Cisco Secure Access에서 머신 터널 구성

목차

소개

네트워크 다이어그램

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

배경 정보

- 시스템 터널 작업

제한 사항

구성

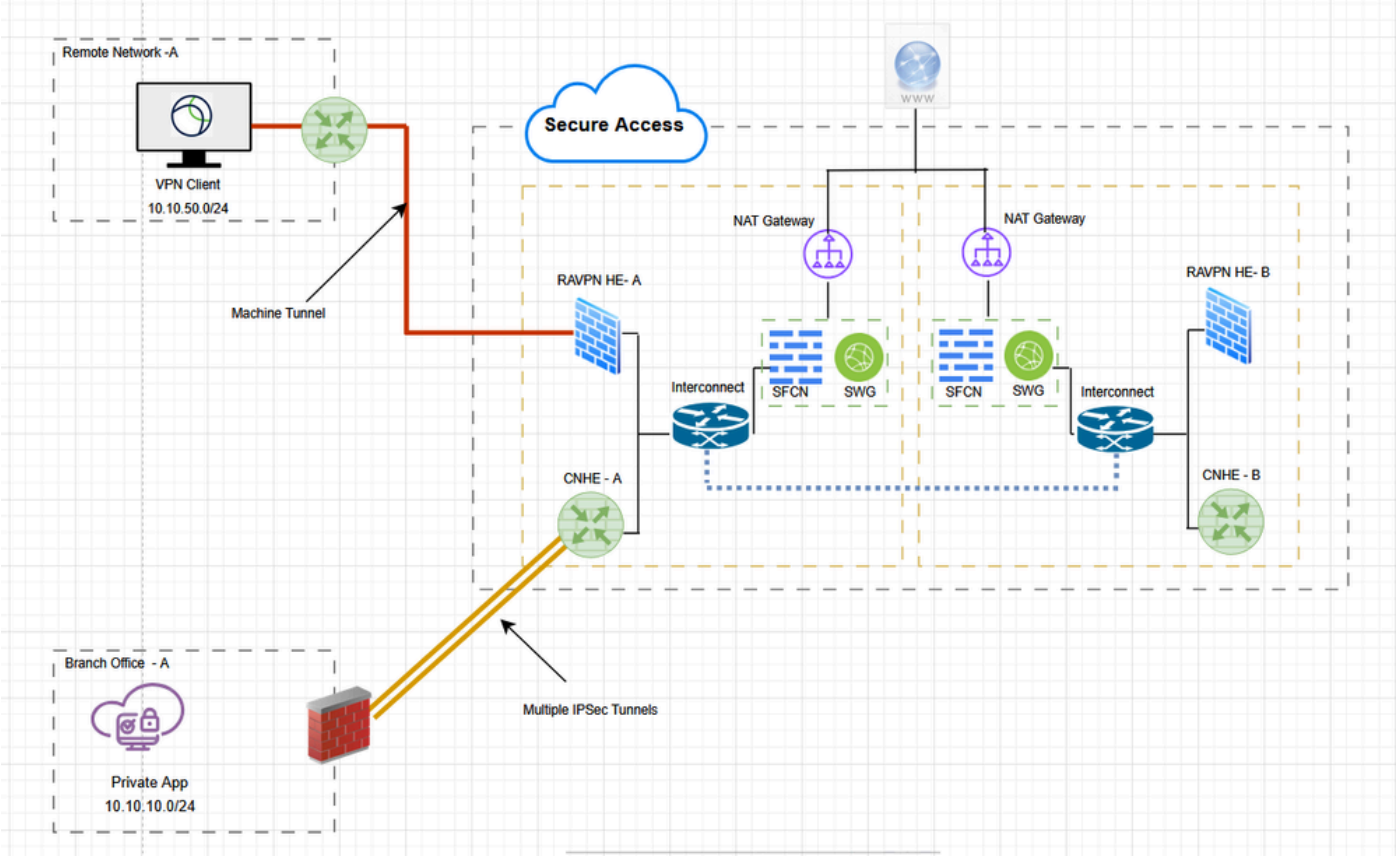
- 방법 1 - 사용자 machine@sse.com으로 머신 터널 구성
- 1단계 - 일반 설정
- 2단계 - 머신 인증서에 대한 인증
- 3단계 - 트래픽 조정(스플릿 터널)
- 4단계 - Cisco Secure Client 컨피그레이션
- 5단계 - machine@sse.comuser이 Cisco Secure Access에 있는지 확인합니다.
- 6단계 - machine@sse.com에 대한 CA 서명 인증서 생성
- 7단계 - 테스트 시스템에서 머신 인증서 가져오기
- 8단계 - 머신 터널에 연결
- 방법 2 - 엔드포인트 인증서를 사용하여 머신 터널 구성
- 5단계 - Cisco Secure Access에서 엔드포인트를 가져올 수 있도록 AD 커넥터를 구성합니다.
- 6단계 - 엔드포인트 디바이스 인증 구성
- 7단계 - 엔드포인트 인증서 생성 및 가져오기
- 8단계 - 머신 터널에 연결
- 방법 3 - 사용자 인증서를 사용하여 머신 터널 구성
- 5단계 - Cisco Secure Access에서 사용자를 가져올 수 있도록 AD 커넥터를 구성합니다.
- 6단계 - 사용자 인증 구성
- 7단계 - 엔드포인트 인증서 생성 및 가져오기
- 8단계 - 머신 터널에 연결

문제 해결

소개

이 문서에서는 보안 액세스를 VPN 게이트웨이로 구성하고 VPN 머신 터널을 통한 보안 클라이언트의 연결을 수락하는 방법에 대해 설명합니다.

네트워크 다이어그램



사전 요구 사항

- 보안 액세스에서 전체 관리자 역할
- Cisco Secure Access에 구성된 하나 이상의 사용자 VPN 프로파일
- Cisco Secure Access의 사용자 IP 풀

요구 사항

다음 항목에 대해 알고 있는 것이 좋습니다.

- 509 인증서
- OpenSSL

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 보안 액세스
- Cisco Secure Client 5.1.10
- Windows 11
- Windows Server 2019 - CA

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Secure Access VPN 머신 터널은 최종 사용자가 VPN 연결을 설정하는 경우뿐만 아니라 클라이언트 시스템의 전원이 켜질 때마다 기업 네트워크에 대한 연결을 보장합니다. 사무실 외부 엔드포인트, 특히 사용자가 VPN을 통해 사무실 네트워크에 연결하는 빈도가 낮은 디바이스에 대해 패치 관리를 수행할 수 있습니다. 회사 네트워크 연결이 필요한 엔드포인트 OS 로그인 스크립트도 이 기능을 활용할 수 있습니다. 사용자 상호 작용 없이 이 터널을 생성하려면 인증서 기반 인증이 사용됩니다.

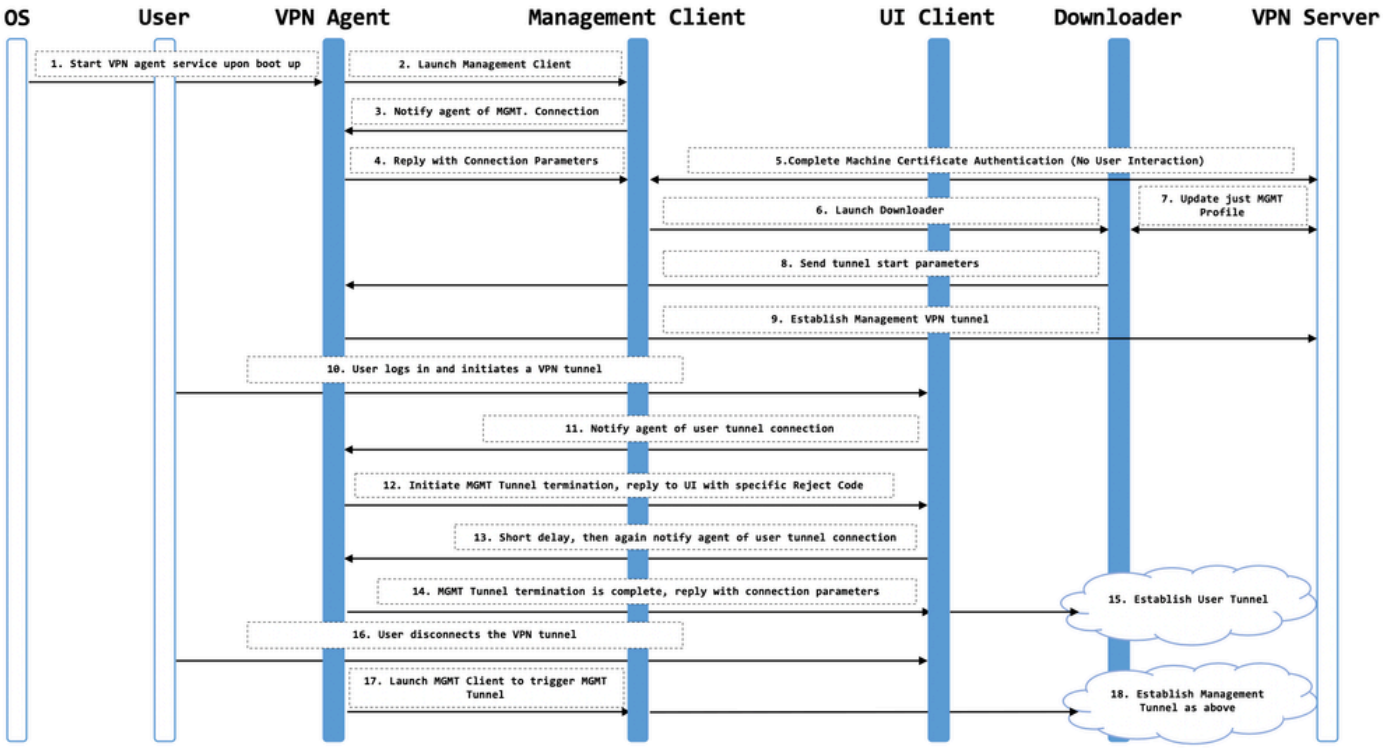
관리자는 Secure Access 머신 터널을 통해 사용자가 로그인하기 전에 사용자의 작업 없이 Cisco Secure Client를 연결할 수 있습니다. 보안 액세스 머신 터널은 엔드포인트가 오프프레미스에 있고 사용자가 시작한 VPN에서 연결이 끊어진 경우 트리거됩니다. Secure Access VPN 머신 터널은 엔드 유저에게 투명하며 사용자가 VPN을 시작하면 자동으로 연결이 끊깁니다.

시스템 터널 작업

Secure Client VPN Agent 서비스는 시스템 부팅 시 자동으로 시작됩니다. 보안 클라이언트 VPN 에이전트는 VPN 프로필을 사용하여 머신 터널 기능이 활성화되었음을 탐지합니다. 머신 터널 기능이 활성화된 경우 에이전트는 관리 클라이언트 애플리케이션을 실행하여 머신 터널 연결을 시작합니다. 관리 클라이언트 애플리케이션은 VPN 프로필의 호스트 항목을 사용하여 연결을 시작합니다. 그런 다음 VPN 터널이 평소처럼 설정되며 한 가지 예외가 있습니다. 시스템 터널은 사용자에게 투명하게 제공되므로 시스템 터널 연결 중에는 소프트웨어 업데이트가 수행되지 않습니다.

사용자는 보안 클라이언트를 통해 VPN 터널을 시작하며, 이는 머신 터널 종료를 트리거합니다. 머신 터널이 종료되면 사용자 터널 설정이 평소처럼 계속됩니다.

사용자가 VPN 터널의 연결을 끊으면 시스템 터널의 자동 재설정이 트리거됩니다.



제한 사항

- 사용자 상호 작용은 지원되지 않습니다.
- Windows(Machine Certificate Store)를 통한 인증서 기반 인증만 지원됩니다.
- 엄격한 서버 인증서 검사가 시행됩니다.
- 개인 프록시는 지원되지 않습니다.
- 공용 프록시가 지원되지 않습니다. ProxyNative 값은 기본 프록시 설정이 브라우저에서 검색되지 않는 플랫폼에서 지원됩니다.
- 보안 클라이언트 사용자 지정 스크립트는 지원되지 않습니다.

구성

방법 1 - 사용자 machine@sse.com으로 머신 터널 구성

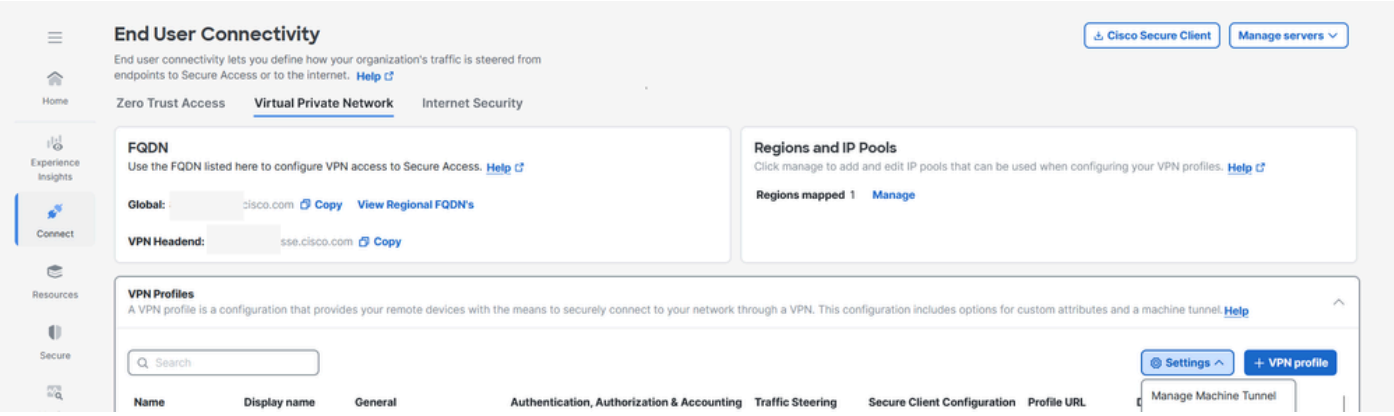
1단계 - 일반 설정

이 시스템 터널에서 사용하는 도메인 및 프로토콜을 포함하여 일반 설정을 구성합니다.

1. Connect(연결) > End User Connectivity(최종 사용자 연결) > Virtual Private Network(가상 사설망)로 이동합니다.

2. VPN Profiles(VPN 프로파일)로 이동하여 머신 터널에 대한 설정을 구성합니다.

   a. Settings(설정)를 클릭한 다음 드롭다운에서 Manage Machine Tunnel(머신 터널 관리)을 선택합니다.



