

# Aprovisionamiento de usuarios y grupos para proteger el acceso mediante ID de entrada

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuración de Cisco Secure Access](#)

[Configurar el aprovisionamiento en Microsoft Entry ID](#)

[Verificación](#)

[Veracidad en Cisco Secure Access](#)

[Verificar en ID de entrada](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe cómo proveer usuarios y grupos desde Entra ID a Cisco Secure Access.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso seguro de Cisco
- ID de entrada

### Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

- Acceso de administrador al panel de Cisco Secure Access
- Acceso de administrador al panel de ID de entrada

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.

## Antecedentes

Cisco Secure Access admite el aprovisionamiento de usuarios y grupos desde Microsoft Entry ID (anteriormente, Azure Active Directory).

Este aprovisionamiento permite a Secure Access mantener un directorio de usuarios autorizados para:

- Inscríbase en Zero Trust Access (ZTA).
- Conéctese a VPNaaS.
- Aplique políticas basadas en identidad a los usuarios de Umbrella Roaming.



Nota: Este documento se centra específicamente en el aprovisionamiento de usuarios y grupos desde la ID de entrada. La configuración de la ID de entrada u otros proveedores de identidad (IdP) para la inscripción ZTA, la autenticación VPNaaS o los ajustes específicos de Umbrella Roaming está fuera del alcance de esta guía.

