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

Table des matières

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.

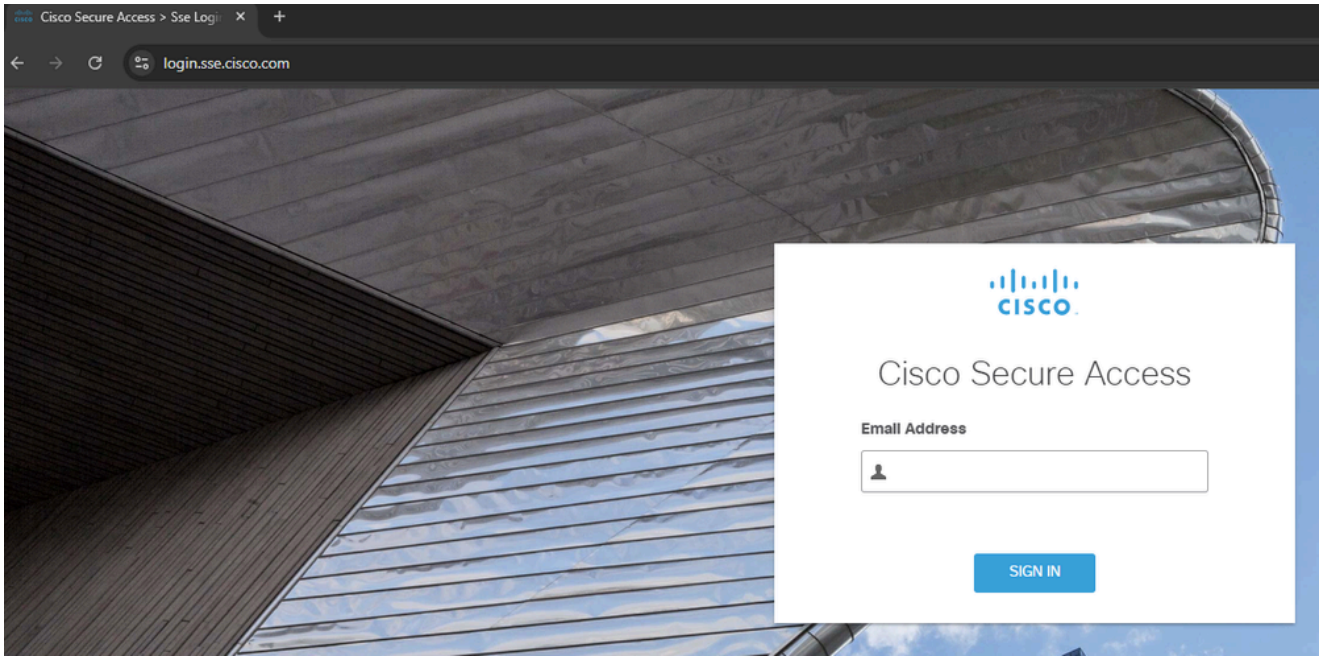
Remarque : Ce document se concentre spécifiquement sur l'approvisionnement des utilisateurs et des groupes à partir de l'ID d'entrée. La configuration d'Entra ID ou d'autres fournisseurs d'identité (IdP) pour l'inscription ZTA, l'authentification VPNaaS ou des paramètres d'itinérance Umbrella spécifiques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

Configurer

Configuration de Cisco Secure Access

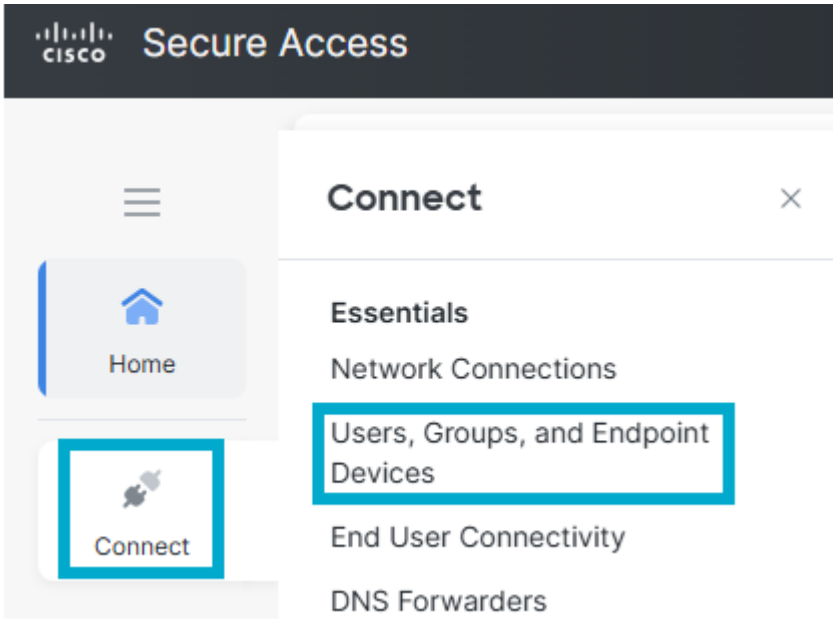
Afin de commencer le processus de mise en service, vous devez d'abord configurer l'intégration du répertoire dans le tableau de bord Cisco Secure Access. Cette étape génère les informations d'identification et les paramètres de configuration nécessaires pour établir une connexion sécurisée avec Microsoft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

