

# OKTA経由でアクセスを保護するためのユーザとグループのプロビジョニング

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[バックグラウンド情報](#)

[設定](#)

[Cisco Secure Accessの設定](#)

[OKTAでのProvisioningの設定](#)

[確認](#)

[Cisco Secure AccessのVerity](#)

[OKTAのVerity](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、OKTAからCisco Secure Accessにユーザグループをプロビジョニングする方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- シスコセキュアアクセス
- オクタ

### 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

- Cisco Secure Accessダッシュボード
- オクタ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## バックグラウンド情報

Cisco Secure Accessは、OKTAからのユーザおよびグループのプロビジョニングをサポートします。

このプロビジョニングにより、セキュアなアクセスが可能になり、次の権限を持つユーザのディレクトリを維持できます。

- ゼロトラストアクセス(ZTA)に登録します。
- VPNaaSに接続します。
- Umbrella Roamingユーザにアイデンティティベースのポリシーを適用します。



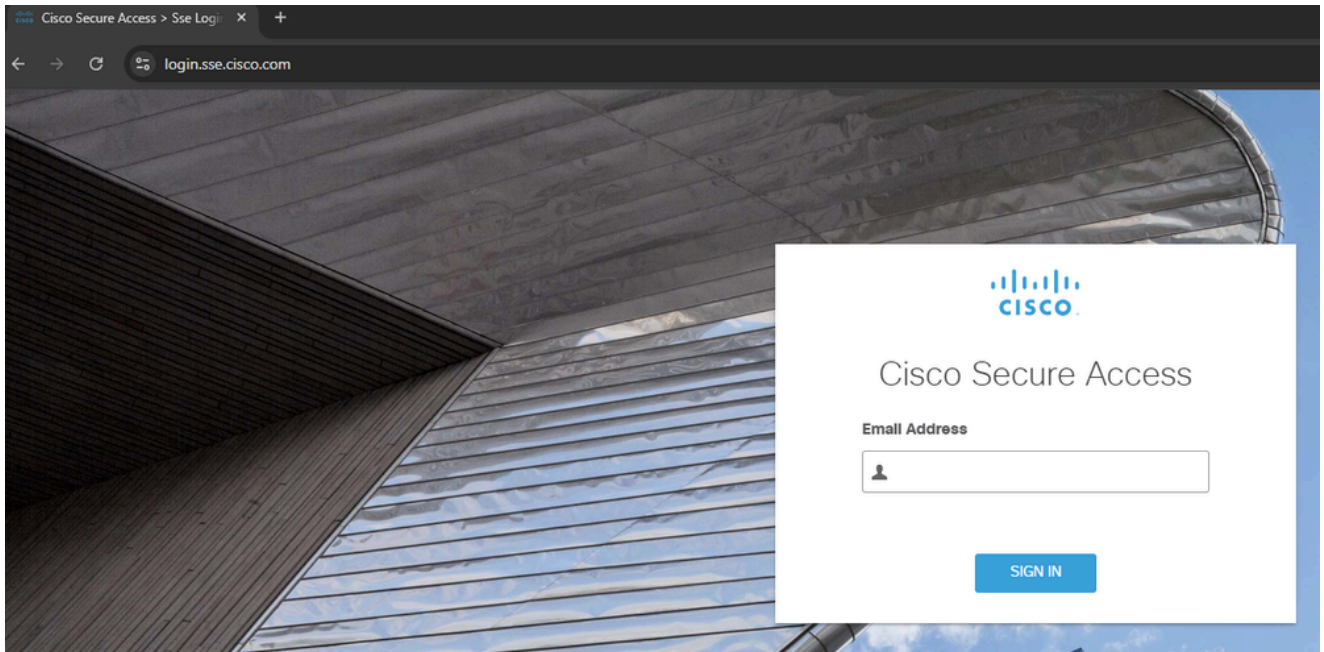
注：このドキュメントでは、特にOKTAからのユーザおよびグループのプロビジョニングに重点を置いています。ZTA登録、VPNaaS認証、または特定のUmbrellaローミング設定に関するEntra ID(IID)またはその他のアイデンティティプロバイダー(IdP)の設定については、このガイドでは説明しません。