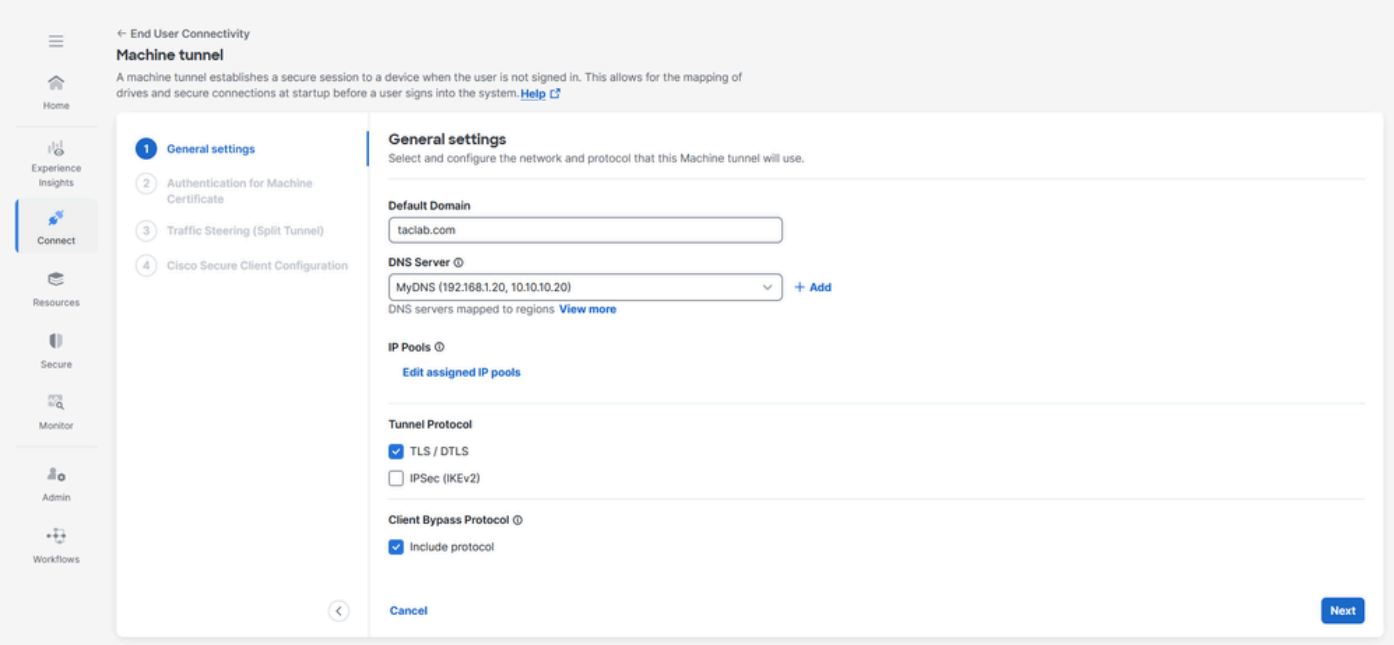
3. Default Domain(기본 도메인)을 입력합니다.
4. Manage Regions and IP Pools(영역 및 IP 풀 관리) 페이지를 통해 매핑된 DNS 서버가 기본 서버로 설정됩니다. 기본 DNS 서버를 수락하거나, 드롭다운에서 다른 DNS 서버를 선택하거나, + Add를 클릭하여 새 DNS 서버 쌍을 추가할 수 있습니다. 다른 DNS 서버를 선택하거나 새 DNS 서버를 추가하면 이 기본 서버를 덮어씁니다.
5. IP Pools(IP 풀) 드롭다운에서 리전당 하나의 IP 풀을 선택합니다. VPN 프로필에는 유효한 컨피그레이션을 위해 각 영역에 하나 이상의 IP 풀이 할당되어야 합니다.
6. 이 컴퓨터 터널에서 사용하는 터널 프로토콜을 선택합니다.
   - TLS/DTLS

- IPSec(IKEv2)
  하나 이상의 프로토콜을 선택해야 합니다.

7. 선택적으로, Include protocol을 선택하여 클라이언트 우회 프로토콜을 적용합니다.

a. IP 프로토콜에 대해 Client Bypass Protocol이 활성화되어 있고 해당 프로토콜에 대해 주소 풀이 구성되지 않은 경우(즉, ASA에서 해당 프로토콜에 대한 IP 주소가 클라이언트에 할당되지 않은 경우), 해당 프로토콜을 사용하는 IP 트래픽은 VPN 터널을 통해 전송되지 않습니다. 그것은 터널 밖으로 보내져야 한다.

b. Client Bypass Protocol(클라이언트 우회 프로토콜)이 비활성화되고 해당 프로토콜에 대해 주소 풀이 구성되지 않은 경우, VPN 터널이 설정되면 클라이언트는 해당 IP 프로토콜에 대한 모든 트래픽을 삭제합니다.



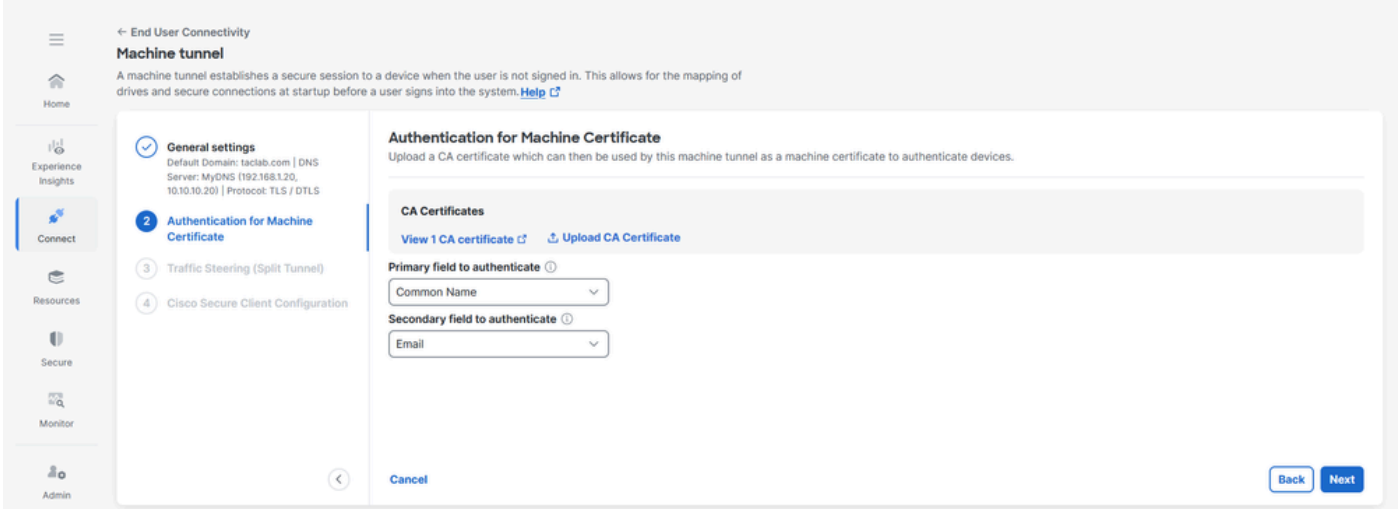
8. 다음을 클릭합니다.

2단계 - 머신 인증서에 대한 인증

머신 터널은 엔드 유저에게 투명하며, 사용자가 VPN 세션을 시작하면 자동으로 연결이 끊깁니다. 사용자 상호 작용 없이 이 터널을 생성하려면 인증서 기반 인증이 사용됩니다.

1. 목록에서 CA 인증서를 선택하거나 Upload CA certificates를 클릭합니다

2. 인증서 기반 인증 필드를 선택합니다. 자세한 내용은 인증서 기반 인증 필드를 참조하십시오



3. 다음을 클릭합니다.

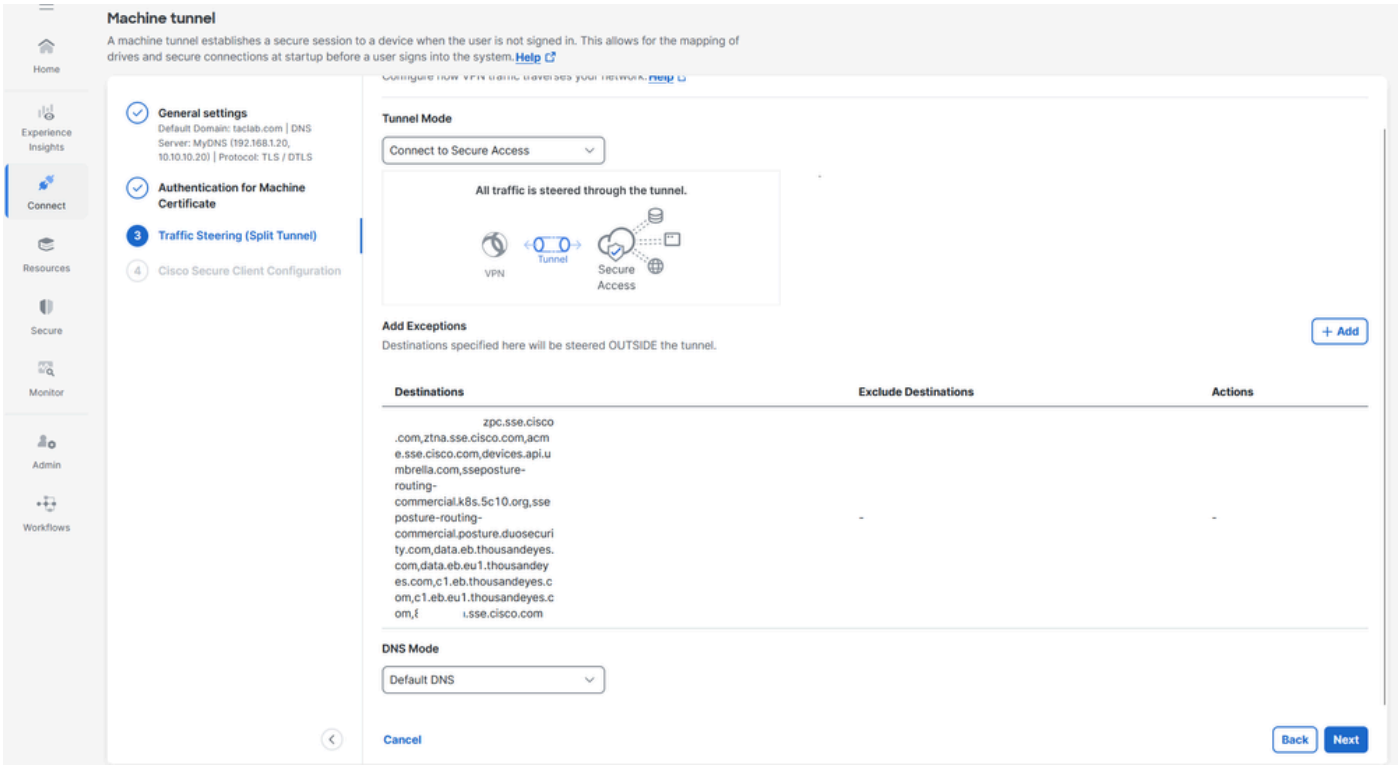
3단계 - 트래픽 조정(스플릿 터널)

트래픽 스티어링(스플릿 터널)의 경우, Secure Access에 대한 전체 터널 연결을 유지 관리하도록 머신 터널을 구성하거나, 필요한 경우에만 스플릿 터널 연결을 사용하여 VPN을 통해 트래픽을 디렉션하도록 구성할 수 있습니다. 자세한 내용은 [머신 터널 트래픽 스티어링을 참조하십시오]

1. 터널 모드를 선택합니다

2. 터널 모드 선택에 따라 예외를 추가할 수 있습니다

3. DNS 모드 선택

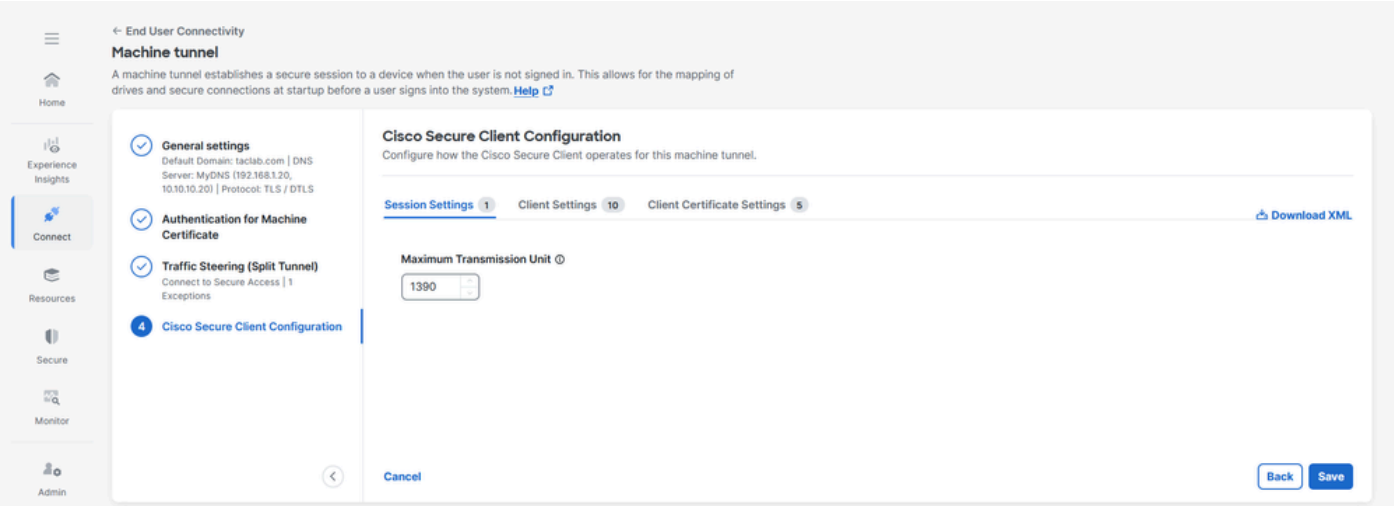


4. 다음을 클릭합니다.

