

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

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuración de Azure](#)

[Configuración de Cisco Secure Access](#)

[Verificación](#)

[Resolución de problemas](#)

[Azure](#)

[Acceso seguro de Cisco](#)

---

## 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



**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](#)

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

# 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.

Crear aplicación en Azure

- 3. Cambie el nombre de la aplicación.  
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 \*   

Homepage URL   

Logo  

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

[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 'visibl

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

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](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?tname=VPN\\_EntraID](https://example1.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tname=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?tname=VPN_EntraID"/> | <input type="text"/> | <input checked="" type="checkbox"/> ⓘ |

[Add reply URL](#)

**Patterns:** https://YOUR\_CISCO\_ANYCONNECT\_FQDN/+CSCOE+/SAML/SP/ACS

Parámetros SAML en Azure

6. Descargue el XML de metadatos de federación.

SAML Certificates

Token signing certificate

Status

Thumbprint

Expiration

Notification Email

App Federation Metadata Url

Certificate (Base64)

Certificate (Raw)

Federation Metadata XML

Active

B3194903628E192F48BC0CB44E7614867F79F17E

3/28/2028, 11:50:10 AM

[https://login.microsoftonline.com/71414a41-5159...](#)

[Download](#)

[Download](#)

[Download](#)

Edit

---

Verification certificates (optional)

Required

Active

Expired

No

0

0

Edit

## 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](#)

## < 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

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](#)

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](#)

Configuración del perfil VPN - Parte 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.

## 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.

**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](#)

## 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.

## 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

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.

### 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

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.

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](#)

[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<br>1 IP Pools<br>TLS / DTLS | SAML                                       | Bypass Secure Access<br>1 Exception(s) | 13 Settings                 | sse.cisco.com/VPN_EntraID | <a href="#">Download XML</a> |

