Configure Cisco Secure Access for RA VPNaaS with Entra ID

Contents

Introduction

This document describes step by step how to configure RA VPN on Cisco Secure Access to authenticate against Entra ID.

Prerequisites

Cisco recommends that you have knowledge of these topics:

- Knowledge using Azure/Entra ID.
- Knowledge with Cisco Secure Access.

Requirements

These requirements must be fulfilled before proceeding further:

- Access to your Cisco Secure Access Dashboard as Full Admin.
- Access to Azure as Admin.
- User provisioning already completed to Cisco Secure Access.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Access Dashboard.
- Microsoft Azure Portal.
- Cisco Secure Client AnyConnect VPN version 5.1.8.105

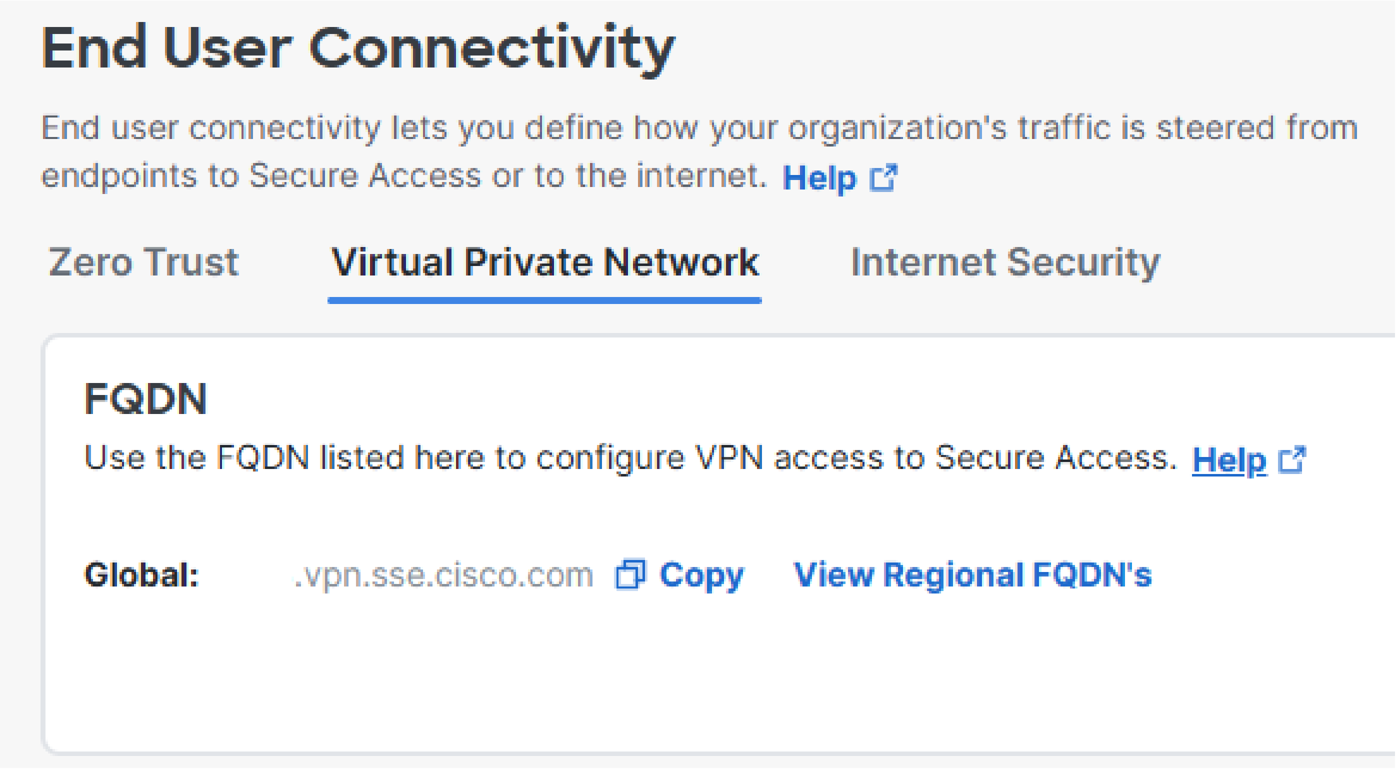
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Azure Configuration

1. Log in to the Cisco Secure Access dashboard and copy the VPN Global FQDN. We are using this FQDN in the Azure Enterprise Application configuration.

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

FQDN

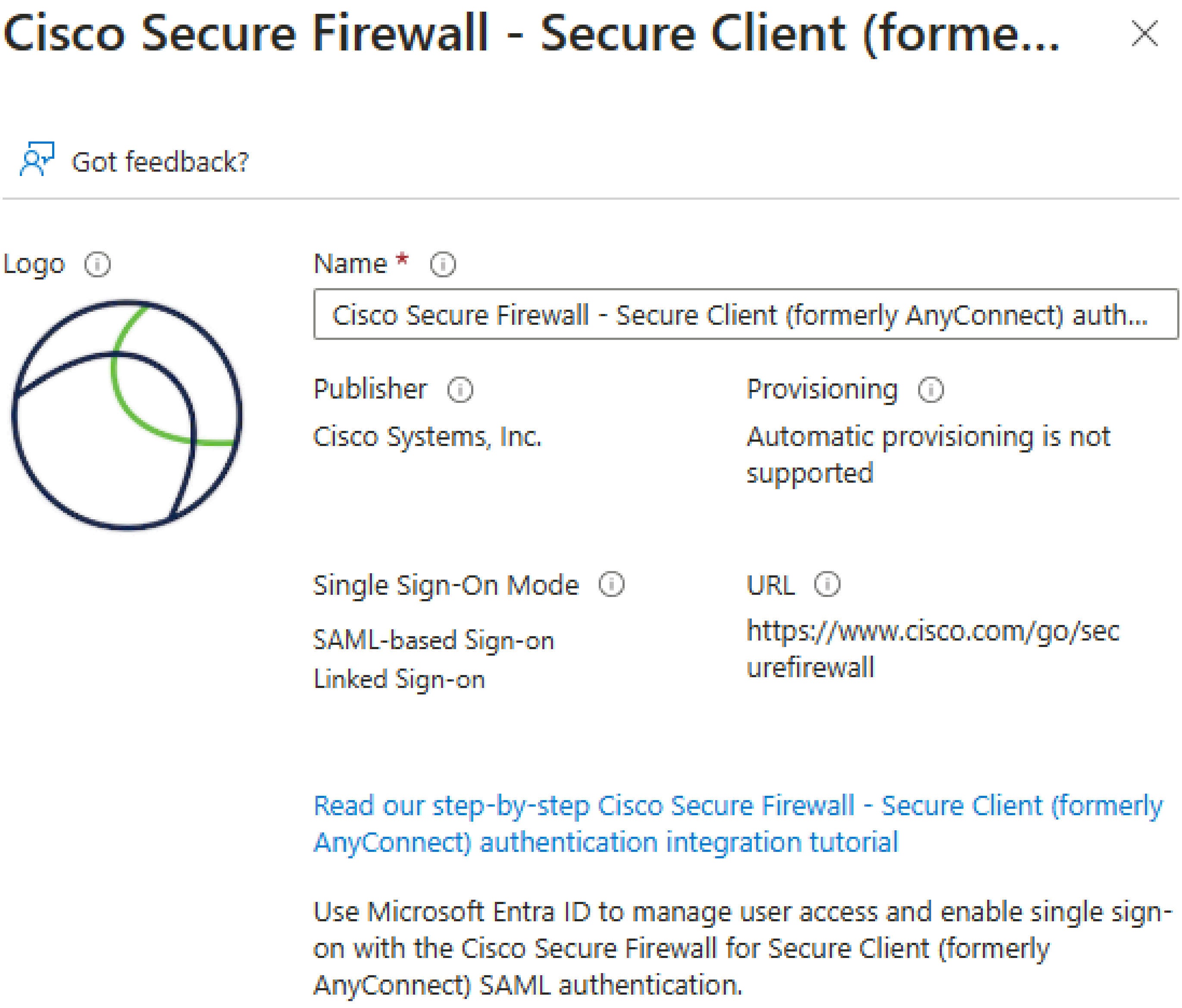
Use the FQDN listed here to configure VPN access to Secure Access. Help

Global: .vpn.sse.cisco.com

VPN Global FQDN

2. Log in to Azure and Create an Enterprise Application for the RA VPN authentication. You can use the predefined application named "Cisco Secure Firewall - Secure Client (formerly AnyConnect) authentication".

