

Assegnazione dell'accesso sicuro a utenti e gruppi tramite DUO

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazione di Cisco Secure Access](#)

[Configurazione del provisioning in Cisco DUO](#)

[Verifica](#)

[Verity in Cisco Secure Access](#)

[Verifica in DUO](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come eseguire il provisioning di utenti e gruppi da Cisco DUO a Cisco Secure Access.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Access
- Cisco DUO

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

- Accesso amministrativo a Cisco Secure Access Dashboard
- L'amministratore accede al dashboard Cisco DUO come amministratore

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Cisco Secure Access supporta il provisioning di utenti e gruppi da DUO.

Questo provisioning consente l'accesso sicuro per la gestione di una directory di utenti autorizzati a:

- Registrarsi in Zero Trust Access (ZTA).
- Connessione a VPNaaS.
- Applicazione di criteri basati sull'identità agli utenti di Umbrella Roaming.



Nota: Questo documento si concentra in modo specifico sul provisioning di utenti e gruppi da DUO. La configurazione dell'ID Entra o di altri provider di identità (IdP) per la registrazione ZTA, l'autenticazione VPNaaS o impostazioni di roaming Umbrella specifiche esula dall'ambito di questa guida.

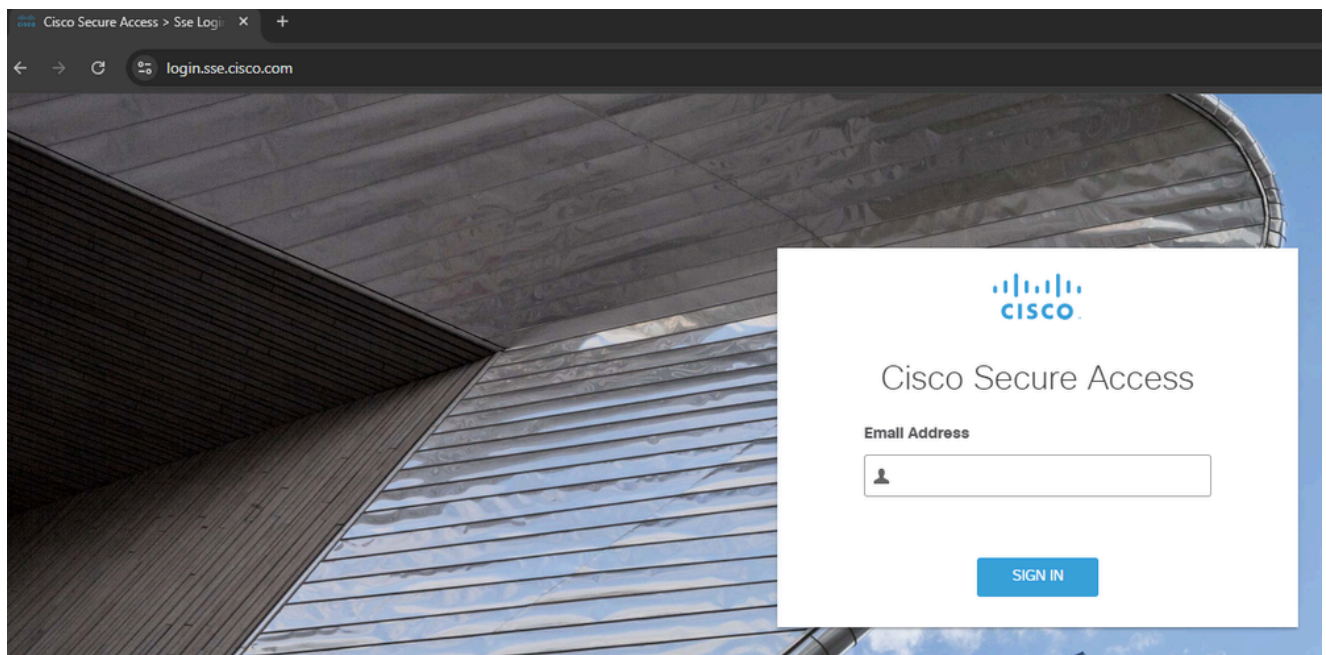
Configurazione

Configurazione di Cisco Secure Access

Per avviare il processo di provisioning, è necessario innanzitutto configurare l'integrazione delle directory nel dashboard Cisco Secure Access. Questo passaggio genera le credenziali e i

