

Cisco Secure Accessでのマシントンネルの設定

内容

[はじめに](#)

[ネットワーク図](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[マシントンネルの操作](#)

[制限事項](#)

[設定](#)

[方法1: ユーザmachine@sse.comでマシントンネルを設定する](#)

[ステップ1: 一般設定](#)

[ステップ2-マシン証明書の認証](#)

[ステップ3: トラフィックのステアリング \(スプリットトンネル\)](#)

[ステップ4: Cisco Secure Clientの設定](#)

[ステップ5: Cisco Secure Accessにmachine@sse.comuserが存在するかどうかを確認します](#)

[手順6: machine@sse.comのCA署名付き証明書を生成する](#)

[ステップ7: テストマシンにマシン証明書をインポートする](#)

[ステップ8-マシントンネルへの接続](#)

[方法2: エンドポイント証明書を使用してマシントンネルを設定する](#)

[ステップ5: Cisco Secure Access\(ACS\)でエンドポイントをインポートできるようにADコネクタを設定します。](#)

[手順6: エンドポイントデバイス認証の設定](#)

[手順7: エンドポイント証明書の生成とインポート](#)

[ステップ8-マシントンネルへの接続](#)

[方法3: ユーザ証明書を使用してマシントンネルを設定する](#)

[ステップ5: Cisco Secure Access\(ACS\)でユーザをインポートできるようにADコネクタを設定します。](#)

[ステップ6: ユーザ認証の設定](#)

[手順7: エンドポイント証明書の生成とインポート](#)

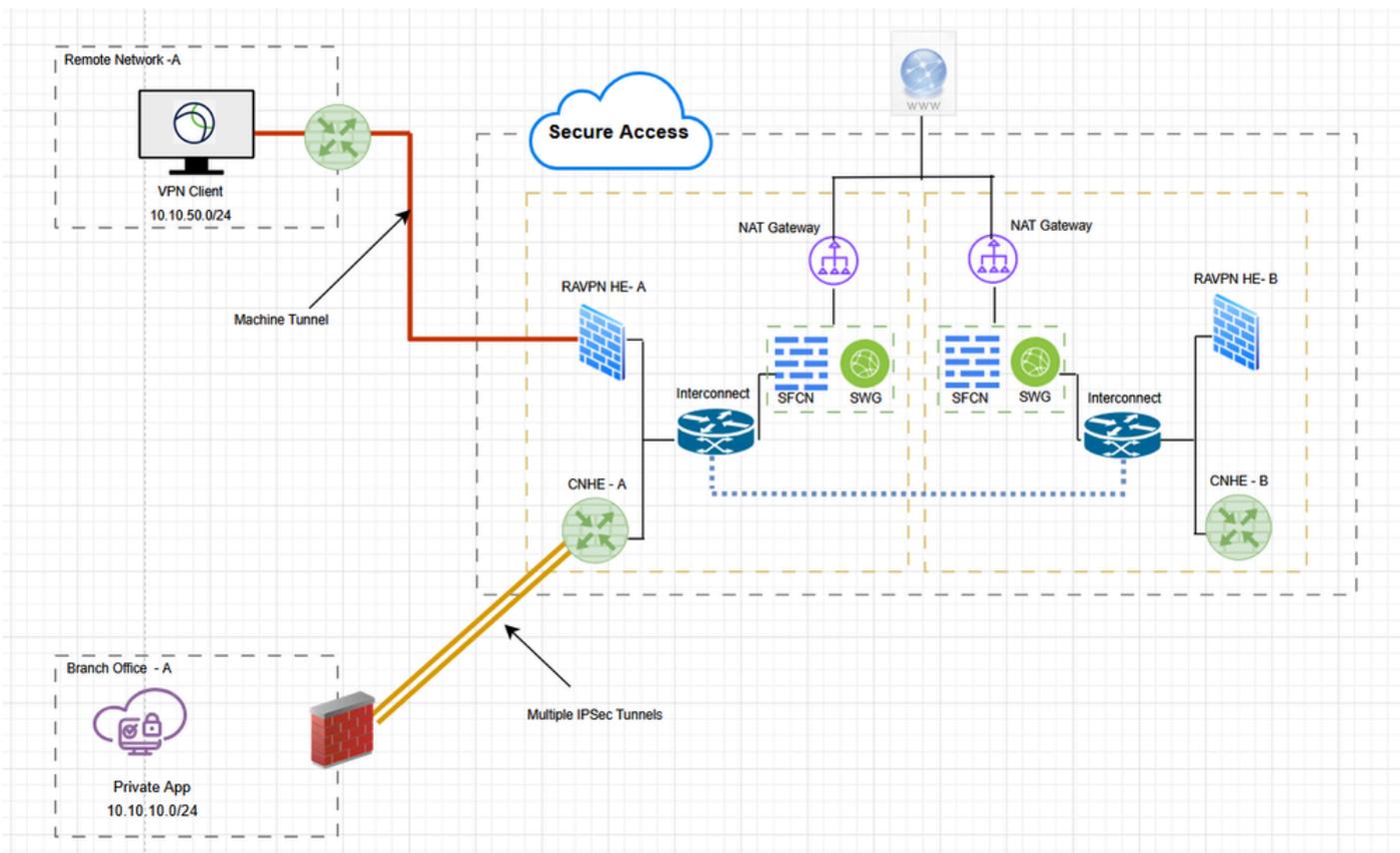
[ステップ8-マシントンネルへの接続](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、セキュアアクセスをVPNゲートウェイとして設定し、VPNマシントンネル経由でセキュアクライアントからの接続を受け入れる方法について説明します。

ネットワーク図



前提条件

- セキュアアクセスの完全な管理者ロール
- Cisco Secure Accessで設定された少なくとも1つのユーザVPNプロファイル
- Cisco Secure Access上のユーザIPプール

要件

次の項目に関する知識があることが推奨されます。

- 509証明書
- OpenSSL

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- シスコセキュアアクセス
- Cisco Secureクライアント5.1.10
- Windows 11
- Windows Server 2019 - CA

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

背景説明

セキュアアクセスVPNマシントンネルは、エンドユーザによってVPN接続が確立されたときだけでなく、クライアントシステムの電源がオンになるたびに企業ネットワークへの接続を確保します。オフィス外のエンドポイント、特にユーザがVPN経由でオフィスのネットワークにほとんど接続していないデバイスに対して、パッチ管理を実行できます。企業ネットワーク接続を必要とするエンドポイントOSログインスクリプトでも、この機能を利用できます。このトンネルをユーザの操作なしで作成するには、証明書ベースの認証が使用されます。

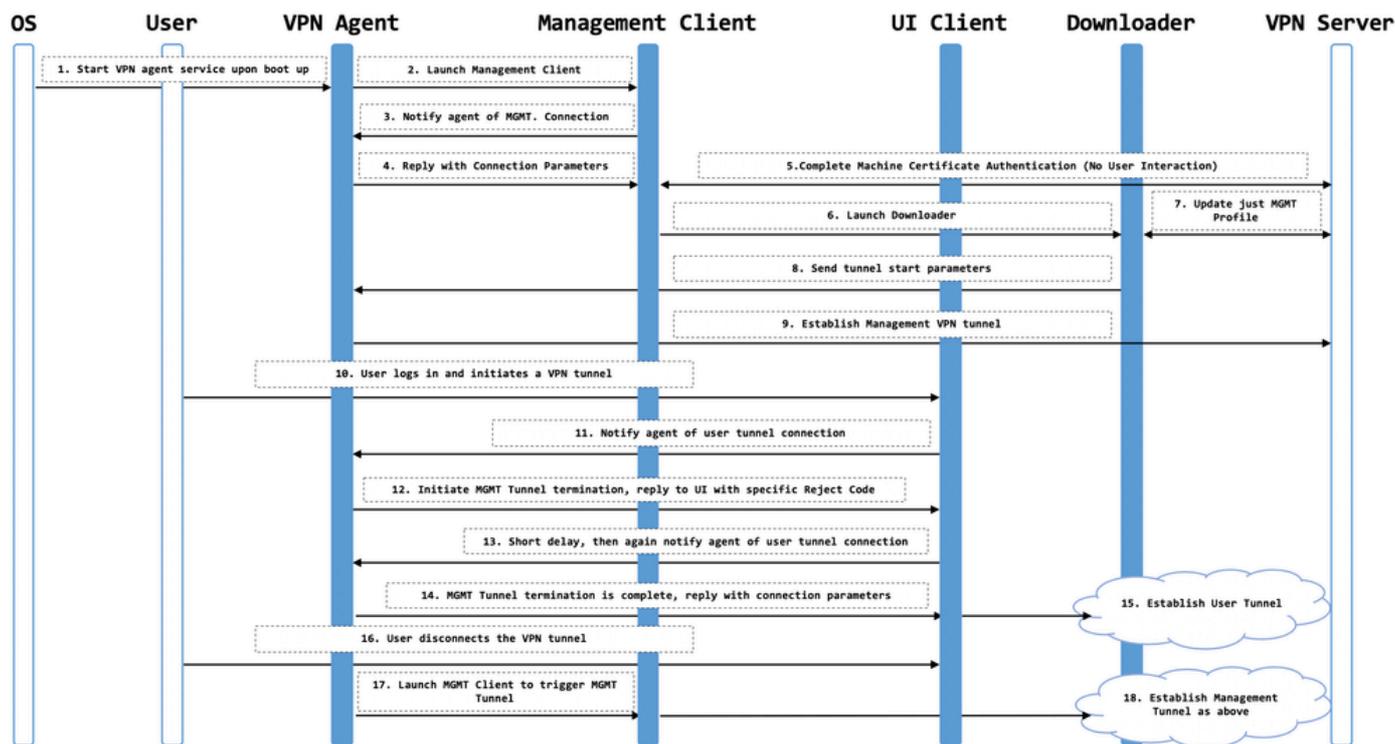
Secure Accessマシントンネルを使用すると、管理者はユーザが介入しなくても、ユーザがログインする前にCisco Secure Clientを接続できます。Secure Accessマシントンネルは、エンドポイントがオフプレミスで、ユーザが開始したVPNから切断されたときにトリガーされます。セキュアアクセスVPNマシントンネルは、エンドユーザに対して透過的であり、ユーザがVPNを開始すると自動的に切断されます。

マシントンネルの操作

セキュアクライアントVPNエージェントサービスは、システムのブート時に自動的に開始されます。セキュアクライアントVPNエージェントは、VPNプロファイルを使用して、マシントンネル機能が有効になっていることを検出します。マシントンネル機能が有効になっている場合、エージェントは管理クライアントアプリケーションを起動してマシントンネル接続を開始します。管理クライアントアプリケーションは、VPNプロファイルからのホストエントリを使用して接続を開始します。次に、VPNトンネルは通常どおり確立されますが、1つの例外があります。マシントンネルはユーザに対して透過的に動作するように意図されているため、マシントンネルの接続中にソフトウェアの更新は行われません。

ユーザがセキュアクライアントを介してVPNトンネルを開始すると、マシントンネルの終端がトリガーされます。マシントンネルの終端時に、ユーザトンネルの確立は通常どおり継続されます。

ユーザがVPNトンネルの接続を解除すると、マシントンネルの自動再確立がトリガーされます。



制限事項

- ユーザーの操作はサポートされていません。
- マシン証明書ストア(Windows)による証明書ベースの認証のみがサポートされます。
- 厳密なサーバ証明書チェックが適用されます。
- プライベートプロキシはサポートされていません。
- パブリックプロキシはサポートされていません (ネイティブプロキシ設定がブラウザから取得されないプラットフォームでは、ProxyNative値がサポートされています)。
- セキュアクライアントカスタマイズスクリプトはサポートされていません

