

Bereitstellung von Benutzern und Gruppen für den sicheren Zugriff über OKTA

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurieren von Cisco Secure Access](#)

[Konfiguration der Bereitstellung in OKTA](#)

[Überprüfung](#)

[Verity in Cisco Secure Access](#)

[Veritas in OKTA](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Benutzergruppen von OKTA für Cisco Secure Access bereitgestellt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicherer Zugriff von Cisco
- OKTA

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

- Cisco Secure Access Dashboard

- OKTA

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Cisco Secure Access unterstützt die Bereitstellung von Benutzern und Gruppen von OKTA.

Diese Bereitstellung ermöglicht Secure Access die Verwaltung eines Verzeichnisses von Benutzern, die autorisiert sind,

- Registrieren Sie sich für Zero Trust Access (ZTA).
- Herstellen einer Verbindung mit VPNaaS
- Anwendung identitätsbasierter Richtlinien auf Umbrella Roaming-Benutzer



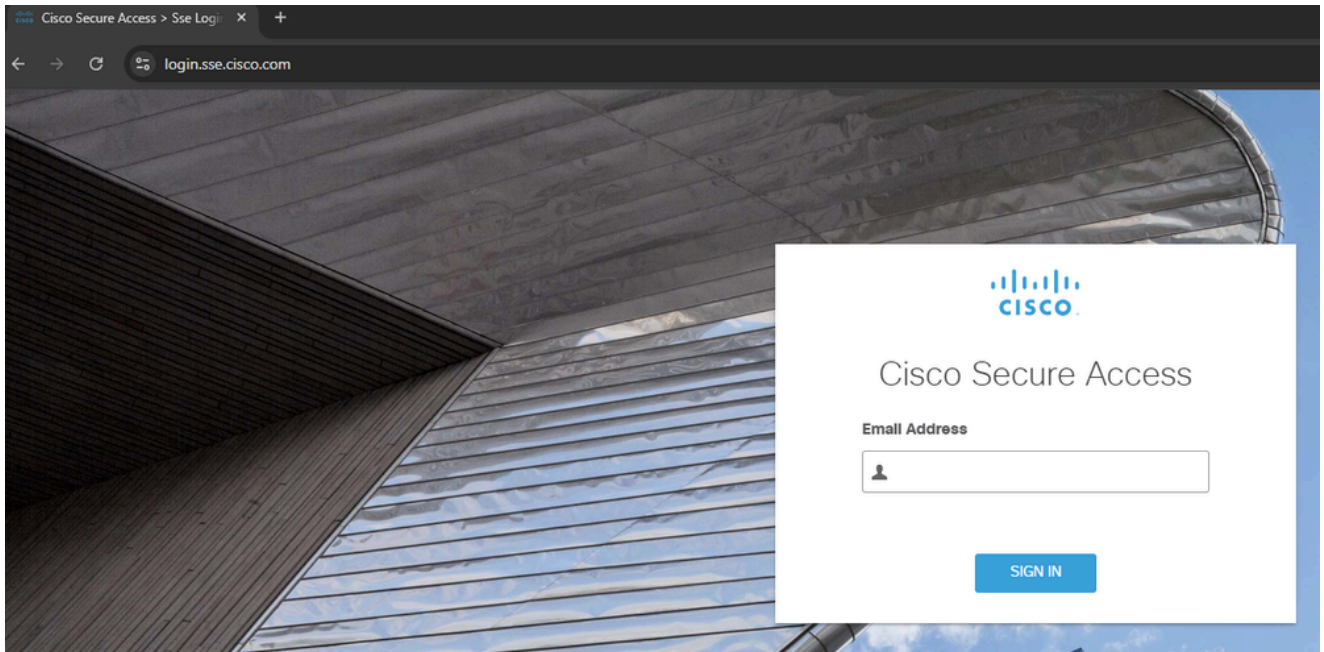
Anmerkung: Dieses Dokument konzentriert sich speziell auf die Bereitstellung von Benutzern und Gruppen von OKTA. Die Konfiguration der Entra-ID oder anderer Identitätsanbieter (IdP) für die ZTA-Registrierung, die VPNaaS-Authentifizierung oder bestimmte Umbrella Roaming-Einstellungen wird in diesem Leitfaden nicht behandelt.

