

# Assegnazione dell'accesso sicuro a utenti e gruppi tramite OKTA

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazione di Cisco Secure Access](#)

[Configura provisioning in OKTA](#)

[Verifica](#)

[Verity in Cisco Secure Access](#)

[Verity in OKTA](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come eseguire il provisioning dei gruppi di utenti da OKTA a Cisco Secure Access.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Access
- OKTA

### Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

- Cisco Secure Access Dashboard

- OKTA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Cisco Secure Access supporta il provisioning di utenti e gruppi da OKTA.

Questo provisioning consente l'accesso sicuro per la gestione di una directory di utenti autorizzati a:

- Registrarsi in Zero Trust Access (ZTA).
- Connessione a VPNaaS.
- Applicazione di criteri basati sull'identità agli utenti di Umbrella Roaming.



Nota: Questo documento si concentra in modo specifico sul provisioning di utenti e gruppi da OKTA. La configurazione dell'ID Entra o di altri provider di identità (IdP) per la registrazione ZTA, l'autenticazione VPNaaS o impostazioni di roaming Umbrella specifiche esula dall'ambito di questa guida.

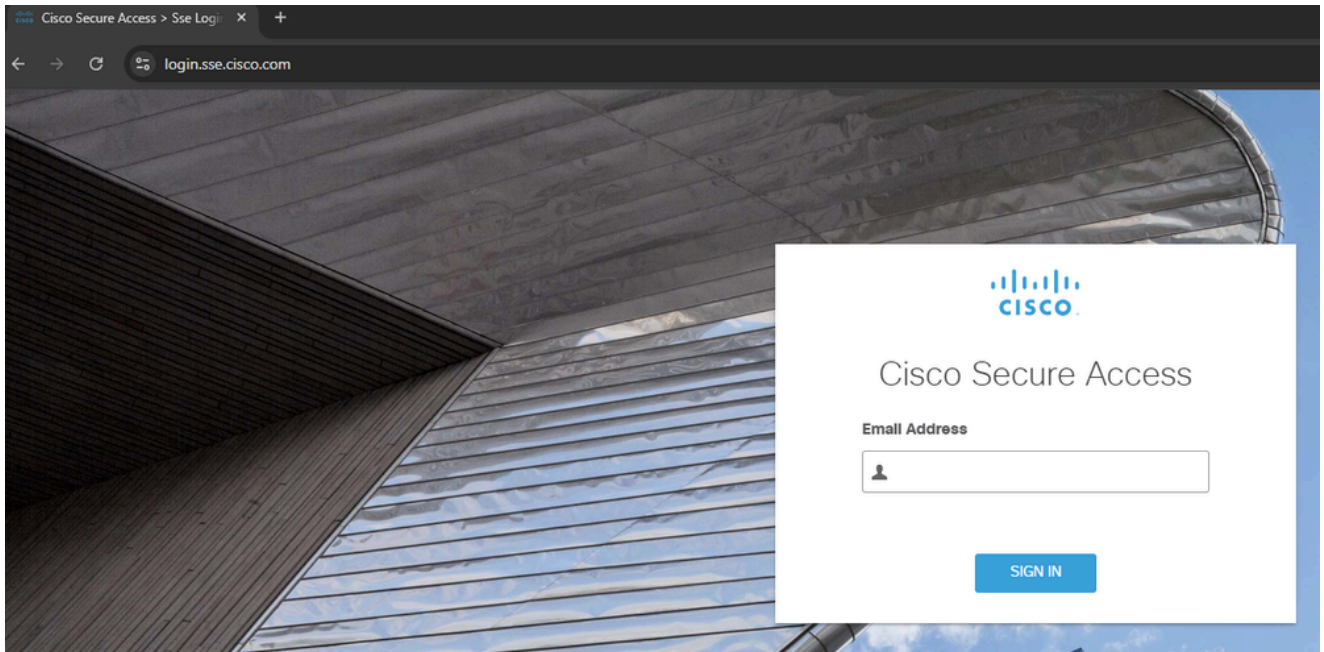
---

## Configurazione

### Configurazione di Cisco Secure Access

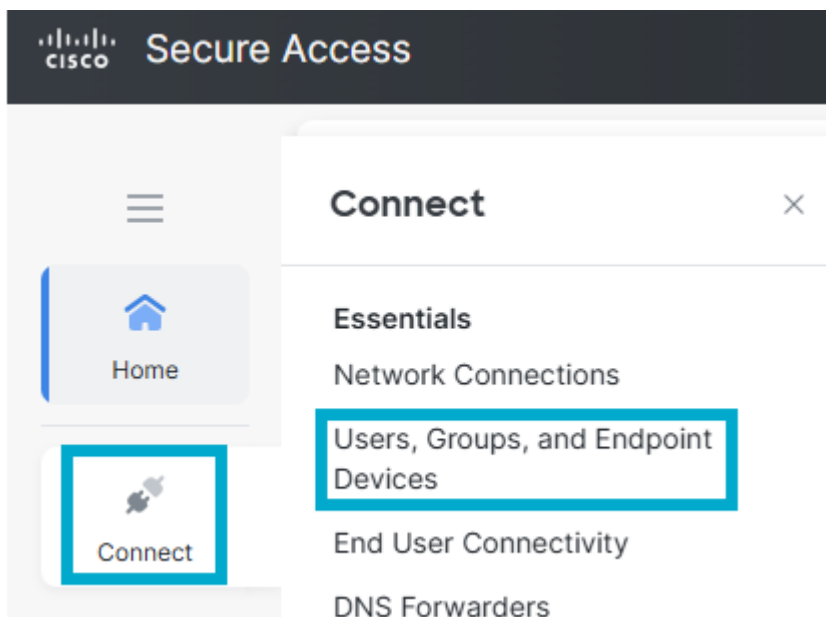
Per avviare il processo di provisioning, è necessario innanzitutto configurare l'integrazione delle directory nel dashboard Cisco Secure Access. Questo passaggio genera le credenziali e i parametri di configurazione necessari per stabilire una connessione protetta con OKTA.

1. Accedere a Cisco Secure Access [Dashboard](#).



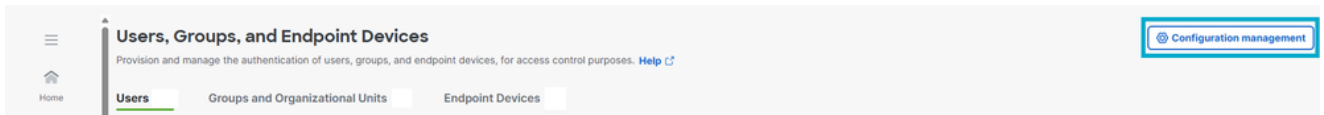
Accedi a CSA

2. Passare a Connetti > Utenti, gruppi e dispositivi endpoint.



Utenti e gruppi

3. Fare clic su Gestione configurazione.



Gestione della configurazione

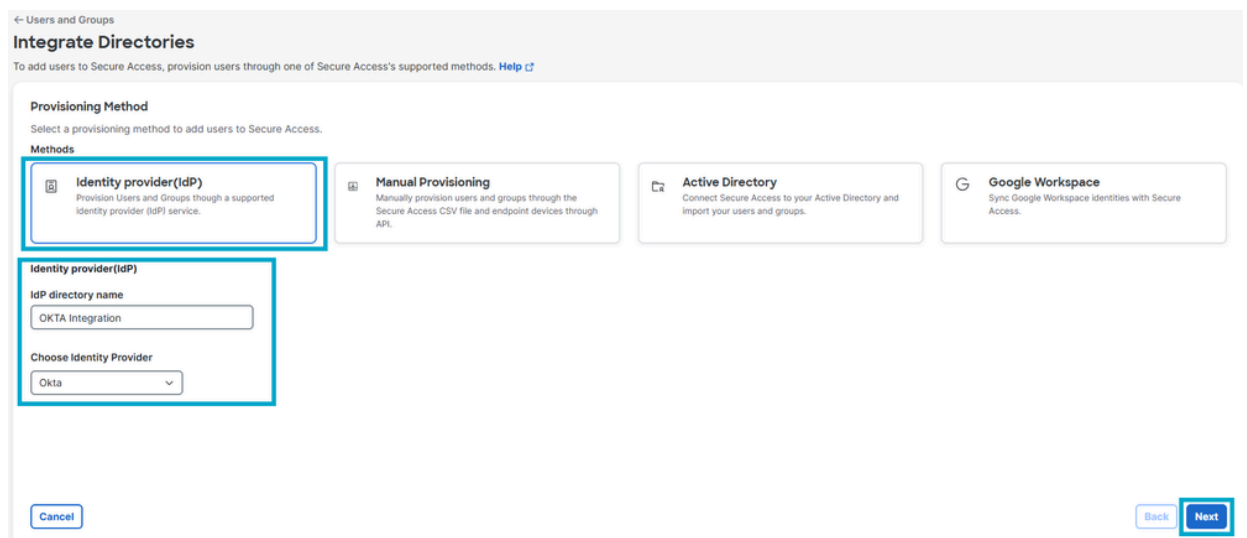
#### 4. Fate clic su Integra directory (Integrate Directory).



