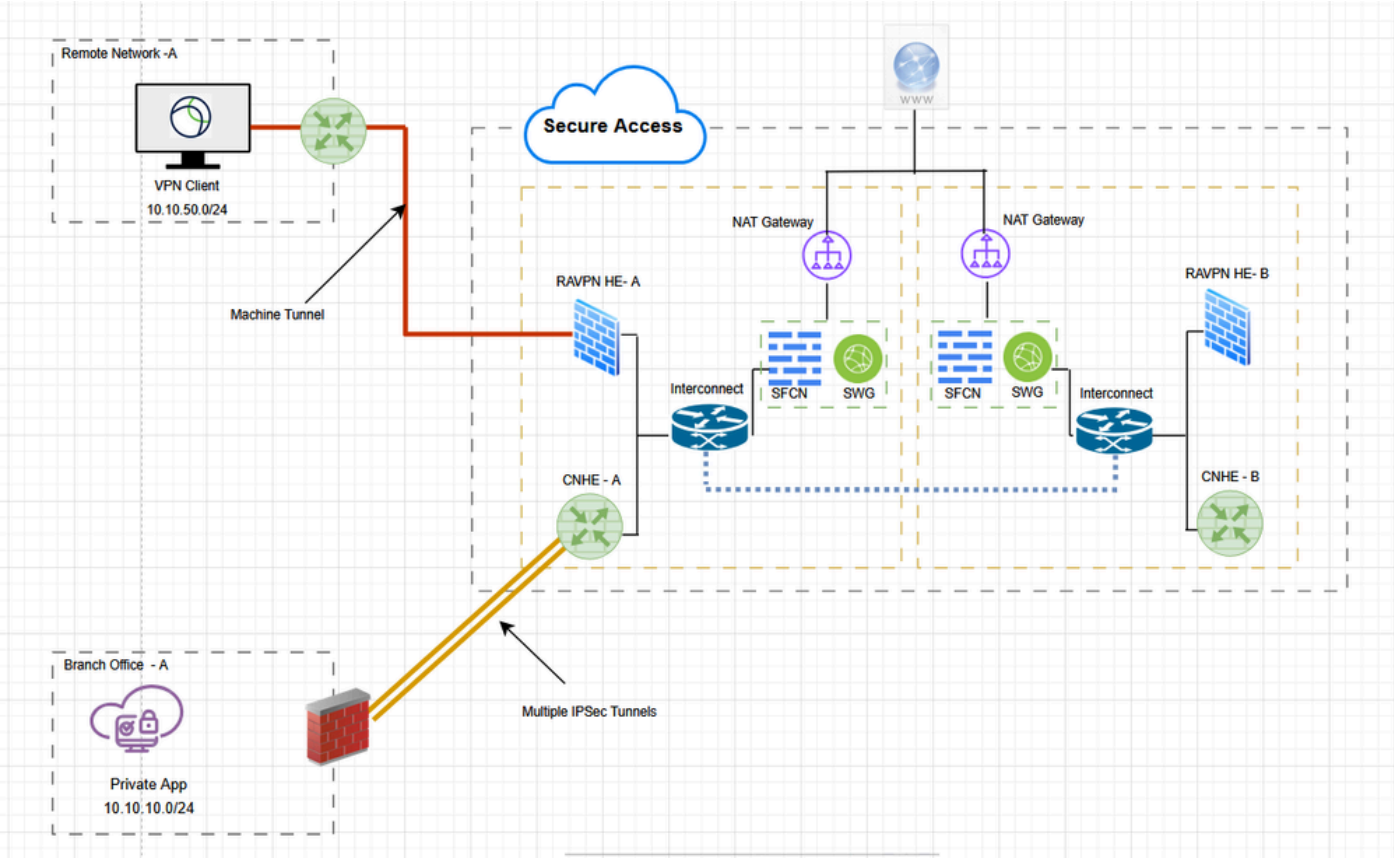
Configuration du tunnel machine sur Cisco Secure Access

Table des matières

Introduction

Ce document décrit comment configurer l'accès sécurisé en tant que passerelle VPN et accepter les connexions du client sécurisé via le tunnel de la machine VPN.

Diagramme du réseau



Conditions préalables

- Rôle Admin complet dans Secure Access.
- Au moins un profil VPN utilisateur configuré sur Cisco Secure Access
- Pool d'adresses IP utilisateur sur Cisco Secure Access

Exigences

Il est recommandé que vous ayez des connaissances sur les sujets suivants :

- 509 Certificats
- OpenSSL

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Accès sécurisé Cisco
- Cisco Secure Client 5.1.10
- Windows 11
- Windows Server 2019 - CA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Un tunnel de machine VPN d'accès sécurisé assure la connectivité au réseau d'entreprise chaque fois que le système client est mis sous tension, et pas seulement lorsqu'une connexion VPN est établie par l'utilisateur final. Vous pouvez effectuer la gestion des correctifs sur les terminaux hors du bureau, en particulier les périphériques qui sont rarement connectés par l'utilisateur, via un VPN, au réseau du bureau. Les scripts de connexion au système d'exploitation des terminaux qui nécessitent une connectivité réseau d'entreprise bénéficient également de cette fonctionnalité. Pour que ce tunnel soit créé sans interaction de l'utilisateur, l'authentification basée sur les certificats est utilisée.

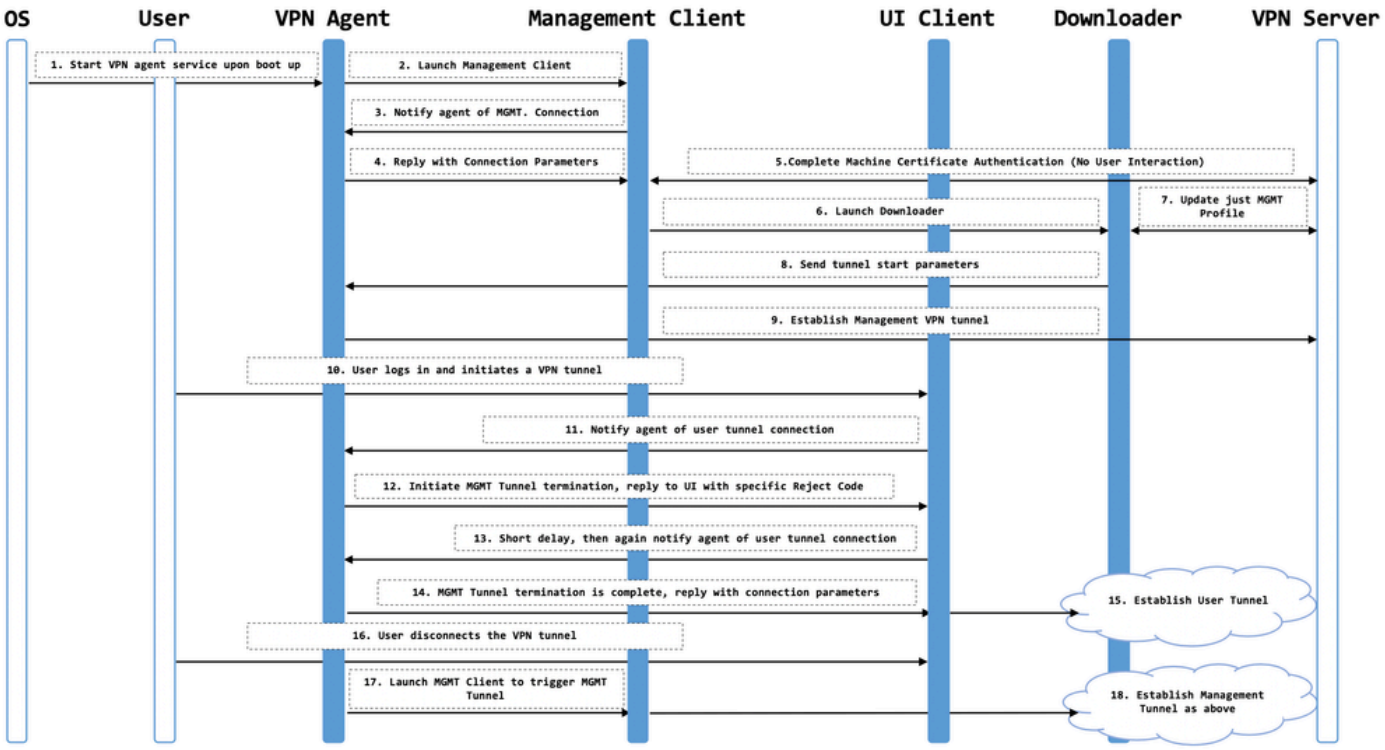
Le tunnel de machine d'accès sécurisé permet aux administrateurs de connecter le client sécurisé Cisco sans intervention de l'utilisateur avant la connexion de l'utilisateur. Le tunnel de machine d'accès sécurisé est déclenché lorsque le point d'extrémité est hors site et déconnecté d'un VPN initié par l'utilisateur. Le tunnel de l'ordinateur VPN d'accès sécurisé est transparent pour l'utilisateur final et se déconnecte automatiquement lorsque l'utilisateur lance le VPN.

Travailler sur le tunnel machine

Le service d'agent VPN du client sécurisé est automatiquement démarré au démarrage du système. L'agent VPN du client sécurisé utilise le profil VPN pour détecter que la fonctionnalité de tunnel de la machine est activée. Si la fonctionnalité de tunnel de machine est activée, l'agent lance l'application cliente de gestion pour initier une connexion de tunnel de machine. L'application cliente de gestion utilise l'entrée d'hôte du profil VPN pour initier la connexion. Ensuite, le tunnel VPN est établi comme d'habitude, à une exception près : aucune mise à jour logicielle n'est effectuée pendant une connexion de tunnel machine, car le tunnel machine est censé être transparent pour l'utilisateur.

L'utilisateur lance un tunnel VPN via le client sécurisé, ce qui déclenche la fin du tunnel de la machine. À la fin du tunnel machine, l'établissement du tunnel utilisateur se poursuit comme d'habitude.

L'utilisateur déconnecte le tunnel VPN, ce qui déclenche le rétablissement automatique du tunnel machine.



Limites

- Interaction utilisateur non prise en charge.
- L'authentification basée sur les certificats via le magasin de certificats de l'ordinateur (Windows) est uniquement prise en charge.
- La vérification stricte des certificats du serveur est appliquée.
- Un proxy privé n'est pas pris en charge.
- Un proxy public n'est pas pris en charge (la valeur ProxyNative est prise en charge sur les plates-formes où les paramètres du proxy natif ne sont pas récupérés à partir du navigateur).
- Les scripts de personnalisation du client sécurisé ne sont pas pris en charge

Configurer

Méthode 1 : configuration du tunnel de la machine avec l'utilisateur machine@sse.com

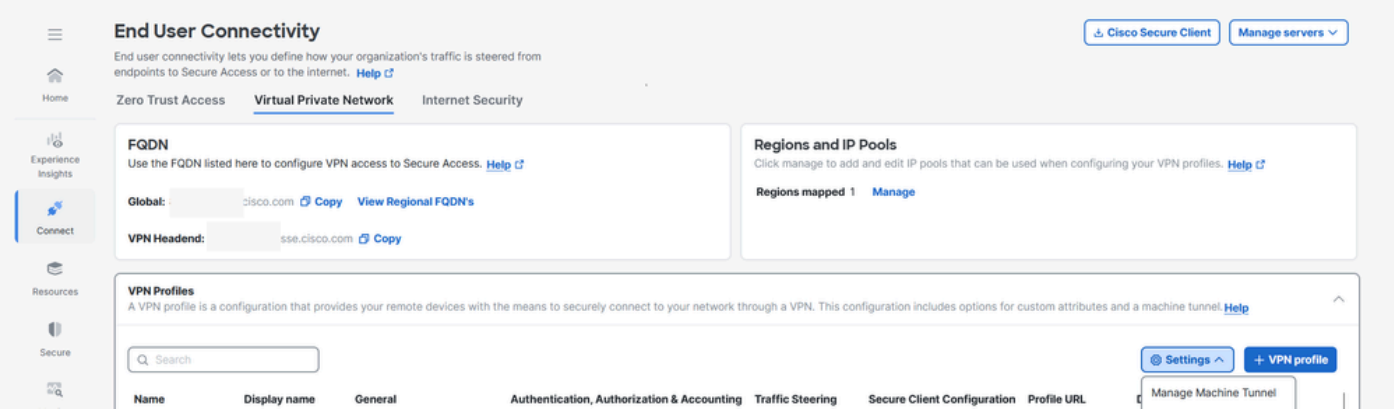
Étape 1 - Paramètres généraux

Configurez les paramètres généraux, y compris le domaine et les protocoles utilisés par le tunnel de cet ordinateur.

1. Accédez à Connect > End User Connectivity > Virtual Private Network.

2. Accédez à VPN Profiles et configurez les paramètres du tunnel de l'ordinateur.

a. Cliquez sur Settings, puis choisissez Manage Machine Tunnel dans la liste déroulante.

