

Provision Users and Groups to Secure Access via Entra ID

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Configure Cisco Secure Access](#)

[Configure Provisioning in Microsoft Entra ID](#)

[Verify](#)

[Verify in Cisco Secure Access](#)

[Verify in Entra ID](#)

[Related Information](#)

Introduction

This document describes how to provision users and groups from Entra ID to Cisco Secure Access.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Access
- Entra ID

Components Used

This document is not restricted to specific software and hardware versions.

- Admin Access to Cisco Secure Access Dashboard

- Admin Access to Entra ID dashboard

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Cisco Secure Access supports the provisioning of users and groups from Microsoft Entra ID (formerly Azure Active Directory).

This provisioning enables Secure Access to maintain a directory of users authorized to:

- Enroll in Zero Trust Access (ZTA).
- Connect to VPNaaS.
- Apply identity-based policies to Umbrella Roaming users.



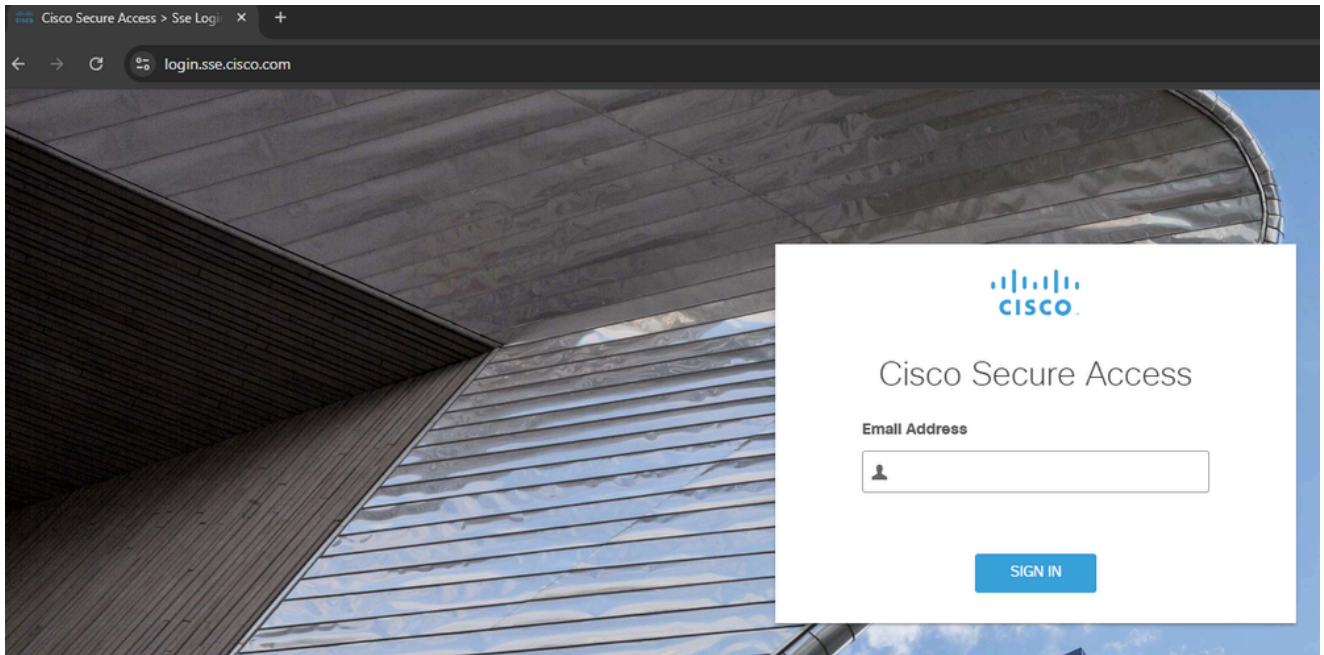
Note: This document focuses specifically on the provisioning of users and groups from Entra ID. The configuration of Entra ID or other Identity Providers (IdP) for ZTA enrollment, VPNaaS authentication, or specific Umbrella Roaming settings is outside the scope of this guide.

