

Configuration des utilisateurs et des groupes pour un accès sécurisé via DUO

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Configuration de Cisco Secure Access](#)

[Configuration du provisionnement dans Cisco DUO](#)

[Vérifier](#)

[Verity dans Cisco Secure Access](#)

[Vérifier dans DUO](#)

[Informations connexes](#)

Introduction

Ce document décrit comment provisionner des utilisateurs et des groupes de Cisco DUO vers Cisco Secure Access.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès sécurisé Cisco
- Cisco DUO

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

- Accès administrateur au tableau de bord Cisco Secure Access
- Admin accède au tableau de bord Cisco DUO en tant qu'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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Cisco Secure Access prend en charge le provisionnement des utilisateurs et des groupes à partir de DUO.

Cette mise en service permet à Secure Access de gérer un répertoire d'utilisateurs autorisés à :

- Inscrivez-vous au programme ZTA (Zero Trust Access).
- Se connecter à VPNaaS.
- Appliquez des politiques basées sur l'identité aux utilisateurs d'Umbrella Roaming.



Remarque : Ce document se concentre spécifiquement sur l'approvisionnement des utilisateurs et des groupes de DUO. La configuration d'Entra ID ou d'autres fournisseurs d'identité (IdP) pour l'inscription ZTA, l'authentification VPNaaS ou des paramètres d'itinérance Umbrella spécifiques n'est pas traitée dans ce guide.