Home > Enterprise Applications > New Application > Cisco Secure Firewall - Secure Client (formerly 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

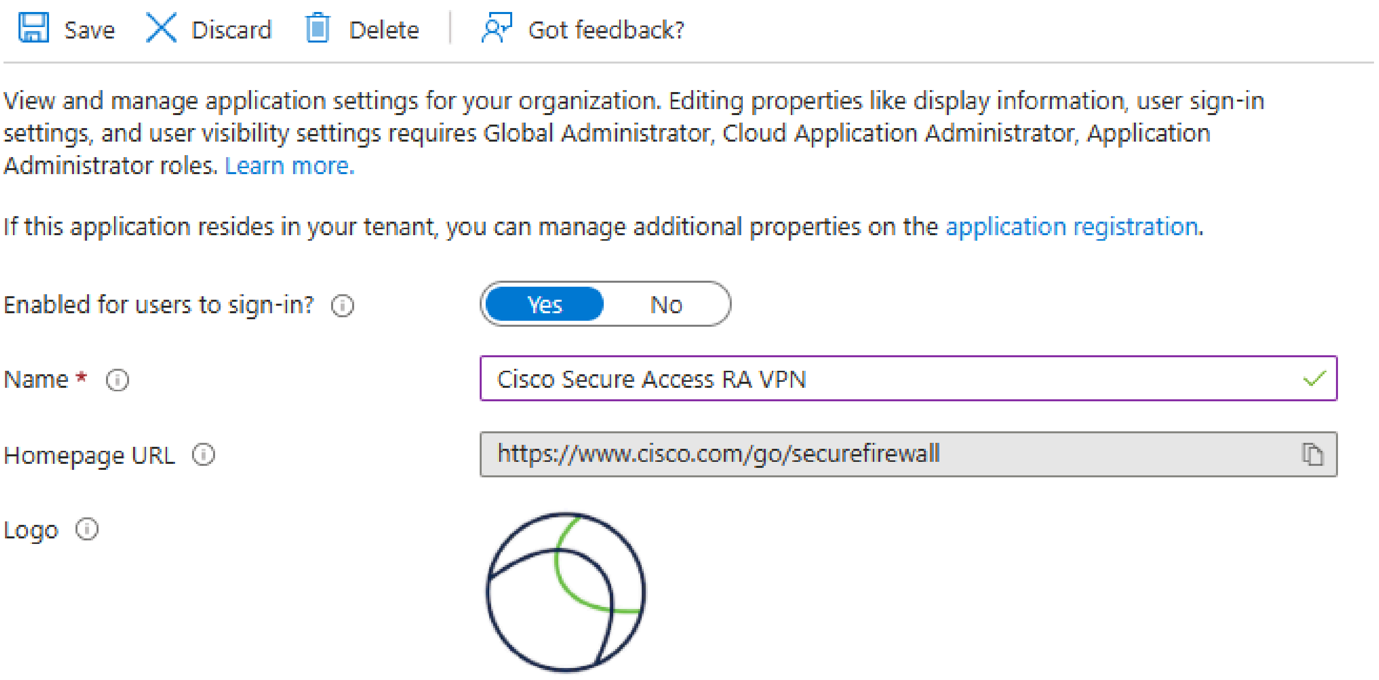
https://www.cisco.com/go/securefirewall

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.

Create App in Azure

3. Rename the Application.
   Properties > Name



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

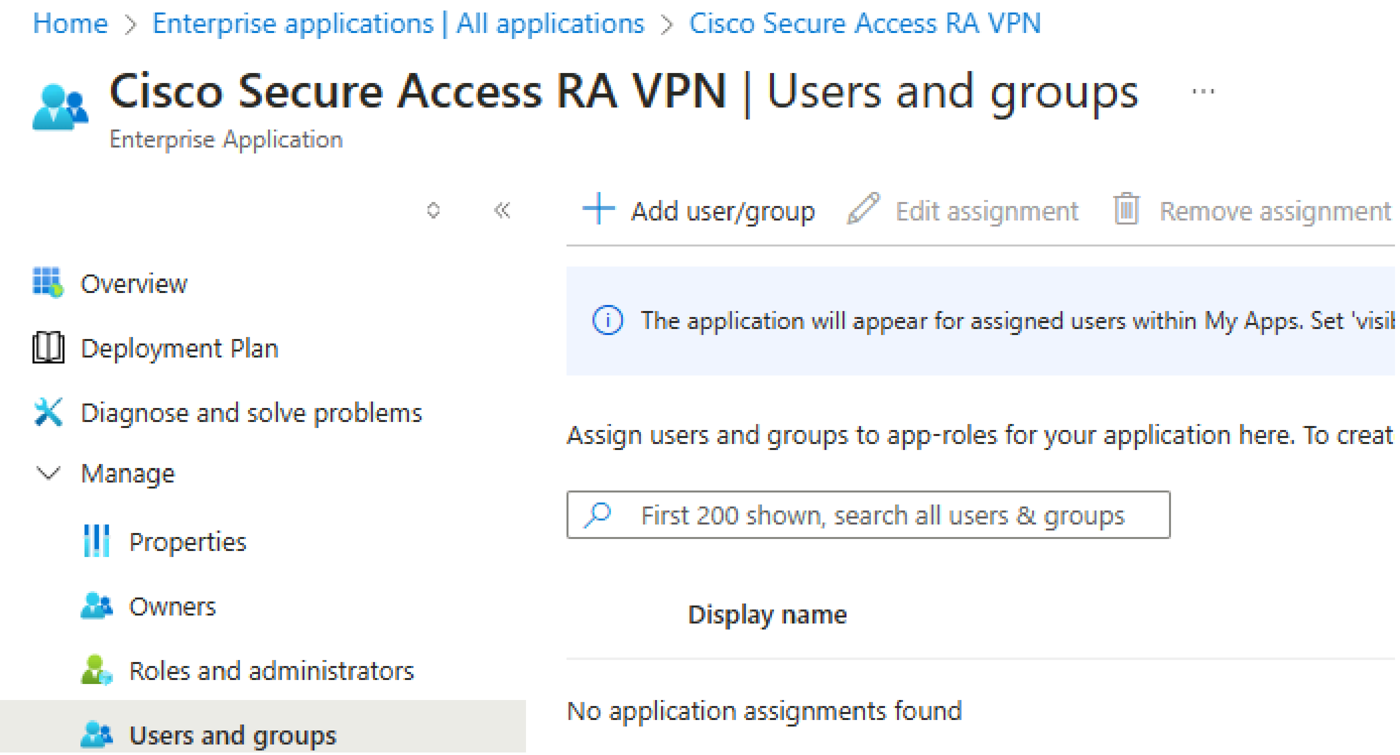
Name * ⓘ Cisco Secure Access RA VPN

Homepage URL ⓘ https://www.cisco.com/go/securefirewall

Logo ⓘ

Rename the Application

4. Within the Enterprise Application, assign the users allow to authenticate using the AnyConnect VPN. **Assign users and groups** > **+ Add user/group** > **Assign**



ⓘ The application will appear for assigned users within My Apps. Set 'visil

Assign users and groups to app-roles for your application here. To creat

First 200 shown, search all users & groups

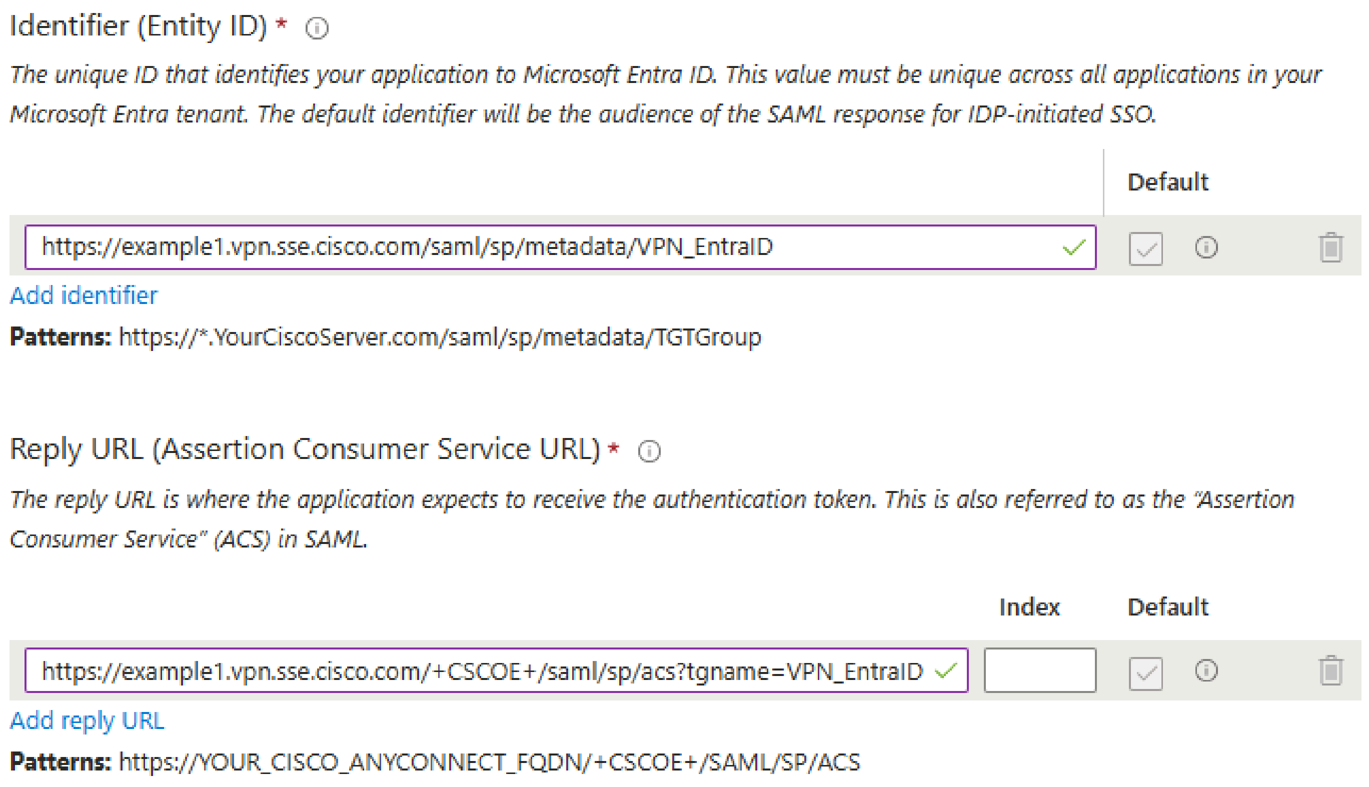
Display name
No application assignments found