1. Connectez-vous au tableau de **bord Cisco Secure Access**.



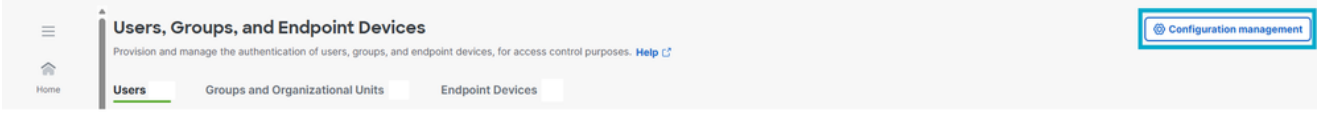
Se connecter à CSA

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



Utilisateurs et groupes

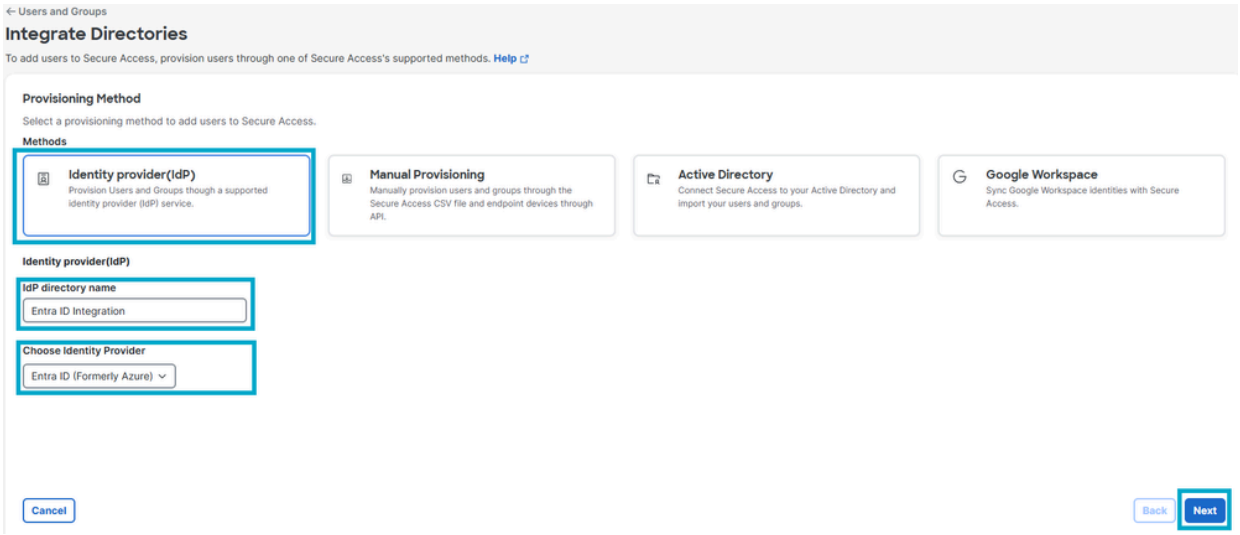
3. Cliquez sur **Gestion de la configuration**.



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

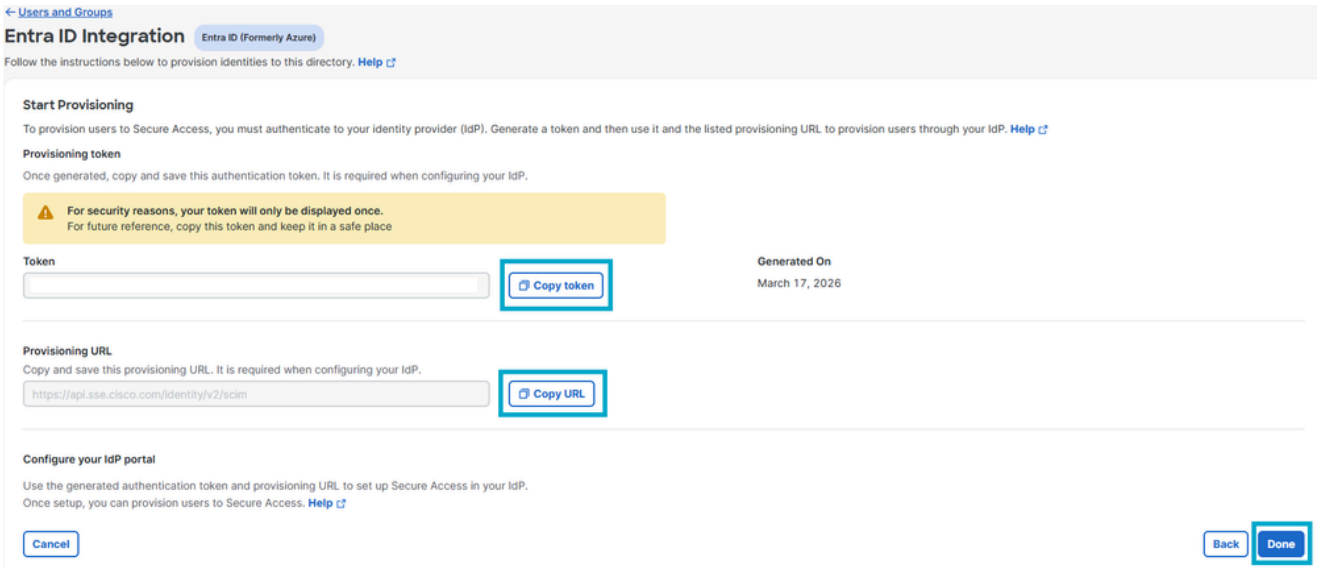
Integrate Directory

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**.



