Provision Users and Groups to Secure Access via OKTA

Contents

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.

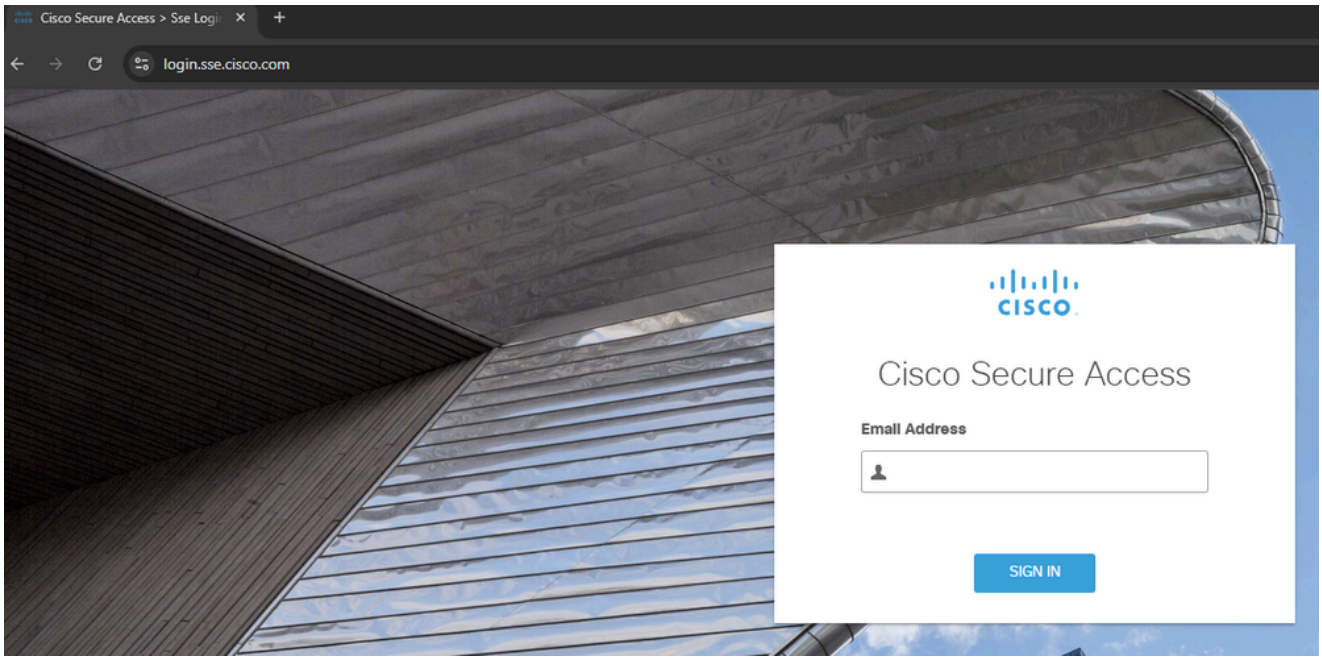
Note: This document focuses specifically on the provisioning of users and groups from OKTA. The configuration of Entra ID or other Identity Providers (IdP) for ZTA enrollment, VPNaaS authentication, or specific Umbrella Roaming settings is outside the scope of this guide.

Configure

Configure Cisco Secure Access

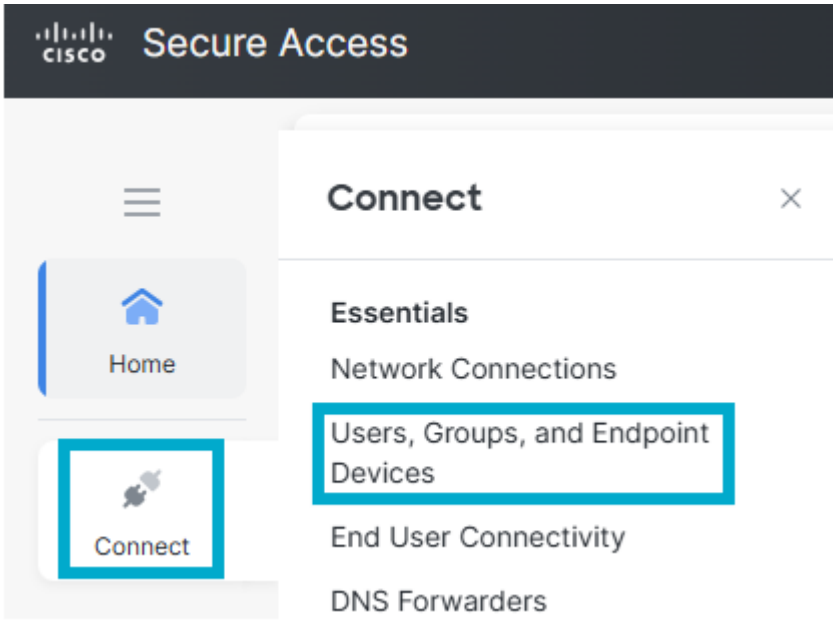
In order to begin the provisioning process, you must first configure the directory integration within the Cisco Secure Access dashboard. This step generates the necessary credentials and configuration parameters required to establish a secure connection with OKTA.