Users/Groups Assigned

5. Click on Single sign-on and configure the SAML parameters. Here we use the FQDN copied in step 1, and also the VPN Profile name you are configuring in "Configuration Cisco Secure Access" later in step 2.

For example, if you VPN Global FQDN is example1.vpn.sse.cisco.com and your Cisco Secure Access VPN Profile name is VPN_EntraID, the values for (Entity ID) and the Reply URL (Assertion Consumer Service URL) are:

Identifier (Entity ID): https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID
Reply URL (Assertion Consumer Service 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
https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID ✓	☑ ⓘ

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.

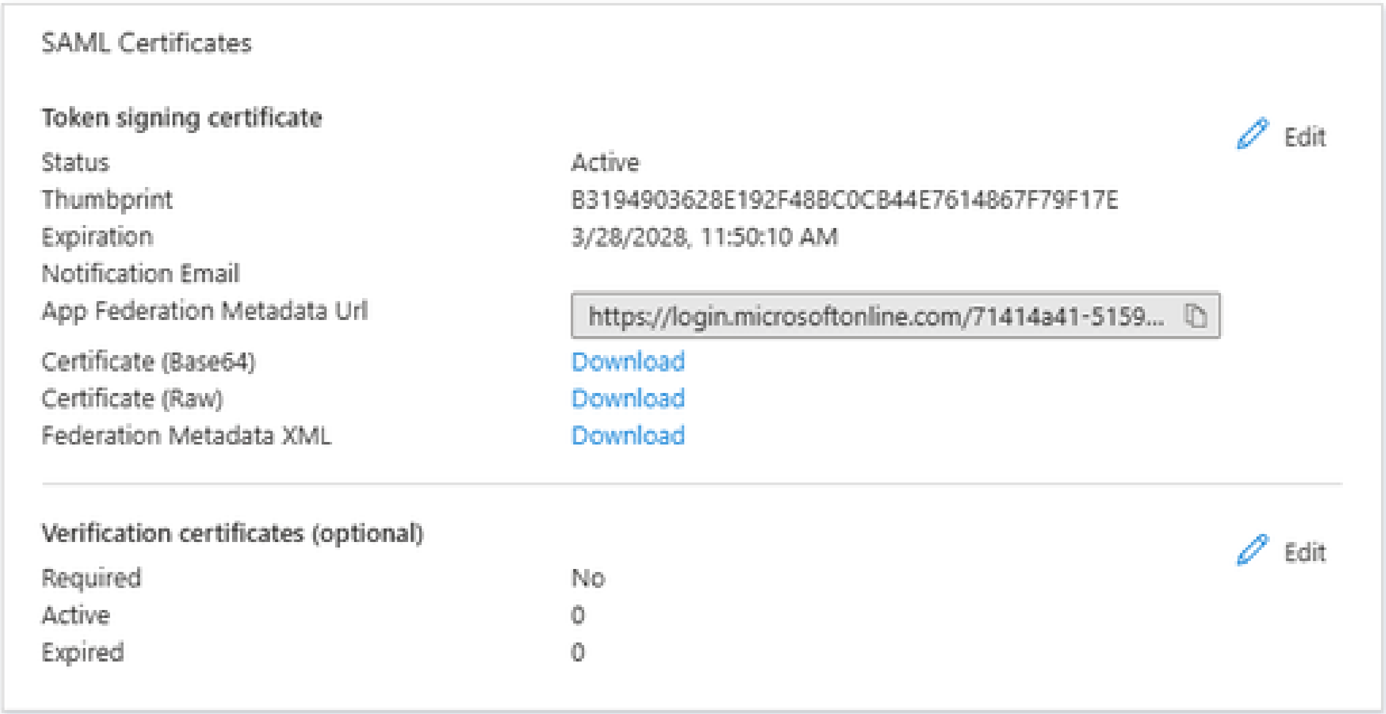
	Index	Default
https://example1.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=VPN_EntraID ✓		☑ ⓘ

Add reply URL

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

SAML Parameters in Azure

6. Download the Federation Metadata XML.



SAML Certificates

Token signing certificate

Status	Active
Thumbprint	B3194903628E192F48BC0CB44E7614867F79F17E
Expiration	3/28/2028, 11:50:10 AM
Notification Email	
App Federation Metadata Url	https://login.microsoftonline.com/71414a41-5159...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