Configure

Configure Cisco Secure Access

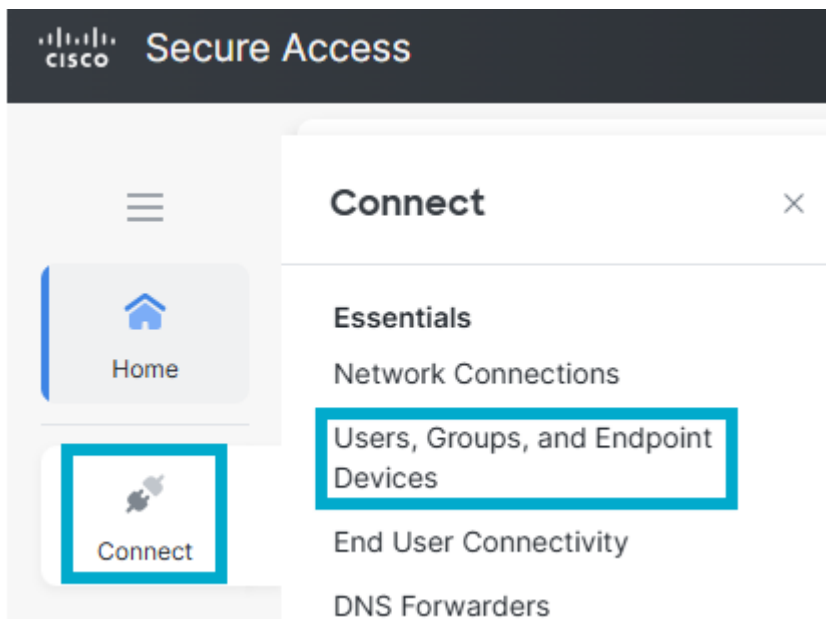
In order to begin the provisioning process, you must first configure the directory integration within the Cisco Secure Access dashboard. This step generates the necessary credentials and configuration parameters required to establish a secure connection with Microsoft Entra ID.

