

# Configurer les utilisateurs et les groupes pour sécuriser l'accès via un ID supplémentaire

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Configuration de Cisco Secure Access](#)

[Configurer la mise en service dans Microsoft Entra ID](#)

[Vérifier](#)

[Verity dans Cisco Secure Access](#)

[Vérifier dans l'ID d'entrée](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit comment provisionner des utilisateurs et des groupes à partir de l'ID d'entrée vers Cisco Secure Access.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès sécurisé Cisco
- ID d'entrée

### Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

- Accès administrateur au tableau de bord Cisco Secure Access
- Accès administrateur au tableau de bord Entra ID

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Cisco Secure Access prend en charge l'approvisionnement des utilisateurs et des groupes à partir de Microsoft Entra ID (anciennement Azure Active Directory).

Cette mise en service permet à Secure Access de gérer un répertoire d'utilisateurs autorisés à :

- Inscrivez-vous au programme ZTA (Zero Trust Access).
- Se connecter à VPNaaS.
- Appliquez des politiques basées sur l'identité aux utilisateurs d'Umbrella Roaming.



Remarque : Ce document se concentre spécifiquement sur l'approvisionnement des utilisateurs et des groupes à partir de l'ID d'entrée. La configuration d'Entra ID ou d'autres fournisseurs d'identité (IdP) pour l'inscription ZTA, l'authentification VPNaaS ou des paramètres d'itinérance Umbrella spécifiques n'est pas traitée dans ce guide.

