Configurar o Cisco Secure Access para RA VPNaaS com Entra ID

Contents

Introdução

Este documento descreve passo a passo como configurar o RA VPN no Cisco Secure Access para autenticar em Entra ID.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento usando a ID do Azure/Entra.
- Conhecimento sobre o Cisco Secure Access.

Requisitos

Estes requisitos devem ser cumpridos antes de prosseguir:

- Acesse seu painel do Cisco Secure Access como administrador total.
- Acesso ao Azure como Administrador.
- Provisionamento de usuário já concluído para o Cisco Secure Access.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Access Dashboard (Painel de acesso seguro da Cisco).
- Portal do Microsoft Azure.

- Cisco Secure Client AnyConnect VPN versão 5.1.8.105

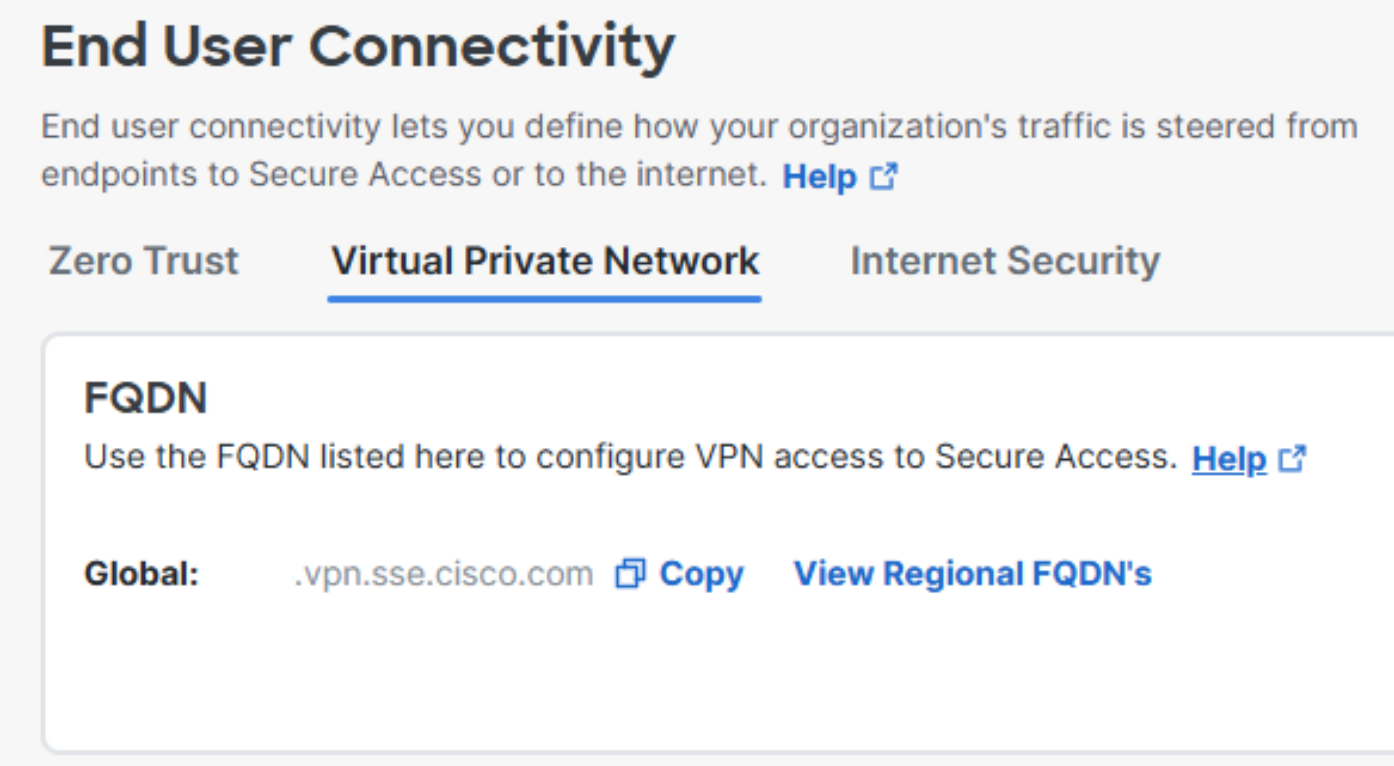
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Configuração do Azure

1. Faça login no painel do Cisco Secure Access e copie o FQDN global da VPN. Estamos usando este FQDN na configuração do Aplicativo Empresarial do Azure.

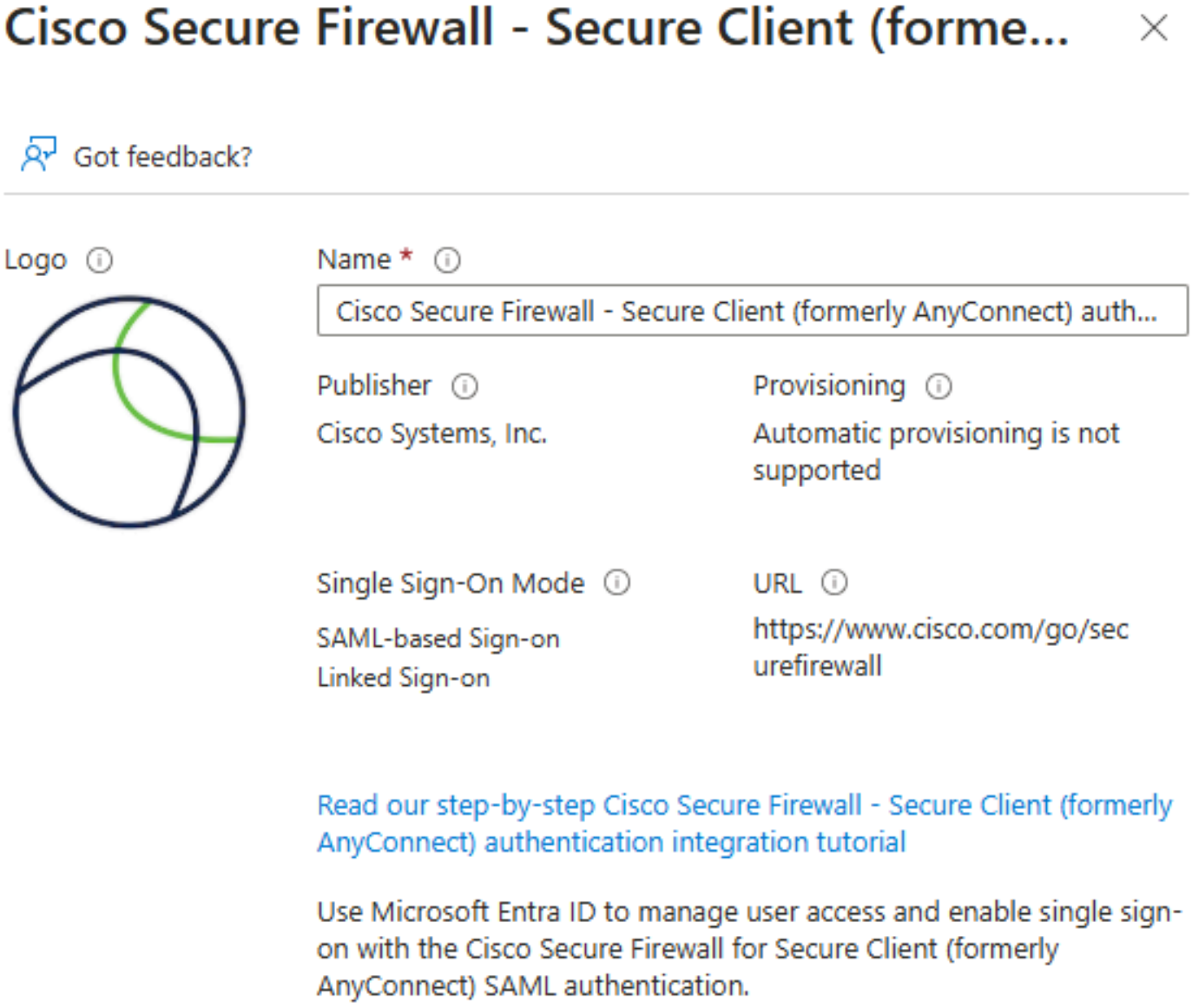
Conectar > Conectividade de Usuário Final > Rede Virtual Privada > FQDN > Global



