使用Entra ID配置RA VPNaaS的安全访问

目录

简介

先决条件

- 要求
- 使用的组件

配置

- Azure配置
- 思科安全访问配置

验证

故障排除

- Azure
- 思科安全访问

简介

本文档分步介绍如何在Cisco安全访问上配置RA VPN以根据Entra ID进行身份验证。

先决条件

Cisco 建议您了解以下主题：

- 使用Azure/Entra ID的知识。
- 思科安全访问知识。

要求

在继续操作之前，必须满足以下要求：

- 以完全管理员身份访问您的思科安全访问控制面板。
- 以管理员身份访问Azure。
- 用户调配已完成Cisco Secure Access。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全访问控制面板。
- Microsoft Azure门户。
- 思科安全客户端AnyConnect VPN版本5.1.8.105

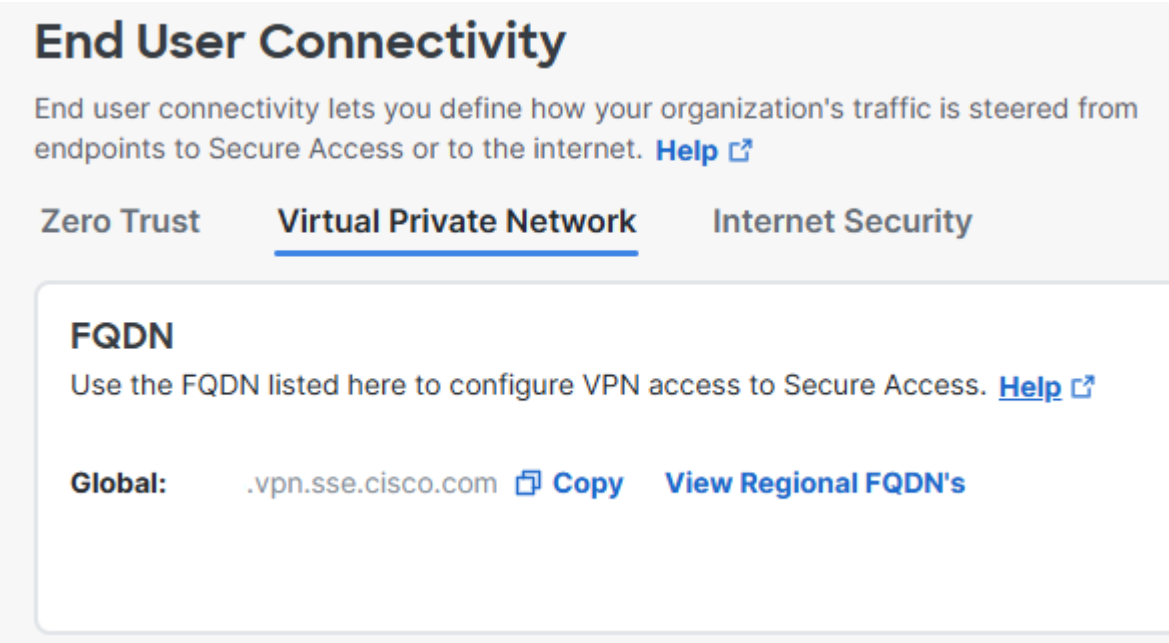
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

Azure配置

1.登录到Cisco Secure Access控制面板并复制VPN 全局FQDN。您正在Azure企业应用程序配置中使用此FQDN。

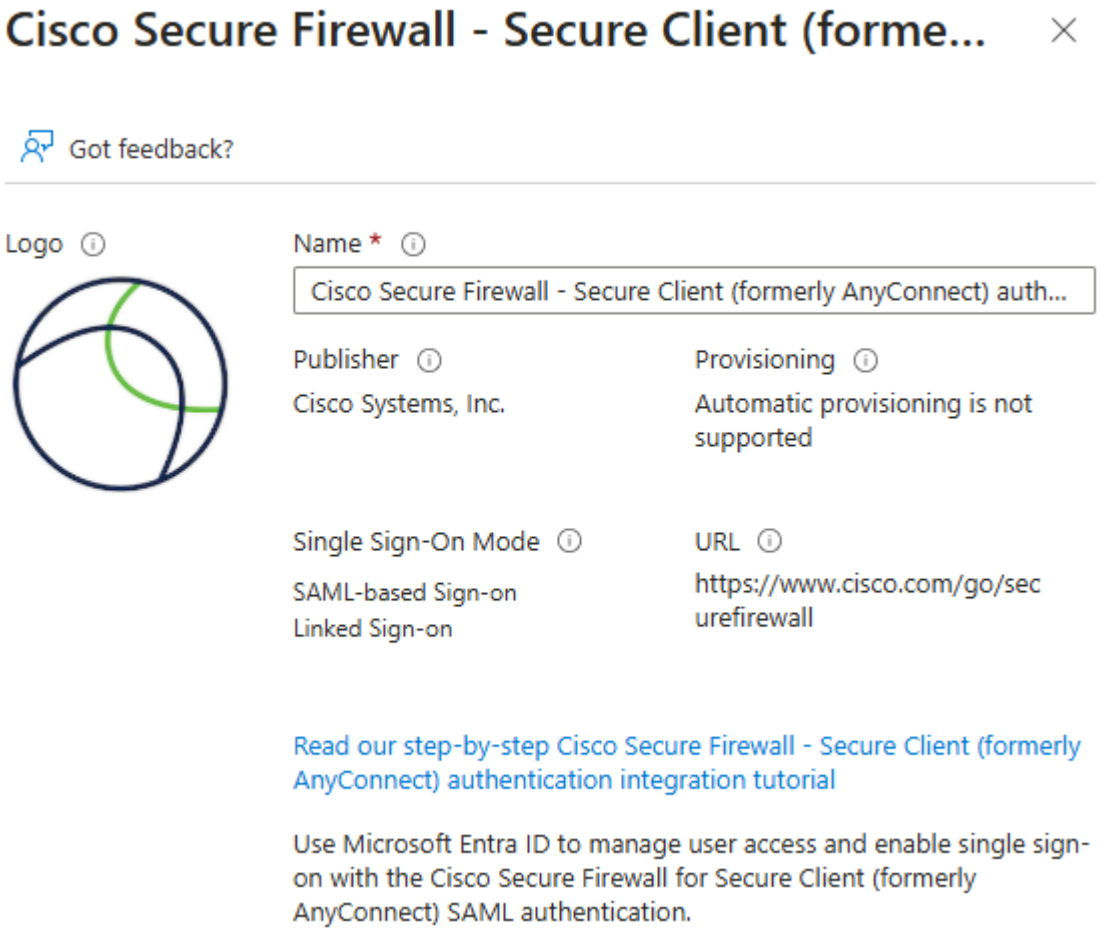
Connect > End User Connectivity > Virtual Private Network > FQDN > Global