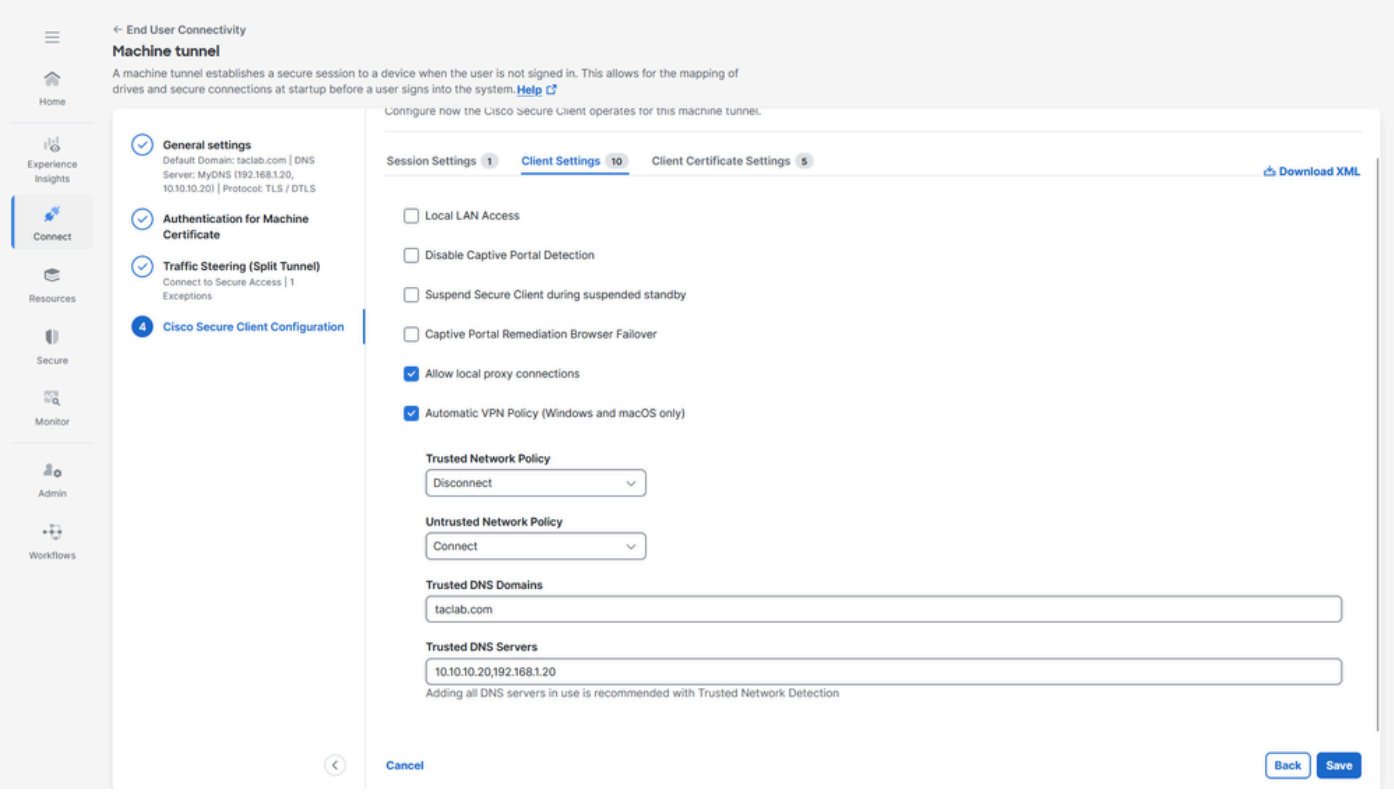
4단계 - Cisco Secure Client 컨피그레이션

특정 VPN 머신 터널의 요구 사항에 따라 Cisco Secure Client 설정의 하위 집합을 수정할 수 있습니다. 자세한 내용은 보안 클라이언트 컨피그레이션을 참조하십시오

1. 프래그먼트화 없이 VPN 터널에서 전송할 수 있는 패킷의 최대 크기인 최대 전송 단위를 확인합니다



2 . 클라이언트 설정, 자세한 내용은 머신 터널 클라이언트 설정을 참조하십시오.



3. 클라이언트 인증서 설정, 옵션을 적절히 선택합니다.

a. Windows 인증서 저장소 재정의 — 관리자가 보안 클라이언트가 클라이언트 인증서 인증을 위해 Windows 시스템(로컬 시스템) 인증서 저장소의 인증서를 사용하도록 할 수 있습니다.

b. 자동 인증서 선택 - 보안 게이트웨이에 여러 인증서 인증이 구성된 경우

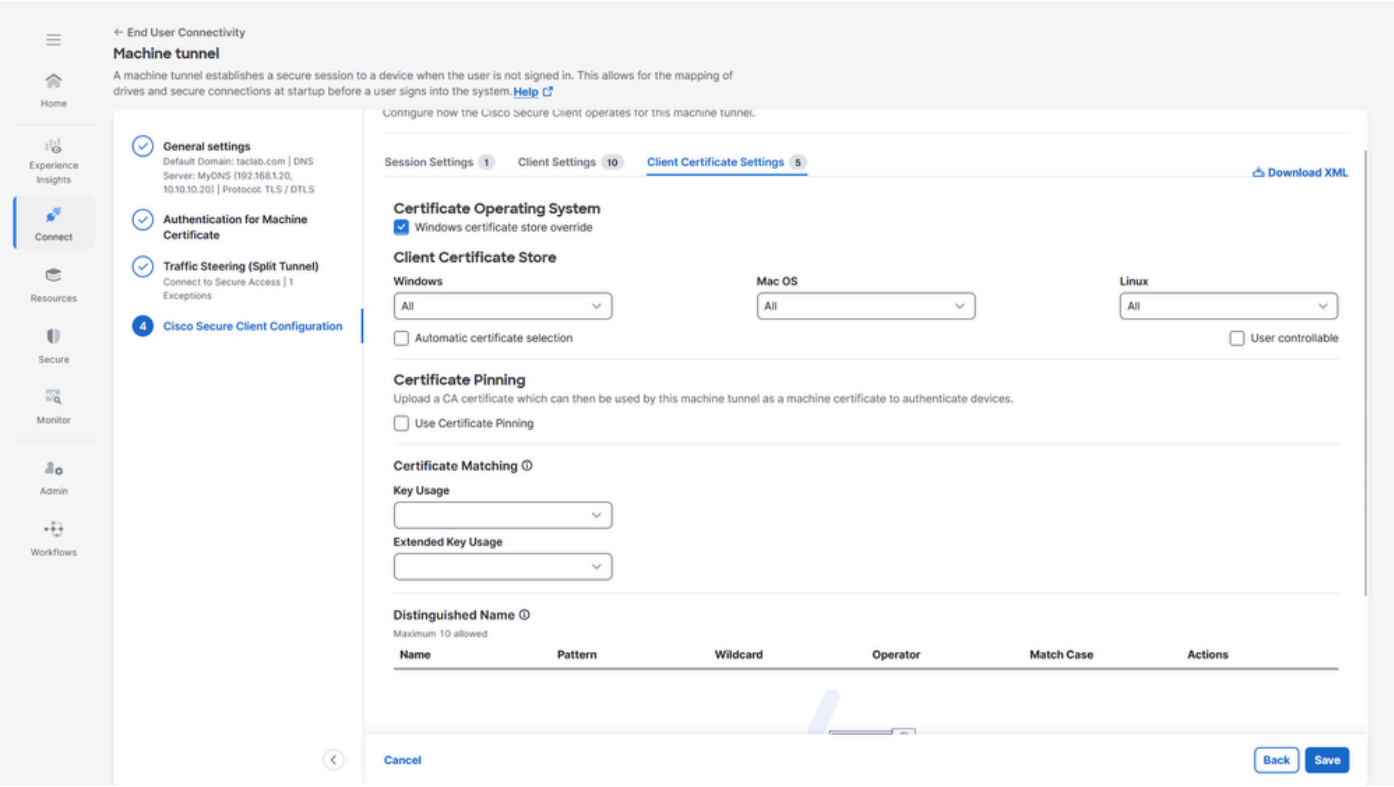
c. Certificate Pinning - 머신 터널에서 디바이스 인증을 위해 머신 인증서로 사용할 수 있는 CA 인증서

d. Certificate Matching(인증서 일치) - 인증서 일치 기준을 지정하지 않으면 Cisco Secure Client가 인증서 일치 규칙을 적용합니다

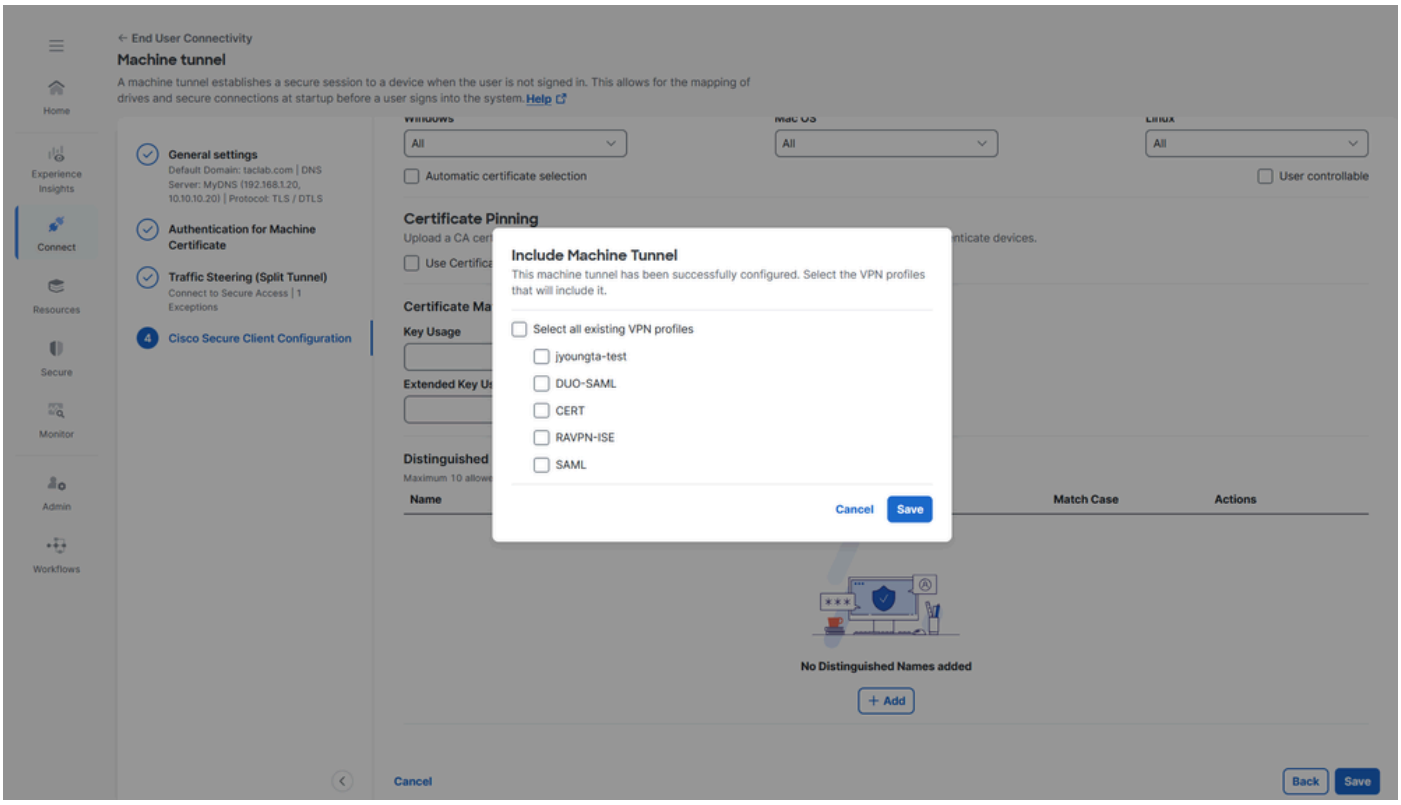
i. 키 사용: 디지털 서명

나. 확장 키 사용: 클라이언트 인증

e. Distinguished Name(고유 이름) - 허용 가능한 클라이언트 인증서를 선택할 때 정확한 일치 기준에 대해 DN(고유 이름)을 지정합니다. 여러 DN을 추가할 경우 각 인증서가 모든 항목에 대해 확인되며 모두 일치해야 합니다.

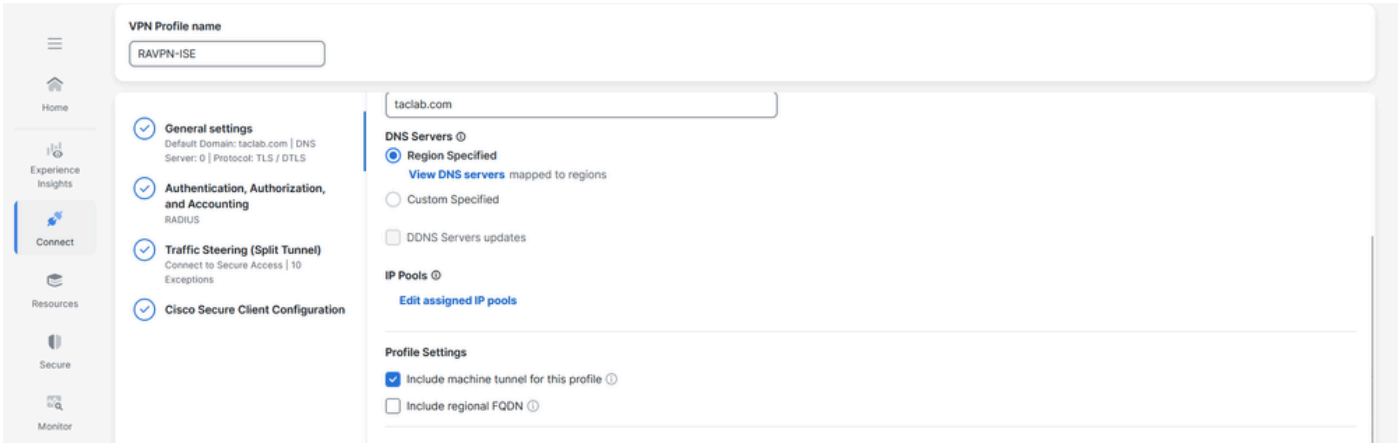


4. 사용자 VPN 프로필에 시스템 터널 프로필을 지정하고 저장을 클릭한 다음 사용자 VPN 프로필을 선택할 수 있는 옵션이 있습니다



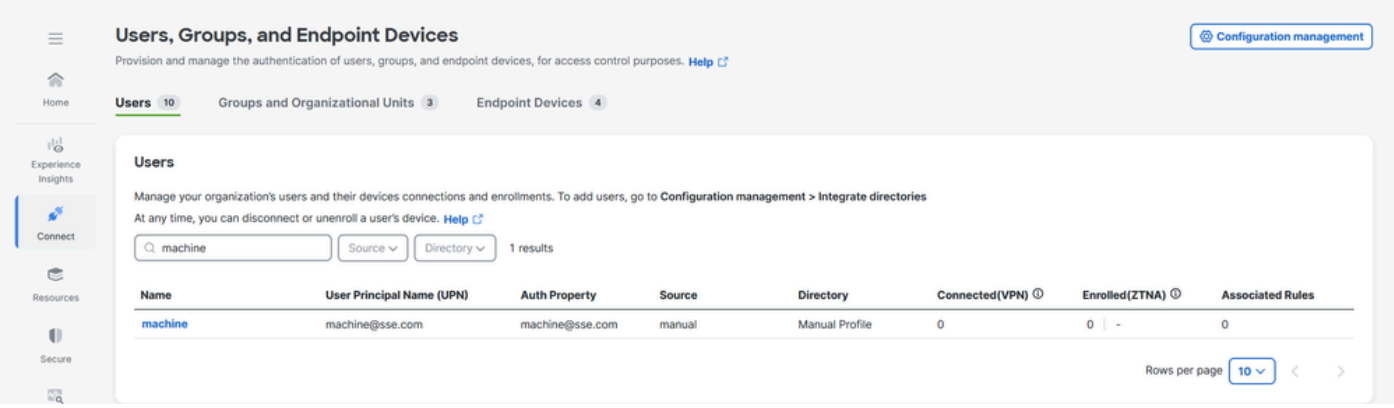
5. 저장을 클릭합니다.

