Configuración de Cisco Secure Access para RA VPNaaS con ID de entrada

Contenido

Introducción

Este documento describe paso a paso cómo configurar RA VPN en Cisco Secure Access para autenticarse contra el ID de entrada.

Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento mediante ID de Azure/Entra.
- Conocimientos con Cisco Secure Access.

Requirements

Estos requisitos deben cumplirse antes de continuar:

- Acceso al panel de Cisco Secure Access como administrador completo.
- Acceso a Azure como administrador.
- El aprovisionamiento de usuarios ya se ha completado en Cisco Secure Access.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Panel de Cisco Secure Access.

- Portal de Microsoft Azure.
- Cisco Secure Client AnyConnect VPN versión 5.1.8.105

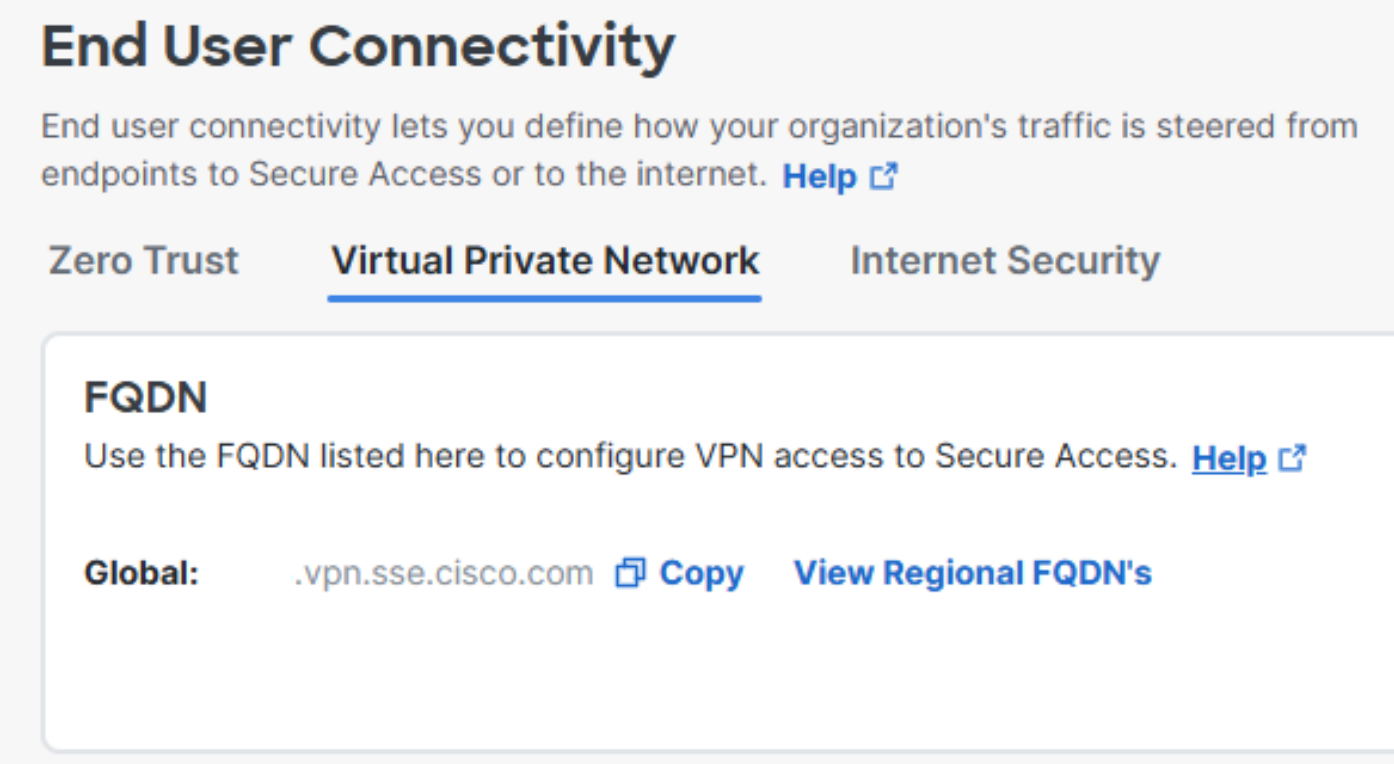
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Configuración de Azure

1. Inicie sesión en el panel de Cisco Secure Access y copie el FQDN global de VPN. Estamos usando este FQDN en la configuración de Azure Enterprise Application.

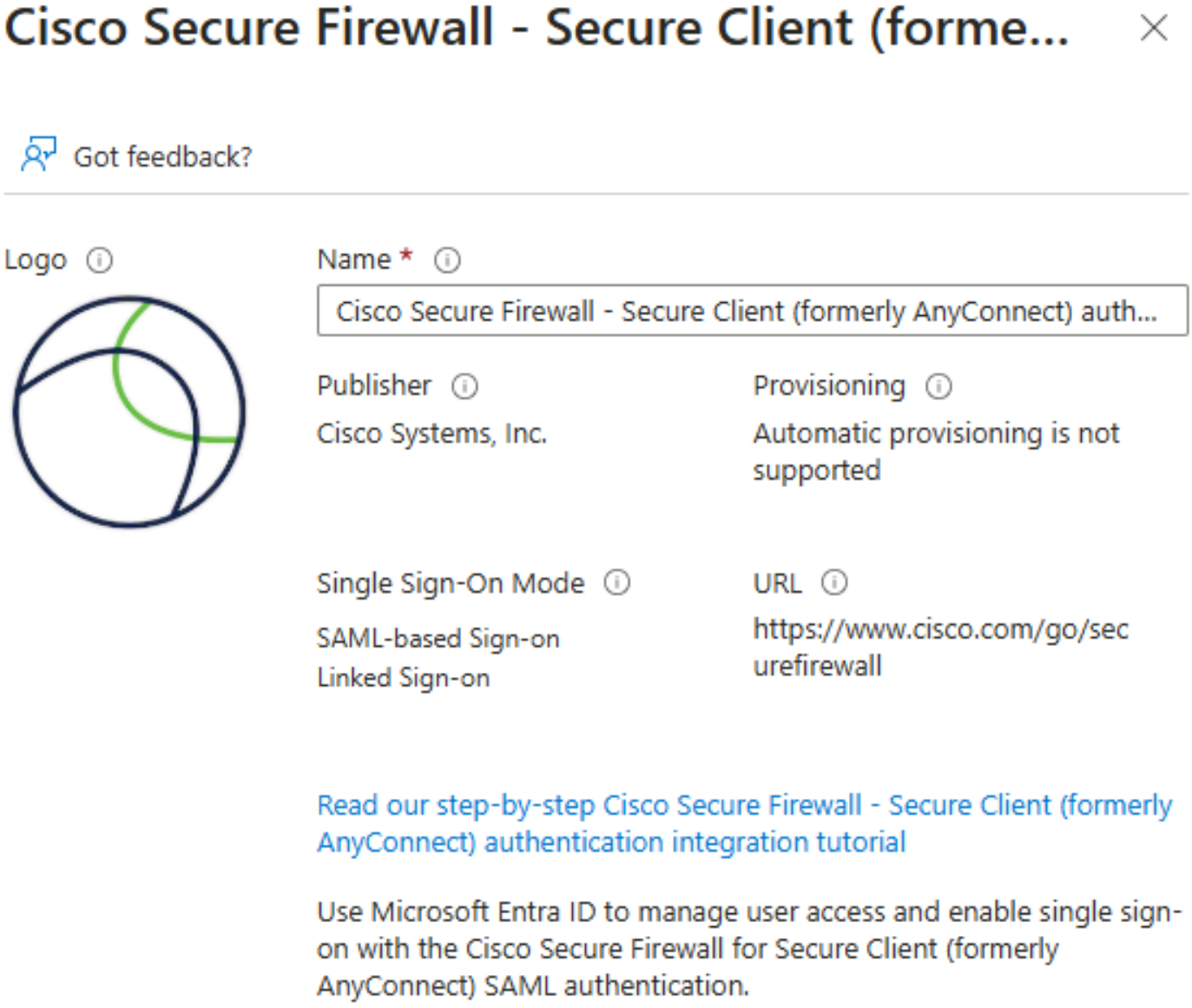
Conectar > Conectividad de usuario final > Red privada virtual > FQDN > Global



