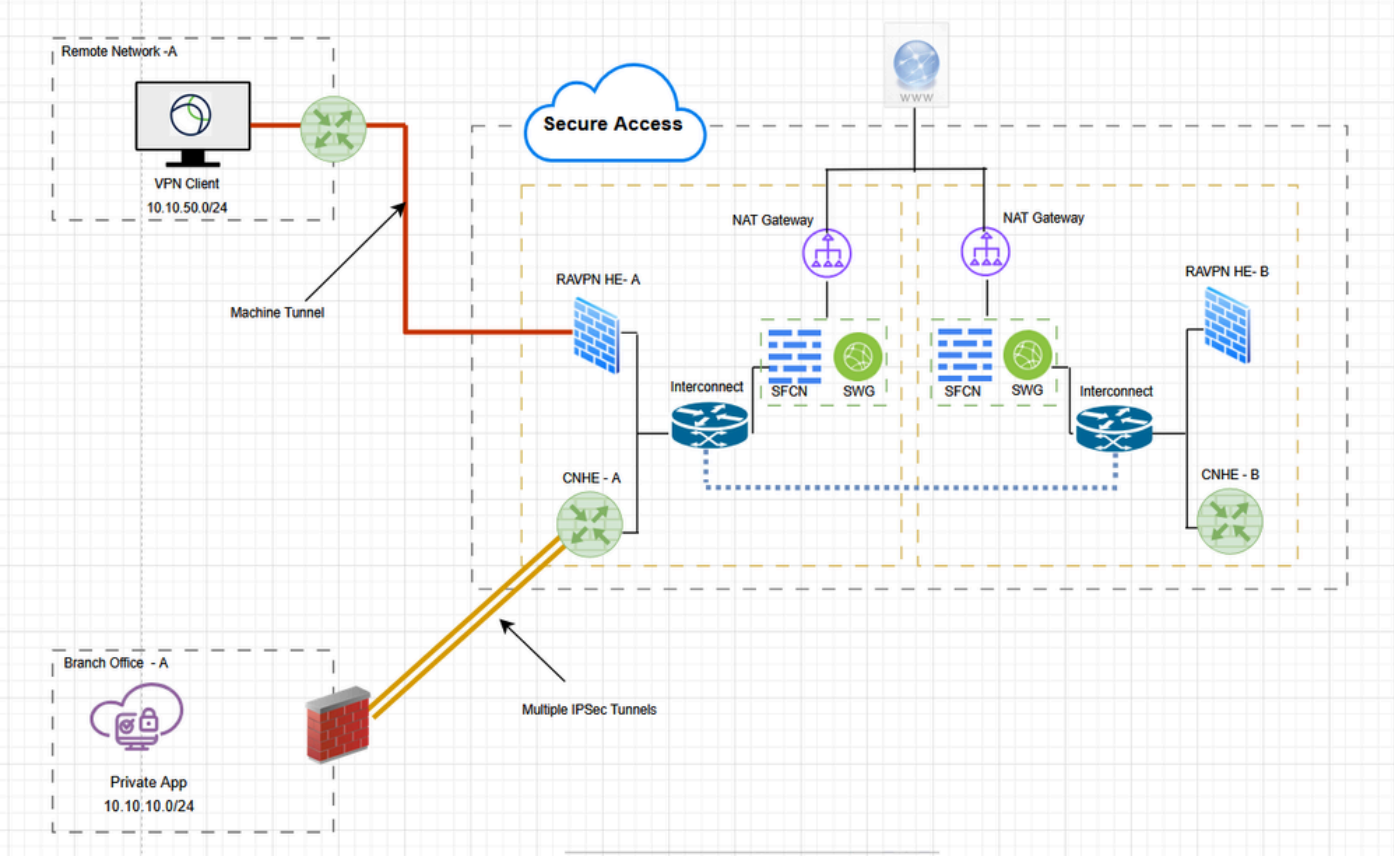
Configurar o túnel da máquina no Cisco Secure Access

Contents

Introdução

Este documento descreve como configurar o Acesso Seguro como o gateway VPN e aceitar conexões do Cliente Seguro através do túnel da máquina VPN.

Diagrama de Rede



Pré-requisitos

- Função de administrador total no acesso seguro.
- Pelo menos um perfil de VPN de usuário configurado no Cisco Secure Access
- Pool IP do usuário no Cisco Secure Access

Requisitos

Recomenda-se que você tenha conhecimento destes tópicos:

- 509 Certificados
- OpenSSL

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Acesso seguro da Cisco
- Cisco Secure Client 5.1.10
- Windows 11
- Windows Server 2019 - CA

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Um túnel de máquina VPN de acesso seguro garante a conectividade com a rede corporativa sempre que o sistema cliente é ligado, não apenas quando uma conexão VPN é estabelecida pelo usuário final. Você pode executar o gerenciamento de patches em endpoints fora do escritório, especialmente em dispositivos que raramente são conectados pelo usuário, via VPN, à rede do escritório. Os scripts de login de SO de endpoint que exigem conectividade de rede corporativa também se beneficiam desse recurso. Para que esse túnel seja criado sem interação do usuário, é usada a autenticação baseada em certificado.

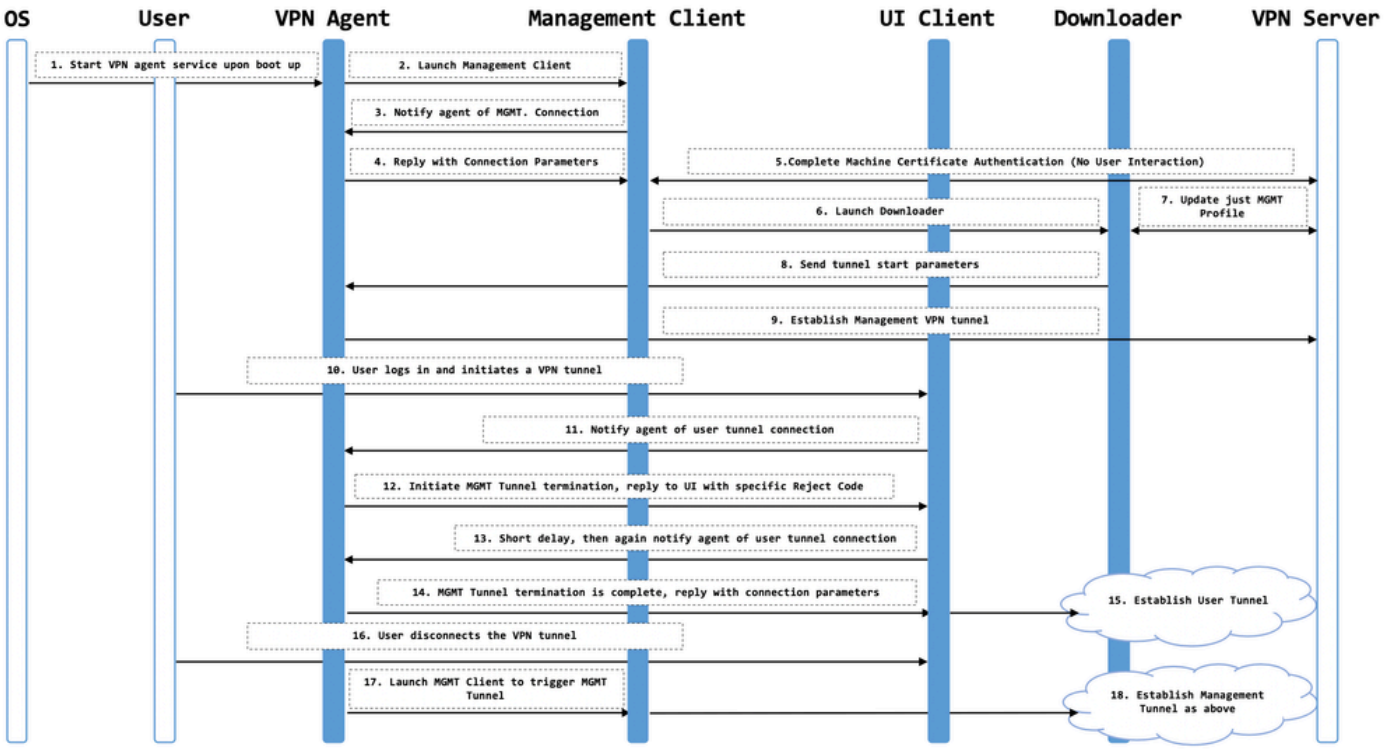
O túnel da máquina do Secure Access permite que os administradores conectem o Cisco Secure Client sem intervenção do usuário antes de o usuário fazer login. O túnel da máquina do Secure Access é acionado quando o endpoint está fora do local e desconectado de uma VPN iniciada pelo usuário. O túnel da máquina VPN de acesso seguro é transparente para o usuário final e se desconecta automaticamente quando o usuário inicia a VPN.

Trabalhando no túnel da máquina

O serviço do agente do Secure Client VPN é iniciado automaticamente na inicialização do sistema. O agente de VPN do Secure Client usa o perfil VPN para detectar se o recurso de túnel da máquina está habilitado. Se o recurso de túnel de máquina estiver habilitado, o agente iniciará o aplicativo cliente de gerenciamento para iniciar uma conexão de túnel de máquina. O aplicativo cliente de gerenciamento usa a entrada do host do perfil VPN para iniciar a conexão. Em seguida, o túnel VPN é estabelecido como de costume, com uma exceção: nenhuma atualização de software é executada durante uma conexão de túnel de máquina, já que o túnel de máquina deve ser transparente para o usuário.

O usuário inicia um túnel VPN por meio do Secure Client, que aciona o término do túnel da máquina. No término do túnel da máquina, o estabelecimento do túnel do usuário continua como de costume.

O usuário desconecta o túnel VPN, que aciona o restabelecimento automático do túnel da máquina.



Limitações

- Não há suporte para interação do usuário.
- Somente há suporte para autenticação baseada em certificado por meio do Repositório de Certificados de Computador (Windows).
- A verificação de Certificado de Servidor restrito é imposta.
- Não há suporte para um proxy privado.
- Não há suporte para um proxy público (há suporte para o valor ProxyNative em plataformas em que as configurações de Proxy Nativo não são recuperadas do navegador).
- Não há suporte para Scripts de Personalização de Cliente Seguro

Configurar

Método 1 - Configurar o túnel da máquina com o usuário machine@sse.com

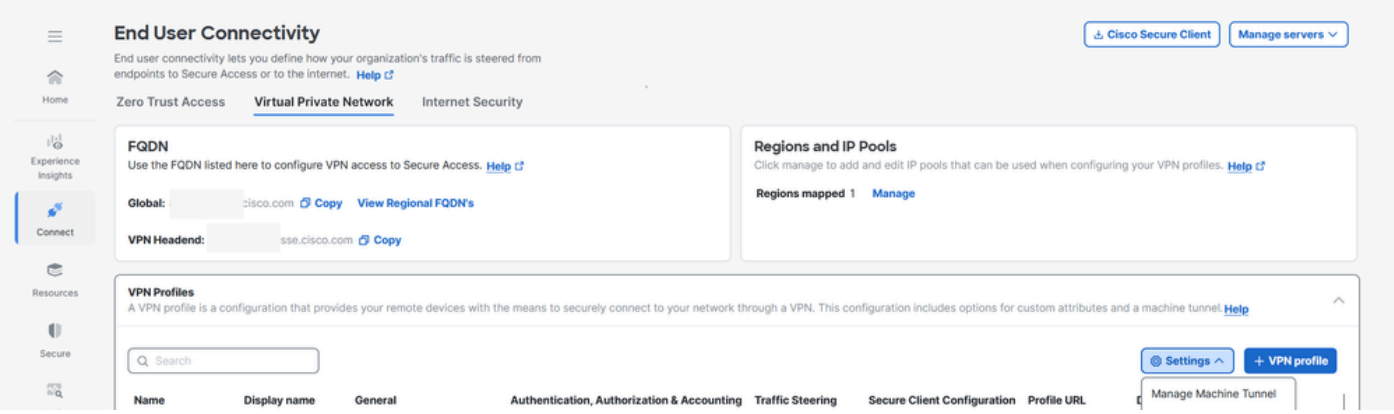
Etapa 1 - Configurações gerais

Defina as configurações gerais, incluindo o domínio e os protocolos que este túnel de máquina usa.

1. Navegue até Connect > End User Connectivity > Virtual Private Network.

2. Navegue até VPN Profiles e defina as configurações para o túnel da máquina.

    a. Clique em Settings e escolha Manage Machine Tunnel na lista suspensa.