VPN全局FQDN

2.登录到Azure并为RA VPN身份验证创建Enterprise应用程序。您可以使用名为Cisco Secure Firewall - Secure Client（以前称为AnyConnect）身份验证的预定义应用程序。

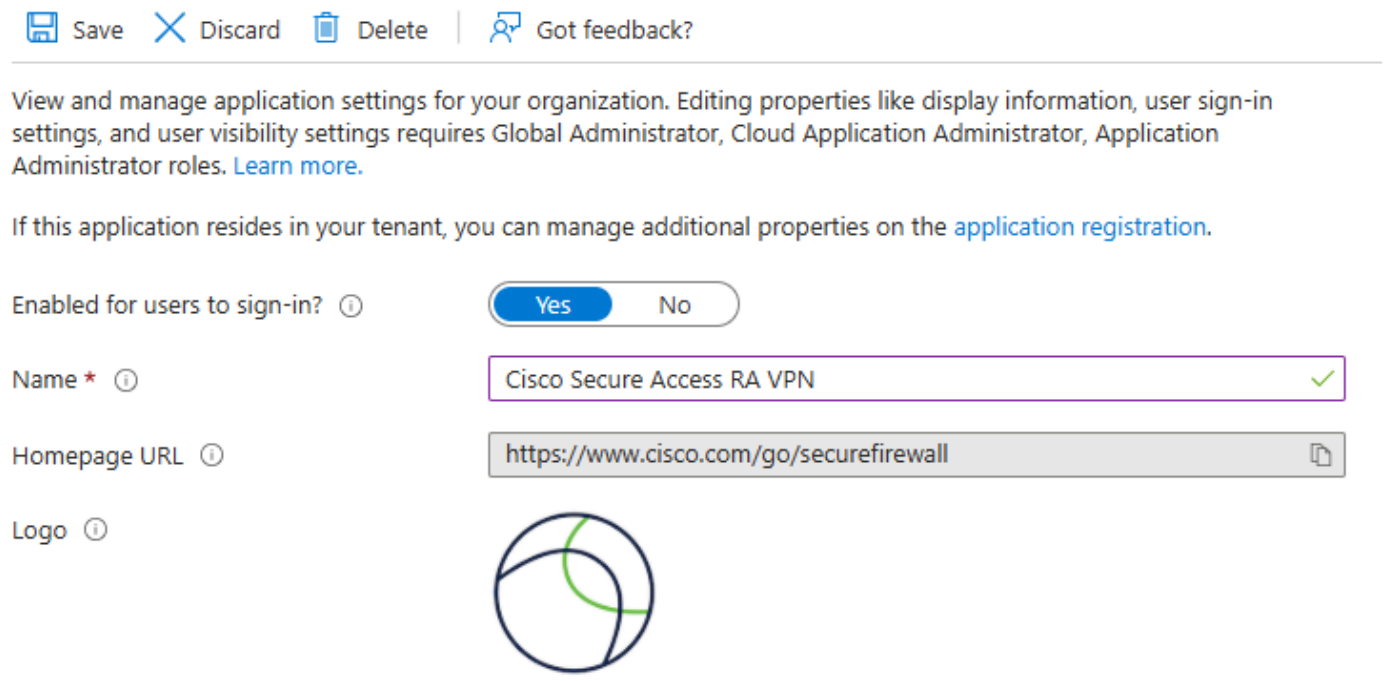
主页>企业应用>新应用>思科安全防火墙 — 安全客户端（以前称为AnyConnect）身份验证>创建