FQDN global de VPN

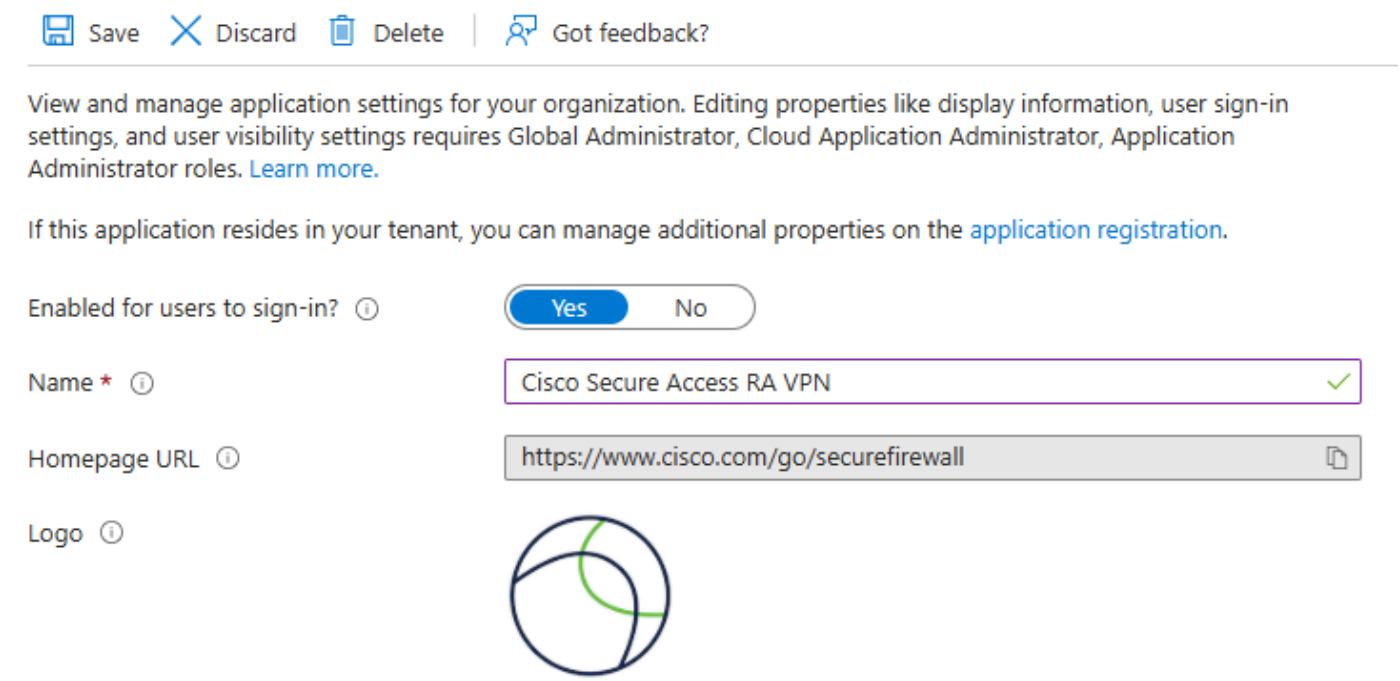
2. Faça logon no Azure e crie um aplicativo empresarial para a autenticação VPN do RA. Você pode usar o aplicativo predefinido chamado "Cisco Secure Firewall - Secure Client (anteriormente AnyConnect) authentication".

Home > Aplicativos corporativos > Novo aplicativo > Cisco Secure Firewall - Autenticação Secure Client (anteriormente AnyConnect) > Criar



Criar Aplicativo no Azure

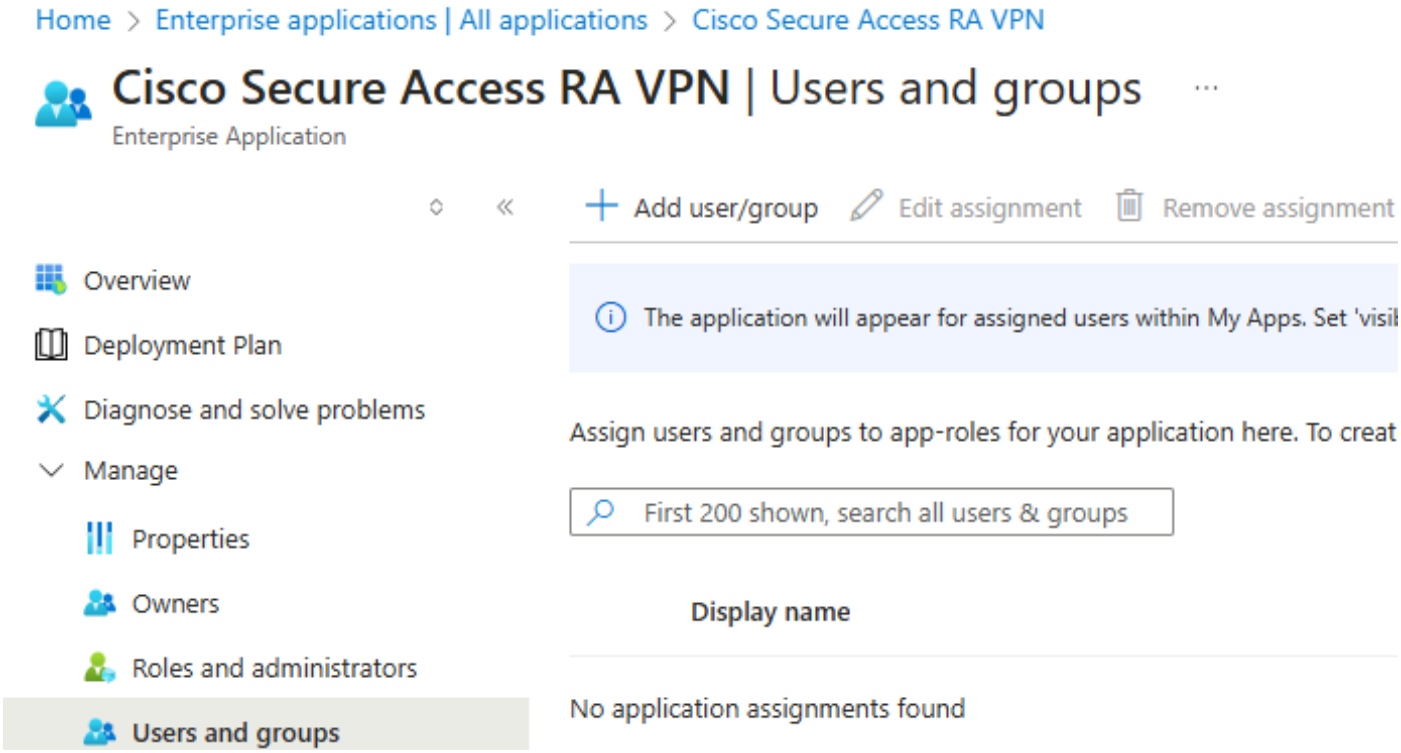
3. Renomeie o Aplicativo.
   Propriedades > Nome



