Entra IDを使用したRA VPNaaSのCisco Secure Accessの設定

内容

はじめに

このドキュメントでは、Cisco Secure AccessでRA VPNを設定してEntra IDに対して認証を行う方法について段階的に説明します。

前提条件

次の項目に関する知識があることが推奨されます。

- Azure/Entra IDを使用する知識。
- シスコセキュアアクセスに関する知識

要件

次の手順に進む前に、次の要件を満たす必要があります。

- Cisco Secure Access DashboardにFull Adminとしてアクセスします。
- 管理者としてAzureにアクセスします。
- Cisco Secure Accessへの[ユーザプロビジョニング](#)はすでに完了しています。

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ダッシュボード：
- Microsoft Azureポータル。

- Cisco Secure Client AnyConnect VPNバージョン5.1.8.105

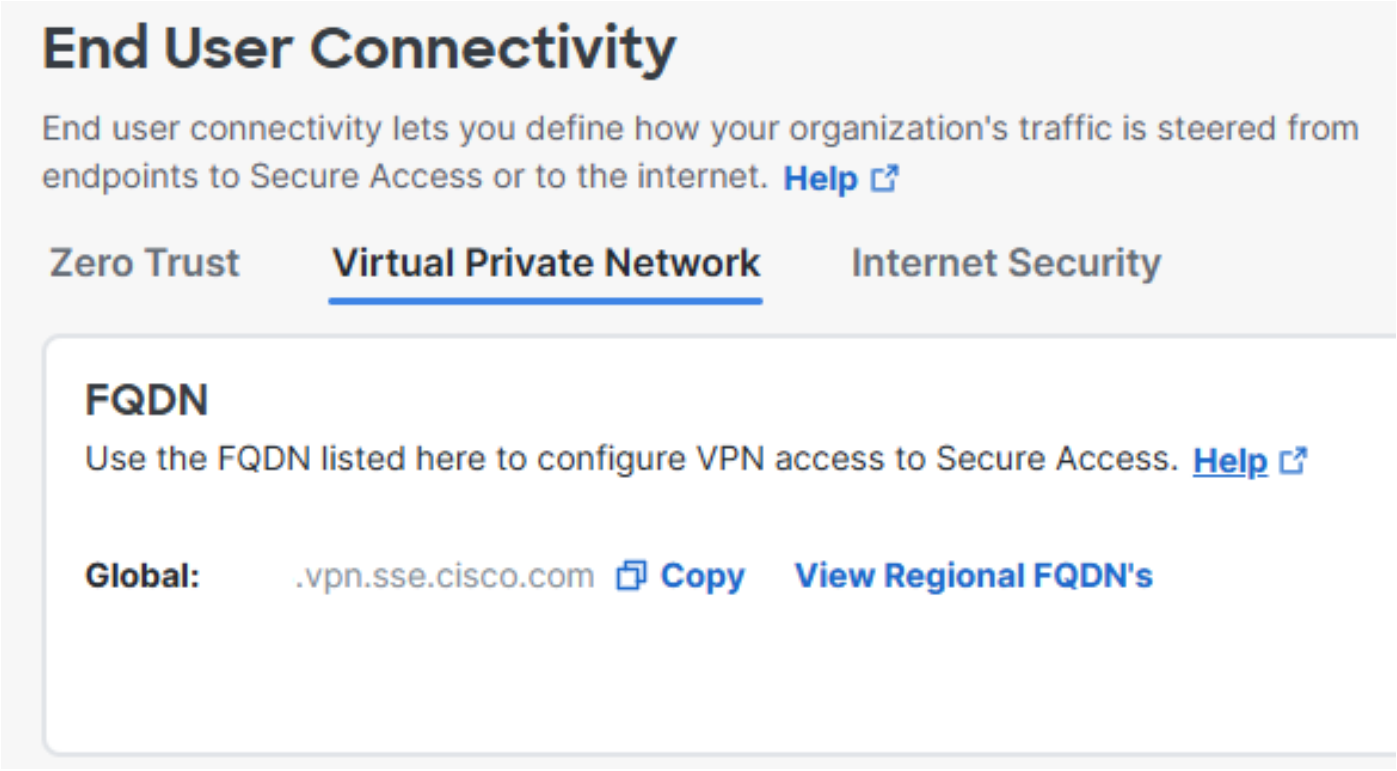
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

Azure構成

1. Cisco Secure Accessダッシュボードにログインし、VPNグローバルFQDNをコピーします。このFQDNは、Azureエンタープライズアプリケーションの構成で使用されています。

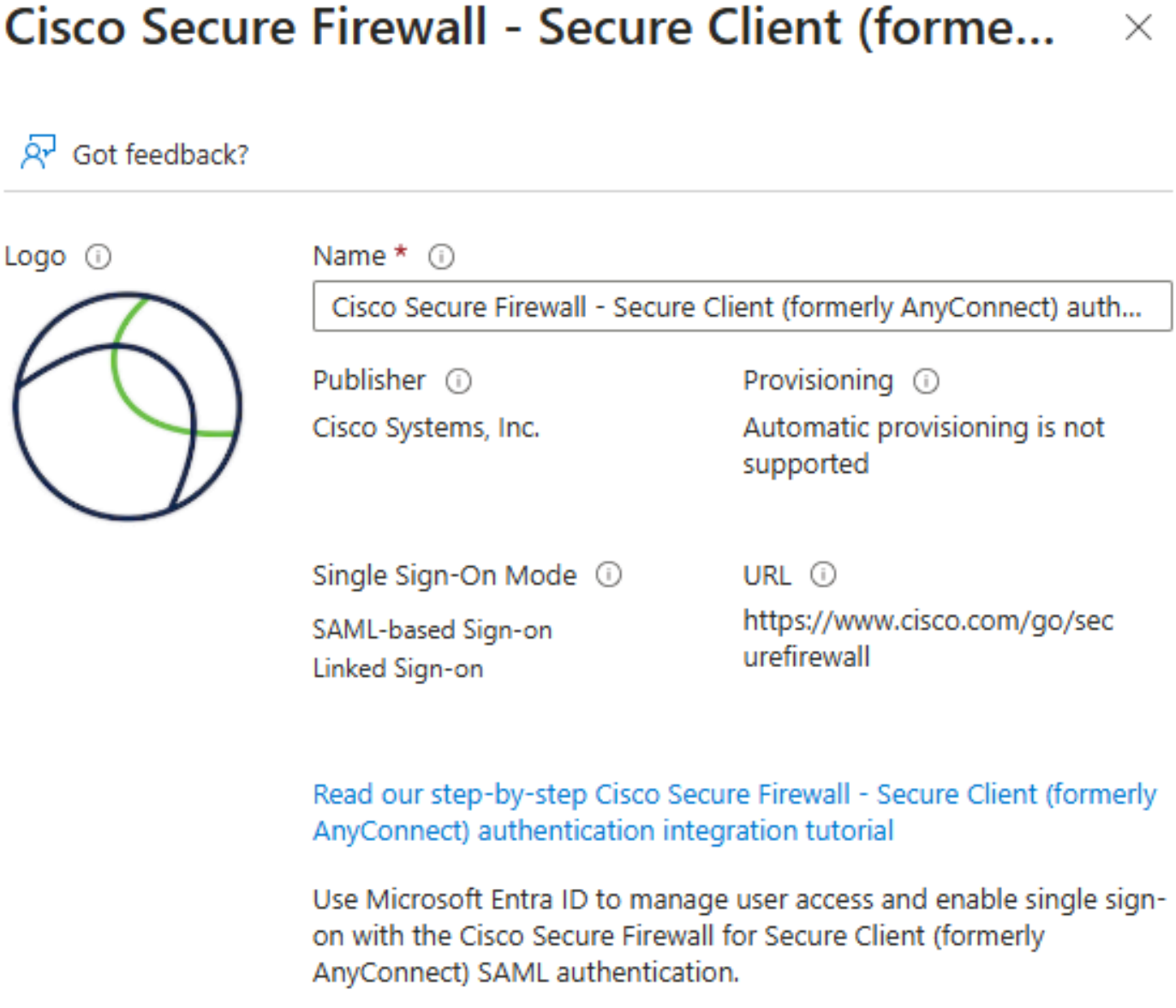
Connect > End User Connectivity > Virtual Private Network > FQDN > Global