---

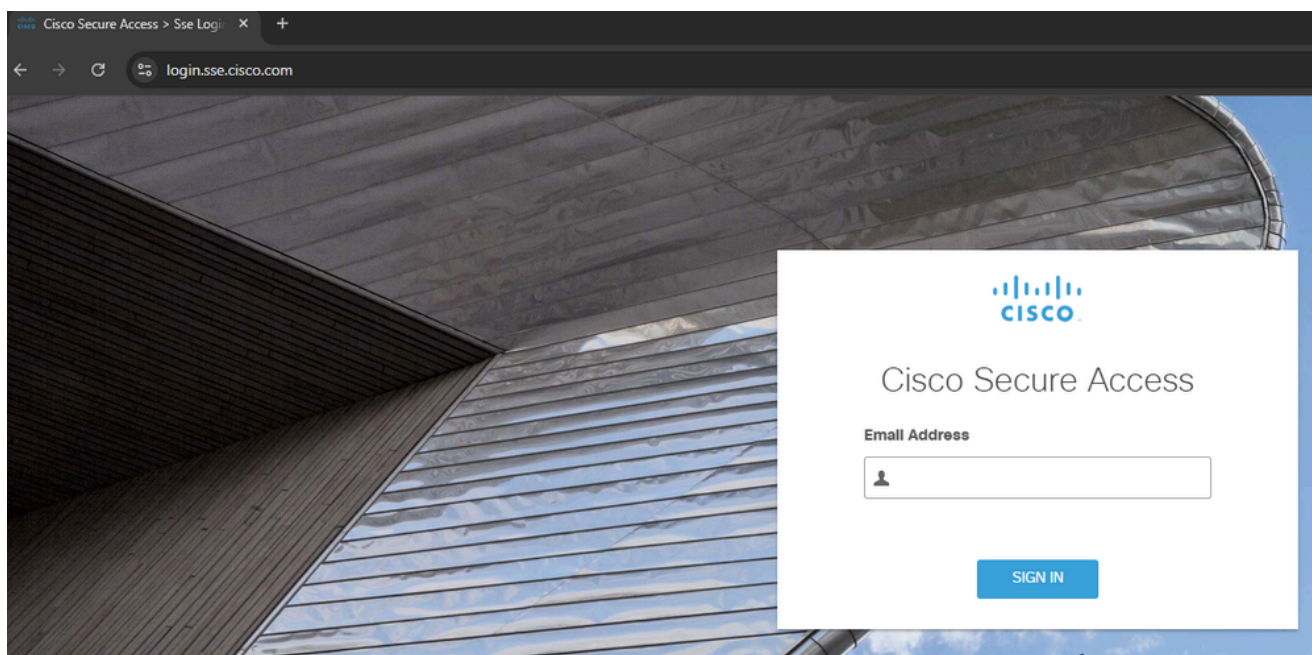
## Configurar

### Configuración de Cisco Secure Access

Para comenzar el proceso de aprovisionamiento, primero debe configurar la integración de directorios en el panel de Cisco Secure Access. Este paso genera las credenciales necesarias y los parámetros de configuración necesarios para establecer una conexión segura con Microsoft

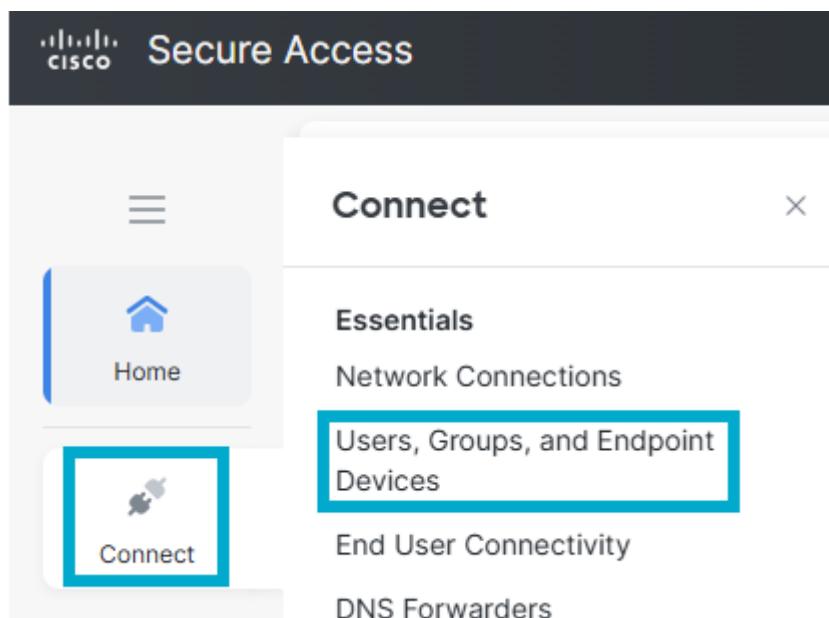
Entry ID.