Renomear o aplicativo

4. No aplicativo empresarial, atribua os usuários que permitem a autenticação usando o AnyConnect VPN.

Atribuir usuários e grupos > + Adicionar usuário/grupo > Atribuir

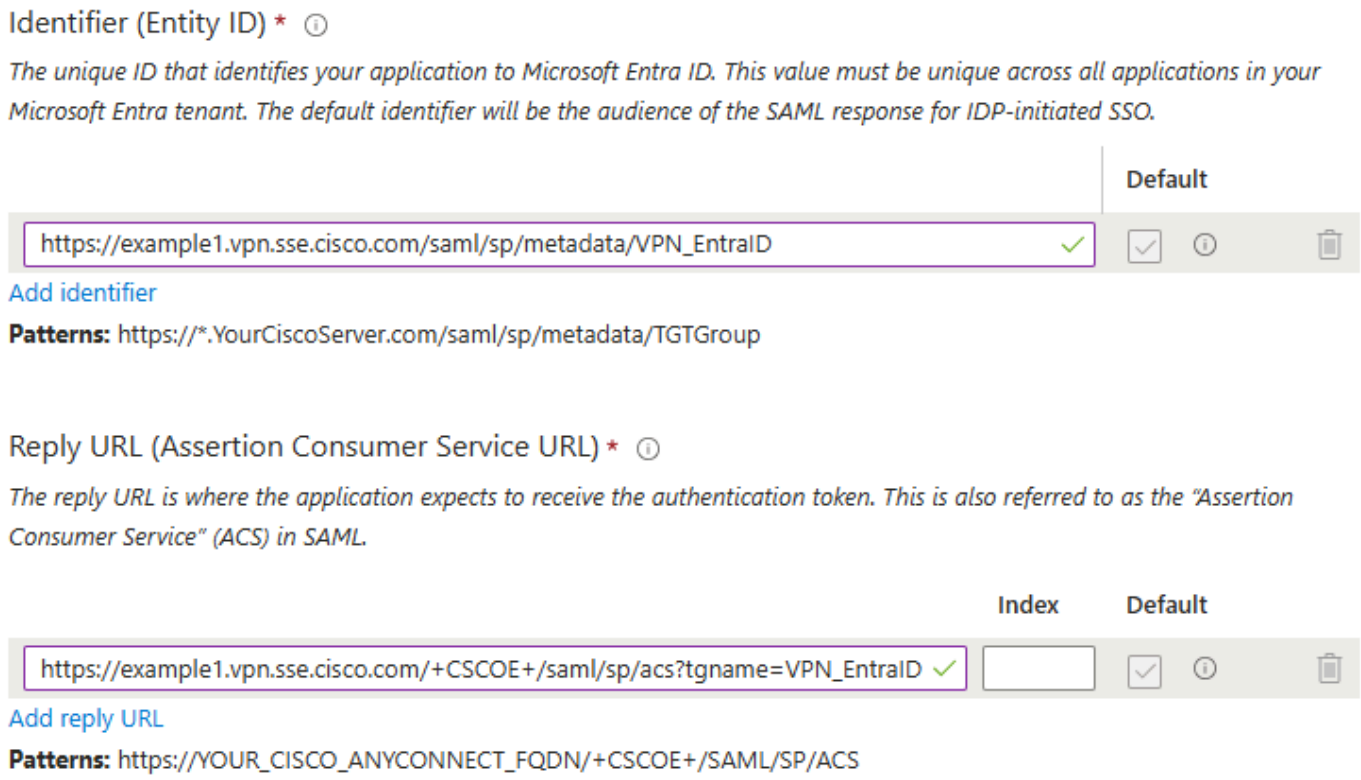


Usuários/Grupos Atribuídos

5. Clique em Logon único e configure os parâmetros SAML. Aqui, usamos o FQDN copiado na etapa 1 e também o nome do Perfil VPN que você está configurando em "Configuração do Cisco Secure Access", mais adiante na etapa 2.

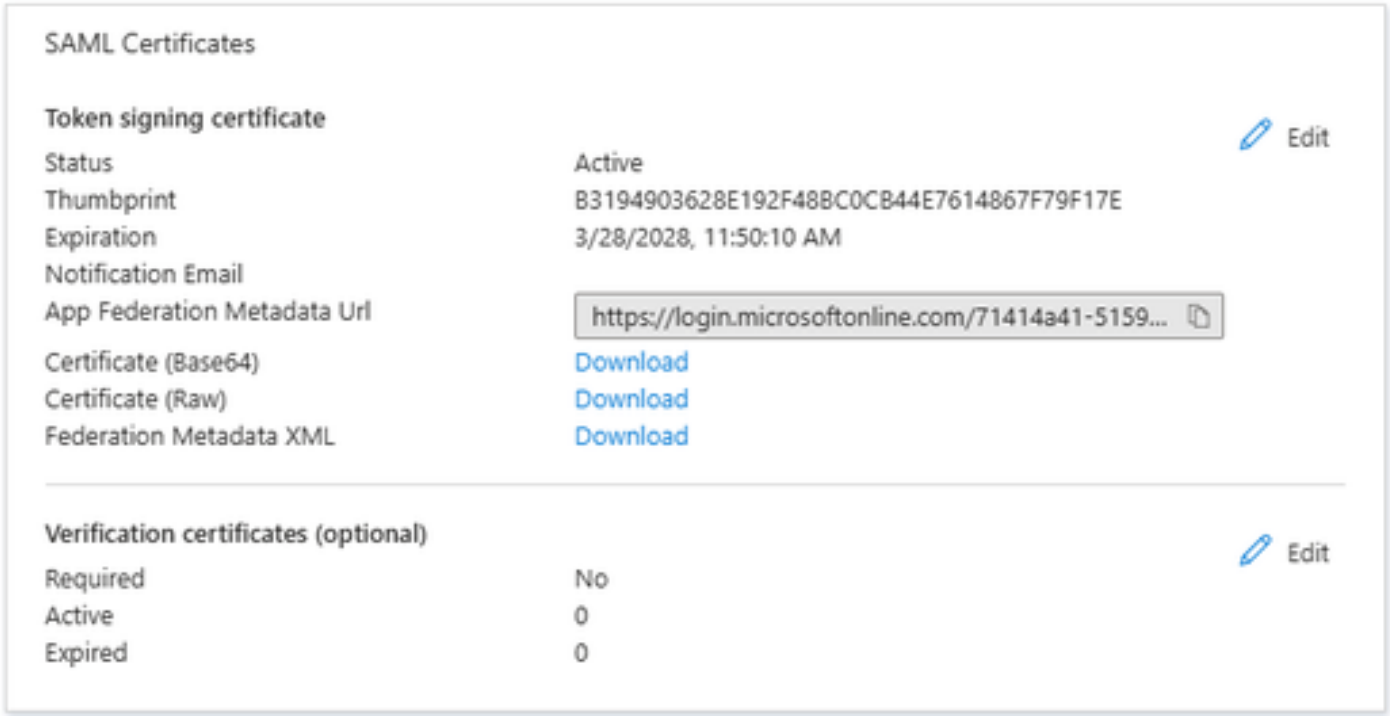
Por exemplo, se o FQDN global da VPN for example1.vpn.sse.cisco.com e o nome do perfil da VPN de acesso seguro da Cisco for VPN_EntraID, os valores de (ID da entidade) e URL de resposta (URL do serviço do consumidor de asserção) serão:

Identificador (ID da entidade):
https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID
URL de Resposta (URL do Serviço de Consumidor de Asserção):
https://example1.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=VPN_EntraID



Parâmetros SAML no Azure

6. Baixe o XML de Metadados da Federação.



Configuração do Cisco Secure Access

1. Inicie a sessão no painel do Cisco Secure Access e adicione um IP Pool.

Conectar > Conectividade do Usuário Final > Rede Virtual Privada > Adicionar Pool de IPs

Região: Selecione a região onde sua VPN RA será implantada.
Nome de exibição: O nome do Pool de IPs da VPN.
Servidor DNS: Crie ou atribua o Servidor DNS que os usuários estão usando para a resolução DNS depois de conectados.
Pool de IPs do Sistema: Usado pelo Secure Access para recursos como a Autenticação Radius, a Solicitação de Autenticação é originada por um IP dentro desse intervalo.
Pool IP: Adicione um novo Pool de IPs e especifique os IPs que os usuários obterão quando estiverem conectados à VPN do RA.