FQDN global de VPN

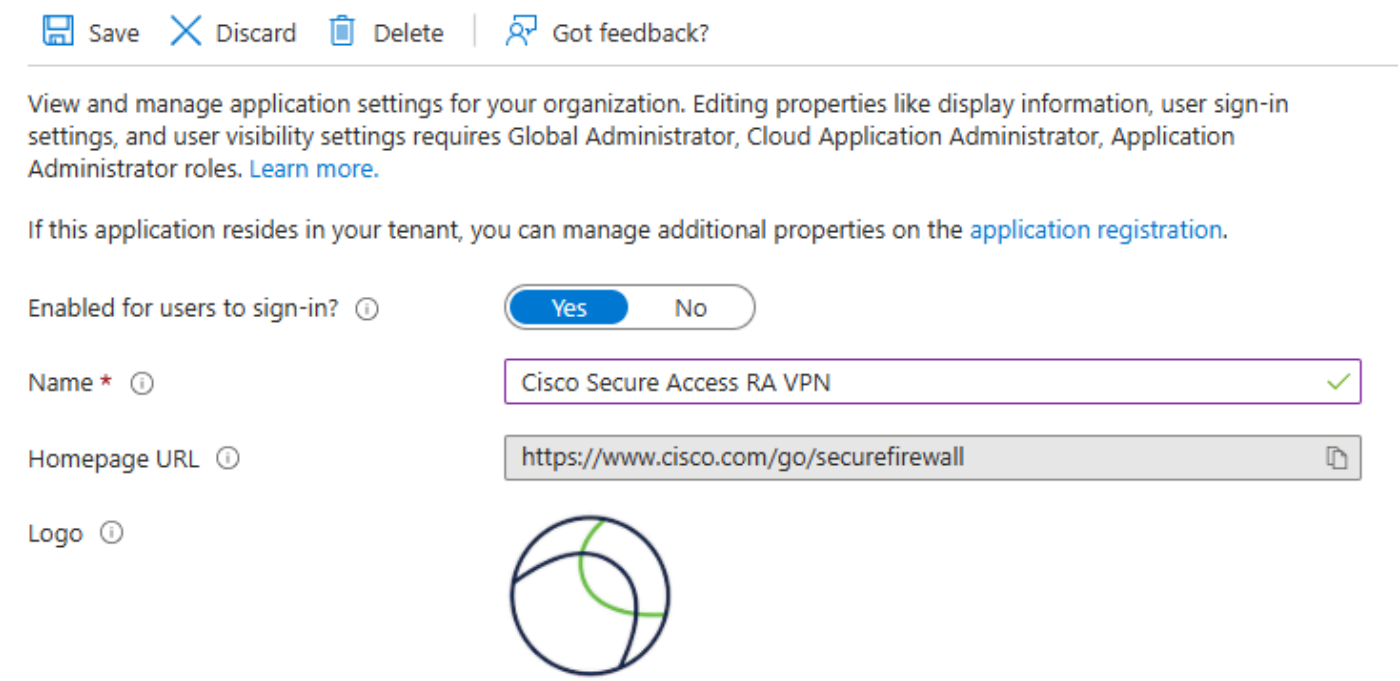
2. Inicie sesión en Azure y cree una aplicación empresarial para la autenticación VPN de RA. Puede utilizar la aplicación predefinida denominada "Cisco Secure Firewall - Secure Client (anteriormente AnyConnect) authentication".

Inicio > Aplicaciones empresariales > Nueva aplicación > Cisco Secure Firewall - Autenticación de Secure Client (anteriormente AnyConnect) > Crear



Crear aplicación en Azure

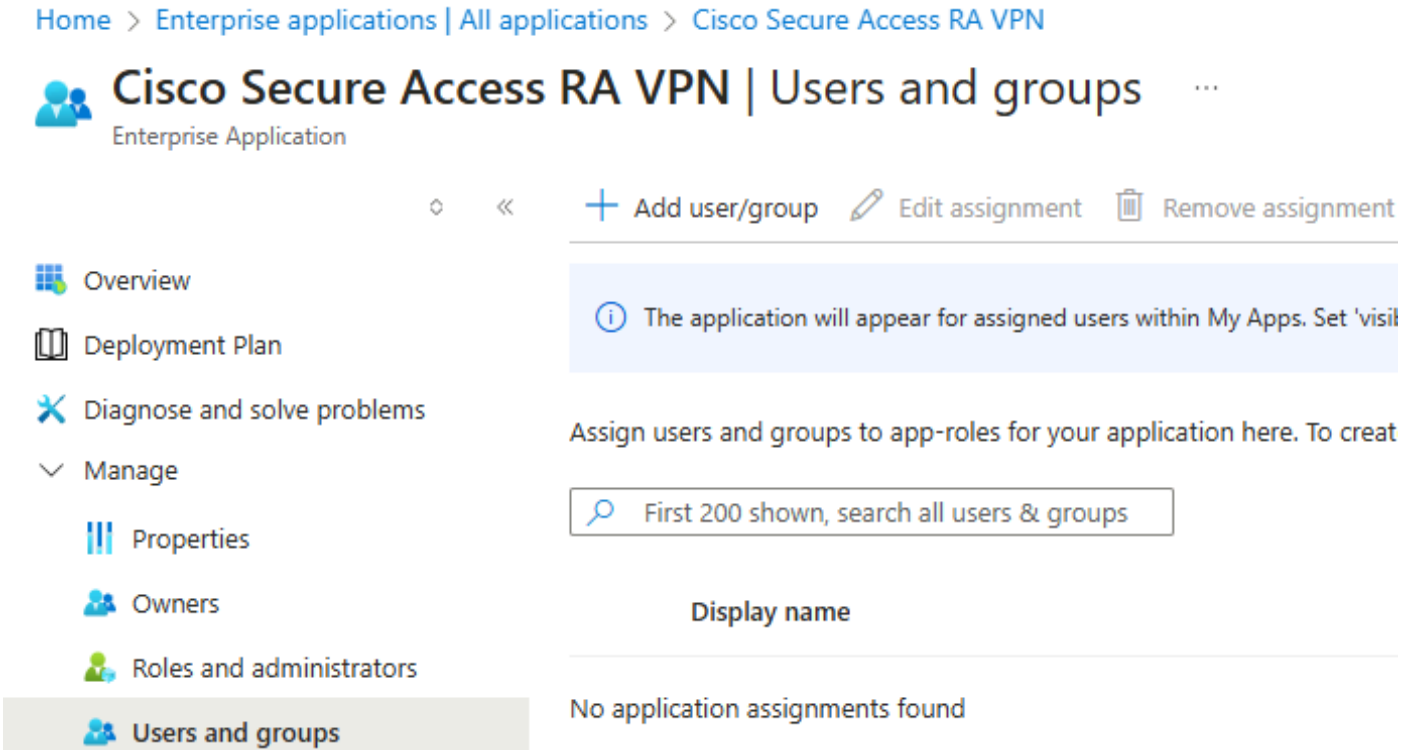
3. Cambie el nombre de la aplicación.
   Properties > Name



