

Gebruikers en groepen voorzien van beveiligde toegang via OKTA

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Cisco Secure Access configureren](#)

[Provisioning configureren in OKTA](#)

[Verifiëren](#)

[Versie in Cisco Secure Access](#)

[Verliefteit in OKTA](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe gebruikersgroepen van OKTA naar Cisco Secure Access kunnen worden aangeboden.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Access
- OKTA

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

- Cisco Secure Access-dashboard

- OKTA

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Cisco Secure Access ondersteunt de provisioning van gebruikers en groepen van OKTA.

Met deze voorziening kan Secure Access een directory bijhouden van gebruikers die geautoriseerd zijn om:

- Inschrijven bij Zero Trust Access (ZTA).
- Maak verbinding met VPNaaS.
- Pas op identiteit gebaseerd beleid toe op Umbrella Roaming-gebruikers.



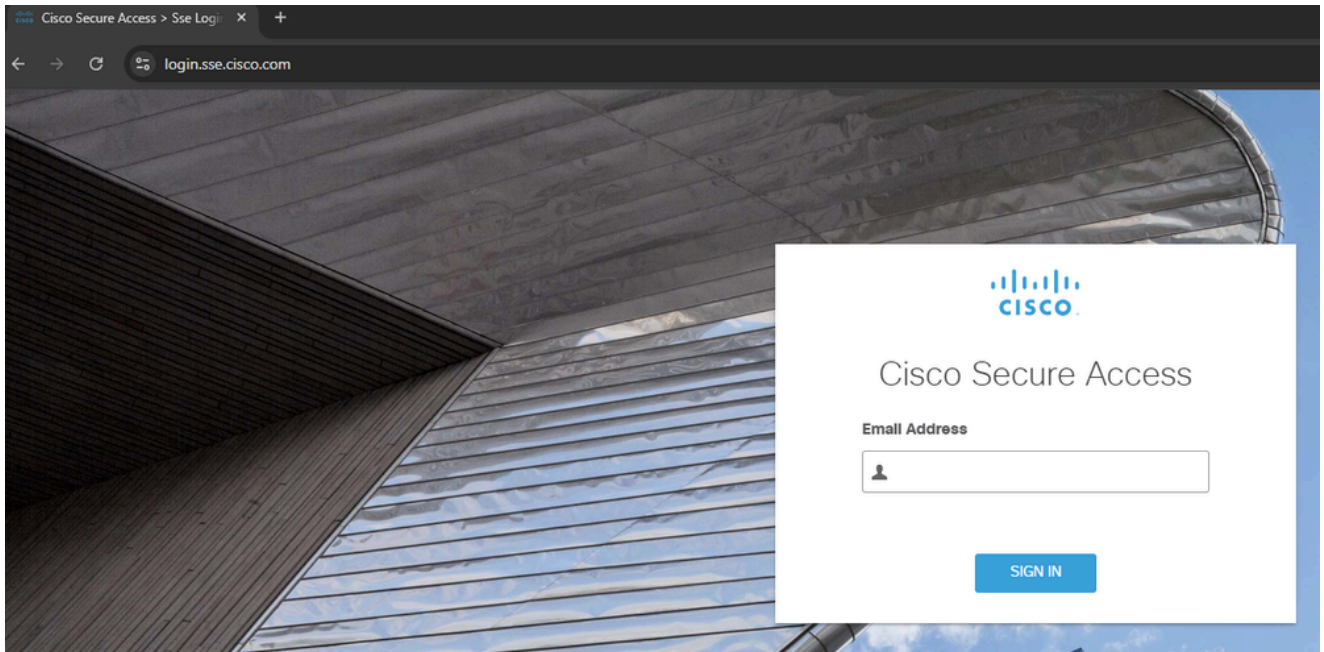
Opmerking: Dit document richt zich specifiek op de provisioning van gebruikers en groepen van OKTA. De configuratie van Entra ID of andere Identity Providers (IdP) voor ZTA-inschrijving, VPNaaS-verificatie of specifieke Umbrella Roaming-instellingen valt buiten het bereik van deze handleiding.