設定

方法1：ユーザmachine@sse.comでマシントンネルを設定する

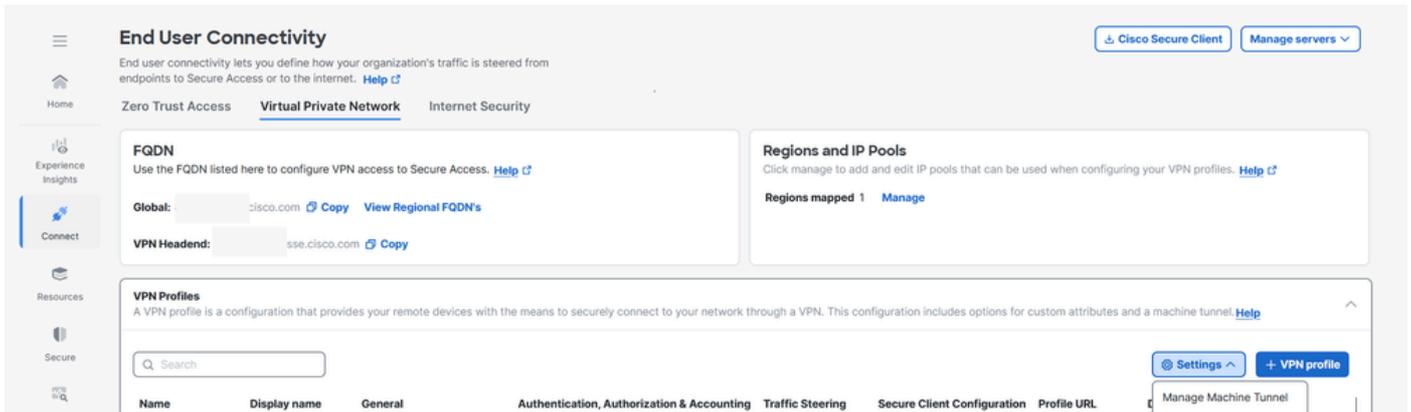
ステップ1：一般設定

このマシントンネルが使用するドメインとプロトコルを含む全般的な設定を構成します。

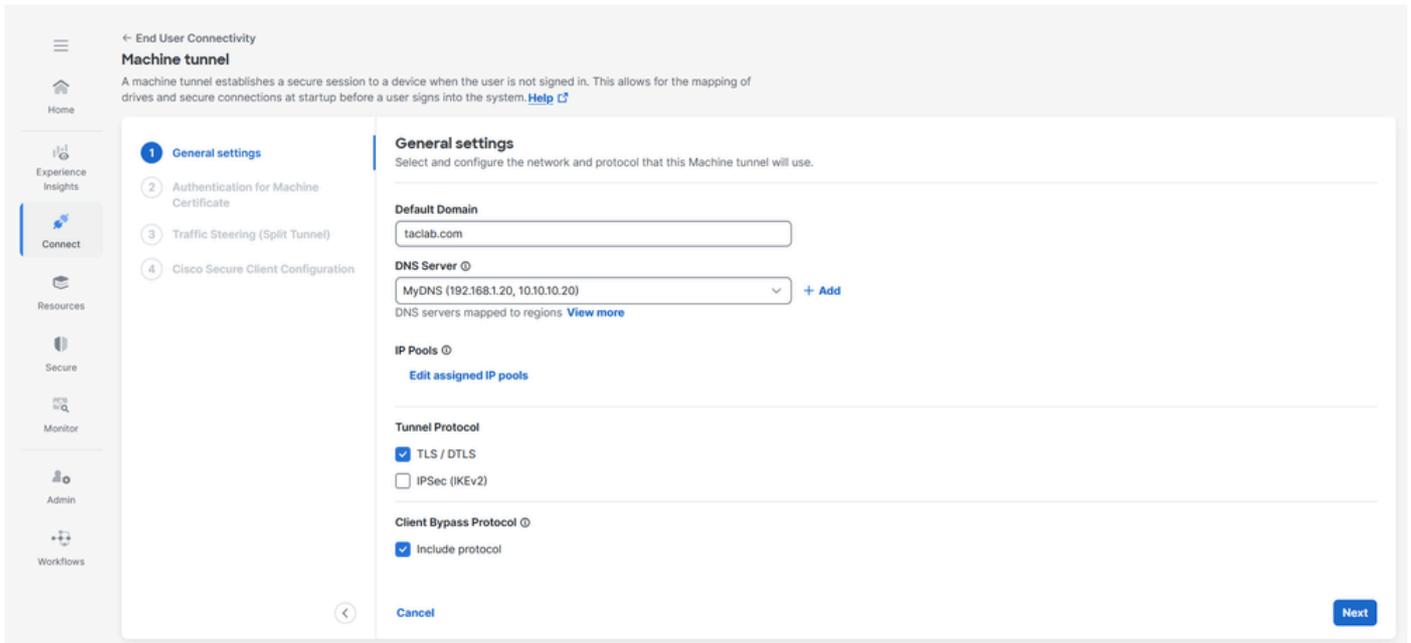
1. Connect > End User Connectivity > Virtual Private Networkの順に選択します。

2. VPN Profilesに移動し、マシントンネルの設定を構成します。

a. Settingsをクリックし、ドロップダウンからManage Machine Tunnelを選択します。



3. Default Domainを入力します。
4. Manage Regions and IP PoolsページでマッピングされたDNS Serverは、デフォルトサーバとして設定されます。デフォルトのDNSサーバをそのまま使用するか、ドロップダウンから別のDNSサーバを選択するか、+追加をクリックして新しいDNSサーバペアを追加します。別のDNSサーバを選択するか、新しいDNSサーバを追加すると、このデフォルトサーバが上書きされます。
5. IP Poolsドロップダウンから、リージョンごとに1つのIPプールを選択します。有効な設定のためには、VPNプロファイルの各リージョンに少なくとも1つのIPプールが割り当てられている必要があります。
6. このマシントンネルが使用するトンネルプロトコルを選択します。
 - TLS/DTLS
 - IPSec(IKEv2)少なくとも1つのプロトコルを選択する必要があります。
7. オプションで、Include protocolにチェックマークを入れて、クライアントバイパスプロトコルを適用します。
 - a. IPプロトコルに対してクライアントバイパスプロトコルが有効になっており、アドレスプールがそのプロトコルに対して設定されていない場合（つまり、そのプロトコルのIPアドレスがASAによってクライアントに割り当てられていない場合）、そのプロトコルを使用するIPトラフィックはVPNトンネルを介して送信されません。トンネルの外部に送信されます。
 - b. クライアントバイパスプロトコルが無効で、アドレスプールがそのプロトコル用に設定されていない場合、クライアントはVPNトンネルが確立されると、そのIPプロトコル用のすべてのトラフィックをドロップします。

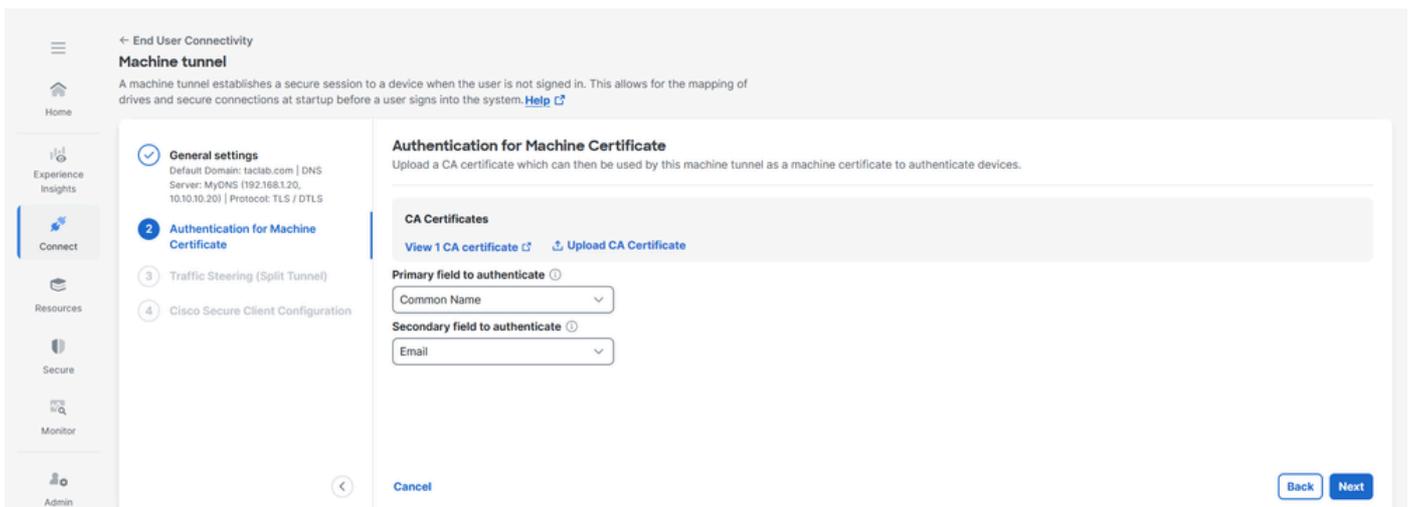


8. Nextをクリックします。

ステップ2 – マシン証明書の認証

マシントンネルはエンドユーザに対して透過的で、ユーザがVPNセッションを開始すると自動的に切断されます。このトンネルをユーザの操作なしで作成するには、証明書ベースの認証が使用されます。

1. リストからCA証明書を選択するか、Upload CA certificatesをクリックします
2. 証明書ベースの認証フィールドを選択します。詳細については、「[証明書ベースの認証フィールド](#)」を参照してください。



3. Nextをクリックします。

ステップ3 : トラフィックのステアリング (スプリットトンネル)

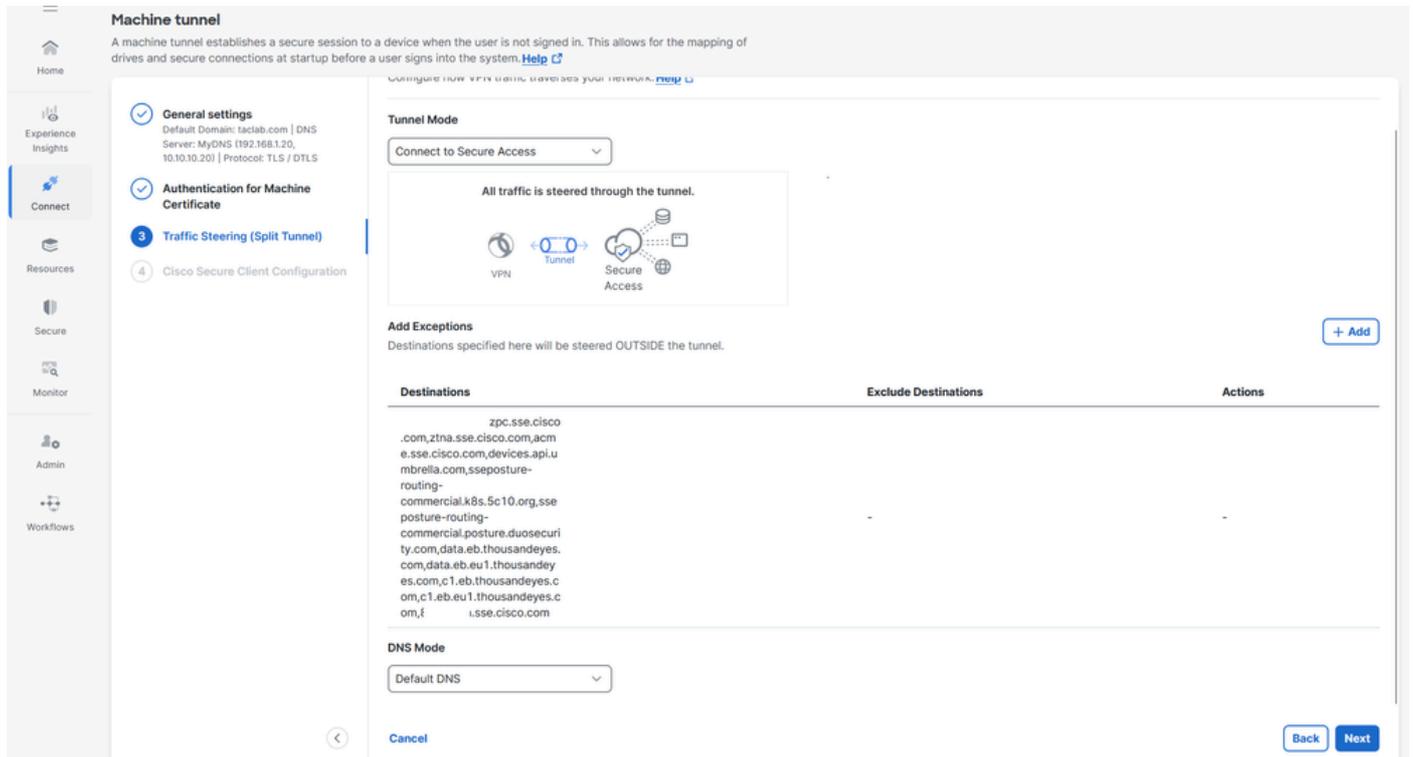
トラフィックステアリング (スプリットトンネル) では、セキュアアクセスへの完全なトンネル