1. Sign in to the **Cisco Secure Access [Dashboard](#)**.



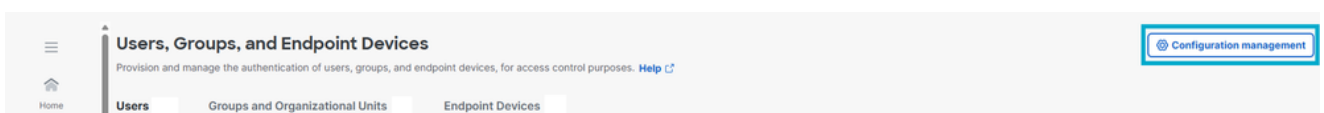
Sign in to CSA

2. Navigate to **Connect > Users, Groups and Endpoint Devices**.

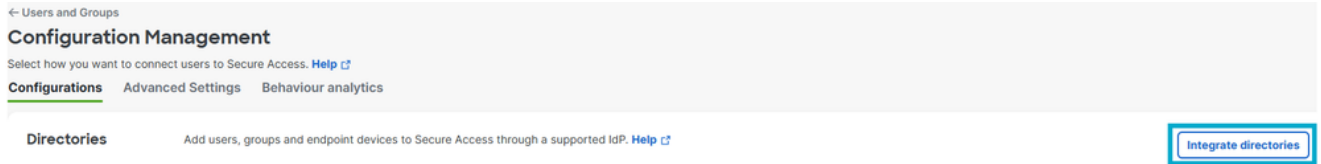


Users and Groups

3. Click **Configuration management**.



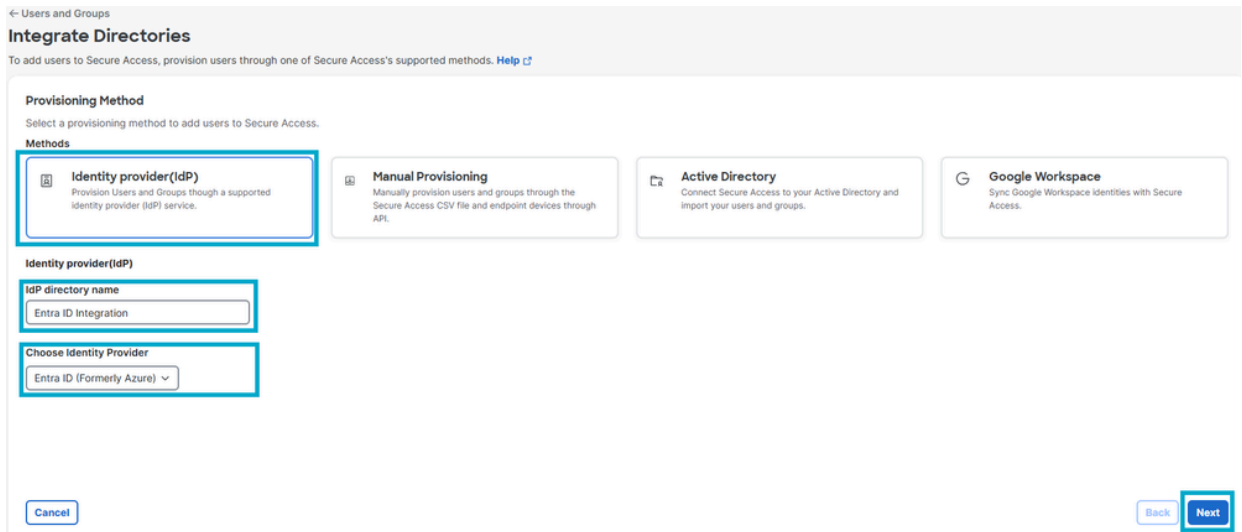
4. Click **Integrate Directory**.



Integrate Directory

5. Under **Provision Method** click **Identity Provider**.

- **IdP directory name: Entra ID Integration.**
- **Choose Identity Provider: Entra ID (Formerly Azure).**
- **Click Next.**



Directory Configuration

6. Click **Generate token**. Save the **generated token** and the **provisioning URL**, then click **Done**.

[← 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](#)

