

Aprovisionamiento de usuarios y grupos para un acceso seguro mediante OKTA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuración de Cisco Secure Access](#)

[Configurar el aprovisionamiento en OKTA](#)

[Verificación](#)

[Veracidad en Cisco Secure Access](#)

[Verity en OKTA](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo proveer grupos de usuarios de OKTA a Cisco Secure Access.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso seguro de Cisco
- OKTA

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

- Panel de Cisco Secure Access

- OKTA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco Secure Access admite el aprovisionamiento de usuarios y grupos de OKTA.

Este aprovisionamiento permite a Secure Access mantener un directorio de usuarios autorizados para:

- Inscríbase en Zero Trust Access (ZTA).
- Conéctese a VPNaaS.
- Aplique políticas basadas en identidad a los usuarios de Umbrella Roaming.



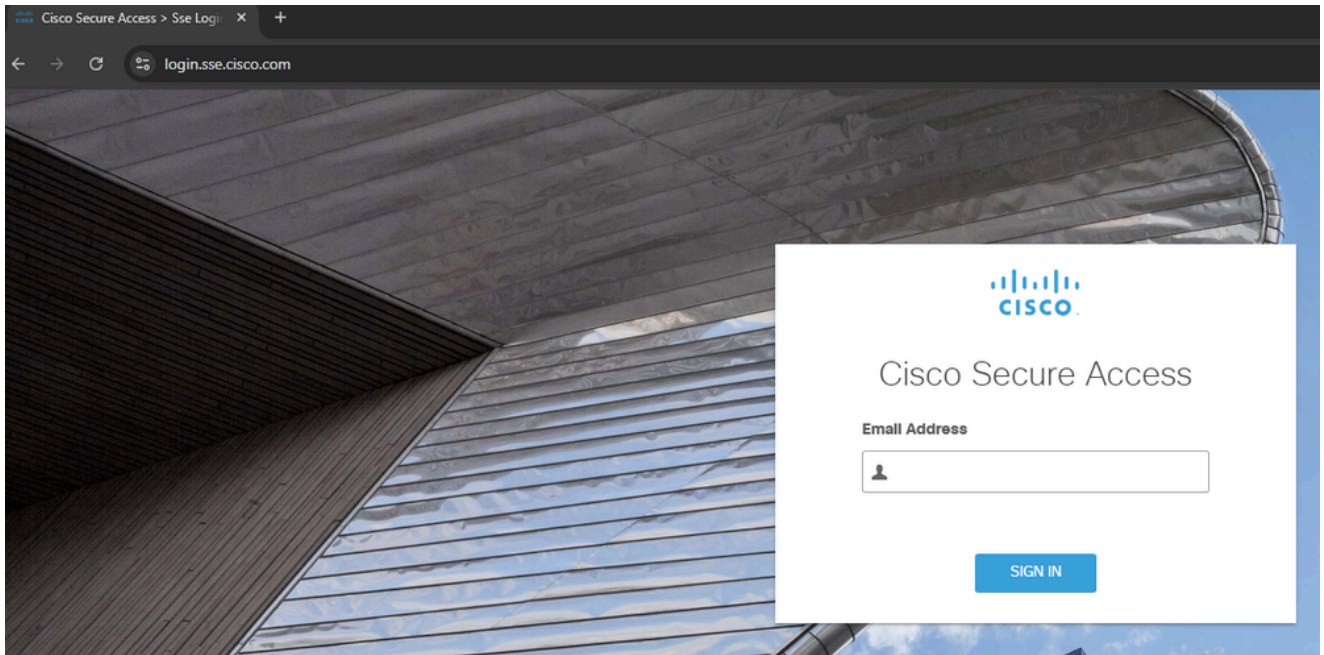
Nota: Este documento se centra específicamente en el aprovisionamiento de usuarios y grupos de OKTA. La configuración de la ID de entrada u otros proveedores de identidad (IdP) para la inscripción ZTA, la autenticación VPNaaS o los ajustes específicos de Umbrella Roaming está fuera del alcance de esta guía.