在Azure中创建应用

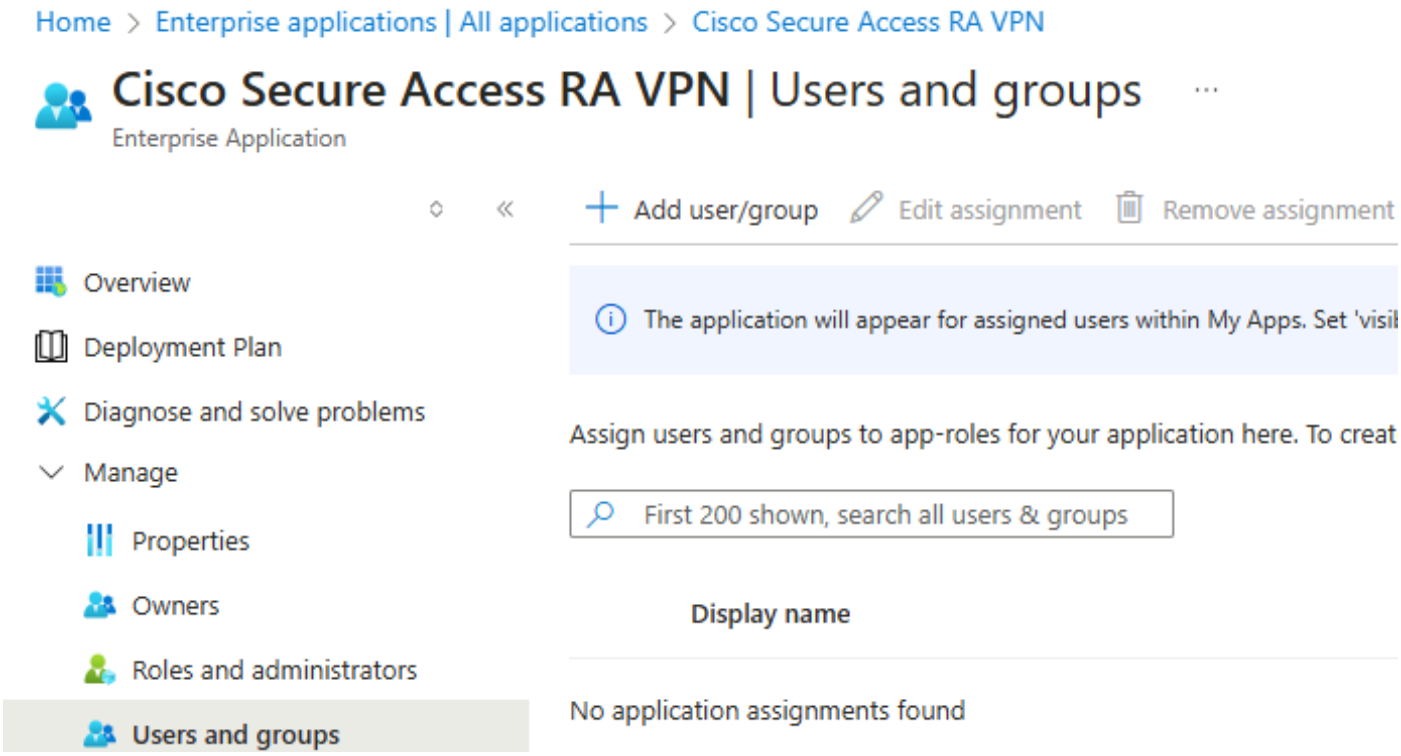
3.重命名应用程序。

Properties > Name



重命名应用程序

4.在Enterprise Application中，将用户分配为允许使用AnyConnect VPN进行身份验证。
分配用户和组> +添加用户/组>分配



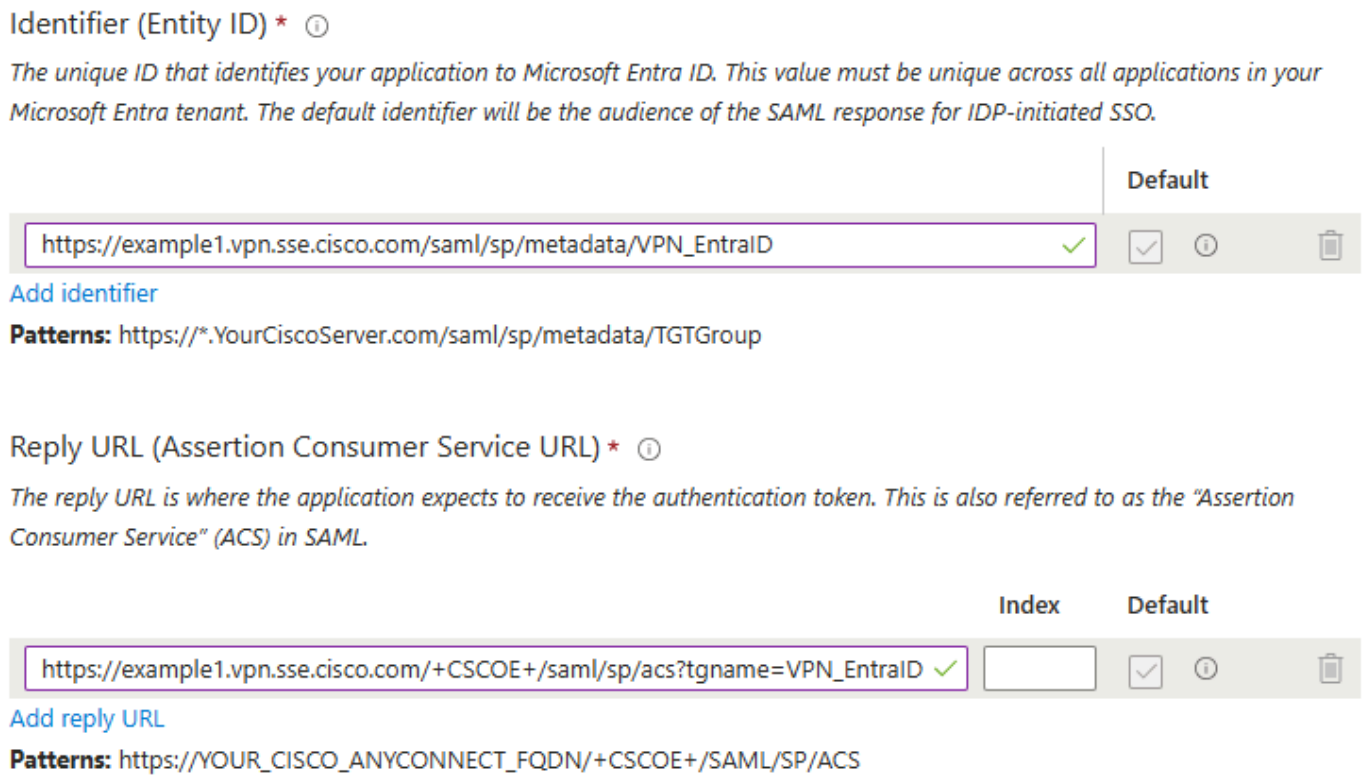
分配的用户/组

5.单击单点登录并配置SAML参数。此处使用步骤1中复制的FQDN，以及步骤2后面的“配置Cisco安全访问”中配置的VPN配置文件名称。

例如，如果将VPN全局FQDN用作example1.vpn.sse.cisco.com，并且您的思科安全访问VPN配置文件名称为VPN_EntraID，则（实体ID）和回复URL（断言消费者服务URL）的值如下：