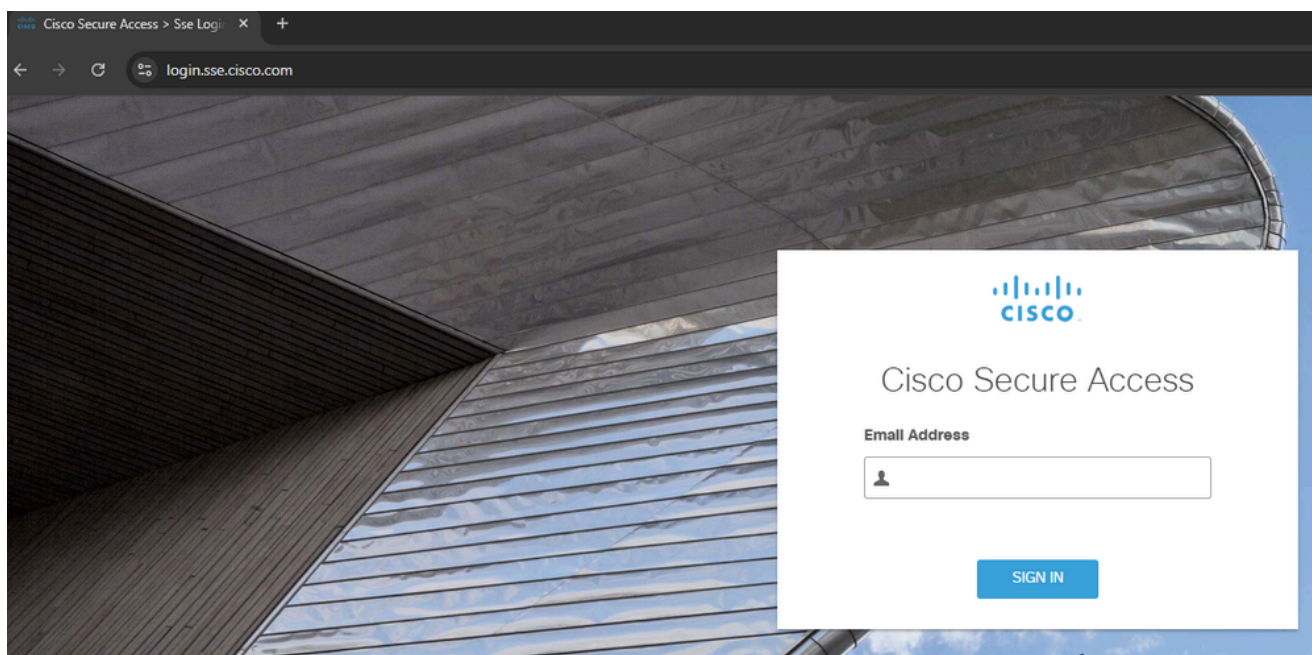
Configurer

Configuration de Cisco Secure Access

Afin de commencer le processus de mise en service, vous devez d'abord configurer l'intégration du répertoire dans le tableau de bord Cisco Secure Access. Cette étape génère les informations d'identification et les paramètres de configuration nécessaires pour établir une connexion

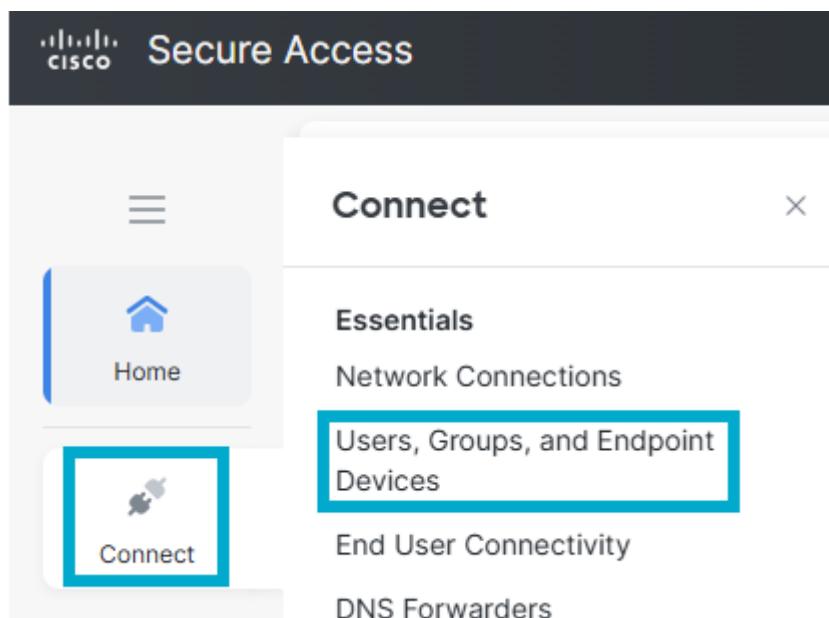
sécurisée avec Microsoft Entra ID.

