在Cisco安全访问上配置计算机隧道

目录

简介

网络图

先决条件

- 要求
- 使用的组件

背景信息

- 使用机器隧道

限制

配置

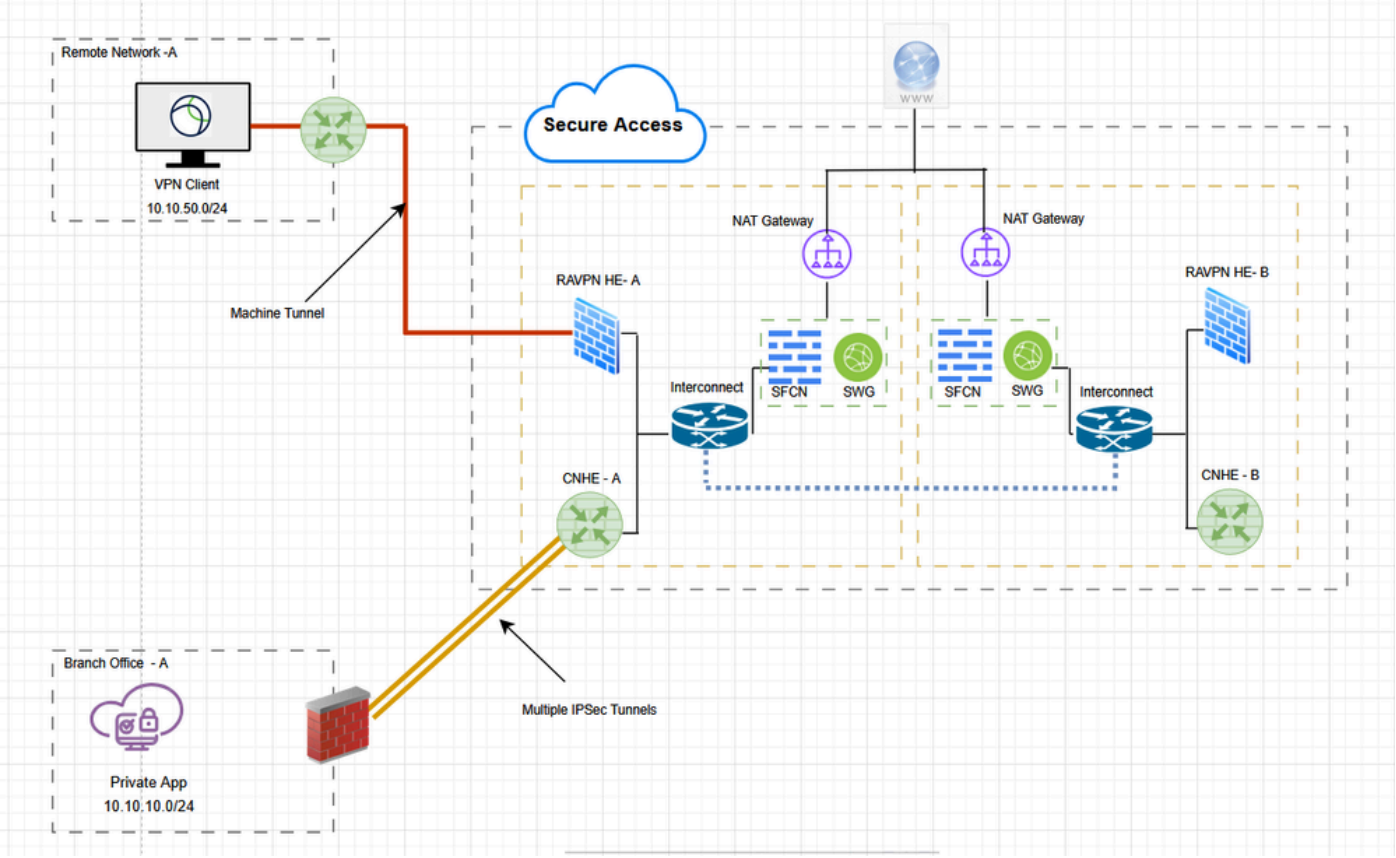
- 方法1 — 使用用户machine@sse.com配置计算机隧道
- 步骤1 — 常规设置
- 第2步 — 计算机证书的身份验证
- 第3步 — 流量引导（分割隧道）
- 第4步 — 思科安全客户端配置
- 第5步 — 验证machine@sse.comuser是否存在于思科安全访问中
- 第6步 — 为machine@sse.com生成CA签名的证书
- 第7步 — 在测试计算机上导入计算机证书
- 步骤8 — 连接到机器隧道
- 方法2 — 使用终端证书配置计算机隧道
- 第5步 — 配置AD连接器以便能够在Cisco Secure Access上导入终端。
- 第6步 — 配置终端设备身份验证
- 第7步 — 生成和导入终端证书
- 步骤8 — 连接到机器隧道
- 方法3 — 使用用户证书配置计算机隧道
- 第5步 — 配置AD连接器以便能够在Cisco Secure Access上导入用户。
- 第6步 — 配置用户身份验证
- 第7步 — 生成和导入终端证书
- 步骤8 — 连接到机器隧道

故障排除

简介

本文档介绍如何将安全访问配置为VPN网关并接受通过VPN机器隧道从安全客户端进行的连接。

网络图



先决条件

- 安全访问中的完全管理员角色。
- 思科安全访问上至少配置了一个用户VPN配置文件
- 思科安全访问上的用户IP池

要求

建议您了解以下主题：

- 509个证书
- OpenSSL

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全访问
- 思科安全客户端5.1.10
- Windows 11
- Windows Server 2019 - CA

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

只要客户端系统通电，安全访问VPN机器隧道即可确保与企业网络的连接，而不仅仅是在最终用户建立VPN连接时。您可以在办公室外终端（尤其是用户通过VPN不经常连接到办公室网络的设备）上执行补丁管理。需要企业网络连接的终端OS登录脚本也受益于此功能。对于要在无用户交互的情况下创建此隧道，将使用基于证书的身份验证。

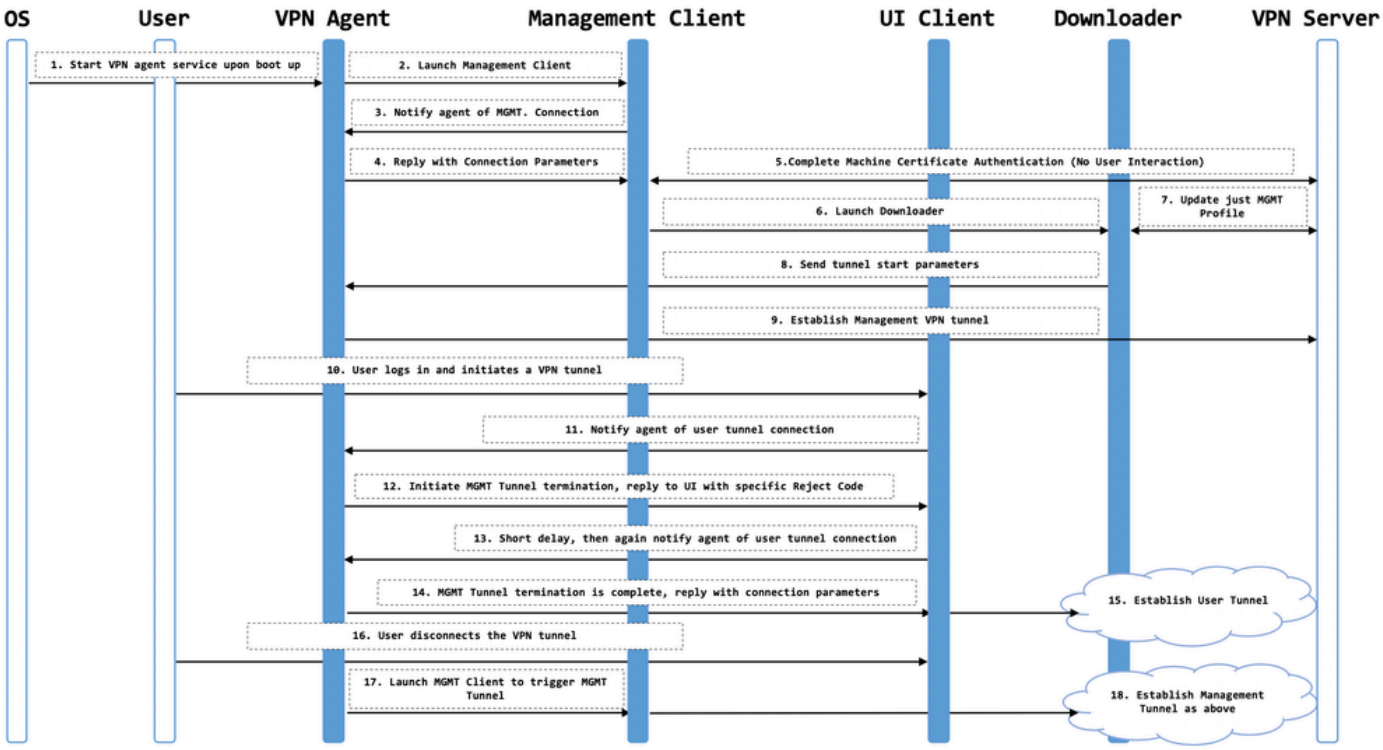
通过安全访问计算机隧道，管理员可以在用户登录之前连接Cisco安全客户端，而无需用户干预。当终端位于外部并与用户发起的VPN断开连接时，会触发安全访问计算机隧道。安全访问VPN机器隧道对最终用户是透明的，在用户启动VPN时自动断开连接。

使用机器隧道

安全客户端VPN代理服务会在系统启动时自动启动。安全客户端VPN代理使用VPN配置文件检测是否启用了计算机隧道功能。如果启用了计算机隧道功能，代理将启动管理客户端应用以启动计算机隧道连接。管理客户端应用使用VPN配置文件中的主机条目发起连接。然后VPN隧道按常规建立，只有一个例外：在计算机隧道连接期间不会执行软件更新，因为计算机隧道对用户是透明的。

用户通过安全客户端启动VPN隧道，这将触发计算机隧道终止。机器隧道终止后，用户隧道建立会照常继续。

用户断开VPN隧道，从而触发自动重新建立机器隧道。



限制

- 不支持用户交互。
- 仅支持通过计算机证书存储区(Windows)进行的基于证书的身份验证。

- 实施严格的服务器证书检查。
- 不支持私有代理。
- 不支持公共代理（在未从浏览器检索本地代理设置的平台上支持ProxyNative值）。
- 不支持安全客户端自定义脚本

配置

方法1 — 使用用户machine@sse.com配置计算机隧道

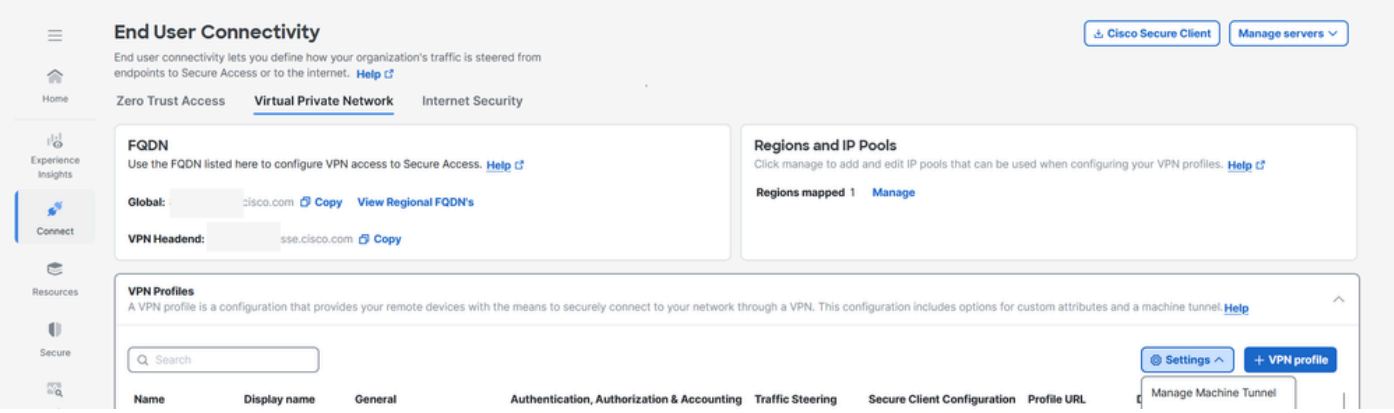
步骤1 — 常规设置

配置常规设置，包括此计算机隧道使用的域和协议。

1.导航到连接>最终用户连接>虚拟专用网络。

2.导航到VPN配置文件并配置计算机隧道的设置。

a.单击Settings，然后从下拉列表中选择Manage Machine Tunnel。

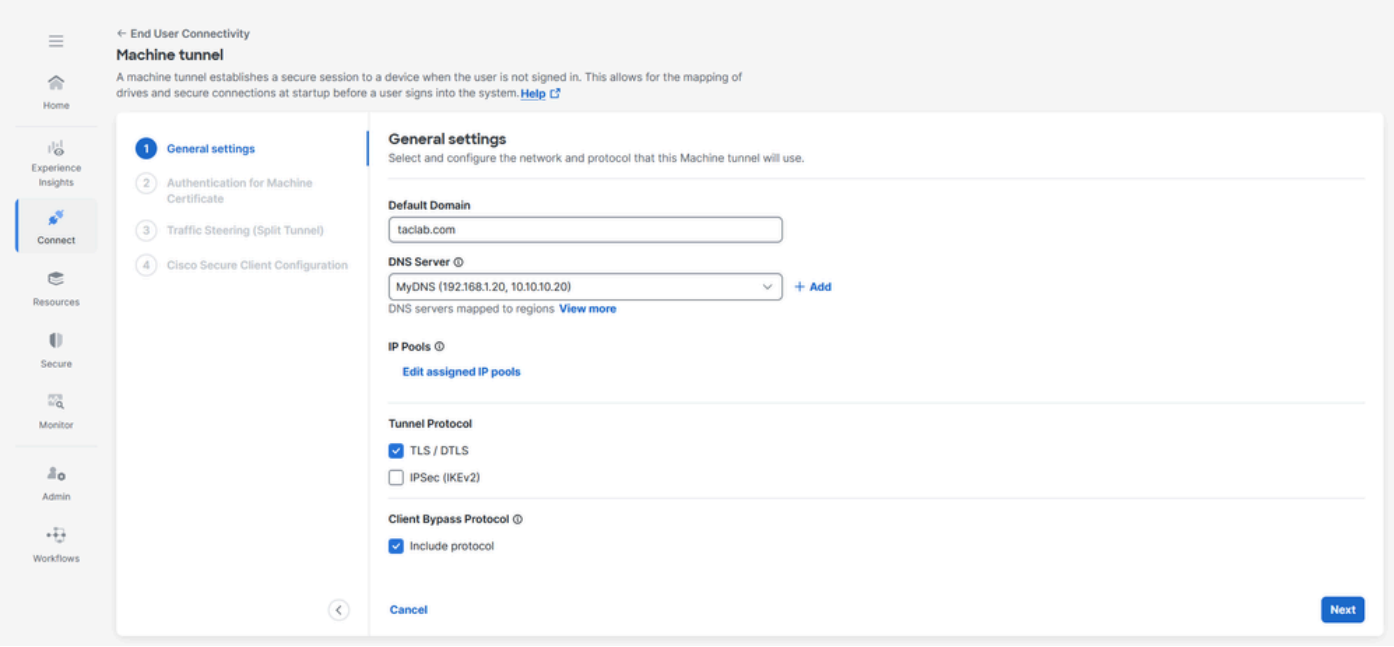


3. 输入Default Domain。
4. 通过Manage Regions and IP Pools页面映射的DNS Server设置为默认服务器。您可以接受默认DNS服务器，从下拉列表中选择其他DNS服务器，或者点击+ Add以添加新的DNS服务器对。选择其他DNS服务器或添加新的DNS服务器会覆盖此默认服务器。
5. 从IP Pools下拉列表中选择每个区域的一个IP池。VPN配置文件必须在每个区域中至少分配一个IP池才能进行有效配置。
6. 选择此计算机隧道使用的隧道协议:
   - TLS/DTLS
   - IPSec(IKEv2)