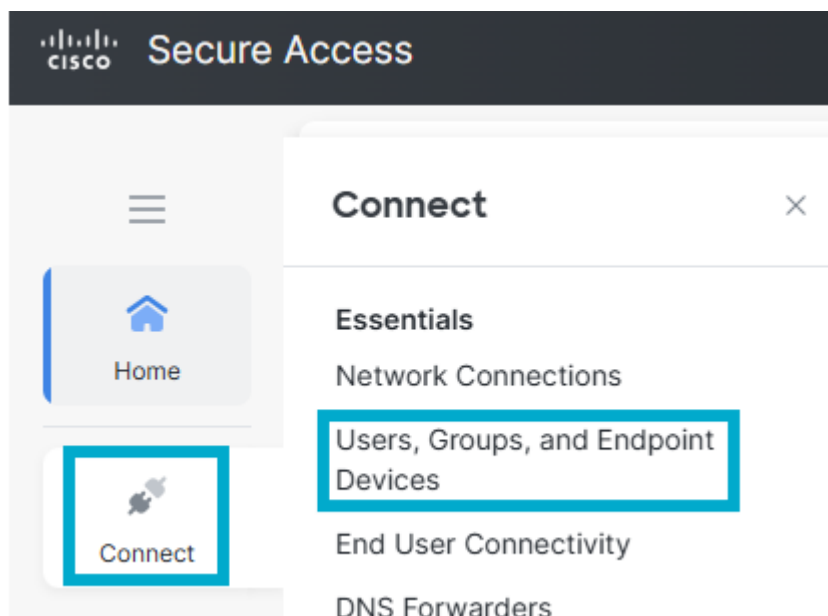
parametri di configurazione necessari per stabilire una connessione protetta con Microsoft Entra ID.

1. Accedi a **Cisco Secure Access Dashboard**.



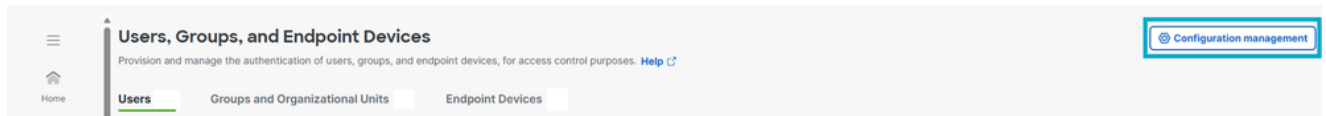
Accedi a CSA

2. Passare a **Connetti > Utenti, gruppi e dispositivi endpoint**.



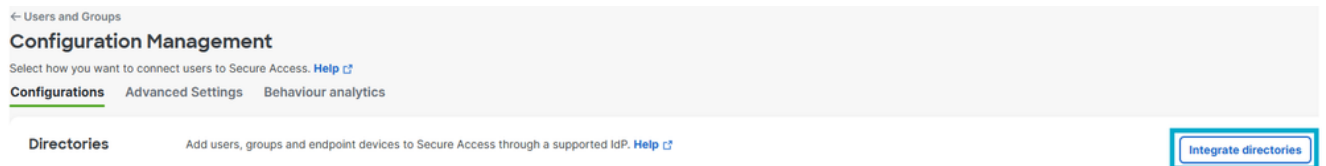
Utenti e gruppi

3. Fare clic su **Gestione configurazione**.



Gestione della configurazione

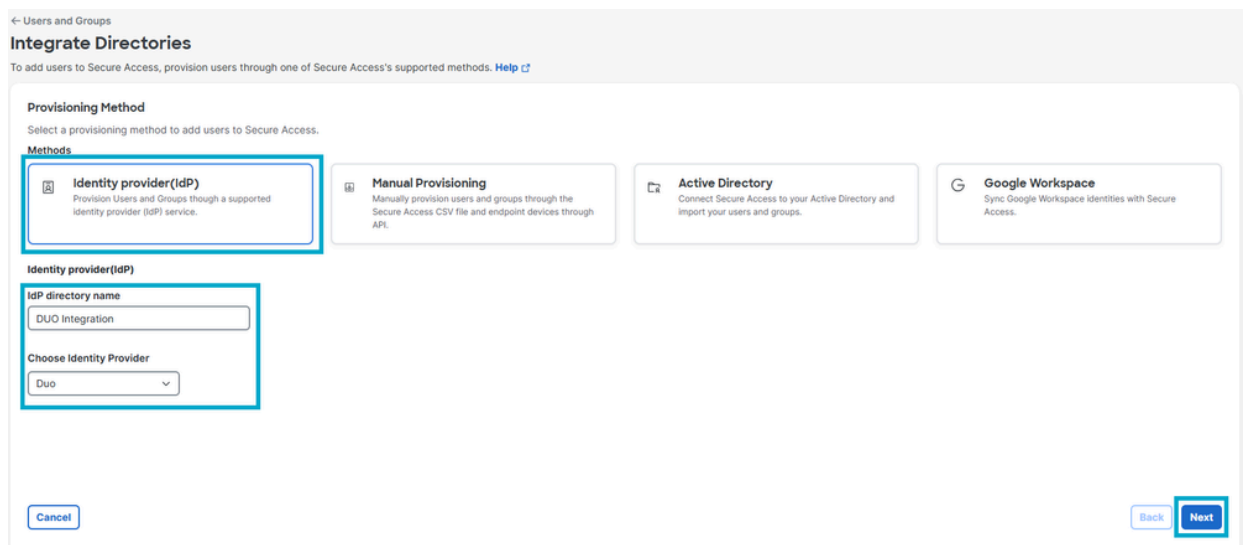
4. Fate clic su **Integra directory (Integrate Directory)**.



