Configuration des utilisateurs et des groupes pour un accès sécurisé via OKTA

Table des matières

Introduction

Ce document décrit comment provisionner des groupes d'utilisateurs d'OKTA vers Cisco Secure Access.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès sécurisé Cisco
- OKTA

Composants utilisés

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

- Tableau de bord Cisco Secure Access

- OKTA

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 d'OKTA.

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.

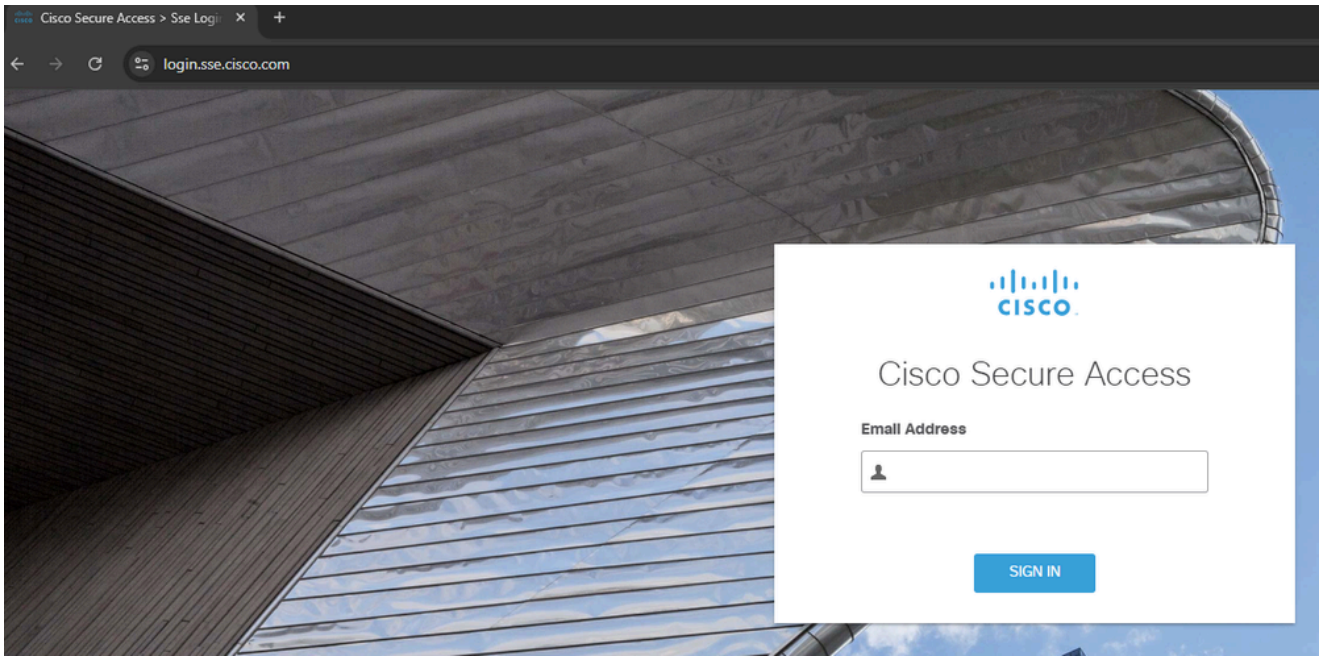
Remarque : Ce document se concentre spécifiquement sur l'approvisionnement des utilisateurs et des groupes à partir d'OKTA. La configuration d'Entra ID ou d'autres fournisseurs d'identité (IdP) pour l'inscription ZTA, l'authentification VPNaaS ou des paramètres d'itinérance Umbrella spécifiques n'est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

Configurer

Configuration de Cisco Secure Access

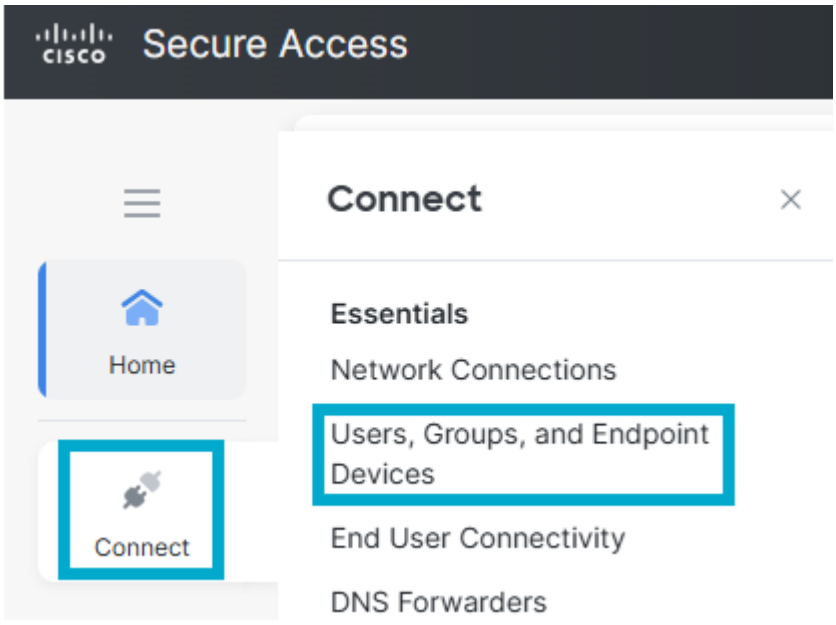
Afin de commencer le processus de mise en service, vous devez d'abord configurer l'intégration du répertoire dans le tableau de bord Cisco Secure Access. Cette étape génère les informations d'identification et les paramètres de configuration nécessaires pour établir une connexion sécurisée avec OKTA.