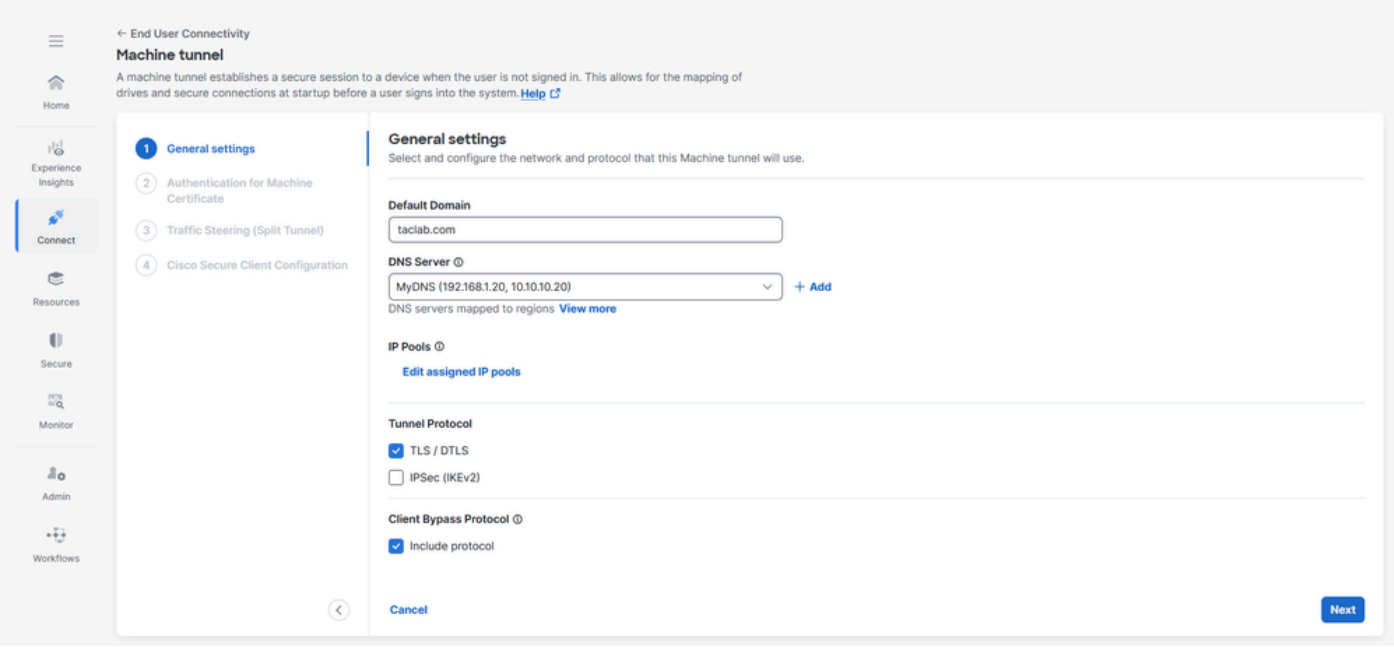


3. Entrez le domaine par défaut.
4. Le serveur DNS mappé via la page Gérer les régions et les pools d'adresses IP est défini comme serveur par défaut. Vous pouvez accepter le serveur DNS par défaut, choisir un autre serveur DNS dans la liste déroulante, ou cliquer sur + Ajouter pour ajouter une nouvelle paire de serveurs DNS. La sélection d'un autre serveur DNS ou l'ajout d'un nouveau serveur DNS remplace ce serveur par défaut.
5. Sélectionnez un pool d'adresses IP par région dans la liste déroulante Pools d'adresses IP. Les profils VPN doivent avoir au moins un pool d'adresses IP attribué dans chaque région pour une configuration valide.
6. Sélectionnez le protocole de tunnel que cette machine utilise comme tunnel :
   - TLS/DTLS
   - IPSec (IKEv2)

   Au moins un protocole doit être sélectionné.
7. Cochez éventuellement la case Include protocol pour appliquer le protocole de contournement client.

   a. Si le protocole de contournement client est activé pour un protocole IP et qu'un pool d'adresses n'est pas configuré pour ce protocole (en d'autres termes, aucune adresse IP pour ce protocole n'a été attribuée au client par l'ASA), tout trafic IP utilisant ce protocole n'est pas envoyé via le tunnel VPN. Il doit être envoyé à l'extérieur du tunnel.

   b. Si le protocole de contournement client est désactivé et qu'aucun pool d'adresses n'est configuré pour ce protocole, le client abandonne tout le trafic pour ce protocole IP une fois le tunnel VPN établi.



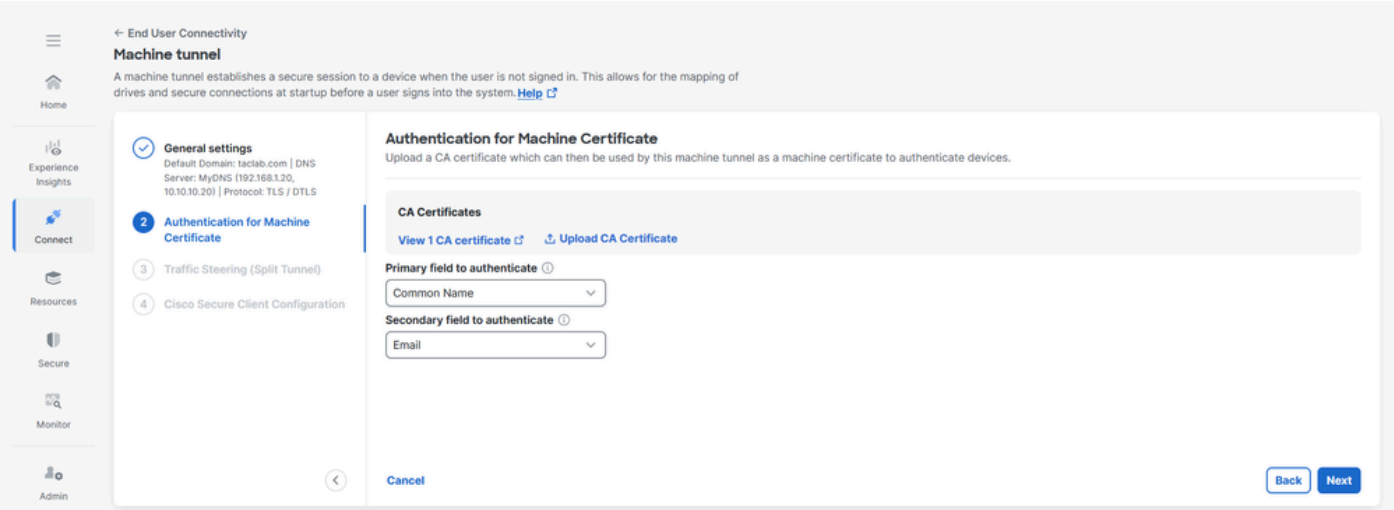
8. Cliquez sur Next

Étape 2 - Authentification pour le certificat de machine

Le tunnel de la machine est transparent pour l'utilisateur final et se déconnecte automatiquement lorsque l'utilisateur lance une session VPN. Pour que ce tunnel soit créé sans interaction de l'utilisateur, l'authentification basée sur les certificats est utilisée.

1. Sélectionnez les certificats CA dans la liste ou cliquez sur Télécharger les certificats CA

2. Sélectionnez les champs d'authentification basée sur les certificats. Pour plus d'informations, consultez [les champs d'authentification par certificat]



3. Cliquez sur Suivant

Étape 3 - Orientation du trafic (tunnel partagé)

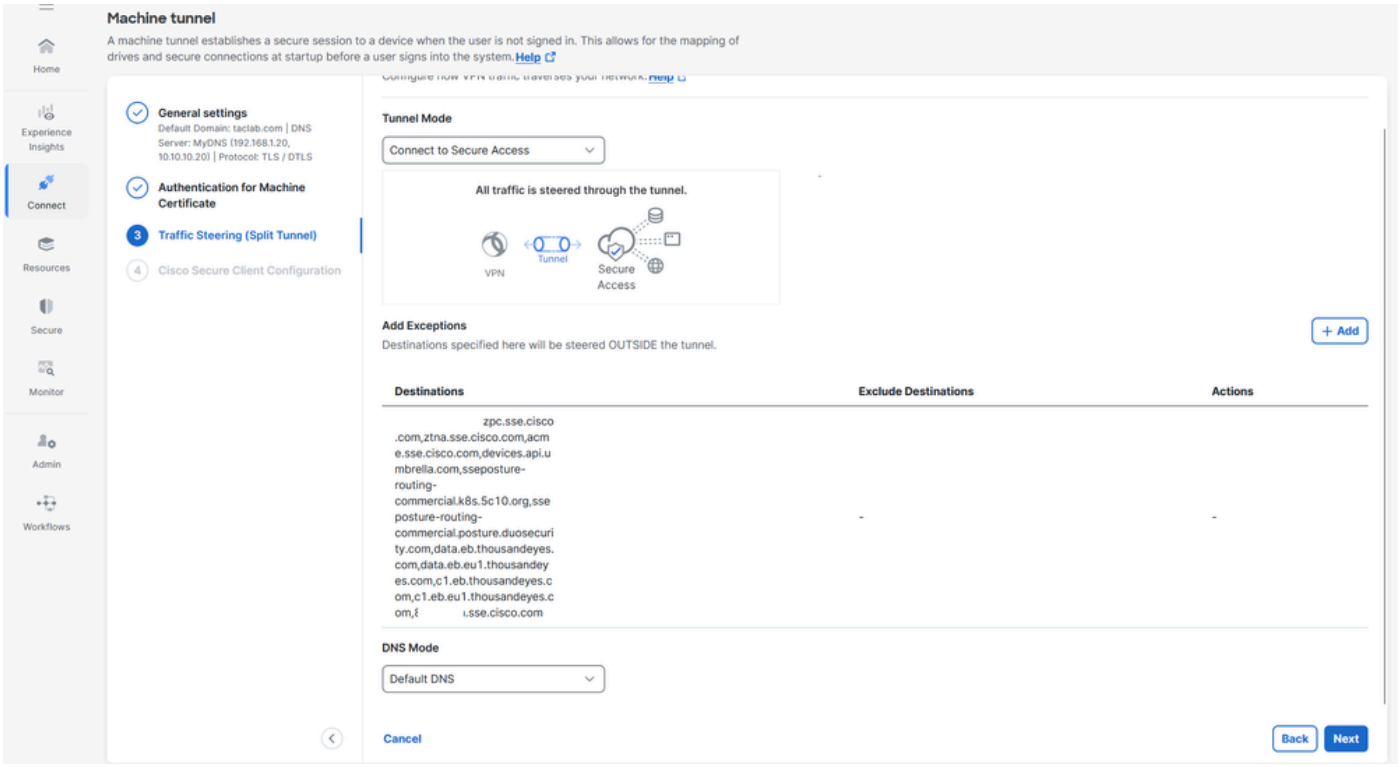
Pour le Traffic Steering (Split Tunnel), vous pouvez configurer un tunnel machine pour maintenir

une connexion de tunnel complète à Secure Access, ou le configurer pour utiliser une connexion de tunnel partagée pour diriger le trafic via le VPN seulement si nécessaire.Pour plus d'informations voir Machine Tunnel traffic Steering

1. Sélectionnez le mode tunnel

2. Selon le mode de tunnel sélectionné , vous pouvez ajouter des exceptions

3. Sélectionnez le mode DNS

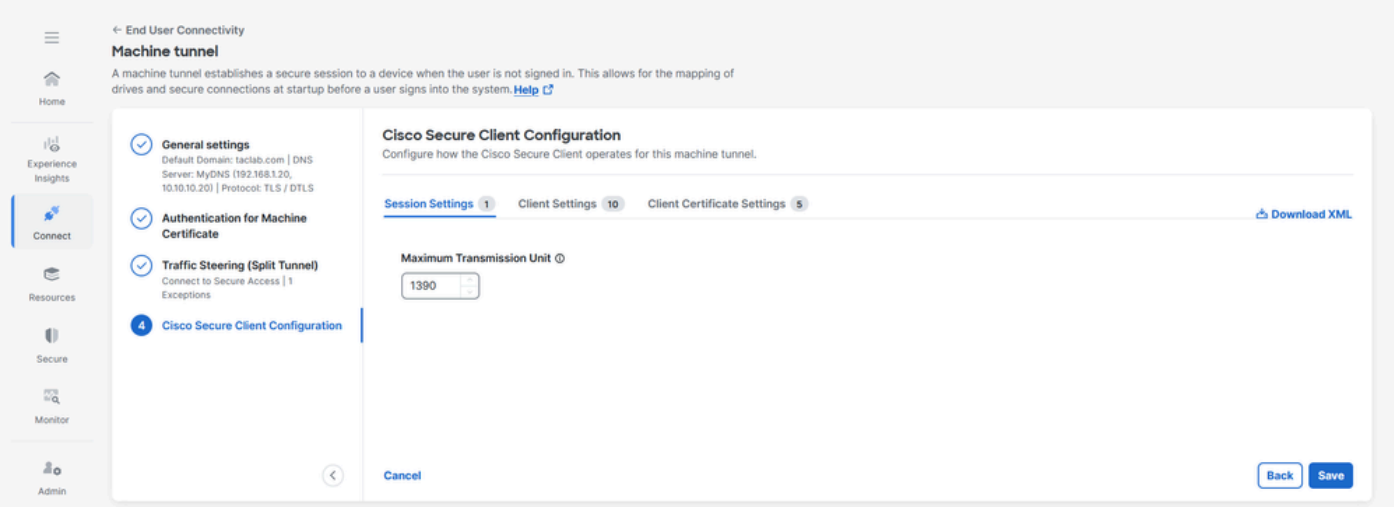


4. Cliquez sur Suivant

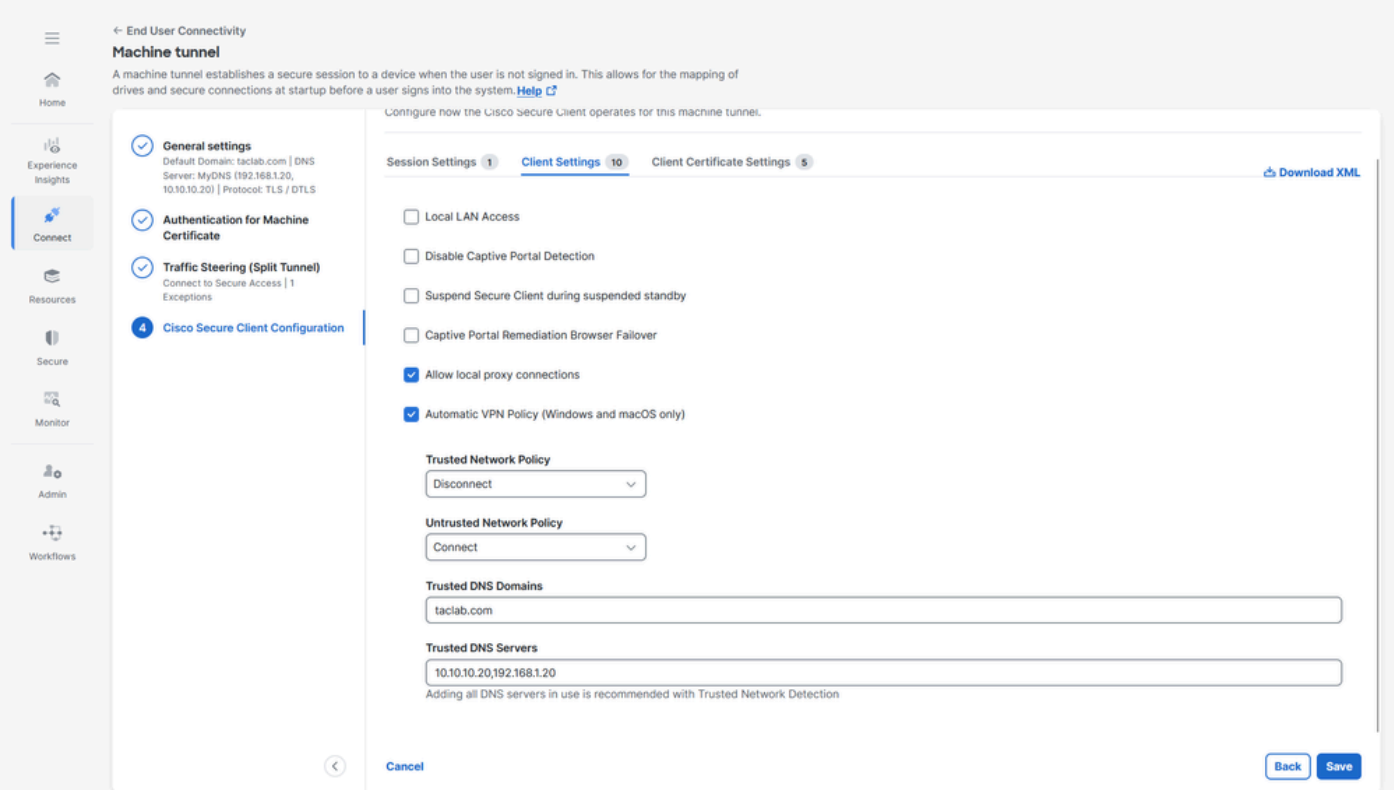
Étape 4 - Configuration du client sécurisé Cisco