6. 시스템 터널 프로파일이 사용자 VPN 프로파일에 연결되었는지 확인합니다.



5단계 - machine@sse.com 사용자가 Cisco Secure Access에 있는지 확인합니다.

1. Connect(연결) > Users(사용자), Groups(그룹) 및 Endpoint Devices(엔드포인트 디바이스) > Users(사용자)로 이동합니다



2 . machine@sse.com 사용자가 수동으로 가져오기를 제공하지 않는 경우 자세한 내용은 수동 사용자 및 그룹 가져오기를 참조하십시오

6단계 - machine@sse.com에 대한 CA 서명 인증서 생성

1. 인증서 서명 요청 생성

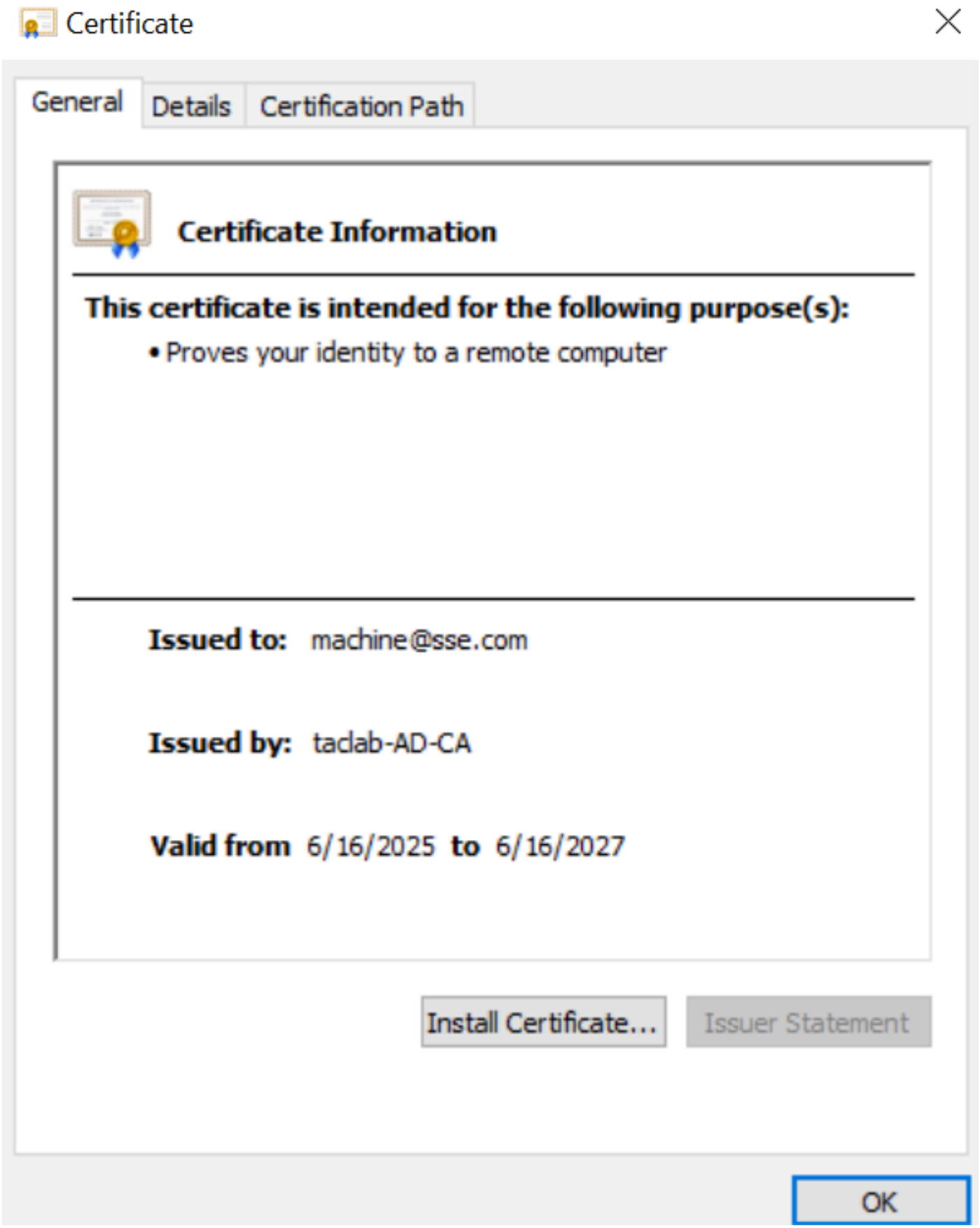
a. 모든 온라인 CSR 생성기 소프트웨어 CSR 생성기 또는 openssl CLI를 사용할 수 있습니다

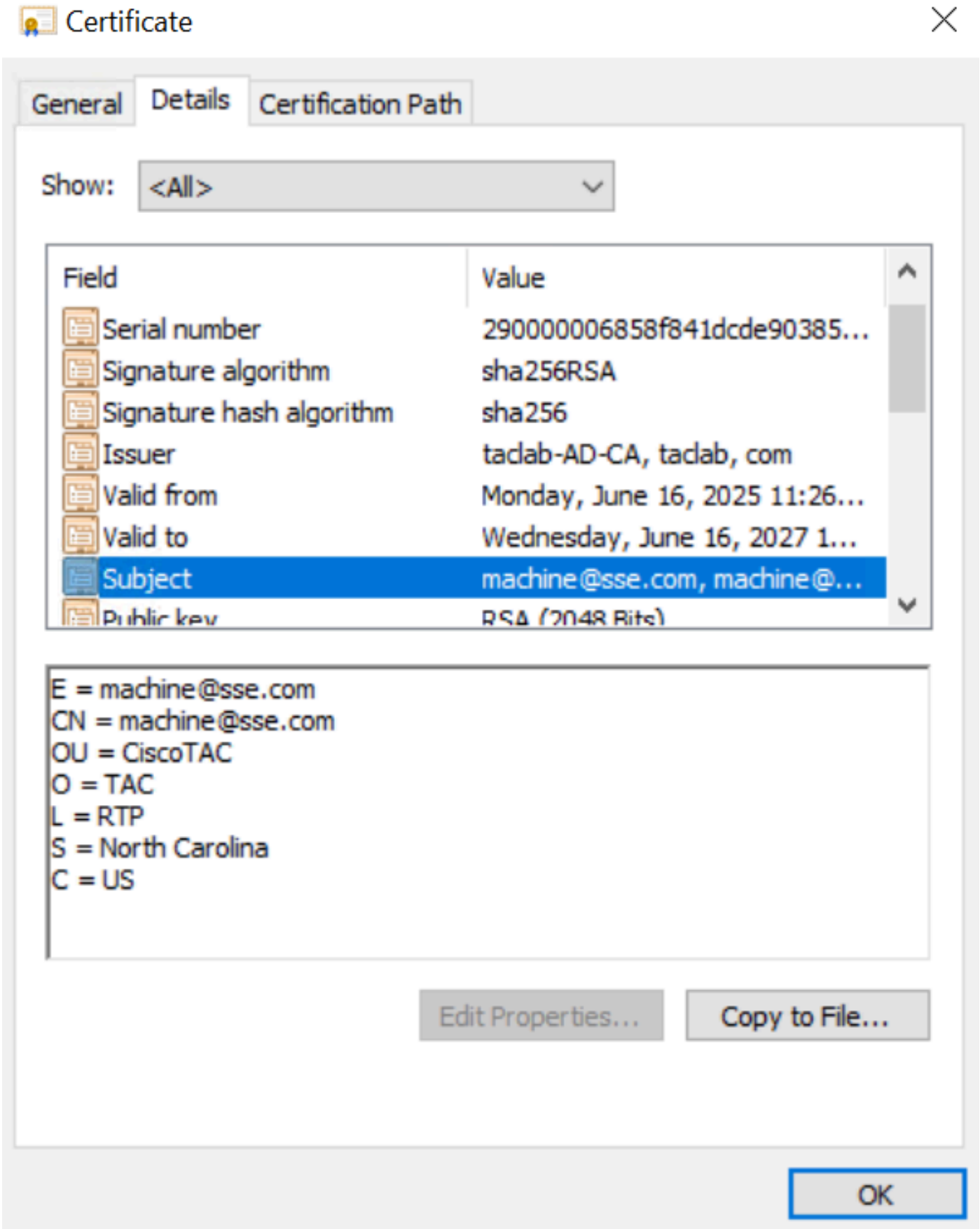
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr

```
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. CSR을 복사하고 머신 인증서를 생성합니다


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



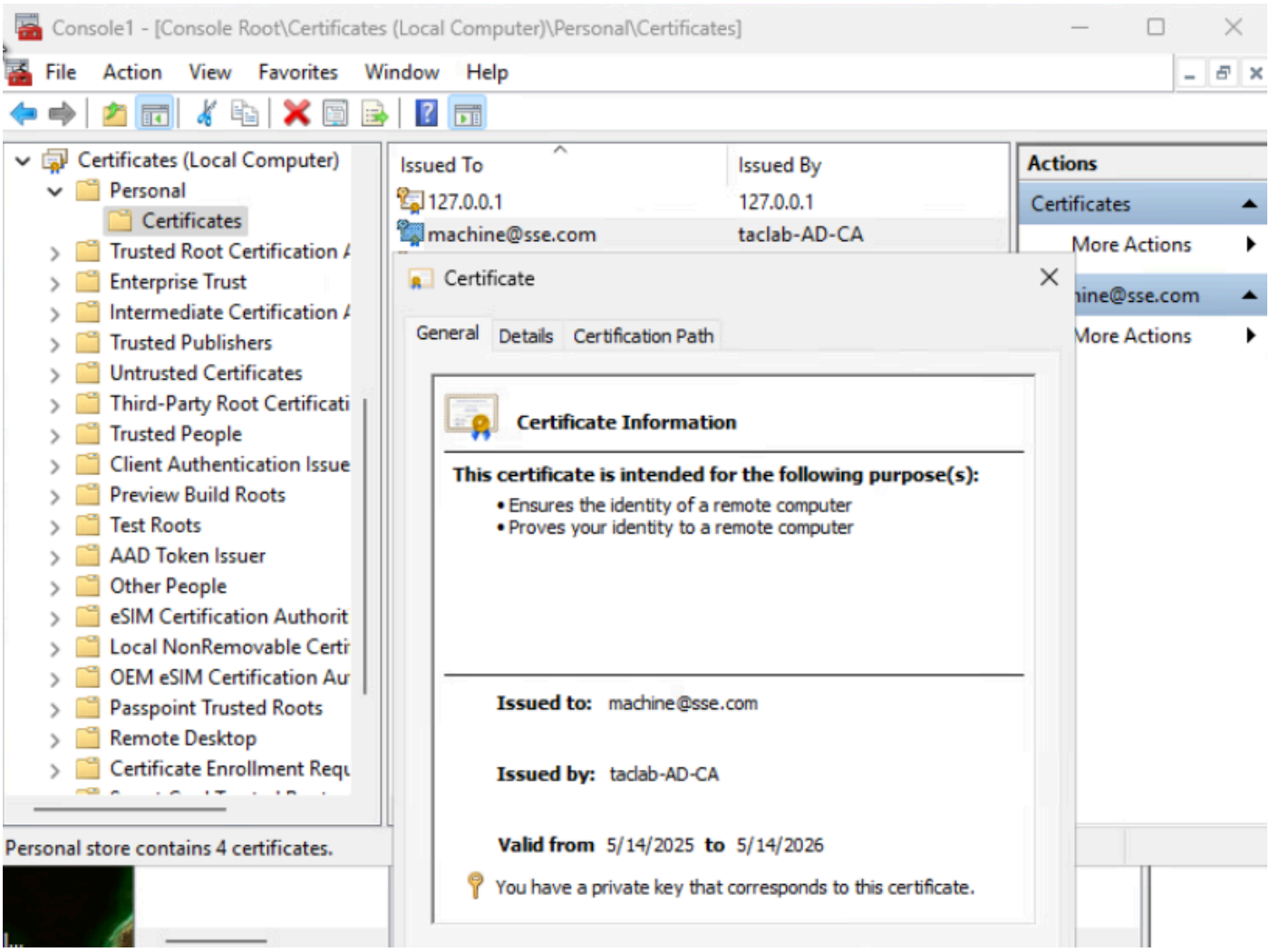
3. 이전 단계(1단계 및 2단계)에서 각각 생성된 키 및 인증서를 사용하여 머신 인증서를 PKCS12 형식으로 변환합니다

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#
```