Integrate Directory

5. In **Metodo di provisioning** fare clic su **Provider di identità**.

- **Nome directory IdP: Integrazione DUO.**
- **Scegli provider di identità (IdP): DUO.**
- **Fare clic su Next (Avanti).**



Configurazione directory

6. Fare clic su **Genera token**. Salvare il **token generato** e l'**URL di provisioning**, quindi fare clic su **Fine**.

CISCO



Admin Login

Enter your admin credentials

Email address

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

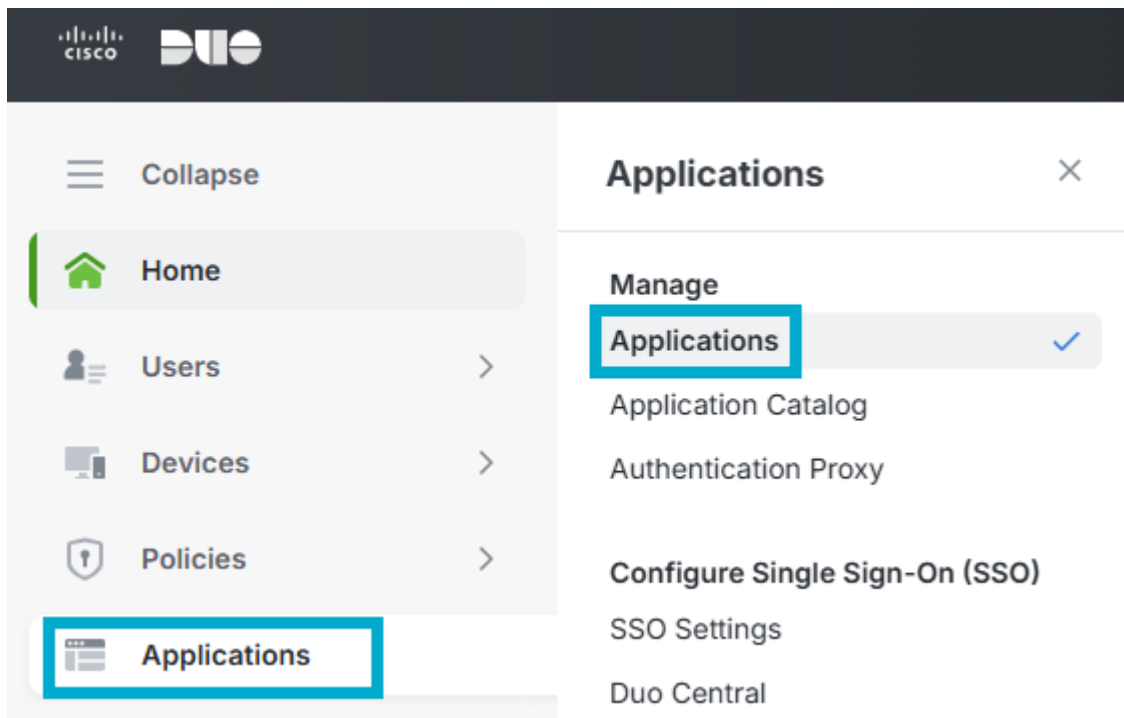
Continue

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

[Privacy Statement](#)