Konfigurieren

Konfigurieren von Cisco Secure Access

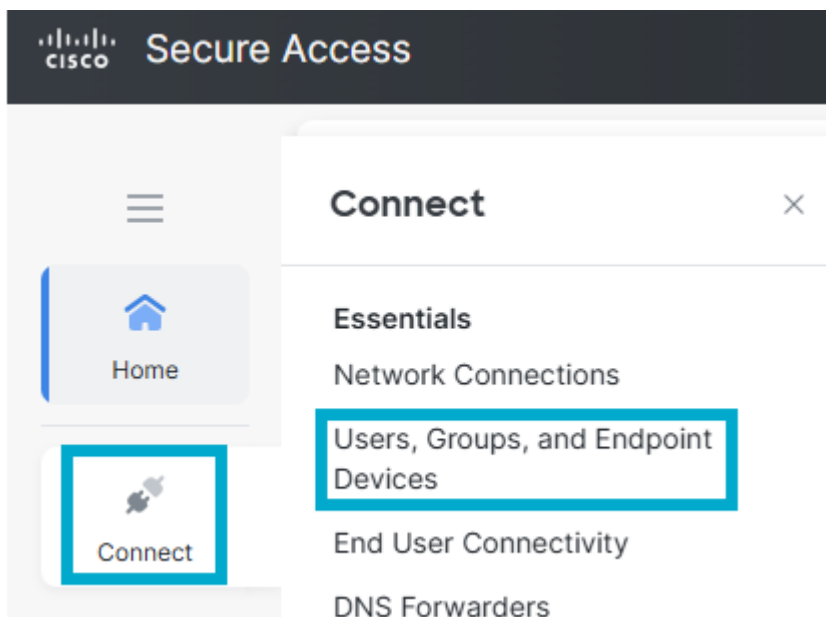
Um mit der Bereitstellung zu beginnen, müssen Sie zunächst die Verzeichnisintegration im Cisco Secure Access Dashboard konfigurieren. In diesem Schritt werden die erforderlichen Anmeldeinformationen und Konfigurationsparameter für den Aufbau einer sicheren Verbindung mit OKTA generiert.