Configurar

Configuración de Cisco Secure Access

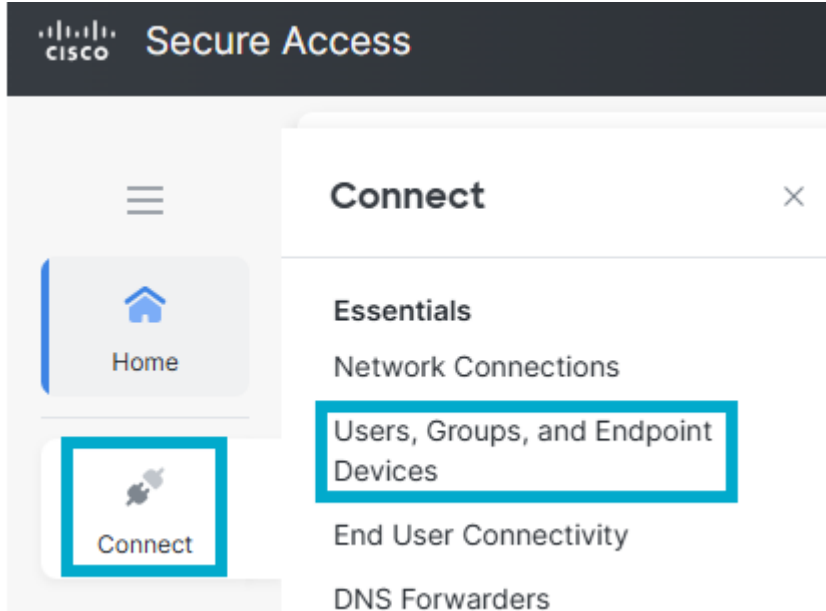
Para comenzar el proceso de aprovisionamiento, primero debe configurar la integración de directorios en el panel de Cisco Secure Access. Este paso genera las credenciales y los parámetros de configuración necesarios para establecer una conexión segura con OKTA.