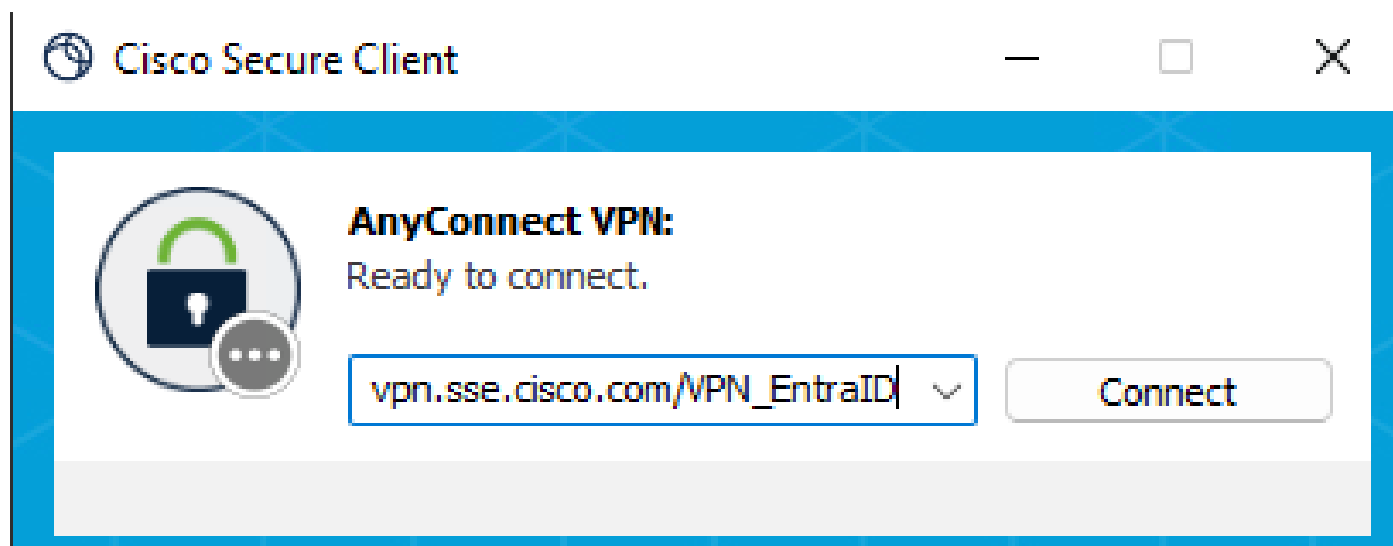
FQDN global y URL de perfil

## 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.

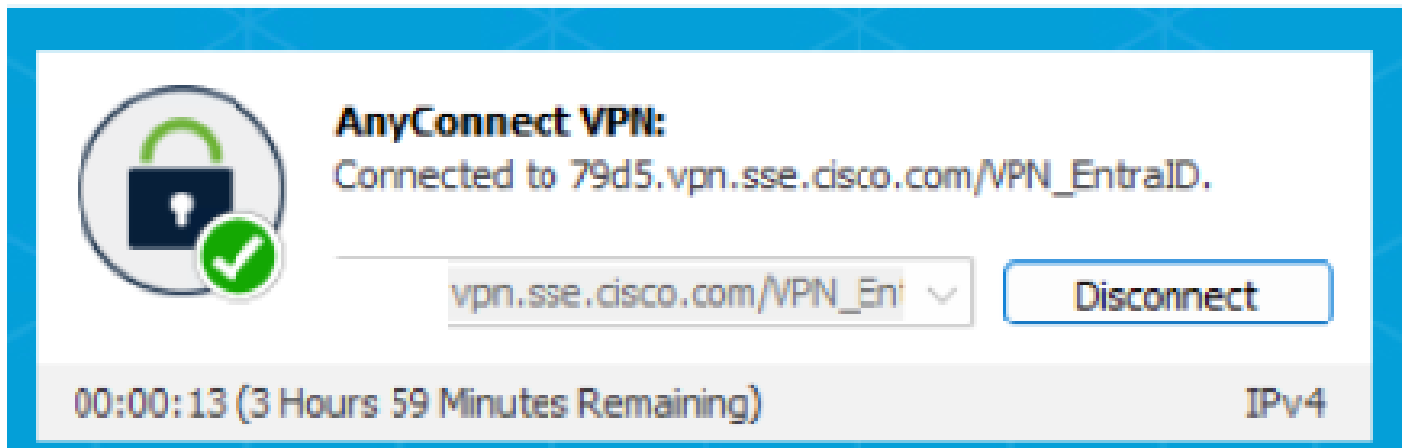
En este ejemplo, proporcionamos la dirección URL del perfil al usuario para el primer intento de conexión.

Antes de la primera conexión:



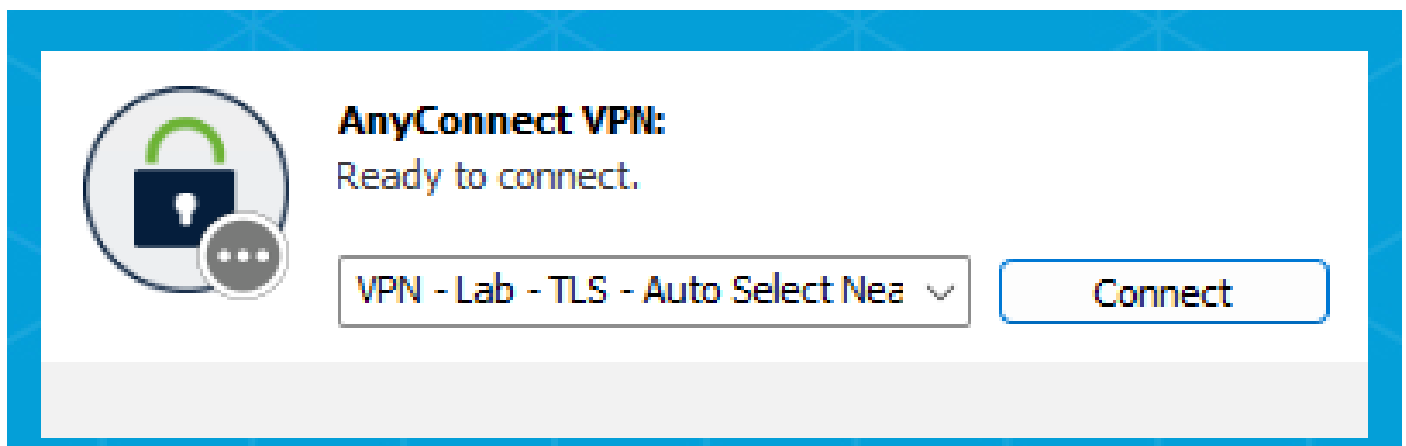
Conexión VPN anterior

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

| 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        |

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

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 'visi

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

🔍 First 200 shown, search all users & groups

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

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

Secure Access

☰

Home

Experience Insights

Connect

Resources

## Users, Groups, and Endpoint Devices

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

**Users** 7

Groups and Organizational Units 4

Endpoint Devices 2

### 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](#)

Source ▼

Directory ▼

3 results

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

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

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](#)

Settings ▼

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

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).