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



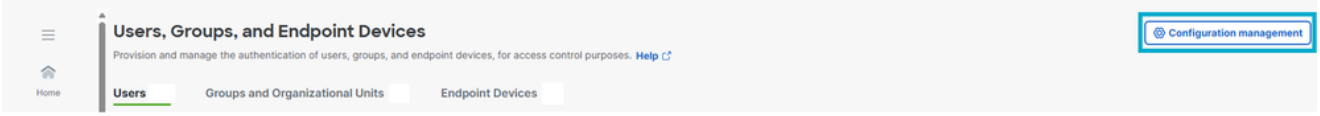
Se connecter à CSA

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



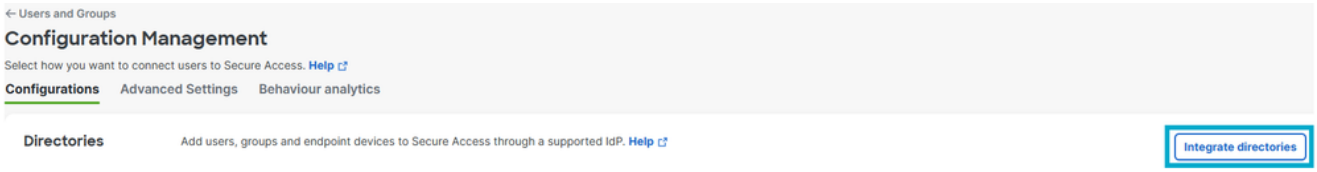
Utilisateurs et groupes

3. Cliquez sur Gestion de la configuration.



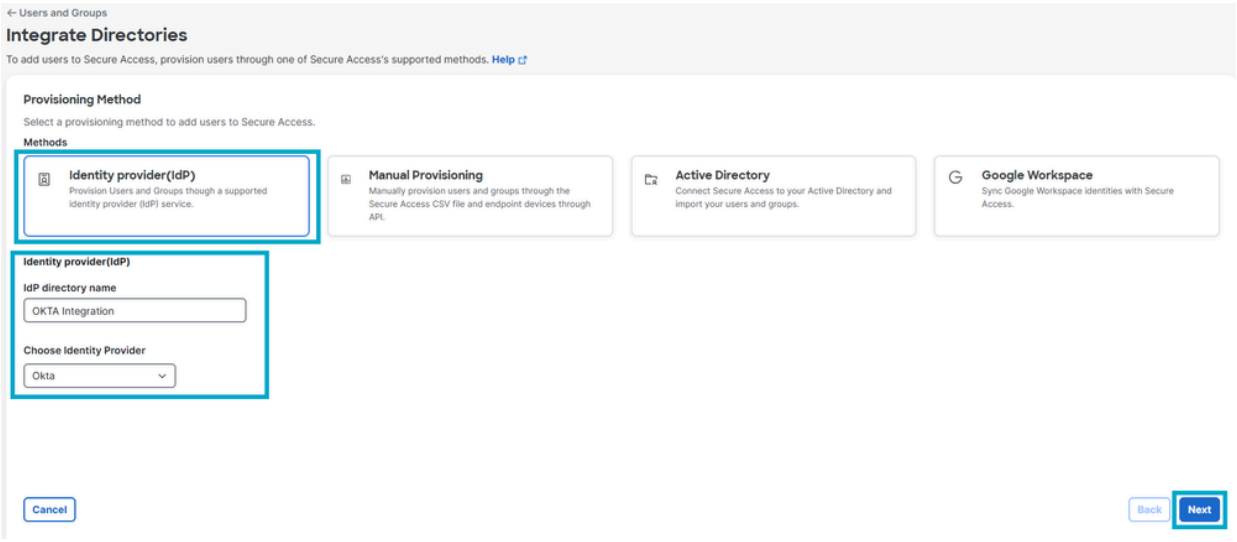
Gestion de la configuration

4. Cliquez sur Intégrer le répertoire.



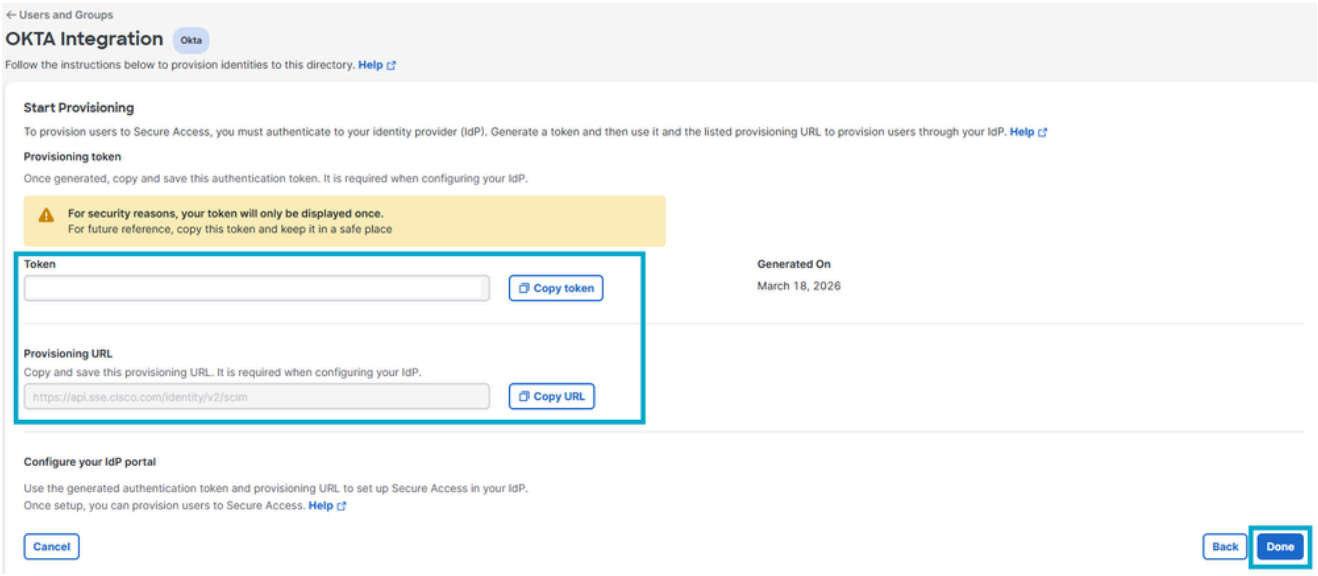
Intégrer un répertoire

5. Sous Méthode de provisionnement, cliquez sur Fournisseur d'identité.
    - Nom du répertoire IdP : Intégration OKTA.
    - Choisir un fournisseur d'identité : OK.
    - Cliquez sur Suivant.



