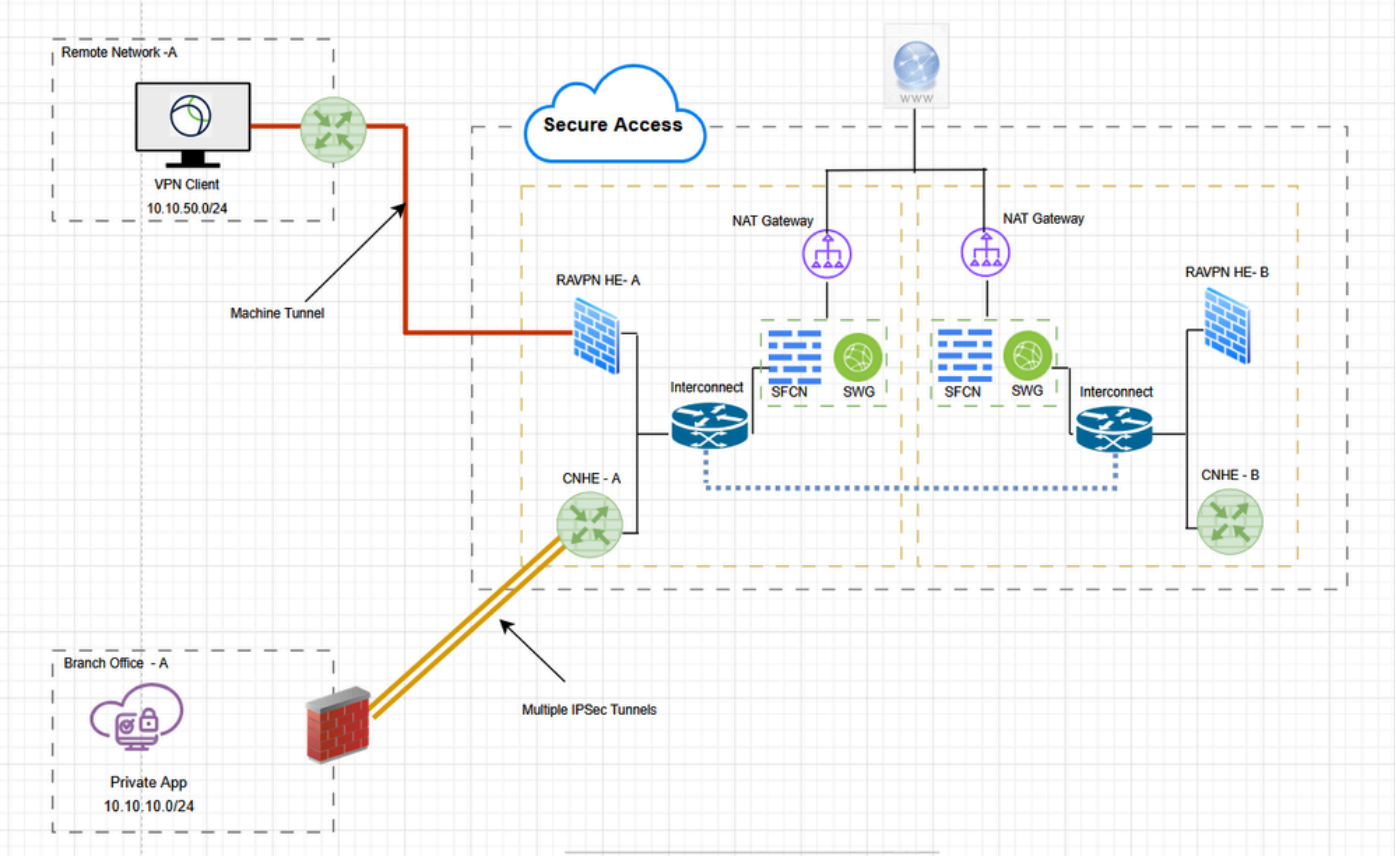
在Cisco Secure Access上配置電腦隧道

目錄

簡介

本文檔介紹如何將Secure Access配置為VPN網關並接受通過VPN機器隧道從安全客戶端進行的連線。

網路圖表



必要條件

- 安全訪問中的完全管理員角色。
- 在Cisco Secure Access上至少配置一個使用者VPN配置檔案
- Cisco Secure Access上的使用者IP池

需求

建議您瞭解以下主題：

- 509個證書
- OpenSSL

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Secure Access
- 思科安全使用者端5.1.10
- Windows 11
- Windows Server 2019 - CA

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

只要客戶端系統通電，安全接入VPN機器隧道就可以確保連線到公司網路，而不僅僅是在終端使用者建立VPN連線時。您可以對辦公室外端點（尤其是使用者通過VPN不經常連線到辦公室網路的裝置）執行補丁管理。需要企業網路連線的終端作業系統登入指令碼也受益於此功能。對於要在沒有使用者互動的情況下建立此隧道，將使用基於證書的身份驗證。

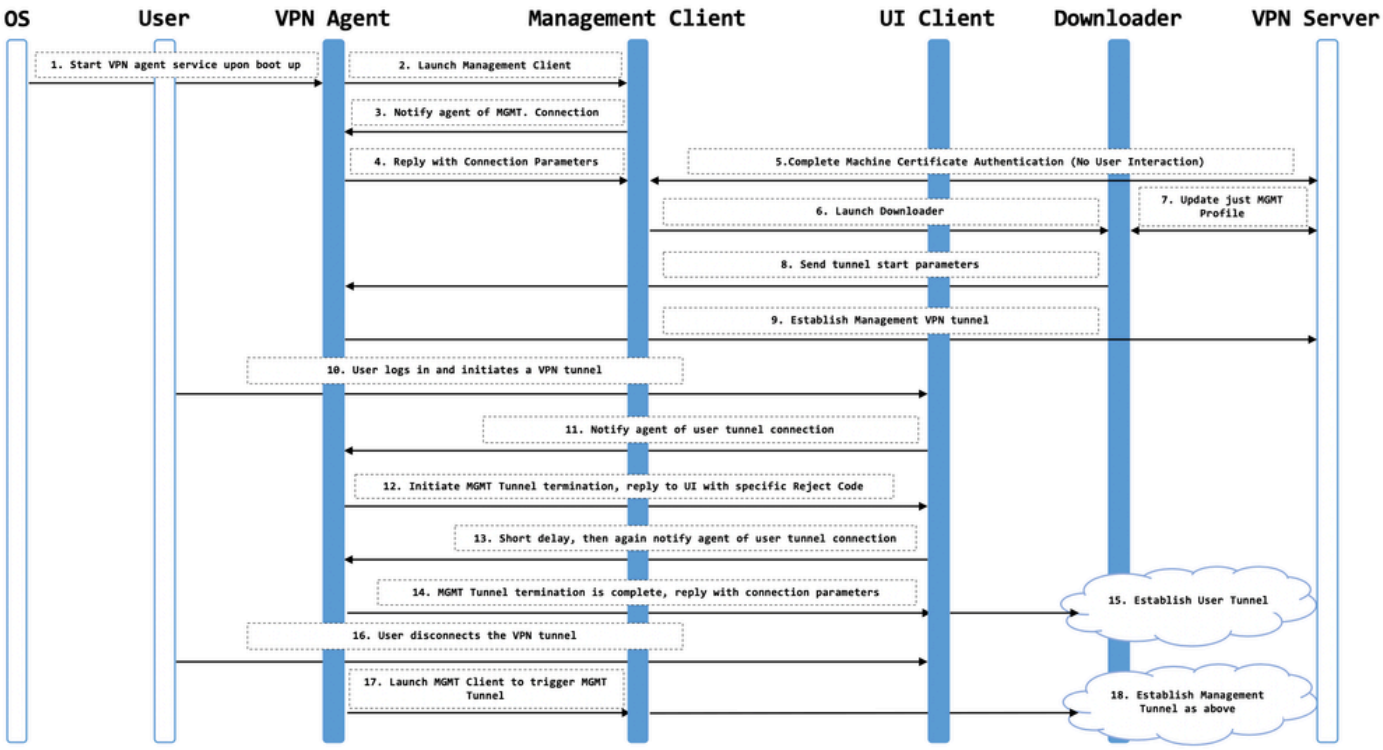
安全訪問電腦隧道允許管理員在使用者登入之前連線Cisco Secure Client，而無需使用者干預。當終端位於外部且與使用者啟動的VPN斷開時，會觸發安全訪問電腦隧道。安全接入VPN機器隧道對終端使用者是透明的，在使用者發起VPN時自動斷開。

正在處理機器隧道

安全客戶端VPN代理服務會在系統啟動時自動啟動。安全客戶端VPN代理使用VPN配置檔案檢測是否啟用了電腦隧道功能。如果啟用了電腦隧道功能，代理將啟動管理客戶端應用程式以啟動電腦隧道連線。管理客戶端應用程式使用VPN配置檔案中的主機條目來啟動連線。然後按慣例建立VPN通道，但有一個例外：在電腦隧道連線期間不會執行軟體更新，因為電腦隧道對使用者是透明的。

使用者通過安全客戶端發起VPN隧道，該隧道會觸發電腦隧道終止。在機器隧道終止時，使用者隧道建立會照常繼續。

使用者斷開VPN隧道，從而觸發自動重新建立機器隧道。



限制

- 不支援使用者互動。
- 僅支援通過電腦證書儲存區(Windows)進行的基於證書的身份驗證。

- 強制實施嚴格的伺服器證書檢查。
- 不支援專用代理。
- 不支援公共代理（在無法從瀏覽器中檢索本機代理設定的平台上支援ProxyNative值）。
- 不支援安全客戶端自定義指令碼

設定

方法1 — 使用使用者machine@sse.com配置電腦隧道

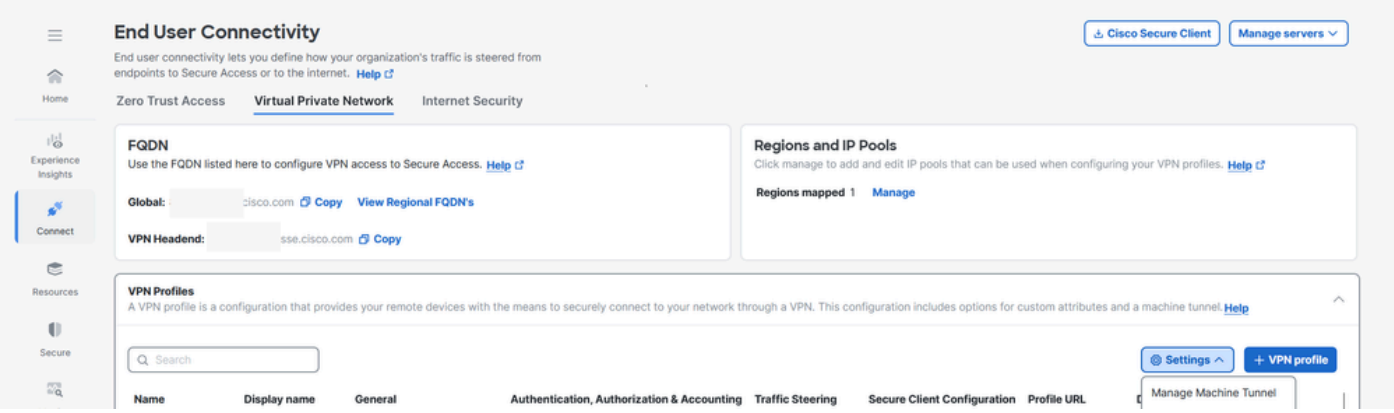
步驟1 — 常規設定

配置常規設定，包括此電腦隧道使用的域和協定。

1.導航至Connect > End User Connectivity > Virtual Private Network。

2.導航到VPN配置檔案，然後配置電腦隧道的設定。

a.按一下Settings，然後從下拉選單中選擇Manage Machine Tunnel。

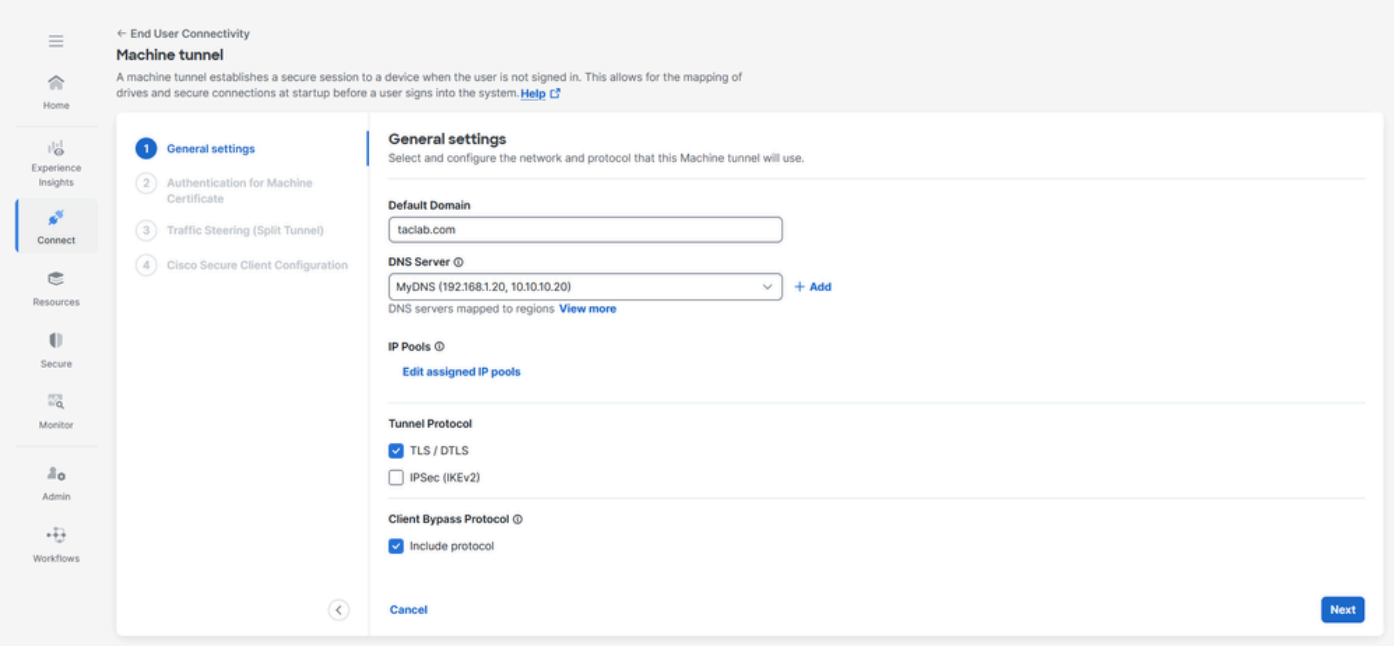


3. 輸入Default Domain。
4. 通過管理區域和IP池頁面對映的DNS伺服器設定為預設伺服器。您可以接受預設DNS伺服器，從下拉選單中選擇其他DNS伺服器，或按一下+ Add新增新的DNS伺服器對。選擇其他DNS伺服器或新增新的DNS伺服器將覆蓋此預設伺服器。
5. 從IP Pools下拉選單中選擇每個區域的一個IP池。VPN配置檔案必須在每個區域中至少分配一個IP池才能進行有效配置。
6. 選擇此電腦隧道使用的隧道協定:
   - TLS/DTLS
   - IPSec(IKEv2)