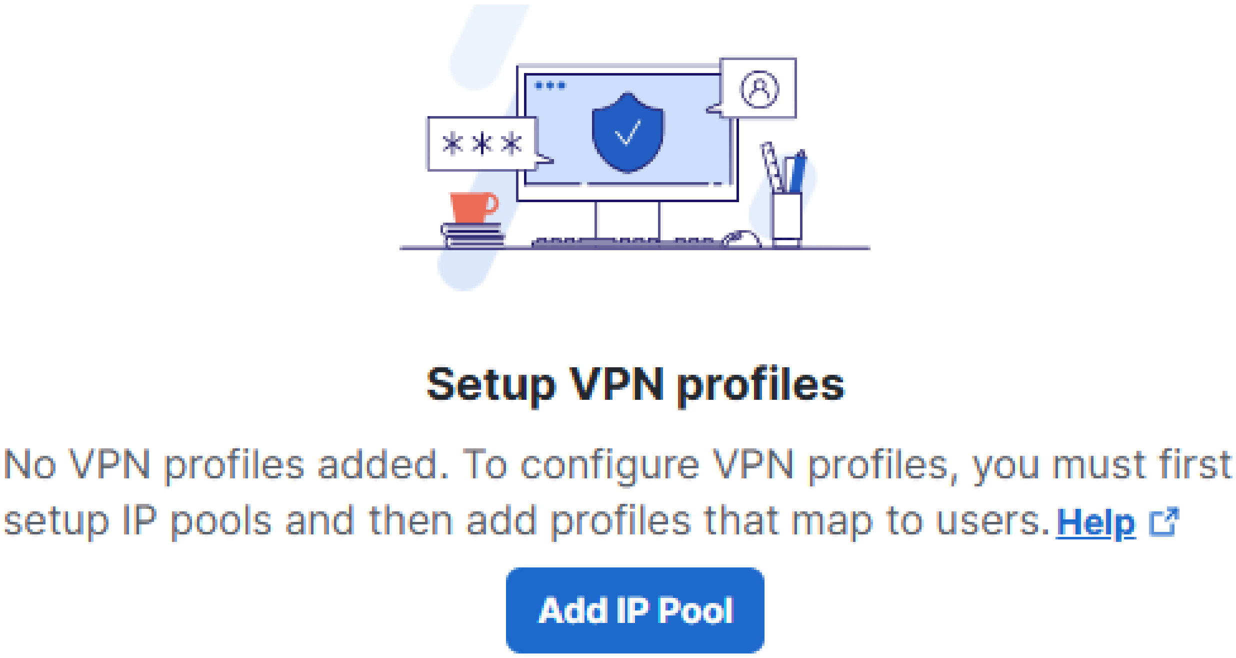
Required	No
Active	0
Expired	0

Cisco Secure Access Configuration

1. Log in to your Cisco Secure Access dashboard, and add an IP Pool.

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

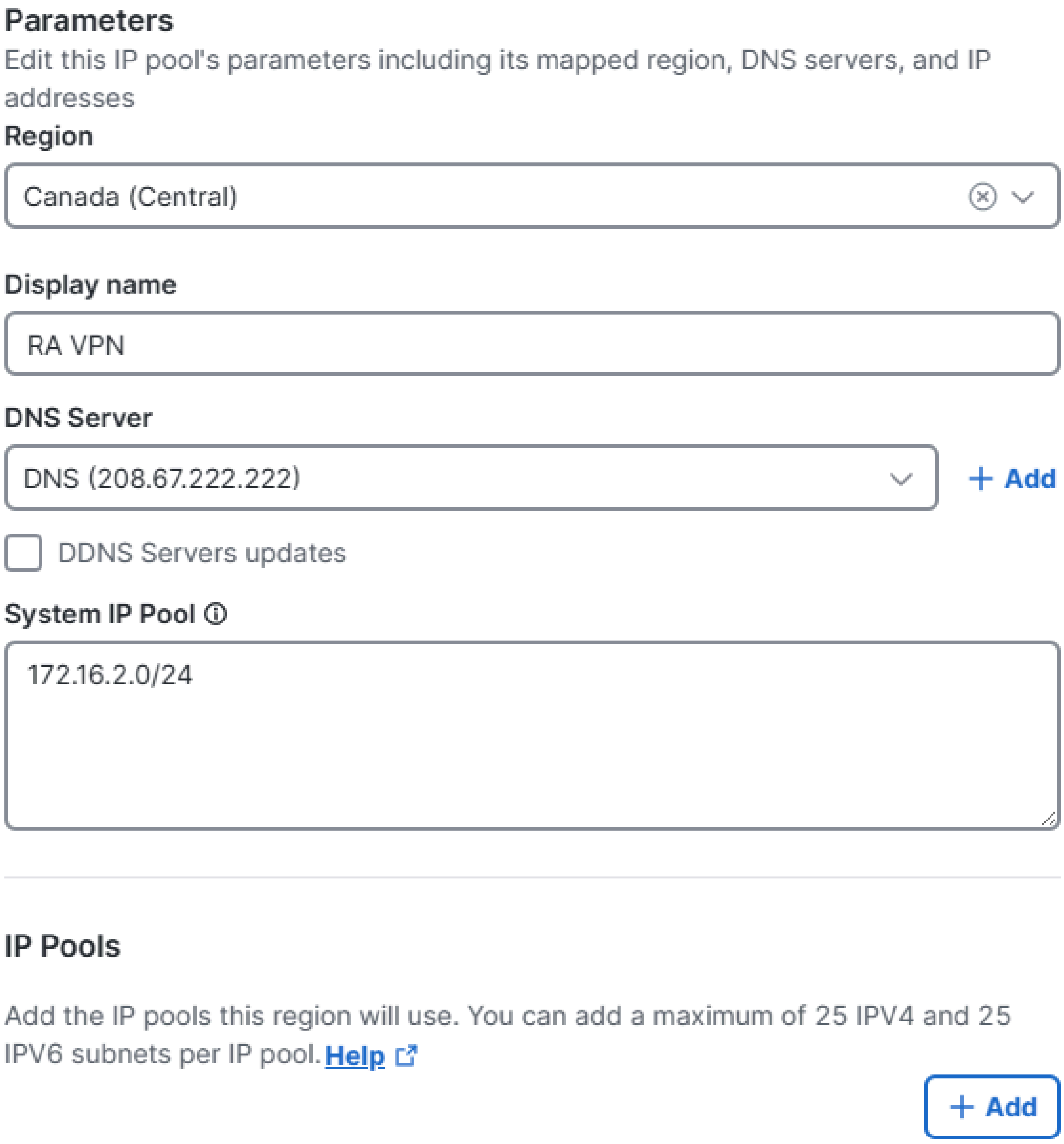
Region: Select the region where your RA VPN is going to be deployed.
Display name: The name for the VPN IP Pool.
DNS Server: Create or assign the DNS Server users are using for DNS resolution once connected.
System IP Pool: Used by Secure Access for features like Radius Authentication, the Authentication Request is sourced by an IP within this range.
IP Pool: Add a new IP Pool and specify the IPs users get once connected to the RA VPN.



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 VPN Profile



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)