接続を維持するようにマシントンネルを設定するか、または必要な場合にのみトラフィックをVPN経由で転送するようにスプリットトンネル接続を使用するように設定できます。詳細については、「[マシントンネルトラフィックステアリング](#)」を参照してください

1. トンネルモードを選択します

2. トンネルモードの選択 (トンネルモードの選択) によっては、例外の追加が可能です。

3. DNSモードの選択

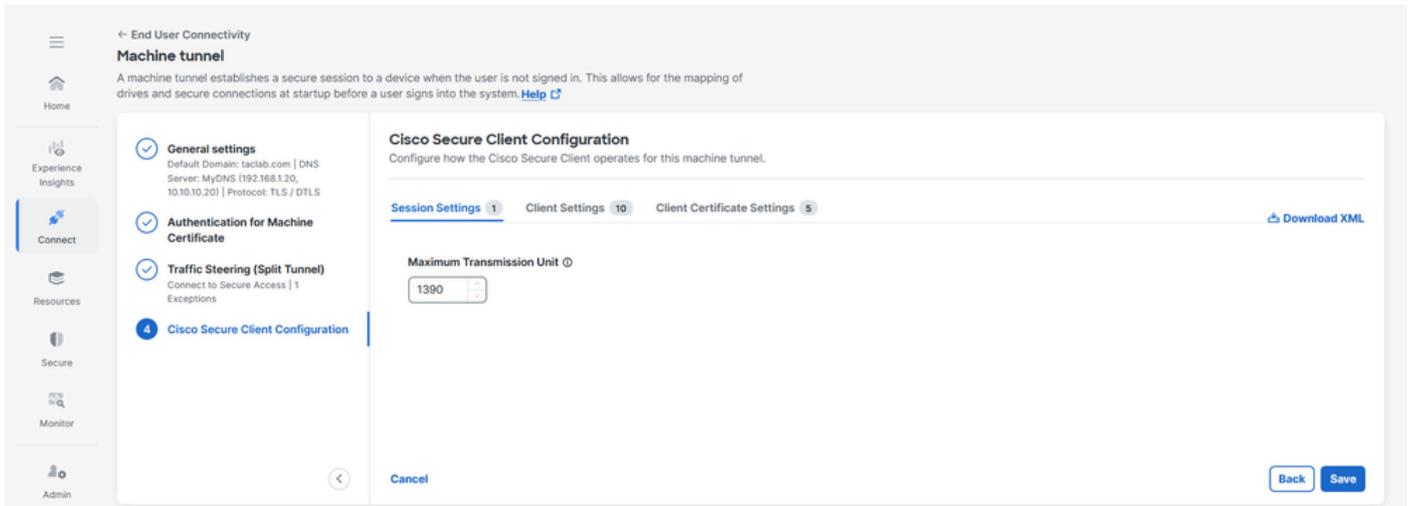


4. Nextをクリックします。

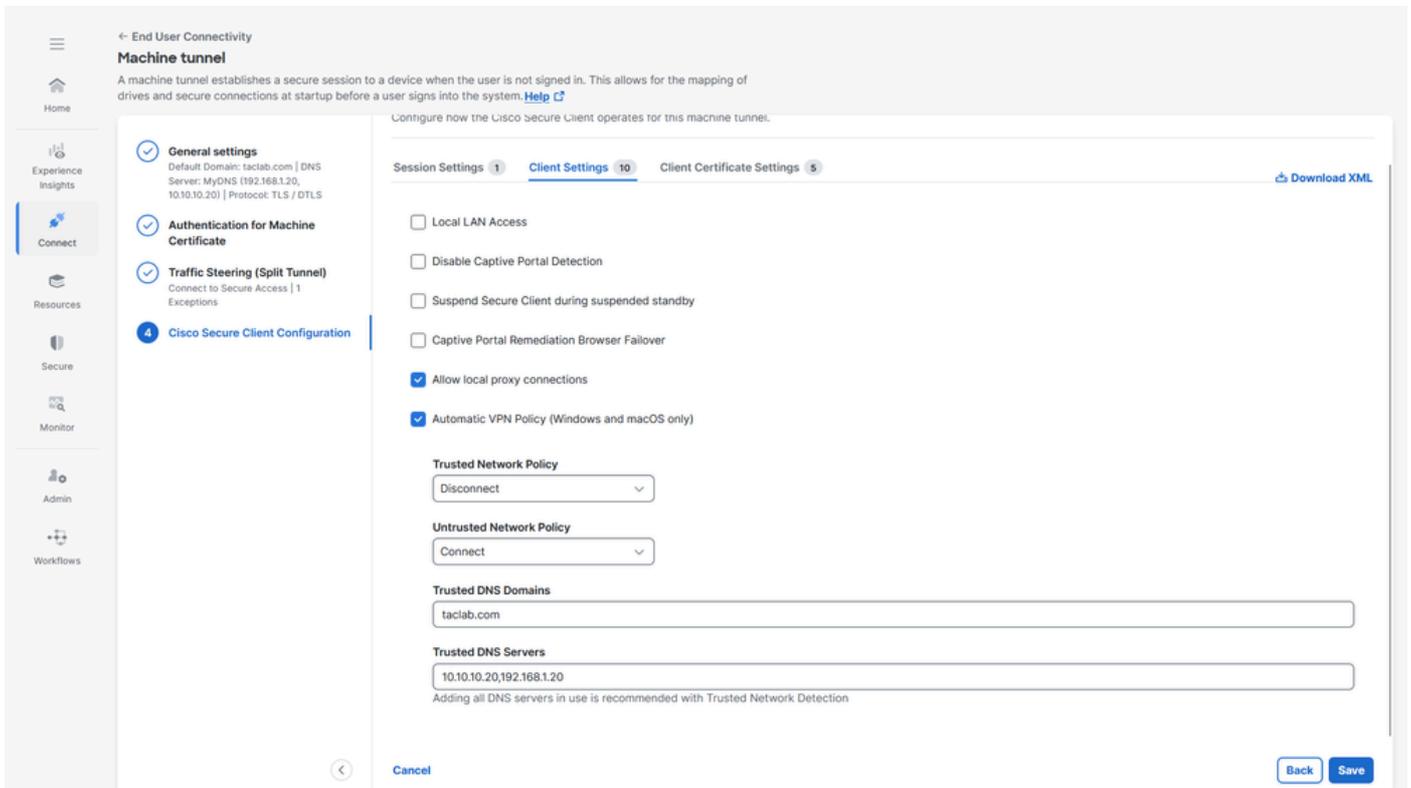
ステップ4: Cisco Secure Clientの設定

特定のVPNマシントンネルのニーズに基づいて、Cisco Secure Client設定のサブセットを変更できます。詳細については、「[セキュアクライアントの設定](#)」を参照してください。

1. 最大伝送ユニット(MTU)、つまり、フラグメンテーションなしでVPNトンネルで送信できるパケットの最大サイズを確認します



2. クライアント設定 (トンネルモード) : 詳細は、『[マシントネルクライアント設定](#)』を参照してください



3. [クライアント証明書の設定]で、オプションを適宜選択します

- a. Windows Certificate Store Override:管理者は、Secure Clientで、Windowsマシン (ローカルシステム) の証明書ストアにある証明書をクライアントの証明書認証に使用できます。
- b. 自動証明書選択 : セキュアゲートウェイで複数の証明書認証が設定されている場合
- c. 証明書のピンニング : デバイスを認証するためのマシン証明書としてマシントネルで使用できるCA証明書
- d. 証明書照合 : 証明書照合基準が指定されていない場合、Cisco Secure Clientは証明書照合ルールを適用します

i. 主な用途 : Digital_Signature

ii. 拡張キー使用法 : クライアント認証

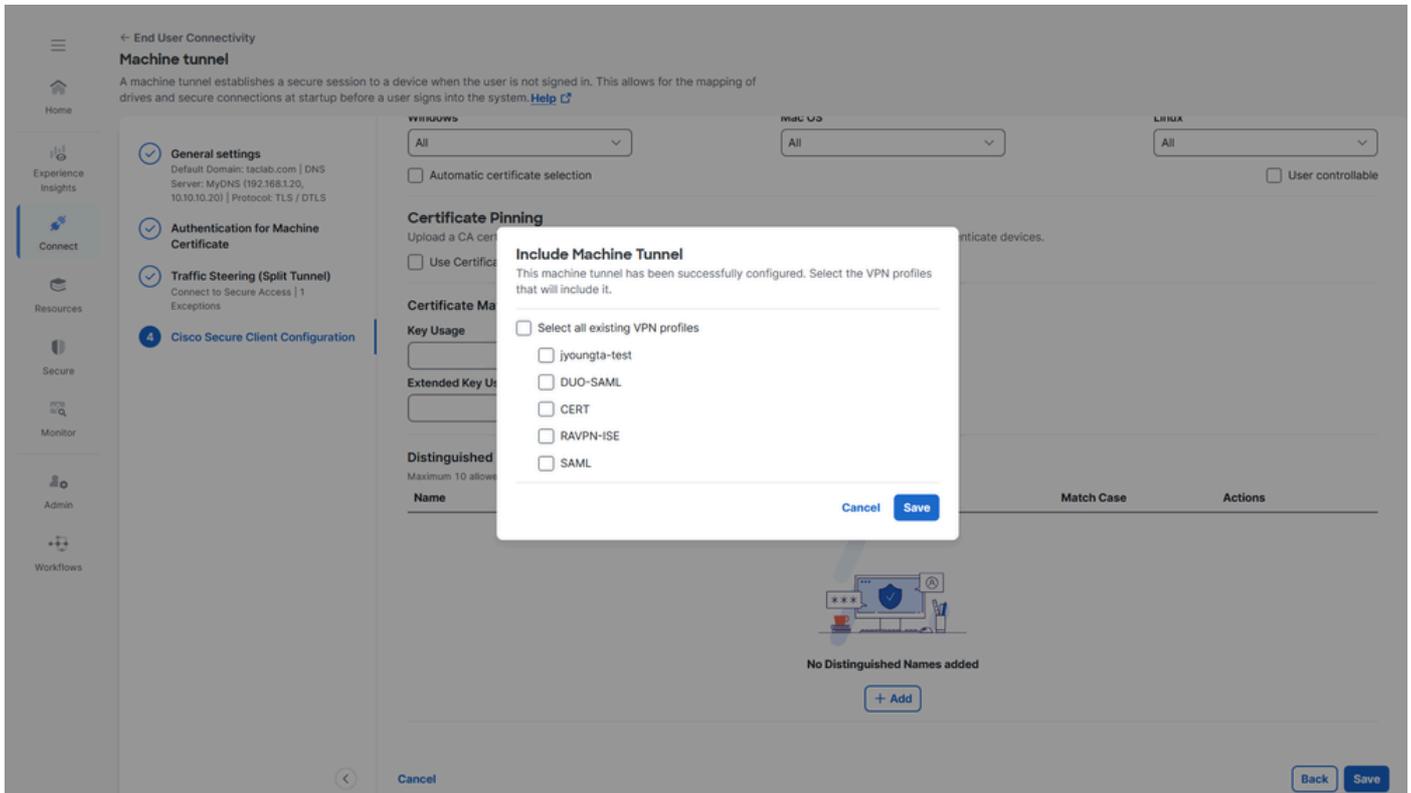
e. Distinguished Name (DN ; 識別名) : 受け入れ可能なクライアント証明書を選択する際の、完全一致基準のための識別名(DN)を指定します。複数の識別名を追加すると、各証明書がすべてのエントリに対してチェックされ、すべてのエントリが一致する必要があります。

The screenshot shows the 'Cisco Secure Client Configuration' page for a 'Machine tunnel'. The left sidebar contains navigation options: Home, Experience Insights, Connect, Resources, Secure, Monitor, Admin, and Workflows. The main content area is titled 'Machine tunnel' and includes a description: 'A machine tunnel establishes a secure session to a device when the user is not signed in. This allows for the mapping of drives and secure connections at startup before a user signs into the system. [Help](#)'. Below this, there are three tabs: 'Session Settings 1', 'Client Settings 10', and 'Client Certificate Settings 5'. The 'Client Certificate Settings' tab is active, showing the following sections:

- Certificate Operating System**: Windows certificate store override
- Client Certificate Store**:
 - Windows: All (dropdown)
 - Mac OS: All (dropdown)
 - Linux: All (dropdown)
 - Automatic certificate selection
 - User controllable
- Certificate Pinning**: Upload a CA certificate which can then be used by this machine tunnel as a machine certificate to authenticate devices. Use Certificate Pinning
- Certificate Matching**:
 - Key Usage: (dropdown)
 - Extended Key Usage: (dropdown)
- Distinguished Name**: Maximum 10 allowed. A table with columns: Name, Pattern, Wildcard, Operator, Match Case, Actions.