   必須至少選擇一個協定。
7. 或者，選中Include protocol以實施客戶端旁路協定。

   a.如果為IP協定啟用了Client Bypass Protocol ，並且沒有為該協定配置地址池（換句話說，ASA沒有為該協定的IP地址分配給客戶端），則使用該協定的任何IP流量都不會通過VPN隧道傳送。它將被傳送到隧道之外。

   b.如果禁用了客戶端旁路協定，並且沒有為該協定配置地址池，則一旦建立VPN隧道，客戶端將丟棄該IP協定的所有流量。



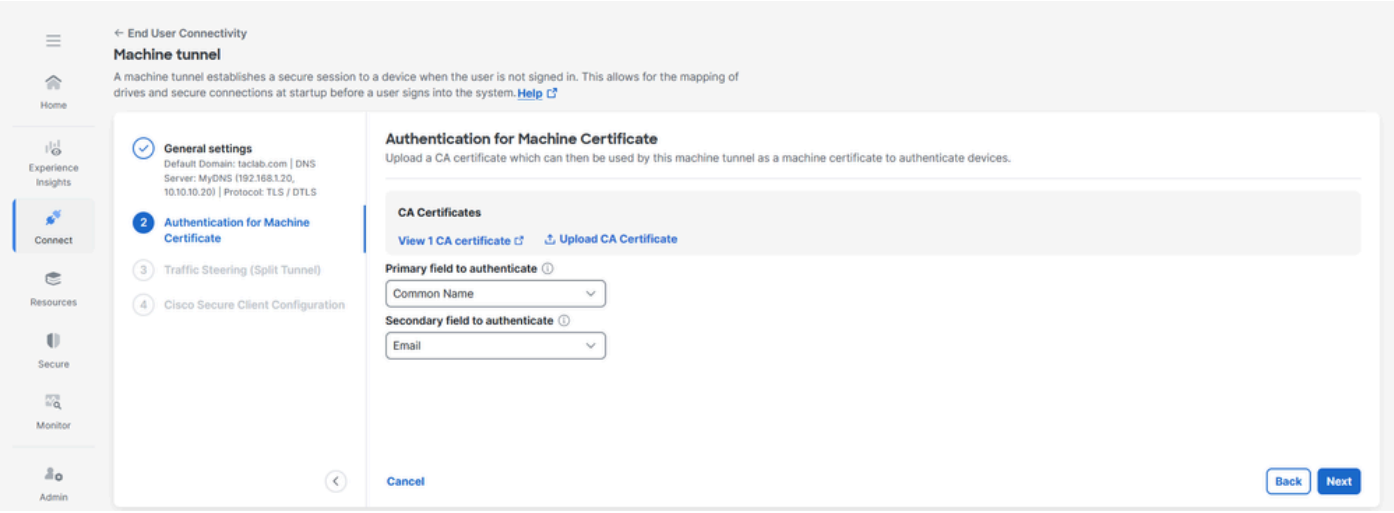
8.按一下「下一步」

步驟2 — 電腦證書的身份驗證

機器隧道對終端使用者是透明的，在使用者發起VPN會話時自動斷開。對於要在沒有使用者互動的情況下建立此隧道，將使用基於證書的身份驗證。

1. 從清單中選擇CA證書，或按一下「上傳CA證書」

2.選擇基於證書的身份驗證欄位。有關詳細資訊，請參閱基於證書的身份驗證欄位



3.按一下「下一步」

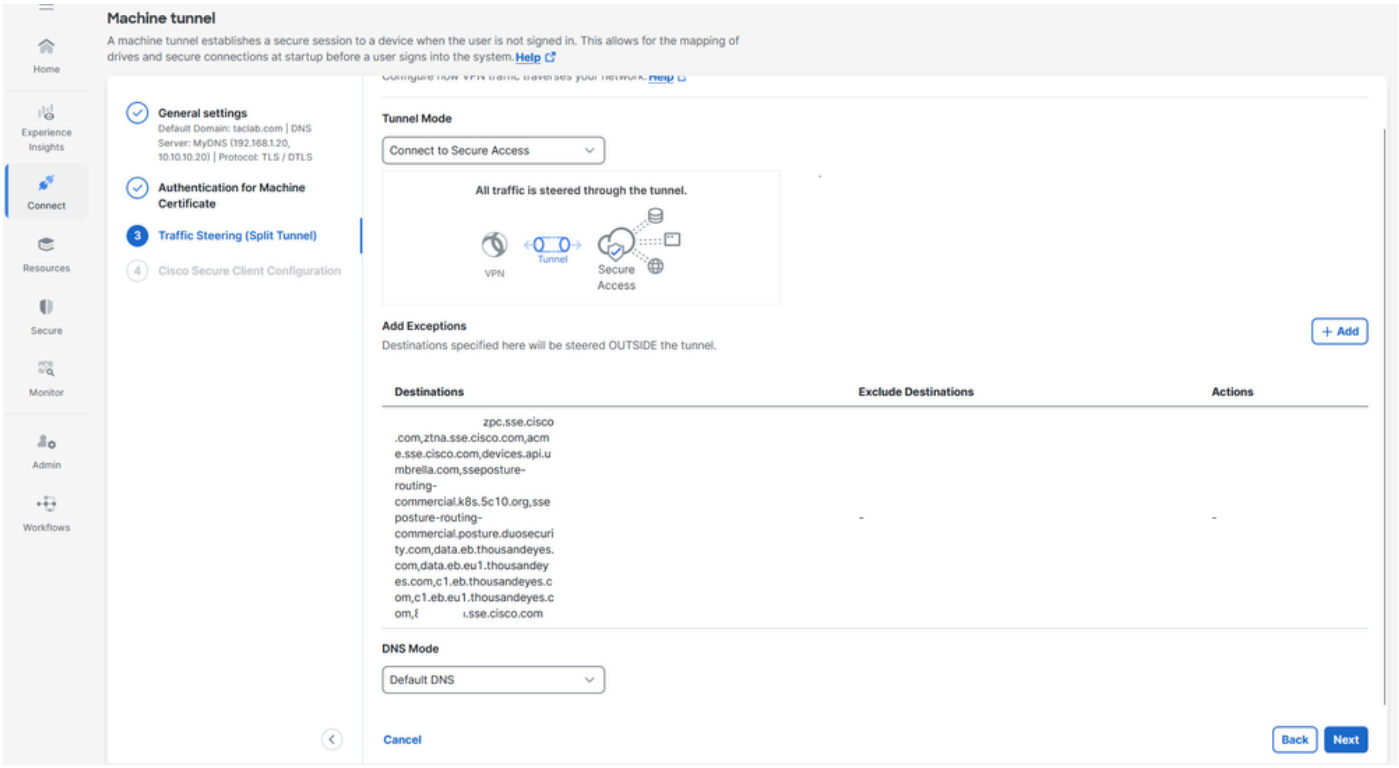
第3步 — 流量引導（拆分隧道）

對於Traffic Steering(Split Tunnel)，您可以配置一個機器隧道以維護與Secure Access的完整隧道連線，或將其配置為僅在必要時使用拆分隧道連線來引導流量通過VPN。有關詳細資訊，請參閱 Machine Tunnel traffic steering

1.選擇隧道模式

2.根據隧道模式的選擇，您可以新增例外

3.選擇DNS模式

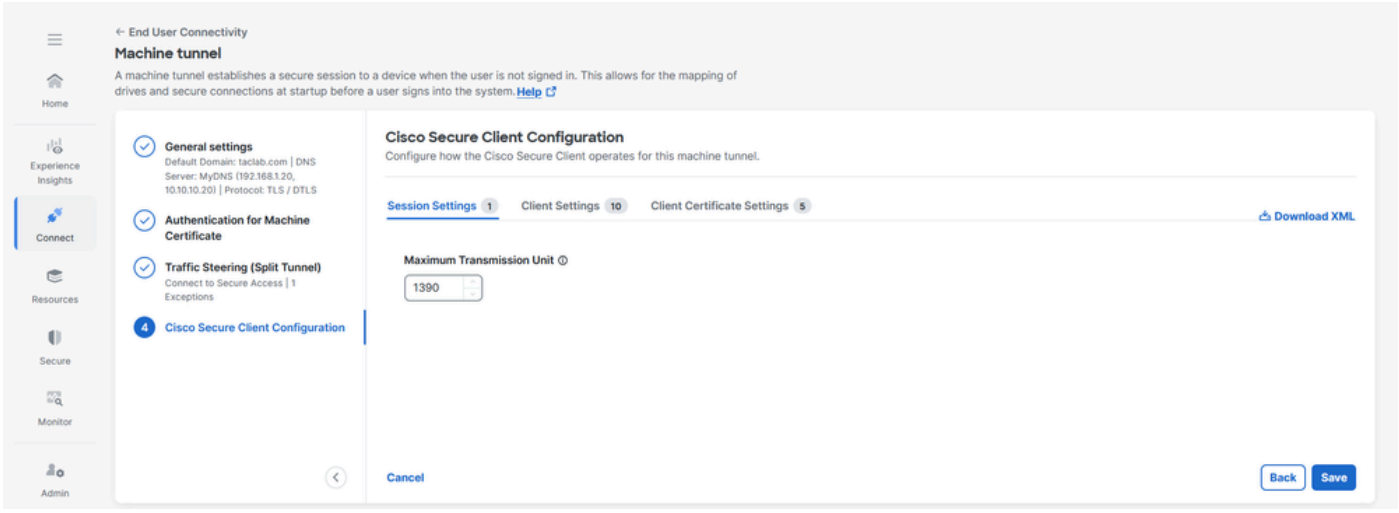


4.按一下「下一步」

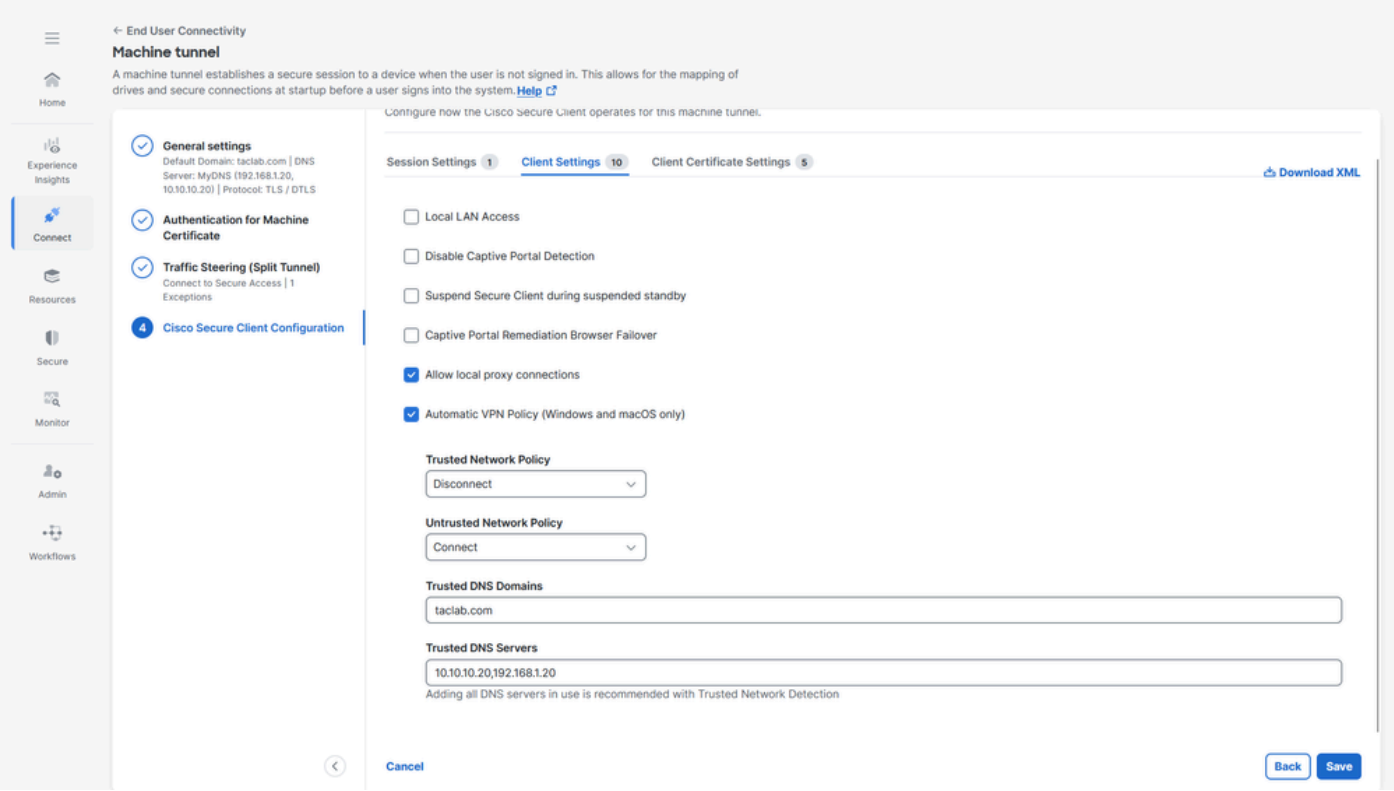
第4步 — 思科安全客戶端配置

您可以根據特定VPN電腦隧道的需求修改Cisco Secure Client設定的子集。有關詳細資訊，請參閱[安全客戶端配置]

