

Provisionar usuários e grupos para acesso seguro via OKTA

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurar o Cisco Secure Access](#)

[Configurar Provisionamento no OKTA](#)

[Verificar](#)

[Verity no Cisco Secure Access](#)

[Verity em OKTA](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como provisionar grupos de usuários do OKTA para o Cisco Secure Access.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso seguro da Cisco
- OKTA

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

- Painel do Cisco Secure Access

- OKTA

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Cisco Secure Access suporta o provisionamento de usuários e grupos do OKTA.

Esse provisionamento permite que o Secure Access mantenha um diretório de usuários autorizados a:

- Inscreva-se no Zero Trust Access (ZTA).
- Conecte-se ao VPNaaS.
- Aplique políticas baseadas em identidade aos usuários do Umbrella Roaming.



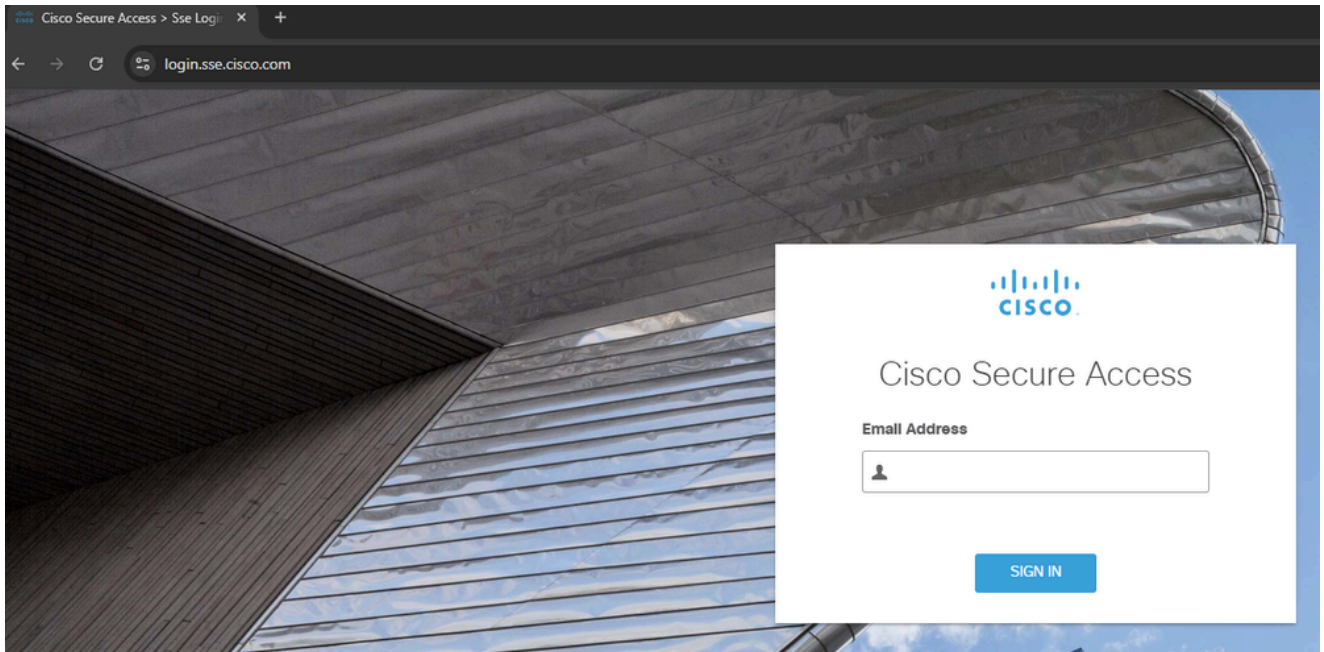
Note: Este documento se concentra especificamente no provisionamento de usuários e grupos do OKTA. A configuração de Entra ID ou outros Provedores de Identidade (IdP) para registro ZTA, autenticação VPNaaS ou configurações específicas de Umbrella Roaming está fora do escopo deste guia.