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

Adicionar perfil de VPN

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

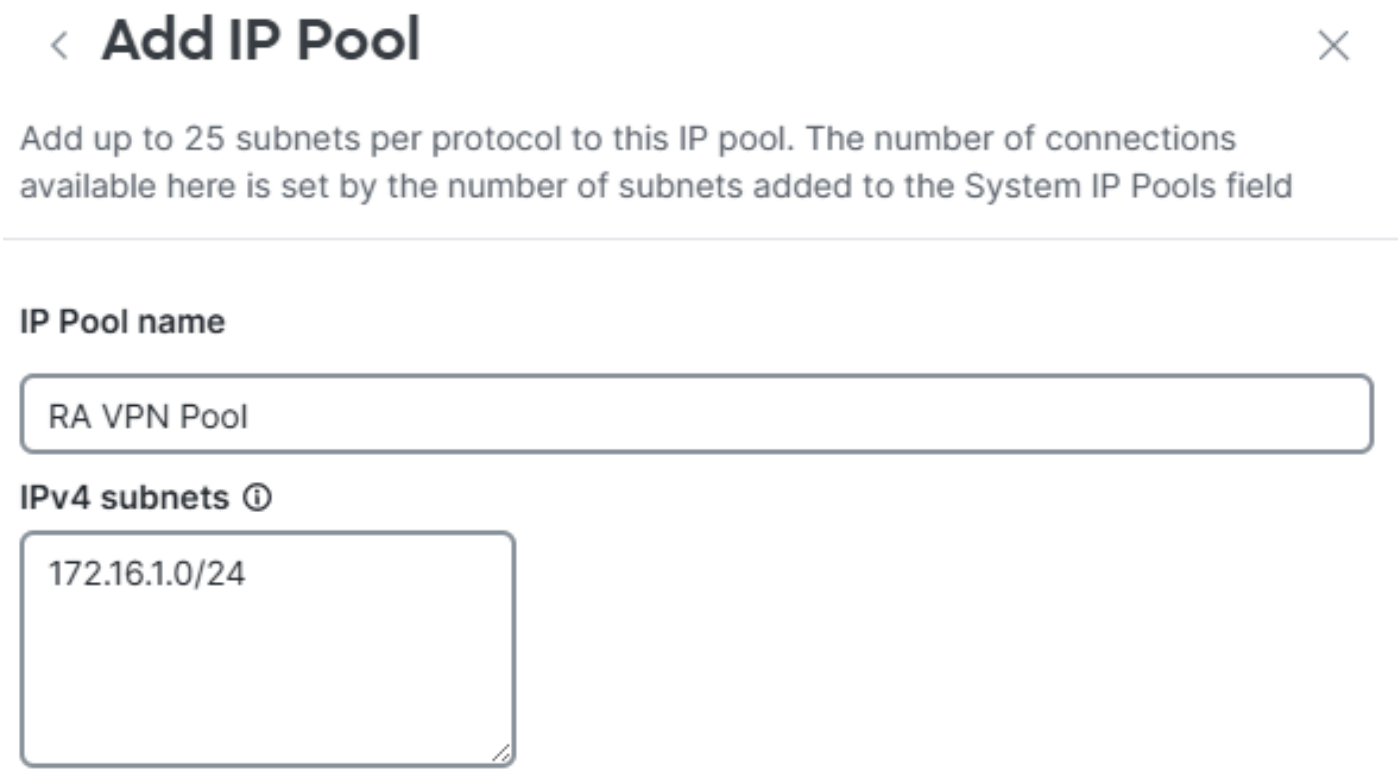
172.16.2.0/24

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

Configuração do pool de IPs - Parte 1

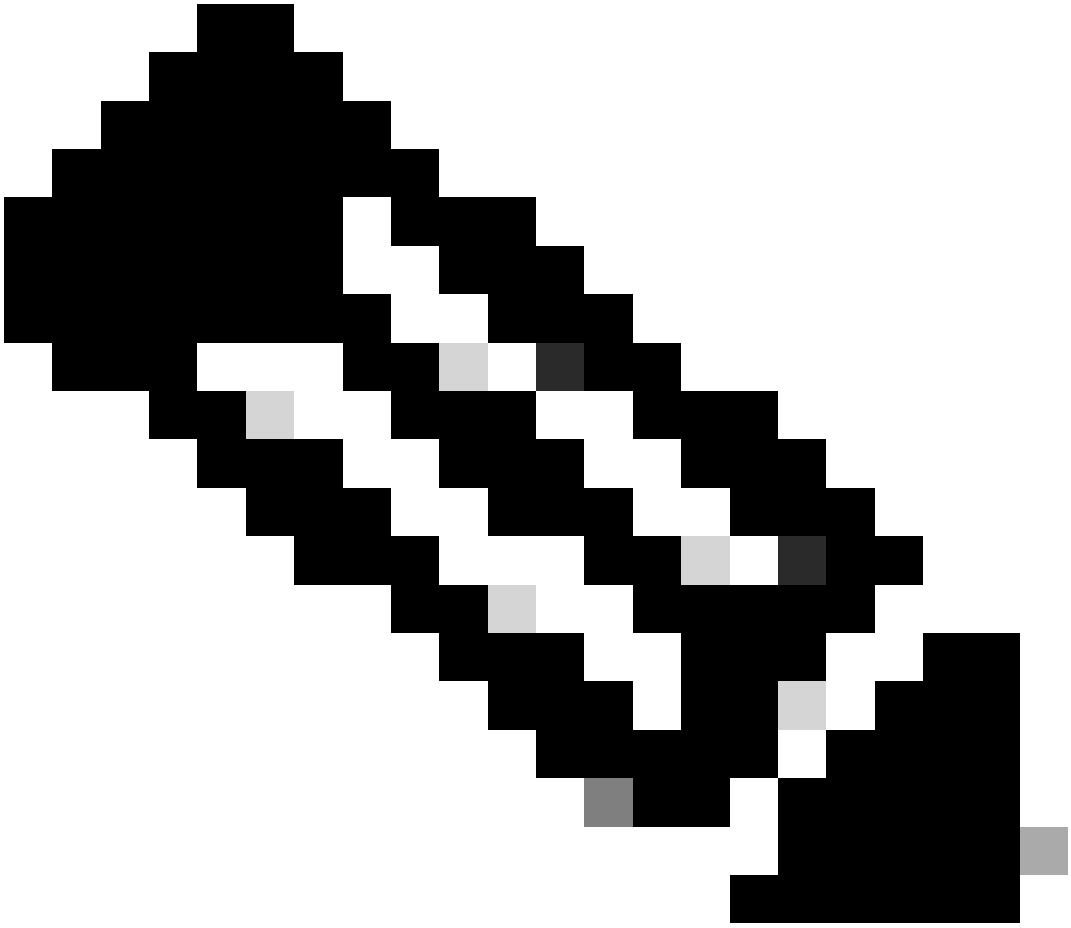


Configuração do pool de IPs - Parte 2

2. Adicione um Perfil de VPN.

Conectar > Conectividade do usuário final > Rede virtual privada > + Perfil de VPN

Configurações gerais

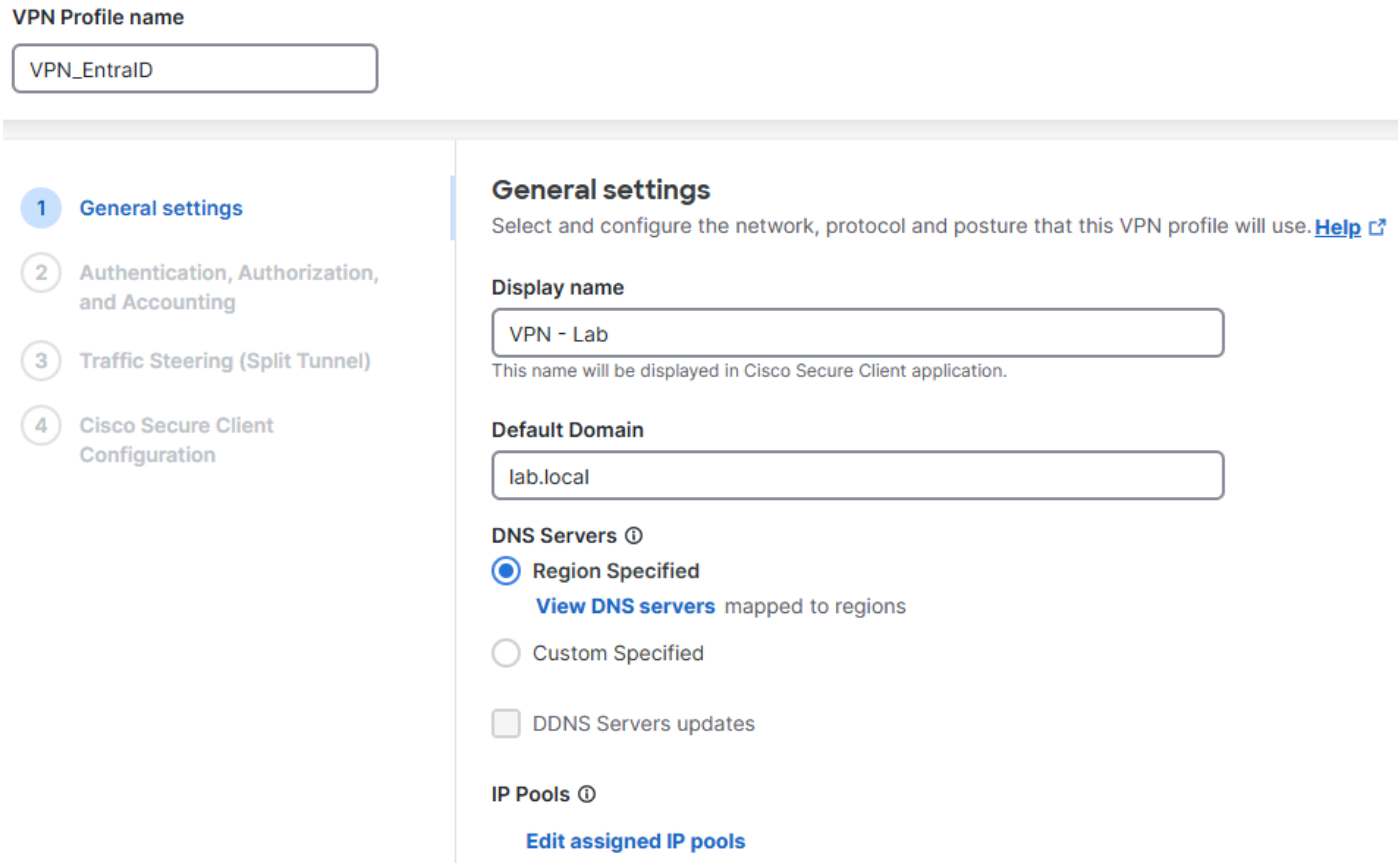


Note: Note: O nome do Perfil de VPN deve corresponder ao nome que você configurou em "Configuração do Azure" na etapa 5. Neste guia de configuração, usamos VPN_EntraID para que estejamos configurando o mesmo no Cisco Secure Access que o nome do Perfil de VPN.