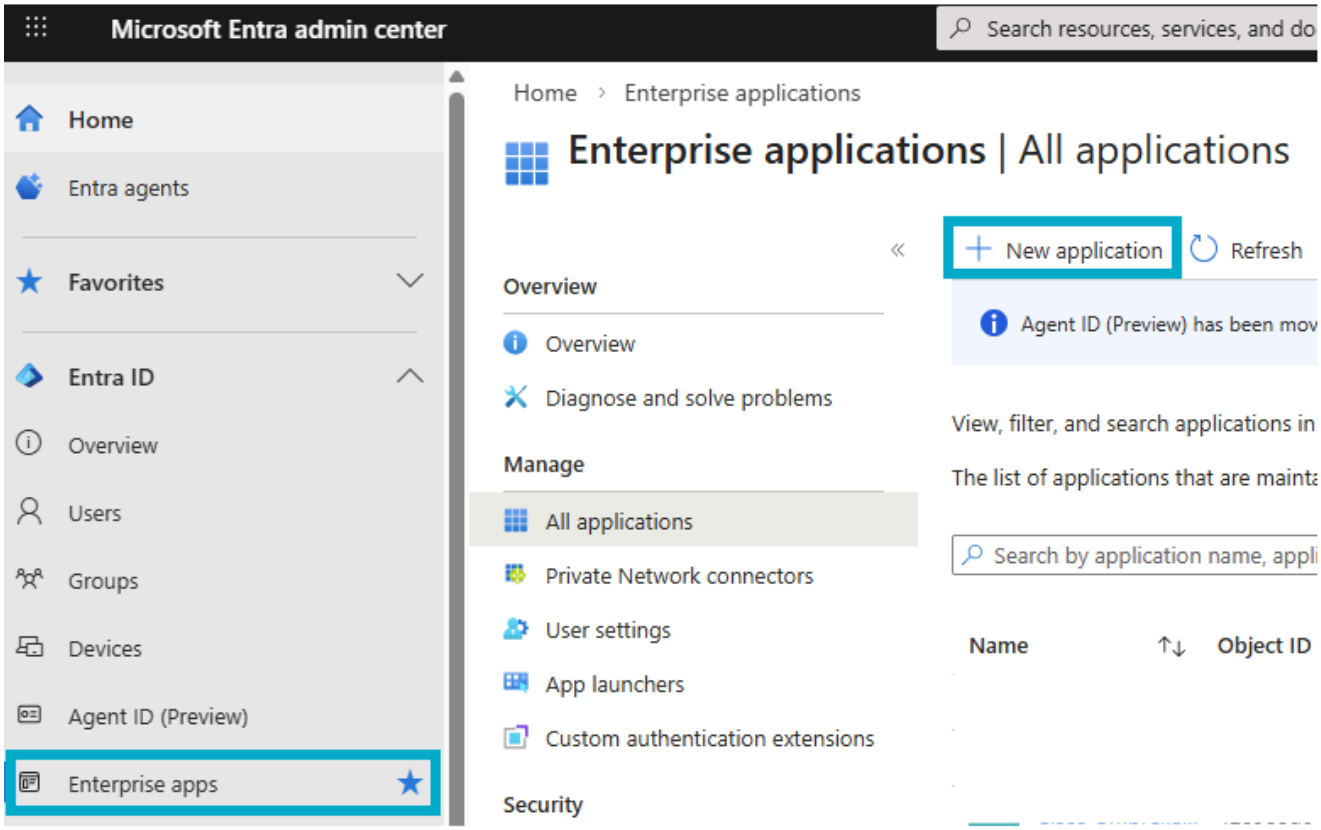
Générer un jeton

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.

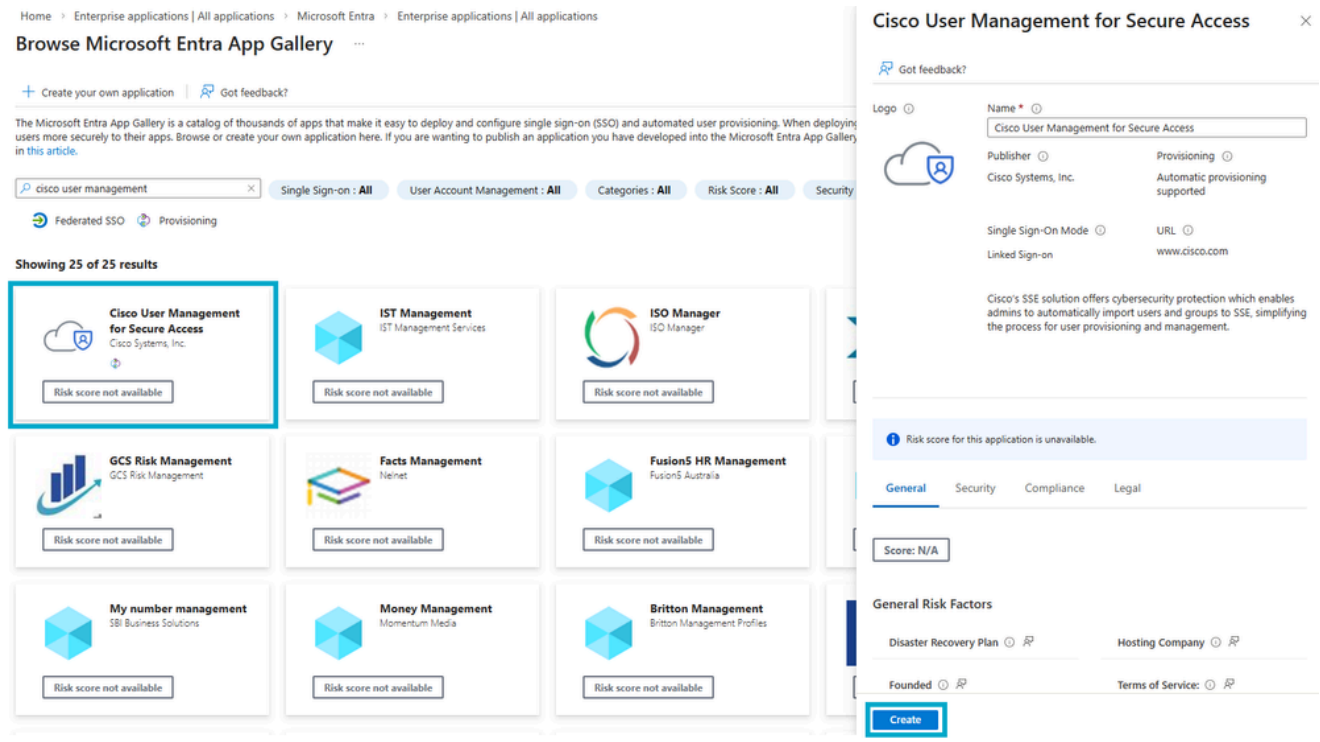
1. Connectez-vous à Entra ID.