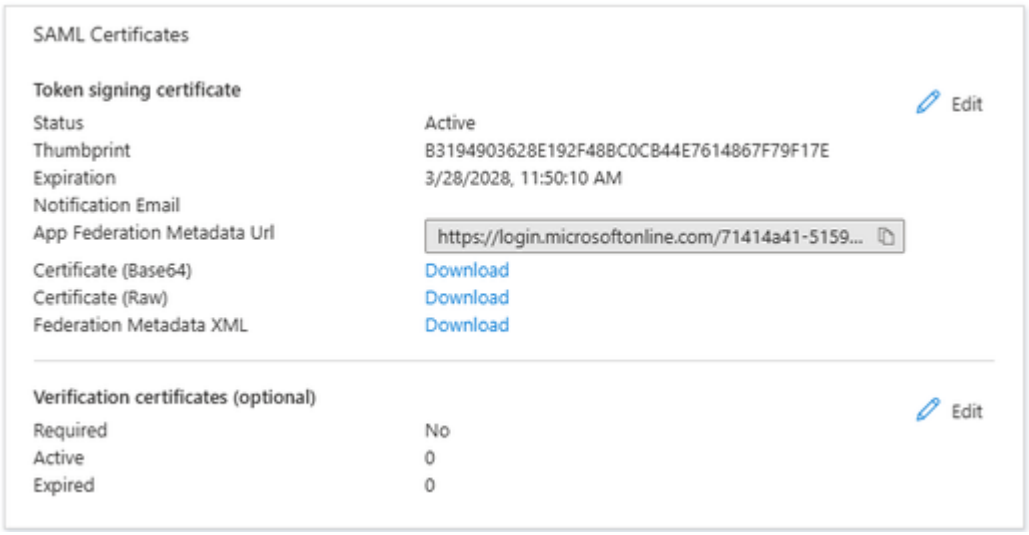
标识符（实体ID）：https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID

回复URL（断言消费者服务
URL）：https://example1.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=VPN_EntraID



Azure中的SAML参数

6.下载联合元数据XML。



思科安全访问配置

1.登录您的Cisco Secure Access控制面板，并添加IP池。

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

地区：选择要部署RA VPN的区域。
显示姓名：VPN IP池的名称。
DNS 服务器连接后，创建或分配用户用于进行DNS解析的DNS服务器。
系统IP池：Secure Access使用诸如Radius身份验证等功能，身份验证请求来自此范围内的IP。
IP池：添加新的IP池，并指定用户连接到RA VPN后获得的IP。



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

添加VPN配置文件

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池配置 — 第1部分

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

2.添加VPN配置文件。

Connect > End User Connectivity > Virtual Private Network > + VPN配置文件

常规设置



注意：VPN配置文件的名称必须与您在步骤5中的配置Azure中配置的名称匹配。在此配置指南中，您使用了VPN_EntraID，因此您将在Cisco安全访问中配置与VPN配置文件名称相同的名称。

VPN配置文件名称：此VPN配置文件的名称，仅在控制面板中可见。

显示姓名：命名最终用户在Secure Client - AnyConnect下拉菜单上看到，当连接到此RA VPN配置文件时，请参阅。
默认域:域用户一旦连接到VPN即可获得这些信息。
DNS Servers :DNS服务器VPN用户连接到VPN后即可访问。
指定的区域：使用与VPN IP池关联的DNS服务器。
指定的自定义：您可以手动分配所需的DNS。
IP 池:用户连接到VPN后分配的IP。
配置文件设置：要包括此VPN配置文件用于机器隧道或包括区域FQDN，以便最终用户选择想要连接到的区域（受所部署的IP池的制约）。
协议：选择希望VPN用户用于流量隧道的协议。
连接时间状态（可选）：如果需要，请在连接时执行VPN状态。更多信息请点击此处

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配置文件配置 — 第1部分

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.

