

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

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[Azure構成](#)

[Cisco Secure Access設定](#)

[確認](#)

[トラブルシューティング](#)

[Azure](#)

[シスコセキュアアクセス](#)

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

End User Connectivity

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. [Help](#)

Zero Trust

Virtual Private Network

Internet Security

FQDN

Use the FQDN listed here to configure VPN access to Secure Access. [Help](#)

Global: .vpn.sse.cisco.com [Copy](#) [View Regional FQDN's](#)


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

Cisco Secure Firewall - Secure Client (forme...



 Got feedback?

Logo ⓘ



Name * ⓘ

Cisco Secure Firewall - Secure Client (formerly AnyConnect) auth...

Publisher ⓘ

Cisco Systems, Inc.

Provisioning ⓘ

Automatic provisioning is not supported

Single Sign-On Mode ⓘ

SAML-based Sign-on
Linked Sign-on

URL ⓘ

<https://www.cisco.com/go/securefirewall>

[Read our step-by-step Cisco Secure Firewall - Secure Client \(formerly AnyConnect\) authentication integration tutorial](#)

Use Microsoft Entra ID to manage user access and enable single sign-on with the Cisco Secure Firewall for Secure Client (formerly AnyConnect) SAML authentication.

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


View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. [Learn more.](#)

If this application resides in your tenant, you can manage additional properties on the [application registration](#).

Enabled for users to sign-in? Yes No

Name *

Homepage URL

Logo 

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ーを割り当てます。

ユーザーとグループの割り当て > +ユーザー/グループの追加 > 割り当て

Home > Enterprise applications | All applications > Cisco Secure Access RA VPN

Cisco Secure Access RA VPN | Users and groups

Enterprise Application

◊ << + Add user/group Edit assignment Remove assignment

Overview

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups**

The application will appear for assigned users within My Apps. Set 'visibility' to 'My Apps' to make this application visible to users.

Assign users and groups to app-roles for your application here. To create a new user or group, click the plus icon.

First 200 shown, search all users & groups

Display name
No application assignments found

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

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
<input type="text" value="https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID"/>	<input checked="" type="checkbox"/> ⓘ

[Add identifier](#)

Patterns: https://*.YourCiscoServer.com/saml/sp/metadata/TGTGroup

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
<input type="text" value="https://example1.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=VPN_EntraID"/>	<input type="text"/>	<input checked="" type="checkbox"/> ⓘ


[Add reply URL](#)

Patterns: https://YOUR_CISCO_ANYCONNECT_FQDN/+CSCOE+/SAML/SP/ACS


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。

SAML Certificates

Token signing certificate		 Edit
Status	Active	
Thumbprint	B3194903628E192F48BC0CB44E7614867F79F17E	
Expiration	3/28/2028, 11:50:10 AM	
Notification Email		
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com/71414a41-5159..."/>	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Verification certificates (optional)

Required	No	 Edit
Active	0	
Expired	0	

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

 ⊗ ▾

Display name

DNS Server

 ▾ [+ Add](#)

DDNS Servers updates

System IP Pool ⓘ

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 Pool



Add up to 25 subnets per protocol to this IP pool. The number of connections available here is set by the number of subnets added to the System IP Pools field

IP Pool name

RA VPN Pool

IPv4 subnets ⓘ

172.16.1.0/24

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ーに表示される「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 Profile name

VPN_EntraID

1 General settings

2 Authentication, Authorization, and Accounting

3 Traffic Steering (Split Tunnel)

4 Cisco Secure Client Configuration

General settings

Select and configure the network, protocol and posture that this VPN profile will use. [Help](#)

Display name

VPN - Lab

This name will be displayed in Cisco Secure Client application.