VPNグローバルFQDN

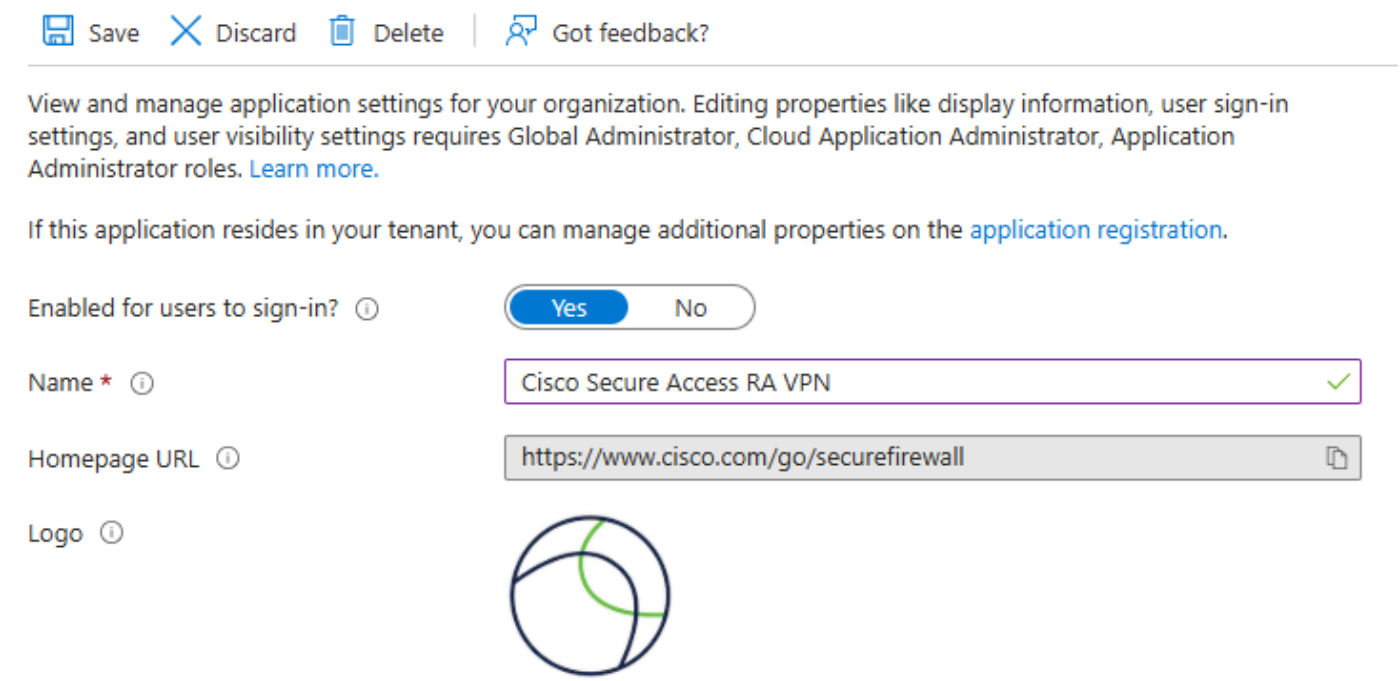
2. Azureにログインし、RA VPN認証用のエンタープライズアプリケーションを作成します。「Cisco Secure Firewall - Secure Client (formerly AnyConnect) authentication」という名前の定義済みアプリケーションを使用できます。

Home > Enterprise Applications > New Application > Cisco Secure Firewall - Secure Client（以前のAnyConnect）authentication > Create



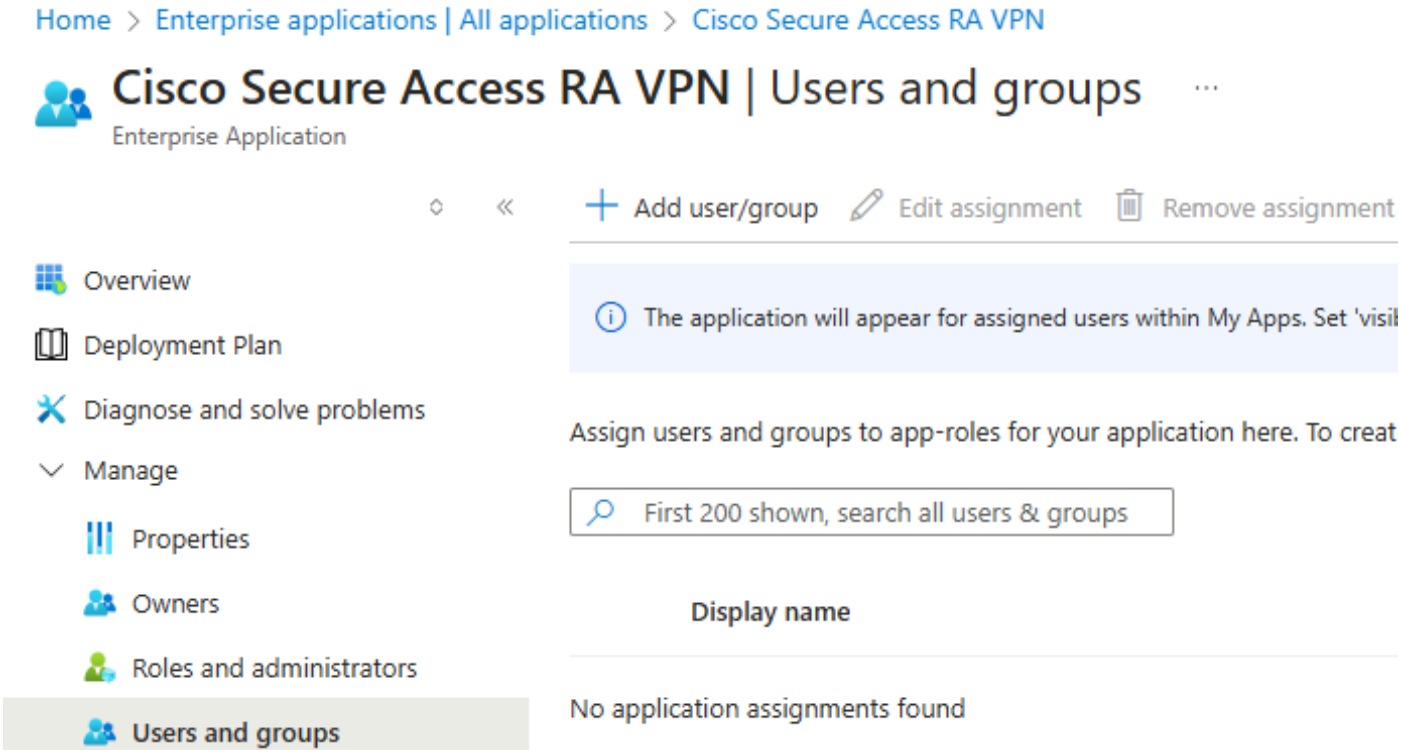
Azureでアプリを作成

3. アプリケーションの名前を変更します。
   プロパティ>名前



アプリケーション名の変更

4. エンタープライズアプリケーション内で、AnyConnect VPNを使用して認証を許可するユーザを割り当てます。
ユーザとグループの割り当て> +ユーザ/グループの追加>割り当て

