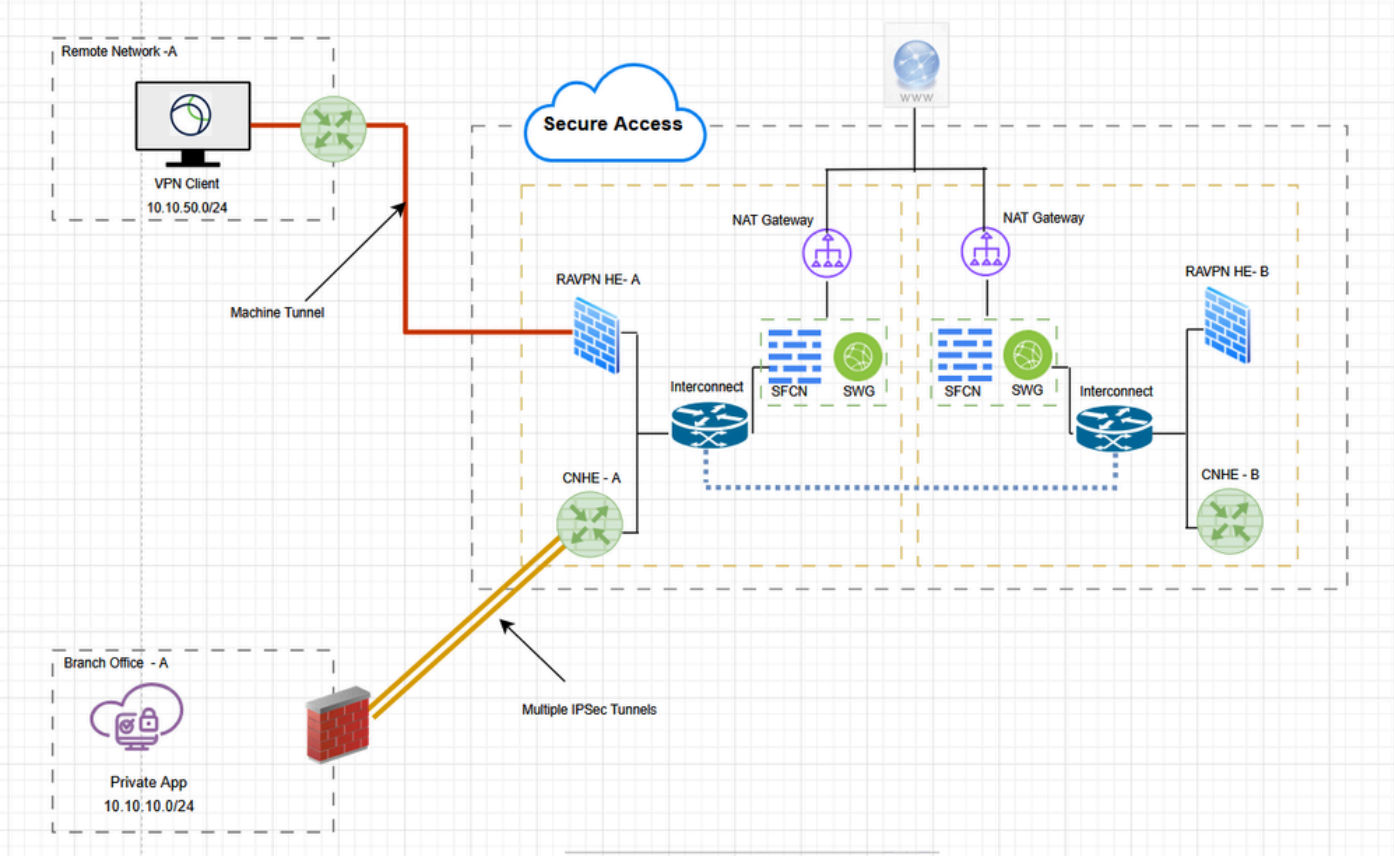
Configurazione del tunnel computer su Cisco Secure Access

Sommario

Introduzione

In questo documento viene descritto come configurare Secure Access come gateway VPN e accettare le connessioni dal client sicuro tramite il tunnel del computer VPN.

Esempio di rete



Prerequisiti

- Ruolo Amministratore completo in Accesso sicuro.
- Almeno un profilo VPN utente configurato su Cisco Secure Access
- Pool di indirizzi IP utente su Cisco Secure Access

Requisiti

È consigliabile conoscere i seguenti argomenti:

- Certificati 509
- OpenSSL

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Access
- Cisco Secure Client 5.1.10
- Windows 11
- Windows Server 2019 - CA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Un tunnel per computer VPN ad accesso sicuro garantisce la connettività alla rete aziendale ogni volta che il sistema client viene acceso, non solo quando l'utente finale stabilisce una connessione VPN. È possibile eseguire la gestione delle patch sugli endpoint fuori sede, in particolare sui dispositivi che l'utente raramente connette alla rete aziendale tramite VPN. Questa funzionalità offre inoltre vantaggi agli script di accesso al sistema operativo degli endpoint che richiedono la connettività di rete aziendale. Per creare il tunnel senza l'interazione dell'utente, viene utilizzata l'autenticazione basata su certificati.

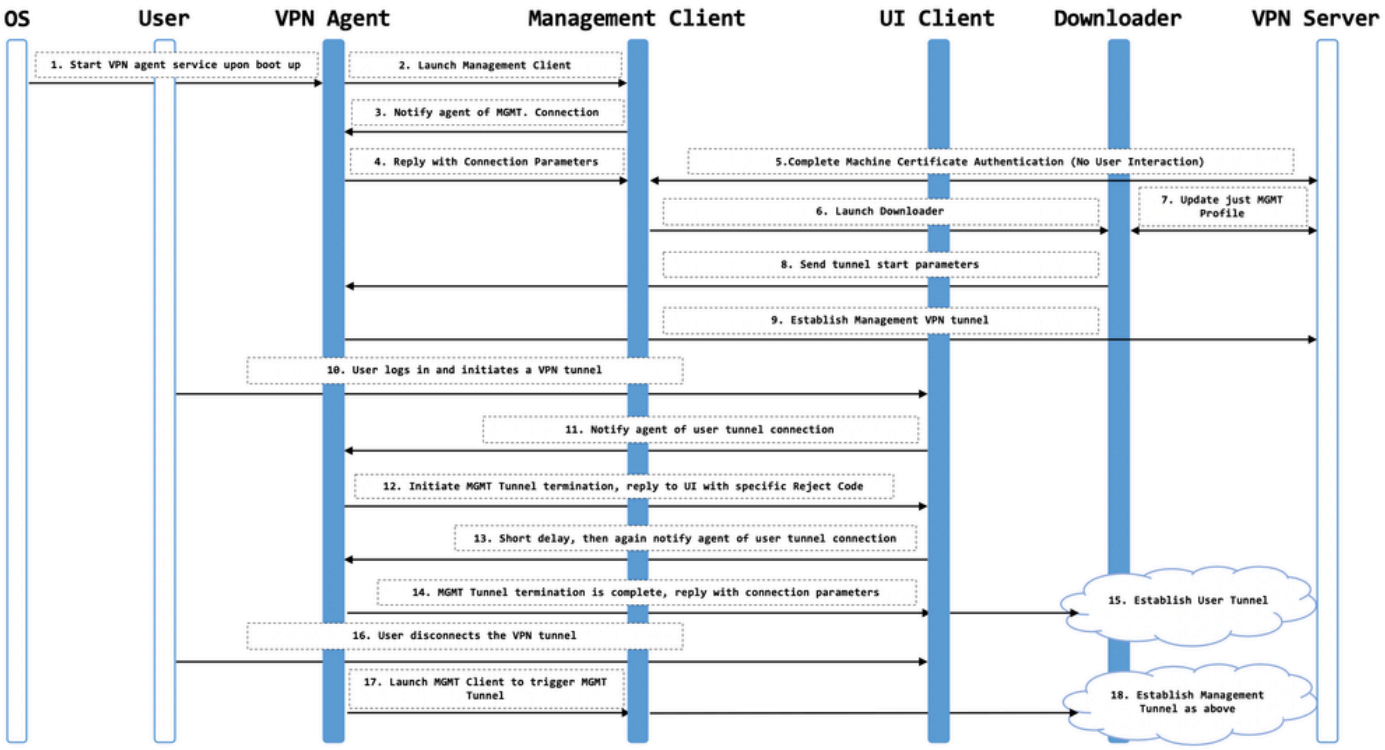
Il tunnel della macchina ad accesso sicuro consente agli amministratori di fare in modo che Cisco Secure Client sia connesso senza l'intervento dell'utente prima del momento in cui quest'ultimo esegue l'accesso. Il tunnel della macchina ad accesso sicuro viene attivato quando l'endpoint è fuori sede e disconnesso da una VPN avviata dall'utente. Il tunnel della macchina VPN ad accesso sicuro è trasparente per l'utente finale e si disconnette automaticamente quando l'utente avvia la VPN.

Lavorare sul tunnel della macchina

Il servizio Agente VPN per client sicuro viene avviato automaticamente all'avvio del sistema. L'agente VPN per client sicuri utilizza il profilo VPN per rilevare che la funzionalità tunnel computer è abilitata. Se la funzionalità tunnel computer è abilitata, l'agente avvia l'applicazione client di gestione per avviare una connessione tunnel computer. L'applicazione client di gestione utilizza la voce host del profilo VPN per avviare la connessione. Quindi, il tunnel VPN viene stabilito come al solito, con un'eccezione: durante la connessione di un tunnel della macchina non viene eseguito alcun aggiornamento software in quanto il tunnel della macchina deve essere trasparente per l'utente.

L'utente avvia un tunnel VPN tramite il client protetto, che attiva la terminazione del tunnel del computer. Alla terminazione del tunnel macchina, la creazione del tunnel utente continua normalmente.

L'utente disconnette il tunnel VPN, che attiva la riattivazione automatica del tunnel del computer.



Limitazioni

- Interazione utente non supportata.
- L'autenticazione basata su certificati tramite l'archivio certificati del computer (Windows) è supportata solo.
- Viene applicata la verifica rigorosa dei certificati del server.
- Proxy privato non supportato.
- Un proxy pubblico non è supportato (il valore ProxyNative è supportato sulle piattaforme in cui le impostazioni Proxy nativo non vengono recuperate dal browser).
- Script di personalizzazione client sicuri non supportati

Configurazione

Metodo 1 - Configurare il tunnel del computer con l'utente machine@sse.com

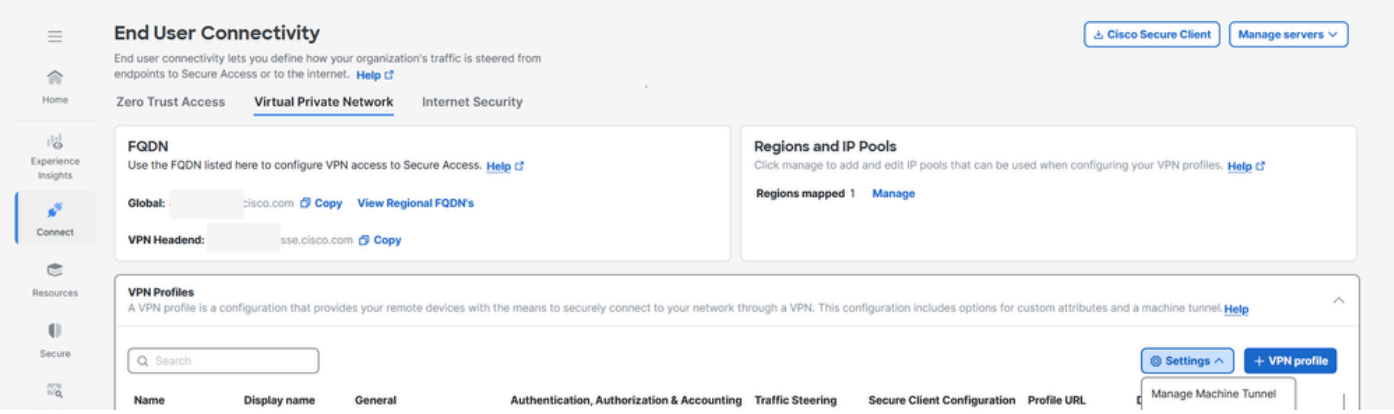
Passaggio 1 - Impostazioni generali

Configurare le impostazioni generali, inclusi il dominio e i protocolli utilizzati dal tunnel del computer.

1. Selezionare Connect > End User Connectivity > Virtual Private Network (Connetti > Connettività utente finale > Rete privata virtuale).

2. Passare a Profili VPN e configurare le impostazioni per il tunnel del computer.

r. Fare clic su Impostazioni, quindi scegliere Gestisci tunnel computer dall'elenco a discesa.