2. Accédez à Applications d'entreprise > Nouvelle application.



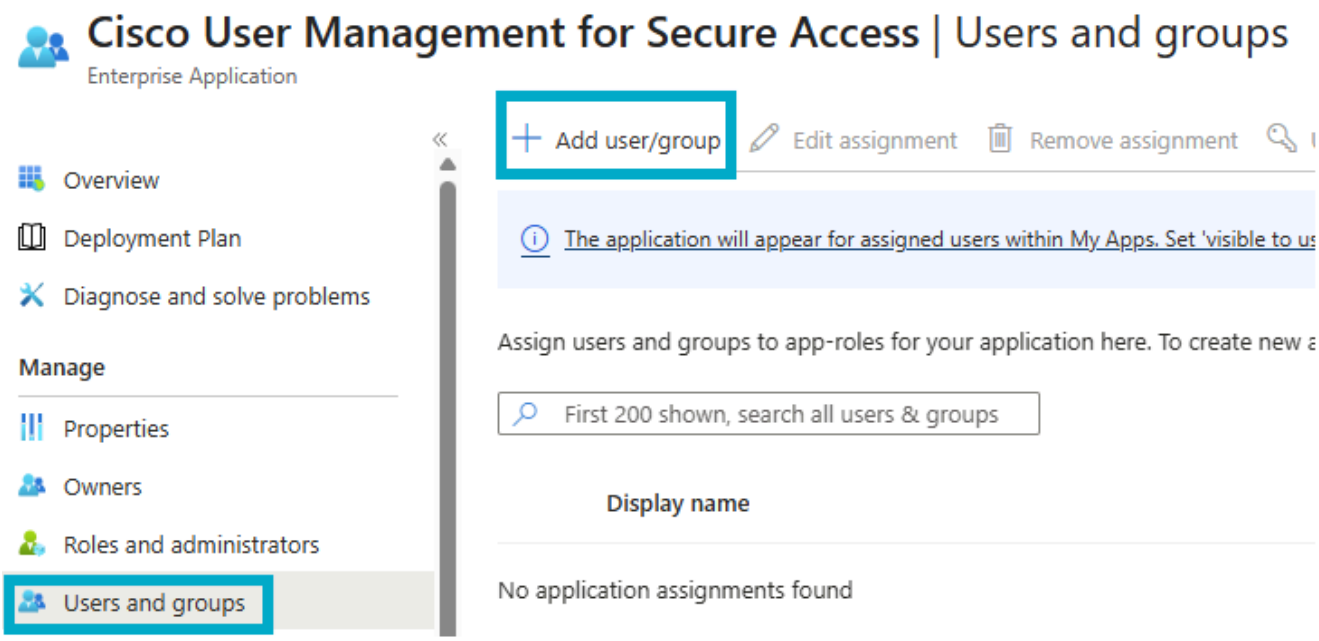
Nouvelle application d'entreprise

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



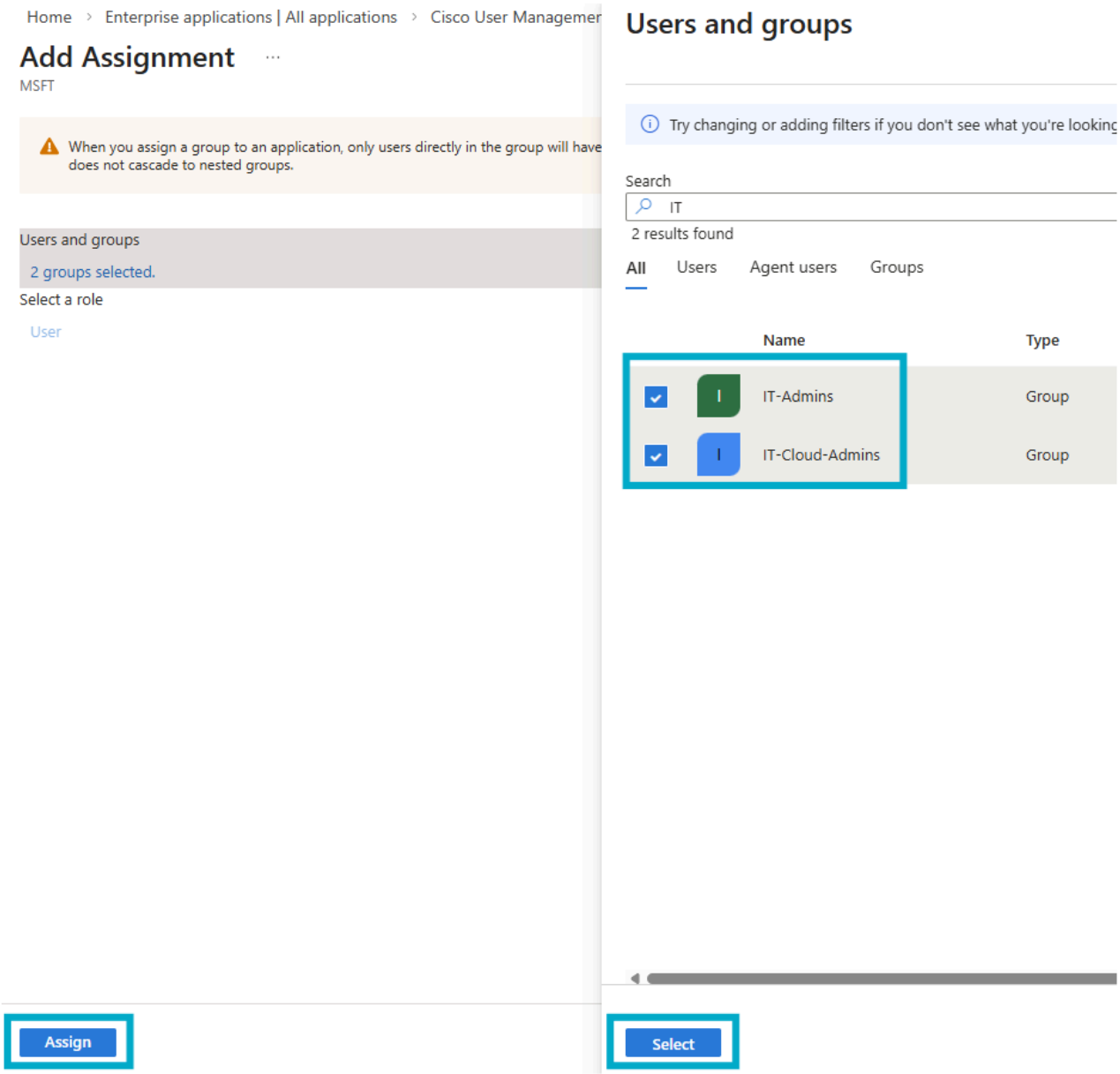
New App

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



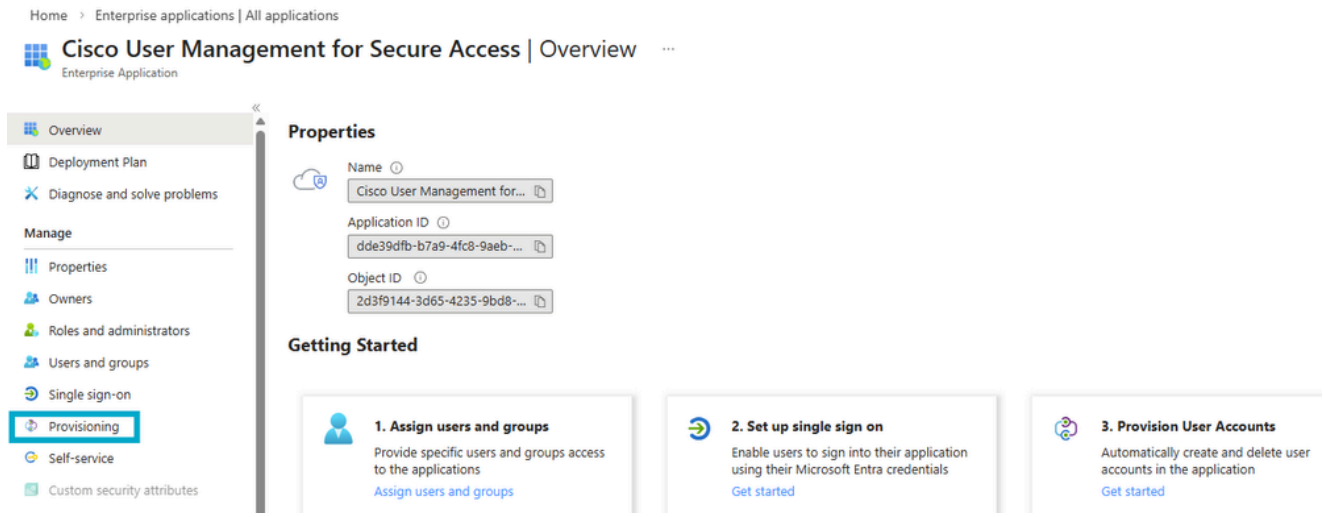
Utilisateurs et groupes supplémentaires