1. Connectez-vous au tableau de [bord Cisco Secure Access](#).



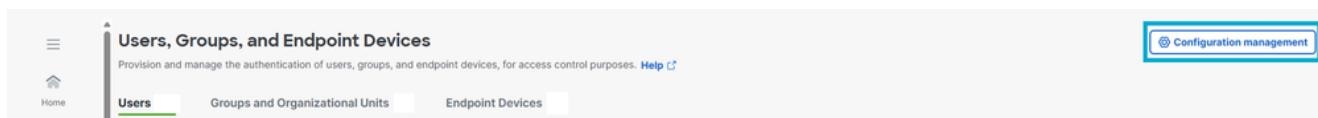
Se connecter à CSA

2. Naviguez jusqu'à **Connect > Users, Groups and Endpoint Devices**.



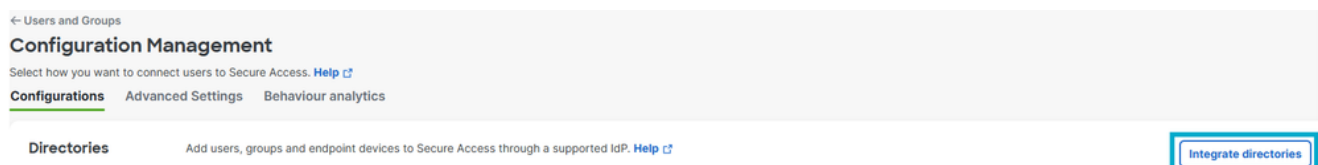
Utilisateurs et groupes

3. Cliquez sur **Gestion de la configuration**.



Gestion de la configuration

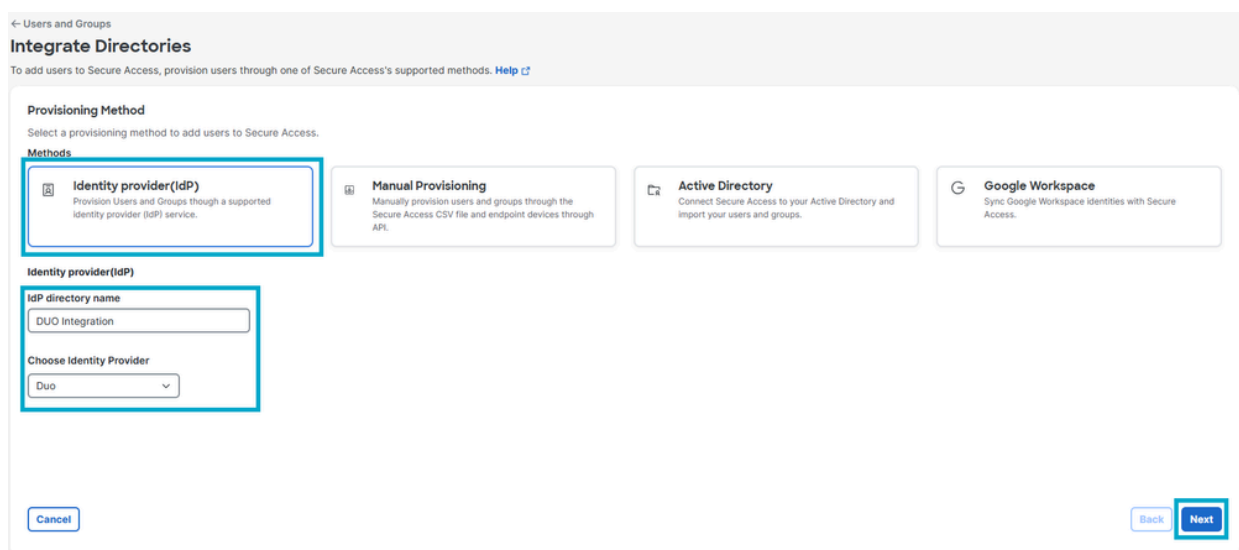
4. Cliquez sur **Intégrer le répertoire**.



Integrate Directory

5. Sous **Méthode de provisionnement**, cliquez sur **Fournisseur d'identités**.

- **Nom du répertoire IdP : Intégration DUO.**
- Choisir un **fournisseur d'identité : DUO.**
- Cliquez sur **Suivant**.



Configuration du répertoire

6. Cliquez sur **Générer un jeton**. Enregistrez le **jeton généré** et l'**URL d'approvisionnement**, puis cliquez sur **Terminé**.