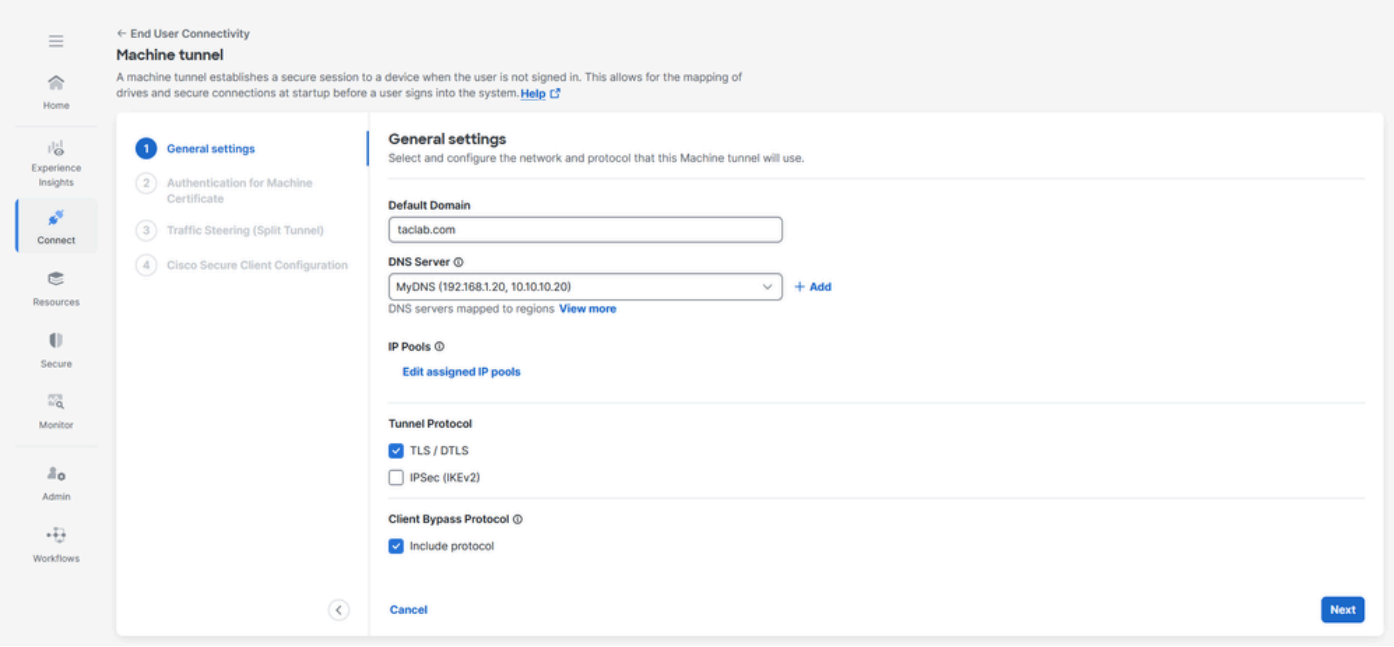


3. Immettere il dominio predefinito.
4. Il server DNS mappato tramite la pagina Gestisci aree e pool IP è impostato come server predefinito. È possibile accettare il server DNS predefinito, scegliere un altro server DNS dall'elenco a discesa oppure fare clic su + Aggiungi per aggiungere una nuova coppia di server DNS. Se si seleziona un altro server DNS o si aggiunge un nuovo server DNS, questo server predefinito viene sovrascritto.
5. Selezionare un pool IP per area dall'elenco a discesa Pool IP. Ai profili VPN deve essere assegnato almeno un pool IP in ogni area per una configurazione valida.
6. Selezionare il protocollo tunnel utilizzato dal tunnel di questo computer:
    - TLS/DTLS
    - IPSec (IKEv2)

      Selezionare almeno un protocollo.
7. Facoltativamente, selezionare Includi protocollo per applicare il protocollo di bypass client.

    r. Se il protocollo IP è abilitato per il protocollo Client Bypass Protocol e non è configurato un pool di indirizzi per tale protocollo (in altre parole, l'ASA non ha assegnato al client alcun indirizzo IP per tale protocollo), il traffico IP che utilizza tale protocollo non verrà inviato tramite il tunnel VPN. Deve essere inviato fuori dal tunnel.

    b. Se il protocollo Client Bypass Protocol è disabilitato e un pool di indirizzi non è configurato per tale protocollo, il client rifiuta tutto il traffico per tale protocollo IP dopo aver stabilito il tunnel VPN.



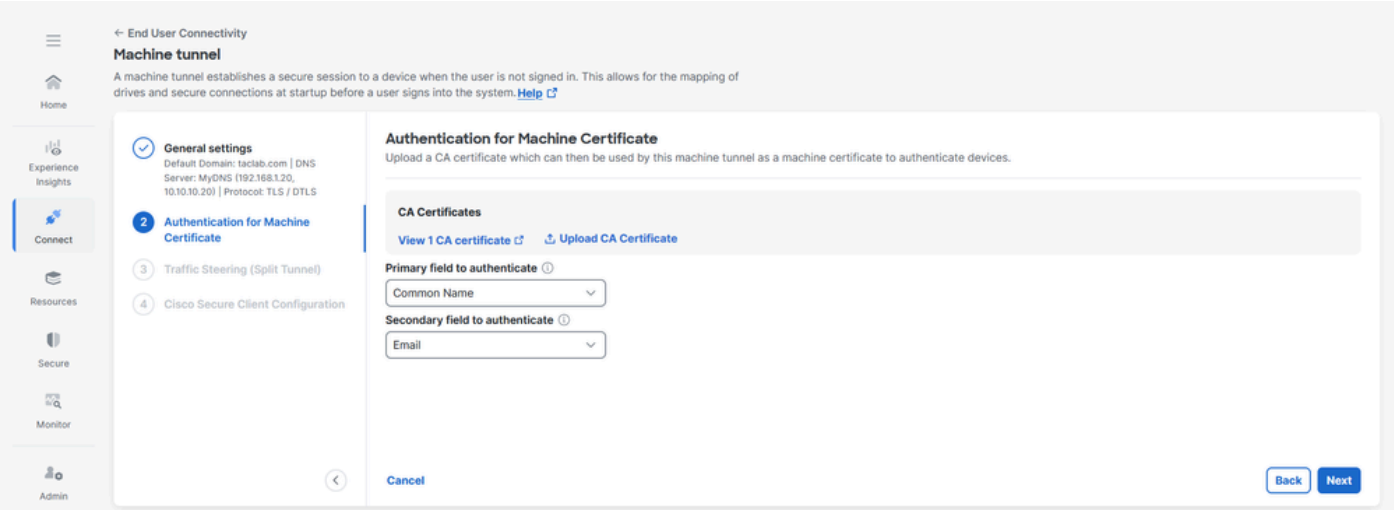
8. Fare clic su Avanti

Passaggio 2 - Autenticazione per certificato computer

Il tunnel del computer è trasparente per l'utente finale e si disconnette automaticamente quando l'utente avvia una sessione VPN. Per creare il tunnel senza l'interazione dell'utente, viene utilizzata l'autenticazione basata su certificati.

1. Scegliere i certificati CA dall'elenco o fare clic su Carica certificati CA

2. Selezionare i campi di autenticazione basata su certificato. Per ulteriori informazioni, vedere [campi di autenticazione basati su certificati]



3. Fare clic su Avanti

Fase 3 - Traffic Steering (Split Tunnel)

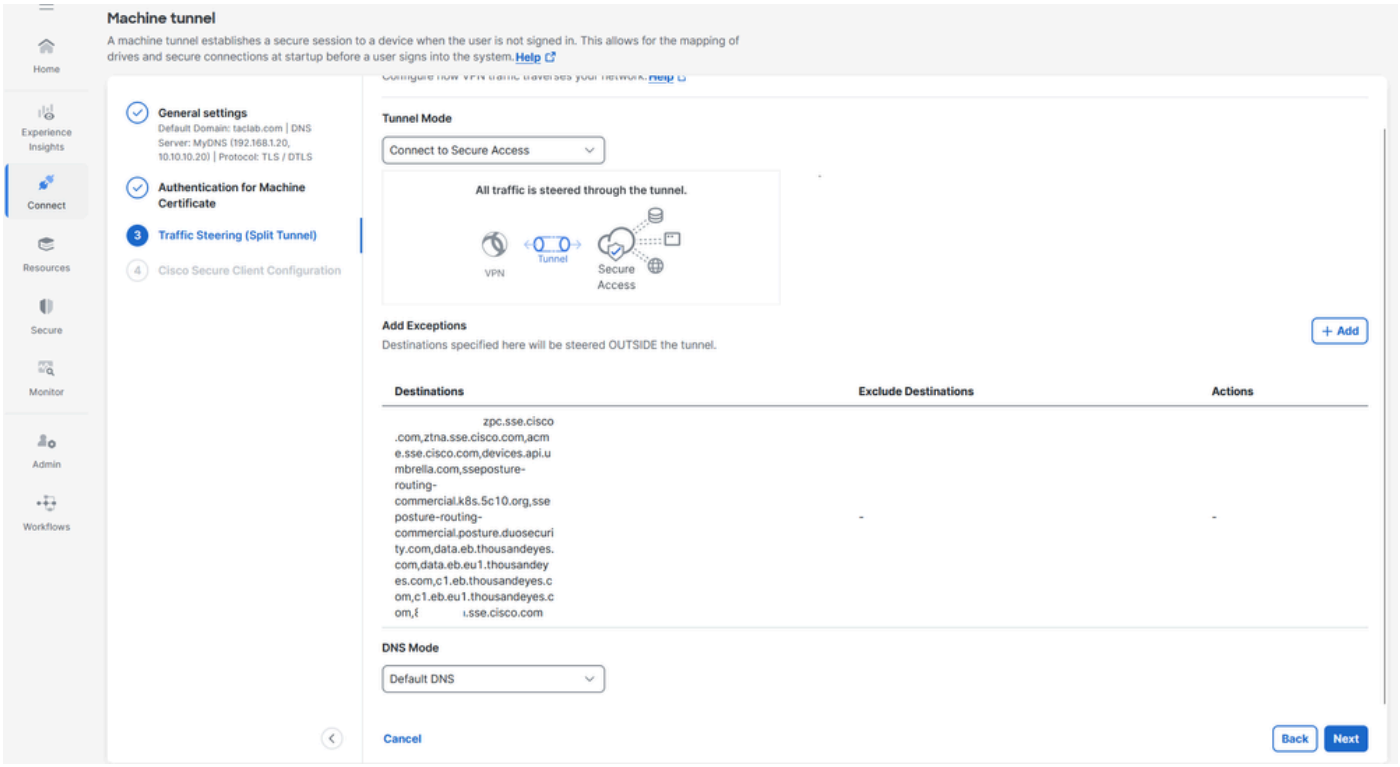
Per Traffic Steering (Split Tunnel), è possibile configurare un tunnel computer in modo da

mantenere una connessione tunnel completa a Secure Access oppure configurarlo in modo da utilizzare una connessione tunnel divisa per indirizzare il traffico attraverso la VPN solo se necessario.Per ulteriori informazioni, vedere Traffic Steering del tunnel computer

1. Selezionare la modalità tunnel

2. A seconda della modalità tunnel selezionata, è possibile aggiungere eccezioni

3. Seleziona modalità DNS

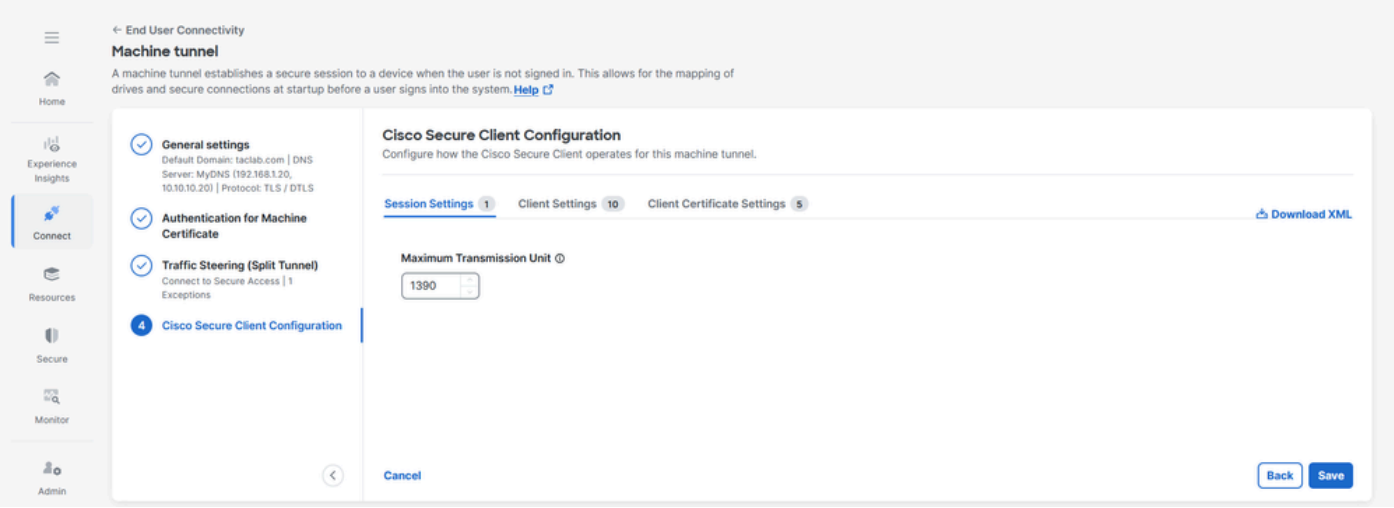


4. Fare clic su Avanti

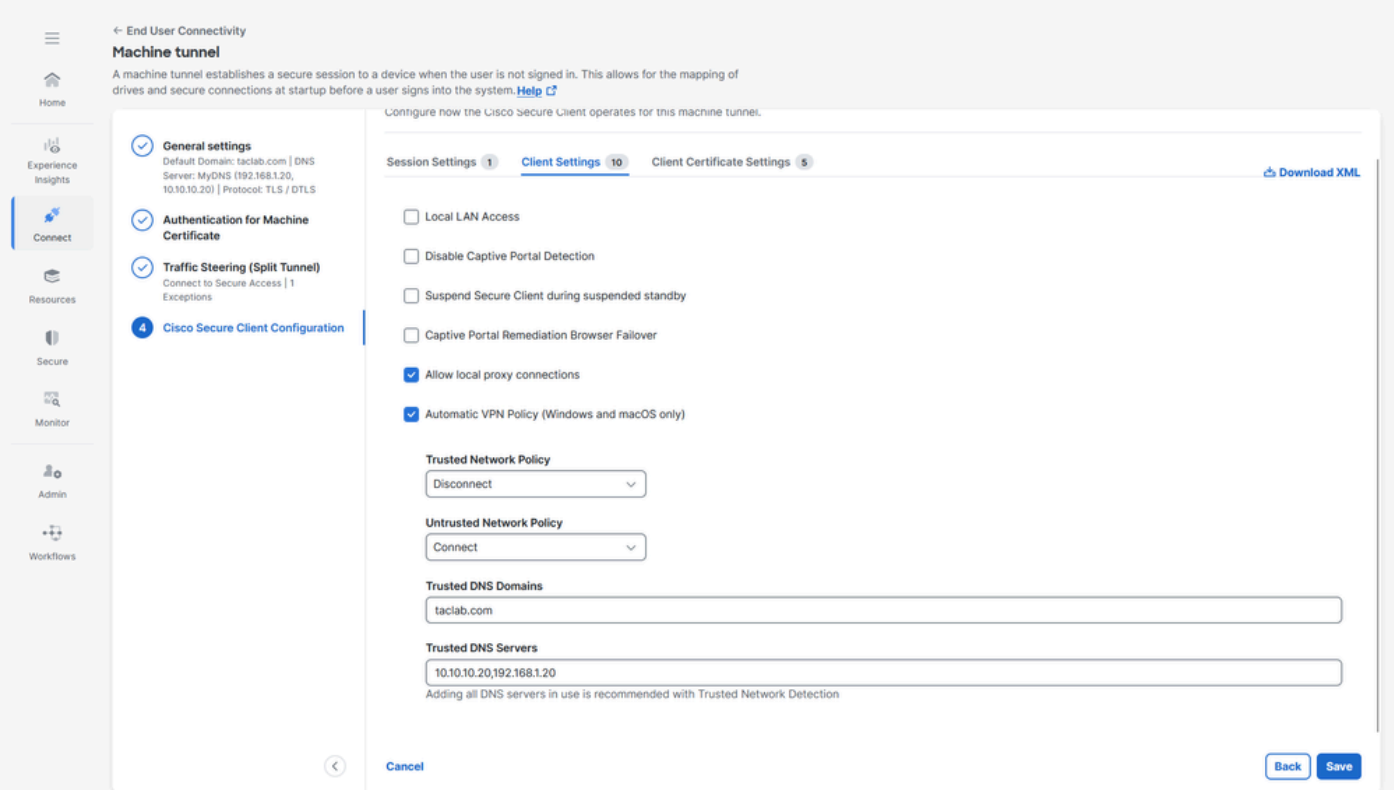
Fase 4 - Configurazione Cisco Secure Client