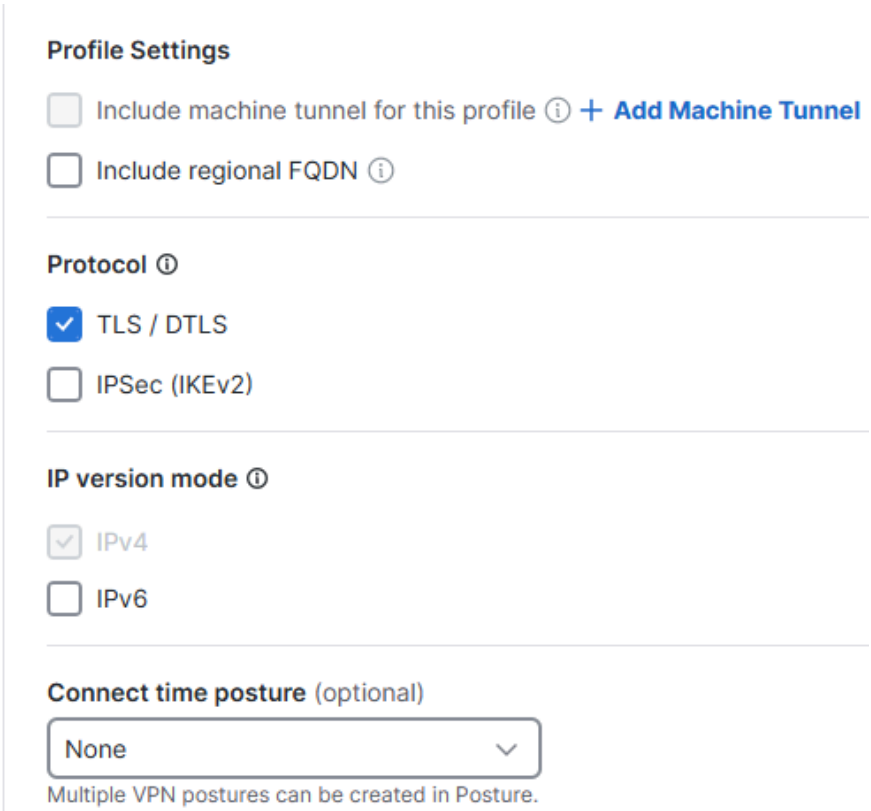
Nome do perfil VPN: Nome para este Perfil VPN, visível somente no painel.

Nome de exibição: O nome que os usuários finais veem no menu suspenso "Secure Client - Anyconnect" ao se conectarem a este Perfil de VPN do RA.
Domínio padrão: Os usuários do domínio são conectados à VPN uma vez.
Servidores DNS: Servidor DNS que os usuários da VPN obtêm uma vez conectados à VPN.
Região Especificada: Usa o servidor DNS associado ao Pool IP da VPN.
Especificado pelo cliente: Você pode atribuir manualmente o DNS desejado.
Pools IP: Os IPs dos usuários são atribuídos depois de conectados à VPN.
Configurações de perfil: Incluir esse perfil de VPN para o túnel da máquina ou incluir o FQDN regional para que o usuário final selecione a região à qual deseja se conectar (está sujeita aos pools de IP implantados).

Protocolos Selecione o protocolo que você deseja que seus Usuários VPN usem para o tunelamento do tráfego.
Possibilidade de tempo de conexão (opcional): Se for necessário fazer VPN Posture no momento da conexão. Mais informações aqui



Configuração do perfil VPN - Parte 1

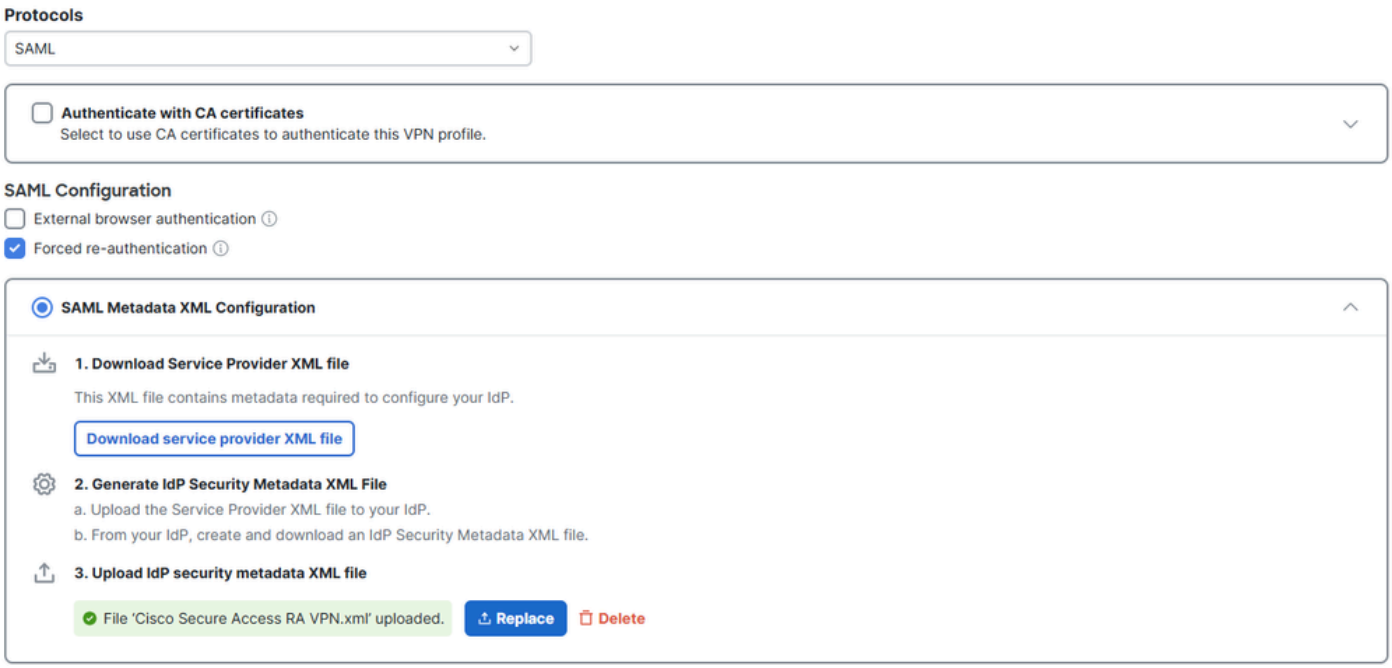


Autenticação, autorização e contabilidade

Protocolos Selecione SAML.

Autenticação com certificados CA: Caso deseje se autenticar usando um Certificado SSL e autorizar em um Provedor IdP SAML.
Forçar reautenticação: Força uma nova autenticação sempre que uma conexão VPN é feita. A reautenticação forçada baseia-se no tempo limite da sessão. Isso pode estar sujeito às configurações de IdP SAML (Azure neste caso).