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



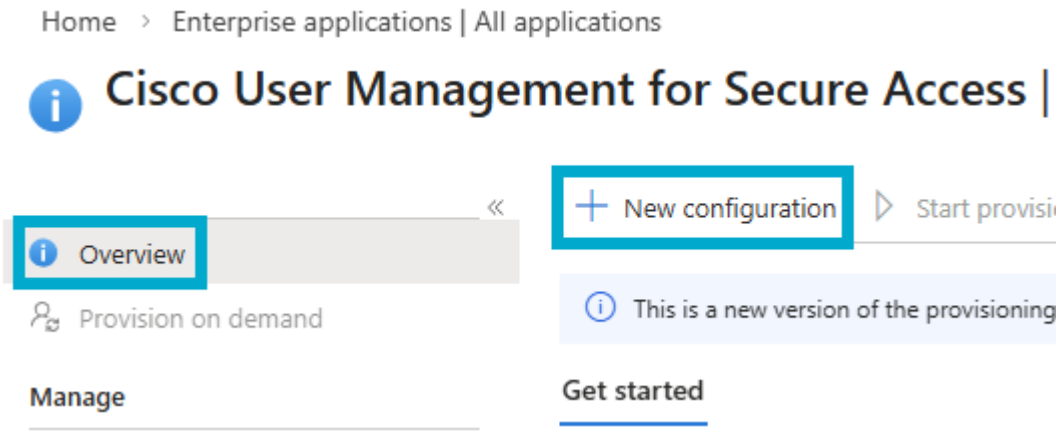
Assign Users and Groups

6. Accédez à Provisioning.



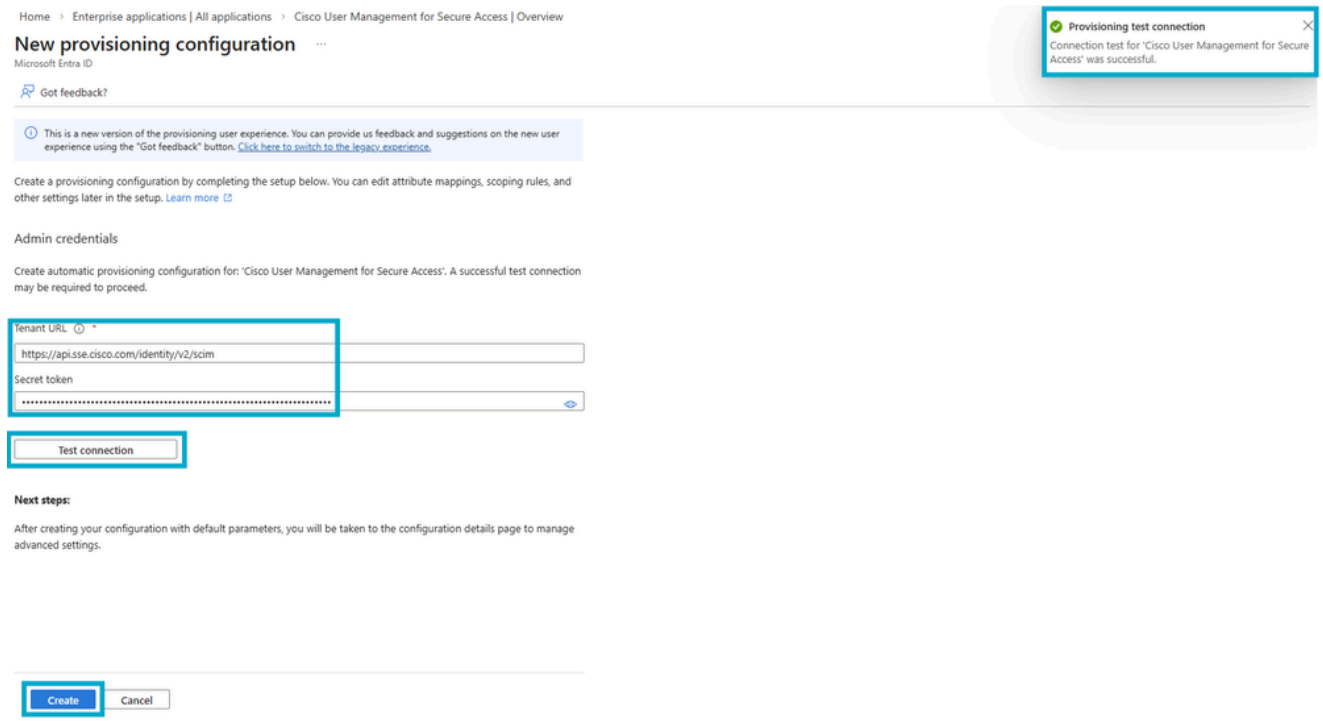
Provisionnement d'ID supplémentaire

7. Cliquez sur Overview, puis sur New Configuration.



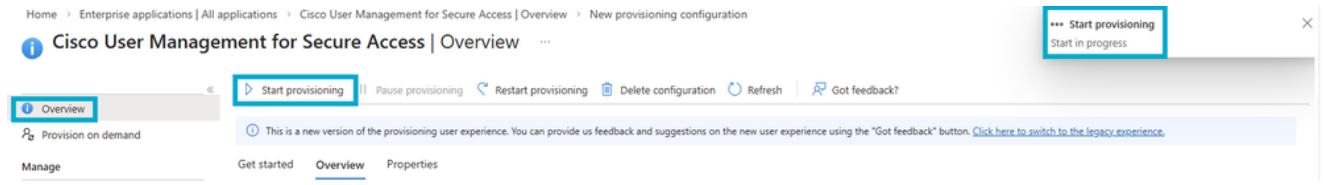
Nouvelle configuration

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.