Directory Configuration

6. Cliquez sur Generate Token. Enregistrez le jeton généré et l'URL d'approvisionnement, puis cliquez sur Done.

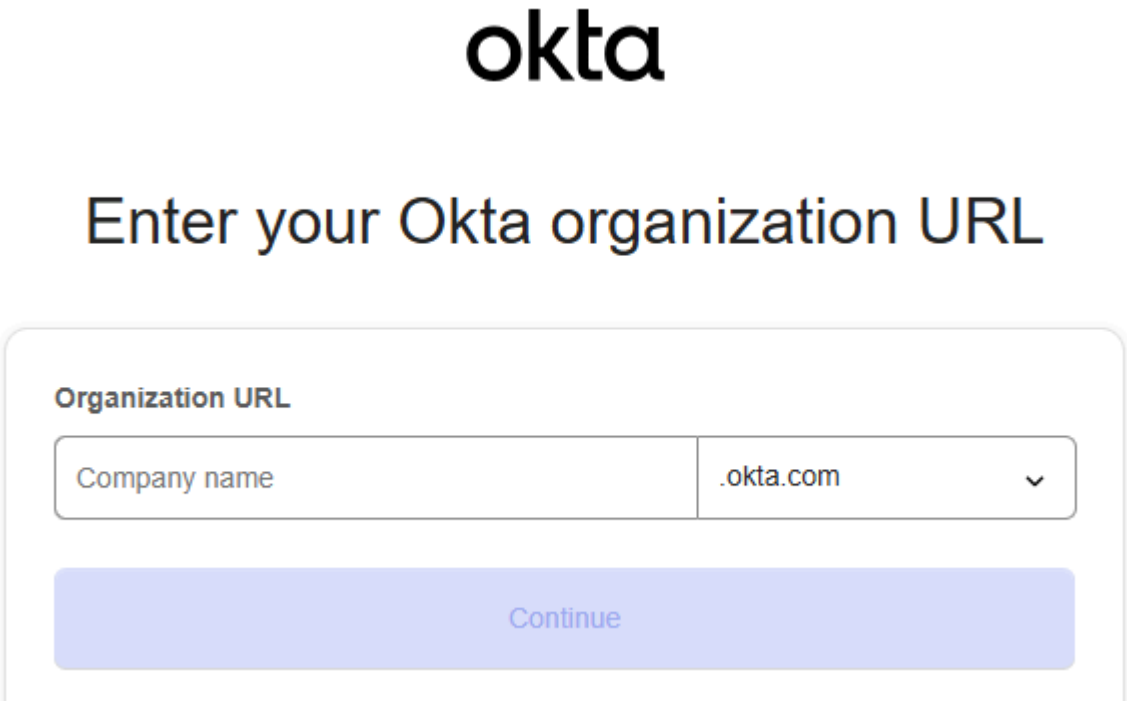


Générer un jeton

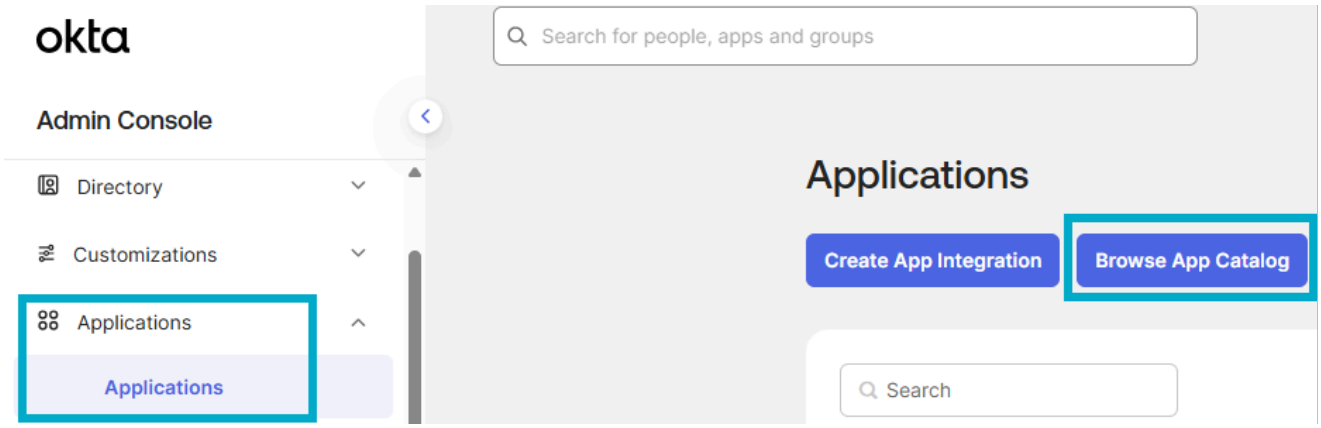
Configurer le provisionnement dans OKTA

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 OKTA pour activer la synchronisation des utilisateurs et des groupes.