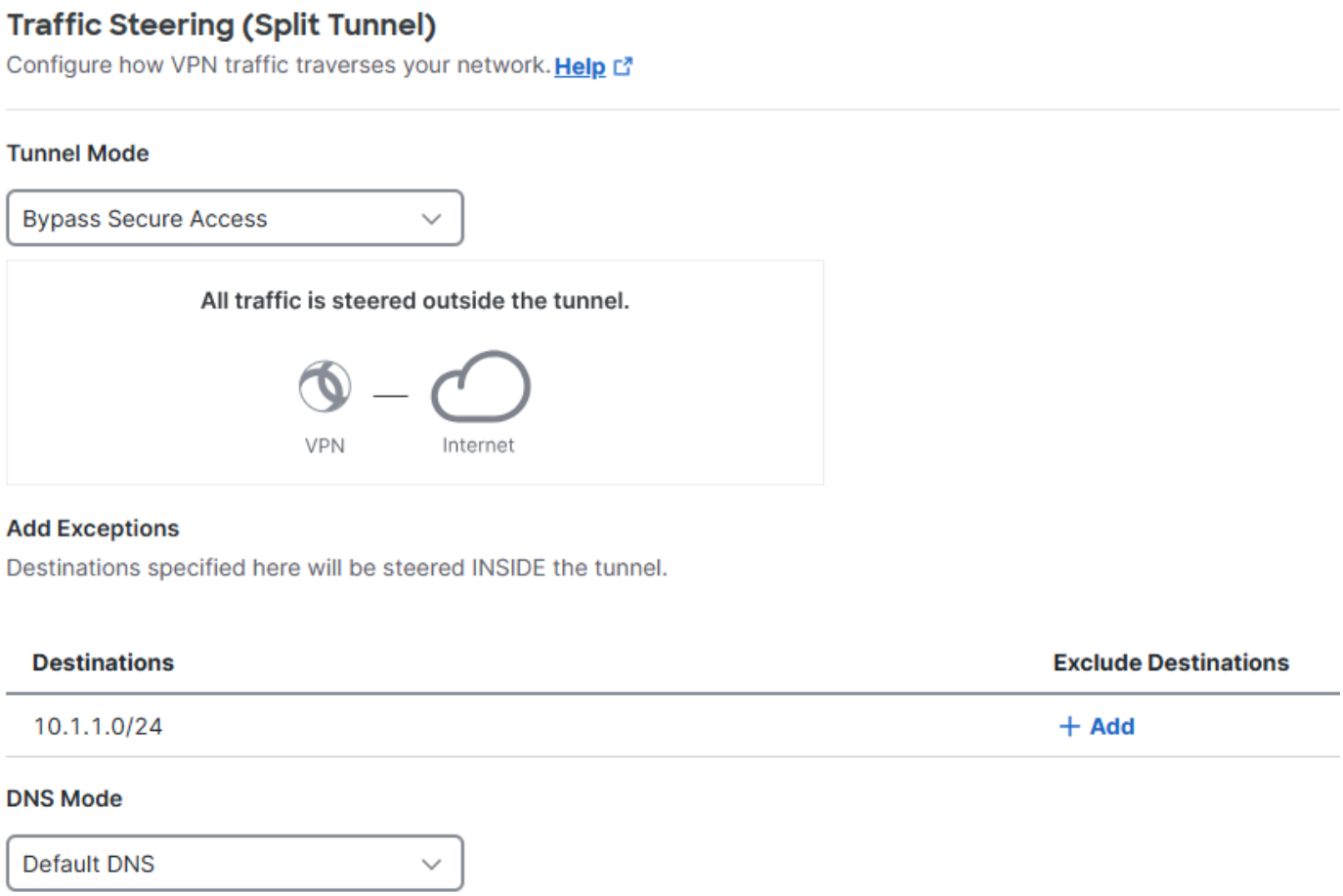
Carregue o arquivo XML de Metadados de Federação do arquivo XML baixado em "Configurar Azure" na etapa 6.



Configuração SAML

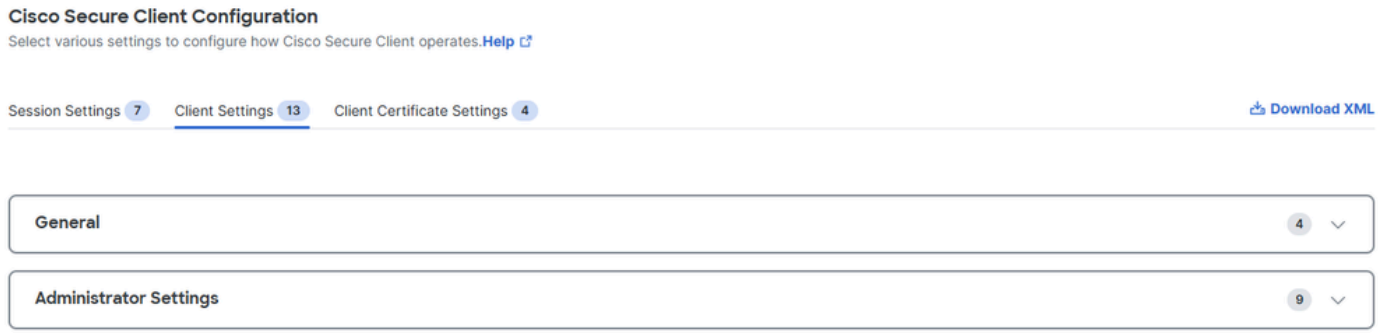
Direção de tráfego (túnel dividido)

Módo de túnel:
Conectar-se ao acesso seguro: Todo o tráfego é enviado pensando no túnel (Tunnel All).
Ignorar acesso seguro: Apenas o tráfego específico definido na seção Exceções é encapsulado (túnel dividido).
Modo DNS:
DNS padrão: Todas as consultas DNS se movem pelos servidores DNS que são definidos pelo Perfil VPN. No caso de uma resposta negativa, as consultas DNS também podem ir para os servidores DNS que estão configurados no adaptador físico.
Encapsulamento de todos os DNS: Encapsula todas as consultas DNS através da VPN.
DNS dividido: Apenas consultas específicas de DNS se movem pelo perfil de VPN, dependendo dos domínios especificados abaixo.



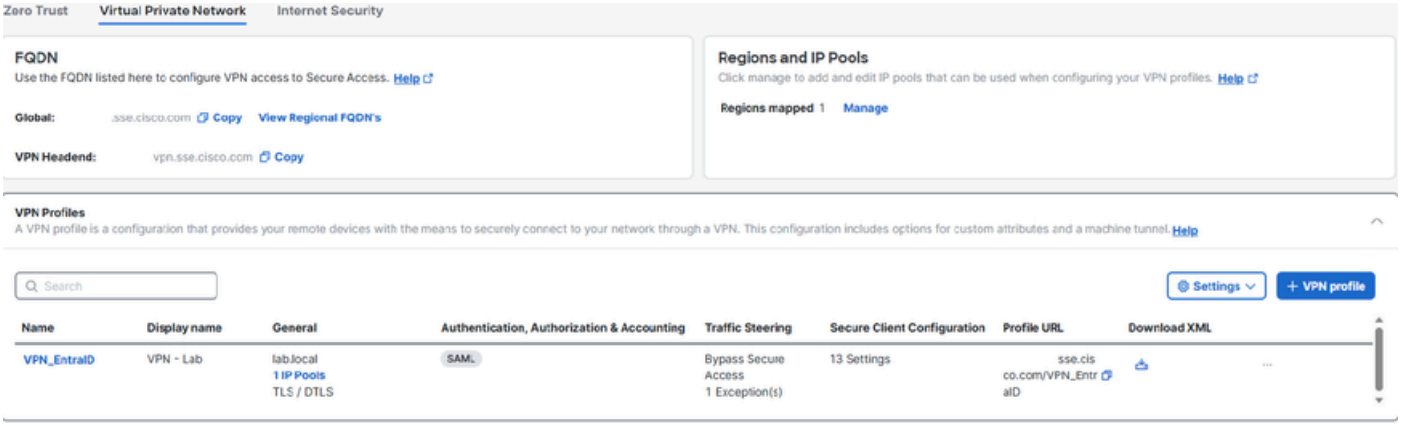
Configuração de direção de tráfego

Configuração do Cisco Secure Client
Para os fins deste guia, não estamos definindo nenhuma dessas configurações avançadas. Os recursos avançados podem ser configurados aqui, por exemplo: TND, Sempre ativo, Correspondência de certificado, Acesso à LAN local, etc. Salve as configurações aqui.



Configurações avançadas

3. Seu Perfil VPN deve ser semelhante a este. Você pode baixar e pré-implantar o perfil xml para os usuários finais (em "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile") para começar a usar a VPN ou fornecer a eles a URL do perfil a ser inserida na interface do usuário do Cisco Secure Client - AnyConnect VPN.