1. Sign in to the **Cisco Secure Access** Dashboard.



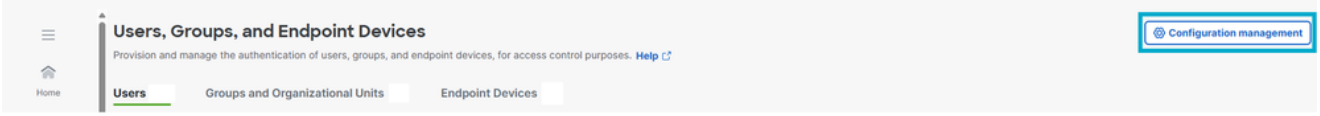
Sign in to CSA

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



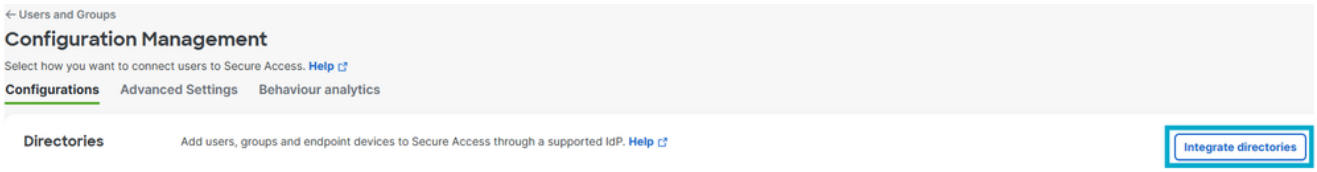
Users and Groups

3. Click **Configuration management**.



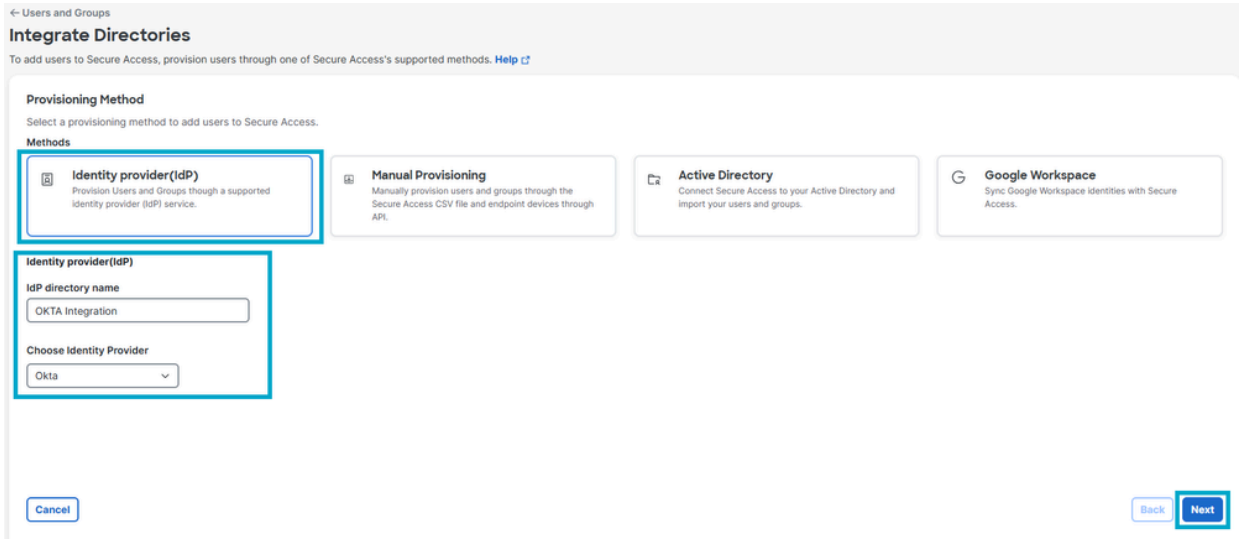
Configuration Management