1. Inicie sesión en el panel de **Cisco Secure Access**.



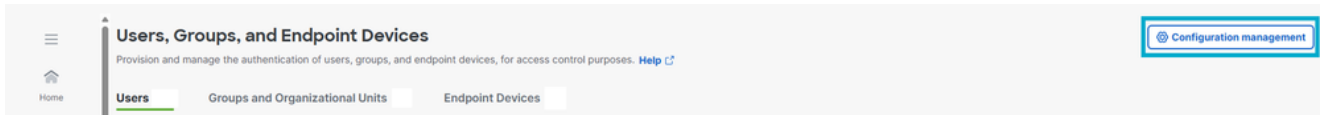
*Iniciar sesión en CSA*

2. Vaya a **Connect > Users, Groups and Endpoint Devices**.



*Usuarios y grupos*

3. Haga clic en **Configuration management**.



Administración de la Configuración

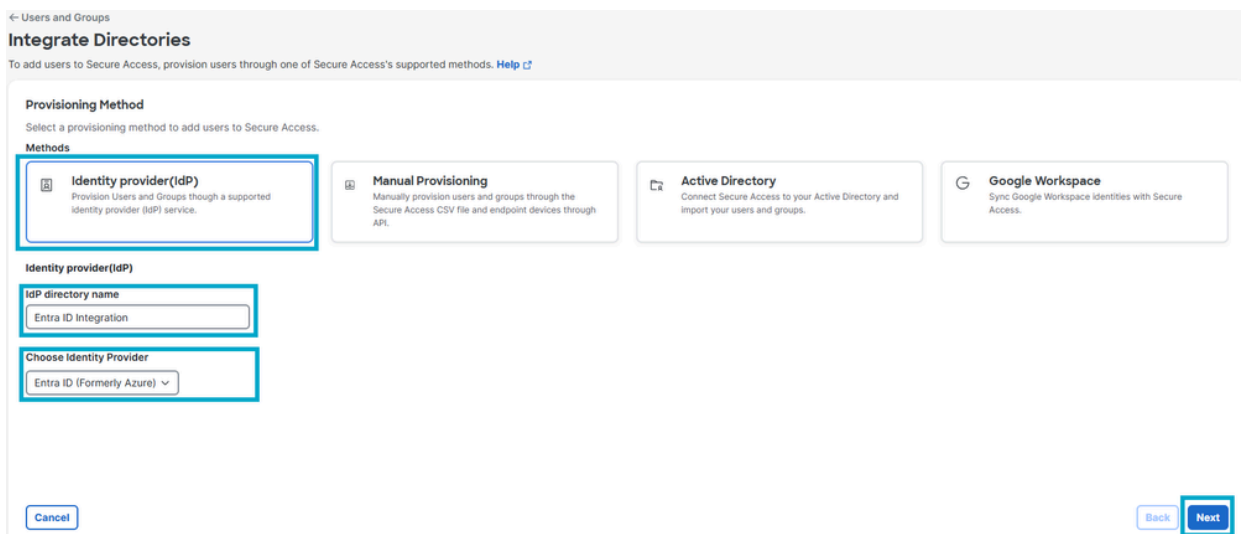
#### 4. Haga clic en **Integrar directorio**.



Integrate Directory

#### 5. En **Método de aprovisionamiento**, haga clic en **Proveedor de identidad**.

- **Nombre del directorio IdP: Integración de ID entrante.**
- **Seleccione el proveedor de identidad: Id. de entrada (antes Azure).**
- Haga clic en **Next (Siguiente)**.



Configuración de directorio

#### 6. Haga clic en **Generar token**. Guarde el **token generado** y la **URL de aprovisionamiento**, luego haga clic en **Finalizado**.

← [Users and Groups](#)

## Entra ID Integration

Entra ID (Formerly Azure)

Follow the instructions below to provision identities to this directory. [Help](#)

### Start Provisioning

To provision users to Secure Access, you must authenticate to your identity provider (IdP). Generate a token and then use it and the listed provisioning URL to provision users through your IdP. [Help](#)

#### Provisioning token

Once generated, copy and save this authentication token. It is required when configuring your IdP.

**⚠ For security reasons, your token will only be displayed once. For future reference, copy this token and keep it in a safe place**

Token  [Copy token](#) Generated On  
March 17, 2026

---

#### Provisioning URL

Copy and save this provisioning URL. It is required when configuring your IdP.

[Copy URL](#)

---

#### Configure your IdP portal

Use the generated authentication token and provisioning URL to set up Secure Access in your IdP. Once setup, you can provision users to Secure Access. [Help](#)