Directory di integrazione

#### 5. In Metodo di provisioning fare clic su Provider di identità.

- Nome directory IdP: Integrazione OKTA.
- Scegli provider di identità: OK.
- Fare clic su Next (Avanti).



*Directory Configuration*

#### 6. Fare clic su Generate Token. Salvare il token generato e l'URL di provisioning, quindi fare clic su 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

<p><b>Token</b></p> <input type="text"/> <a href="#">Copy token</a>	<p><b>Generated On</b></p> <p>March 18, 2026</p>
<p><b>Provisioning URL</b></p> <p>Copy and save this provisioning URL. It is required when configuring your IdP.</p> <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](#)

Genera token

## Configura provisioning in OKTA

Dopo aver generato le credenziali nel dashboard Cisco Secure Access, è necessario configurare le impostazioni di provisioning nel tenant OKTA per abilitare la sincronizzazione di utenti e gruppi.

1. Accedere a [OKTA](#).

# okta

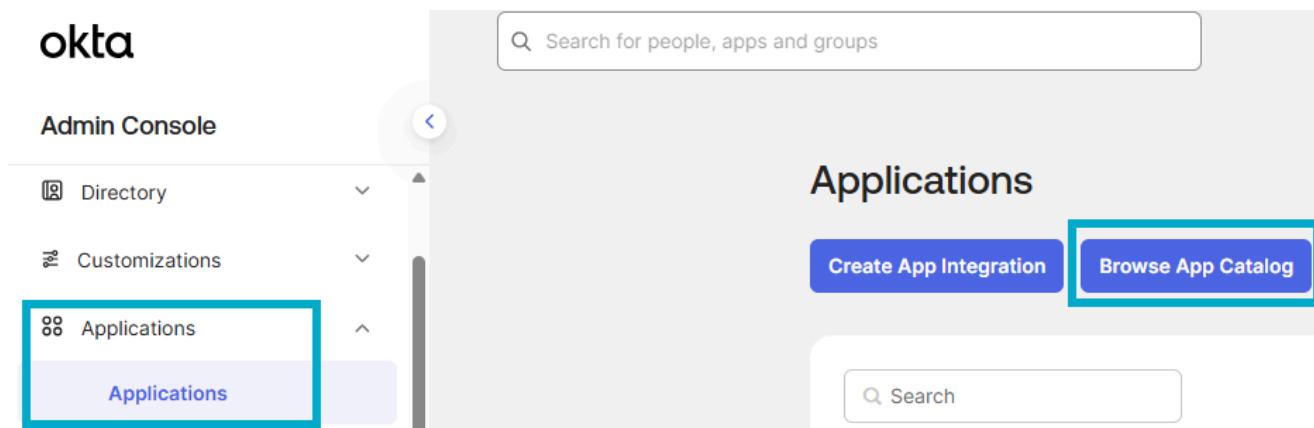
## Enter your Okta organization URL

**Organization URL**

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

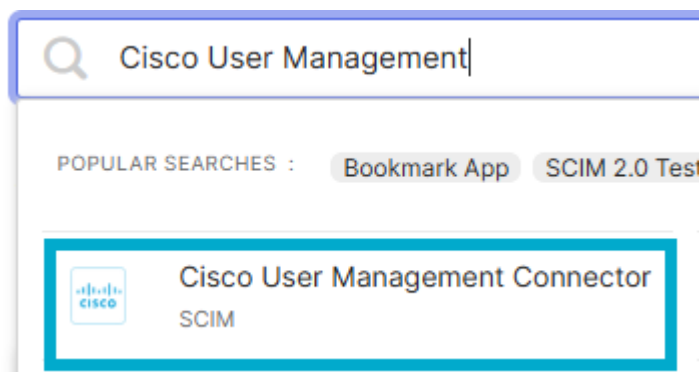
[Continue](#)

2. Passare a Applicazioni > Catalogo app browser.



Sfoggia catalogo app

3. Selezionare l'app Cisco User Management Connector.



App Cisco

4. Fare clic su Aggiungi integrazione.

Last updated: December 2, 2024

+ Add Integration



## Cisco User Management Connector

SCIM

Aggiungi integrazione

### 5. Selezionate Fatto (Done).

## + 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

Aggiungi app

### 6. Fare clic su Provisioning > Configura integrazione API.

**Cisco User Management Connector**

Active ▾ View Logs Monitor Imports

General **Provisioning** Import Assignments Push Groups

Settings  
Integration

**1** [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)

**Provisioning is not enabled**

Enable provisioning to automate Cisco User Management Connector user account creation, deactivation, and updates.