1. Connectez-vous à OKTA.

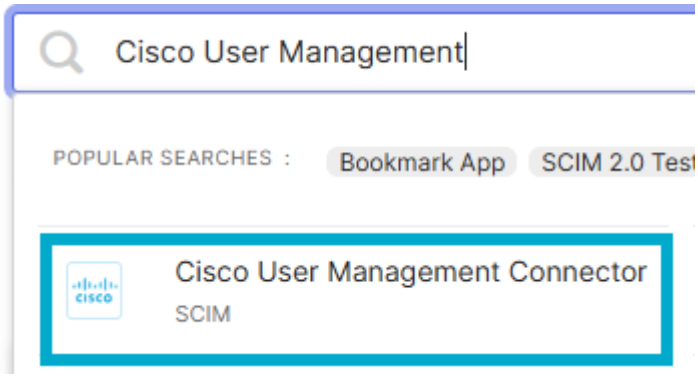


2. Accédez à Applications > Browser App Catalog.



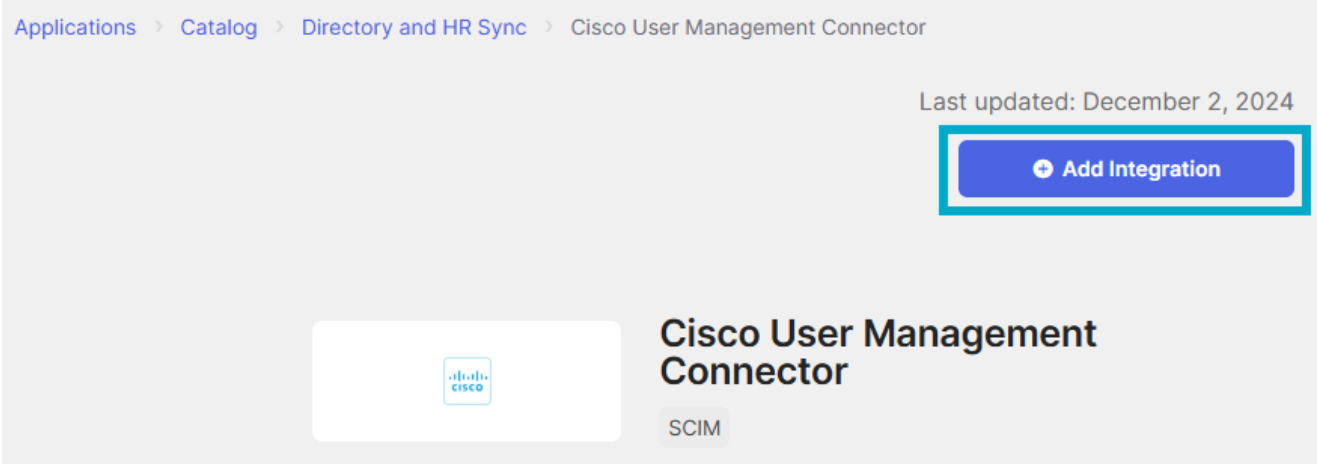
Parcourir le catalogue des applications

3. Sélectionnez l'application Cisco User Management Connector.



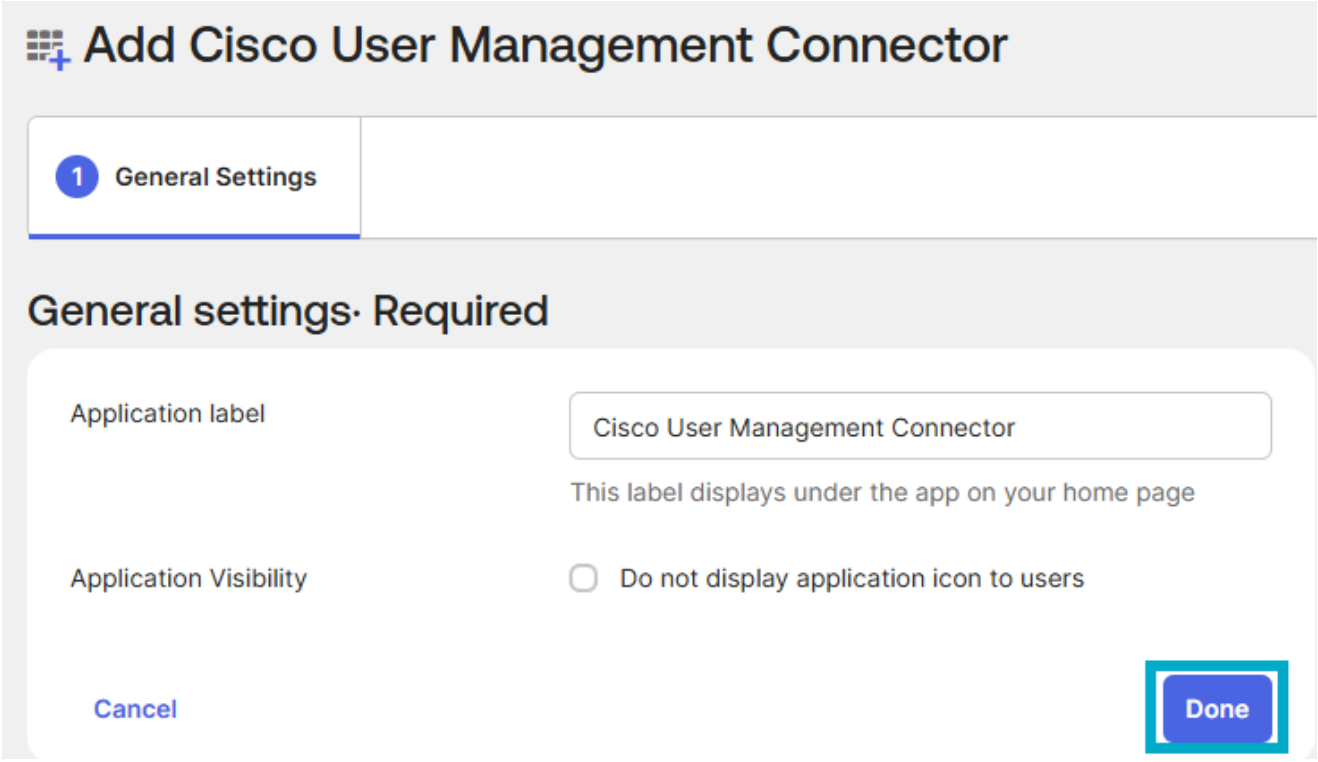
Application Cisco

