

Provision Users and Groups to Secure Access via DUO

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Configure Cisco Secure Access](#)

[Configure Provisioning in Cisco DUO](#)

[Verify](#)

[Verify in Cisco Secure Access](#)

[Verify in DUO](#)

[Related Information](#)

Introduction

This document describes how to provision users and groups from Cisco DUO to Cisco Secure Access.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Access
- Cisco DUO

Components Used

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

- Admin access to Cisco Secure Access Dashboard

- Admin access Cisco DUO dashboard as Admin

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 DUO.

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.



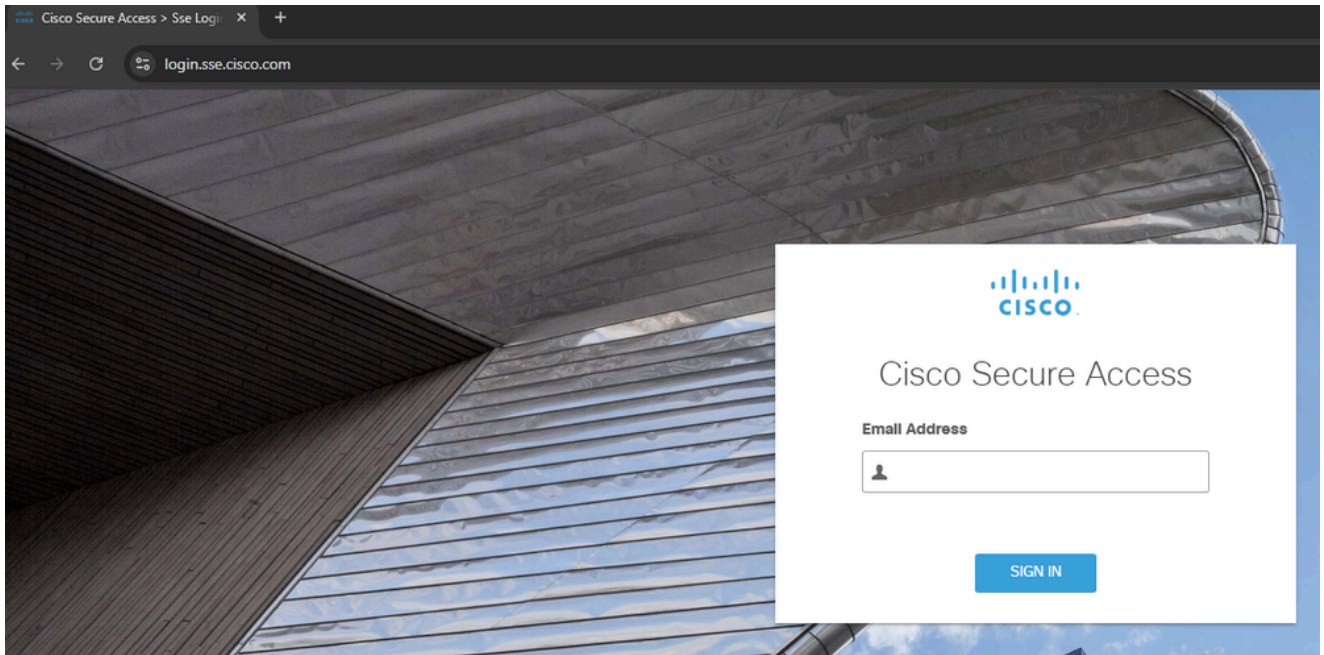
Note: This document focuses specifically on the provisioning of users and groups from DUO. The configuration of Entra ID or other Identity Providers (IdP) for ZTA enrollment, VPNaaS authentication, or specific Umbrella Roaming settings is outside the scope of this guide.

