

# Provision Users and Groups to Secure Access via OKTA

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Configure](#)

[Configure Cisco Secure Access](#)

[Configure Provisioning in OKTA](#)

### [Verify](#)

[Verify in Cisco Secure Access](#)

[Verify in OKTA](#)

### [Related Information](#)

---

## Introduction

This document describes how to provision user groups from OKTA to Cisco Secure Access.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Access
- OKTA

### Components Used

This document is not restricted to specific software and hardware versions.

- Cisco Secure Access Dashboard
- 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. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

Cisco Secure Access supports the provisioning of users and groups from OKTA.

This provisioning enables Secure Access to maintain a directory of users authorized to:

- Enroll in Zero Trust Access (ZTA).
- Connect to VPNaaS.
- Apply identity-based policies to Umbrella Roaming users.



**Note:** This document focuses specifically on the provisioning of users and groups from OKTA. The configuration of Entra ID or other Identity Providers (IdP) for ZTA enrollment, VPNaaS authentication, or specific Umbrella Roaming settings is outside the scope of this guide.

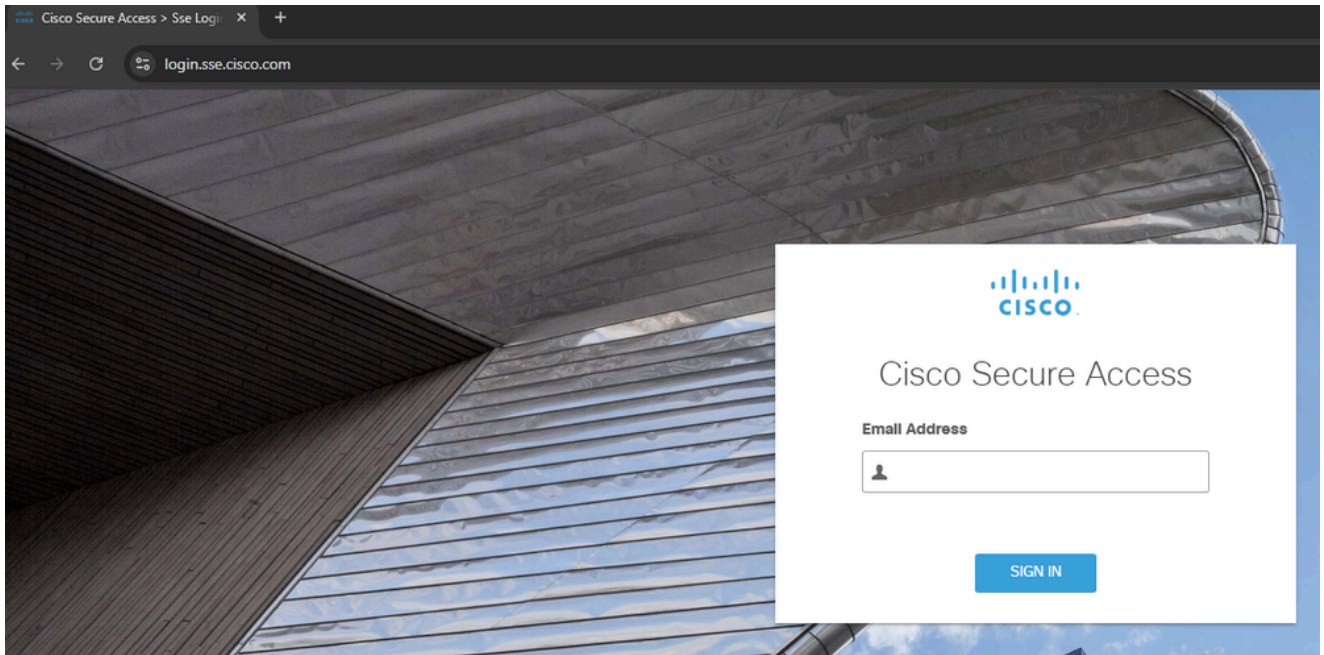
---

## Configure

### Configure Cisco Secure Access

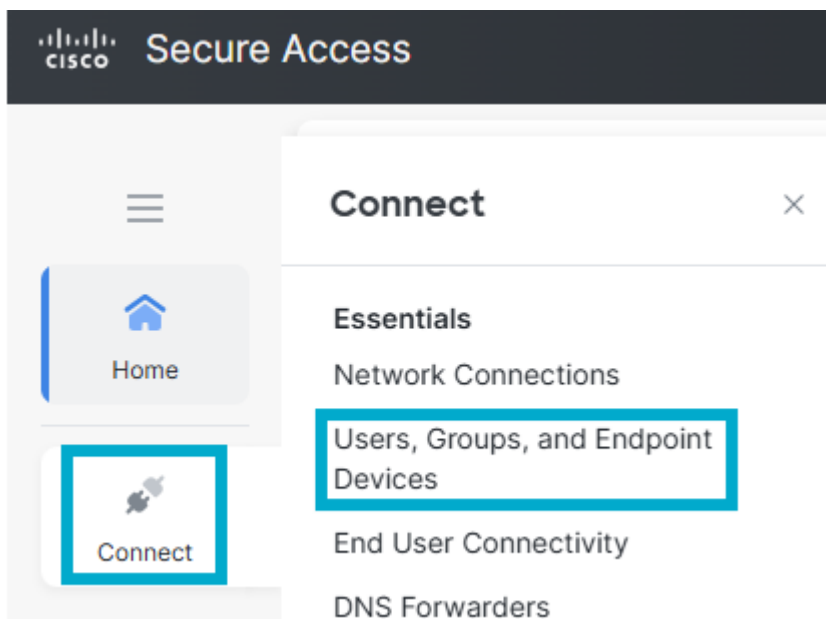
In order to begin the provisioning process, you must first configure the directory integration within the Cisco Secure Access dashboard. This step generates the necessary credentials and configuration parameters required to establish a secure connection with OKTA.