4. Click **Integrate Directory**.



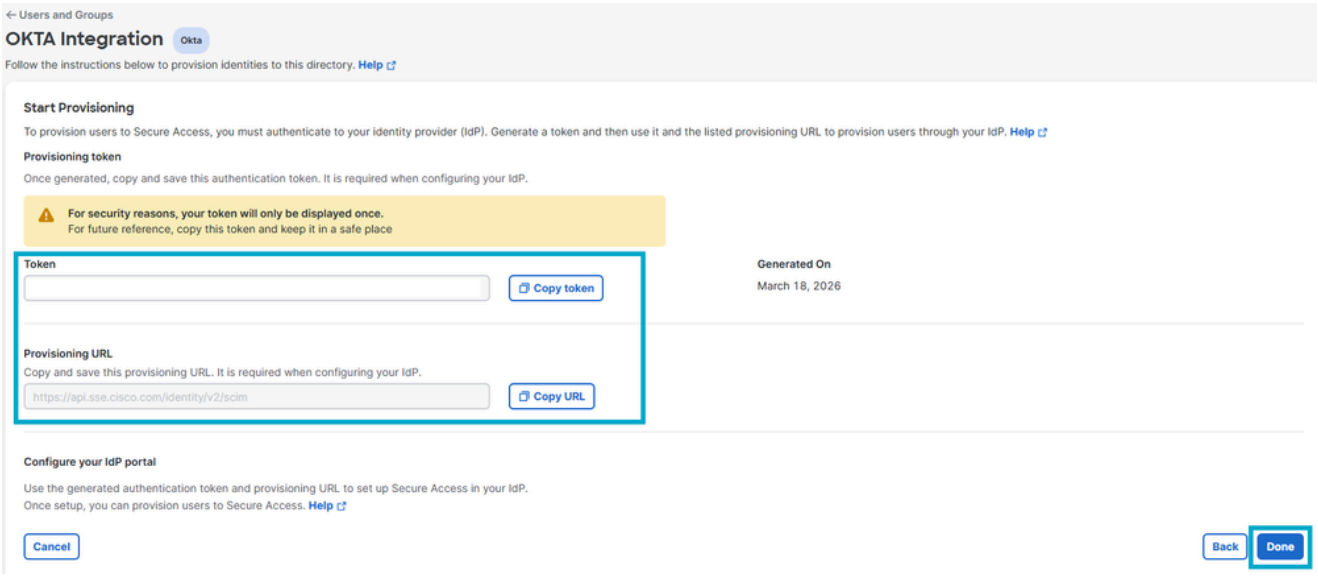
Integrate Directory

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.**

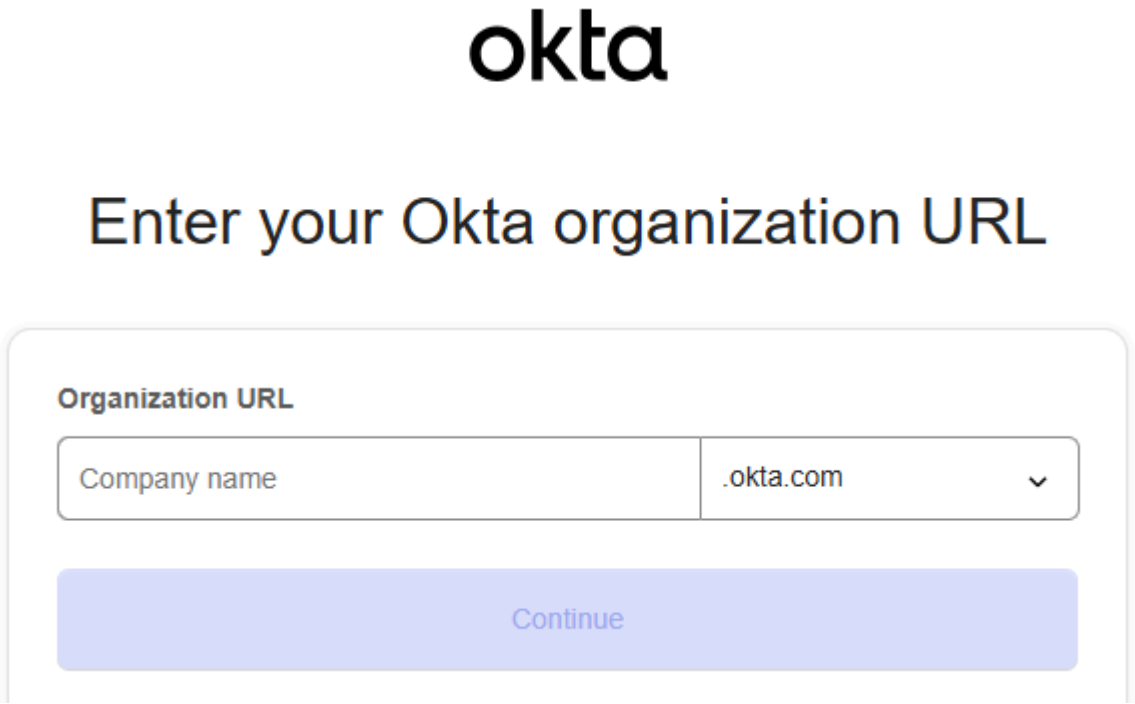


Generate Token

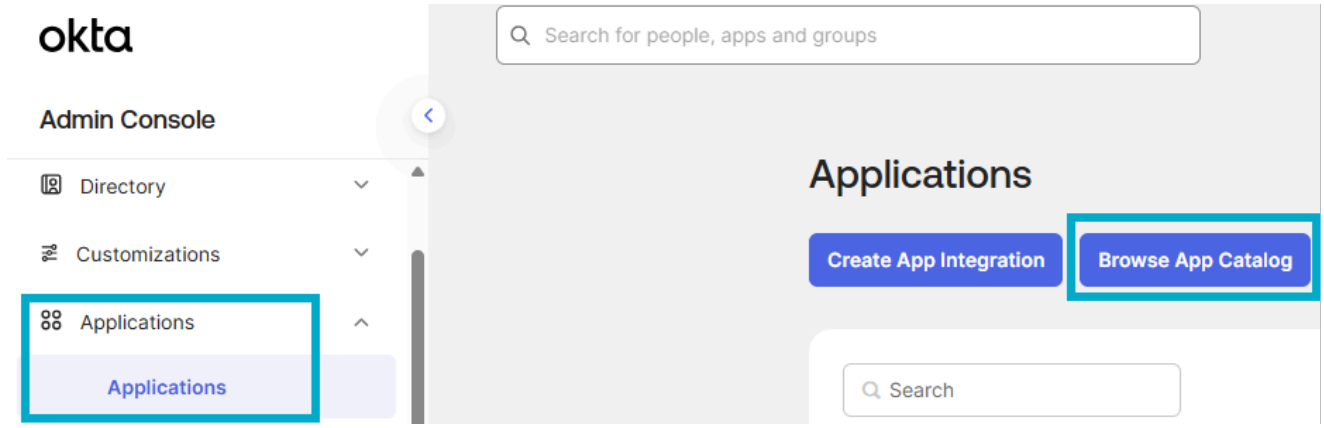
Configure Provisioning in OKTA

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.