Configure

Configure Cisco Secure Access

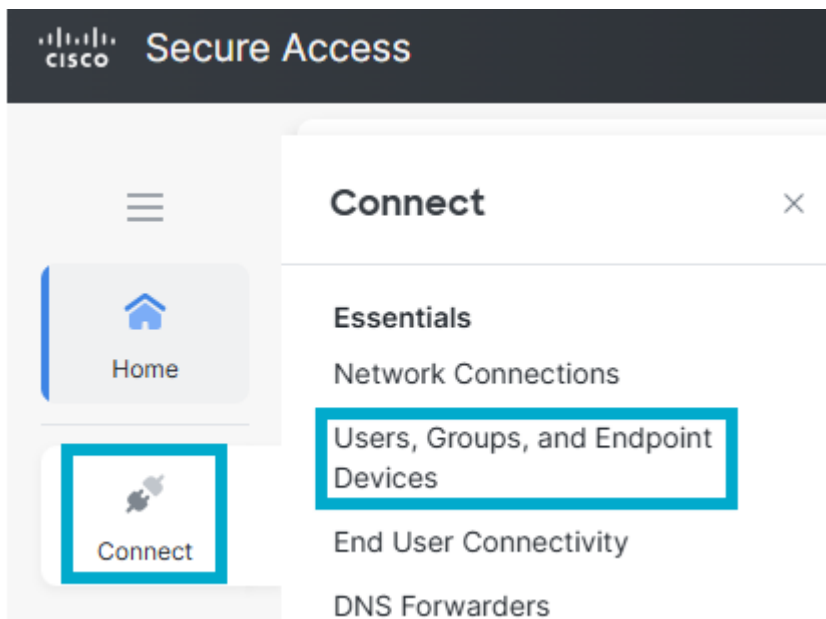
In order to begin the provisioning process, you must first configure the directory integration within the Cisco Secure Access dashboard. This step generates the necessary credentials and configuration parameters required to establish a secure connection with Microsoft Entra ID.

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



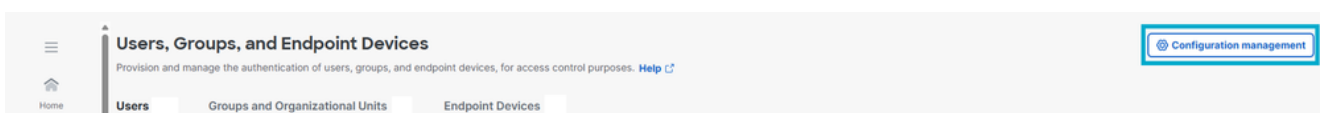
Sign in to CSA

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

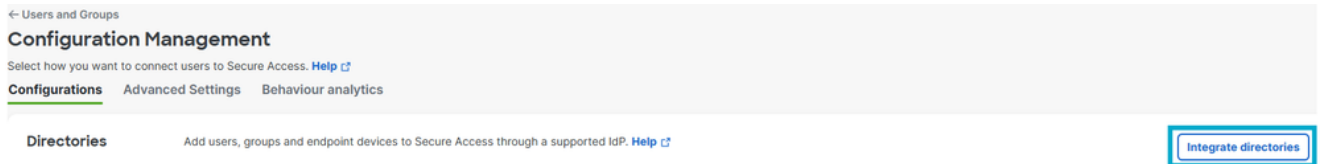


Users and Groups

3. Click **Configuration management**.



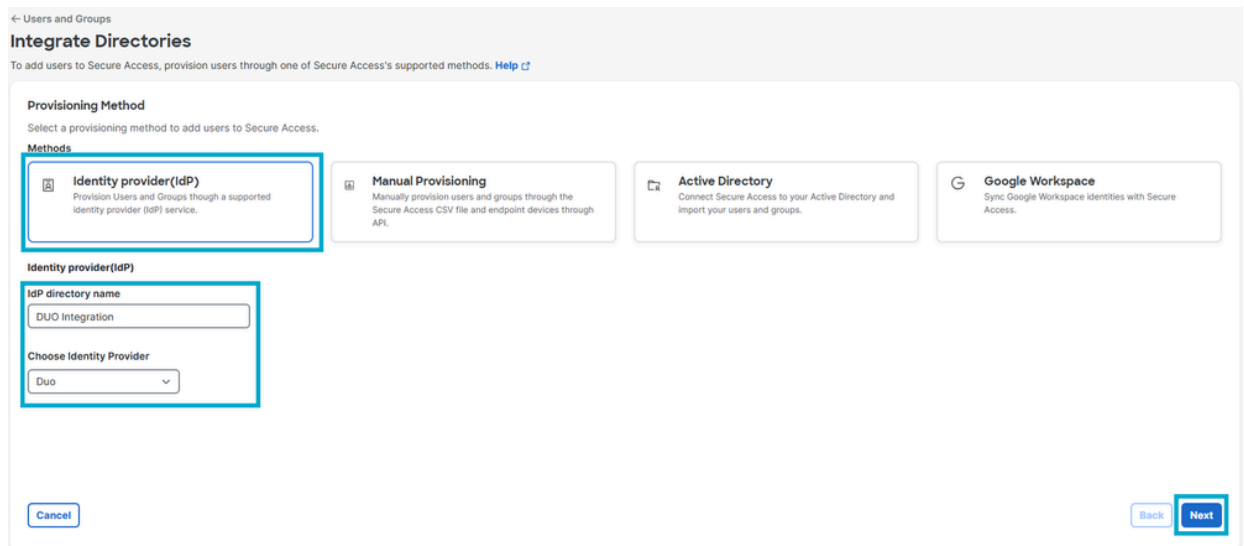
4. Click **Integrate Directory**.