Vous pouvez modifier un sous-ensemble des paramètres du client sécurisé Cisco en fonction des besoins d'un tunnel de machine VPN particulier. Pour plus d'informations, consultez Configuration du client sécurisé

1. Vérifiez l'unité de transmission maximale, la plus grande taille du paquet qui peut être envoyé dans le tunnel VPN sans fragmentation



2. Paramètres du client , veuillez vous reporter à Paramètres du client du tunnel de machine pour plus d'informations



3. Paramètres du certificat client, sélectionnez les options appropriées

a. Remplacement du magasin de certificats Windows — Permet à un administrateur de demander au client sécurisé d'utiliser des certificats dans le magasin de certificats de l'ordinateur Windows (système local) pour l'authentification du certificat client.

b. Sélection automatique des certificats - Lorsque l'authentification de certificats multiples est configurée sur la passerelle sécurisée

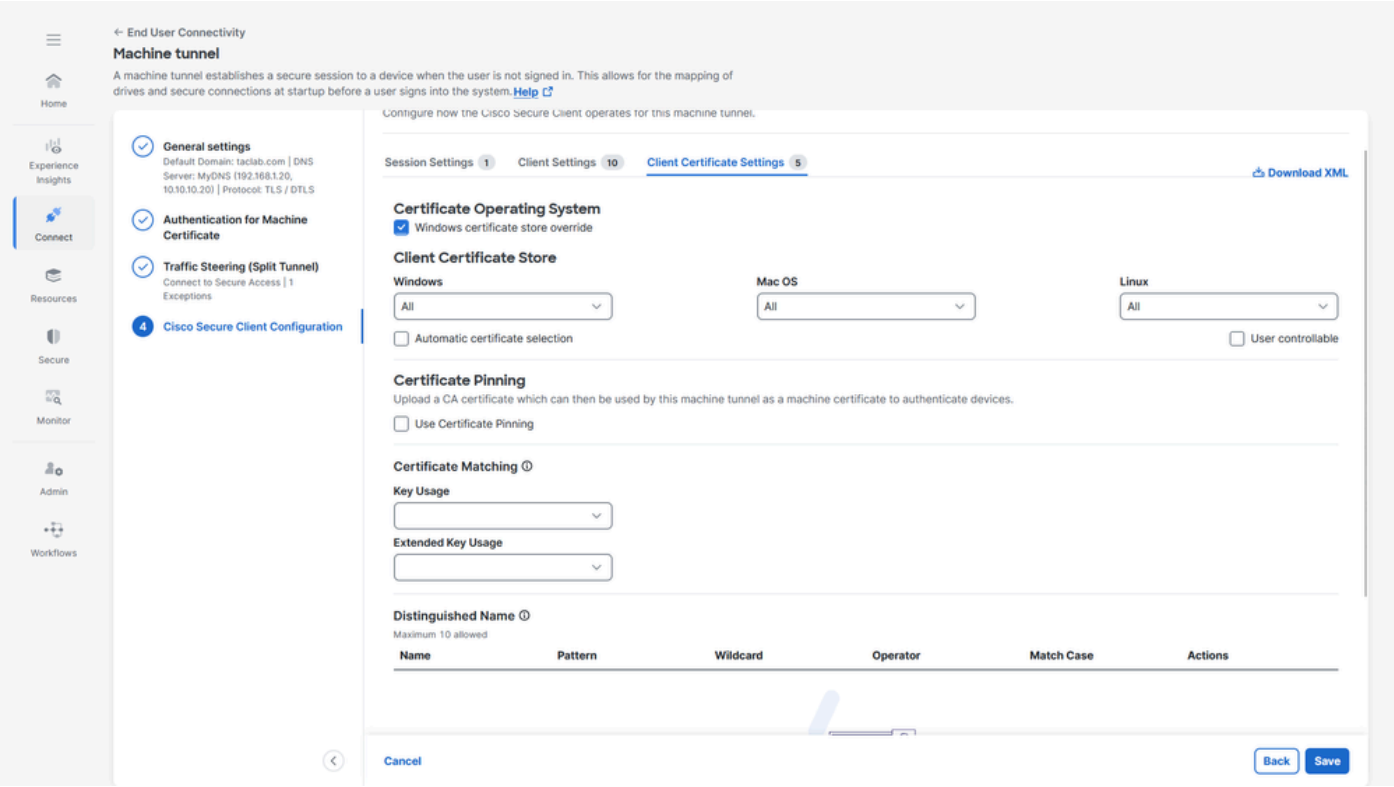
c. Épinglage de certificat : certificat CA pouvant être utilisé par le tunnel de machine comme certificat de machine pour authentifier les périphériques

d. Correspondance de certificat - Si aucun critère de correspondance de certificat n'est spécifié, Cisco Secure Client applique les règles de correspondance de certificat

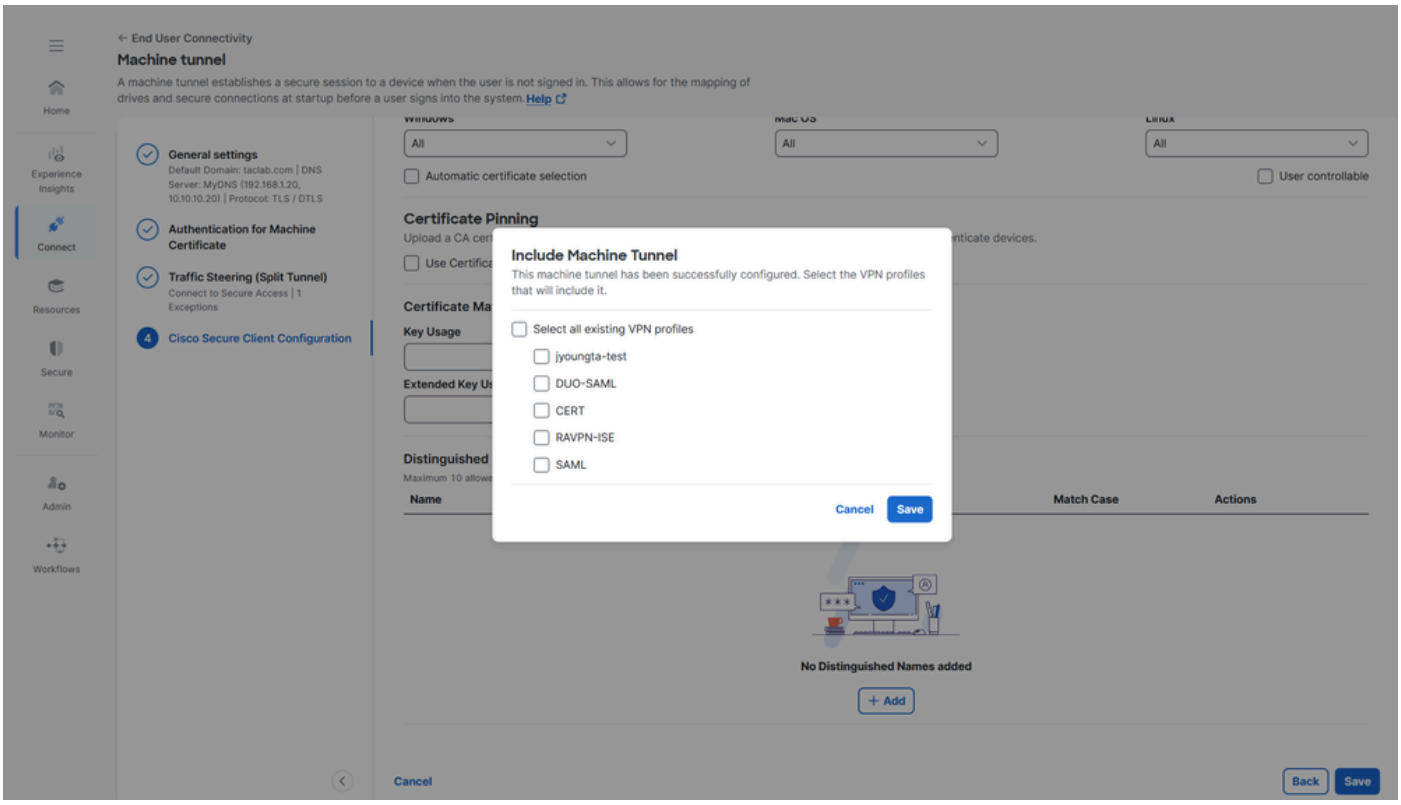
i. Utilisation de la clé : Signature_Numérique

ii. Utilisation étendue de la clé : Authentification client

e. Nom distinctif - Spécifie les noms distinctifs (DN) pour les critères de correspondance exacts lors du choix de certificats clients acceptables. Lorsque vous ajoutez plusieurs noms distinctifs, chaque certificat est comparé à toutes les entrées et toutes doivent correspondre.

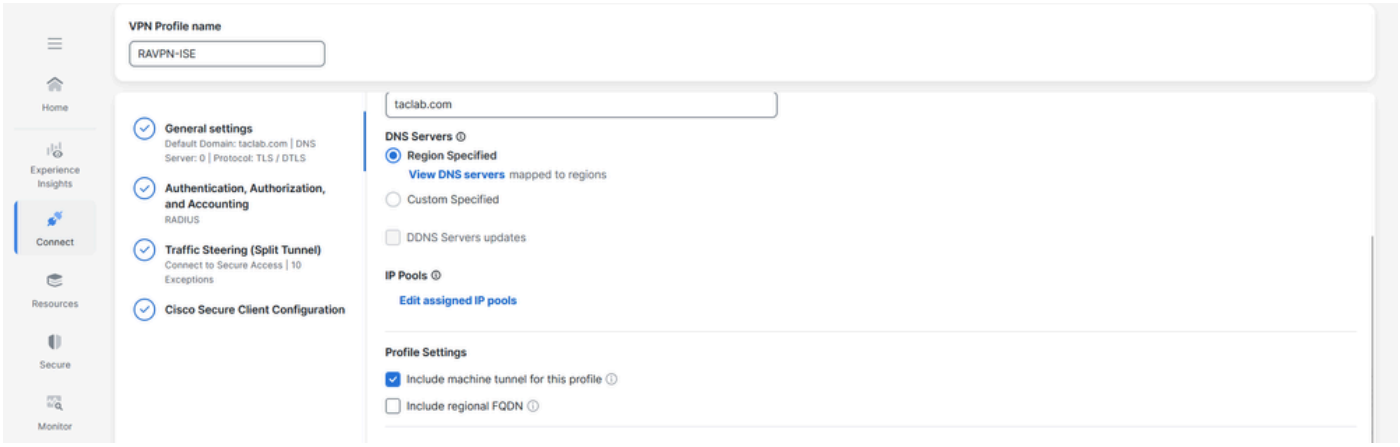


4. Affectez un profil de tunnel de machine à un profil VPN d'utilisateur, cliquez sur Enregistrer et puis il y a une option pour sélectionner les profils VPN d'utilisateur



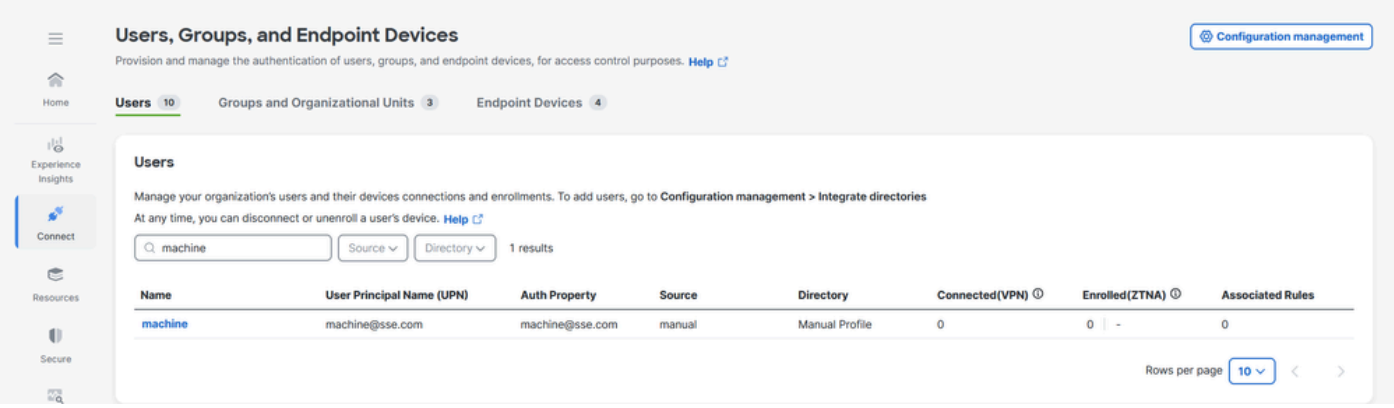
5. Cliquez sur Enregistrer

6. Vérifiez si le profil de tunnel machine est attaché à un profil VPN utilisateur



Étape 5 - Vérifiez si l'utilisateur machine@sse.com est présent dans l'accès sécurisé Cisco

1. Accédez à Connect > Users, Groups, and Endpoint Devices > Users



2. Si l'utilisateur machine@sse.com n'est pas présent l'importation manuellement. Pour plus d'informations, voir Importation manuelle d'utilisateurs et de groupes