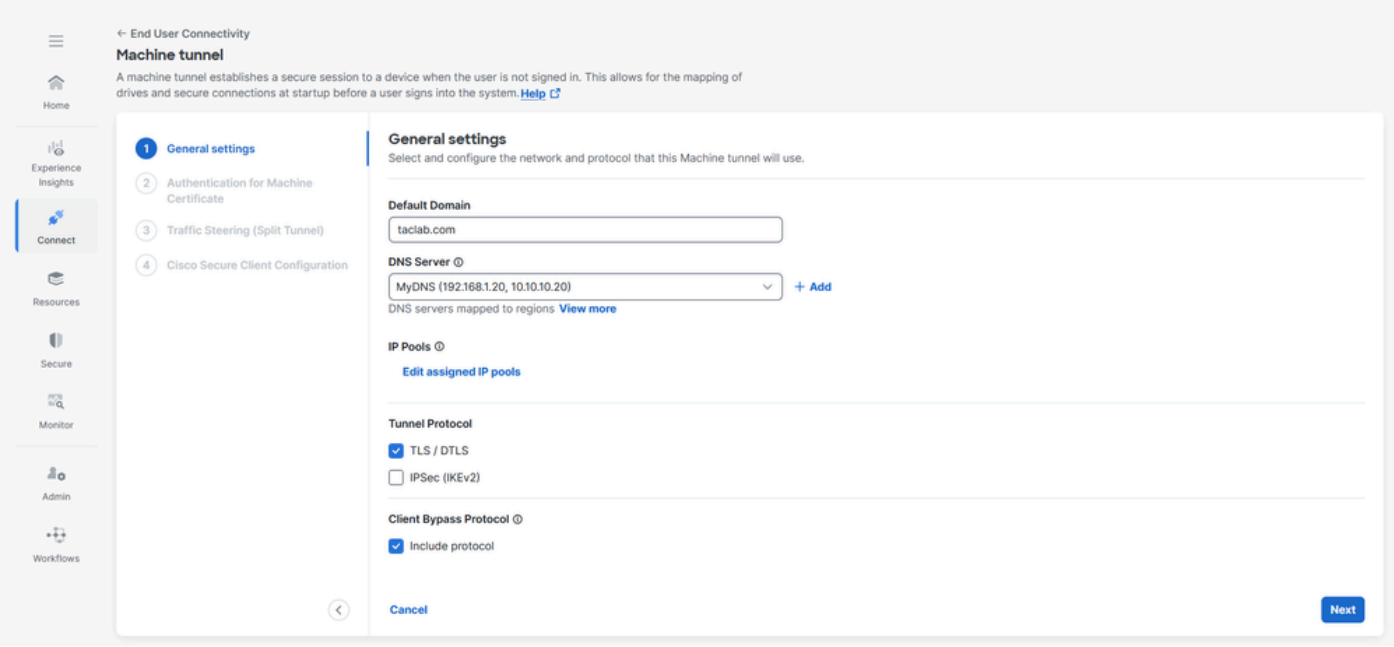


3. Insira o domínio padrão.
4. O servidor DNS mapeado através da página Gerenciar regiões e pools de IP é definido como o servidor padrão. Você pode aceitar o servidor DNS padrão, escolher outro servidor DNS na lista suspensa ou clicar em + Adicionar para adicionar um novo par de servidores DNS. Selecionar outro servidor DNS ou adicionar um novo servidor DNS substitui esse servidor padrão.
5. Selecione um pool de IP por região na lista suspensa IP Pools. Os perfis VPN devem ter pelo menos um pool IP atribuído em cada região para uma configuração válida.
6. Selecione o protocolo de túnel que este túnel de máquina usa:
   - TLS/DTLS
   - IPSec (IKEv2)

   Pelo menos um protocolo deve ser selecionado.
7. Opcionalmente, marque Incluir protocolo para impor o protocolo de desvio do cliente.

   a. Se o Client Bypass Protocol estiver habilitado para um protocolo IP e um pool de endereços não estiver configurado para esse protocolo (em outras palavras, nenhum endereço IP para esse protocolo foi atribuído ao cliente pelo ASA), qualquer tráfego IP que use esse protocolo não será enviado através do túnel VPN. Deve ser enviado para fora do túnel.

   b. Se o Client Bypass Protocol estiver desabilitado e um pool de endereços não estiver configurado para esse protocolo, o cliente descartará todo o tráfego para esse protocolo IP quando o túnel VPN for estabelecido.



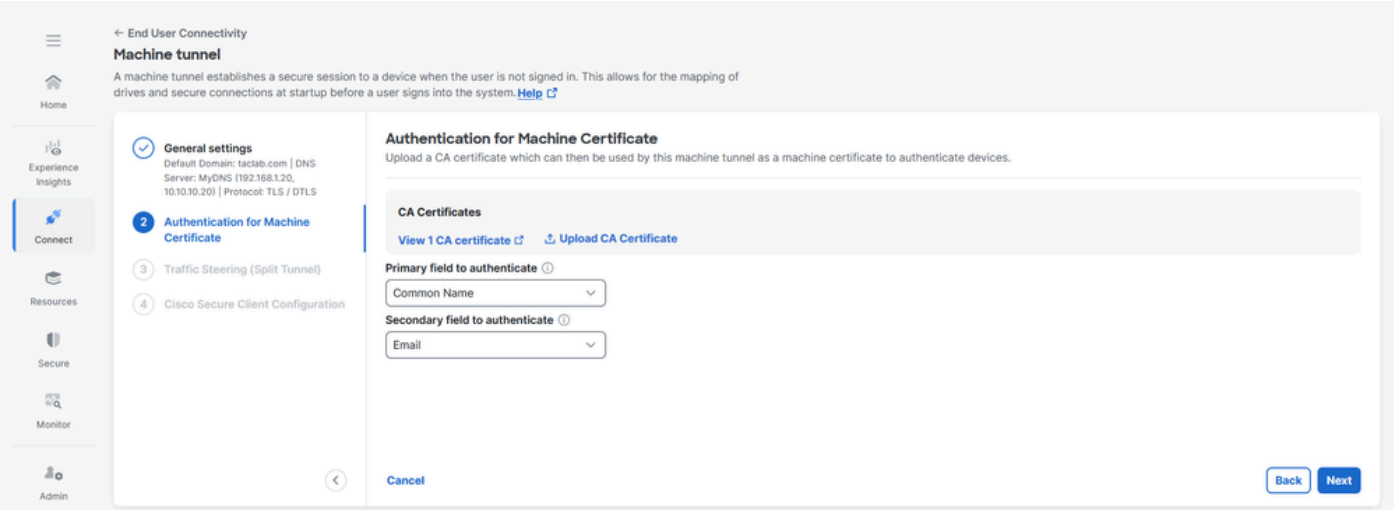
8. Clique em Próximo

Etapa 2 - Autenticação do certificado da máquina

O túnel da máquina é transparente para o usuário final e se desconecta automaticamente quando o usuário inicia uma sessão VPN. Para que esse túnel seja criado sem interação do usuário, é usada a autenticação baseada em certificado.

1. Selecione os certificados da AC na lista ou clique em Enviar certificados da AC

2. Selecione os campos de autenticação baseados em certificado. Para obter mais informações, consulte campos de autenticação baseada em certificado



3. Clique em Próximo

Etapa 3 - Direcionamento de tráfego (túnel dividido)

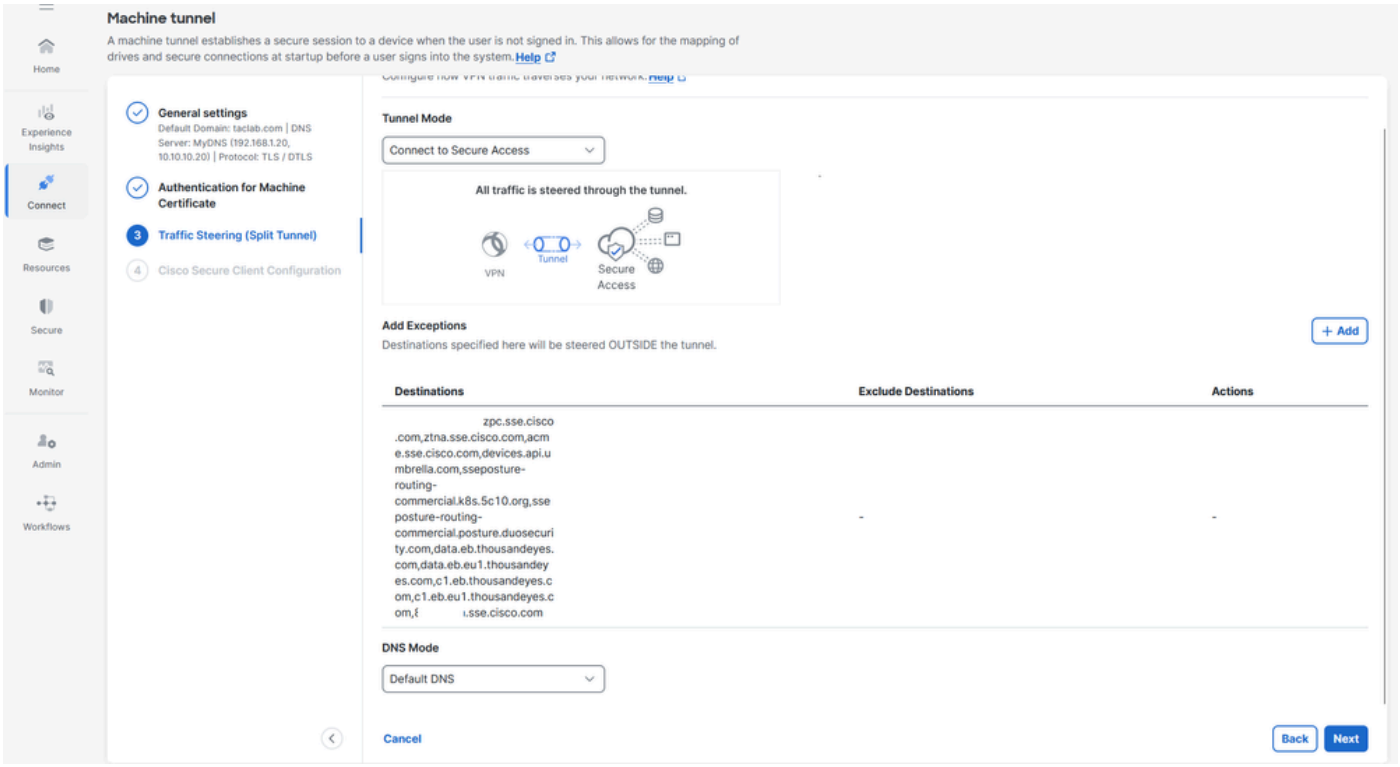
Para Traffic Steering (Split Tunnel), você pode configurar um túnel de máquina para manter uma

conexão de túnel completa para Secure Access, ou configurá-lo para usar uma conexão de túnel dividido para direcionar o tráfego através da VPN apenas se necessário.Para obter mais informações, consulte [Direção de tráfego de Machine Tunnel]

1. Selecione o modo de túnel

2. Dependendo da seleção do Modo de túnel , você pode Adicionar exceções

3. Selecione o modo DNS

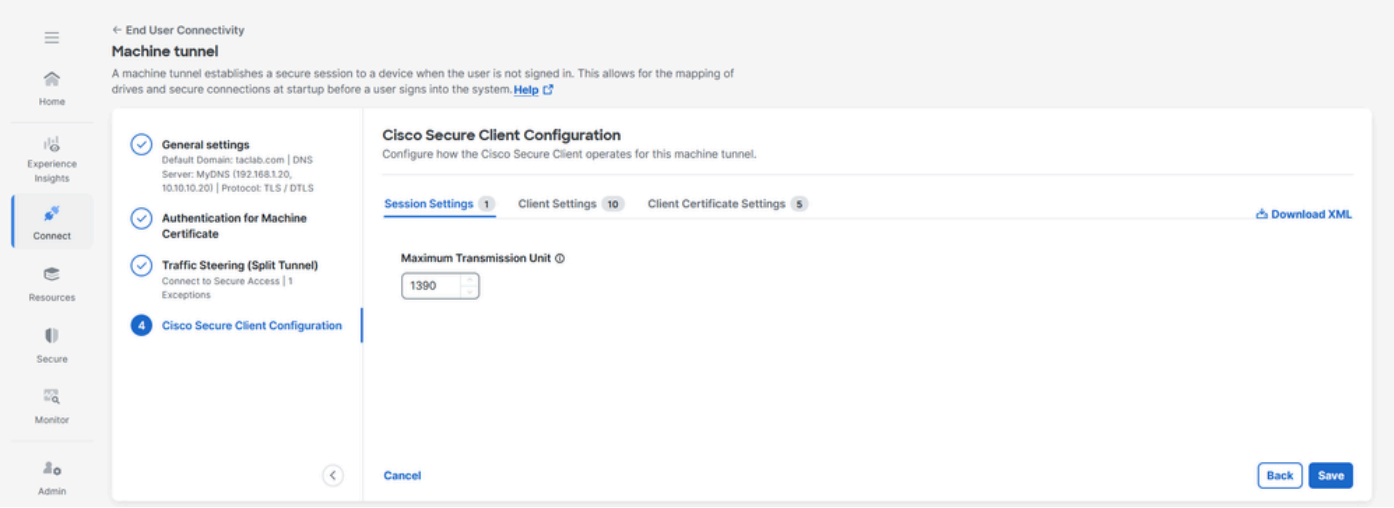


4. Clique em Próximo

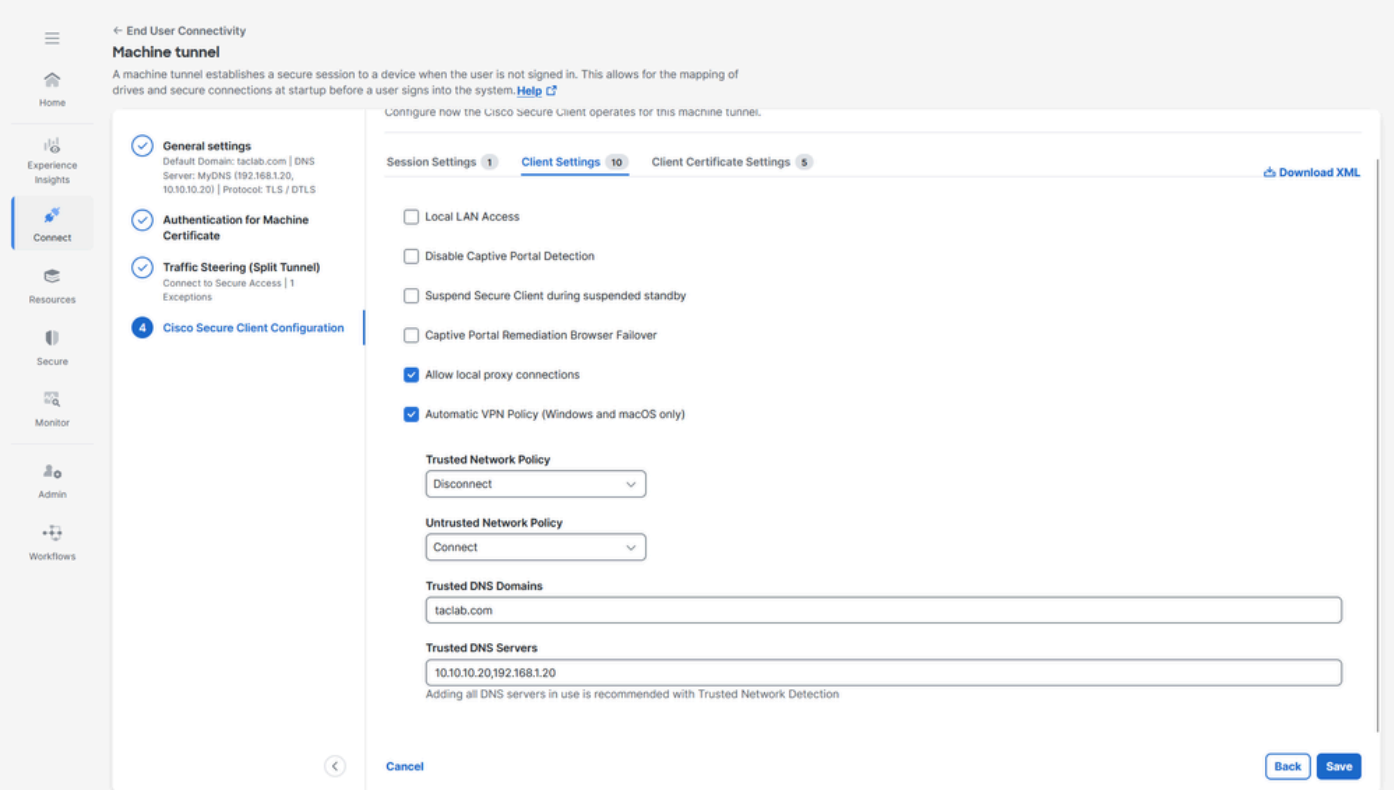
Etapa 4 - Configuração do Cisco Secure Client