□ DDNS Servers updates

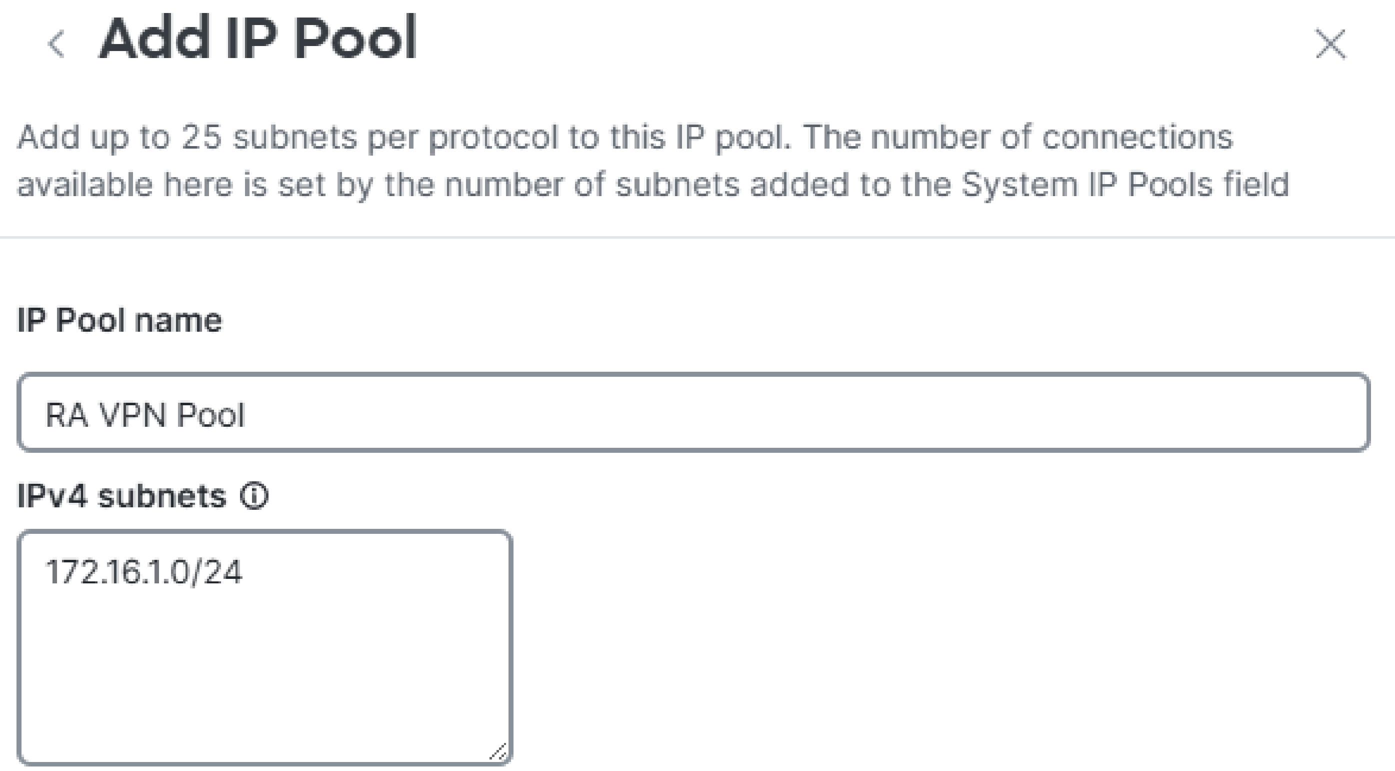
System IP Pool

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

Config of IP Pool - Part 1



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

Config of IP Pool - Part 2

2. Add a VPN Profile.

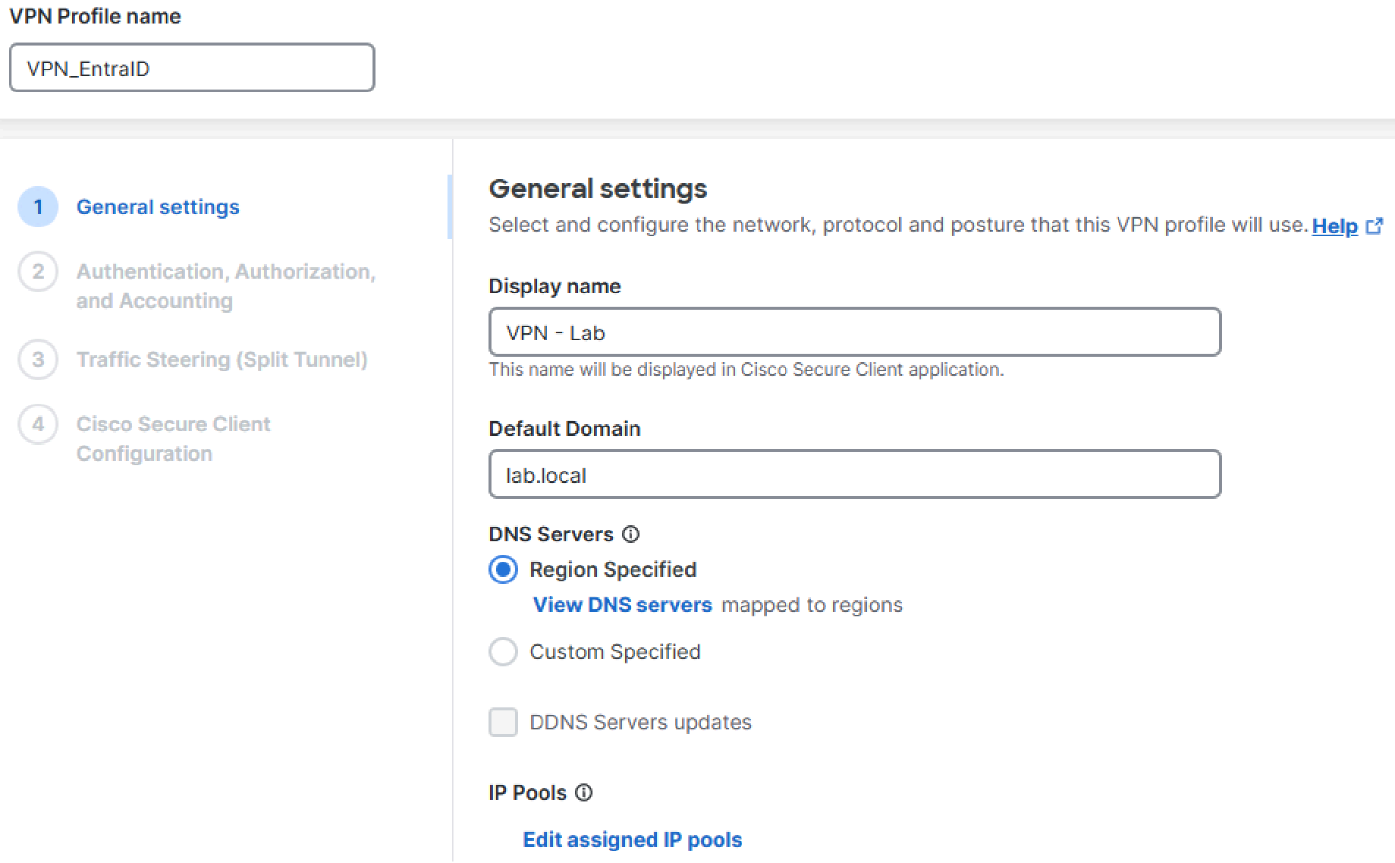
   Connect > End User Connectivity > Virtual Private Network > + VPN Profile

General Settings

Note: Note: The name of the VPN Profile must match with the name you configured in "Configuration Azure" in step 5. In this configuration guide we used VPN_EntraID so we are configuring the same in Cisco Secure Access as VPN Profile name.

VPN Profile name: Name for this VPN Profile, visible in the dashboard only.

Display name: Name end users see on the 'Secure Client - Anyconnect' drop-down menu see when connecting to this RA VPN Profile.
Default Domain: Domain users get once connected to the VPN.
DNS Servers: DNS Server the VPN users get once connected to the VPN.
  Region Specified: Uses the DNS server associated to the VPN IP Pool.
  Custom Specified: You can manually assign the DNS desired.
IP Pools: IPs the users get assigned once connected to the VPN.
Profile Settings: To include this VPN Profile for Machine Tunnel or to include regional FQDN so the end user selects the Region they want to connect to (is subject to IP Pools deployed).
Protocols: Select the protocol you want your VPN Users to use for the tunneling of the traffic.
Connect time posture (Optional): If required to do VPN Posture at the connect time. More information here



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

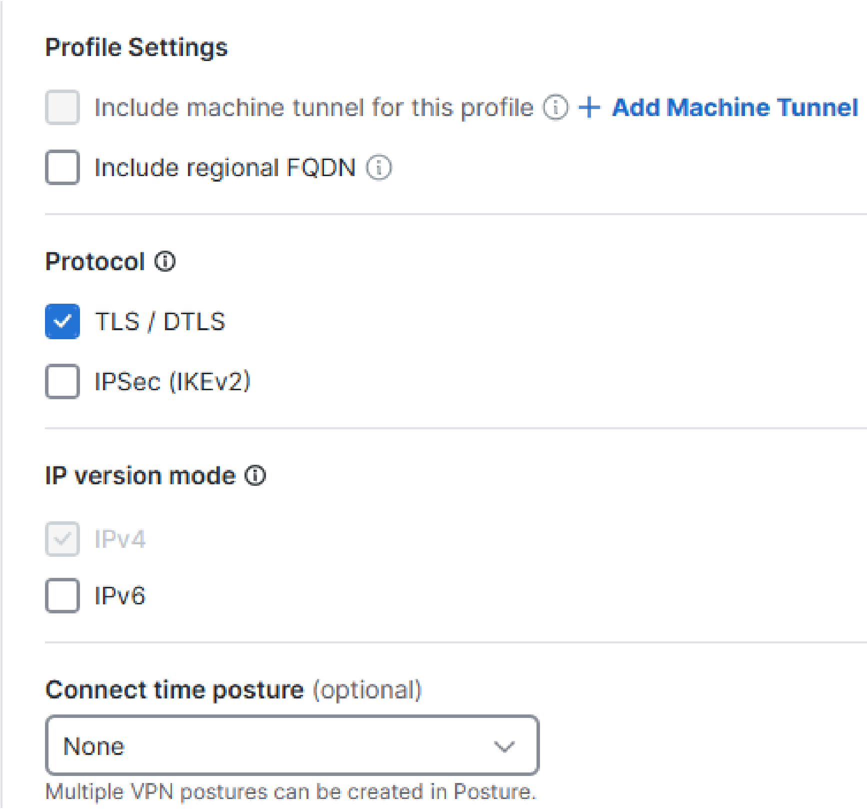
○ Custom Specified

□ DDNS Servers updates

IP Pools

Edit assigned IP pools

VPN Profile config - Part 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.

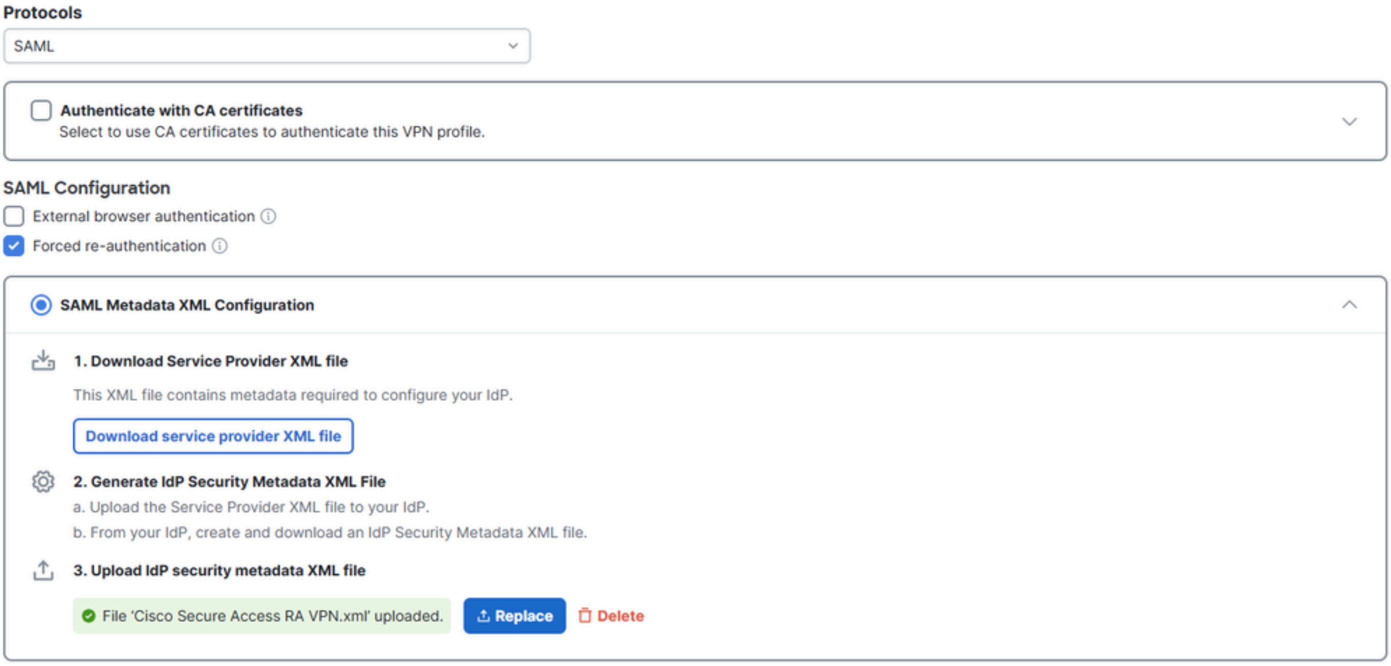
VPN Profile config - Part 2

Authentication, Authorization, and Accounting

Protocols: Select SAML.