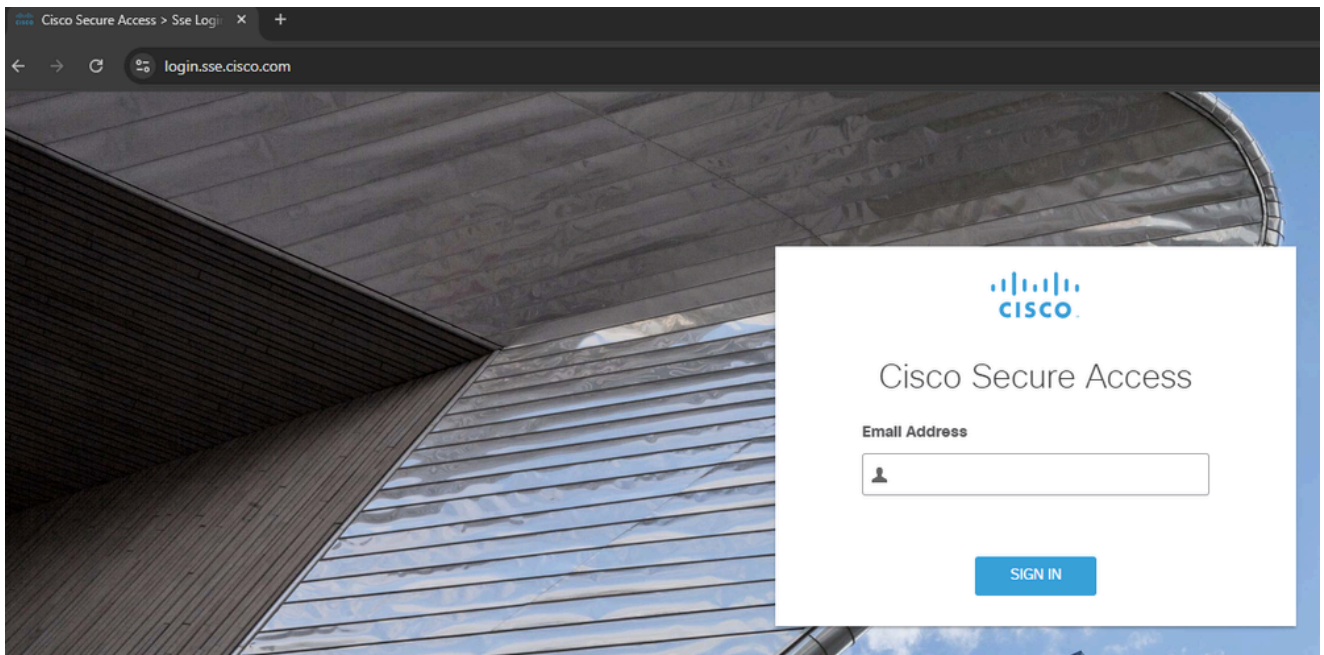
---

## Configurer

### Configuration de Cisco Secure Access

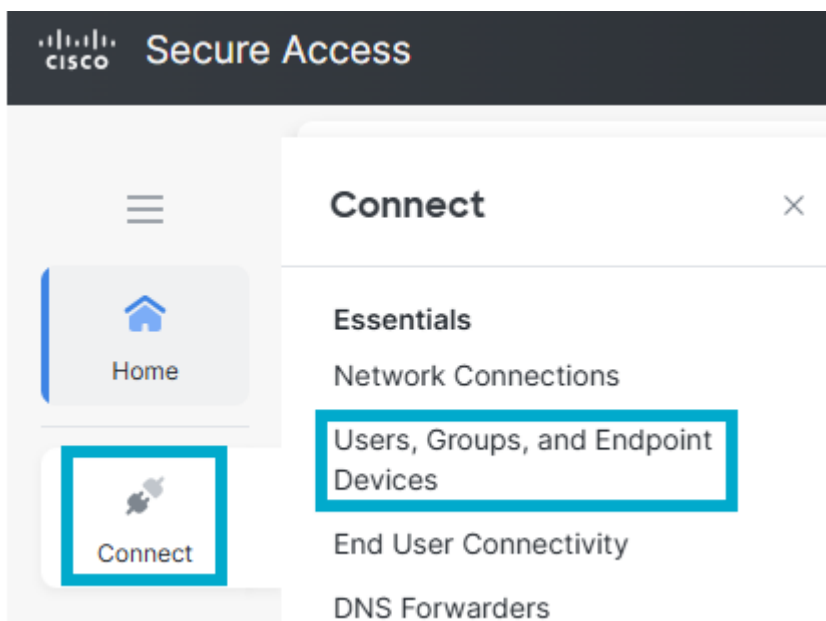
Afin de commencer le processus de mise en service, vous devez d'abord configurer l'intégration du répertoire dans le tableau de bord Cisco Secure Access. Cette étape génère les informations d'identification et les paramètres de configuration nécessaires pour établir une connexion sécurisée avec Microsoft Entra ID.