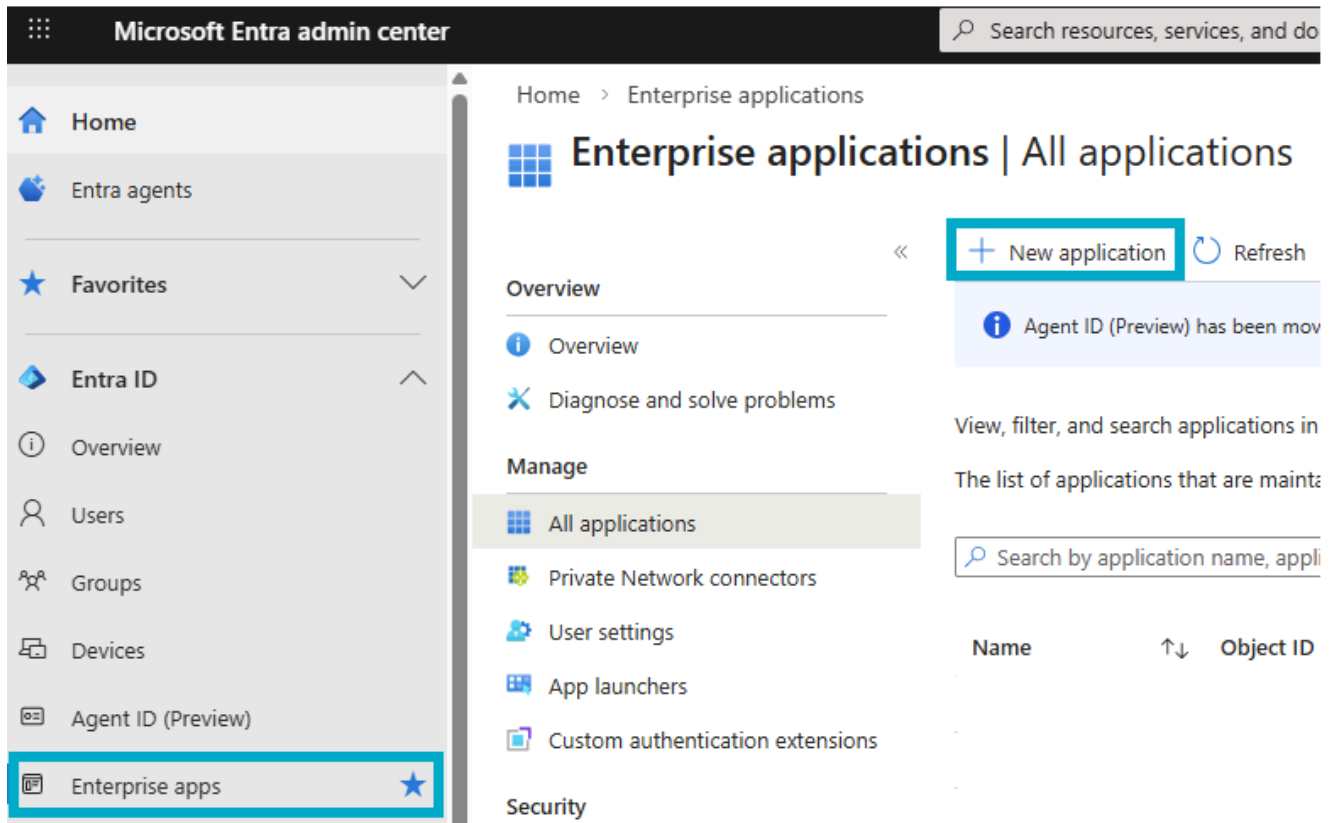
[Cancel](#) [Back](#) [Done](#)