## 設定

### Cisco Secure Accessの設定

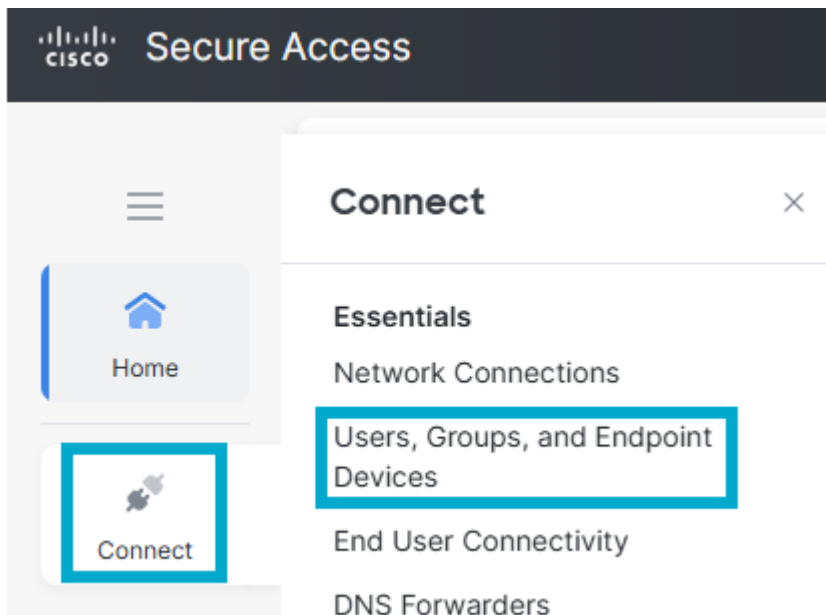
プロビジョニングプロセスを開始するには、まずCisco Secure Accessダッシュボード内でディレクトリ統合を設定する必要があります。この手順では、OKTAとのセキュリティで保護された接続を確立するために必要な資格情報と構成パラメータを生成します。