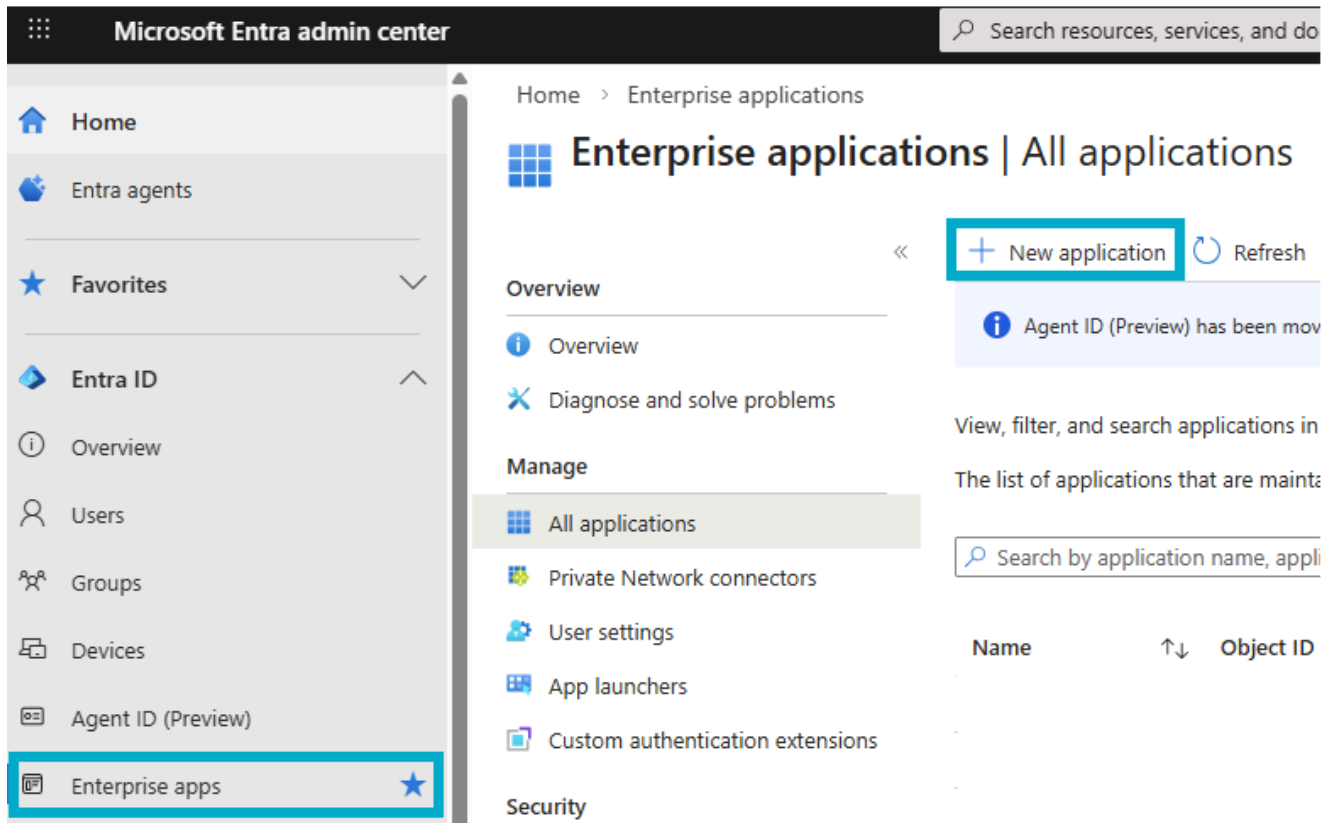
[Cancel](#) [Back](#) [Done](#)