È possibile modificare un sottoinsieme delle impostazioni di Cisco Secure Client in base alle esigenze di un particolare tunnel del computer VPN. Per ulteriori informazioni, vedere Configurazione client sicura

1. Verificare Maximum Transmission Unit, ossia le dimensioni massime del pacchetto che può essere inviato nel tunnel VPN senza frammentazione



2. Impostazioni client , per ulteriori informazioni fare riferimento a [Impostazioni client tunnel computer]



3. Impostazioni certificato client, selezionare le opzioni di conseguenza

a. Sostituzione archivio certificati di Windows - Consente a un amministratore di indicare a Secure Client di utilizzare i certificati nell'archivio certificati del computer Windows (sistema locale) per l'autenticazione dei certificati del client.

b. Selezione automatica dei certificati - Quando sul gateway sicuro è configurata l'autenticazione con più certificati

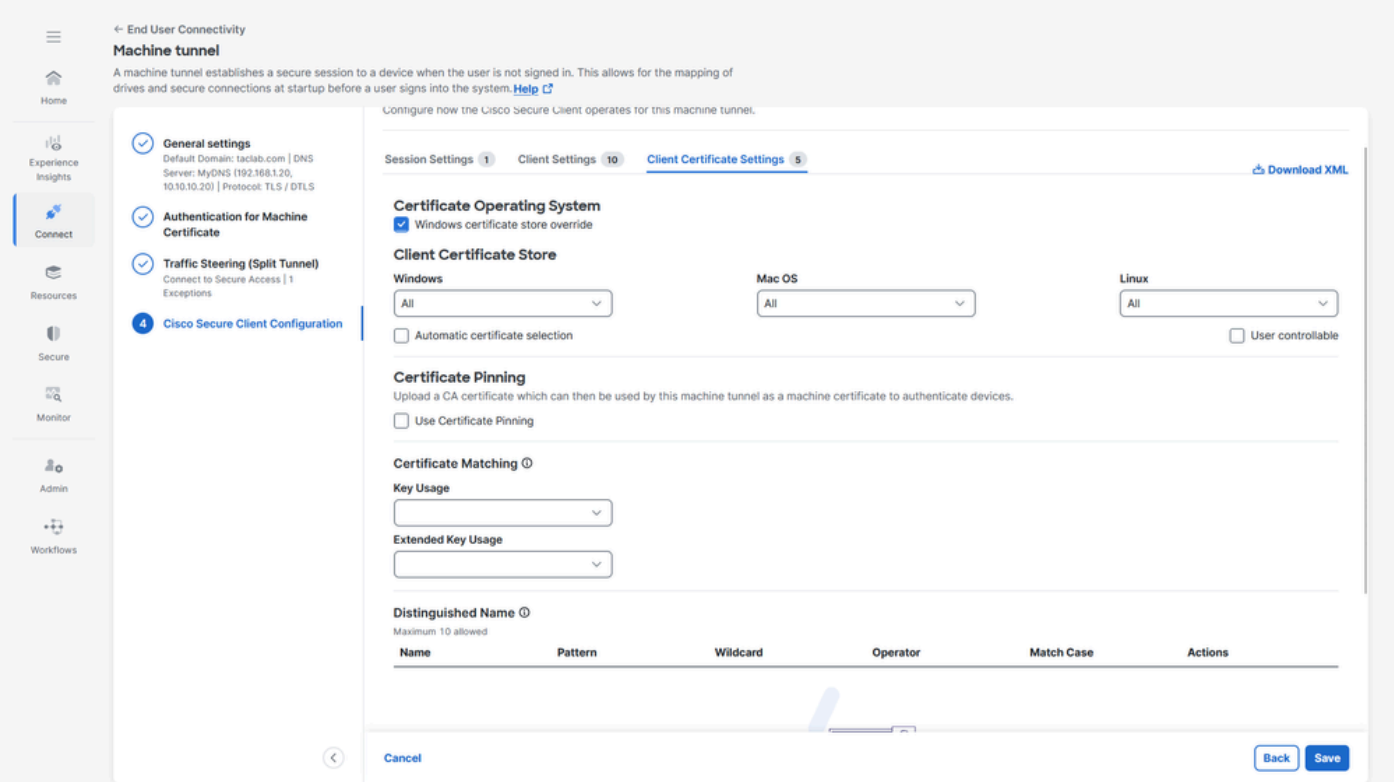
c. Certificate Pinning - Certificato CA che può essere utilizzato dal tunnel del computer come certificato del computer per autenticare i dispositivi

d. Corrispondenza certificato - Se non viene specificato alcun criterio di corrispondenza certificato, Cisco Secure Client applica le regole di corrispondenza certificato

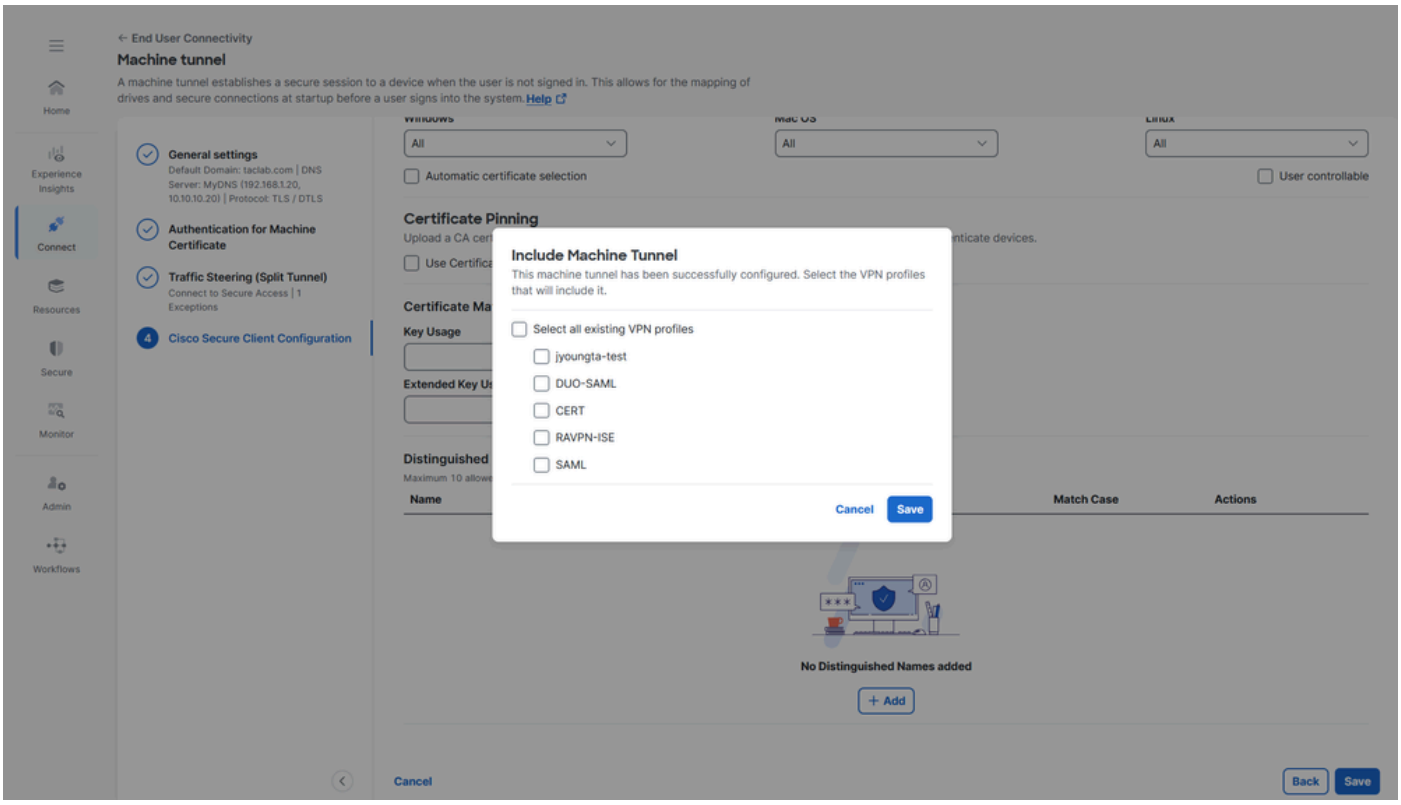
i. Utilizzo chiave: Firma_Digitale

ii. Utilizzo chiave esteso: Autenticazione client

e. Nome distinto: specifica i nomi distinti (DN) per i criteri di corrispondenza esatta nella scelta dei certificati client accettabili. Quando si aggiungono più nomi distinti, ogni certificato viene confrontato con tutte le voci e tutte devono corrispondere.

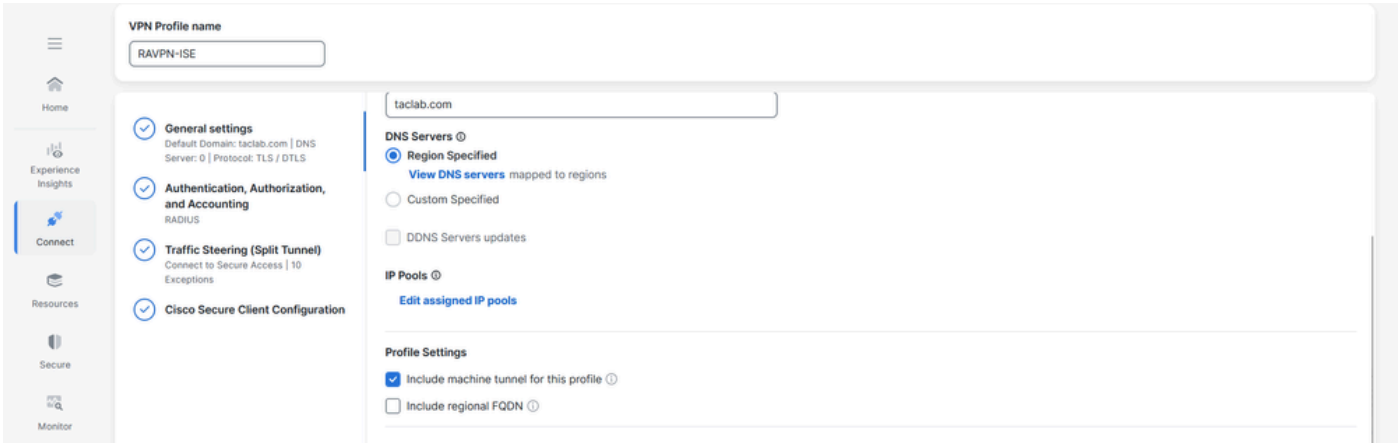


4. Assegnare il profilo del tunnel computer a un profilo VPN utente, fare clic su Salva, quindi è disponibile un'opzione per selezionare i profili VPN utente



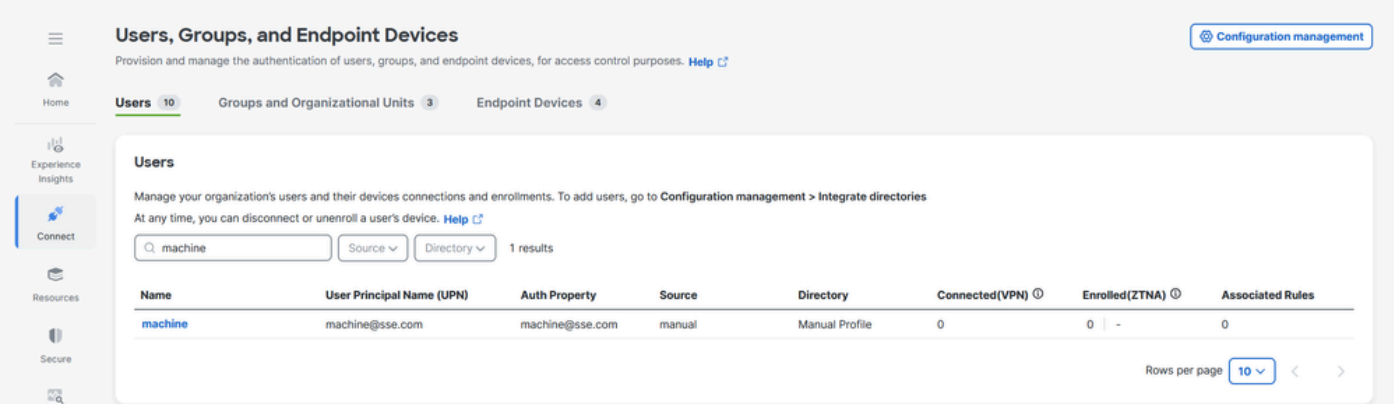
5. Fare clic su Salva

6. Verificare se il profilo del tunnel computer è collegato a un profilo VPN utente



Passaggio 5 - Verificare se l'utente machine@sse.com è presente in Cisco Secure Access

1. Passare a Connetti > Utenti, gruppi e dispositivi endpoint > Utenti



2. Se l'utente machine@sse.com non è presente, eseguire l'importazione manualmente. Per ulteriori informazioni, vedere Importazione manuale di utenti e gruppi