Integrate Directory

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

- **IdP directory name: DUO Integration.**
- **Choose Identity Provider (IdP): DUO.**
- **Click Next.**



Directory Configuration

6. Click **Generate token**. Save the **generated token** and the **provisioning URL**, then click **Done**.

CISCO



Admin Login

Enter your admin credentials

Email address

Save my email address and login options
Not recommended for public or shared computers

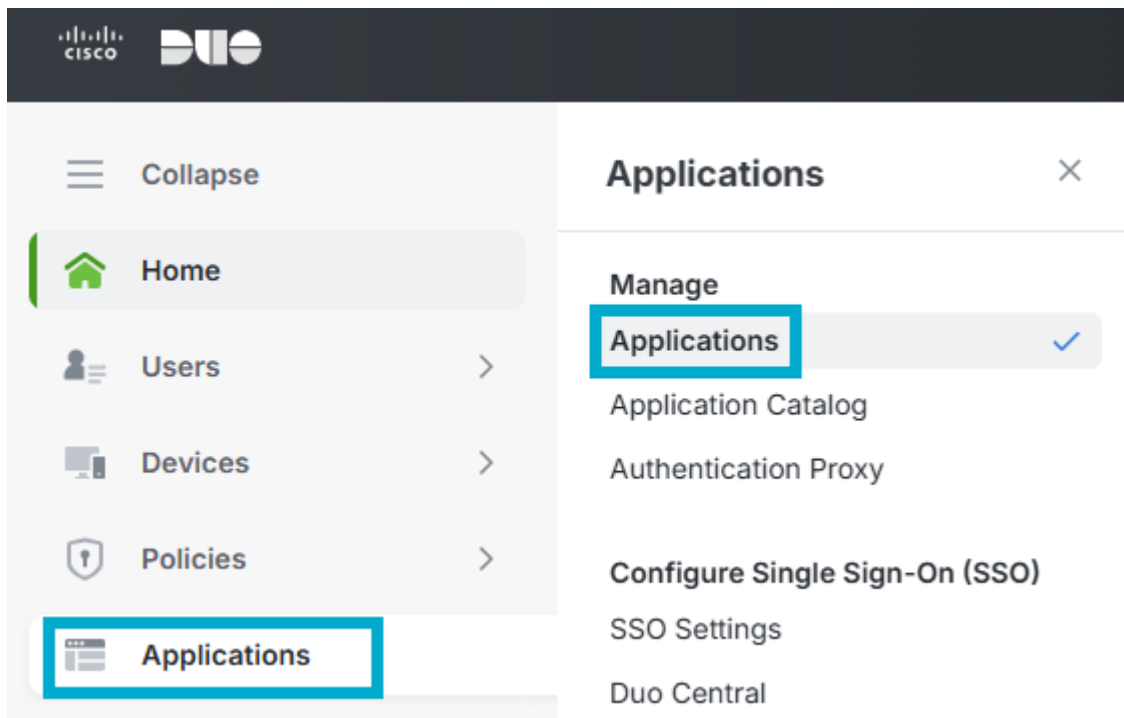
Continue

Want to protect your organization with Duo? [Start a free trial](#)

[Privacy Statement](#)

