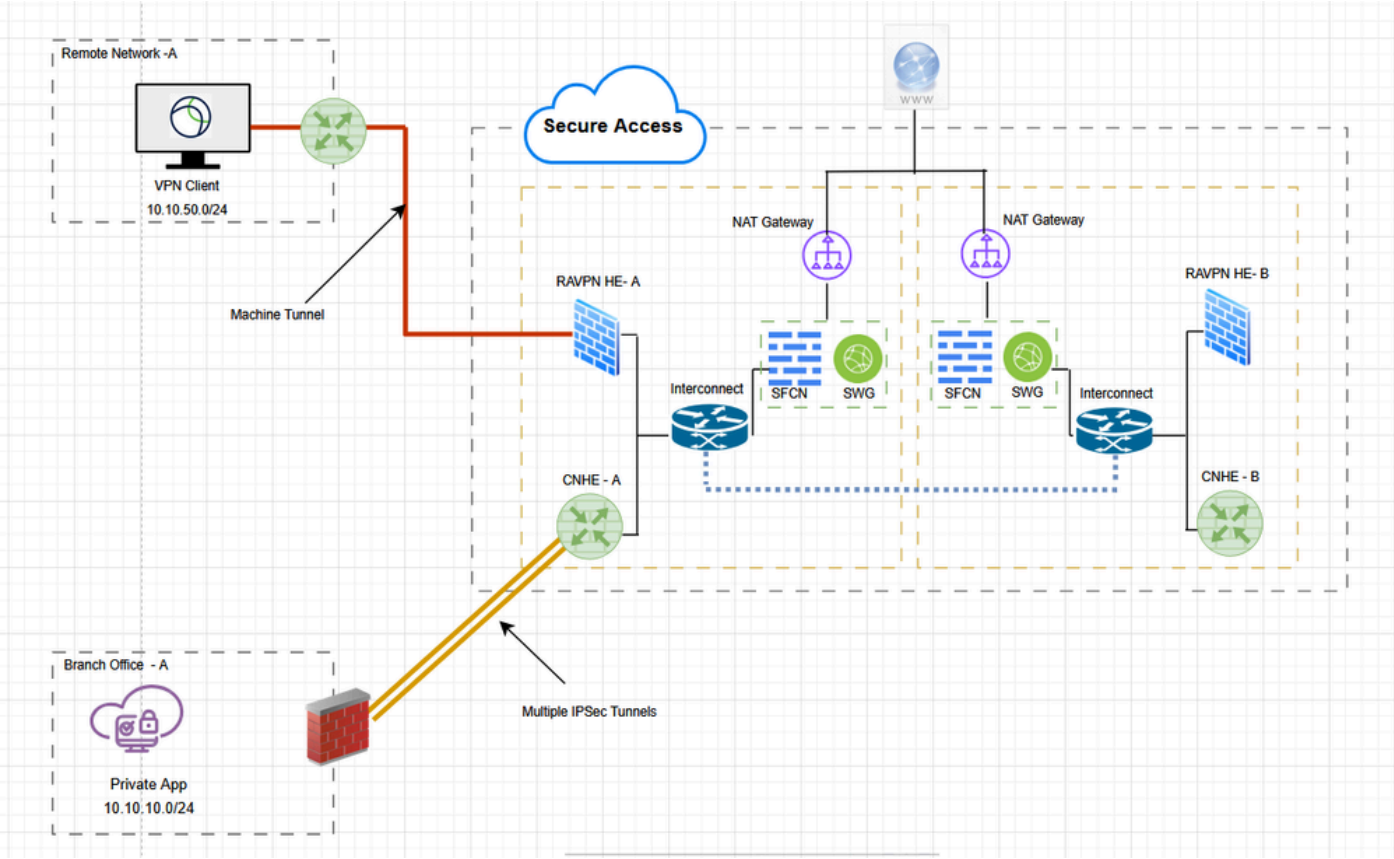
Configuración del túnel de máquina en Cisco Secure Access

Contenido

Introducción

Este documento describe cómo configurar Secure Access como gateway VPN y aceptar conexiones del Secure Client a través del túnel de la máquina VPN.

Diagrama de la red



Prerequisites

- Función de administrador completa en Secure Access.
- Al menos un perfil de usuario VPN configurado en Cisco Secure Access
- Grupo de IP de usuario en Cisco Secure Access

Requirements

Se recomienda que tenga conocimiento de estos temas:

- 509 Certificados
- OpenSSL

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Acceso seguro de Cisco
- Cisco Secure Client 5.1.10
- Windows 11
- Windows Server 2019 (CA)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Un túnel de máquina VPN de acceso seguro garantiza la conectividad a la red corporativa siempre que se encienda el sistema cliente, no solo cuando el usuario final establece una conexión VPN. Puede realizar la administración de parches en terminales fuera de la oficina, especialmente en dispositivos que el usuario no conecta con frecuencia, a través de VPN, a la red de la oficina. Los scripts de inicio de sesión de Endpoint OS que requieren conectividad de red corporativa también se benefician de esta función. Para que este túnel se cree sin la interacción del usuario, se utiliza la autenticación basada en certificados.

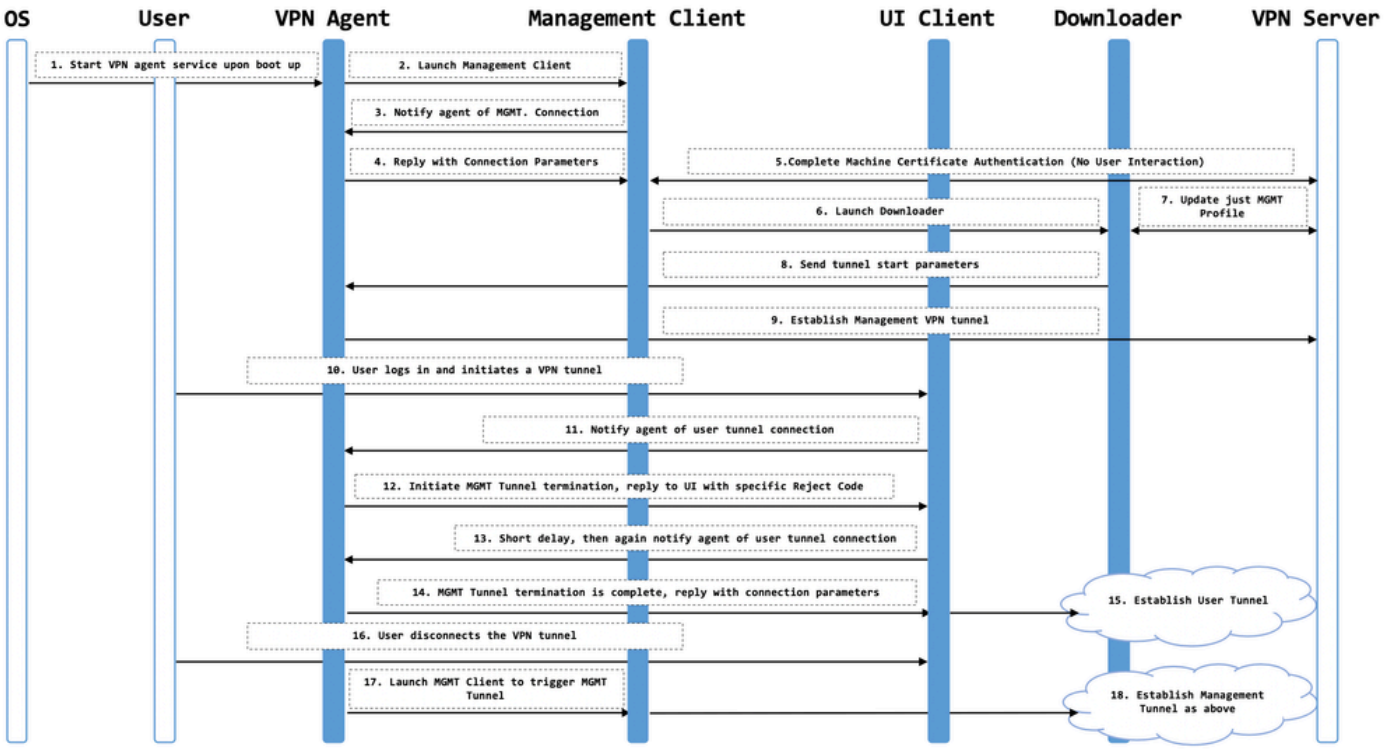
El túnel del equipo Secure Access permite a los administradores tener Cisco Secure Client conectado sin la intervención del usuario antes de que este inicie sesión. El túnel del equipo de acceso seguro se activa cuando el terminal está fuera de las instalaciones y desconectado de una VPN iniciada por el usuario. El túnel del equipo VPN de acceso seguro es transparente para el usuario final y se desconecta automáticamente cuando el usuario inicia la VPN.

Trabajo en túnel de máquina

El servicio de agente Secure Client VPN se inicia automáticamente al arrancar el sistema. El agente VPN de Secure Client utiliza el perfil VPN para detectar que la función de túnel de máquina está habilitada. Si la función de túnel de máquina está activada, el agente inicia la aplicación cliente de administración para iniciar una conexión de túnel de máquina. La aplicación cliente de administración utiliza la entrada de host del perfil VPN para iniciar la conexión. A continuación, el túnel VPN se establece de la forma habitual, con una excepción: no se realiza ninguna actualización de software durante una conexión de túnel de máquina, ya que el túnel de máquina debe ser transparente para el usuario.

El usuario inicia un túnel VPN a través de Secure Client, que activa la terminación del túnel de la máquina. Tras la terminación del túnel de la máquina, el establecimiento del túnel del usuario continúa de la forma habitual.

El usuario desconecta el túnel VPN, lo que activa el restablecimiento automático del túnel de la máquina.



Limitaciones

- No se admite la interacción del usuario.
- La autenticación basada en certificados a través del Almacén de certificados del equipo (Windows) sólo se admite.
- Se aplica la comprobación estricta de certificados de servidor.
- No se admite un proxy privado.
- No se admite un proxy público (el valor ProxyNative se admite en plataformas en las que no se recupera la configuración del proxy nativo del explorador).
- No se admiten scripts de personalización de cliente seguro

Configurar

Método 1: configurar el túnel de la máquina con el usuario machine@sse.com

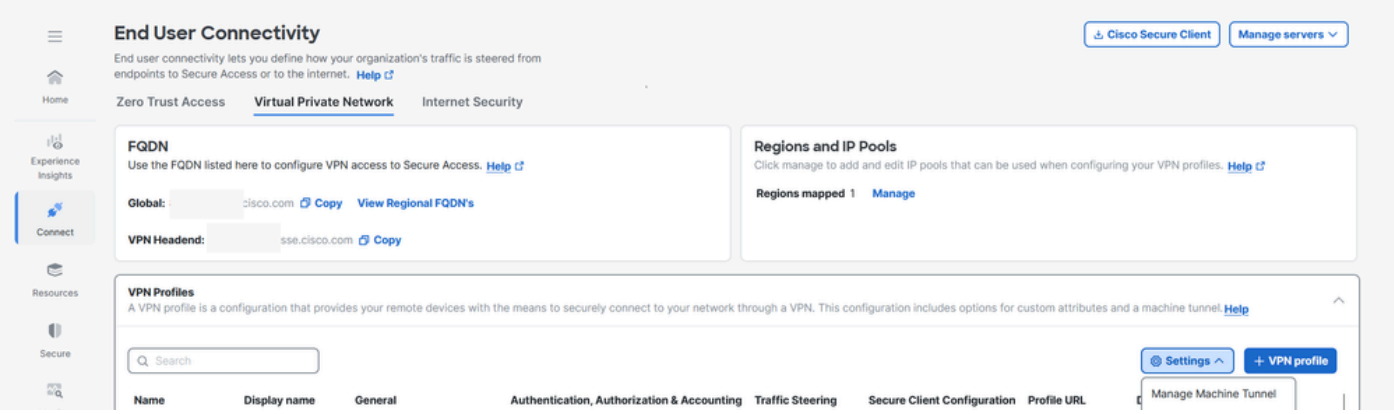
Paso 1: Configuración general

Configure los parámetros generales, incluidos el dominio y los protocolos que utiliza este túnel de máquina.

1. Vaya a Conexión > Conectividad de usuario final > Red privada virtual.

2. Navegue hasta Perfiles VPN y configure los parámetros para el túnel de la máquina.

    a. Haga clic en Settings y, a continuación, seleccione Manage Machine Tunnel en el menú desplegable.