*Generar token*

## Configurar el aprovisionamiento en Microsoft Entry ID

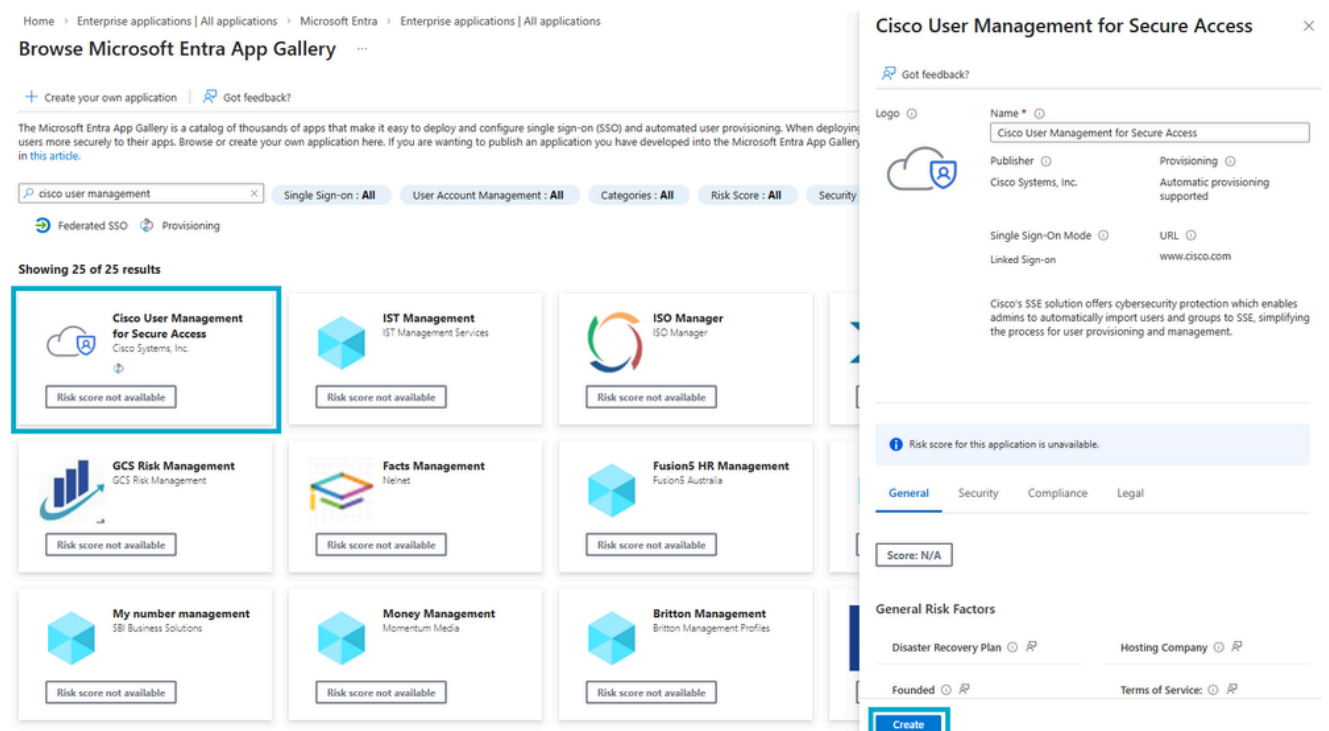
Una vez que haya generado sus credenciales en el panel de Cisco Secure Access, debe configurar los ajustes de aprovisionamiento dentro de su arrendatario de Microsoft Entra ID para habilitar la sincronización de usuarios y grupos.

1. Inicie sesión en [Entra ID](#).
2. Vaya a Aplicaciones de empresa > Nueva aplicación.



Nueva aplicación empresarial

3. En la Galería de aplicaciones de Entra, busque Administración de usuarios de Cisco para Secure Access y haga clic en Crear.



New App

4. Vaya a Usuarios y grupos > Agregar usuario/grupo.

The screenshot shows the Cisco User Management for Secure Access interface. The title is "Cisco User Management for Secure Access | Users and groups" with "Enterprise Application" below it. On the left, there is a navigation menu with "Overview", "Deployment Plan", "Diagnose and solve problems", and a "Manage" section containing "Properties", "Owners", "Roles and administrators", and "Users and groups" (which is highlighted with a blue box). The main content area has a top bar with a blue box around the "+ Add user/group" button, and other buttons for "Edit assignment", "Remove assignment", and a search icon. Below this is a light blue information box with an 'i' icon and the text: "The application will appear for assigned users within My Apps. Set 'visible to us". Underneath, it says "Assign users and groups to app-roles for your application here. To create new e". There is a search box containing "First 200 shown, search all users & groups". Below the search box is a table header "Display name" with a horizontal line. The table content shows "No application assignments found".