1. Cisco Secure Access [Dashboard](#)にサインインします。



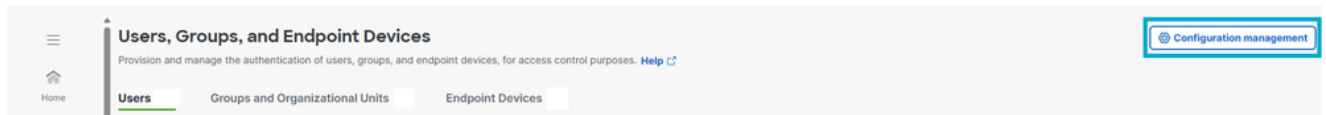
CSAへのサインイン

2. Connect > Users, Groups and Endpoint Devicesの順に移動します。



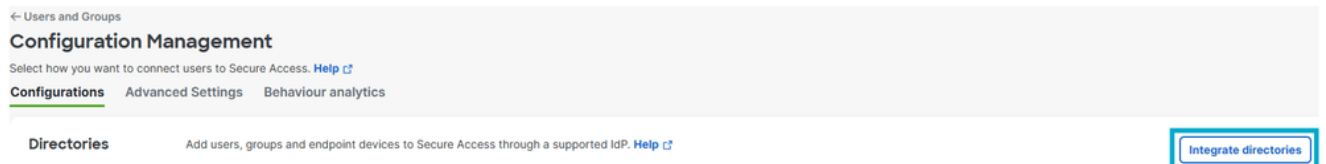
ユーザとグループ

3. Configuration managementをクリックします。



構成管理

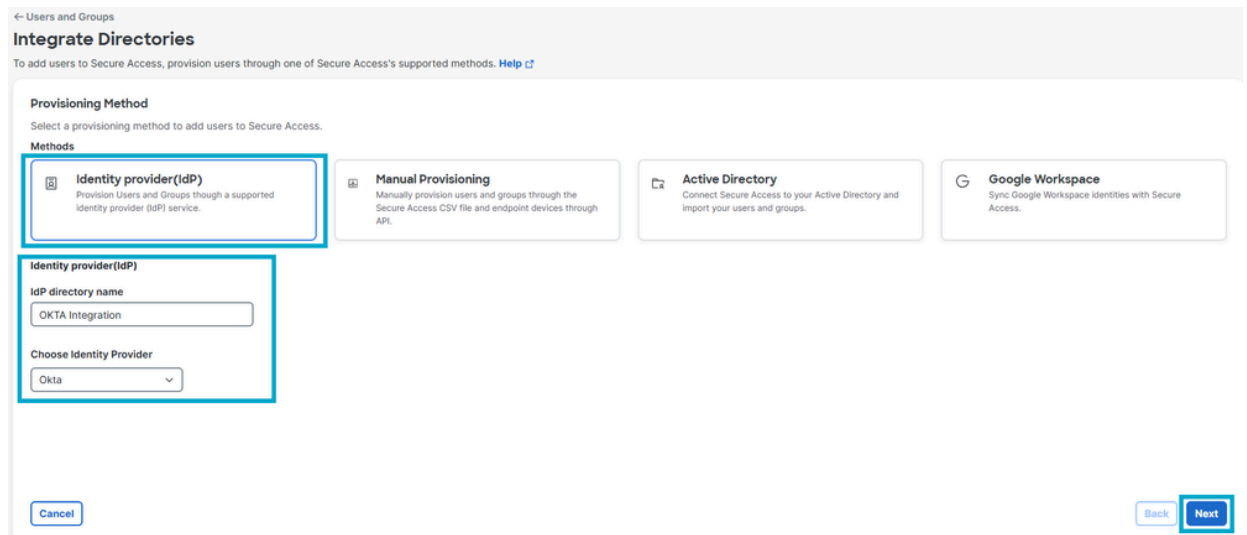
#### 4. Integrate Directoryをクリックします。



ディレクトリの統合

#### 5. Provision MethodでIdentity Providerをクリックします。

- IdPディレクトリ名 : OKTA統合。
- Identity Provider: OKTAを選択します。
- [Next] をクリックします。



ディレクトリ設定

#### 6. Generate Tokenをクリックします。生成されたトークンとプロビジョニングURLを保存し、Doneをクリックします。

← 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"/> <input type="button" value="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"/> <input type="button" value="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](#)

トークンの生成

## OKTAでのProvisioningの設定

Cisco Secure Accessダッシュボードでクレデンシャルを生成したら、OKTAテナント内でプロビジョニング設定を構成して、ユーザとグループの同期を有効にする必要があります。