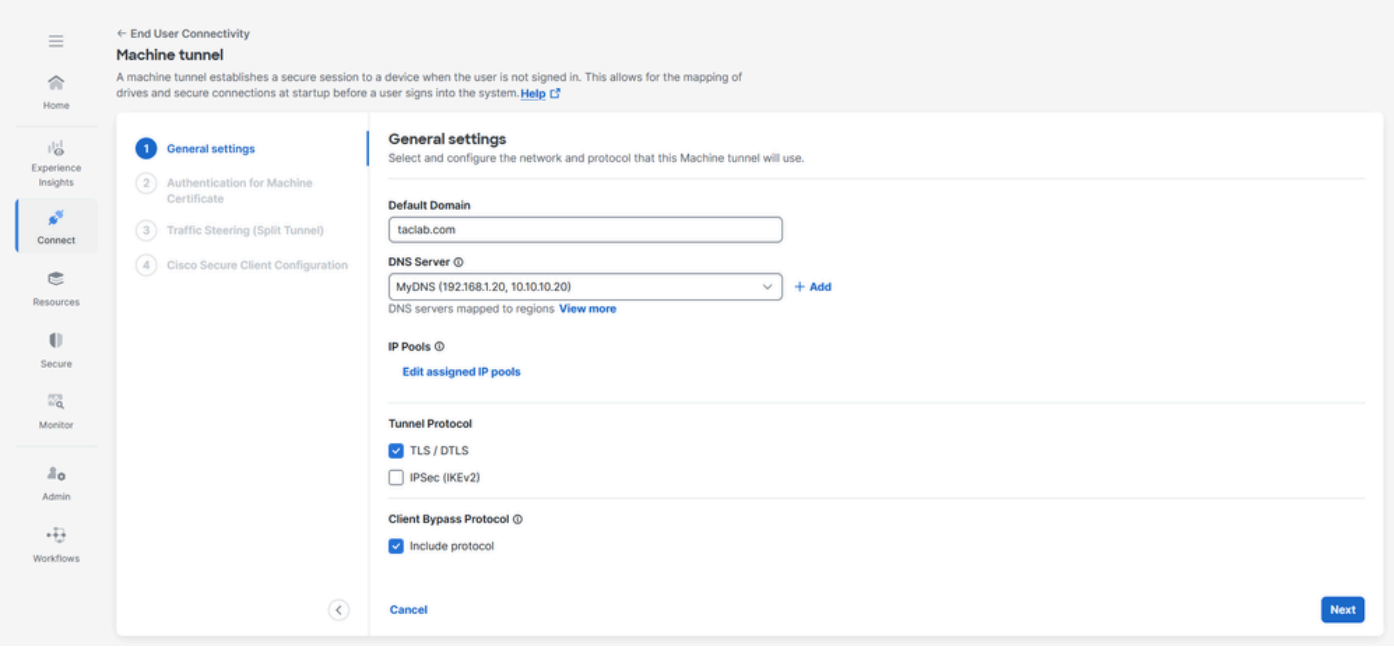


3. Introduzca el dominio predeterminado.
4. El servidor DNS asignado a través de la página Administrar regiones y grupos IP se establece como el servidor predeterminado. Puede aceptar el servidor DNS predeterminado, elegir otro servidor DNS del menú desplegable o hacer clic en + Agregar para agregar un nuevo par de servidores DNS. Al seleccionar otro servidor DNS o agregar uno nuevo, se sobrescribe este servidor predeterminado.
5. Seleccione un conjunto de IP por región en el menú desplegable IP Pools. Los perfiles VPN deben tener al menos un conjunto IP asignado en cada región para una configuración válida.
6. Seleccione el Protocolo de túnel que este túnel de máquina utiliza:
    - TLS/DTLS
    - IPSec (IKEv2)

    Se debe seleccionar al menos un protocolo.
7. Opcionalmente, marque Incluir protocolo para aplicar el protocolo de omisión de cliente.

    a. Si el protocolo de omisión del cliente está habilitado para un protocolo IP y no se configura un conjunto de direcciones para ese protocolo (es decir, ASA no asignó ninguna dirección IP para ese protocolo al cliente), el tráfico IP que utiliza ese protocolo no se enviará a través del túnel VPN. Debe enviarse fuera del túnel.

    b. Si se inhabilita el Protocolo de omisión del cliente y no se configura un conjunto de direcciones para ese protocolo, el cliente descarta todo el tráfico para ese protocolo IP una vez que se establece el túnel VPN.



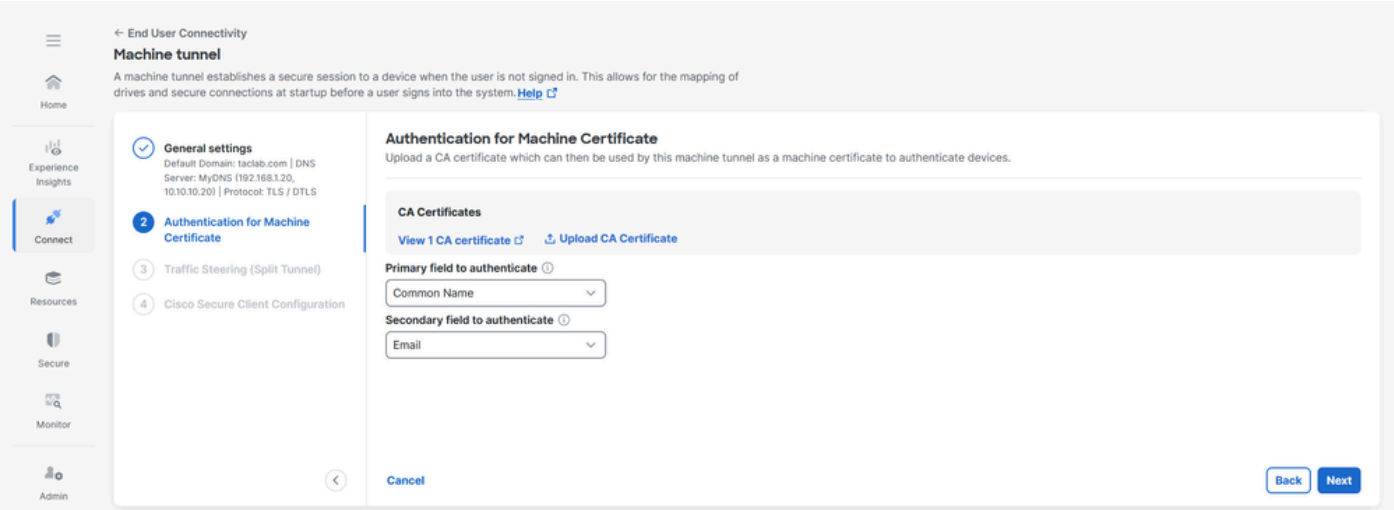
8. Haga clic en Next .

Paso 2 - Autenticación para el certificado de máquina

El túnel de la máquina es transparente para el usuario final y se desconecta automáticamente cuando el usuario inicia una sesión VPN. Para que este túnel se cree sin la interacción del usuario, se utiliza la autenticación basada en certificados.

1. Elija certificados de CA de la lista o haga clic en Cargar certificados de CA

2. Seleccione los campos de autenticación basados en certificados. Para obtener más información, vea campos de autenticación basados en certificados



3. Haga clic en Next .

Paso 3: Dirección del tráfico (túnel dividido)

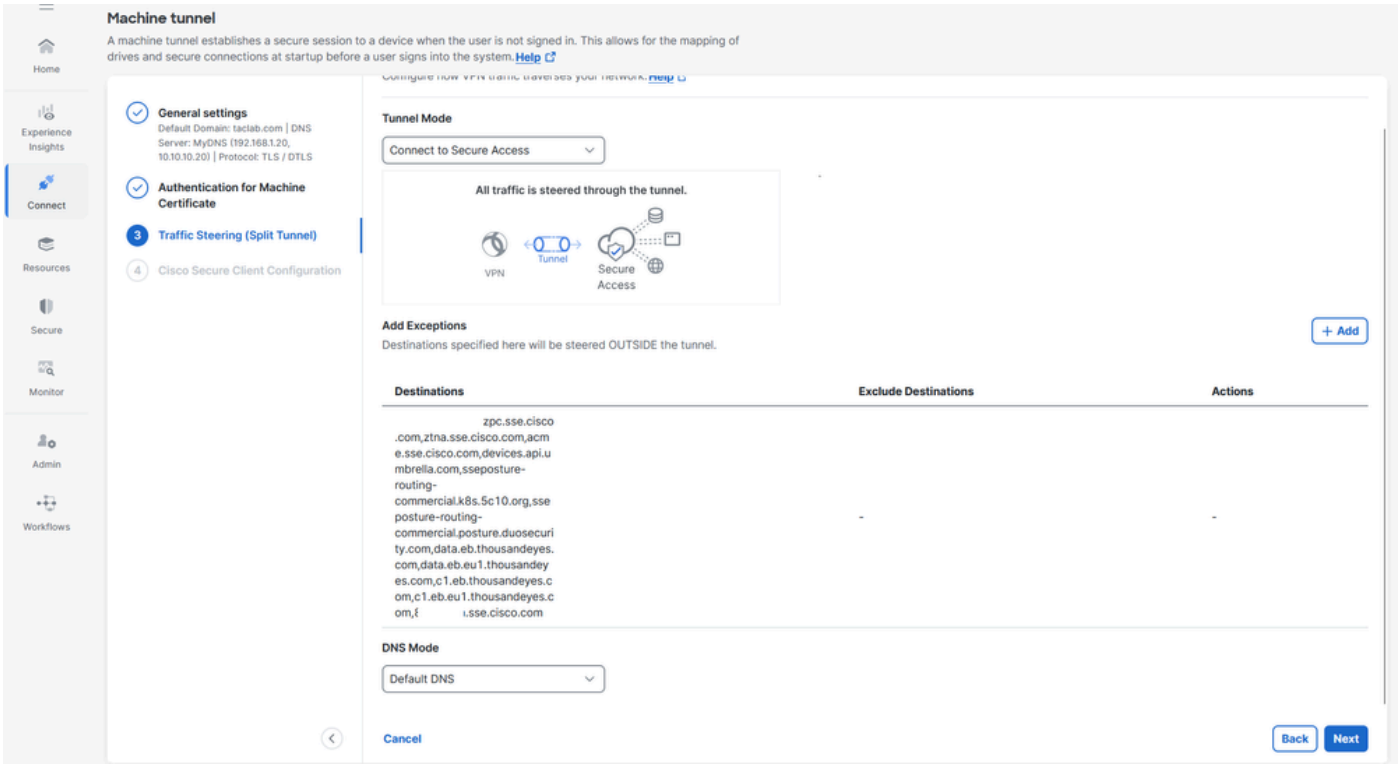
Para Traffic Steering (túnel dividido), puede configurar un túnel de máquina para mantener una

conexión de túnel completa a Secure Access, o configurarlo para utilizar una conexión de túnel dividido para dirigir el tráfico a través de VPN solamente si es necesario.Para obtener más información, consulte Dirección del tráfico del túnel de máquina

1. Seleccione el modo de túnel

2. Dependiendo de la selección del modo de túnel , puede agregar excepciones

3. Seleccione Modo DNS

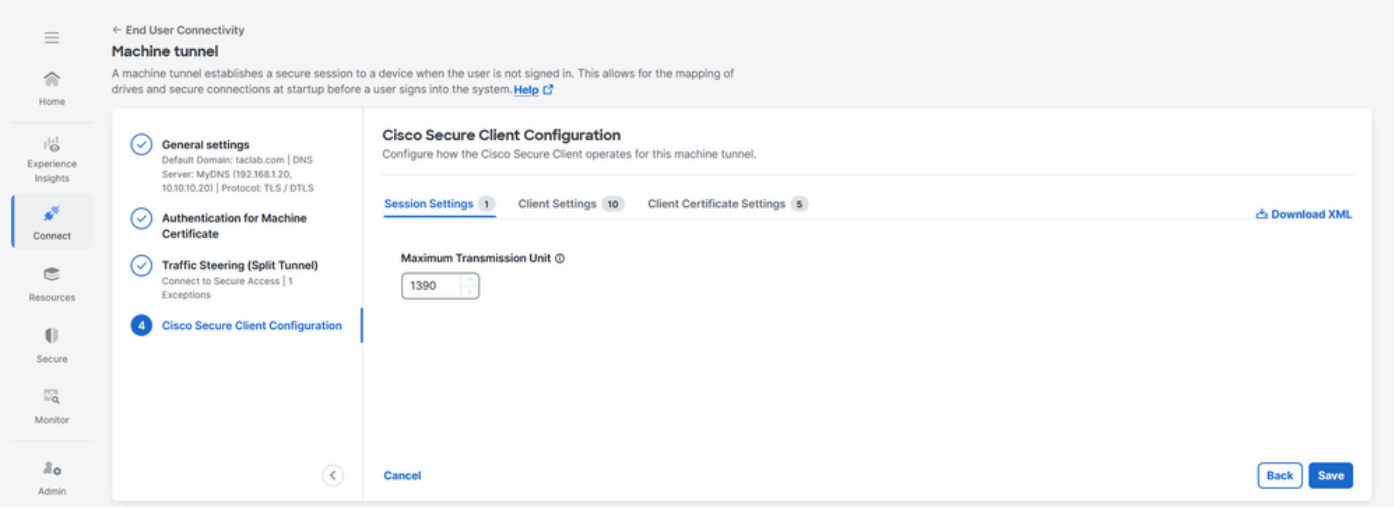


4. Haga clic en Siguiente

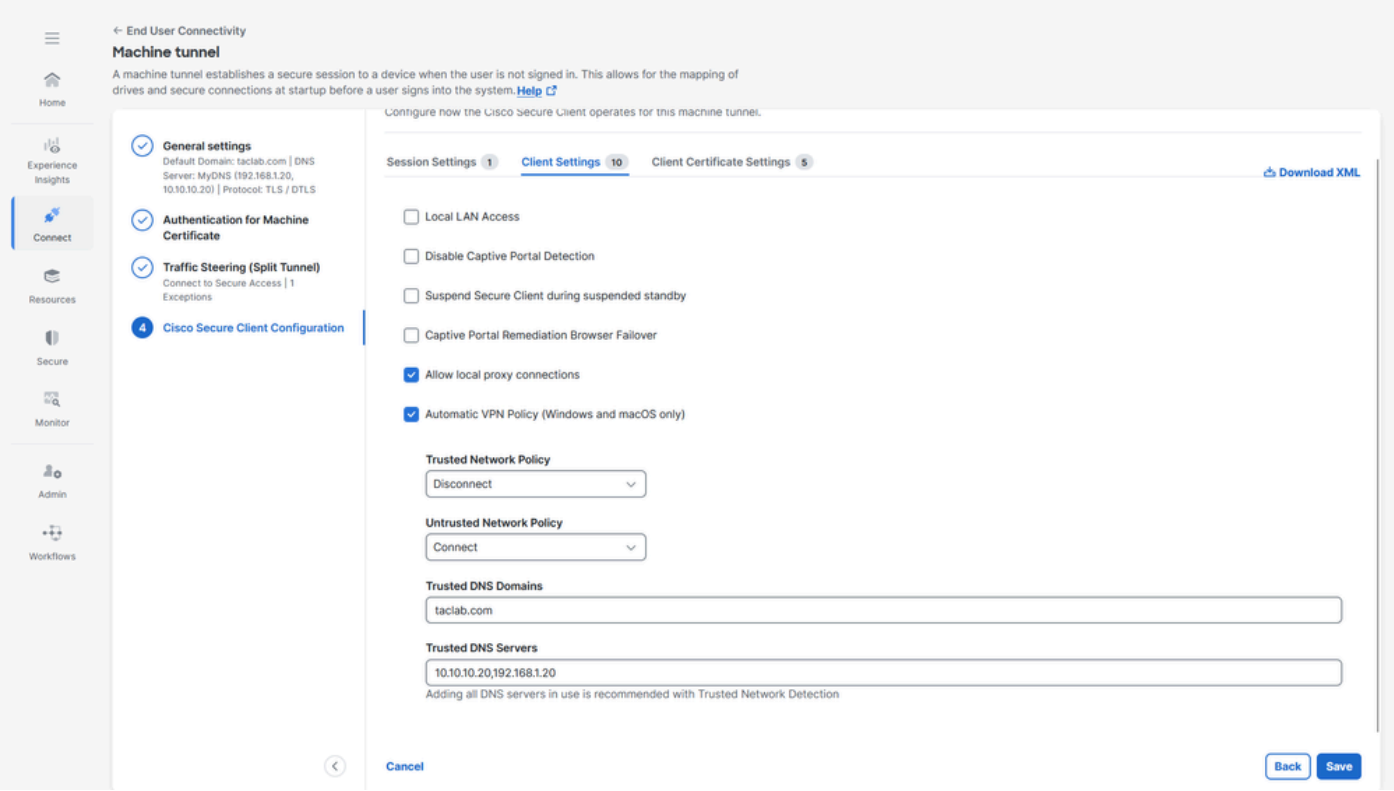
Paso 4: Configuración de Cisco Secure Client