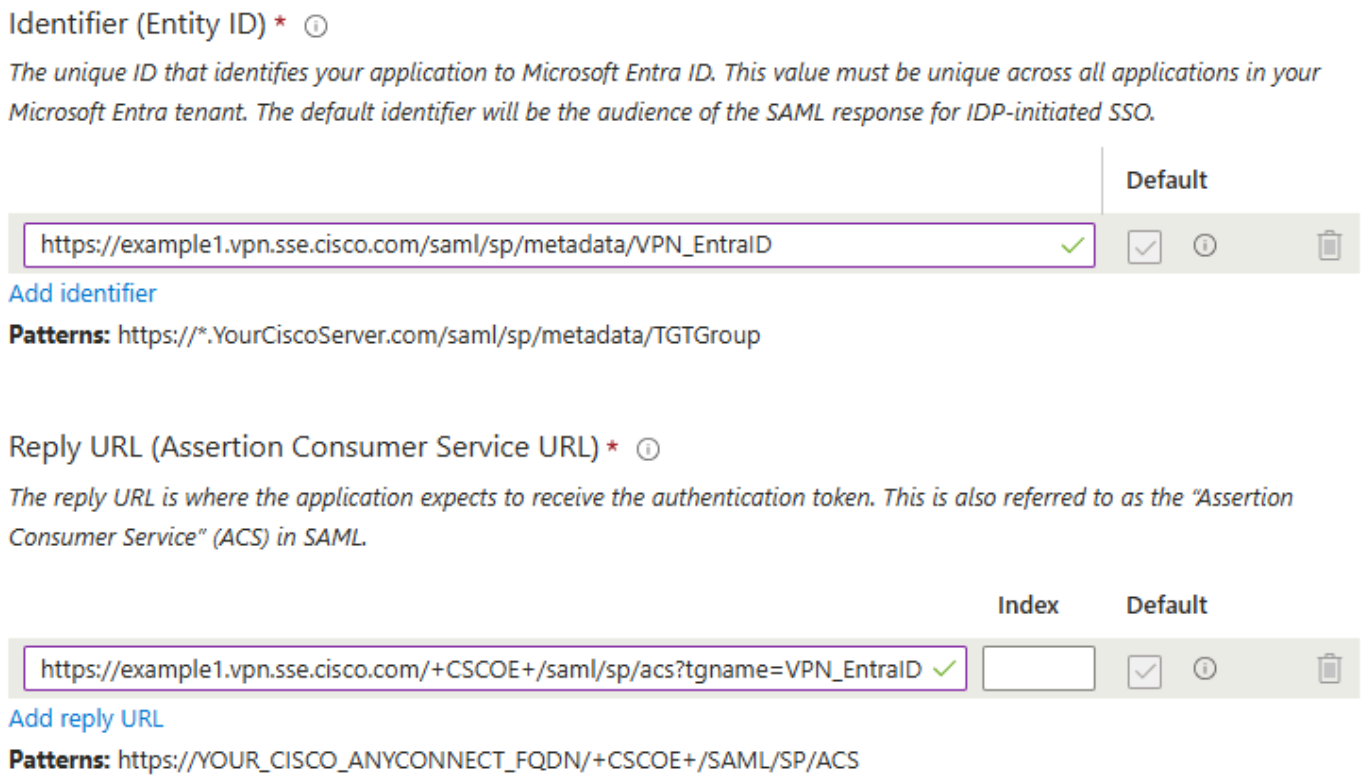


割り当てられたユーザー/グループ

5. 「シングル・サインオン」をクリックし、SAMLパラメータを構成します。ここでは、ステップ1でコピーしたFQDNと、ステップ2の「Cisco Secure Accessの設定」で設定したVPNプロファイル名を使用します。

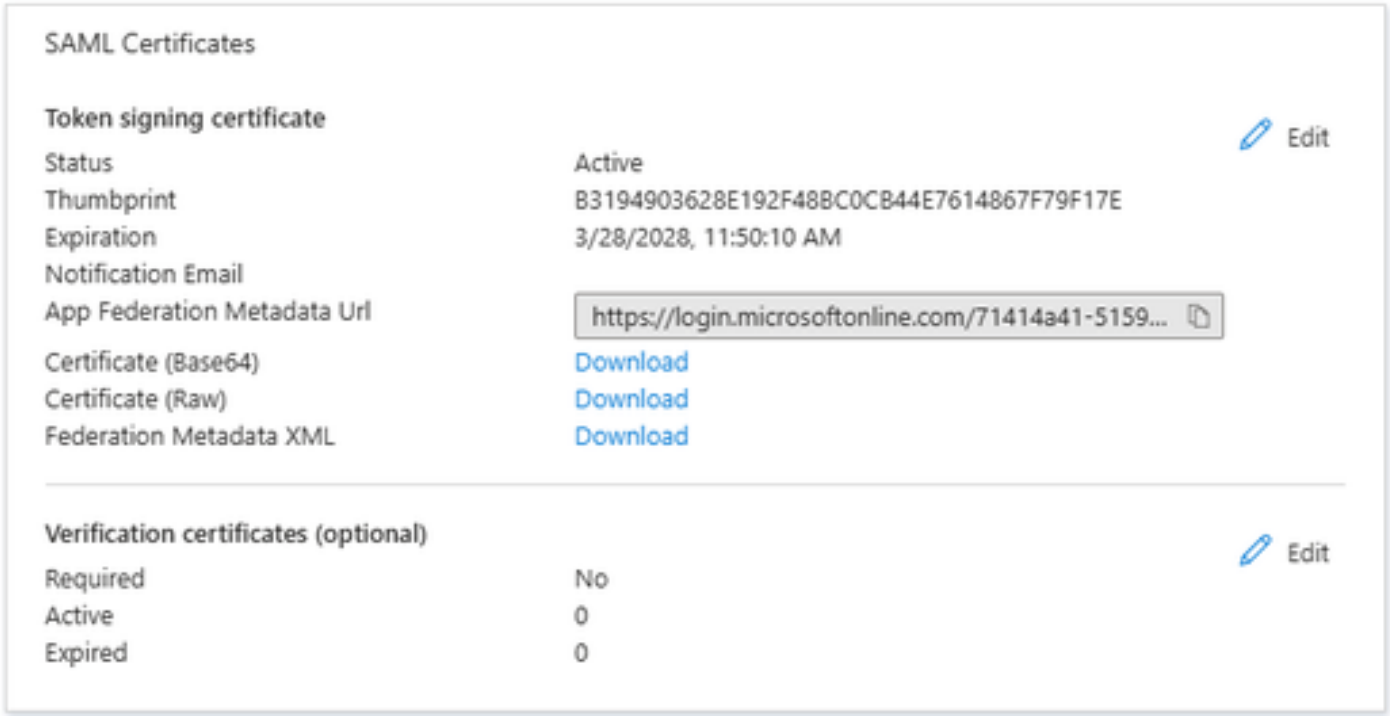
たとえば、VPNグローバルFQDNがexample1.vpn.sse.cisco.comで、Cisco Secure Access VPNプロファイル名がVPN_EntraIDの場合、（エンティティID）と応答URL（アサーションコンシューマサービスURL）の値は次のようになります。

識別子（エンティティID）:https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID
返信URL（アサーションコンシューマサービス
URL）:https://example1.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=VPN_EntraID



AzureのSAMLパラメーター

6. フェデレーションメタデータXMLをダウンロードします。



Cisco Secure Access設定

1. Cisco Secure Accessダッシュボードにログインし、IPプールを追加します。

   Connect > End User Connectivity > Virtual Private Network > Add IP Pool

Region:RA VPNを展開するリージョンを選択します。
表示名：VPN IPプールの名前。
DNSサーバ：ユーザが接続後にDNS解決に使用するDNSサーバを作成するか、割り当てます。
システムIPプール：Radius認証などの機能のためにセキュアアクセスによって使用されます。認証要求はこの範囲内のIPから送信されます。
IP Pool:新しいIP Poolを追加し、RA VPNに接続した後にユーザが取得するIPを指定します。

Setup VPN profiles

No VPN profiles added. To configure VPN profiles, you must first setup IP pools and then add profiles that map to users. Help

Add IP Pool

VPNプロファイルの追加

Parameters

Edit this IP pool's parameters including its mapped region, DNS servers, and IP addresses

Region

Canada (Central)

Display name

RA VPN

DNS Server

DNS (208.67.222.222)