Étape 6 - Générez un certificat CA signé pour machine@sse.com

1. Générer une demande de signature de certificat

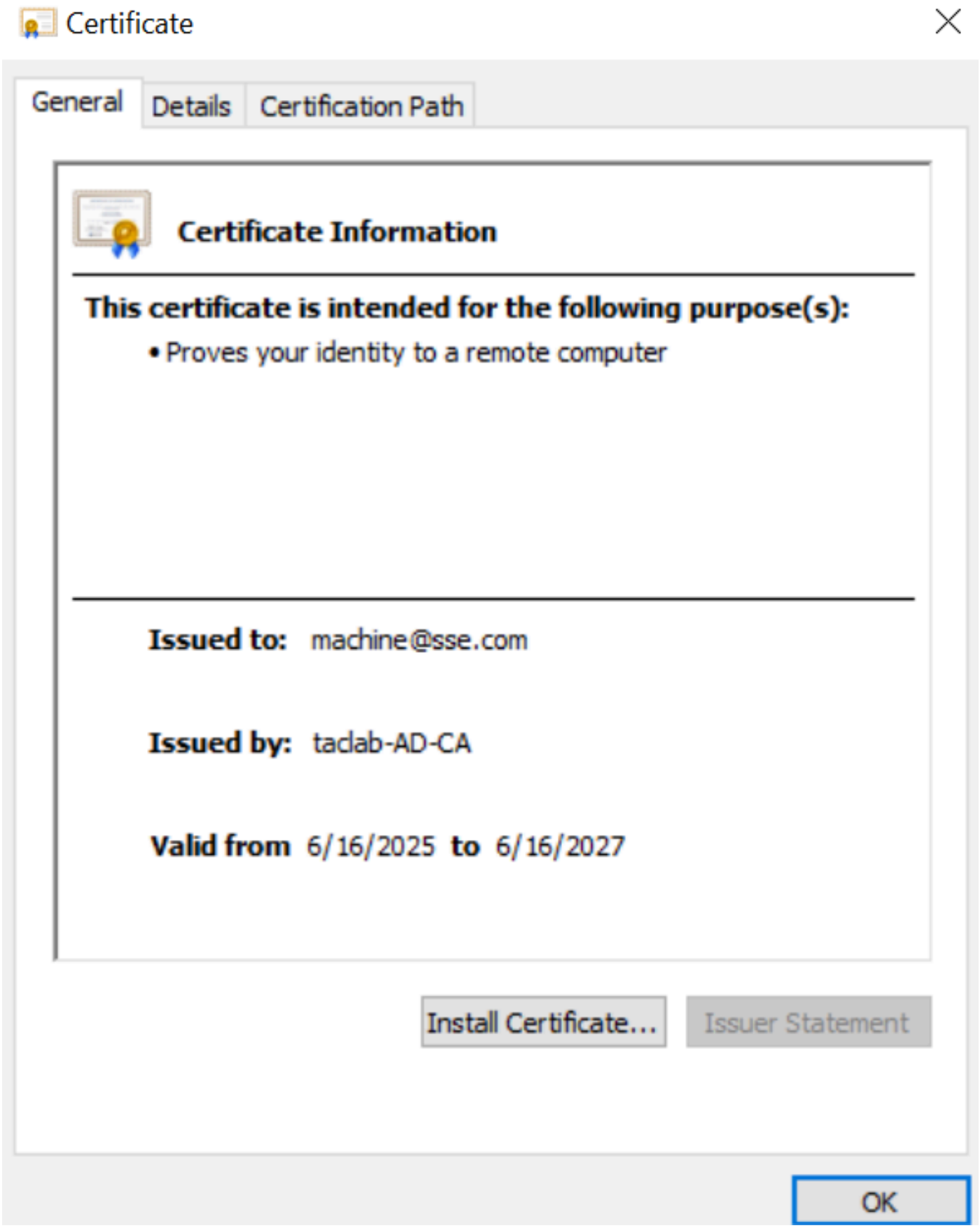
a. Nous pouvons utiliser n'importe quel logiciel de générateur de CSR en ligne CSR Generator ou une CLI openssl

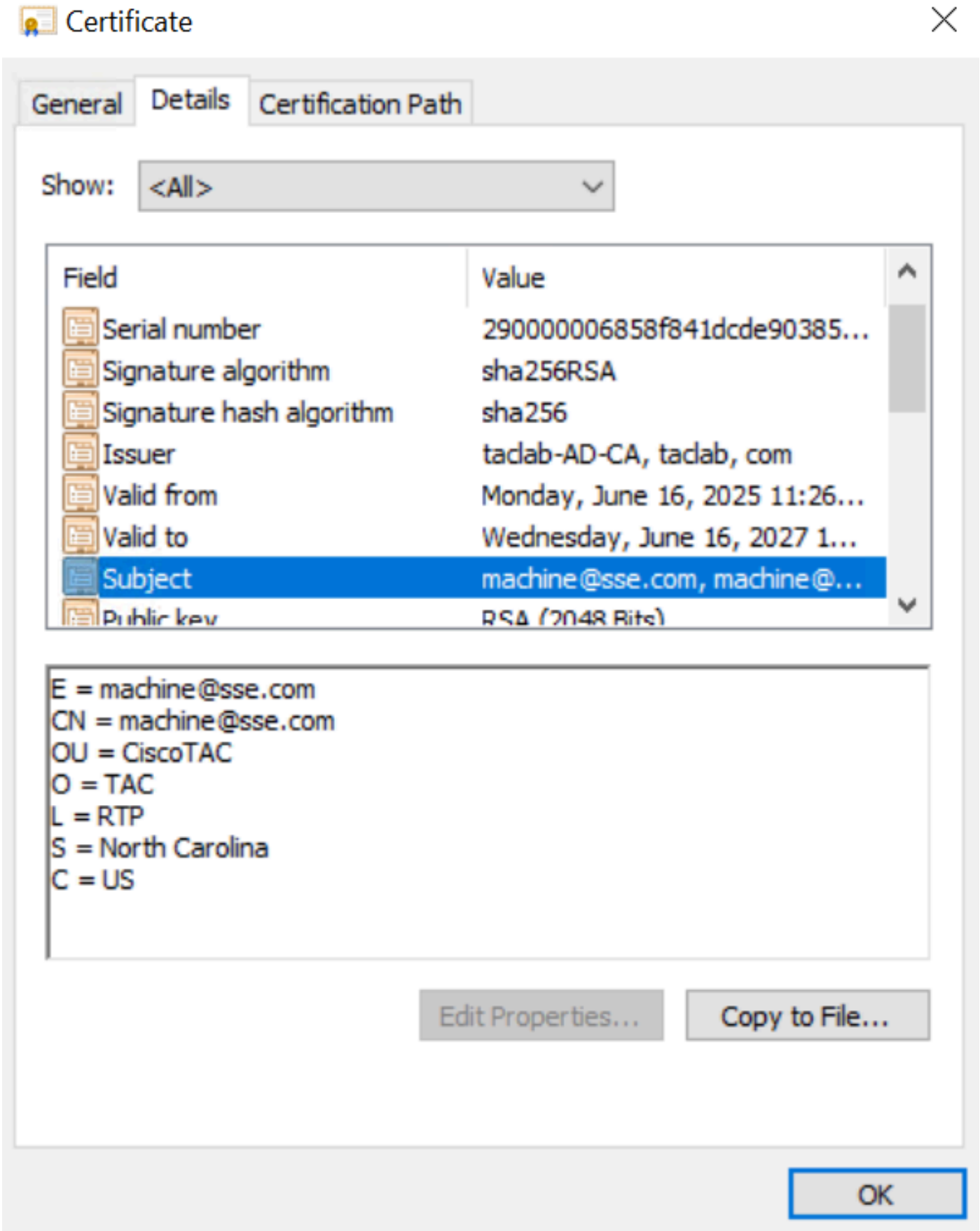
openssl req -newkey rsa : 2048 -nodes -keyout cert.key -out cert.csr

```
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. Copiez le CSR et générez un certificat machine


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



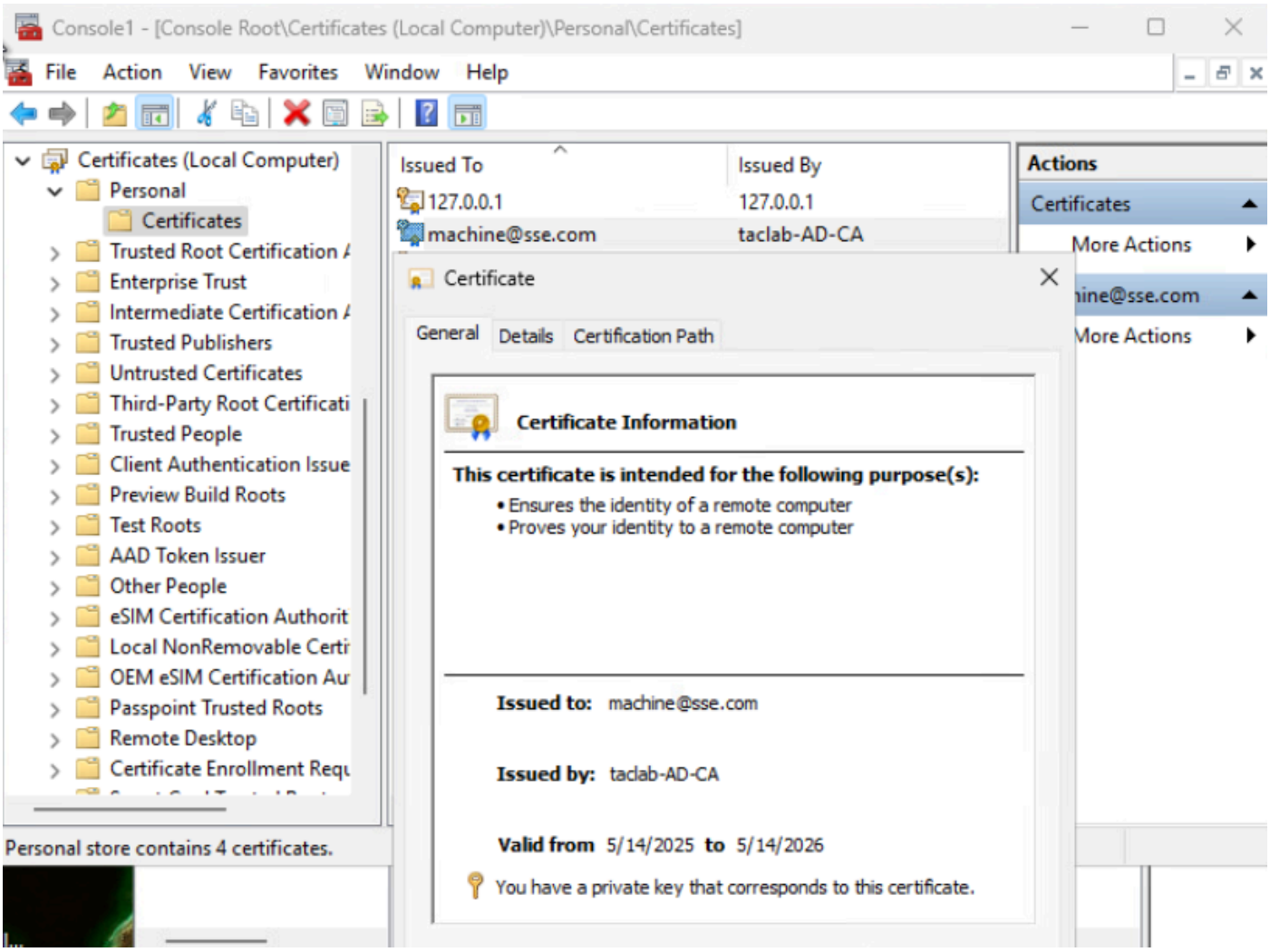
3. Convertissez le certificat de la machine au format PKCS12 en utilisant la clé et le certificat générés dans les étapes précédentes (étapes 1 et 2) respectivement

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#
```

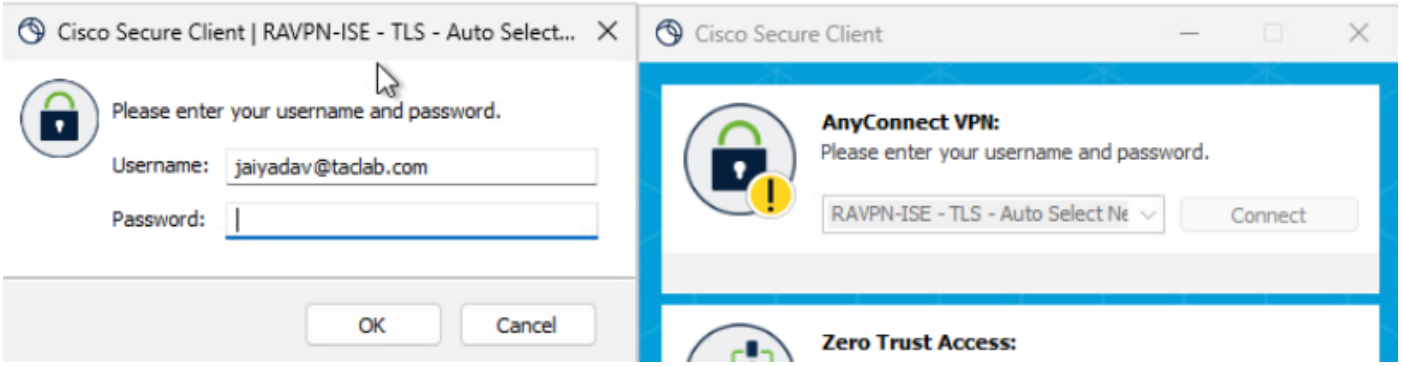
Étape 7 - Importez le certificat de machine sur une machine de test