1. Connectez-vous au tableau de [bord Cisco Secure Access](#).



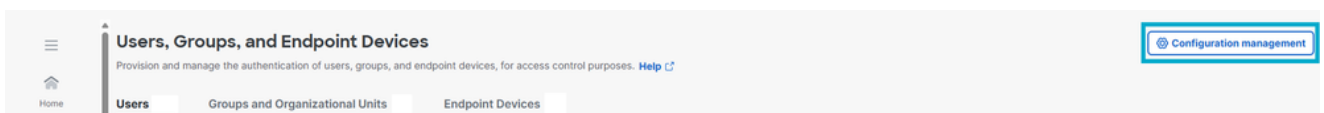
*Se connecter à CSA*

2. Naviguez jusqu'à **Connect > Users, Groups and Endpoint Devices**.

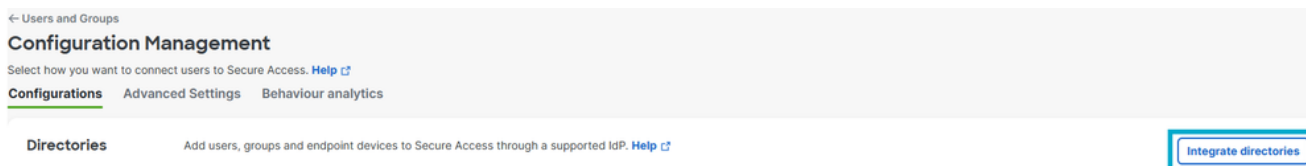


*Utilisateurs et groupes*

3. Cliquez sur **Gestion de la configuration**.



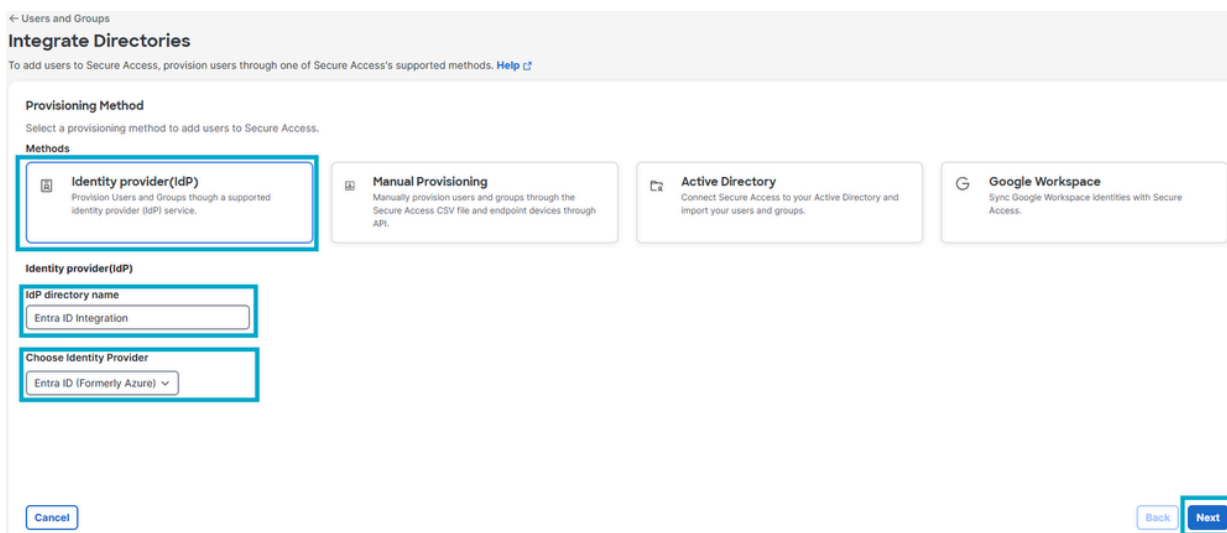
4. Cliquez sur **Intégrer le répertoire.**



*Integrate Directory*

5. Sous **Méthode de provisionnement**, cliquez sur **Fournisseur d'identité.**

- **Nom du répertoire IdP : Intégration de l'ID.**
- **Choisir un fournisseur d'identité : Entra ID (anciennement Azure).**
- Cliquez sur **Suivant.**



*Configuration du répertoire*

6. Cliquez sur **Generate token**. Enregistrez le **jeton généré** et l'**URL d'approvisionnement**, puis cliquez sur **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](#)