1. Inicie sesión en el panel de Cisco Secure Access.



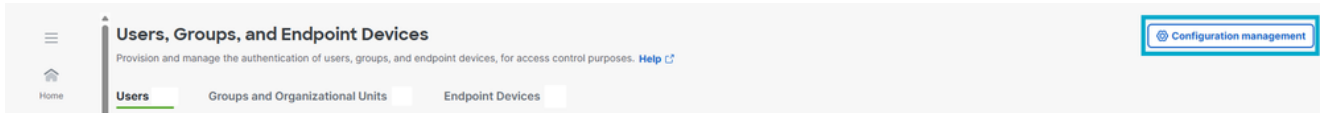
Iniciar sesión en CSA

2. Vaya a Connect > Users, Groups and Endpoint Devices.



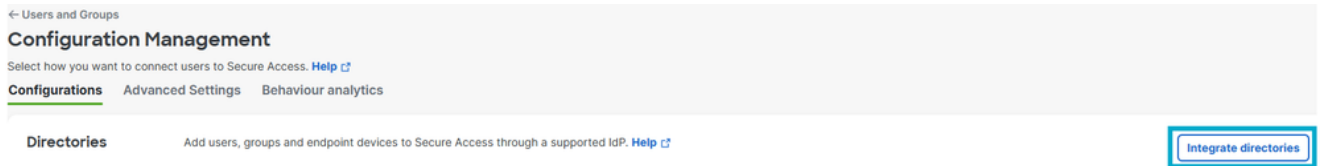
Usuarios y grupos

3. Haga clic en Configuration management.



Administración de la Configuración

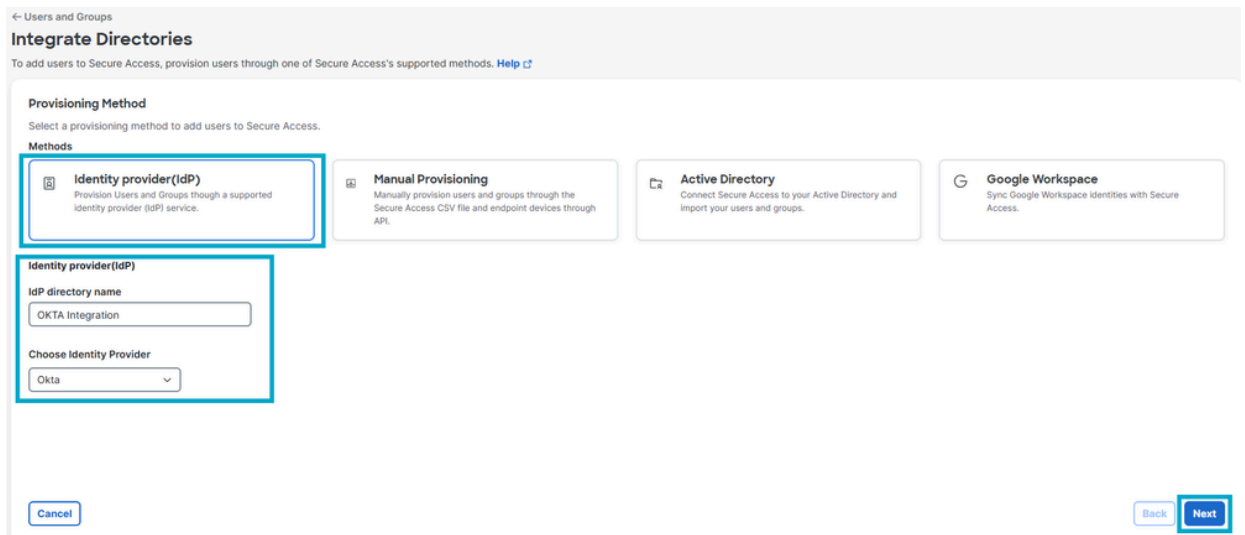
4. Haga clic en Integrar directorio.



Directorio integrado

5. En Método de aprovisionamiento, haga clic en Proveedor de identidad.

- Nombre del directorio IdP: Integración de OKTA.
- Elija el proveedor de identidad: ESTÁ BIEN.
- Haga clic en Next (Siguiente).



Directory Configuration

6. Haga clic en Generar token. Guarde el token generado y la URL de aprovisionamiento, luego haga clic en Finalizado.

← 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](#)

Generar token

Configurar el aprovisionamiento en OKTA

Una vez que haya generado sus credenciales en el panel de Cisco Secure Access, debe configurar los ajustes de aprovisionamiento dentro de su arrendatario de OKTA para habilitar la sincronización de usuarios y grupos.