   必须至少选择一个协议。
7. 或者，选中Include protocol以实施客户端旁路协议。

   a.如果为IP协议启用了客户端旁路协议，但未为该协议配置地址池（换句话说，ASA未将该协议的IP地址分配给客户端），则使用该协议的任何IP流量都不会通过VPN隧道发送。它将被发送到隧道外部。

   b.如果禁用了客户端旁路协议，并且没有为该协议配置地址池，则一旦建立VPN隧道，客户端将丢弃该IP协议的所有流量。



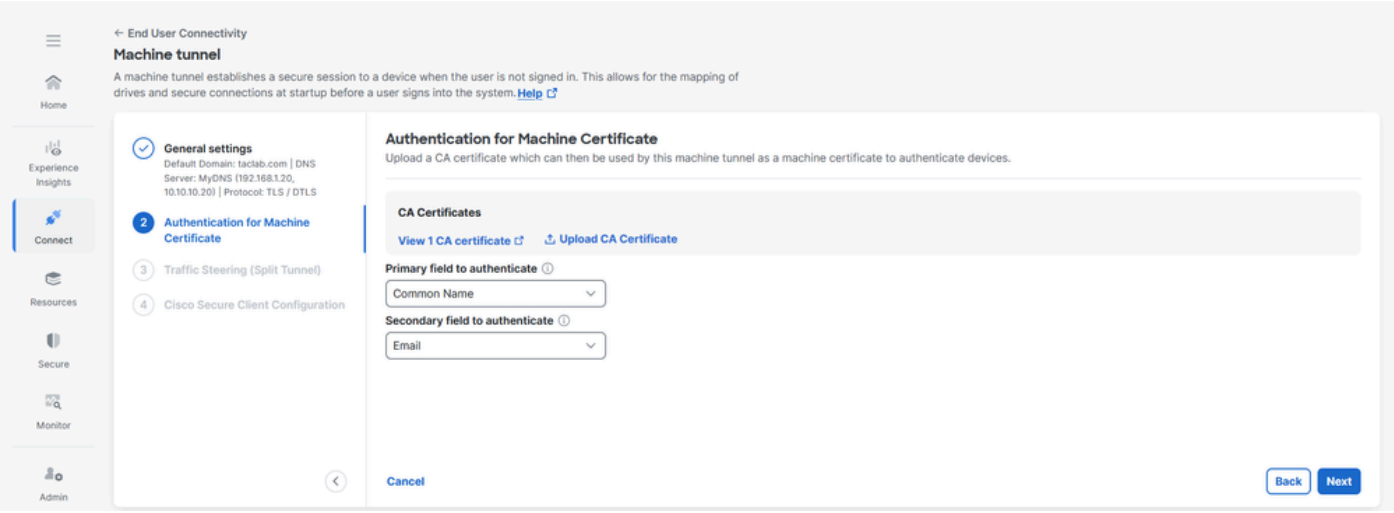
8.单击“下一步”

第2步 — 计算机证书的身份验证

机器隧道对最终用户是透明的，并在用户启动VPN会话时自动断开。对于要在无用户交互的情况下创建此隧道，将使用基于证书的身份验证。

1. 从列表中选择CA证书或点击上传CA证书(Upload CA certificates)

2.选择基于证书的身份验证字段。有关详细信息，请参阅基于证书的身份验证字段



3.单击“下一步”

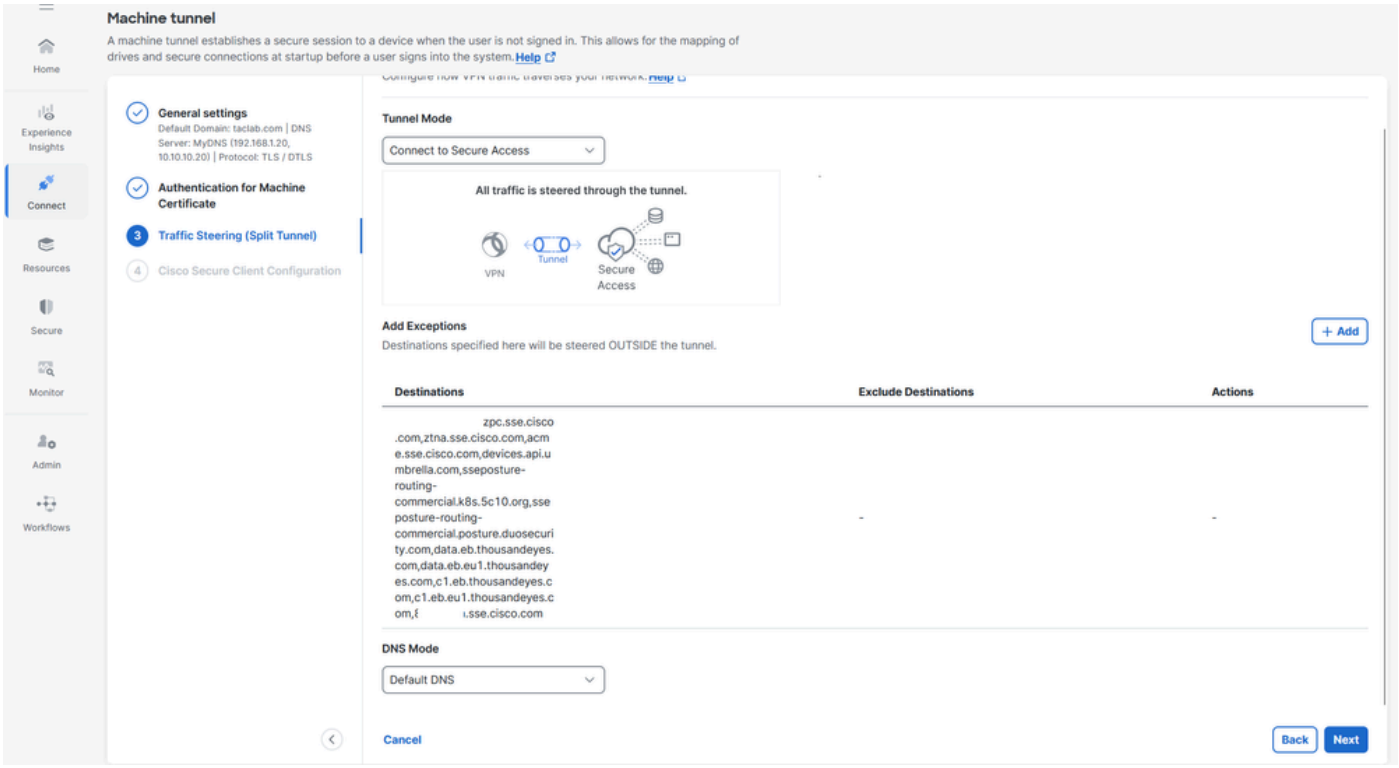
第3步 — 流量引导（分割隧道）

对于Traffic Steering(Split Tunnel)，您可以配置机器隧道以维护与Secure Access的完整隧道连接，或将其配置为仅在必要时使用拆分隧道连接来引导流量通过VPN。有关详细信息，请参阅 Machine Tunnel traffic steering

1.选择隧道模式

2.根据隧道模式选择，您可以添加例外

3.选择DNS模式

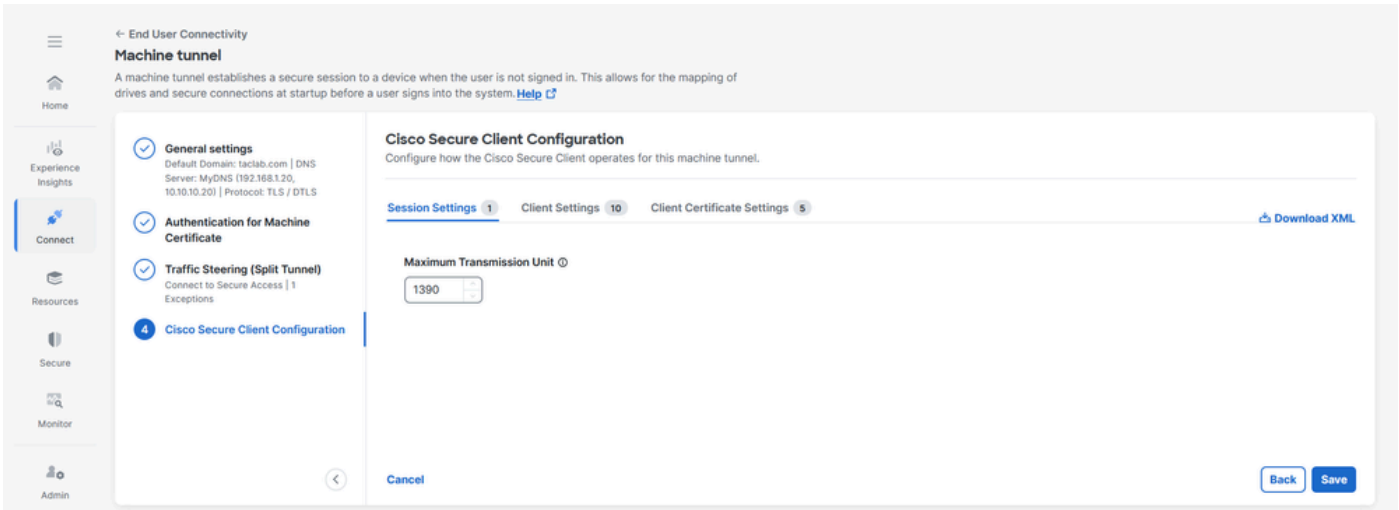


4.单击“下一步”

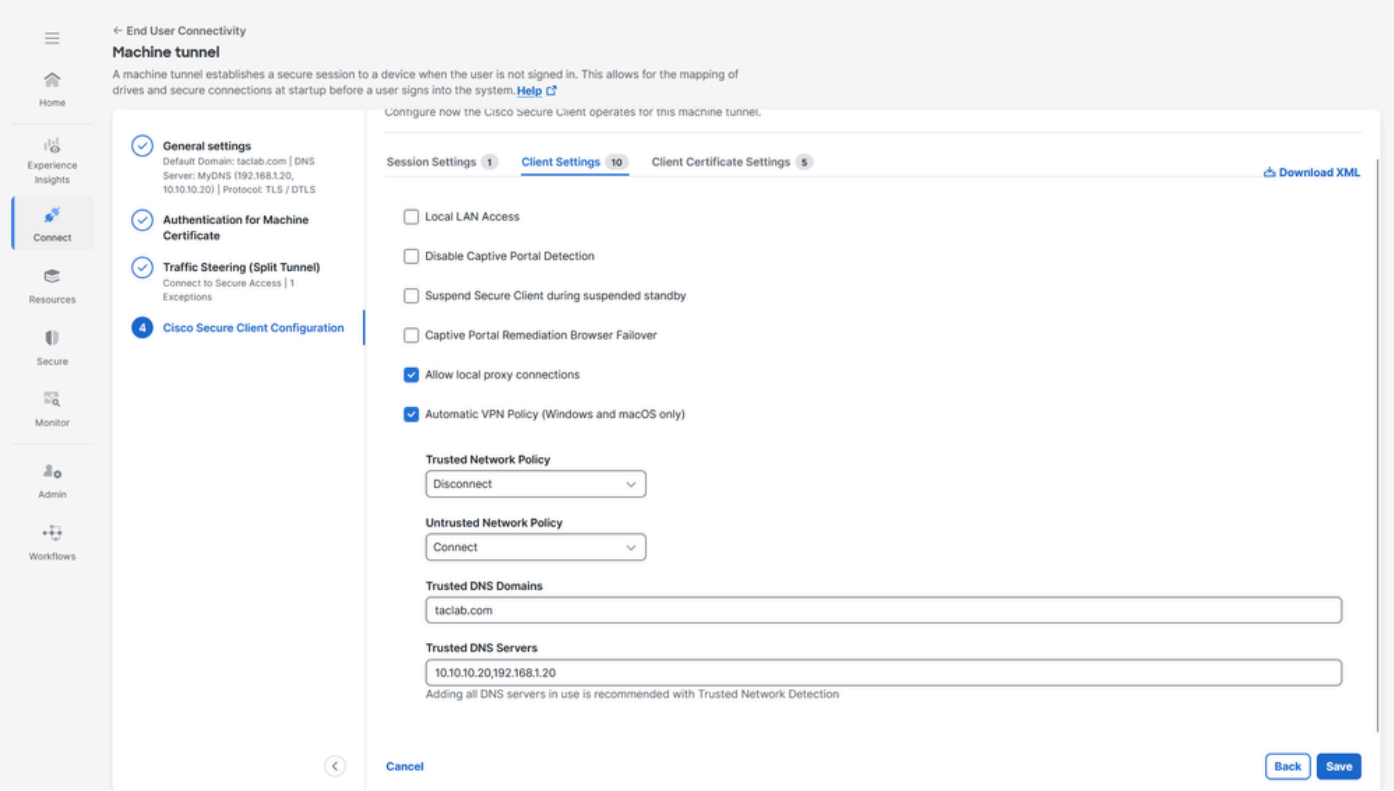
第4步 — 思科安全客户端配置

您可以根据特定VPN计算机隧道的需求修改Cisco安全客户端设置子集。有关详细信息，请参阅[安全客户端配置]