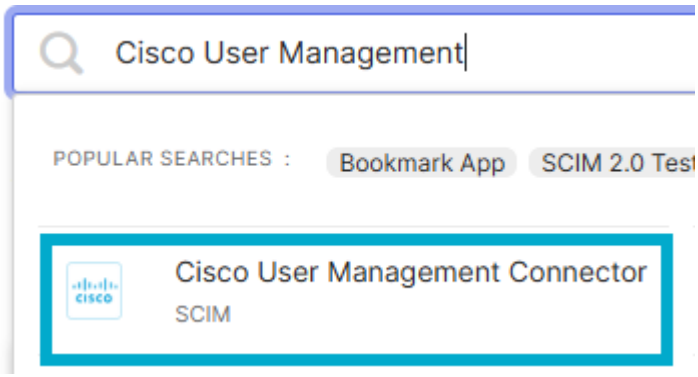


2. Navigate to **Applications > Browser App Catalog**.



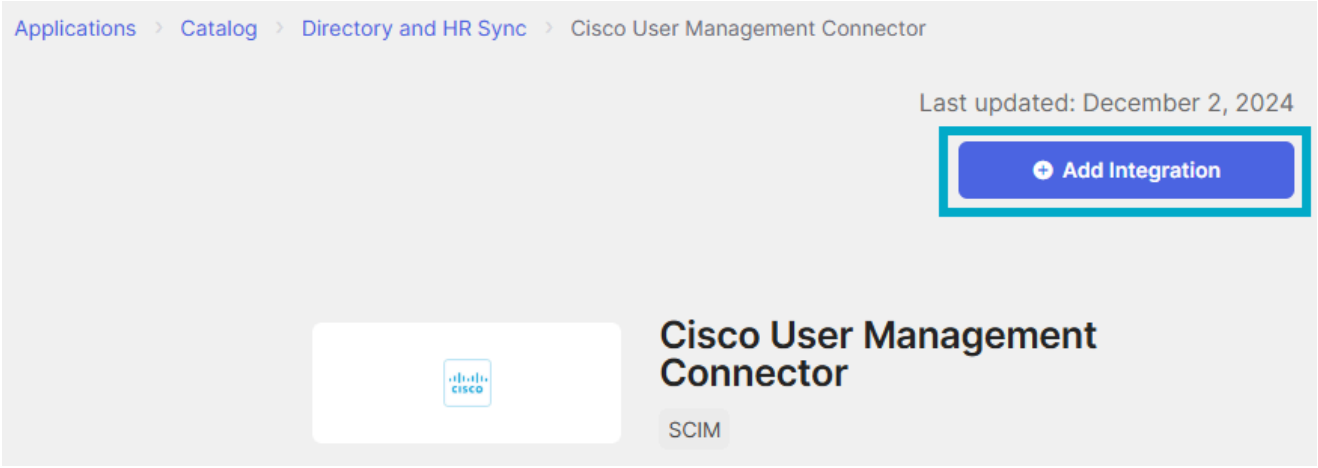
Browse App Catalog

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



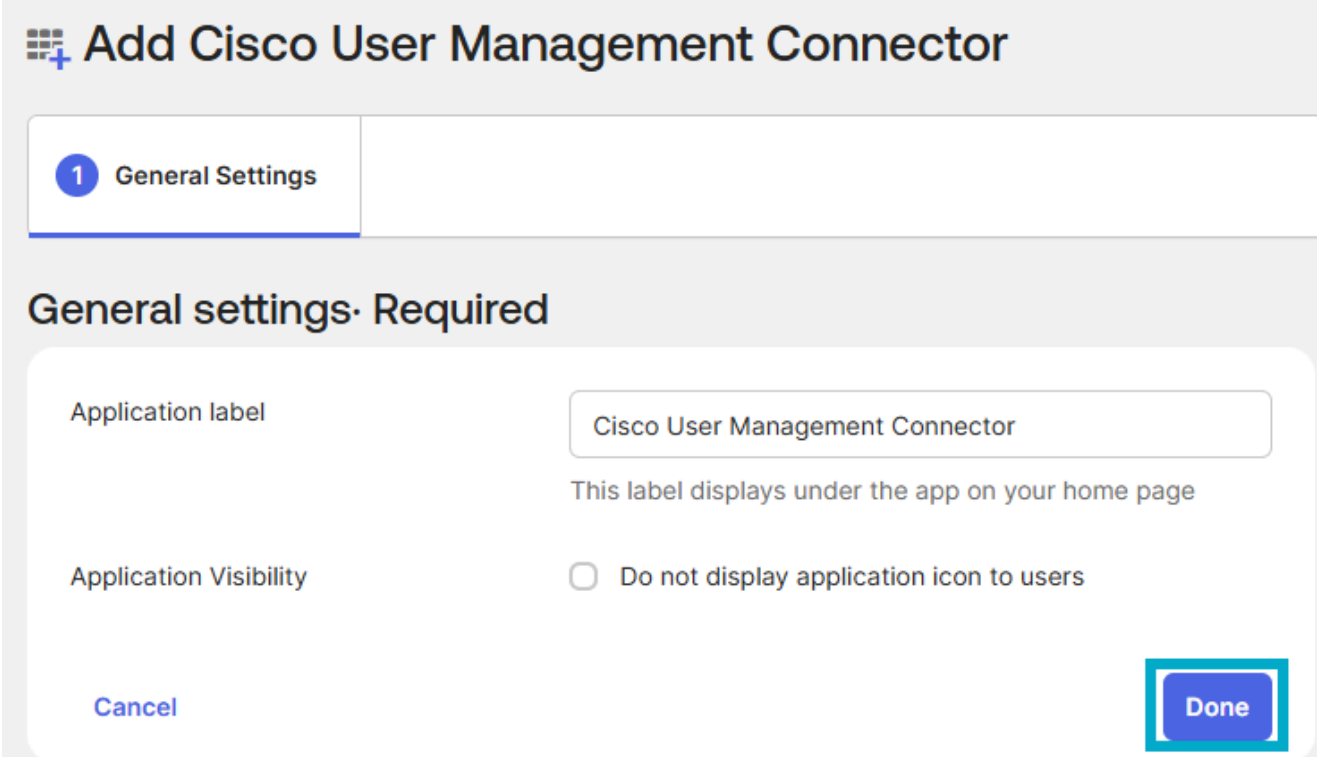
Cisco App