1.驗證最大傳輸單元，這是在VPN通道中可傳送且無需分段的最大封包大小



2. 客戶端設定，請參閱[電腦隧道客戶端設定]以獲取詳細資訊



3.客戶端證書設定，相應地選擇選項

a. Windows證書儲存區覆蓋 — 允許管理員指示Secure Client使用Windows電腦（本地系統）證書儲存中的證書進行客戶端證書身份驗證。

b. 自動憑證選擇 — 在安全閘道上設定多個憑證驗證時

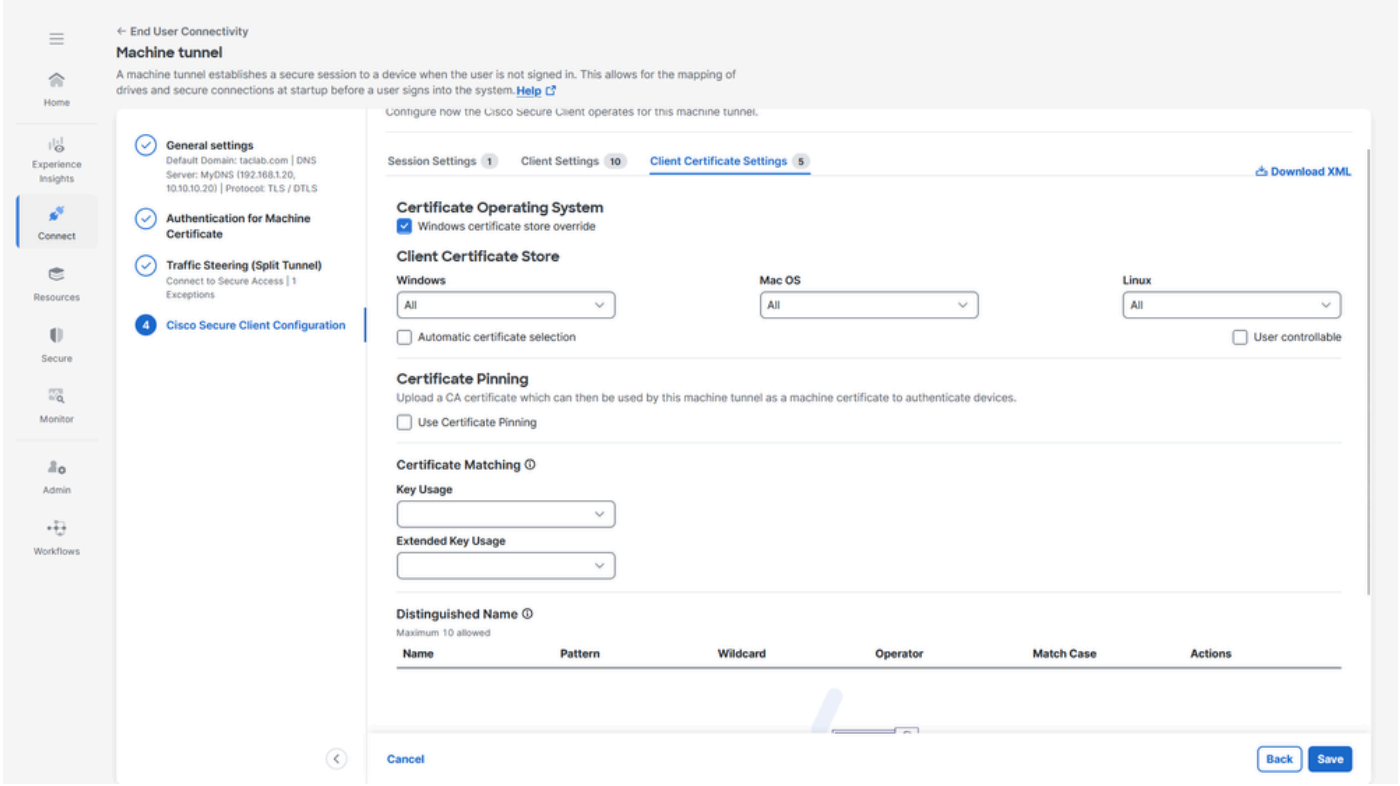
c. Certificate Pinning - CA證書，電腦隧道可將其用作對裝置進行身份驗證的電腦證書

d.證書匹配 — 如果未指定證書匹配條件，思科安全客戶端將應用證書匹配規則

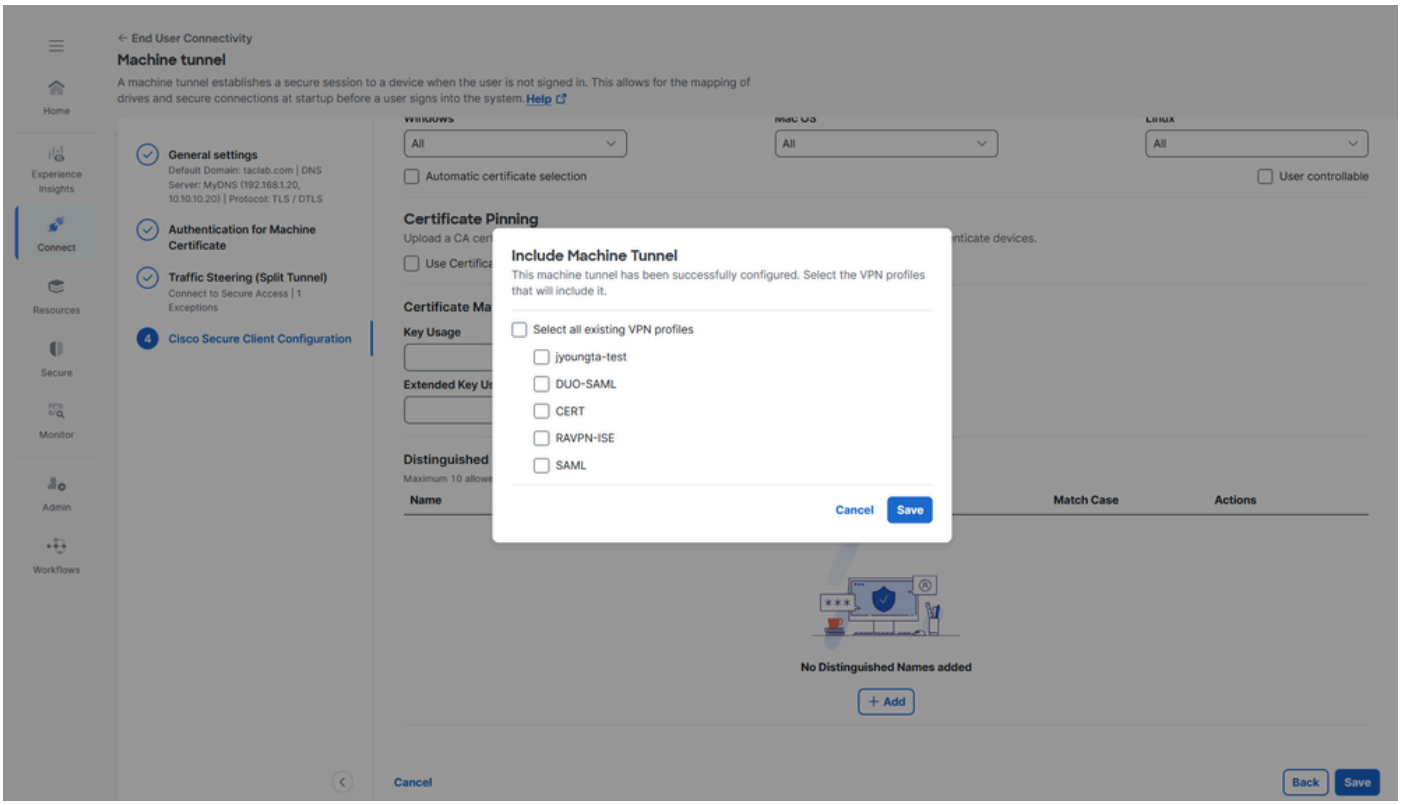
i.金鑰用法： 數位簽章

二。擴展金鑰用法：使用者端驗證

e.Distinguished Name — 在選擇可接受的客戶端證書時指定完全匹配條件的唯一判別名(DN)。新增多個可分辨名稱時，會根據所有條目檢查每個證書，並且所有條目必須匹配。