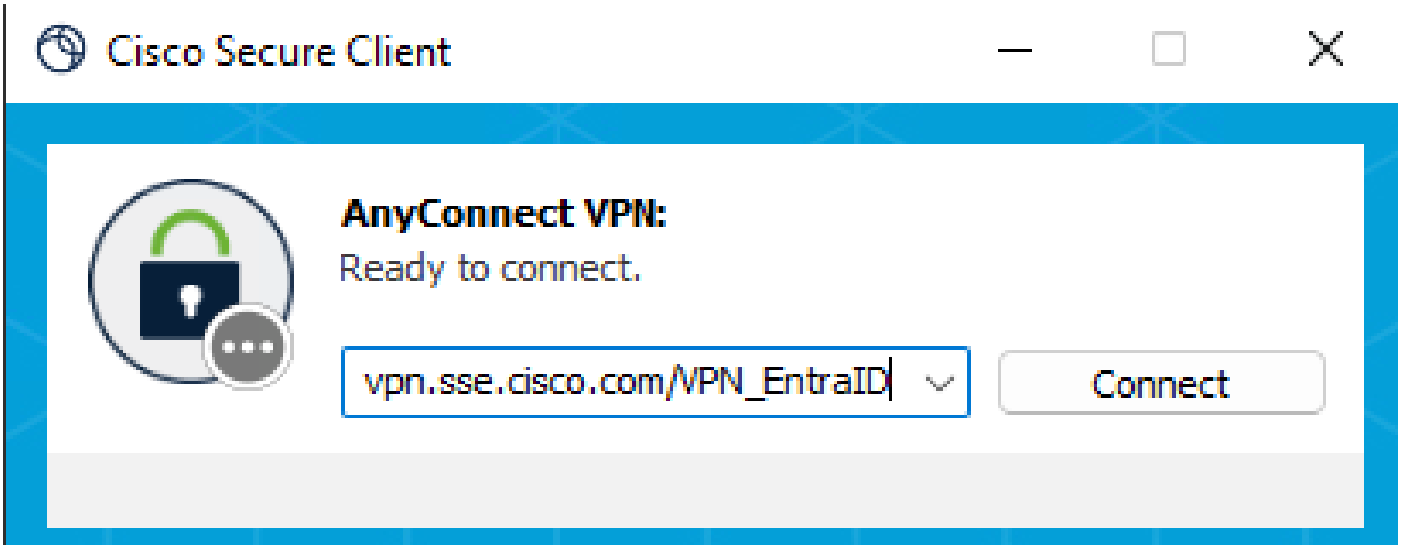
FQDN global e URL de perfil

Verificar

Neste ponto, a configuração da VPN do RA deve estar pronta para o teste.
Observe que na primeira vez que os usuários se conectam, eles precisam receber o endereço URL do perfil ou pré-implantar o perfil xml em seus PCs em "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile", reiniciar o serviço VPN e eles devem ver no menu suspenso a opção para se conectar a este perfil VPN.

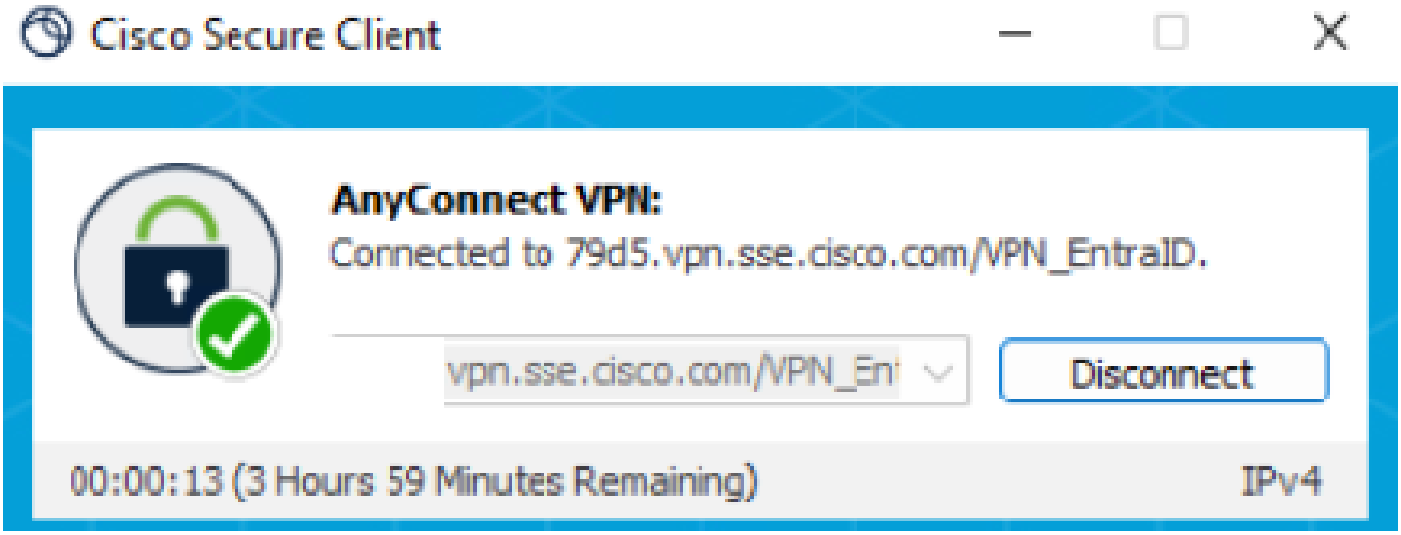
Neste exemplo, fornecemos o endereço URL do perfil ao usuário para a primeira tentativa de conexão.

Antes da primeira conexão:



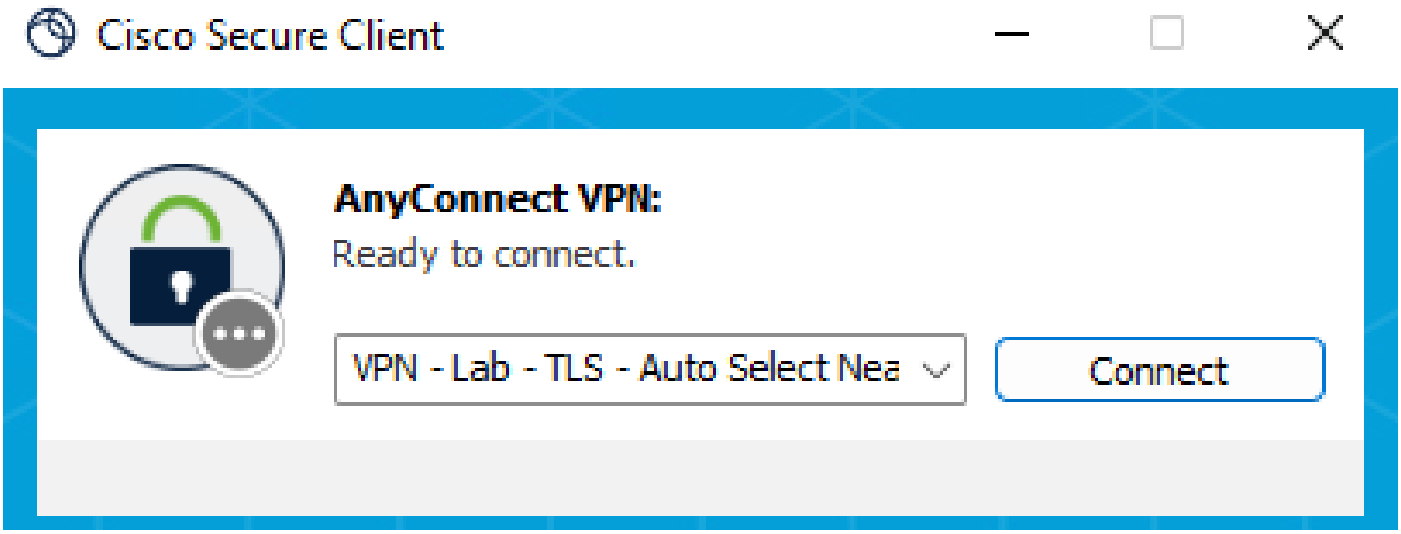
Conexão VPN anterior

Digite suas credenciais e conecte-se à VPN:



Conectado à VPN

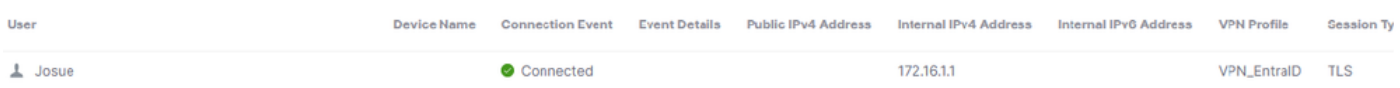
Depois de se conectar pela primeira vez, no menu suspenso, você deve ser capaz de ver agora a opção para se conectar ao perfil de VPN "VPN - Lab":



Após a primeira conexão VPN

Verifique nos Logs de acesso remoto se o usuário conseguiu se conectar:

Monitor > Log de Acesso Remoto



Logs no Cisco Secure Access

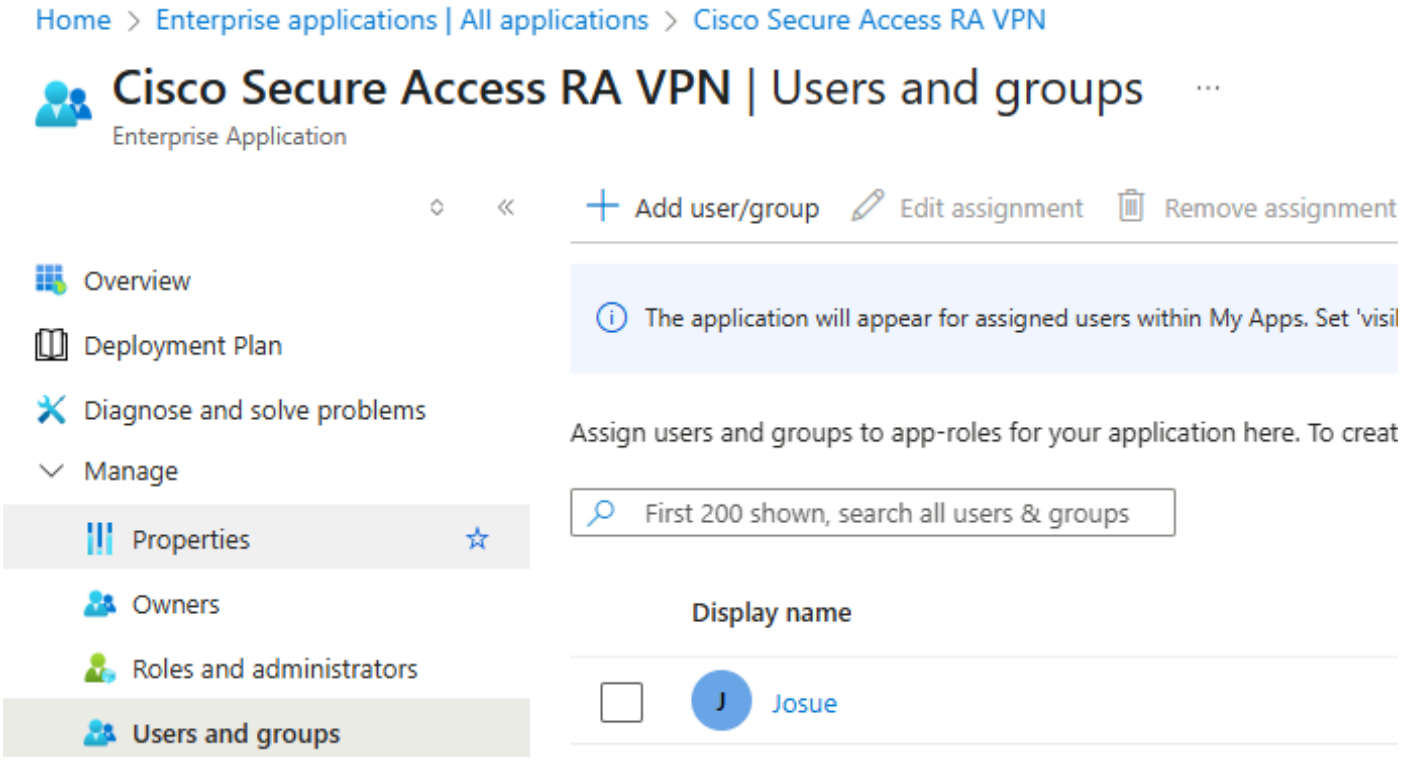
Troubleshooting

Aqui está descrito o Troubleshooting básico que pode ser executado para alguns problemas comuns:

Azure

No Azure, certifique-se de que os usuários tenham sido atribuídos ao aplicativo empresarial criado para a autenticação no Cisco Secure Access:

Home > Aplicativos corporativos > Cisco Secure Access RA VPN > Gerenciar > Usuários e grupos

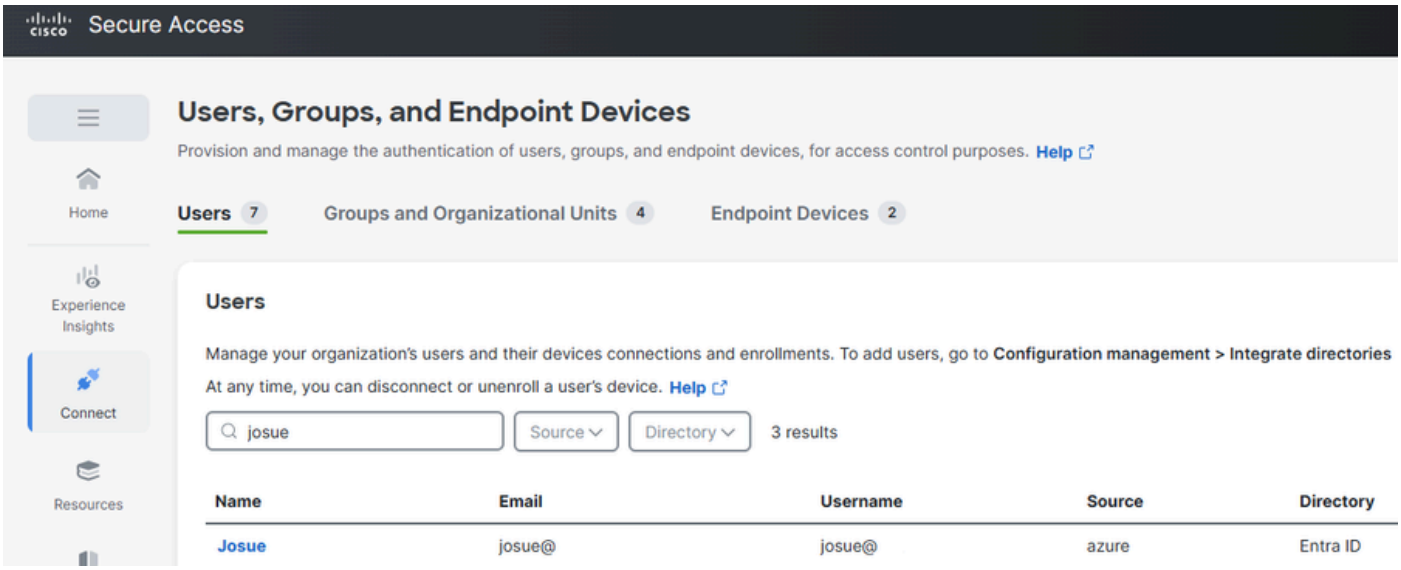


Verificar atribuição de usuários

Acesso seguro da Cisco

No Cisco Secure Access, certifique-se de que você tenha provisionado os usuários que têm permissão para se conectar via RA VPN, e que também os usuários provisionados no Cisco Secure Access (em usuários, grupos e dispositivos de endpoint) correspondam aos usuários no Azure (os usuários atribuídos no aplicativo empresarial).

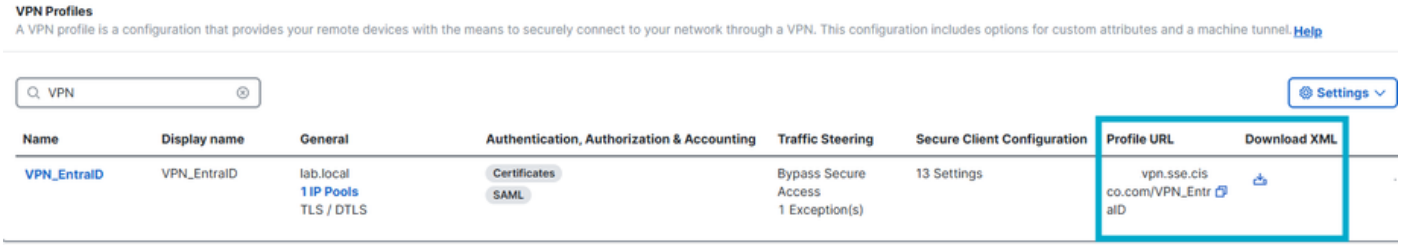
Conectar > Usuários, Grupos e Dispositivos de Endpoint



Usuários no Cisco Secure Access

Verifique se o usuário recebeu o arquivo XML correto no PC ou se recebeu o URL do perfil, conforme indicado na etapa "Verificar".

Conectar > Conectividade do usuário final > Rede virtual privada



URL de perfil e perfil .xml

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.