruppen und Endgeräte > Benutzer



2. Wenn machine@sse.com Benutzer nicht vorhanden ist, den Import manuell. Weitere Informationen finden Sie unter Manueller Import von Benutzern und Gruppen

Schritt 6 - Erstellen eines CA-signierten Zertifikats für machine@sse.com

1. Generieren einer Zertifikatsignierungsanforderung

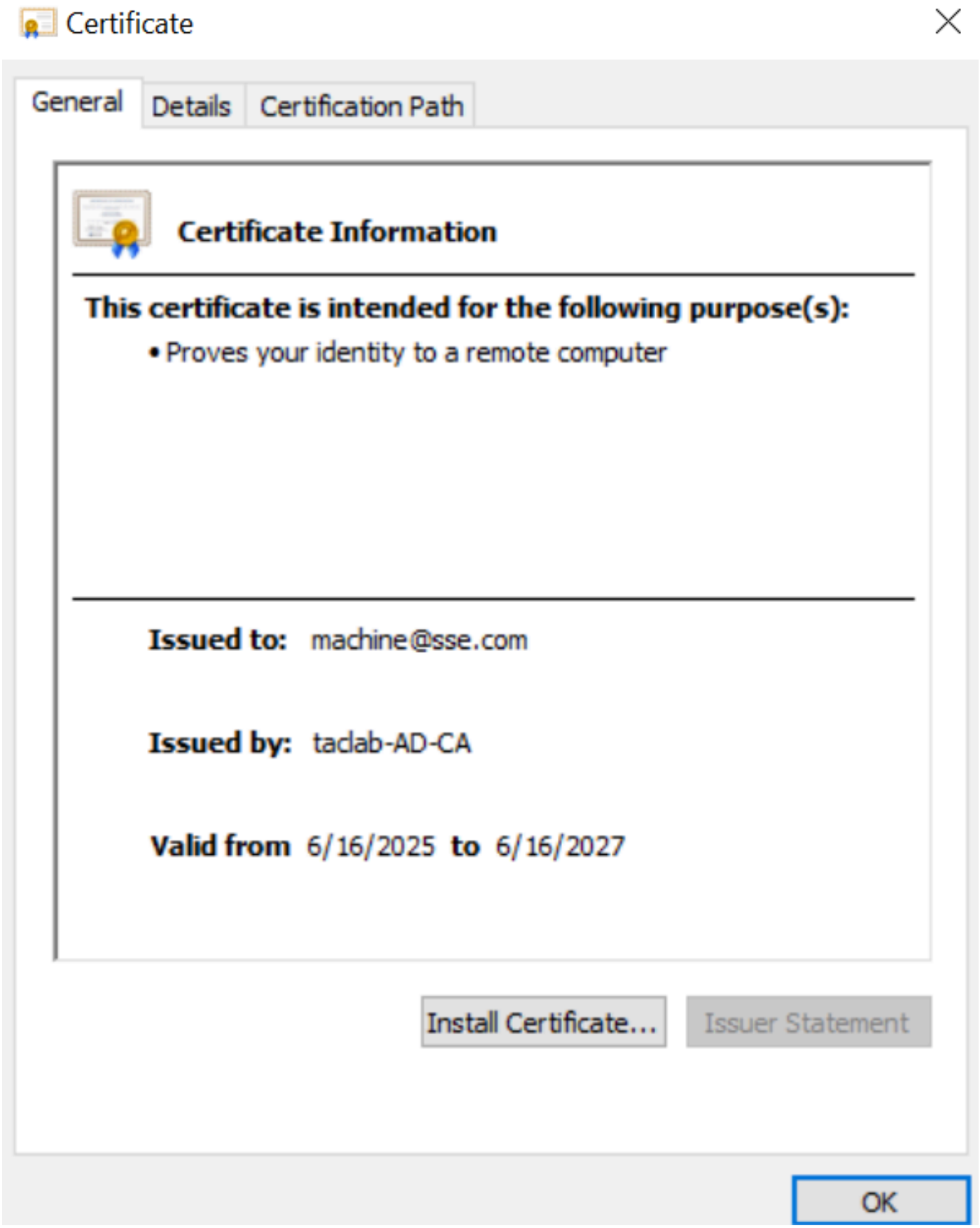
antwort: Wir können jede CSR-Generator-Software online verwenden, CSR Generator oder eine openssl CLI

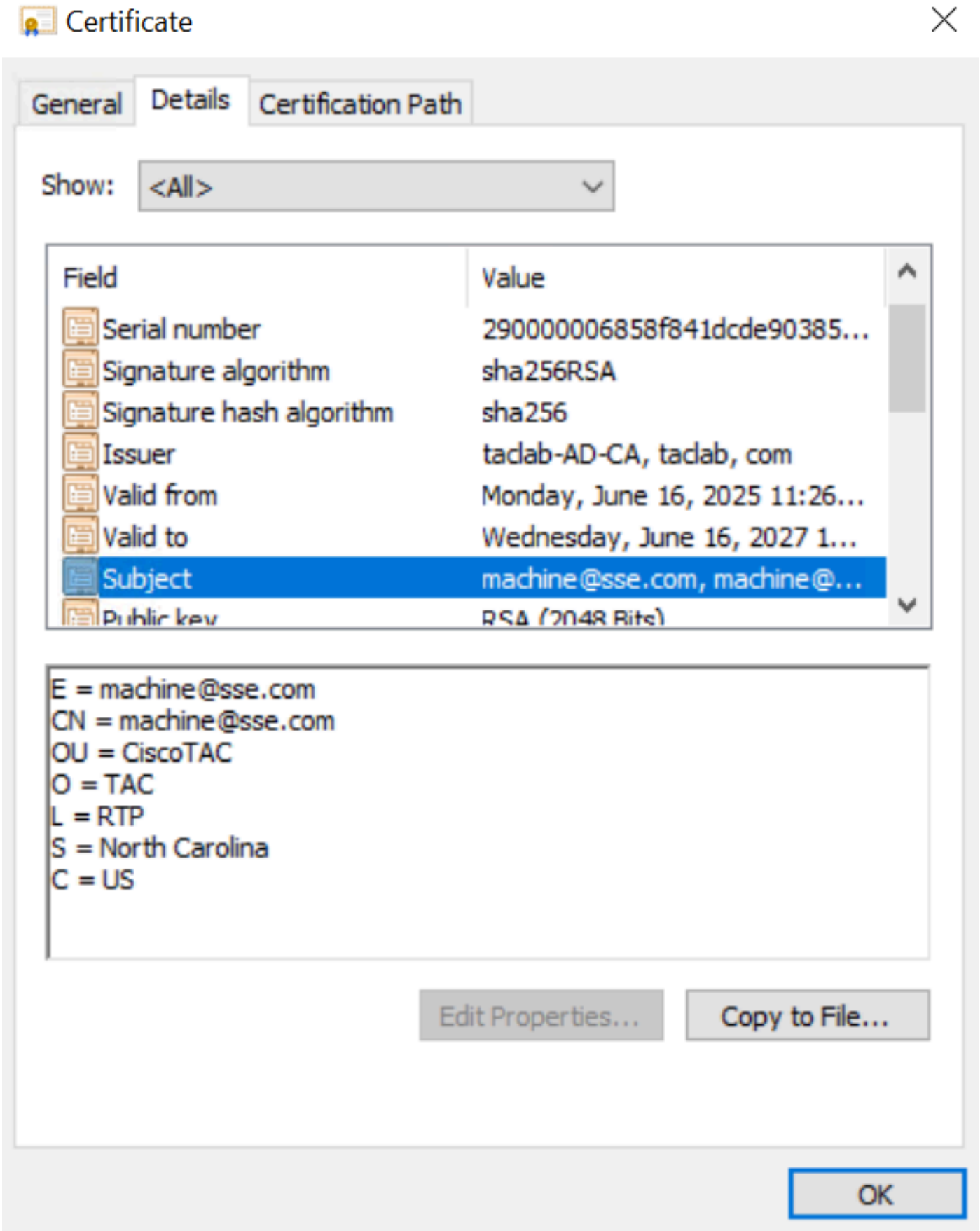
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr

```
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. Kopieren Sie den CSR, und generieren Sie ein Computerzertifikat.


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



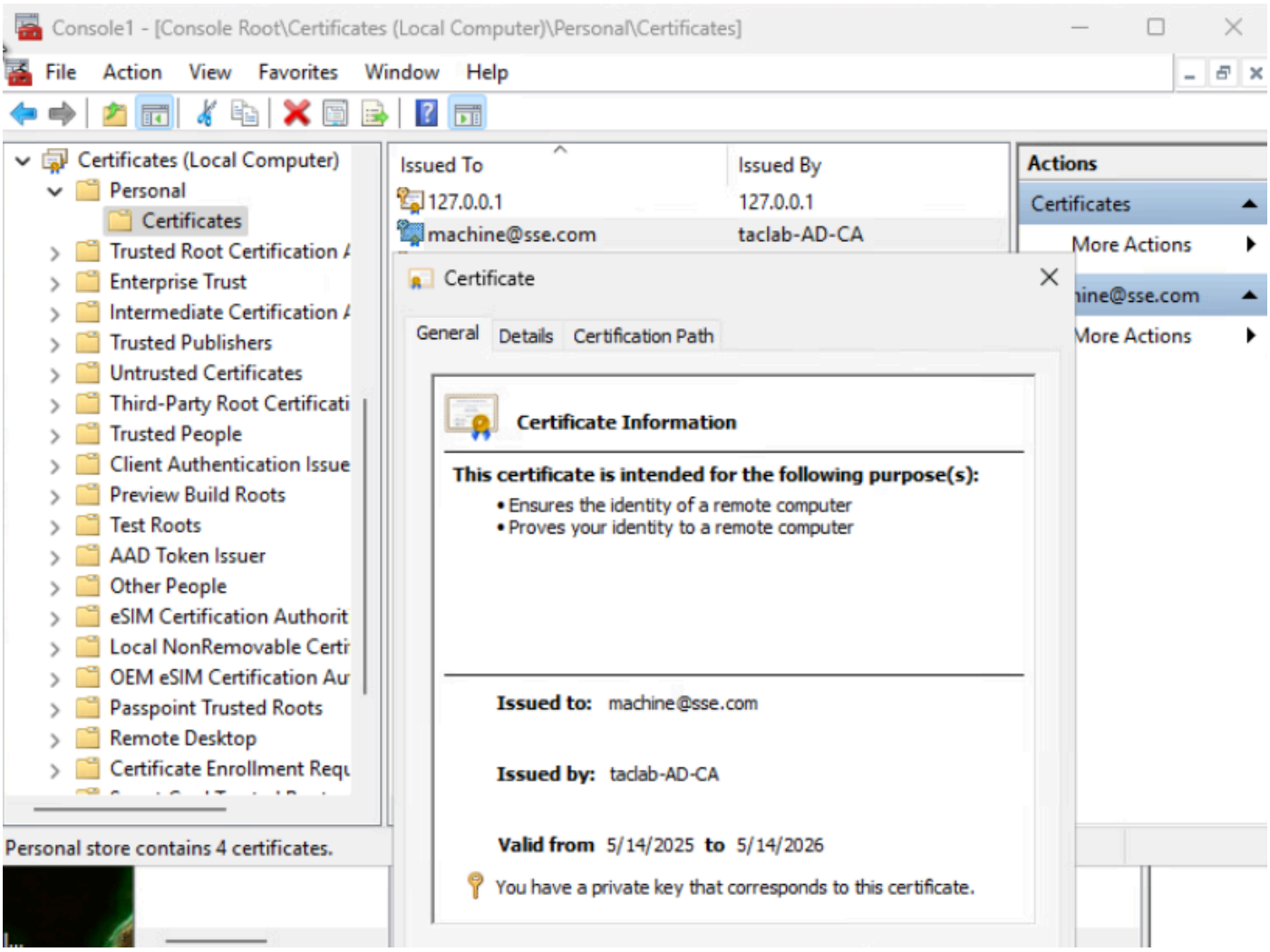
3. Konvertieren Sie das Computerzertifikat in das PKCS12-Format, indem Sie den in den vorherigen Schritten (Schritt 1 bzw. 2) generierten Schlüssel und das Zertifikat verwenden.

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#
```