1. Inicie sesión en [OKTA](#).

okta

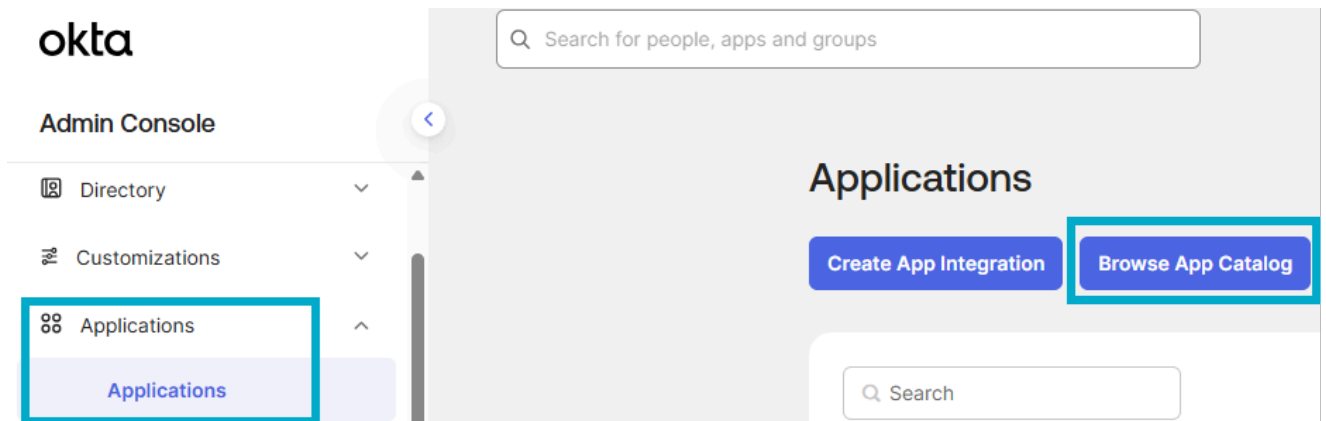
Enter your Okta organization URL

Organization URL

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

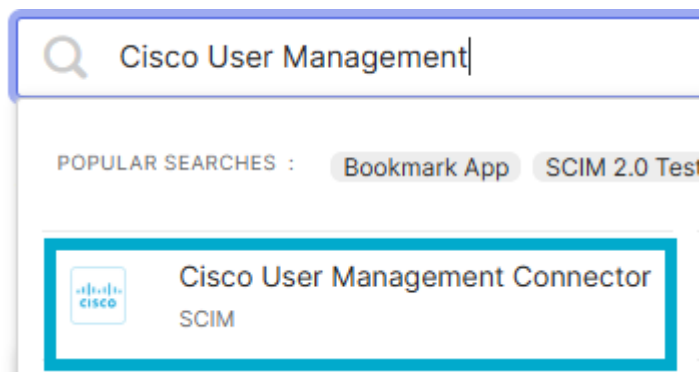
[Continue](#)

2. Vaya a Aplicaciones > Catálogo de aplicaciones del navegador.



Examinar catálogo de aplicaciones

3. Seleccione la aplicación Cisco User Management Connector.



Aplicación de Cisco

4. Haga clic en Agregar integración.

Last updated: December 2, 2024

+ Add Integration



Cisco User Management Connector

SCIM

Agregar integración

5. Haga clic en Done (Listo).

+ 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

Agregar aplicación

6. Haga clic en Provisioning > Configure API Integration.

Cisco User Management Connector

Active ▾ [User Icon] [User Icon] 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

Configurar integración de API

7. Haga clic en Enable API Integration e ingrese los Tokens Based URL y API guardados del paso #6 de la Configuración de Secure Access. Haga clic en Test API Credentials y luego en 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

Prueba de API

8. Vaya a Provisioning > To App. Active las opciones Create Users, Update User Attributes y Deactivate Users, y haga clic en 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

Aprovisionar a la aplicación



Nota: Compruebe que selecciona estos atributos para la sincronización con Secure Access. Secure Access sólo muestra los atributos Nombre mostrado y Nombre usuario para los usuarios, no los atributos Nombre dado y Nombre familiar: Nombre de usuario, Nombre, Familia, Nombre, Nombre para mostrar, Correo electrónico

(Opcional) Agregue un [atributo objectGUID](#) y cree la asignación de perfiles de usuario. Si necesita importar el atributo objectGUID para los usuarios, agregue un nuevo atributo y asigne los atributos en la asignación de perfiles.



9. Para agregar personas/grupos, haga clic en Asignaciones > Asignar > Asignar a personas/Asignar a grupos.

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 overlaid on the table. Below the table, the text 'No groups found' is displayed.

Asignación

10. Seleccione los grupos o personas que desea aprovisionar para Secure Access, haga clic en Asignar y, a continuación, en Finalizado.

Assign Cisco User Management Connector to Groups ×

		Assign
	OKTA - Secure Access Users	Assigned

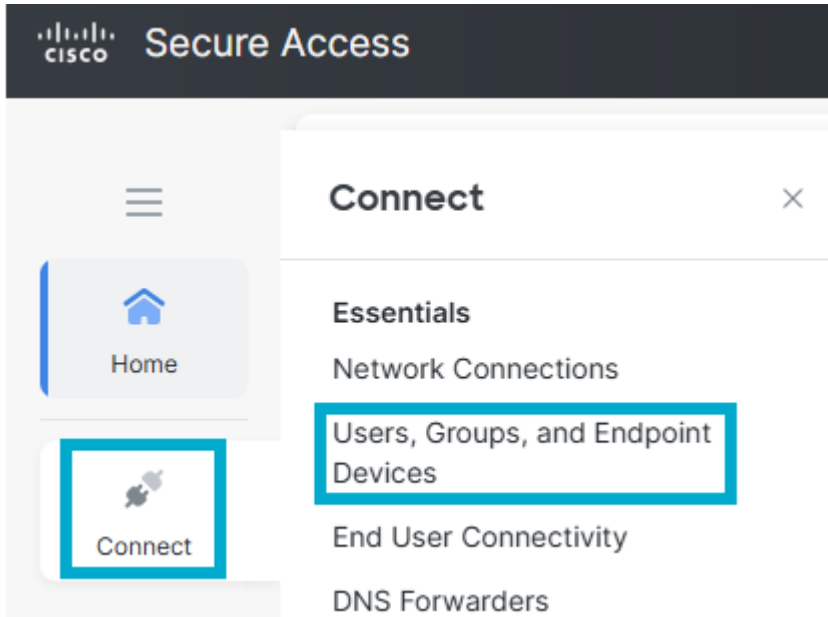
[Done](#)