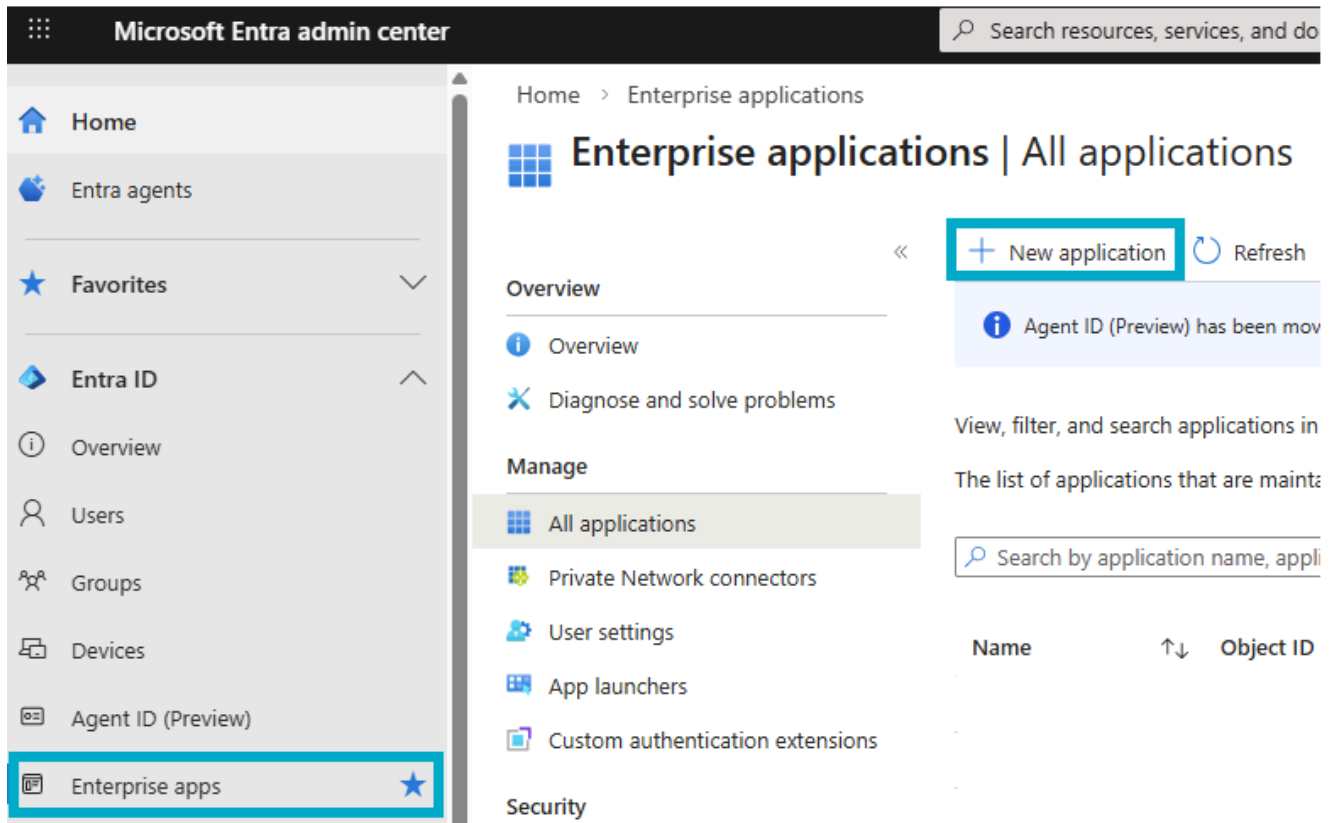
[Cancel](#) [Back](#) [Done](#)