1. Melden Sie sich beim Cisco Secure Access [Dashboard an](#).



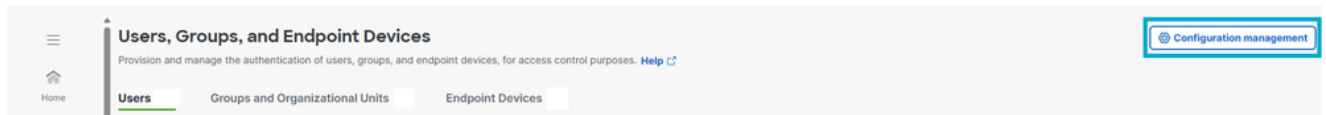
Bei CSA anmelden

2. Navigieren Sie zu Verbinden > Benutzer, Gruppen und Endgeräte.



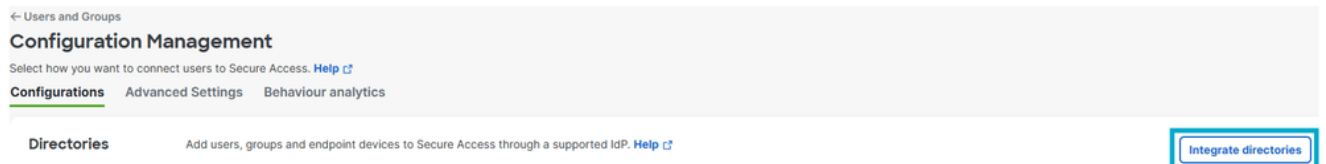
Benutzer und Gruppen

3. Klicken Sie auf Konfigurationsmanagement.



Konfigurationsverwaltung

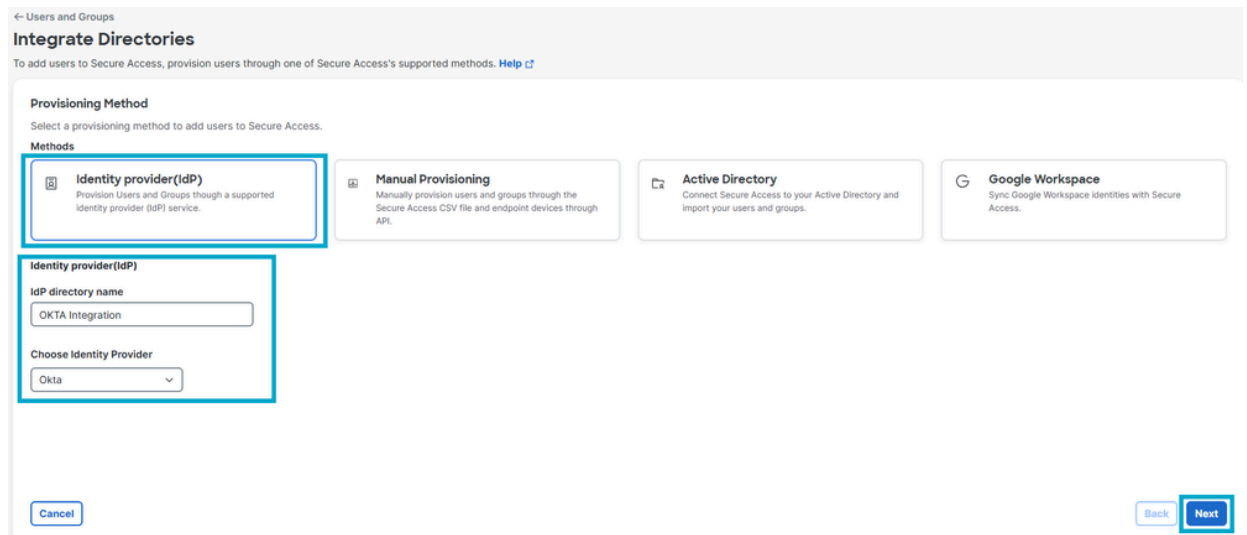
4. Klicken Sie auf Verzeichnis integrieren.



Verzeichnis integrieren

5. Klicken Sie unter Bereitstellungsmethode auf Identitätsanbieter.

- IdP-Verzeichnisname: OKTA-Integration.
- Identitätsanbieter auswählen: OKTA.
- Klicken Sie auf Next (Weiter).



Directory Configuration

6. Klicken Sie auf Token generieren. Speichern Sie das generierte Token und die Bereitstellungs-URL, und klicken Sie dann auf Fertig.

← 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>Token</p> <input type="text"/> Copy token	<p>Generated On</p> <p>March 18, 2026</p>
<p>Provisioning URL</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"/> 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 generieren

Konfiguration der Bereitstellung in OKTA

Nachdem Sie Ihre Anmeldeinformationen im Cisco Secure Access Dashboard generiert haben, müssen Sie die Bereitstellungseinstellungen in Ihrem OKTA-Tenant konfigurieren, um die Synchronisierung von Benutzern und Gruppen zu ermöglichen.