+ Add

DDNS Servers updates

System IP Pool

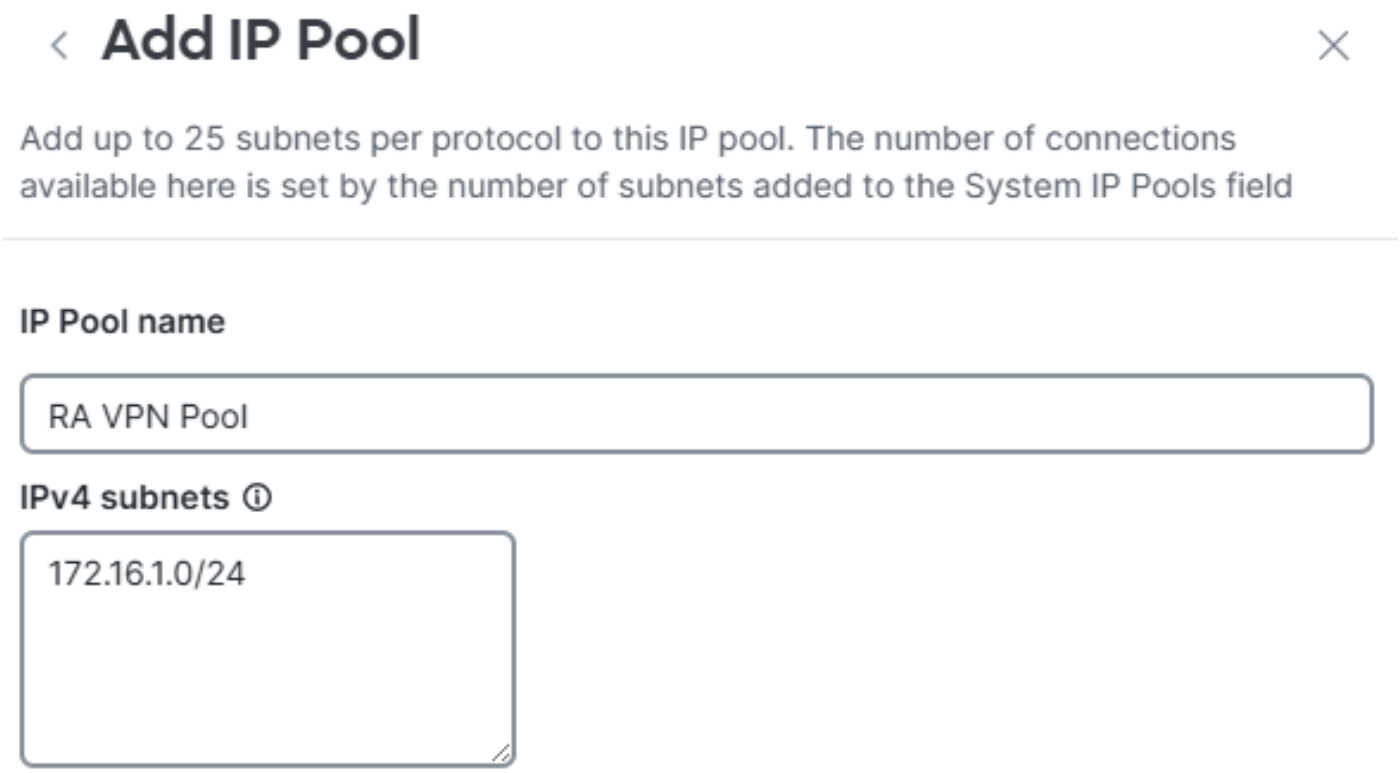
172.16.2.0/24

IP Pools

Add the IP pools this region will use. You can add a maximum of 25 IPV4 and 25 IPV6 subnets per IP pool. Help

+ Add

IPプールの設定 – パート1

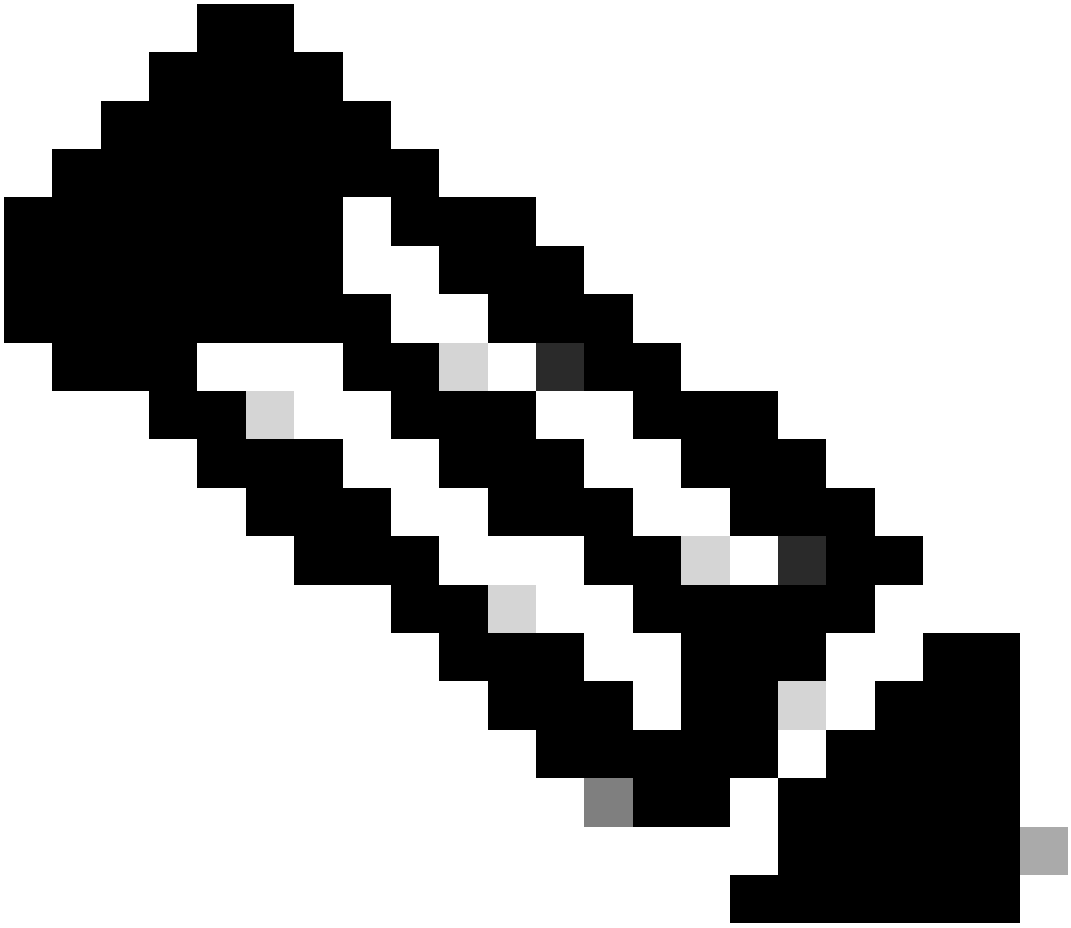


IPプールの設定 – パート2

2. VPNプロファイルを追加します。

Connect > End User Connectivity > Virtual Private Network > + VPN Profile

一般設定

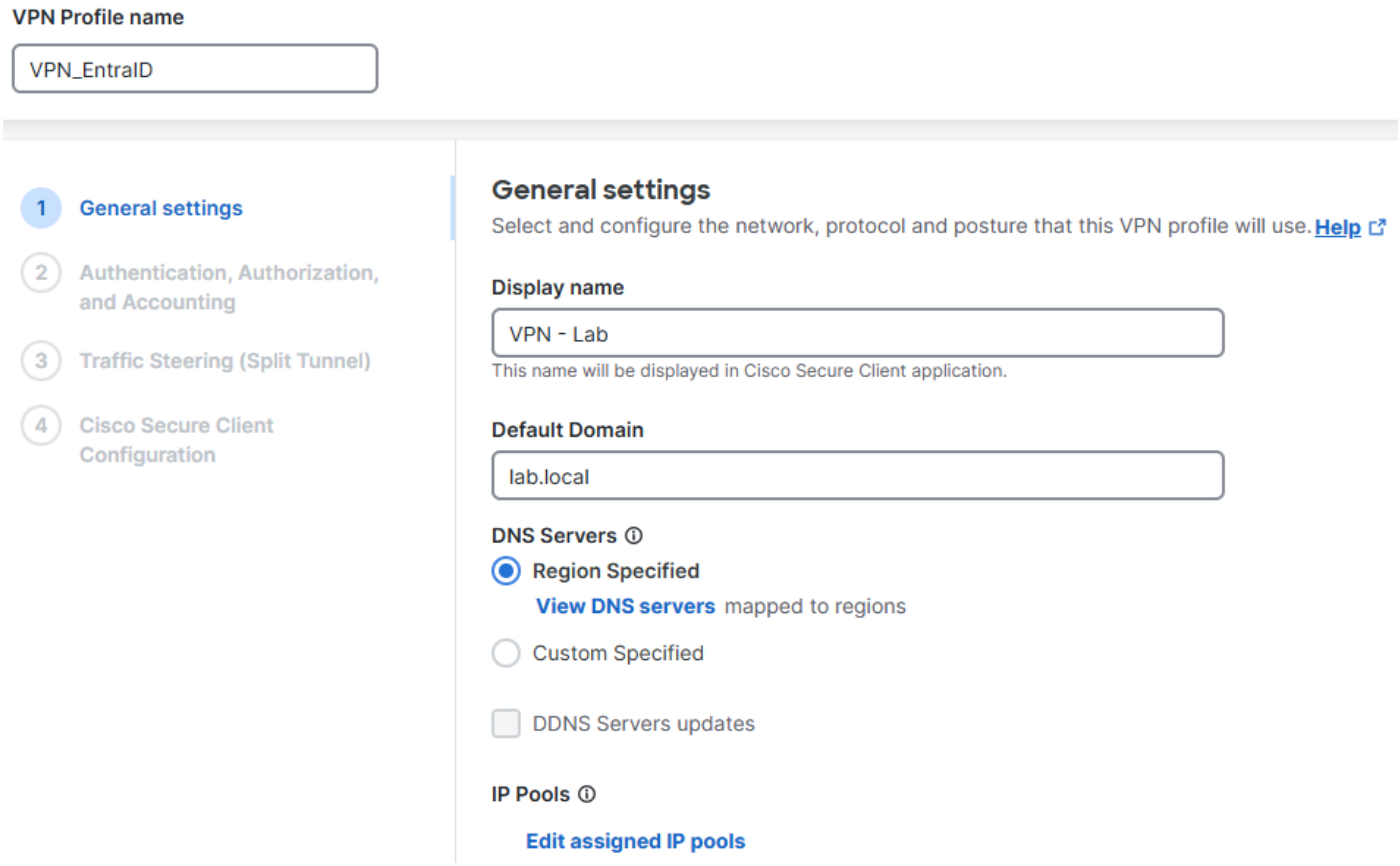


注:VPNプロファイルの名前は、ステップ5の「Configuration Azure」で設定した名前と一致している必要があります。このコンフィギュレーションガイドではVPN_EntraIDを使用しているため、Cisco Secure AccessでもVPNプロファイル名として同じ名前を設定します。