1. Sign in to the **Cisco Secure Access [Dashboard](#)**.



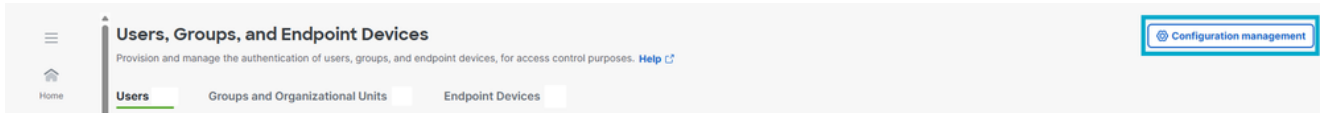
*Sign in to CSA*

2. Navigate to **Connect > Users, Groups and Endpoint Devices**.



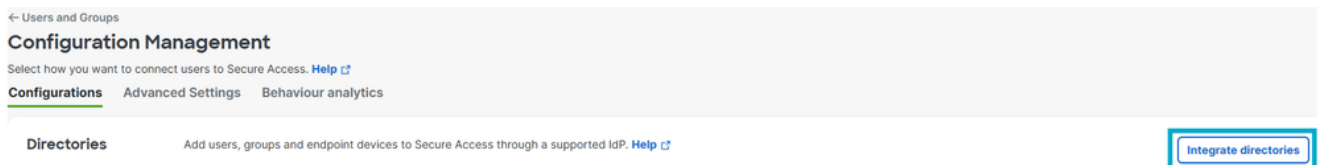
*Users and Groups*

3. Click **Configuration management**.



*Configuration Management*

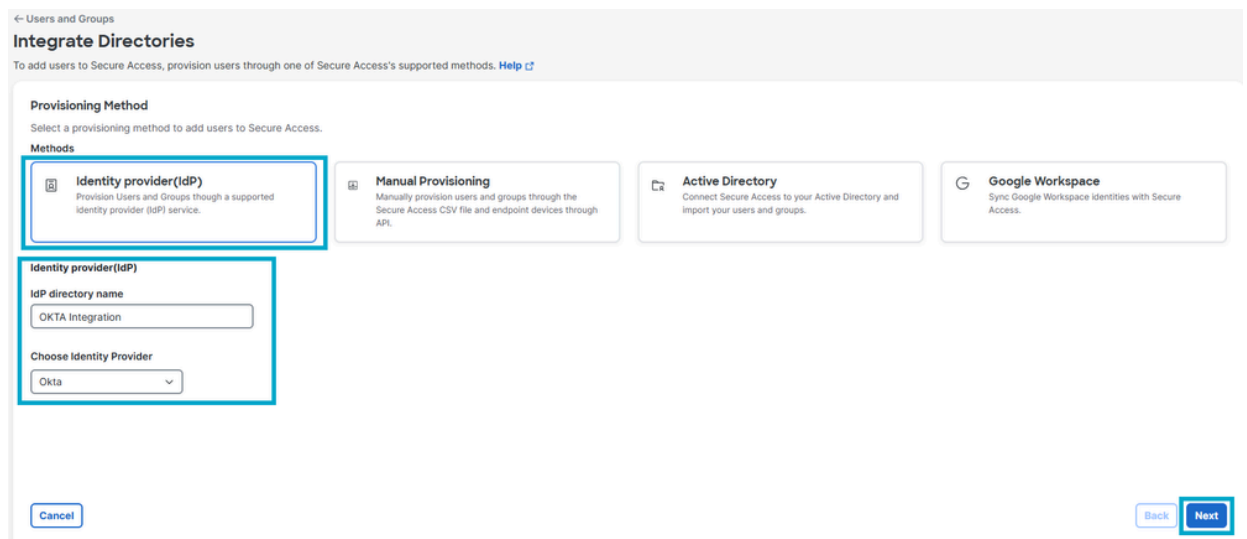
#### 4. Click **Integrate Directory**.



*Integrate Directory*

#### 5. Under Provision Method click **Identity Provider**.

- **IdP directory name: OKTA Integration.**
- **Choose Identity Provider: OKTA.**
- **Click Next.**



*Directory Configuration*

#### 6. Click **Generate Token**. Save the **generated token** and the **provisioning URL**, then click **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](#)

*Generate Token*

## Configure Provisioning in OKTA

Once you have generated your credentials in the Cisco Secure Access dashboard, you must configure the provisioning settings within your OKTA tenant to enable the synchronization of users and groups.