Configureren

Cisco Secure Access configureren

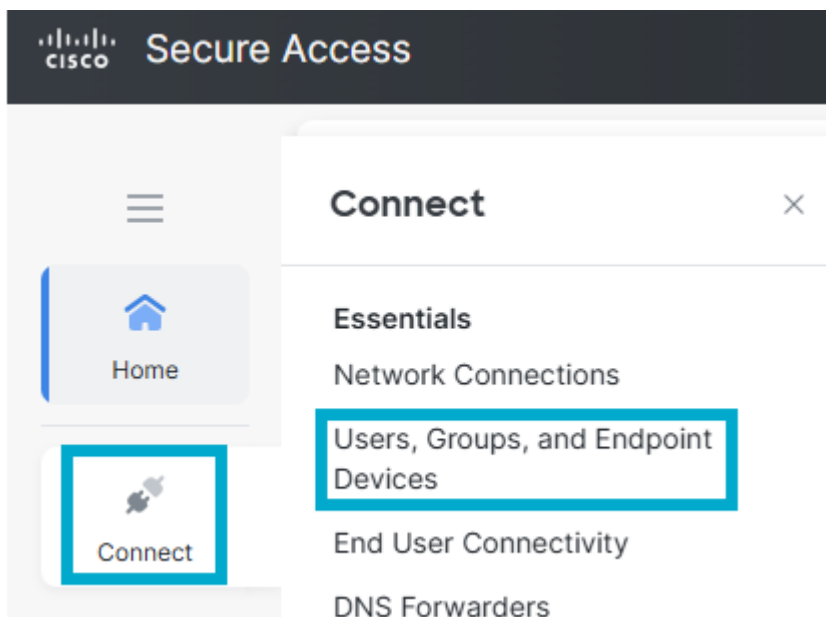
Om het provisioningproces te starten, moet u eerst de directory-integratie configureren in het Cisco Secure Access-dashboard. Deze stap genereert de nodige referenties en configuratieparameters die nodig zijn om een beveiligde verbinding met OKTA tot stand te brengen.