Puede modificar un subconjunto de la configuración de Cisco Secure Client en función de las necesidades de un túnel de máquina VPN determinado. Para obtener más información, vea Configuración de Secure Client

1. Verifique la unidad de transmisión máxima, el tamaño más grande del paquete que se puede enviar en el túnel VPN sin fragmentación



2. Configuración del cliente , consulte Configuración del cliente de túnel de máquina para obtener más información



3. Configuración de certificados de cliente, seleccione las opciones correspondientes

a. Anulación del almacén de certificados de Windows : permite a un administrador indicar a Secure Client que utilice certificados del almacén de certificados del equipo Windows (sistema local) para la autenticación de certificados de cliente.

b. Selección automática de certificados: cuando se configura la autenticación de certificados múltiples en el gateway seguro

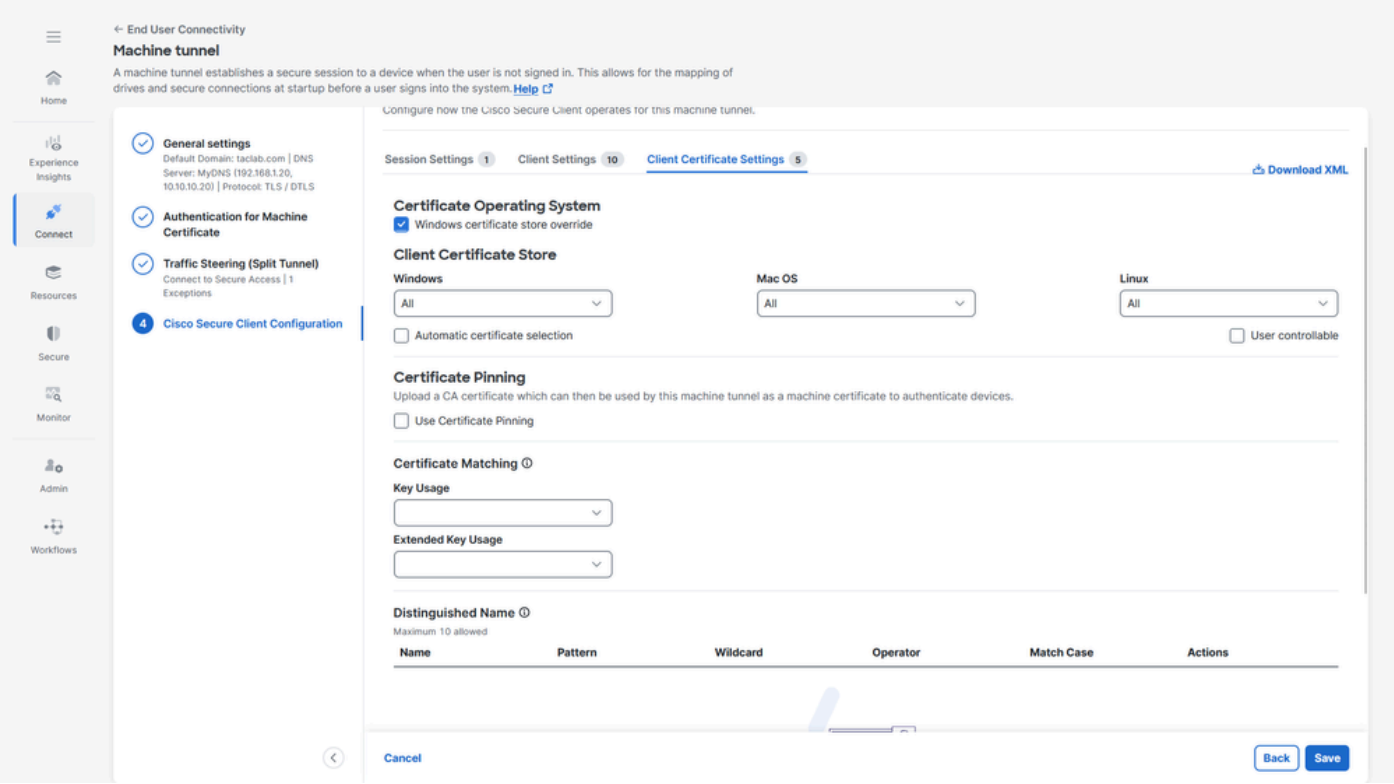
c. Fijación de certificados: certificado de CA que puede ser utilizado por el túnel de la máquina como certificado de la máquina para autenticar dispositivos

d. Coincidencia de certificados: si no se especifica ningún criterio de coincidencia de certificados, Cisco Secure Client aplica las reglas de coincidencia de certificados

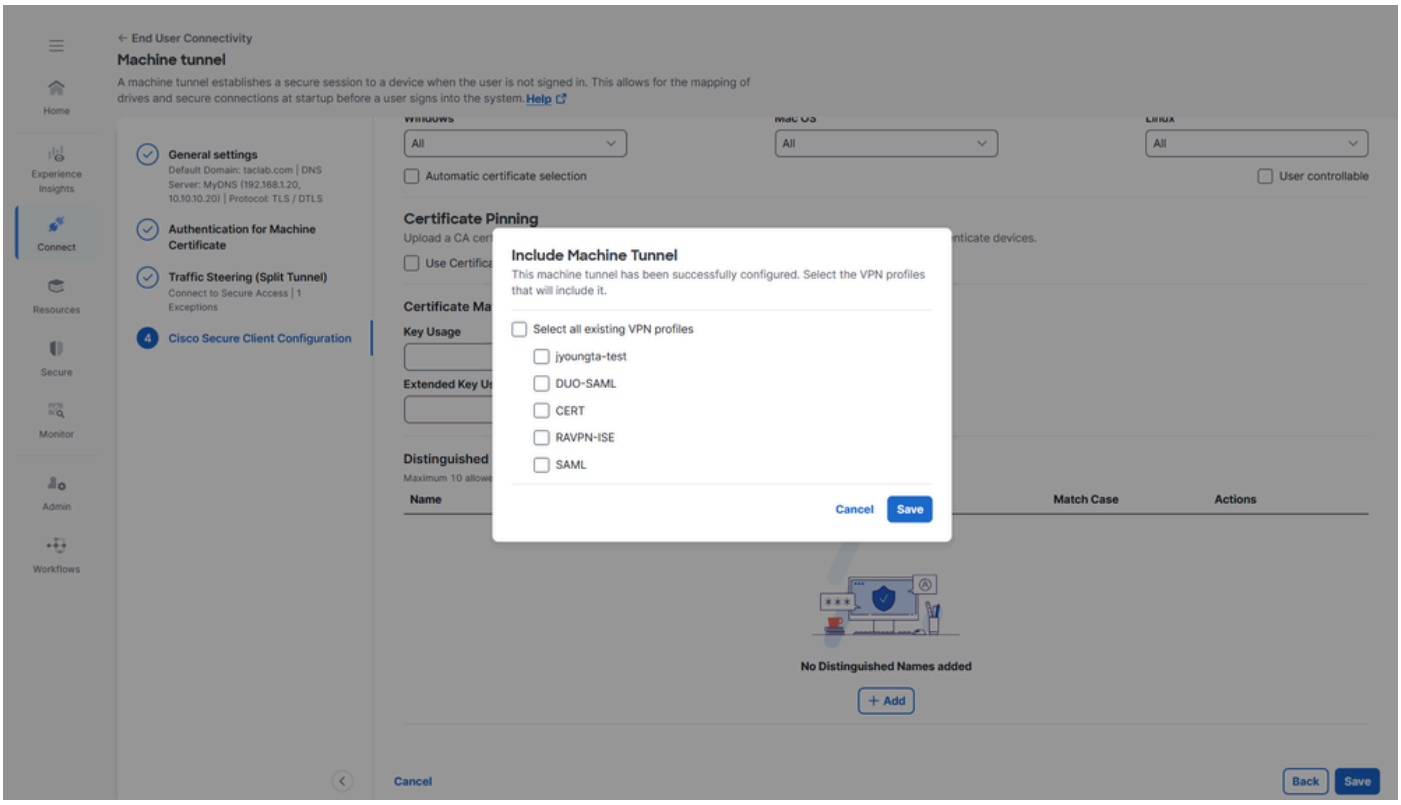
i. Uso de claves: Firma_digital

ii. Uso de clave ampliada: Autenticación del cliente

e. Nombre distinguido: especifica nombres distinguidos (DN) para los criterios de coincidencia exacta al elegir certificados de cliente aceptables. Cuando agrega varios nombres distinguidos, cada certificado se compara con todas las entradas y todas ellas deben coincidir.

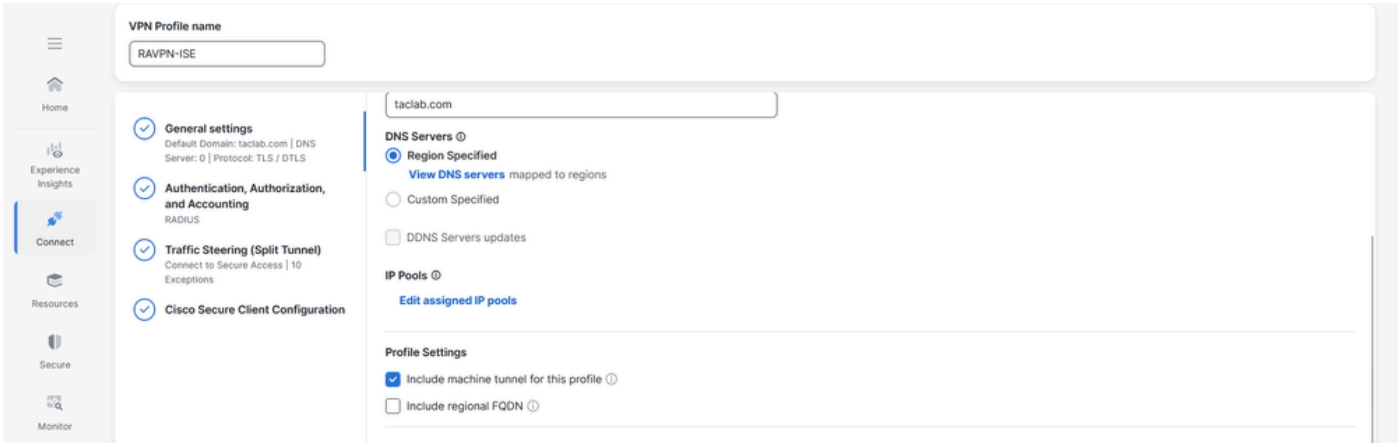


4. Asigne un perfil de túnel de máquina a un perfil de usuario VPN, haga clic en Guardar y luego hay una opción para seleccionar los perfiles de usuario VPN



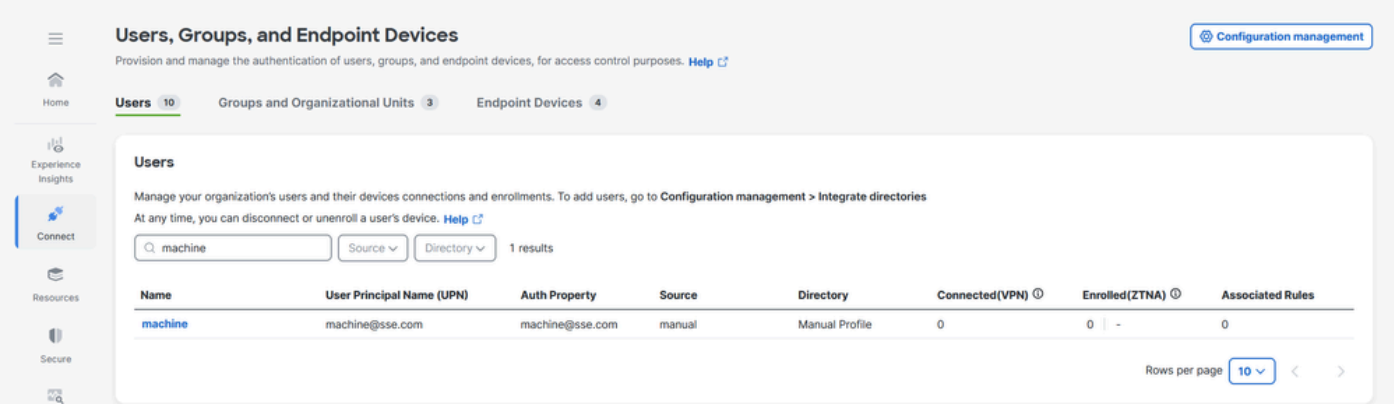
5. Haga clic en Guardar

6. Compruebe si el perfil de túnel de máquina está conectado a un perfil de VPN de usuario



Paso 5 - Verifique si el usuario machine@sse.com está presente en Cisco Secure Access

1. Vaya a Conexión > Usuarios, grupos y dispositivos de terminal > Usuarios



2. Si el usuario machine@sse.com no está presente, la importación se realiza manualmente. Para obtener más información, consulte Importación manual de usuarios y grupos