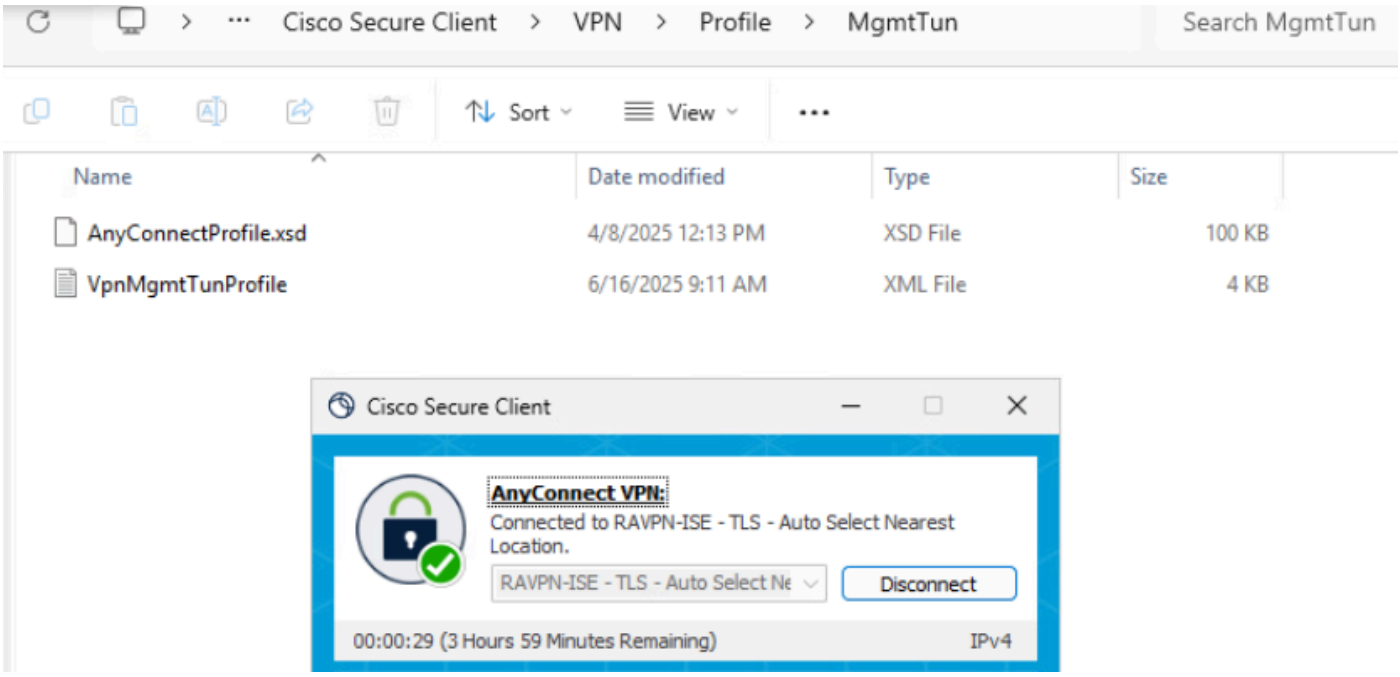
a. Importer le certificat de l'ordinateur PKCS12 dans le magasin local ou de l'ordinateur



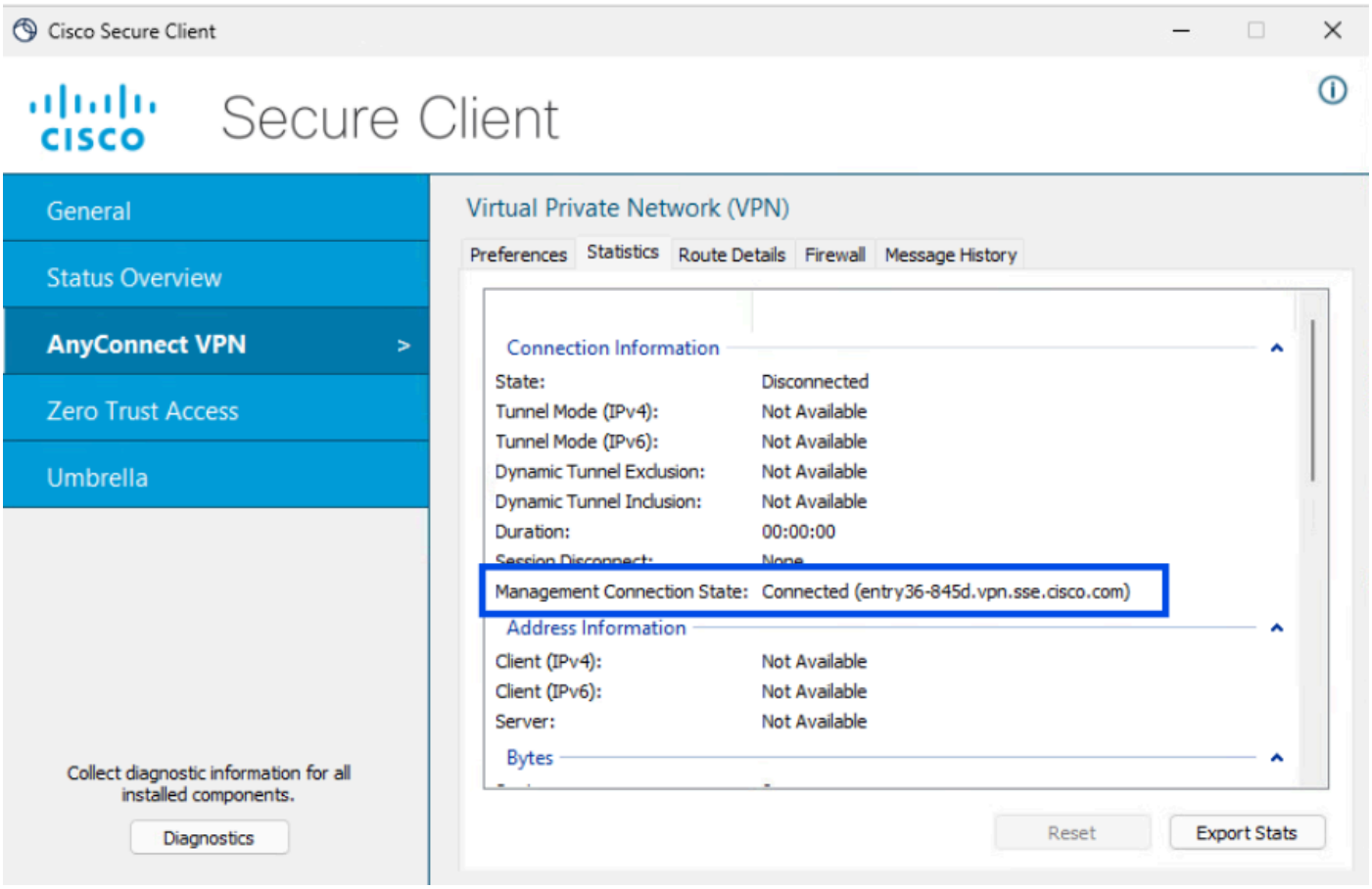
Étape 8 - Connectez-vous au tunnel machine

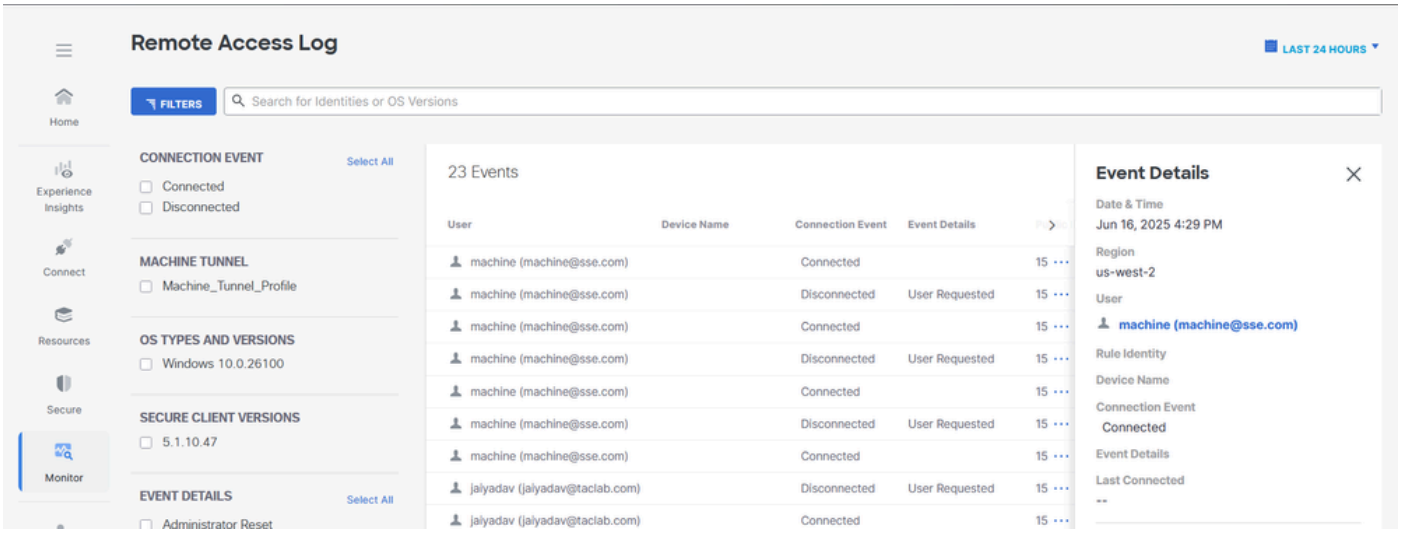
a. Connectez-vous à un tunnel utilisateur , ce qui déclenche le téléchargement du profil xml de la machine.





b. Vérification de la connectivité du tunnel machine





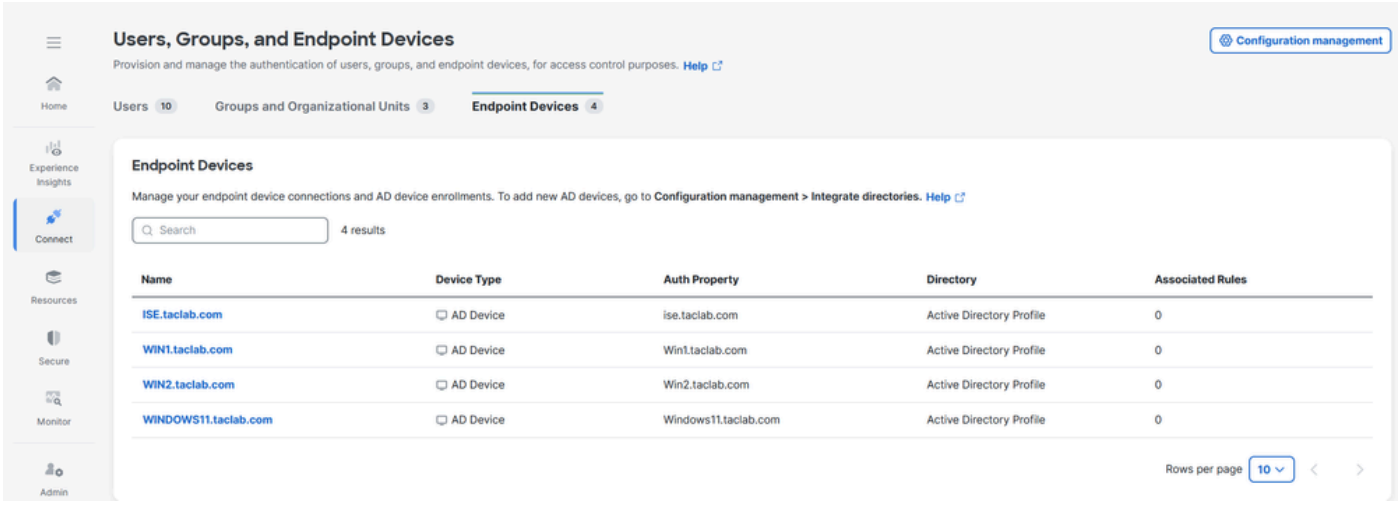
Méthode 2 : configuration du tunnel de la machine à l'aide du certificat de terminal

Dans ce cas, pour que le champ principal s'authentifie, sélectionnez le champ de certificat qui contient le nom du périphérique (nom de l'ordinateur). Secure Access utilise le nom du périphérique comme identificateur de tunnel de la machine. Le format du nom de l'ordinateur doit correspondre au format de l'identificateur de périphérique choisi

Passez en revue les étapes 1 à 4 pour la configuration du tunnel machine

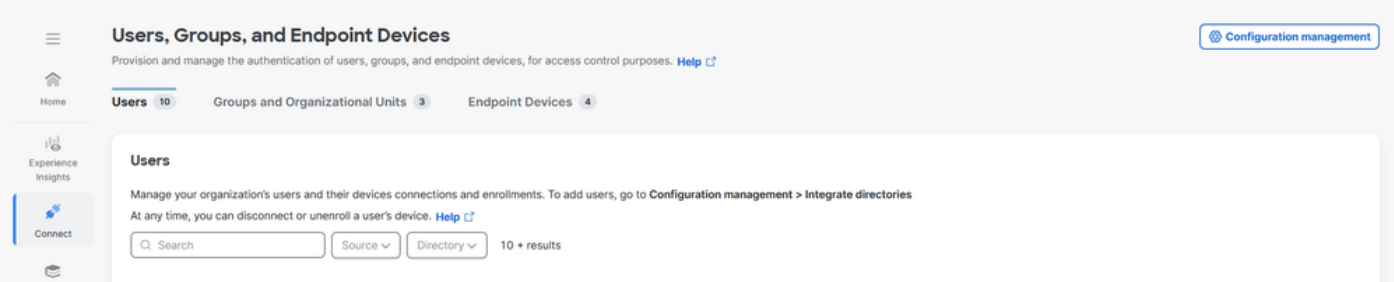
Étape 5 - Configurez le connecteur Active Directory pour pouvoir importer des terminaux sur Cisco Secure Access .