4. Click **Add Integration**.



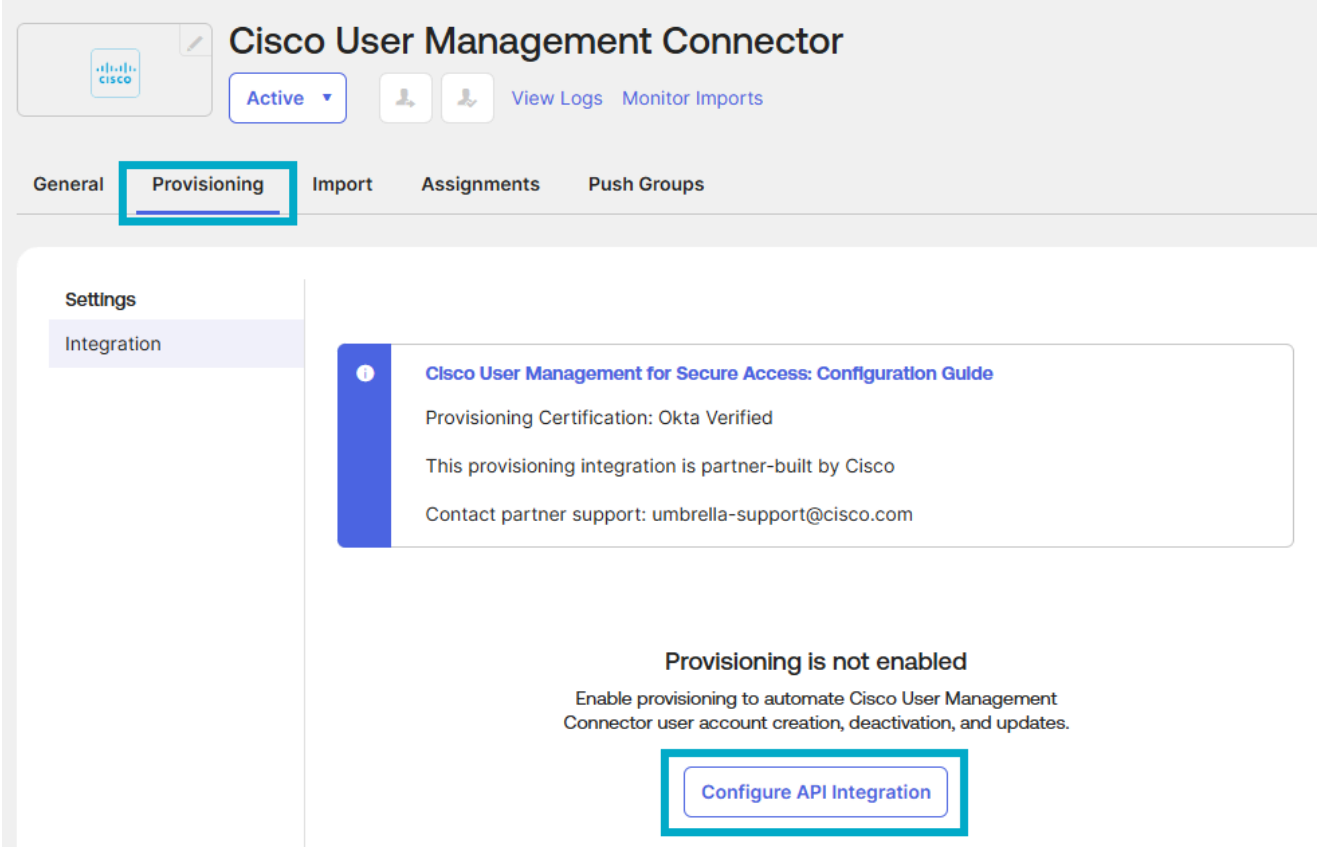
Add Integration

5. Click **Done**.



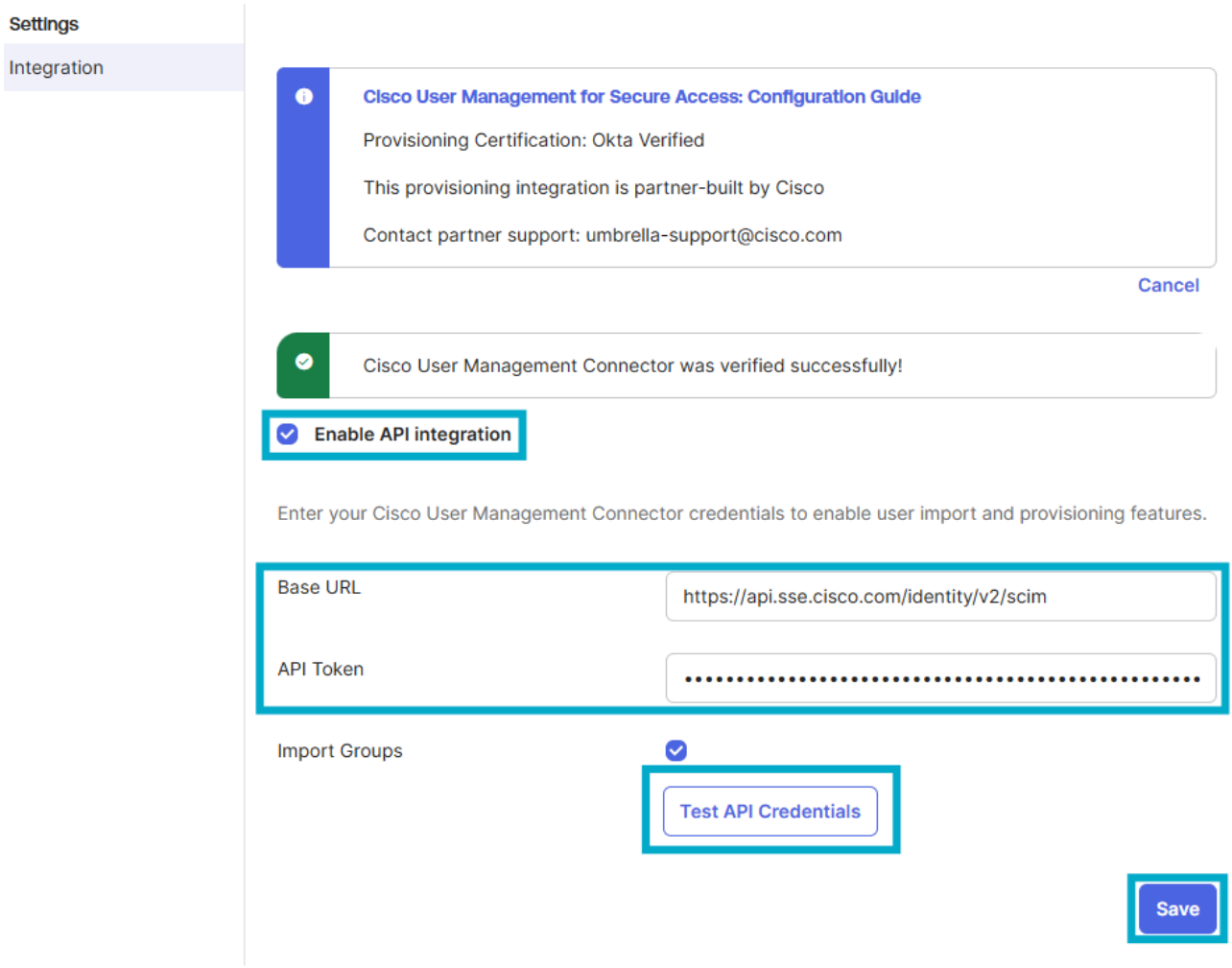
Add App

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



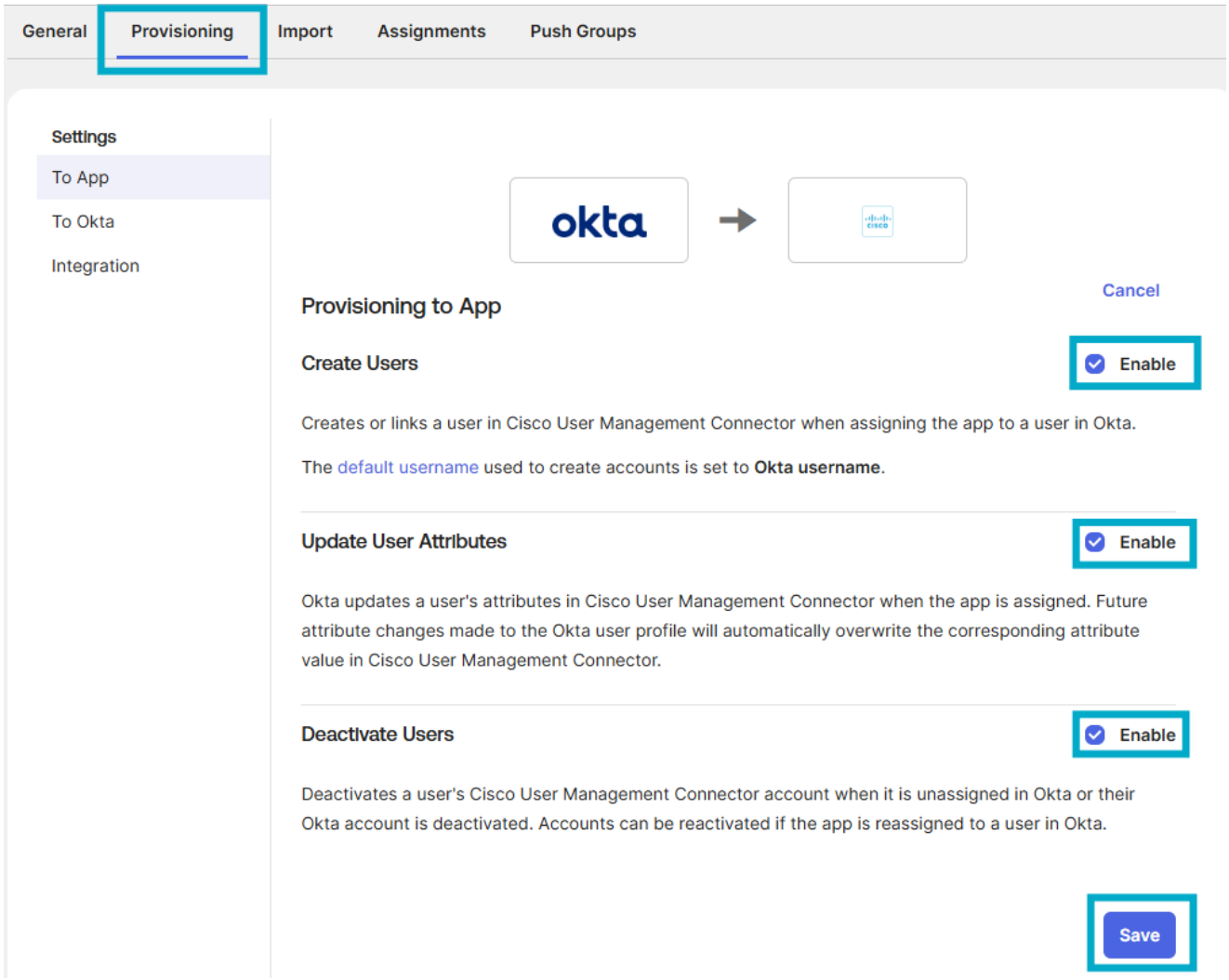