Cambiar el nombre de la aplicación

4. En la aplicación Enterprise, asigne a los usuarios que permiten la autenticación mediante AnyConnect VPN.

Asignar usuarios y grupos > + Agregar usuario/grupo > Asignar

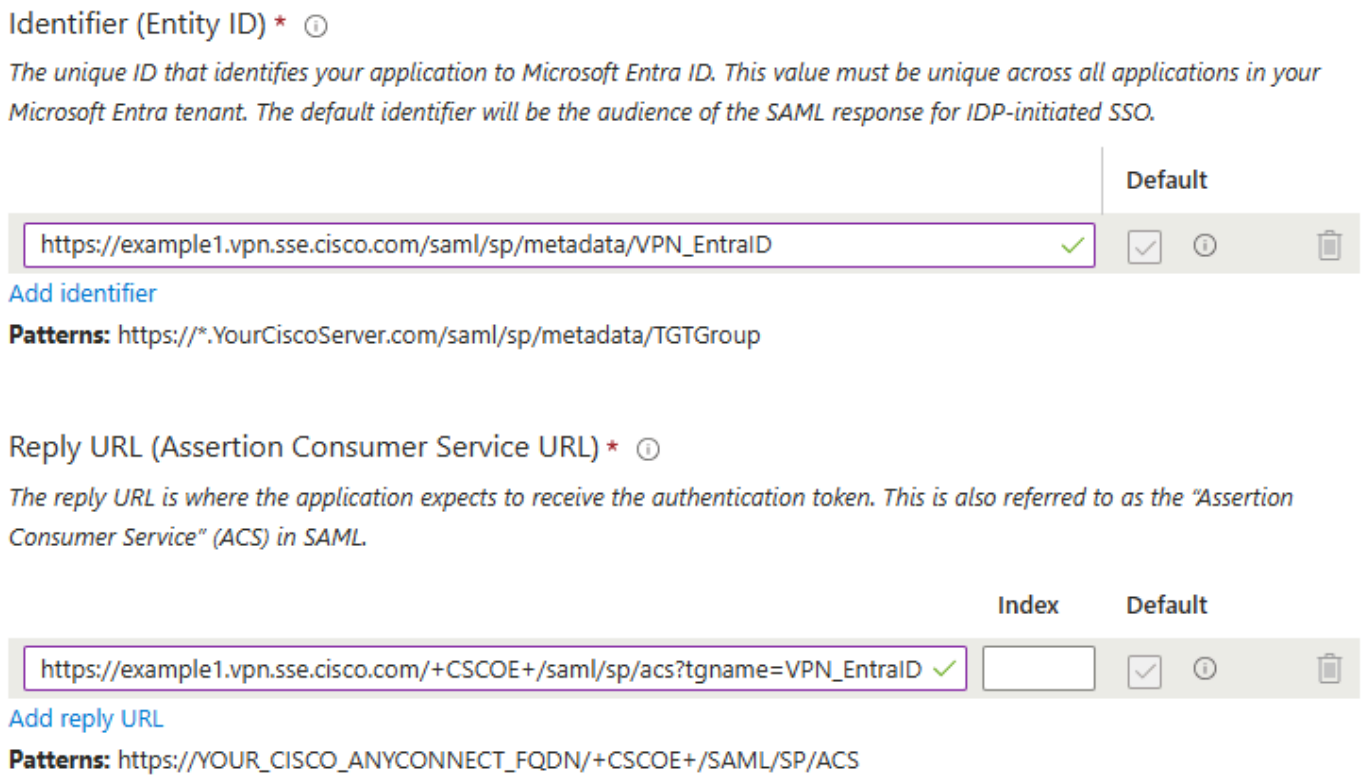


Usuarios/grupos asignados

5. Haga clic en Single Sign-on y configure los parámetros SAML. Aquí utilizamos el FQDN copiado en el paso 1 y también el nombre del perfil de VPN que está configurando en "Configuración de Cisco Secure Access", más adelante en el paso 2.

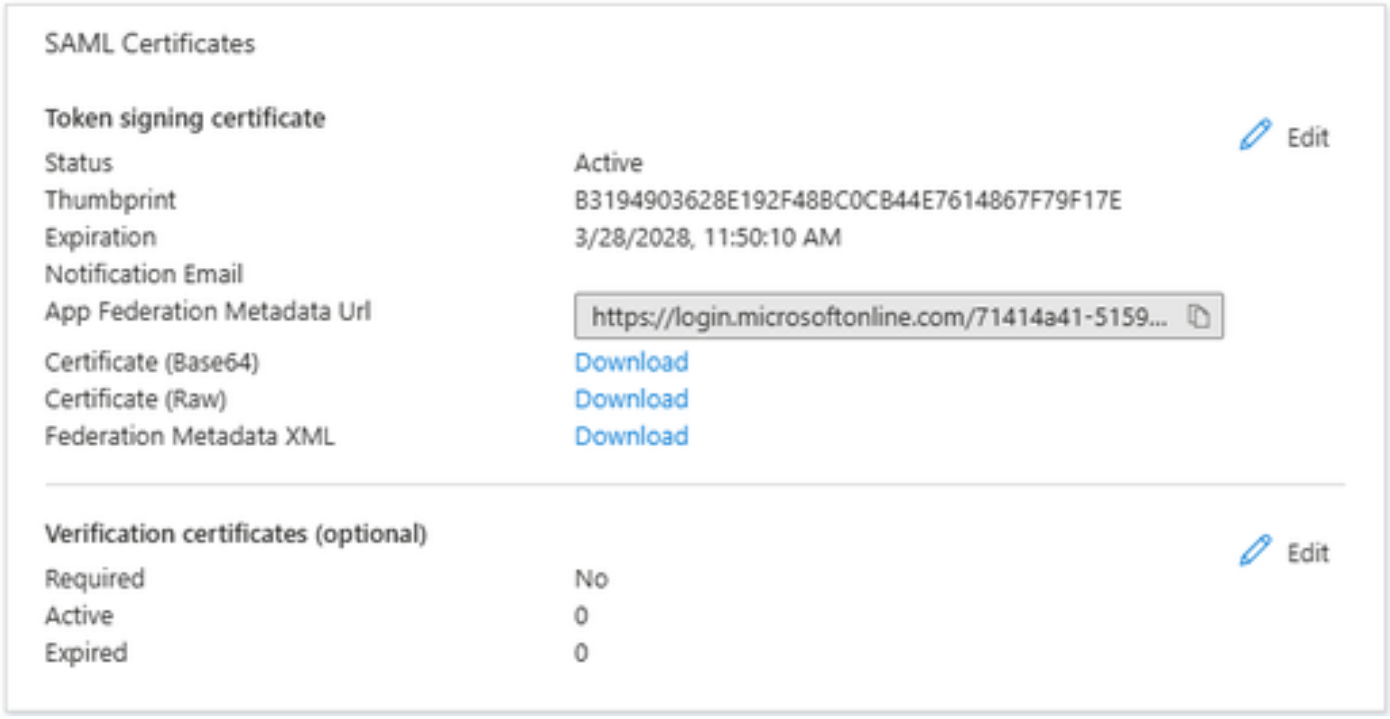
Por ejemplo, si el FQDN global de VPN es example1.vpn.sse.cisco.com y el nombre del perfil de VPN de Cisco Secure Access es VPN_EntraID, los valores de (Id. de entidad) y URL de respuesta (URL de servicio al consumidor de aserción) son:

Identificador (ID de entidad): https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID
URL de respuesta (URL de servicio de consumidor de afirmación): https://example1.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=VPN_EntraID



Parámetros SAML en Azure

6. Descargue el XML de metadatos de federación.



Configuración de Cisco Secure Access

1. Inicie sesión en el panel de Cisco Secure Access y agregue un grupo de IP.

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

Región: Seleccione la región en la que se implementará la VPN de RA.
Nombre para mostrar: El nombre del conjunto IP de VPN.
Servidor DNS: Cree o asigne los usuarios del servidor DNS que utilizan para la resolución DNS una vez conectados.
Conjunto IP del sistema: Utilizada por Secure Access para funciones como Radius Authentication, la solicitud de autenticación se origina en una IP dentro de este rango.
Conjunto IP: Agregue un nuevo conjunto de IP y especifique las IP que los usuarios obtendrán una vez conectados a la VPN de 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