*Générer un jeton*

## Configurer la mise en service dans Microsoft Entra ID

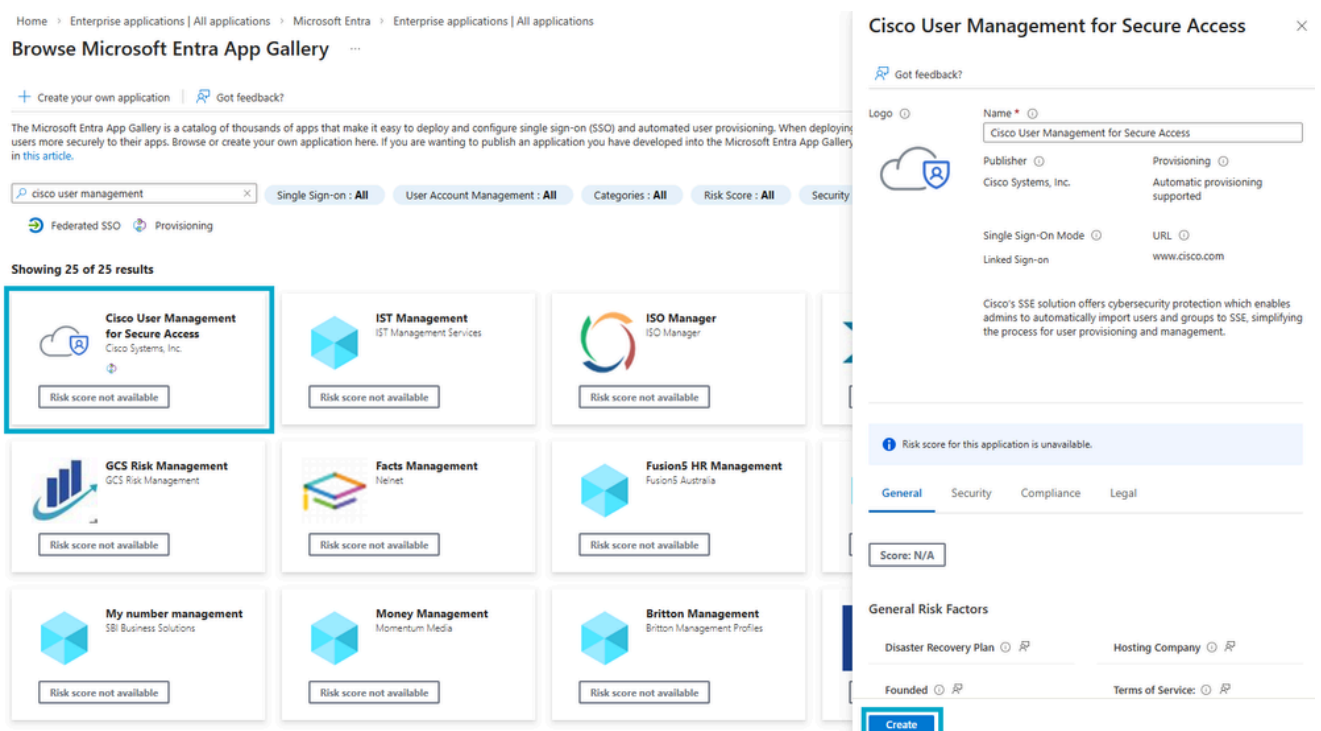
Une fois que vous avez généré vos informations d'identification dans le tableau de bord Cisco Secure Access, vous devez configurer les paramètres d'approvisionnement dans votre locataire Microsoft Entra ID pour activer la synchronisation des utilisateurs et des groupes.

1. Connectez-vous à [Entra ID](#).
2. Accédez à Applications d'entreprise > Nouvelle application.



Nouvelle application d'entreprise

3. Dans la galerie d'applications Entra, recherchez Cisco User Management for Secure Access et cliquez sur Create.



New App

4. Accédez à Utilisateurs et groupes > Ajouter un utilisateur/groupe.

The screenshot displays the Cisco User Management for Secure Access interface. The main heading is "Cisco User Management for Secure Access | Users and groups" with "Enterprise Application" below it. On the left, a navigation menu includes "Overview", "Deployment Plan", "Diagnose and solve problems", and a "Manage" section with "Properties", "Owners", "Roles and administrators", and "Users and groups" (highlighted with a blue box). The main content area features a toolbar with "Add user/group" (highlighted with a blue box), "Edit assignment", and "Remove assignment". Below the toolbar is an information message: "The application will appear for assigned users within My Apps. Set 'visible to us". A search bar contains the text "First 200 shown, search all users & groups". A table header "Display name" is visible, followed by the text "No application assignments found".

Utilisateurs et groupes supplémentaires

5. Attribuez les utilisateurs/groupe que vous souhaitez provisionner à Cisco Secure Access et cliquez sur Select, puis sur 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