1.验证最大传输单元，这是数据包在不分段的情况下可在VPN隧道中发送的最大大小



2. 客户端设置，有关详细信息，请参阅[计算机隧道客户端设置]



3.客户端证书设置，相应地选择选项

a. Windows Certificate Store Override — 允许管理员指示安全客户端使用Windows计算机（本地系统）证书存储中的证书进行客户端证书身份验证。

b.自动证书选择 — 在安全网关上配置多个证书身份验证时

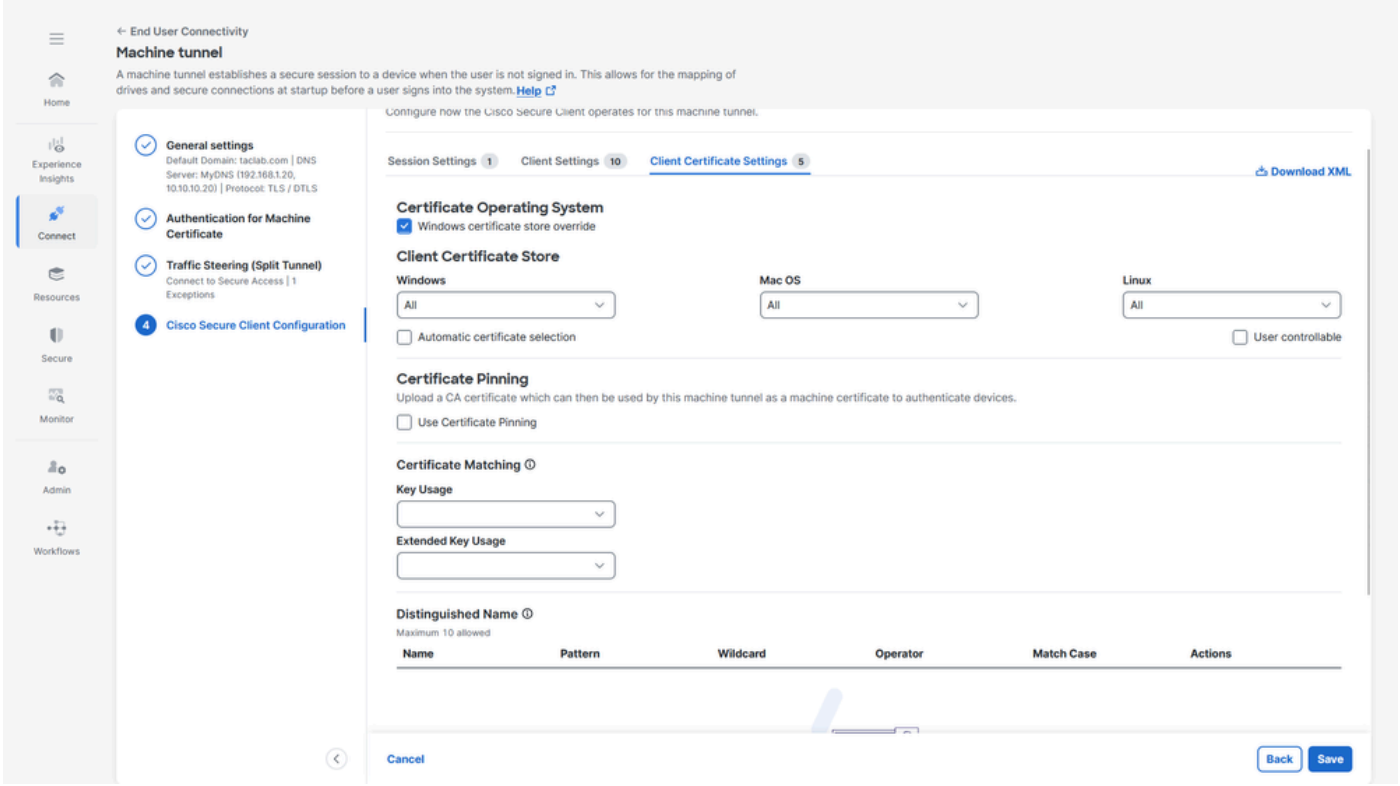
c.证书固定 — 计算机隧道可用作设备身份验证的机器证书的CA证书

d.证书匹配 — 如果未指定证书匹配条件，Cisco安全客户端将应用证书匹配规则

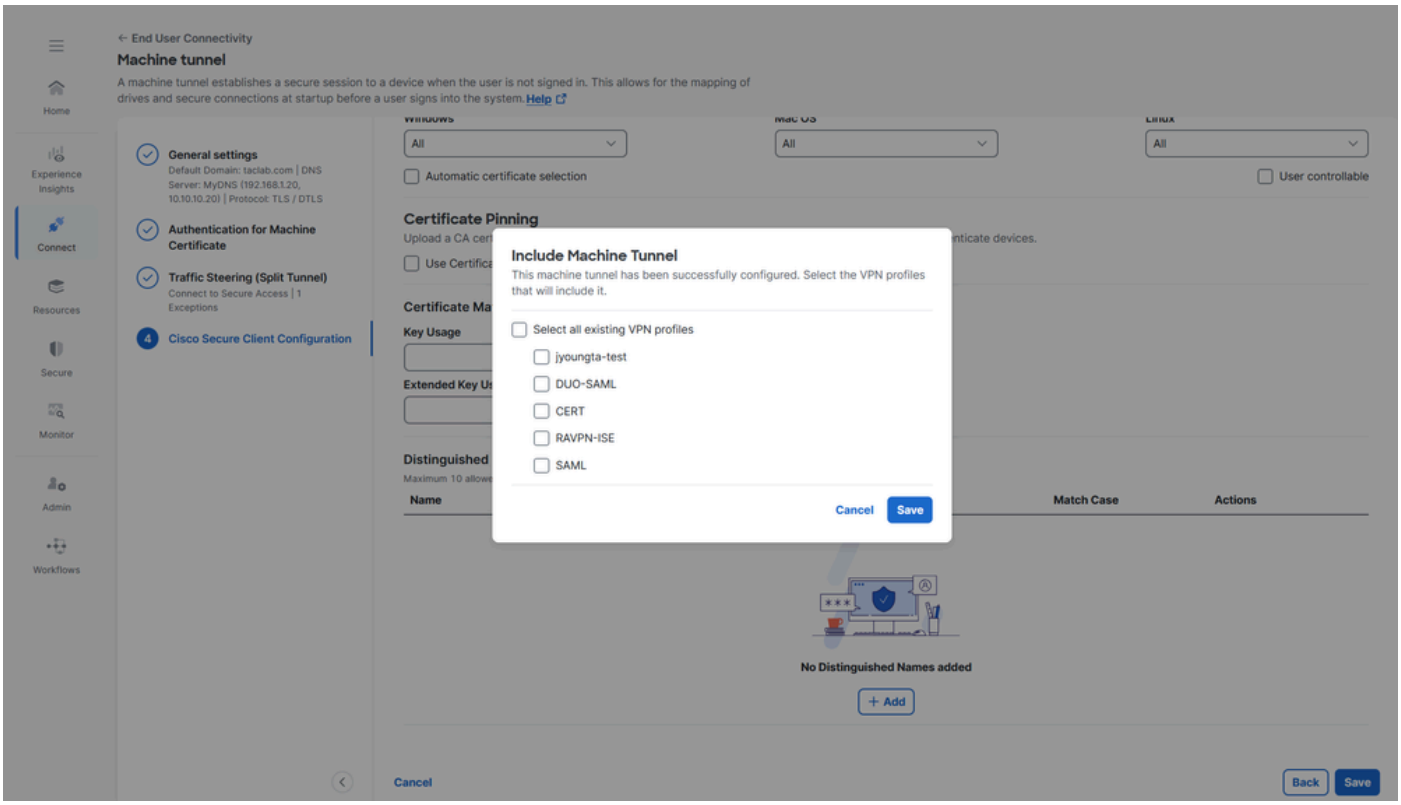
i.密钥用法： 数字签名

二、扩展密钥用法：客户端身份验证

e.Distinguished Name — 在选择可接受的客户端证书时指定完全匹配条件的可分辨名称(DN)。添加多个可分辨名称时，会根据所有条目检查每个证书，并且所有条目必须匹配。