Configure API Integration

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



API Test

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



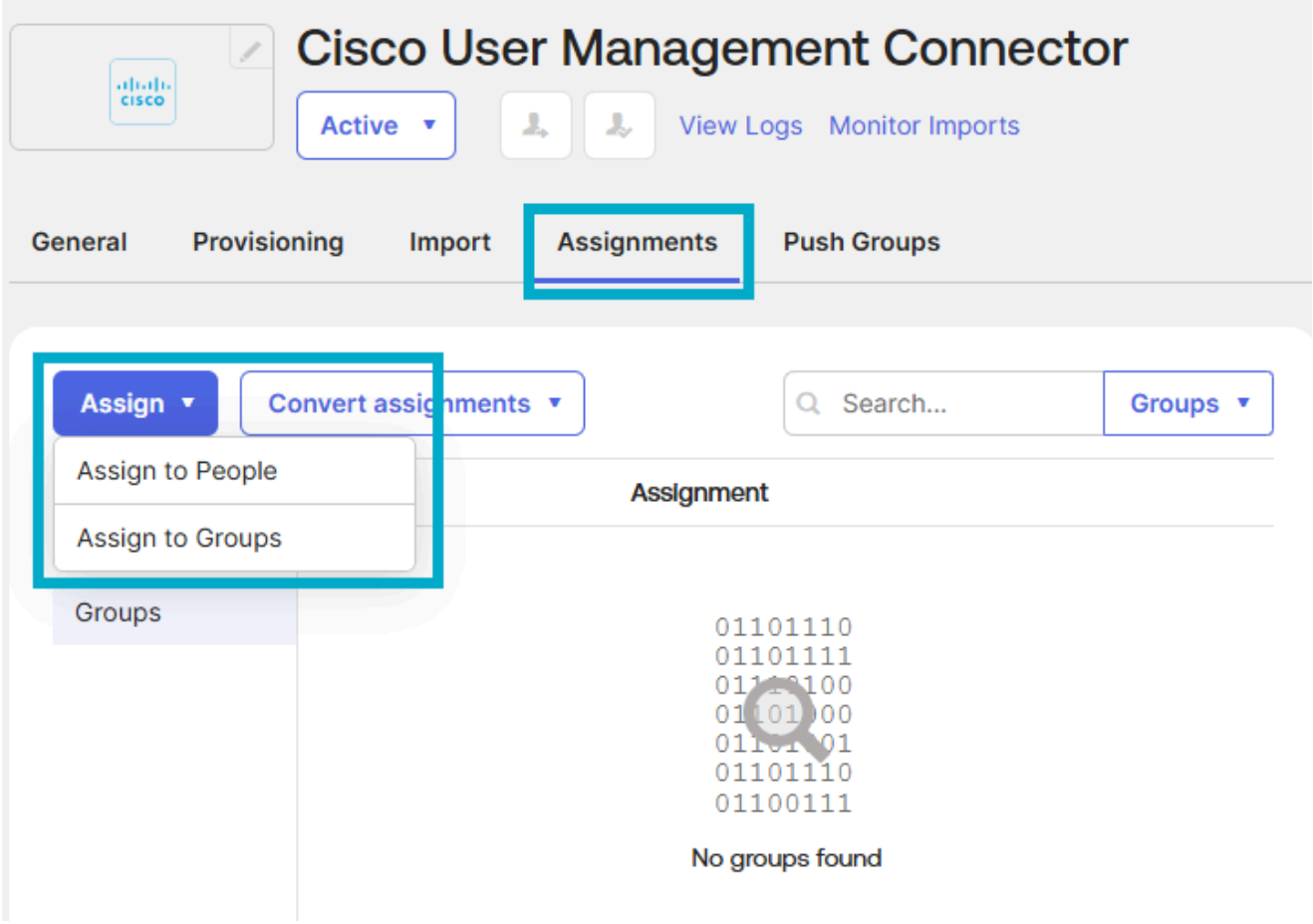
Provision to App

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.