1. [OKTA](#)にサインインします。

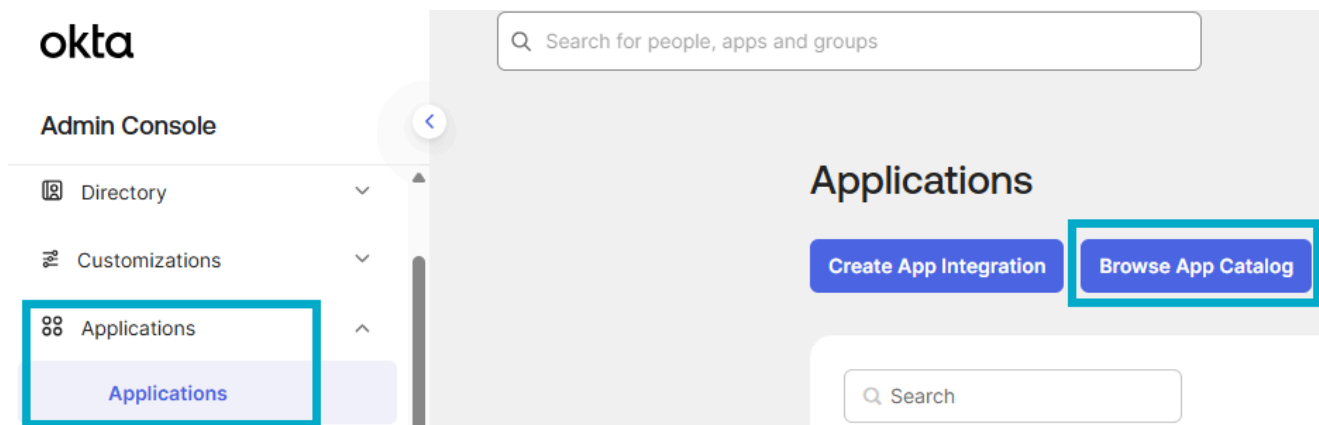
# okta

## Enter your Okta organization URL

Organization URL

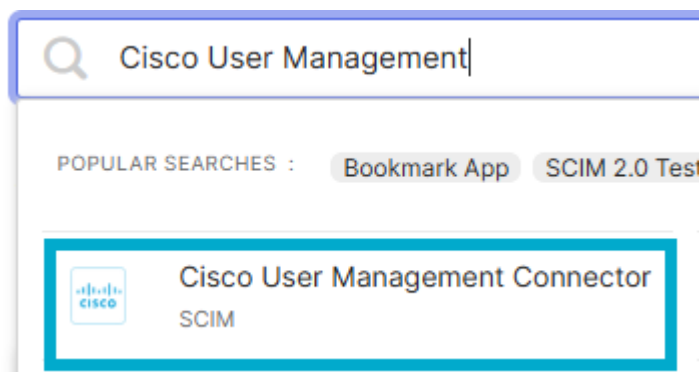
<input type="text" value="Company name"/>	<input type="text" value=".okta.com"/> ▼
---	--

2. Applications > Browser App Catalogの順に移動します。



アプリカタログの参照

3. Cisco User Management Connectorアプリケーションを選択します。



シスコアプリケーション

4. Add Integrationをクリックします。

Last updated: December 2, 2024

+ Add Integration



## Cisco User Management Connector

SCIM

統合の追加

5. [Done] をクリックします。

## 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

アプリの追加

6. Provisioning > Configure API Integrationの順にクリックします。

**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](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](#)

API統合の設定

7. Enable API Integrationをクリックし、セキュアアクセス設定のステップ#6でBased URL と API Tokensavedを入力します。Test API Credentialsをクリックし、次にSaveをクリックします。

Settings

Integration

**Info** 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

**Success** 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テスト

8. Provisioning > To Appの順に移動します。Create Users、Update User Attributes、および Deactivate Usersのオプションを有効にし、Saveをクリックします。

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

アプリへのプロビジョニング



注：セキュアアクセスへの同期に次の属性を選択していることを確認してください。セキュアアクセスでは、ユーザの表示名とユーザ名の属性のみがリストされ、ユーザ名、名、ファミリー、名前、表示名、電子メールの特定の名前とファミリー名の属性はリストされません

( オプション ) [objectGUID属性](#)を追加し、ユーザプロファイルマッピングを作成します。ユーザのobjectGUID属性をインポートする必要がある場合は、新しい属性を追加し、プロファイルマッピングに属性をマッピングします。

9. 個人/グループを追加するには、Assignments > Assign > Assign to People/Assign to Groupsの順にクリックします。

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.