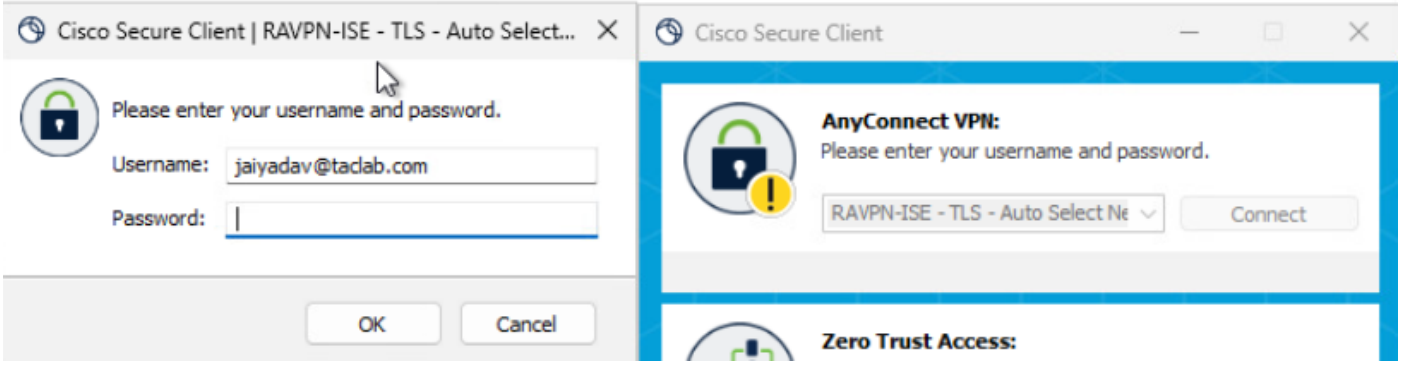
7단계 - 테스트 시스템에서 머신 인증서 가져오기

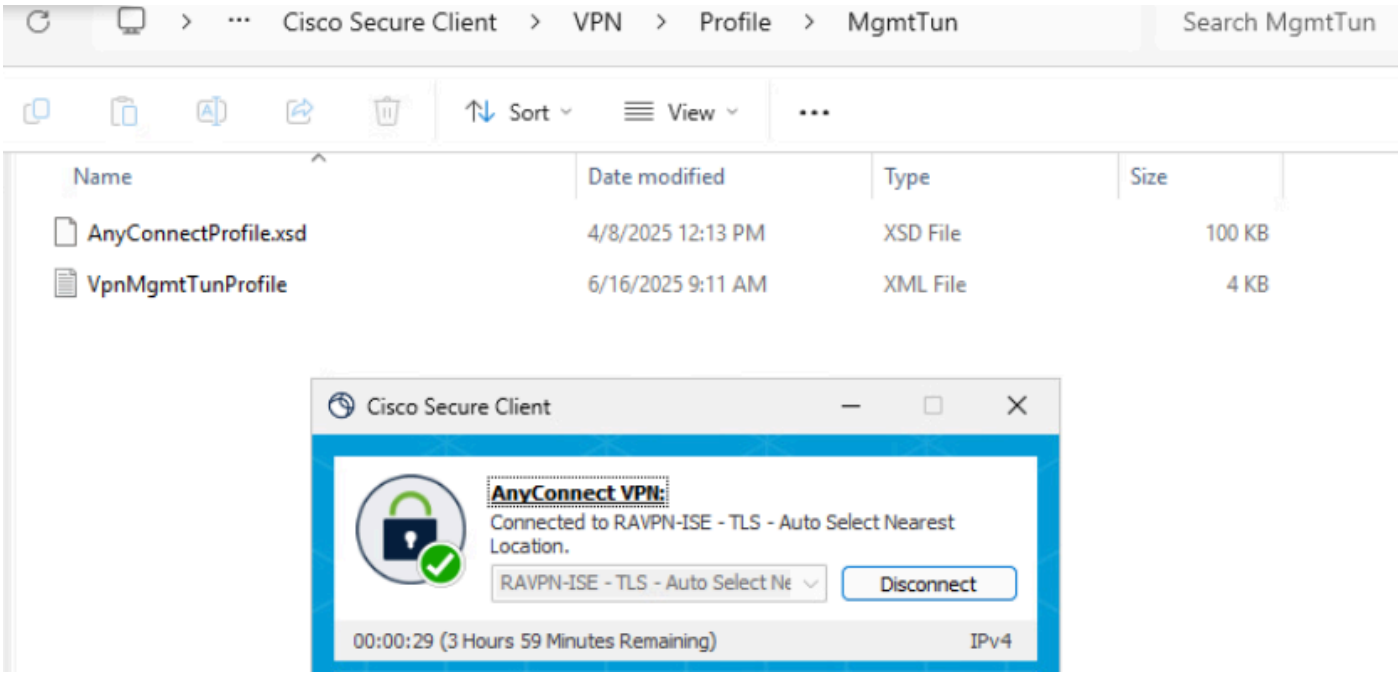
a. 로컬 또는 머신 저장소 아래에 PKCS12 머신 인증서를 가져옵니다.



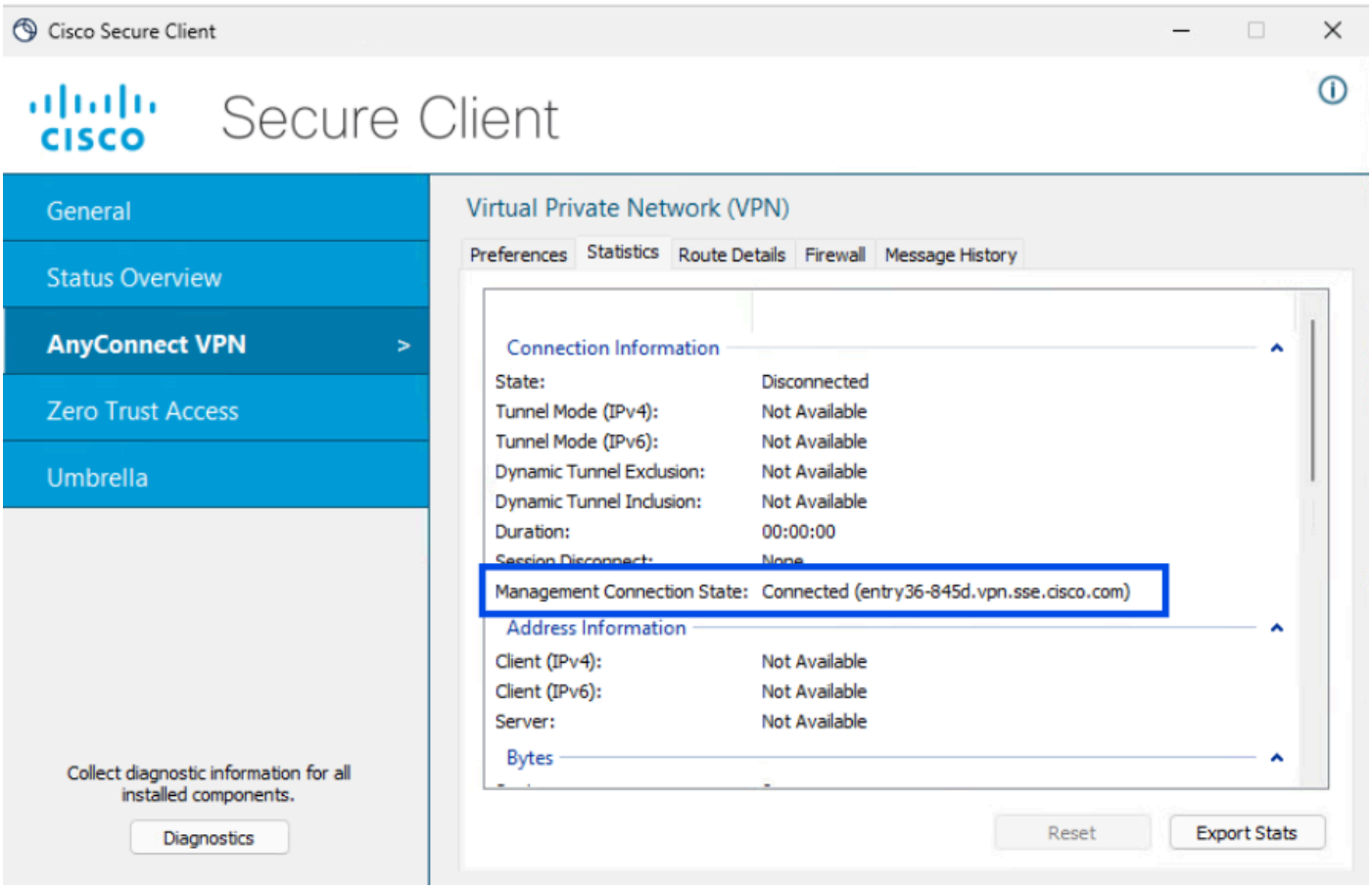
8단계 - 머신 터널에 연결

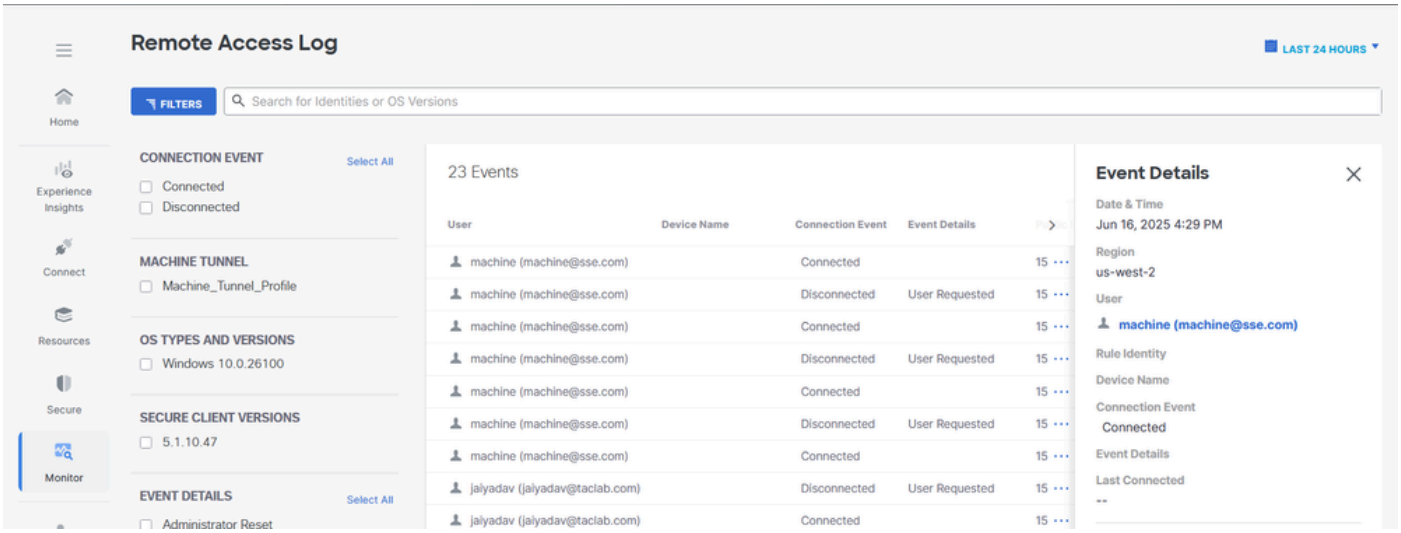
a. 사용자 터널에 연결하면 머신 xml 프로파일이 다운로드됩니다.




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. 시스템 터널 연결 확인


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



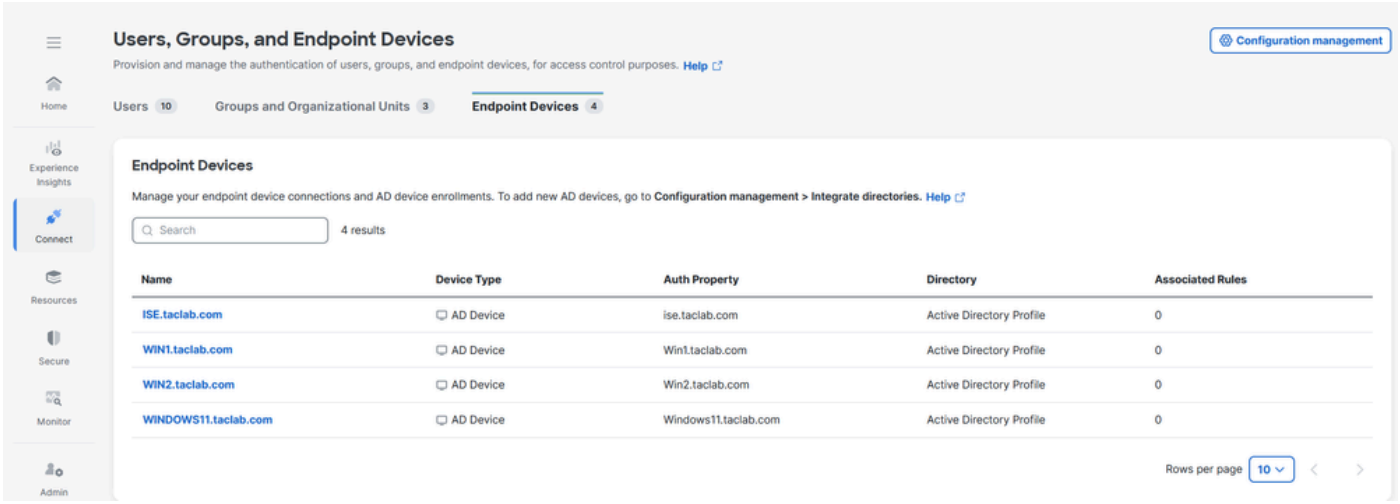
방법 2 - 엔드포인트 인증서를 사용하여 머신 터널 구성

이 경우 Primary(기본) 필드에서 인증하려면 디바이스 이름(컴퓨터 이름)이 포함된 인증서 필드를 선택합니다. Secure Access에서는 디바이스 이름을 머신 터널 식별자로 사용합니다. 컴퓨터 이름의 형식은 선택한 장치 식별자의 형식과 일치해야 합니다

시스템 터널 컨피그레이션에 대해 1단계에서 4단계까지 진행합니다.

5단계 - Cisco Secure Access에서 엔드포인트를 가져올 수 있도록 AD 커넥터를 구성합니다.

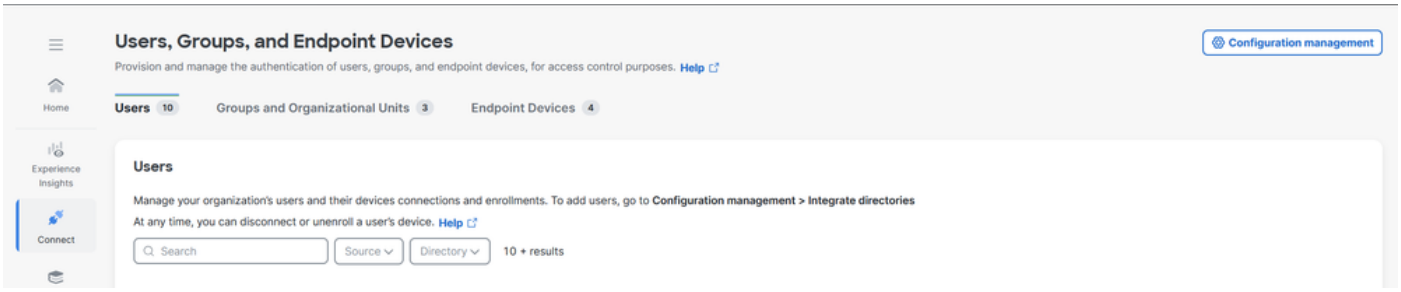
자세한 내용은 On-Perm Active Directory 통합을 참조하십시오



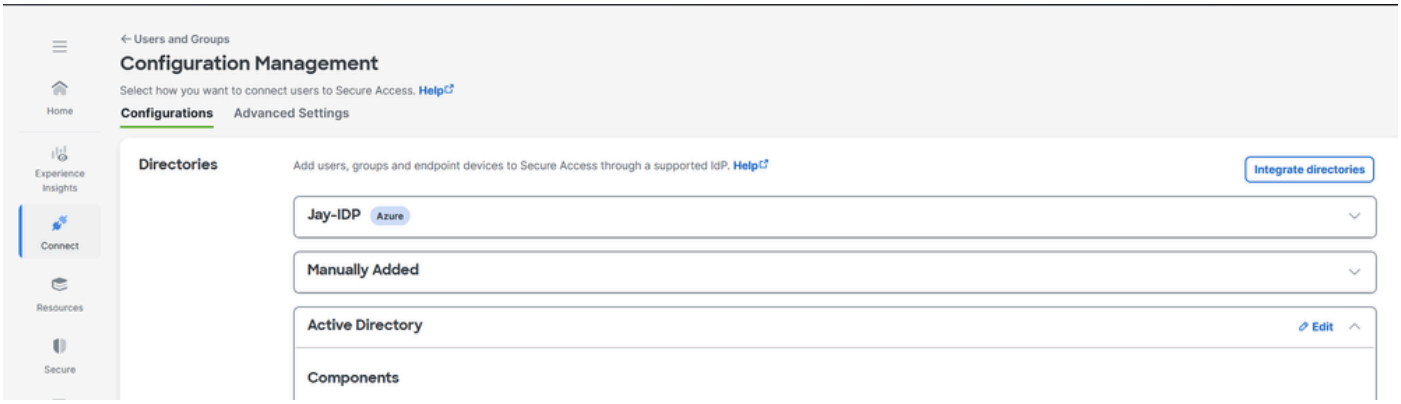
6단계 - 엔드포인트 디바이스 인증 구성

1. Connect(연결) > Users(사용자), Groups(그룹) 및 Endpoint Devices(엔드포인트 디바이스)로 이동합니다.

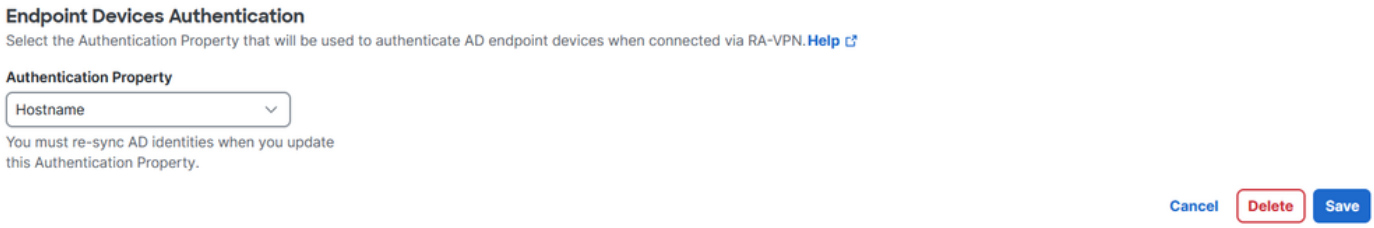
2. 구성 관리를 클릭합니다.