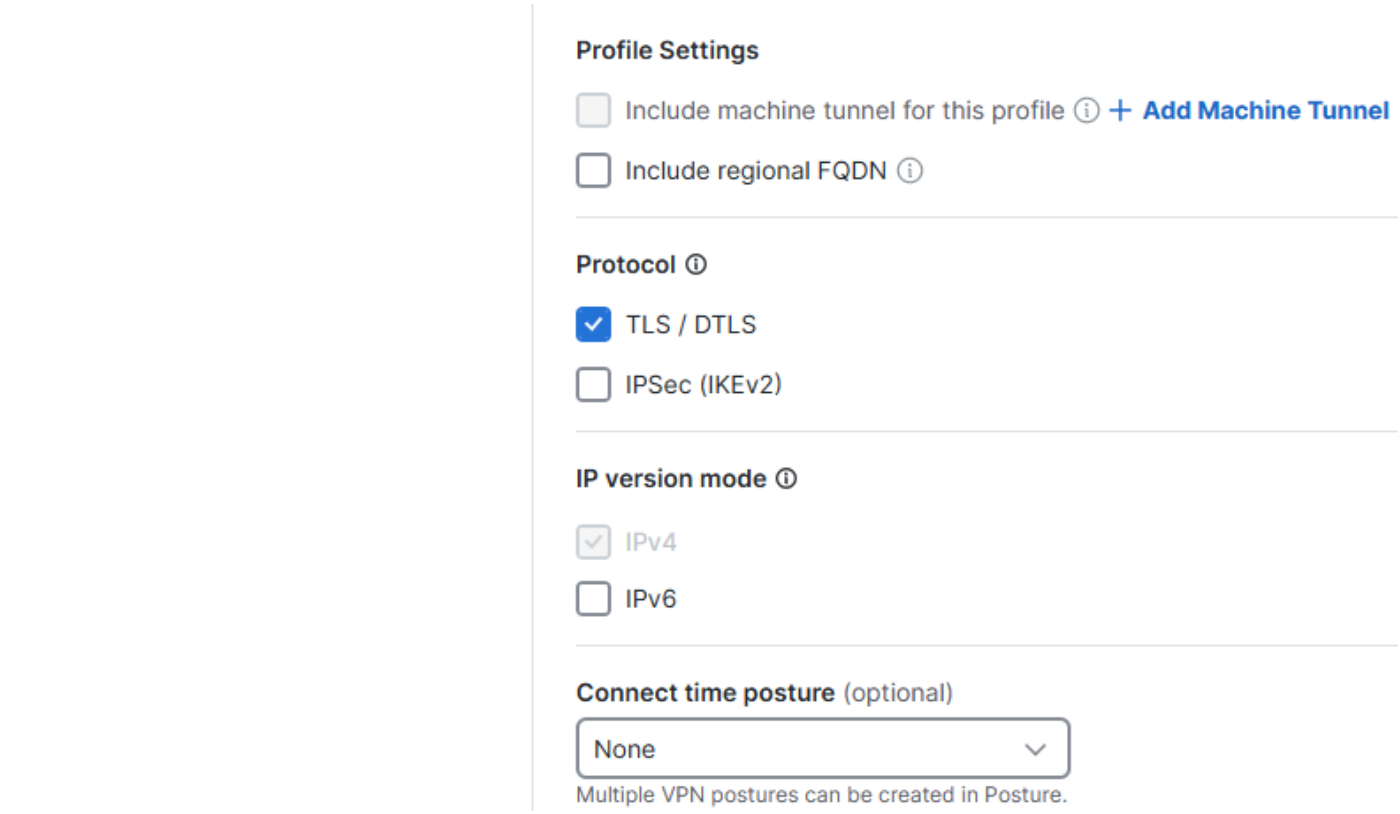
VPNプロファイル名：このVPNプロファイルの名前。ダッシュボードにのみ表示されます。

表示名：このRA VPNプロファイルに接続する際にエンドユーザに表示される「セキュアクライアント – Anyconnect」ドロップダウンメニューの名前。
デフォルトドメイン：ドメインユーザは、VPNに接続されると取得されます。
DNSサーバ：VPNユーザがVPNに接続すると取得されるDNSサーバ。
　Region Specified:VPN IPプールに関連付けられたDNSサーバを使用します。
　カスタム指定：必要なDNSを手動で割り当てることができます。
IPプール：ユーザは、VPNに接続されると割り当てられます。
プロファイル設定：このVPNプロファイルをマシントンネルに含めるか、または地域FQDNを含めて、エンドユーザが接続先の地域を選択するようにします（IPプールが展開されます）。
プロトコル：VPNユーザがトラフィックのトンネリングに使用するプロトコルを選択します。

Connect time posture（オプション）:必要に応じて、接続時にVPN Postureを実行します。詳細については、こちらを参照してください。



VPNプロファイルの設定 – パート1



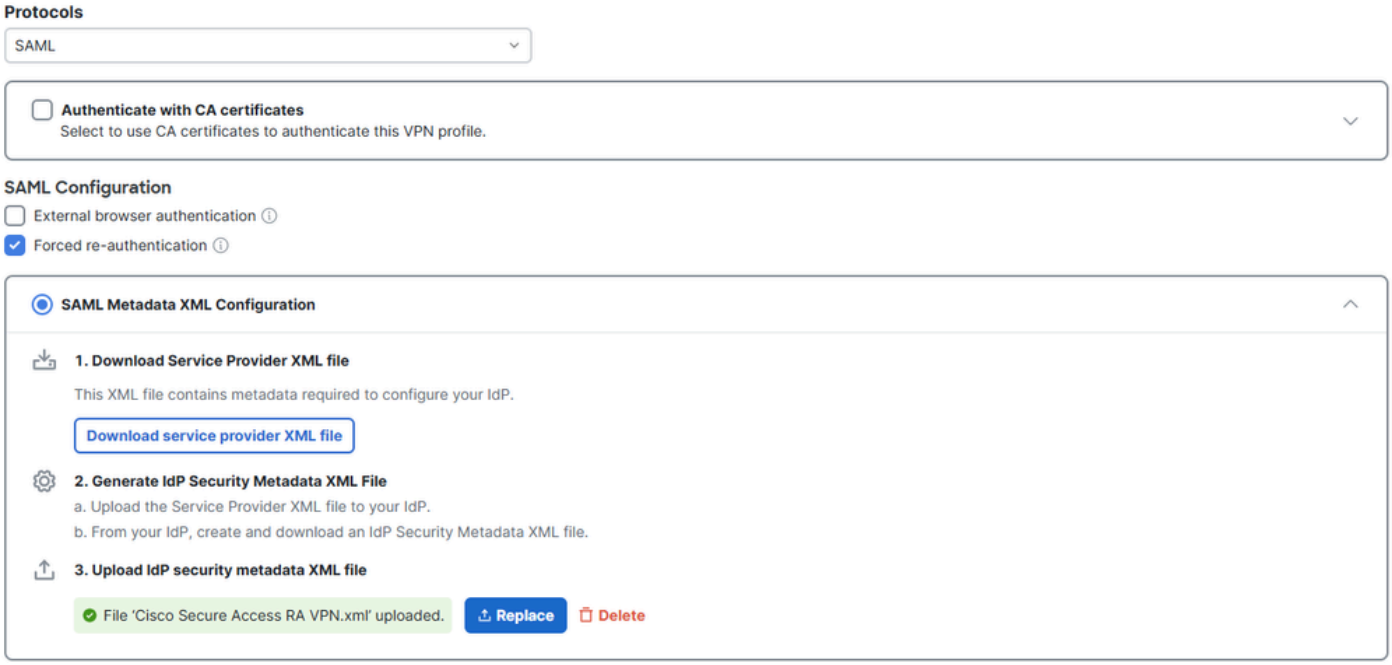
VPNプロファイルの設定 – パート2

認証、許可、およびアカウンティング

プロトコル：SAMLを選択します。

CA証明書による認証:SSL証明書を使用して認証し、IdP SAMLプロバイダーに対して認可する場合。
Force re-authentication:VPN接続が確立されるたびに、再認証を強制します。強制再認証は、セッションタイムアウトに基づいています。これは、SAML IdP設定の対象となる可能性があります（この場合はAzure）。