Pour plus d'informations, consultez [Intégration Active Directory sur site]

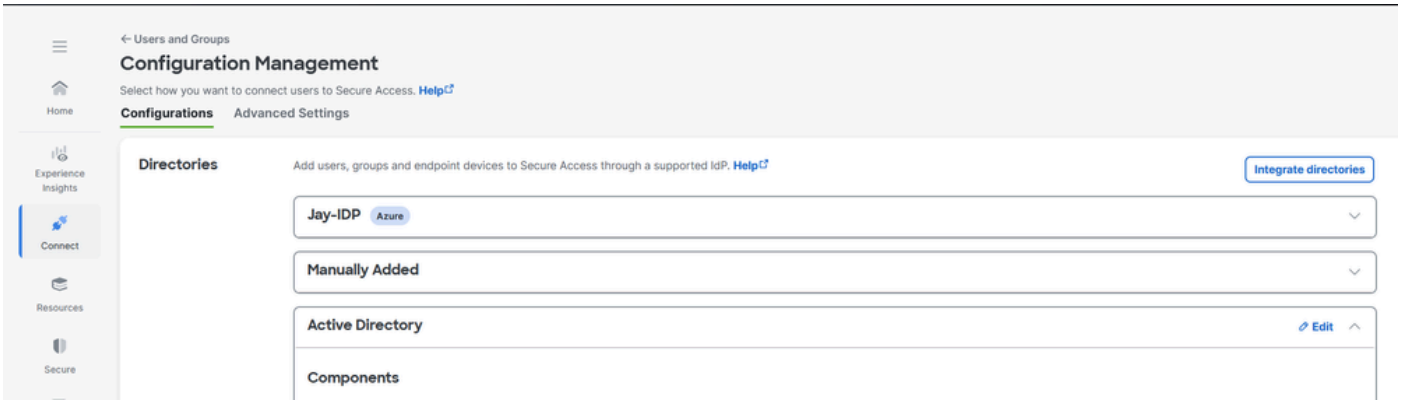


Étape 6 - Configurez l'authentification des périphériques finaux

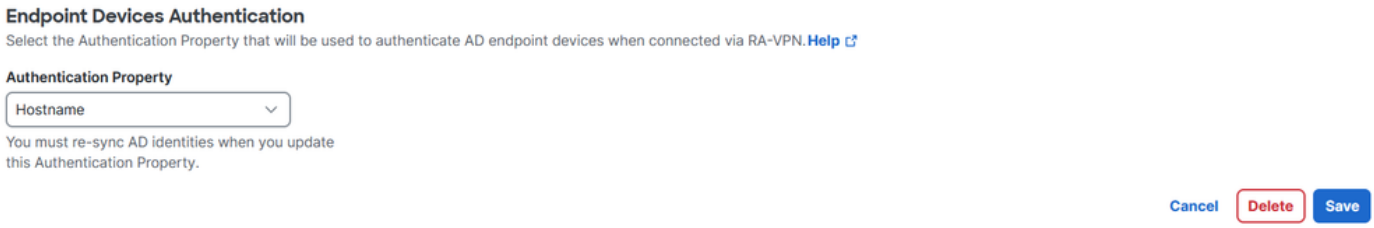
1. Accédez à Connect > Users, Groups and Endpoint Devices.
2. Cliquez sur Gestion de la configuration



3. Sous Configurations , modifiez Active Directory



4. Définissez la propriété d'authentification des périphériques finaux sur Nom d'hôte



5. Cliquez sur Save et redémarrez les services du connecteur AD sur les serveurs sur lesquels il est installé

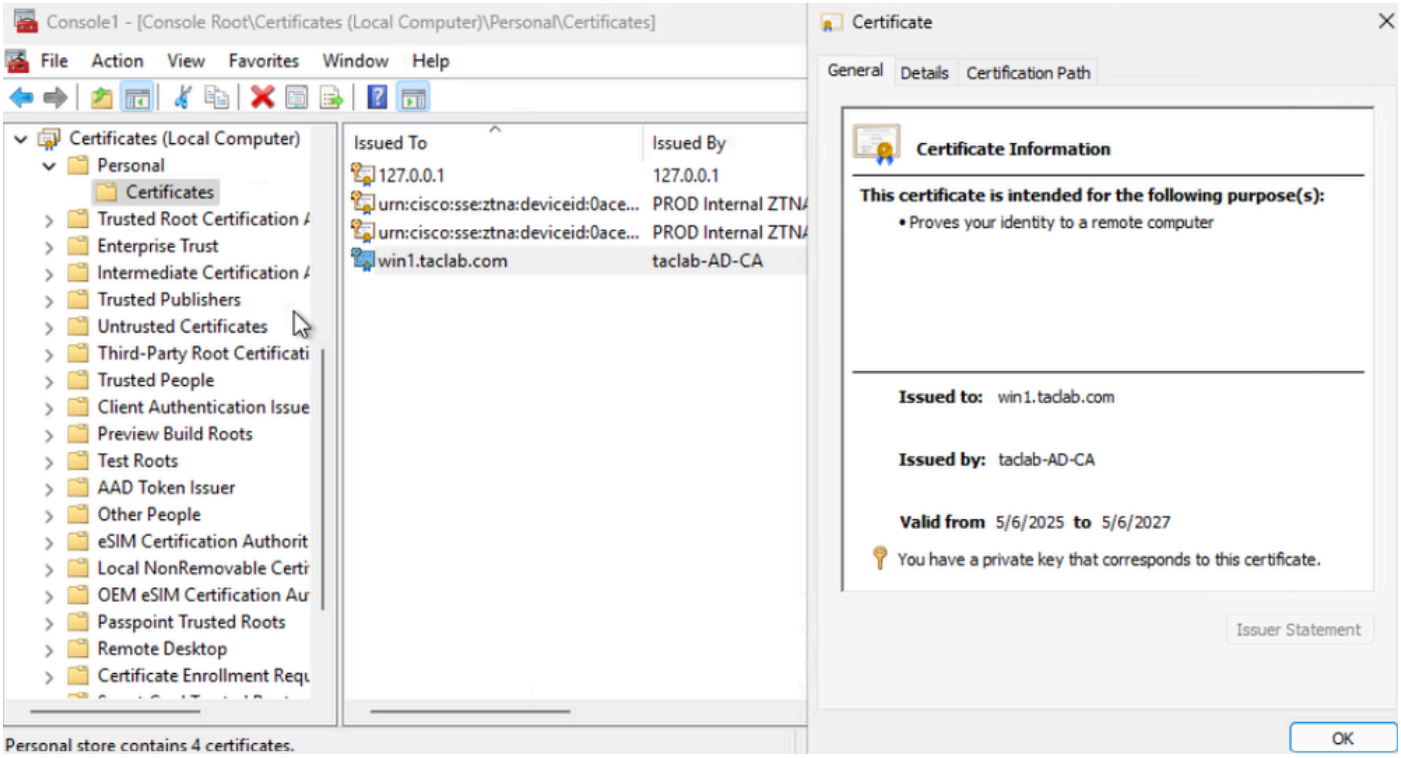
Étape 7 - Générez et importez un certificat de point de terminaison

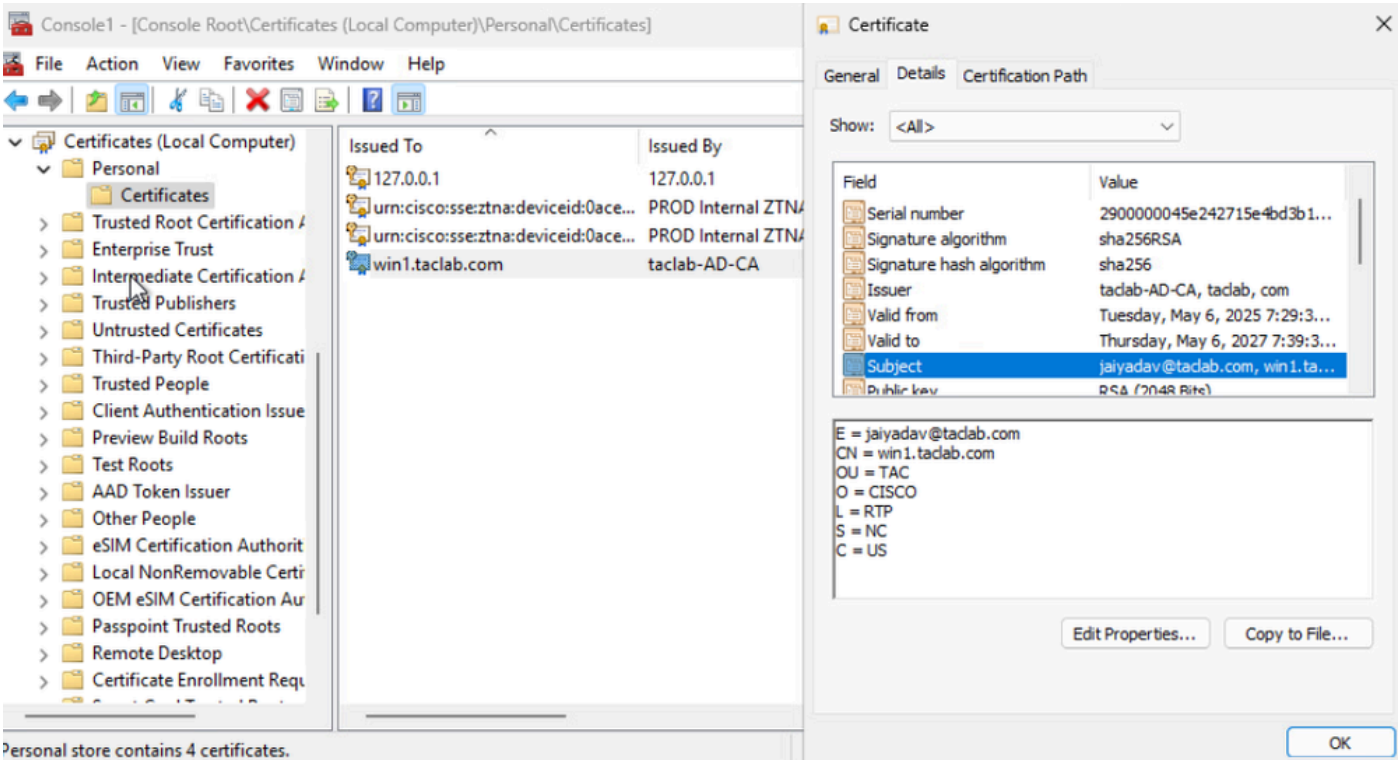
a. Générer un CSR, ouvrir un générateur CSR ou un outil OpenSSL

b. Générer un certificat de point de terminaison à partir de CA

c. Convertissez le fichier .cert au format PKCS12

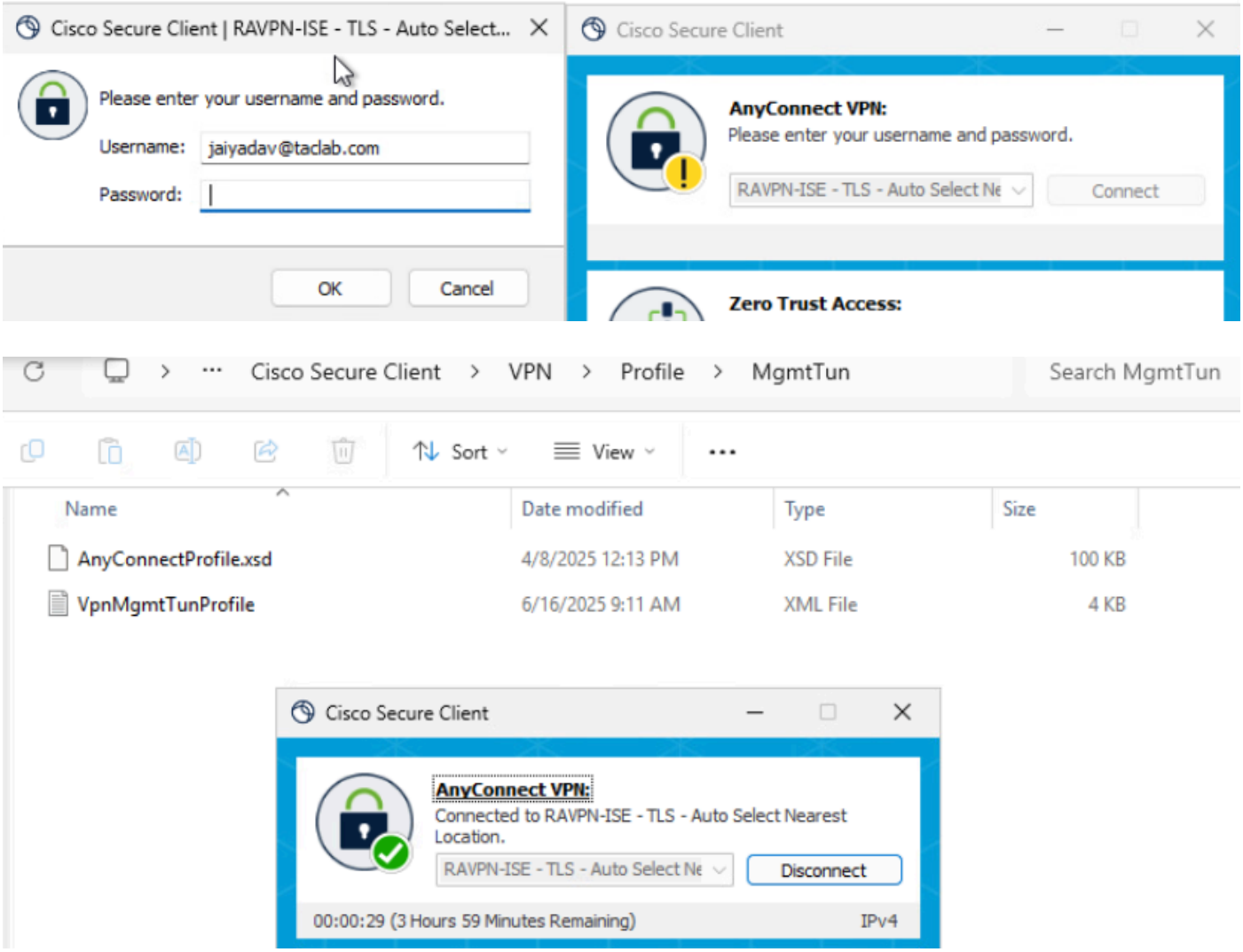
d. Importer le certificat PKCS12 dans le magasin de certificats du point de terminaison