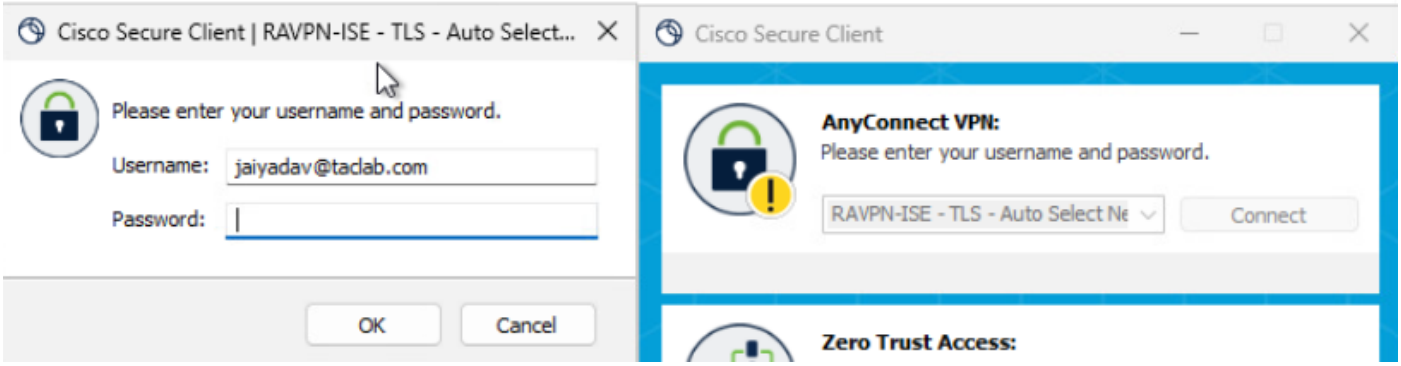
Schritt 7 - Importieren des Computerzertifikats auf einen Testcomputer

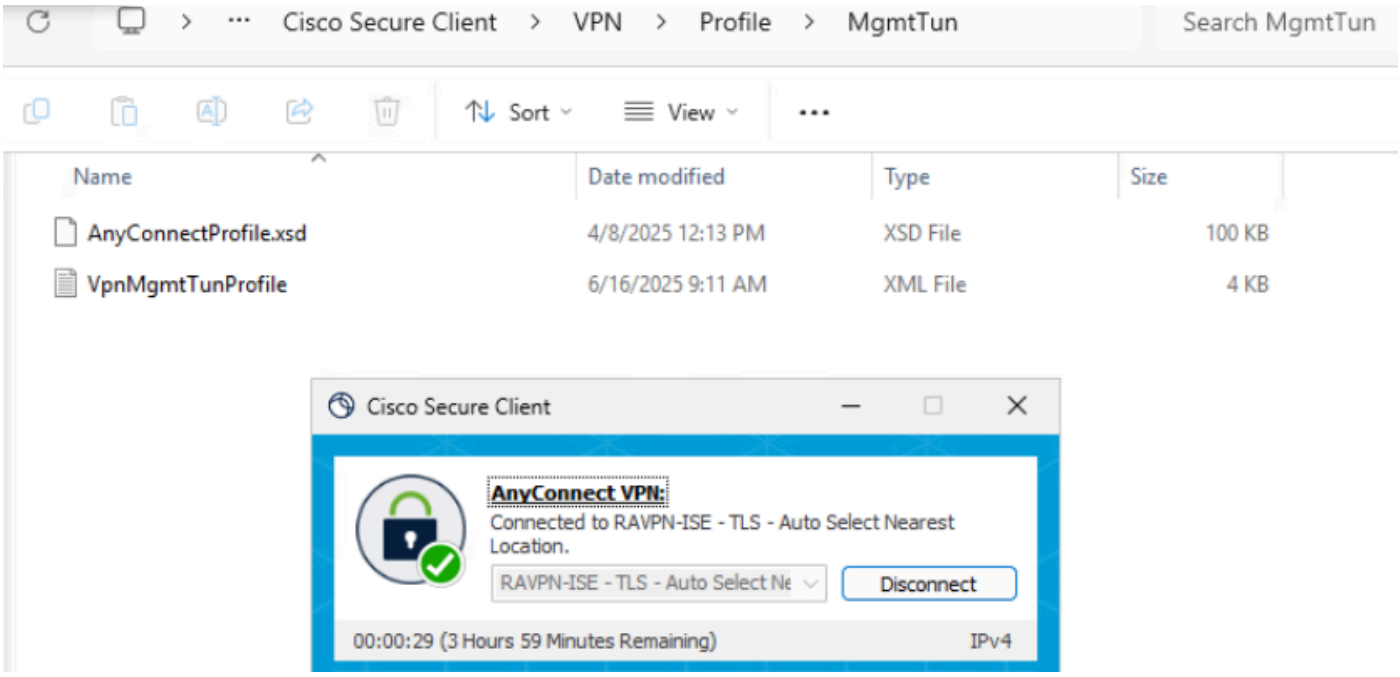
antwort: PKCS12-Computerzertifikat in lokalen Speicher oder Computerspeicher importieren