Configurar

Configurar o Cisco Secure Access

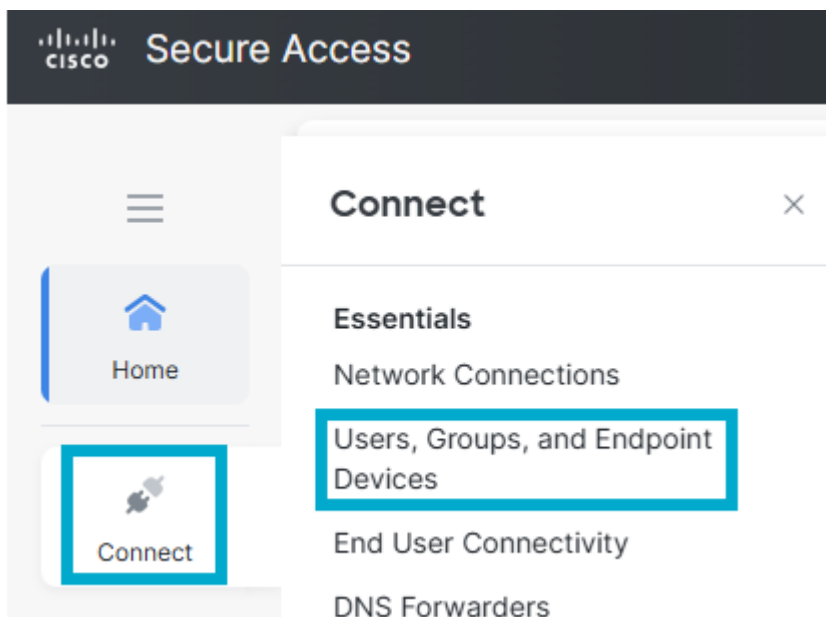
Para iniciar o processo de provisionamento, você deve primeiro configurar a integração de diretórios no painel do Cisco Secure Access. Esta etapa gera as credenciais necessárias e os parâmetros de configuração necessários para estabelecer uma conexão segura com o OKTA.

1. Inicie sessão no Cisco Secure Access [Dashboard](#).



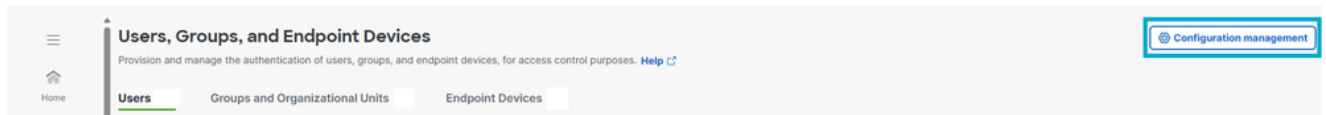
Entrar no CSA

2. Navegue até Connect > Users, Groups and Endpoint Devices.



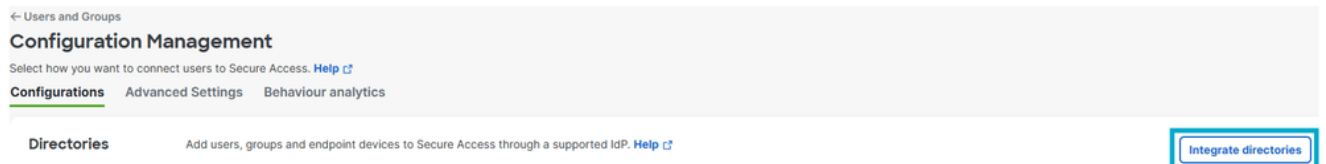
Usuários e grupos

3. Clique em Gerenciamento de configuração.



Gerenciamento de configuração

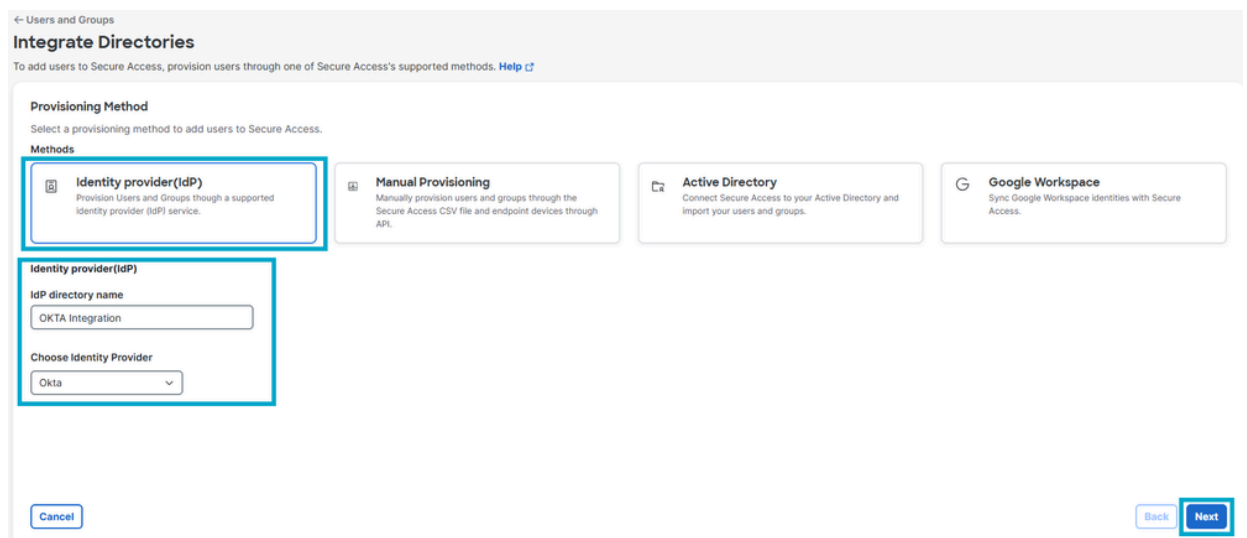
4. Clique em Integrar diretório.