Generate Token

Configure Provisioning in Microsoft Entra ID

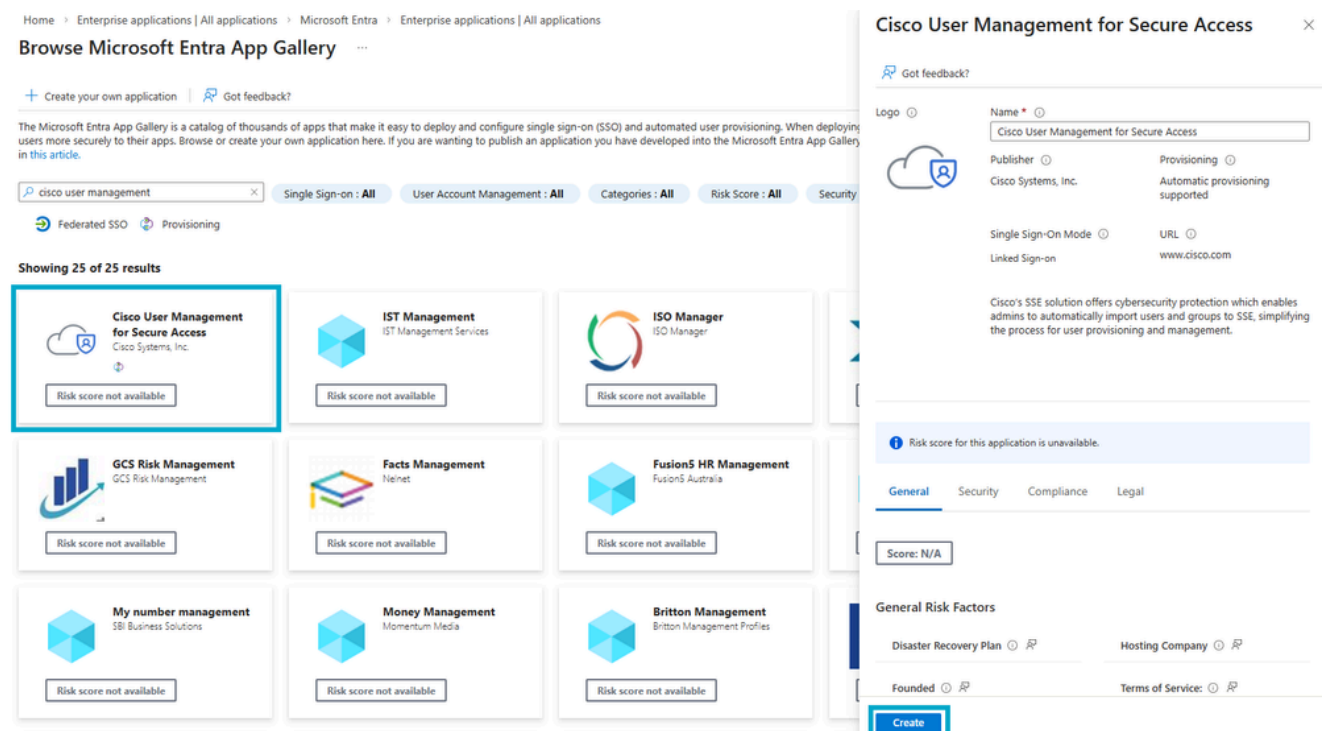
Once you have generated your credentials in the Cisco Secure Access dashboard, you must configure the provisioning settings within your Microsoft Entra ID tenant to enable the synchronization of users and groups.

1. Sign in to [Entra ID](#).
2. Navigate to **Enterprise Apps > New Application**.



New Enterprise App

3. In the **Entra App Gallery** look for **Cisco User Management for Secure Access** and click **Create**.



New App

4. Navigate to **Users and Groups > Add user/group**.

Cisco User Management for Secure Access | Users and groups
Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

Properties
Owners
Roles and administrators
Users and groups

« + Add user/group Edit assignment Remove assignment

[The application will appear for assigned users within My Apps. Set 'visible to us](#)