Passaggio 6 - Generare un certificato CA firmato per machine@sse.com

1. Generare una richiesta di firma del certificato

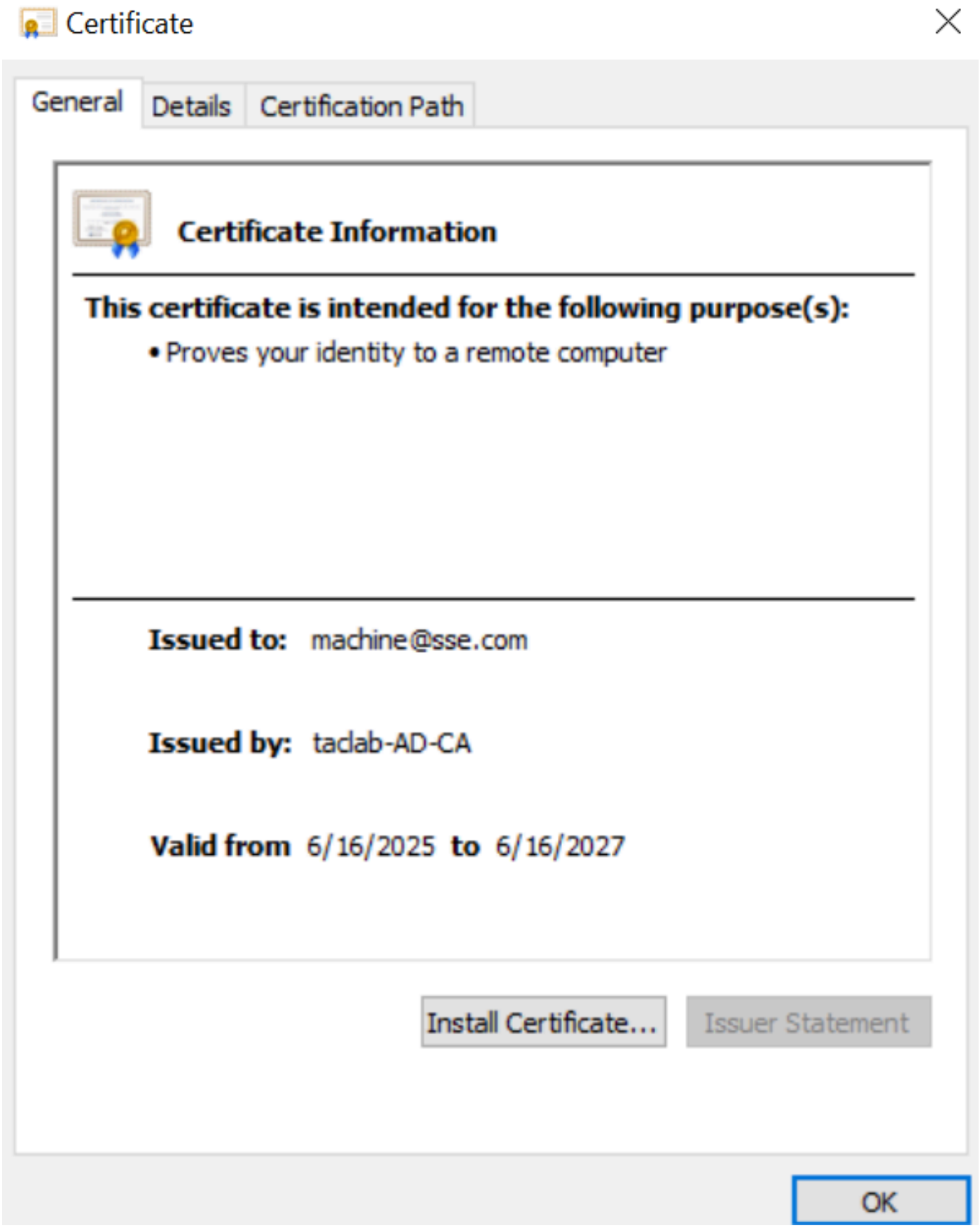
r. Possiamo utilizzare qualsiasi software di generazione CSR online CSR Generator o una CLI openssl

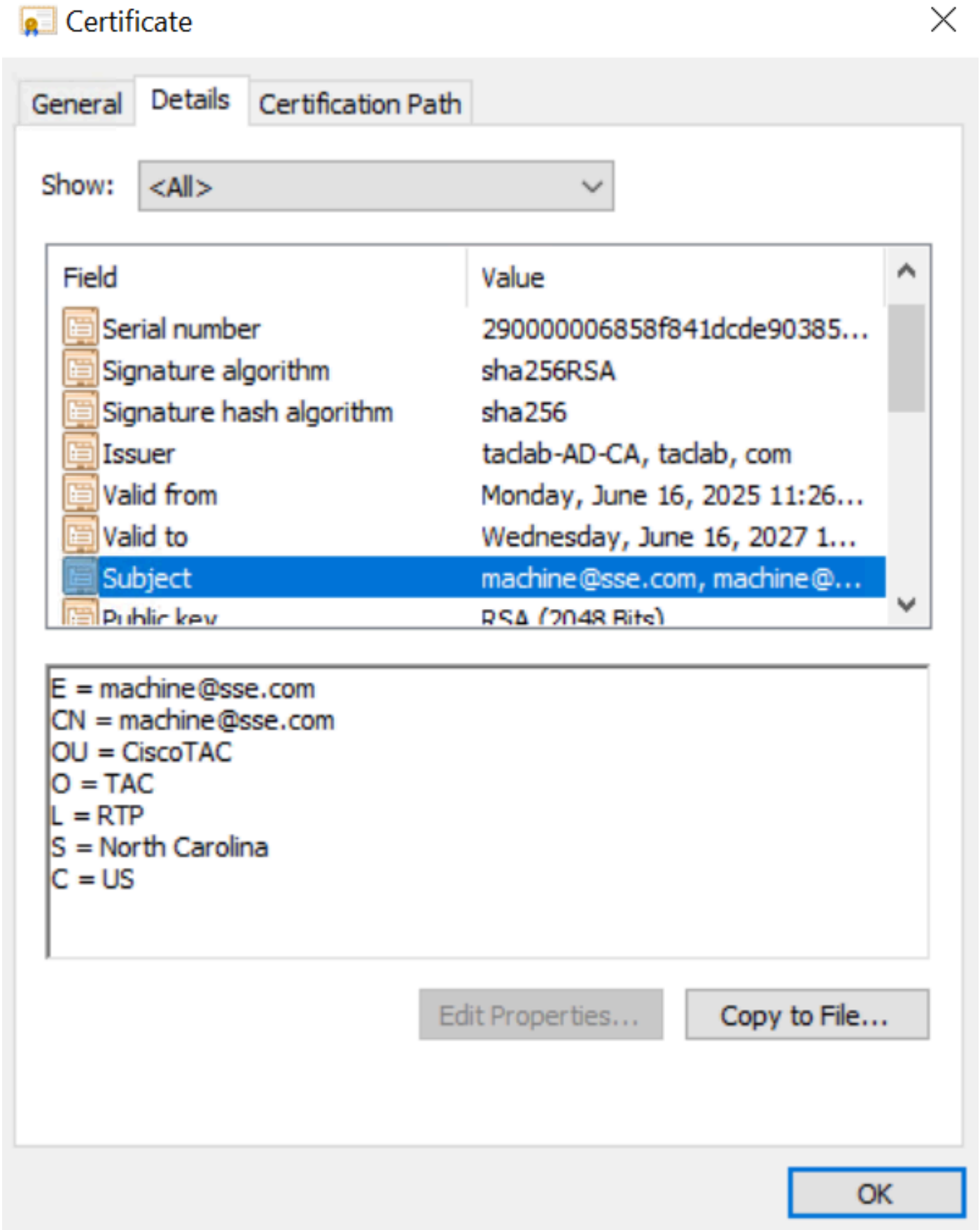
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr

```
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. Copiare il CSR e generare un certificato del computer


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



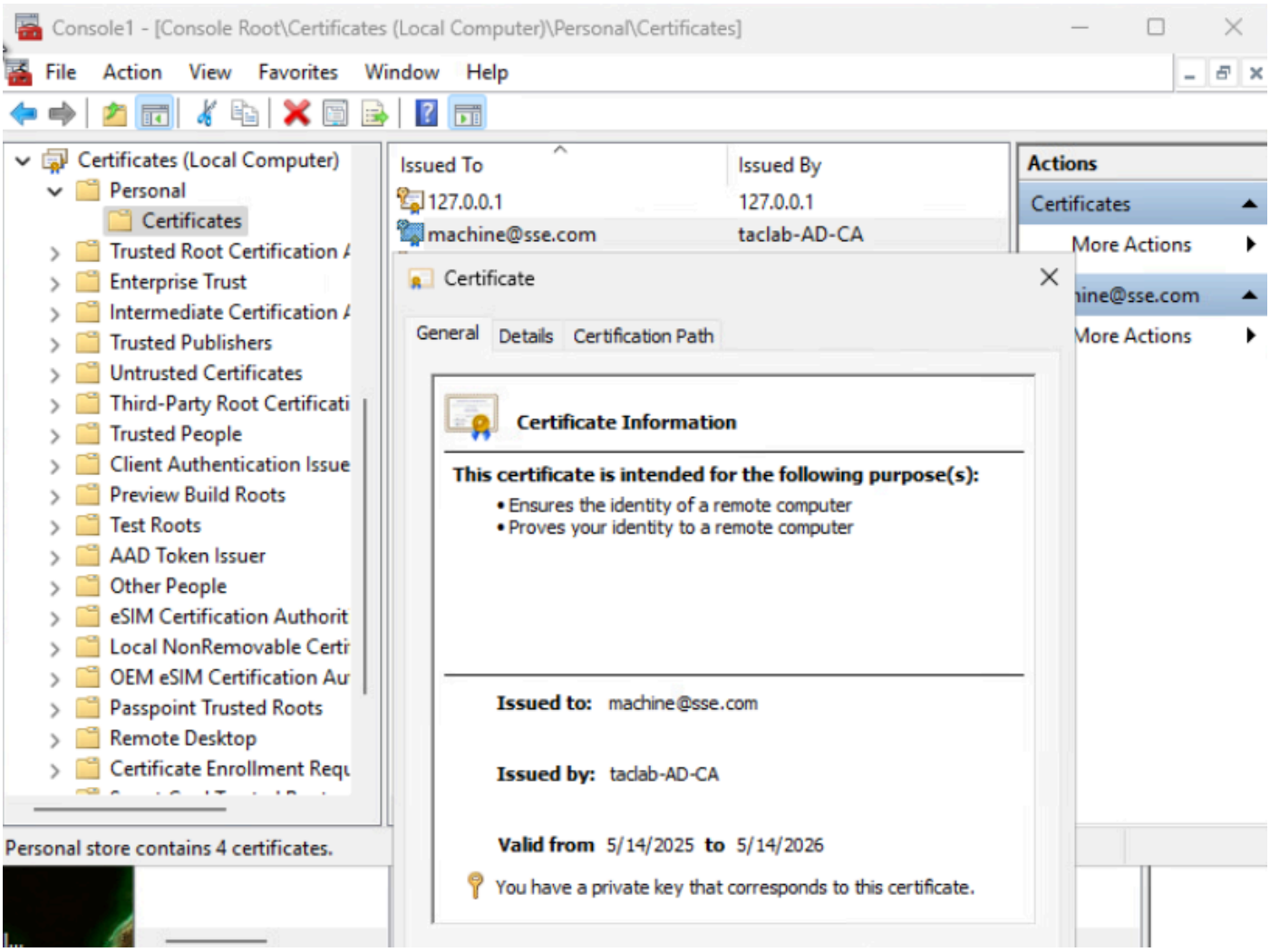
3. Convertire il certificato del computer nel formato PKCS12 utilizzando rispettivamente la chiave e il certificato generati nei passaggi precedenti (passaggio 1 e 2)

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#
```

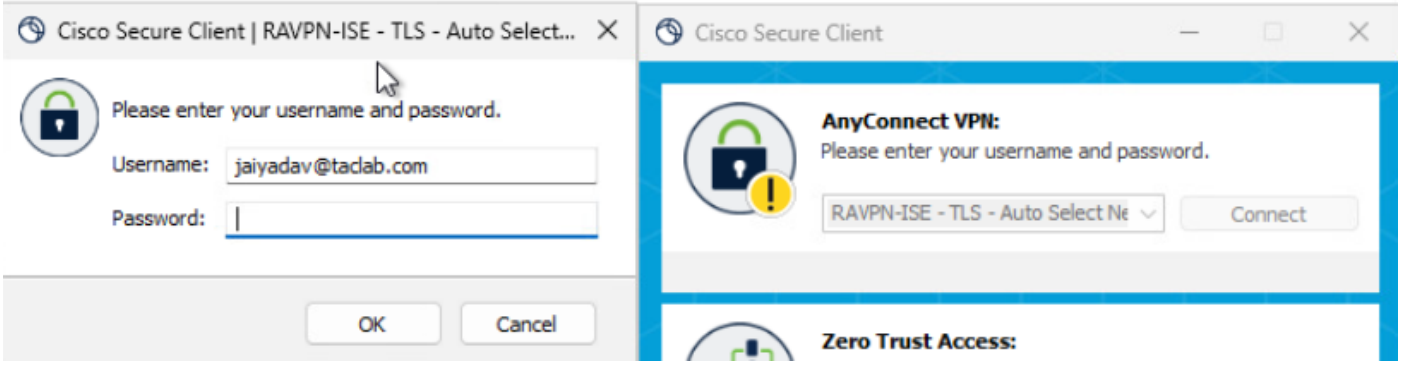
Fase 7 - Importazione del certificato del computer in un computer di prova