4. Cliquez sur Ajouter une intégration.



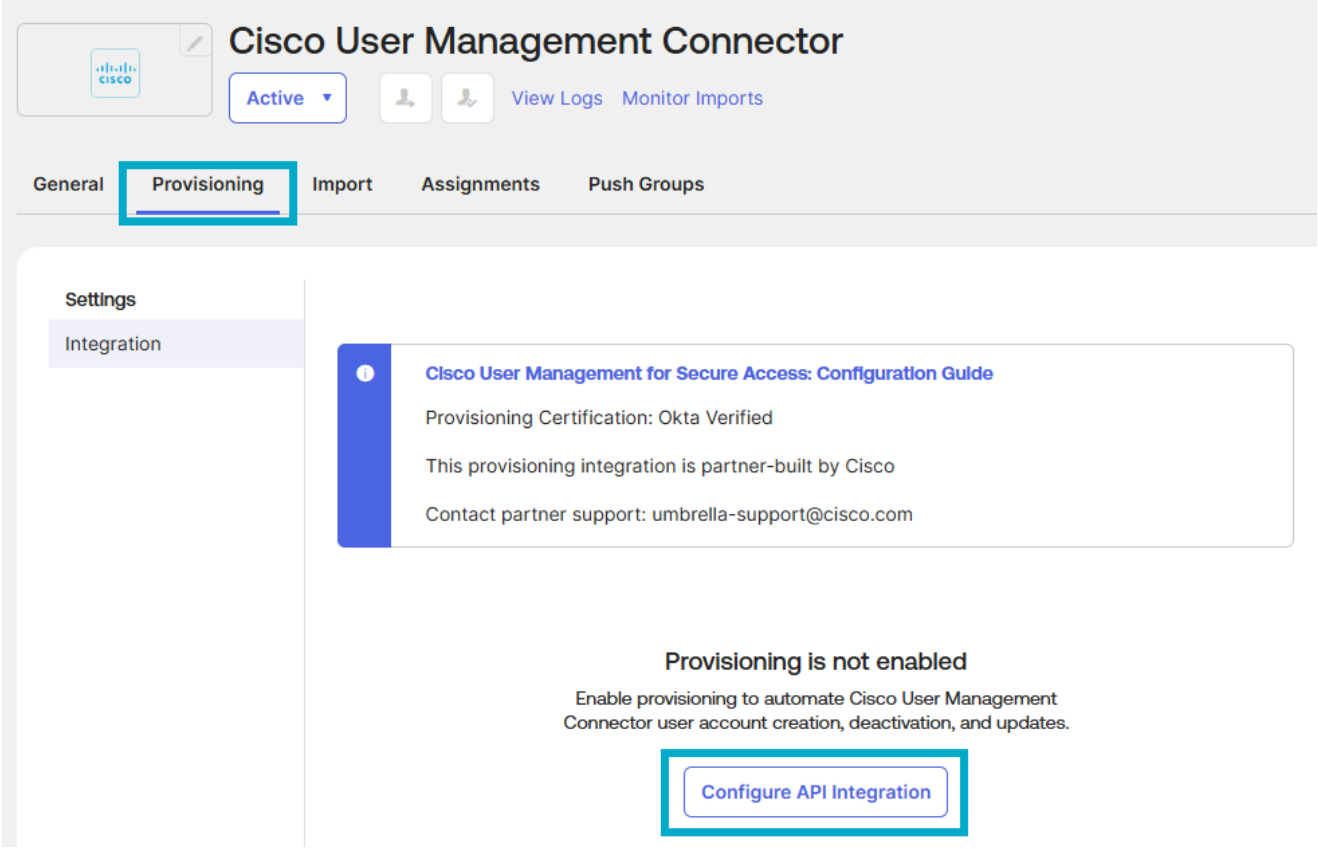
Ajouter une intégration

5. Cliquez sur Terminé.



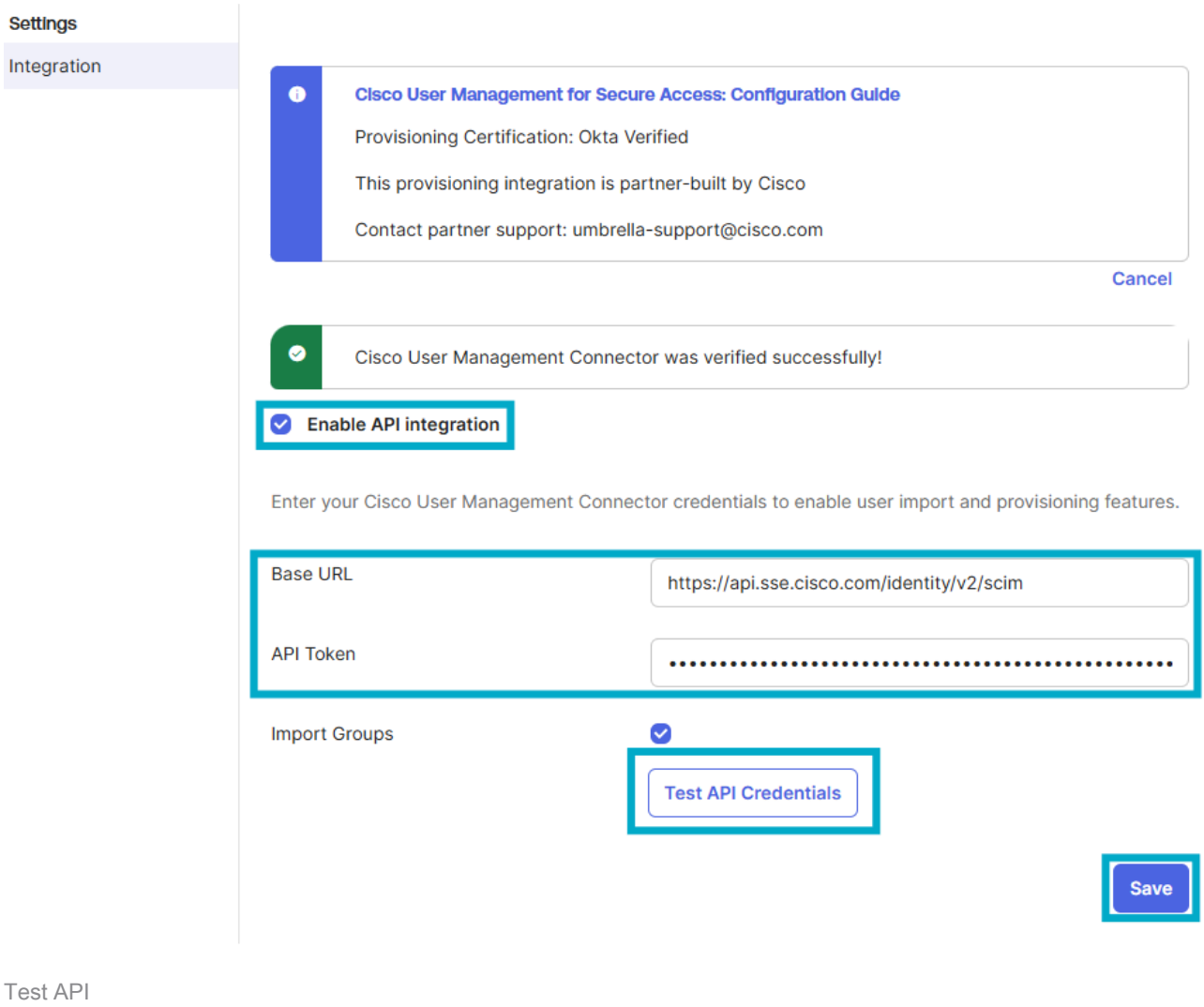
Ajouter une application

6. Cliquez sur Provisioning > Configure API Integration.

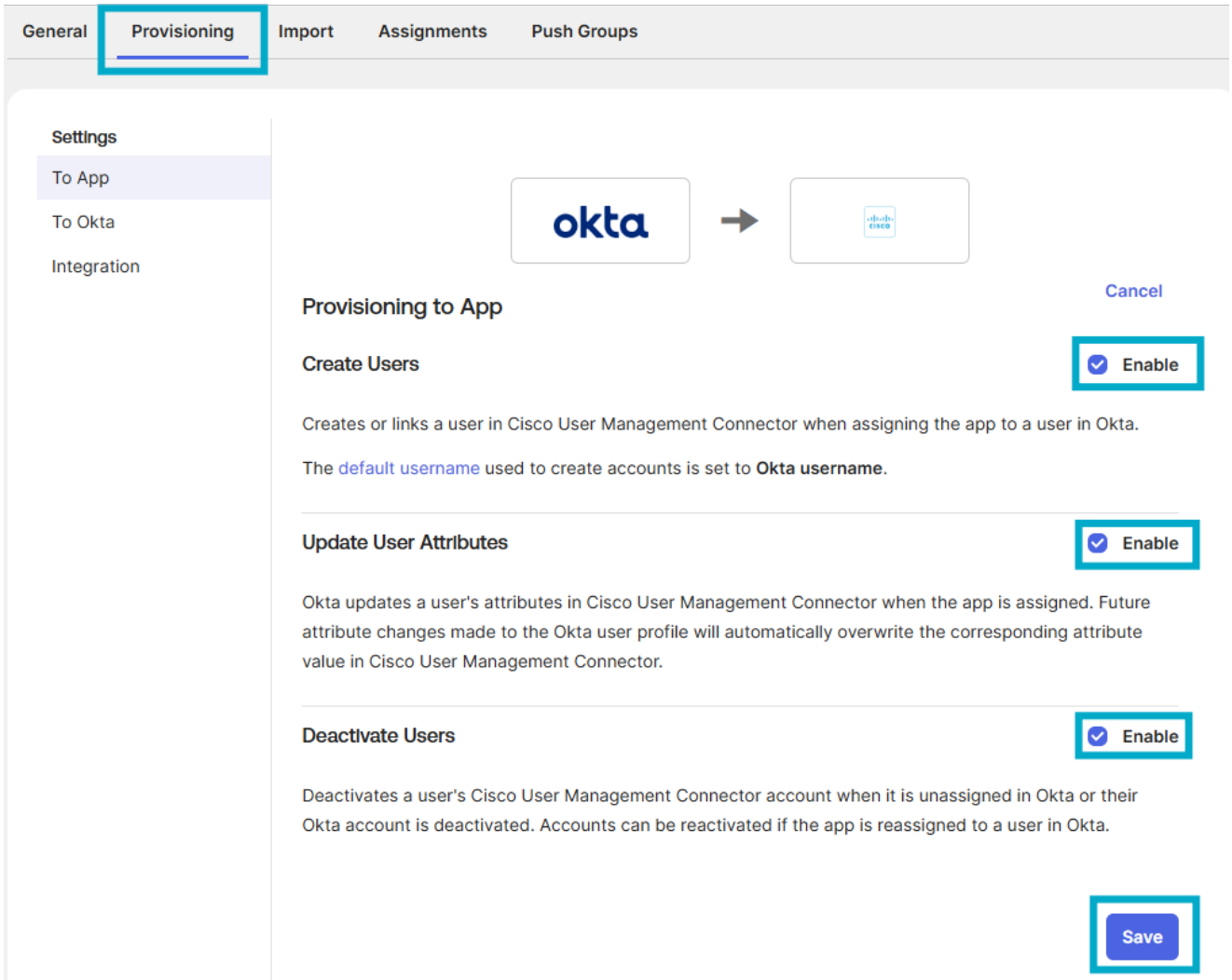


Configurer l'intégration API

7. Cliquez sur Enable API Integration et entrez l'URL basée sur et les jetons d'API enregistrés à l'étape #6 de la configuration d'accès sécurisé. Cliquez sur Test API Credentials, puis sur Save.



8. Accédez à Provisioning > To App. Activez les options Create Users, Update User Attributes et Deactivate Users, puis cliquez sur Save.