Agregar 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

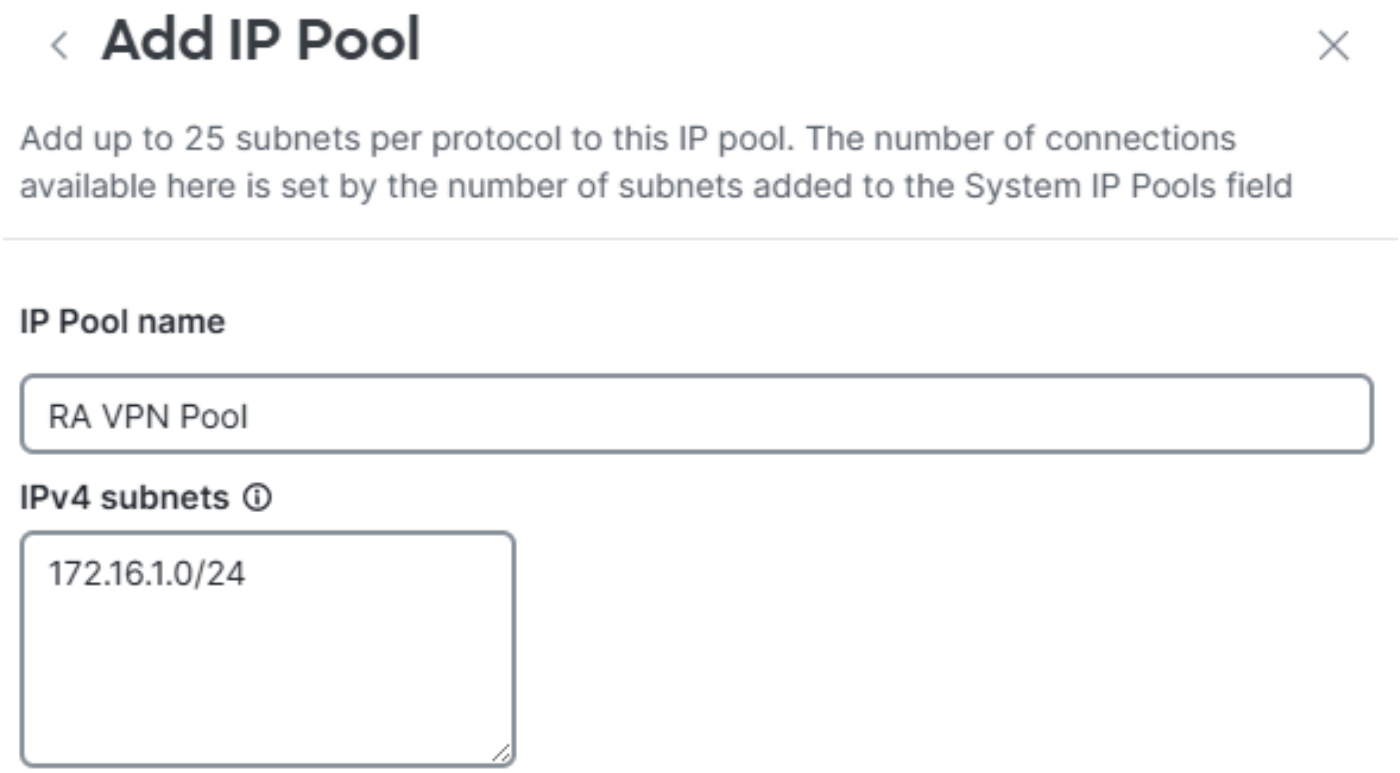
172.16.2.0/24

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

Configuración del pool IP - Parte 1

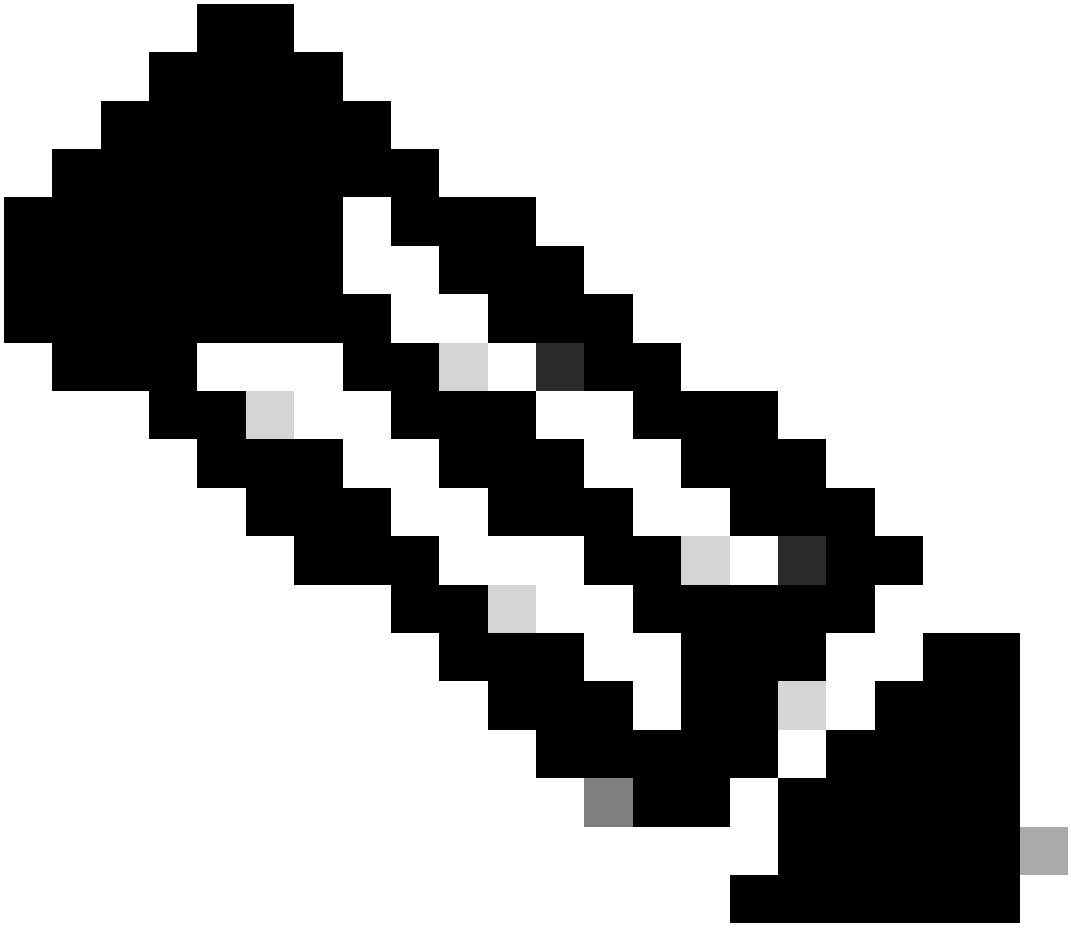


Configuración del pool IP - Parte 2

2. Agregue un perfil de VPN.

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

Configuración general



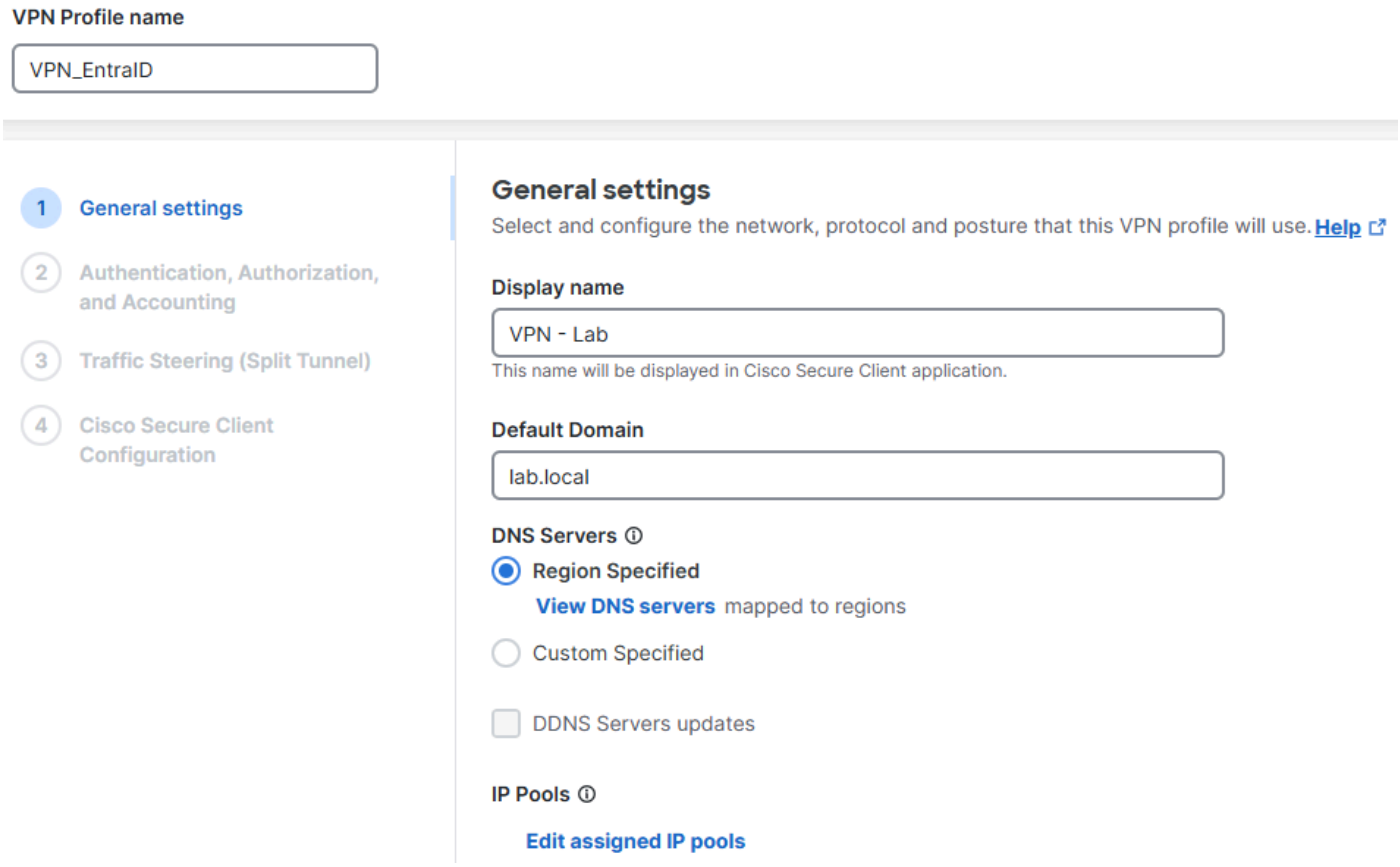
> Nota: Nota: El nombre del perfil de VPN debe coincidir con el nombre que configuró en "Configuration Azure" en el paso 5. En esta guía de configuración usamos VPN_EntraID, por lo que estamos configurando lo mismo en Cisco Secure Access que el nombre del perfil de VPN.