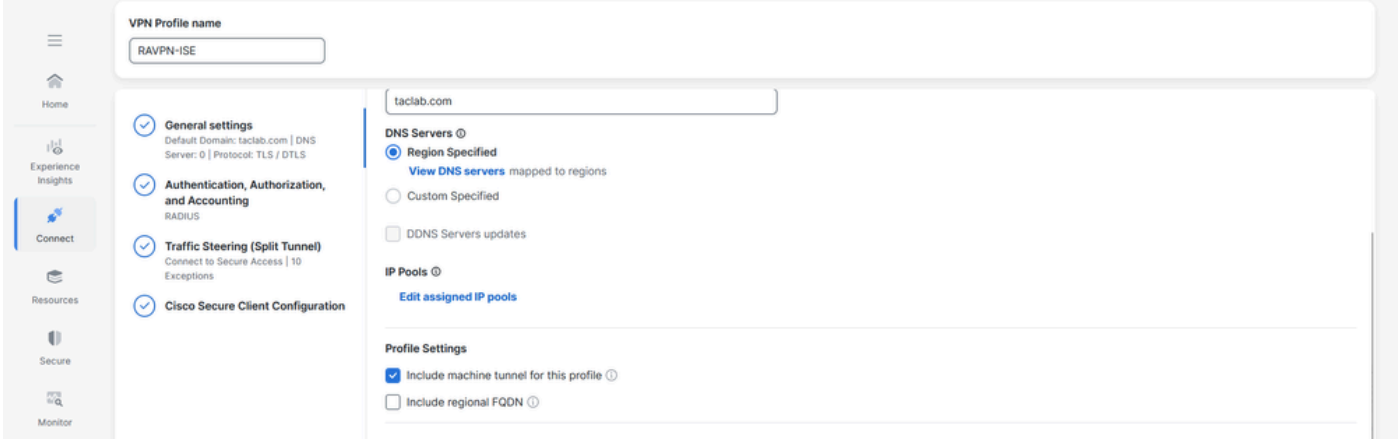


4.将计算机隧道配置文件分配给用户VPN配置文件，单击Save，然后选择用户VPN配置文件



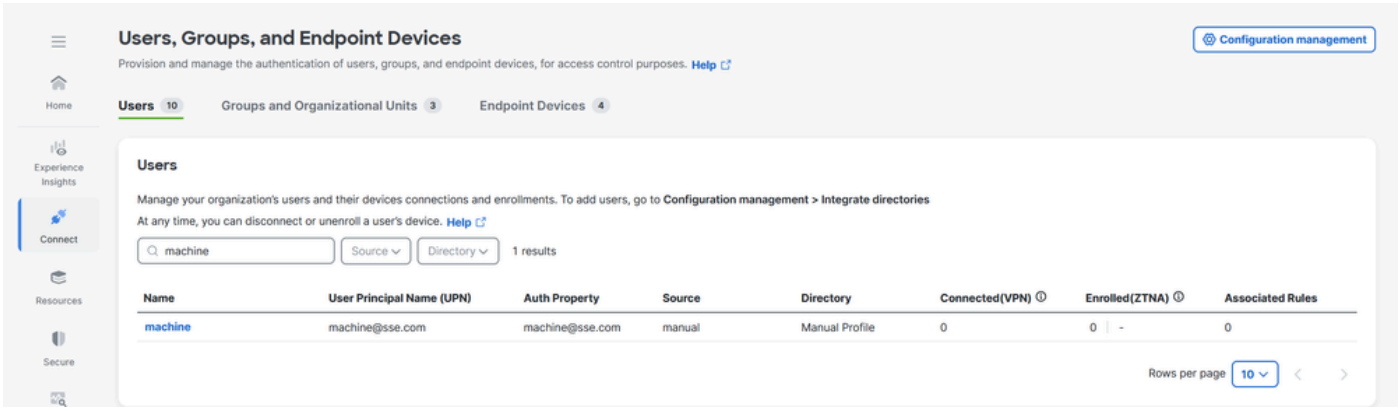
5.单击保存

6.验证计算机隧道配置文件是否已连接到用户VPN配置文件



第5步 — 验证machine@sse.com用户是否存在于思科安全访问中

1.导航到连接>用户、组和终端设备>用户



2. 如果machine@sse.com用户未手动显示导入。有关详细信息，请参阅手动导入用户和组

第6步 — 为machine@sse.com生成CA签名证书

1.生成证书签名请求

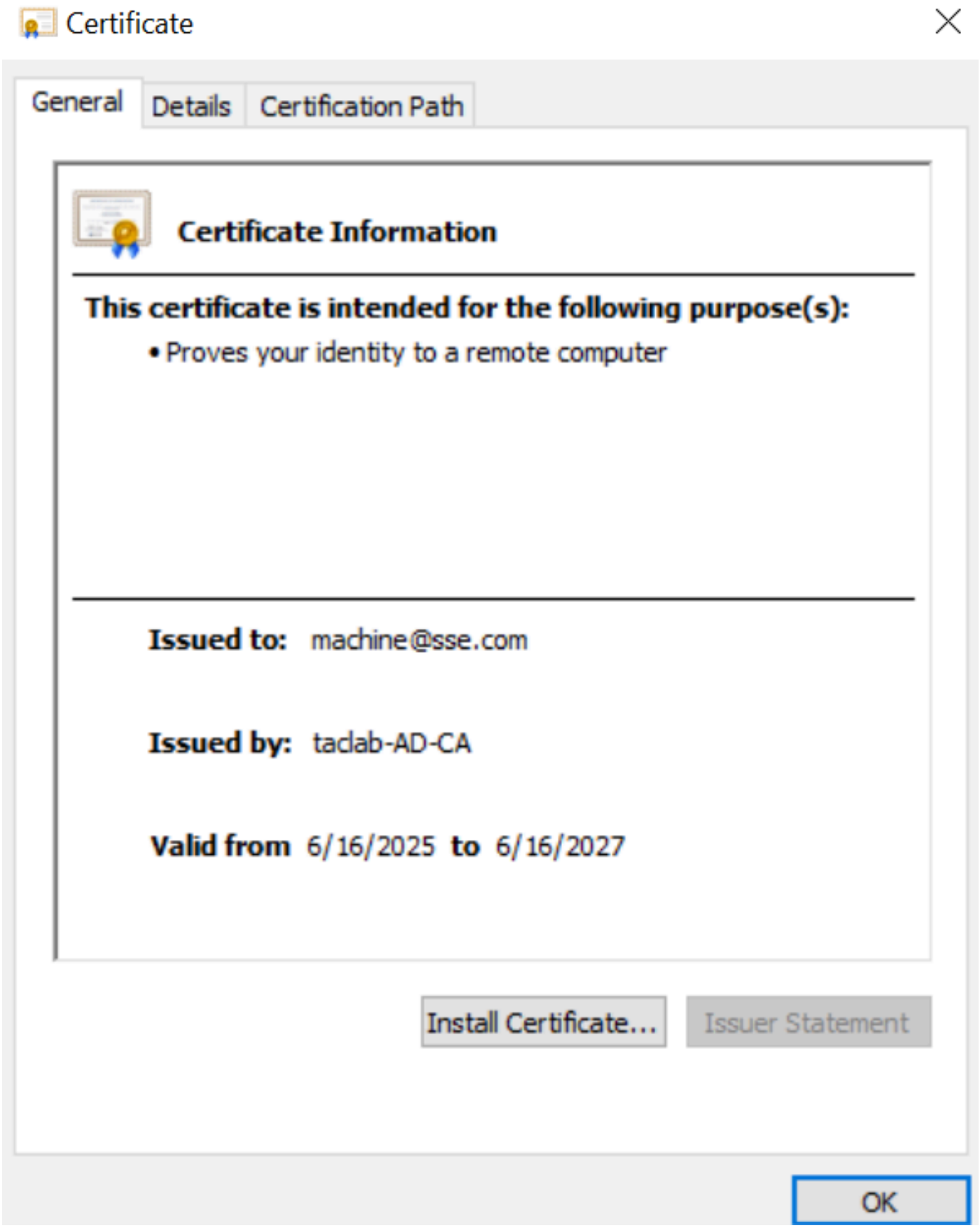
a.我们可以使用任何在线CSR生成器软件CSR生成器或openssl CLI

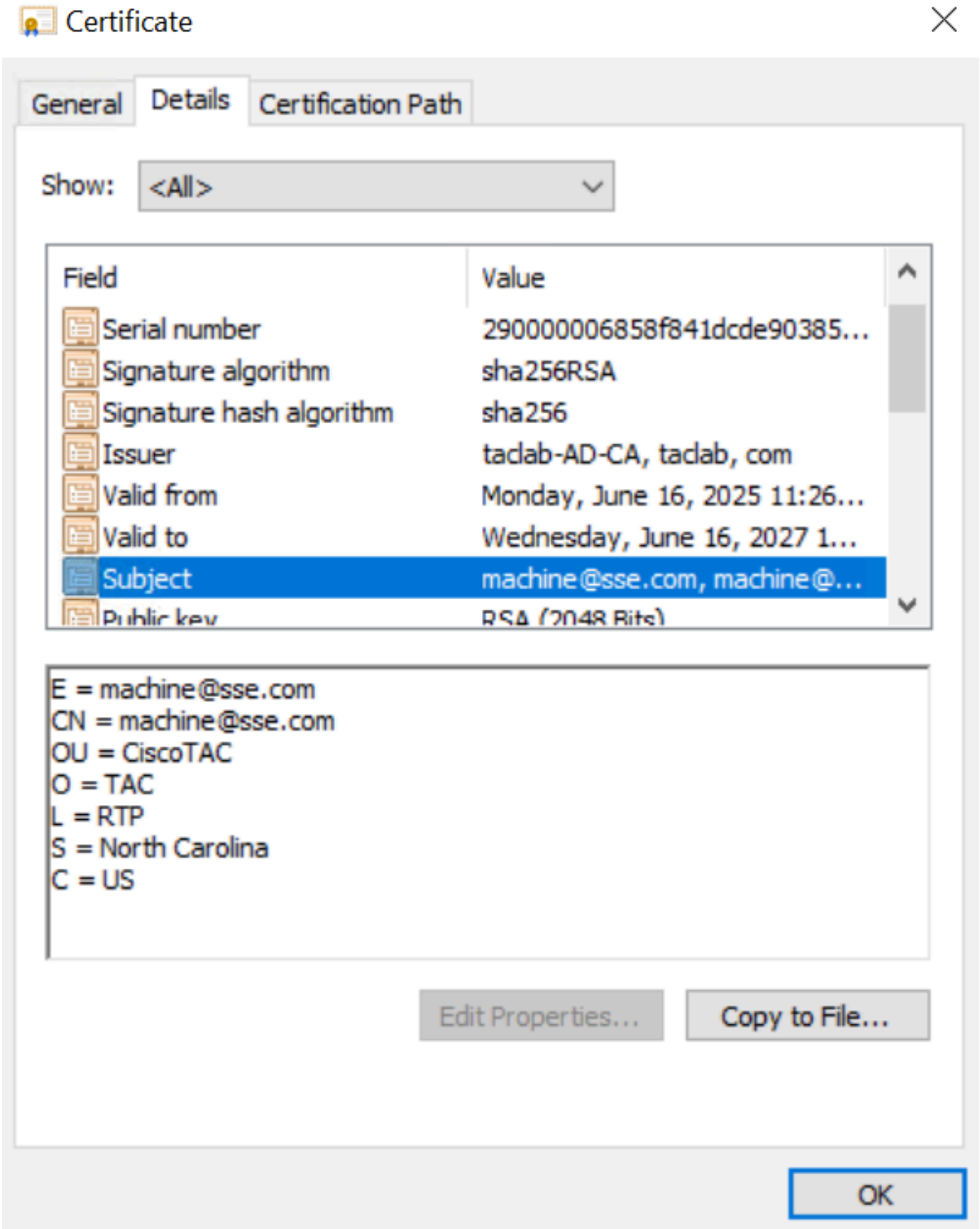
```
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr
```

```
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.复制CSR并生成计算机证书


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



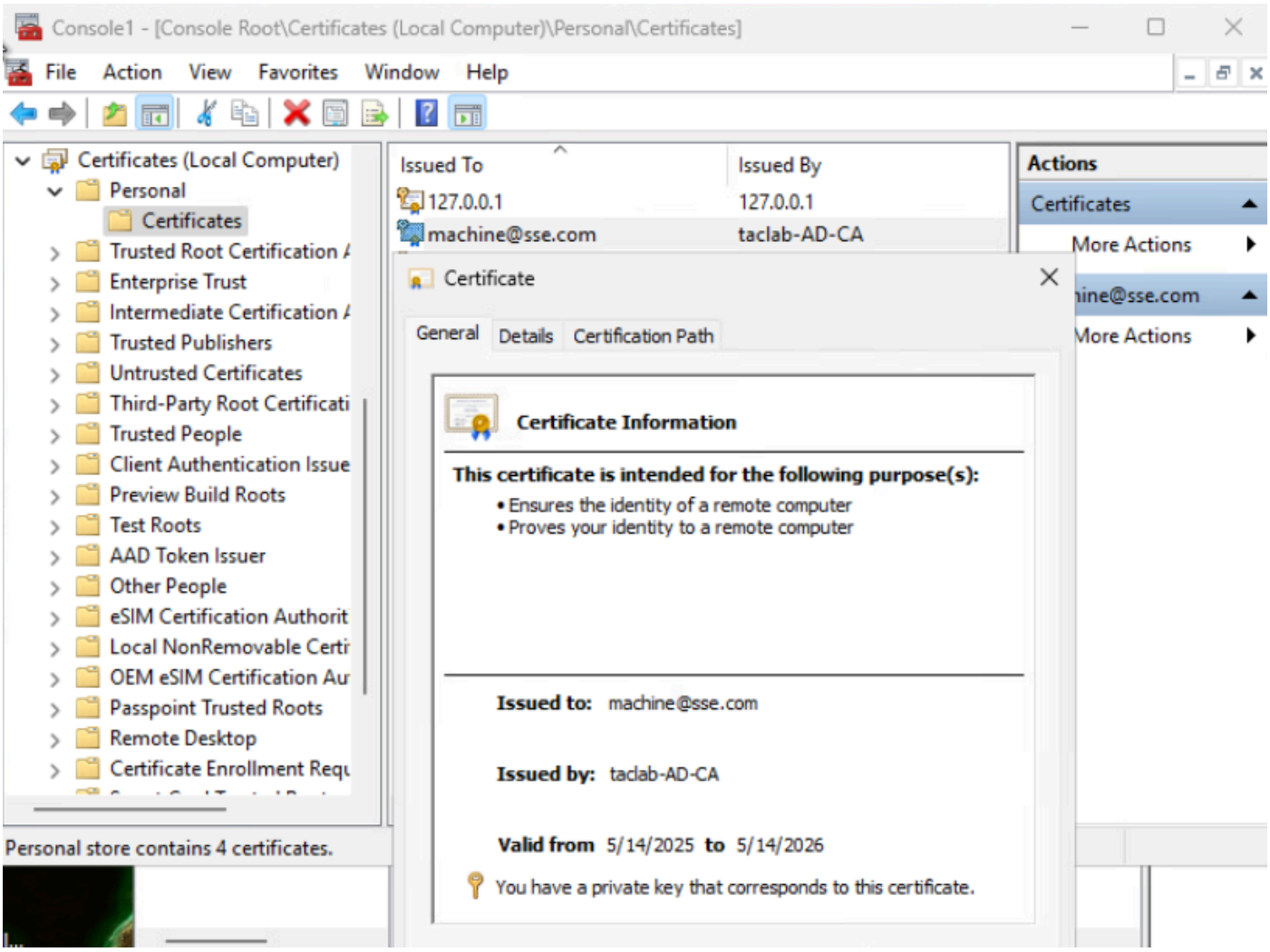
3.使用分别在前面的步骤（步骤1和2）中生成的密钥和证书，将计算机证书转换为PKCS12格式

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#
```