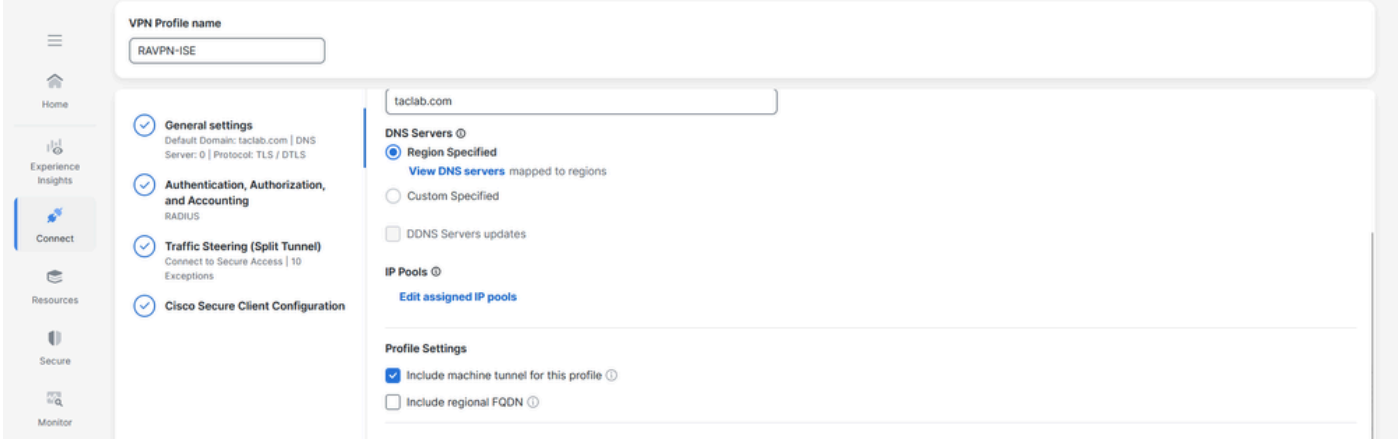


4.將電腦隧道配置檔案分配給使用者VPN配置檔案，按一下Save，然後選擇用於選擇使用者VPN配置檔案的選項



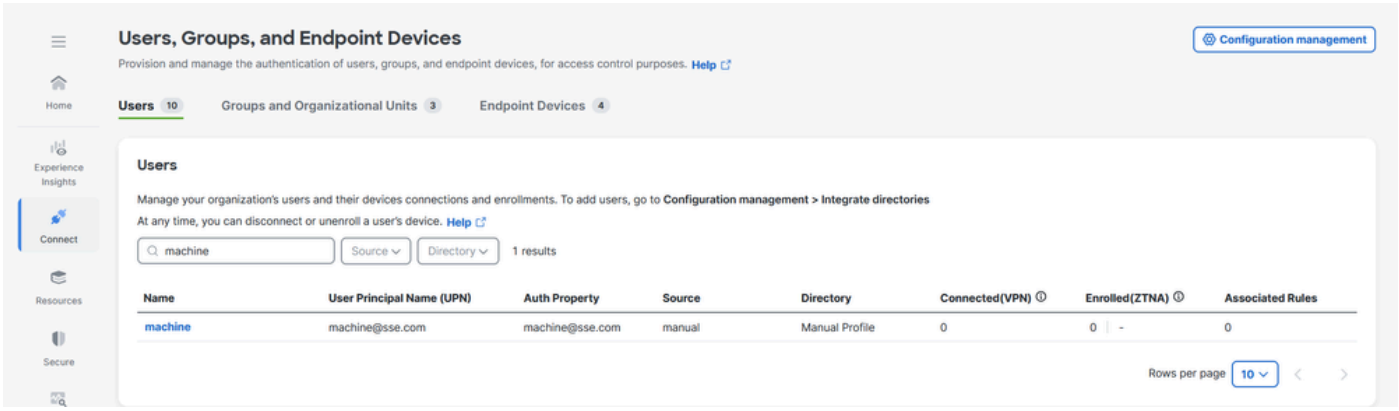
5.按一下Save

6.驗證電腦隧道配置檔案是否附加到使用者VPN配置檔案



步驟5 — 驗證machine@sse.com使用者是否位於思科安全存取中

1.導航至Connect > Users， Groups and Endpoint Devices > Users



2. 如果machine@sse.com使用者未手動顯示匯入。有關詳細資訊，請參閱手動匯入使用者和組

第6步 — 為machine@sse.com生成CA簽名證書

1.生成證書簽名請求

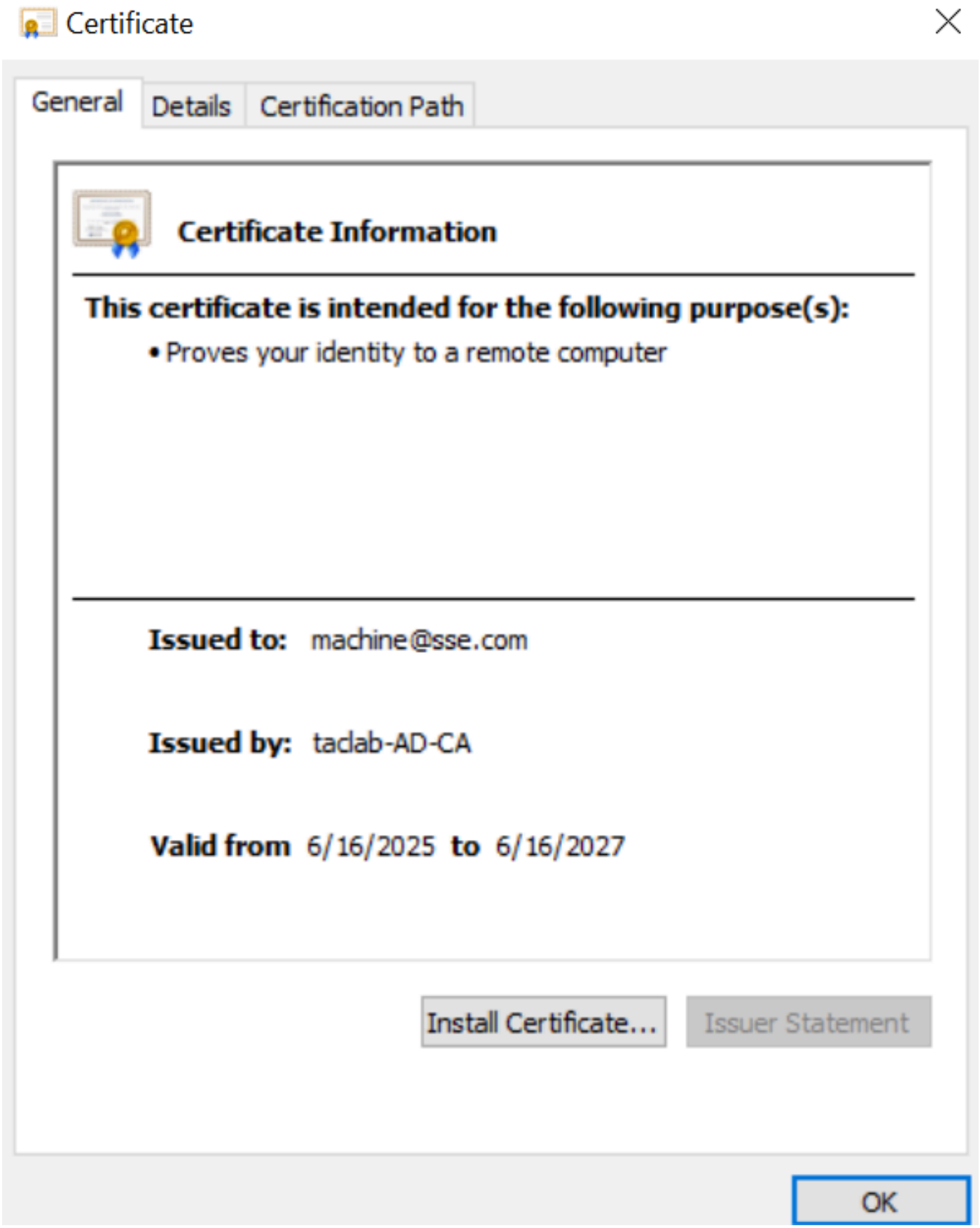
a.我們可以使用任何線上CSR產生器軟體CSR產生器或openssl CLI

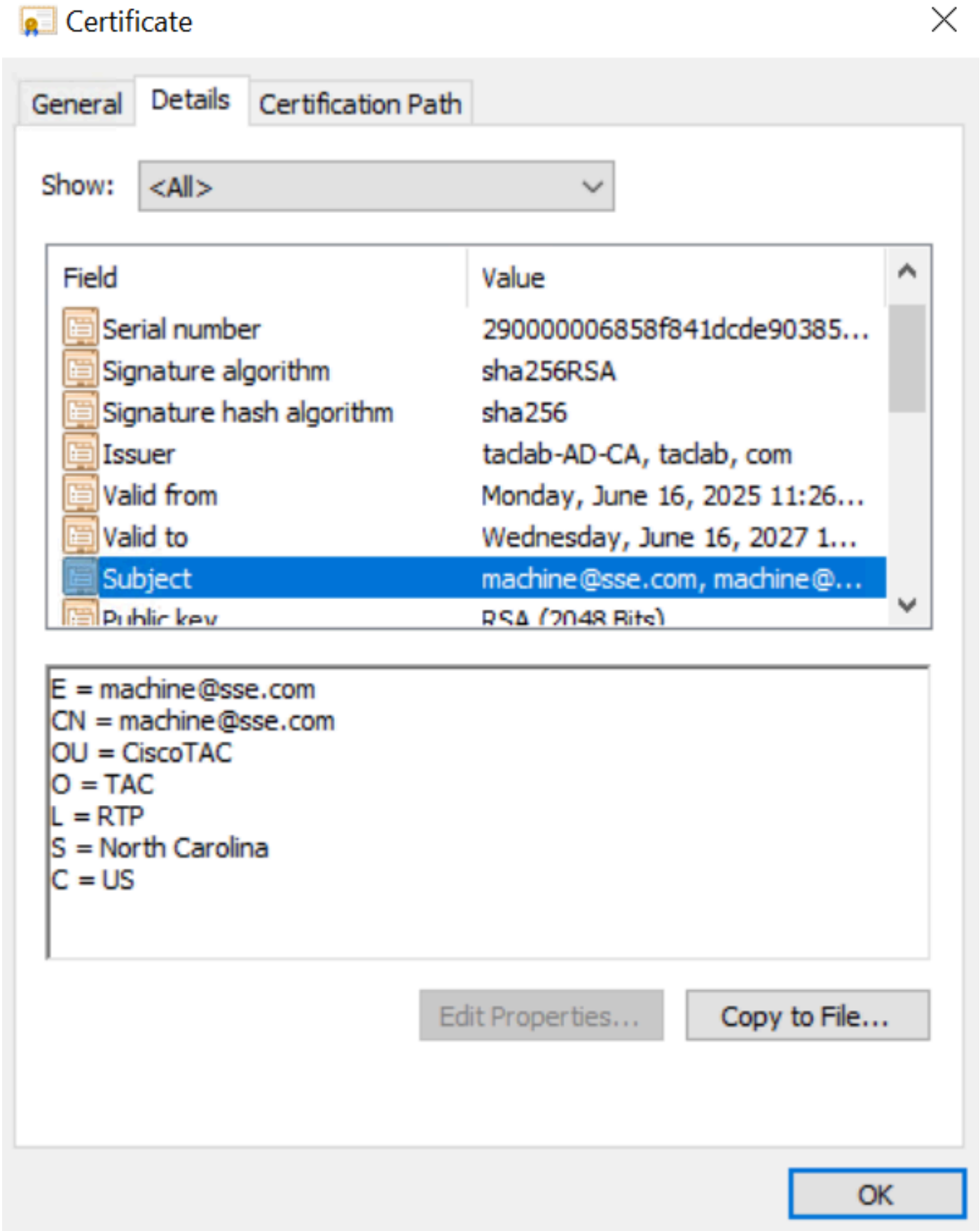
```
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr
```

```
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.複製CSR並生成電腦證書


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



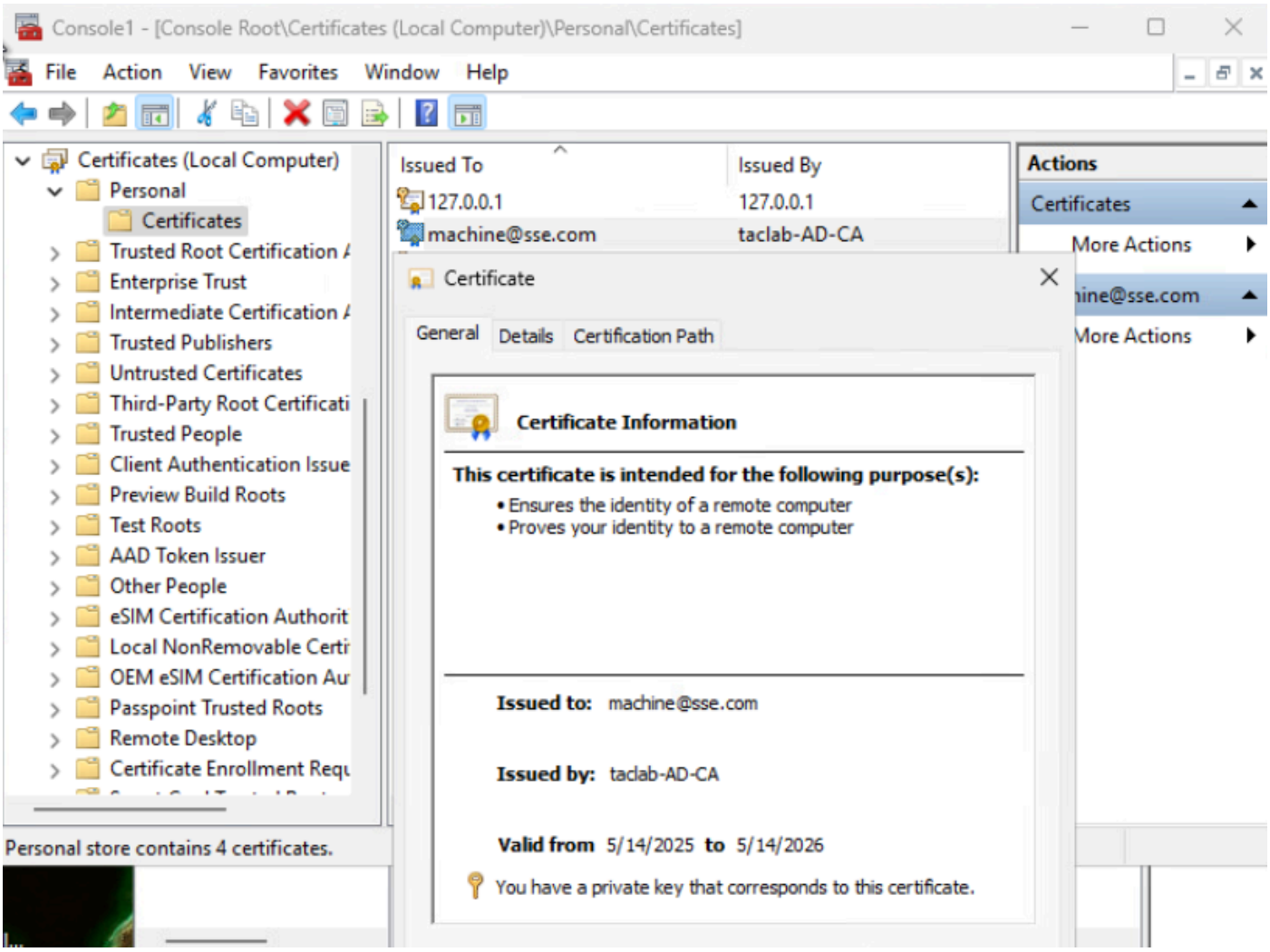
3.使用分別在前面的步驟（步驟1和2）中生成的金鑰和證書將電腦證書轉換為PKCS12格式

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#
```