Paso 6 - Generar un certificado firmado por CA para machine@sse.com

1. Genere una solicitud de firma de certificado

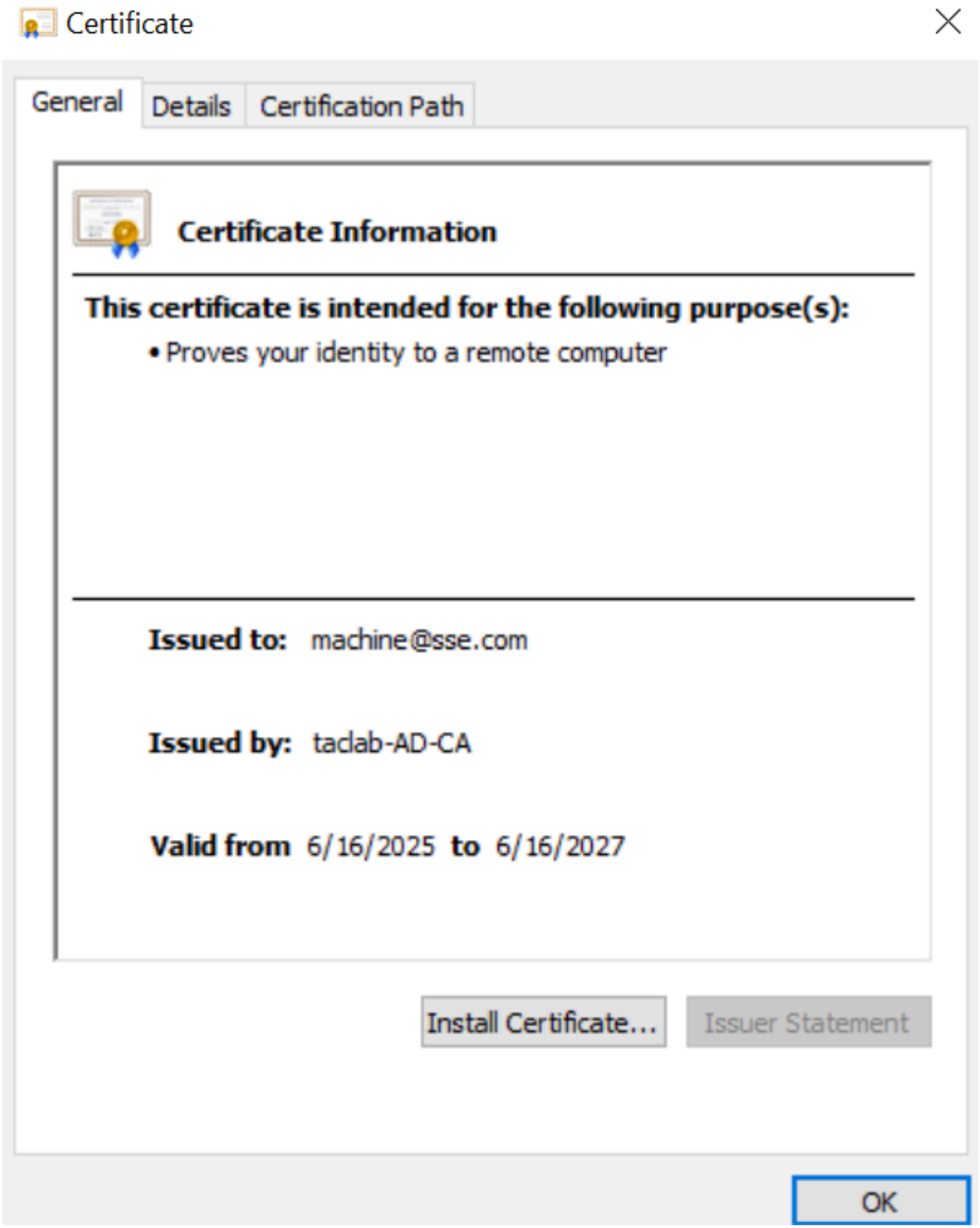
a. Podemos utilizar cualquier software en línea generador de CSR generador de CSR o una CLI openssl

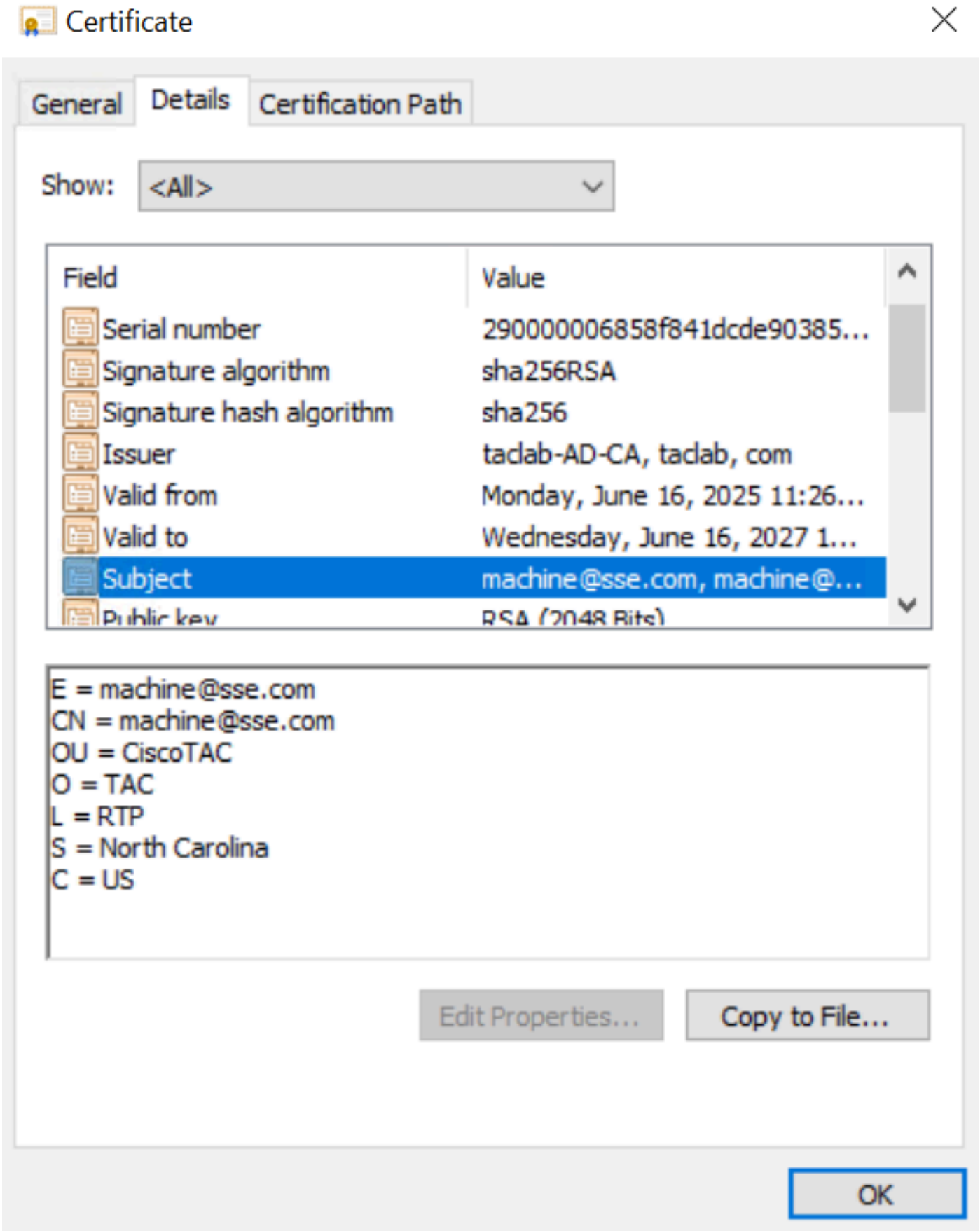
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr

```
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. Copie el CSR y genere un certificado de máquina


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



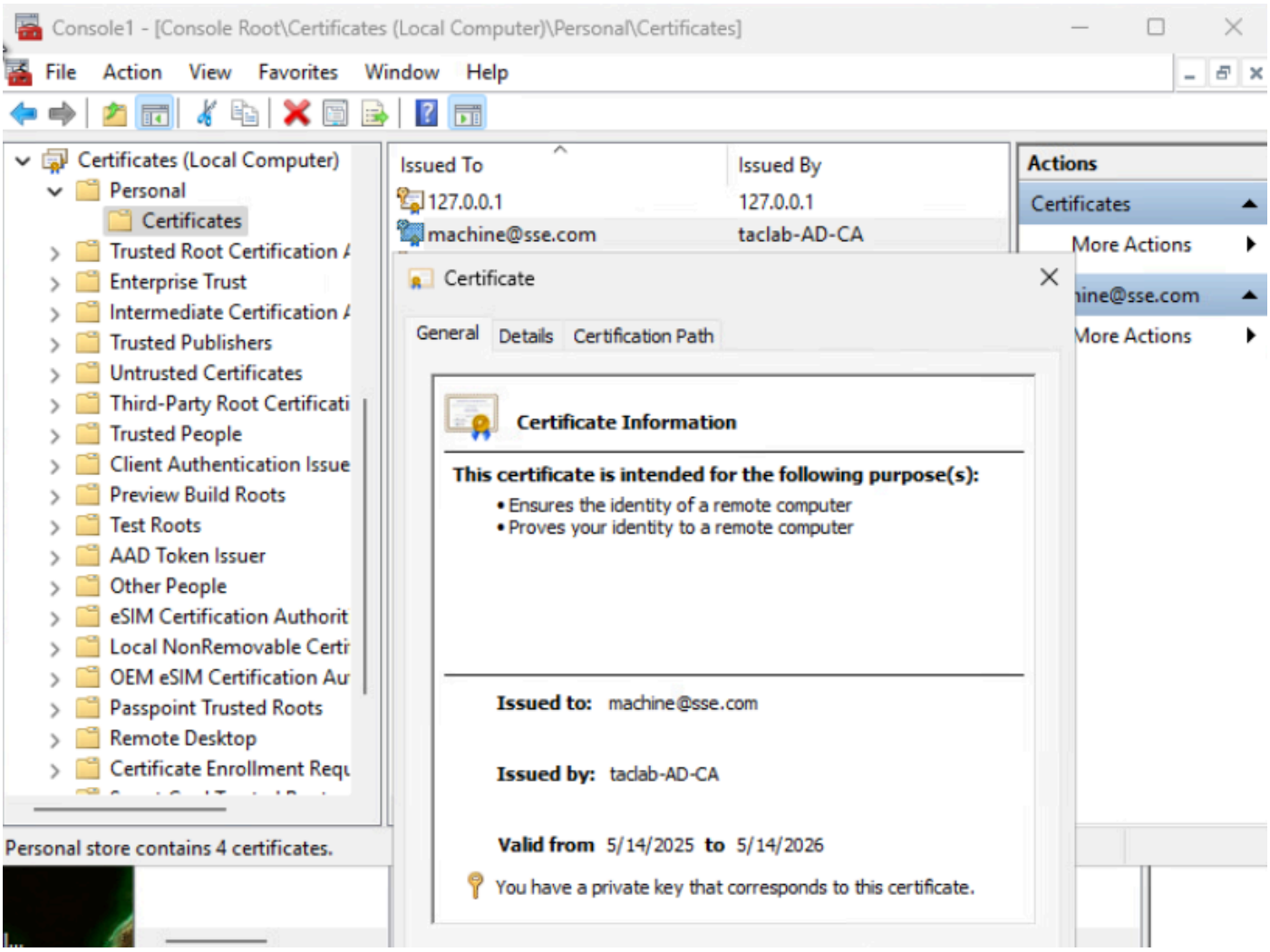
3. Convierta el certificado de máquina en formato PKCS12 utilizando la clave y el certificado generados en pasos anteriores (paso 1 y 2) respectivamente

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#
```

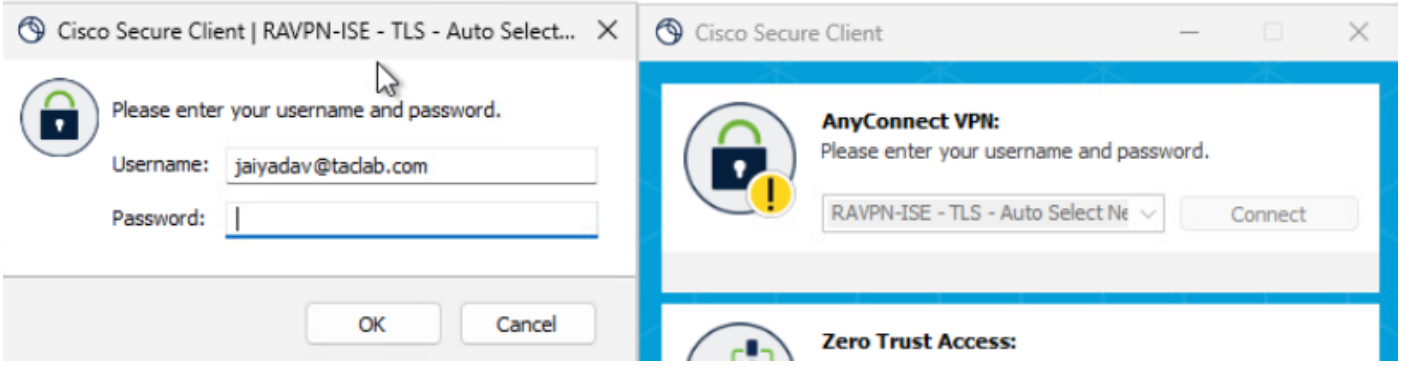
Paso 7 - Importar el certificado de equipo en un equipo de prueba

