

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

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Configuration de Cisco Secure Access](#)

[Configurer le provisionnement dans OKTA](#)

[Vérifier](#)

[Verity dans Cisco Secure Access](#)

[Verity en OKTA](#)

[Informations connexes](#)

---

## 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.

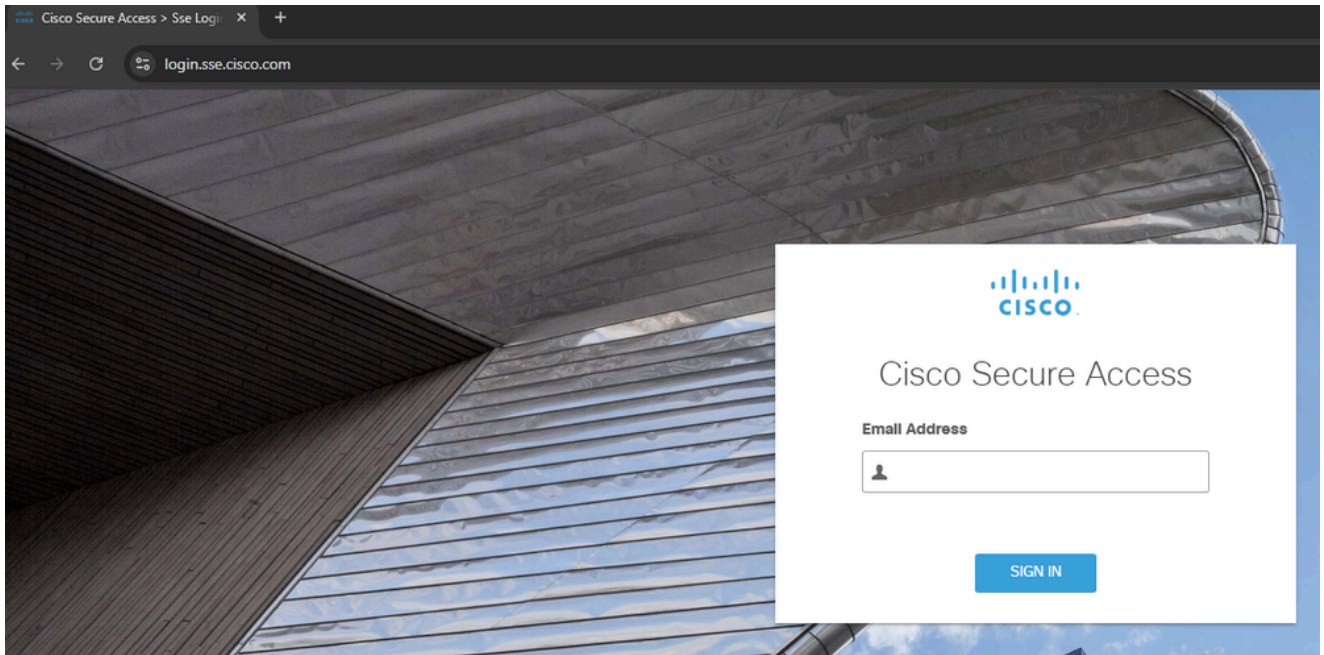
---

## Configurer

### Configuration de Cisco Secure Access

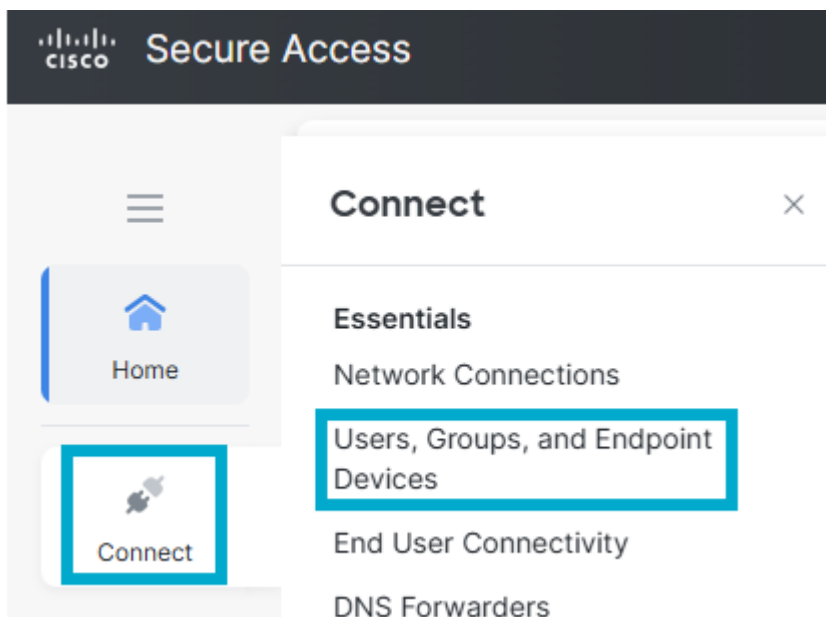
Afin de commencer le processus de mise en service, vous devez d'abord configurer l'intégration du répertoire dans le tableau de bord Cisco Secure Access. Cette étape génère les informations d'identification et les paramètres de configuration nécessaires pour établir une connexion sécurisée avec OKTA.