Introducir usuarios y grupos

5. Asigne los usuarios/grupos que desee aprovisionar a Cisco Secure Access y haga clic en Seleccionar y, a continuación, en Asignar.

## Add Assignment

MSFT

⚠ When you assign a group to an application, only users directly in the group will have access. Access does not cascade to nested groups.

### Users and groups

2 groups selected.

Select a role

User

Assign

## Users and groups



🔍 Try changing or adding filters if you don't see what you're looking for

Search

IT

2 results found

All Users Agent users Groups

	Name	Type
<input checked="" type="checkbox"/>	 IT-Admins	Group
<input checked="" type="checkbox"/>	 IT-Cloud-Admins	Group

Select

*Assign Users and Groups*

## 6. Vaya a Aprovisionamiento.

Home > Enterprise applications | All applications

## Cisco User Management for Secure Access | Overview

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators
  - Users and groups
  - Single sign-on
  - Provisioning**
  - Self-service
  - Custom security attributes

### Properties

Name: Cisco User Management for...

Application ID: dde39dfb-b7a9-4fc8-9aeb-...

Object ID: 2d3f9144-3d65-4235-9bd8-...

### Getting Started

- 1. Assign users and groups**  
Provide specific users and groups access to the applications  
[Assign users and groups](#)
- 2. Set up single sign on**  
Enable users to sign into their application using their Microsoft Entra credentials  
[Get started](#)
- 3. Provision User Accounts**  
Automatically create and delete user accounts in the application  
[Get started](#)

Aprovisionamiento de ID de entrada

7. Haga clic en Descripción general y luego en Nueva configuración.

Home > Enterprise applications | All applications

## Cisco User Management for Secure Access |

- Overview**
- Provision on demand

[+ New configuration](#) [Start provisioning](#)

**Get started**

This is a new version of the provisioning

Nueva configuración

8. Ingrese la URL del arrendatario y el token secreto guardados del paso #6 de la configuración de acceso seguro. Haga clic en Test Configuration y luego en Create. Después de crear la configuración, accederá a la página de detalles de la configuración para administrar los parámetros avanzados.

## New provisioning configuration

Microsoft Entra ID

Got feedback?

This is a new version of the provisioning user experience. You can provide us feedback and suggestions on the new user experience using the "Got feedback" button. [Click here to switch to the legacy experience.](#)

Create a provisioning configuration by completing the setup below. You can edit attribute mappings, scoping rules, and other settings later in the setup. [Learn more](#)

### Admin credentials

Create automatic provisioning configuration for "Cisco User Management for Secure Access". A successful test connection may be required to proceed.

Tenant URL

Secret token

Test connection

### Next steps:

After creating your configuration with default parameters, you will be taken to the configuration details page to manage advanced settings.

Create Cancel

Probar integración

Provisioning test connection  
Connection test for "Cisco User Management for Secure Access" was successful.

## 9. Vaya a Descripción general > Iniciar aprovisionamiento.

## Cisco User Management for Secure Access | Overview

Overview Start provisioning Pause provisioning Restart provisioning Delete configuration Refresh Got feedback?