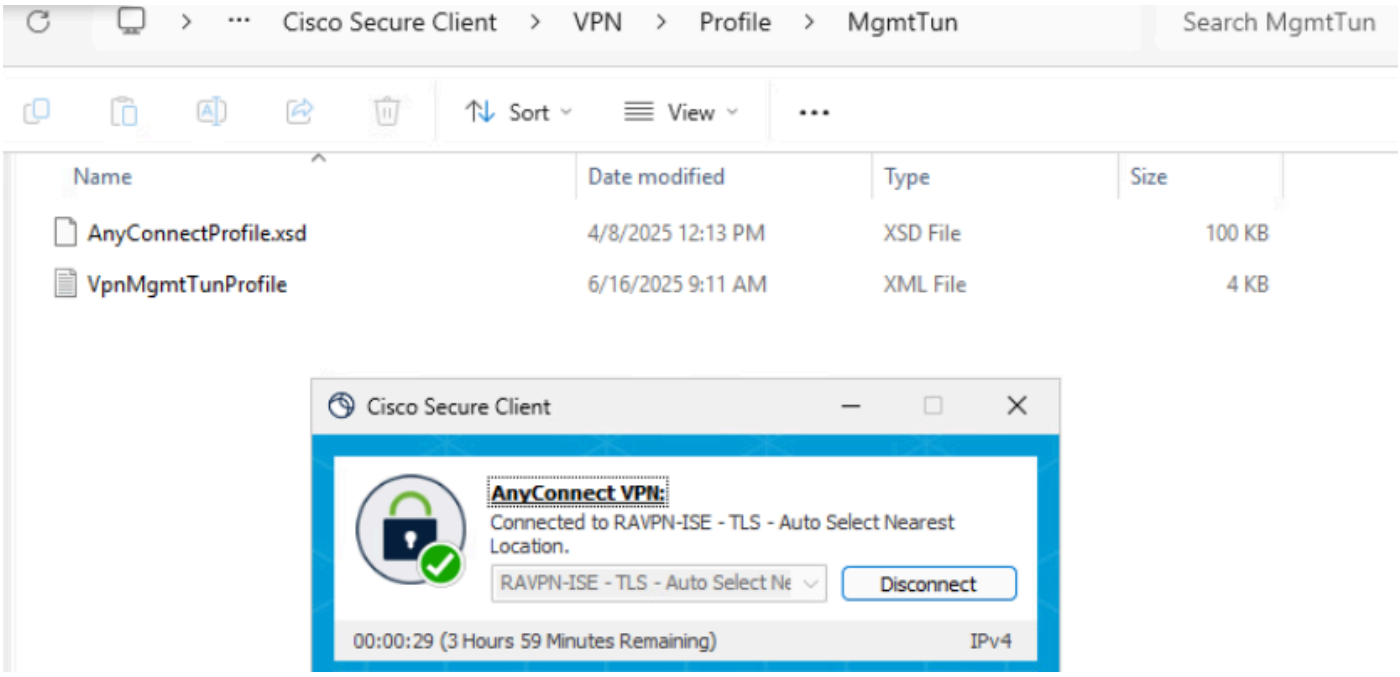
a. Importar el certificado de equipo PKCS12 en un almacén local o de equipo



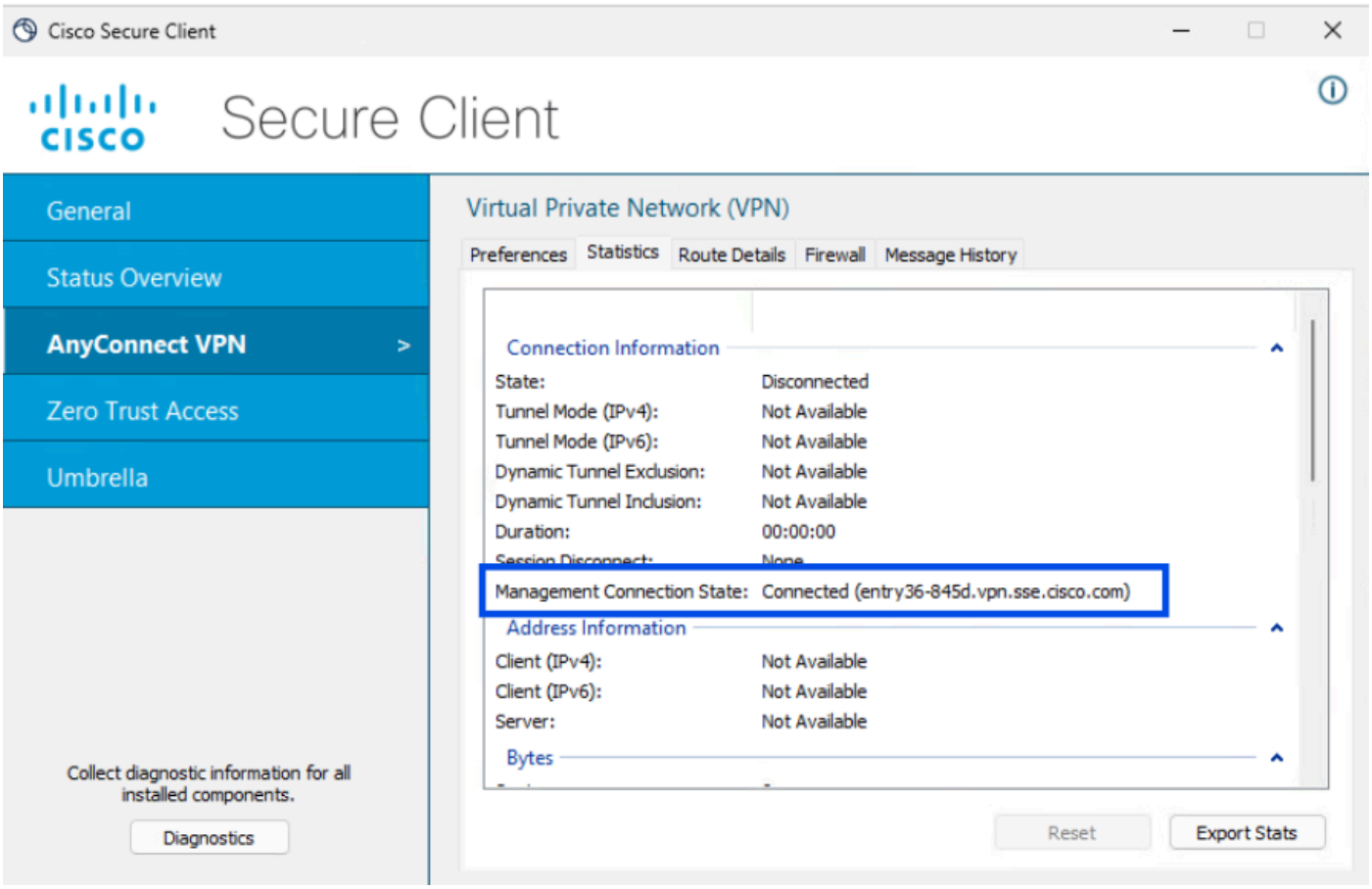
Paso 8: Conexión al túnel de la máquina

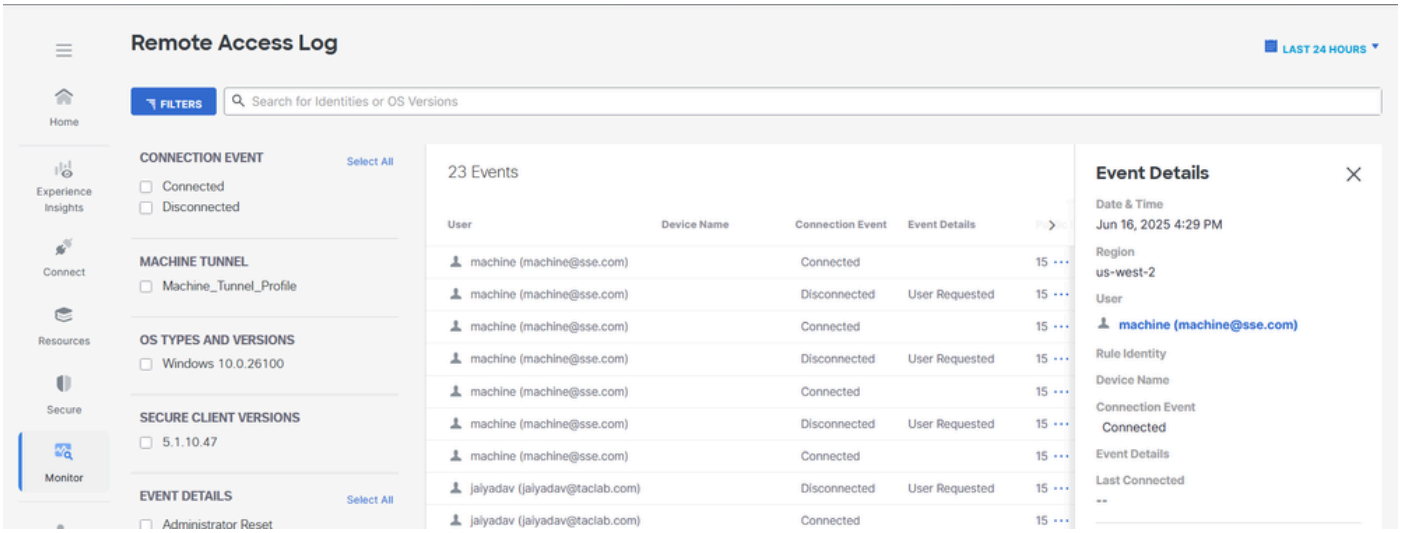
a. Conectar a un túnel de usuario , esto activa el perfil xml de la máquina que se va a descargar.





b. Verifique la conectividad del túnel de la máquina





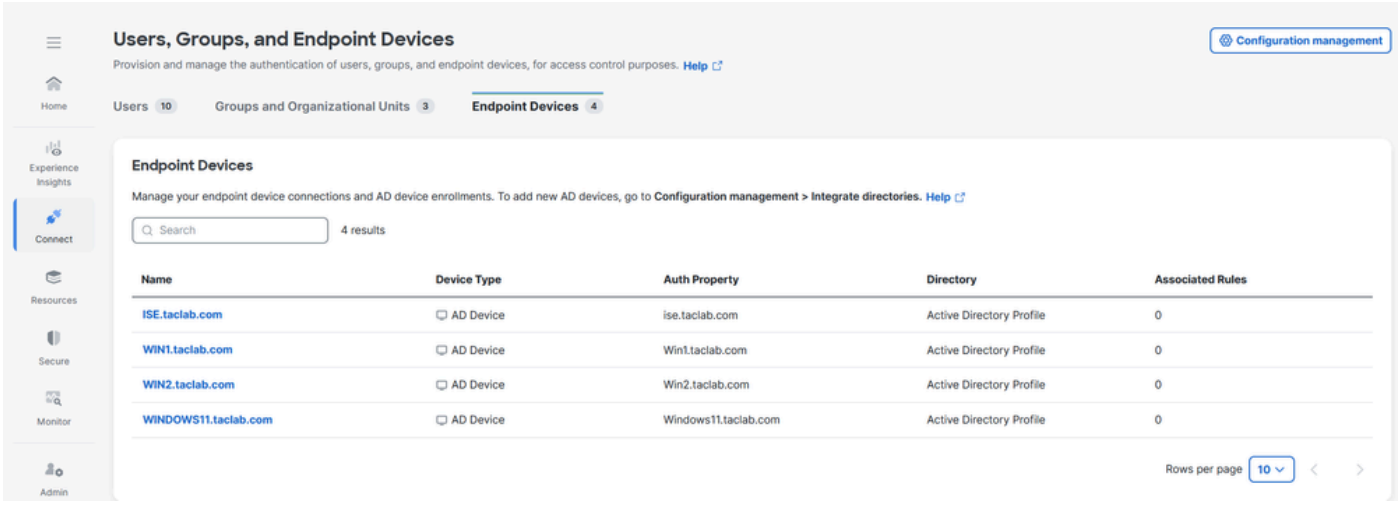
Método 2: configurar el túnel de la máquina mediante el certificado de terminal

En este caso, para que el campo principal se autentique, elija el campo de certificado que contiene el nombre de dispositivo (nombre de equipo). Secure Access utiliza el nombre del dispositivo como identificador del túnel de la máquina. El formato del nombre del equipo debe coincidir con el formato del identificador de dispositivo elegido

Vaya del paso 1 al paso 4 para la configuración del túnel de la máquina

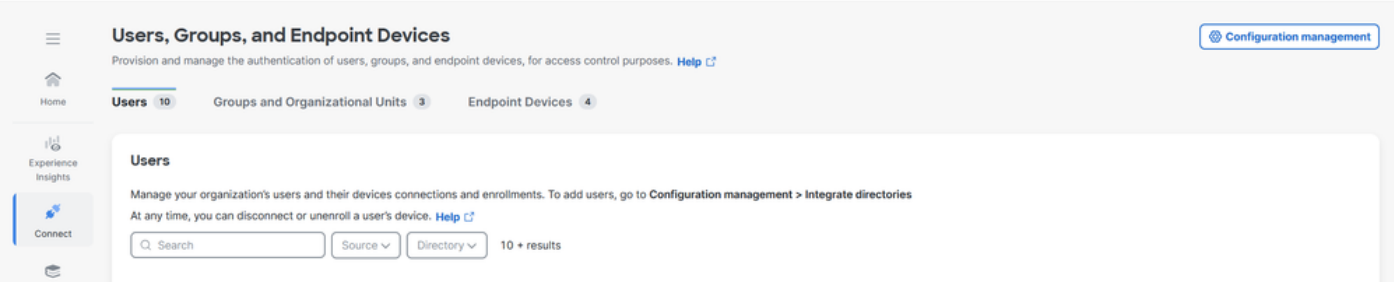
Paso 5 - Configure el conector de AD para poder importar terminales en Cisco Secure Access .