1. Melden Sie sich bei [OKTA an](#).

okta

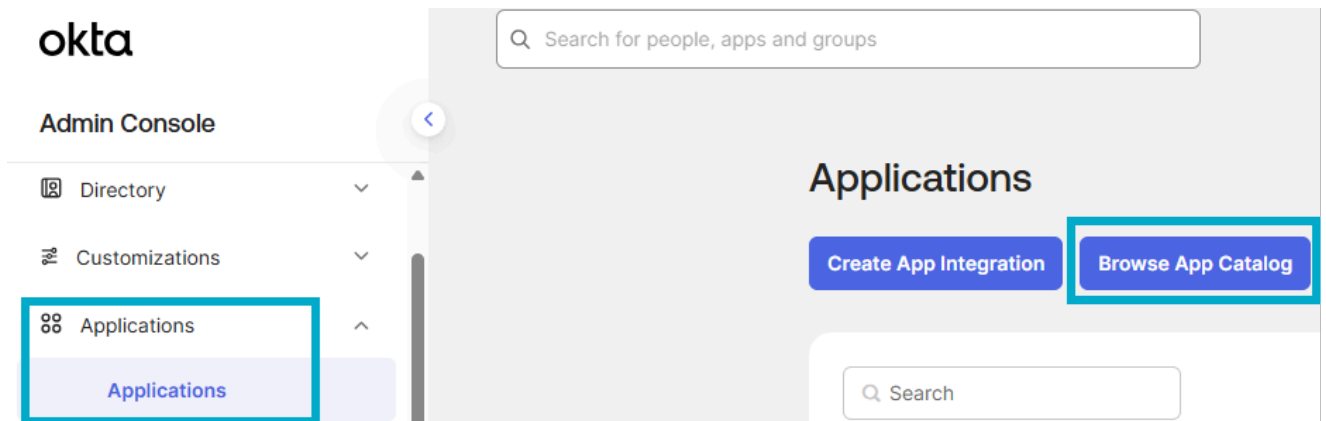
Enter your Okta organization URL

Organization URL

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

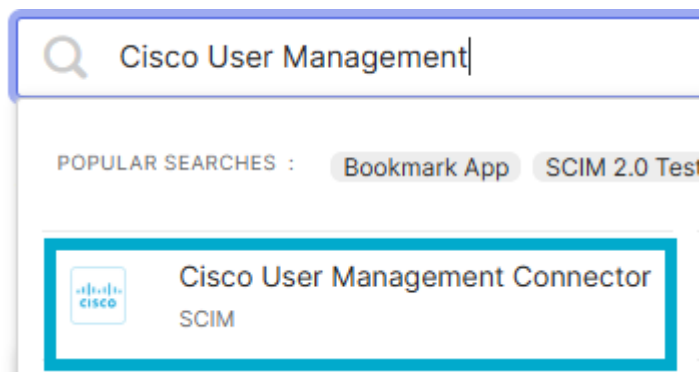
[Continue](#)

2. Navigieren Sie zu Anwendungen > Browser App Catalog.



Katalog durchsuchen

3. Wählen Sie die Cisco User Management Connector-App aus.



Cisco Anwendung

4. Klicken Sie auf Integration hinzufügen.

Last updated: December 2, 2024

+ Add Integration



Cisco User Management Connector

SCIM

Integration hinzufügen

5. Klicken Sie auf Done (Fertig).

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 hinzufügen

6. Klicken Sie auf 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 indicator set to 'Active', and links for 'View Logs' and 'Monitor Imports'. Below the header, there are navigation tabs: 'General', 'Provisioning' (which is selected and 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 displays a message: '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 message, a status message reads 'Provisioning is not enabled' with a sub-message: '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 status message.

API-Integration konfigurieren

7. Klicken Sie auf API-Integration aktivieren, und geben Sie die Based URL und API Token ein, die in Schritt #6 der Secure Access Configuration gespeichert sind. Klicken Sie auf Test API Credentials (API-Anmeldeinformationen testen) und dann auf 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

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. Navigieren Sie zu Provisioning > To App. Aktivieren Sie die Optionen Benutzer erstellen, Benutzerattribute aktualisieren und Benutzer deaktivieren, und klicken Sie auf Speichern.