3 . Configurations(컨피그레이션)에서 Active Directory를 편집합니다.



4. 엔드포인트 장치 인증 속성을 호스트 이름으로 설정



5. [저장]을 클릭하고 AD 커넥터 서비스가 설치된 서버에서 AD 커넥터 서비스를 다시 시작합니다

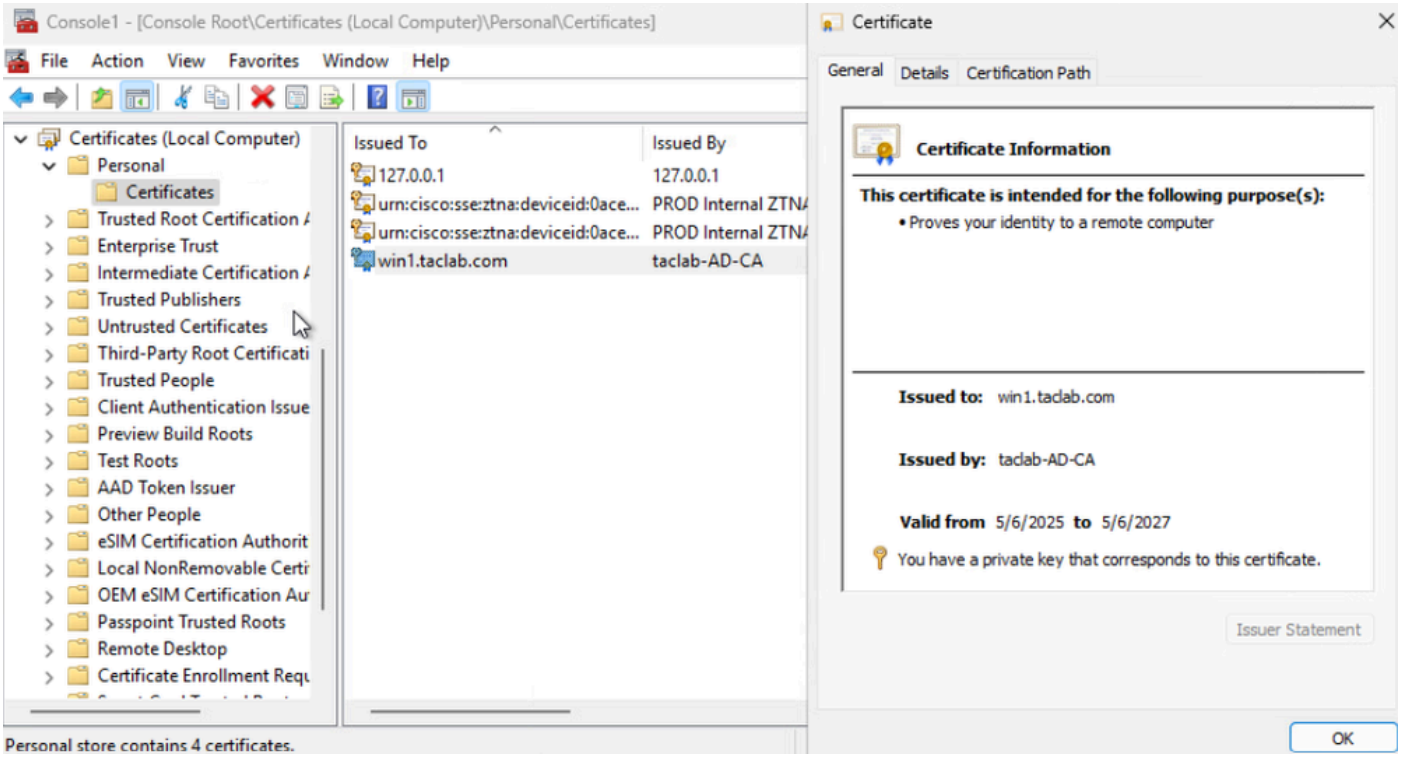
7단계 - 엔드포인트 인증서 생성 및 가져오기

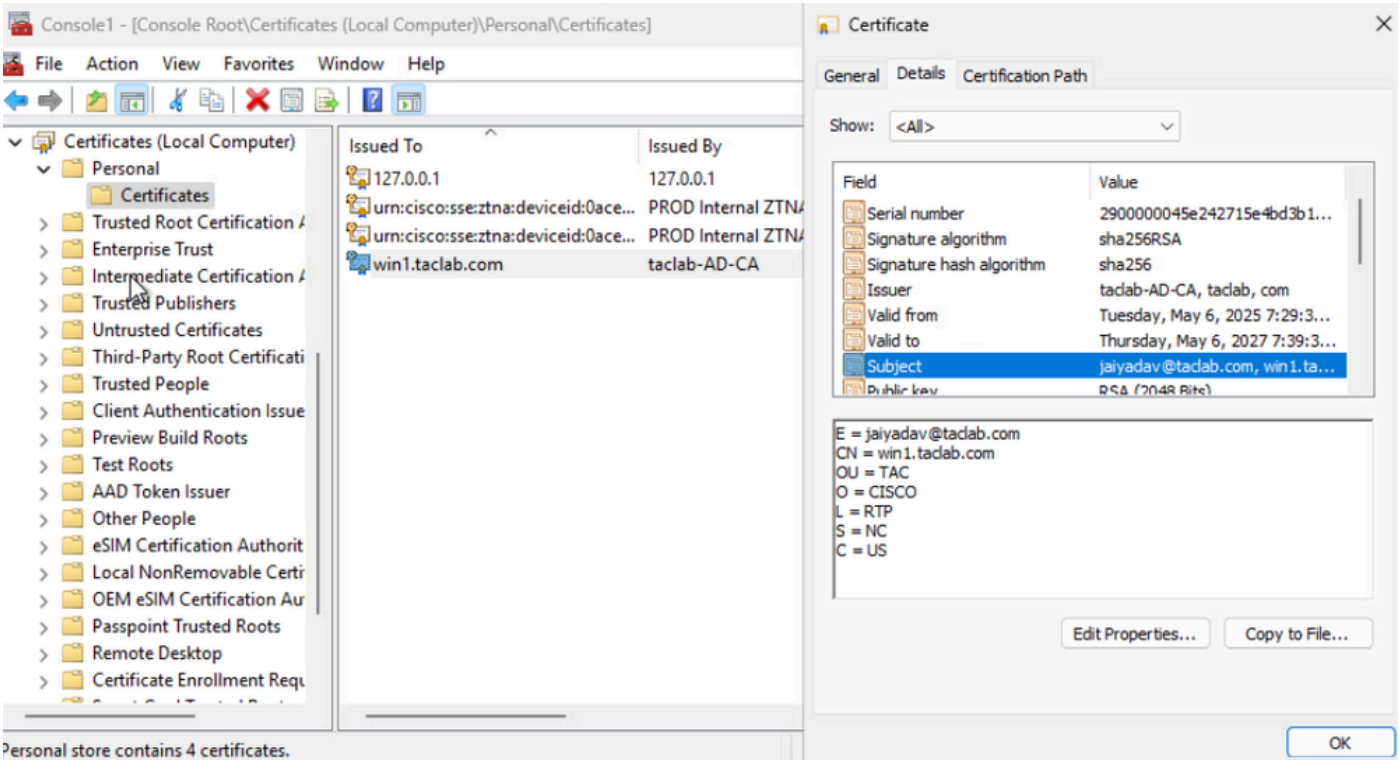
a. CSR 생성, CSR 생성기 또는 OpenSSL 툴 열기

b. CA에서 엔드포인트 인증서 생성

c. .cert 파일을 PKCS12 형식으로 변환합니다.