1. Meld u aan bij het Cisco Secure Access [Dashboard](#).



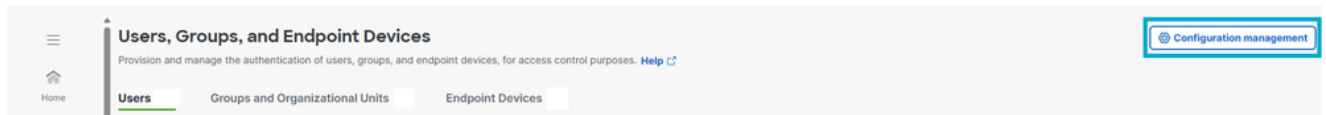
Inloggen bij CSA

2. Navigeer naar Verbinden > Gebruikers, Groepen en Eindpuntapparaten.



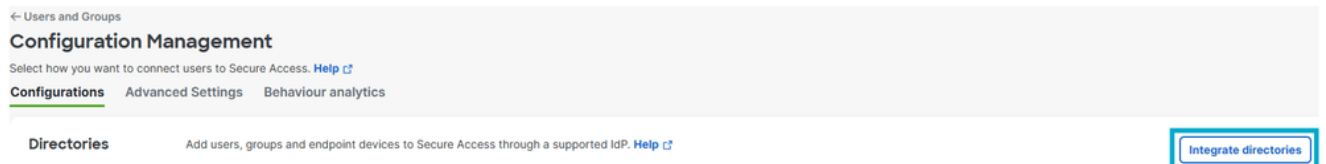
Gebruikers en groepen

3. Klik op Configuratiebeheer.



Configuratiebeheer

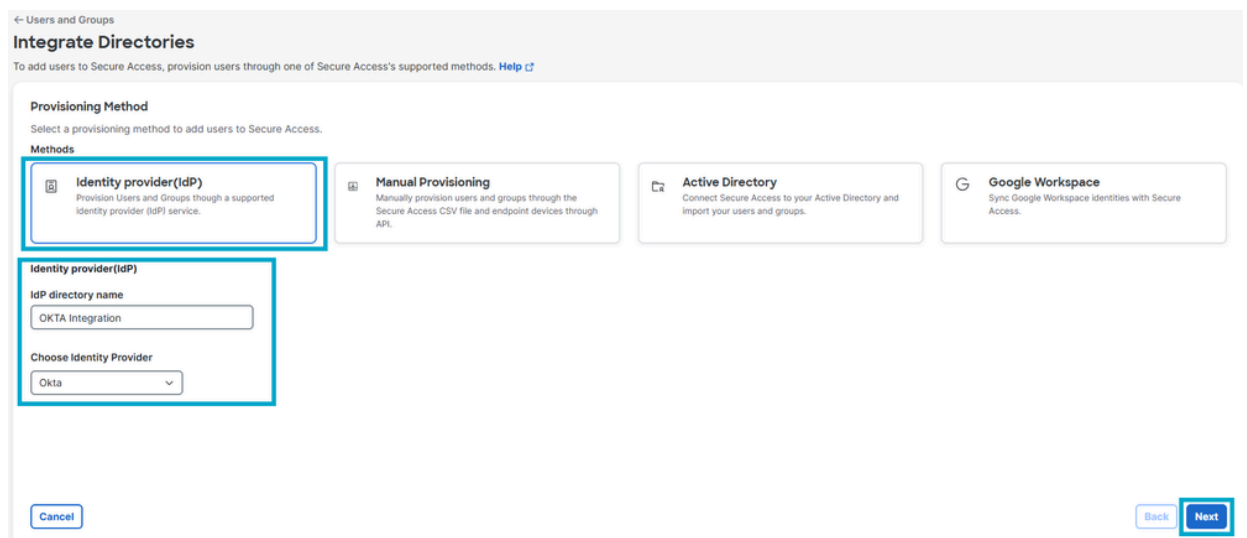
4. Klik op Directory integreren.



Directory integreren

5. Klik onder Provisioning Method op Identity Provider.

- IdP-directorynaam: OKTA Integration.
- Kies Identiteitsprovider: OKTA.
- Klik op Next (Volgende).



Directory Configuration

6. Klik op Token genereren. Sla de gegenereerde token en de provisioning-URL op en klik op Gereed.

← 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

Token <input type="text"/> Copy token	Generated On 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"/> 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](#)

Token genereren

Provisioning configureren in OKTA

Nadat u uw referenties hebt gegenereerd in het Cisco Secure Access-dashboard, moet u de provisioning-instellingen configureren in uw OKTA-tenant om de synchronisatie van gebruikers en groepen mogelijk te maken.