Default Domain

lab.local

DNS Servers ⓘ

Region Specified

[View DNS servers](#) mapped to regions

Custom Specified

DDNS Servers updates

IP Pools ⓘ

[Edit assigned IP pools](#)

VPNプロファイルの設定 - パート1

Profile Settings

Include machine tunnel for this profile ⓘ [+ Add Machine Tunnel](#)

Include regional FQDN ⓘ

Protocol ⓘ

TLS / DTLS

IPsec (IKEv2)

IP version mode ⓘ

IPv4

IPv6

Connect time posture (optional)

None

Multiple VPN postures can be created in Posture.

VPNプロファイルの設定 - パート2

認証、許可、およびアカウントテイング

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。

Protocols

SAML

Authenticate with CA certificates
Select to use CA certificates to authenticate this VPN profile.

SAML Configuration

External browser authentication ⓘ

Forced re-authentication ⓘ

SAML Metadata XML Configuration

1. Download Service Provider XML file
This XML file contains metadata required to configure your IdP.
[Download service provider XML file](#)

2. Generate IdP Security Metadata XML File
a. Upload the Service Provider XML file to your IdP.
b. From your IdP, create and download an IdP Security Metadata XML file.

3. Upload IdP security metadata XML file

File 'Cisco Secure Access RA VPN.xml' uploaded. [Replace](#) [Delete](#)

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。

Traffic Steering (Split Tunnel)

Configure how VPN traffic traverses your network. [Help](#)

Tunnel Mode

Bypass Secure Access

All traffic is steered outside the tunnel.



Add Exceptions

Destinations specified here will be steered INSIDE the tunnel.

Destinations

10.1.1.0/24

Exclude Destinations

[+ Add](#)

DNS Mode

Default DNS

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。

Cisco Secure Client Configuration

Select various settings to configure how Cisco Secure Client operates. [Help](#)

Session Settings 7

Client Settings 13

Client Certificate Settings 4

[Download XML](#)

General

4

Administrator Settings

9

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。

Zero Trust **Virtual Private Network** Internet Security

FQDN
Use the FQDN listed here to configure VPN access to Secure Access. [Help](#)

Global: .sse.cisco.com [Copy](#) [View Regional FQDN's](#)

VPN Headend: vpn.sse.cisco.com [Copy](#)

Regions and IP Pools
Click manage to add and edit IP pools that can be used when configuring your VPN profiles. [Help](#)

Regions mapped 1 [Manage](#)

VPN Profiles
A VPN profile is a configuration that provides your remote devices with the means to securely connect to your network through a VPN. This configuration includes options for custom attributes and a machine tunnel. [Help](#)

🔍 Search ⚙️ Settings + VPN profile

Name	Display name	General	Authentication, Authorization & Accounting	Traffic Steering	Secure Client Configuration	Profile URL	Download XML
VPN_EntraID	VPN - Lab	lab.local 1 IP Pools TLS / DTLS	SAML	Bypass Secure Access 1 Exception(s)	13 Settings	sse.cisco.com/VPN_EntraID	📄