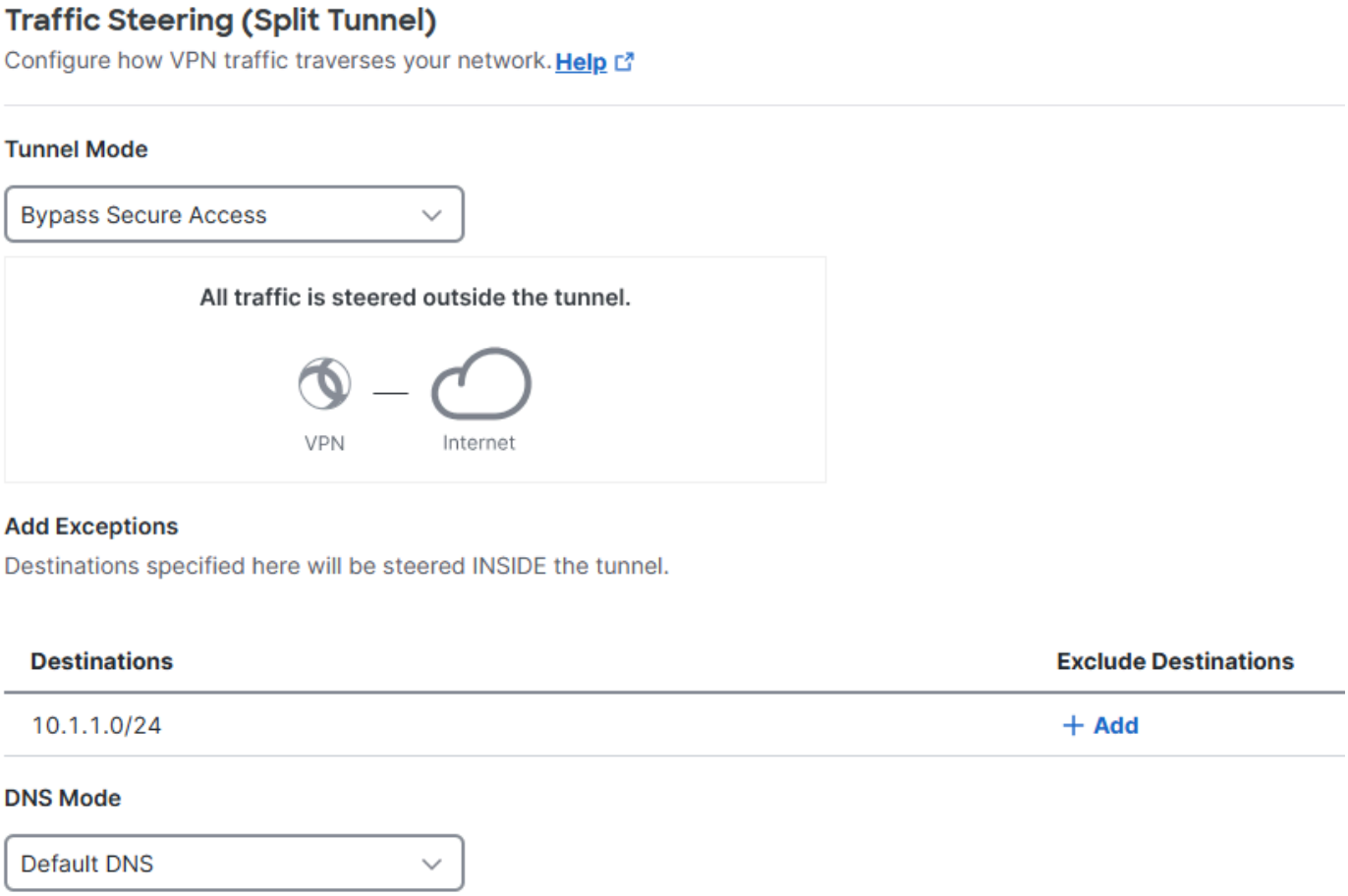
手順6の「Azureの構成」でダウンロードしたXMLファイルのフェデレーションメタデータXMLファイルをアップロードします。



SAML構成

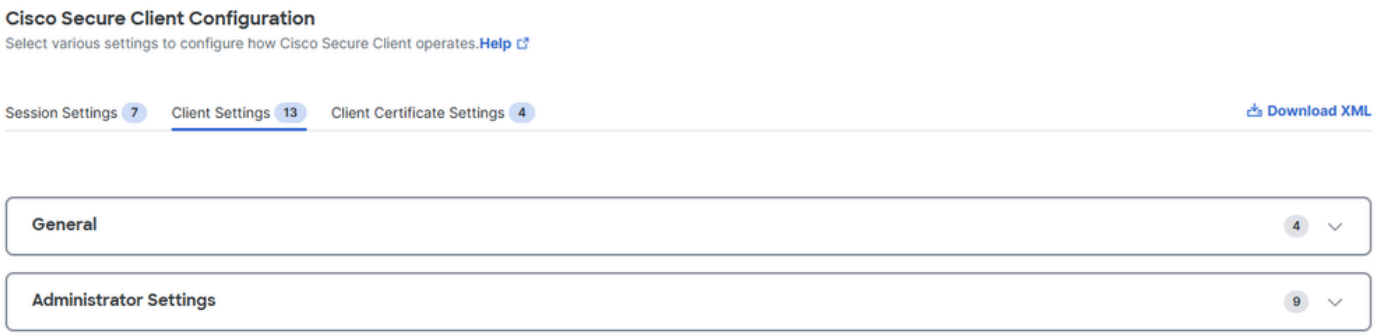
トラフィックステアリング（スプリットトンネル）

Tunnel Mode（トンネル モード）：
　セキュアアクセスへの接続：すべてのトラフィックはトンネル(Tunnel All)経由で送信されます。
　Bypass Secure Access: Exceptionsセクションで定義された特定のトラフィックのみがトンネル化されます（スプリットトンネル）。
DNSモード：
　デフォルトDNS：すべてのDNSクエリは、VPNプロファイルによって定義されたDNSサーバを経由します。否定応答の場合、DNSクエリは、物理アダプタで設定されているDNSサーバにも送信できます。
　Tunnel All DNS：すべてのDNSクエリをVPN経由でトンネリングします。
　スプリットDNS：以下で指定されたドメインに応じて、特定のDNSクエリのみがVPNプロファイルを通過します。



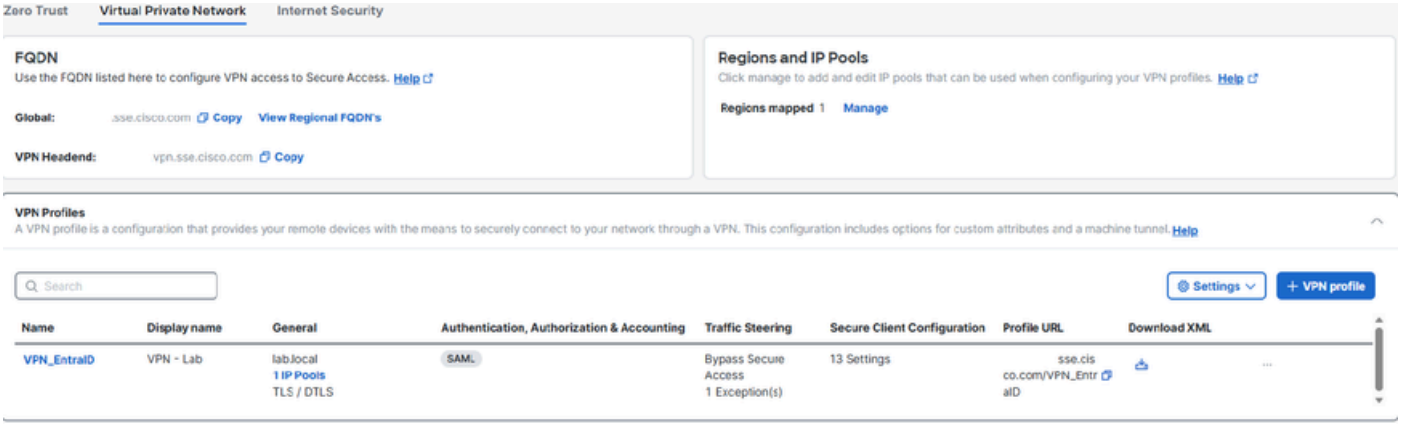
トラフィックステアリング設定

Cisco Secure Clientの設定
このガイドでは、これらの詳細設定は設定しません。ここでは、TND、Always-On、証明書照合、ローカルLanアクセスなどの高度な機能を設定できます。 設定をここに保存します。