1. Sign in to [OKTA](#).

# okta

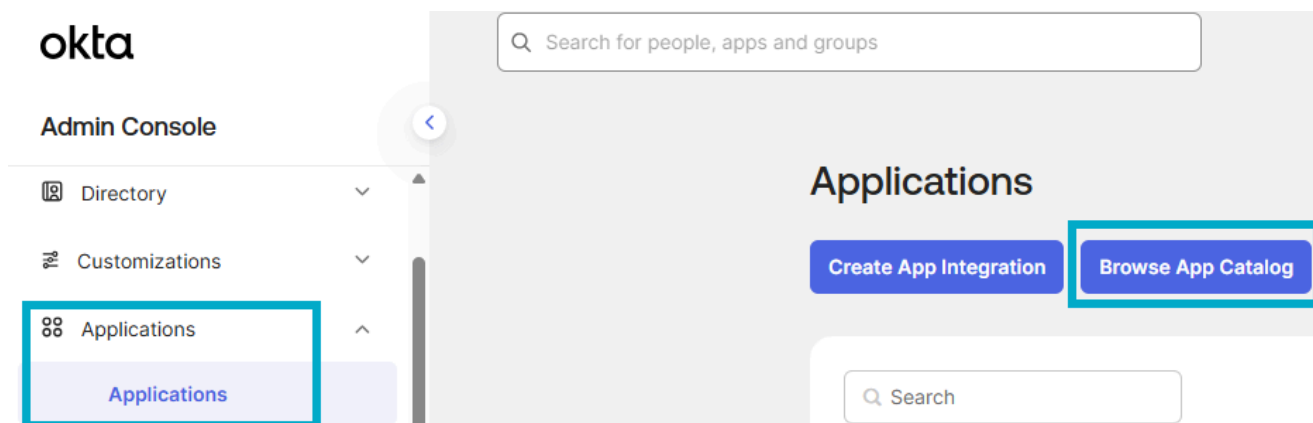
## Enter your Okta organization URL

**Organization URL**

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

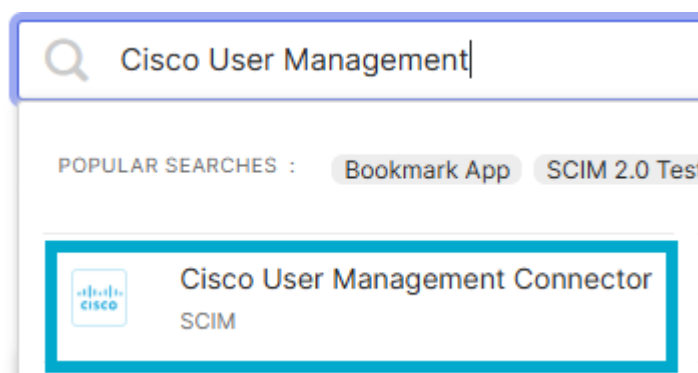
[Continue](#)

2. Navigate to **Applications > Browser App Catalog**.



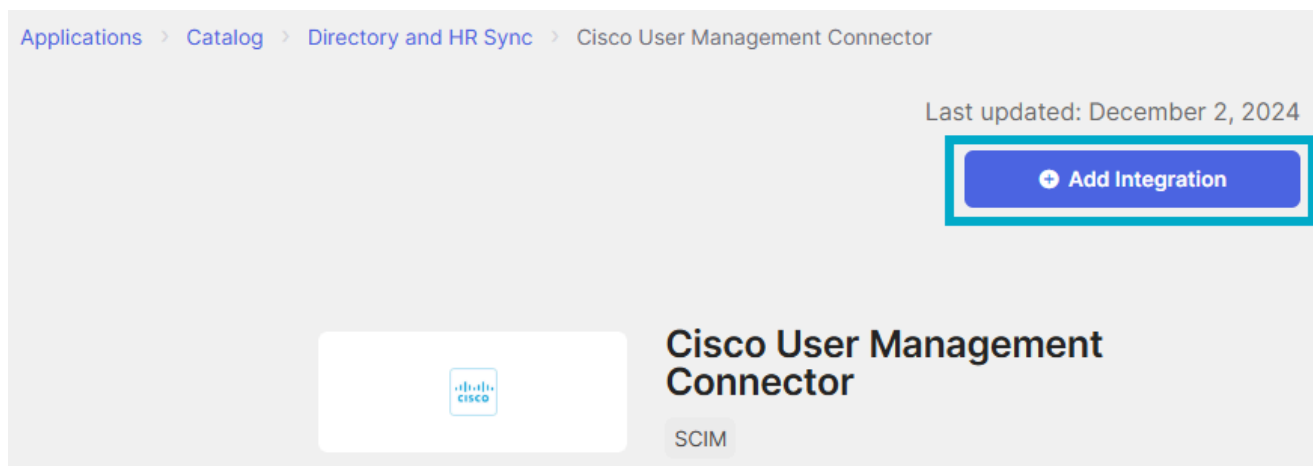
*Browse App Catalog*

3. Select **Cisco User Management Connector** app.



*Cisco App*

4. Click **Add Integration**.



*Add Integration*

5. Click **Done**.

**Add Cisco User Management Connector**

1 General Settings

### General settings - Required

Application label

This label displays under the app on your home page

Application Visibility  Do not display application icon to users

[Cancel](#) [Done](#)

*Add App*

6. Click **Provisioning > Configure API Integration**.

**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](#)

*Configure API Integration*

7. Click **Enable API Integration** and enter the **Based URL** and **API Tokens** saved from step #6 of the Secure Access Configuration. Click **Test API Credentials** and then **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**

API Test

8. Navigate to **Provisioning > To App**. Enable the options **Create Users, Update User Attributes and Deactivate Users**, click **Save**.

General **Provisioning** Import Assignments Push Groups

Settings  
To App  
To Okta  
Integration



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

*Provision to App*



**Note:** Verify that you select these attributes for synchronization to Secure Access. Secure Access only lists the Display name and Username attributes for users, not the Given name and Family name attributes: Username, Given name, Family, name, Display name, Email

(Optional) Add an [objectGUID Attribute](#) and Create the User Profile Mapping. If you need to import the objectGUID attribute for users, add a new attribute and map the attributes in the profile mapping.

9. In order to add people/groups, click **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 set to "Active", and links for "View Logs" and "Monitor Imports". Below the header is a navigation bar with tabs for "General", "Provisioning", "Import", "Assignments" (which is highlighted with a red box), and "Push Groups".