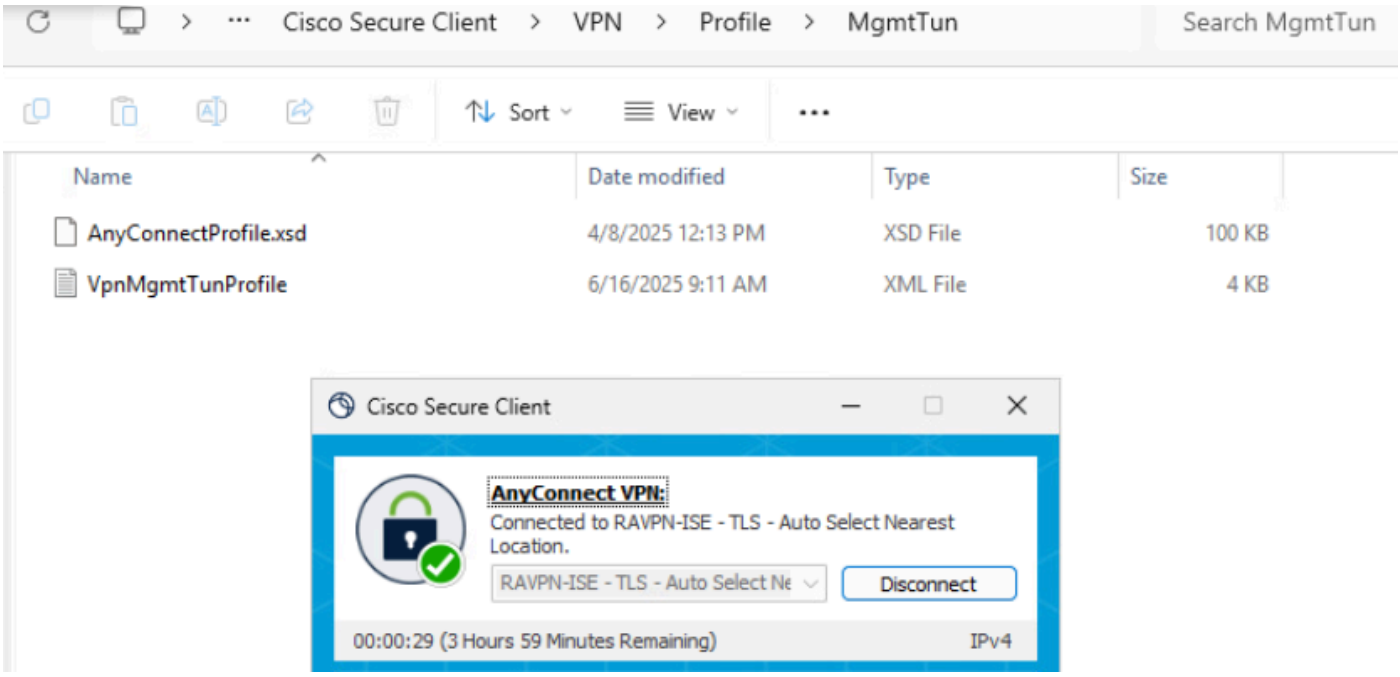
r. Importa il certificato del computer PKCS12 nell'archivio locale o del computer



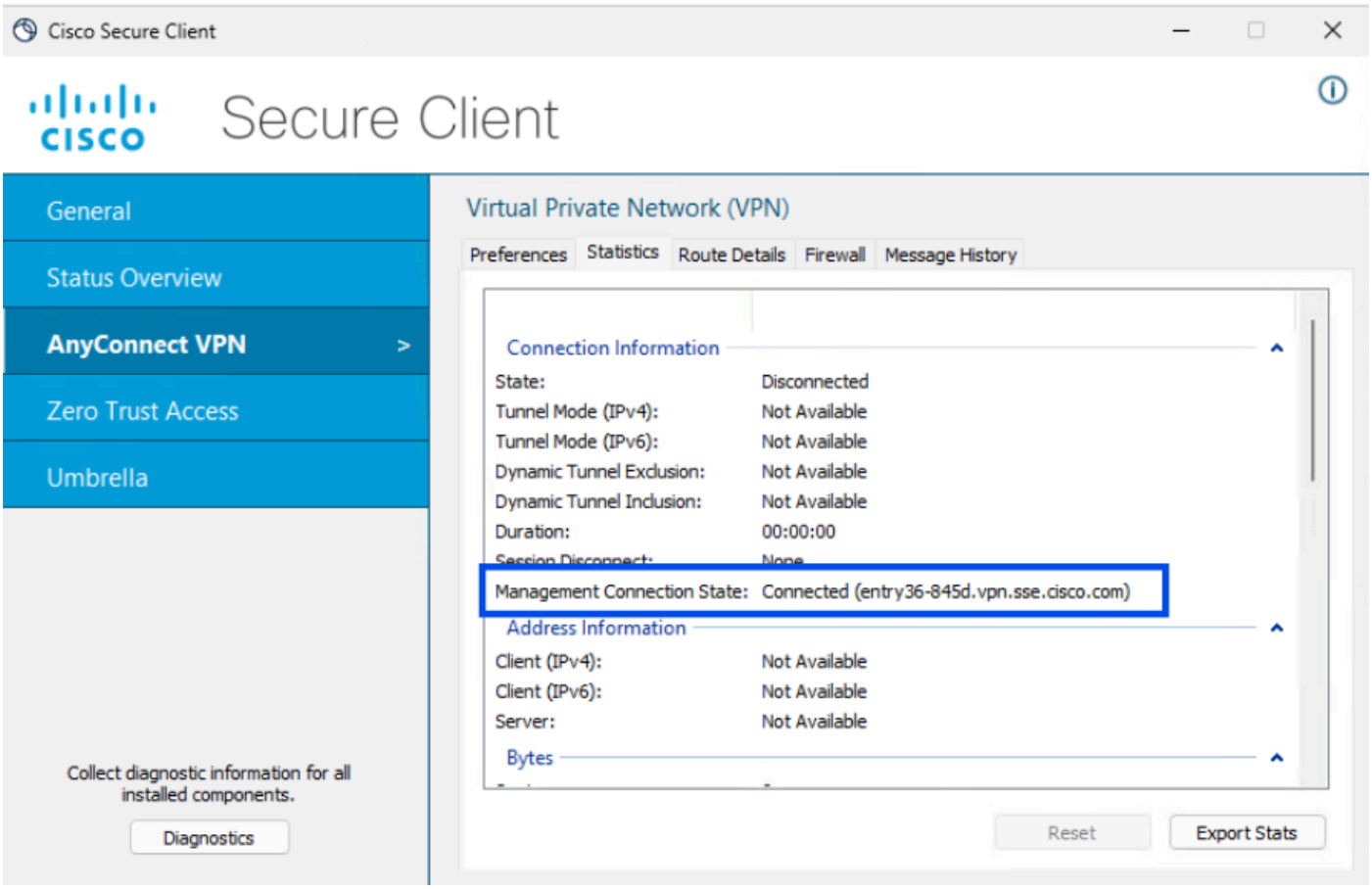
Fase 8 - Connessione al tunnel del computer

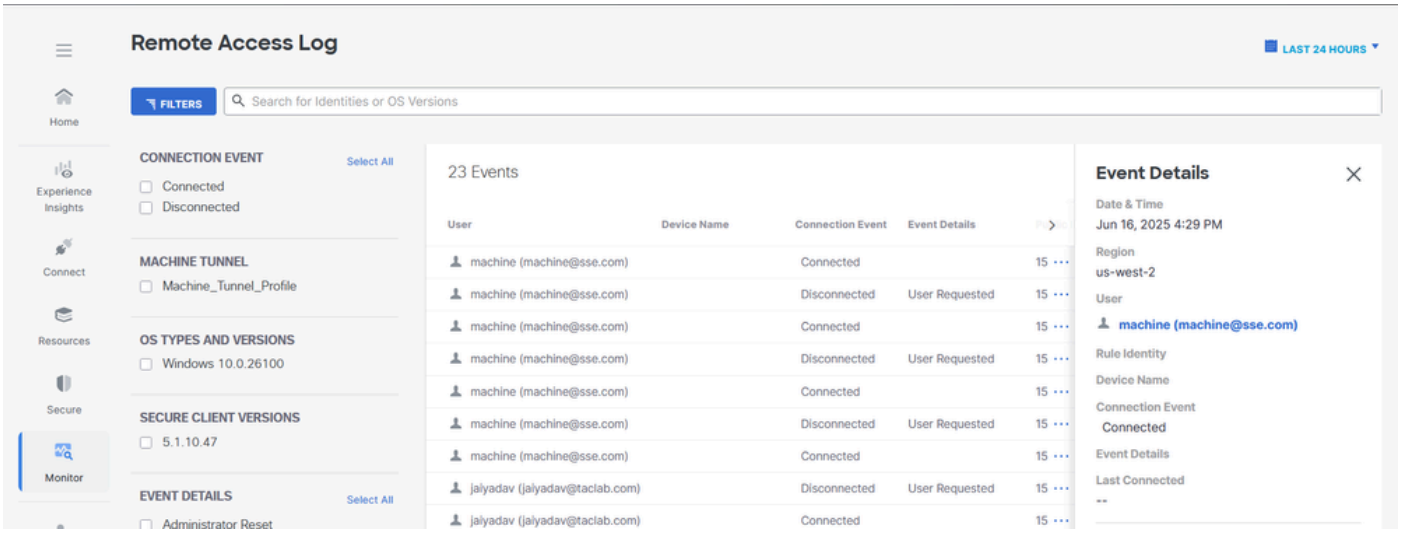
r. Connetti a tunnel utente , attiva il profilo xml del computer da scaricare.





b. Verifica connettività tunnel computer





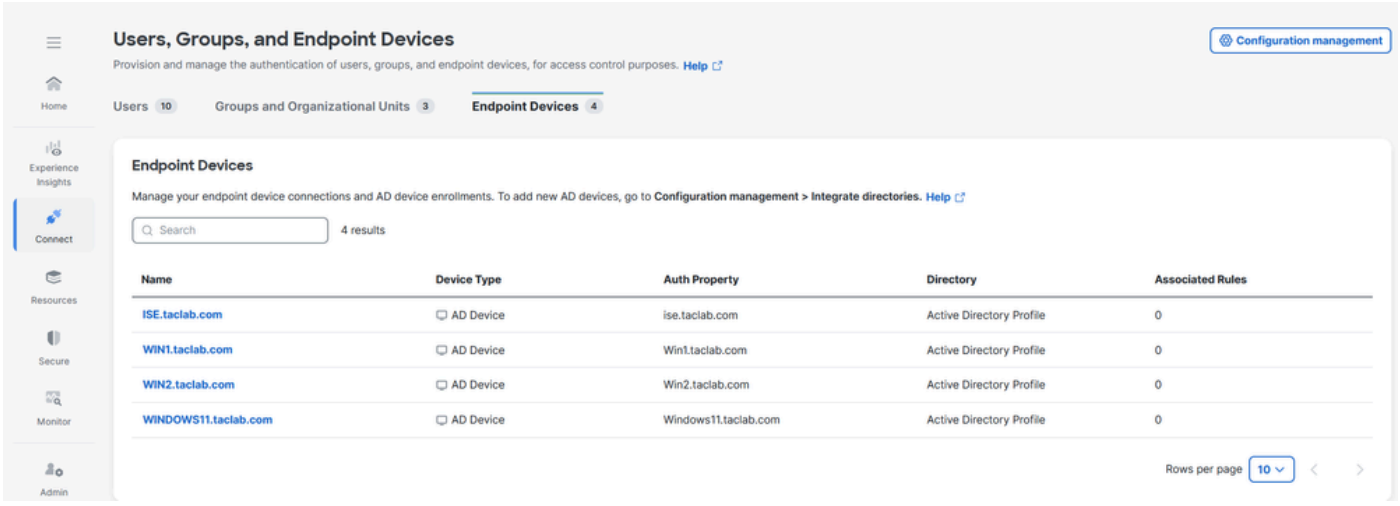
Metodo 2 - Configurazione del tunnel del computer con il certificato dell'endpoint

In questo caso, per autenticare il campo Primario, scegliere il campo del certificato che contiene il nome del dispositivo (nome computer). Secure Access utilizza il nome del dispositivo come identificatore del tunnel del computer. Il formato del nome del computer deve corrispondere al formato dell'identificatore di dispositivo scelto

Eseguire i passaggi da 1 a 4 per la configurazione del tunnel del computer

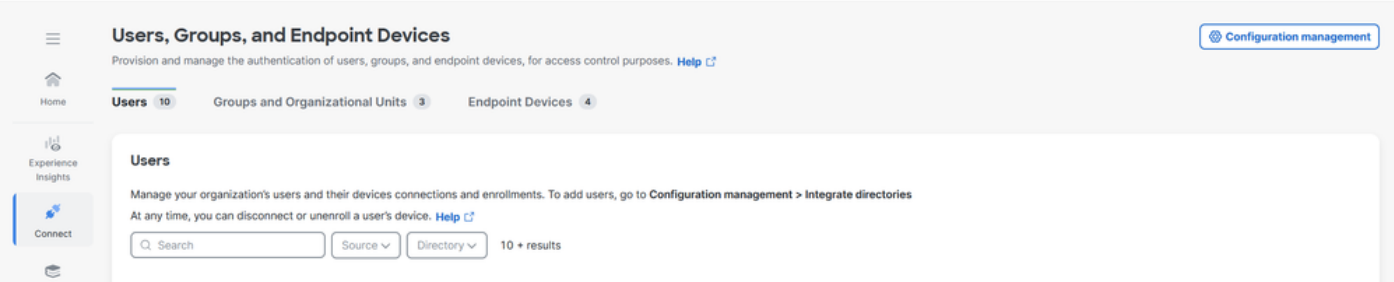
Passaggio 5 - Configurare il connettore AD per l'importazione degli endpoint su Cisco Secure Access.