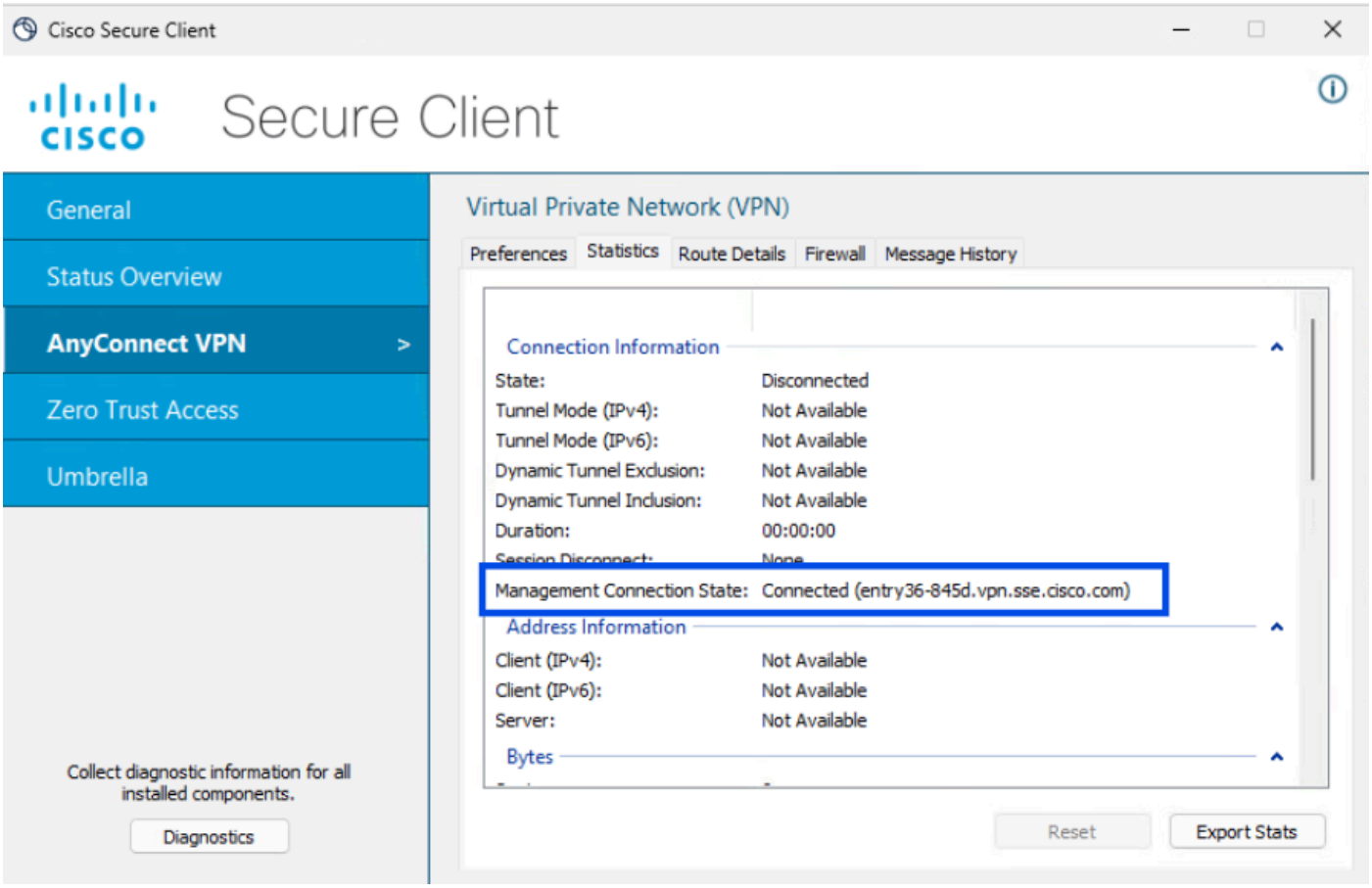


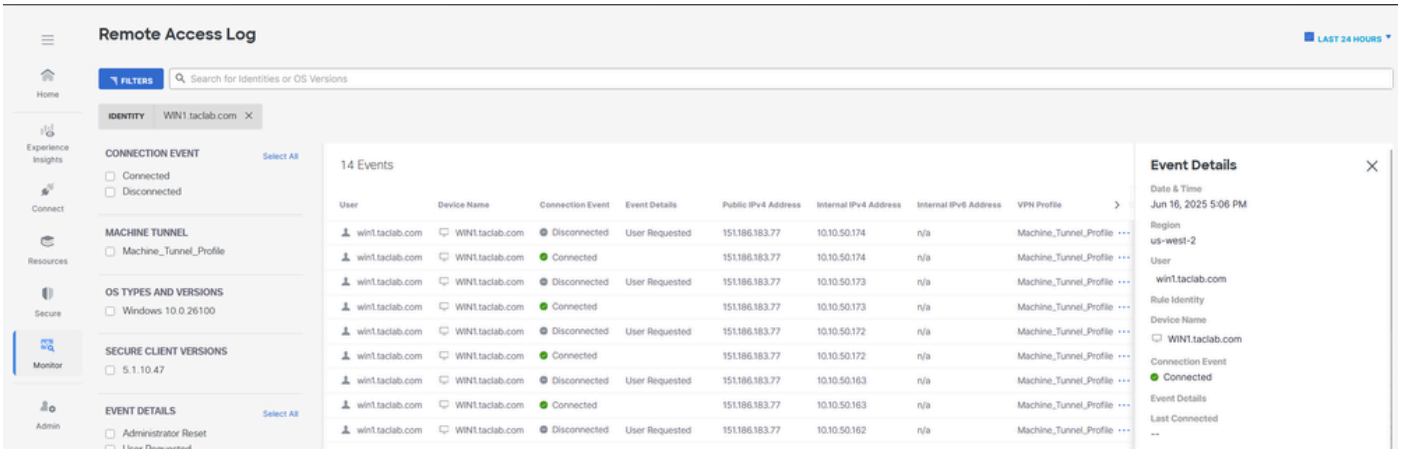
Étape 8 - Connectez-vous au tunnel machine

a. Se connecter à un tunnel utilisateur , il déclenche le téléchargement du profil xml du tunnel de la machine



b. Vérification de la connectivité du tunnel machine





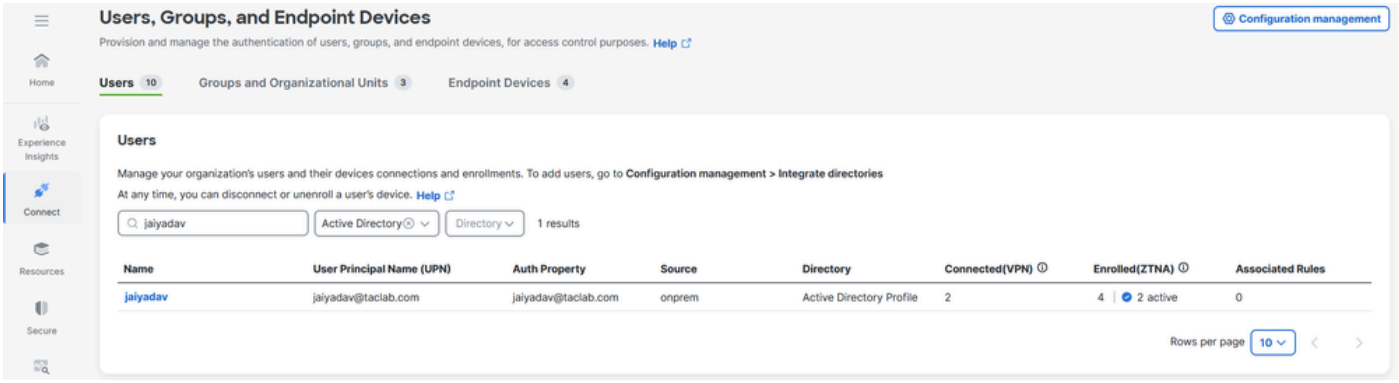
Méthode 3 : configuration du tunnel de la machine à l'aide du certificat utilisateur

Dans ce cas, pour que le champ principal s'authentifie, sélectionnez le champ de certificat qui contient l'e-mail de l'utilisateur ou l'UPN. L'accès sécurisé utilise l'e-mail ou l'UPN comme identificateur de tunnel de la machine. Le format de l'e-mail ou de l'UPN doit correspondre au format de l'identificateur de périphérique choisi

Suivez les étapes 1 à 4 pour la configuration du tunnel de machine

Étape 5 - Configurez le connecteur Active Directory pour pouvoir importer des utilisateurs sur Cisco Secure Access .

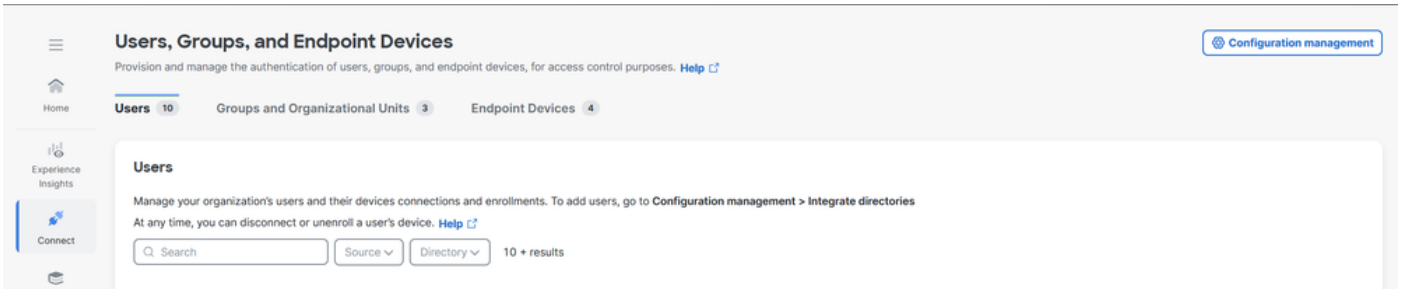
Pour plus d'informations, consultez Intégration Active Directory sur site



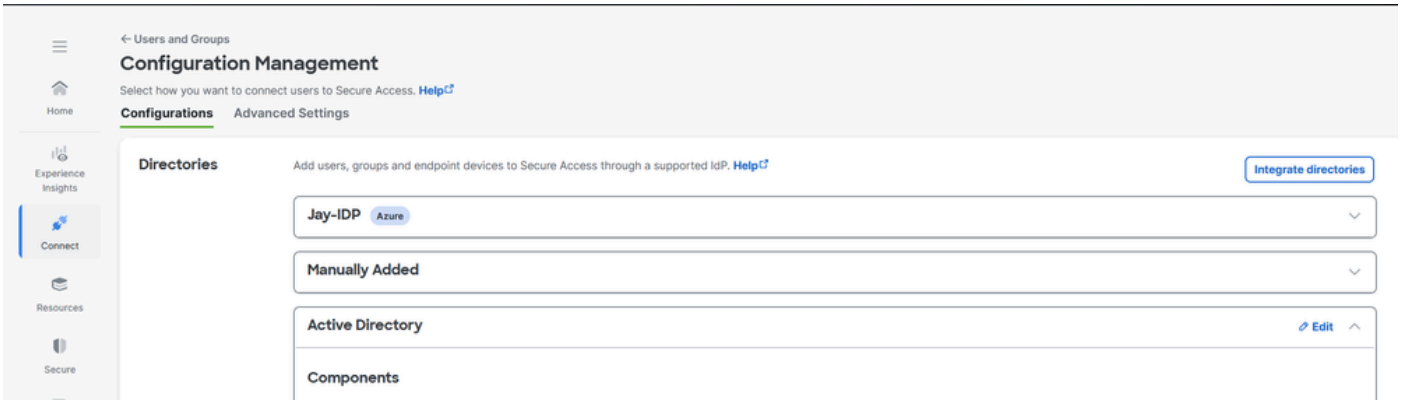
Étape 6 - Configurez l'authentification des utilisateurs

1. Accédez à Connect > Users, Groups and Endpoint Devices.

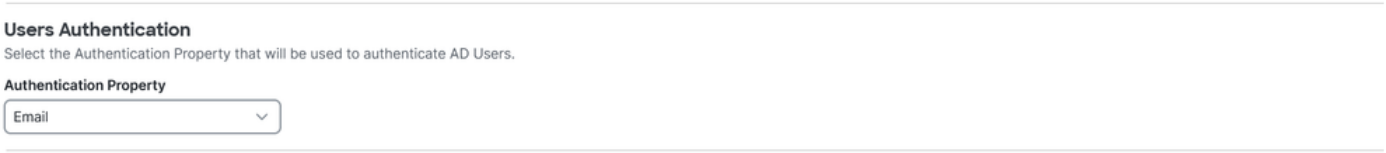
2. Cliquez sur Gestion de la configuration



3. Sous Configurations , modifiez Active Directory



4. Définir la propriété Authentification des utilisateurs sur E-mail



5. Cliquez sur Save et redémarrez les services du connecteur AD sur les serveurs sur lesquels il est installé

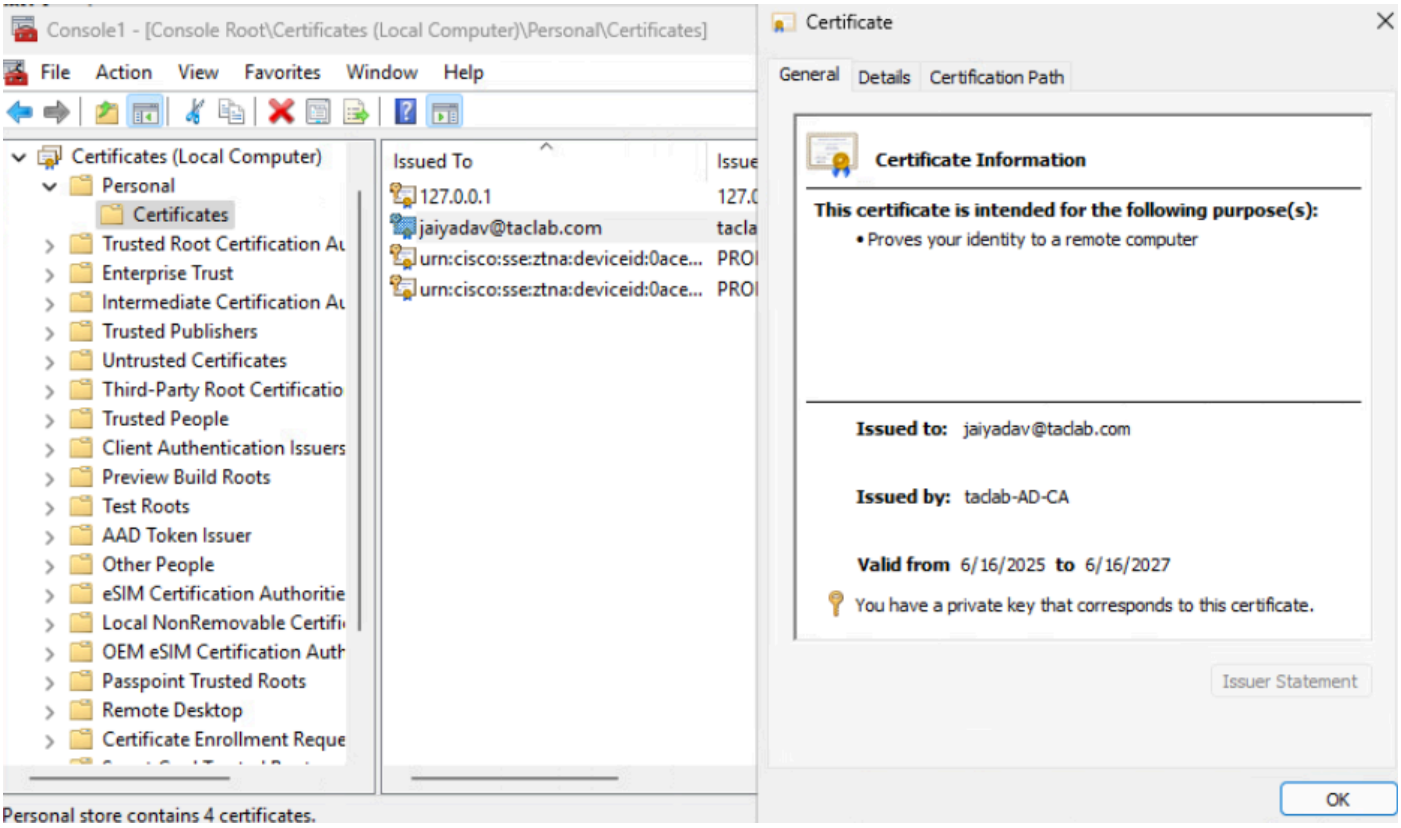
Étape 7 - Générez et importez un certificat de point de terminaison