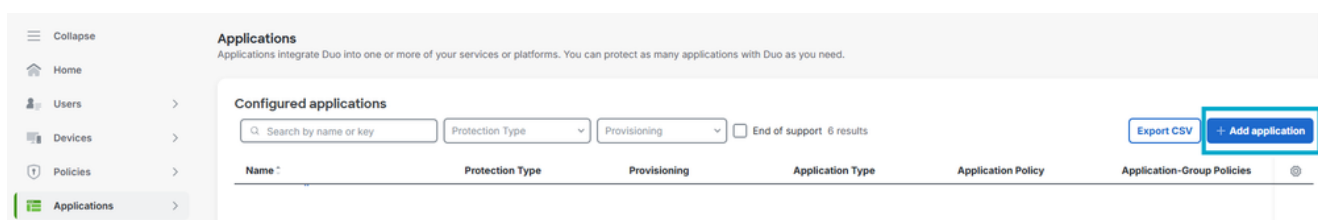
DUO Log In

2. Navigate to **Applications > Applications**.



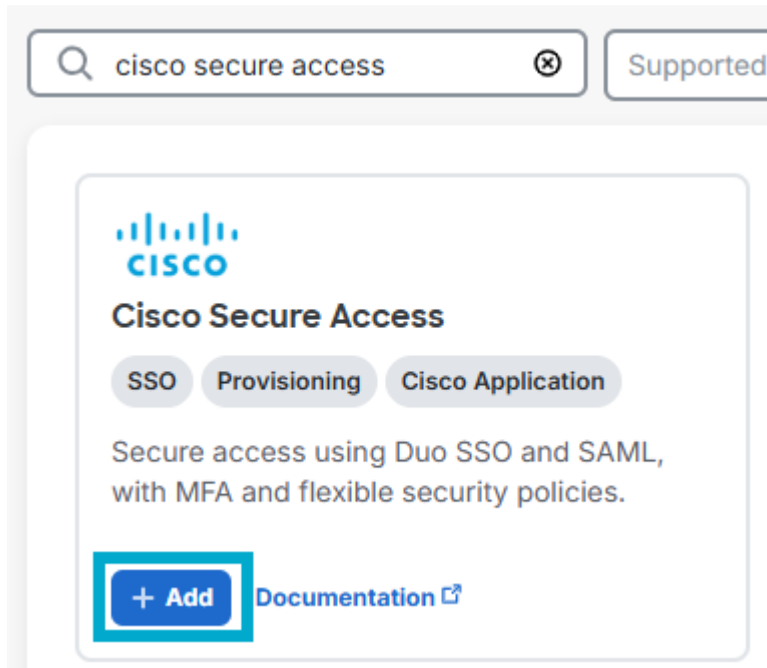
DUO Applications

3. Click **Add application**.



DUO Add App

4. Look for **Cisco Secure Access** and click **Add**.



Add CSA App

5. Click **Provisioning**. Enter the **Tenant URL** and **Secret Token** saved from step #6 of the Secure Access Configuration, and click **Connect to Application**.

Cisco Secure Access - Single Sign-On

Single Sign-On

Provisioning

Provisioning

Duo Verified

Disabled

Set up user provisioning with Cisco Secure Access.

[Learn more about provisioning.](#)

Authentication

Set up an authentication mechanism with your application to secure the connection.

Base URL *

https://api.sse.cisco.com/identity/v2/scim

Duo user attributes and group information will be sent to this URL.

Token *

..... Show

The bearer token or API token provided by your application

Connect to application



Successfully connected to the application

Finish setting up this connection to ensure that Duo can send user information to the application.

API Connect App

6. Under the same **Provisioning** tab, scroll down to **Attribute mapping** and ensure your attributes are as shown in this specific order.

Token *

..... Show

The bearer token or API token provided by your application

Connect to application

Attribute mapping

Configure how Duo user attributes are mapped to the attributes in your application so that user information is received in the correct format. To view or create Duo user attributes, go to [User Attributes](#).

Duo user attribute *	Application attribute
Username	userName
Display Name	displayName
Email Address	emails
Last Name	name.familyName
First Name	name.givenName

Edit mappings

Select all

Required attributes

userName

Optional attributes

authName

displayName

emails

name.familyName

name.formatted

name.givenName

nativeObjectId


Selected (5 items) [Cancel](#)

DUO Mapping

- Under the same **Provisioning** tab, scroll down to **Groups** and assign the group(s) to sync to Secure Access.

Groups

Select existing groups that will receive updates from Duo in this application.