Você pode modificar um subconjunto de configurações do Cisco Secure Client com base nas necessidades de um túnel de máquina VPN específico. Para obter mais informações, consulte [Configuração de Cliente Seguro]

1. Verificar a Unidade Máxima de Transmissão, o maior tamanho do pacote que pode ser enviado no túnel VPN sem fragmentação



2. Configurações do cliente , consulte Configurações do cliente do túnel da máquina para obter mais informações



3. Configurações de Certificado do Cliente, selecione as opções de acordo

a. Substituição do Repositório de Certificados do Windows — Permite que um administrador direcione o Cliente Seguro para utilizar certificados no repositório de certificados da máquina Windows (Sistema Local) para autenticação de certificado de cliente.

b. Seleção automática de certificado - Quando a autenticação de vários certificados é configurada no gateway seguro

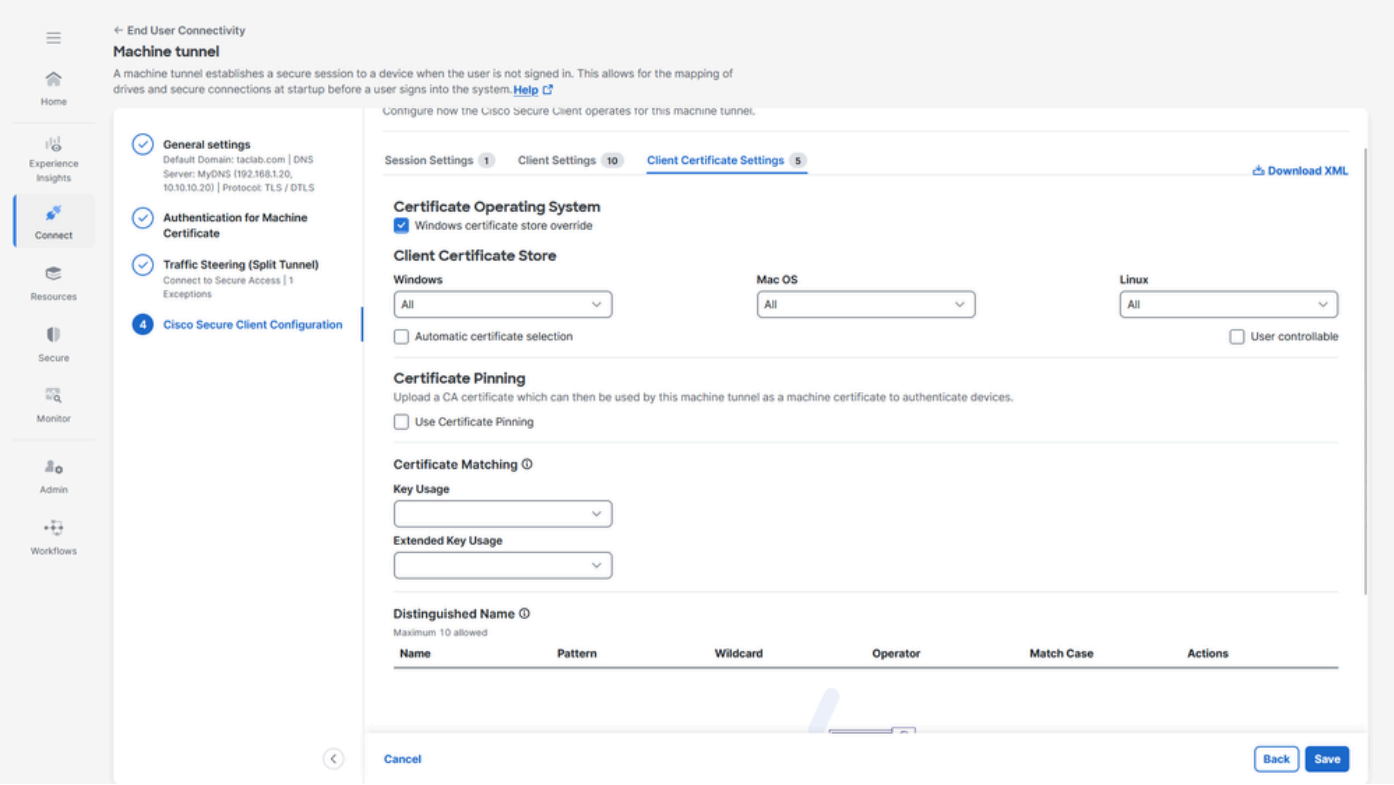
c. Fixação de Certificado - Certificado CA que pode ser usado pelo túnel da máquina como um certificado da máquina para autenticar dispositivos

d. Correspondência de certificado - Se nenhum critério de correspondência de certificado for especificado, o Cisco Secure Client aplicará as regras de correspondência de certificado

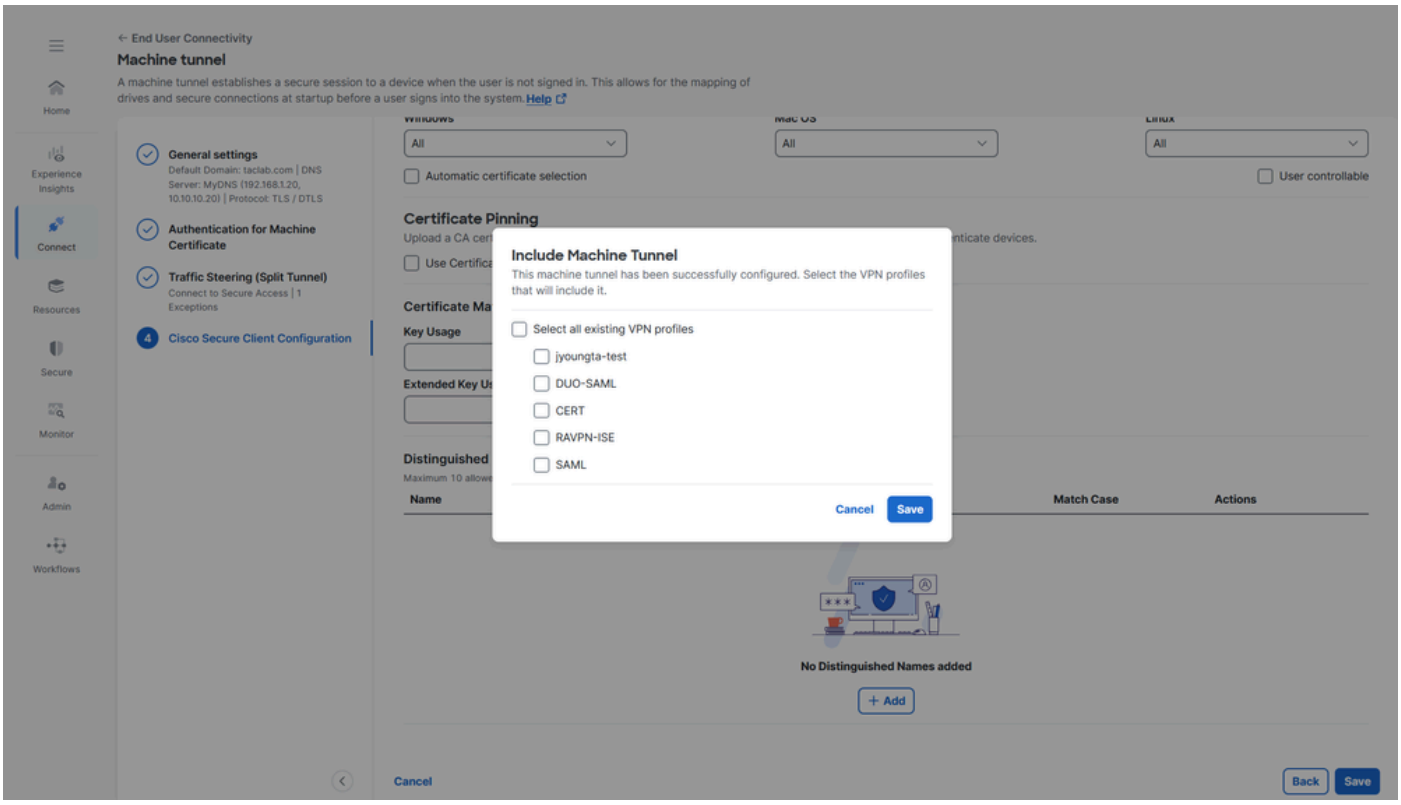
i. Uso de chave: Assinatura_Digital

ii) Uso estendido de chave: Autenticação do Cliente

e. Nome Distinto - Especifica nomes distintos (DNs) para critérios de correspondência exata na escolha de certificados de cliente aceitáveis. Quando você adiciona vários Nomes Distintos, cada certificado é verificado em relação a todas as entradas e todas elas devem ser correspondentes.

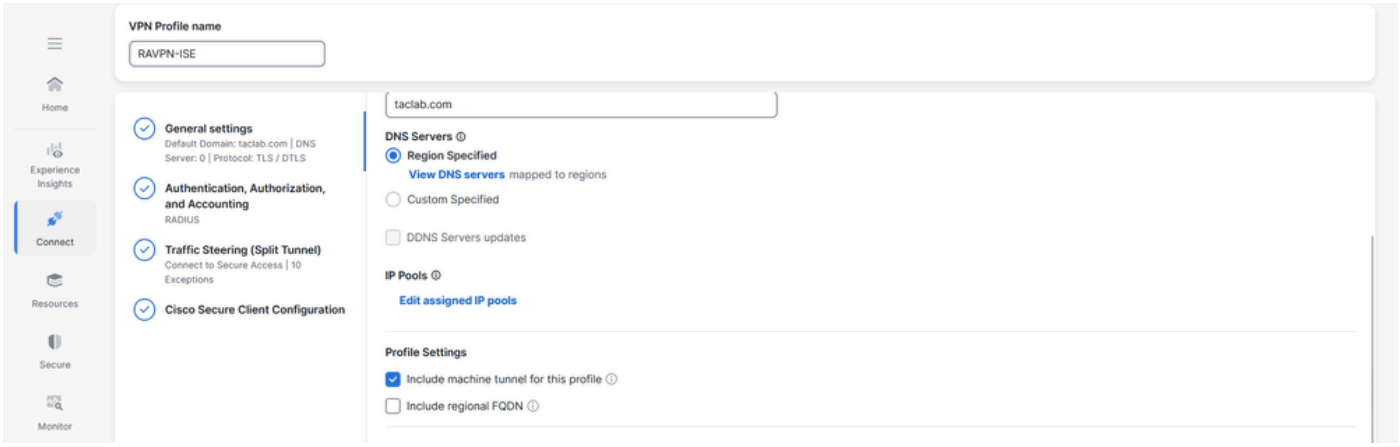


4. Atribua o perfil Machine Tunnel a um perfil de User VPN, clique em Save e então há uma opção para selecionar os perfis de User VPN



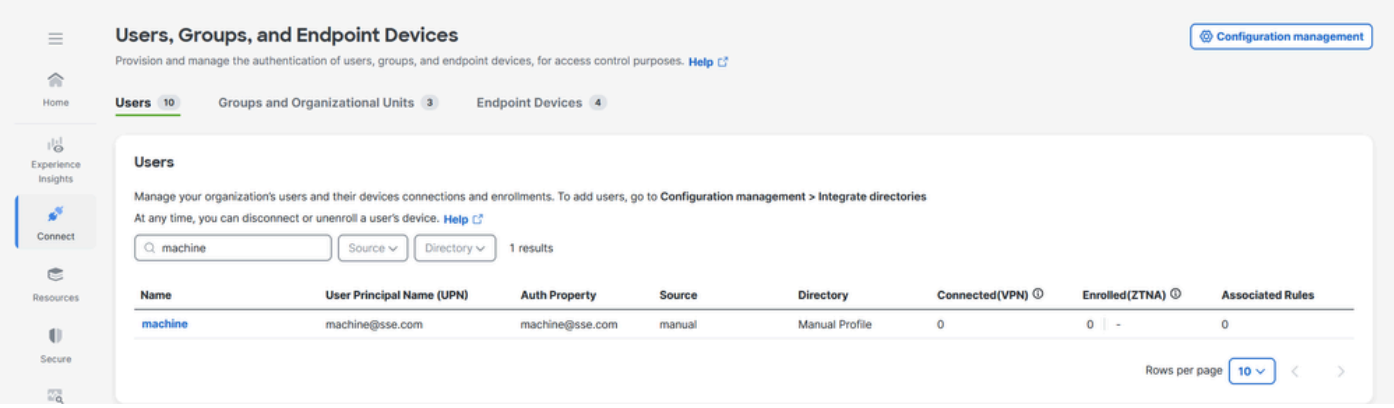
5. Clique em Salvar

6. Verifique se o perfil do Túnel da Máquina está anexado a um perfil de VPN do Usuário



Etapa 5 - Verificar se o usuário machine@sse.com está presente no Cisco Secure Access

1. Navegue até Connect > Users,Groups, and Endpoint Devices > Users



2. Se o usuário machine@sse.com não estiver presente na importação manualmente. Para obter mais informações, consulte Importação manual de usuários e grupos

Etapa 6 - Gerar um certificado assinado por uma autoridade de certificação para machine@sse.com