Provision on demand

Get started Overview Properties

Iniciar aprovisionamiento

Start provisioning  
Start in progress

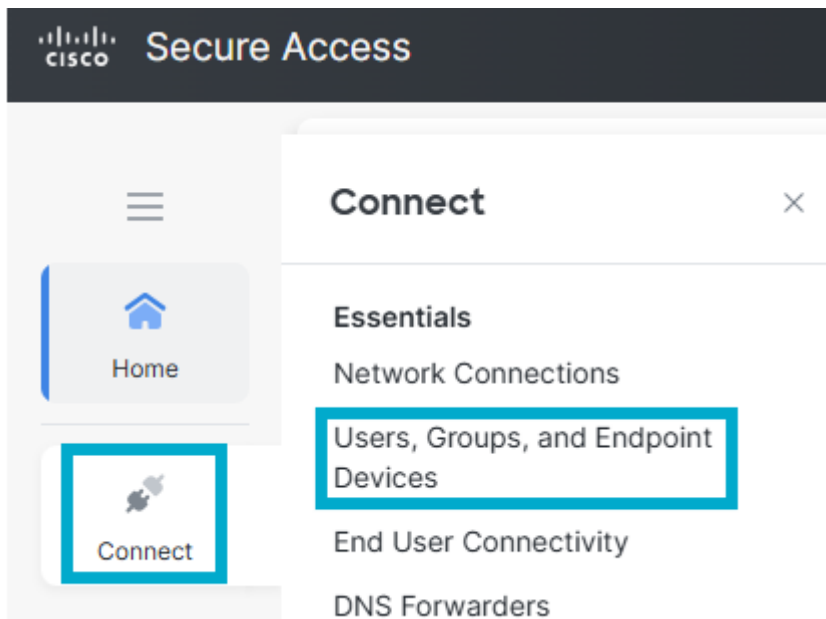


Nota: Si el ciclo de aprovisionamiento inicial no logra aprovisionar los usuarios/grupos, haga clic en Restart provisioning. Esta acción fuerza a Entra ID a intentar la primera sincronización de nuevo de sus usuarios y grupos.

## Verificación

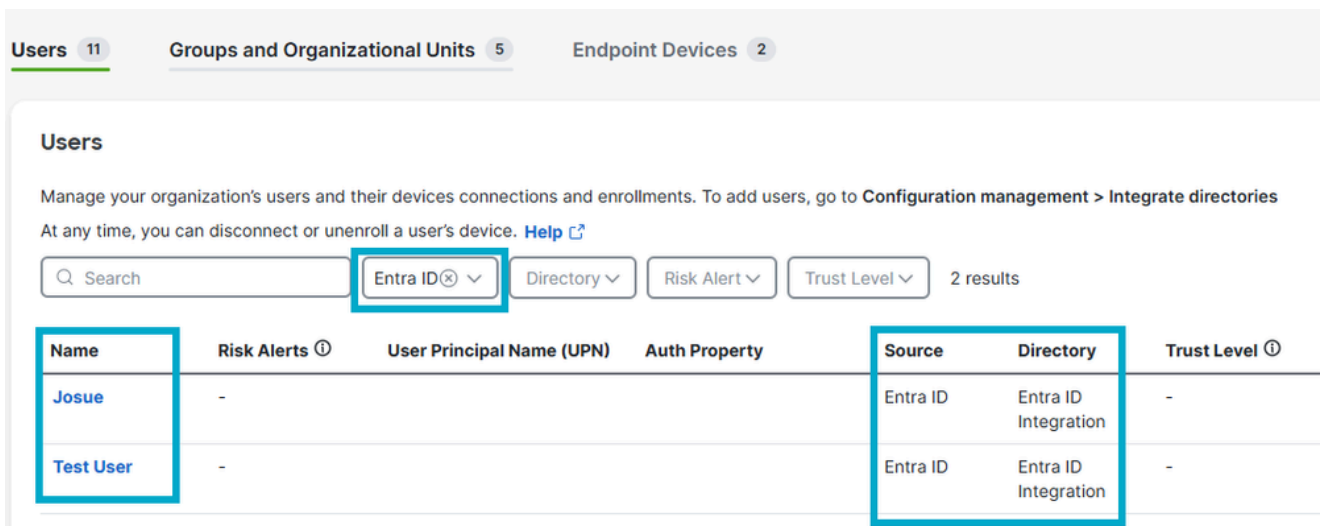
Veracidad en Cisco Secure Access

- Vaya a Connect > Users, Groups and Endpoint Devices.



Users and Groups in CSA

- Haga clic en Usuarios.



Verificar usuarios en CSA

- Haga clic en Grupos y unidades organizativas.