Para obtener más información, vea Integración de Active Directory permanente

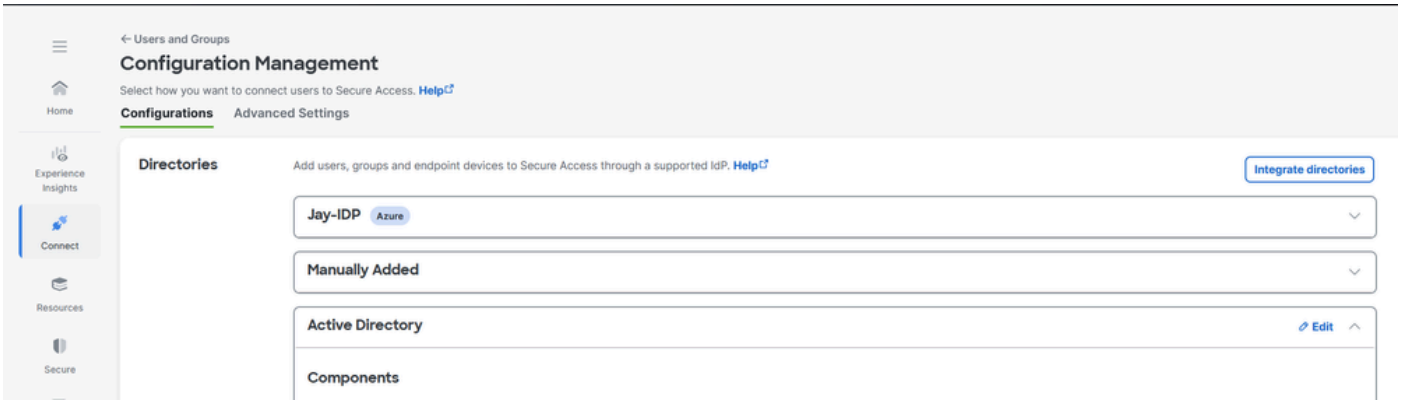


Paso 6: Configuración de la autenticación de dispositivos de terminal

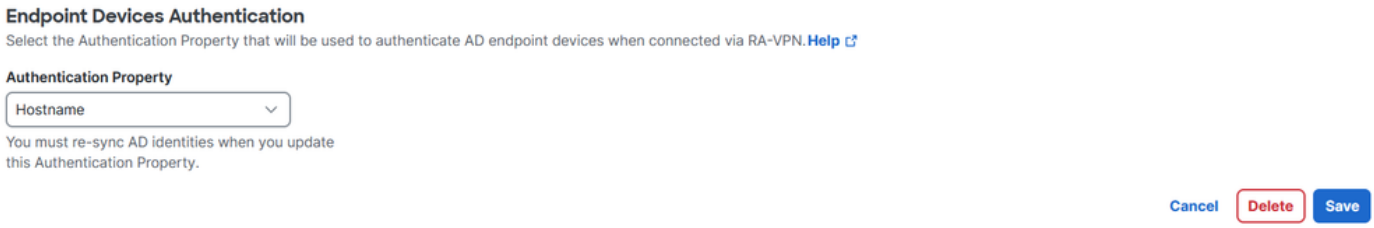
1. Vaya a Connect > Users,Groups and Endpoint Devices.
2. Haga clic en Administración de configuración



3. En Configuraciones , edite Active Directory



4. Establezca la Propiedad Authentication de Dispositivos de Extremo en Hostname



5. Haga clic en Guardar y reinicie los servicios del conector de AD en los servidores donde está instalado

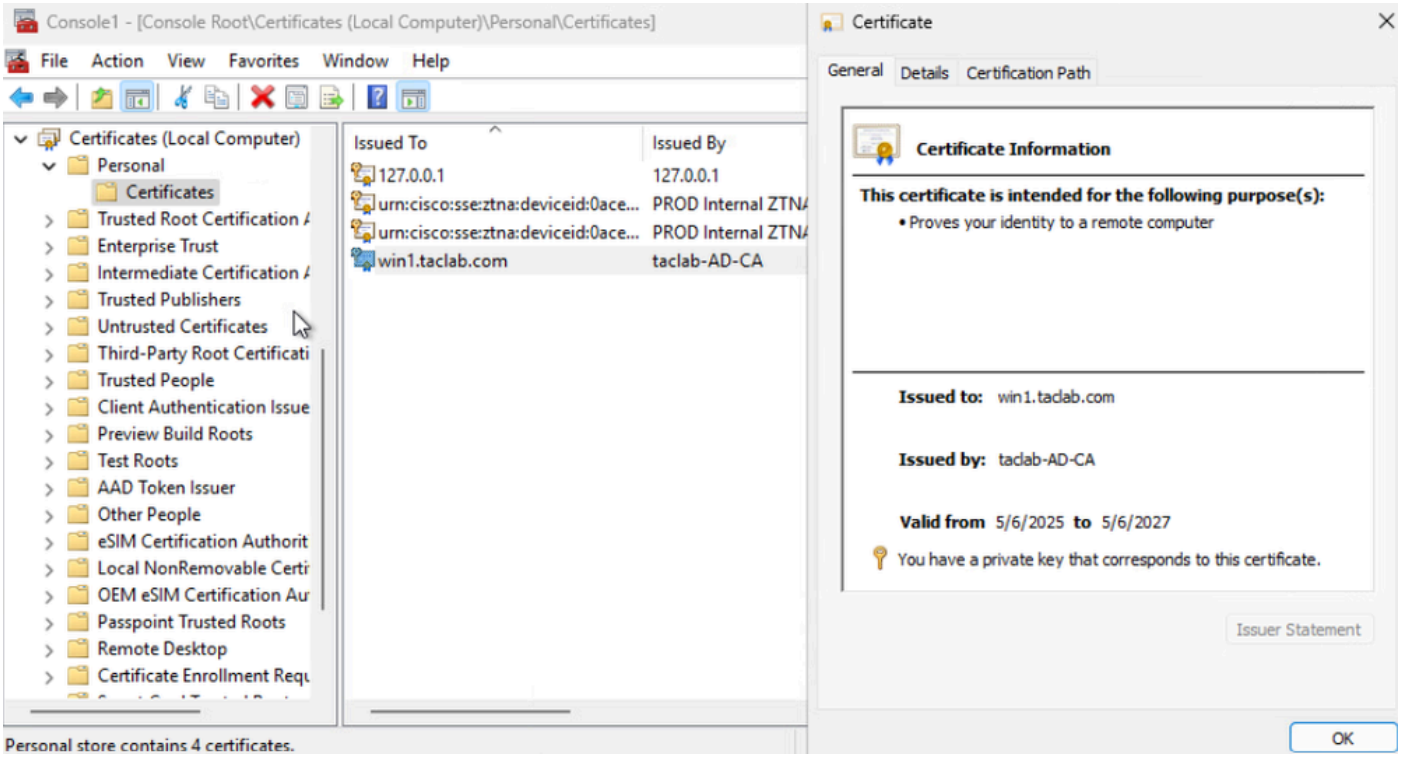
Paso 7 - Generar e importar certificado de terminal

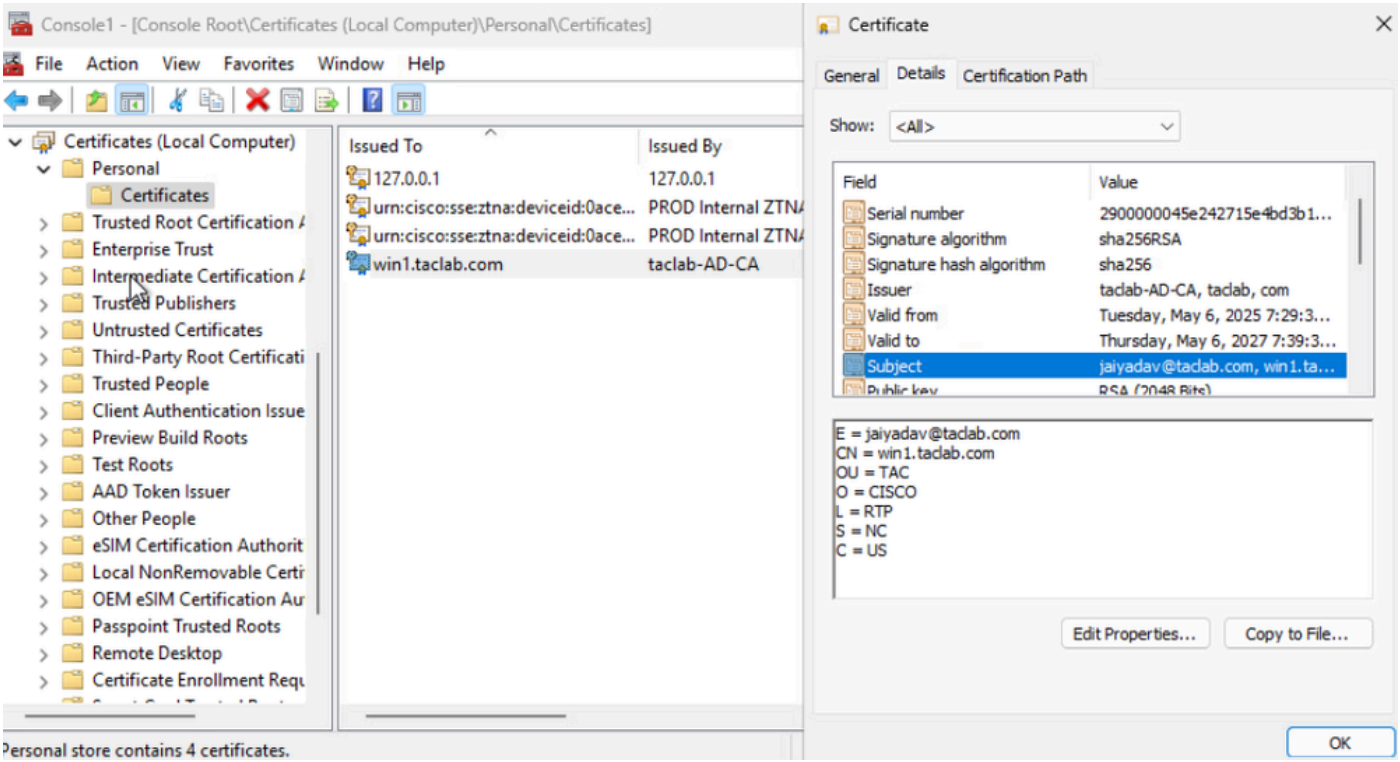
a. Generar CSR , abrir un generador CSR o una herramienta OpenSSL

b. Generar un certificado de extremo desde CA

c. Convertir el archivo .cert en formato PKCS12

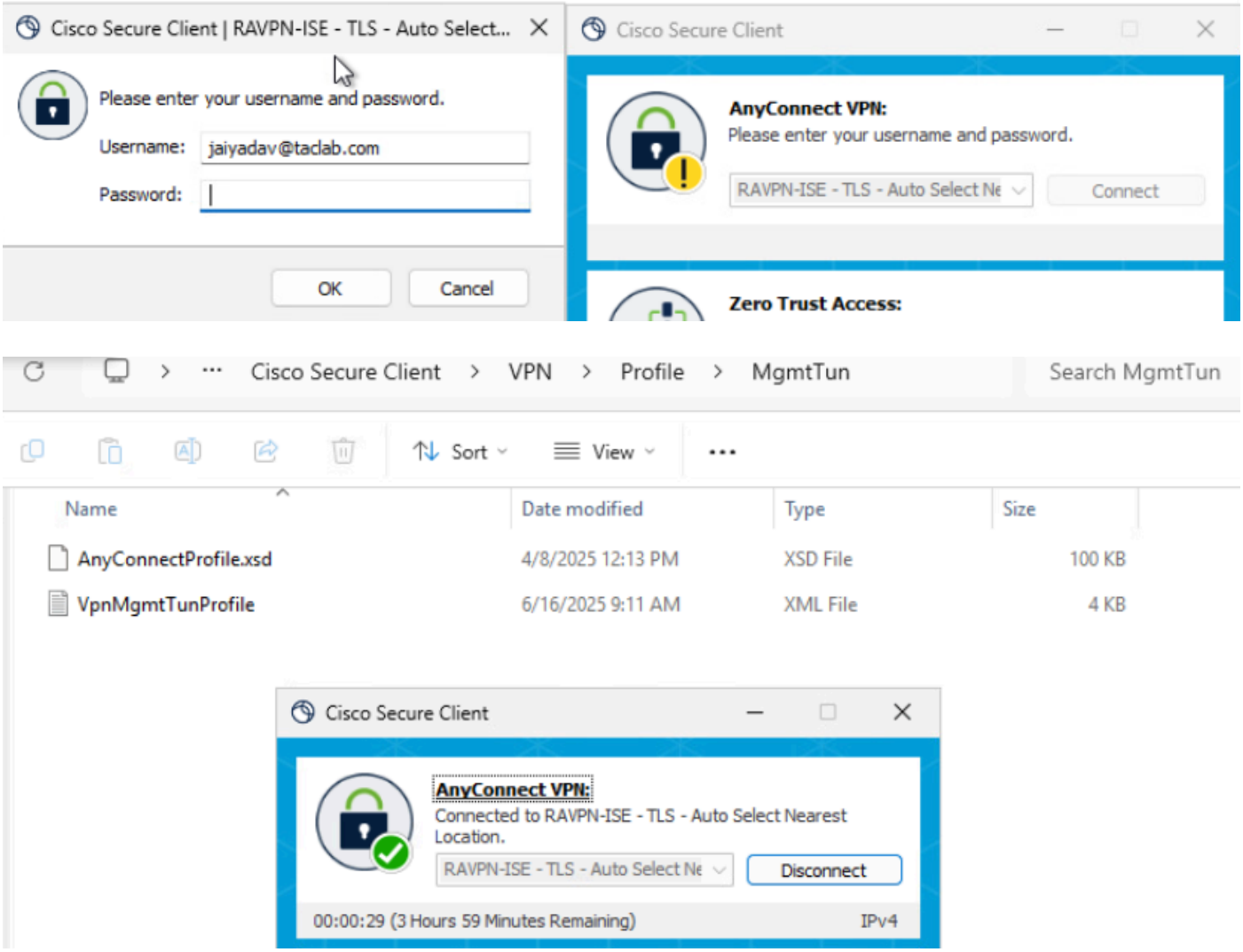
d. Importar el certificado PKCS12 en el almacén de certificados de terminal