CISCO



Admin Login

Enter your admin credentials

Email address

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

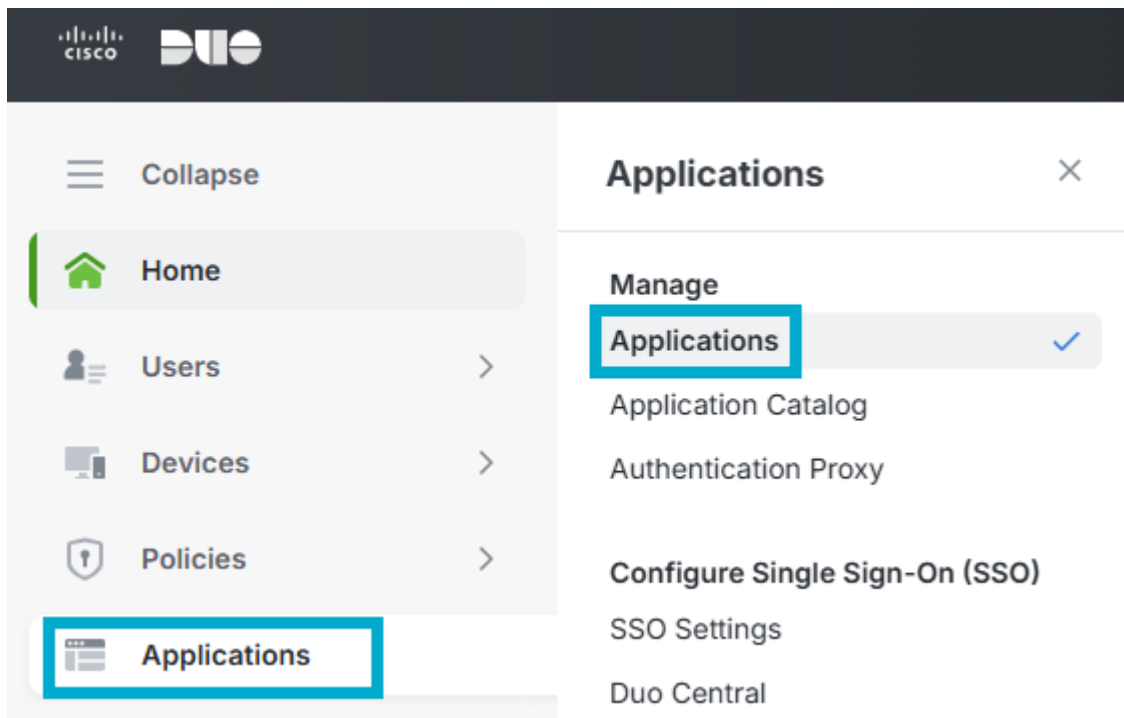
Continue

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

[Privacy Statement](#)