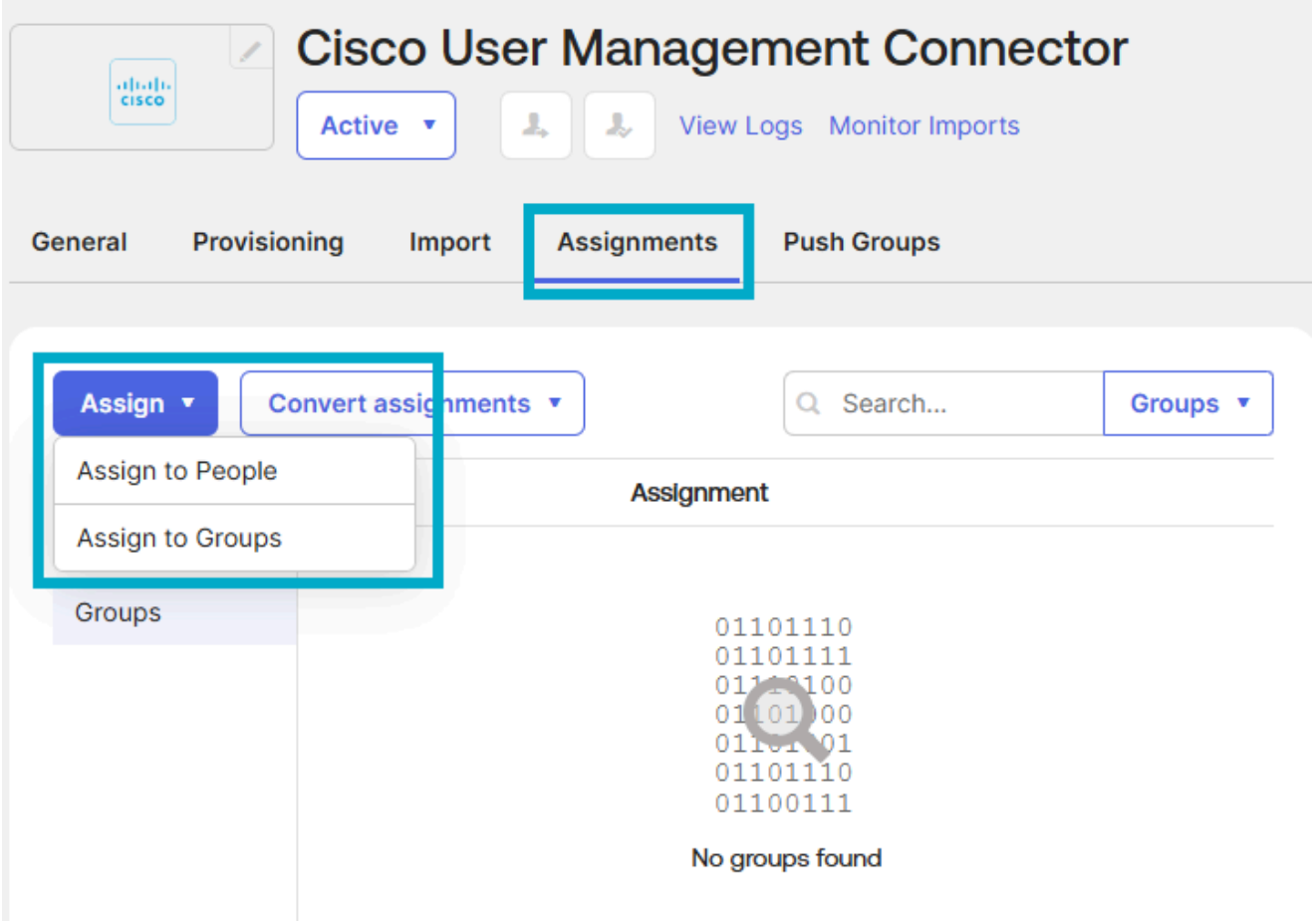
Approvisionnement de l'application

Remarque : Vérifiez que vous avez sélectionné ces attributs pour la synchronisation avec l'accès sécurisé. L'accès sécurisé répertorie uniquement les attributs Nom d'affichage et Nom d'utilisateur pour les utilisateurs, et non les attributs Prénom et Nom de famille : Nom d'utilisateur, Prénom, Famille, Nom, Nom d'affichage, E-mail

(Facultatif) Ajoutez un attribut objectGUID et créez le mappage de profil utilisateur. Si vous devez importer l'attribut objectGUID pour les utilisateurs, ajoutez un nouvel attribut et mappez les attributs dans le mappage de profil.

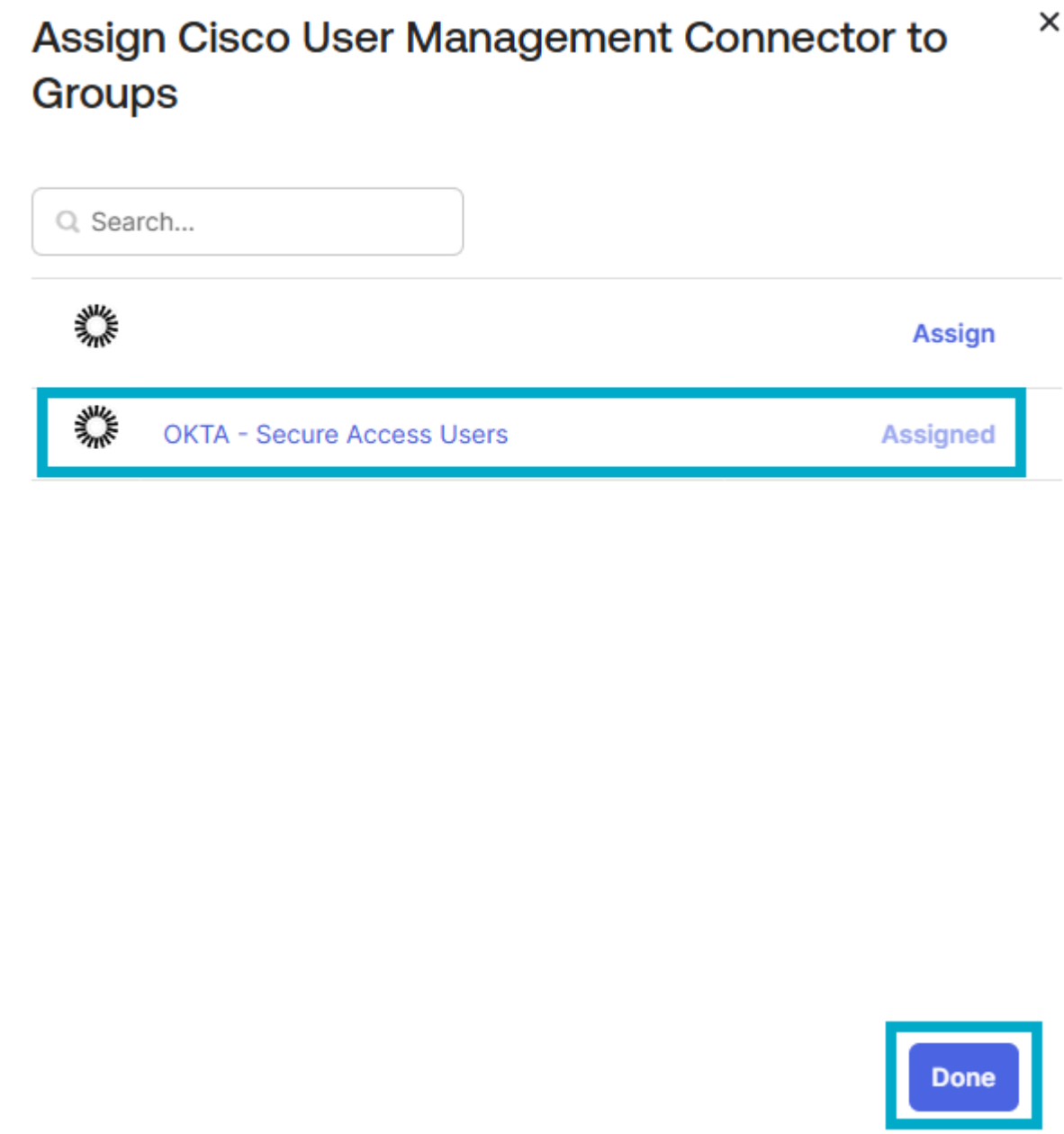
---

9. Pour ajouter des personnes/groupes, cliquez sur Affectations > Affecter > Affecter à des personnes/Affecter à des groupes.



Devoir

10. Sélectionnez les groupes/personnes que vous souhaitez affecter à l'accès sécurisé et cliquez sur Assign, puis sur Done.