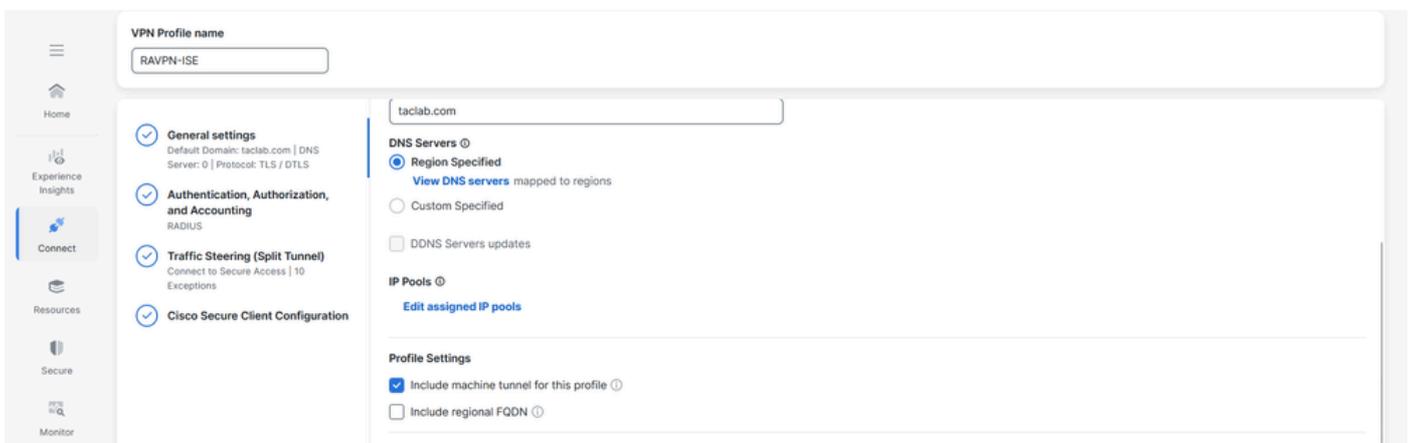
At the bottom, there are 'Cancel', 'Back', and 'Save' buttons.

4. ユーザVPNプロファイルにマシントンネルプロファイルを割り当て、Saveをクリックすると、ユーザVPNプロファイルを選択するオプションがあります



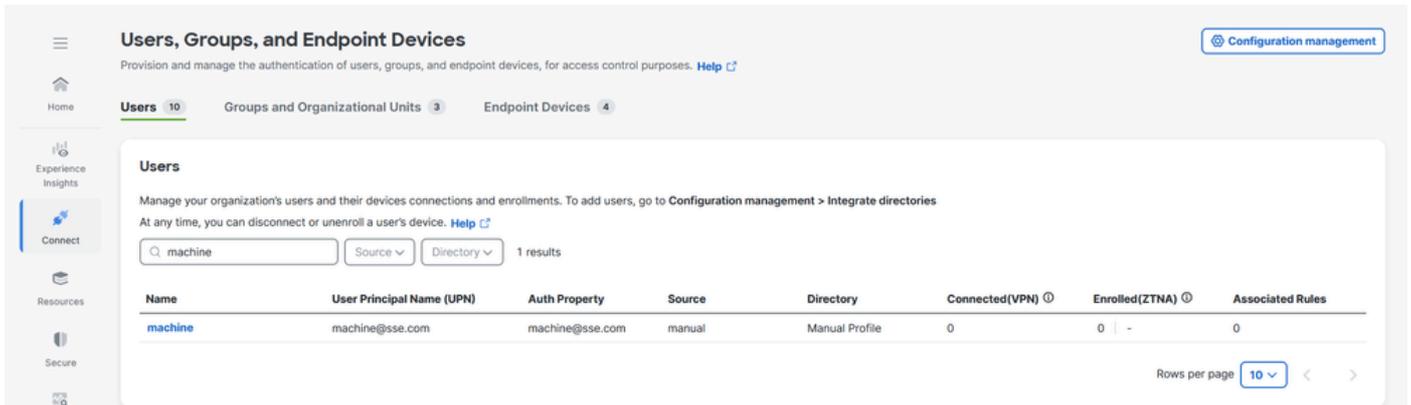
5. 「保存」をクリックします。

6. マシントネルプロファイルがユーザVPNプロファイルに接続されているかどうかを確認します



ステップ5: Cisco Secure Accessに machine@sse.com ユーザが存在するかどうかを確認します

1. Connect > Users, Groups, and Endpoint Devices > Usersの順に移動します。



2. [machine@sse.com](#)ユーザが手動でインポートを提示しない場合。詳細については、「[ユーザとグループの手動インポート](#)」を参照してください。

ステップ6:[machine@sse.com](#)用のCA署名付き証明書を生成する

1. 証明書署名要求を生成する

a. オンラインのCSRジェネレータソフトウェアである[CSR Generator](#)またはopenssl CLIを使用できます

openssl要求 – 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. CSRをコピーし、マシン証明書を生成する

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

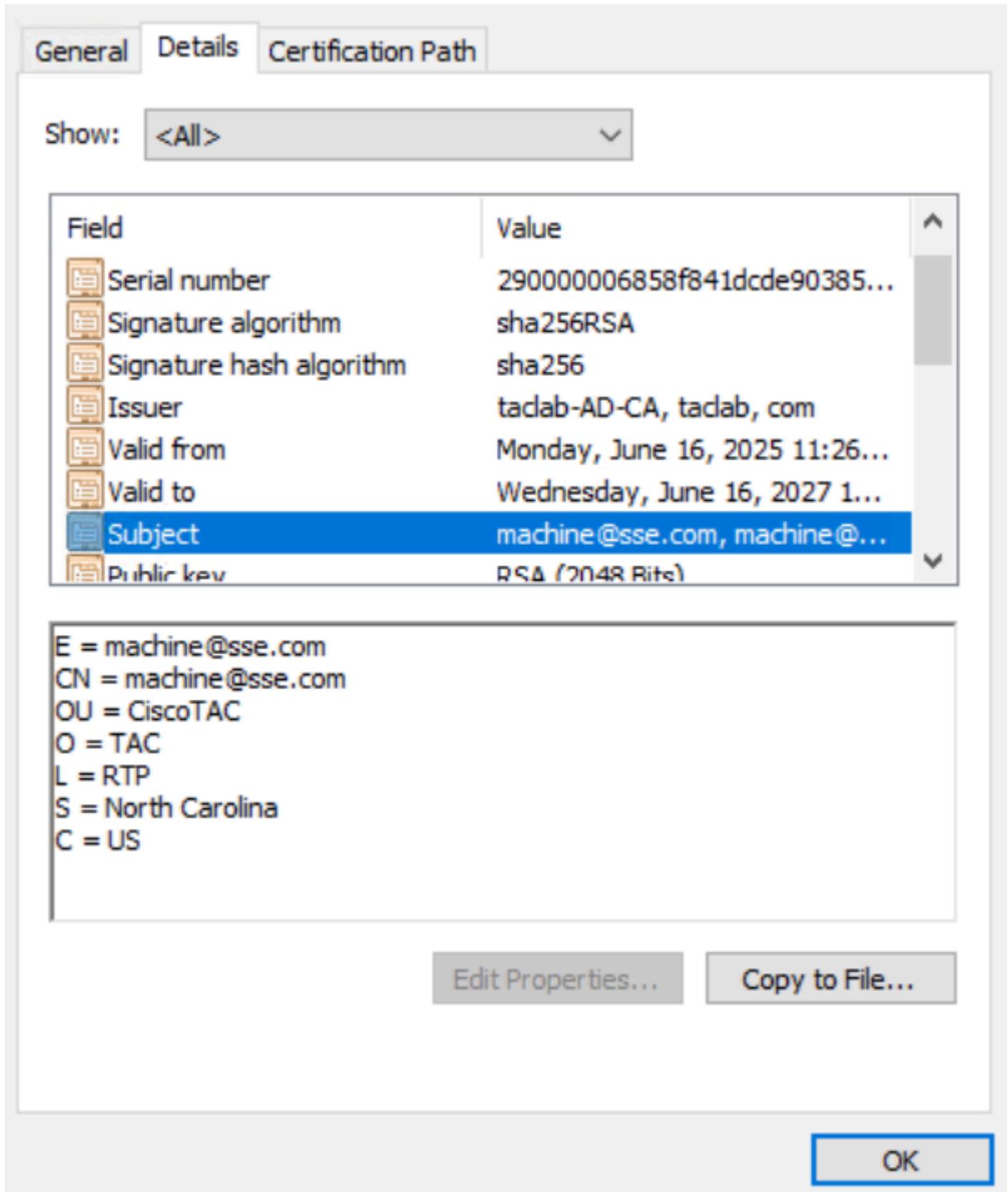
Issued by: tadab-AD-CA

Valid from 6/16/2025 **to** 6/16/2027

Install Certificate...

Issuer Statement

OK



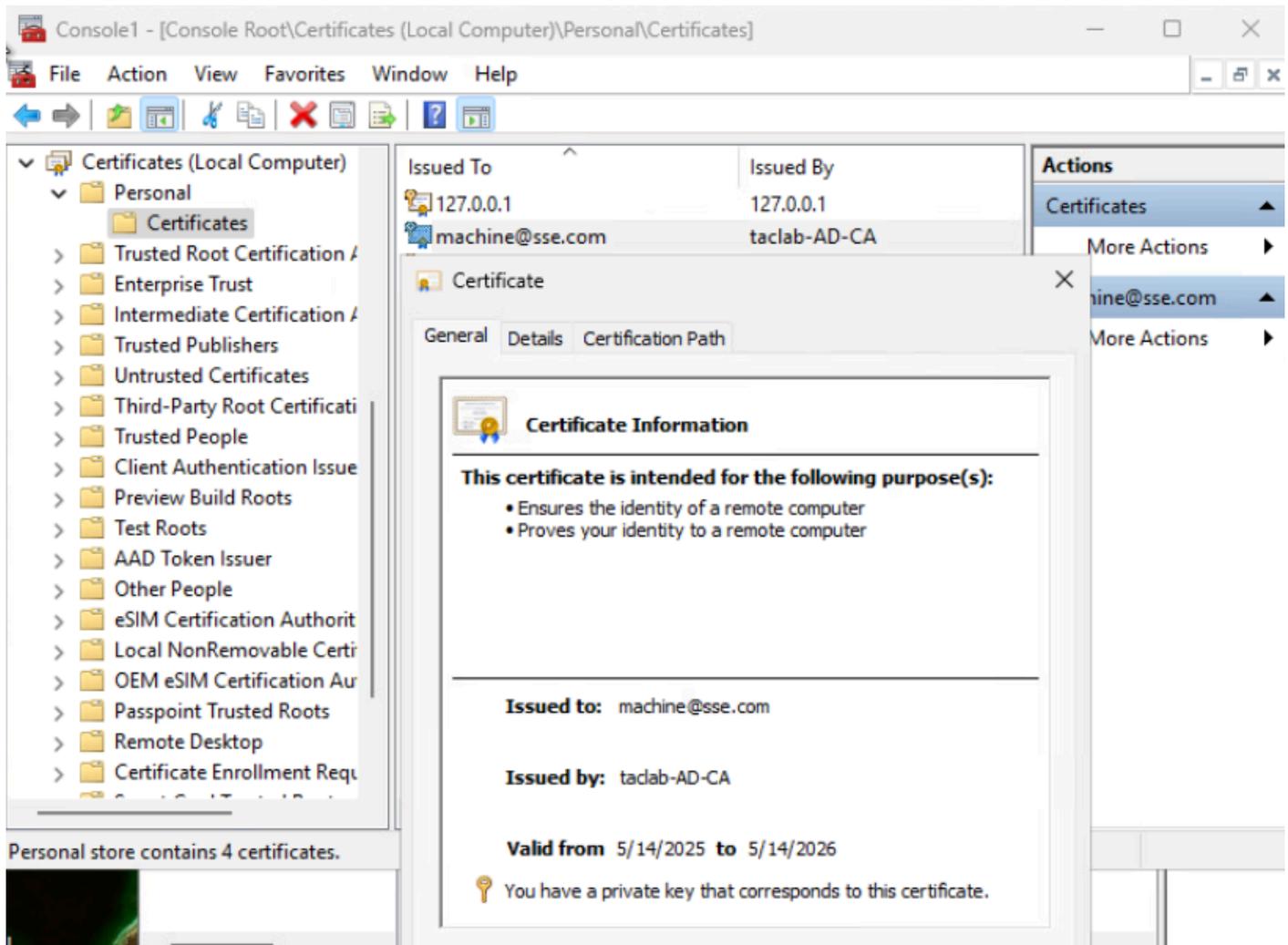
3. 前の手順 (ステップ1および2) で生成されたキーと証明書をそれぞれ使用して、マシン証明書をPKCS12形式に変換します

```
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#
```