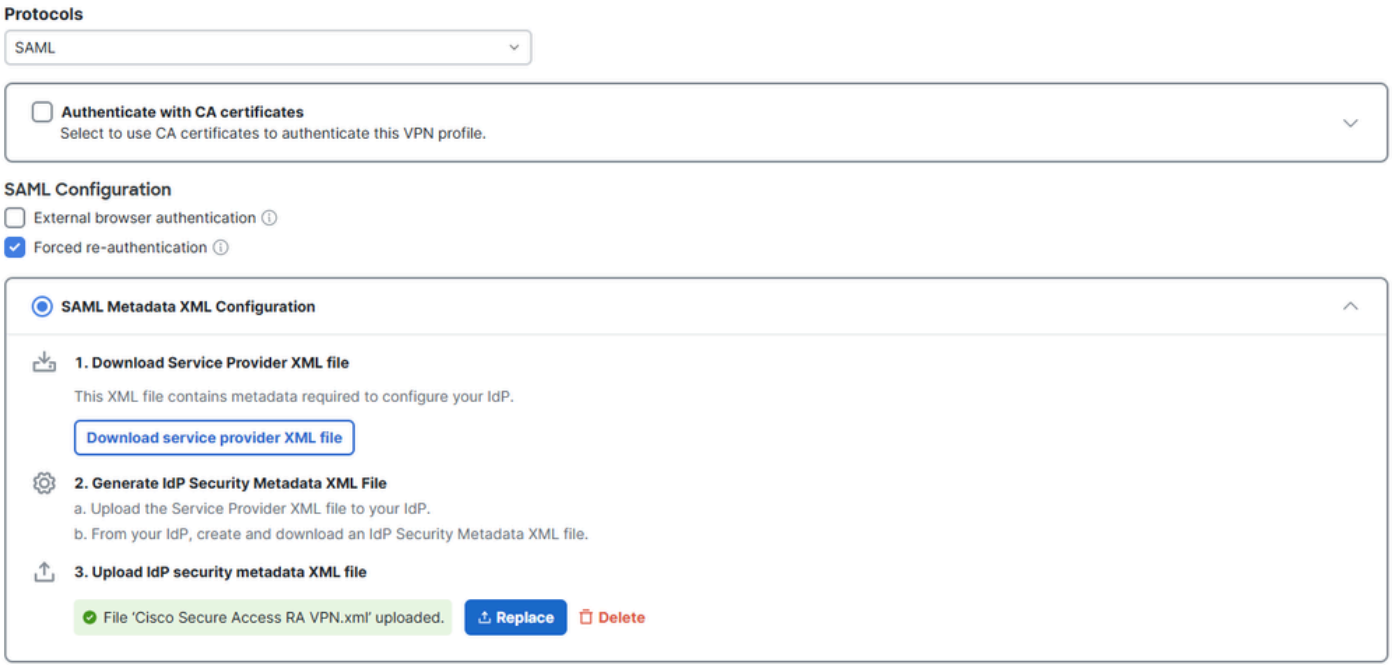
VPN配置文件配置 — 第2部分

验证、授权和记帐

协议：选择SAML。

使用CA证书进行身份验证：如果您想要使用SSL证书进行身份验证并根据IdP SAML提供程序进行授权。
强制重新身份验证：每当建立VPN连接时都会强制重新进行身份验证。强制重新身份验证基于会话超时。这可以接受SAML IdP设置（本例中为Azure）。