Per ulteriori informazioni, vedere Integrazione Active Directory permanente

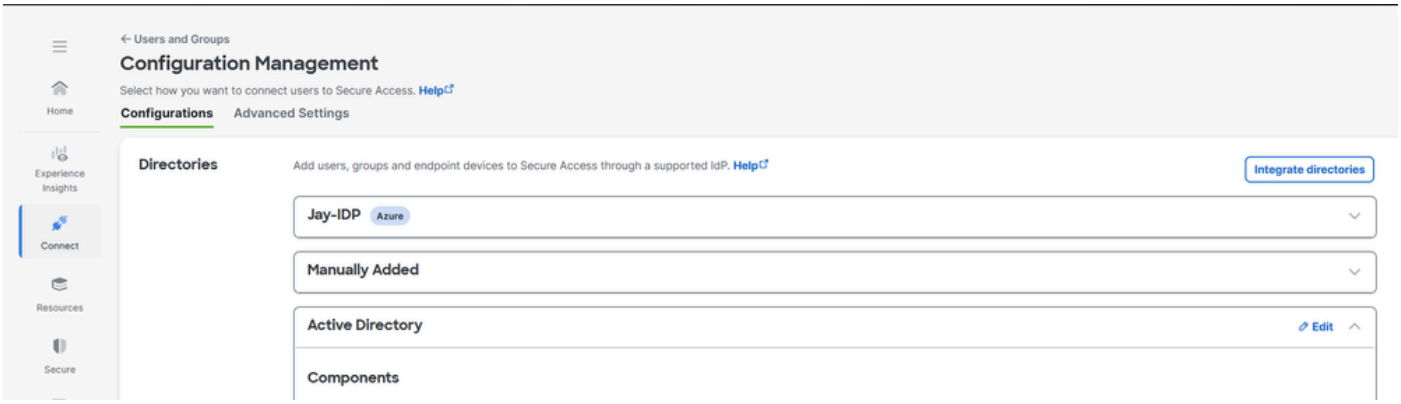


Passaggio 6 - Configurazione dell'autenticazione dei dispositivi di endpoint

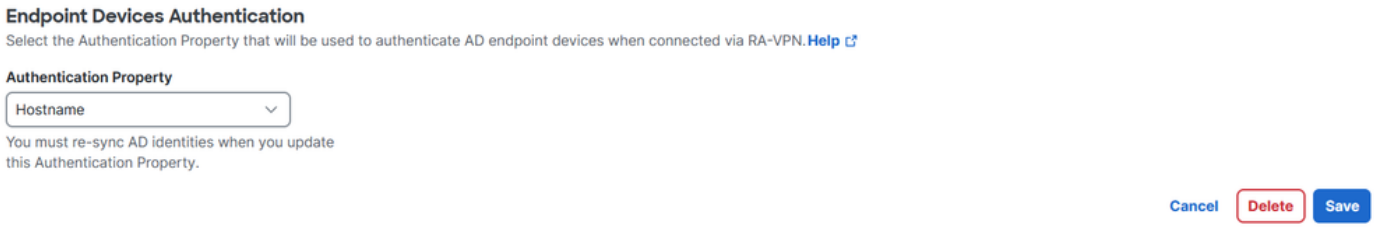
1. Passare a Connetti > Utenti, gruppi e dispositivi endpoint.
2. Fare clic su Gestione configurazione



3. In Configurazioni modificare Active Directory



4. Impostare la proprietà di autenticazione Dispositivi endpoint su Hostname



5. Fare clic su Salva e riavviare i servizi di AD Connector sui server in cui è installato

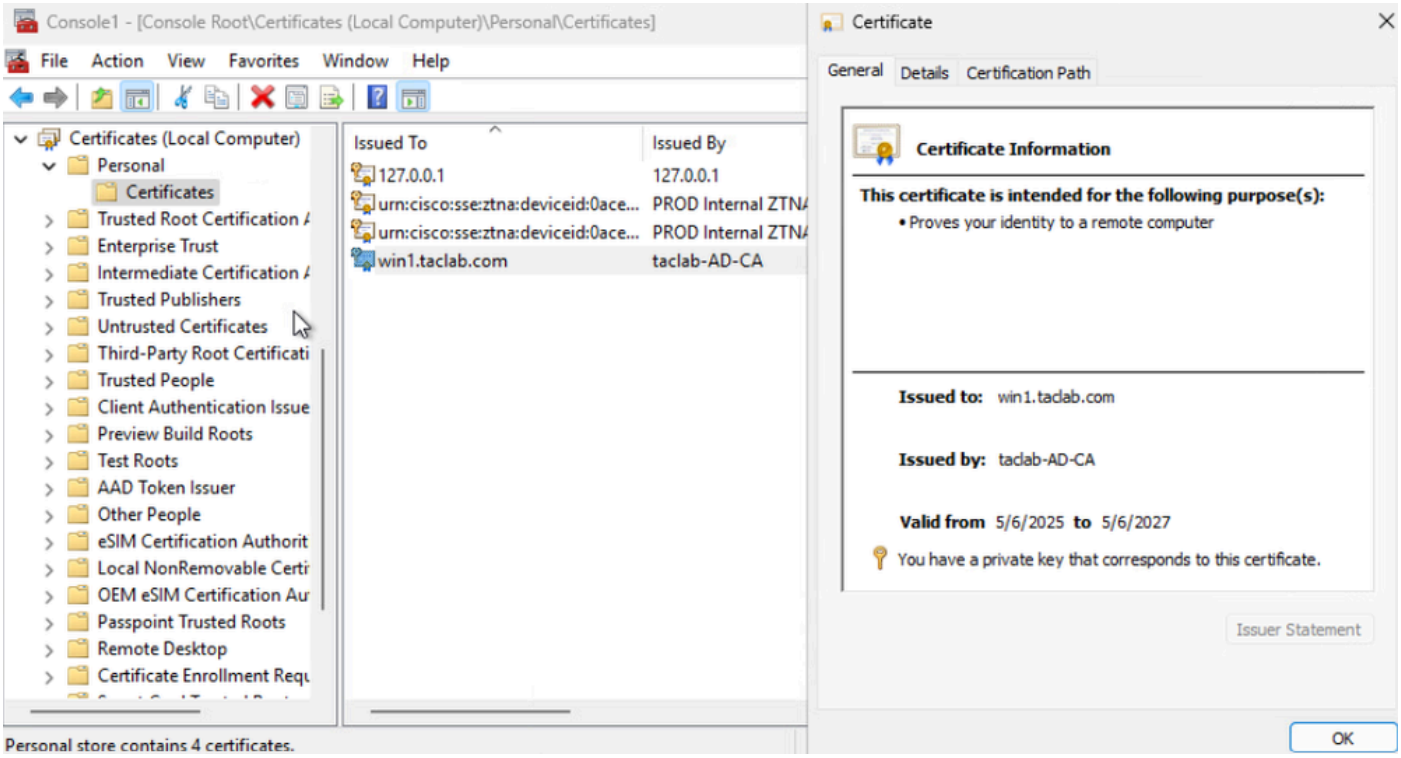
Fase 7 - Generazione e importazione del certificato dell'endpoint

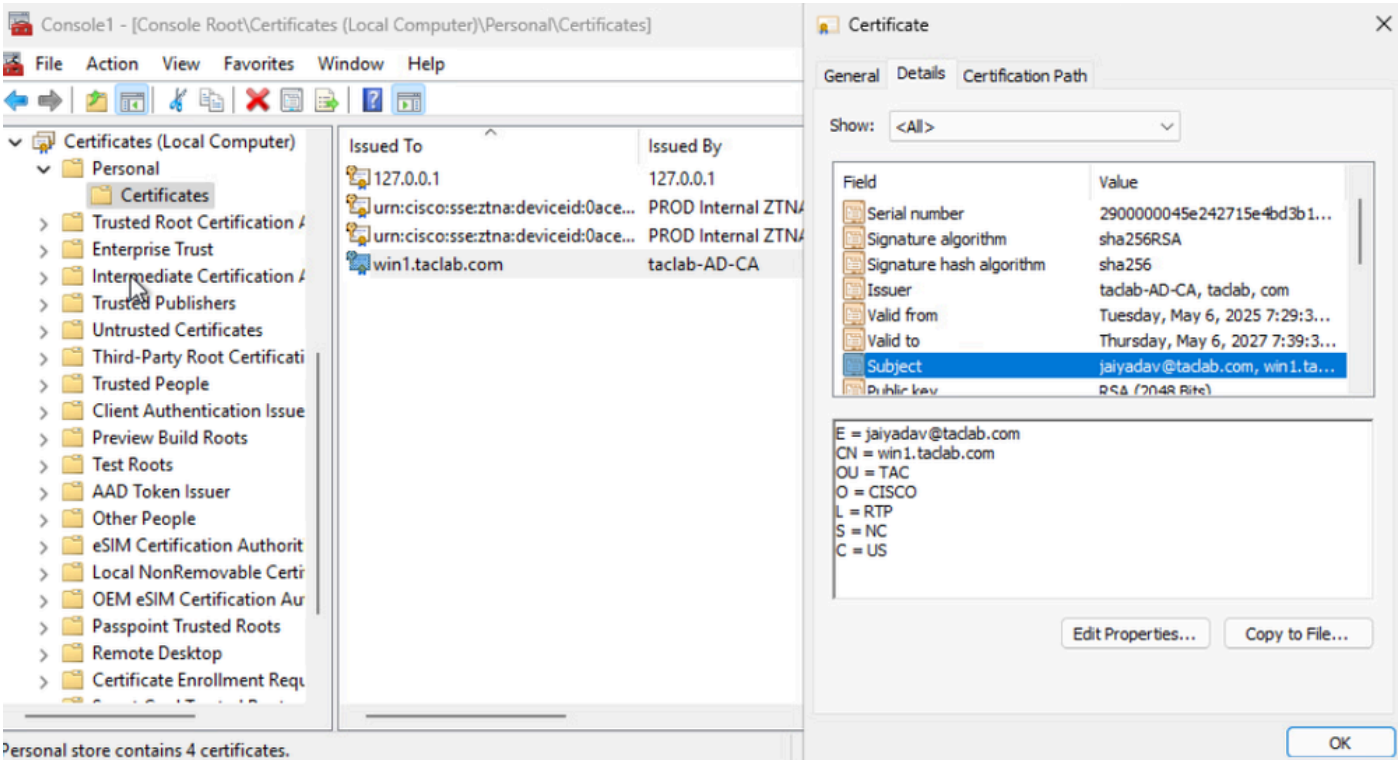
r. generare CSR , aprire un generatore CSR o uno strumento OpenSSL

b. Genera un certificato endpoint dalla CA

c. Convertire il file .cert nel formato PKCS12

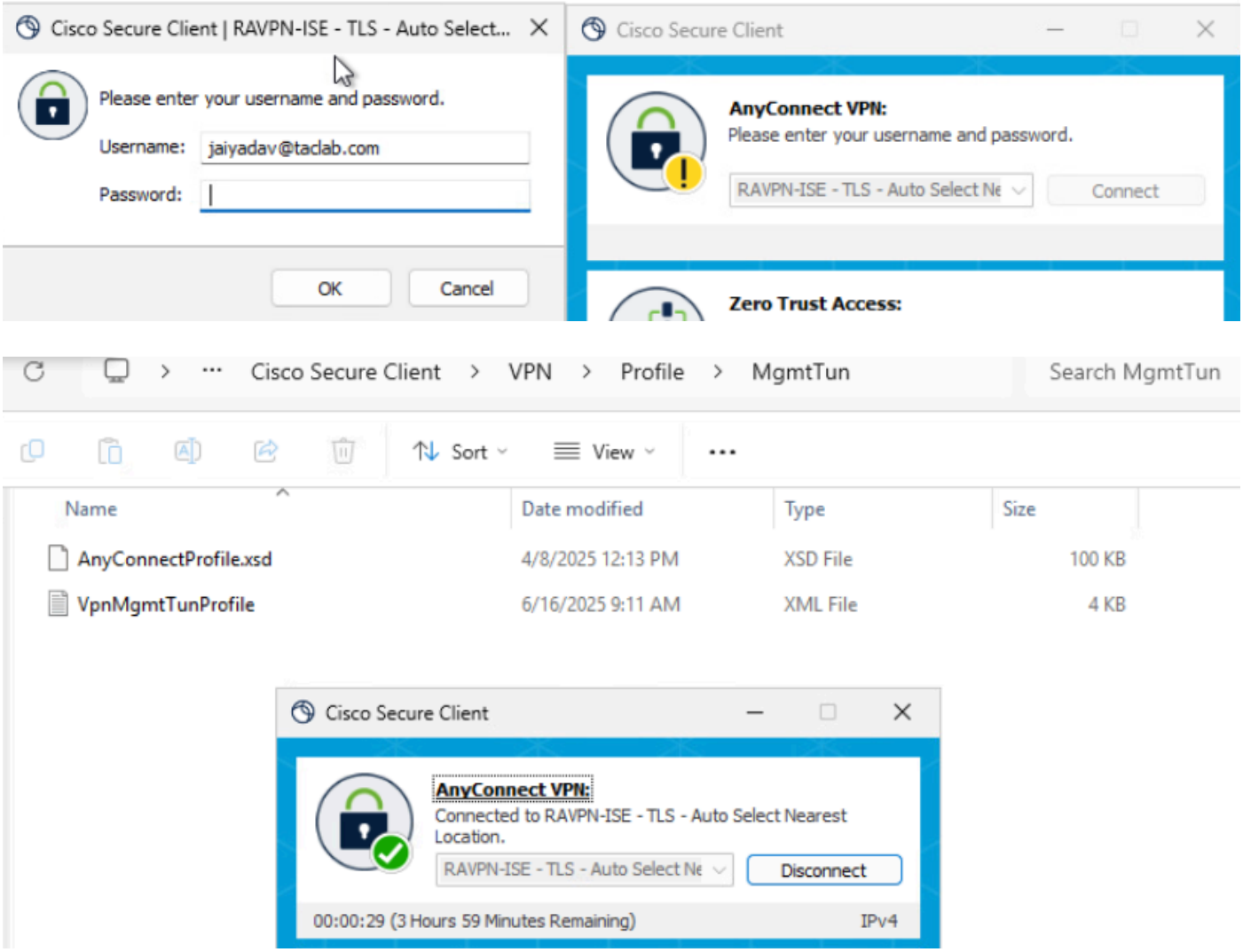
d. Importa il certificato PKCS12 nell'archivio certificati dell'endpoint