Nombre del perfil VPN: Nombre de este perfil VPN, visible solo en el panel.

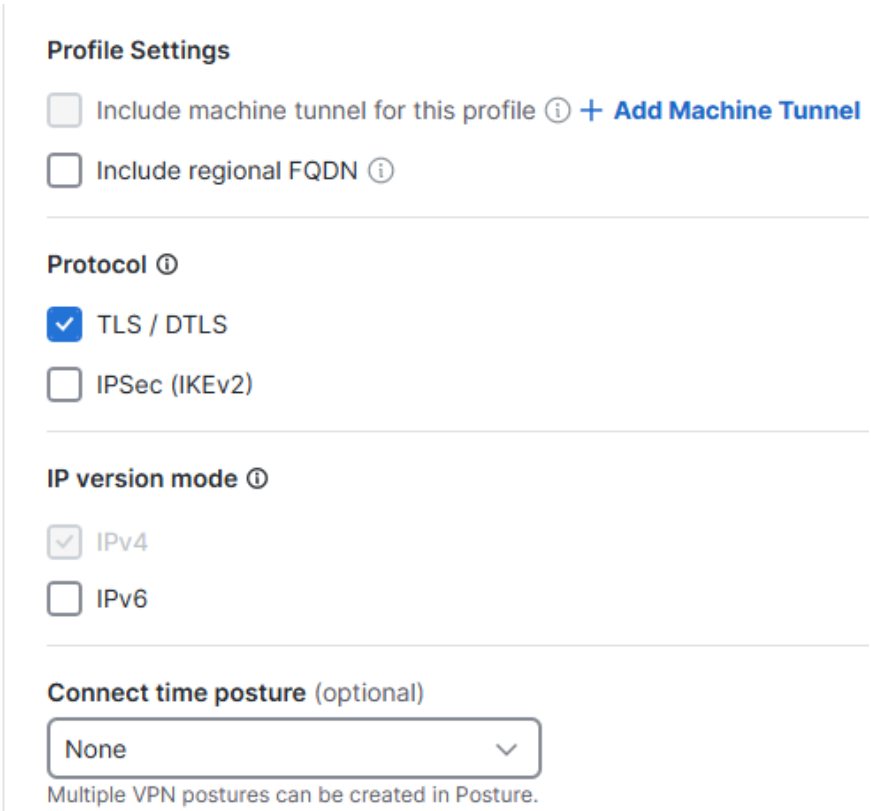
Nombre para mostrar: Los usuarios finales de nombre aparecen en el menú desplegable 'Secure Client - Anyconnect' para ver cuándo se conectan a este perfil VPN de RA.
Dominio predeterminado: Los usuarios del dominio se conectan una vez a la VPN.
Servidores DNS: Servidor DNS: los usuarios de VPN se conectan una vez a la VPN.
- Región especificada: Utiliza el servidor DNS asociado al grupo de IP VPN.
- Personalizado especificado: Puede asignar manualmente el DNS que desee.

Conjuntos IP: IP que los usuarios se asignan una vez conectados a la VPN.
Configuración de perfil: Para incluir este perfil VPN para el túnel de máquina o para incluir el FQDN regional de modo que el usuario final seleccione la región a la que desea conectarse (está sujeta a los grupos de IP implementados).

Protocolos: Seleccione el protocolo que desea que utilicen los usuarios de VPN para la tunelización del tráfico.
Tiempo de conexión (opcional): Si se requiere para realizar la postura de VPN en el momento de la conexión. Más información aquí



Configuración del perfil VPN - Parte 1



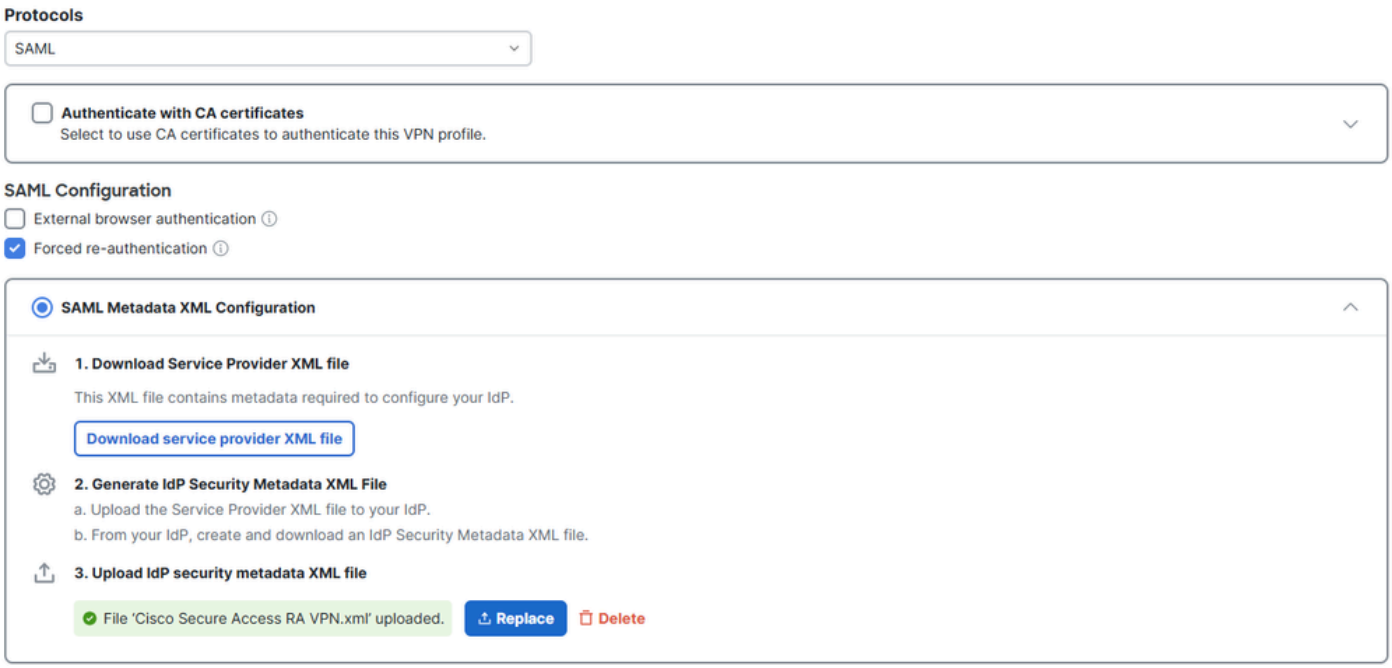
Configuración del perfil VPN - Parte 2

Autenticación, autorización y contabilidad

Protocolos: Seleccione SAML.

Autenticación con certificados de CA: En caso de que desee autenticarse utilizando un Certificado SSL y autorizar contra un Proveedor SAML de IdP.
Forzar reautenticación: Fuerza una reautenticación cada vez que se realiza una conexión VPN. La reautenticación forzada se basa en el tiempo de espera de la sesión. Esto podría estar sujeto a la configuración de IdP de SAML (Azure en este caso).