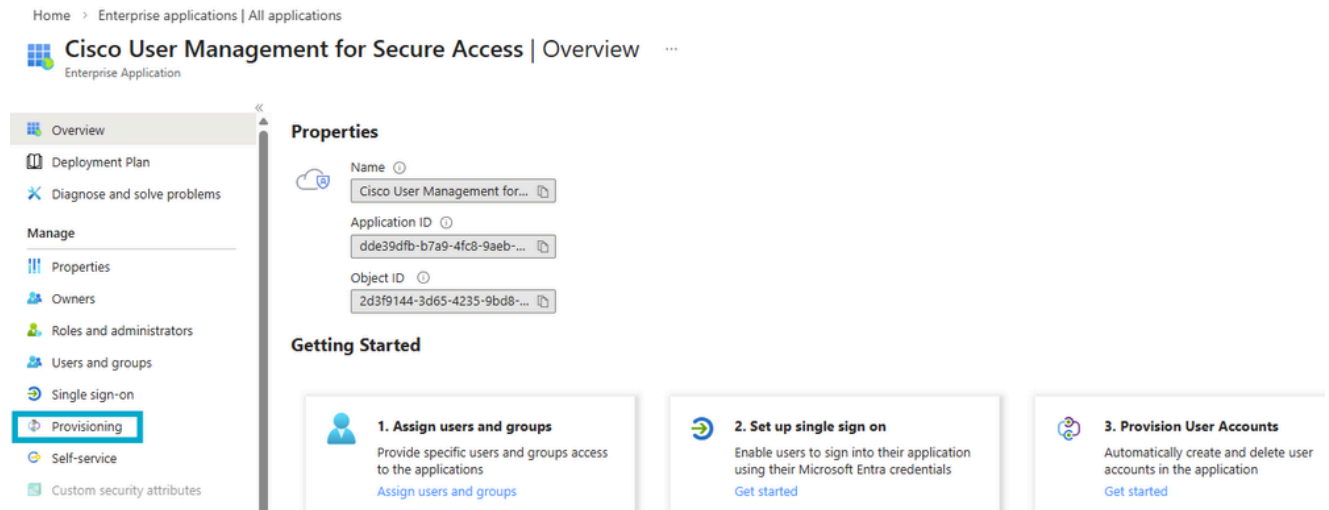
All Users Agent users Groups

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

Select

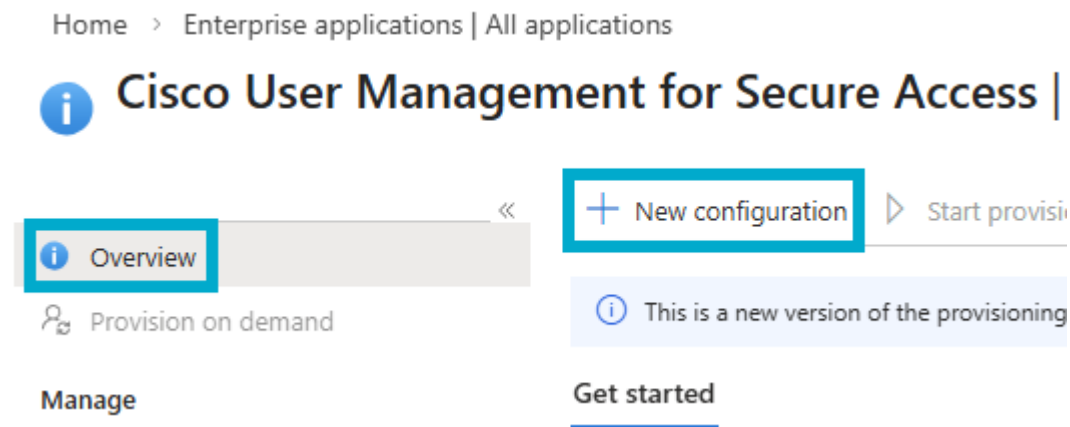
*Assign Users and Groups*

## 6. Accédez à Provisioning.



Provisionnement d'ID supplémentaire

7. Cliquez sur Overview, puis sur New Configuration.



Nouvelle configuration

8. Entrez l'URL du locataire et le jeton secret enregistrés à l'étape #6 de la configuration d'accès sécurisé. Cliquez sur Test Configuration, puis sur Create.

Après avoir créé votre configuration, vous accédez à la page des détails de configuration pour gérer les paramètres avancés.