 Users or groups will be automatically created, updated, and deactivated in this application.

Select groups

Groups

DUO - Users x

x

v

Use groups with SSO access

Exclude group information

If checked, Duo will send only user details without group information.

Users

User deprovisioning behavior

Deactivate Users

Removing a group or user will keep the users in your application but set them to disabled.

Delete Users

Removing a group or user will permanently delete the users in your application.

Save

Provision Group

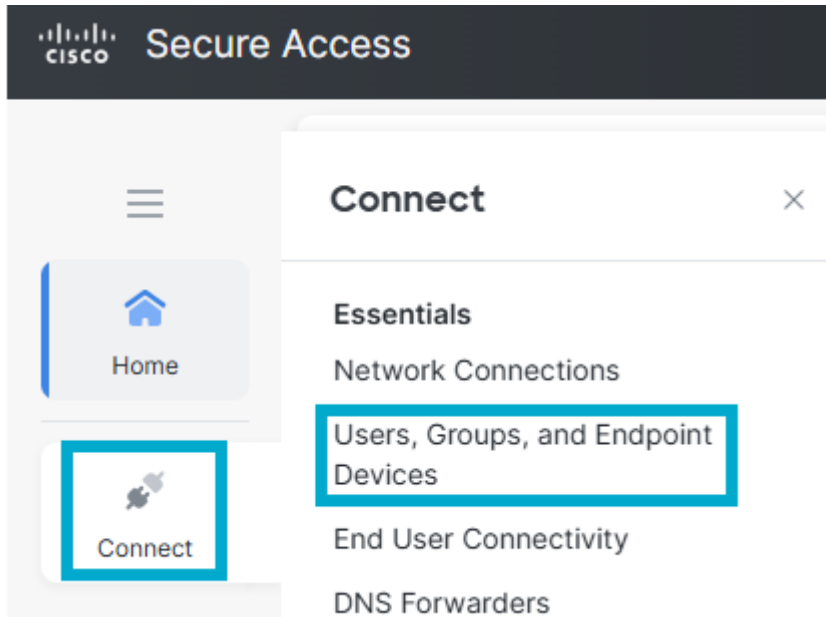


Note: If users do not get provisioned to Secure Access in the proper format, ensure you configure the Attribute Mapping as stated [here](#).

Verify

Verity 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 6

Endpoint Devices 2

Users

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

Search Source DUO Integration Risk Alert Trust Level 1 results

Name	Risk Alerts ⓘ	User Principal Name (UPN)	Auth Property	Source	Directory
Josue	-	j @ ...	j @ ...	Duo	DUO Integration

Verify Users in CSA

- Click **Groups and Organizational Units**.

Users 7 **Groups and Organizational Units** 6 Endpoint Devices 2

6 Groups 0 Organizational Units

Groups and Organizational Units

Manage your organization's groups and Organizational Units. To add new groups or OUs, go to **Configuration management > Integrate**