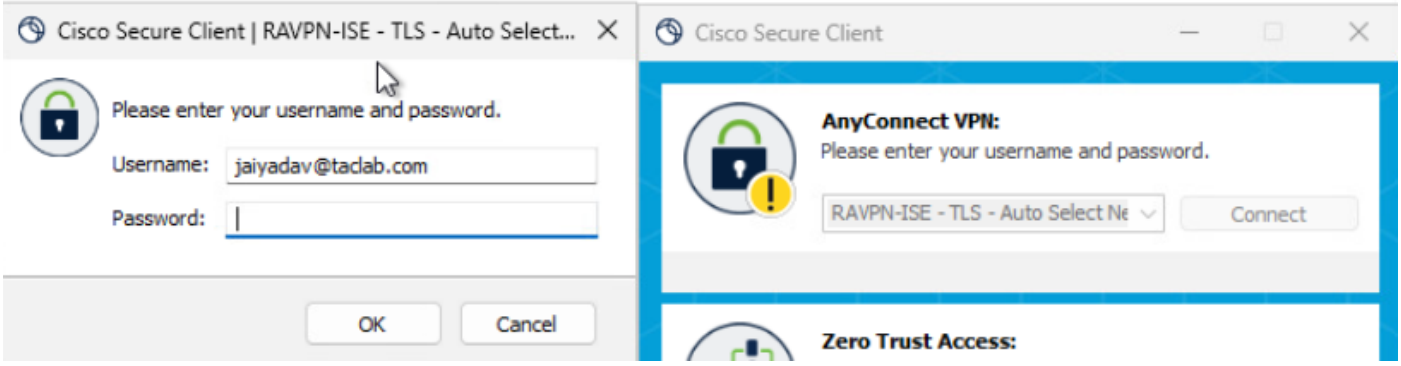
步驟7 — 在測試電腦上匯入電腦證書

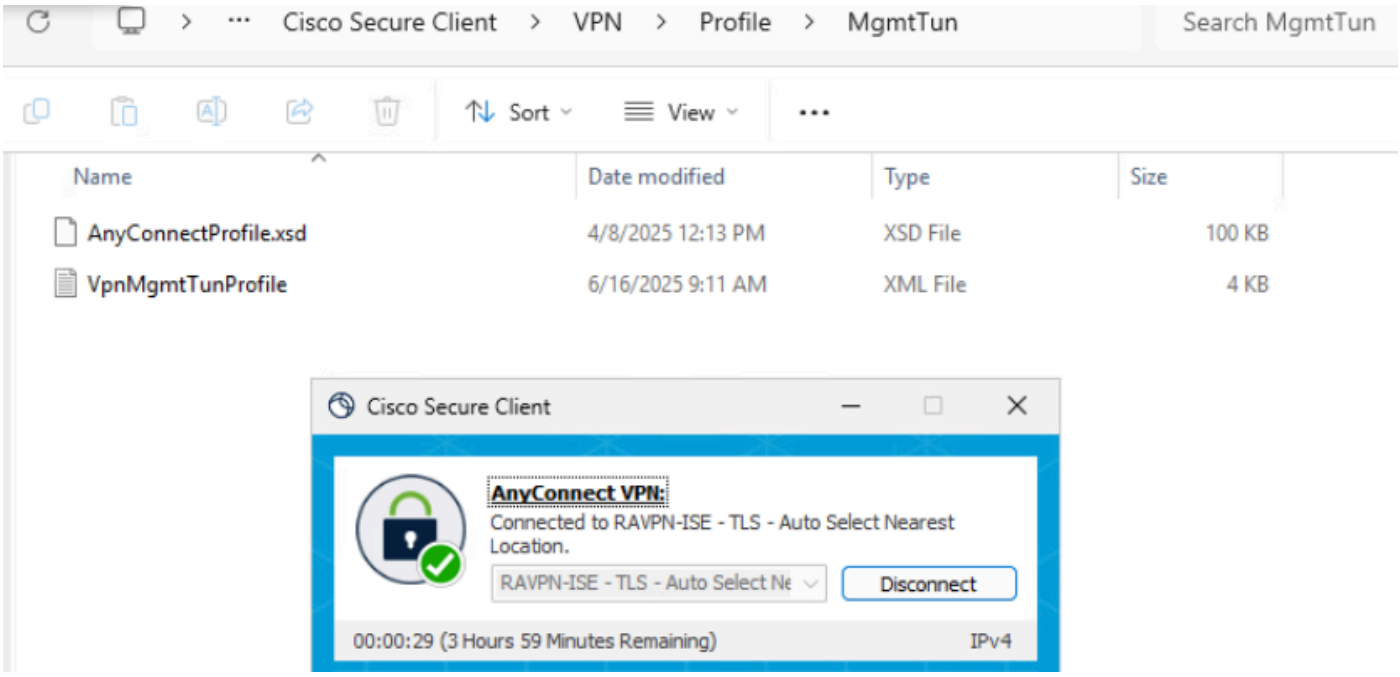
a.在本地或電腦儲存下匯入PKCS12電腦證書



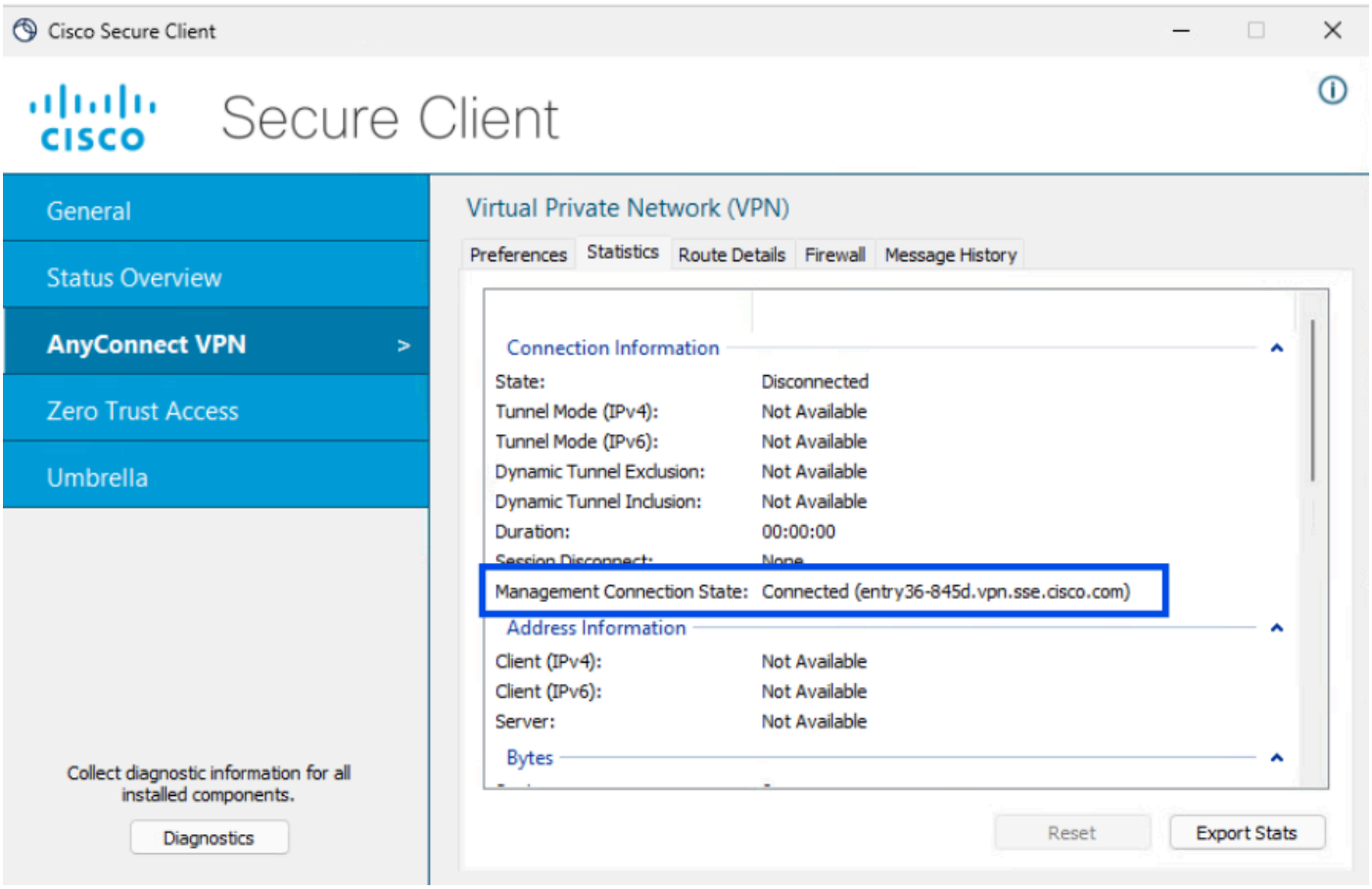
步驟8 — 連線到機器隧道

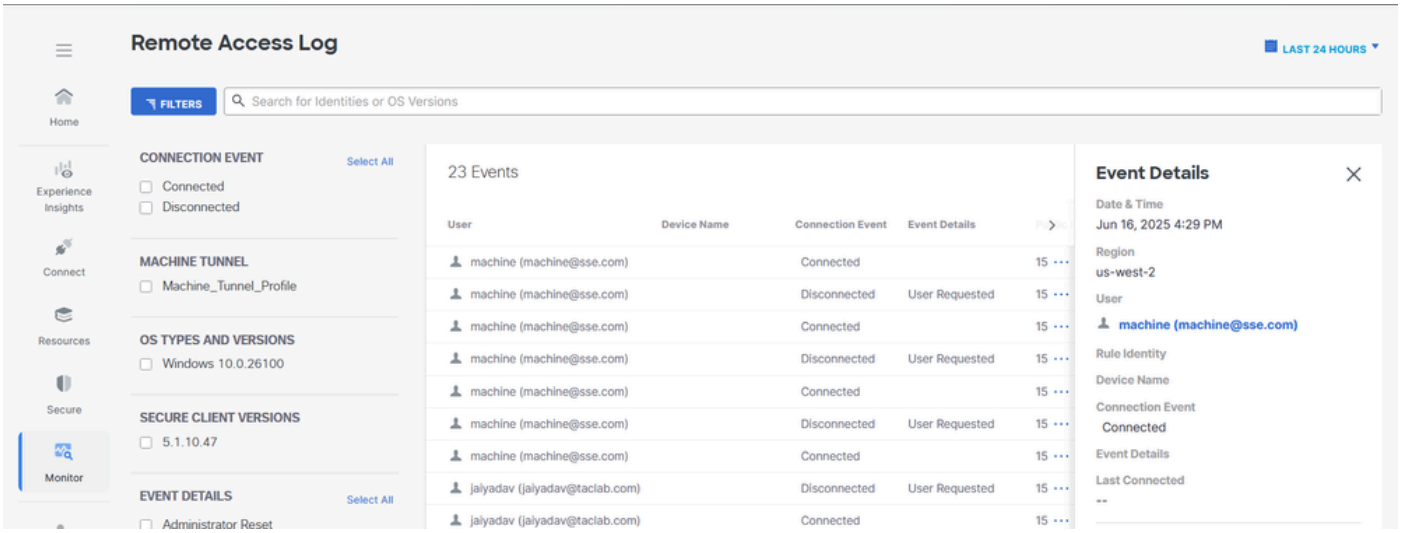
a.連線到使用者隧道，這將觸發要下載的電腦xml配置檔案。




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.驗證電腦隧道連線


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



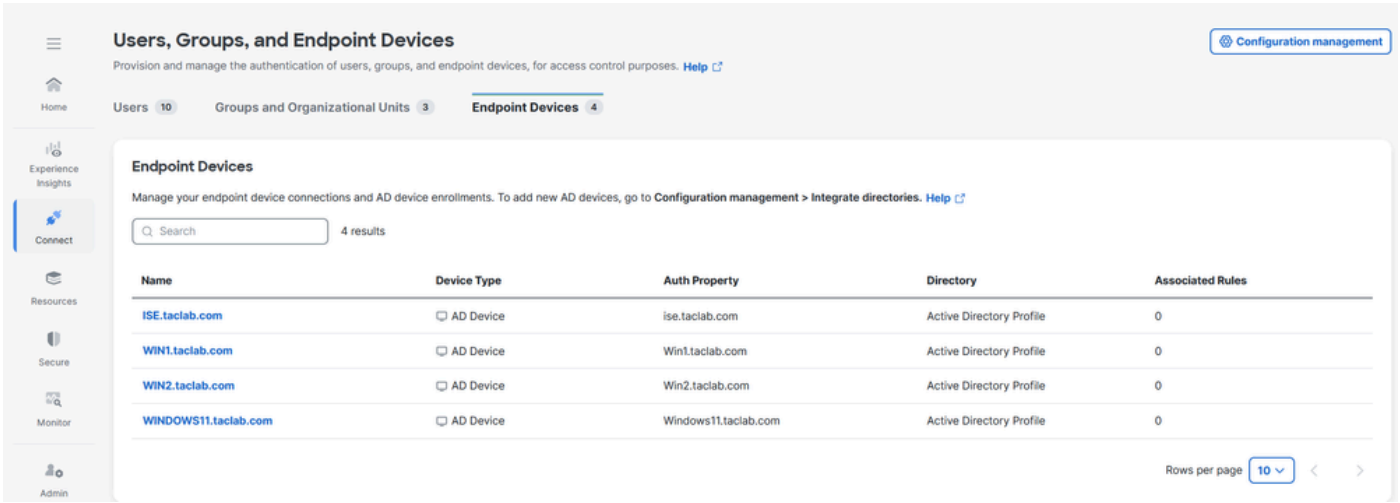
方法2 — 使用終端證書配置電腦隧道

在這種情況下，Primary欄位要進行身份驗證，請選擇包含裝置名稱（電腦名稱）的證書欄位。 安全訪問使用裝置名稱作為機器隧道識別符號。電腦名稱的格式必須與所選裝置識別符號的格式匹配