1. Gerar uma solicitação de Assinatura de Certificado

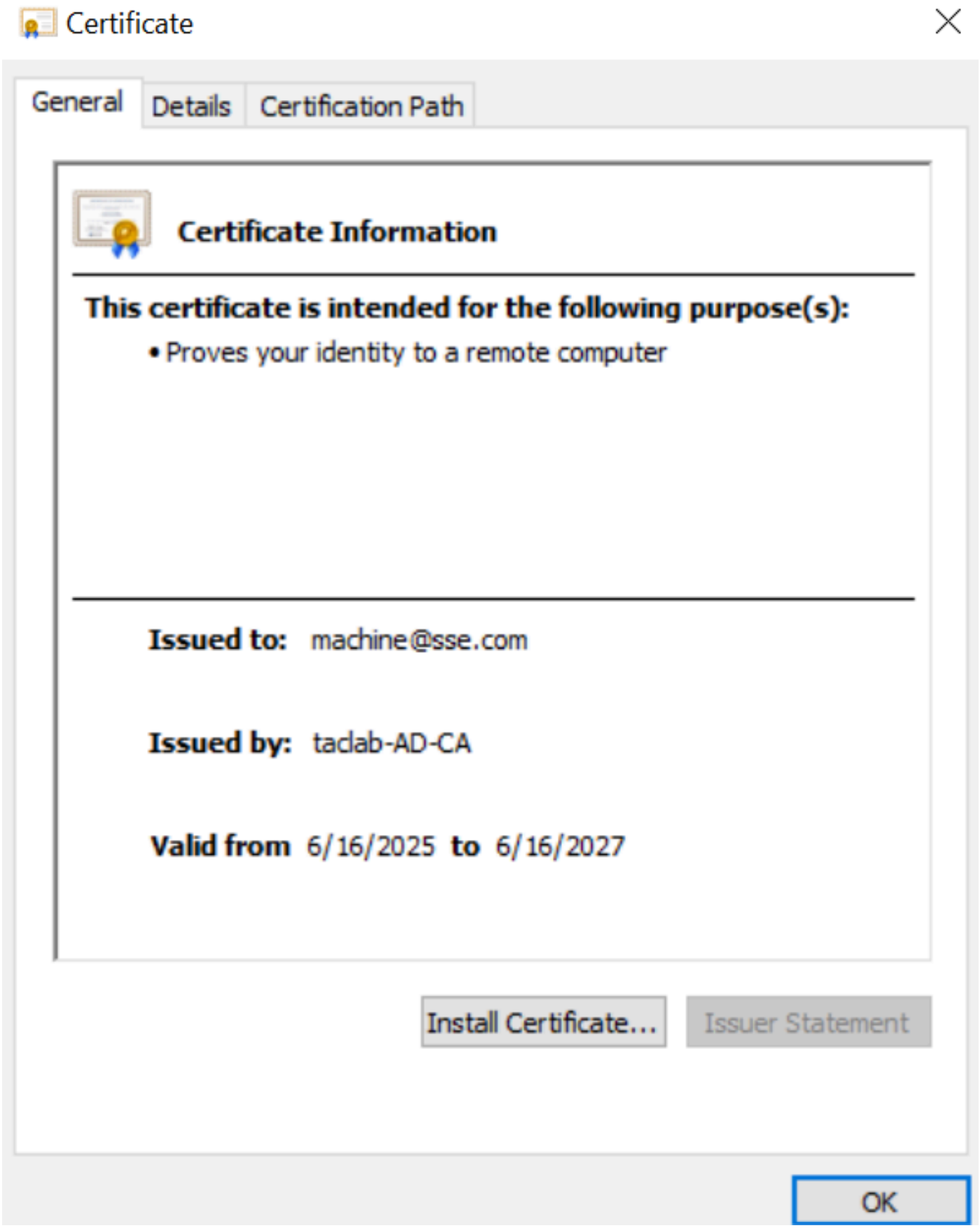
a. Podemos usar qualquer software gerador de CSR on-line Gerador de CSR ou uma CLI do openssl

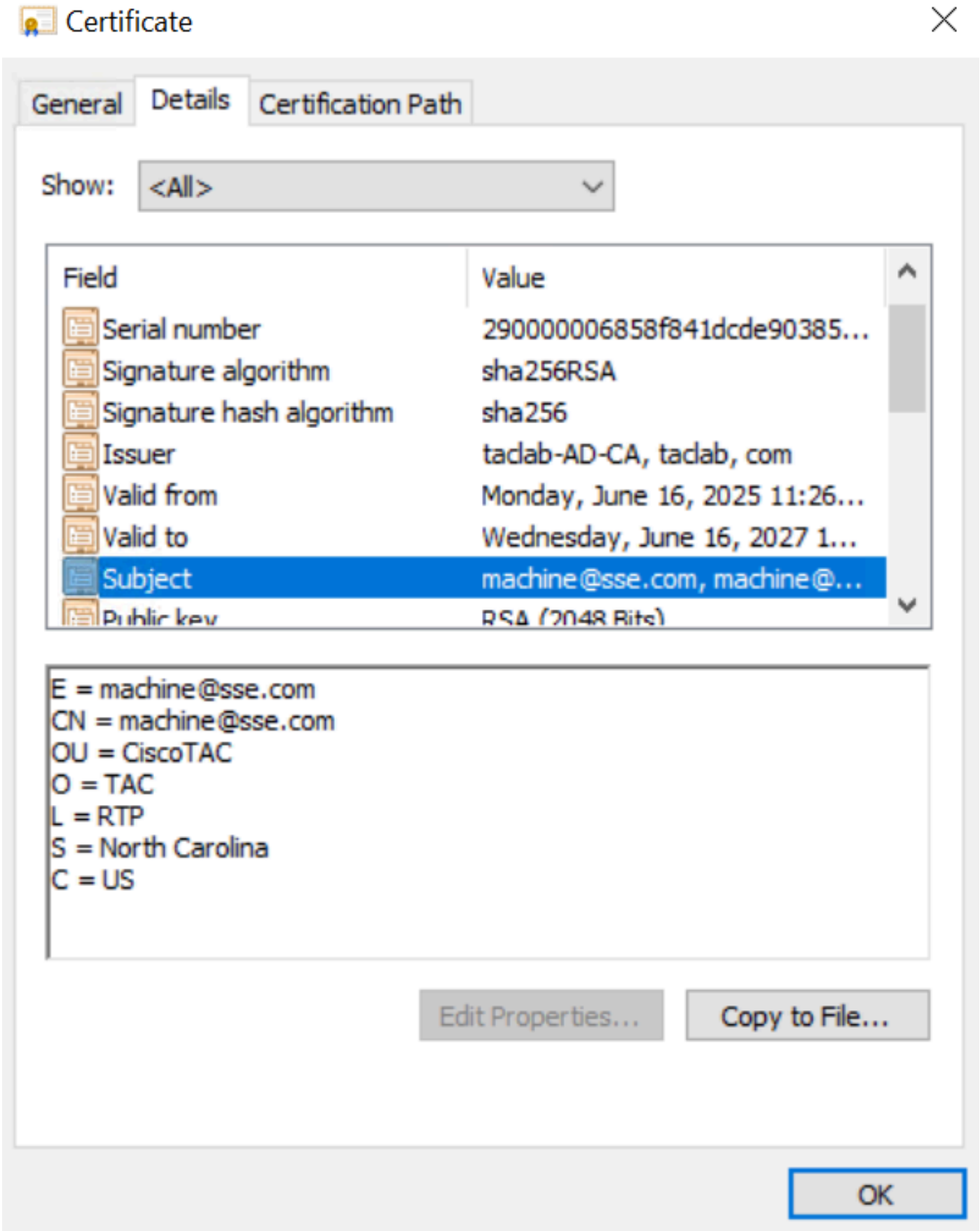
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr

```
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 o CSR e gere um 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



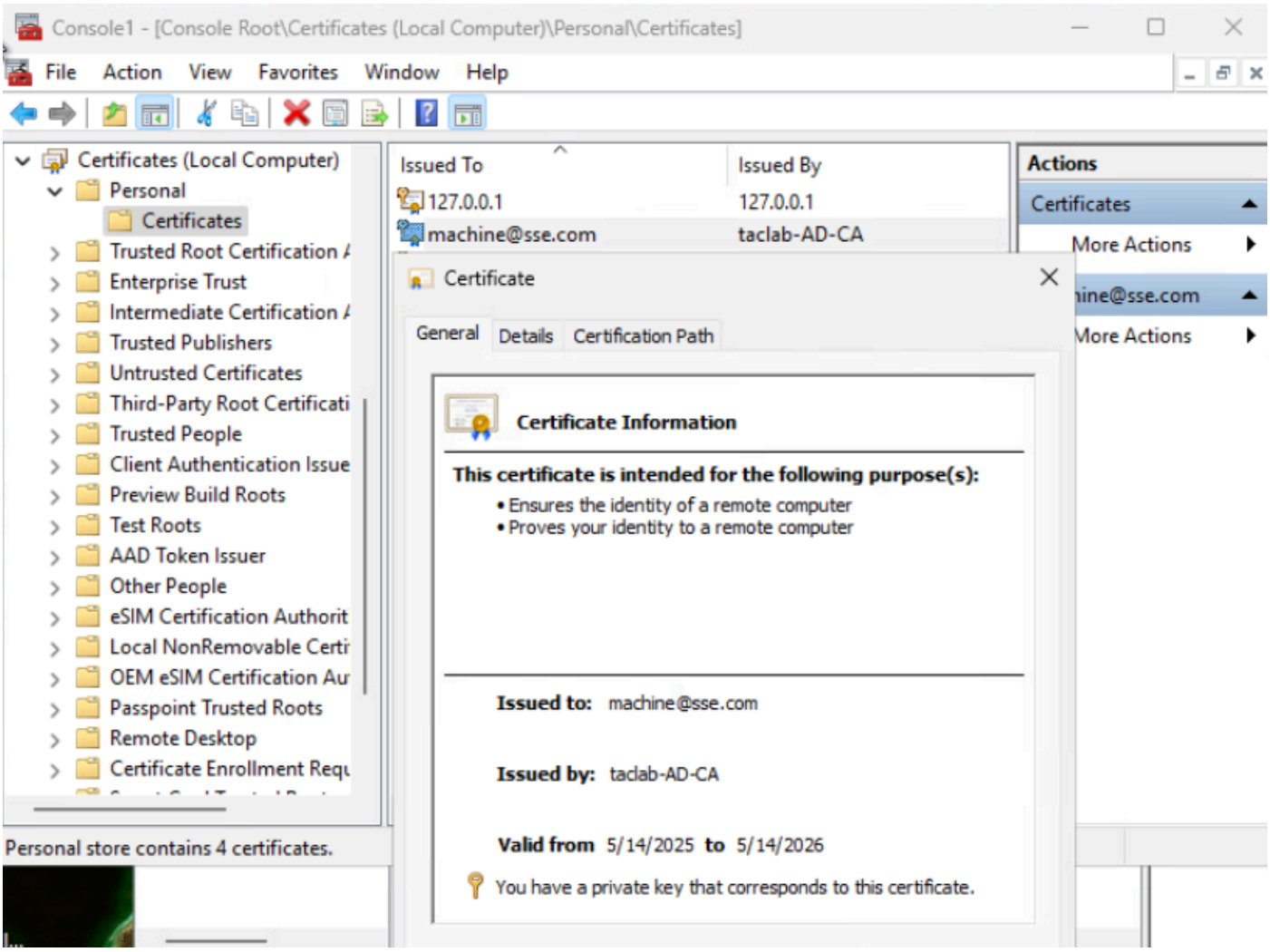
3. Converta o certificado da máquina no formato PKCS12 usando a chave e o certificado gerados nas etapas anteriores (etapa 1 e 2), respectivamente

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#
```

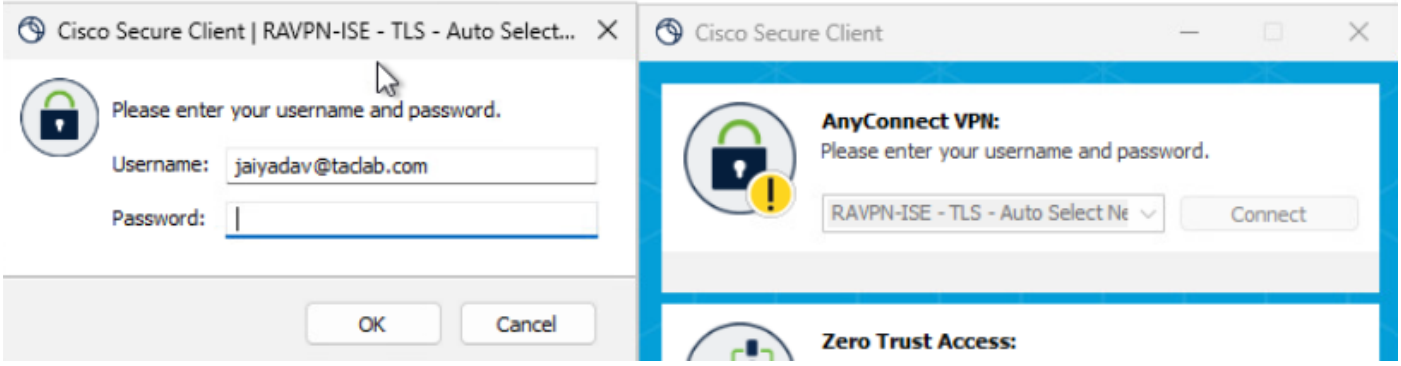
Etapa 7 - Importar o certificado da máquina em uma máquina de teste