Intégration des tests

9. Accédez à Overview > Start Provisioning.



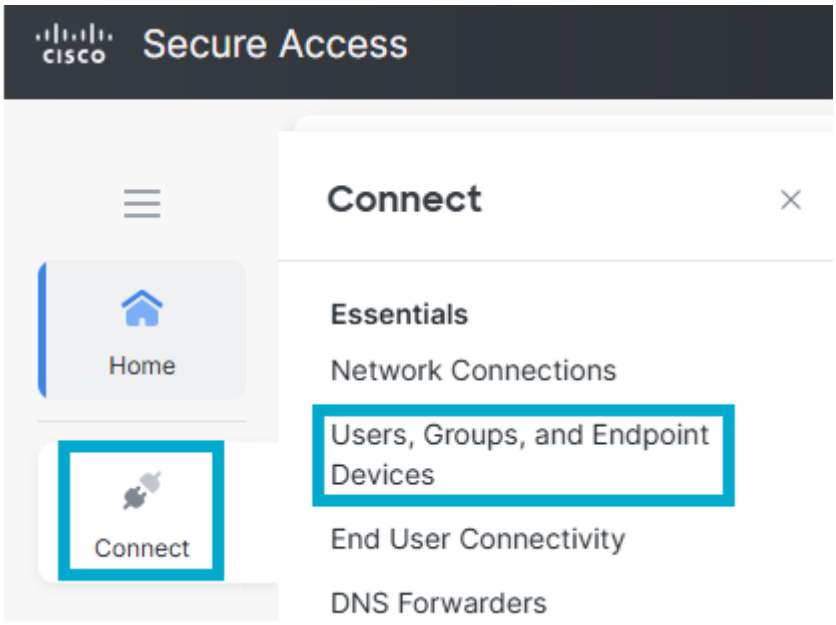
Démarrer le provisionnement

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

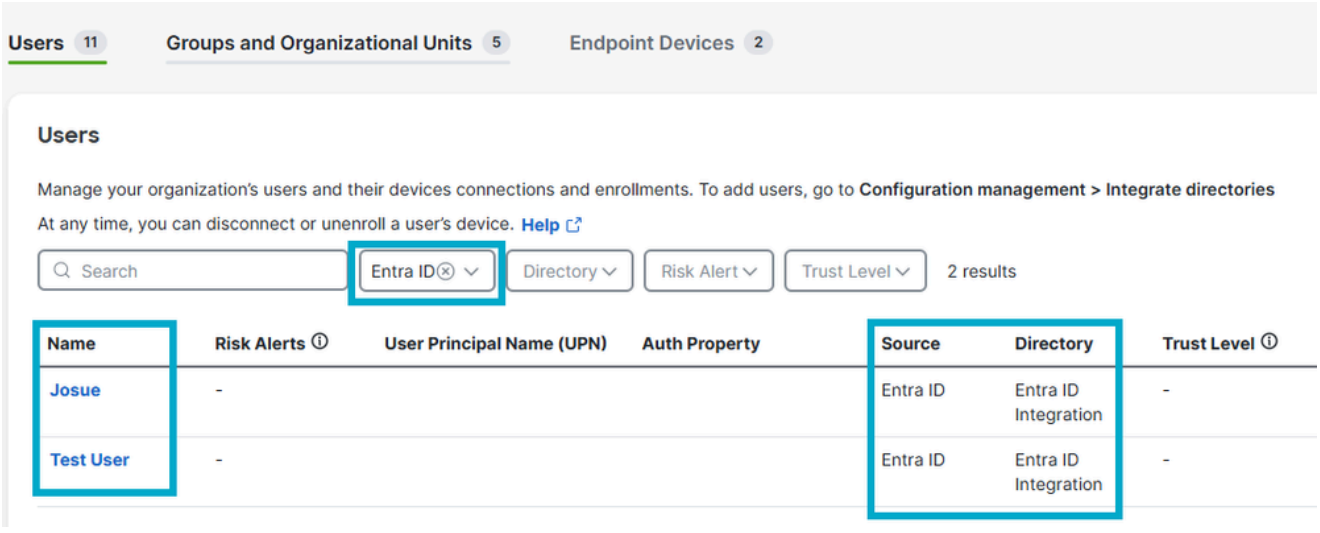
Verity dans Cisco Secure Access

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



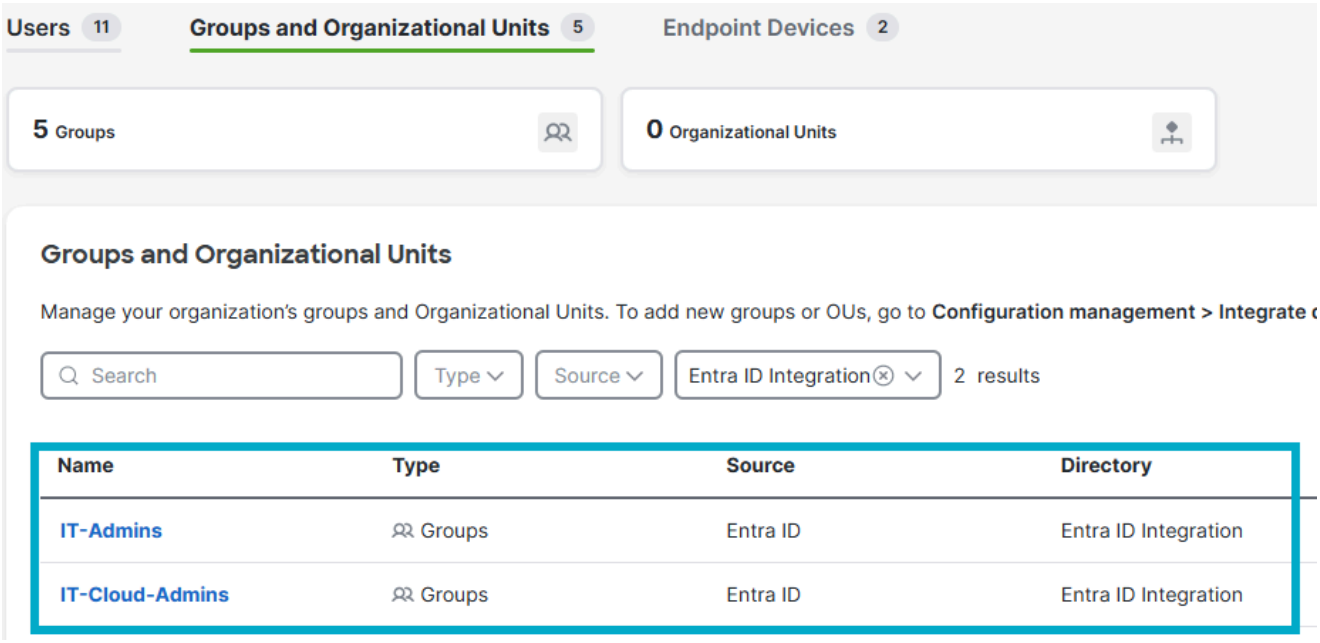
Users and Groups in CSA

- Cliquez sur Utilisateurs.