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

Bereitstellung für Anwendung



Anmerkung: Überprüfen Sie, ob Sie diese Attribute für die Synchronisierung mit Secure Access ausgewählt haben. In Secure Access werden nur die Attribute "Anzeigename" und "Benutzername" für Benutzer aufgeführt, nicht die Attribute "Vorname" und "Nachname": Benutzername, Vorname, Familie, Name, Anzeigename, E-Mail

(Optional) Fügen Sie ein [objectGUID-Attribut hinzu](#), und erstellen Sie die Benutzerprofilzuordnung. Wenn Sie das objectGUID-Attribut für Benutzer importieren müssen, fügen Sie ein neues Attribut hinzu, und ordnen Sie die Attribute in der Profilzuordnung zu.



9. Um Personen/Gruppen hinzuzufügen, klicken Sie auf Assignments > Assign > Assign to People/Assign to Groups.

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 table with the heading 'Assignment'. The table contains 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 table, the text 'No groups found' is displayed.

Zuweisung

10. Wählen Sie die Gruppen/Personen aus, die Sie für den sicheren Zugriff bereitstellen möchten, und klicken Sie auf Zuweisen und dann auf Fertig.

Assign Cisco User Management Connector to Groups ×

		Assign
	OKTA - Secure Access Users	Assigned

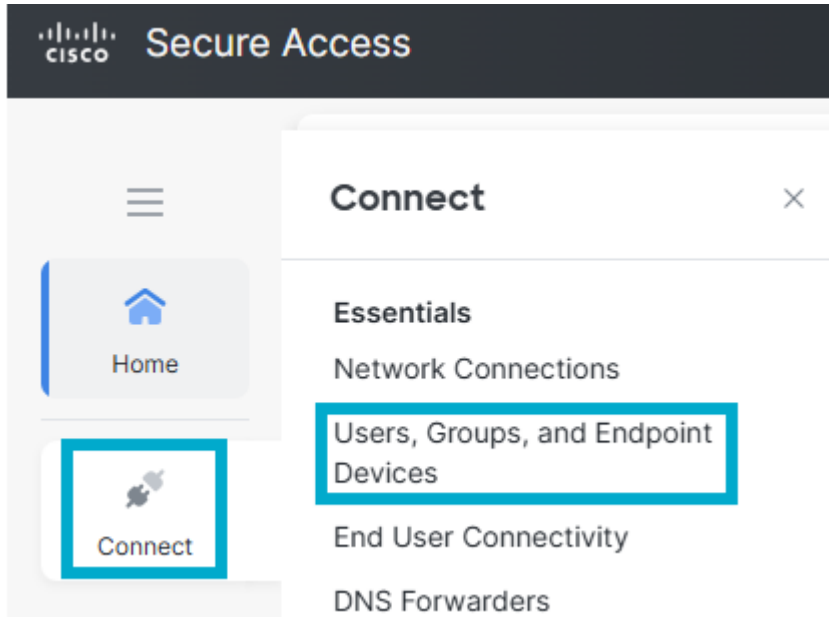
[Done](#)