[Configure API Integration](#)

Configura integrazione API

7. Fare clic su Enable API Integration (Abilita integrazione API) e immettere l'URL basato e il token API salvati nel passaggio 6 della configurazione Secure Access. Fare clic su Prova credenziali API e quindi su Salva.

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. Passare a Provisioning > All'applicazione. Abilitare le opzioni Crea utenti, Aggiorna attributi utente e Disattiva utenti e fare clic su Salva.

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

Provisioning per app



Nota: Verificare di aver selezionato questi attributi per la sincronizzazione con Secure Access. Secure Access elenca solo gli attributi Nome visualizzato e Nome utente per gli utenti, non gli attributi Nome specificato e Nome famiglia: Nome utente, Nome, Famiglia, Nome, Nome visualizzato, E-mail

(Facoltativo) Aggiungere un [attributo objectGUID](#) e creare il mapping del profilo utente. Se è necessario importare l'attributo objectGUID per gli utenti, aggiungere un nuovo attributo e mappare gli attributi nel mapping del profilo.

9. Per aggiungere persone/gruppi, fare clic su Assegnazioni > Assegna > Assegna a persone/Assegna a gruppi.

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 word "Assignment" is centered. 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" string. Below the list, the text "No groups found" is displayed.

Assegnazione

10. Selezionare i gruppi/le persone che si desidera attivare per Accesso sicuro e fare clic su Assegna e quindi su Fine.

# Assign Cisco User Management Connector to Groups

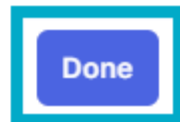


Assign



OKTA - Secure Access Users

Assigned

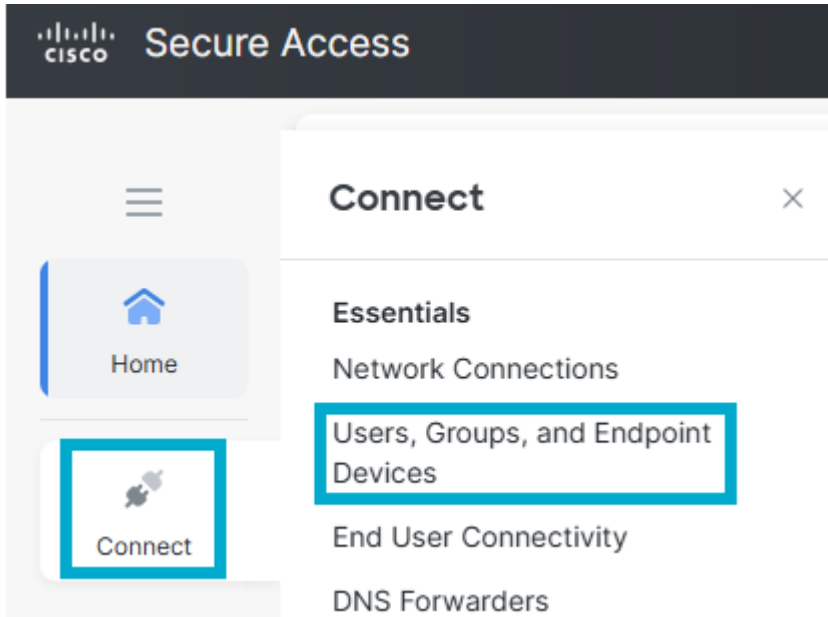


Assegna gruppi

## Verifica

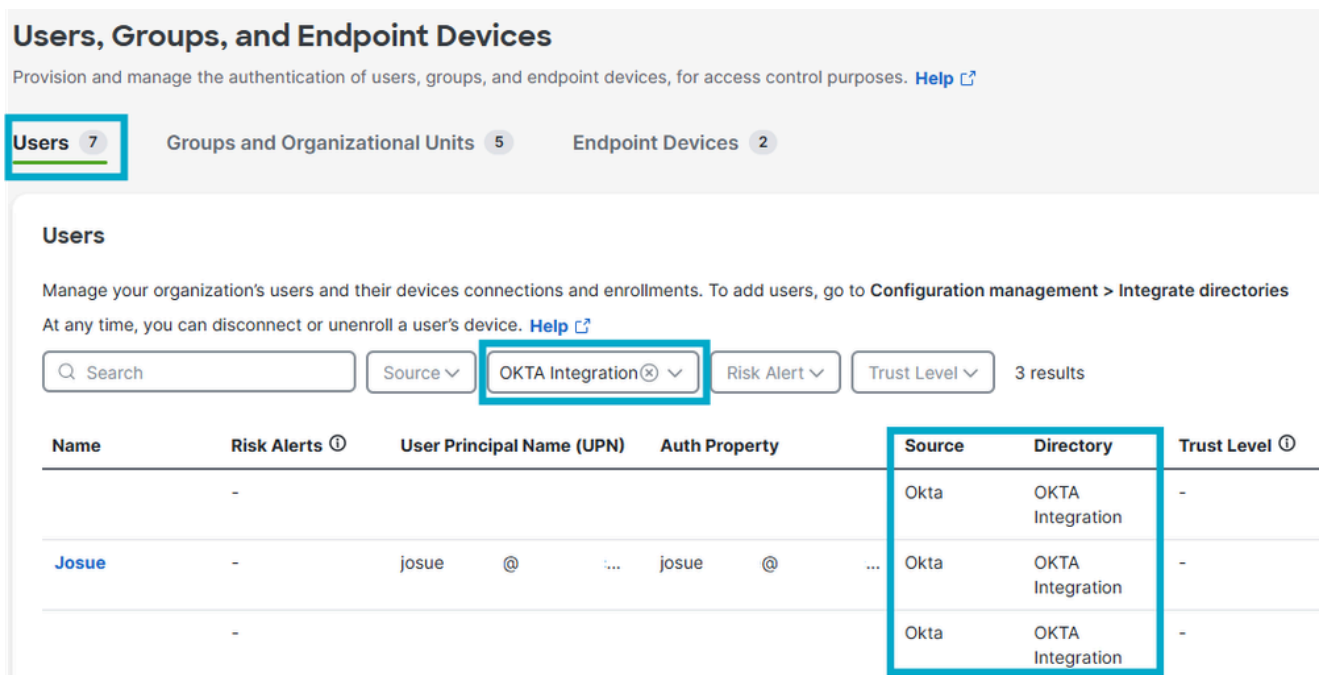
Verity in Cisco Secure Access

- Passare a Connetti > Utenti, gruppi e dispositivi endpoint.



Utenti e gruppi in CSA

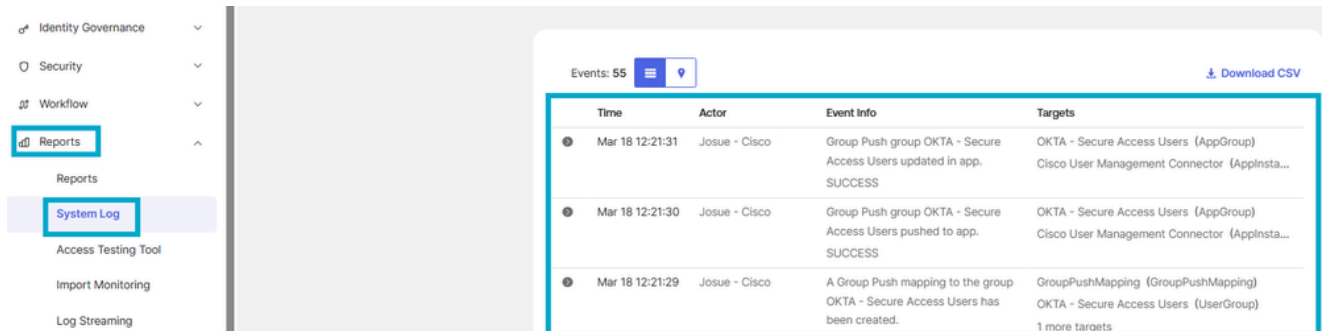
- Fare clic su Utenti.



Verifica degli utenti in CSA

# Verity in OKTA

- Passare a Rapporti > Log di sistema.



The screenshot shows the Okta Reports interface. On the left sidebar, 'Reports' and 'System Log' are highlighted. The main content area displays a table of system events. The table has four columns: Time, Actor, Event Info, and Targets. There are three rows of data, all with a status of SUCCESS. The first two rows describe group push updates, and the third row describes a group push mapping creation.

Time	Actor	Event Info	Targets
Mar 18 12:21:31	Josue - Cisco	Group Push group OKTA - Secure Access Users updated in app.	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.	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

Log OKTA

## Informazioni correlate

[Configura provider di identità](#)

[Assegna ruoli a utenti e gruppi da Okta](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).