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



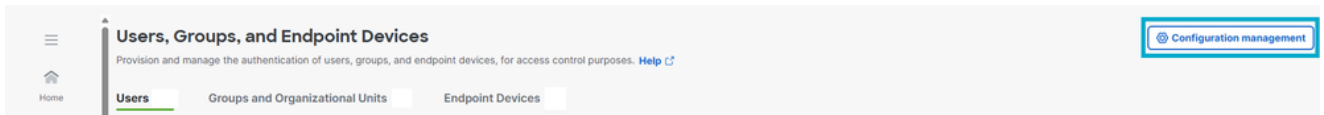
Se connecter à CSA

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



Utilisateurs et groupes

3. Cliquez sur Gestion de la configuration.



Gestion de la configuration

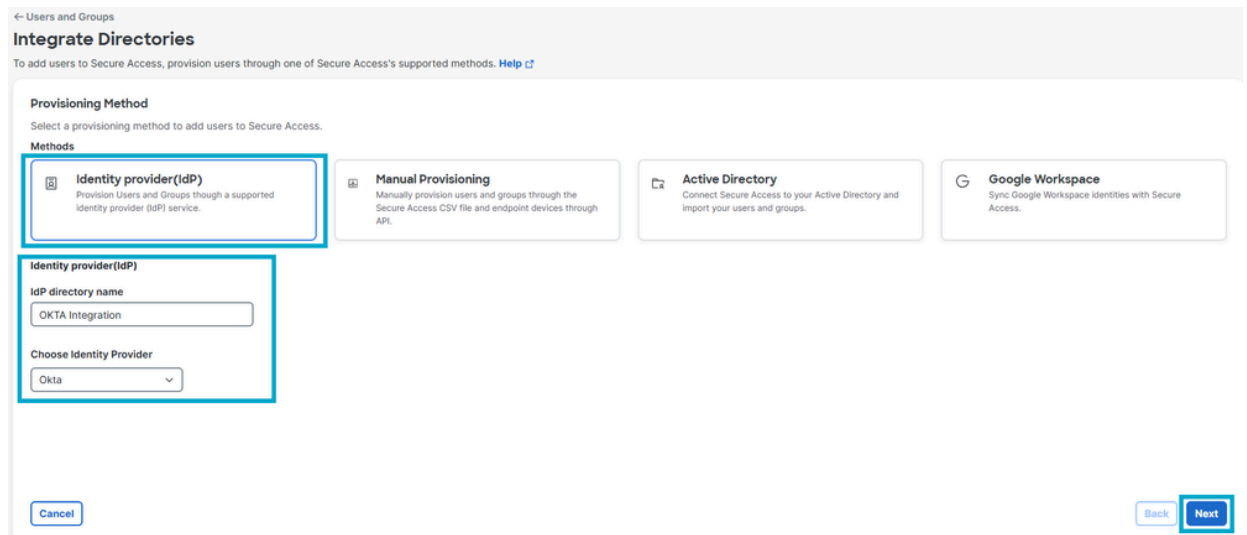
#### 4. Cliquez sur Intégrer le répertoire.



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.

← Users and Groups

## OKTA Integration Okta

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**

<b>Token</b> <input type="text"/> <a href="#">Copy token</a>	<b>Generated On</b> March 18, 2026
--	---------------------------------------

---

#### Provisioning URL

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

<input type="text" value="https://api.sse.cisco.com/identity/v2/scim"/> <a href="#">Copy URL</a>
---