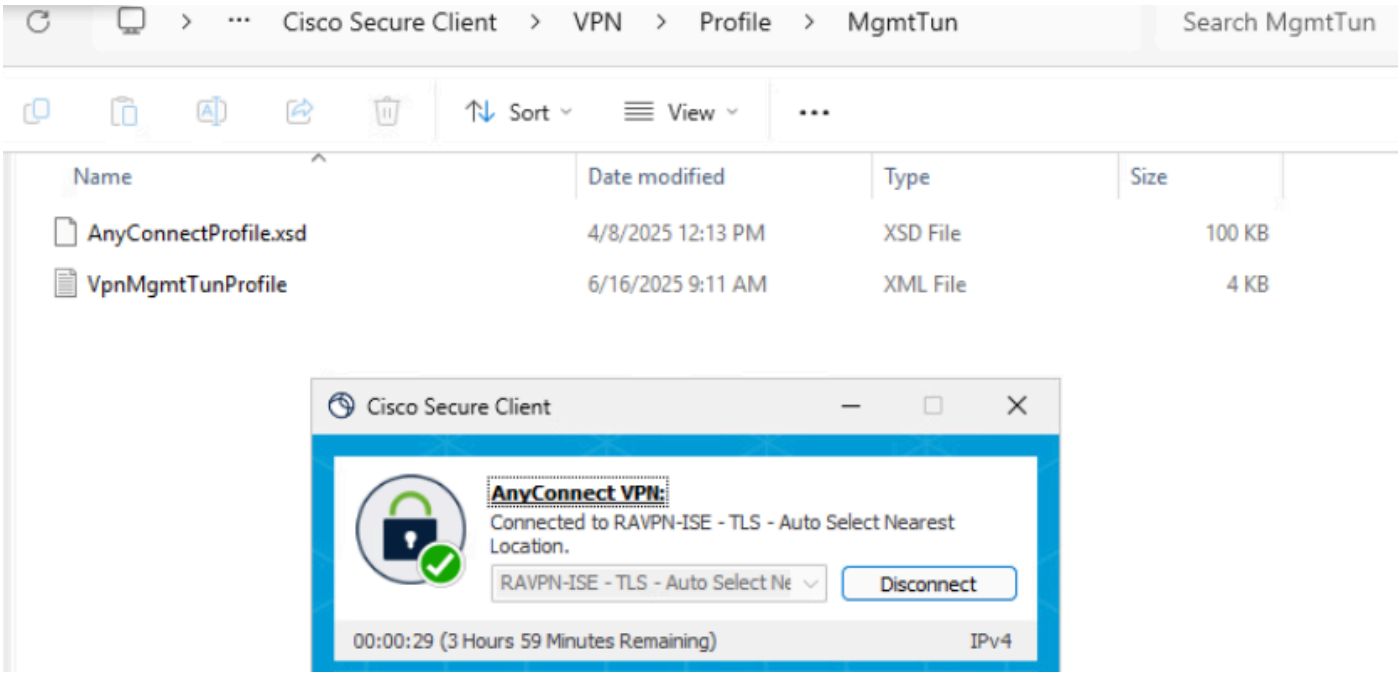
a. Importar o certificado da máquina PKCS12 no armazenamento local ou da máquina



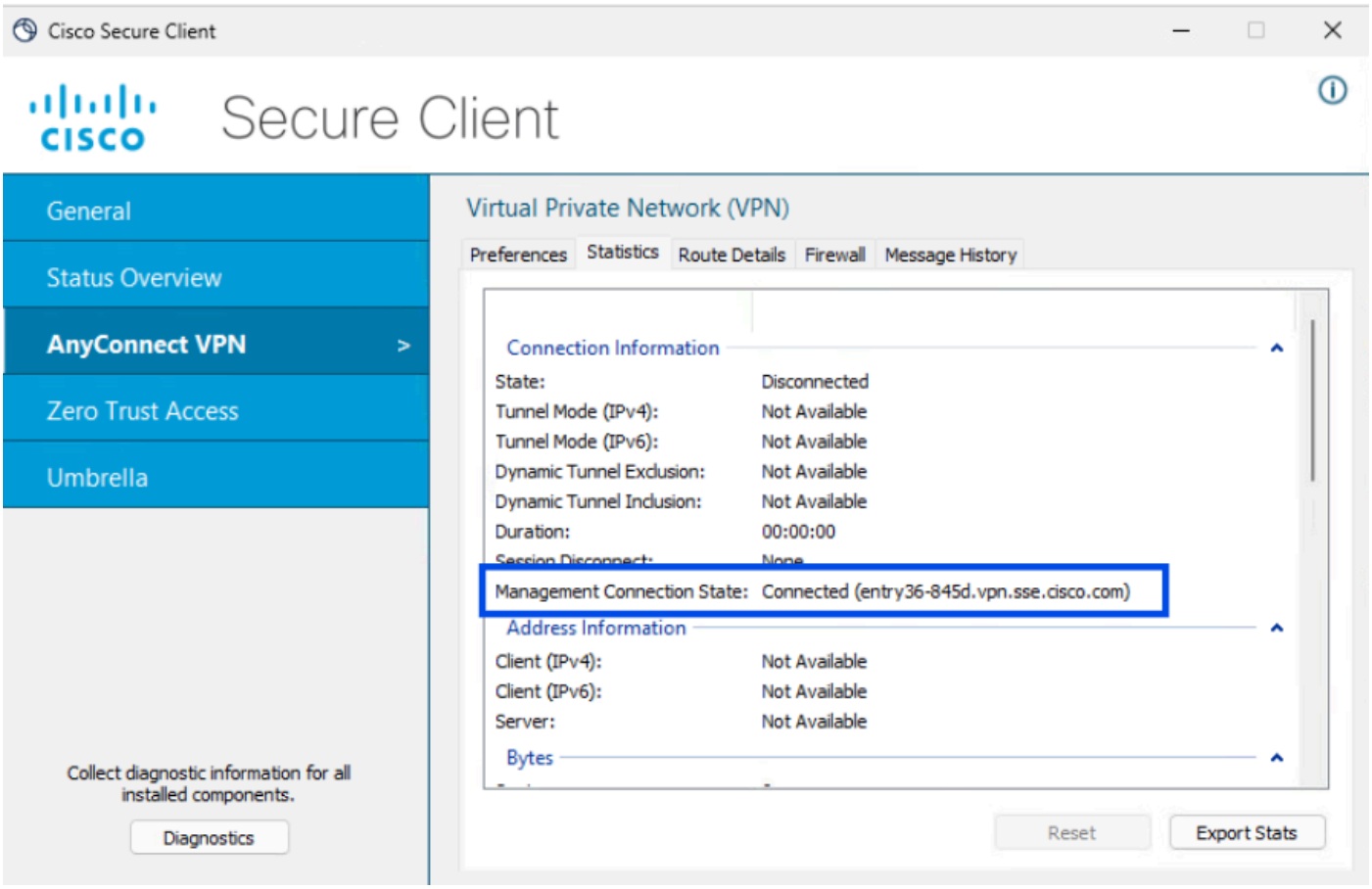
Etapa 8 - Conectar ao túnel da máquina

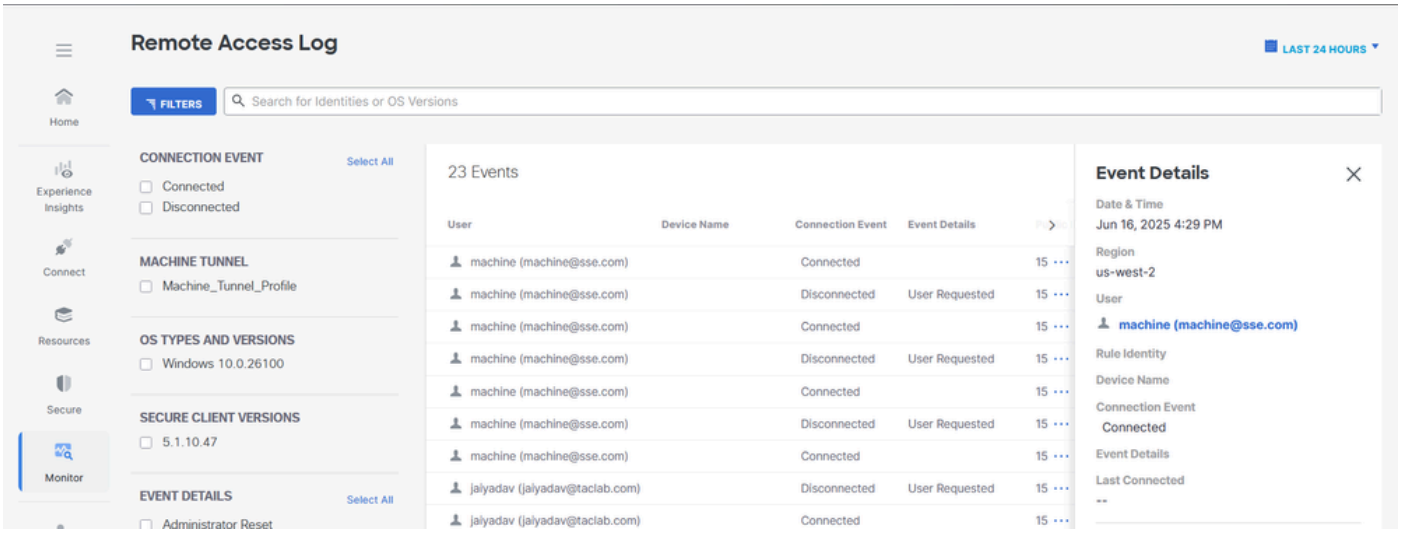
a. Conecte-se a um túnel do usuário , isso aciona o perfil xml da máquina a ser baixado.





b. Verifique a conectividade do túnel da máquina





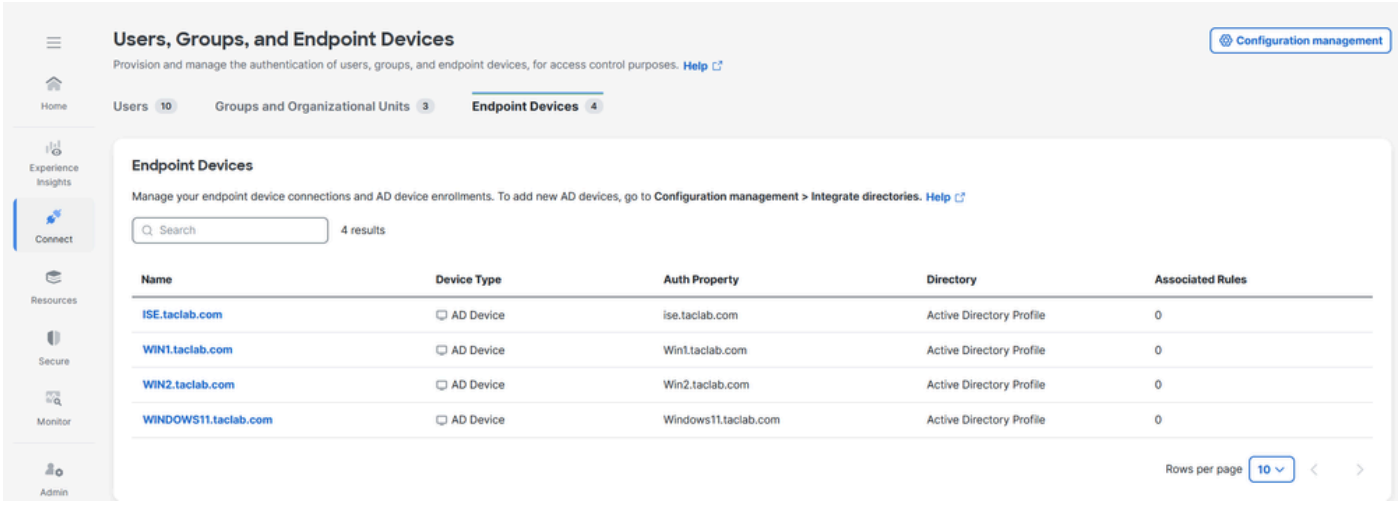
Método 2 - Configurar o túnel da máquina usando o certificado do ponto final

Nesse caso, no campo Primário para autenticação, escolha o campo de certificado que contém o nome do dispositivo (nome do computador). O Secure Access usa o nome do dispositivo como o identificador de túnel da máquina. O formato do nome do computador deve corresponder ao formato do identificador de dispositivo escolhido

Siga as etapas de 1 a 4 para a configuração do túnel da máquina

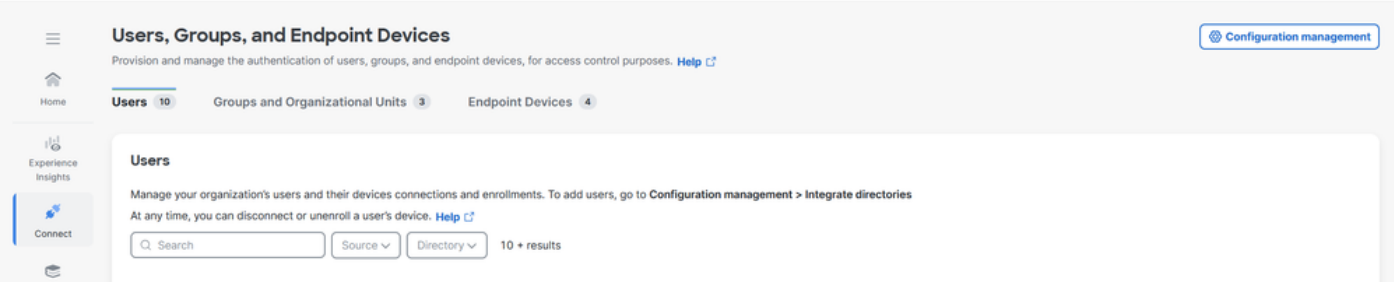
Etapa 5 - Configurar o conector AD para poder importar endpoints no Cisco Secure Access .