## 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.

## Intégration des tests

## 9. Accédez à Overview > Start Provisioning.

## Cisco User Management for Secure Access | Overview

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

Provision on demand

Manage Get started Overview Properties

Start provisioning  
Start in progress

## Démarrer le provisionnement

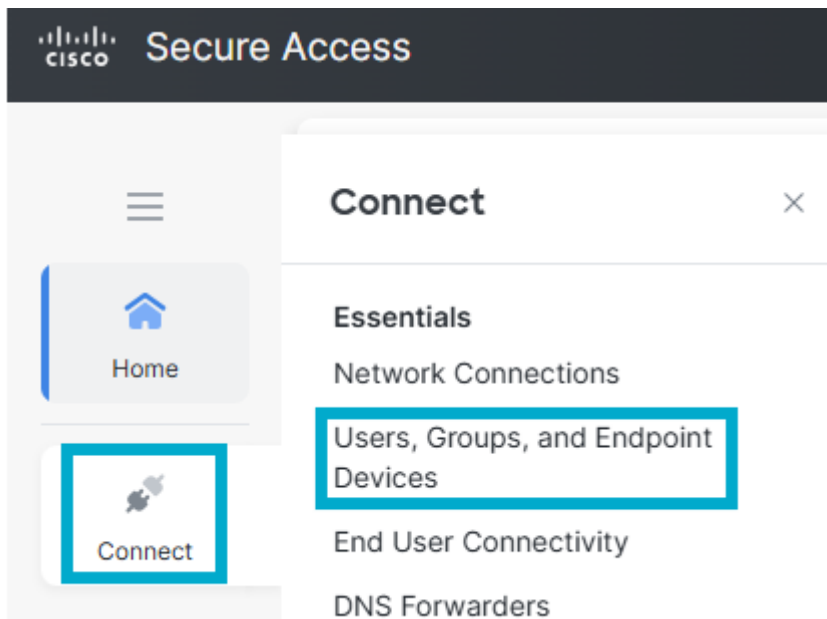


Remarque : Si le cycle d'approvisionnement initial ne permet pas d'approvisionner les utilisateurs/groupes, cliquez sur [Restart provisioning](#). Cette action force Entra ID à tenter à nouveau la première synchronisation de vos utilisateurs et groupes.

## Vérifier

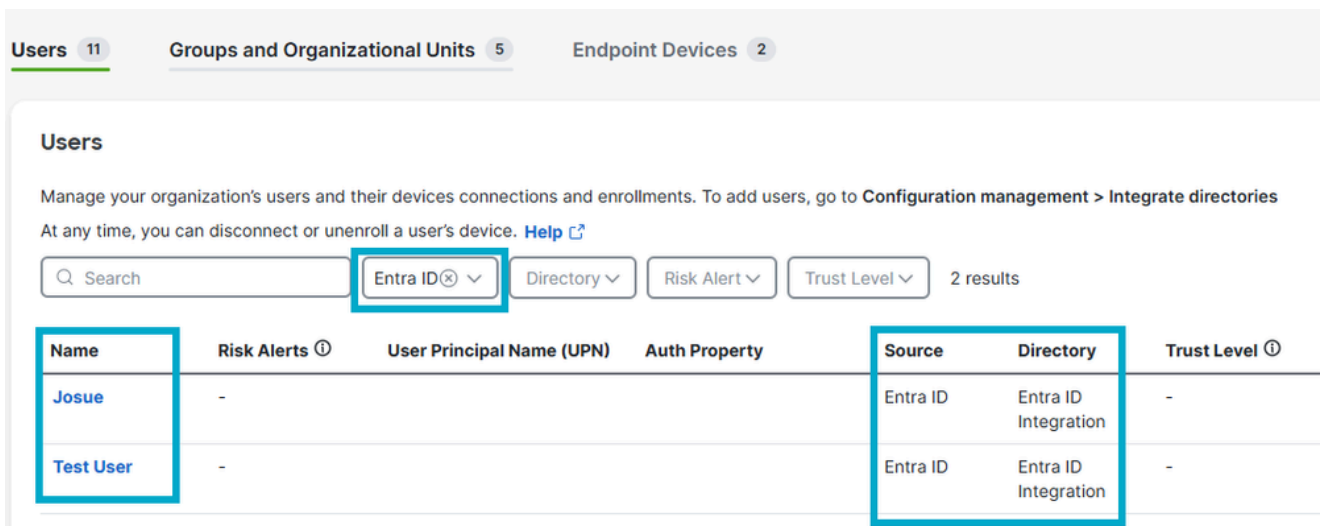
## Verity dans Cisco Secure Access

- Naviguez jusqu'à Connect > Users, Groups and Endpoint Devices.