Assign users and groups to app-roles for your application here. To create new e

First 200 shown, search all users & groups

Display name

No application assignments found

Entra Users and Groups

5. Assign the **users/groups** you want to provision to Cisco Secure Access and click **Select** and then **Assign**.

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

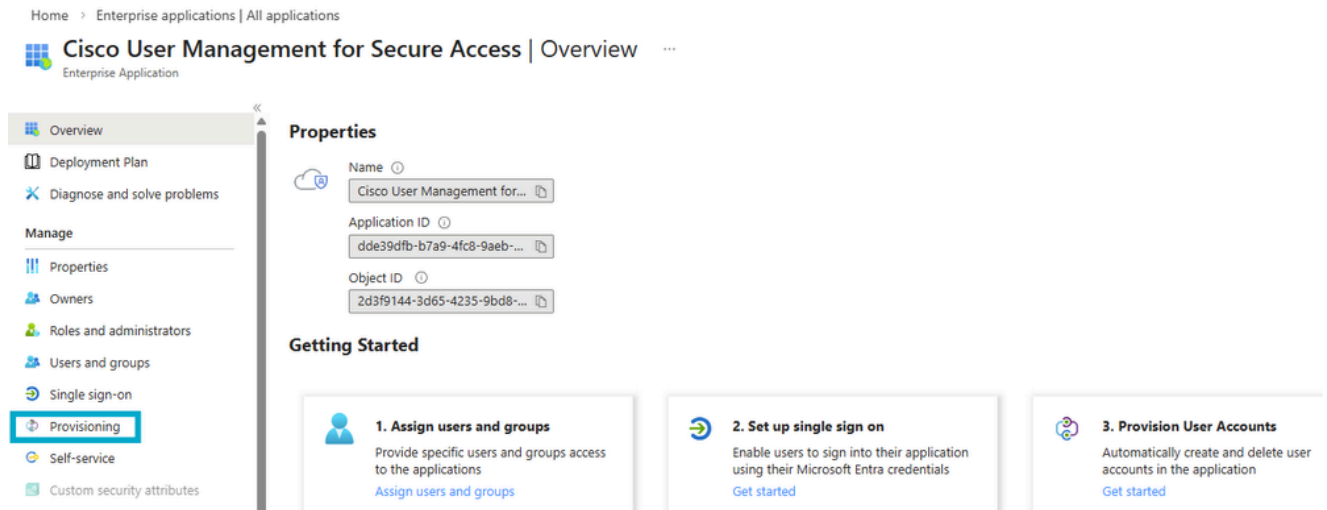
All Users Agent users Groups

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

Select

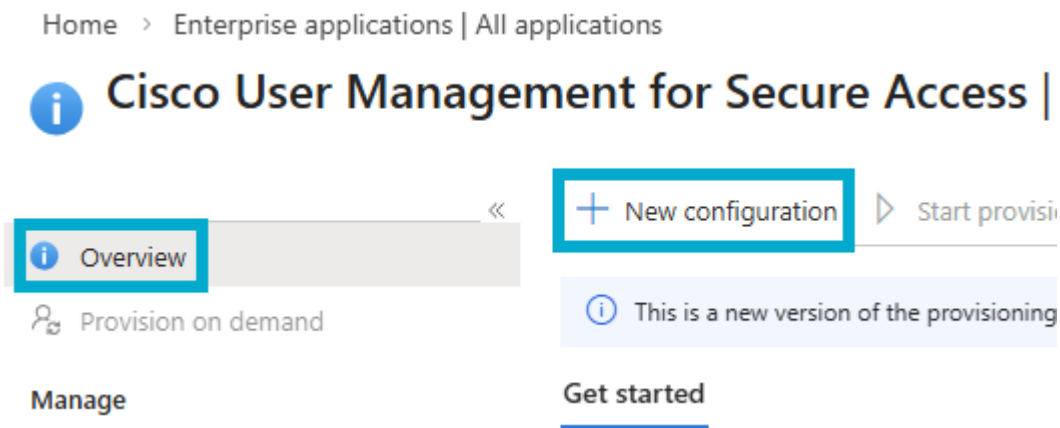
Assign Users and Groups

6. Navigate to **Provisioning**.



Entra ID Provisioning

7. Click **Overview** and then **New Configuration**.



New Configuration

8. Enter the **Tenant URL** and **Secret Token** saved from step #6 of the Secure Access Configuration. Click **Test Configuration** and then **Create**.
After creating your configuration, you are taken to the configuration details page to manage advanced settings.

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

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

Test Integration

9. Navigate to Overview > Start Provisioning.

Home > Enterprise applications | All applications > Cisco User Management for Secure Access | Overview > New provisioning configuration