1. Log in bij [OKTA](#).

okta

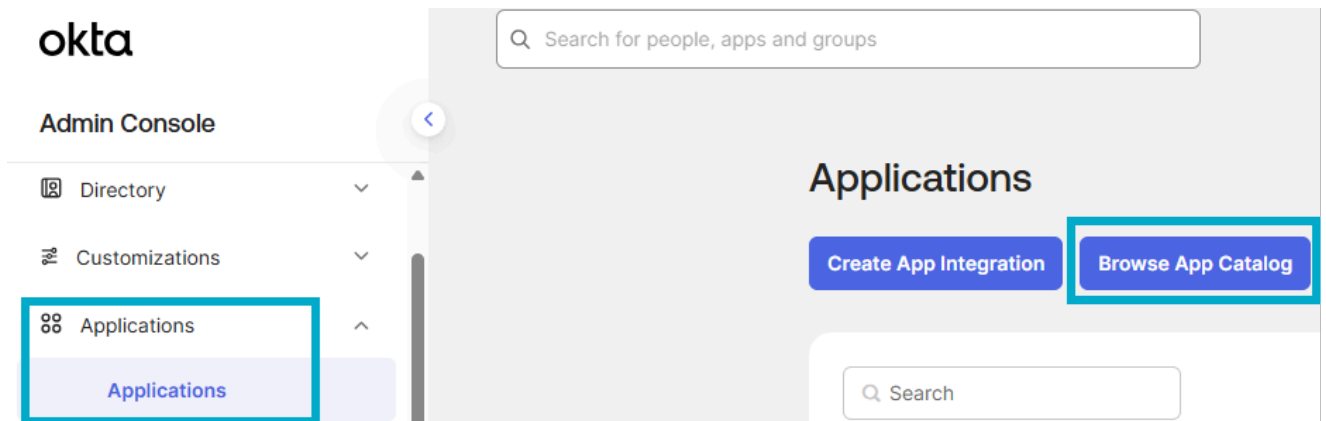
Enter your Okta organization URL

Organization URL

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

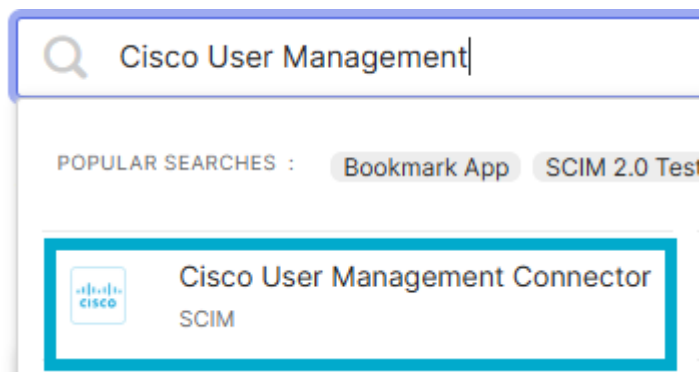
[Continue](#)

2. Navigeer naar Toepassingen > Browser App Catalogus.



Bladeren in app-catalogus

3. Selecteer de app Cisco User Management Connector.



Cisco-app

4. Klik op Integratie toevoegen.

Last updated: December 2, 2024

+ Add Integration



Cisco User Management Connector

SCIM

Integratie toevoegen

5. Klik op Gereed.

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

App toevoegen

6. Klik op Provisioning > Configure API Integration (API-integratie configureren).

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

Provisioning is not enabled

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

[Configure API Integration](#)

API-integratie configureren

7. Klik op API-integratie inschakelen en voer de op basis gebaseerde URL en API-token in die zijn opgeslagen in stap 6 van de configuratie voor beveiligde toegang. Klik op API-referenties testen en vervolgens op Opslaan.

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

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

API-test

8. Navigeer naar Provisioning > To App. Schakel de opties Gebruikers maken, Gebruikerskenmerken bijwerken en Gebruikers deactiveren in, klik op Opslaan.

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

Levering aan app



Opmerking: controleer of u deze kenmerken hebt geselecteerd voor synchronisatie met Secure Access. Secure Access vermeldt alleen de attributen Display name en User name voor gebruikers, niet de attributen Given name en Family name: User name, Given name, Family, name, Display name, Email

(Optioneel) Voeg een [objectGUID-kenmerk toe](#) en maak de toewijzing van gebruikersprofielen. Als u het objectGUID-kenmerk voor gebruikers moet importeren, voegt u een nieuw kenmerk toe en koppelt u de kenmerken in de profieltoewijzing.

- Als u mensen/groepen wilt toevoegen, klikt u op Toewijzingen > Toewijzen > Toewijzen aan mensen/Toewijzen aan groepen.