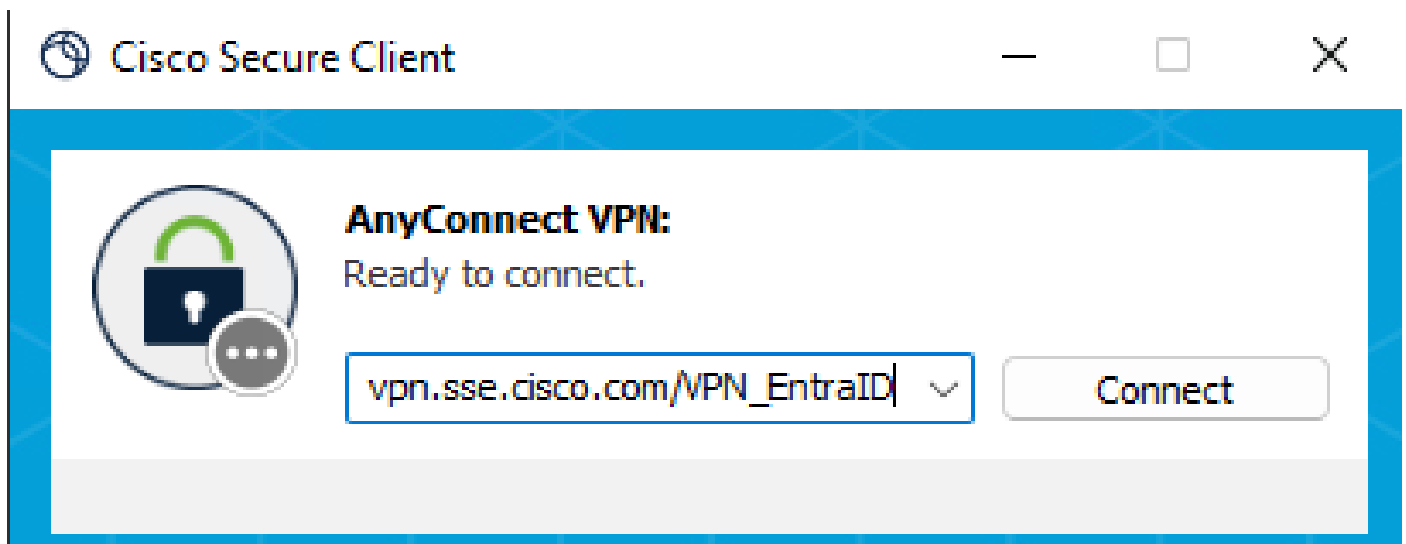
グローバルFQDNとプロフィールURL

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、プロフィール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プロフィー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プロフィー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。