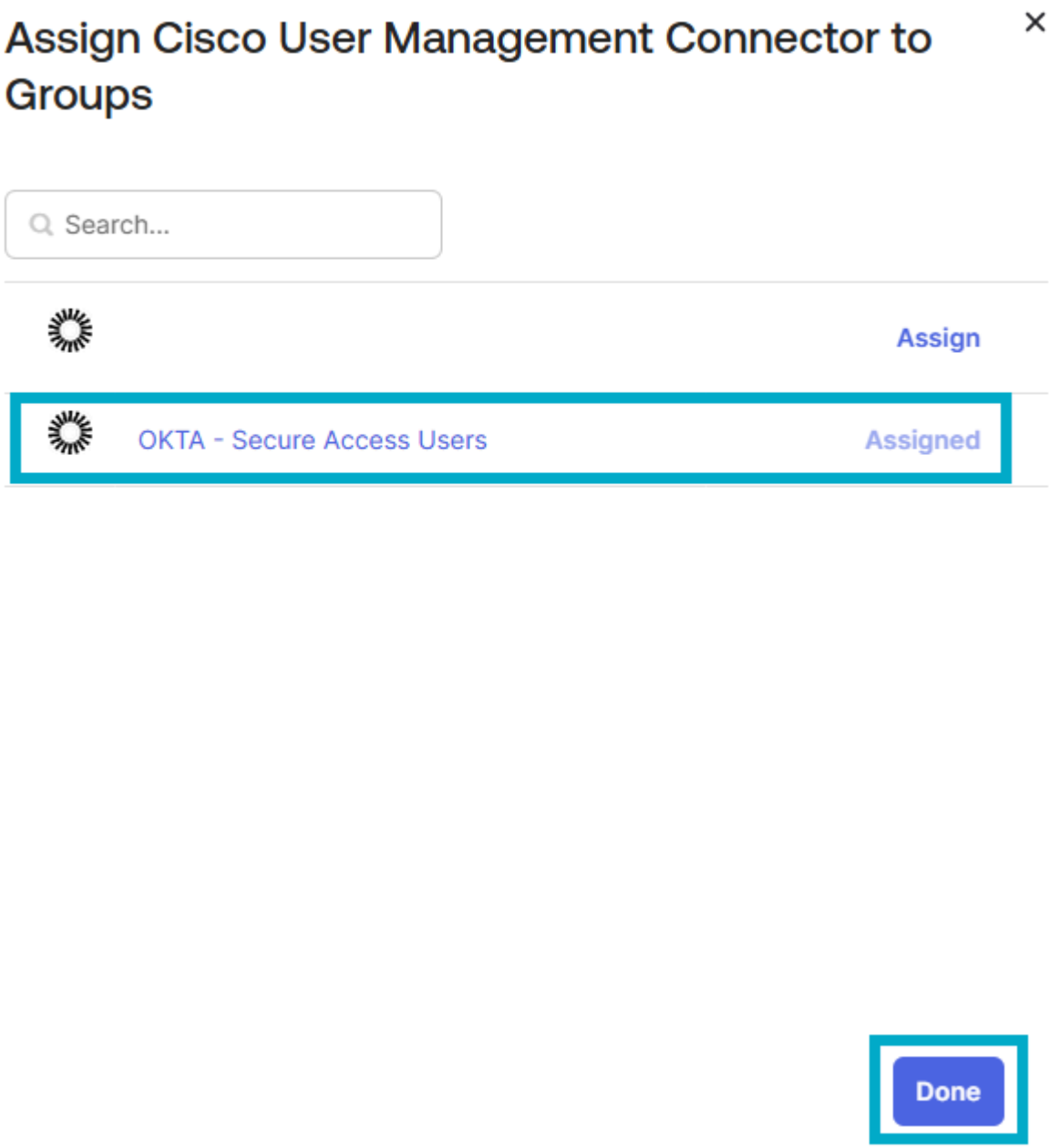
---

9. In order to add people/groups, click **Assignments > Assign > Assign to People/Assign to Groups**.



Assignment

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

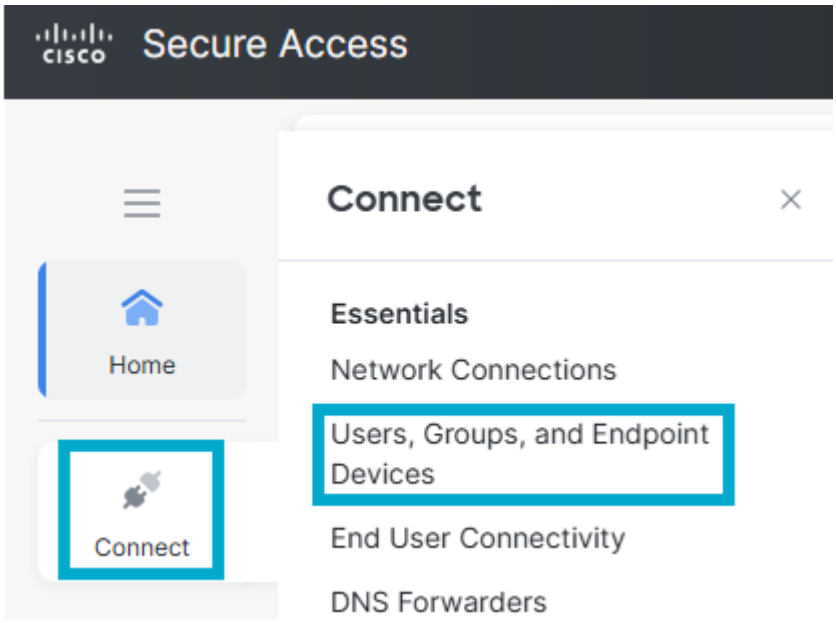


Assign Groups

Verify

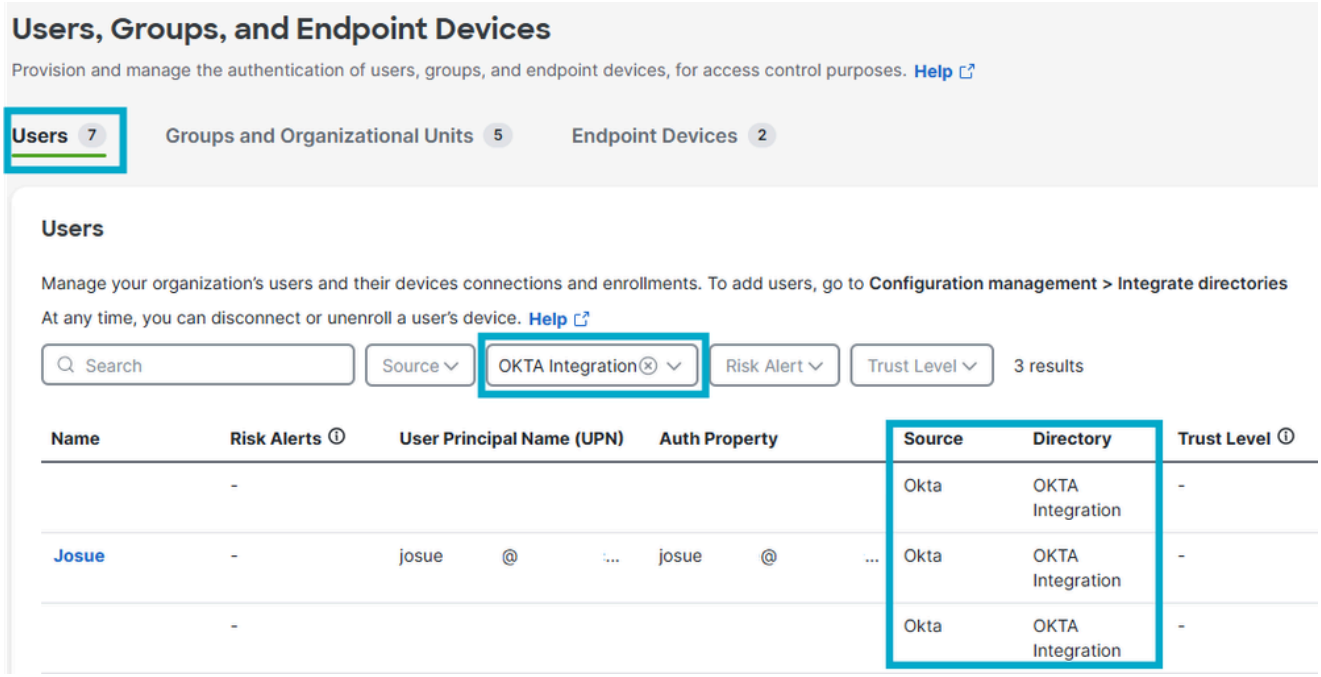
Verity in Cisco Secure Access