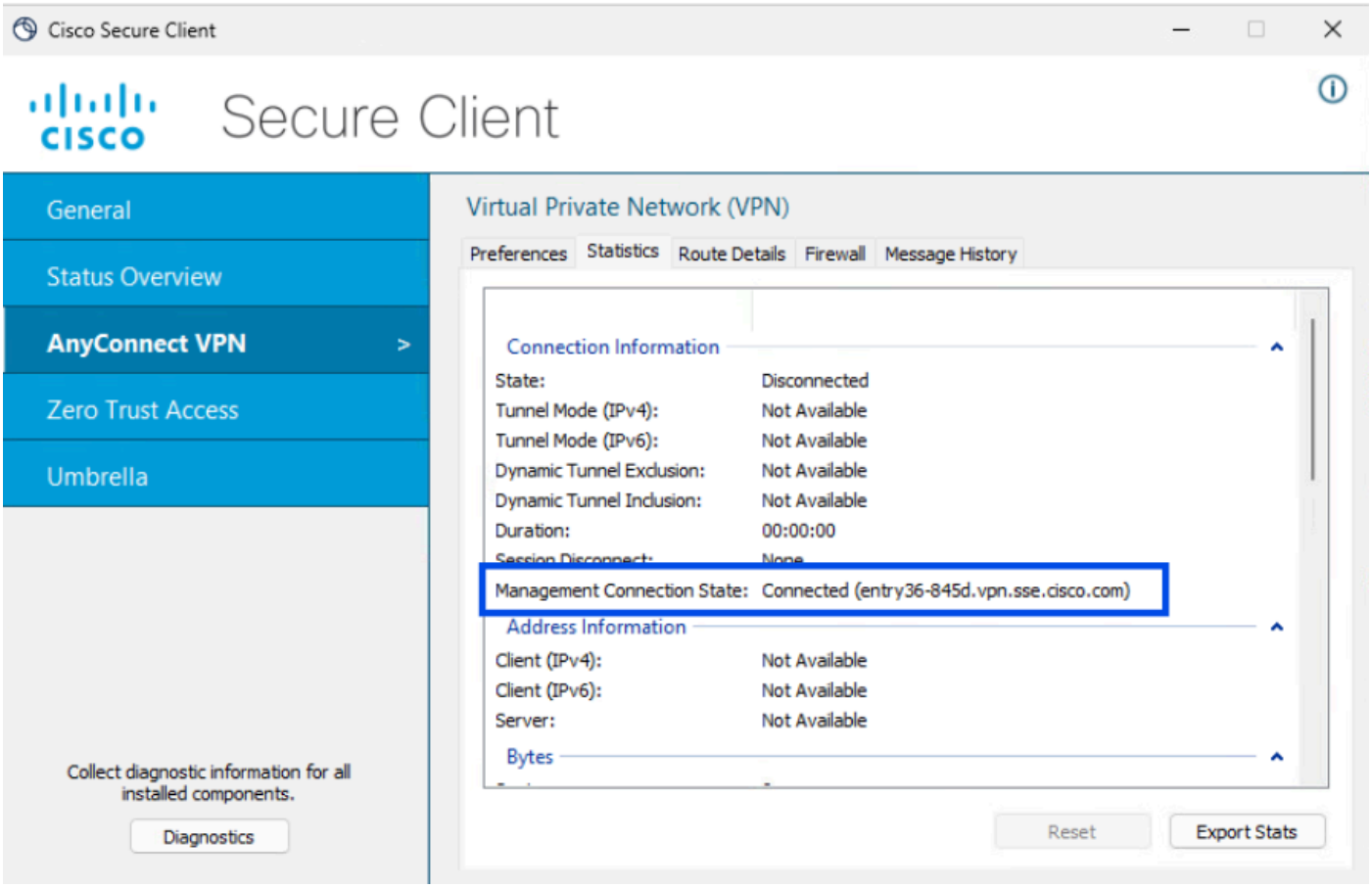


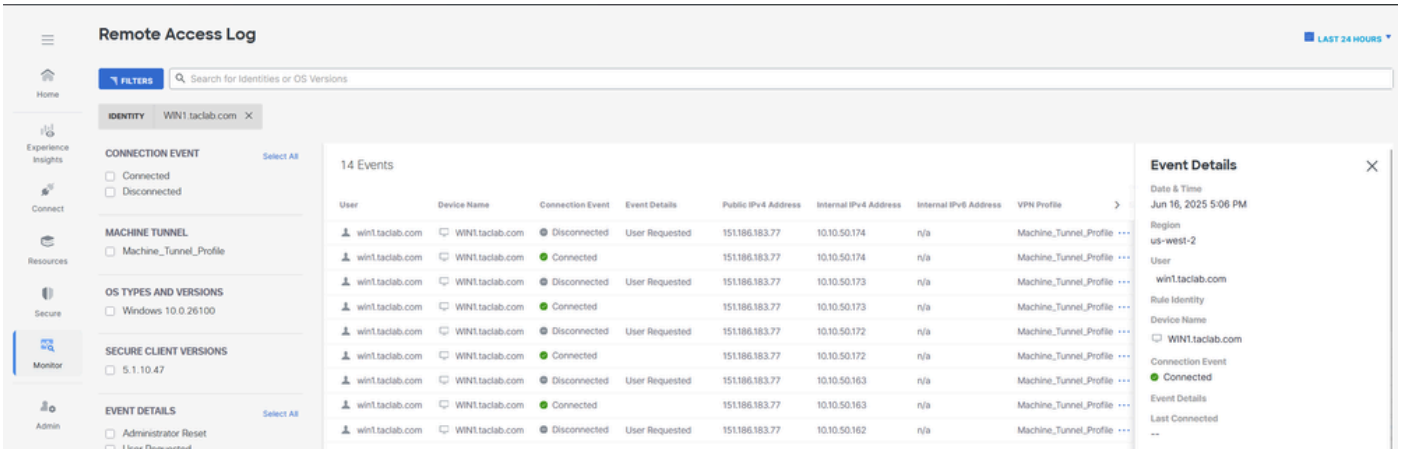
Paso 8: Conexión al túnel de la máquina

a. Conectar a un túnel de usuario , activa la descarga del perfil xml del túnel de máquina



b. Verifique la conectividad del túnel de la máquina





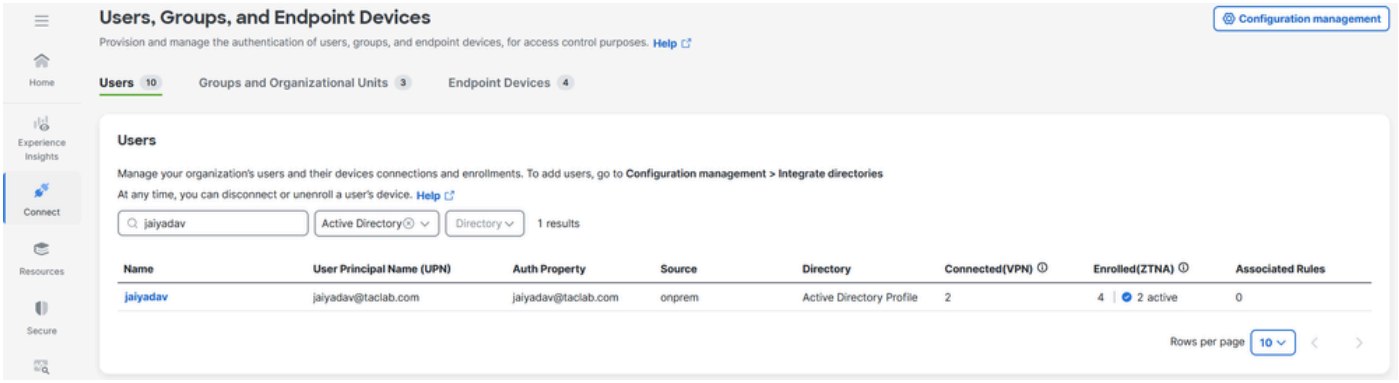
Método 3: configurar el túnel de la máquina mediante el certificado de usuario

En este caso, para que el campo principal se autentique, elija el campo de certificado que contiene el correo electrónico del usuario o UPN. Secure Access utiliza el correo electrónico o UPN como identificador del túnel de la máquina. El formato del correo electrónico o UPN debe coincidir con el formato del identificador de dispositivo seleccionado

Vaya a los pasos del 1 al 4 para la configuración del túnel de máquina

Paso 5 - Configure el conector de AD para poder importar usuarios en Cisco Secure Access .

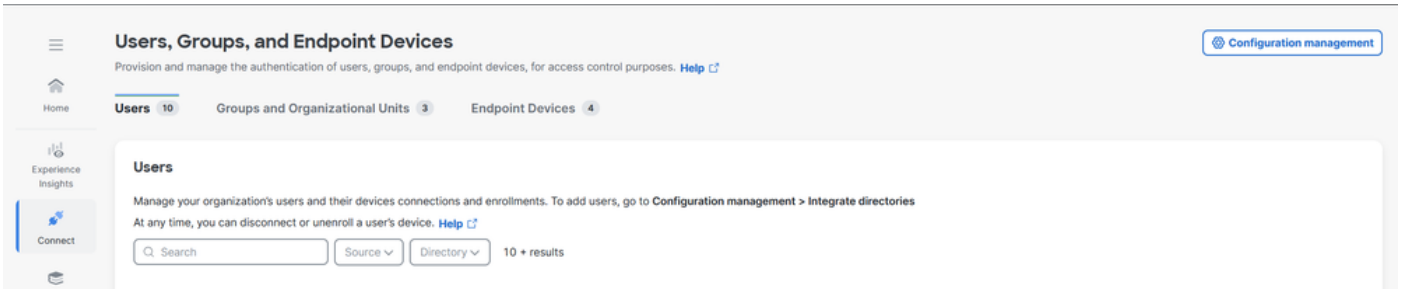
Para obtener más información, vea Integración de Active Directory permanente



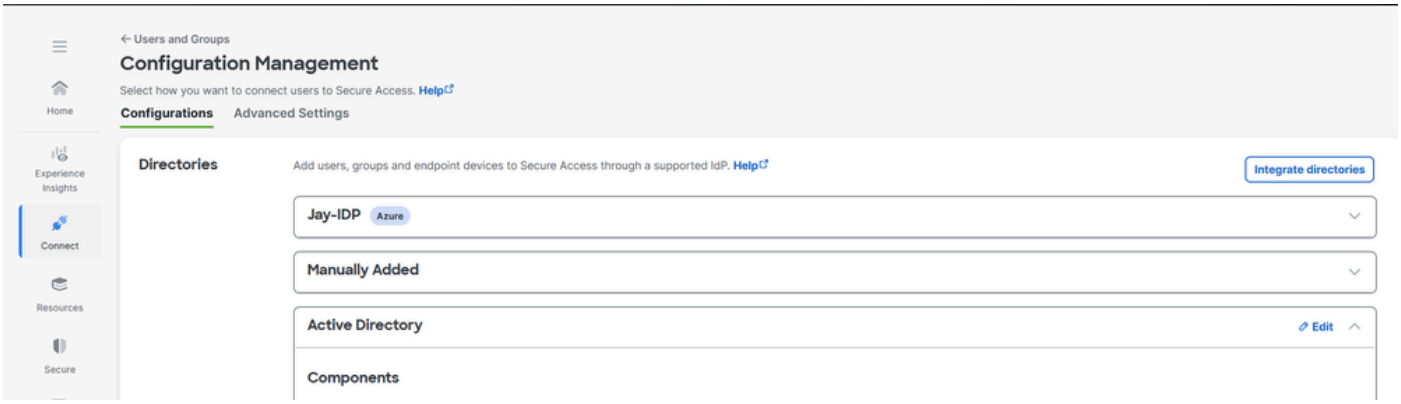
Paso 6: Configuración de la autenticación de usuarios

1. Vaya a Connect > Users,Groups and Endpoint Devices.

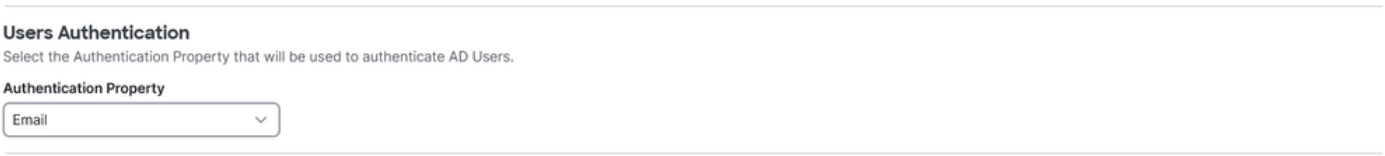
2. Haga clic en Administración de configuración



3. En Configuraciones , edite Active Directory



4. Establezca la propiedad de autenticación de usuarios en Correo electrónico



5. Haga clic en Guardar y reinicie los servicios del conector de AD en los servidores donde está instalado

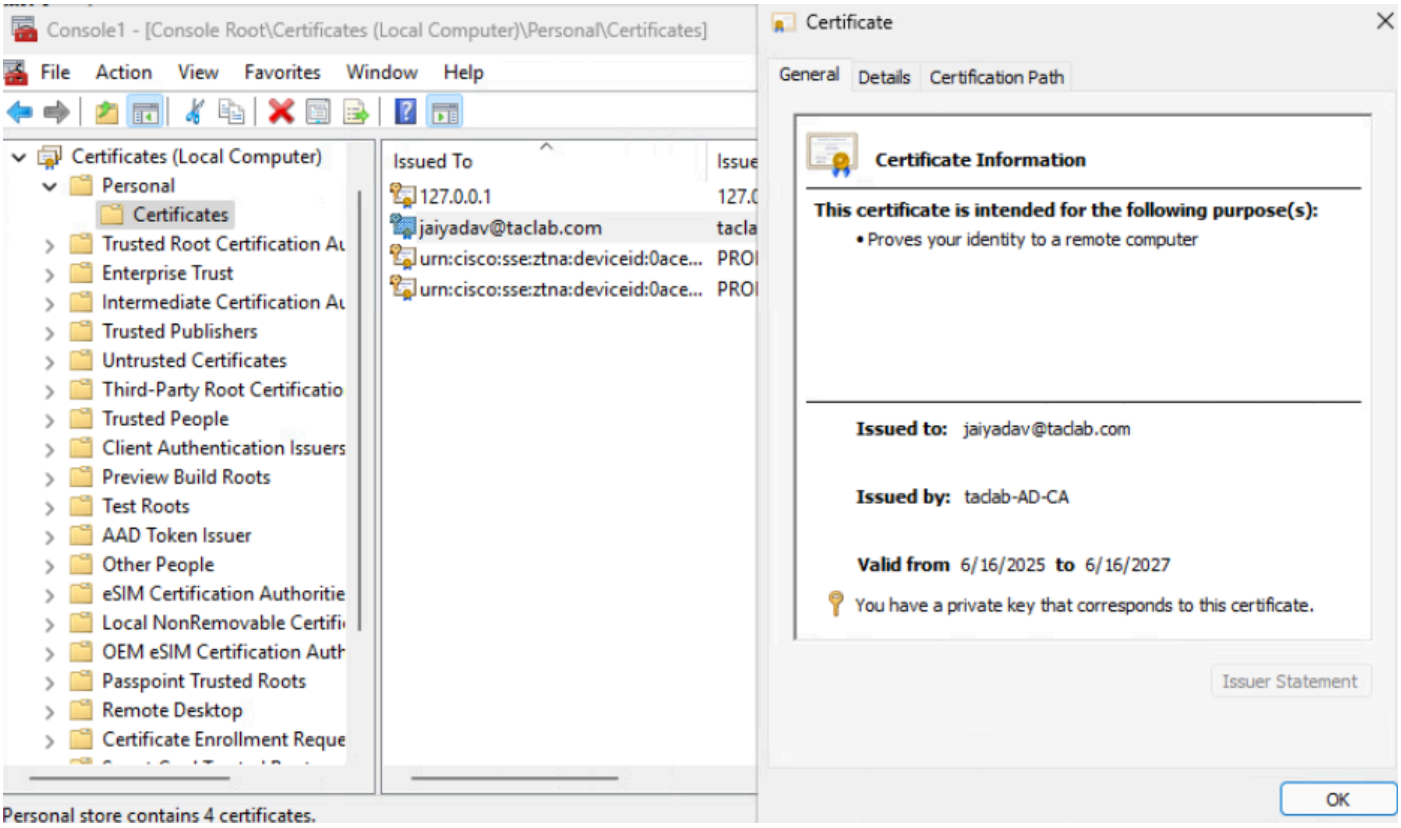
Paso 7 - Generar e importar certificado de terminal