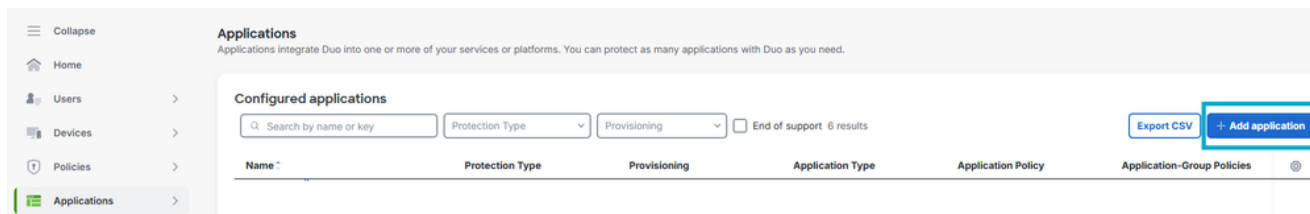
Connexion DUO

2. Accédez à Applications > Applications.



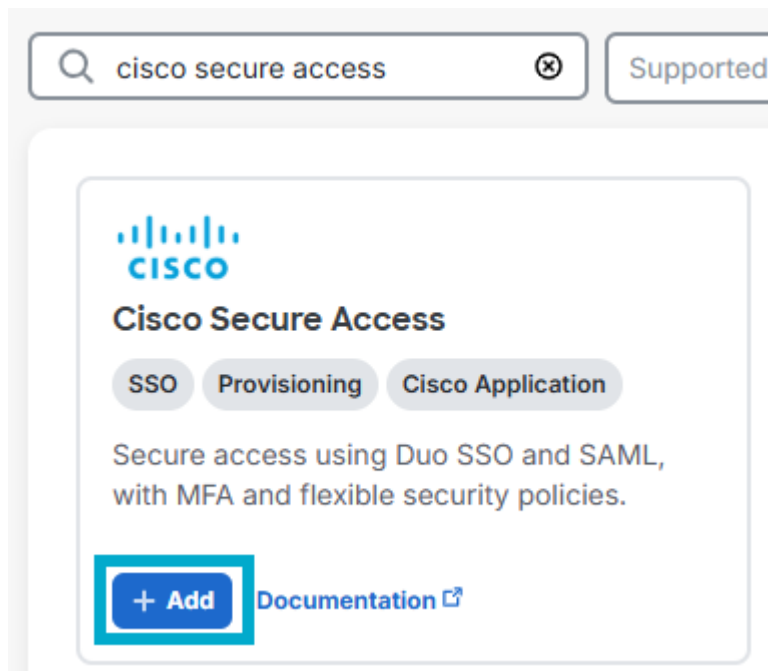
Applications DUO

3. Cliquez sur Ajouter une application.



DUO Add App

4. Recherchez Cisco Secure Access et cliquez sur Add.



Ajouter une application CSA

5. Cliquez sur Provisioning. Entrez l'URL du locataire et le jeton secret enregistrés à l'étape #6 de la configuration d'accès sécurisé, puis cliquez sur 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. Sous le même onglet Provisioning, faites défiler jusqu'à Attribute mapping et assurez-vous que vos attributs sont tels qu'ils apparaissent dans cet ordre spécifique.

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](#)

Mappage DUO

7. Sous le même onglet Provisioning, faites défiler jusqu'à Groups et attribuez le ou les groupes à synchroniser avec 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

▼

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

Groupe de provision

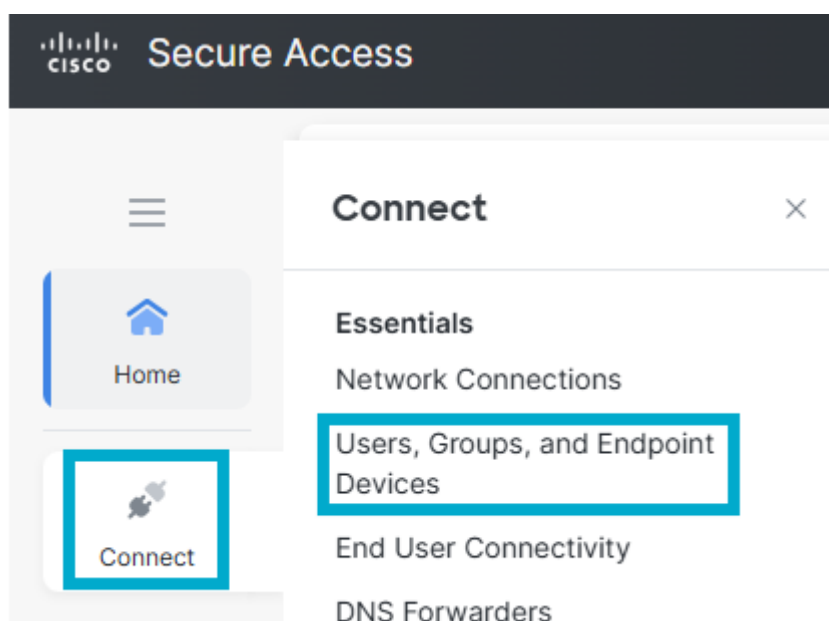


Remarque : Si les utilisateurs ne reçoivent pas les privilèges d'accès sécurisés au format approprié, assurez-vous de configurer le mappage d'attribut comme indiqué [ici](#).

Vérifier

Verity dans Cisco Secure Access

- Naviguez jusqu'à Connect > Users, Groups and Endpoint Devices.



Users and Groups in CSA

- Cliquez sur Utilisateurs.

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

- Cliquez sur Groupes et unités d'organisation.