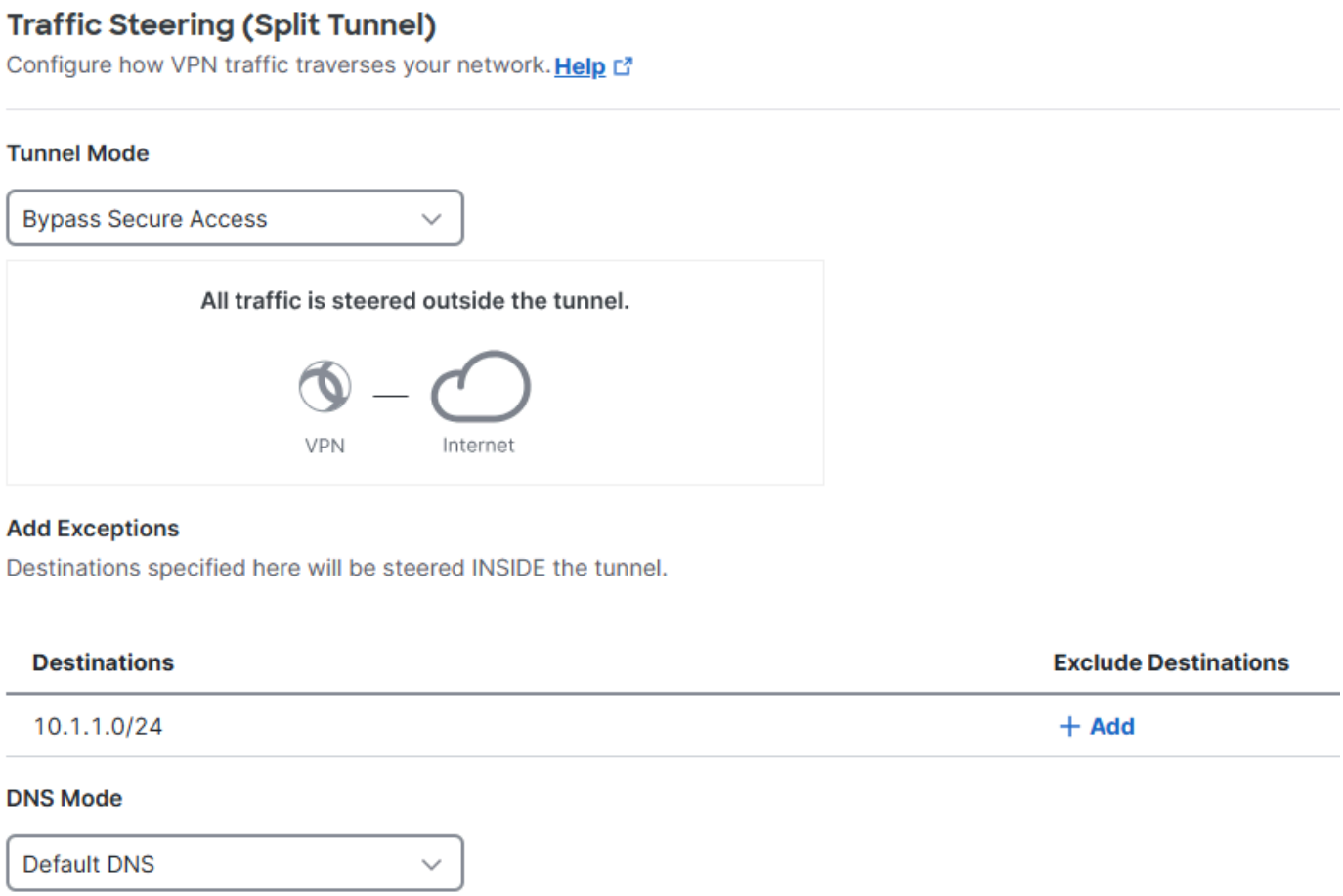
Cargue el archivo XML de metadatos de federación del archivo XML descargado en "Configurar Azure" en el paso 6.



Configuración de SAML

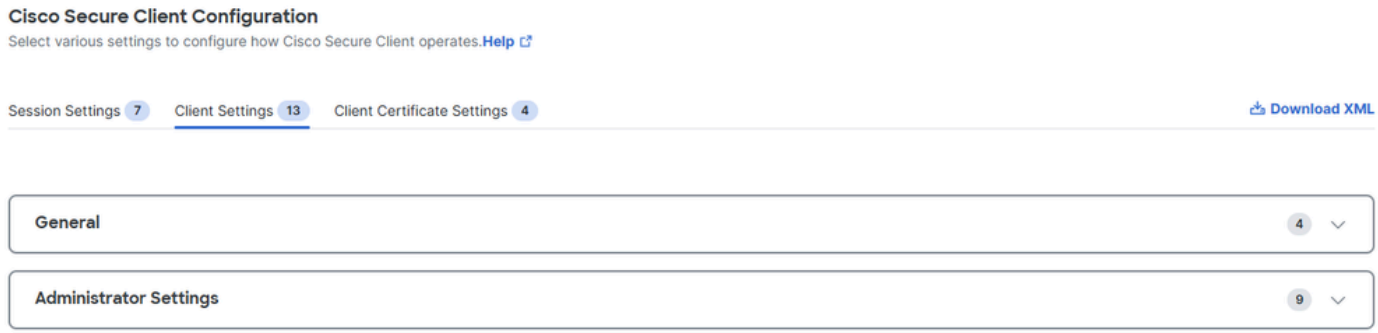
Dirección de tráfico (túnel dividido)

Modo de túnel:
Conexión a Secure Access: Todo el tráfico se envía a través del túnel (Tunnel All).
Omitir acceso seguro: Sólo el tráfico específico definido en la sección Excepciones es tunelizado (Túnel dividido).
Modo DNS:
DNS predeterminado: Todas las consultas DNS se mueven a través de los servidores DNS definidos por el perfil VPN. En el caso de una respuesta negativa, las consultas DNS también pueden dirigirse a los servidores DNS que están configurados en el adaptador físico.
Tunnel All DNS: Tuneliza todas las consultas DNS a través de la VPN.
DNS Dividido: Solo las consultas específicas de DNS se desplazan a través del perfil VPN, en función de los dominios especificados a continuación.



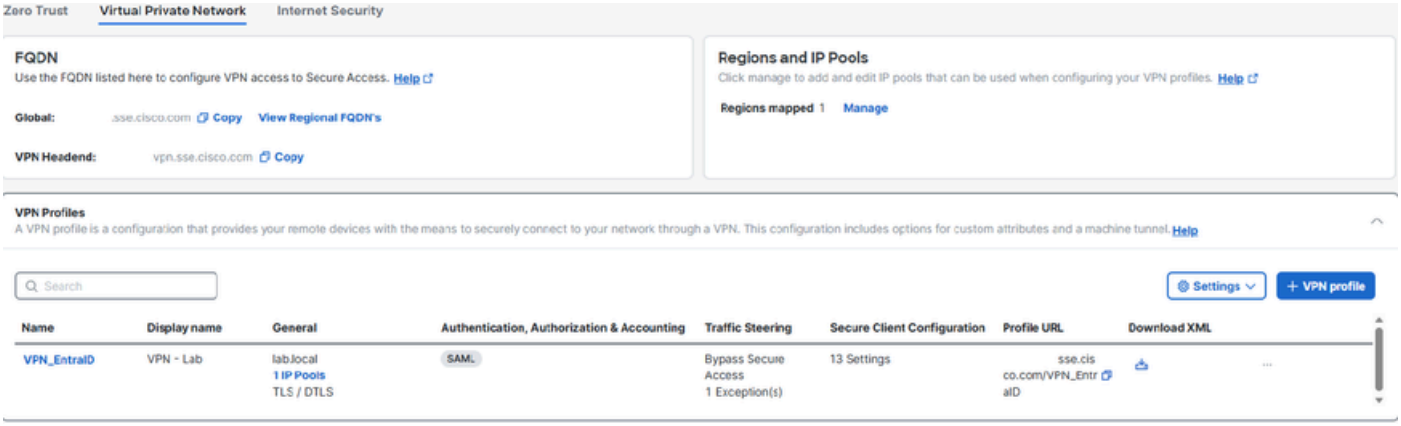
Configuración de dirección de tráfico

Configuración de Cisco Secure Client
A efectos de esta guía, no estamos configurando ninguno de estos parámetros avanzados. Las funciones avanzadas se pueden configurar aquí, por ejemplo: TND, Always-On, Certificate Matching, Local Lan Access, etc. Guarde la configuración aquí.



Configuración avanzada

3. Su perfil de VPN debe tener este aspecto. Puede descargar e implementar previamente el perfil xml a los usuarios finales (en "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile") para empezar a utilizar la VPN, o proporcionarles la URL del perfil que se introducirá en la interfaz de usuario de Cisco Secure Client - AnyConnect VPN.