Para obter mais informações, consulte Integração do Ative Diretory no local

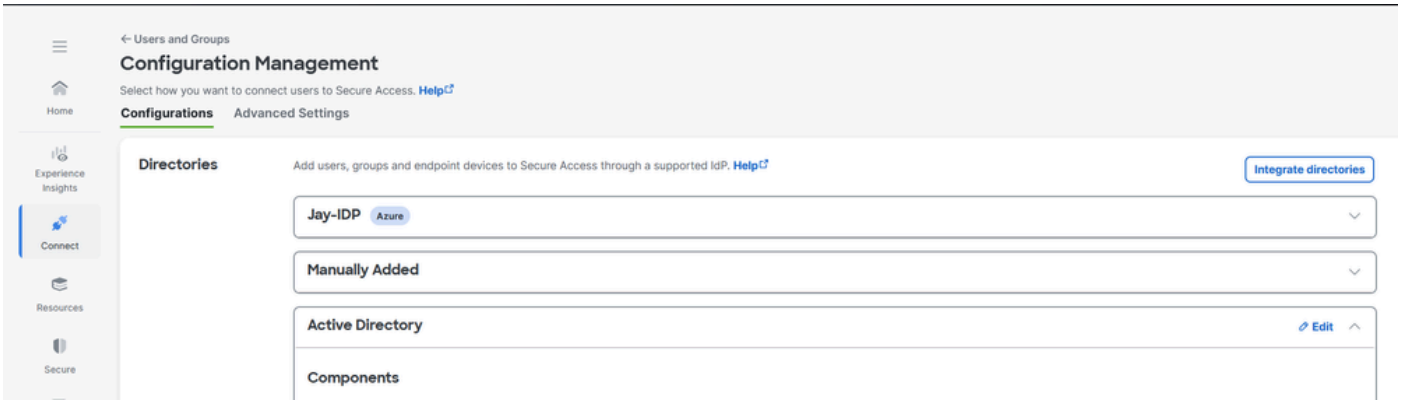


Etapa 6 - Configurar a autenticação dos dispositivos de endpoint

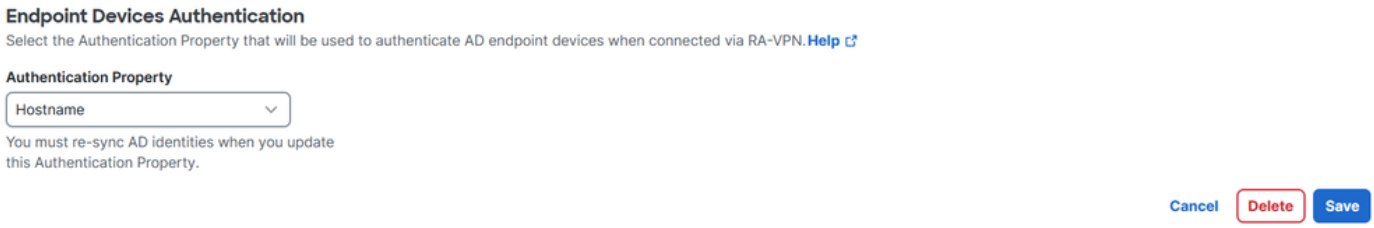
1. Navegue até Connect > Users,Groups and Endpoint Devices.
2. Clique em Gerenciamento de configuração



3. Em Configurações, edite o Ative Diretory



4. Definir a Propriedade de Autenticação de Dispositivos de Ponto Final como Nome de Host



5. Clique em Salvar e reinicie os serviços do AD Connector nos servidores em que o AD Connector está instalado

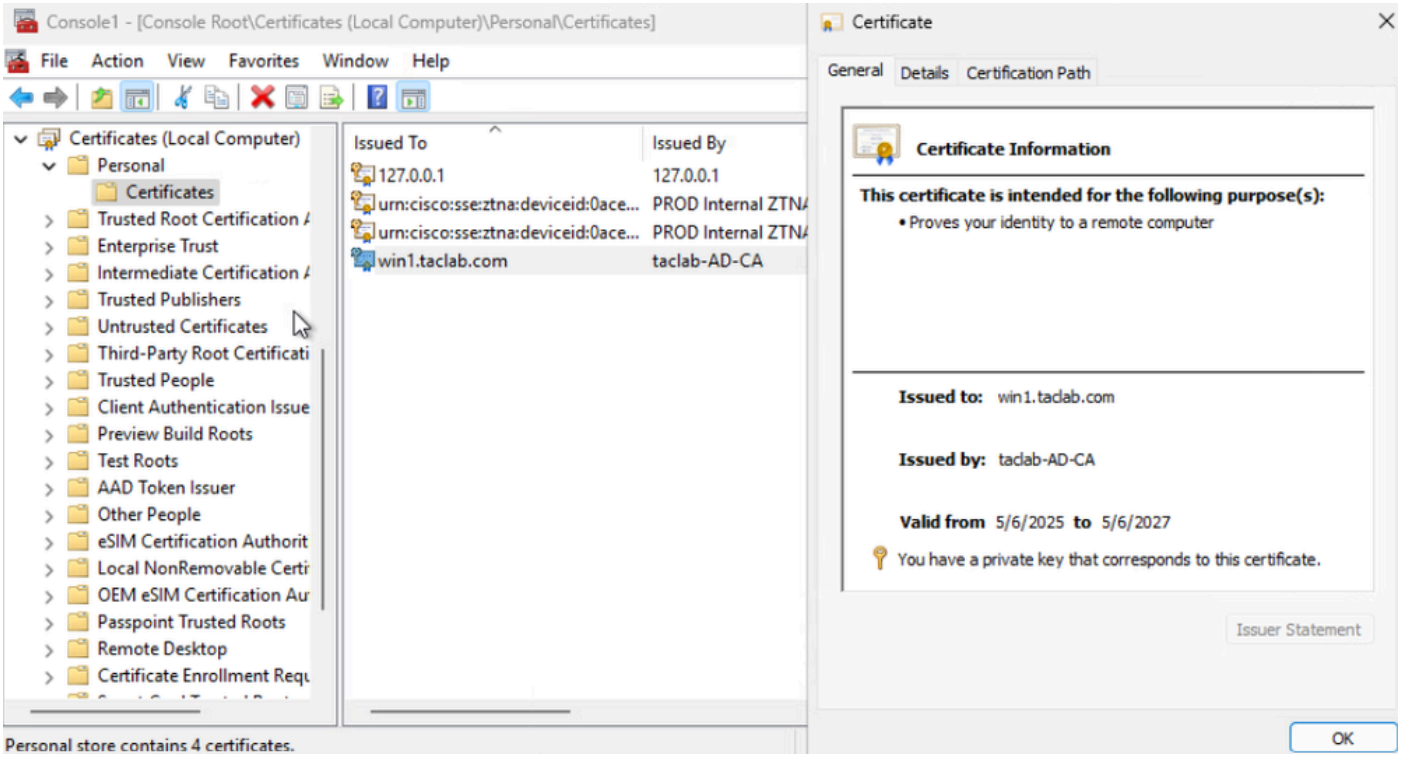
Etapa 7 - Gerar e Importar Certificado de Endpoint

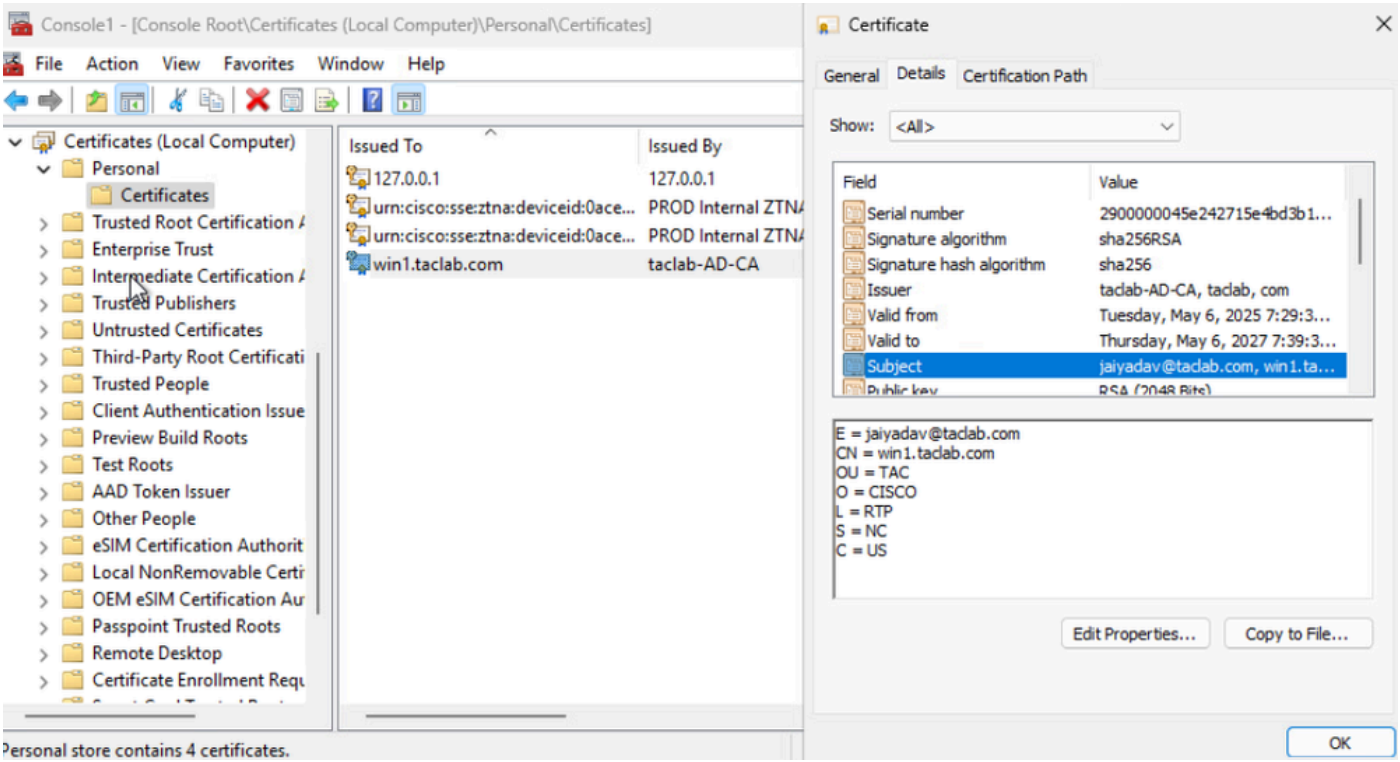
a. Gerar CSR , abrir um gerador de CSR ou ferramenta OpenSSL

b. Gerar um certificado de ponto de extremidade da autoridade de certificação

c. Converta o arquivo .cert no formato PKCS12

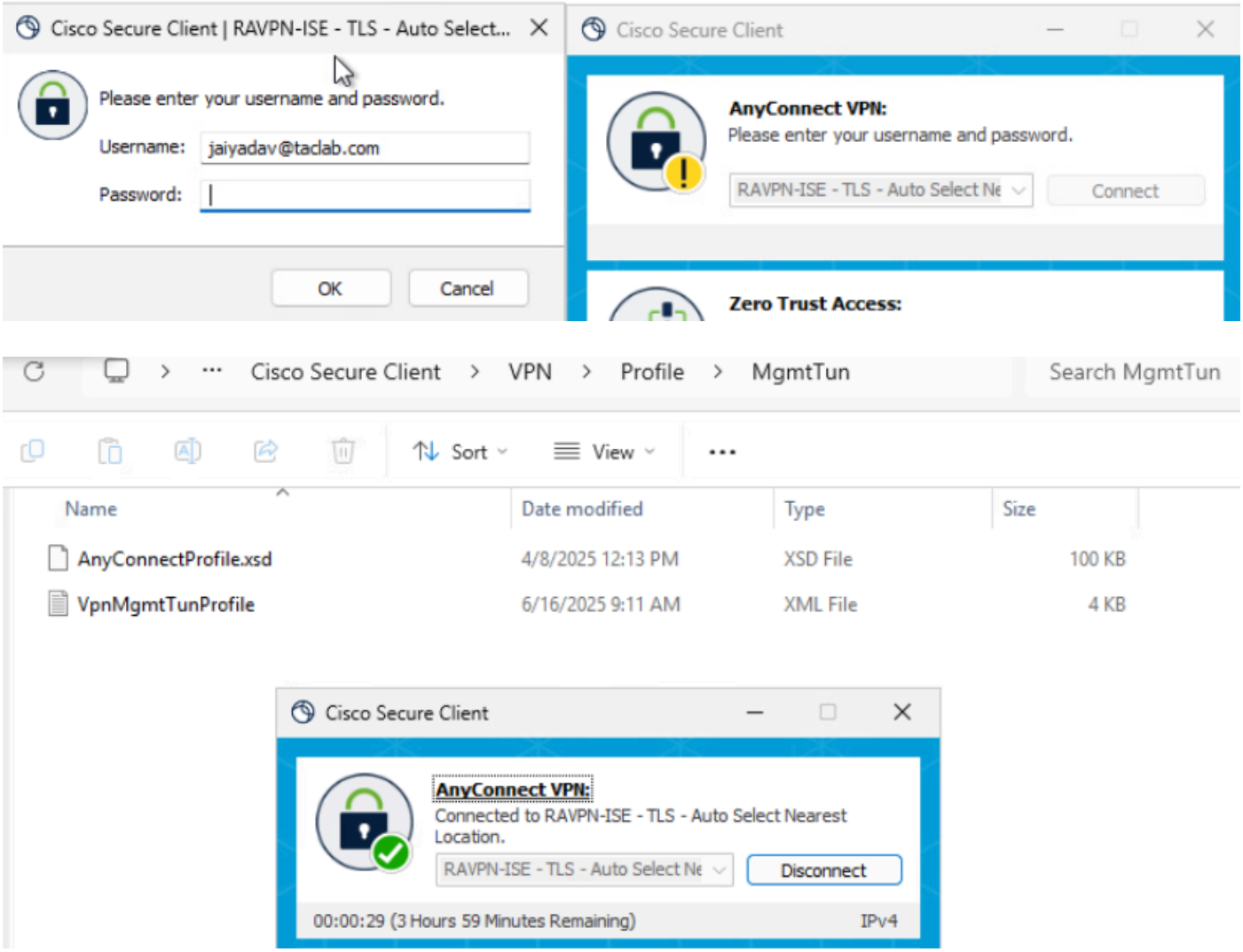
d. Importar o certificado PKCS12 no repositório de certificados do ponto de extremidade