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**

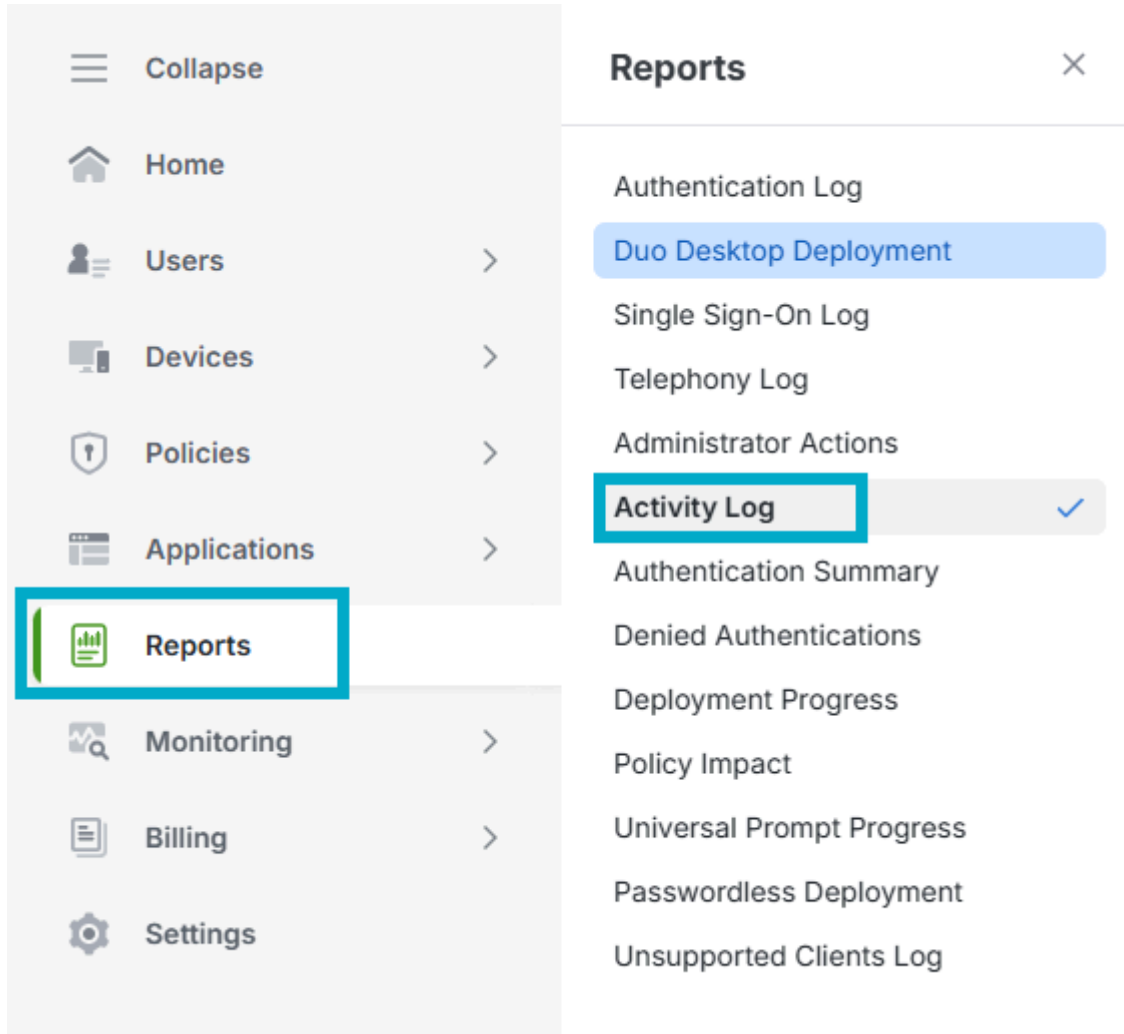
Search Type Source DUO Integration 1 results

Name	Type	Source	Directory
DUO - Users	Groups	Duo	DUO Integration

Verify Group in CSA

Vérifier dans DUO

- Accédez à Rapports > Journal d'activité.



Duo Activity Log

- Filtrer en fonction du nom de l'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

Journaux de provisionnement DUO

Informations connexes

[Configurer les fournisseurs d'identité](#)

[Provisionner des utilisateurs et des groupes à partir de Duo](#)

[Mappage des attributs \(obligatoire\)](#)

[Authentification unique duo pour Cisco Secure Access](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.