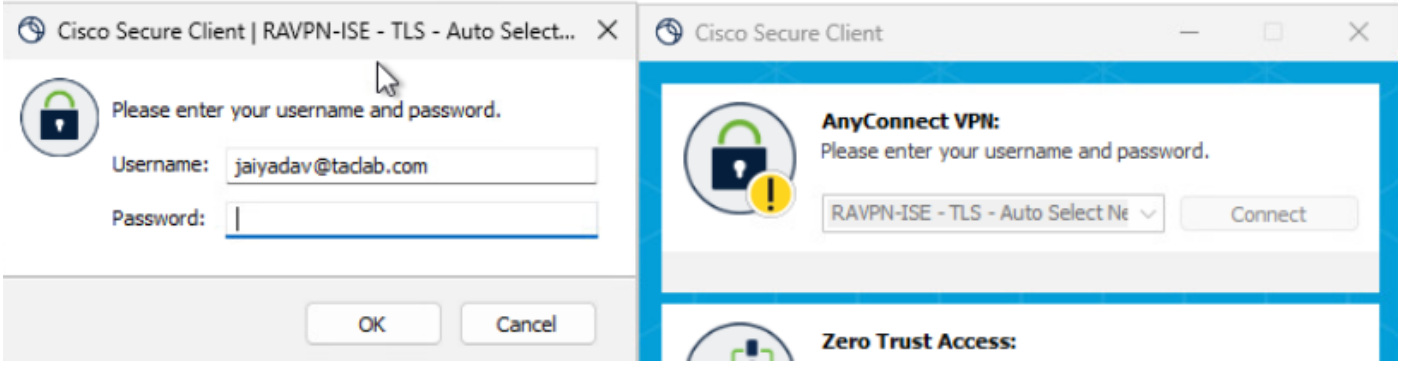
第7步 — 在测试计算机上导入计算机证书

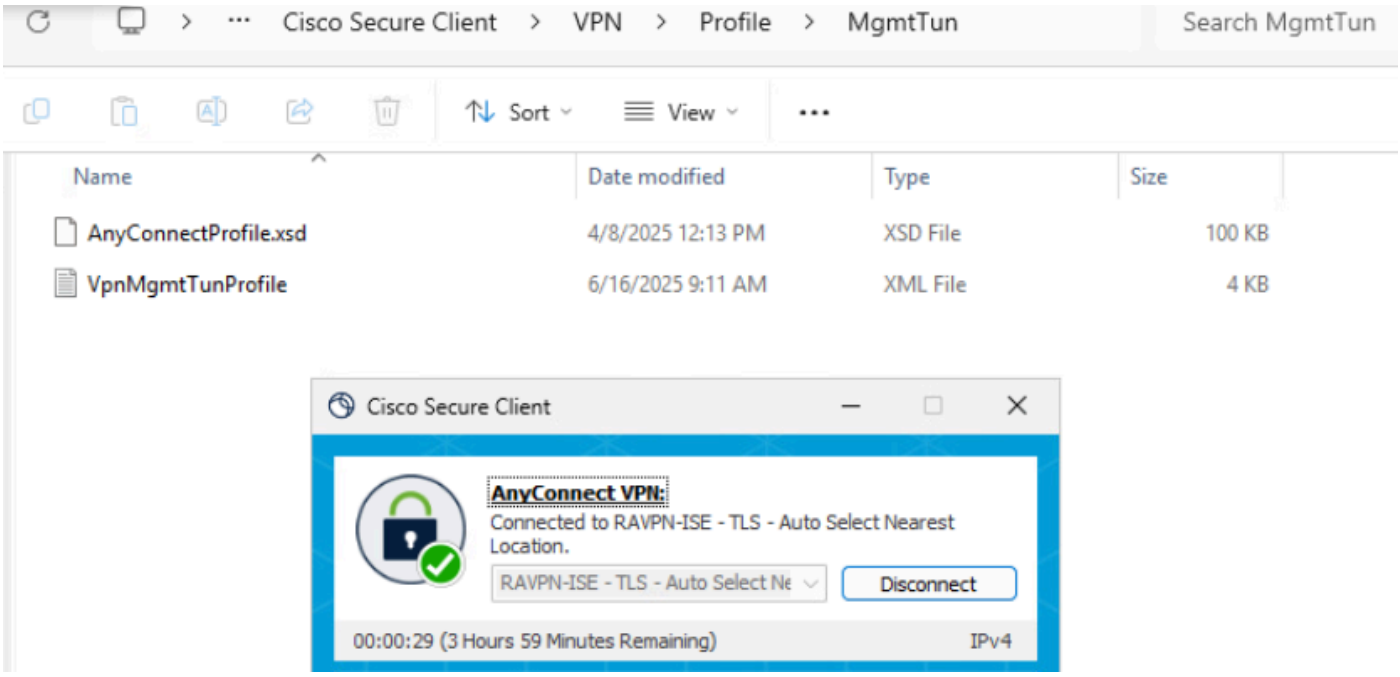
a.在本地或计算机存储下导入PKCS12计算机证书



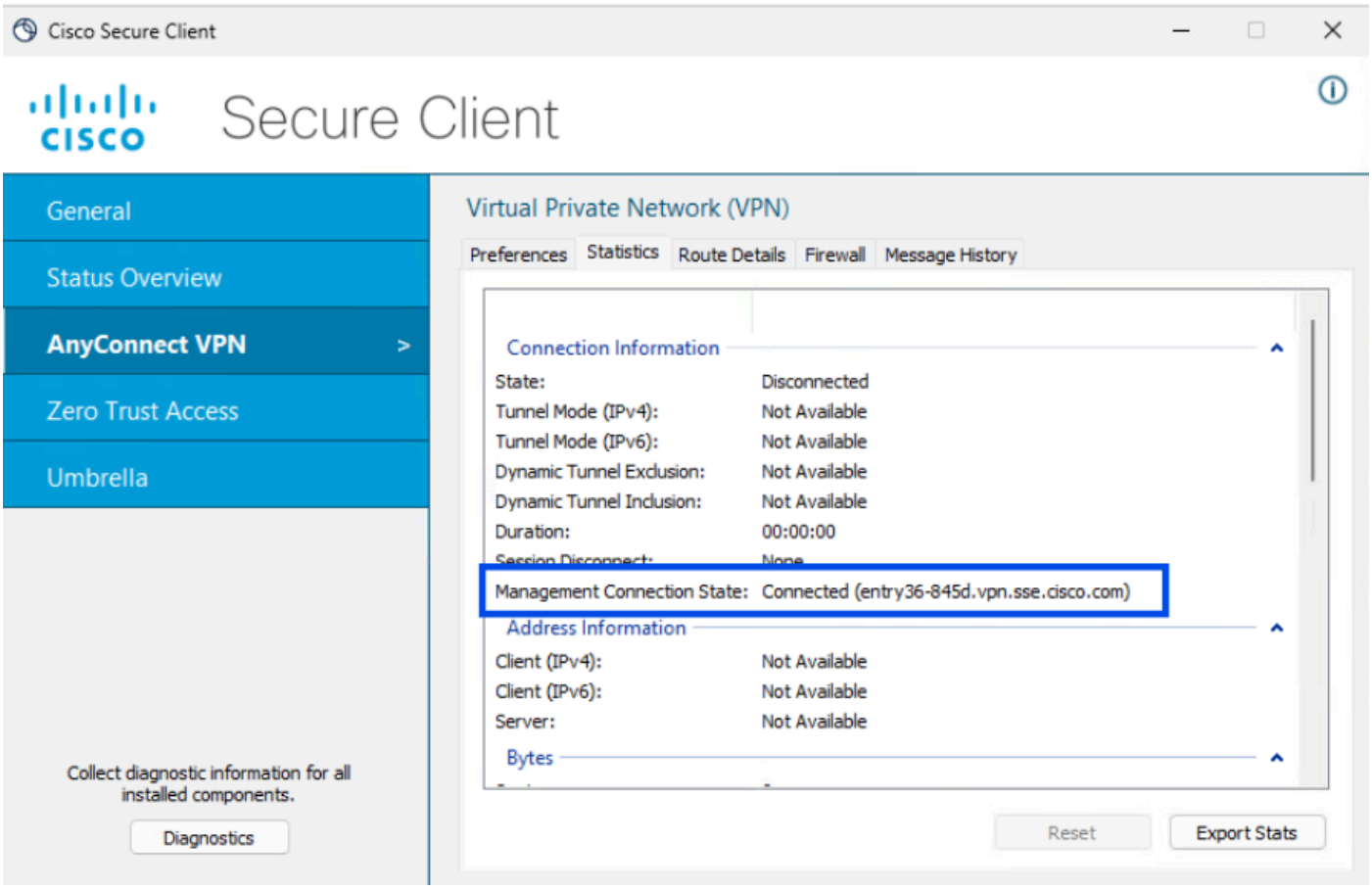
步骤8 — 连接到机器隧道

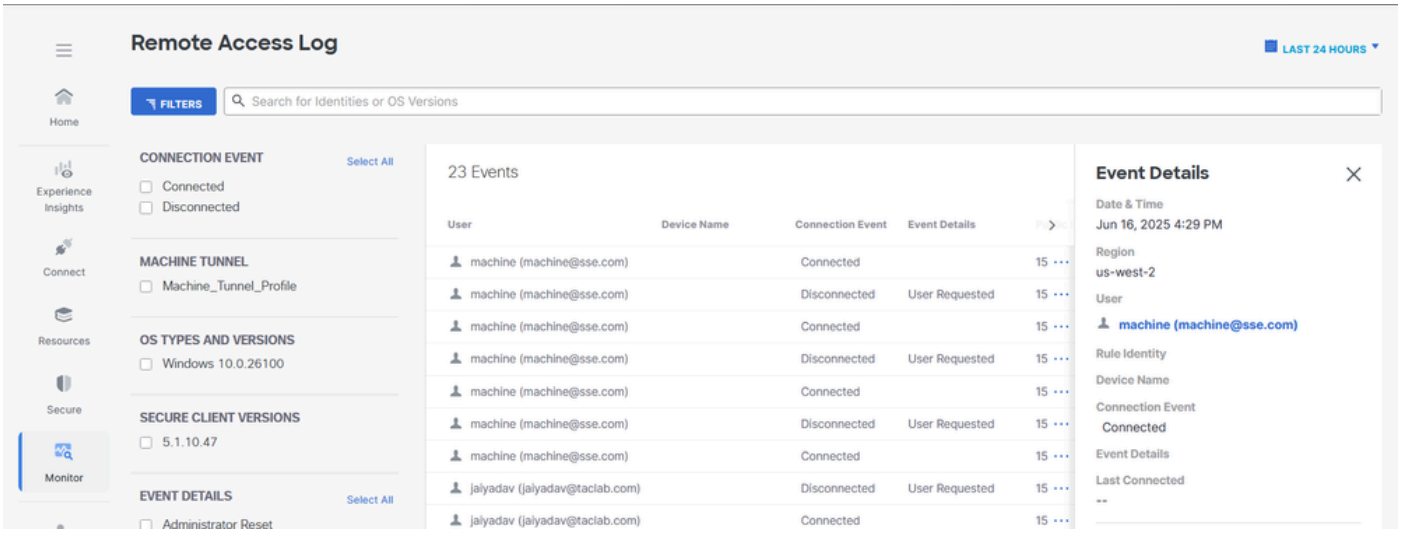
a.连接到用户隧道，这将触发要下载的计算机xml配置文件。




Cisco Secure Client > VPN > Profile > MgmtTun
Search MgmtTun
Sort
View
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 Ne
Disconnect
00:00:29 (3 Hours 59 Minutes Remaining)
IPv4

b.验证计算机隧道连接


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
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



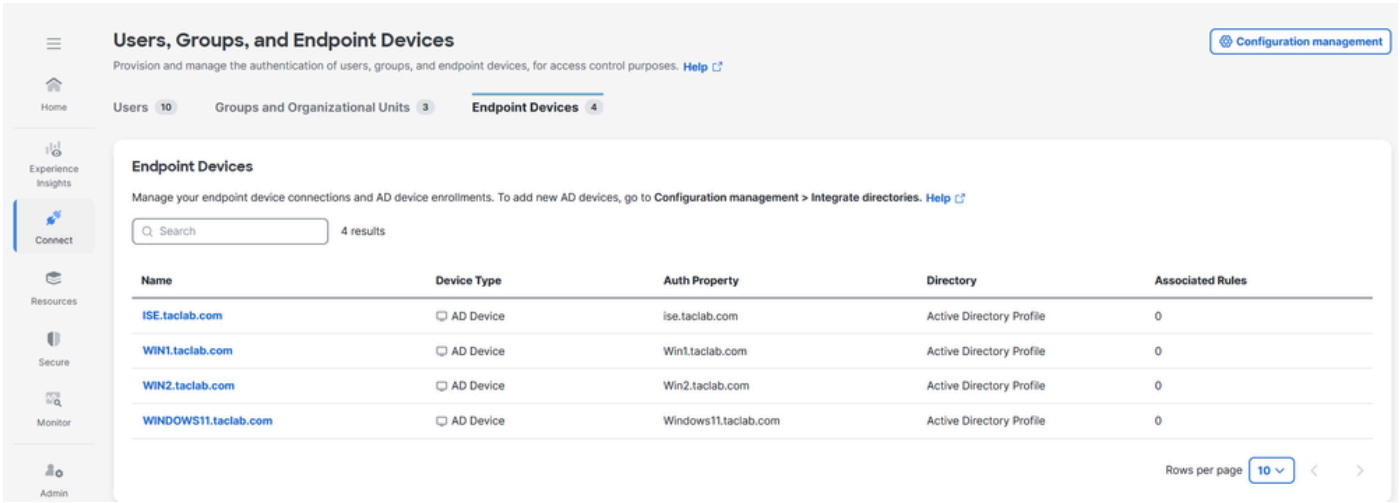
方法2 — 使用终端证书配置计算机隧道

在本例中，Primary字段要进行身份验证，请选择包含设备名称（计算机名称）的证书字段。 安全访问使用设备名称作为机器隧道标识符。计算机名称的格式必须与所选设备标识符的格式匹配