高度な設定

3. VPNプロファイルは次のようになります。エンドユーザ(「C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile」の下)にxmlプロファイルをダウンロードして事前展開し、VPNの使用を開始するか、Cisco Secure Client - AnyConnect VPN UIで入力するプロファイルURLをエンドユーザに提供します。



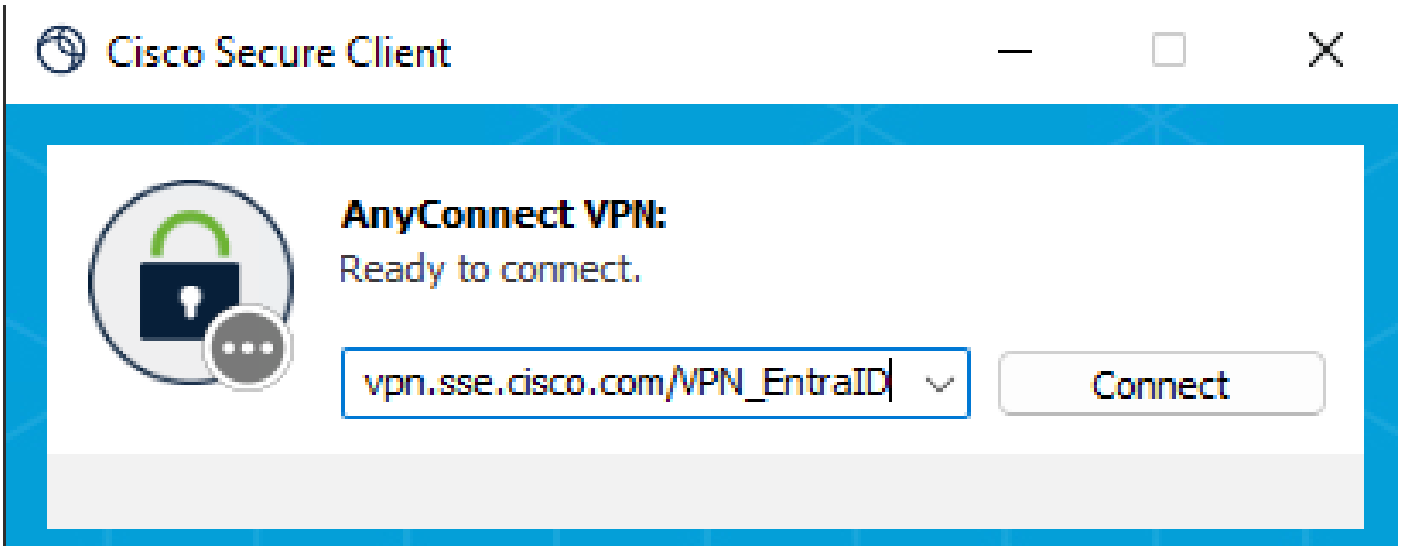
グローバルFQDNとプロファイルURL

確認

この時点で、RA VPN設定はテスト可能な状態になっている必要があります。
ユーザが初めて接続する際には、プロファイルURLアドレスをユーザに付与するか、PCの「C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile」の下にxmlプロファイルを事前展開してからVPNサービスを再起動し、ドロップダウンメニューにこのVPNプロファイルに接続するためのオプションが表示される必要があることに注意してください。