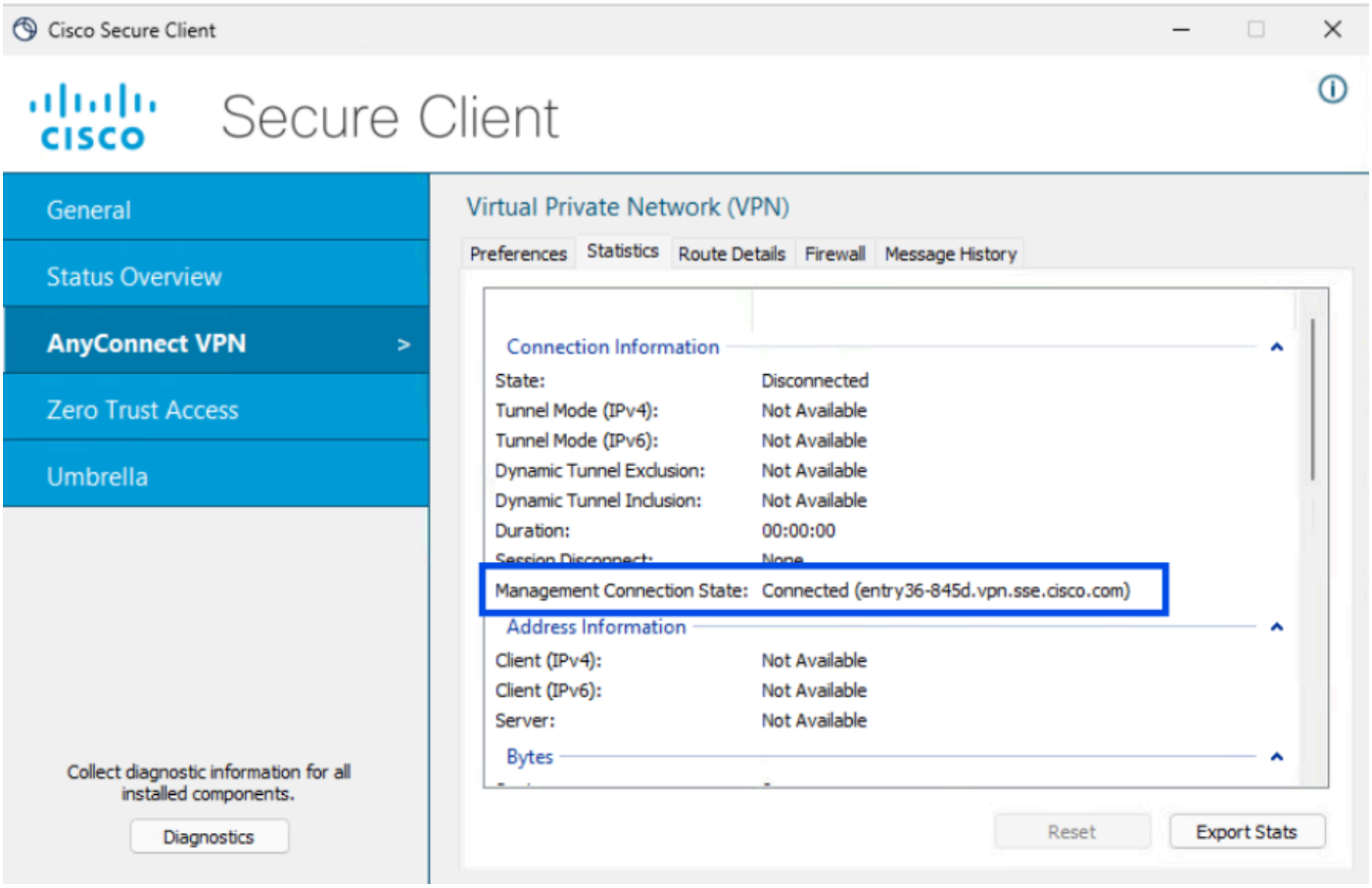


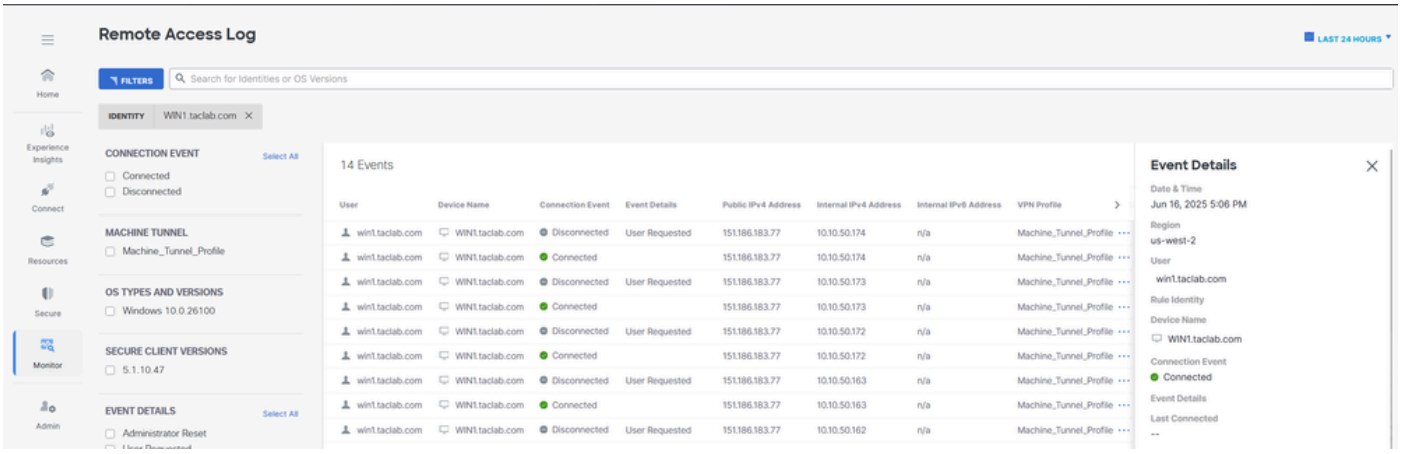
Etapa 8 - Conectar ao túnel da máquina

a. Connect to a User Tunnel , ele aciona o download do perfil xml do túnel da máquina



b. Verifique a conectividade do túnel da máquina





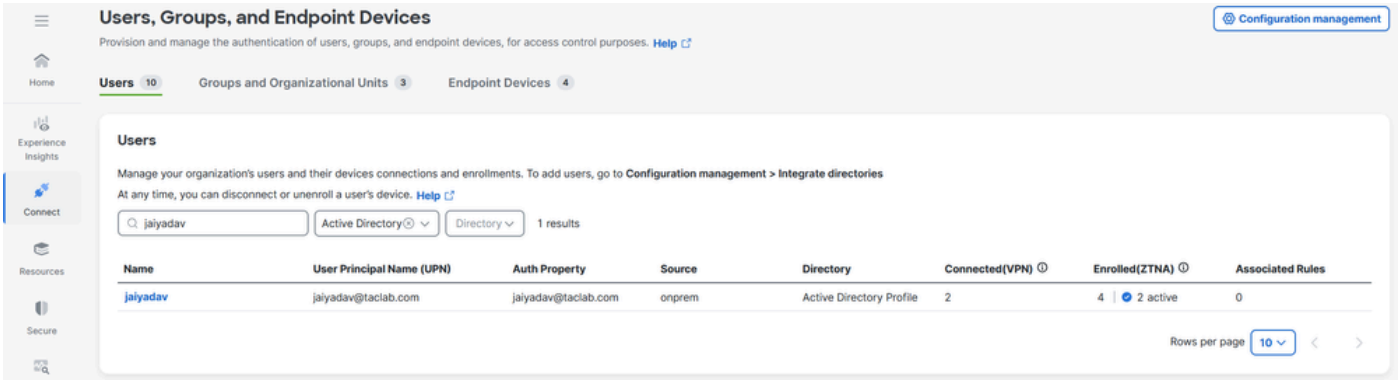
Método 3 - Configurar o túnel da máquina usando o certificado do usuário

Nesse caso, no campo Primário para autenticação, escolha o campo de certificado que contém o email do usuário ou UPN. O Secure Access usa o e-mail ou UPN como o identificador de túnel da máquina. O formato do email ou UPN deve corresponder ao formato do identificador de dispositivo escolhido

Siga as etapas de 1 a 4 para a configuração do túnel da máquina

Etapa 5 - Configurar o conector AD para poder importar usuários no Cisco Secure Access .

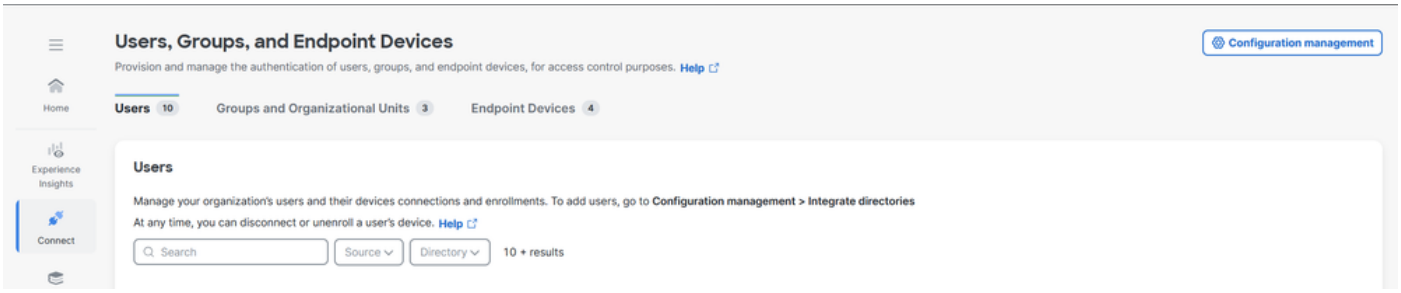
Para obter mais informações, consulte Integração do Ative Diretory no local



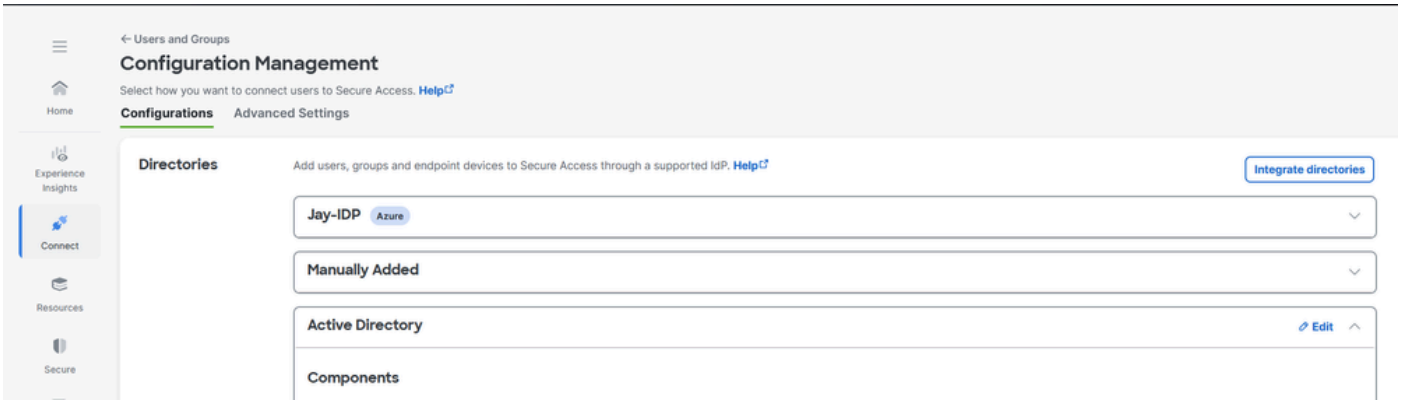
Etapa 6 - Configurar a autenticação de usuários

1. Navegue até Connect > Users,Groups and Endpoint Devices.

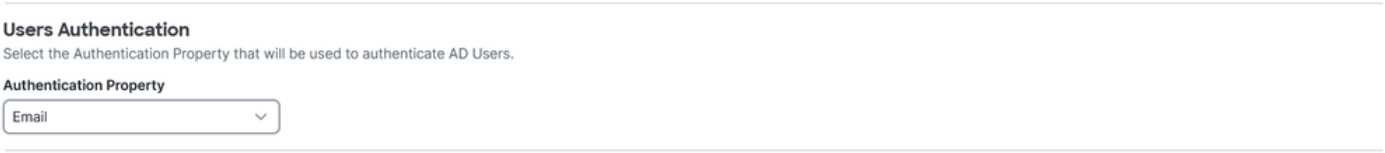
2. Clique em Gerenciamento de configuração



3. Em Configurações, edite o Ative Diretory



4. Definir Propriedade de Autenticação de Usuários como Email



5. Clique em Salvar e reinicie os serviços do AD Connector nos servidores em que o AD Connector está instalado

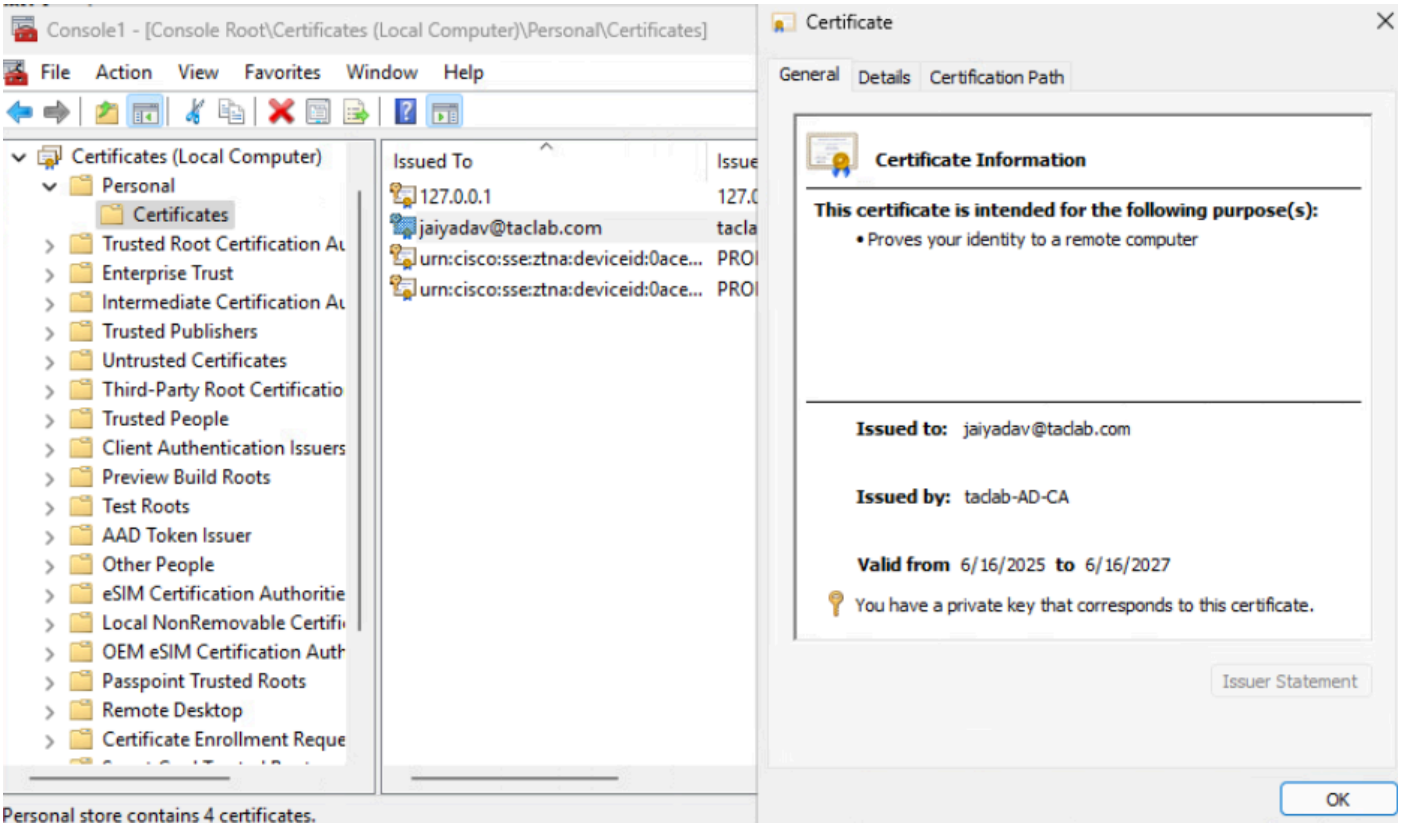
Etapa 7 - Gerar e Importar Certificado de Endpoint