---

#### 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 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](#).

# okta

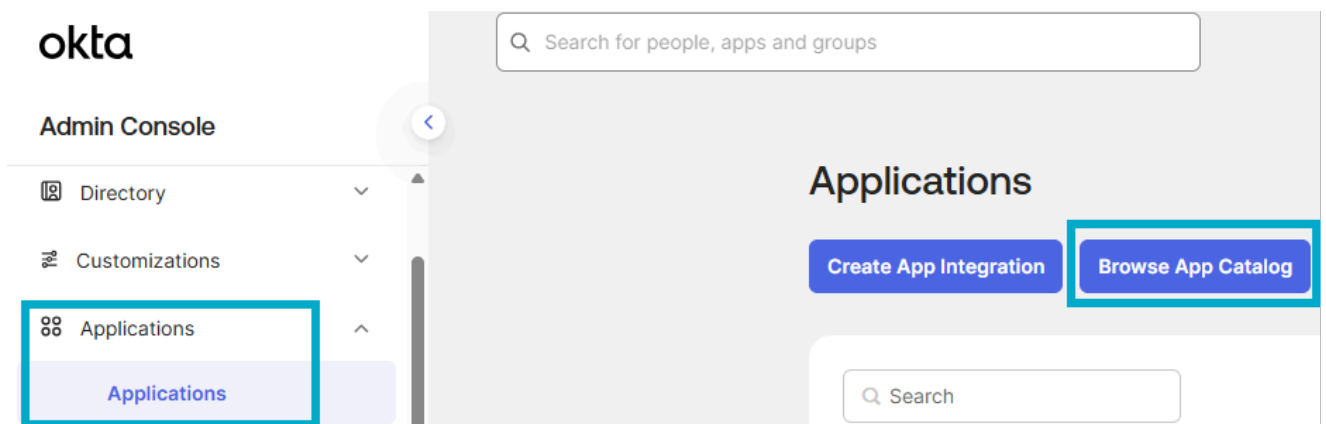
## Enter your Okta organization URL

**Organization URL**

<input type="text" value="Company name"/>	<input type="text" value=".okta.com"/> <span>▼</span>
---	---

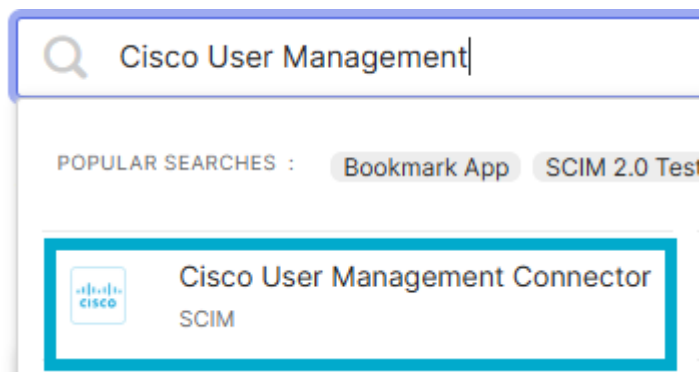
[Continue](#)

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.

Last updated: December 2, 2024

+ Add Integration



## Cisco User Management Connector

SCIM

Ajouter une intégration

5. Cliquez sur Terminé.

## Add Cisco User Management Connector

1 General Settings

### General settings · Required

Application label

Cisco User Management Connector

This label displays under the app on your home page

Application Visibility

Do not display application icon to users

Cancel

Done

Ajouter une application

6. Cliquez sur Provisioning > Configure API Integration.

The screenshot shows the Cisco User Management Connector interface. At the top, there is a header with the Cisco logo, a status dropdown set to 'Active', and two user icons. Below the header are navigation tabs: 'General', 'Provisioning' (highlighted with a red box), 'Import', 'Assignments', and 'Push Groups'. On the left side, there is a 'Settings' sidebar with 'Integration' selected. The main content area features a blue information box with a '1' icon, containing the text: 'Cisco User Management for Secure Access: Configuration Guide', 'Provisioning Certification: Okta Verified', 'This provisioning integration is partner-built by Cisco', and 'Contact partner support: umbrella-support@cisco.com'. Below this box, a message states 'Provisioning is not enabled' and 'Enable provisioning to automate Cisco User Management Connector user account creation, deactivation, and updates.' A red-bordered button labeled 'Configure API Integration' is positioned below the message.

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.

Settings

Integration

**Cisco User Management for Secure Access: Configuration Guide**  
Provisioning Certification: Okta Verified  
This provisioning integration is partner-built by Cisco  
Contact partner support: [umbrella-support@cisco.com](mailto:umbrella-support@cisco.com)

Cancel

Cisco User Management Connector was verified successfully!

**Enable API integration**

Enter your Cisco User Management Connector credentials to enable user import and provisioning features.