Asignar grupos

Verificación

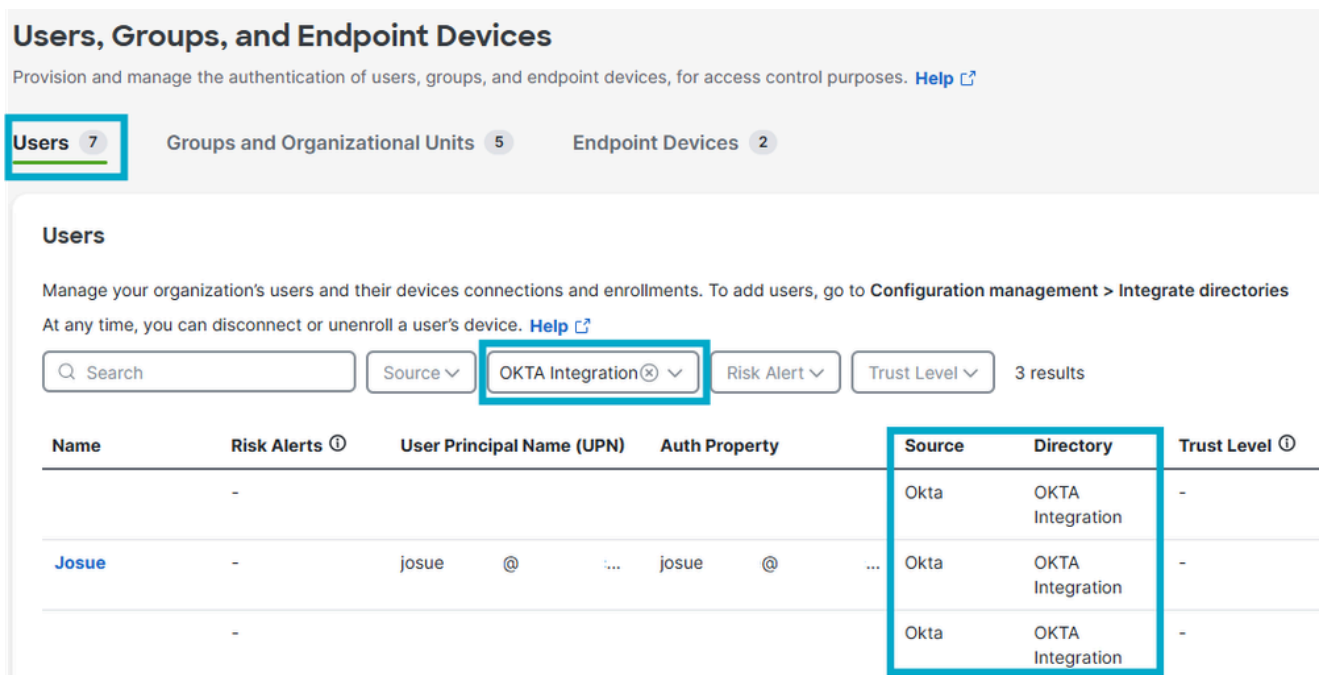
Veracidad en Cisco Secure Access

- Vaya a Connect > Users, Groups and Endpoint Devices.



Usuarios y grupos en CSA

- Haga clic en Usuarios.



Verificar usuarios en CSA

Verity en OKTA

- Vaya a Informes > Registro del sistema.

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

Registros de OKTA

Información Relacionada

[Configurar proveedores de identidad](#)

[Aprovisionamiento de usuarios y grupos desde Okta](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).