Vérifier les utilisateurs dans CSA

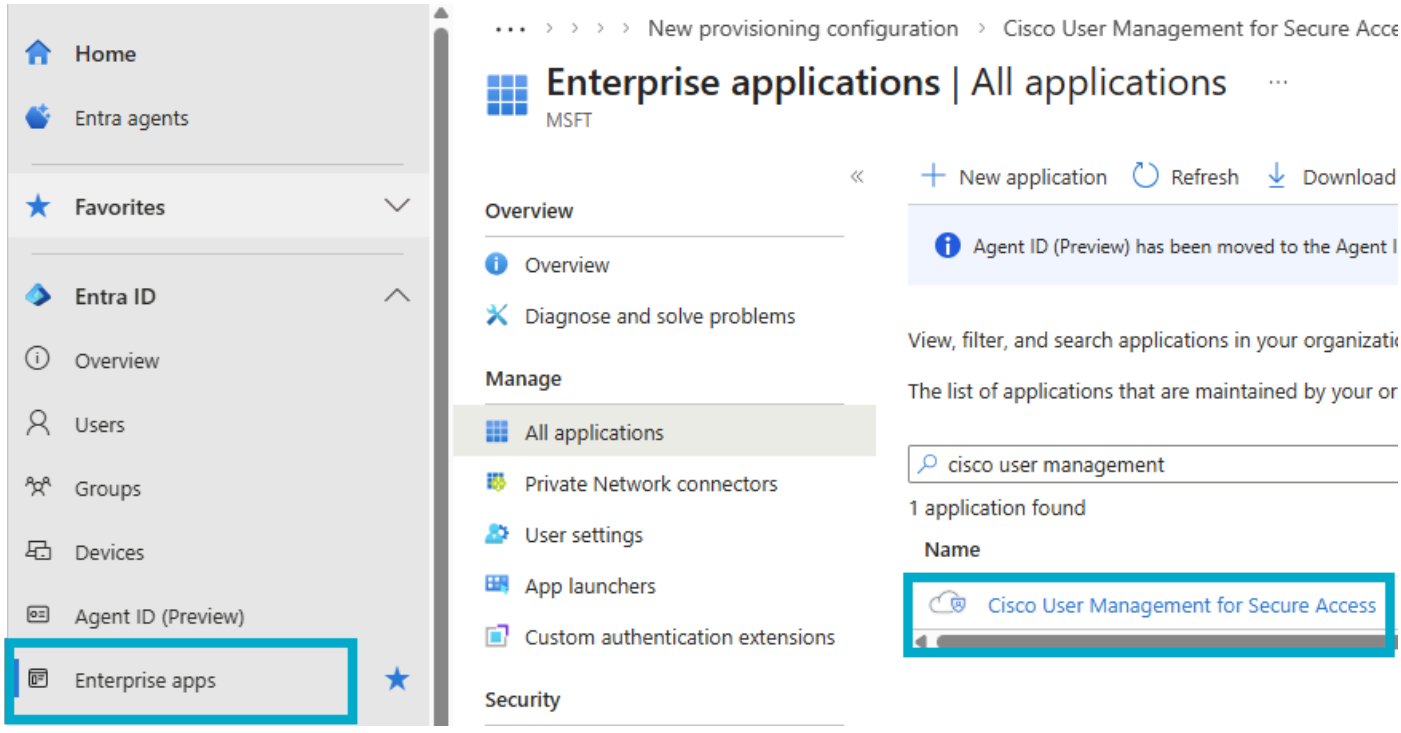
- Cliquez sur Groupes et unités d'organisation.



Verify Groups in CSA

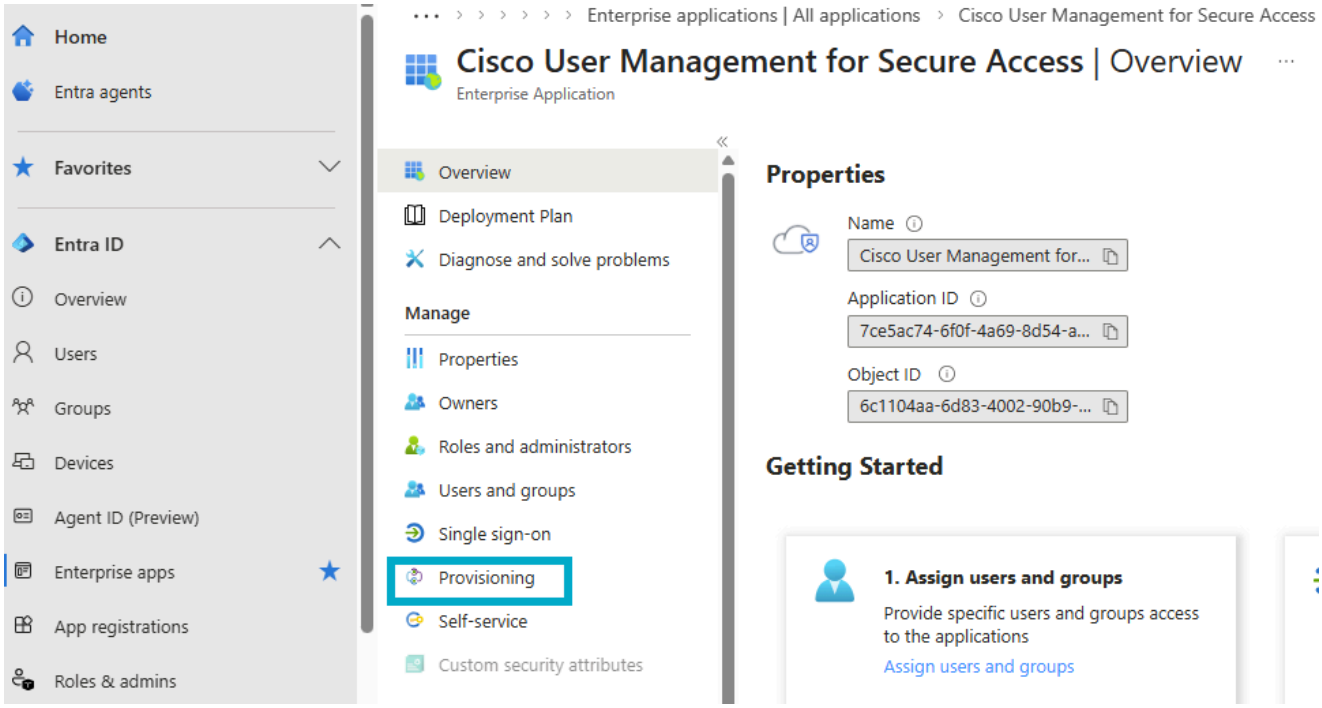
Vérifier dans l'ID d'entrée

- Accédez à Enterprise Apps et cliquez sur Cisco User Management for Secure Access.