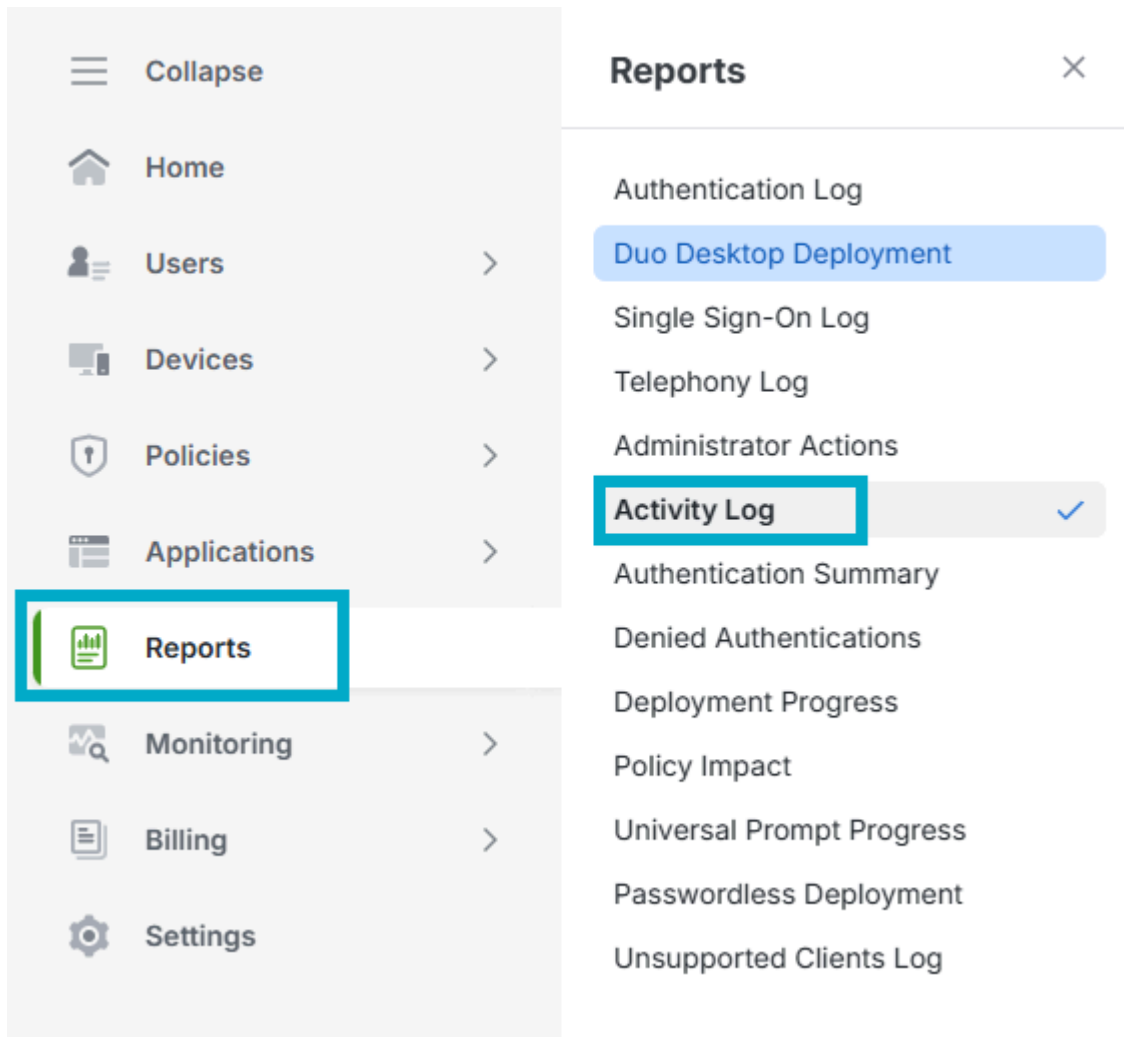
Search Type Source DUO Integration 1 results

Name	Type	Source	Directory
DUO - Users	Groups	Duo	DUO Integration

Verify Group in CSA

Verify in DUO

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



DUO Activity Log

- Filter based on the name of the Application.

Activity Log

1 Type to search Last 24 hours Filters Reset all 23 results Export

Search by actor, application, affected

Timestamp (CST)	Action	Actor	Affected	Application	Access device	Log details
03:11:57 PM Mar 18, 2026	Group provisioning succeeded	Automated Provisioning Integration System	DUO - Users Outbound SCIM Sync	Cisco Secure Access - Single Sign-On	—	View details
03:11:56 PM Mar 18, 2026	Group provisioning succeeded	Automated Provisioning Integration System	DUO - Users Outbound SCIM Sync	Cisco Secure Access - Single Sign-On	—	View details
03:11:55 PM Mar 18, 2026	User provisioning succeeded	Automated Provisioning Integration System	j...@... Outbound SCIM Sync	Cisco Secure Access - Single Sign-On	—	View details
03:11:55 PM Mar 18, 2026	Provisioning successfully connected	Josue Brenes Administrator	Cisco Secure Access - Single Sign-On Outbound SCIM Sync	Cisco Secure Access - Single Sign-On	—	View details
03:11:51 PM Mar 18, 2026	Enabled provisioning	Josue Brenes Administrator	Cisco Secure Access - Single Sign-On Outbound SCIM Sync	Cisco Secure Access - Single Sign-On	—	View details

DUO Provisioning Logs

Related Information

[Configure Identity Providers](#)

[Provision Users and Groups from Duo](#)

[Attribute Mapping \(Mandatory\)](#)

[Duo Single Sign-On for Cisco Secure Access](#)