Gruppen zuweisen

Überprüfung

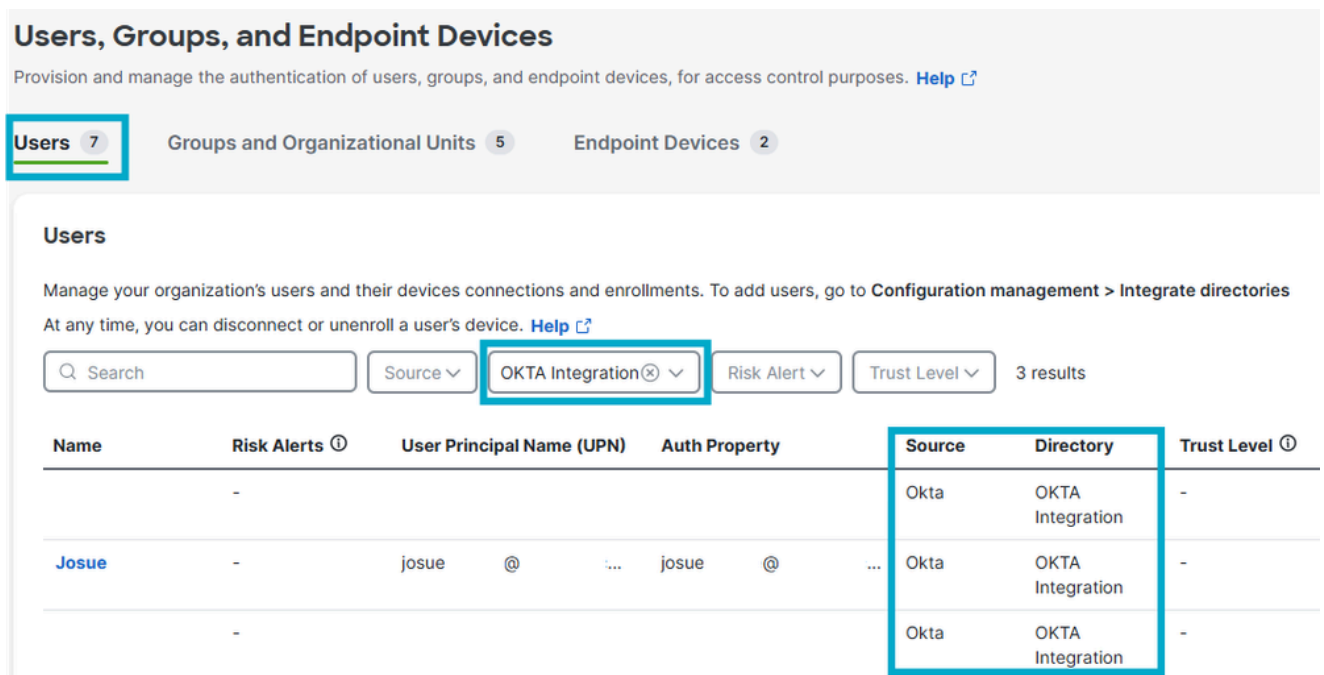
Verity in Cisco Secure Access

- Navigieren Sie zu Verbinden > Benutzer, Gruppen und Endgeräte.



Benutzer und Gruppen in CSA

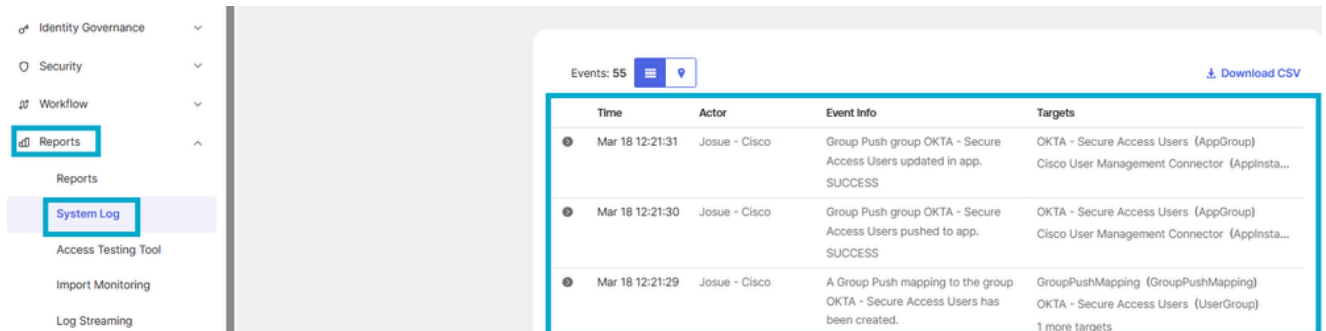
- Klicken Sie auf Benutzer.



Benutzer in CSA überprüfen

Veritas in OKTA

- Navigieren Sie zu Berichte > Systemprotokoll.



Events: 55 [Download CSV](#)

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

OKTA-Protokolle

Zugehörige Informationen

[Identitätsanbieter konfigurieren](#)

[Bereitstellung von Benutzern und Gruppen von Okta aus](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.