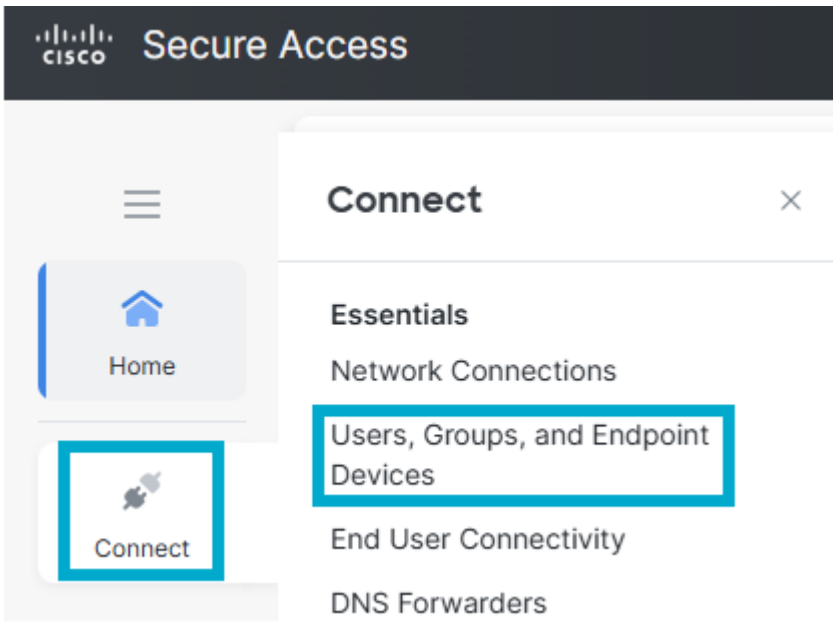


Affecter des groupes

Vérifier

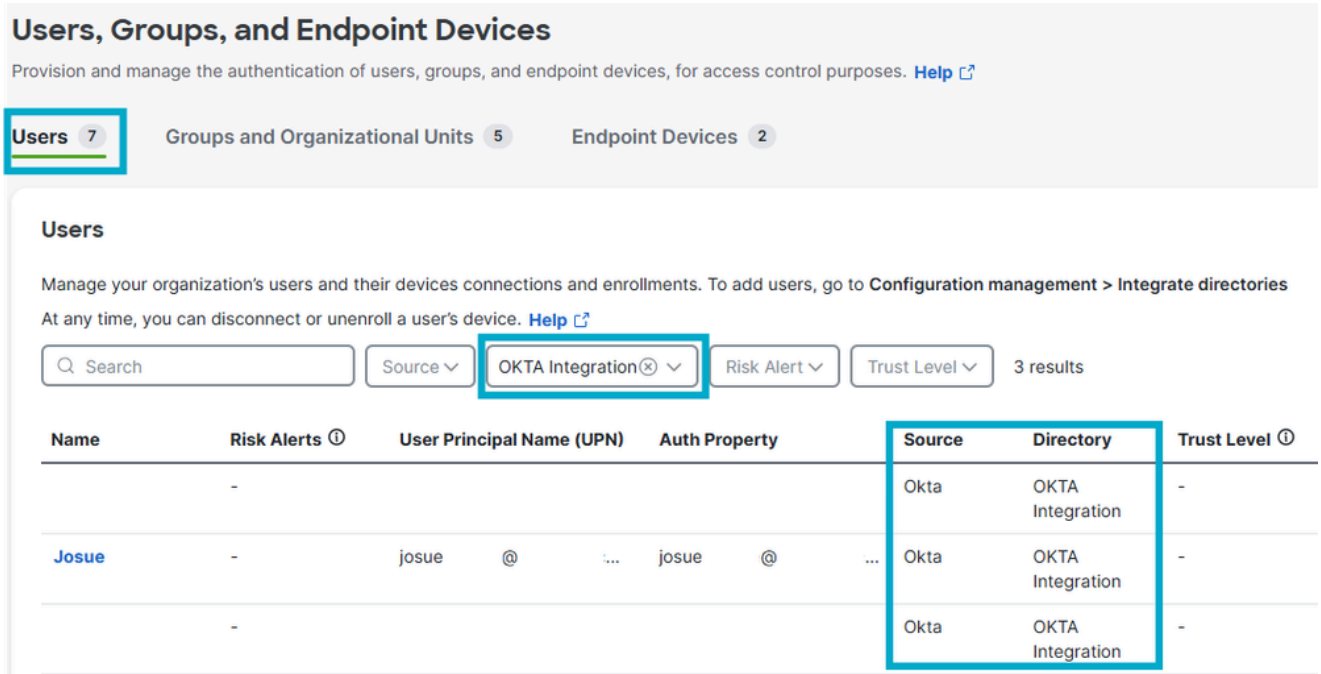
Verity dans Cisco Secure Access

- Accédez à Connect > Users, Groups and Endpoint Devices.



Utilisateurs et groupes dans CSA

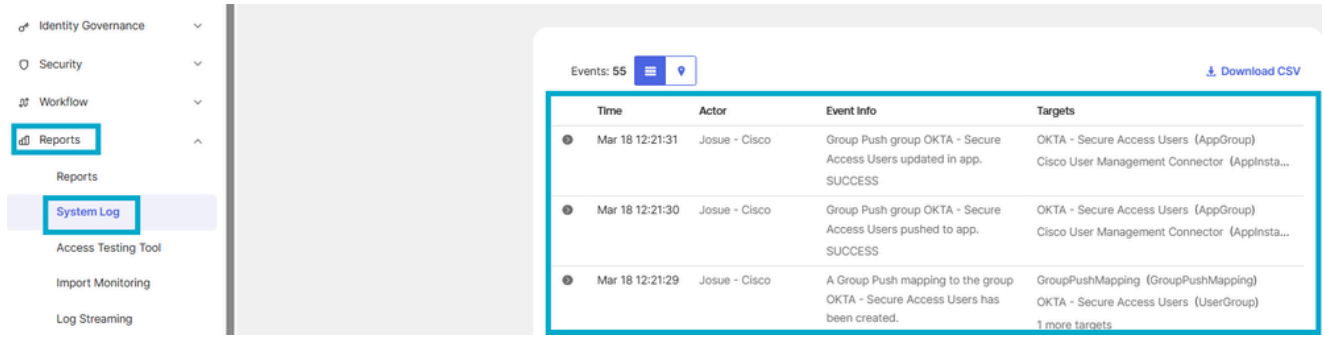
- Cliquez sur Utilisateurs.



Vérifier les utilisateurs dans CSA

Verity en OKTA

- Accédez à Rapports > Journal système.



Journaux OKTA

Informations connexes

[Configurer les fournisseurs d'identité]

[Provisionner des utilisateurs et des groupes à partir d'Okta]

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.