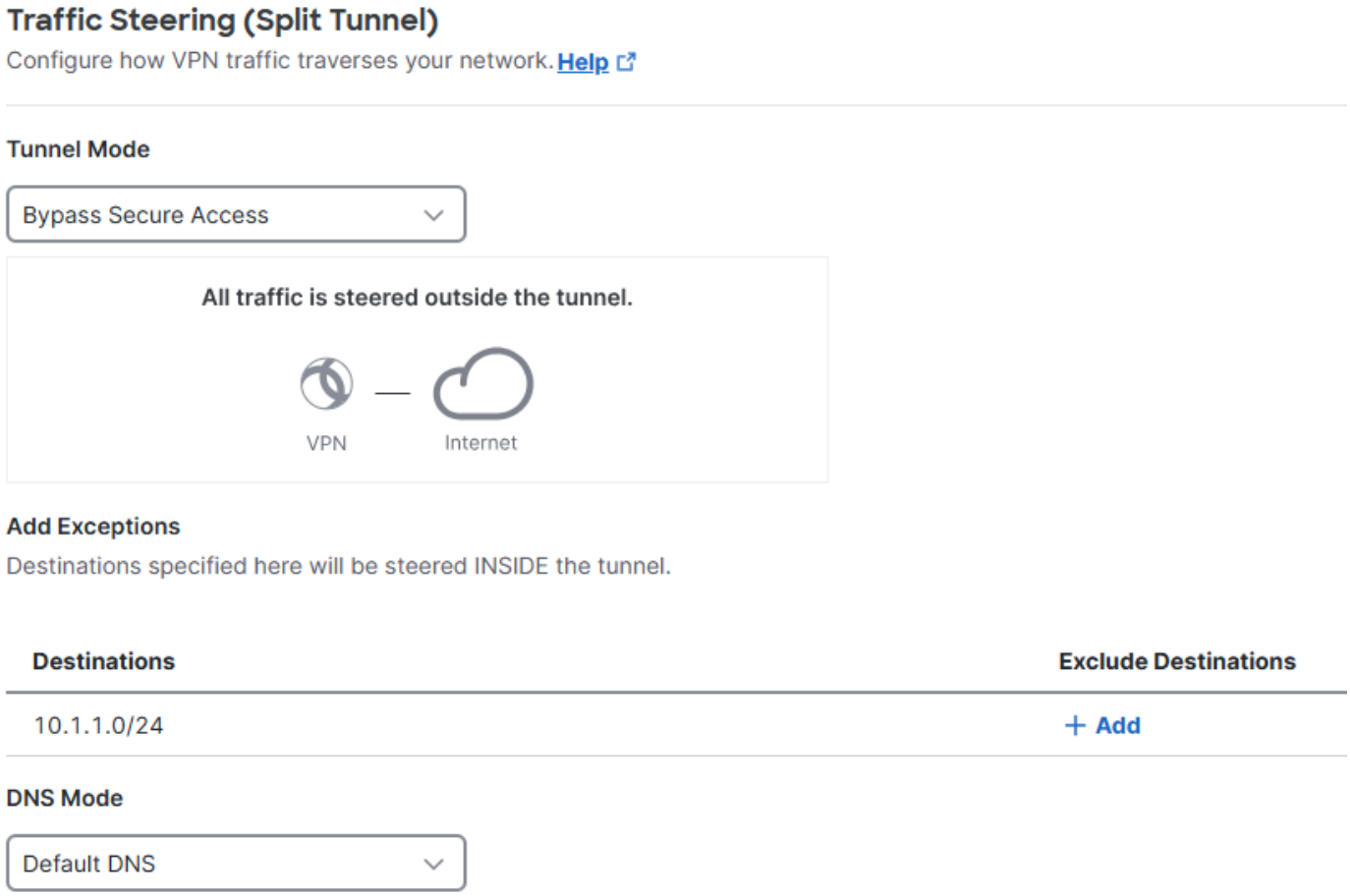
上传在步骤6中的“配置Azure”中下载的XML文件联合元数据XML文件。



SAML配置

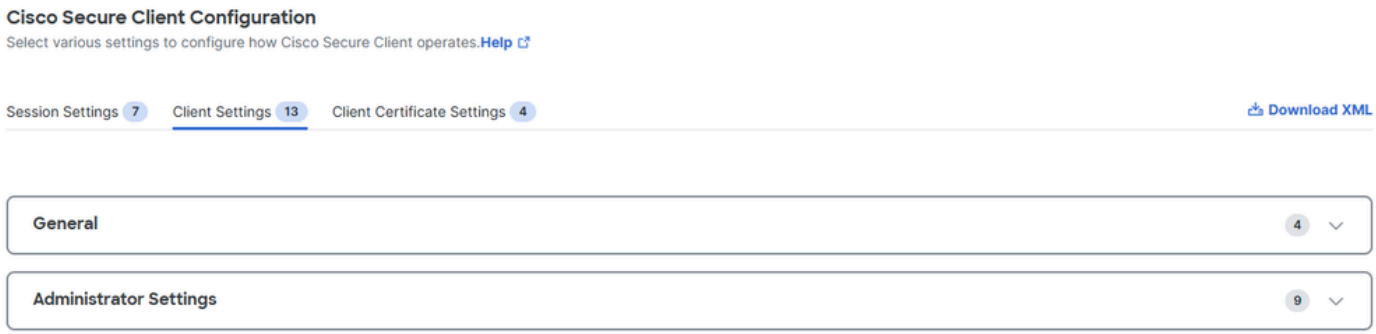
流量引导（分割隧道）

通道模式:
　连接到安全访问：所有流量通过隧道(Tunnel All)发送。
　绕过安全访问：仅在例外情况部分中定义的特定流量通过隧道传输（拆分隧道）。
DNS模式：
　默认DNS:所有DNS查询都通过VPN配置文件定义的DNS服务器。如果出现否定响应，DNS查询还可以转到物理适配器上配置的DNS服务器。
　所有DNS隧道：通过VPN隧道传输所有DNS查询。
　Split DNS:只有特定的DNS查询会通过VPN配置文件，具体取决于下面指定的域。



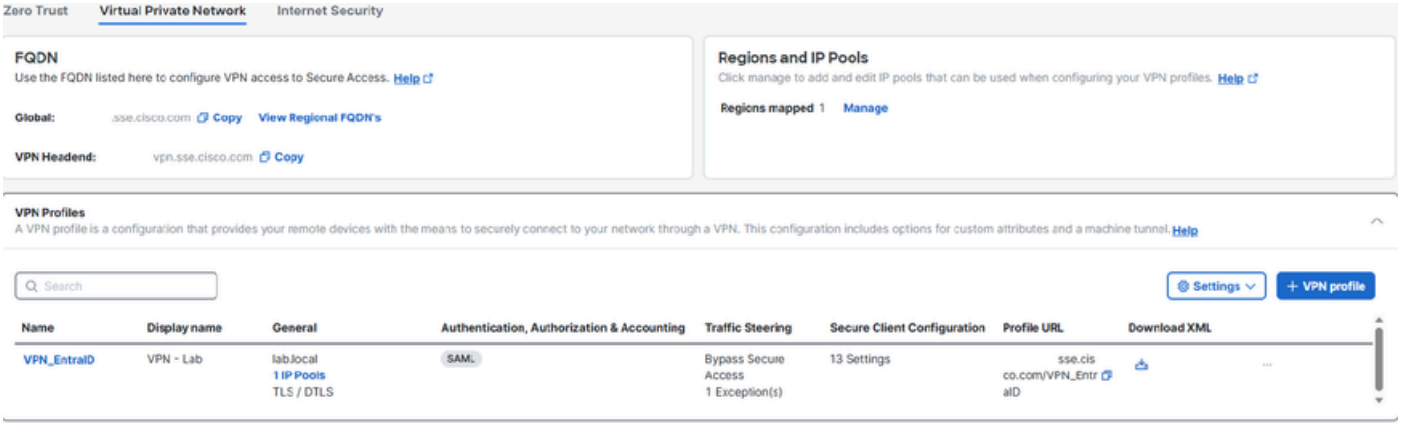
流量引导配置

思科安全客户端配置
在本指南中，您不会配置任何这些高级设置。可在此处配置高级功能。例如：TND、永远在线、证书匹配、本地LAN访问等。请在此处保存设置。



高级设置

3.您的VPN配置文件必须如下所示。您可以将xml配置文件下载并预部署给最终用户（在C:\ProgramData\Cisco\Cisco安全客户端\VPN\Profile下），以开始使用VPN，或向他们提供要在Cisco安全客户端 — AnyConnect VPN UI中输入的配置文件URL。



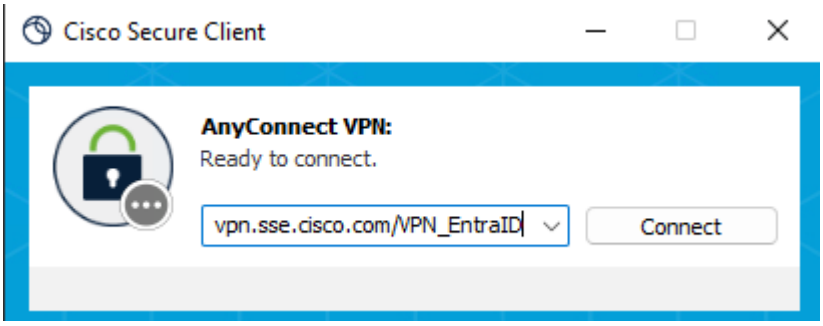
全局FQDN和配置文件URL

验证

此时，您的RA VPN配置必须准备好进行测试。
请注意，用户首次连接时，需要为其提供配置文件URL地址或在其个人电脑中预部署XML配置文件（位于C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile下），重新启动VPN服务，并且他们必须在下拉菜单中看到连接到此VPN配置文件的选项。