Authentication with CA Certificates: In case you want to authenticate using an SSL Certificate and authorize against an IdP SAML Provider.
Force re-authentication: Forces a re-authentication whenever a VPN connection is made. Forced re-authentication is based on Session Timeout. This could be subjected to the SAML IdP settings (Azure in this case).

Upload the XML file Federation Metadata XML file downloaded in "Configure Azure" in step 6.



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.

SAML Config

Traffic Steering (Split Tunnel)

Tunnel Mode:

Connect to Secure Access: All traffic is sent thought the tunnel (Tunnel All).

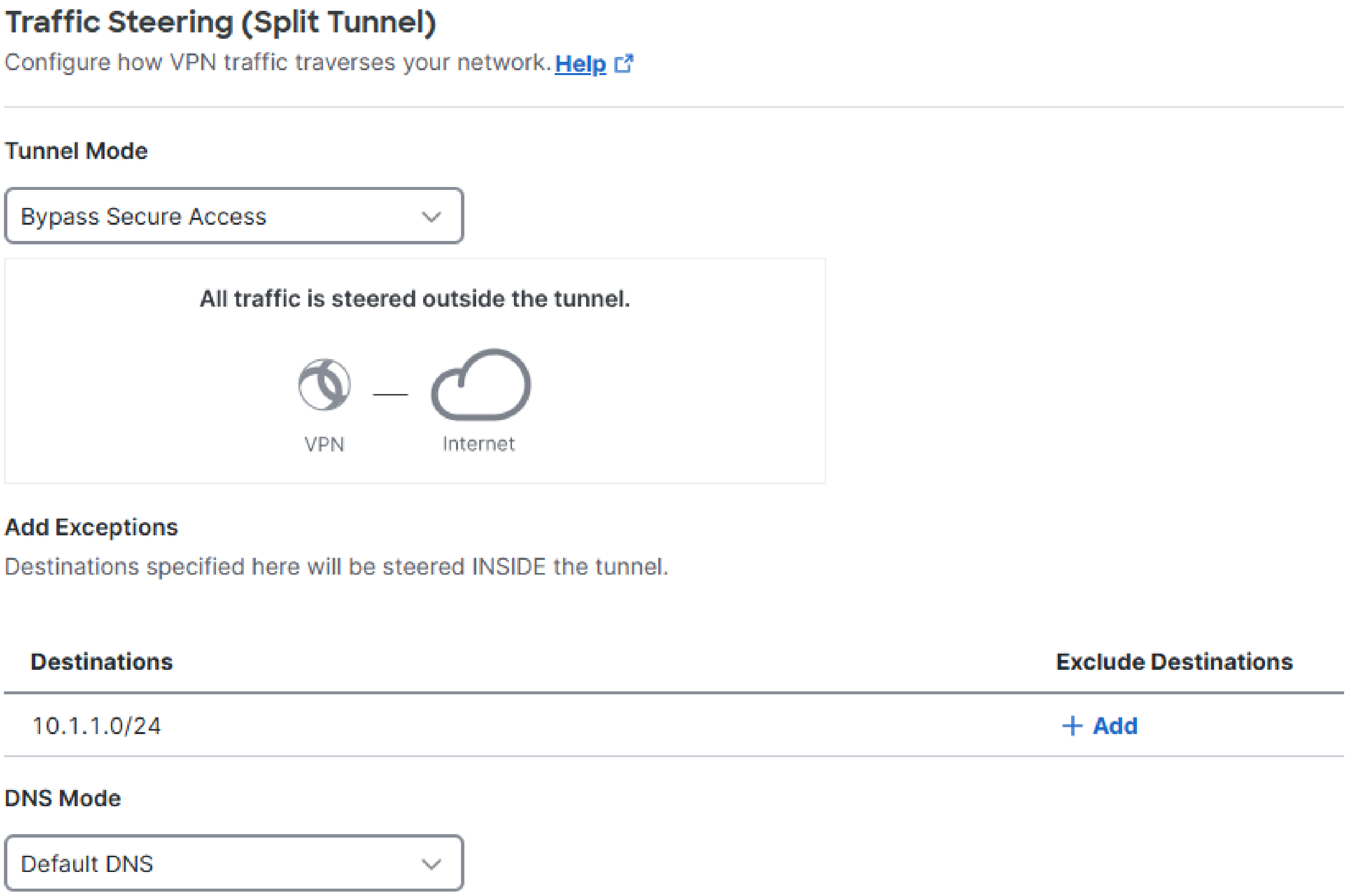
Bypass Secure Access: Just specific traffic defined the in Exceptions section is tunneled (Split Tunnel).

DNS Mode:

Default DNS: All of the DNS queries move through the DNS servers which are defined by the VPN Profile. In the case of a negative response, the DNS queries can also go to the DNS servers which are configured on the physical adapter.

Tunnel All DNS: Tunnels all DNS queries via the VPN.

Split DNS: Just specific DNS queries move through the VPN profile, depending on the domains specified below.



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	Exclude Destinations
10.1.1.0/24	+ Add

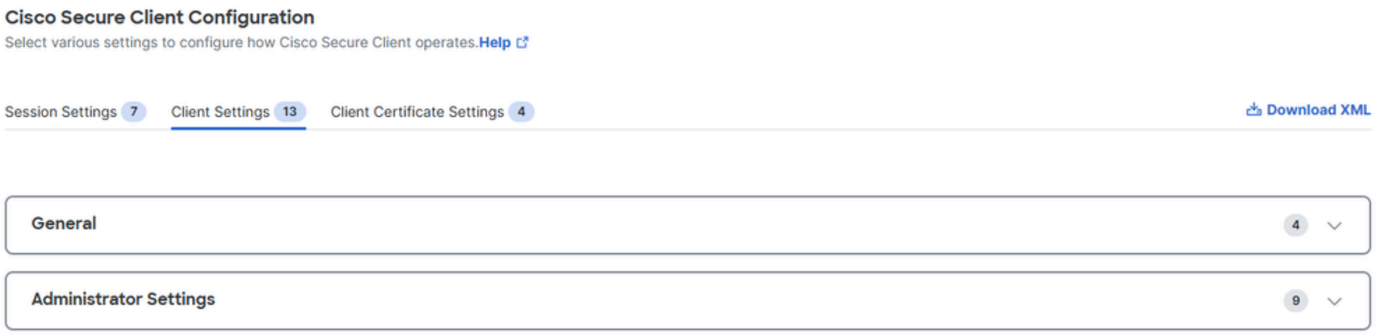
DNS Mode

Default DNS

Traffic Steering Config

Cisco Secure Client Configuration

For the purpose of this guide, we are not configuring any of these advanced settings. Advanced features can be configured here, for example: TND, Always-On, Certificate Matching, Local Lan Access, and so on. Save the settings here.



Cisco Secure Client Configuration

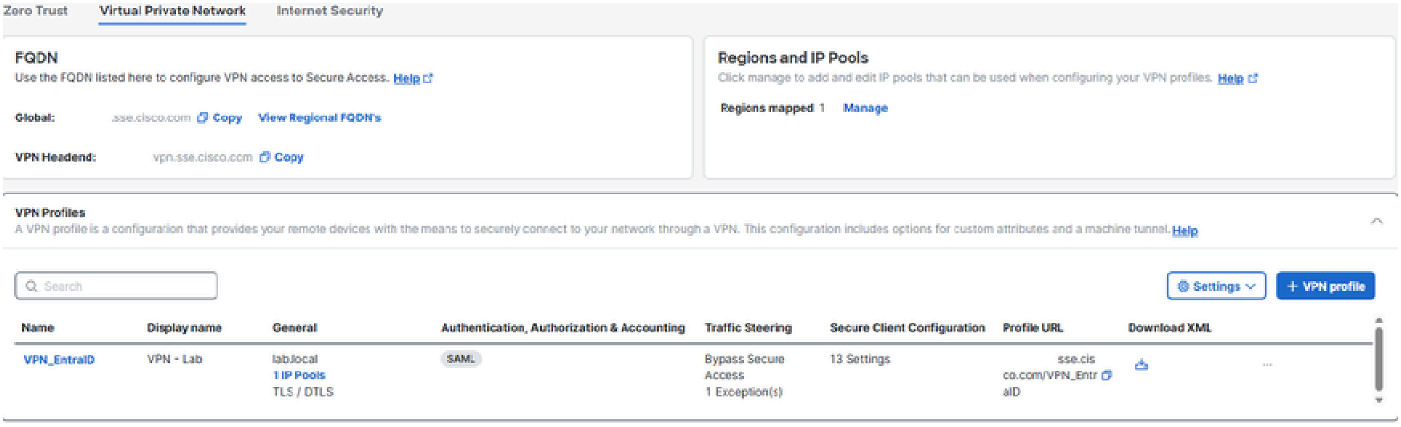
Select various settings to configure how Cisco Secure Client operates. Help

General 4

Administrator Settings 9

Advanced Settings

3. Your VPN Profile must look like this. You can download and pre-deploy the xml profile to the end users (under "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile") to start using the VPN, or provide them with the Profile URL to be entered in the Cisco Secure Client - AnyConnect VPN UI.