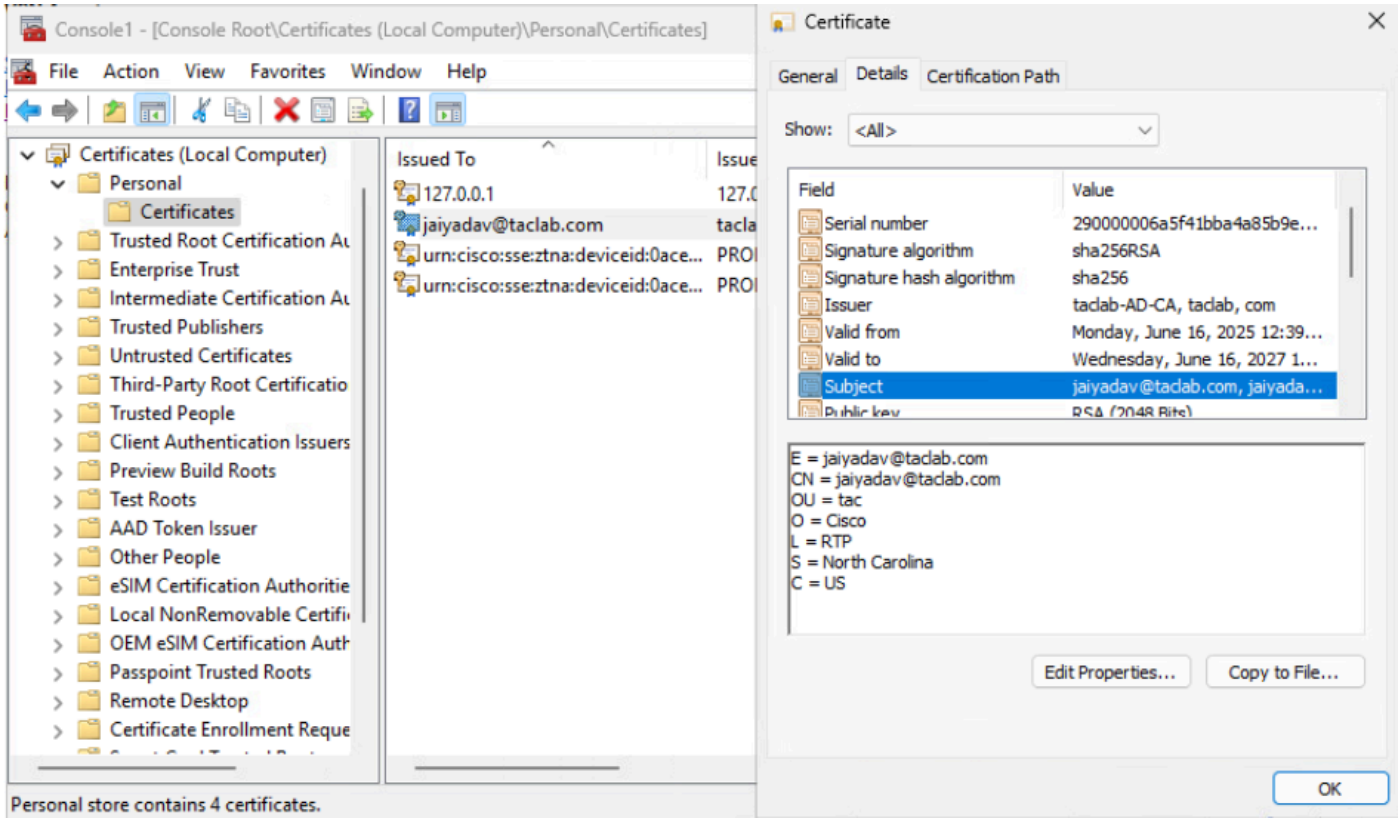
a. Générer un CSR, ouvrir un générateur CSR ou un outil OpenSSL

b. Générer un certificat de point de terminaison à partir de CA

c. Convertissez le fichier .cert au format PKCS12

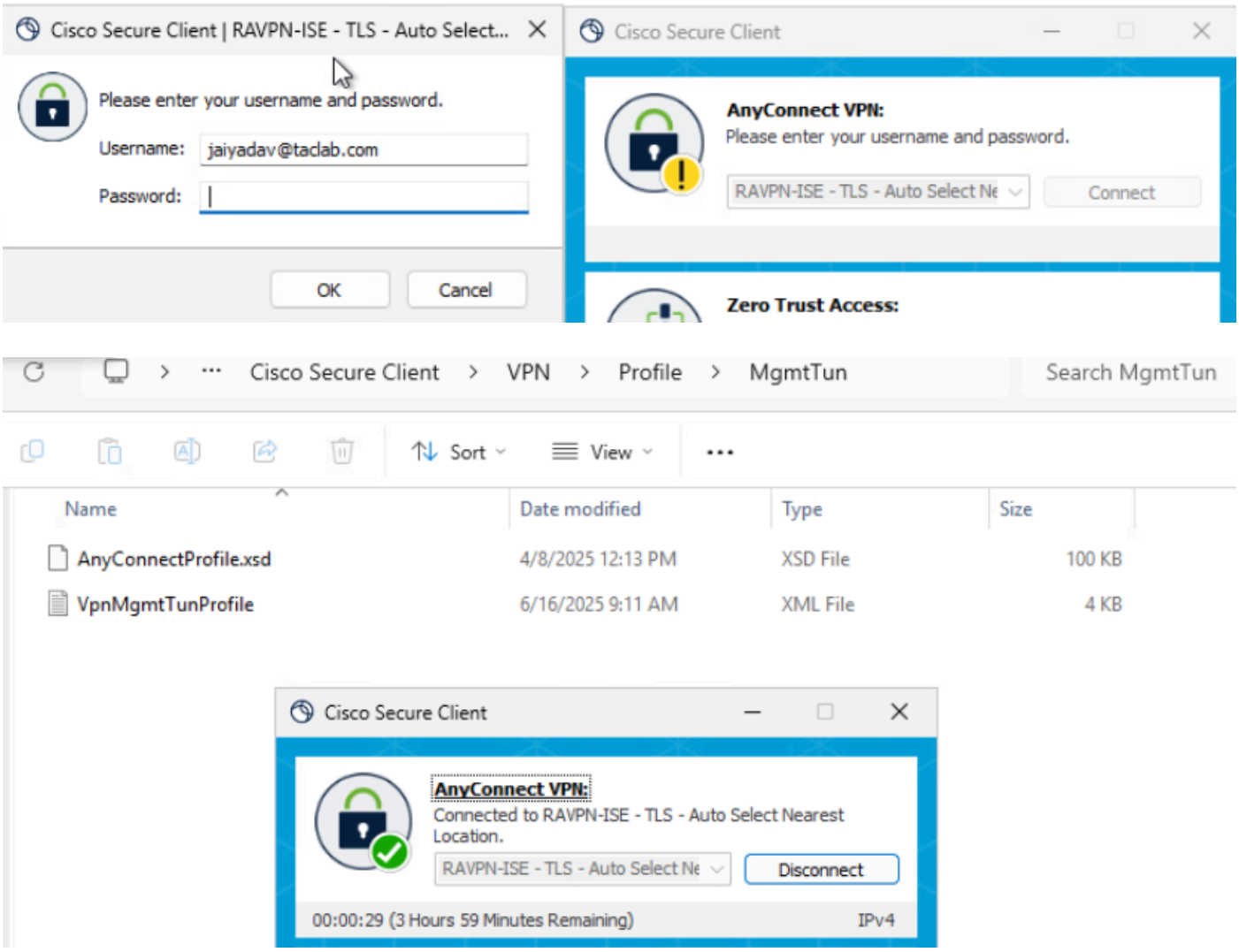
d. Importer le certificat PKCS12 dans le magasin de certificats du point de terminaison



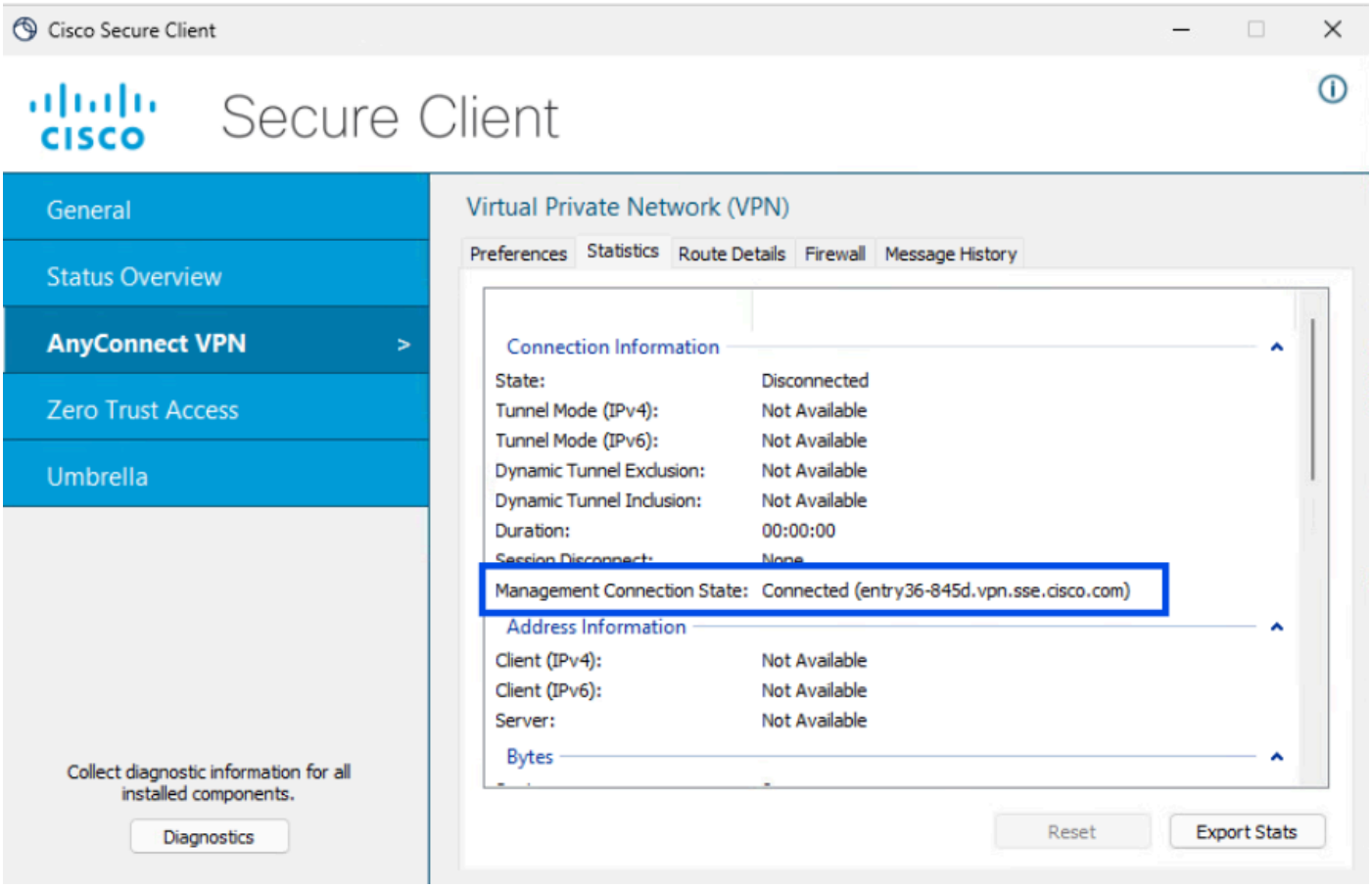


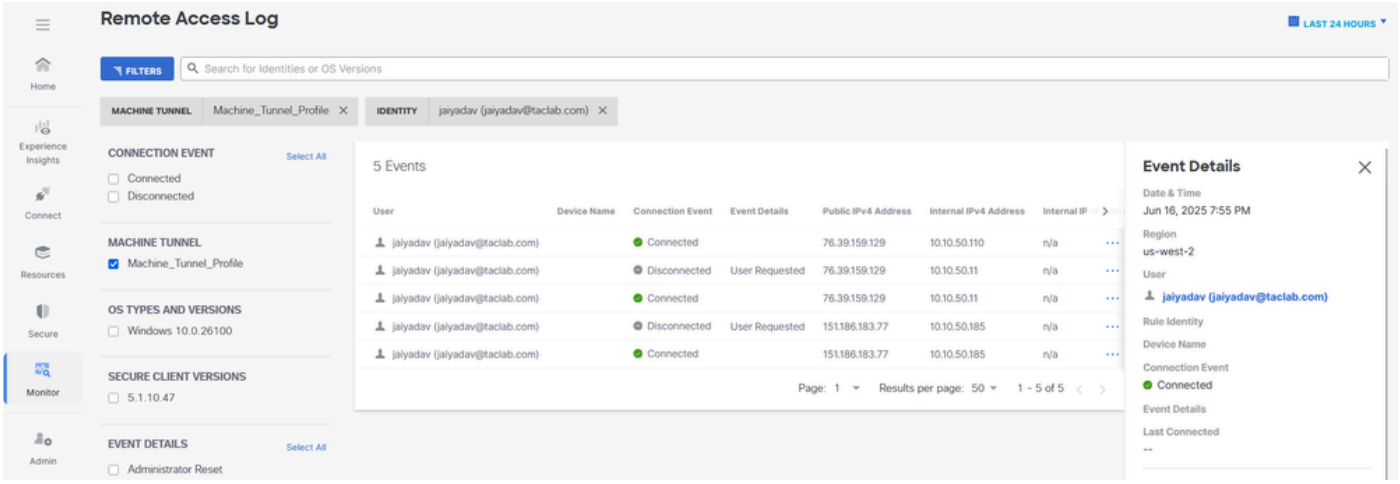
Étape 8 - Connectez-vous au tunnel machine

a. Se connecter à un tunnel utilisateur , il déclenche le téléchargement du profil xml du tunnel de la machine



b. Vérification de la connectivité du tunnel machine





Dépannage

Extrayez le bundle DART et ouvrez les journaux AnyConnectVPN et analysez les messages d'erreur

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.