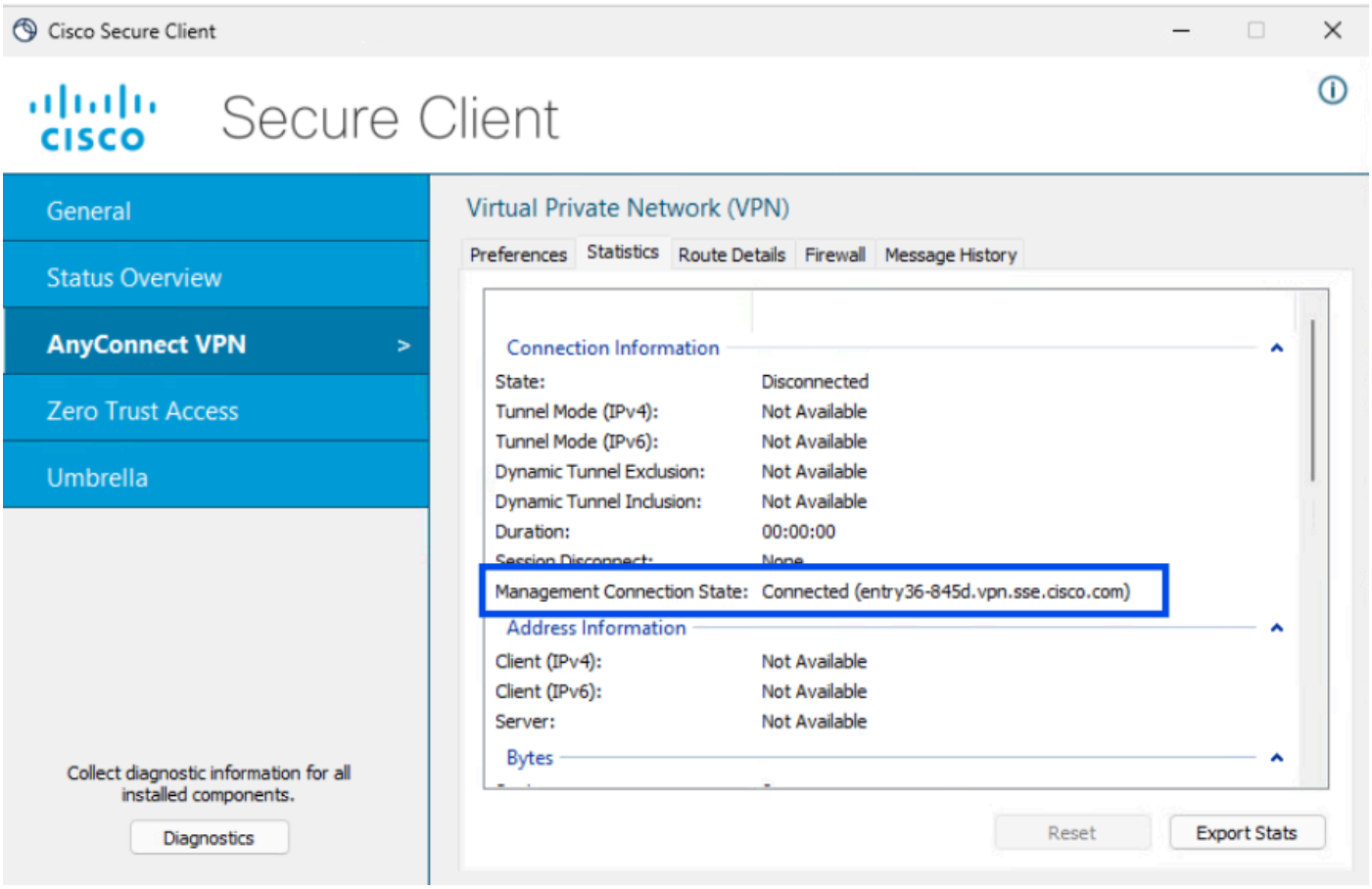
Schritt 8 - Herstellen einer Verbindung mit dem Maschinentunnel

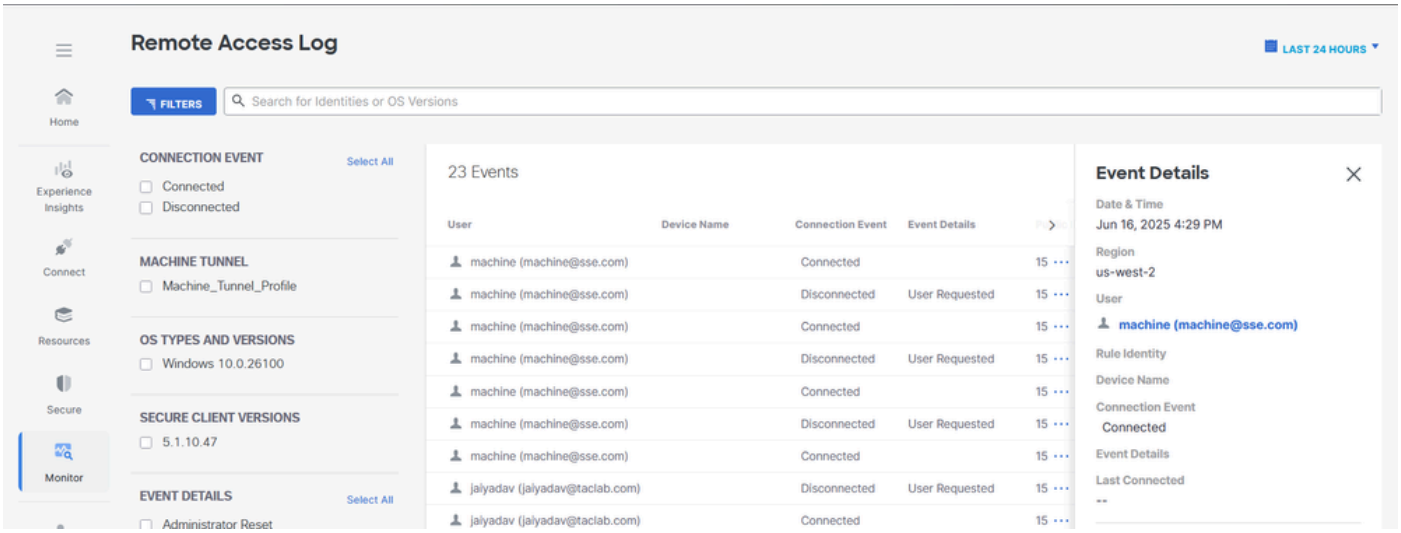
antwort: Stellt eine Verbindung zu einem Benutzertunnel her, löst dies das herunterzuladende XML-Computerprofil aus.





b. Überprüfen der Tunnelverbindung





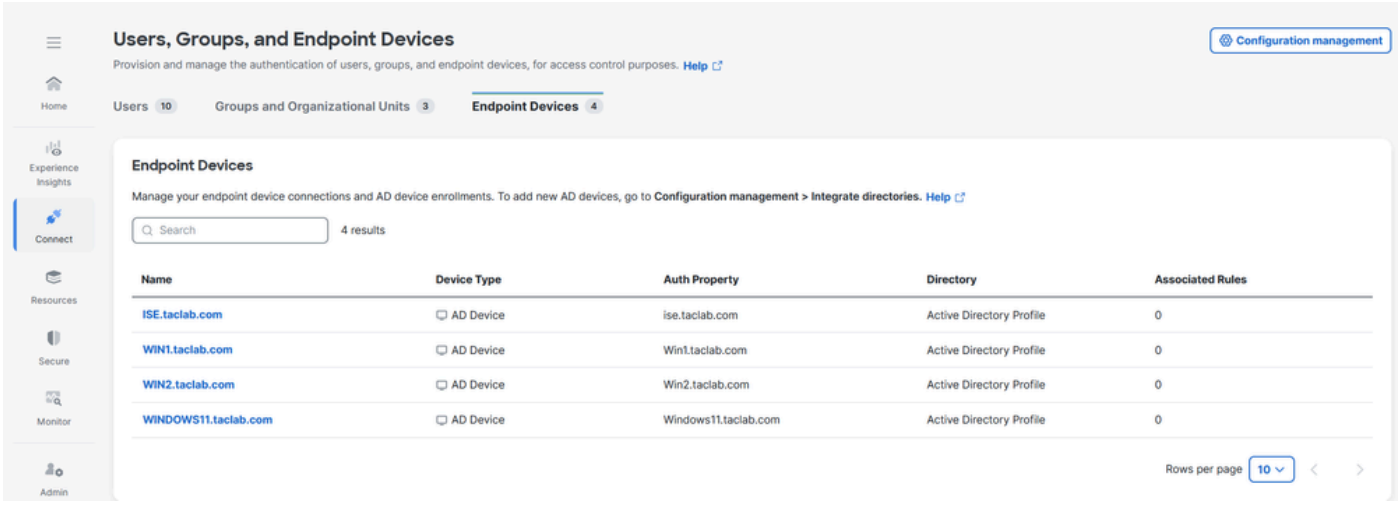
Methode 2: Konfigurieren des Maschinentunnels mithilfe des Endpunktzertifikats

In diesem Fall wählen Sie für das Primärfeld, das authentifiziert werden soll, das Zertifikatfeld aus, das den Gerätenamen (Computername) enthält. Secure Access verwendet den Gerätenamen als Tunnelkennung des Systems. Das Format des Computernamens muss mit dem Format der ausgewählten Gerätekennung übereinstimmen.

Durchlaufen der Schritte 1 bis 4 für die Konfiguration des Maschinentunnels

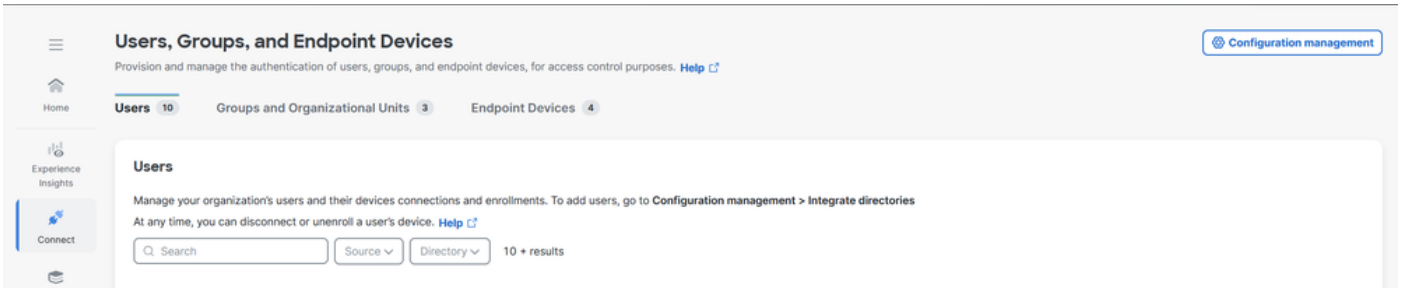
Schritt 5: Konfigurieren Sie den AD-Connector, um Endpunkte in Cisco Secure Access importieren zu können.