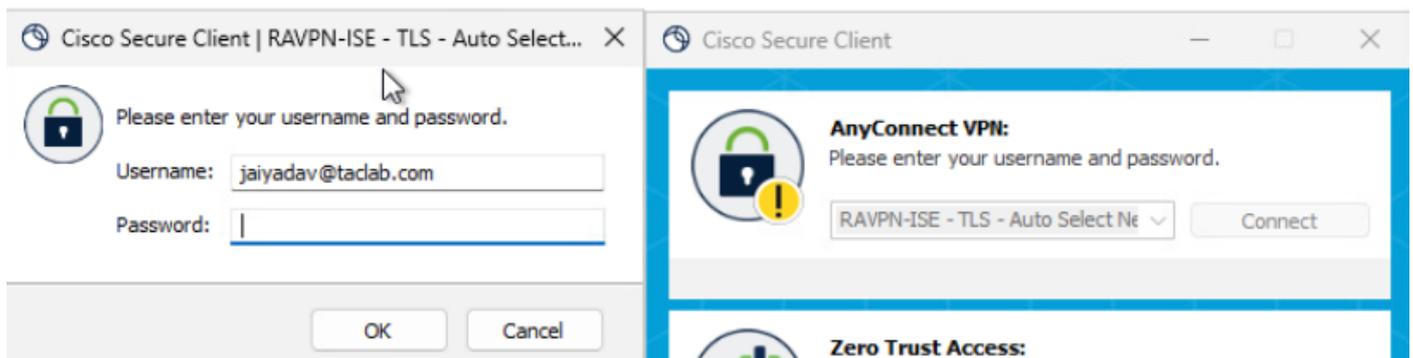
ステップ7 : テストマシンにマシン証明書をインポートする

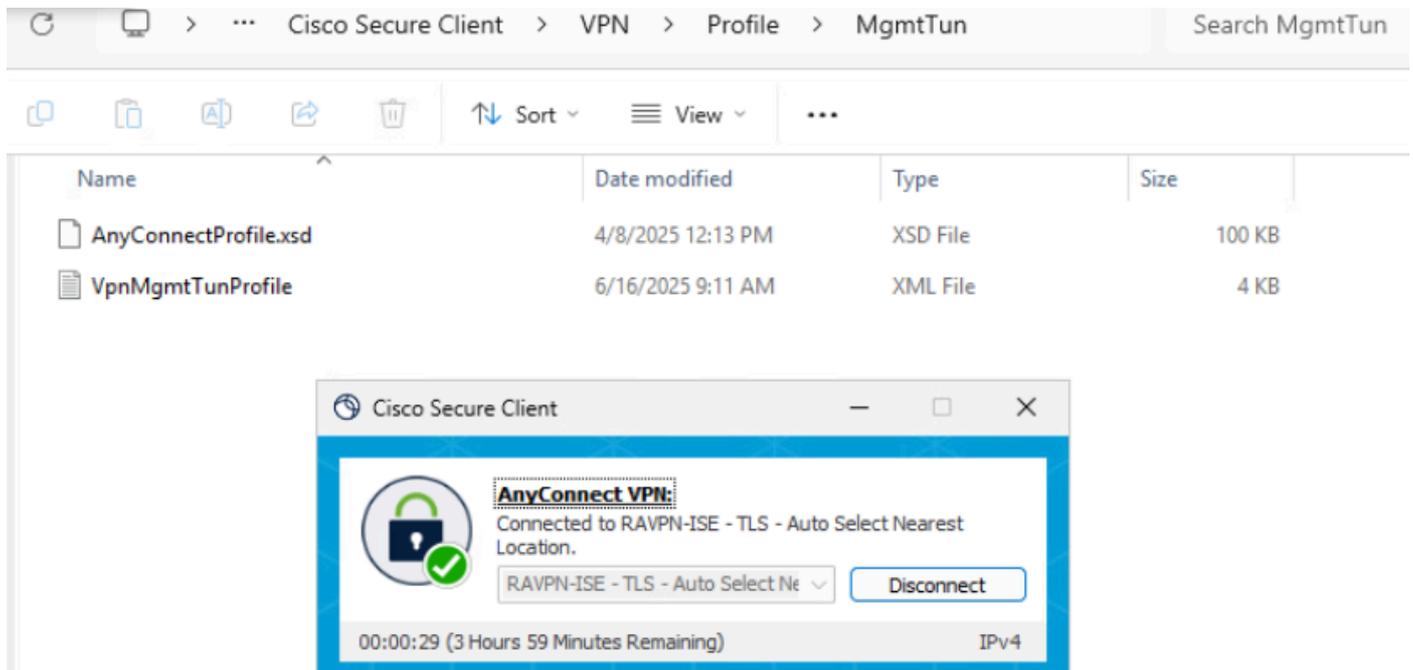
a. ローカルストアまたはマシンストアにPKCS12マシン証明書をインポートします



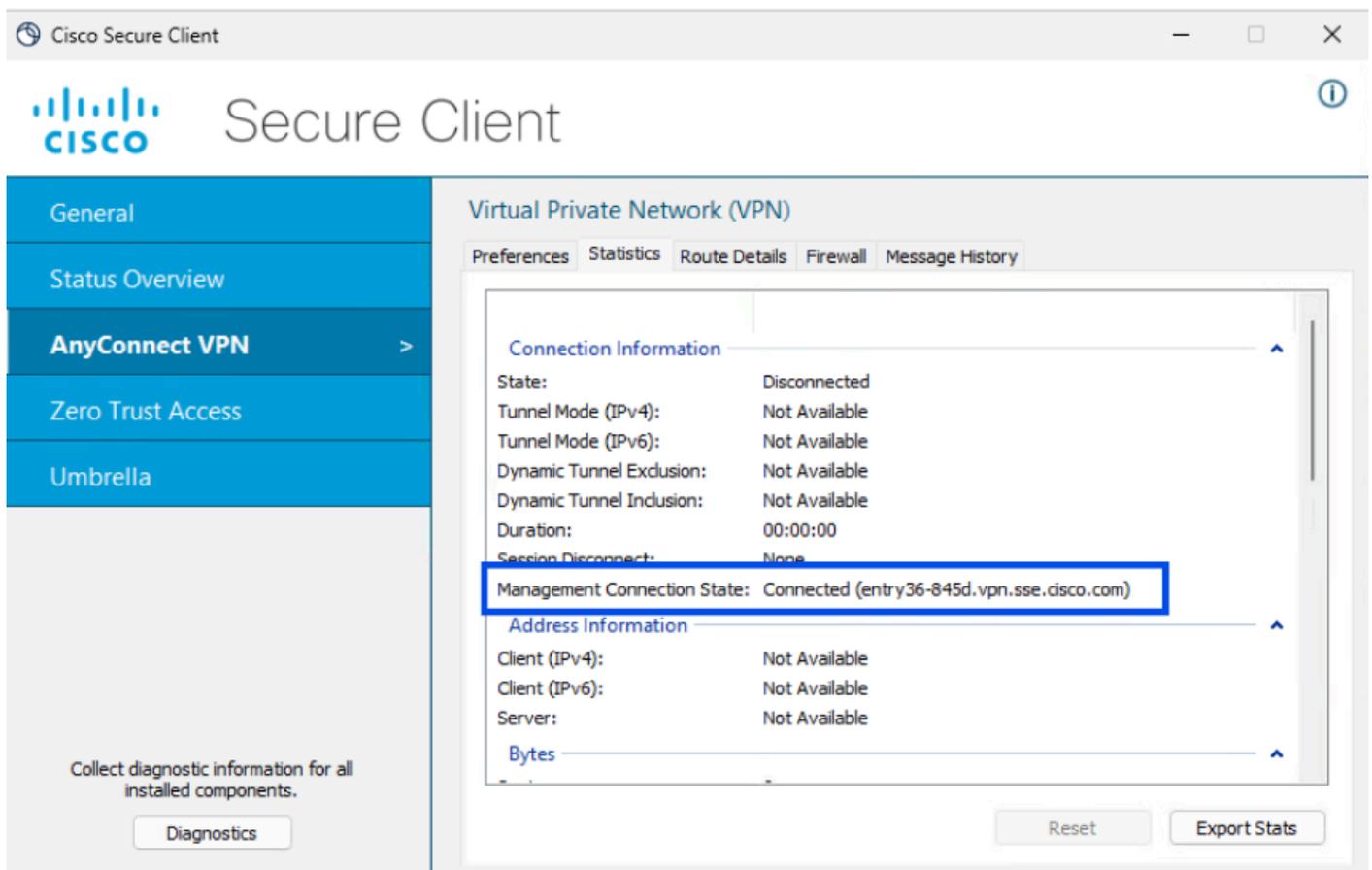
ステップ8 – マシントネルへの接続

a. ユーザトンネル(UTT)に接続します。これにより、マシンxmlプロファイルのダウンロードがトリガーされます。





b. マシントネル接続の確認



Remote Access Log LAST 24 HOURS

Search for Identities or OS Versions

CONNECTION EVENT Select All

Connected
 Disconnected

MACHINE TUNNEL

Machine_Tunnel_Profile

OS TYPES AND VERSIONS

Windows 10.0.26100

SECURE CLIENT VERSIONS

5.1.10.47

EVENT DETAILS Select All

Administrator Reset

23 Events

User	Device Name	Connection Event	Event Details	
machine (machine@sse.com)		Connected		15 ...
machine (machine@sse.com)		Disconnected	User Requested	15 ...
machine (machine@sse.com)		Connected		15 ...
machine (machine@sse.com)		Disconnected	User Requested	15 ...
machine (machine@sse.com)		Connected		15 ...
machine (machine@sse.com)		Disconnected	User Requested	15 ...
machine (machine@sse.com)		Connected		15 ...
jaiyadav (jaiyadav@taclab.com)		Disconnected	User Requested	15 ...
jaiyadav (jaiyadav@taclab.com)		Connected		15 ...

Event Details ×

Date & Time
Jun 16, 2025 4:29 PM

Region
us-west-2

User
machine (machine@sse.com)

Rule Identity

Device Name

Connection Event
Connected

Event Details
Last Connected
...