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

Start provisioning
Start in progress

Start Provisioning

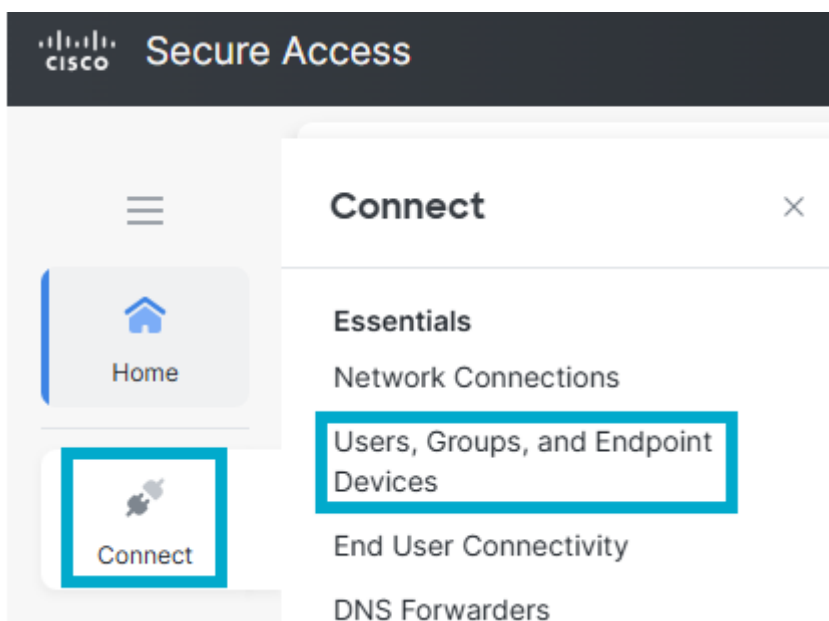


Note: If the initial provisioning cycle fails to provision the users/groups, click Restart provisioning. This action forces Entra ID to attempt the the first synchronization again of your users and groups.

Verify

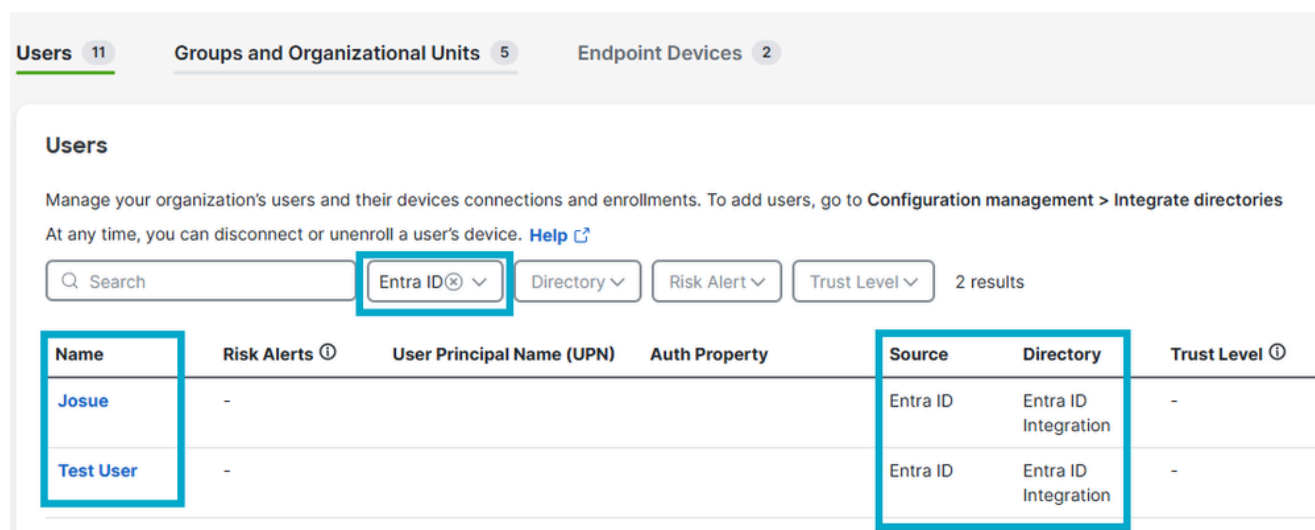
Verify in Cisco Secure Access

- Navigate to **Connect > Users, Groups and Endpoint Devices**.



Users and Groups in CSA

- Click **Users**.



Verify Users in CSA

- Click **Groups and Organizational Units**.

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**

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

Name	Type	Source	Directory
IT-Admins	Groups	Entra ID	Entra ID Integration
IT-Cloud-Admins	Groups	Entra ID	Entra ID Integration

Verify Groups in CSA

Verify in Entra ID

- Navigate to **Enterprise Apps** and click **Cisco User Management for Secure Access**.