Base URL	<input type="text" value="https://api.sse.cisco.com/identity/v2/scim"/>
API Token	<input type="password" value="....."/>

Import Groups

**Test API Credentials**

**Save**

Test API

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

General **Provisioning** Import Assignments Push Groups

Settings  
To App  
To Okta  
Integration

okta → Cisco

Provisioning to App Cancel

Create Users Enable

Creates or links a user in Cisco User Management Connector when assigning the app to a user in Okta.  
The [default username](#) used to create accounts is set to **Okta username**.

Update User Attributes Enable

Okta updates a user's attributes in Cisco User Management Connector when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in Cisco User Management Connector.

Deactivate Users Enable

Deactivates a user's Cisco User Management Connector account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

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.

The screenshot displays the Cisco User Management Connector interface. At the top, the title "Cisco User Management Connector" is visible, along with a status indicator "Active" and navigation links for "View Logs" and "Monitor Imports". Below this, a navigation bar contains tabs for "General", "Provisioning", "Import", "Assignments" (which is highlighted with a red box), and "Push Groups".



In the "Assignments" section, there are two main buttons: "Assign" (highlighted with a red box) and "Convert assignments". The "Assign" button has a dropdown menu open, showing two options: "Assign to People" and "Assign to Groups" (both also highlighted with a red box). To the right of these buttons is a search bar labeled "Search..." and a "Groups" dropdown menu.

Below the search bar, the text "Assignment" is displayed. Underneath, there is a list of binary strings: 01101110, 01101111, 01101100, 01101100, 01101101, 01101110, and 01100111. A magnifying glass icon is positioned over the second "01101100" entry. Below the list, the text "No groups found" is displayed.

At the bottom left of the interface, the word "Devoir" is visible.

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

# Assign Cisco User Management Connector to Groups ×

		<a href="#">Assign</a>
	OKTA - Secure Access Users	Assigned

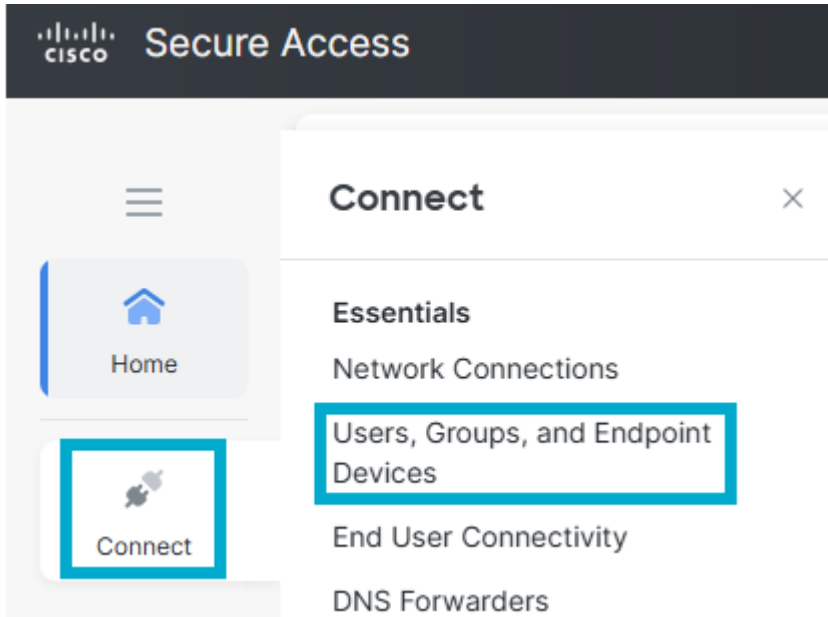
[Done](#)