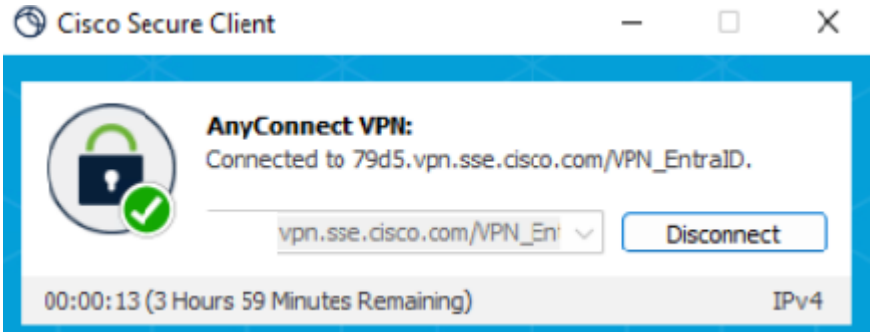
在本例中，您将配置文件URL地址提供给用户进行首次连接尝试。

在第一个连接之前：



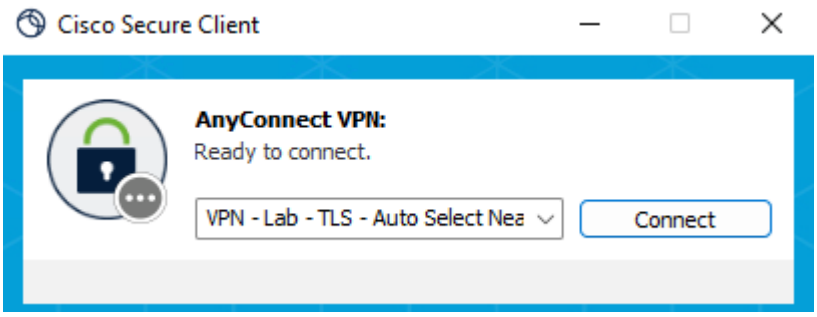
以前的VPN连接

输入您的凭证并连接到VPN:



已连接到VPN

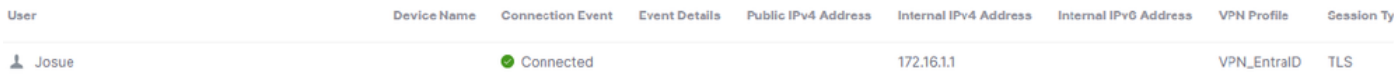
首次连接后，从下拉菜单中，您必须能够看到用于连接到VPN — 实验室VPN配置文件的选项：