執行步驟1到步驟4進行電腦隧道配置

第5步 — 配置AD聯結器，使其能夠在Cisco Secure Access上匯入終端。

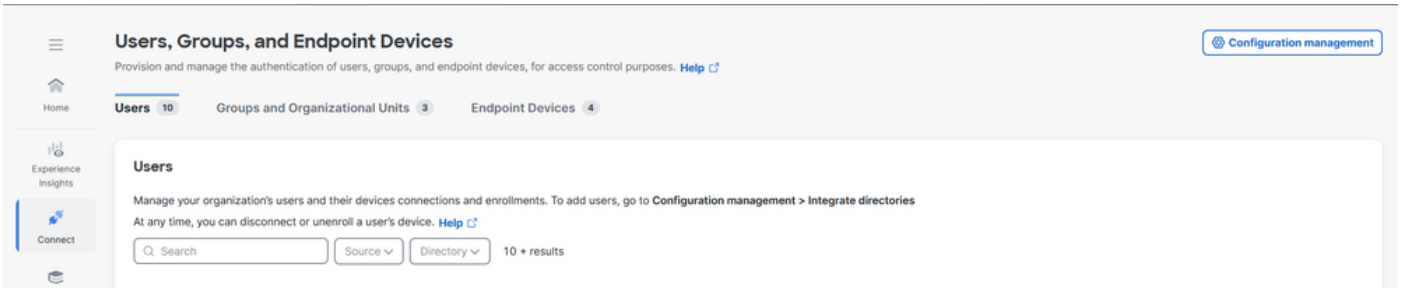
有關詳細資訊，請參閱永久的Active Directory整合



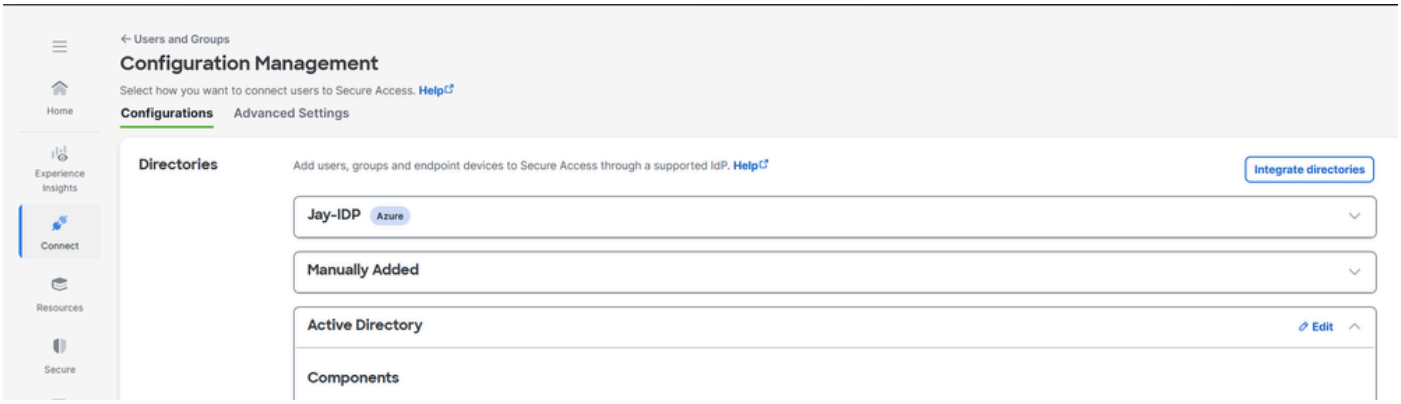
第6步 — 配置終端裝置身份驗證

1.導航至Connect > Users， Groups and Endpoint Devices。

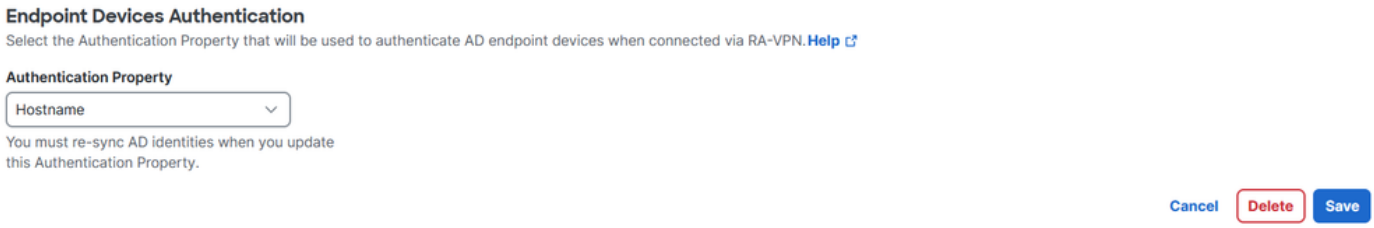
2.按一下Configuration management



3. 在Configurations下，編輯Active Directory



4.將Endpoint Devices Authentication Property設定為主機名



5.按一下Save並在安裝其AD聯結器的伺服器上重新啟動AD聯結器服務

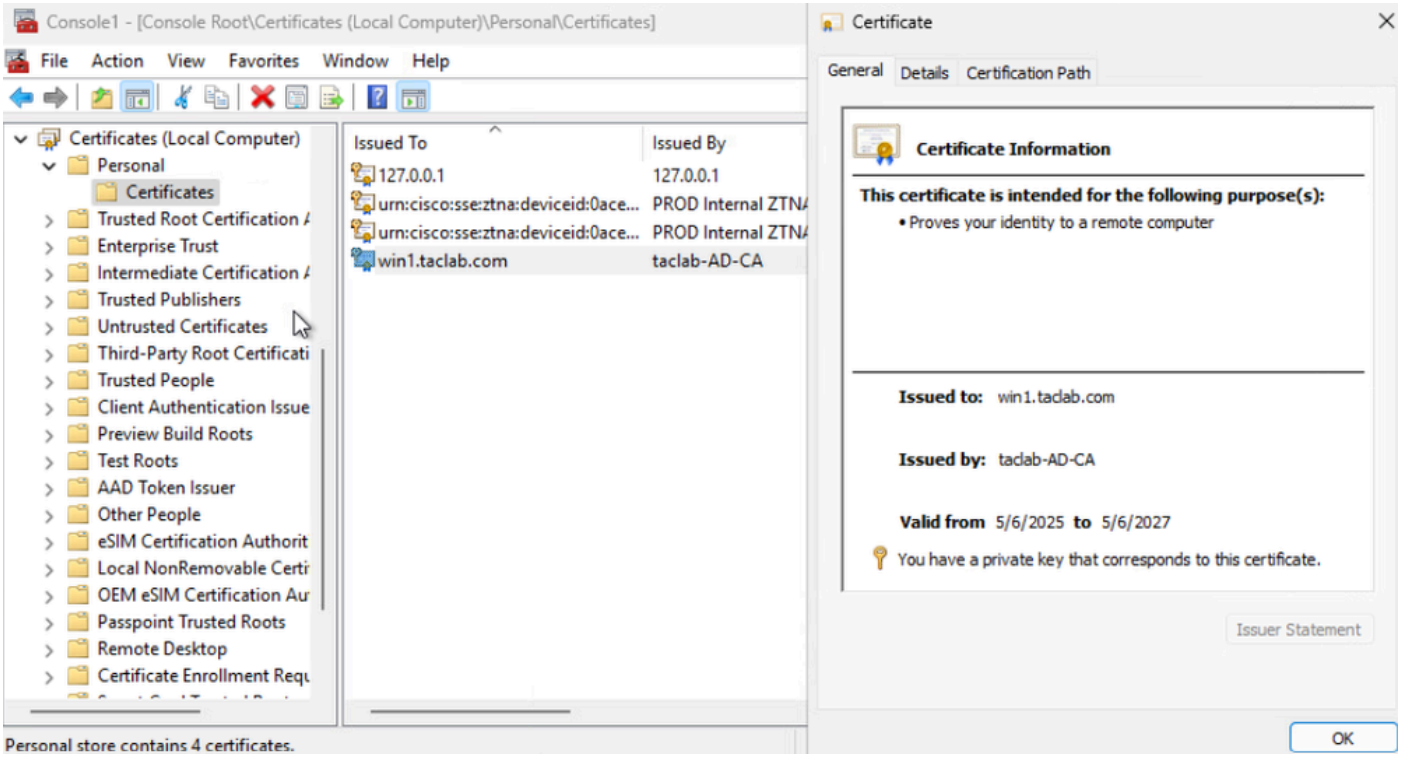
第7步 — 生成和匯入終端證書