Users and Groups in CSA

- Cliquez sur Utilisateurs.



Vérifier les utilisateurs dans CSA

- Cliquez sur Groupes et unités d'organisation.

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

## Vérifier dans l'ID d'entrée

- Accédez à Enterprise Apps et cliquez sur 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.

Search: cisco user management

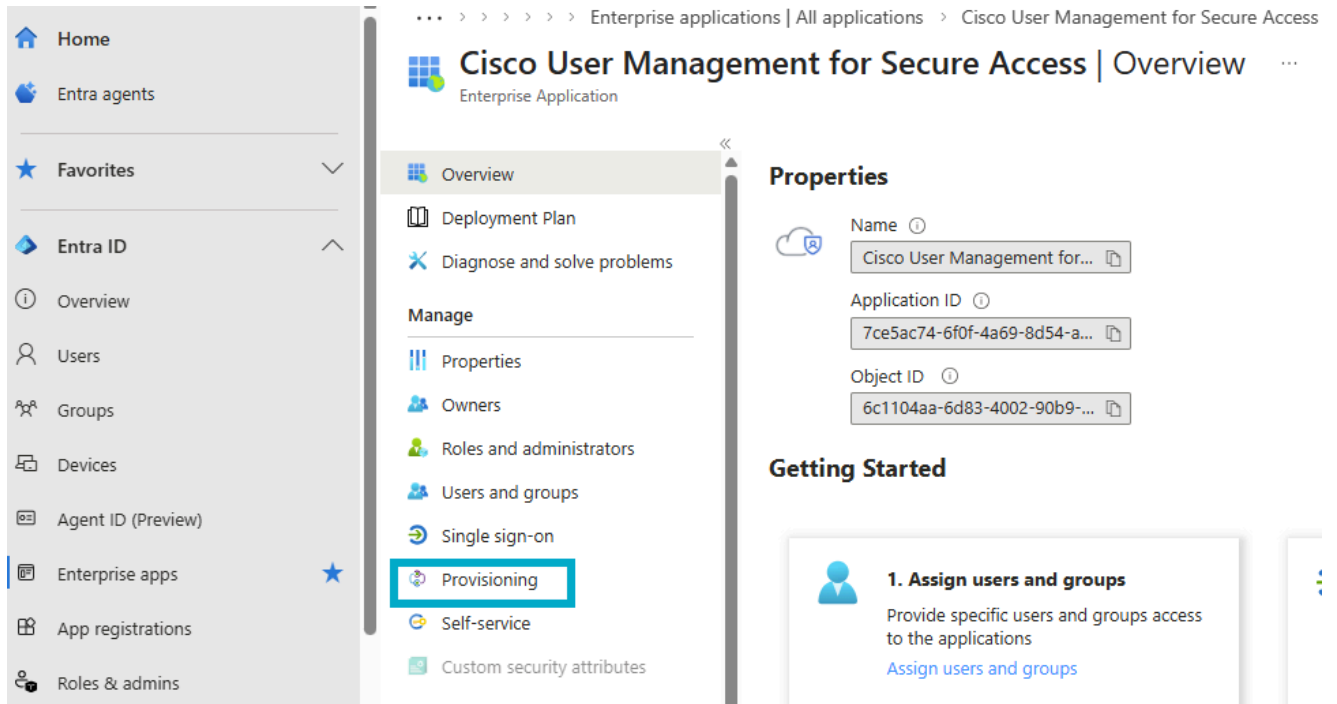
1 application found

Name

- Cisco User Management for Secure Access**

Vérifier dans Entra

- Cliquez sur Provisioning.



*Verify in Entra ID*

- Cliquez sur 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: 2 | USER: 2

Verify Provisioning in Entra

- Cliquez sur 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

## Informations connexes

[Configurer les fournisseurs d'identité](#)

[Attribuer des privilèges d'accès aux utilisateurs et aux groupes à partir de Microsoft Entra ID](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.