Weitere Informationen finden Sie unter [Dauerhafte Active Directory-Integration.]

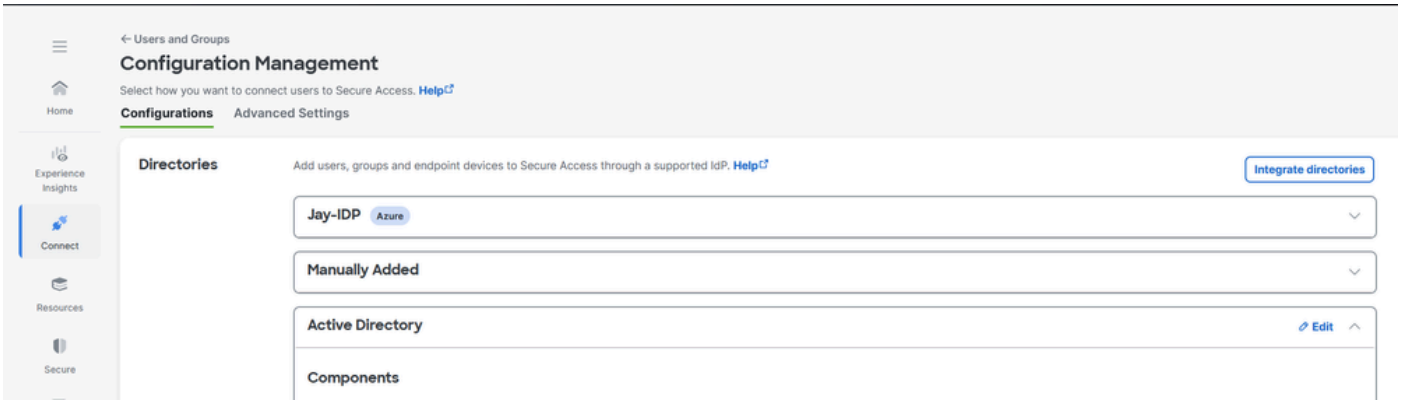


Schritt 6: Konfigurieren der Authentifizierung von Endgeräten

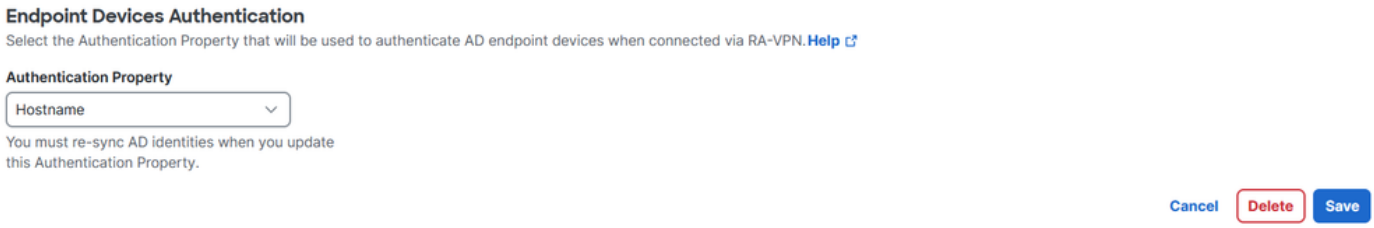
1. Navigieren Sie zu Verbinden > Benutzer, Gruppen und Endgeräte.
2. Klicken Sie auf Konfigurationsmanagement



3. Bearbeiten Sie unter Konfigurationen Active Directory.



4. Legen Sie die Authentifizierungseigenschaft für Endgeräte auf Hostname fest.



5. Klicken Sie auf Speichern und starten Sie die AD Connector-Dienste auf den Servern neu, auf denen die AD Connector-Dienste installiert sind

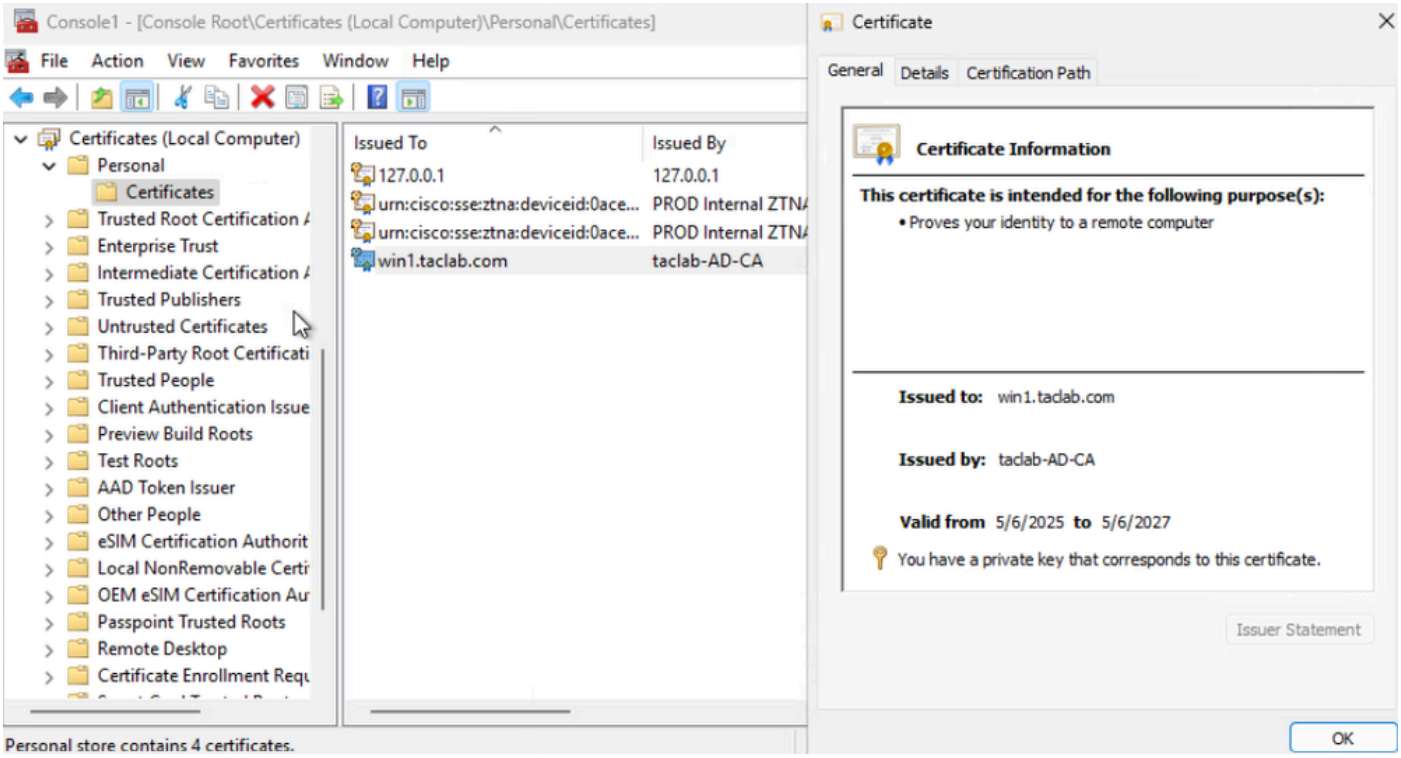
Schritt 7 - Generieren und Importieren eines Endpunktzertifikats