Diretório de integração

5. Em Método de provisionamento, clique em Provedor de identidade.

- Nome do diretório IdP: Integração OKTA.
- Escolher Provedor de Identidade: OKTA.
- Clique em Next.



Directory Configuration

6. Clique em Gerar token. Salve o token gerado e o URL de provisionamento e clique em Concluído.

← 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](#)

Gerar token

Configurar Provisionamento no OKTA

Depois de ter gerado suas credenciais no painel do Cisco Secure Access, você deve definir as configurações de provisionamento em seu locatário OKTA para habilitar a sincronização de usuários e grupos.

1. Entre no [OKTA](#).

okta

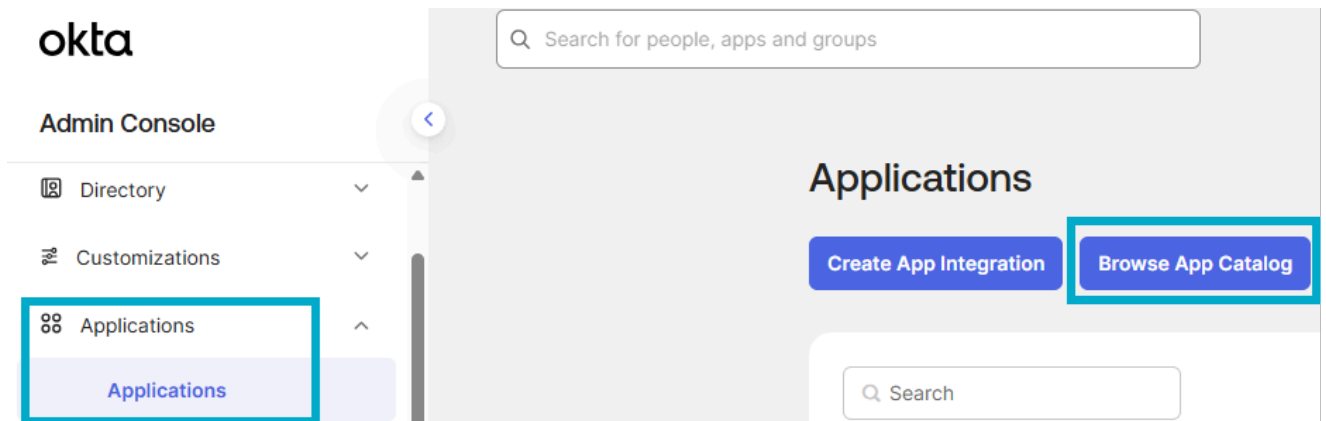
Enter your Okta organization URL

Organization URL

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

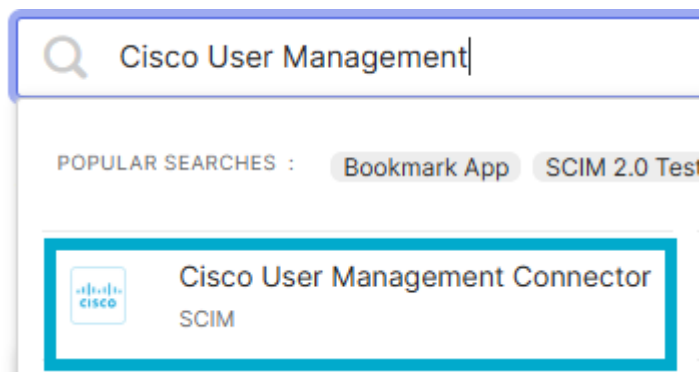
[Continue](#)

2. Navegue até Aplicativos > Catálogo de aplicativos do navegador.



Procurar Catálogo de Aplicativos

3. Selecione o aplicativo Cisco User Management Connector.



Aplicativo da Cisco

4. Clique em Add Integration.

Last updated: December 2, 2024

+ Add Integration



Cisco User Management Connector

SCIM

Adicionar integração

5. Clique em Concluído.

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

Adicionar aplicativo

6. Clique em Provisionamento > Configurar integração de 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

Provisioning is not enabled

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

[Configure API Integration](#)

Configurar Integração de API

7. Clique em Enable API Integration e insira os tokens Based URL e API salvos da etapa #6 da Secure Access Configuration. Clique em Testar credenciais da API e em Salvar.