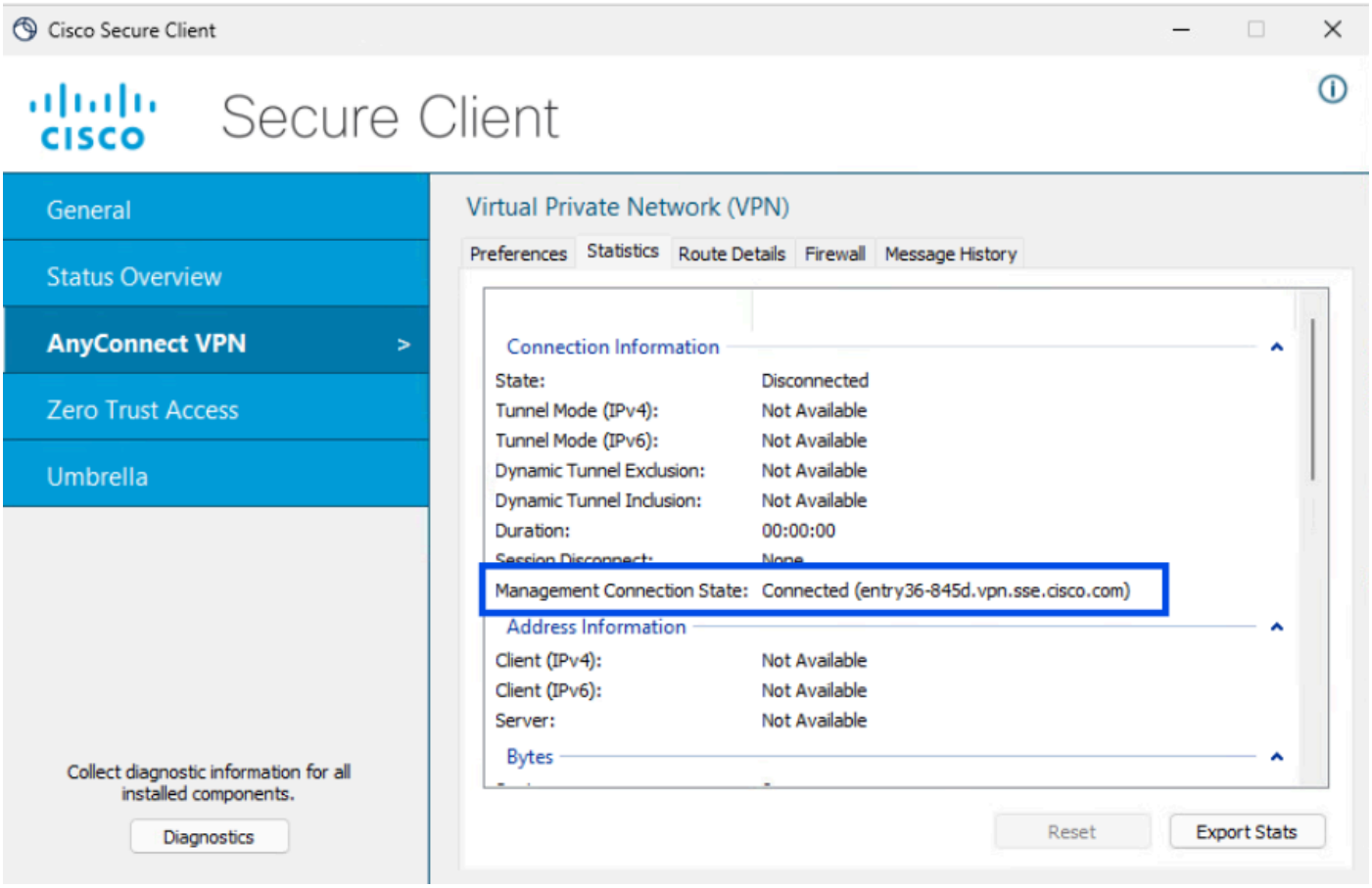


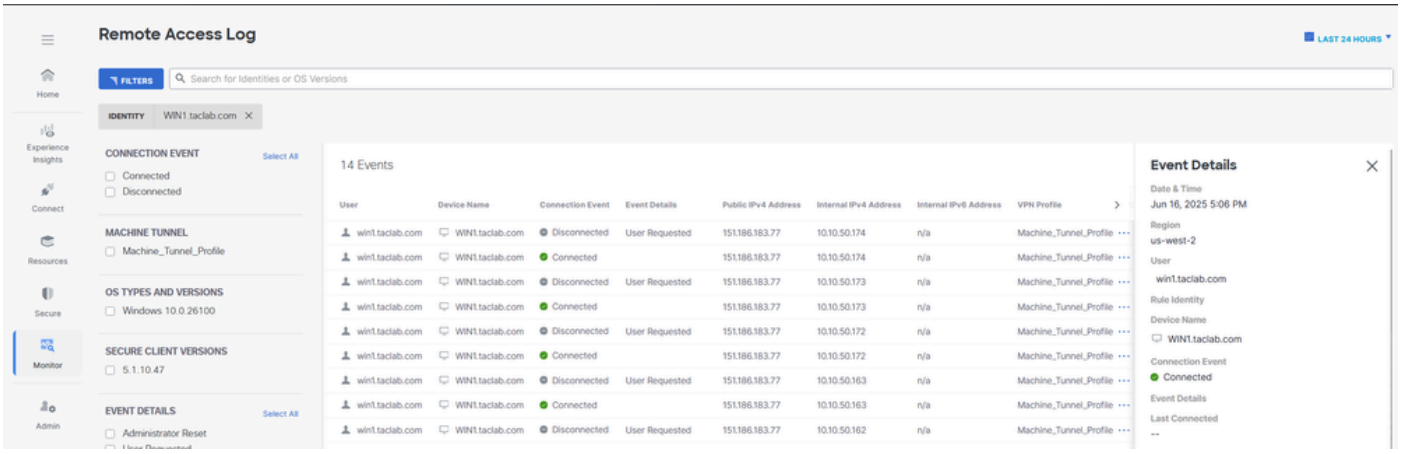
Fase 8 - Connessione al tunnel del computer

r. Connetti a tunnel utente , attiva il download del profilo XML del tunnel computer



b. Verifica connettività tunnel computer





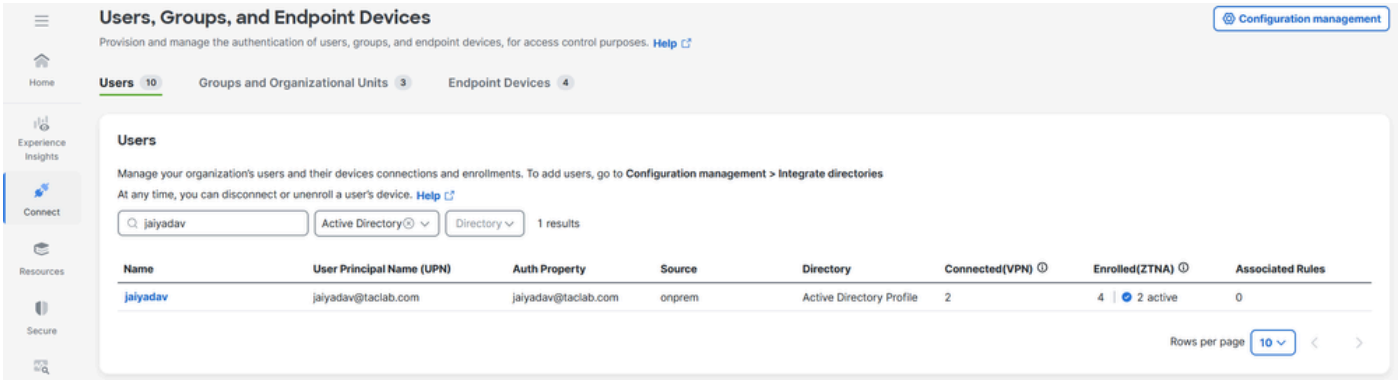
Metodo 3 - Configurare il tunnel del computer utilizzando il certificato utente

In questo caso, per autenticare il campo Primario, scegliere il campo del certificato che contiene l'indirizzo di posta elettronica o l'UPN dell'utente. Secure Access utilizza l'indirizzo di posta elettronica o l'UPN come identificatore del tunnel del computer. Il formato del messaggio di posta elettronica o dell'UPN deve corrispondere al formato dell'identificatore di dispositivo scelto

Eseguire i passaggi da 1 a 4 per la configurazione del tunnel della macchina

Passaggio 5 - Configurare il connettore AD in modo da poter importare gli utenti su Cisco Secure Access.

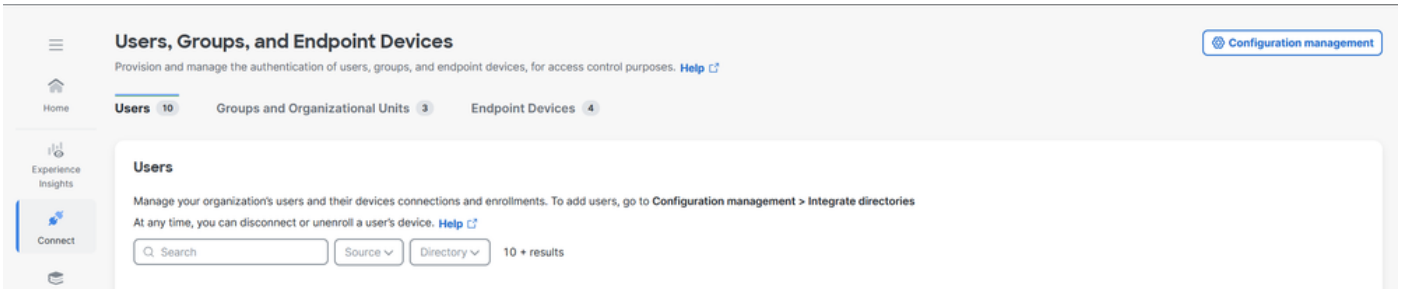
Per ulteriori informazioni, vedere Integrazione Active Directory permanente



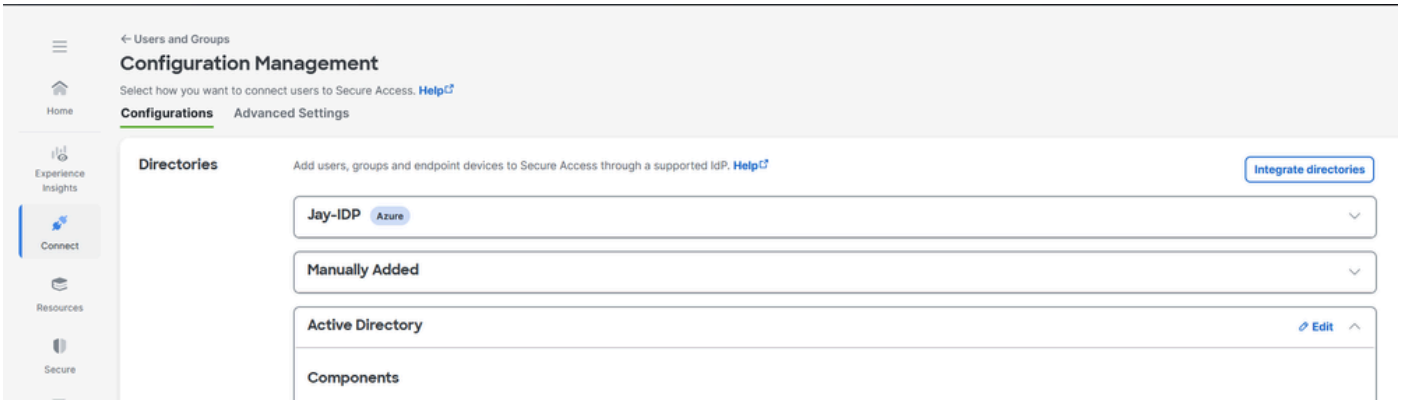
Passaggio 6 - Configurazione dell'autenticazione degli utenti

1. Passare a Connetti > Utenti, gruppi e dispositivi endpoint.

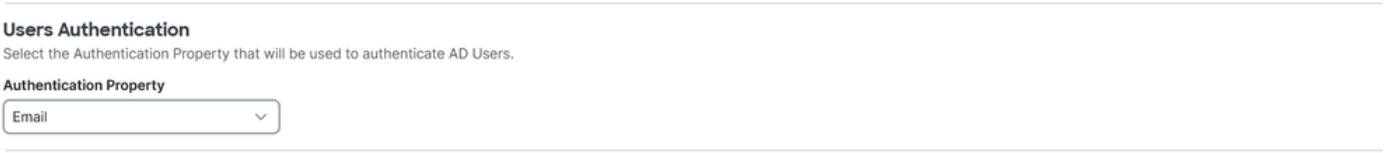
2. Fare clic su Gestione configurazione



3. In Configurazioni modificare Active Directory



4. Impostare la proprietà di autenticazione degli utenti su Posta elettronica



5. Fare clic su Salva e riavviare i servizi di AD Connector sui server in cui è installato

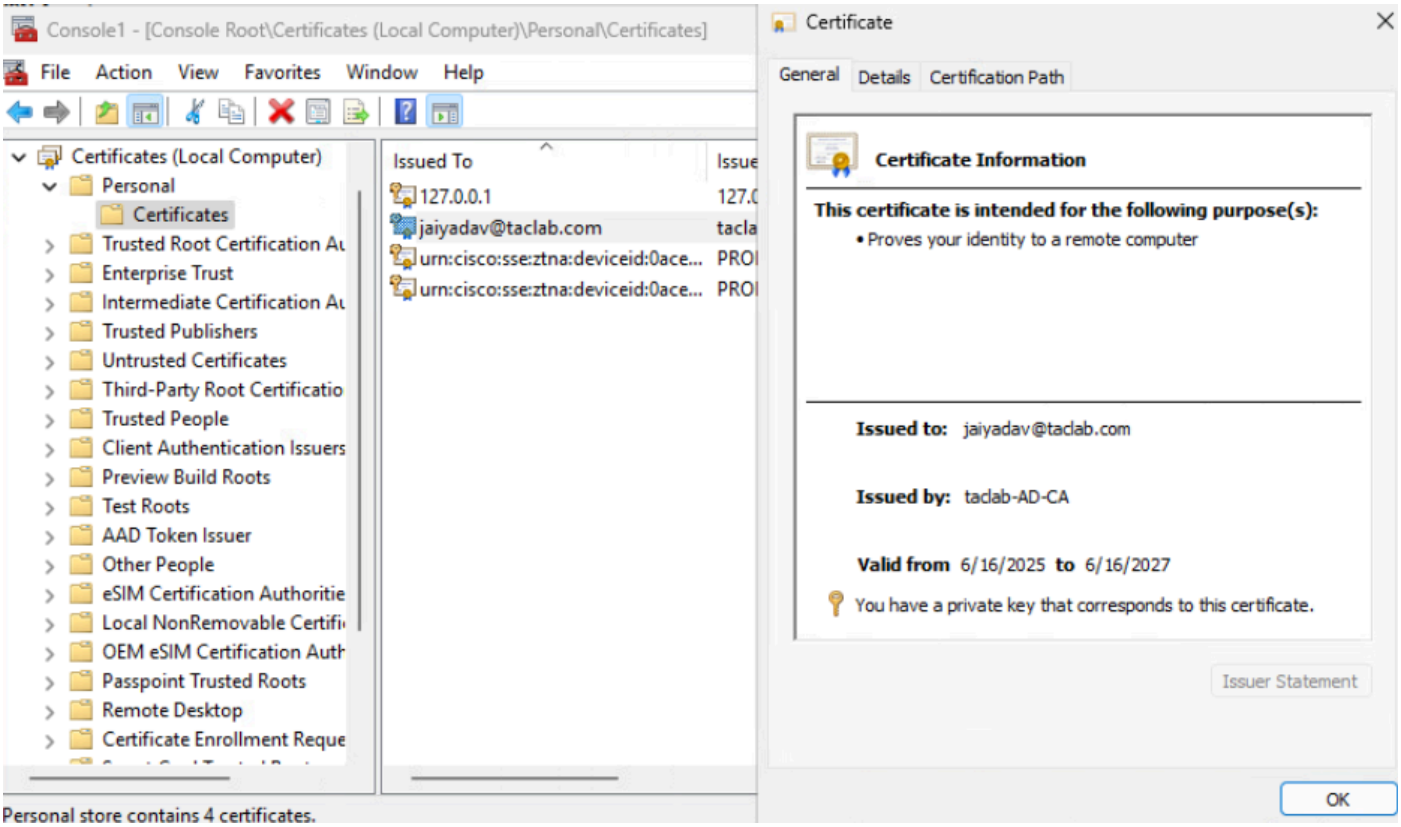
Fase 7 - Generazione e importazione del certificato dell'endpoint