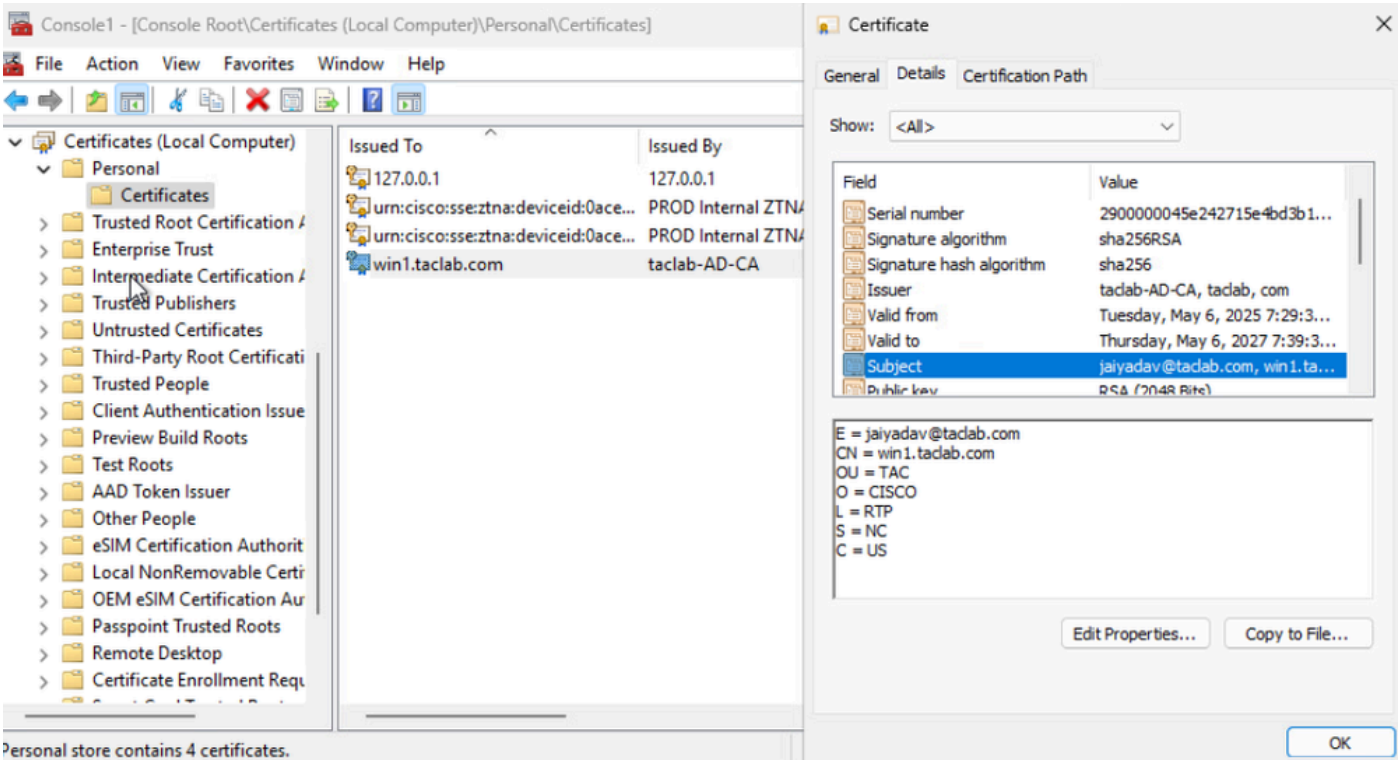
antwort: CSR generieren , CSR-Generator oder OpenSSL-Tool öffnen

b. Endpunktzertifikat von CA generieren

c. Konvertieren Sie die .cert-Datei in das PKCS12-Format

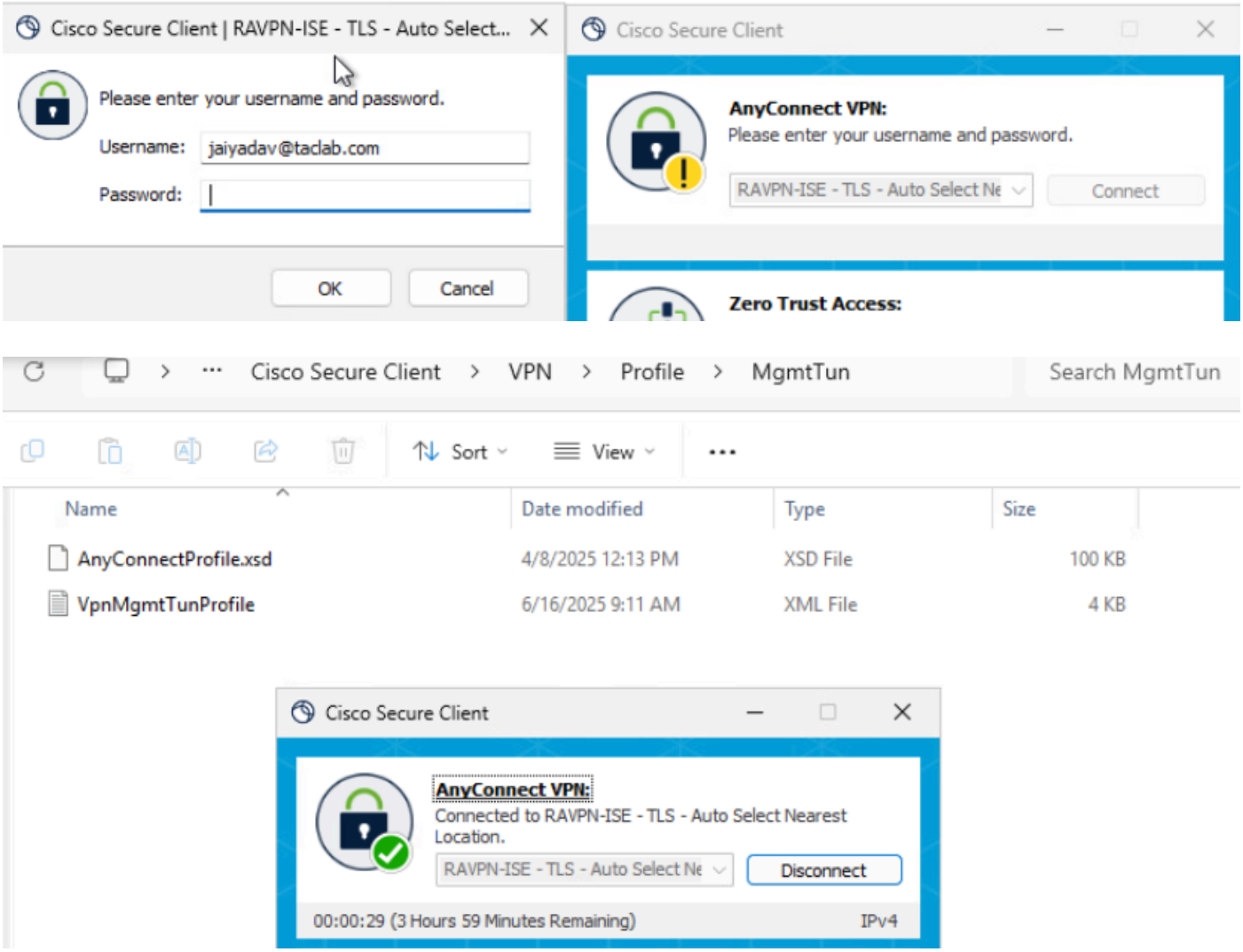
d. PKCS12-Zertifikat in Endpunktzertifikatsspeicher importieren