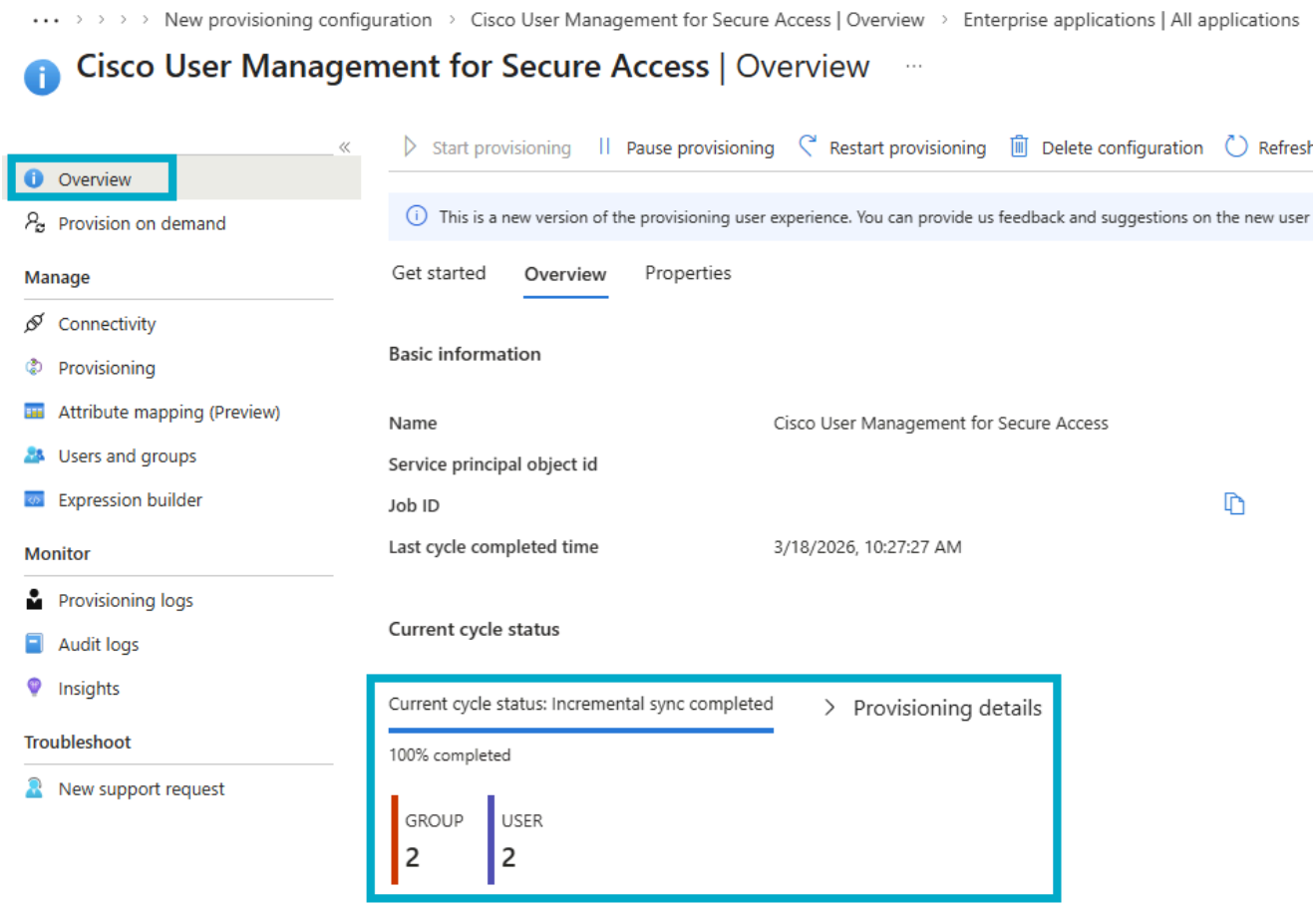
Vérifier dans Entra

- Cliquez sur Provisioning.



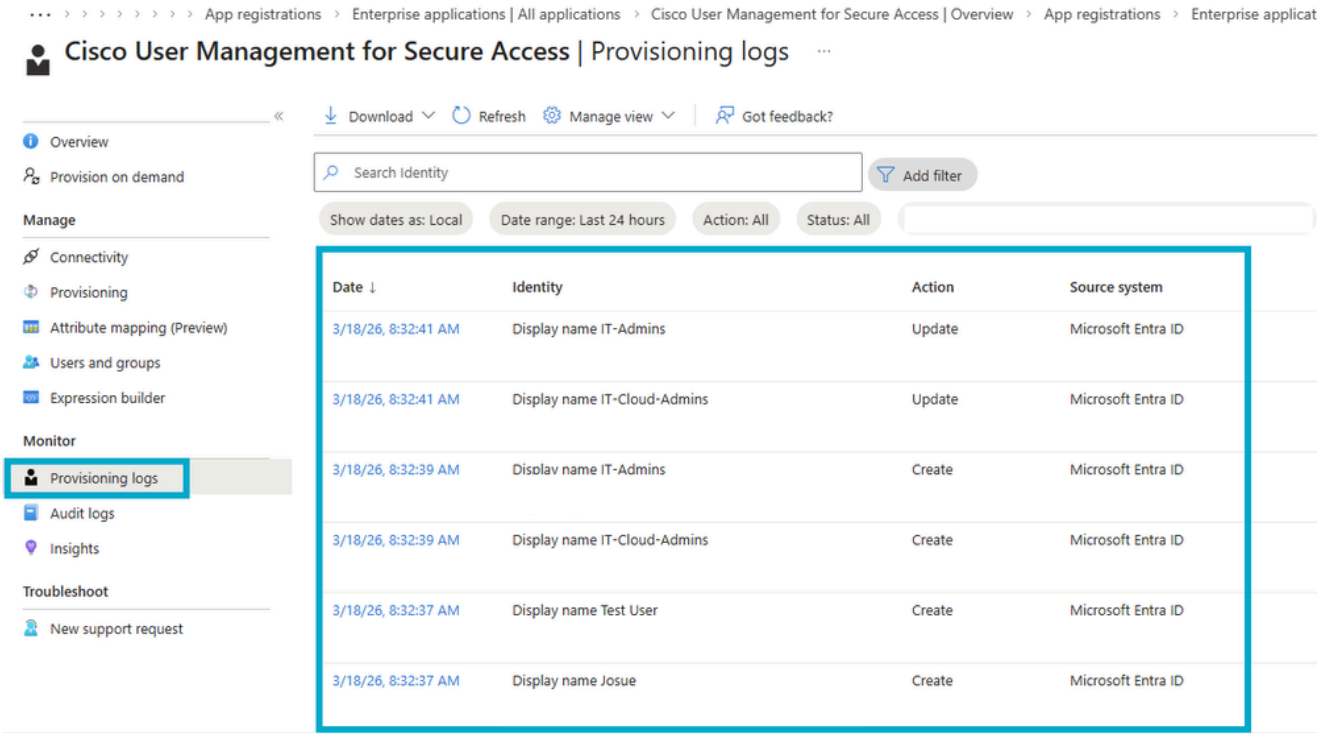
Verify in Entra ID

- Cliquez sur Overview.



Verify Provisioning in Entra

- Cliquez sur Provisioning logs.



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.