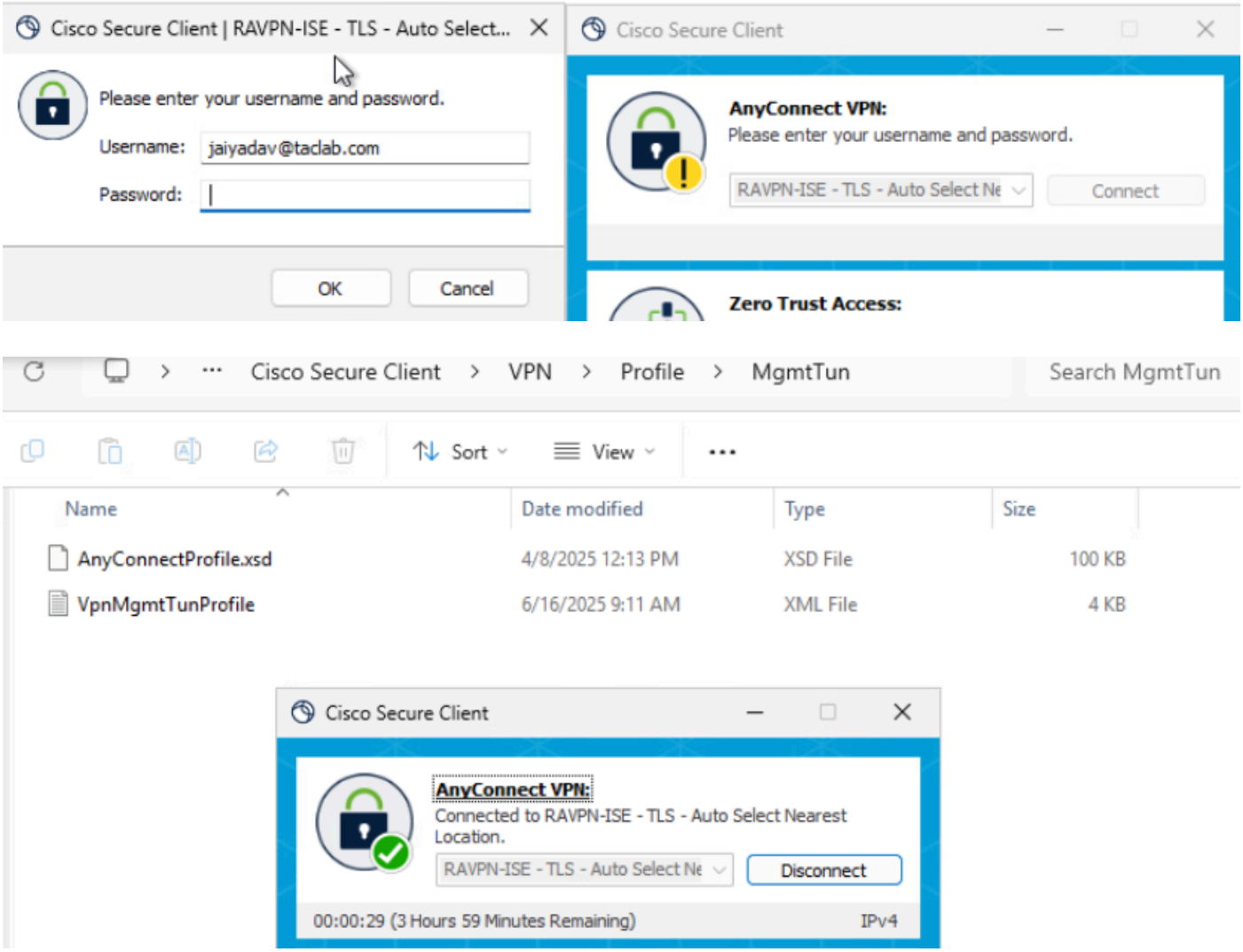
d. 엔드포인트 인증서 저장소에서 PKCS12 인증서 가져오기



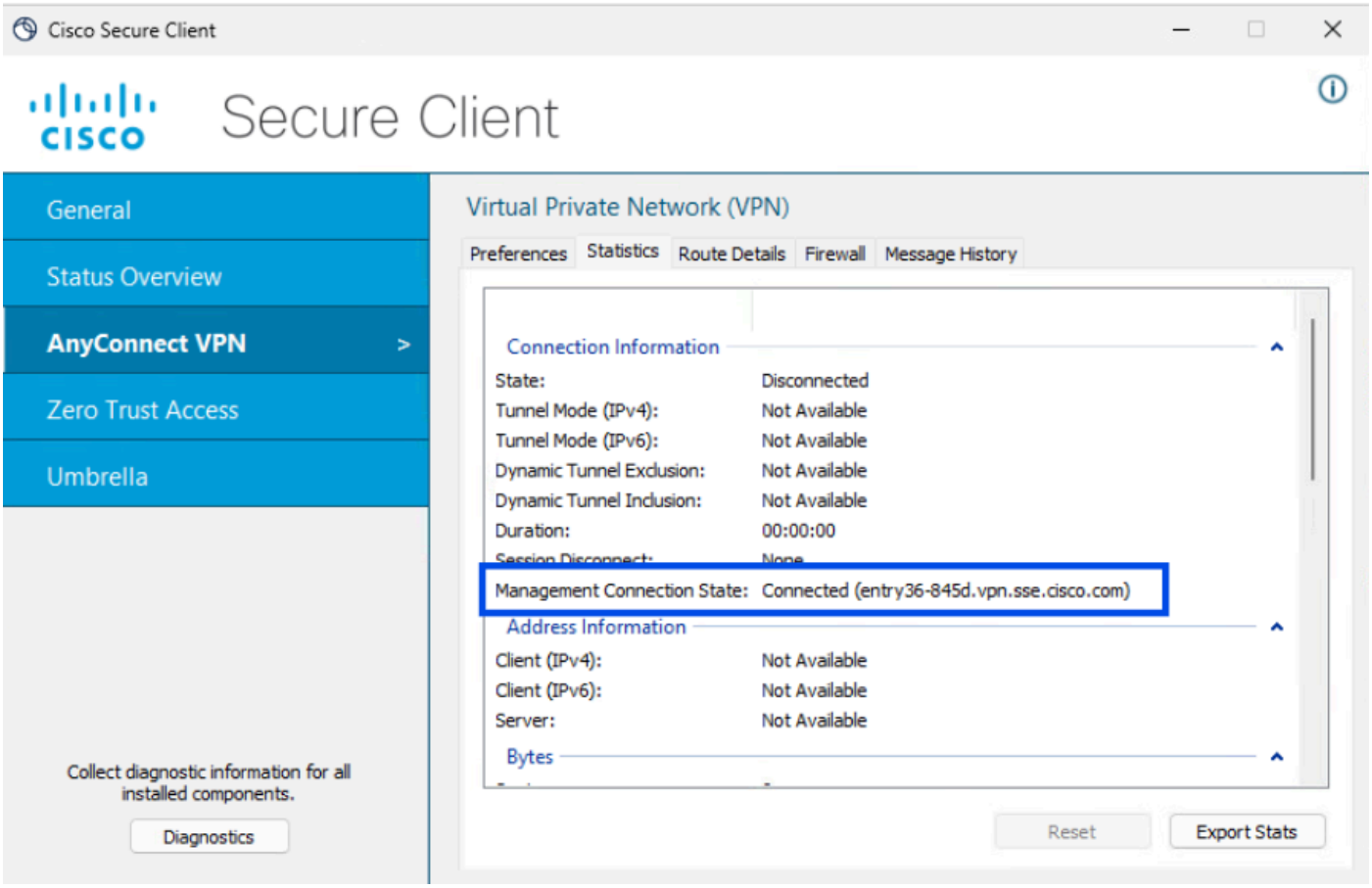


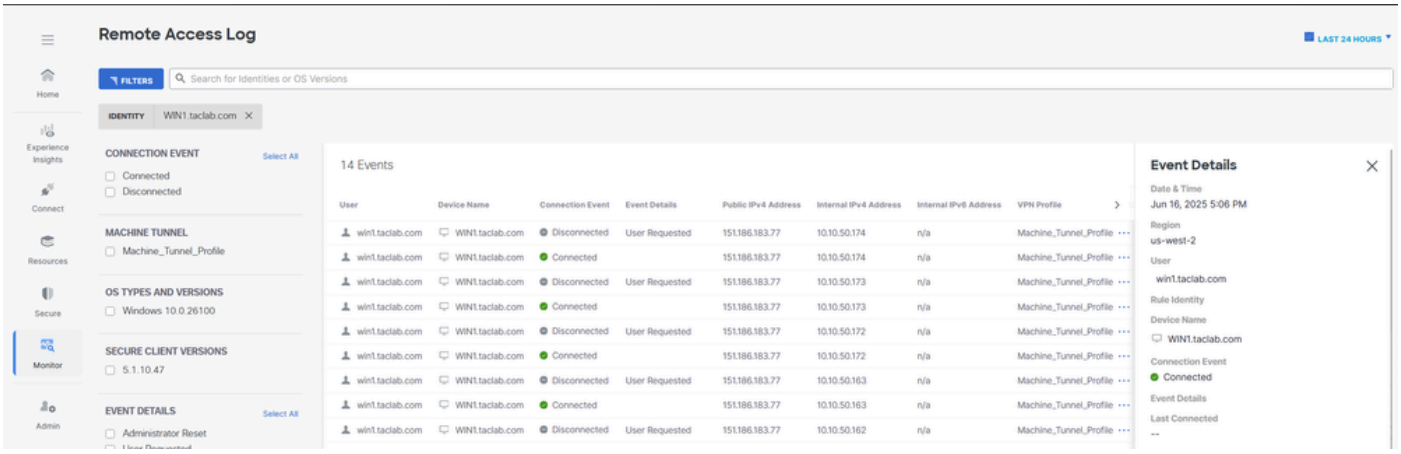
8단계 - 머신 터널에 연결

a. 사용자 터널에 연결하면 시스템 터널 xml 프로파일 다운로드가 트리거됩니다


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. 시스템 터널 연결 확인





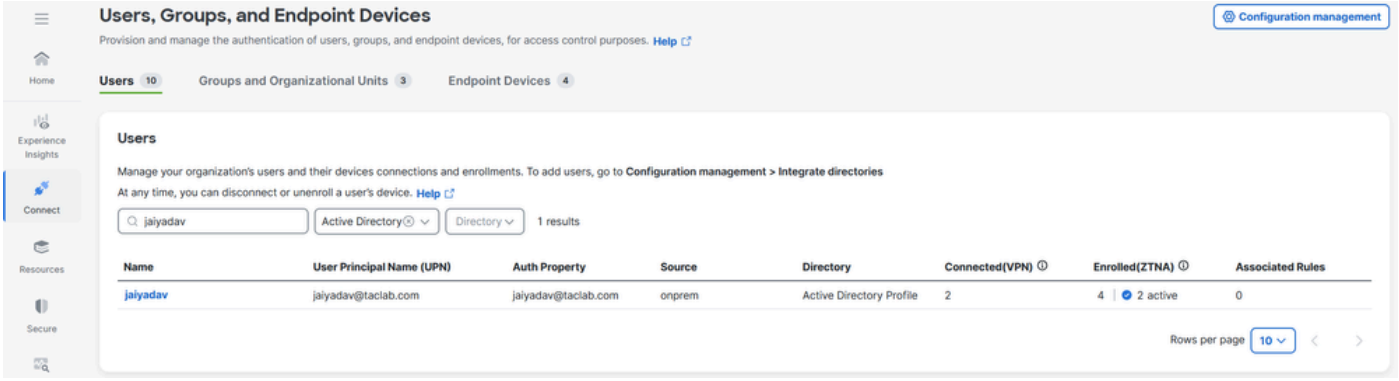
방법 3 - 사용자 인증서를 사용하여 머신 터널 구성

이 경우 Primary(기본) 필드에서 인증하려면 사용자 이메일 또는 UPN이 포함된 인증서 필드를 선택합니다. Secure Access에서는 이메일 또는 UPN을 머신 터널 식별자로 사용합니다. 이메일 또는 UPN의 형식은 선택한 장치 식별자의 형식과 일치해야 합니다

시스템 터널 컨피그레이션에 대한 1~4단계를 진행합니다

5단계 - Cisco Secure Access에서 사용자를 가져올 수 있도록 AD 커넥터를 구성합니다.

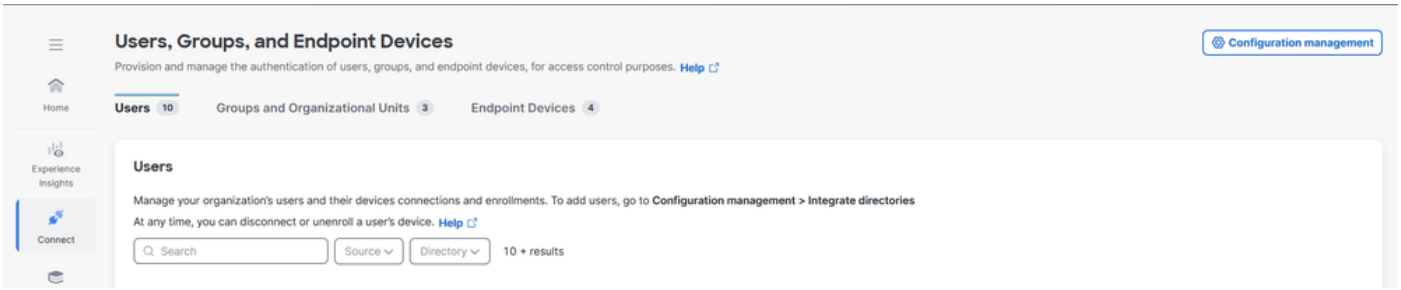
자세한 내용은 On-Perm Active Directory 통합을 참조하십시오



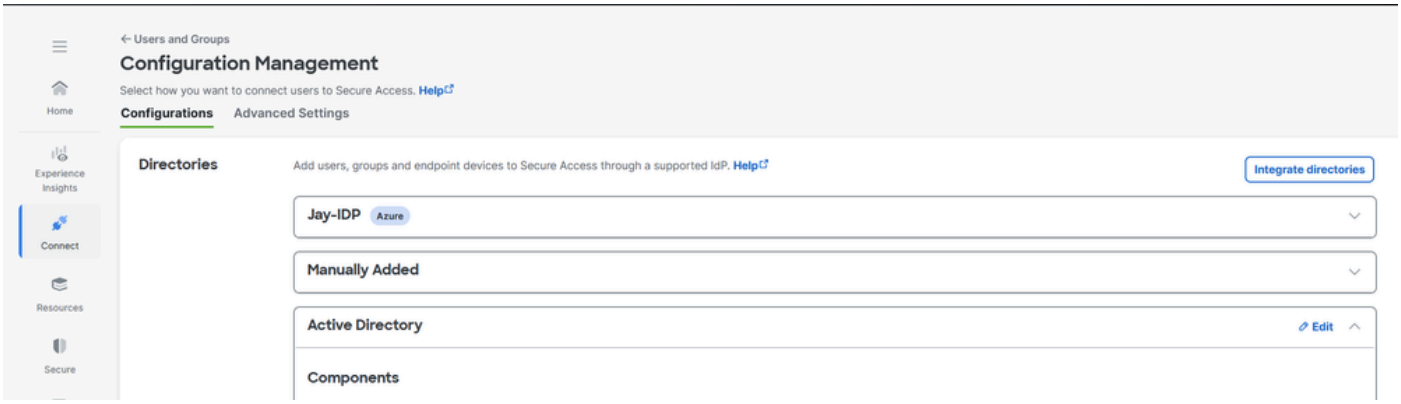
6단계 - 사용자 인증 구성

1. Connect(연결) > Users(사용자), Groups(그룹) 및 Endpoint Devices(엔드포인트 디바이스)로 이동합니다.

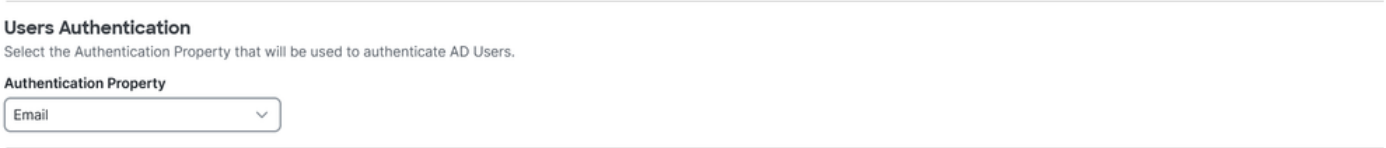
2. 구성 관리를 클릭합니다.



3 . Configurations(컨피그레이션)에서 Active Directory를 편집합니다.