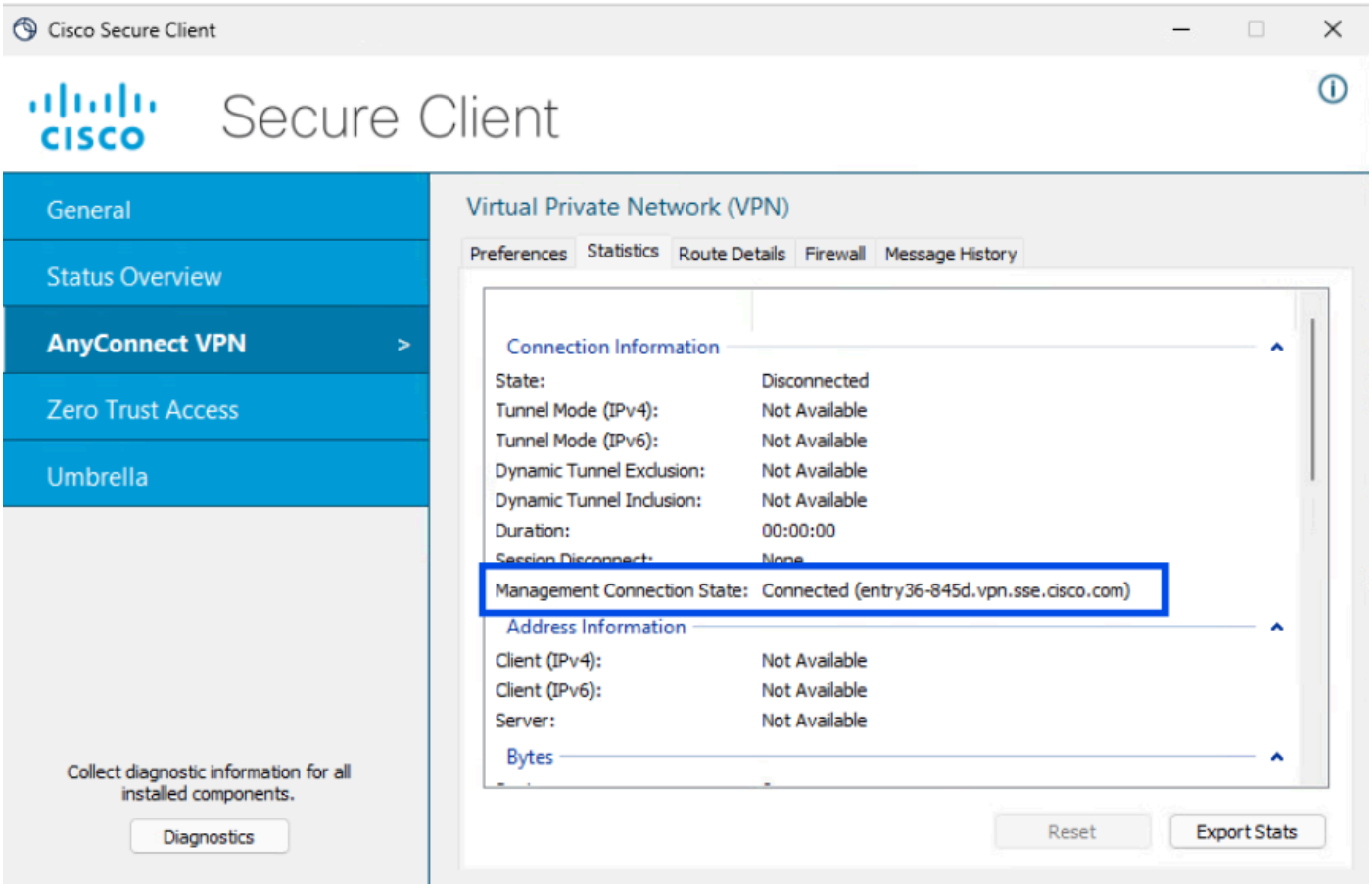


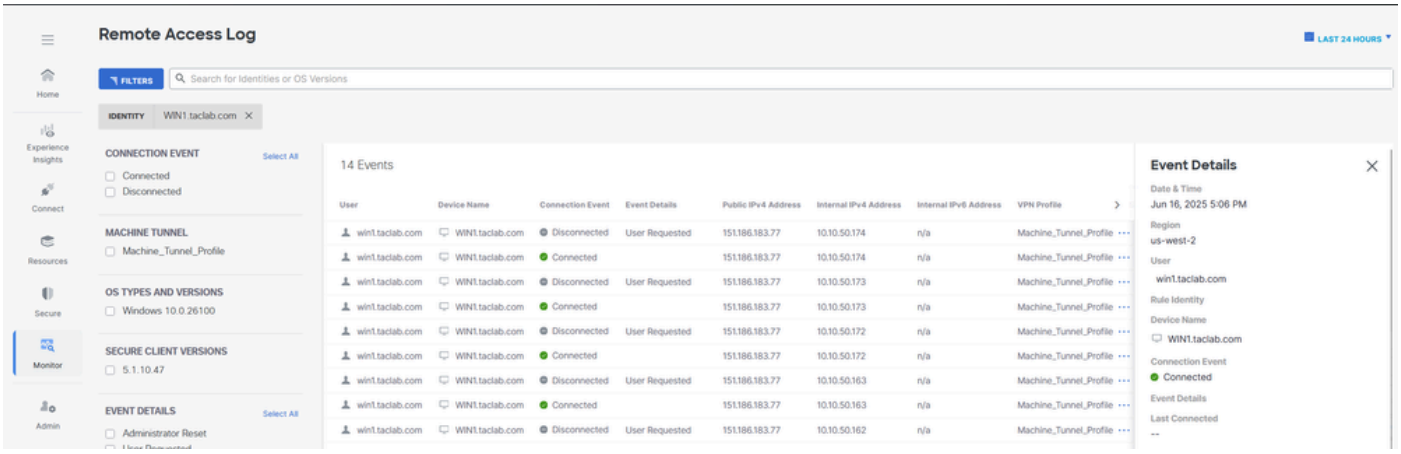
Schritt 8 - Herstellen einer Verbindung mit dem Maschinentunnel

antwort: Verbindung zu einem Benutzertunnel , löst es den Download des xml-Profils des Maschinentunnels aus



b. Überprüfen der Tunnelverbindung





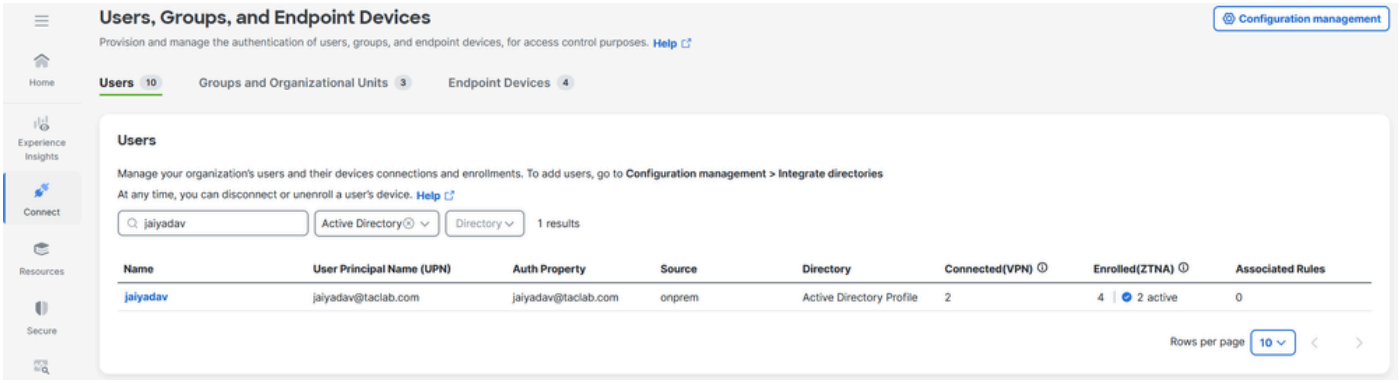
Methode 3: Konfigurieren des Maschinentunnels mithilfe des Benutzerzertifikats

In diesem Fall wählen Sie für die Authentifizierung des primären Felds das Zertifikatfeld aus, das die Benutzer-E-Mail oder UPN enthält. Secure Access verwendet die E-Mail- oder UPN-Nummer als Tunnelkennung. Das Format der E-Mail oder des UPN muss mit dem Format der ausgewählten Gerätekennung übereinstimmen.

Gehen Sie durch die Schritte 1 bis 4 für die Konfiguration des Maschinentunnels.

Schritt 5: Konfigurieren Sie den AD-Connector, damit Benutzer in Cisco Secure Access importiert werden können.

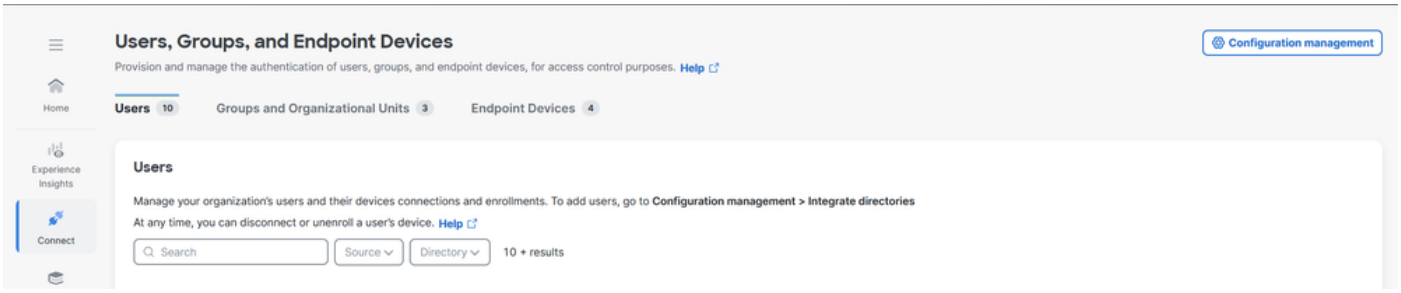
Weitere Informationen finden Sie unter Dauerhafte Active Directory-Integration.



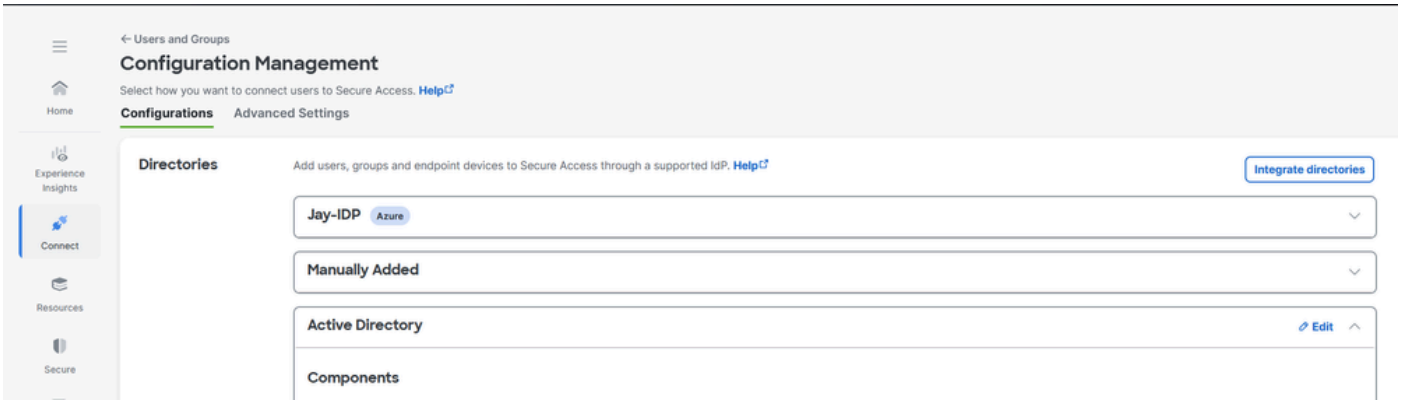
Schritt 6: Konfigurieren der Benutzerauthentifizierung

1. Navigieren Sie zu Verbinden > Benutzer, Gruppen und Endgeräte.

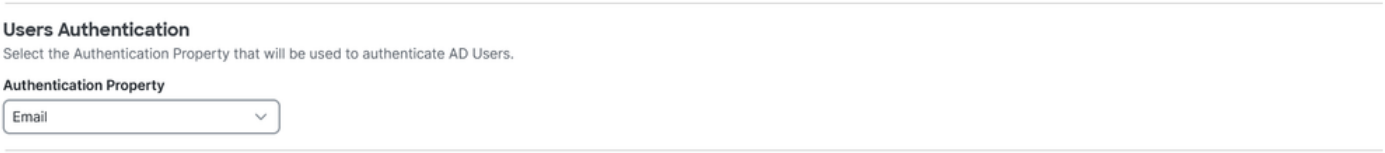
2. Klicken Sie auf Konfigurationsmanagement