执行步骤1到步骤4进行计算机隧道配置

第5步 — 配置AD连接器以便能够在Cisco Secure Access上导入终端。

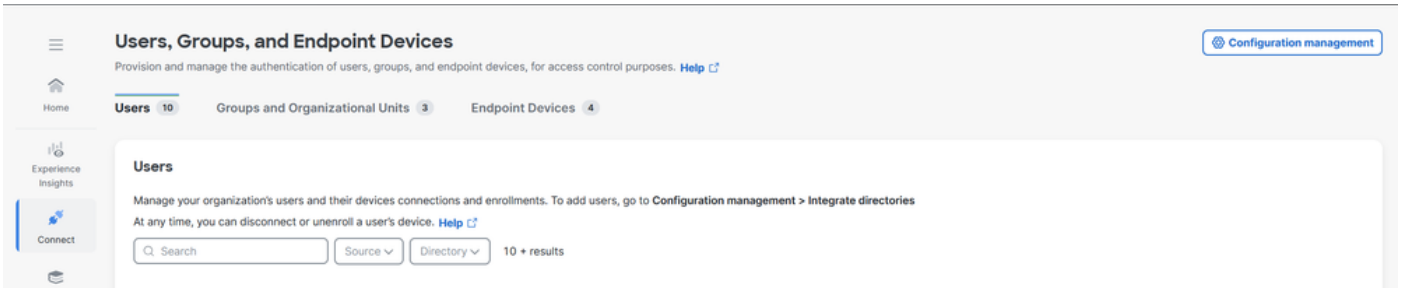
有关详细信息，请参阅永久活动目录集成



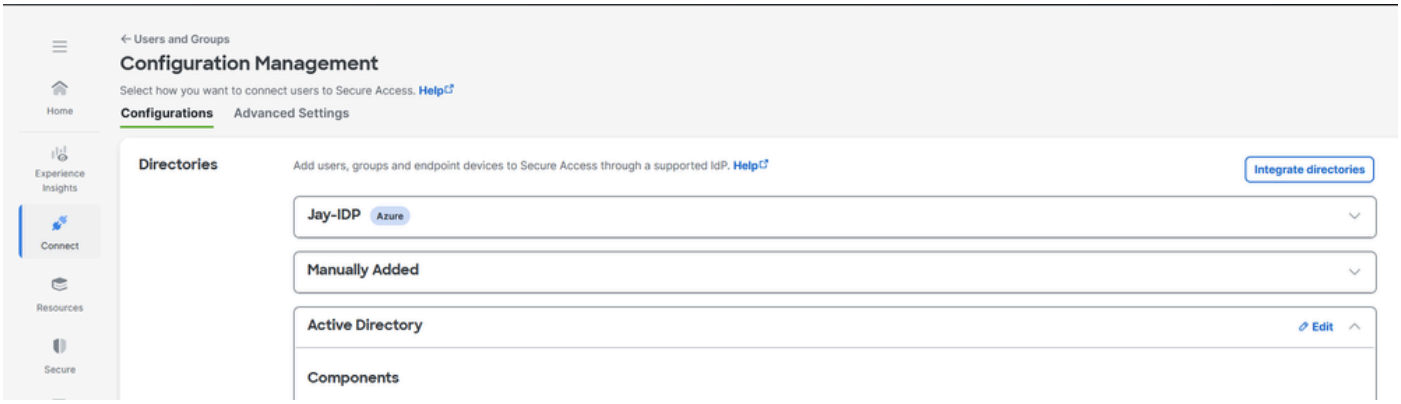
第6步 — 配置终端设备身份验证

1.导航至连接>用户、组和终端设备。

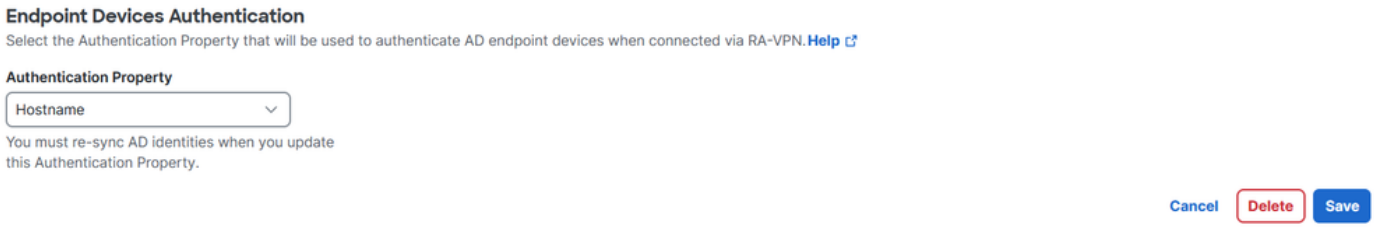
2.单击Configuration management



3. 在配置下，编辑Active Directory



4.将Endpoint Devices Authentication Property设置为主机名



5.单击Save并在安装有AD连接器的服务器上重新启动AD连接器服务

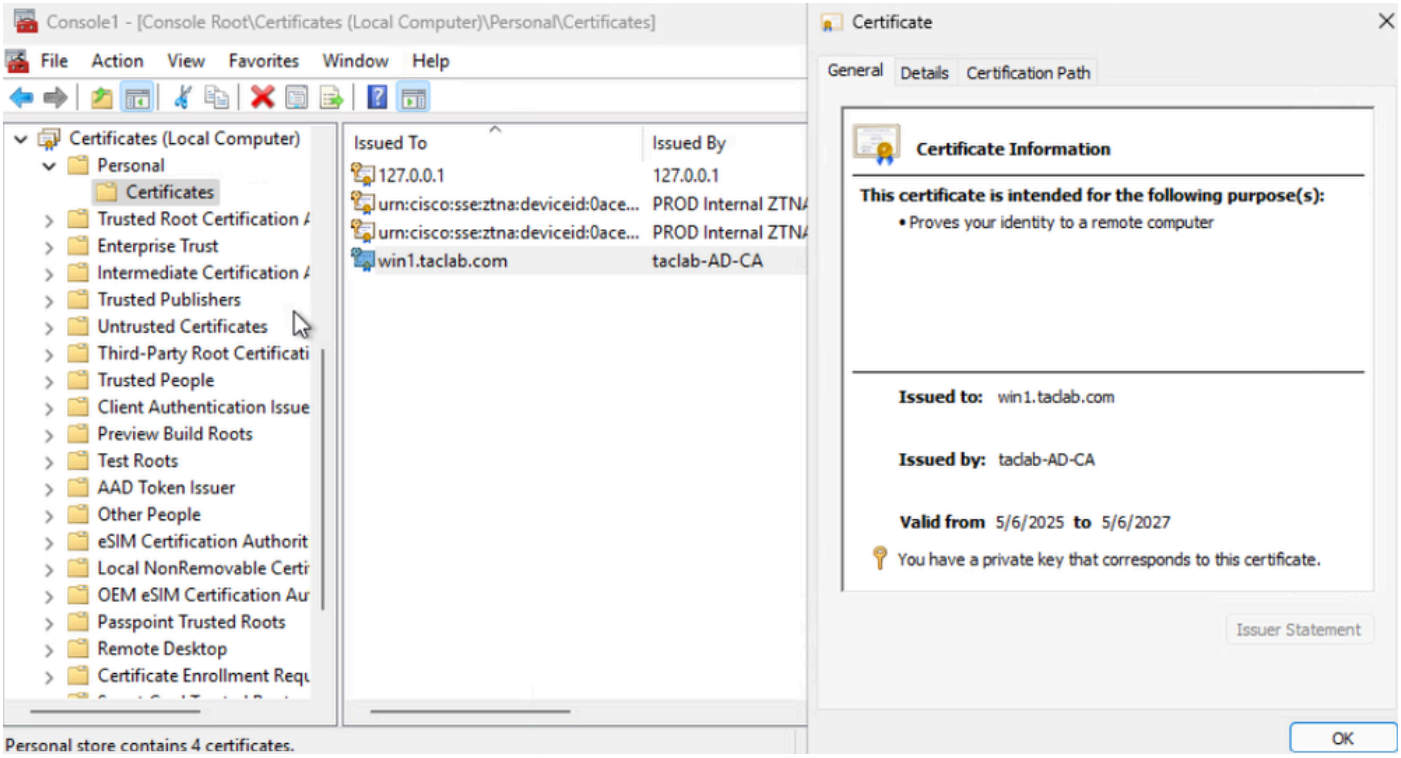
第7步 — 生成和导入终端证书

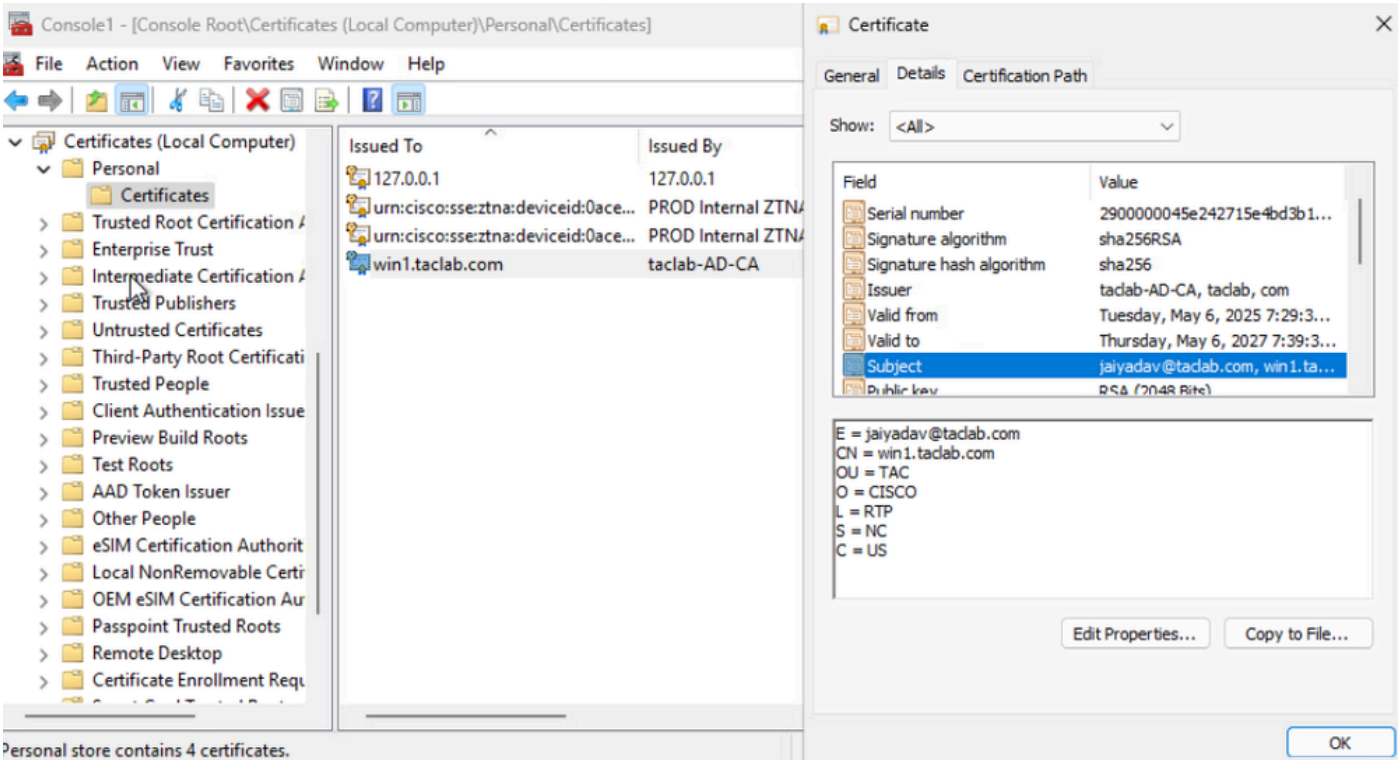
a.生成CSR，打开CSR生成器或OpenSSL工具

b.从CA生成终端证书

c.将.cert文件转换为PKCS12格式

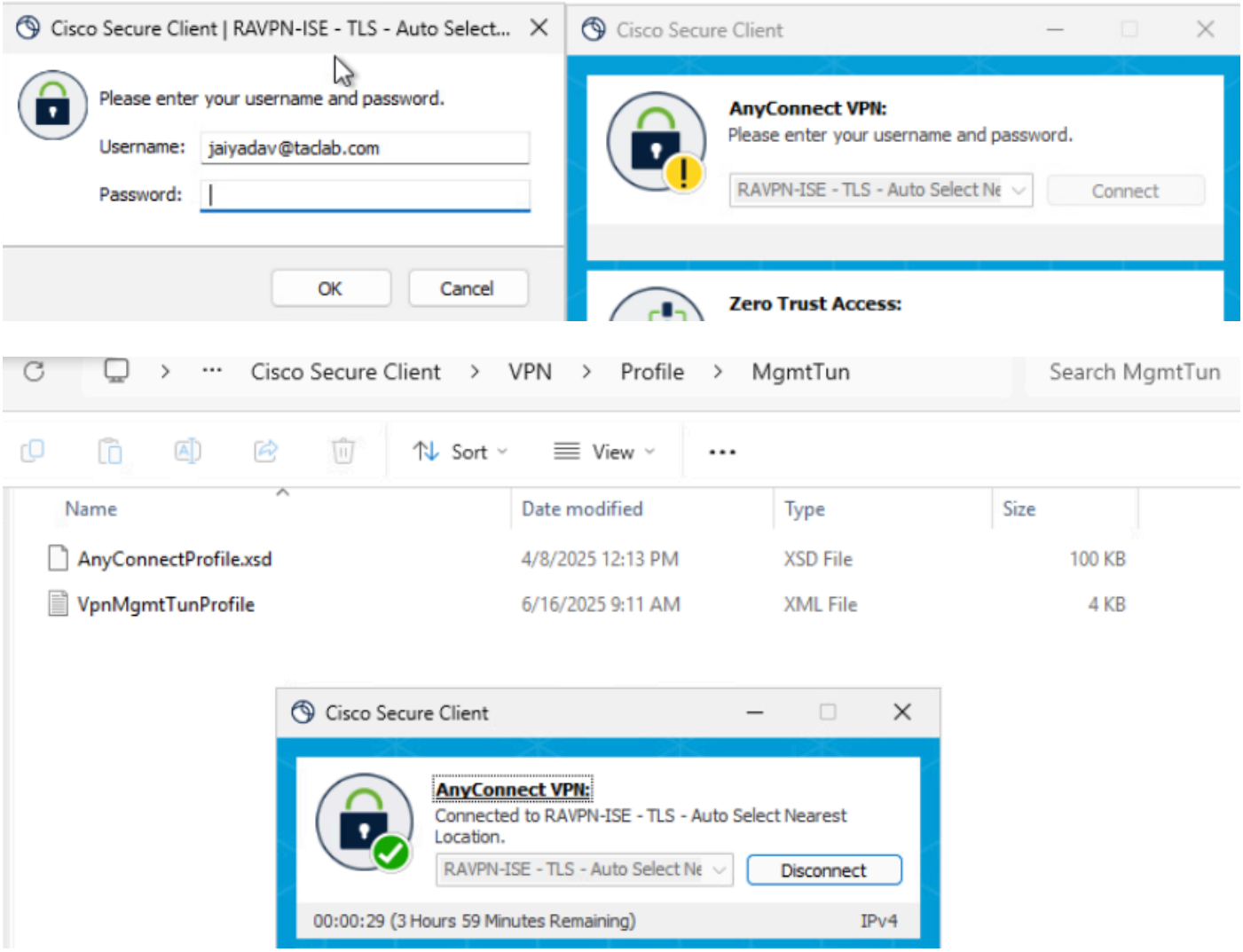
d.在终端证书存储中导入PKCS12证书



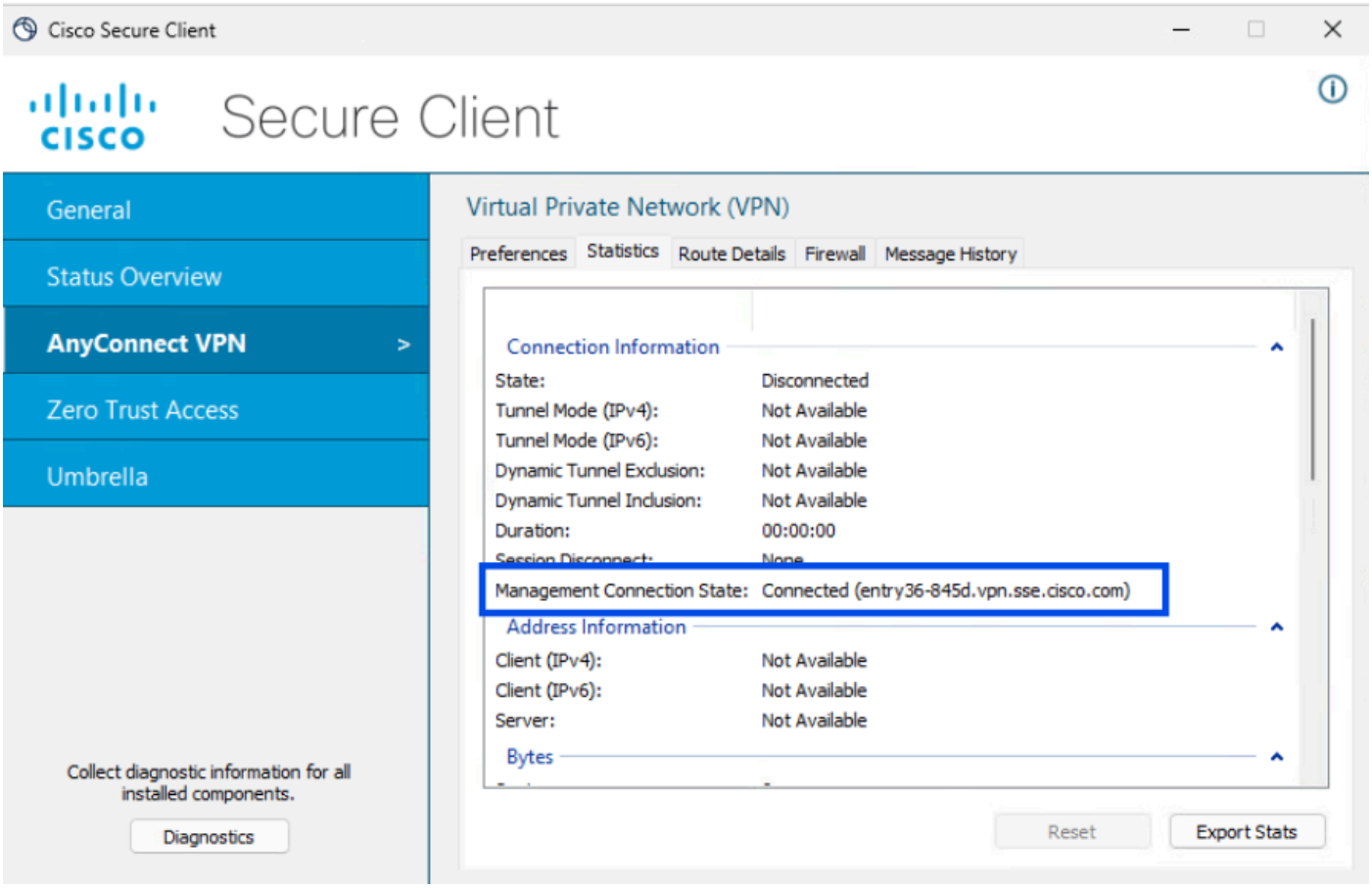


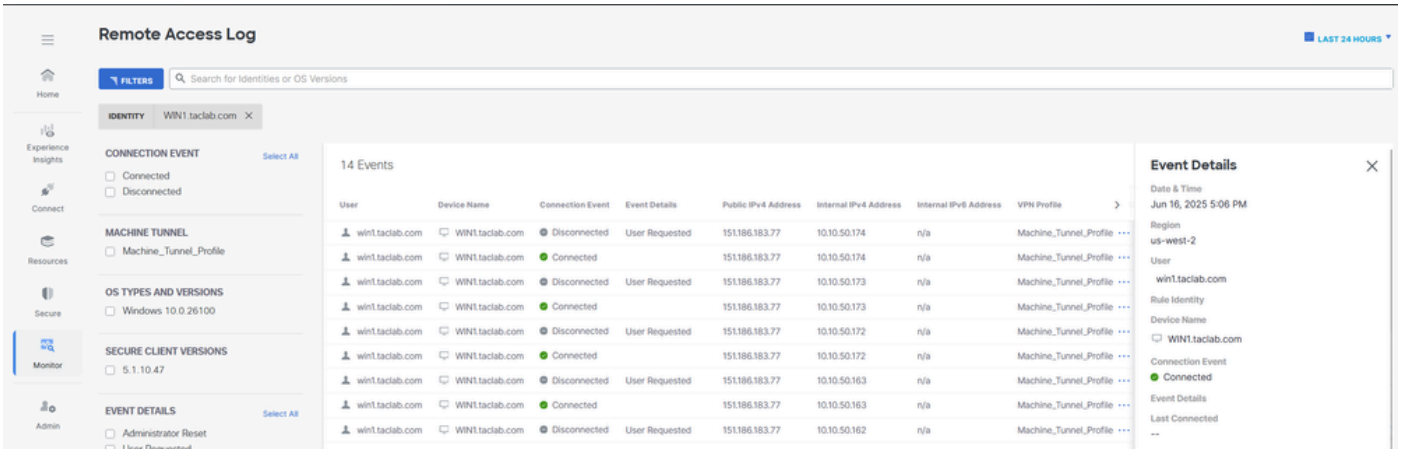