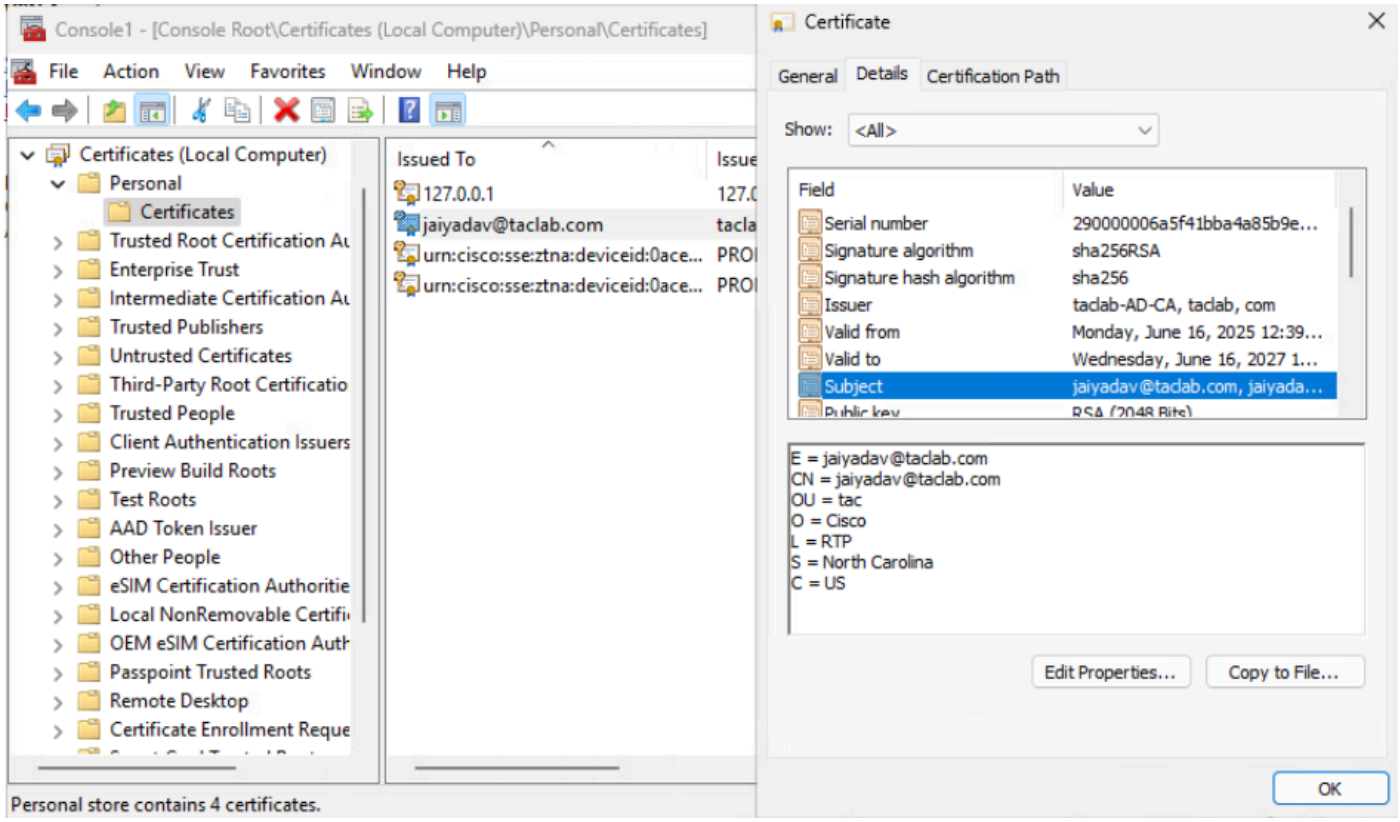
a. Generar CSR , abrir un generador CSR o una herramienta OpenSSL

b. Generar un certificado de extremo desde CA

c. Convertir el archivo .cert en formato PKCS12

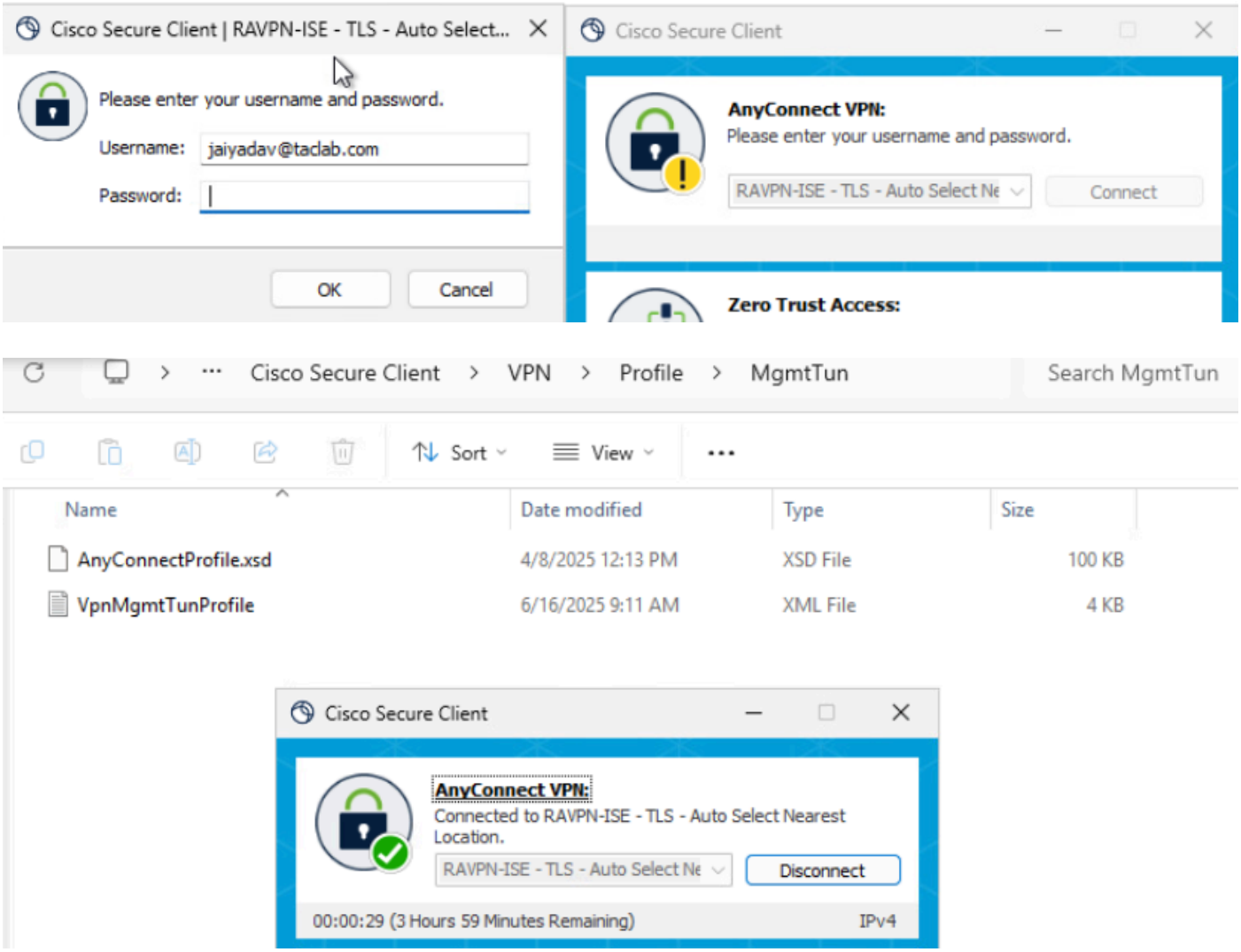
d. Importar el certificado PKCS12 en el almacén de certificados de terminal



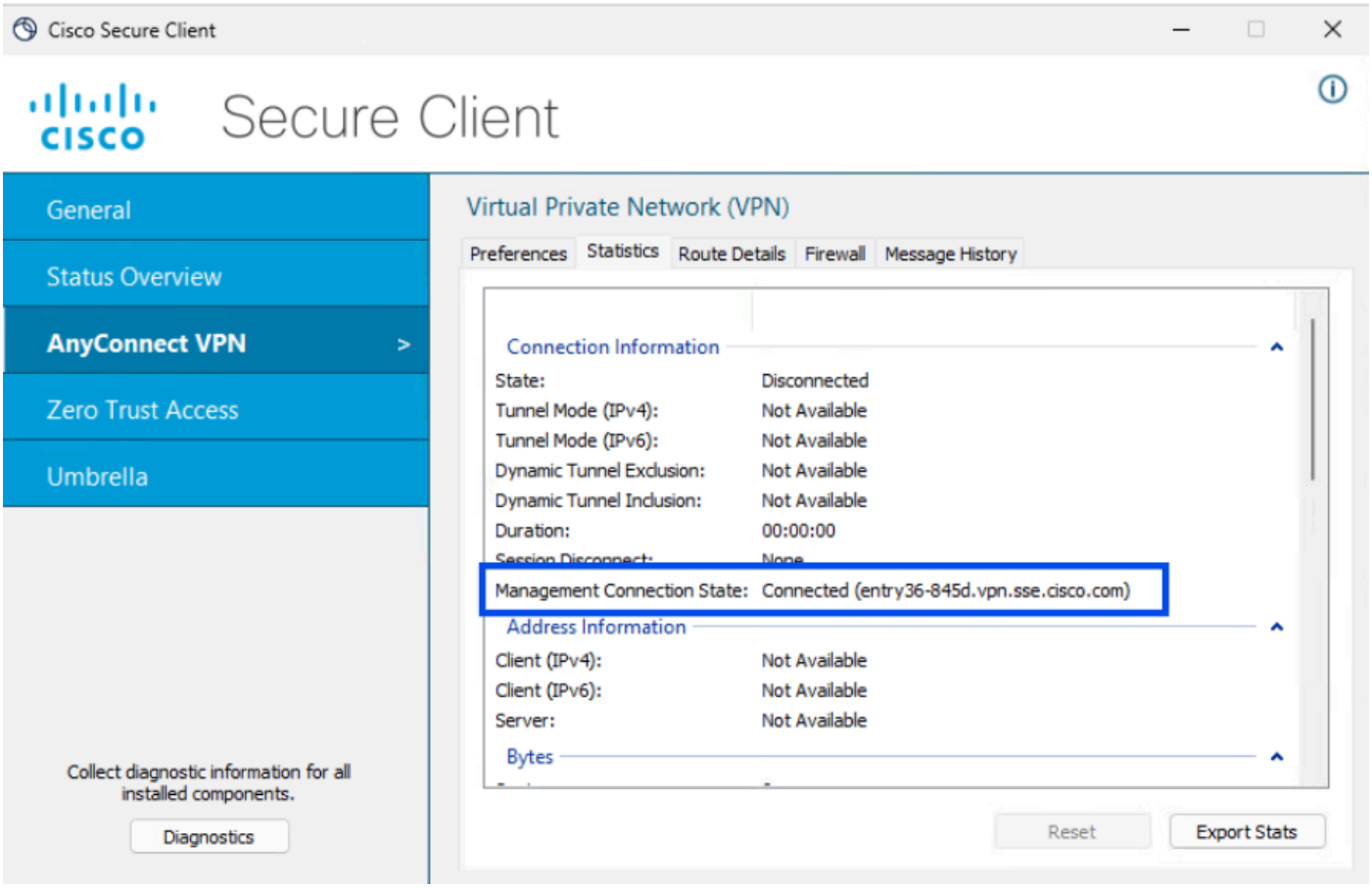


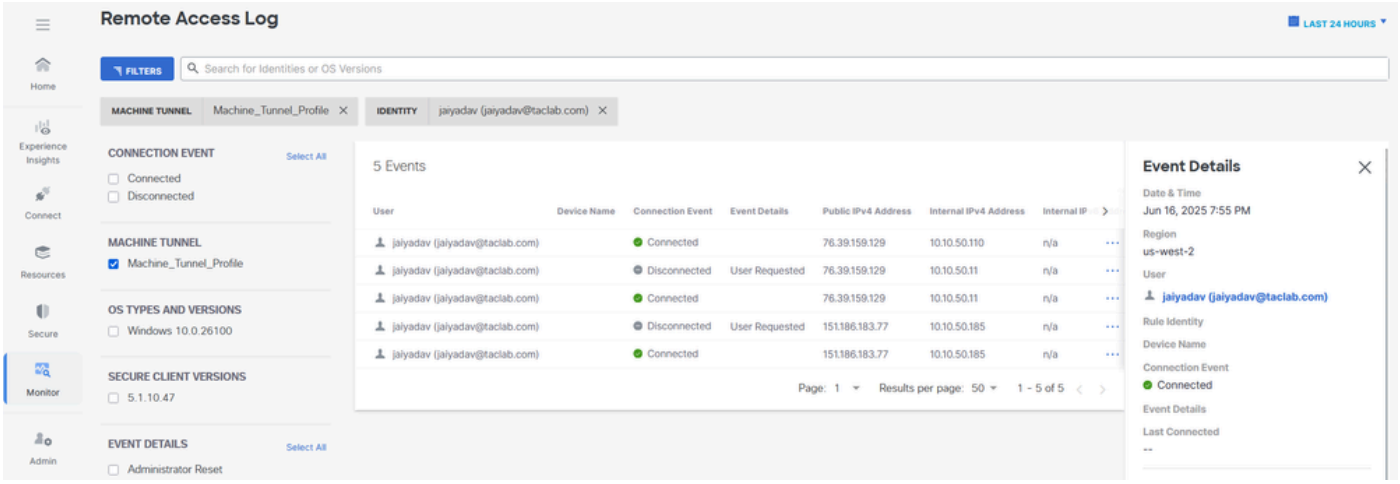
Paso 8: Conexión al túnel de la máquina

a. Conectar a un túnel de usuario , activa la descarga del perfil xml del túnel de máquina



b. Verifique la conectividad del túnel de la máquina





Troubleshoot

Extraiga el paquete DART y abra los registros de AnyConnectVPN y analice los mensajes de error

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).