割り当て

10. セキュアアクセスにプロビジョニングするグループ/ユーザを選択し、Assign、Doneの順にクリックします。

# Assign Cisco User Management Connector to Groups

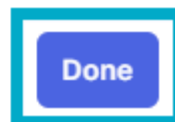


Assign



OKTA - Secure Access Users

Assigned

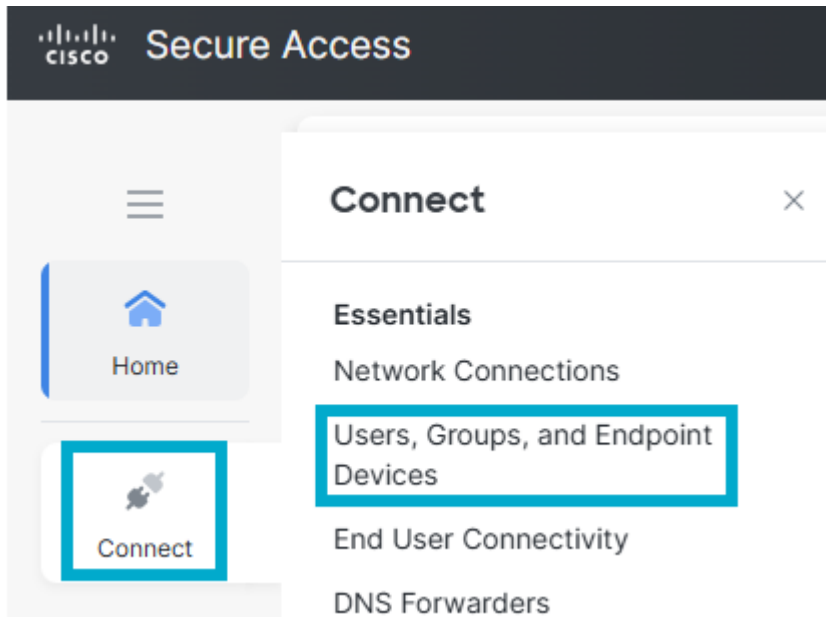


グループの割り当て

確認

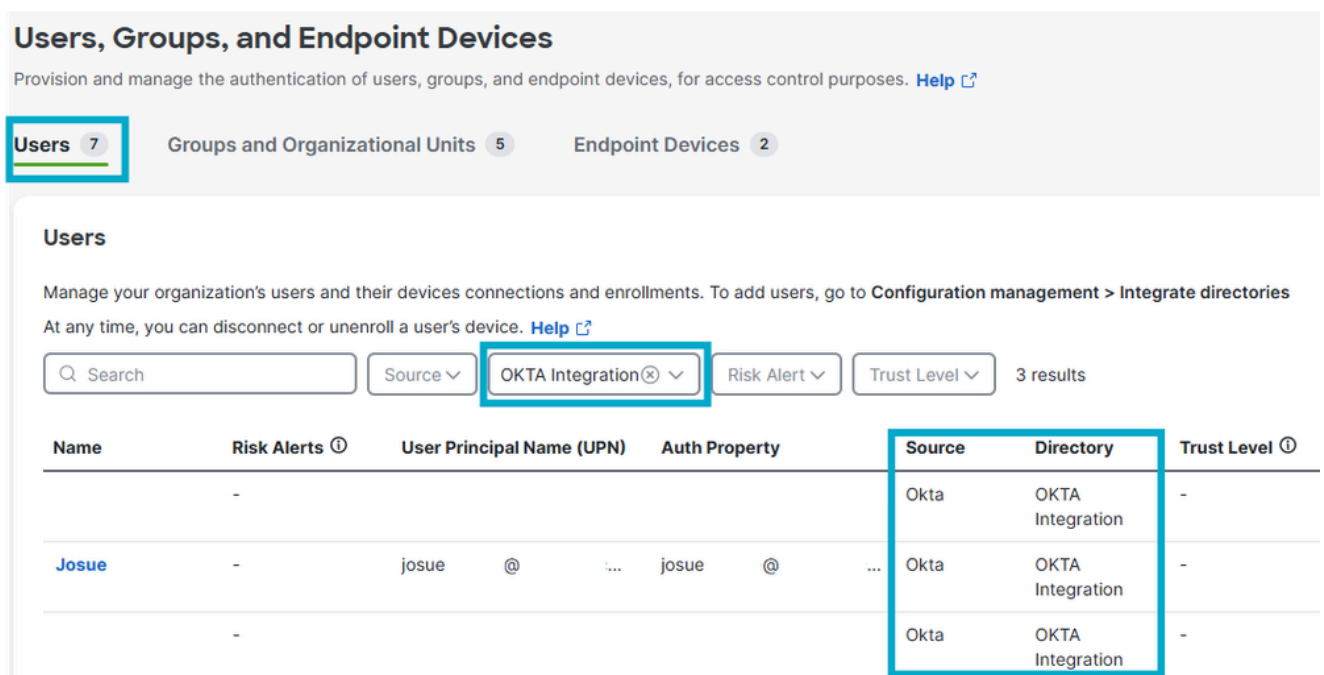
Cisco Secure AccessのVerity

- Connect > Users, Groups and Endpoint Devicesの順に移動します。



CSAのユーザとグループ

- [Users] をクリックします。



CSAでのユーザの確認

# OKTAのVerity

- Reports > System Logの順に選択します。

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ログ

## 関連情報

[アイデンティティプロバイダーの設定](#)

[Oktaからのユーザとグループのプロビジョニング](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。