在第一个VPN连接之后

签入用户能够连接的远程访问日志：

Monitor > Remote Access Log



登录思科安全访问

故障排除

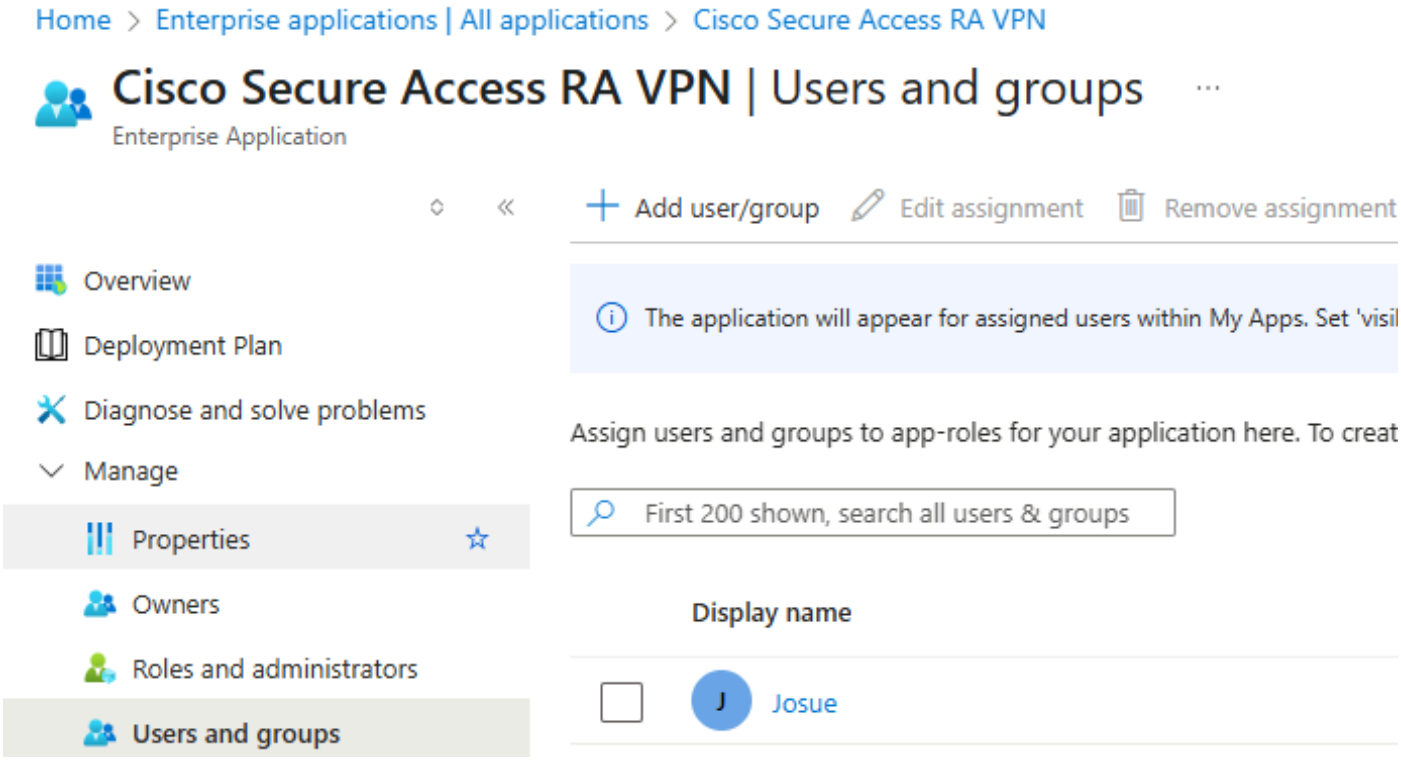
以下是一些常见问题可以执行的基本故障排除：

Azure

在Azure中，确保已将用户分配到为根据思科安全访问进行身份验证而创建的企业应用：

主页(Home)>企业应用(Enterprise Applications)>思科安全访问RA VPN(Cisco Secure Access

RA VPN)>管理(Manage)>用户和组(Users and Groups)

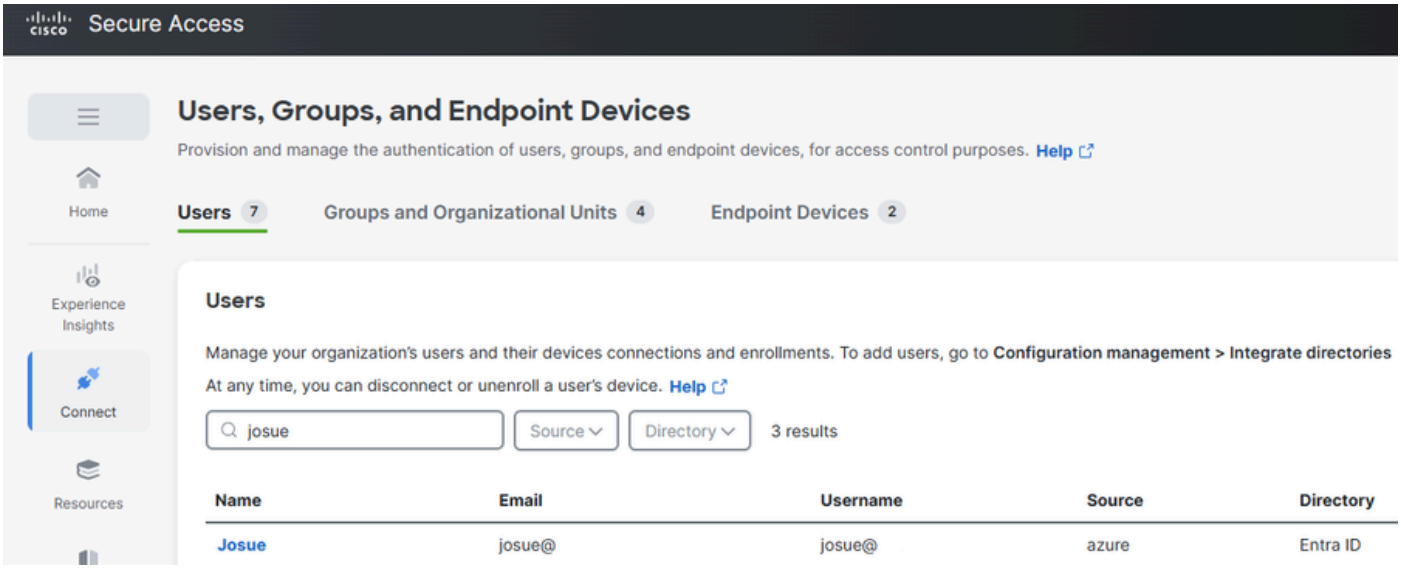


验证用户分配

思科安全访问

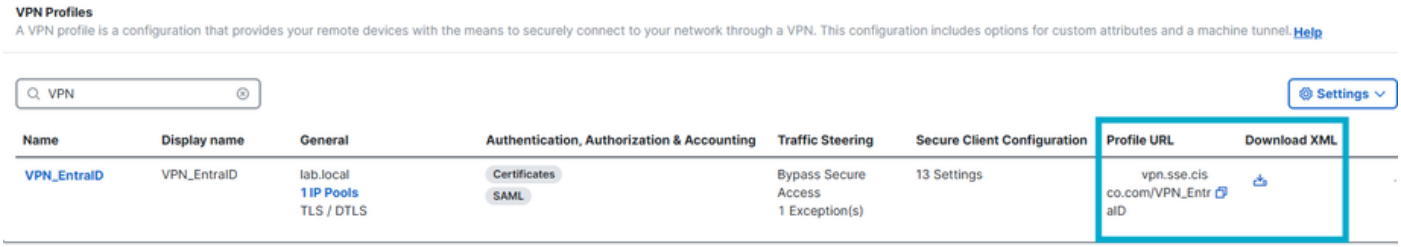
在Cisco Secure Access中，请确保已调配允许通过RA VPN连接的用户，并且Cisco Secure Access中调配的用户（在用户、组和终端设备下）与Azure中的用户（在企业应用中分配的用户）匹配。

Connect > Users、Groups和Endpoint Devices



按照Verify步骤中的说明，验证用户已在PC上调配了正确的XML文件，或已为该用户提供了配置文件URL。

Connect > End User Connectivity > Virtual Private Network



配置文件URL和.xml配置文件

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。