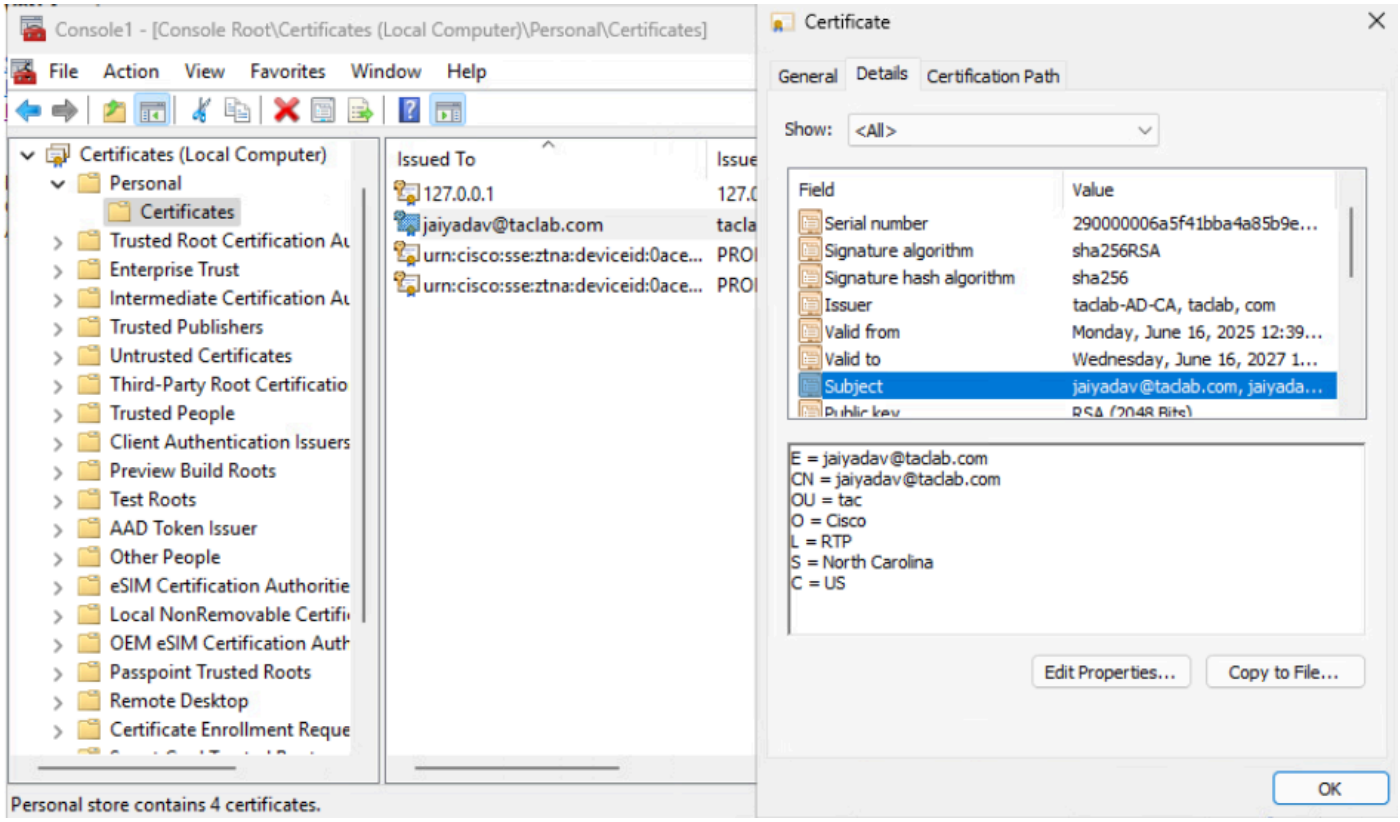
a. Gerar CSR , abrir um gerador de CSR ou ferramenta OpenSSL

b. Gerar um certificado de ponto de extremidade da autoridade de certificação

c. Converta o arquivo .cert no formato PKCS12

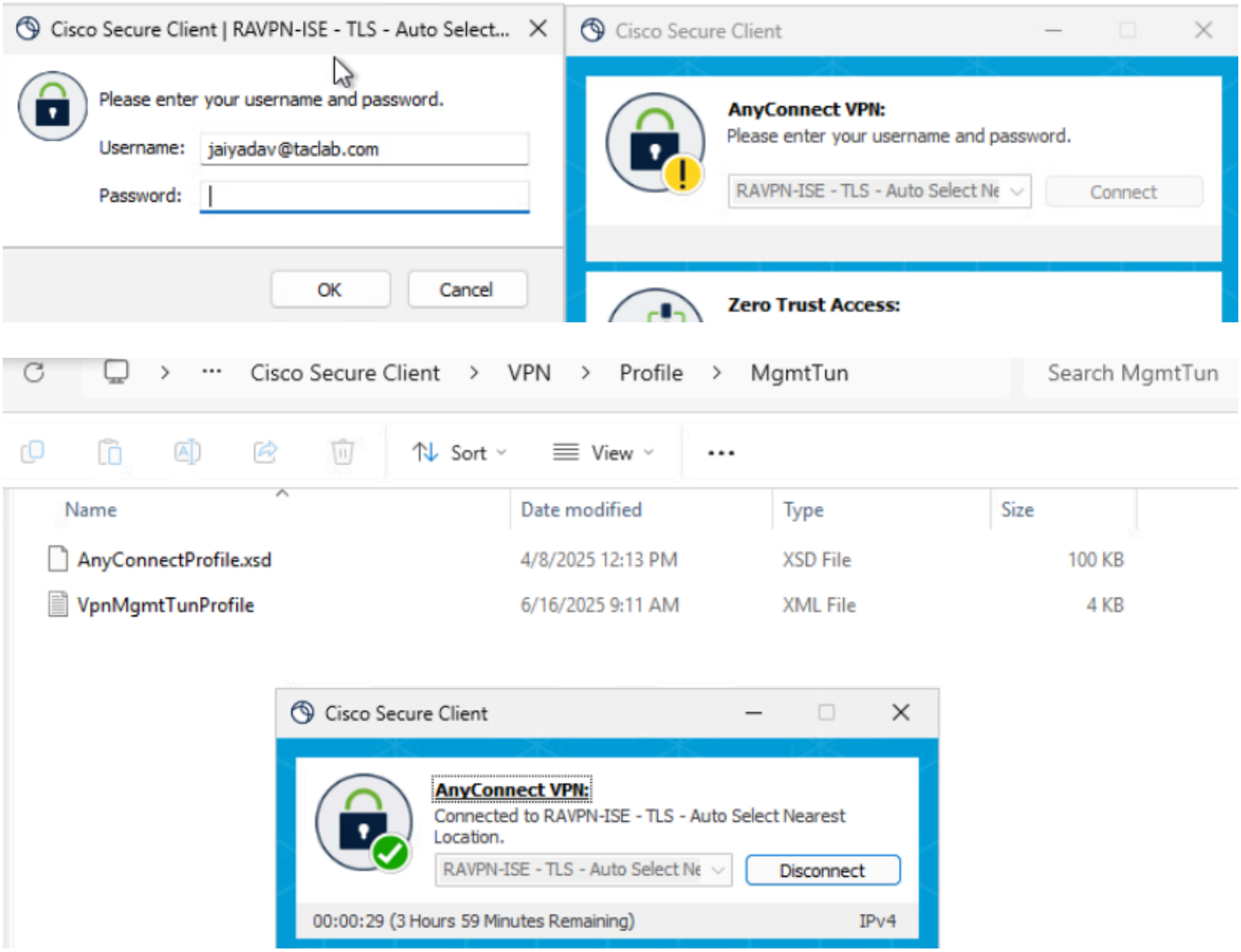
d. Importar o certificado PKCS12 no repositório de certificados do ponto de extremidade



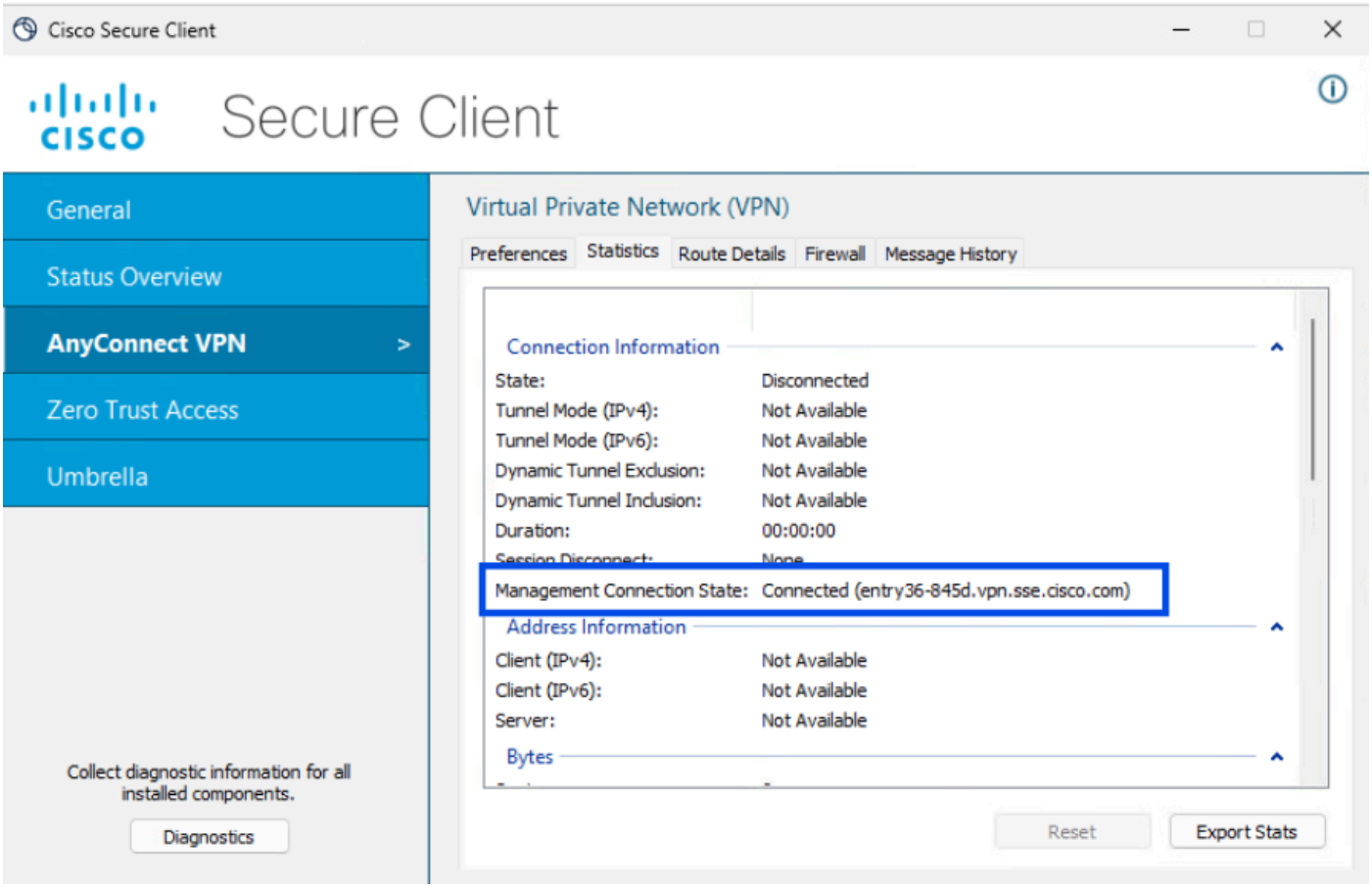


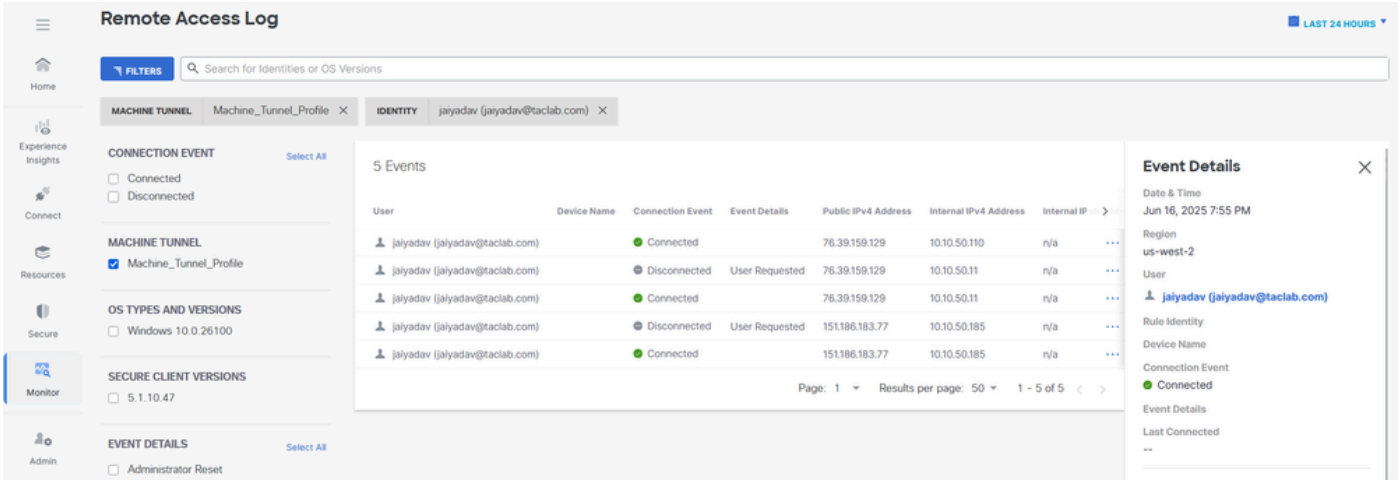
Etapa 8 - Conectar ao túnel da máquina

a. Connect to a User Tunnel , ele aciona o download do perfil xml do túnel da máquina



b. Verifique a conectividade do túnel da máquina





Troubleshooting

Extraia o pacote DART, abra os logs do AnyConnectVPN e analise as mensagens de erro

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.