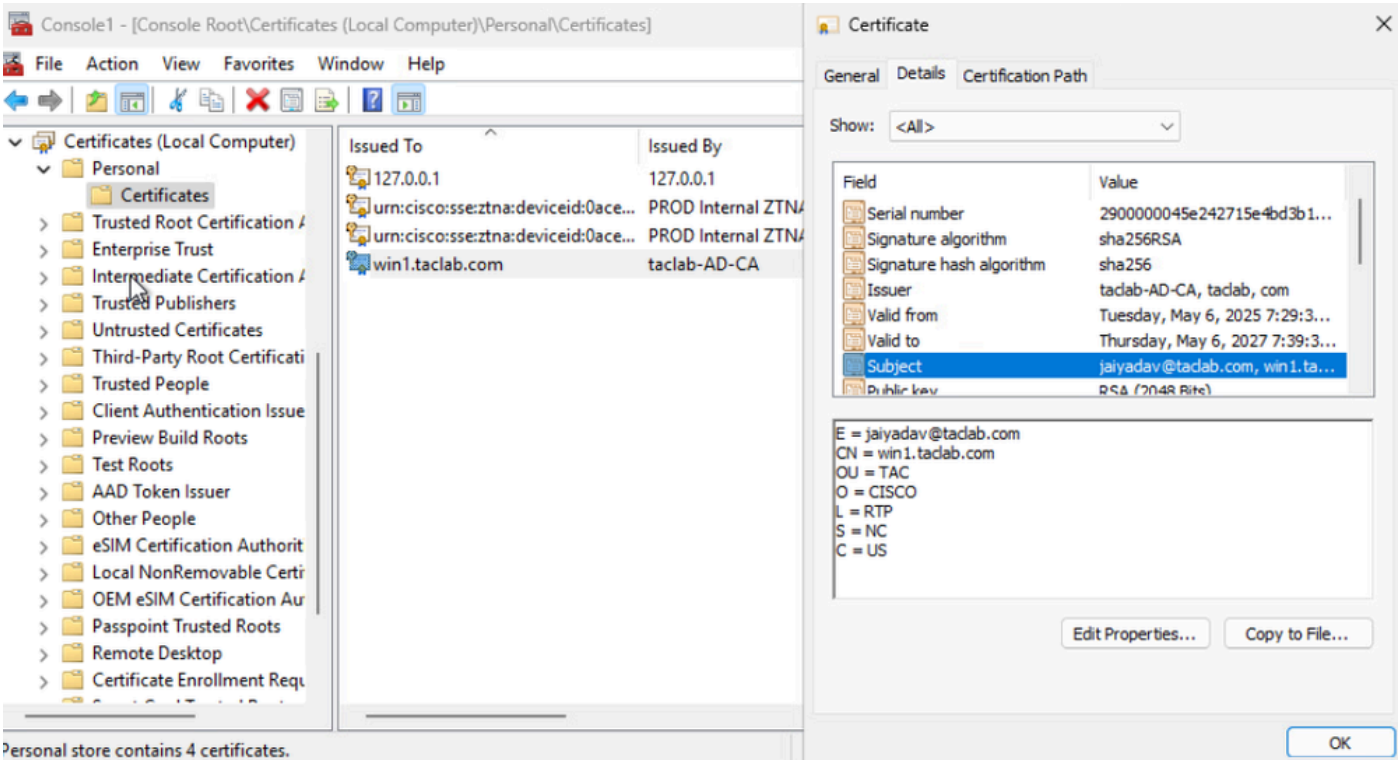
a.生成CSR，開啟CSR生成器或OpenSSL工具

b.從CA生成終端證書

c.將.cert檔案轉換為PKCS12格式

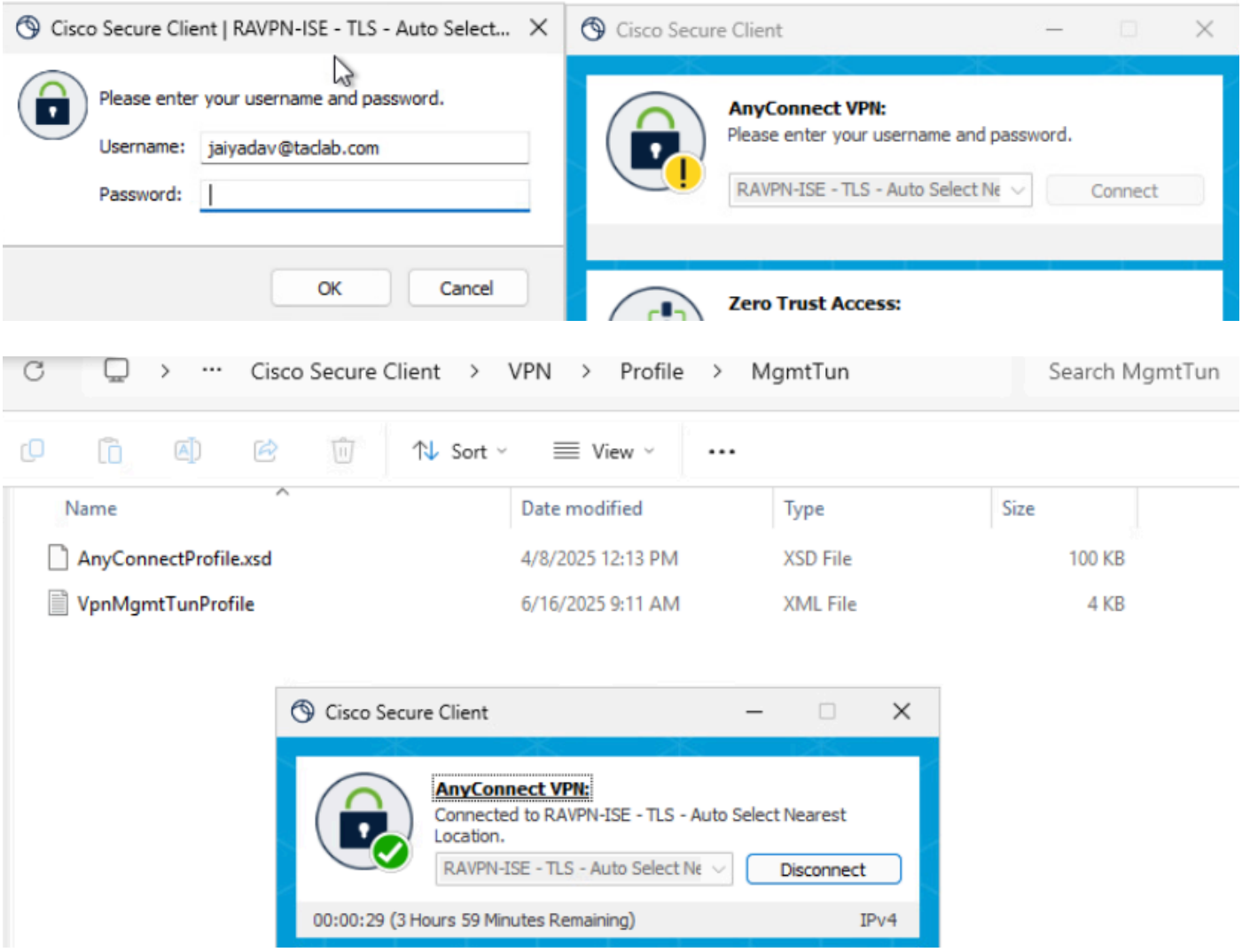
d.在端點證書儲存中匯入PKCS12證書



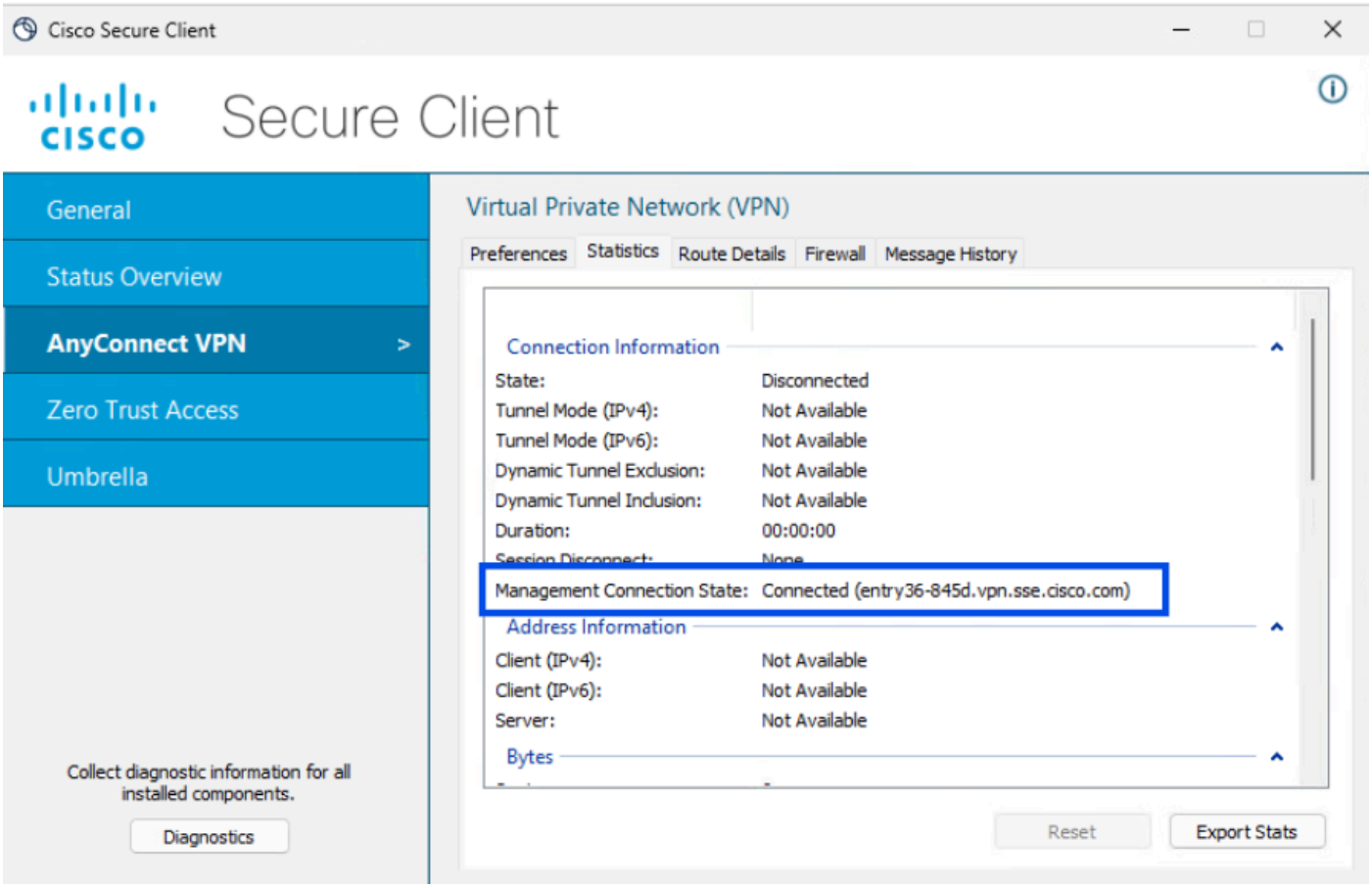


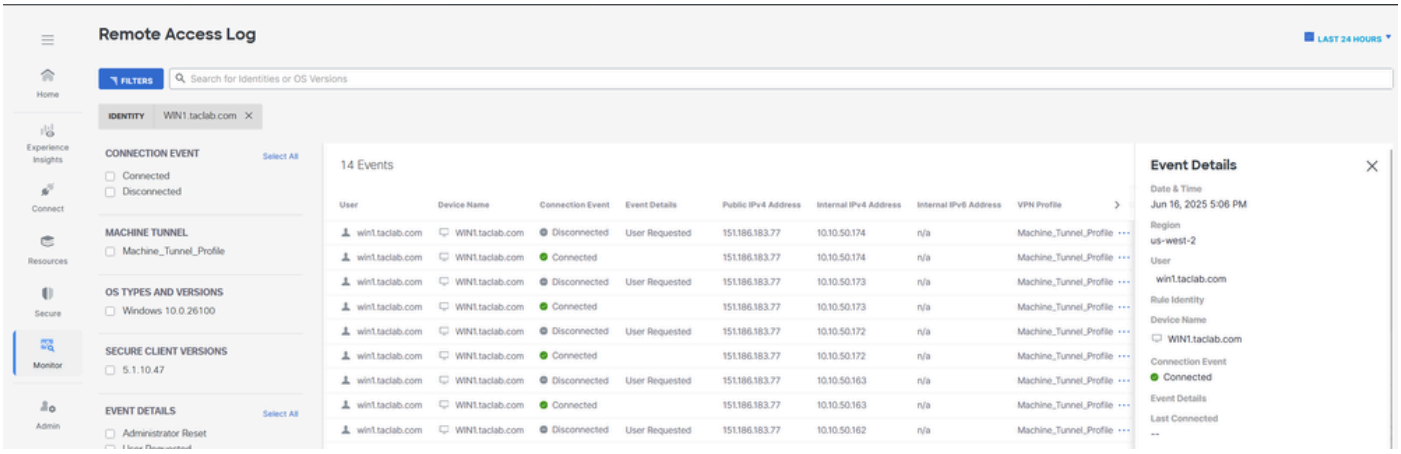
步驟8 — 連線到機器隧道

a.連線到使用者隧道，它會觸發電腦隧道xml配置檔案的下載


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.驗證電腦隧道連線





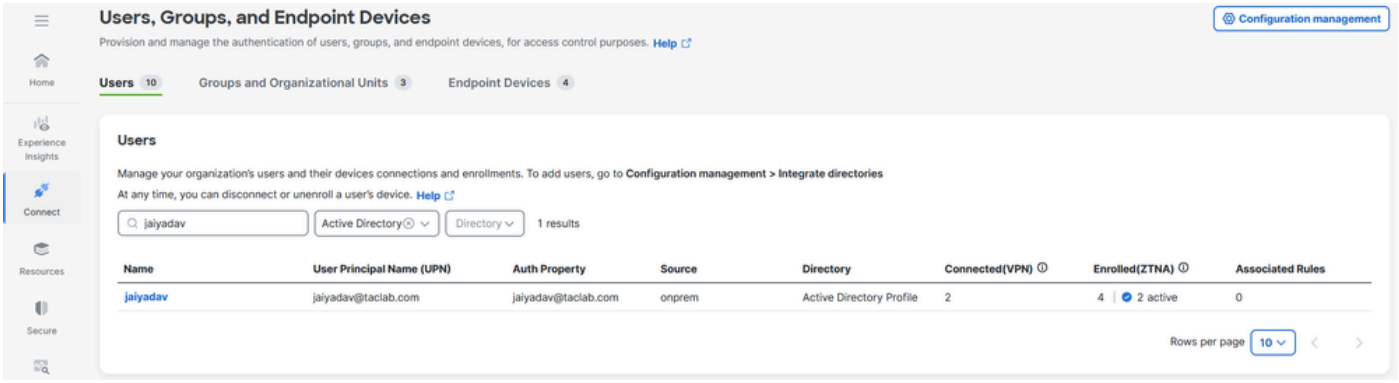
方法3 — 使用使用者證書配置電腦隧道

在這種情況下，Primary欄位要進行身份驗證，請選擇包含使用者電子郵件或UPN的證書欄位。Secure Access使用電子郵件或UPN作為機器隧道識別符號。電子郵件或UPN的格式必須與所選裝置識別符號的格式匹配