步骤8 — 连接到机器隧道

a.连接到用户隧道，它会触发计算机隧道xml配置文件的下载


Cisco Secure Client | RAVPN-ISE - TLS - Auto Select...
Please enter your username and password.
Username: jaiyadav@taclab.com
Password:
OK
Cancel
Cisco Secure Client
AnyConnect VPN:
Please enter your username and password.
RAVPN-ISE - TLS - Auto Select Ne
Connect
Zero Trust Access:
Cisco Secure Client > VPN > Profile > MgmtTun
Search MgmtTun
Sort
View
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 Ne
Disconnect
00:00:29 (3 Hours 59 Minutes Remaining)
IPv4

b.验证计算机隧道连接





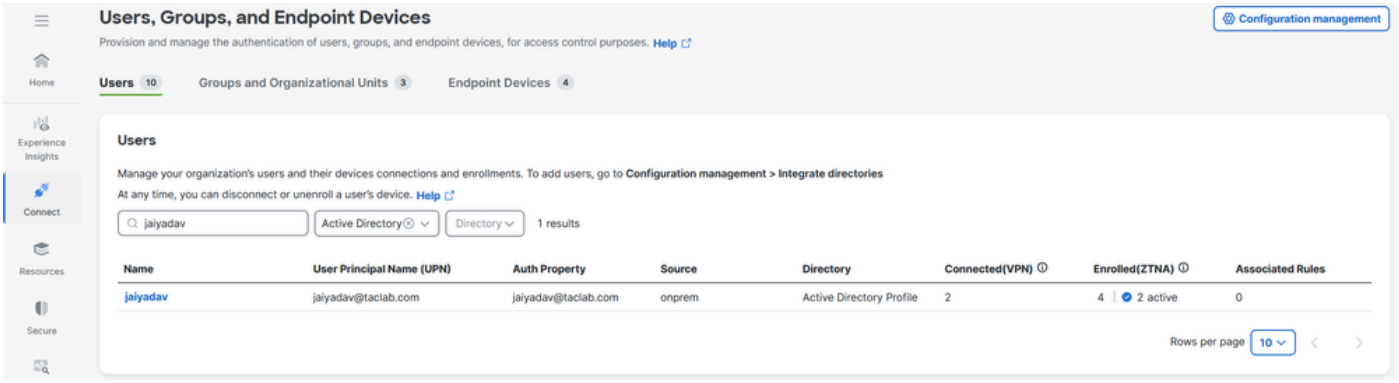
方法3 — 使用用户证书配置计算机隧道

在本例中，Primary字段要进行身份验证，请选择包含用户邮件或UPN的证书字段。安全访问使用电子邮件或UPN作为机器隧道标识符。电子邮件或UPN的格式必须与所选设备标识符的格式匹配