Affecter des groupes

## Vérifier

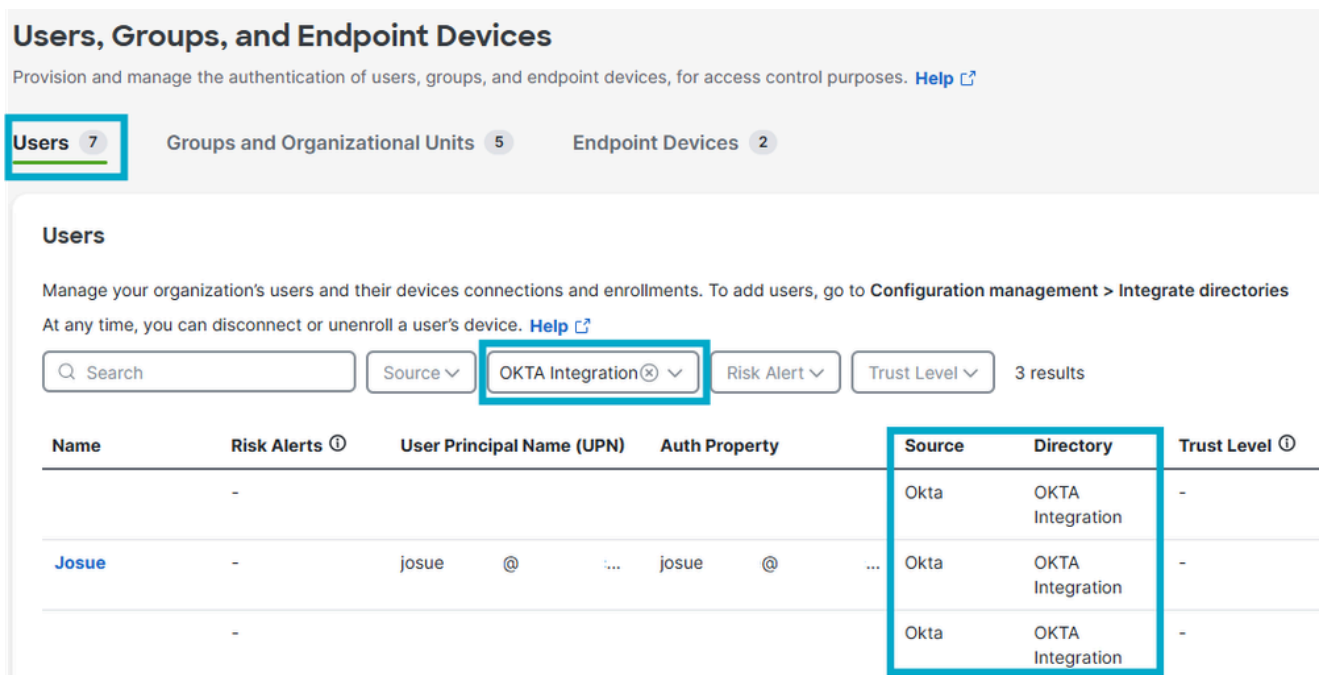
Verity dans Cisco Secure Access

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



Utilisateurs et groupes dans CSA

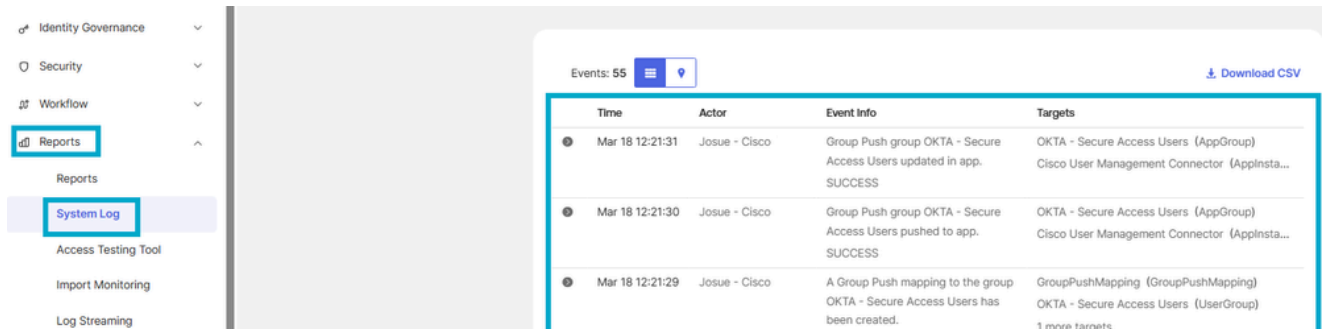
- Cliquez sur Utilisateurs.



Vérifier les utilisateurs dans CSA

# Verity en OKTA

- Accédez à Rapports > Journal système.



The screenshot shows the OKTA System Log interface. On the left, a navigation menu is visible with 'Reports' and 'System Log' highlighted. The main content area displays a table of events with columns for Time, Actor, Event Info, and Targets. The table contains three rows of event data.

Time	Actor	Event Info	Targets
Mar 18 12:21:31	Josue - Cisco	Group Push group OKTA - Secure Access Users updated in app. SUCCESS	OKTA - Secure Access Users (AppGroup) Cisco User Management Connector (AppInsta...
Mar 18 12:21:30	Josue - Cisco	Group Push group OKTA - Secure Access Users pushed to app. SUCCESS	OKTA - Secure Access Users (AppGroup) Cisco User Management Connector (AppInsta...
Mar 18 12:21:29	Josue - Cisco	A Group Push mapping to the group OKTA - Secure Access Users has been created.	GroupPushMapping (GroupPushMapping) OKTA - Secure Access Users (UserGroup) 1 more targets

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.