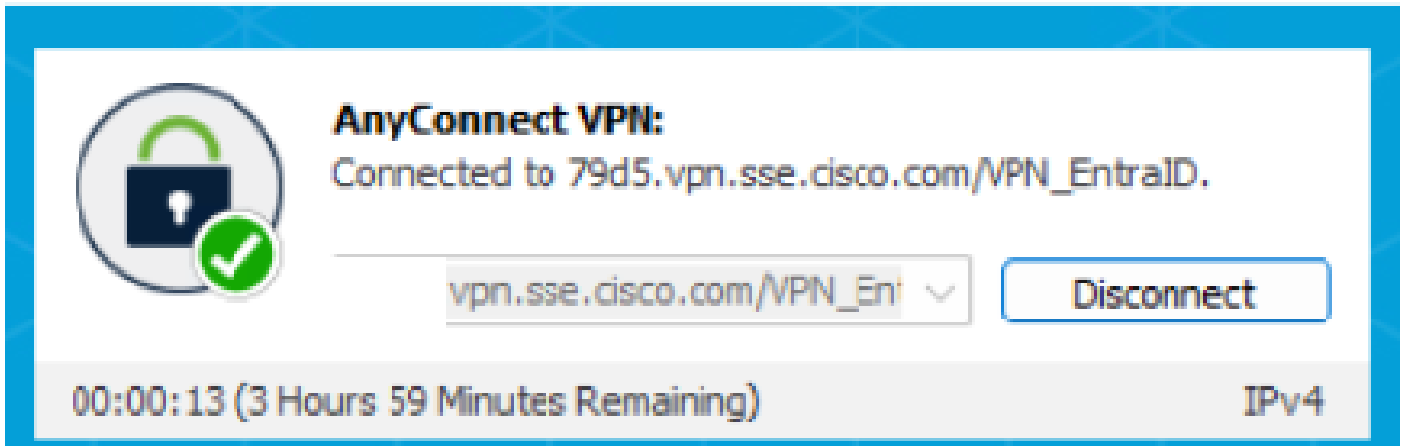
この例では、最初の接続試行でプロフィールURLアドレスをユーザに割り当てます。

最初の接続の前：



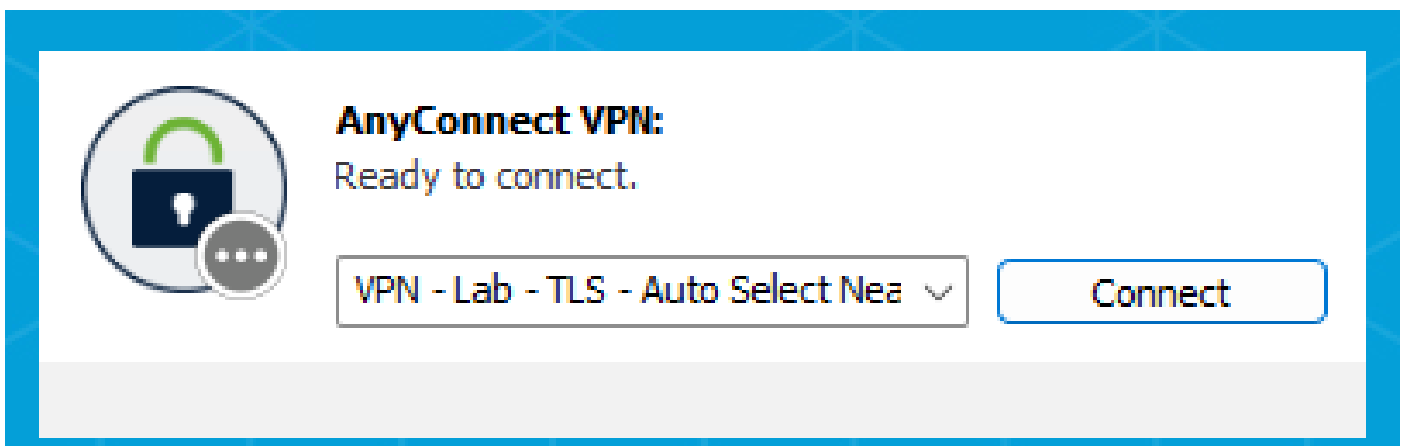
以前のVPN接続

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が、



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)

User	Device Name	Connection Event	Event Details	Public IPv4 Address	Internal IPv4 Address	Internal IPv6 Address	VPN Profile	Session Type
↑ Josue		Connected			172.16.1.1		VPN_EntraID	TLS

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

Home > Enterprise applications | All applications > Cisco Secure Access RA VPN

Cisco Secure Access RA VPN | Users and groups

Enterprise Application


◊ << + Add user/group ✎ Edit assignment 🗑 Remove assignment

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties ☆
 - Owners
 - Roles and administrators
 - Users and groups**

📘 The application will appear for assigned users within My Apps. Set 'visibility' to 'Visible to all users' to make this application visible to all users.

Assign users and groups to app-roles for your application here. To create a new user or group, click the plus icon.

🔍 First 200 shown, search all users & groups

Display name
<input type="checkbox"/>  Josue

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

Users, Groups, and Endpoint Devices

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

Home

Users 7

Groups and Organizational Units 4

Endpoint Devices 2

Experience Insights

Connect

Resources

Users

Manage your organization's users and their devices connections and enrollments. To add users, go to **Configuration management > Integrate directories**. At any time, you can disconnect or unenroll a user's device. [Help](#)

3 results

Name	Email	Username	Source	Directory
Josue	josue@	josue@	azure	Entra ID

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

VPN Profiles

A VPN profile is a configuration that provides your remote devices with the means to securely connect to your network through a VPN. This configuration includes options for custom attributes and a machine tunnel. [Help](#)

Q VPN Settings

Name	Display name	General	Authentication, Authorization & Accounting	Traffic Steering	Secure Client Configuration	Profile URL	Download XML
VPN_EntraID	VPN_EntraID	lab.local 1 IP Pools TLS / DTLS	Certificates SAML	Bypass Secure Access 1 Exception(s)	13 Settings	vpn.sse.cis.co.com/VPN_EntraID	

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。