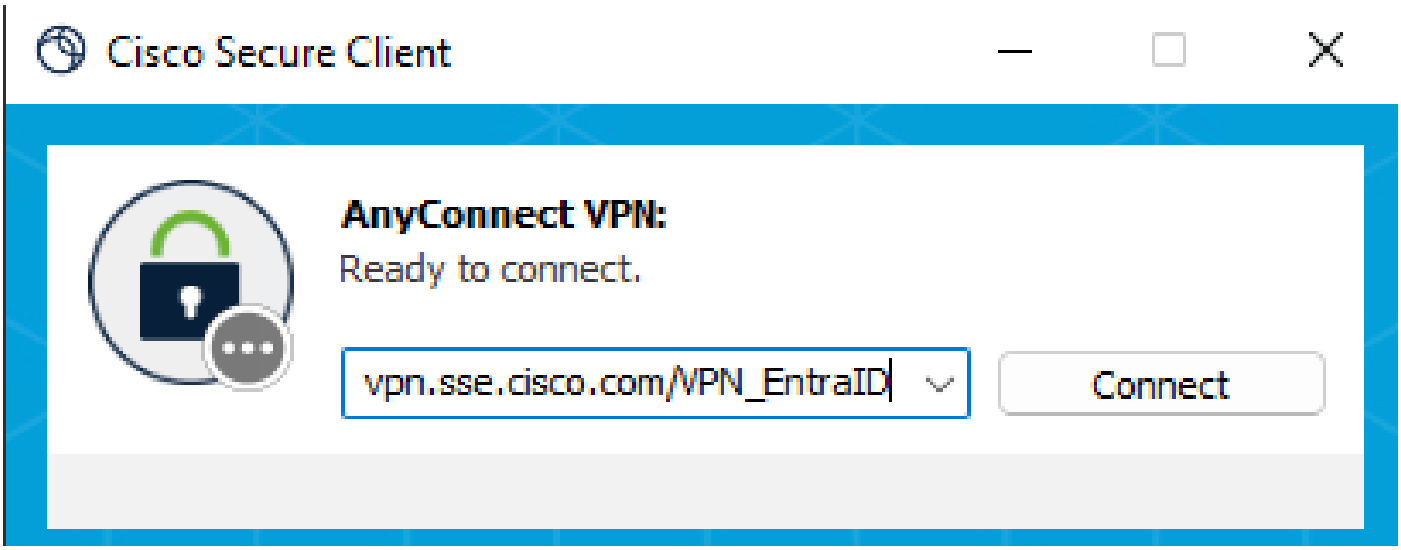
FQDN global y URL de perfil

Verificación

En este momento, la configuración VPN de RA debe estar lista para la prueba.
Tenga en cuenta que la primera vez que los usuarios se conectan, deben recibir la dirección URL del perfil o preimplementar el perfil xml en sus PC en "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile", reiniciar el servicio VPN y deben ver en el menú desplegable la opción para conectarse a este perfil VPN.

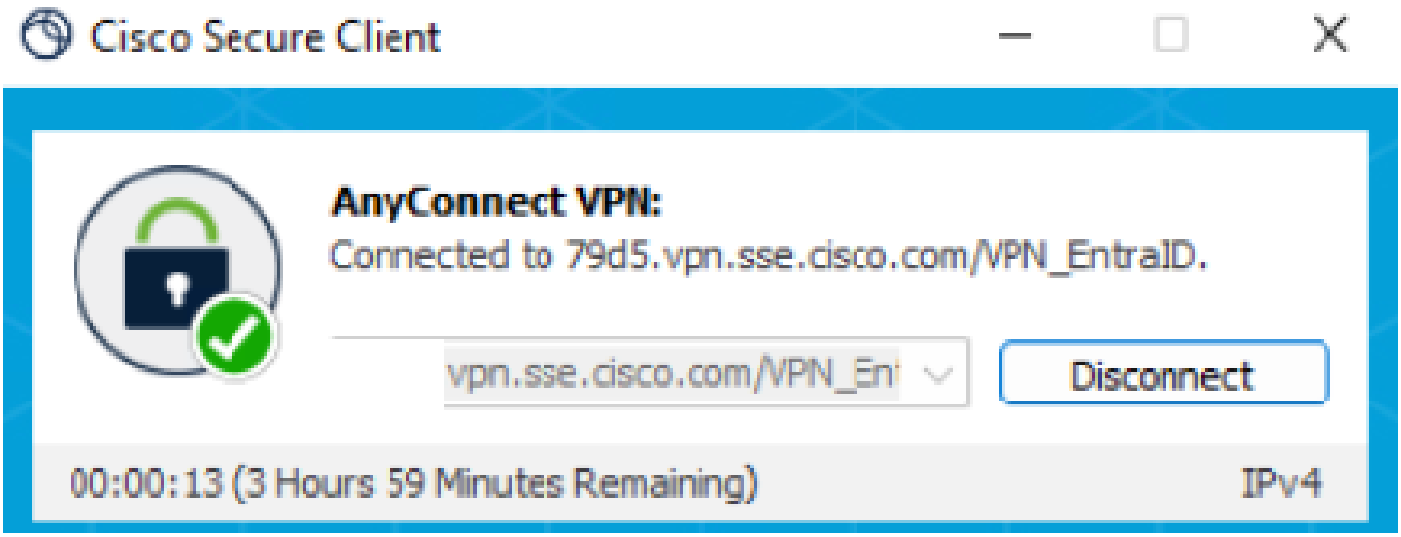
En este ejemplo, proporcionamos la dirección URL del perfil al usuario para el primer intento de conexión.

Antes de la primera conexión:



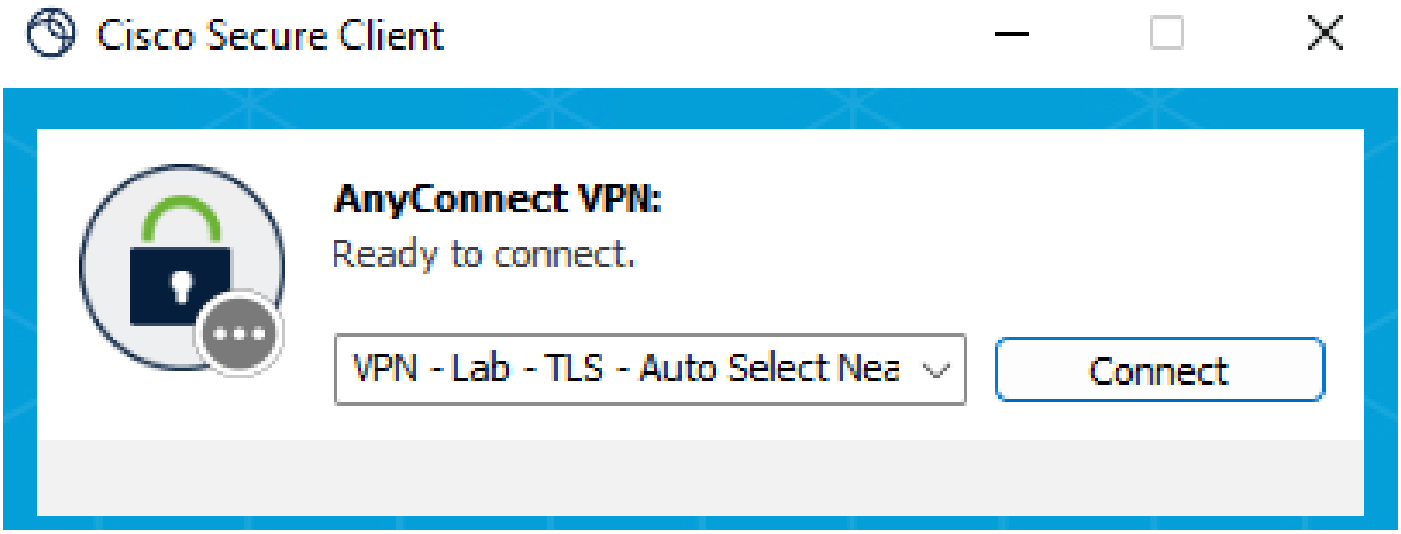
Conexión VPN anterior

Introduzca sus credenciales y conéctese a la VPN:



Conectado a VPN

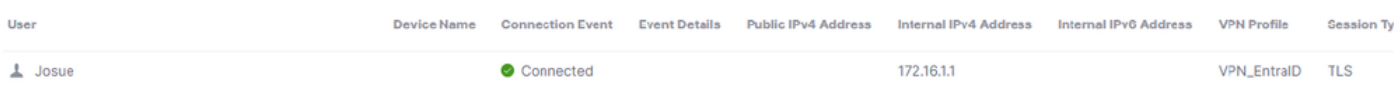
Después de conectarse por primera vez, desde el menú desplegable, debe poder ver ahora la opción para conectarse al perfil VPN "VPN - Lab":



Después de la primera conexión VPN

Proteja los registros de acceso remoto a los que se pudo conectar el usuario:

Supervisar > Registro de acceso remoto



Registros en Cisco Secure Access

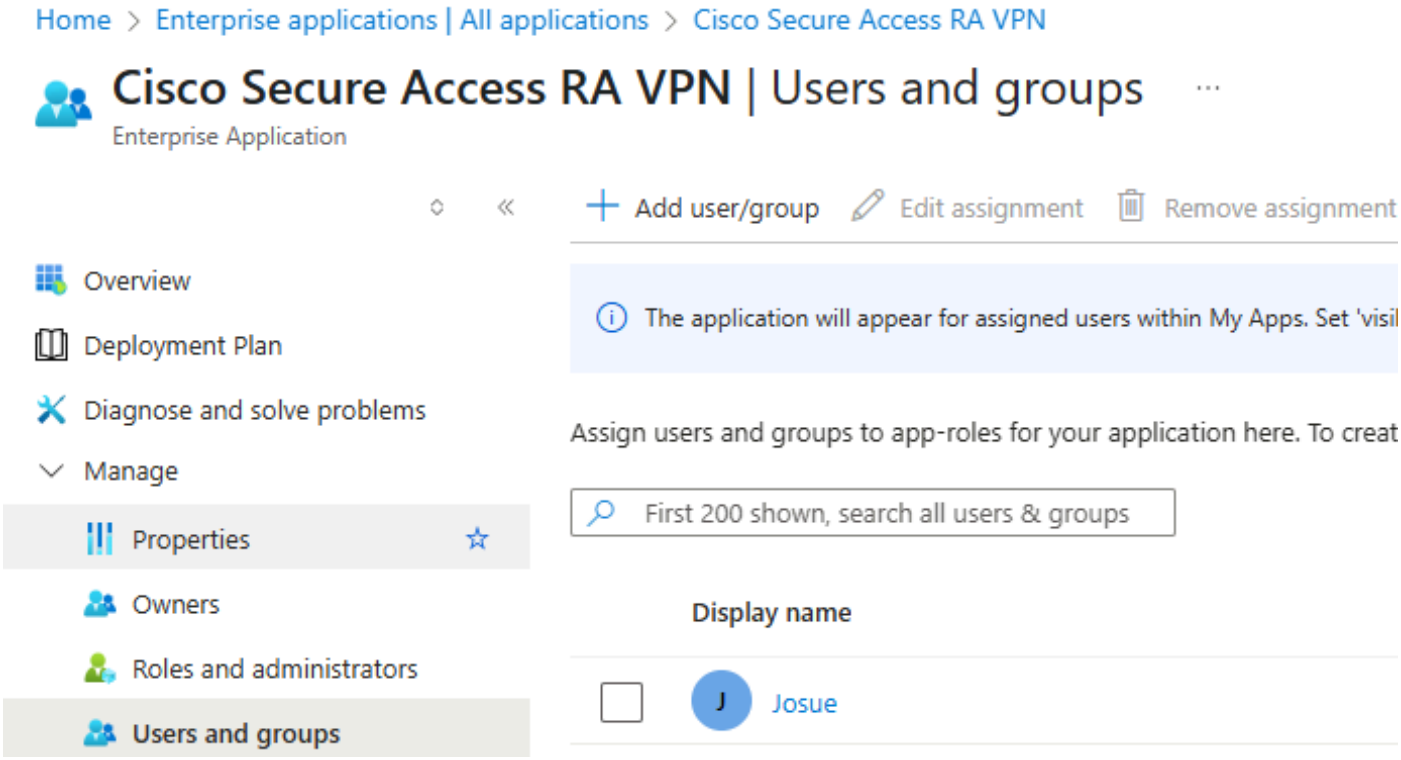
Resolución de problemas

Aquí se describe la solución de problemas básica que se puede realizar para algunos problemas comunes:

Azure

En Azure, asegúrese de que los usuarios se han asignado a la aplicación de empresa creada para la autenticación con Cisco Secure Access:

Inicio > Aplicaciones empresariales > Cisco Secure Access RA VPN > Gestionar > Usuarios y grupos

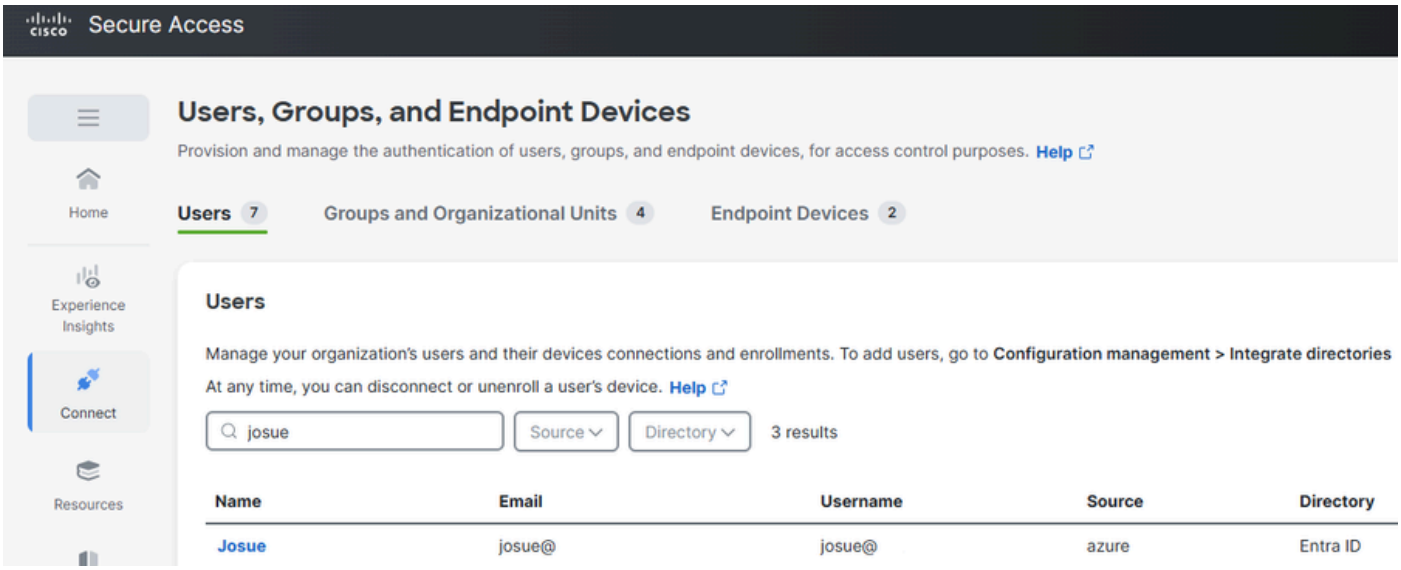


Verificar asignación de usuarios

Acceso seguro de Cisco

En Cisco Secure Access, asegúrese de que ha aprovisionado a los usuarios que tienen permiso para conectarse a través de VPN de RA y de que también los usuarios aprovisionados en Cisco Secure Access (en usuarios, grupos y dispositivos de terminales) coinciden con los usuarios de Azure (los usuarios asignados en la aplicación de empresa).

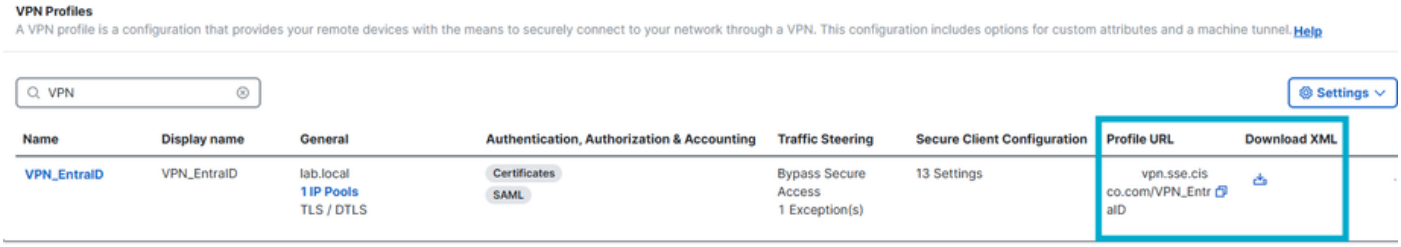
Connect > Users, Groups, and Endpoint Devices



Usuarios de Cisco Secure Access

Compruebe que se ha proporcionado al usuario el archivo XML correcto en el PC o que se le ha proporcionado la URL del perfil, como se indica en el paso "Comprobar".

Conectar > Conectividad de usuario final > Red privada virtual



Perfil URL y perfil .xml

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).