3. Bearbeiten Sie unter Konfigurationen Active Directory.



4. Legen Sie die Authentifizierungseigenschaft des Benutzers auf E-Mail fest.



5. Klicken Sie auf Speichern und starten Sie die AD Connector-Dienste auf den Servern neu, auf denen die AD Connector-Dienste installiert sind

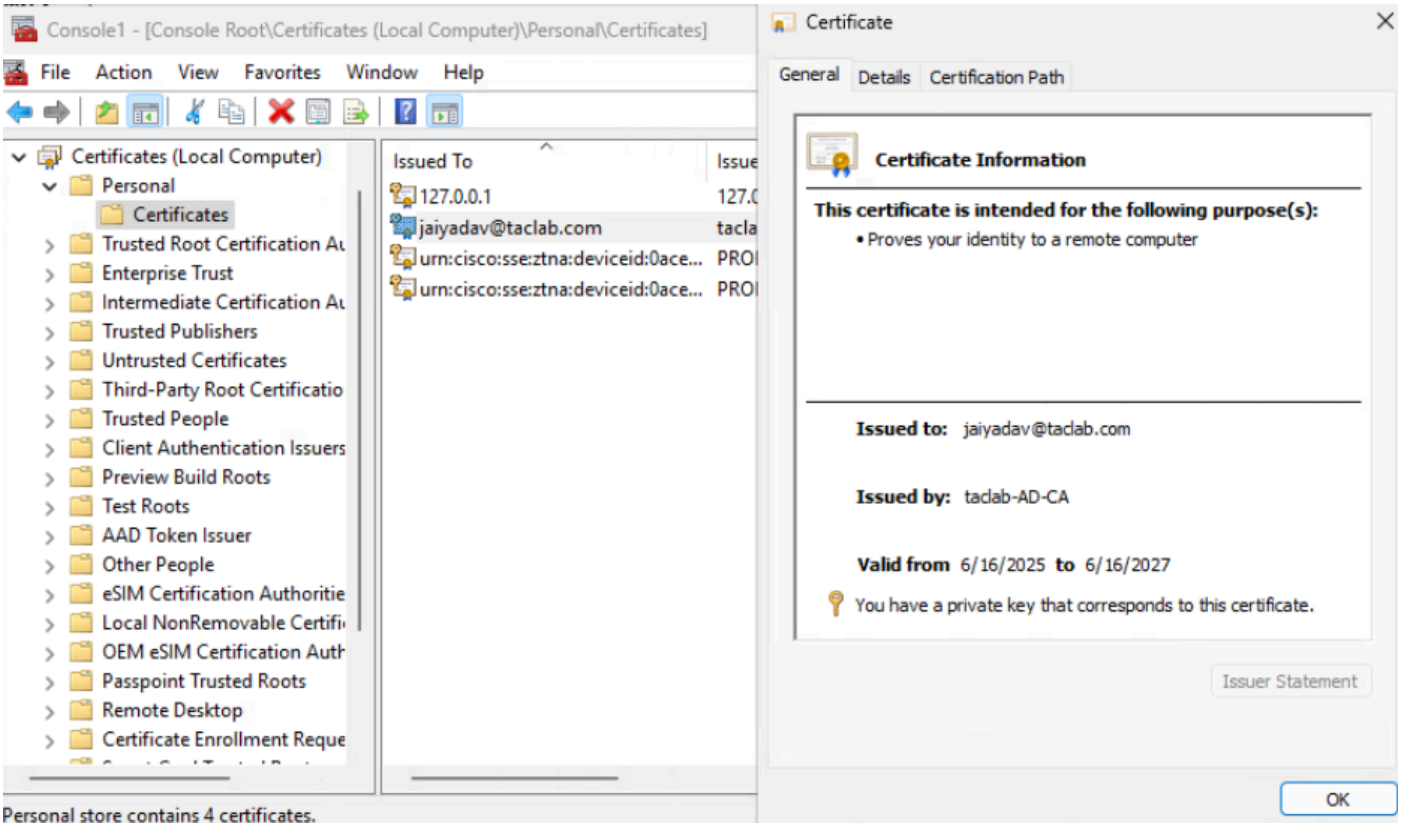
Schritt 7 - Generieren und Importieren eines Endpunktzertifikats

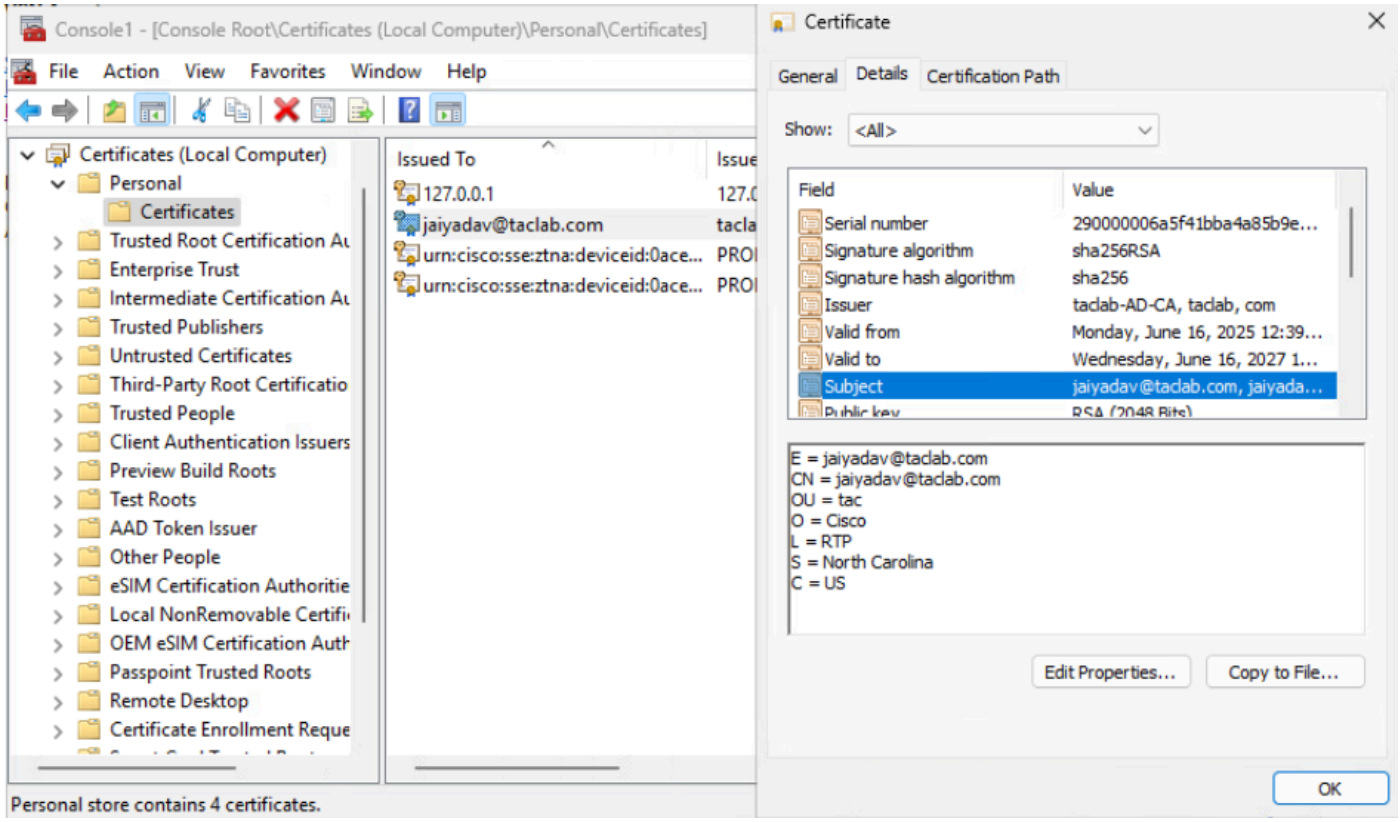
antwort: CSR generieren , CSR-Generator oder OpenSSL-Tool öffnen