執行步驟1至4進行電腦隧道配置

第5步 — 配置AD聯結器，使其能夠匯入Cisco Secure Access上的使用者。

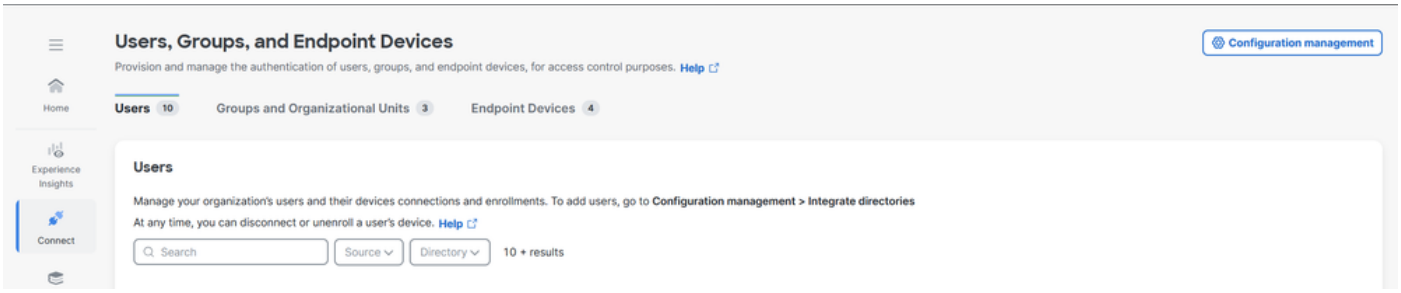
有關詳細資訊，請參閱永久的Active Directory整合



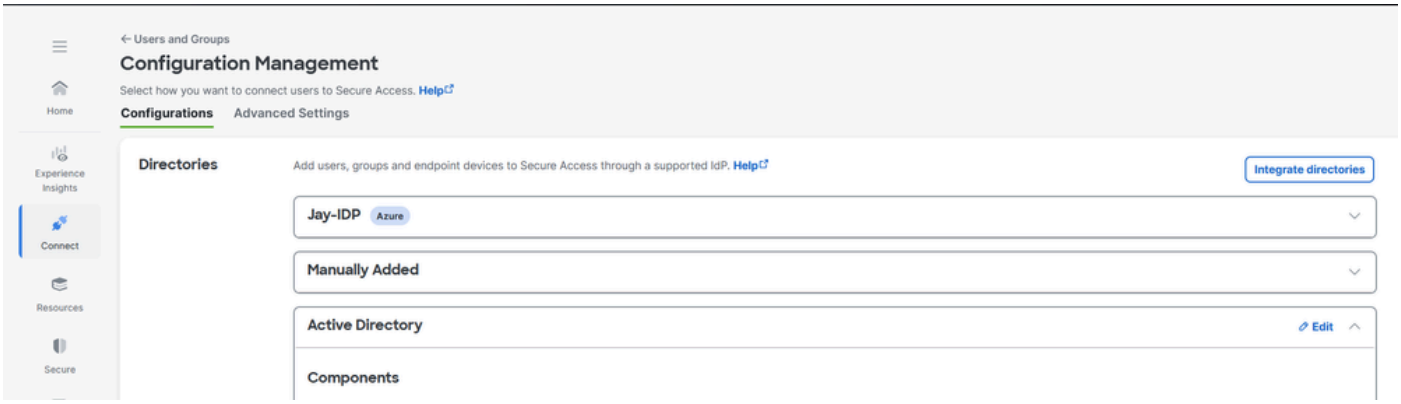
步驟6 — 配置使用者身份驗證

1.導航至Connect > Users， Groups and Endpoint Devices。

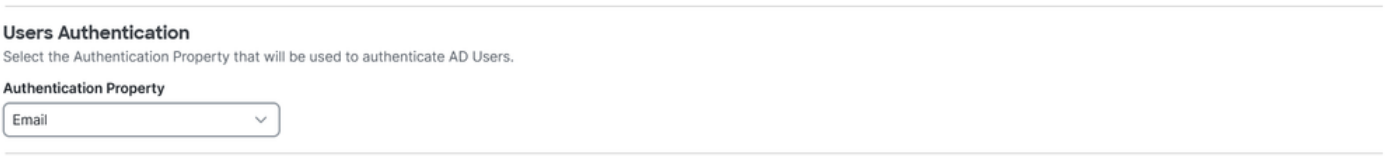
2.按一下Configuration management



3. 在Configurations下，編輯Active Directory



4.將「使用者身份驗證」屬性設定為「電子郵件」



5.按一下Save並在安裝其AD聯結器的伺服器上重新啟動AD聯結器服務

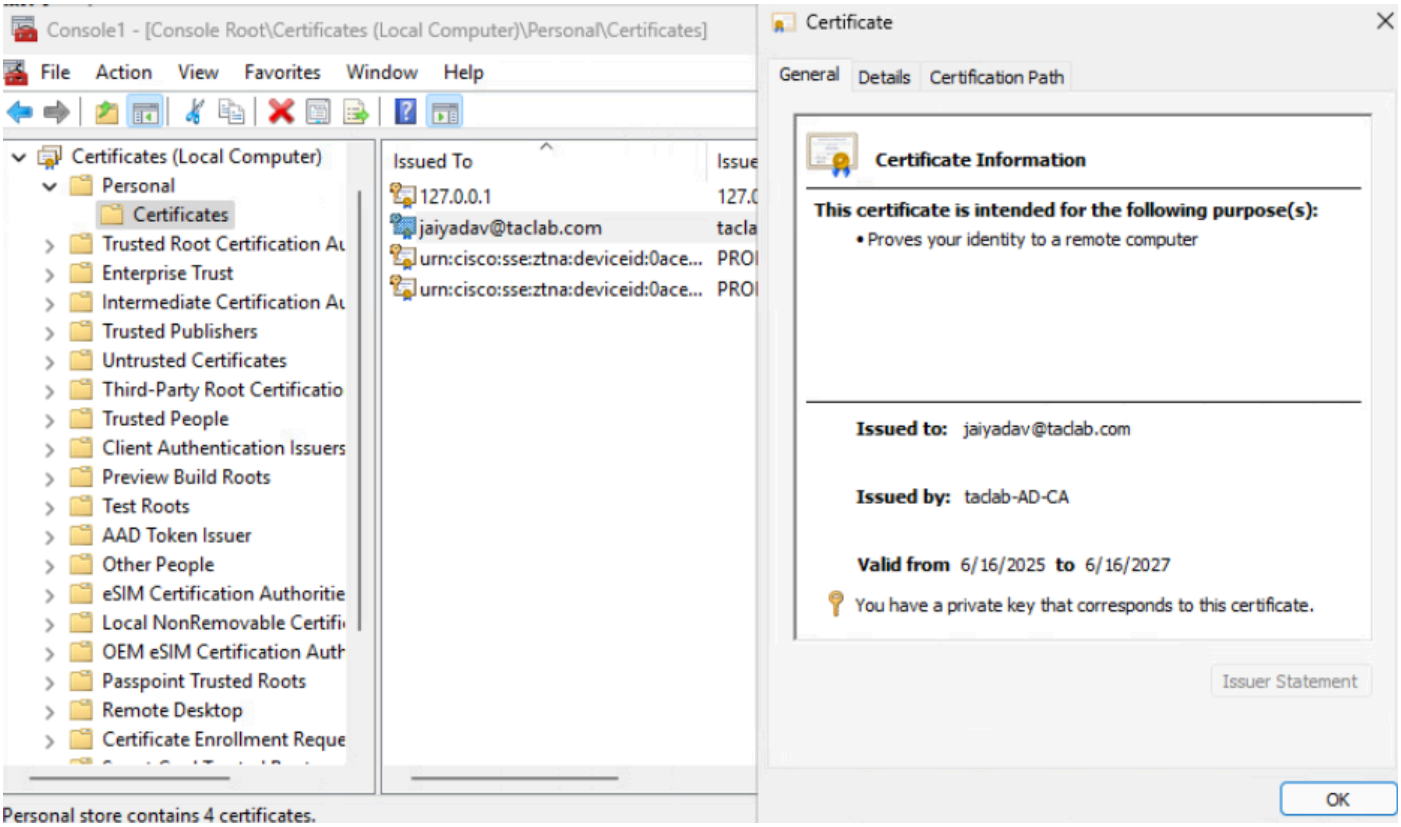
第7步 — 生成和匯入終端證書

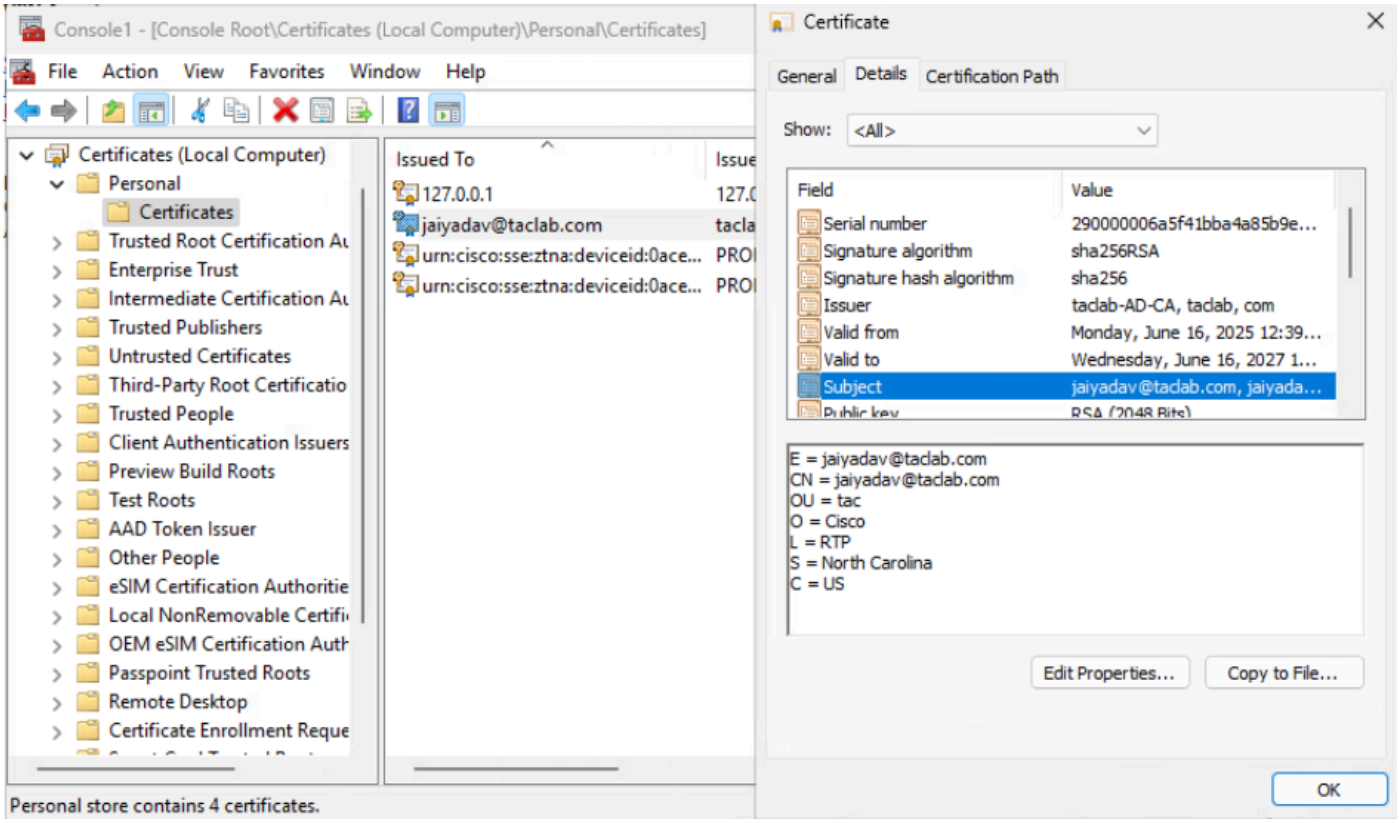
a.生成CSR，開啟CSR生成器或OpenSSL工具

b.從CA生成終端證書

c.將.cert檔案轉換為PKCS12格式

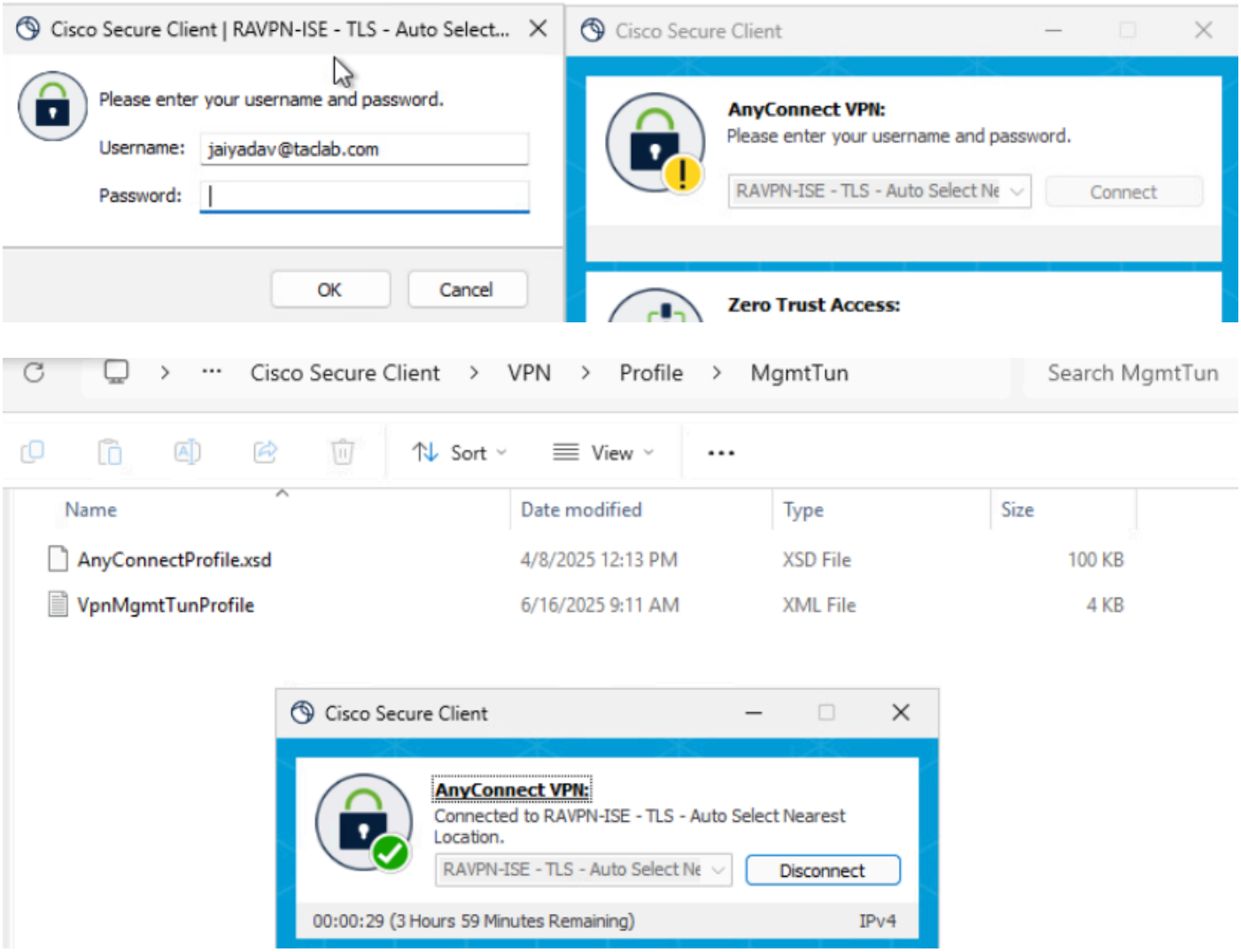
d.在端點證書儲存中匯入PKCS12證書



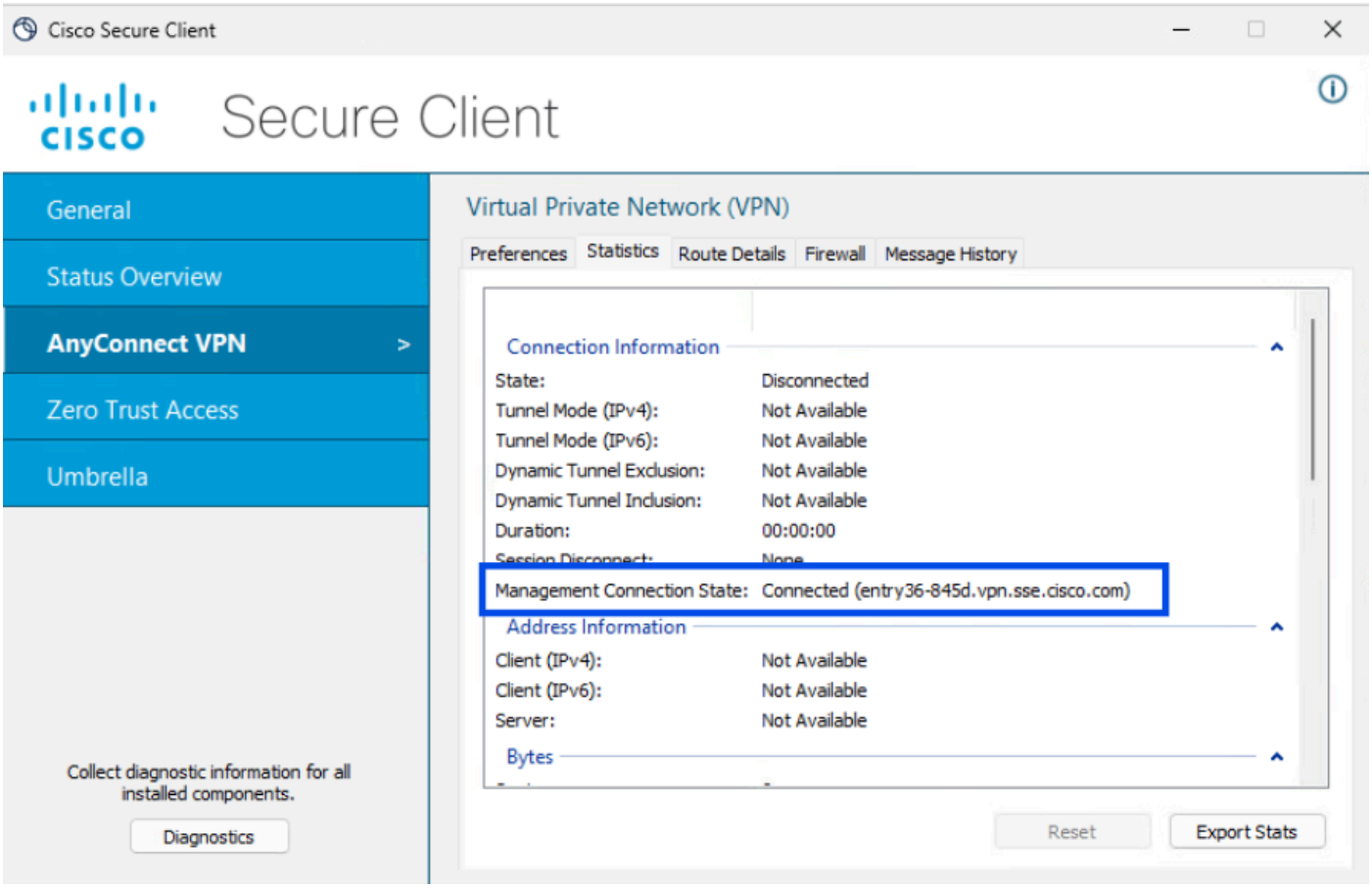


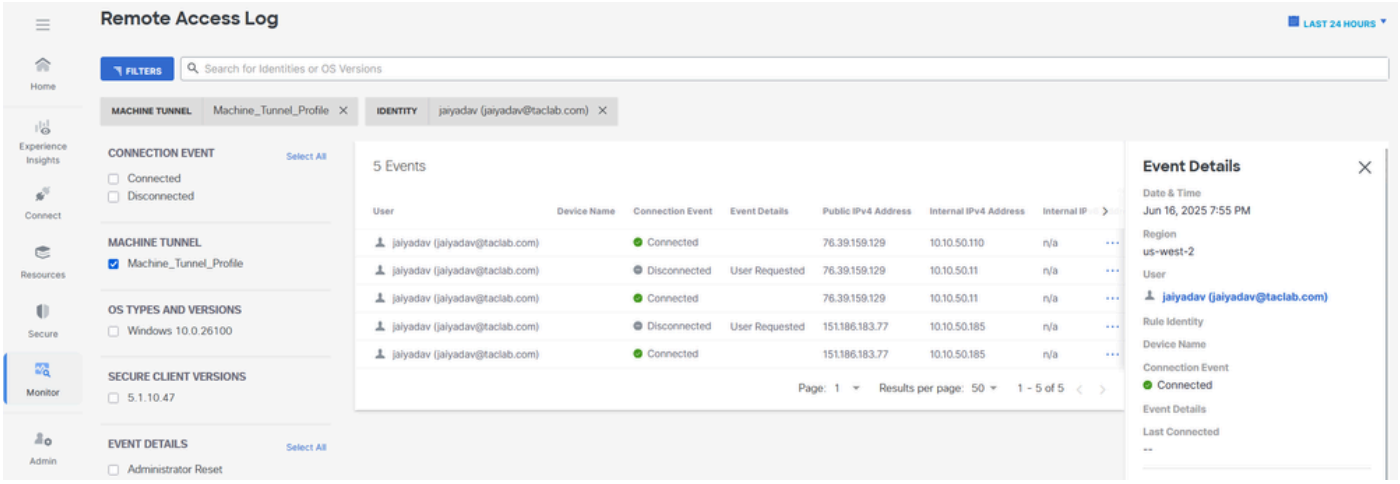
步驟8 — 連線到機器隧道

a.連線到使用者隧道，它會觸發電腦隧道xml配置檔案的下載



b.驗證電腦隧道連線





疑難排解

提取DART捆綁包，開啟AnyConnectVPN日誌並分析錯誤消息

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。