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

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	

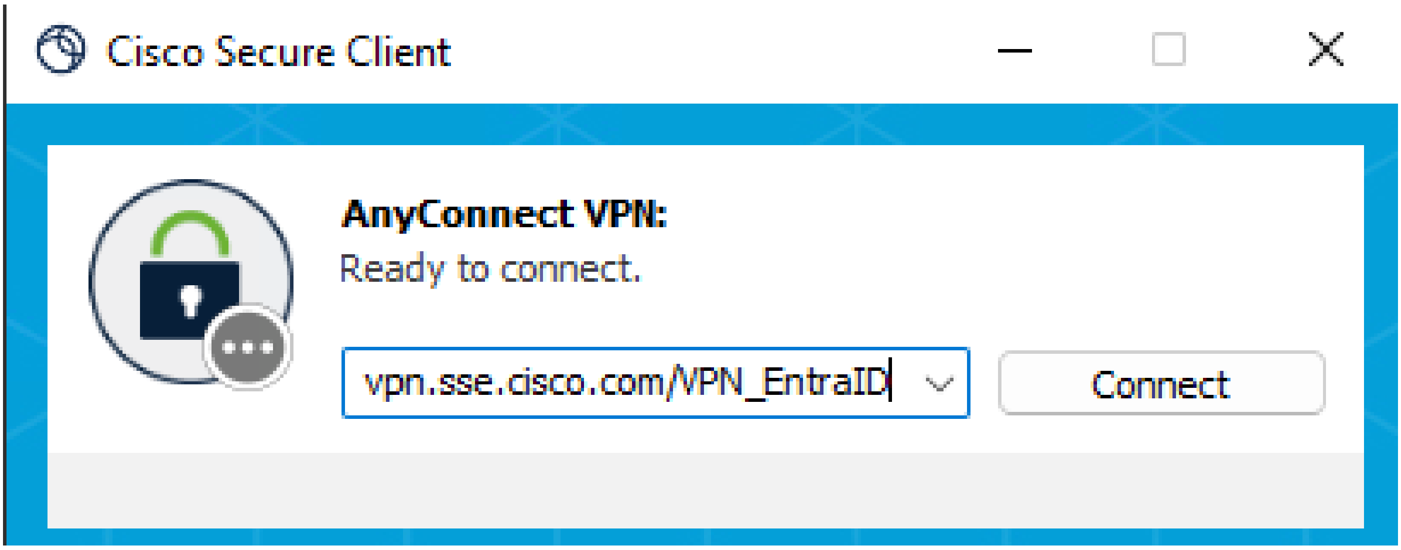
Global FQDN and Profile URL

Verify

At this point, your RA VPN configuration must be ready for testing.
Please notice that the first time the users connect, they need to be given the Profile URL address or pre-deploy the xml profile in their PCs under "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile", restart the VPN service and they must see in the drop-down menu the option to connect to this VPN Profile.

In this example, we give the Profile URL address to the user for the first connection attempt.

Prior the first connection:

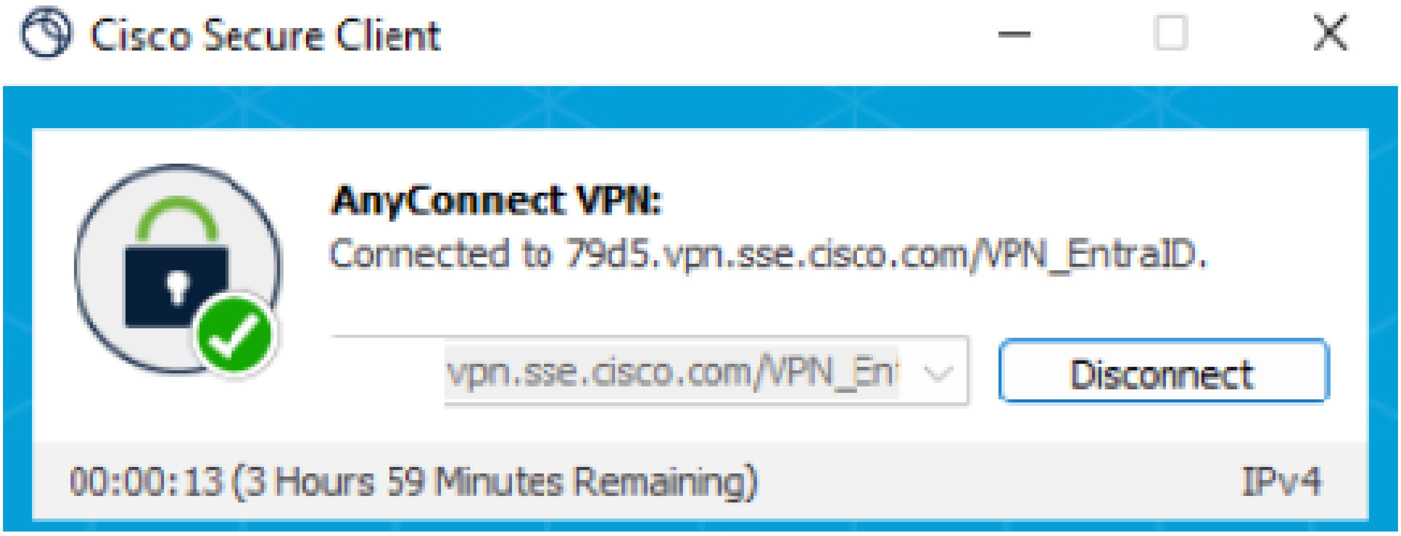


AnyConnect VPN:
Ready to connect.

vpn.sse.cisco.com/VPN_EntraID

Prior VPN Connection

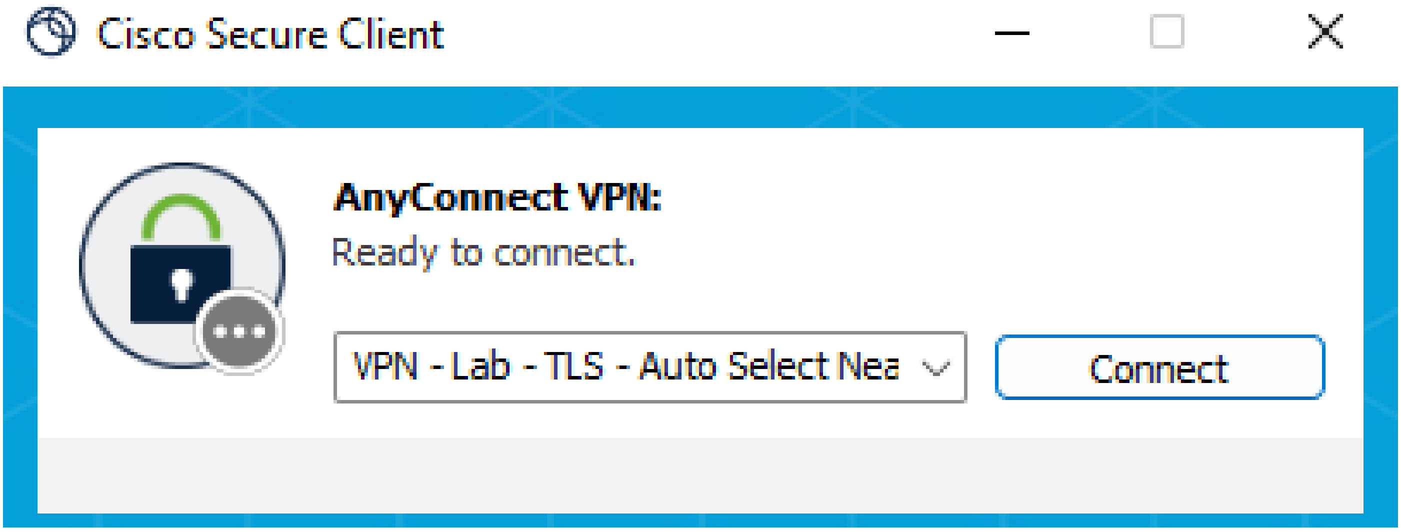
Enter your credentials and connect to the VPN:



Cisco Secure Client
AnyConnect VPN:
Connected to 79d5.vpn.sse.cisco.com/VPN_EntraID.
vpn.sse.cisco.com/VPN_En
Disconnect
00:00:13 (3 Hours 59 Minutes Remaining)
IPv4