Users 11   **Groups and Organizational Units** 5   Endpoint Devices 2

5 Groups   0 Organizational Units

### Groups and Organizational Units

Manage your organization's groups and Organizational Units. To add new groups or OUs, go to **Configuration management > Integrate c**

Search   Type ▾   Source ▾   Entra ID Integration ⊗ ▾   2 results

Name	Type	Source	Directory
<a href="#">IT-Admins</a>	Groups	Entra ID	Entra ID Integration
<a href="#">IT-Cloud-Admins</a>	Groups	Entra ID	Entra ID Integration

Verify Groups in CSA

## Verificar en ID de entrada

- Navegue hasta Aplicaciones empresariales y haga clic en Administración de usuarios de Cisco para acceso seguro.

Home   Entra agents

**Favorites**

Entra ID

Overview

Users

Groups

Devices

Agent ID (Preview)

**Enterprise apps**

... > > > > New provisioning configuration > Cisco User Management for Secure Access

## Enterprise applications | All applications

MSFT

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications**
- Private Network connectors
- User settings
- App launchers
- Custom authentication extensions

Security

«   + New application   Refresh   Download

**Agent ID (Preview) has been moved to the Agent I**

View, filter, and search applications in your organization

The list of applications that are maintained by your or

Search: cisco user management

1 application found

Name

**Cisco User Management for Secure Access**

Verificar en entrada

- Haga clic en Provisioning.

The screenshot displays the Cisco User Management for Secure Access interface. On the left is a navigation sidebar with options like Home, Entra agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, and Roles & admins. The main content area shows the breadcrumb path: Enterprise applications | All applications > Cisco User Management for Secure Access. The title is 'Cisco User Management for Secure Access | Overview'. Below the title is a sub-menu with 'Overview' selected and 'Provisioning' highlighted with a red box. Other sub-menu items include Deployment Plan, Diagnose and solve problems, Manage, Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Self-service, and Custom security attributes. On the right, the 'Properties' section shows fields for Name, Application ID, and Object ID, each with a copy icon. Below that is the 'Getting Started' section with a card titled '1. Assign users and groups' and a link to 'Assign users and groups'.

*Verify in Entra ID*

- Haga clic en Descripción general.

# Cisco User Management for Secure Access | Overview

Start provisioning | Pause provisioning | Restart provisioning | Delete configuration | Refresh

This is a new version of the provisioning user experience. You can provide us feedback and suggestions on the new user

Get started | **Overview** | Properties

### Basic information

Name: Cisco User Management for Secure Access

Service principal object id

Job ID

Last cycle completed time: 3/18/2026, 10:27:27 AM

### Current cycle status

Current cycle status: Incremental sync completed > Provisioning details

100% completed

GROUP	USER
2	2

Verify Provisioning in Entra

- Haga clic en Provisioning logs.

# Cisco User Management for Secure Access | Provisioning logs

Download | Refresh | Manage view | Got feedback?

Search Identity

Show dates as: Local | Date range: Last 24 hours | Action: All | Status: All

Date ↓	Identity	Action	Source system
3/18/26, 8:32:41 AM	Display name IT-Admins	Update	Microsoft Entra ID
3/18/26, 8:32:41 AM	Display name IT-Cloud-Admins	Update	Microsoft Entra ID
3/18/26, 8:32:39 AM	Display name IT-Admins	Create	Microsoft Entra ID
3/18/26, 8:32:39 AM	Display name IT-Cloud-Admins	Create	Microsoft Entra ID
3/18/26, 8:32:37 AM	Display name Test User	Create	Microsoft Entra ID
3/18/26, 8:32:37 AM	Display name Josue	Create	Microsoft Entra ID

## Información Relacionada

[Configurar proveedores de identidad](#)

[Aprovisione usuarios y grupos desde el ID de Microsoft Entry](#)

## 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).