In the "Assignments" section, there is a sub-header with two buttons: "Assign" (highlighted with a red box) and "Convert assignments". Below these buttons is a search bar labeled "Search..." and a "Groups" dropdown menu. A dropdown menu is open under the "Assign" button, showing two options: "Assign to People" and "Assign to Groups", both of which are also highlighted with a red box.

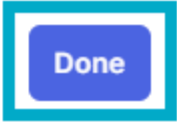
Below the dropdown menu, there is a "Groups" section with a list of binary strings: 01101110, 01101111, 01101100, 01101100, 01101101, 01101110, and 01100111. A magnifying glass icon is positioned over the list. Below the list, it says "No groups found".

*Assignment*

10. Select the **groups/people** you want to provision to Secure Access and click **Assign** and then **Done**.

# Assign Cisco User Management Connector to Groups ×

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

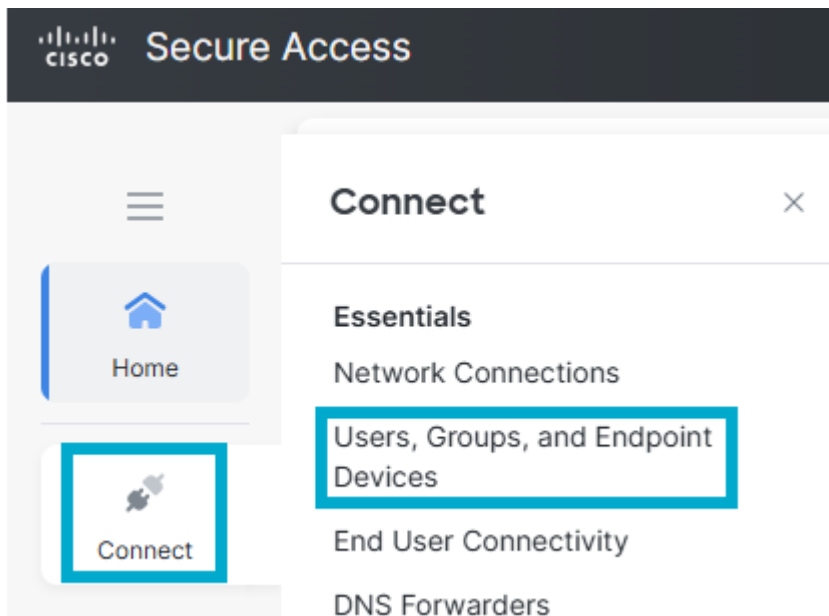


*Assign Groups*

## Verify

### Verify in Cisco Secure Access

- Navigate to **Connect > Users, Groups and Endpoint Devices**.



Users and Groups in CSA

- Click **Users**.

### Users, Groups, and Endpoint Devices

Provision and manage the authentication of users, groups, and endpoint devices, for access control purposes. [Help](#)

**Users** 7    Groups and Organizational Units 5    Endpoint Devices 2

**Users**

Manage your organization's users and their devices connections and enrollments. To add users, go to **Configuration management > Integrate directories**. At any time, you can disconnect or unenroll a user's device. [Help](#)

3 results

Name	Risk Alerts ⓘ	User Principal Name (UPN)	Auth Property	Source	Directory	Trust Level ⓘ
	-			Okta	OKTA Integration	-
<b>Josue</b>	-	josue @ ...	josue @ ...	Okta	OKTA Integration	-
	-			Okta	OKTA Integration	-

Verify Users in CSA

## Verity in OKTA

- Navigate to **Reports > System Log**.

The screenshot shows the Okta System Log interface. On the left is a navigation menu with categories: Identity Governance, Security, Workflow, Reports, and System Log (highlighted). Under Reports, there are sub-items: Reports, System Log (highlighted), Access Testing Tool, Import Monitoring, and Log Streaming. The main content area displays a table of events with 55 total events. The table has columns for Time, Actor, Event Info, and Targets. Three events are visible, all from 'Josue - Cisco' on 'Mar 18'.

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 (Applnsta...)
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 (Applnsta...)
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 Logs*

## Related Information

[Configure Identity Providers](#)

[Provision Users and Groups from Okta](#)