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

Teste de API

8. Navegue até Provisionamento > Para aplicativo. Ative as opções Criar usuários, Atualizar atributos do usuário e Desativar usuários e clique em Salvar.

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

Provisionar para Aplicativo



Note: Verifique se você selecionou esses atributos para sincronização com o Secure Access. O Secure Access lista apenas os atributos Nome de exibição e Nome de usuário para usuários, não os atributos Nome fornecido e Nome da família: Nome de usuário, Nome fornecido, Família, Nome, Nome de exibição, Email

(Opcional) Adicione um [Atributo objectGUID](#) e crie o Mapeamento de Perfil de Usuário. Se precisar importar o atributo objectGUID para usuários, adicione um novo atributo e mapeie os atributos no mapeamento de perfil.

9. Para adicionar pessoas/grupos, clique em Atribuições > Atribuir > Atribuir a pessoas/Atribuir 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 set to "Active", and navigation 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-navigation bar with buttons for "Assign" (highlighted with a red box), "Convert assignments", a search field, and a "Groups" dropdown. The "Assign" dropdown menu is open, showing two options: "Assign to People" and "Assign to Groups", both of which are also highlighted with a red box.

Below the navigation bar, there is a table with the following content:



Assignment	
01101110	
01101111	
01101100	
01101100	
01101101	
01101110	
01100111	

Below the table, the text "No groups found" is displayed. A magnifying glass icon is overlaid on the table content.

Atribuição

10. Selecione os grupos/pessoas que você deseja provisionar para o Secure Access e clique em Atribuir e em Concluído.

Assign Cisco User Management Connector to Groups ×

		Assign
	OKTA - Secure Access Users	Assigned

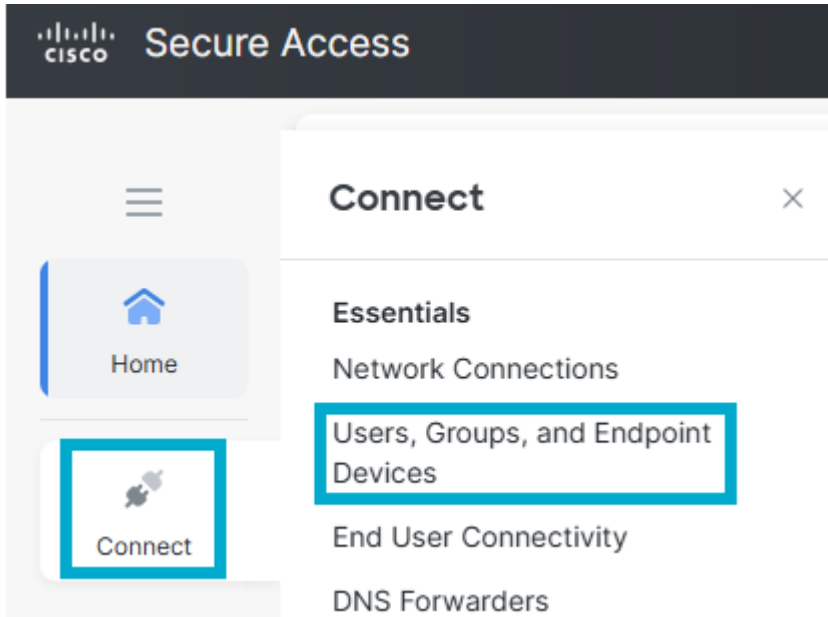
[Done](#)