执行步骤1至4进行计算机隧道配置

第5步 — 配置AD连接器以便能够在Cisco Secure Access上导入用户。

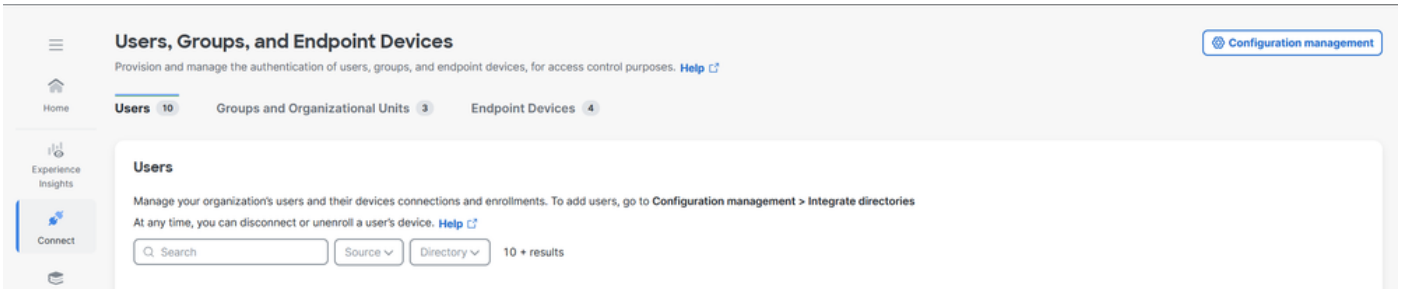
有关详细信息，请参阅永久活动目录集成



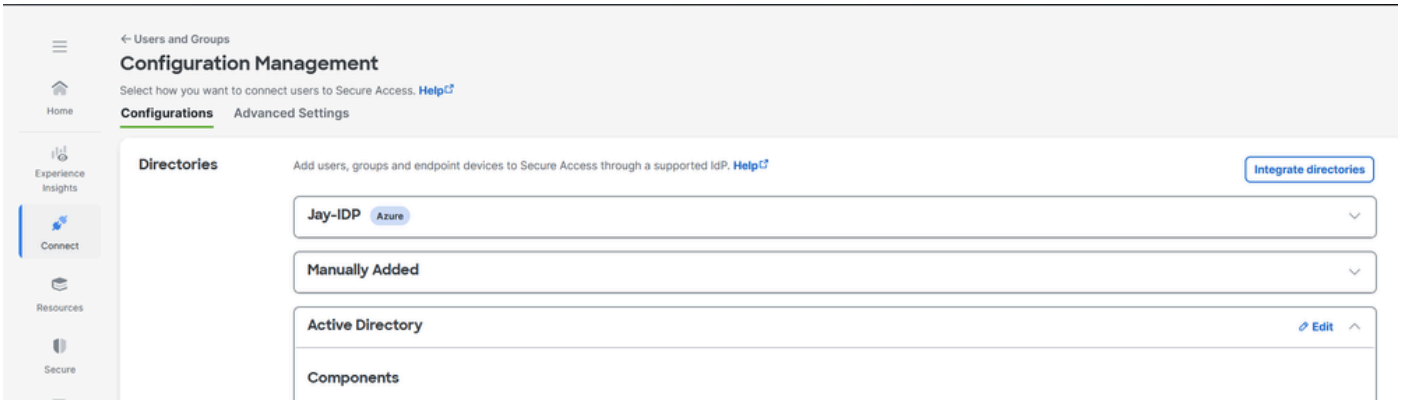
第6步 — 配置用户身份验证

1.导航至连接>用户、组和终端设备。

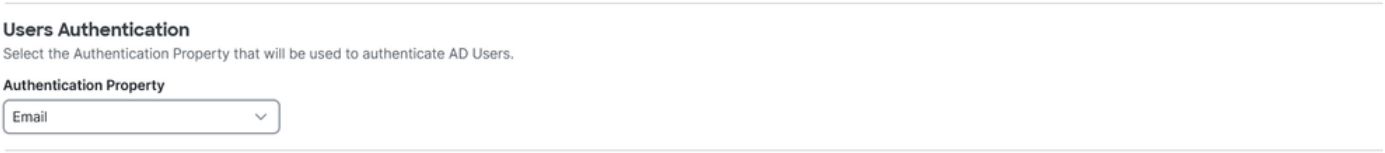
2.单击Configuration management



3. 在配置下，编辑Active Directory



4.将用户身份验证属性设置为电子邮件



5.单击Save并在安装有AD连接器的服务器上重新启动AD连接器服务

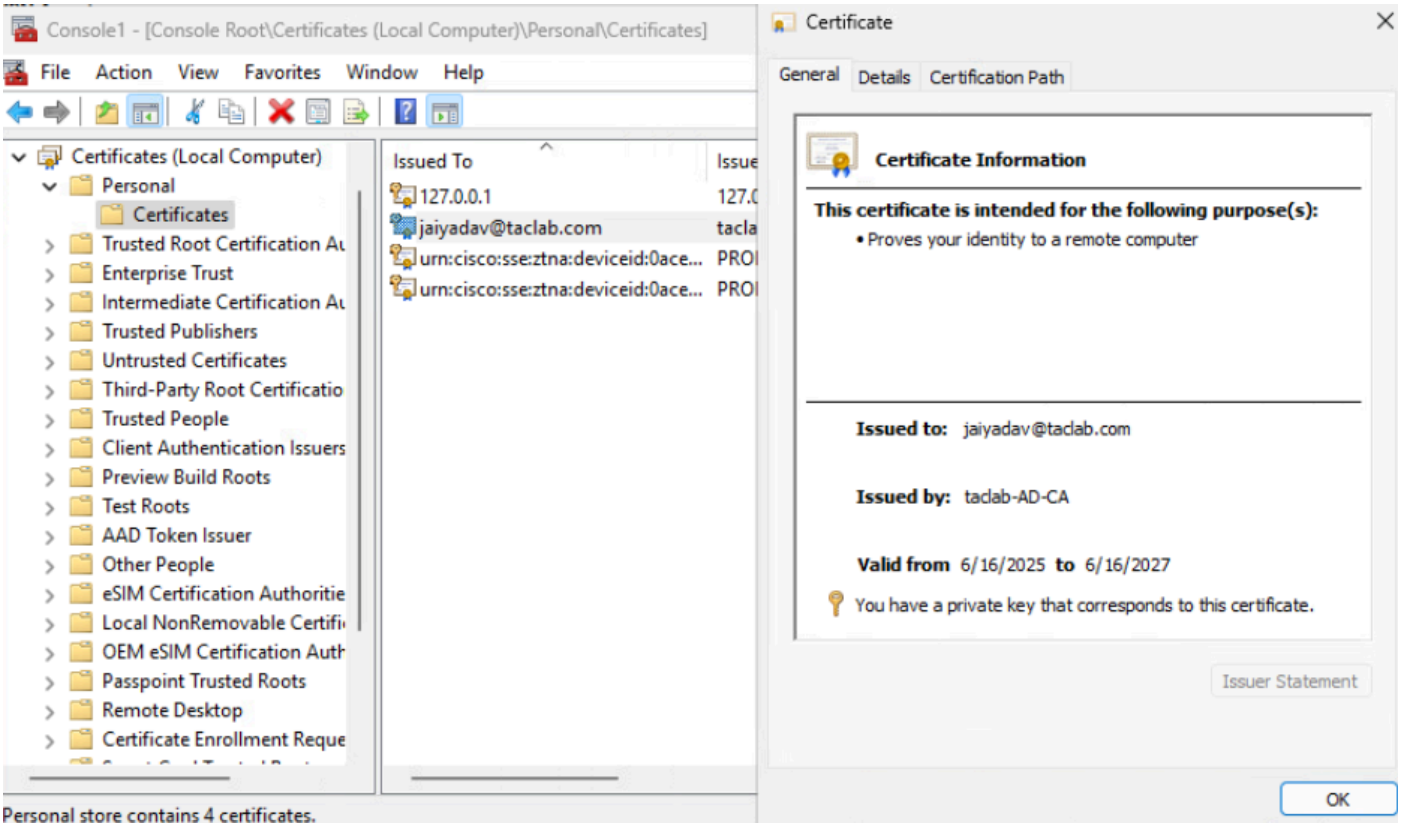
第7步 — 生成和导入终端证书

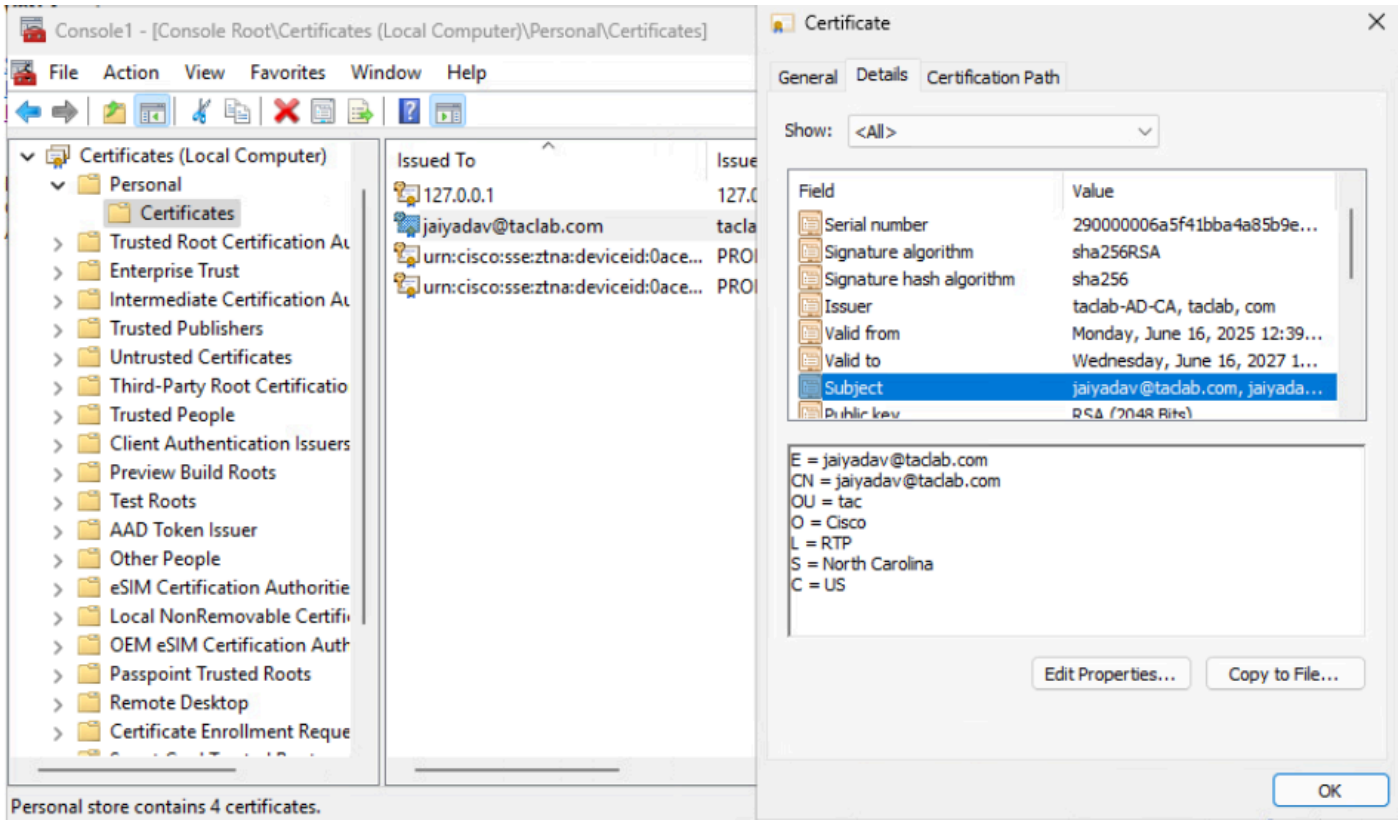
a.生成CSR，打开CSR生成器或OpenSSL工具

b.从CA生成终端证书

c.将.cert文件转换为PKCS12格式

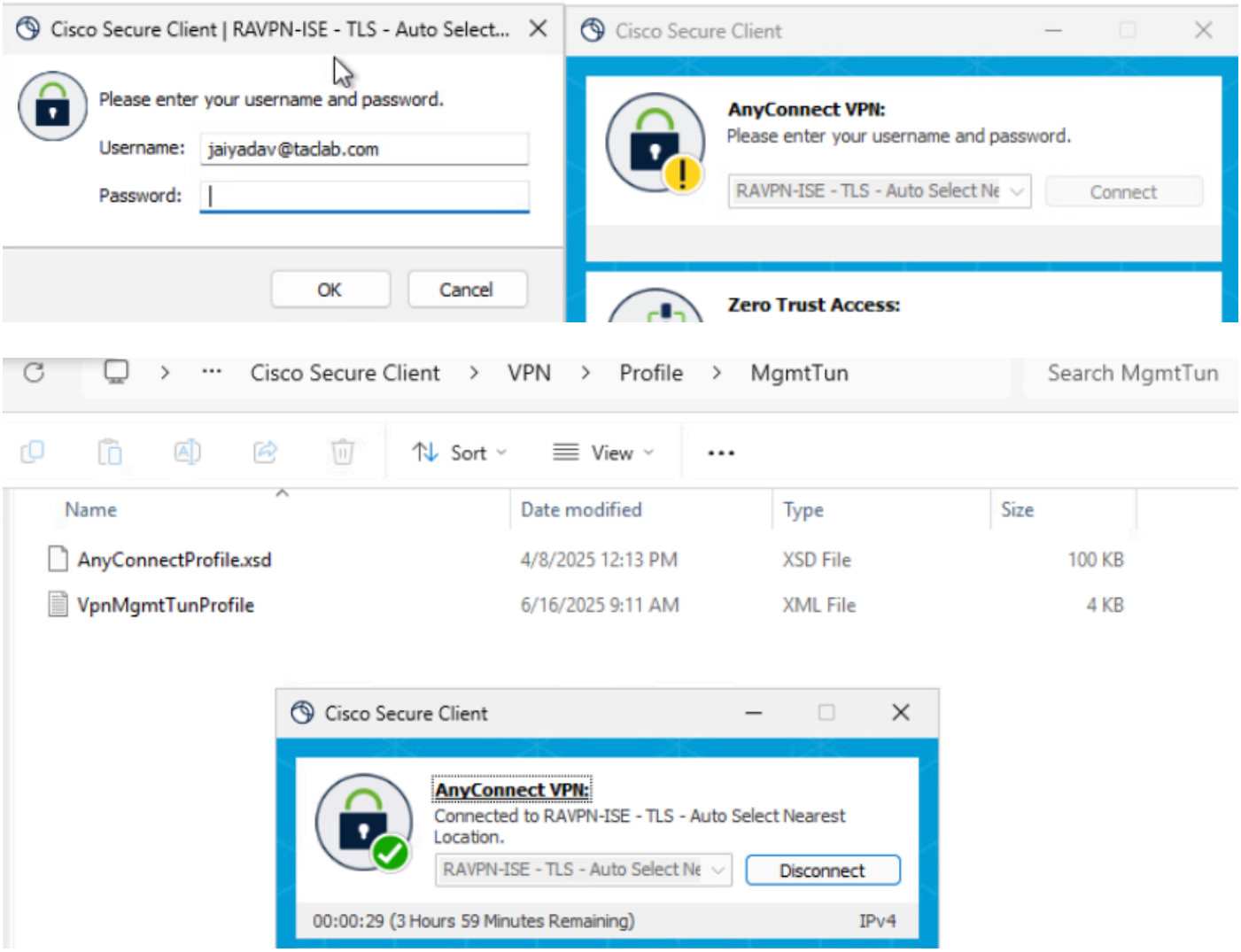
d.在终端证书存储中导入PKCS12证书



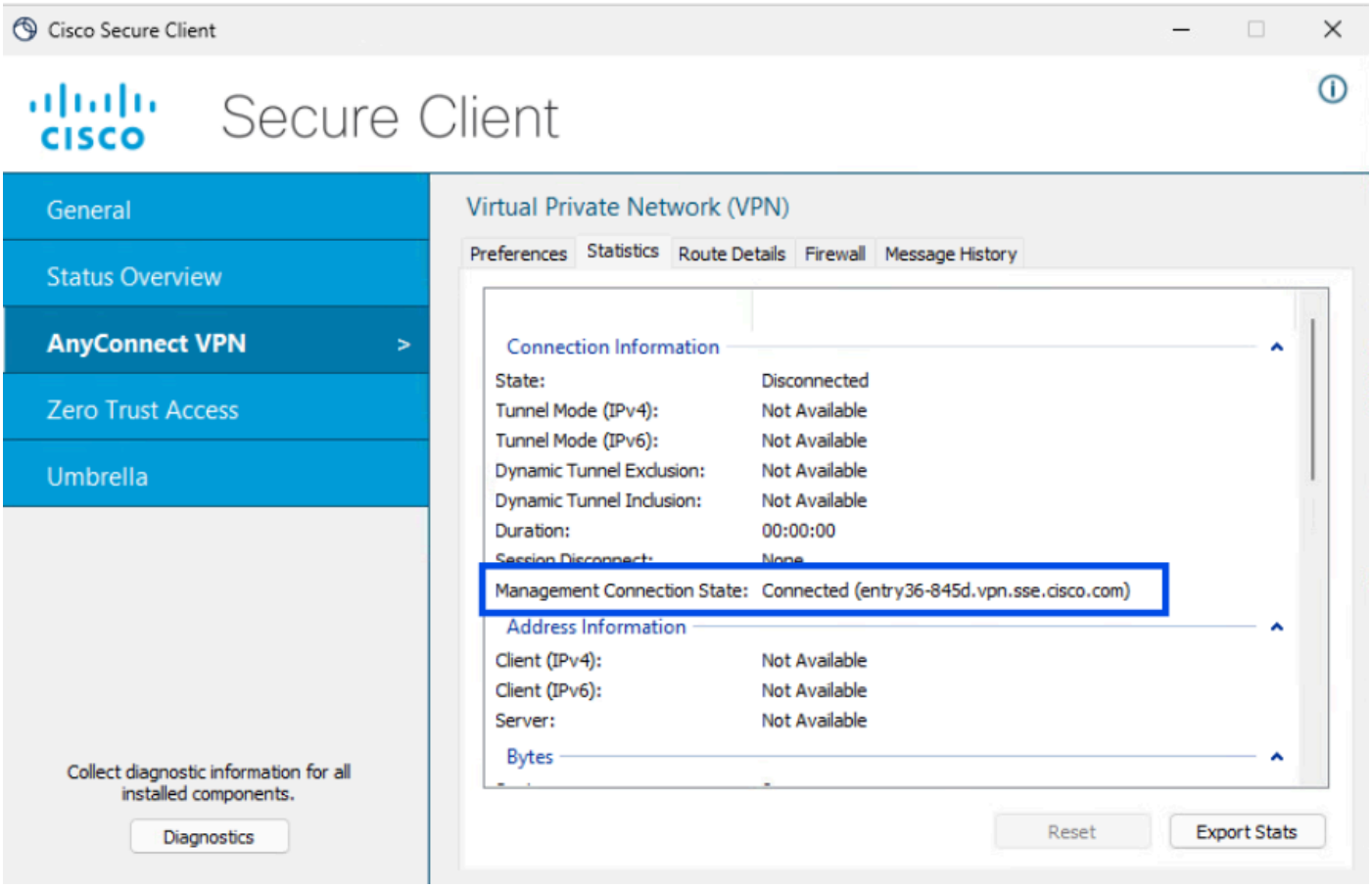


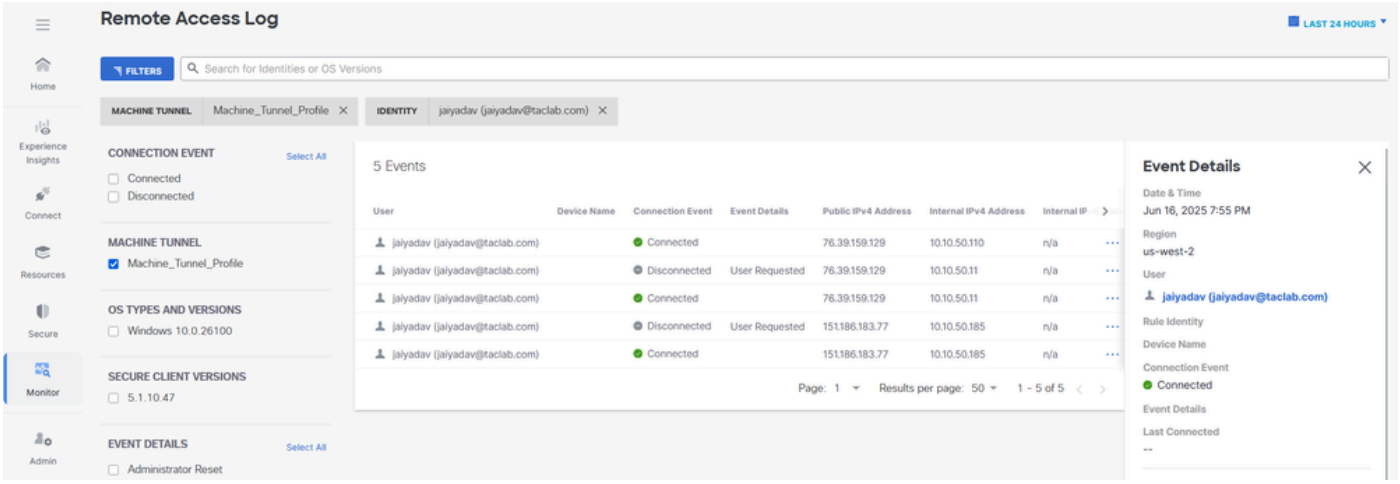
步骤8 — 连接到机器隧道

a.连接到用户隧道，它会触发计算机隧道xml配置文件的下载



b.验证计算机隧道连接





故障排除

提取DART捆绑包，打开AnyConnectVPN日志并分析错误消息

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。