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



Users and Groups in CSA

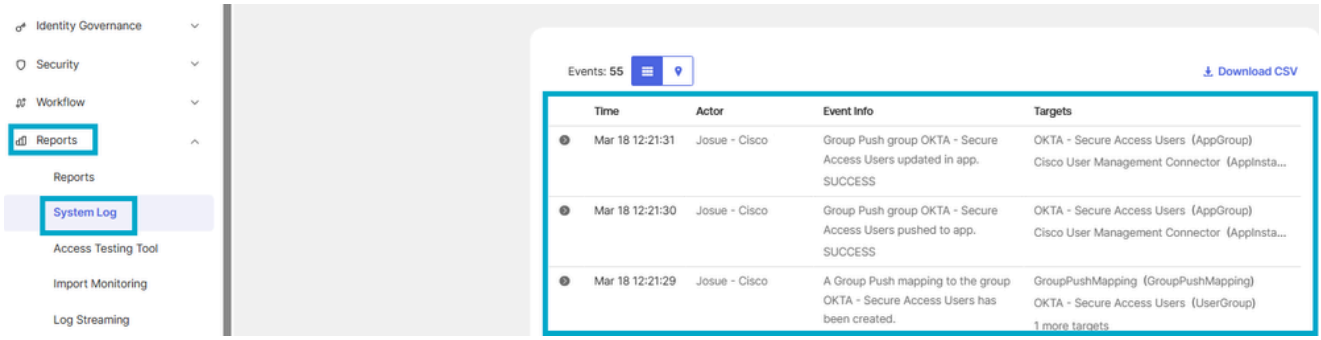
- Click **Users**.



Verify Users in CSA

Verity in OKTA

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



OKTA Logs

Related Information

[Configure Identity Providers]

[Provision Users and Groups from Okta]