方法2：エンドポイント証明書を使用してマシントンネルを設定する

この場合、Primary field to authenticateでは、デバイス名（コンピュータ名）を含む証明書フィールドを選択します。Secure Accessは、マシントンネルIDとしてデバイス名を使用します。コンピュータ名の形式は、選択したデバイスIDの形式と一致する必要があります

マシントンネル設定のステップ1からステップ4に進みます

ステップ5: Cisco Secure Access(ACS)でエンドポイントをインポートできるようにADコネクタを設定します。

詳細については、「[On-Perm Active Directory Integration](#)」

Users, Groups, and Endpoint Devices Configuration management

Provision and manage the authentication of users, groups, and endpoint devices, for access control purposes. [Help](#)

Users 10 Groups and Organizational Units 3 **Endpoint Devices 4**

Endpoint Devices

Manage your endpoint device connections and AD device enrollments. To add new AD devices, go to [Configuration management > Integrate directories](#). [Help](#)

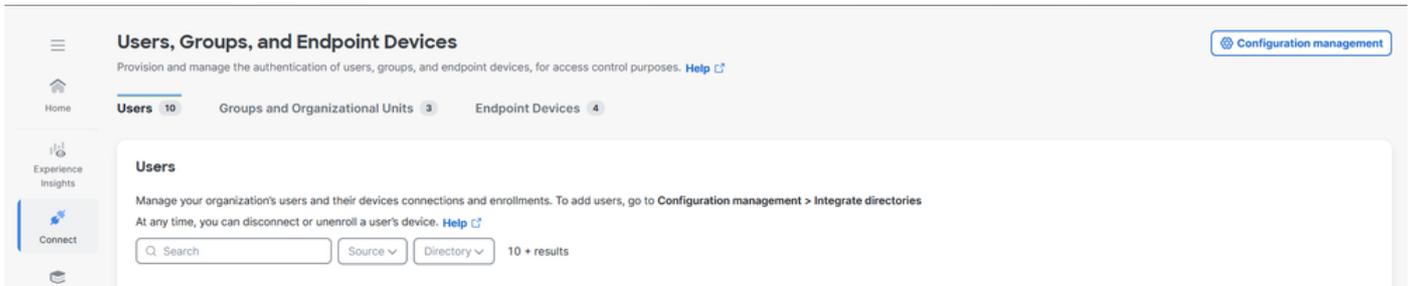
Search 4 results

Name	Device Type	Auth Property	Directory	Associated Rules
ISE.taclab.com	AD Device	ise.taclab.com	Active Directory Profile	0
WIN1.taclab.com	AD Device	Win1.taclab.com	Active Directory Profile	0
WIN2.taclab.com	AD Device	Win2.taclab.com	Active Directory Profile	0
WINDOWS11.taclab.com	AD Device	Windows11.taclab.com	Active Directory Profile	0

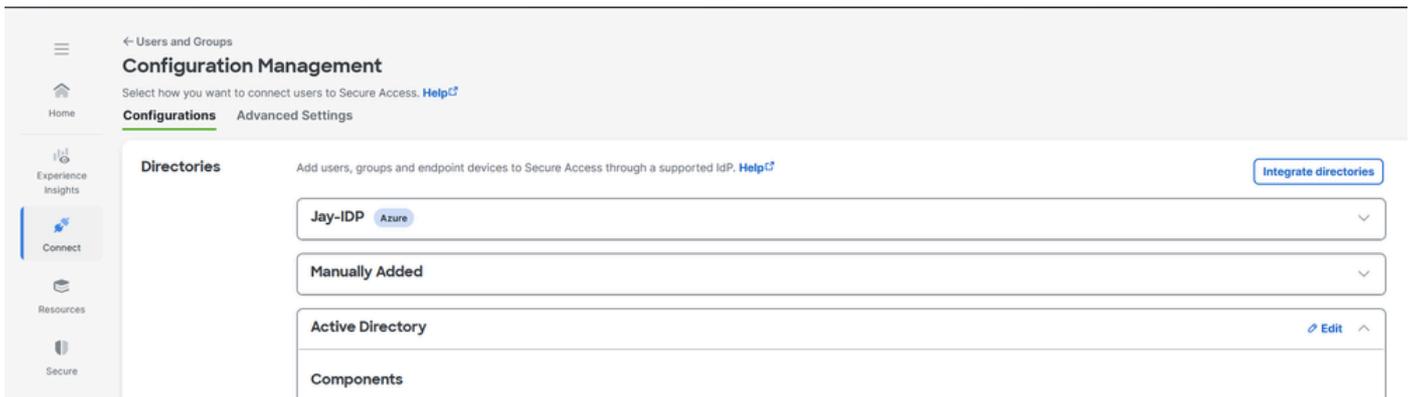
Rows per page 10 < >

手順6: エンドポイントデバイス認証の設定

1. [接続] > [ユーザー、グループ、およびエンドポイントデバイス]に移動します。
2. Configuration managementをクリックします。



3. ConfigurationsでActive Directoryを編集します。



4. エンドポイントデバイスの認証プロパティをホスト名に設定します

Endpoint Devices Authentication

Select the Authentication Property that will be used to authenticate AD endpoint devices when connected via RA-VPN. [Help](#)

Authentication Property

Hostname

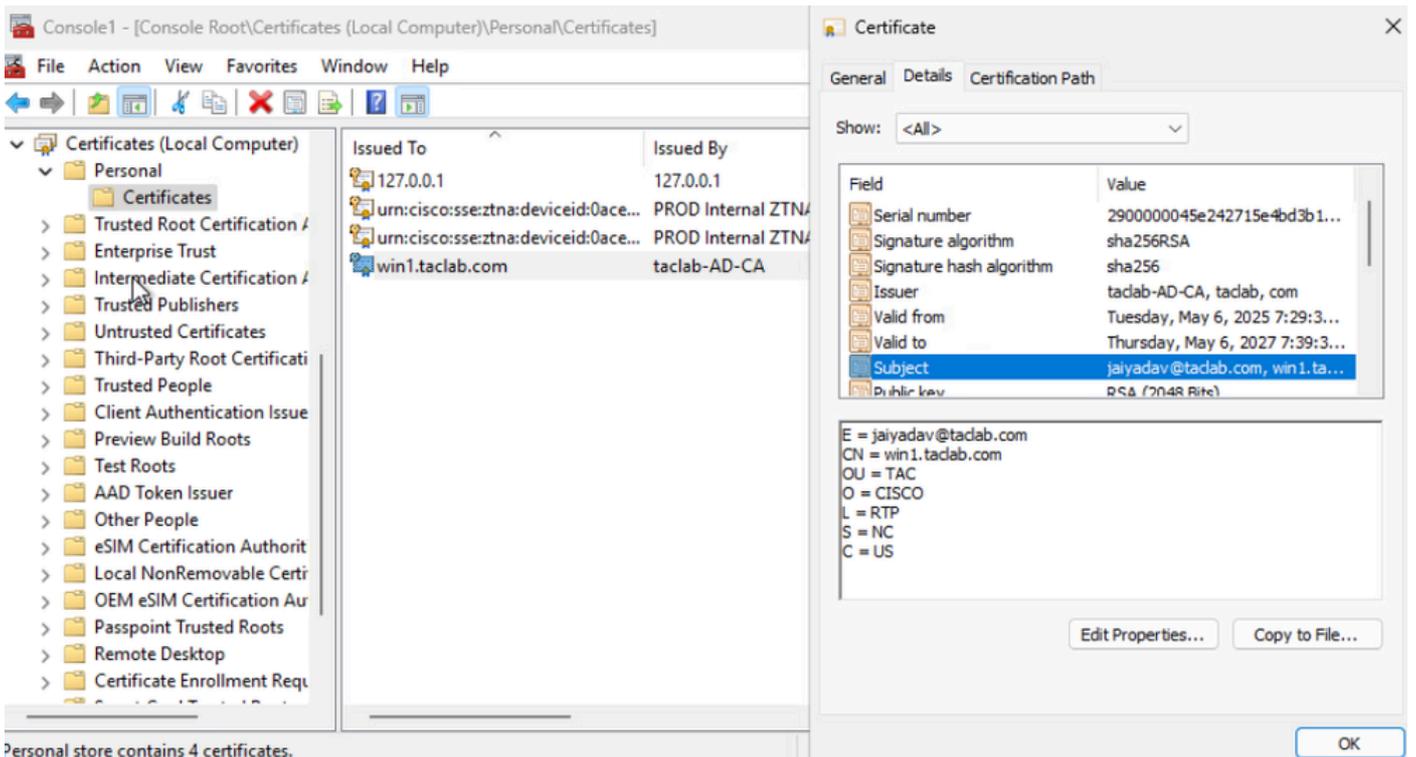
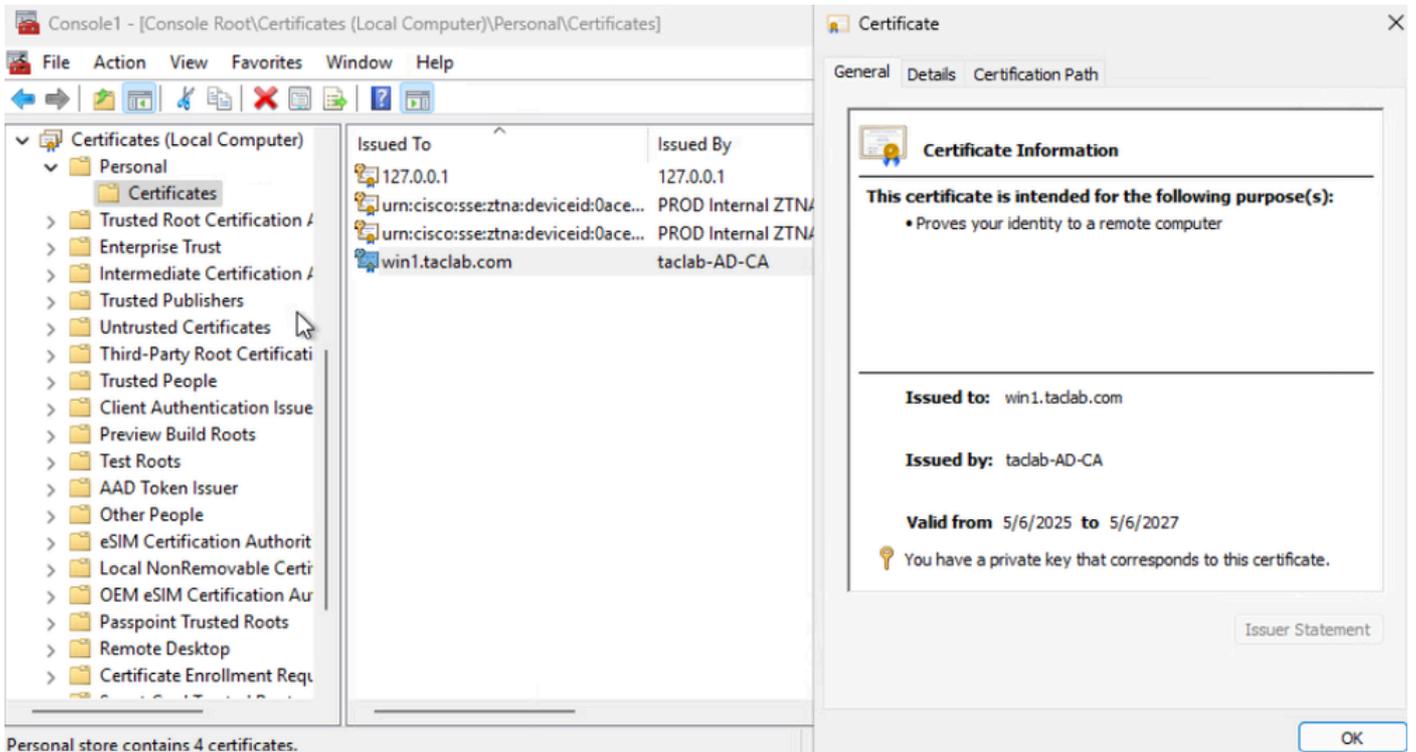
You must re-sync AD identities when you update this Authentication Property.