Connected to VPN

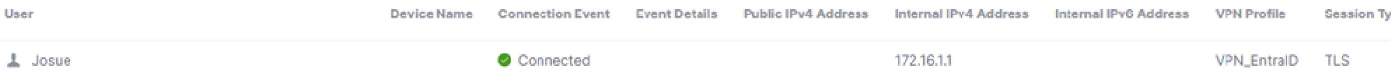
After connecting the first time, from the drop-down menu, you must be able to see now the option to connect to the "VPN - Lab" VPN Profile:



After the first VPN Connection

Check in the Remote Access Logs that the user was able to connect:

Monitor > Remote Access Log



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

Logs in Cisco Secure Access

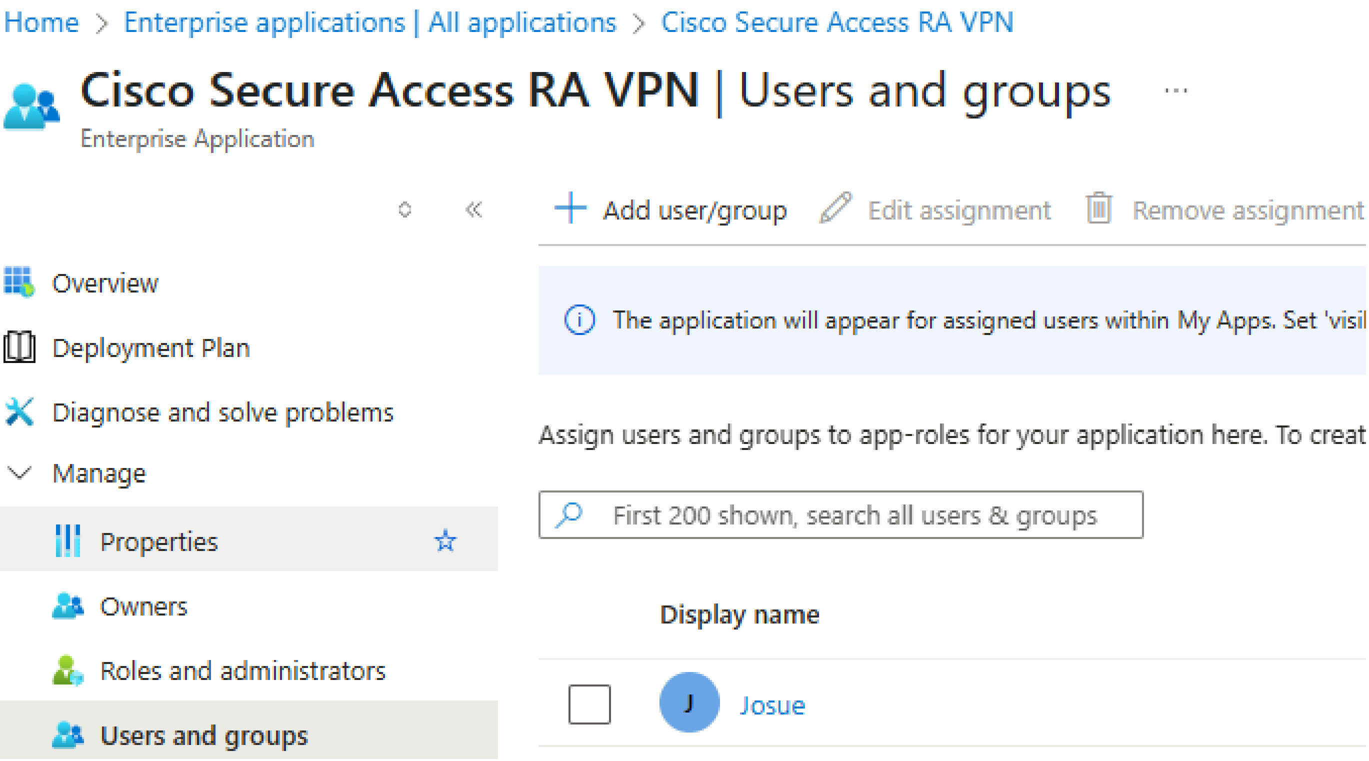
Troubleshooting

Here is described the basic troubleshooting that can be performed for some common issues:

Azure

In Azure make sure that the users have been assigned to the Enterprise Application created for the authentication against Cisco Secure Access:

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



The application will appear for assigned users within My Apps. Set 'visil

Assign users and groups to app-roles for your application here. To creat

First 200 shown, search all users & groups

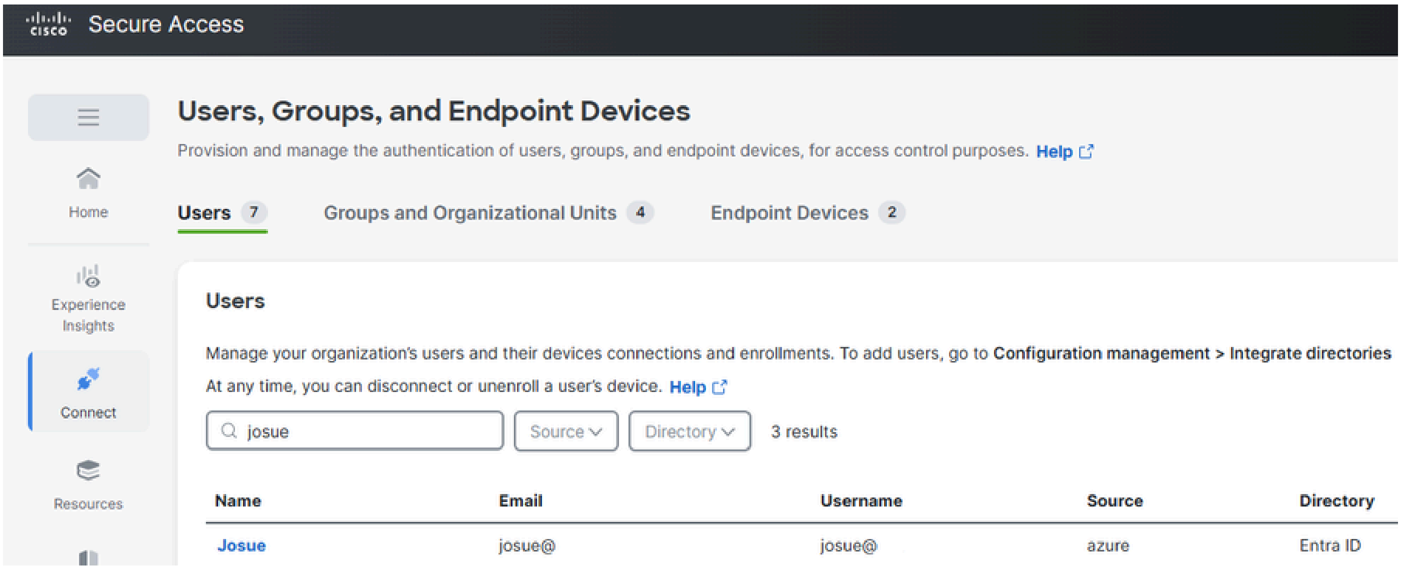
	Display name
□	J Josue

Verify assignment of users

Cisco Secure Access

In Cisco Secure Access, make sure you have provisioned the users that are allowed to connect via RA VPN, and that also the users provisioned in Cisco Secure Access (under users, groups and endpoint devices) match with the users in Azure (the users assigned in the enterprise application).

Connect > Users, Groups, and Endpoint Devices



Provision and manage the authentication of users, groups, and endpoint devices, for access control purposes. Help

Manage your organization's users and their devices connections and enrollments. To add users, go to Configuration management > Integrate directories

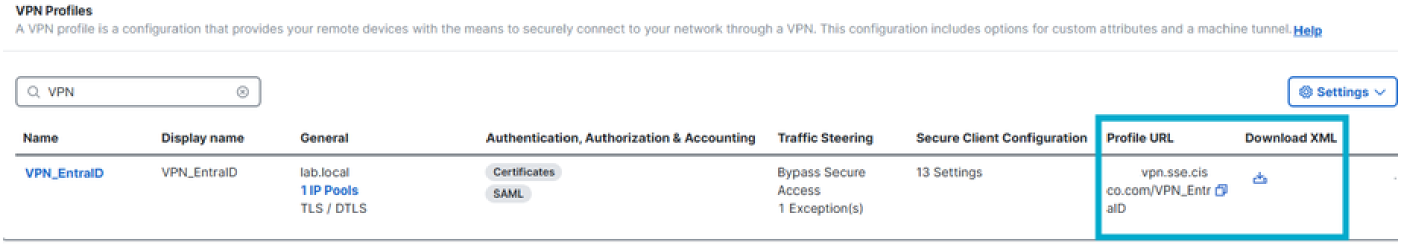
At any time, you can disconnect or unenroll a user's device. Help

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

Users in Cisco Secure Access

Verify that the user has been provisioned with either the correct XML file on the PC, or that the user has been given the Profile URL, as stated in the "Verify" step.

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

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.cisco.com/VPN_EntraID	

Profile URL and .xml profile