The screenshot shows the Cisco User Management Connector interface. At the top, there is a header with the Cisco logo, a status indicator 'Active', and navigation links for 'View Logs' and 'Monitor Imports'. Below the header, there are tabs for 'General', 'Provisioning', 'Import', 'Assignments', and 'Push Groups'. The 'Assignments' tab is selected and highlighted with a red box. In the main content area, there is a search bar and a 'Groups' dropdown menu. A red box highlights the 'Assign' dropdown menu, which is open and shows two options: 'Assign to People' and 'Assign to Groups'. Below the search bar, there is a list of assignments represented by binary strings (01101110, 01101111, 01101100, 01101101, 01101110, 01100111). A magnifying glass icon is positioned over the list, and the text 'No groups found' is displayed below it.

toewijzing

10. Selecteer de groepen/personen die u wilt inrichten voor Secure Access en klik op Toewijzen en vervolgens op Gereed.

Assign Cisco User Management Connector to Groups

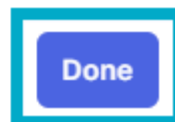


Assign



OKTA - Secure Access Users

Assigned

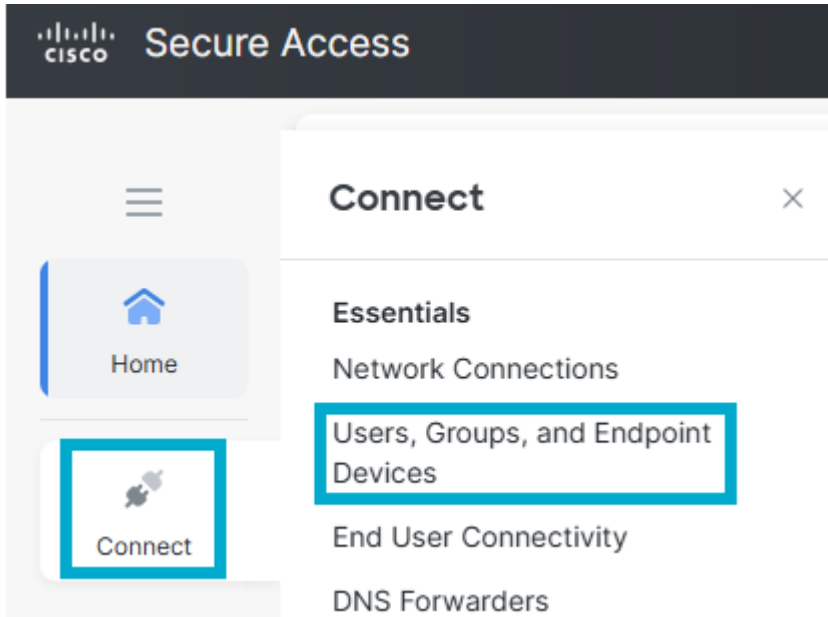


Groepen toewijzen

Verifiëren

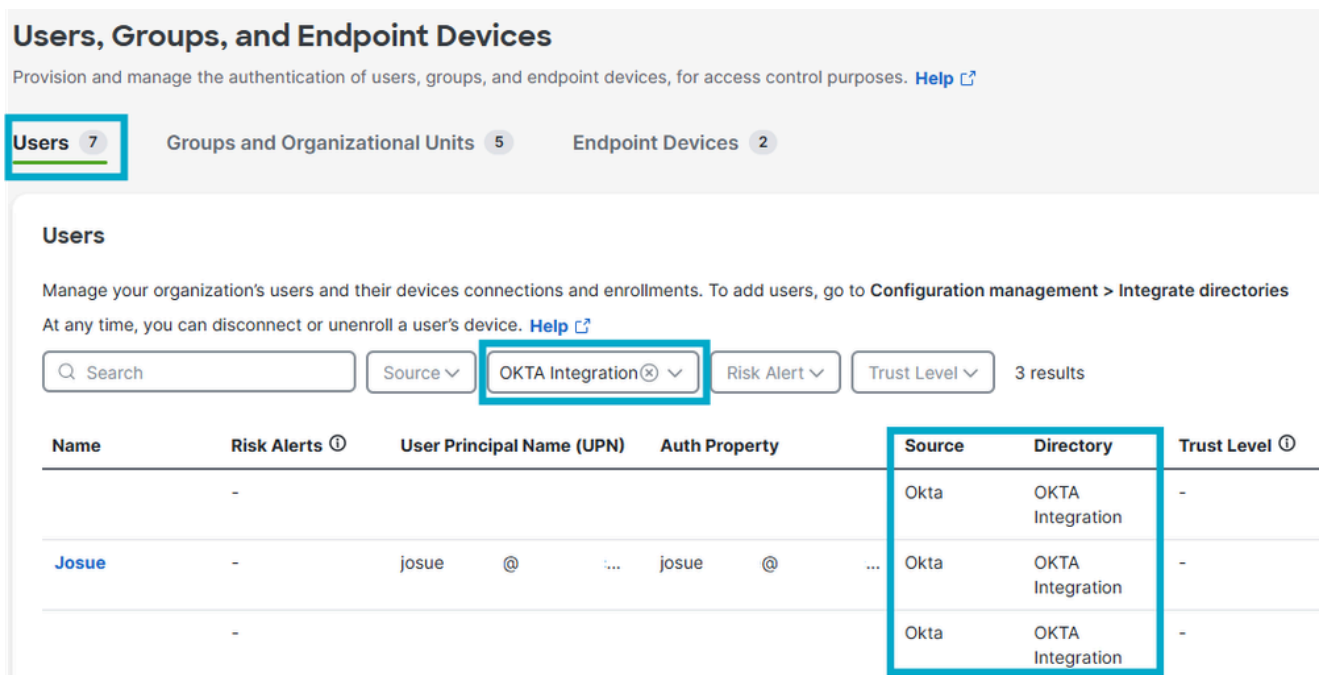
Versie in Cisco Secure Access

- Navigeer naar Verbinden > Gebruikers, groepen en eindpuntapparaten.



Gebruikers en groepen in CSA

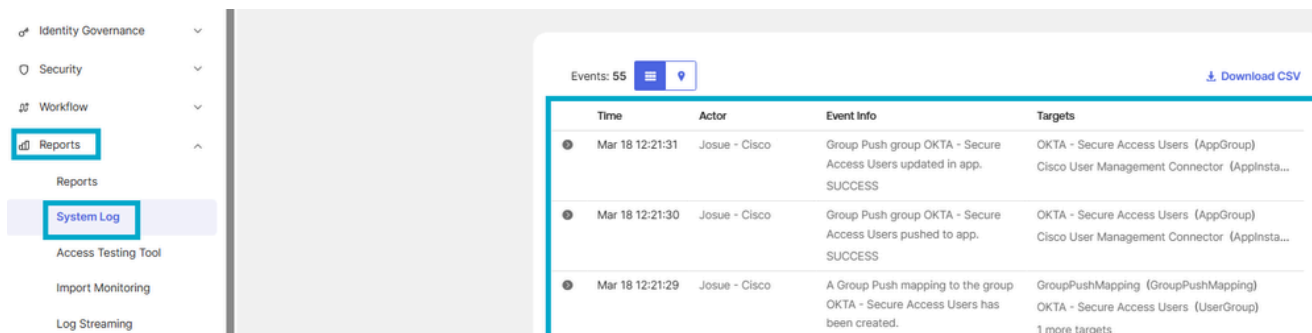
- Klik op Gebruikers.



Gebruikers verifiëren in CSA

Veraliteit in OKTA

- Navigeer naar Rapporten > Systeemlogboek.



OKTA-logboeken

Gerelateerde informatie

[Identiteitsproviders configureren](#)

[Aanbieding Gebruikers en groepen van Okta](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.