[Cancel](#) [Delete](#) [Save](#)

5. AD Connectorサービスがインストールされているサーバで、Saveをクリックして再起動します

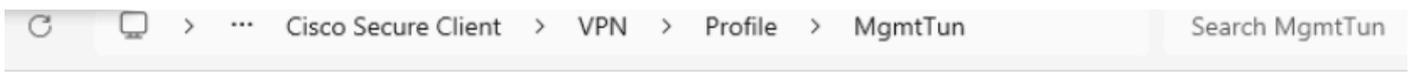
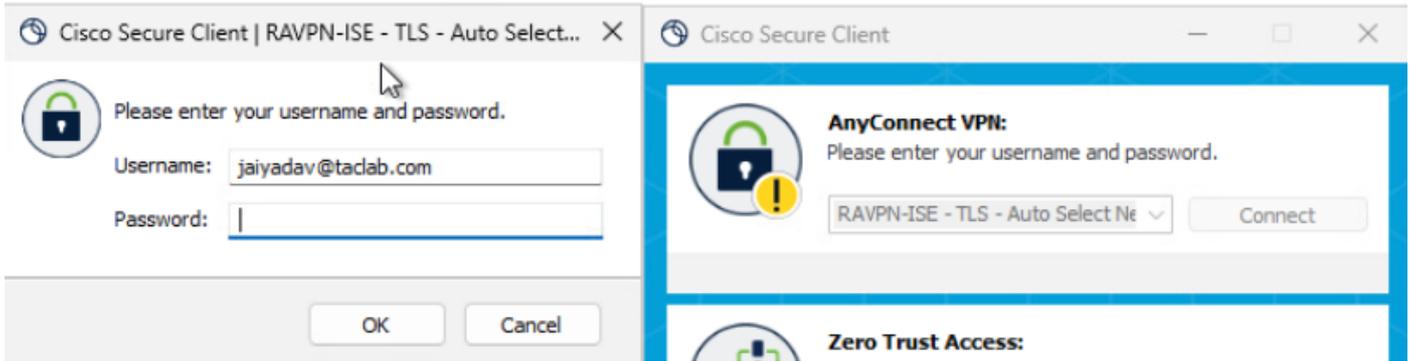
手順7：エンドポイント証明書の生成とインポート

- CSRを生成し、CSRジェネレータまたはOpenSSLツールを開きます。
- CAからエンドポイント証明書を生成する
- .certファイルをPKCS12形式に変換します。
- エンドポイント証明書ストアへのPKCS12証明書のインポート



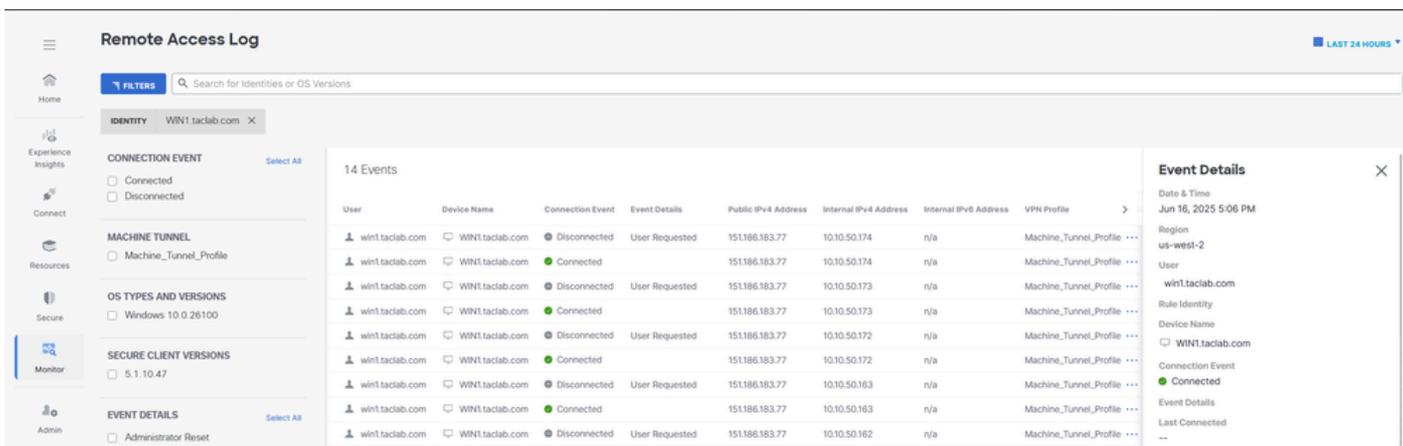
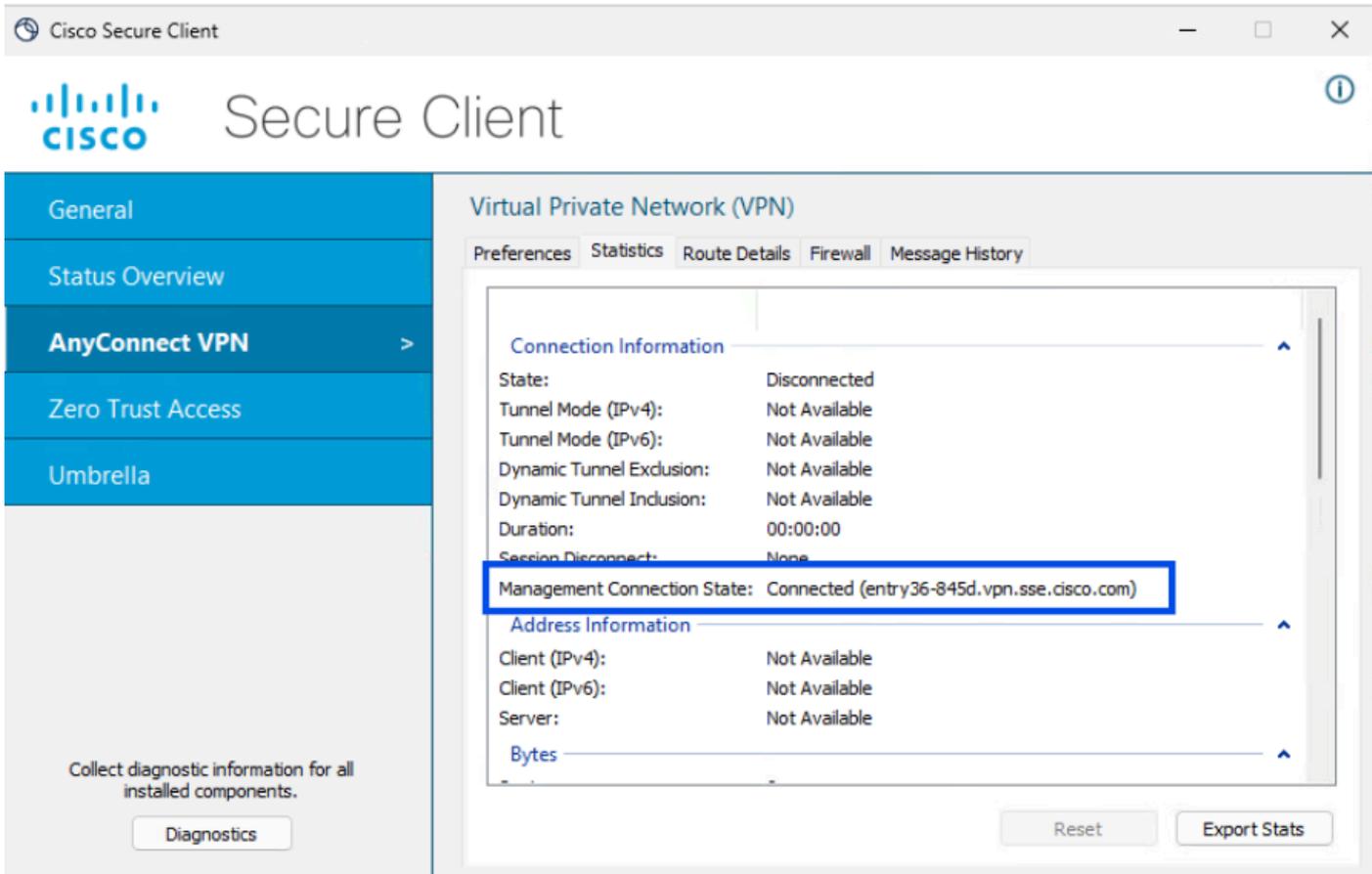
ステップ8 – マシントネルへの接続

a. ユーザトンネル(UTP)に接続すると、マシントネルxmlプロファイルのダウンロードがトリガーされます



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

b. マシントネル接続の確認



方法3：ユーザ証明書を使用してマシントンネルを設定する

この場合、Primary field to authenticateでは、ユーザの電子メールまたはUPNを含む証明書フィールドを選択します。セキュアアクセスでは、マシントンネルIDとして電子メールまたはUPNが使用されます。電子メールまたはUPNの形式は、選択したデバイスIDの形式と一致する必要があります