4. 사용자 인증 속성을 전자 메일로 설정



5. [저장]을 클릭하고 AD 커넥터 서비스가 설치된 서버에서 AD 커넥터 서비스를 다시 시작합니다

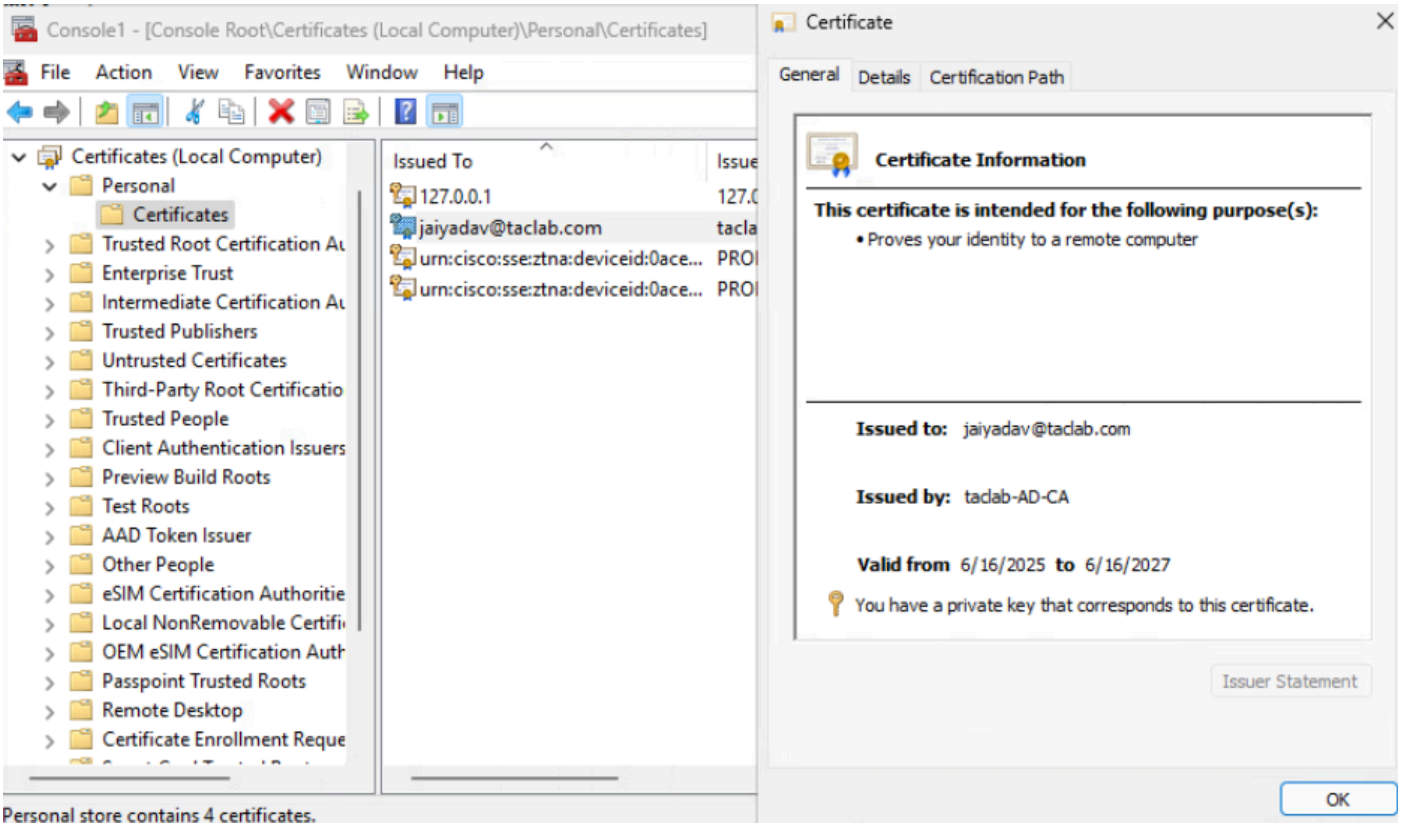
7단계 - 엔드포인트 인증서 생성 및 가져오기

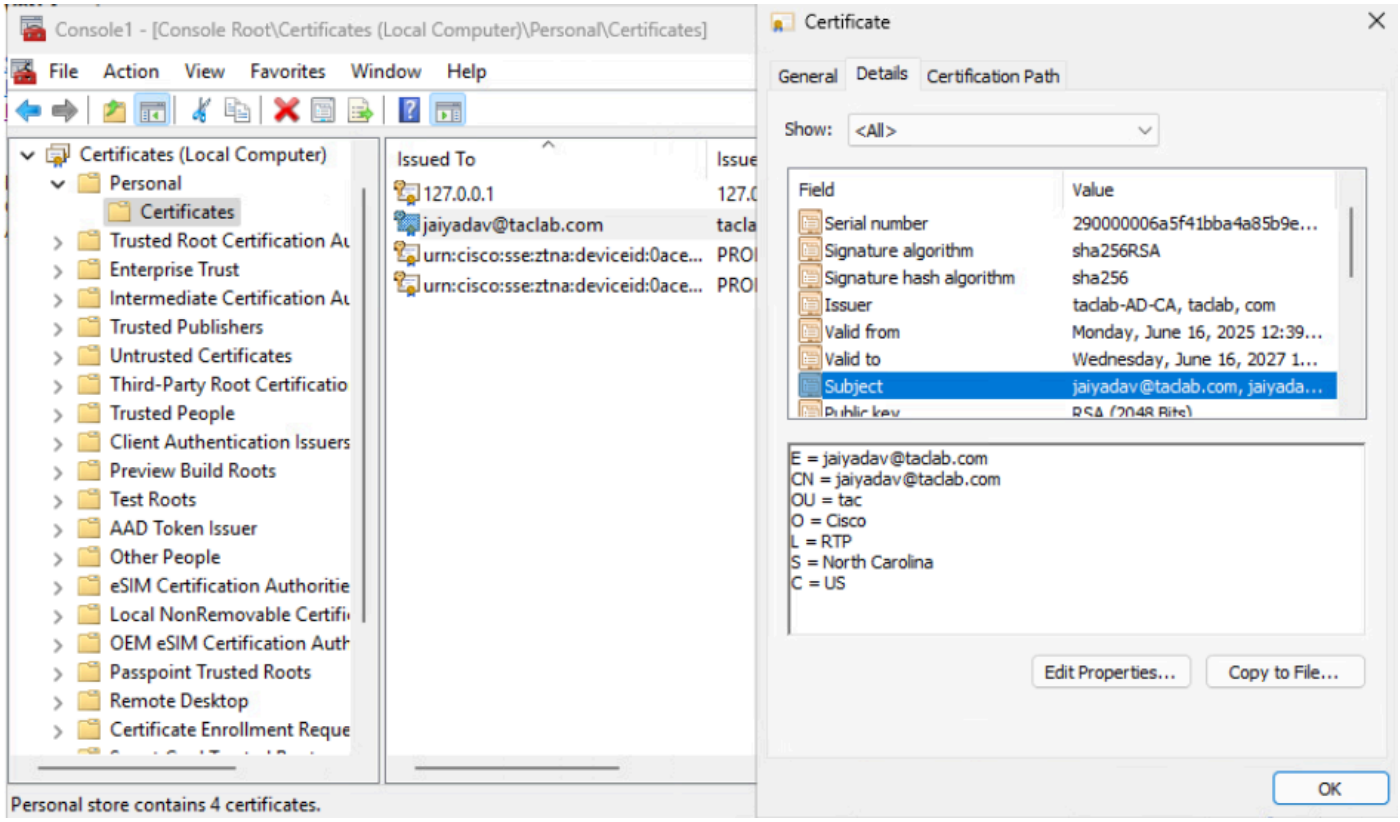
a. CSR 생성, CSR 생성기 또는 OpenSSL 툴 열기

b. CA에서 엔드포인트 인증서 생성

c. .cert 파일을 PKCS12 형식으로 변환합니다.

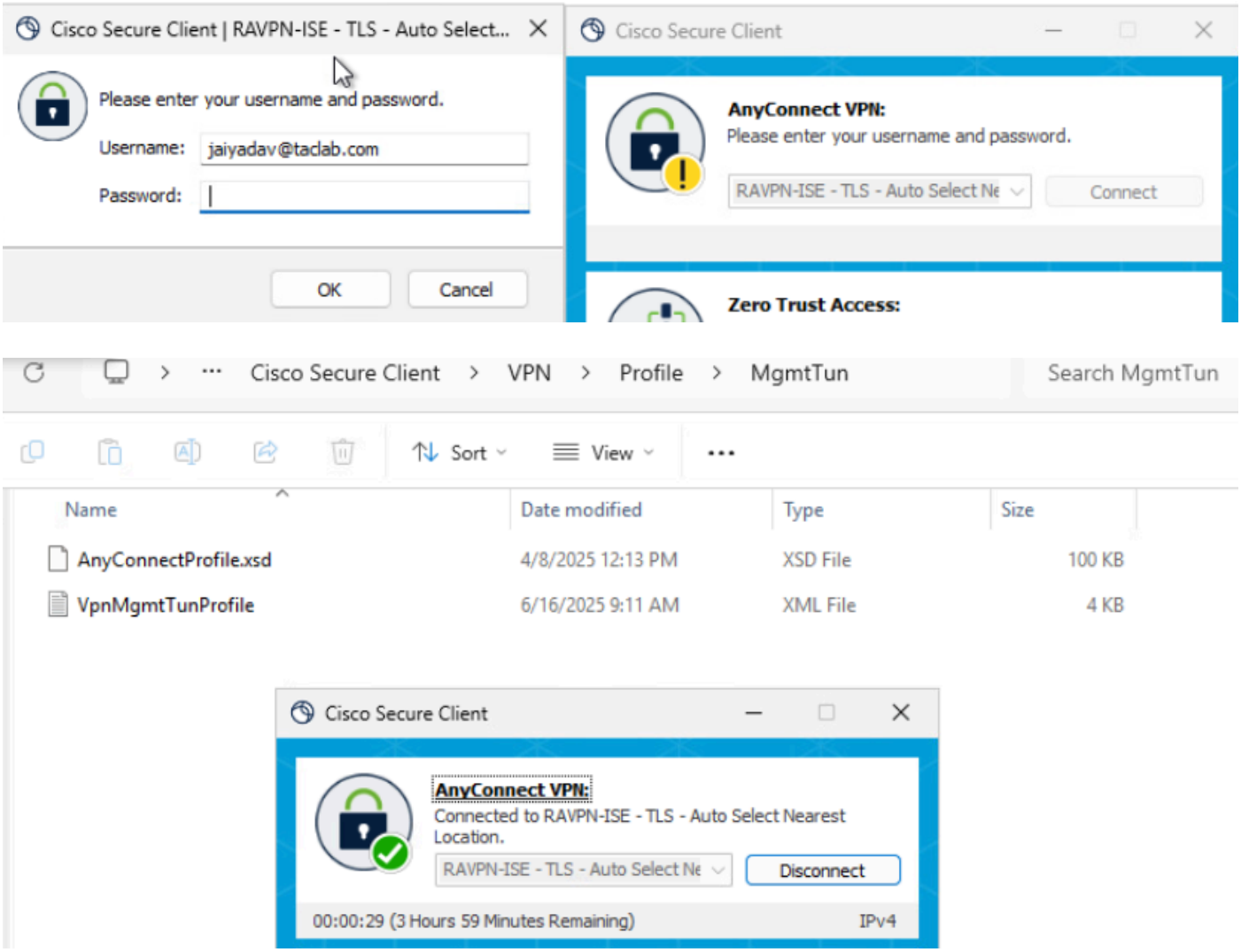
d. 엔드포인트 인증서 저장소에서 PKCS12 인증서 가져오기



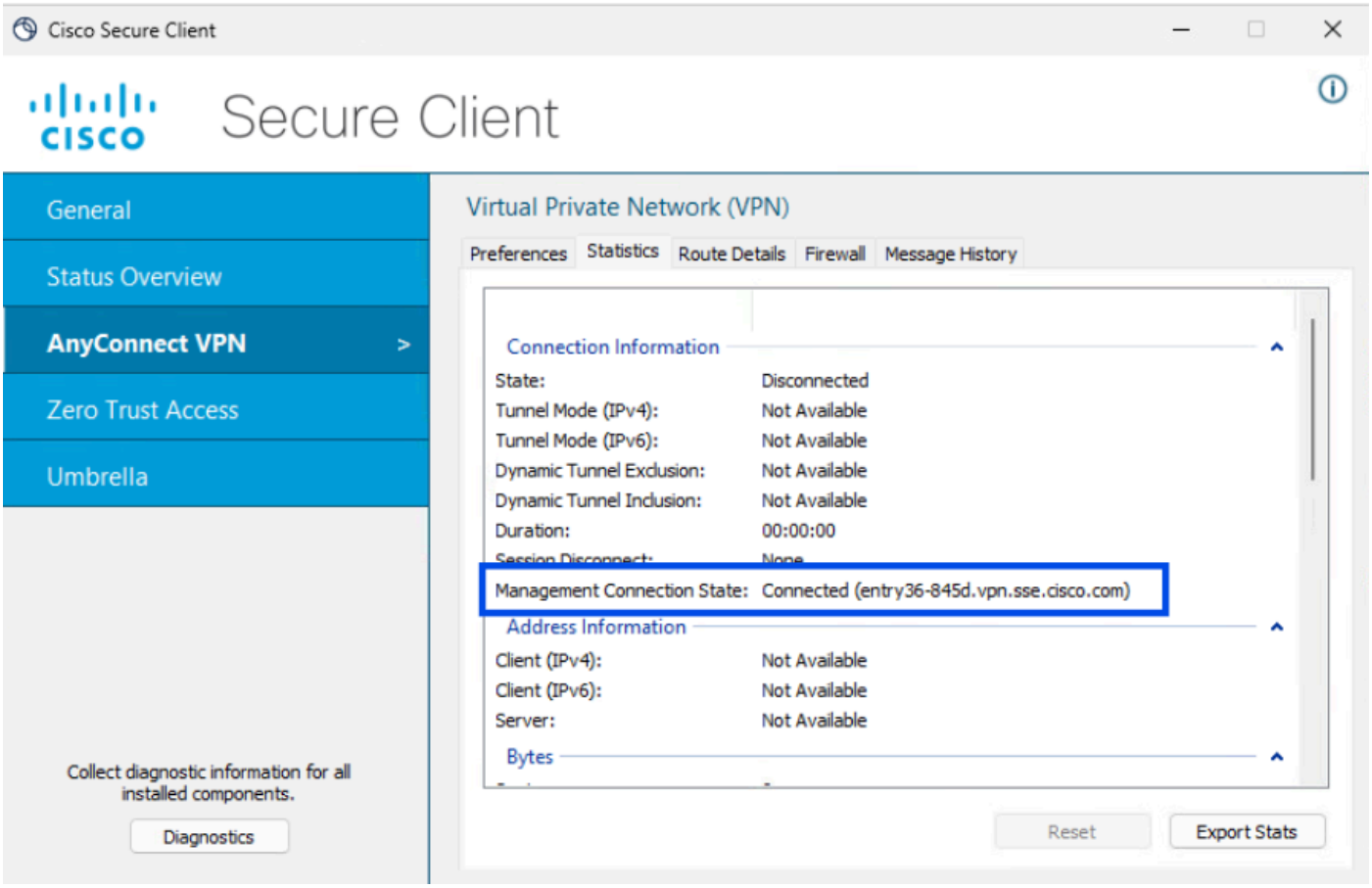


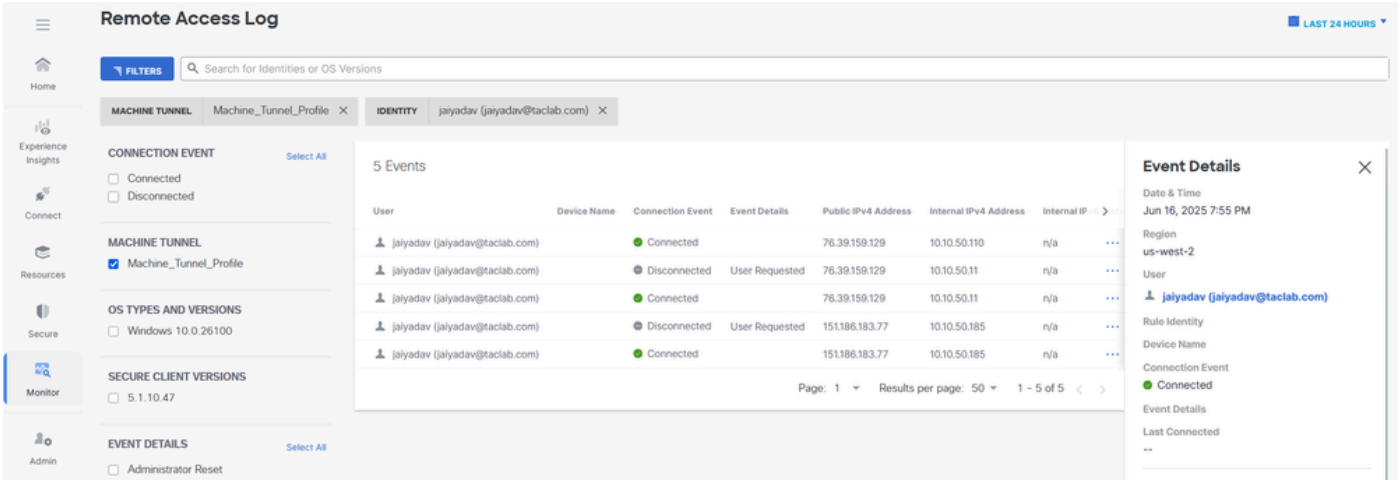
8단계 - 머신 터널에 연결

a. 사용자 터널에 연결하면 시스템 터널 xml 프로파일 다운로드가 트리거됩니다



b. 시스템 터널 연결 확인





문제 해결

DART 번들의 압축을 풀고 AnyConnectVPN 로그를 열고 오류 메시지를 분석합니다.

DARTMODULE_0603_1656.zip\Cisco Secure Client\AnyConnect VPN\Logs

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.