Atribuir grupos

Verificar

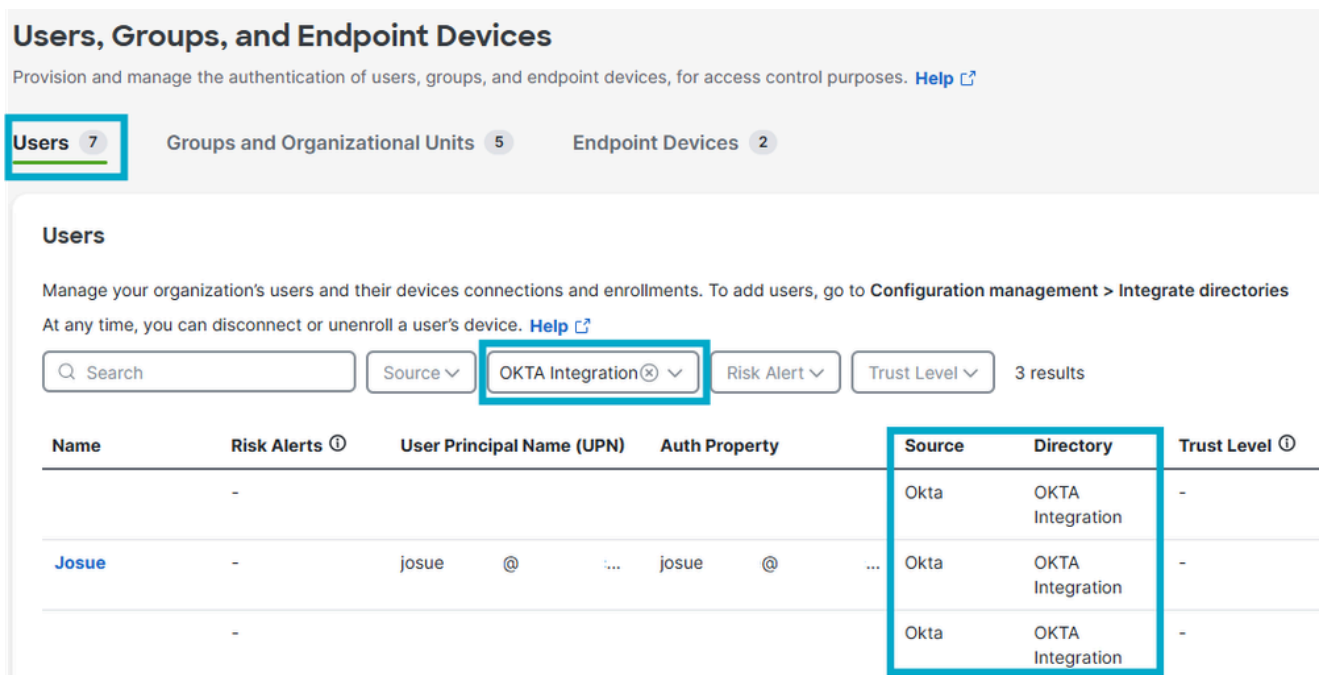
Verity no Cisco Secure Access

- Navegue para Connect > Users, Groups and Endpoint Devices.



Usuários e grupos no CSA

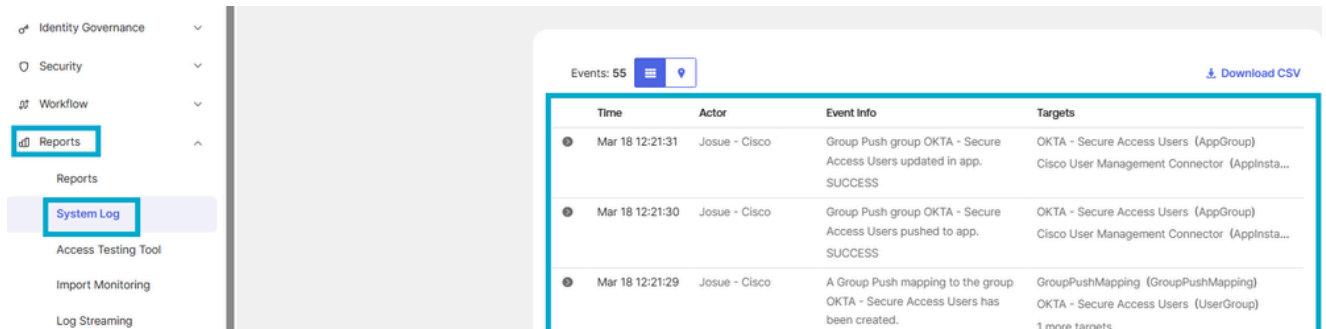
- Clique em Users.



Verificar usuários no CSA

Verity em OKTA

- Navegue até Relatórios > Log do sistema.



The screenshot displays the Okta Admin console interface. On the left sidebar, the 'Reports' menu is expanded, and 'System Log' is selected. The main content area shows 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'.

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

Logs OKTA

Informações Relacionadas

[Configurar Provedores de Identidade](#)

[Provisionar usuários e grupos do Okta](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.