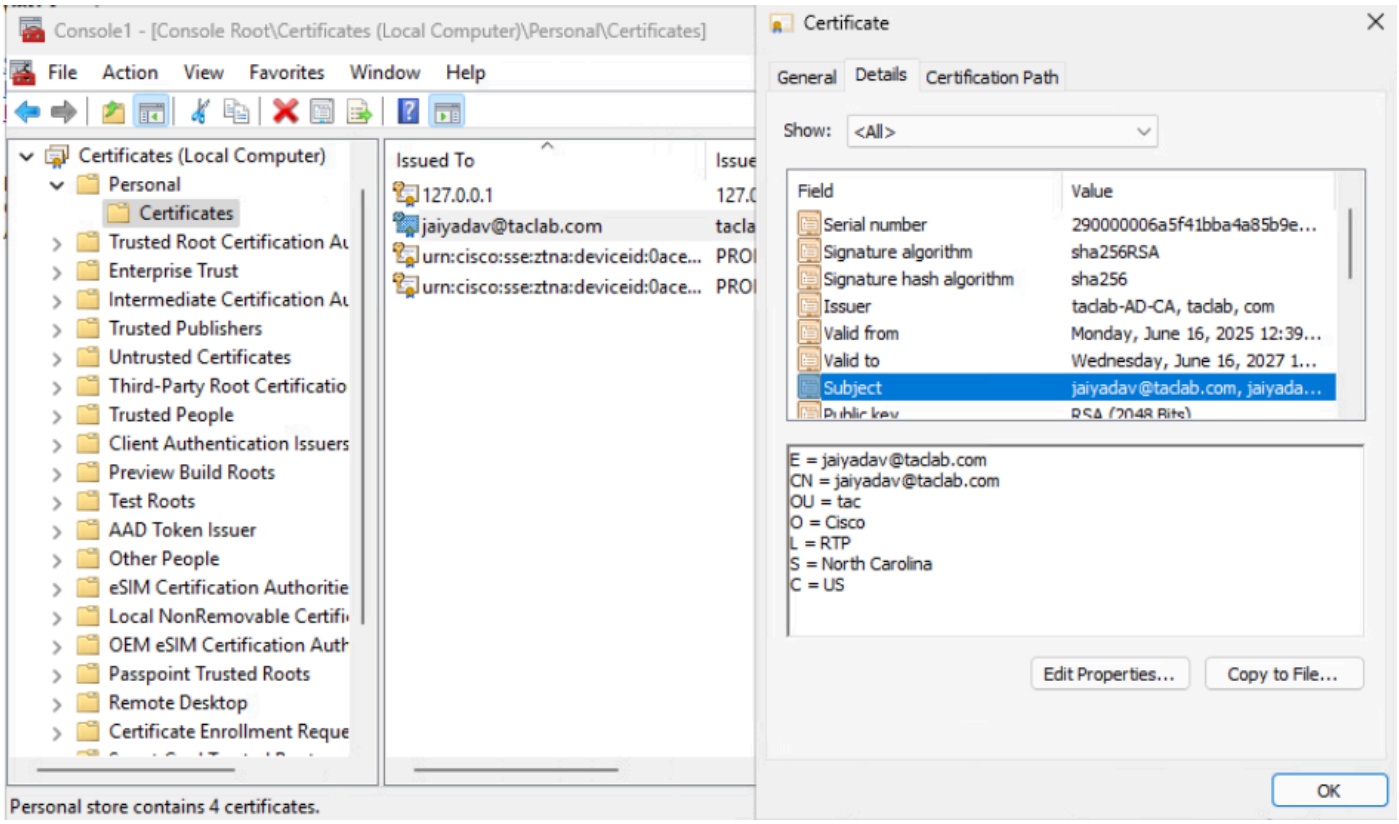
r. generare CSR , aprire un generatore CSR o uno strumento OpenSSL

b. Genera un certificato endpoint dalla CA

c. Convertire il file .cert nel formato PKCS12

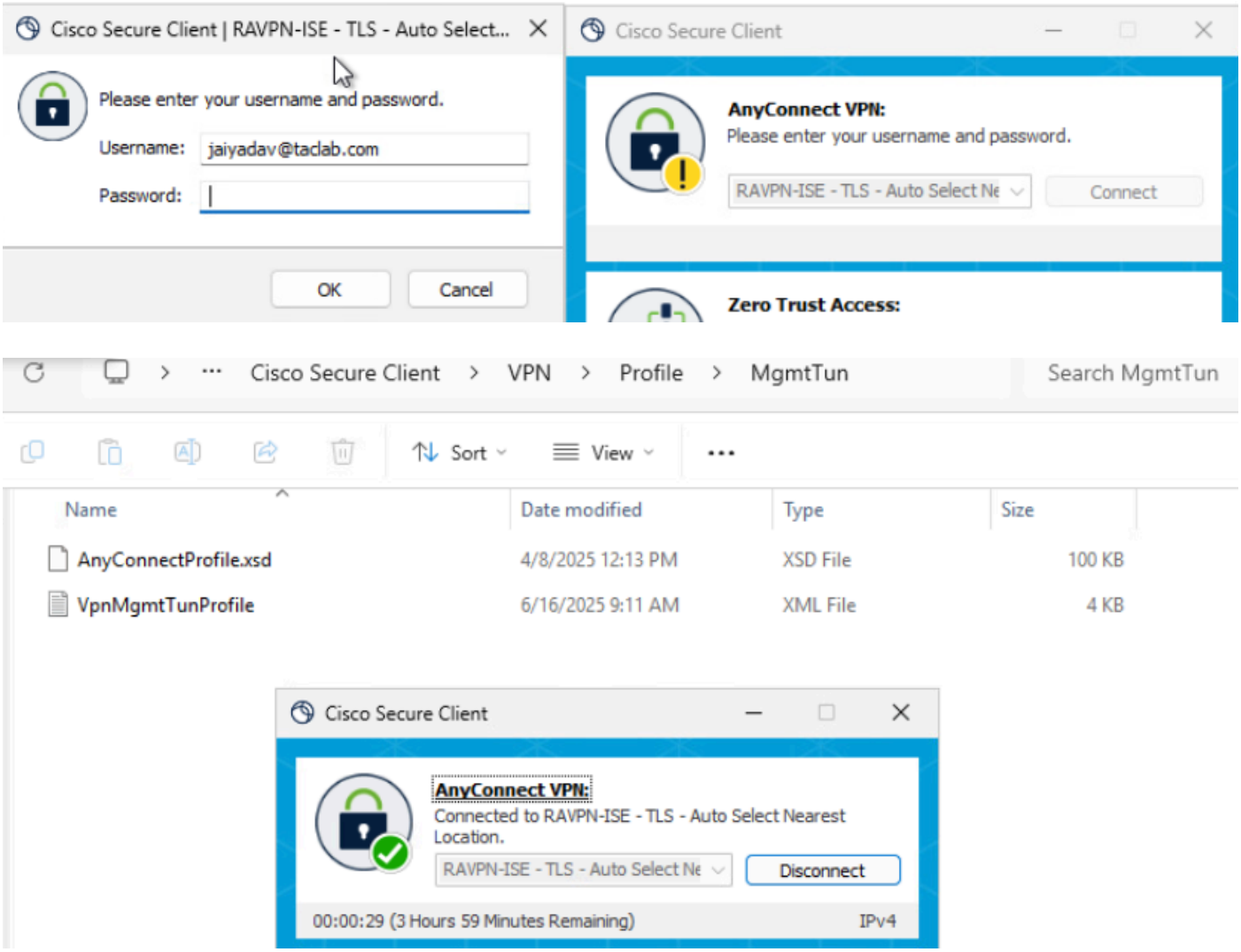
d. Importa il certificato PKCS12 nell'archivio certificati dell'endpoint



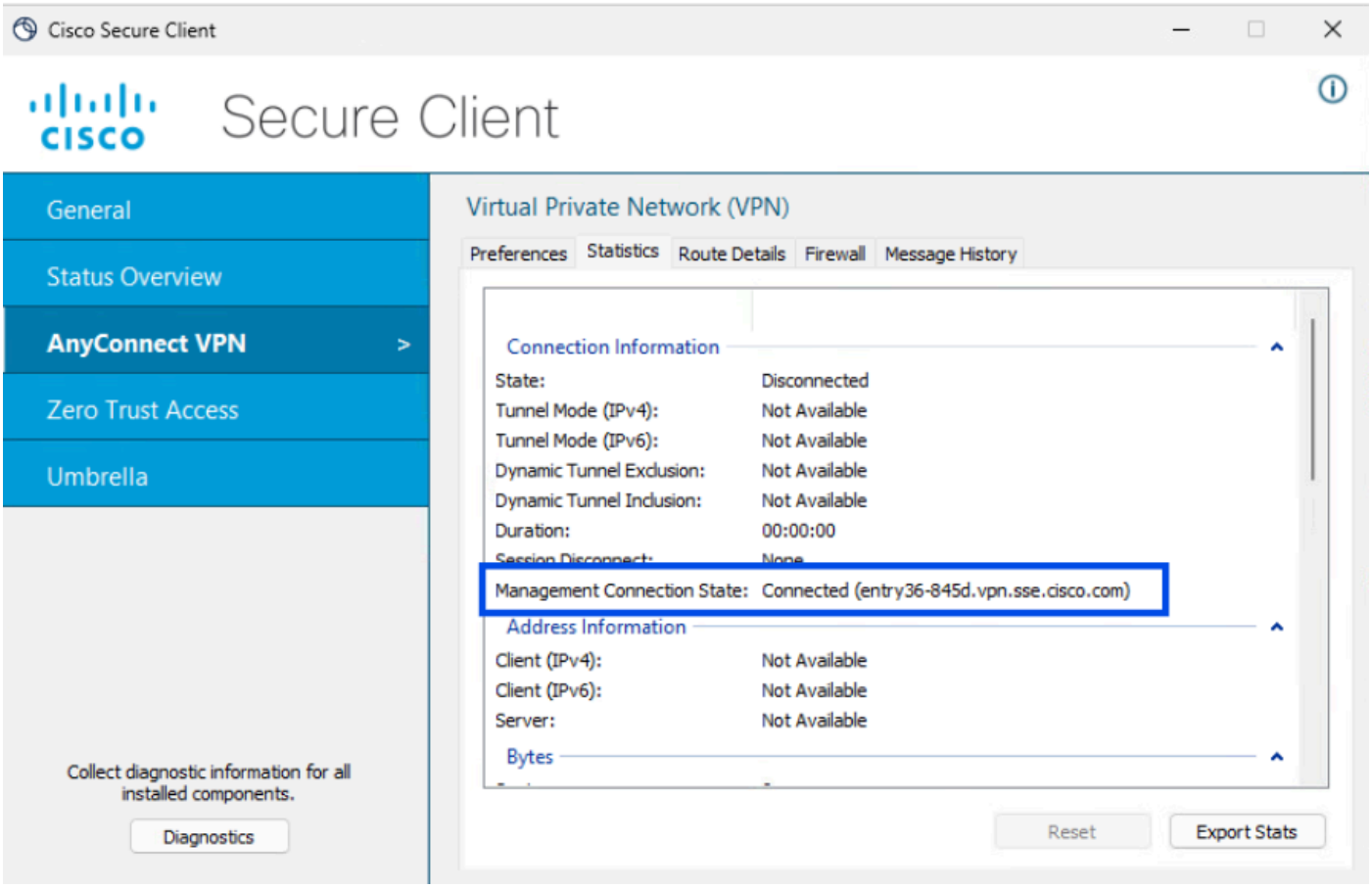


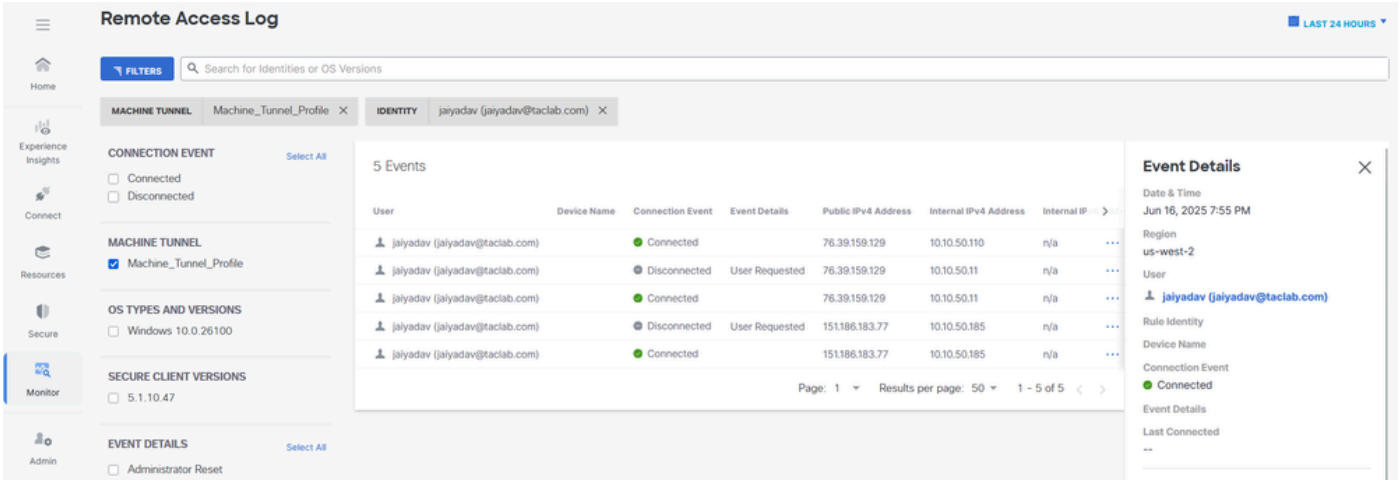
Fase 8 - Connessione al tunnel del computer

r. Connetti a tunnel utente , attiva il download del profilo XML del tunnel computer



b. Verifica connettività tunnel computer





Risoluzione dei problemi

Estrarre il bundle DART, aprire i log di AnyConnect VPN e analizzare i messaggi di errore

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).