マシントンネル設定の手順1～4を実行します

ステップ5: Cisco Secure Access(ACS)でユーザをインポートできるようにADコネクタを設定します。

詳細については、「[On-Perm Active Directory Integration](#)」

ステップ6: ユーザ認証の設定

1. [接続] > [ユーザー、グループ、およびエンドポイントデバイス]に移動します。
2. Configuration managementをクリックします。

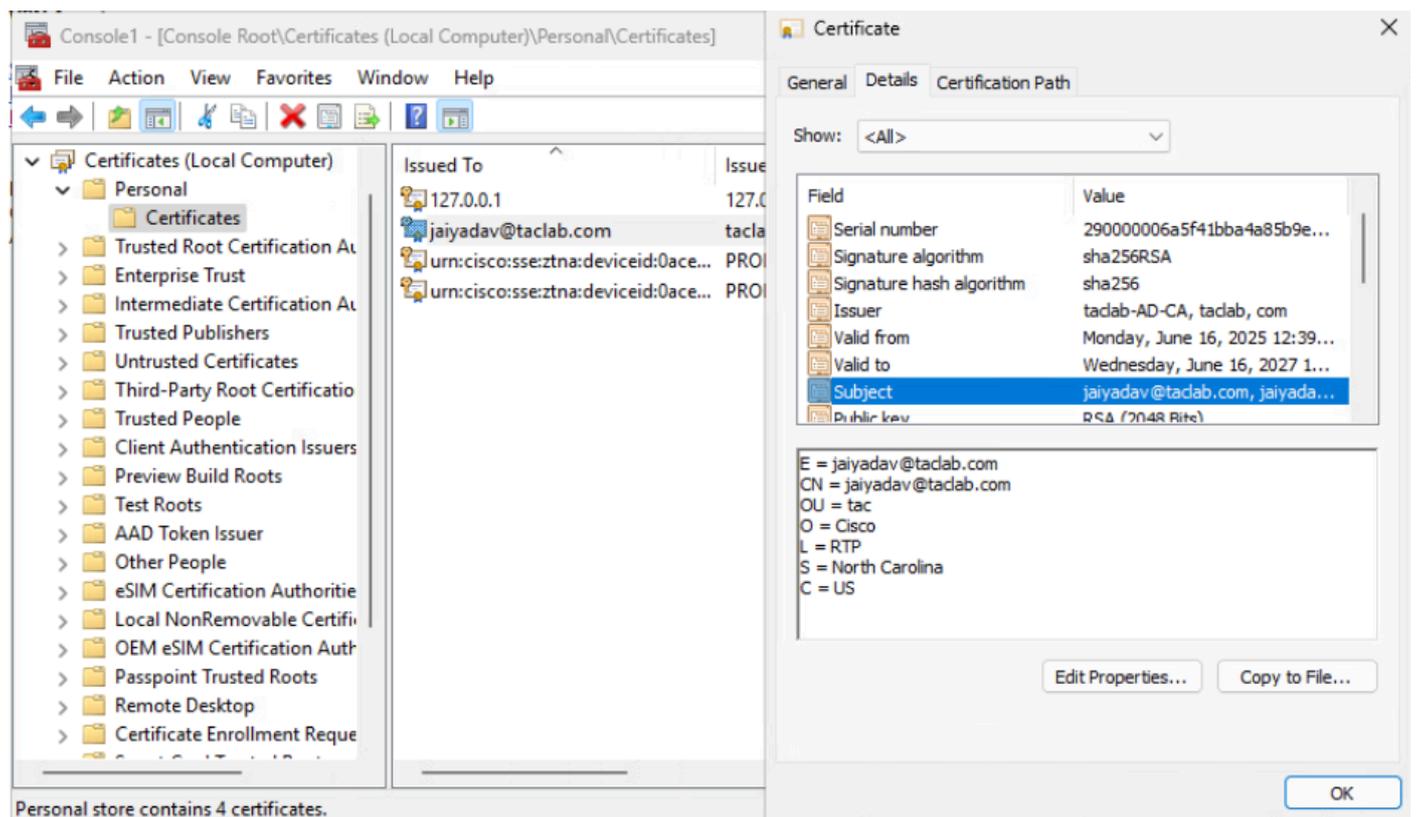
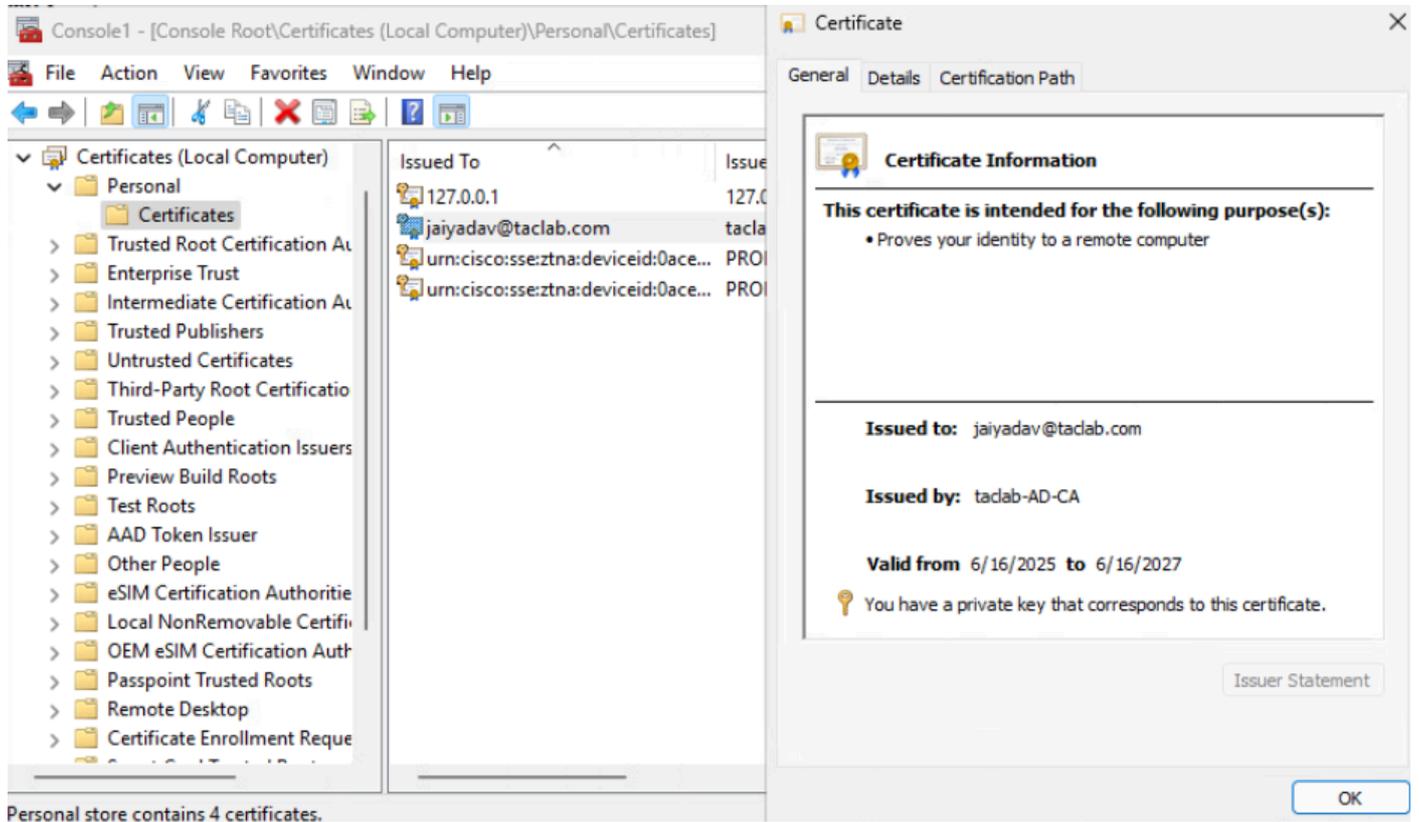
3. ConfigurationsでActive Directoryを編集します。

4. Users Authentication PropertyをEmailに設定します。

5. AD Connectorサービスがインストールされているサーバで、Saveをクリックして再起動します

手順7: エンドポイント証明書の生成とインポート

- CSRを生成し、CSRジェネレーターまたはOpenSSLツールを開きます。
- CAからエンドポイント証明書を生成する
- .certファイルをPKCS12形式に変換します。
- エンドポイント証明書ストアへのPKCS12証明書のインポート

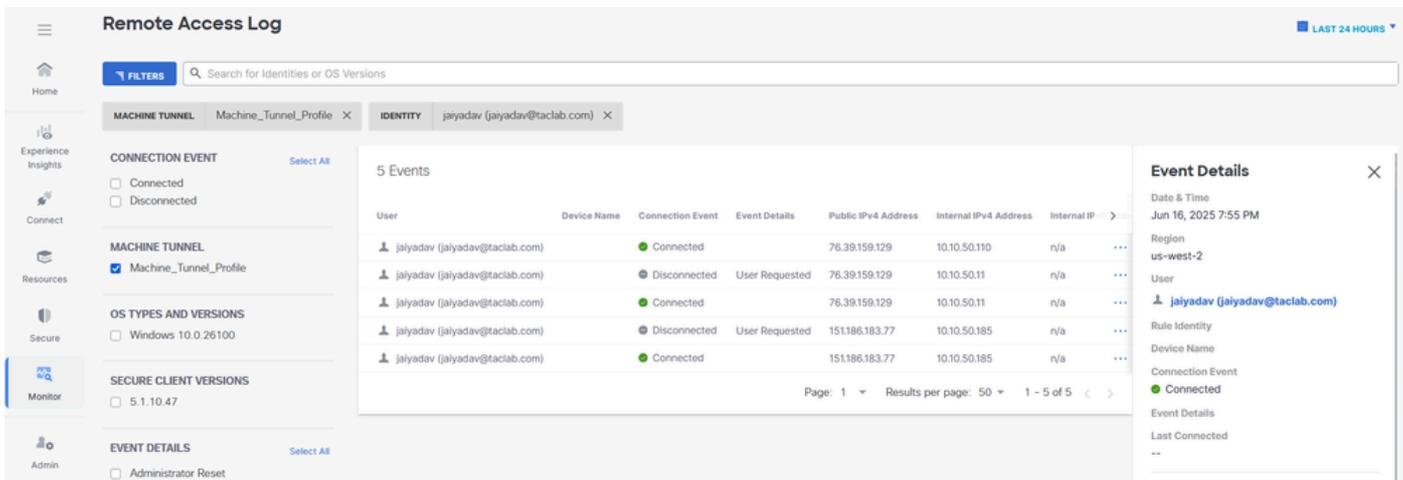
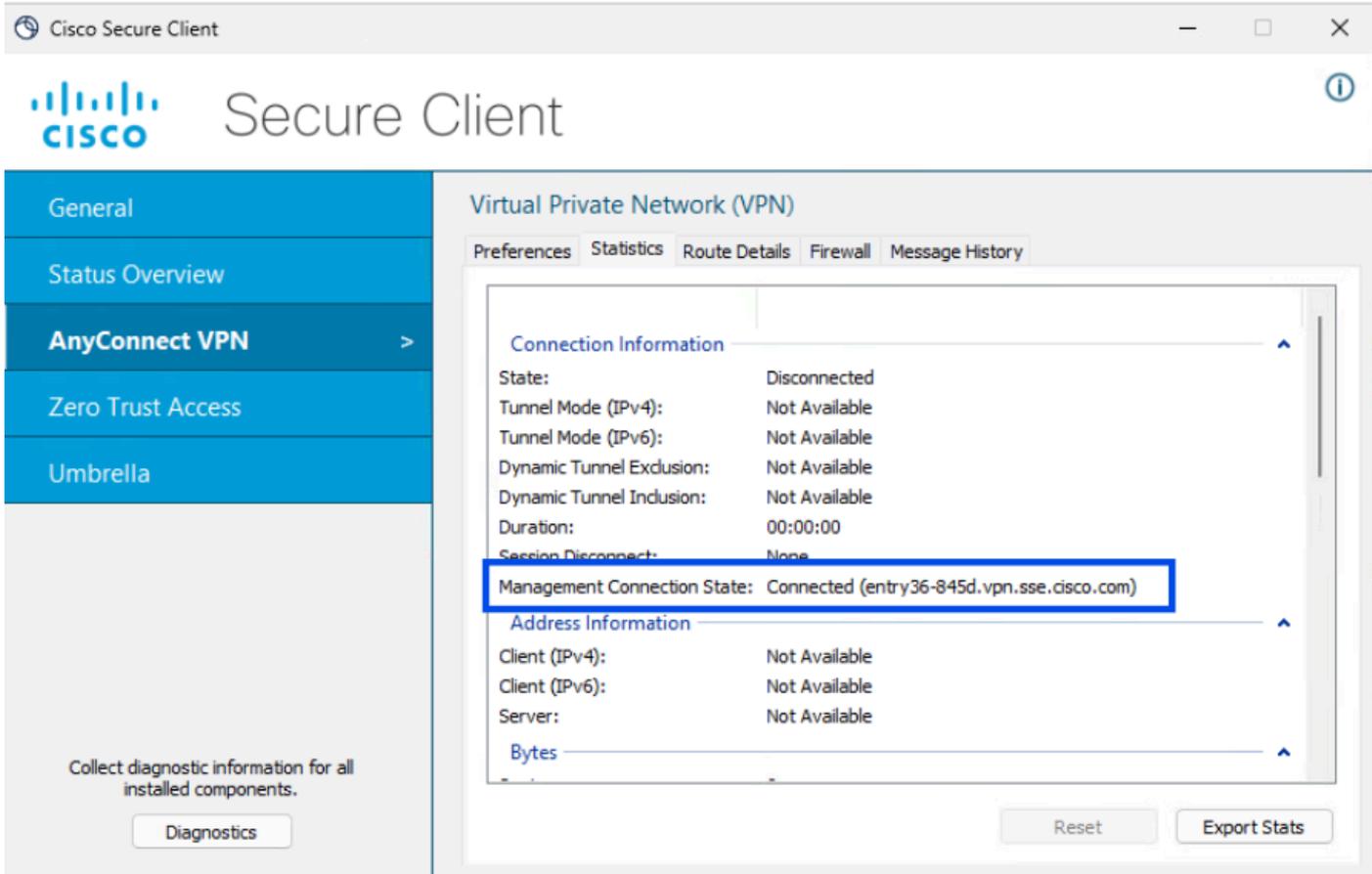


ステップ8 – マシントネルへの接続

a. ユーザトンネル(UTP)に接続すると、マシントネルxmlプロファイルのダウンロードがトリガーされます

The screenshot shows the Cisco Secure Client interface. On the left, a dialog box prompts for a username and password. The username is 'jaiyadav@taclab.com'. On the right, the main client window shows the 'AnyConnect VPN' section with a dropdown menu set to 'RAVPN-ISE - TLS - Auto Select Ne' and a 'Connect' button. Below this, the 'Zero Trust Access' section is partially visible. At the bottom, a file explorer window shows the 'Cisco Secure Client > VPN > Profile > MgmtTun' directory. It contains two files: 'AnyConnectProfile.xsd' (100 KB, XSD File, modified 4/8/2025 12:13 PM) and 'VpnMgmtTunProfile' (4 KB, XML File, modified 6/16/2025 9:11 AM). An inset window shows the client after connection, displaying 'AnyConnect VPN: Connected to RAVPN-ISE - TLS - Auto Select Nearest Location.' with a 'Disconnect' button and a timer showing '00:00:29 (3 Hours 59 Minutes Remaining)'. The IP address 'IPv4' is also shown.

b. マシントネル接続の確認



トラブルシューティング

DARTバンドルを抽出し、AnyConnectVPNログを開いてエラーメッセージを分析する

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。