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

« + New application Refresh Download

Overview

- Overview
- Diagnose and solve problems

Manage

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

Security

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 organization.

cisco user management

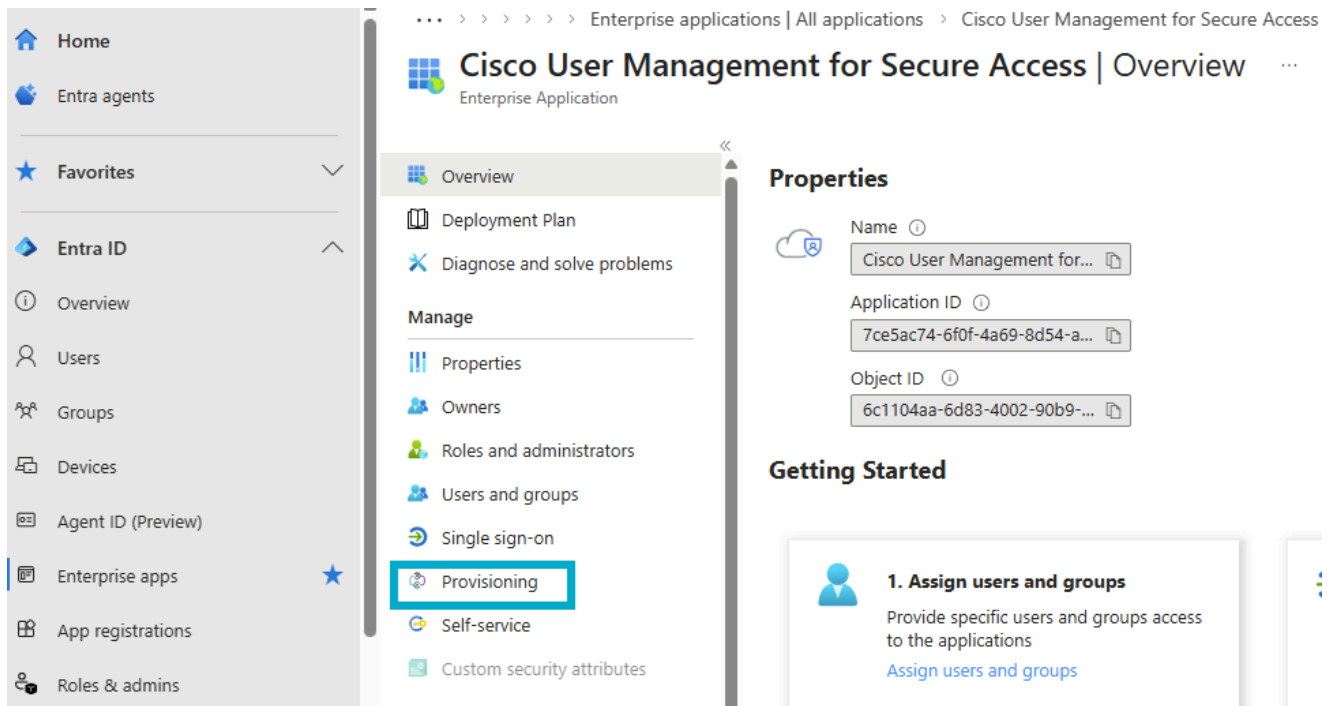
1 application found

Name

Cisco User Management for Secure Access

Verify in Entra

- Click **Provisioning**.



Verify in Entra ID

- Click **Overview**.

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

- Click **Provisioning logs**.

Cisco User Management for Secure Access | Provisioning logs

Download | Refresh | Manage view | Got feedback?

Search Identity | Add filter

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	Disolav 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

Related Information

[Configure Identity Providers](#)

[Provision Users and Groups from Microsoft Entra ID](#)