b. Endpunktzertifikat von CA generieren

c. Konvertieren Sie die .cert-Datei in das PKCS12-Format

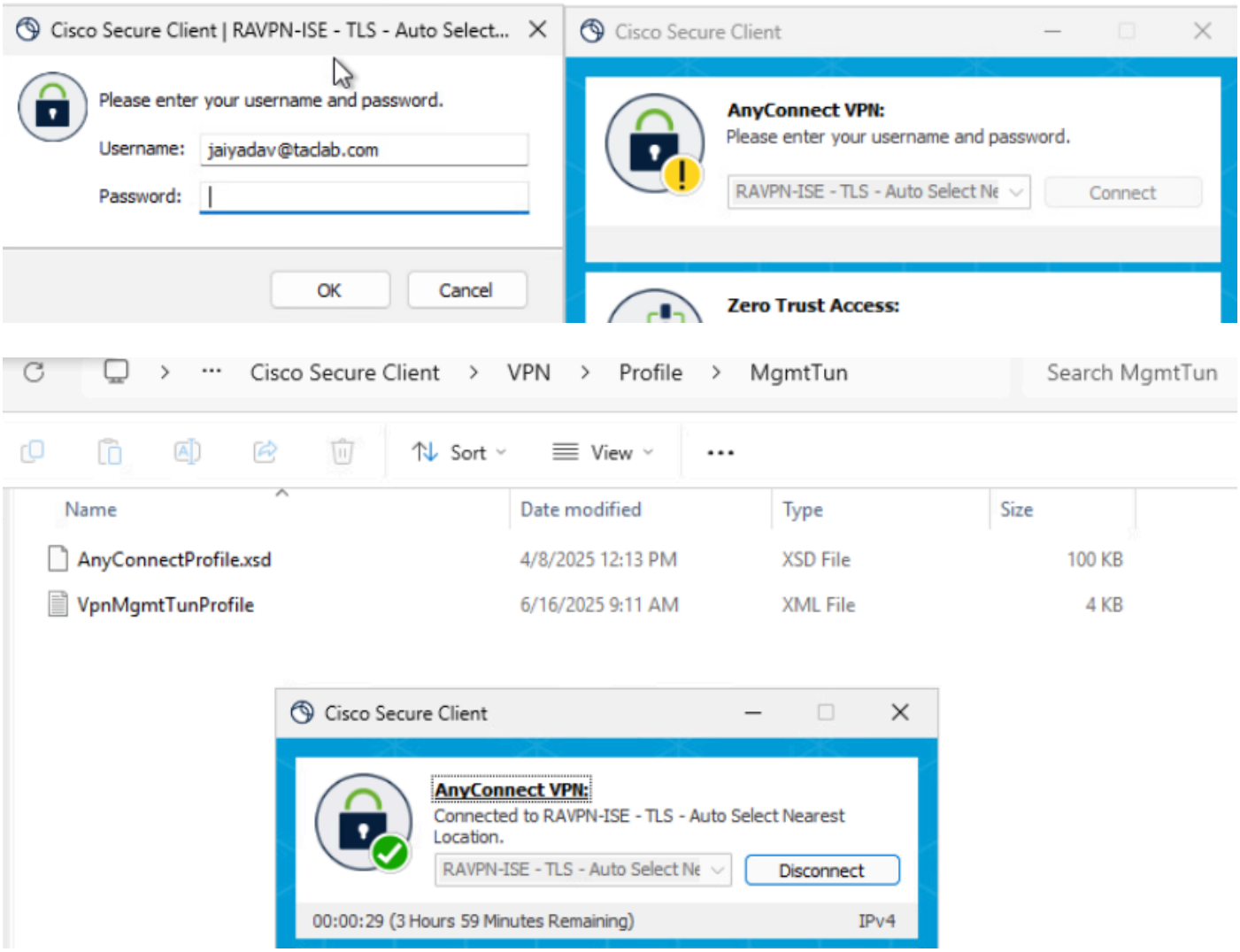
d. PKCS12-Zertifikat in Endpunktzertifikatsspeicher importieren



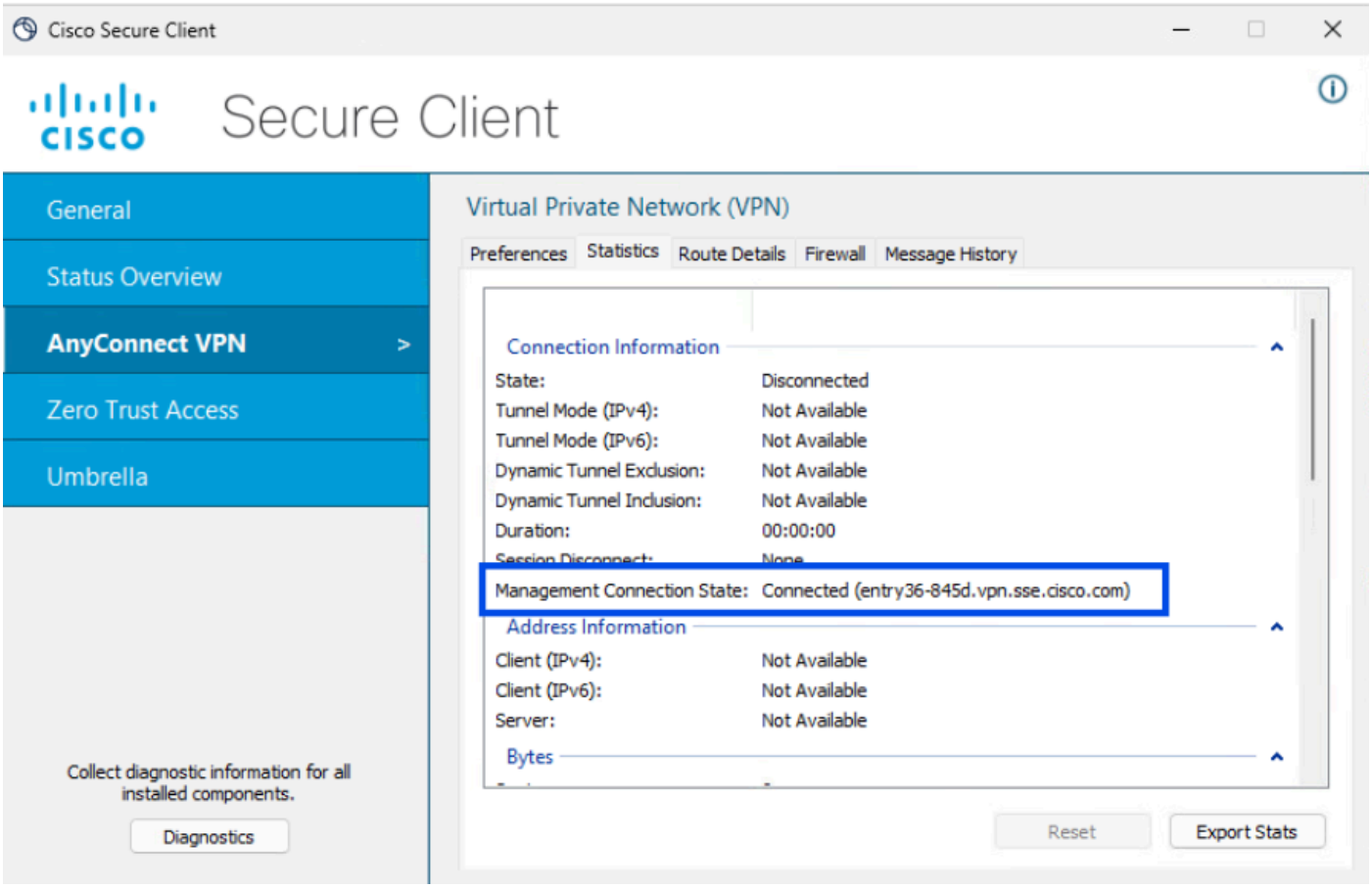


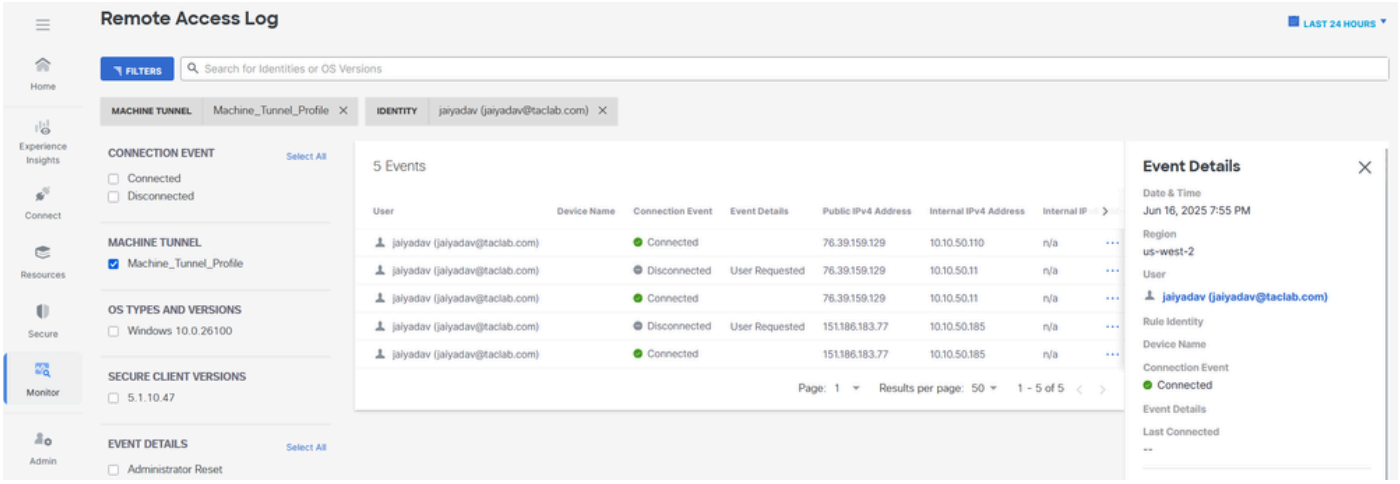
Schritt 8 - Herstellen einer Verbindung mit dem Maschinentunnel

antwort: Verbindung zu einem Benutzertunnel , löst es den Download des xml-Profils des Maschinentunnels aus



b. Überprüfen der Tunnelverbindung





Fehlerbehebung

Extrahieren Sie das DART-Paket, öffnen Sie die AnyConnect VPN-Protokolle, und analysieren Sie die Fehlermeldungen.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.