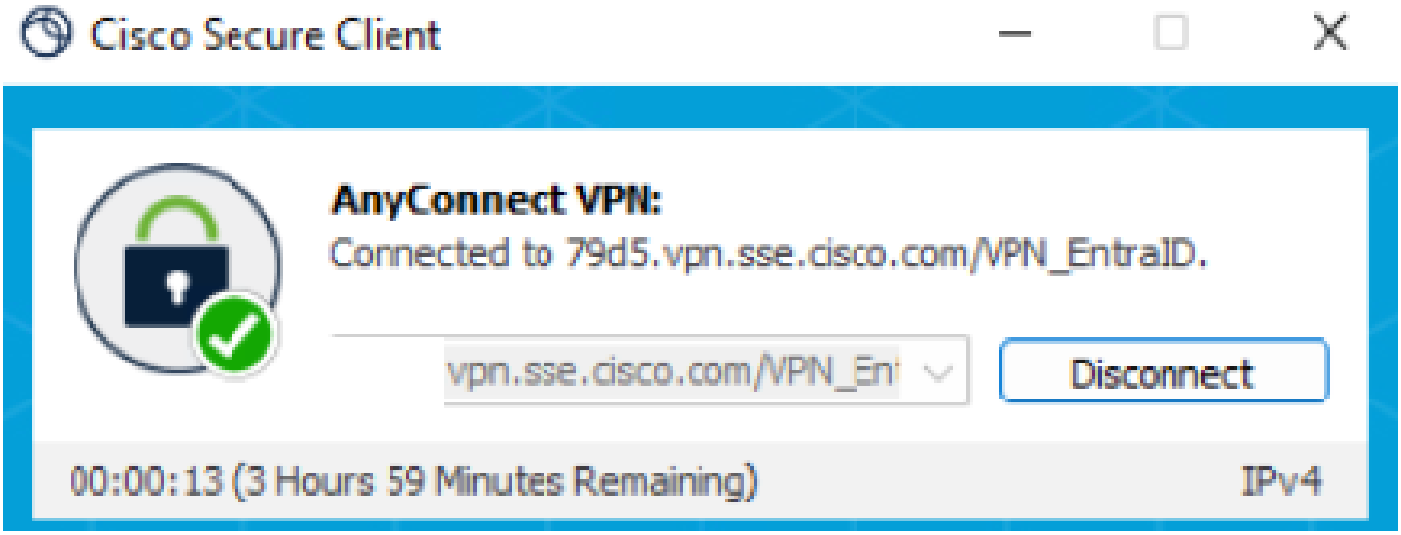
この例では、最初の接続試行でプロファイルURLアドレスをユーザに割り当てます。

最初の接続の前：



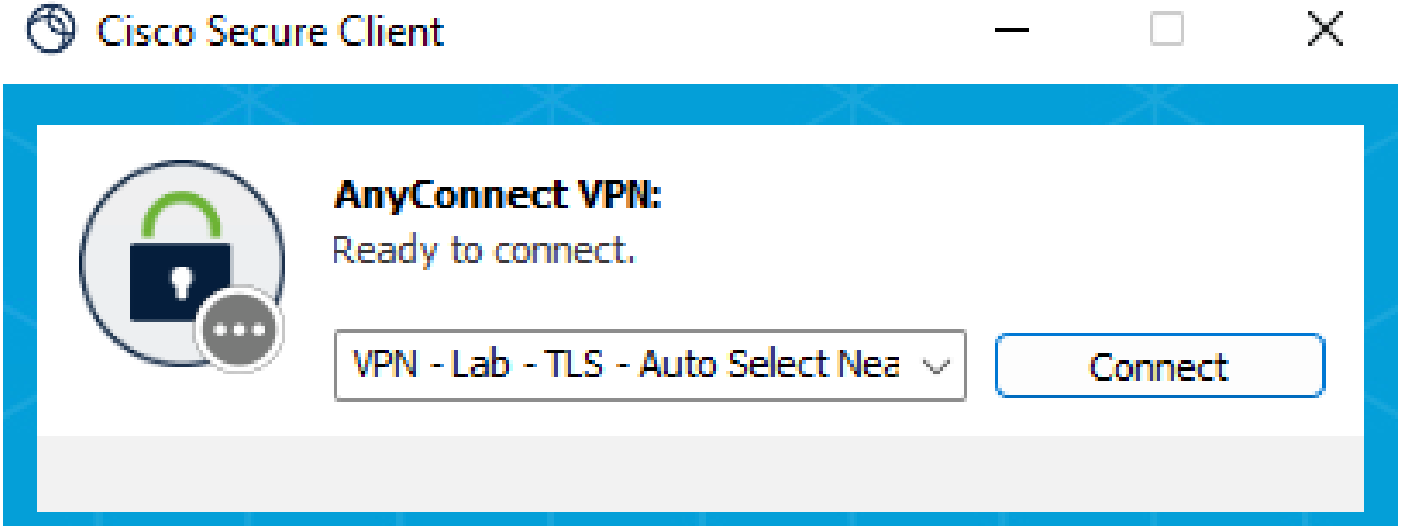
以前のVPN接続

クレデンシャルを入力し、VPNに接続します。



VPNに接続

初めて接続した後、ドロップダウンメニューから「VPN - Lab」VPNプロファイルに接続するオプションが表示されるはずです。



最初のVPN接続後

リモートアクセスログで、ユーザが接続できたことを確認します。

Monitor > Remote Access Log（モニタ>リモートアクセスログ）

Cisco Secure Accessのログ

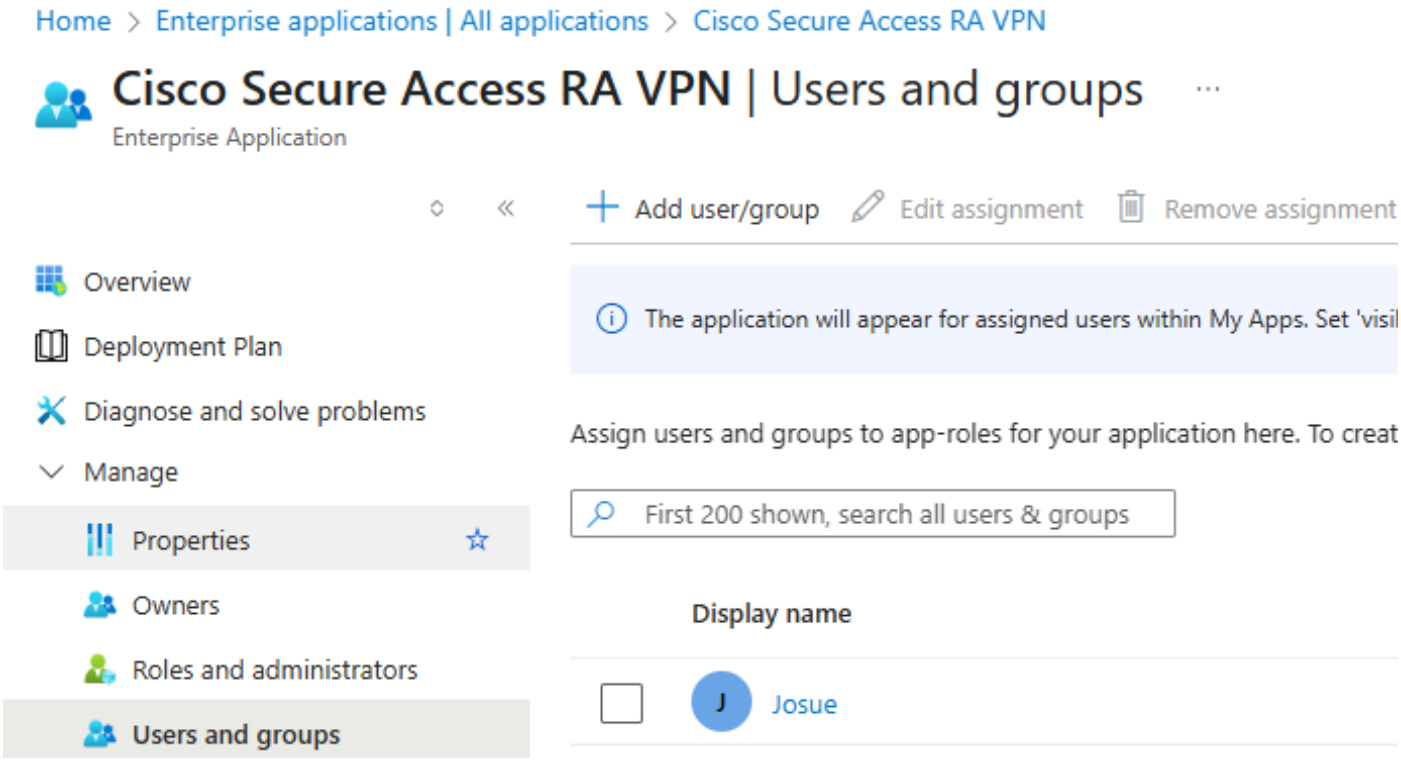
トラブルシューティング

一般的な問題に対して実行できる基本的なトラブルシューティングを次に示します。

Azure

Azureで、Cisco Secure Accessに対する認証用に作成されたエンタープライズアプリケーションにユーザーが割り当てられていることを確認します。

Home > Enterprise Applications > Cisco Secure Access RA VPN > Manage > Users and Groups

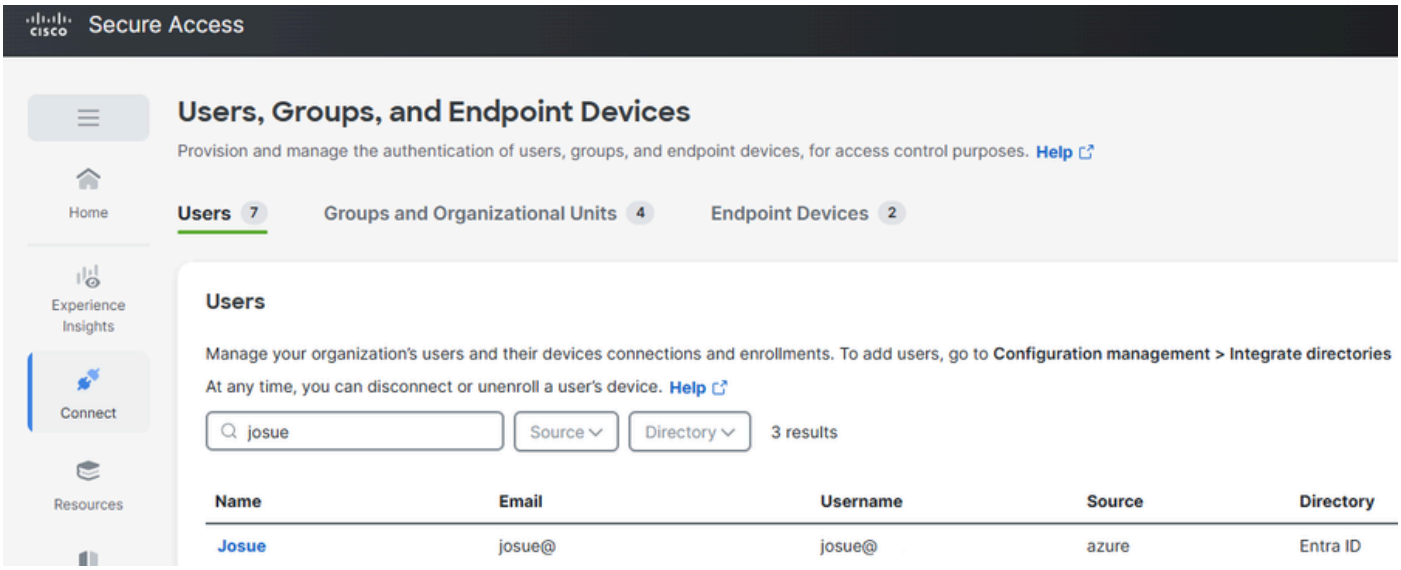


ユーザの割り当ての確認

シスコセキュアアクセス

Cisco Secure Accessで、RA VPN経由での接続が許可されているユーザがプロビジョニングされていること、およびCisco Secure Accessで（ユーザ、グループ、エンドポイントデバイスの下で）プロビジョニングされているユーザがAzureのユーザ（エンタープライズアプリケーションで割り当てられているユーザ）と一致していることを確認します。

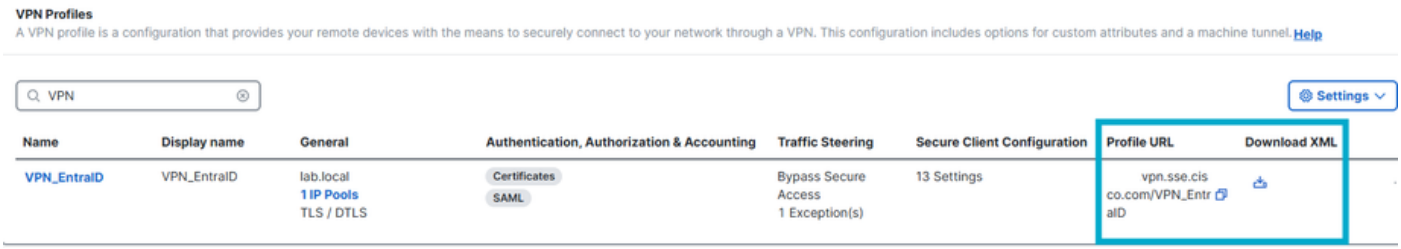
Connect > Users, Groups, and Endpoint Devices



シスコセキュアアクセスのユーザ

ユーザがPC上で正しいXMLファイルを使用してプロビジョニングされているか、「確認」手順で説明されているように、ユーザにプロファイルURLが提供されていることを確認します。

Connect > End User Connectivity > Virtual Private Network



プロファイルURLおよび.xmlプロファイル

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。