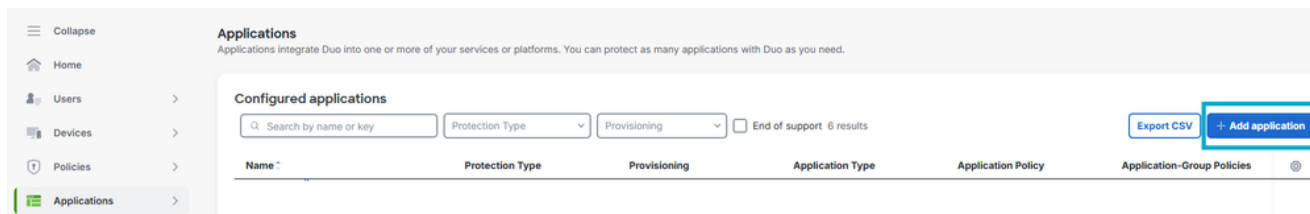
DUO Log In

2. Passare a Applicazioni > Applicazioni.



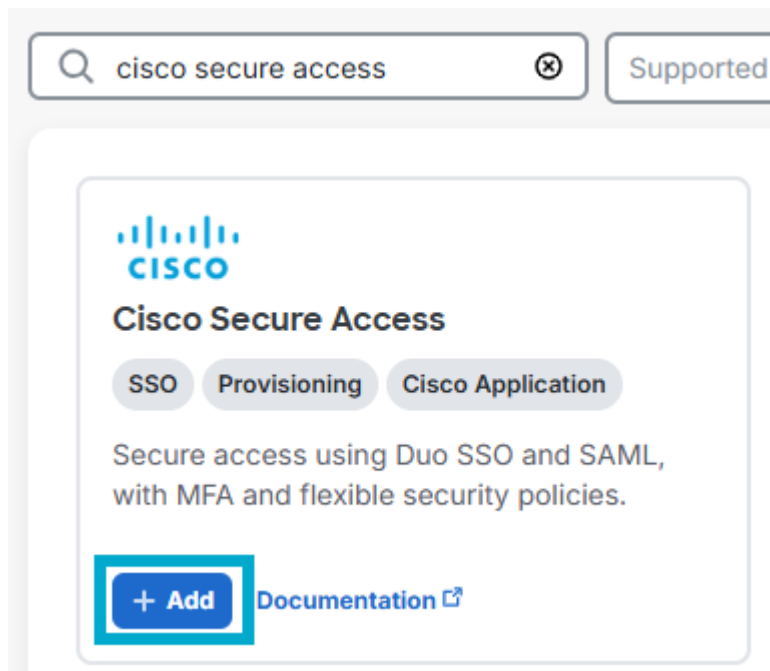
Applicazioni DUO

3. Fare clic su Aggiungi applicazione.



DUO Add App

4. Cercare Cisco Secure Access e fare clic su Add (Aggiungi).



Aggiungi app CSA

5. Fare clic su Provisioning. Immettere l'URL tenant e il token segreto salvati dal passaggio n. 6 della configurazione di accesso sicuro e fare clic su Connetti all'applicazione.

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. Nella stessa scheda Provisioning, scorrere verso il basso fino a Mappatura attributi e verificare che gli attributi siano quelli mostrati in questo ordine specifico.

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](#)

Mapping DUO

7. Nella stessa scheda Provisioning, scorrere verso il basso fino a Gruppi e assegnare i gruppi da sincronizzare con Accesso sicuro.

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

Gruppo di provisioning

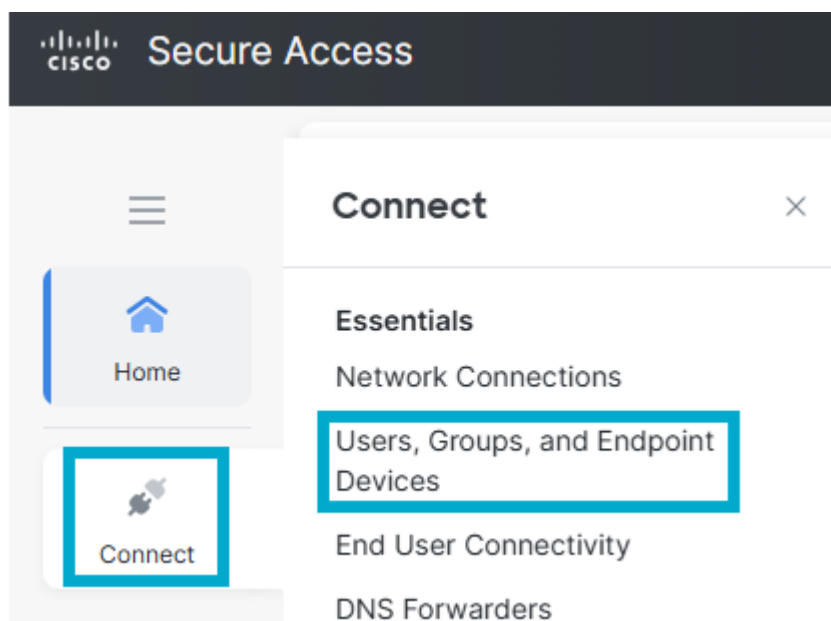


Nota: Se agli utenti non viene assegnato l'accesso protetto nel formato corretto, assicurarsi di configurare il mapping degli attributi come indicato [qui](#).

Verifica

Verity in Cisco Secure Access

- Passare a Connetti > Utenti, gruppi e dispositivi endpoint.



Users and Groups in CSA

- Fare clic su Utenti.

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

- Fare clic su Gruppi e unità organizzative.

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**

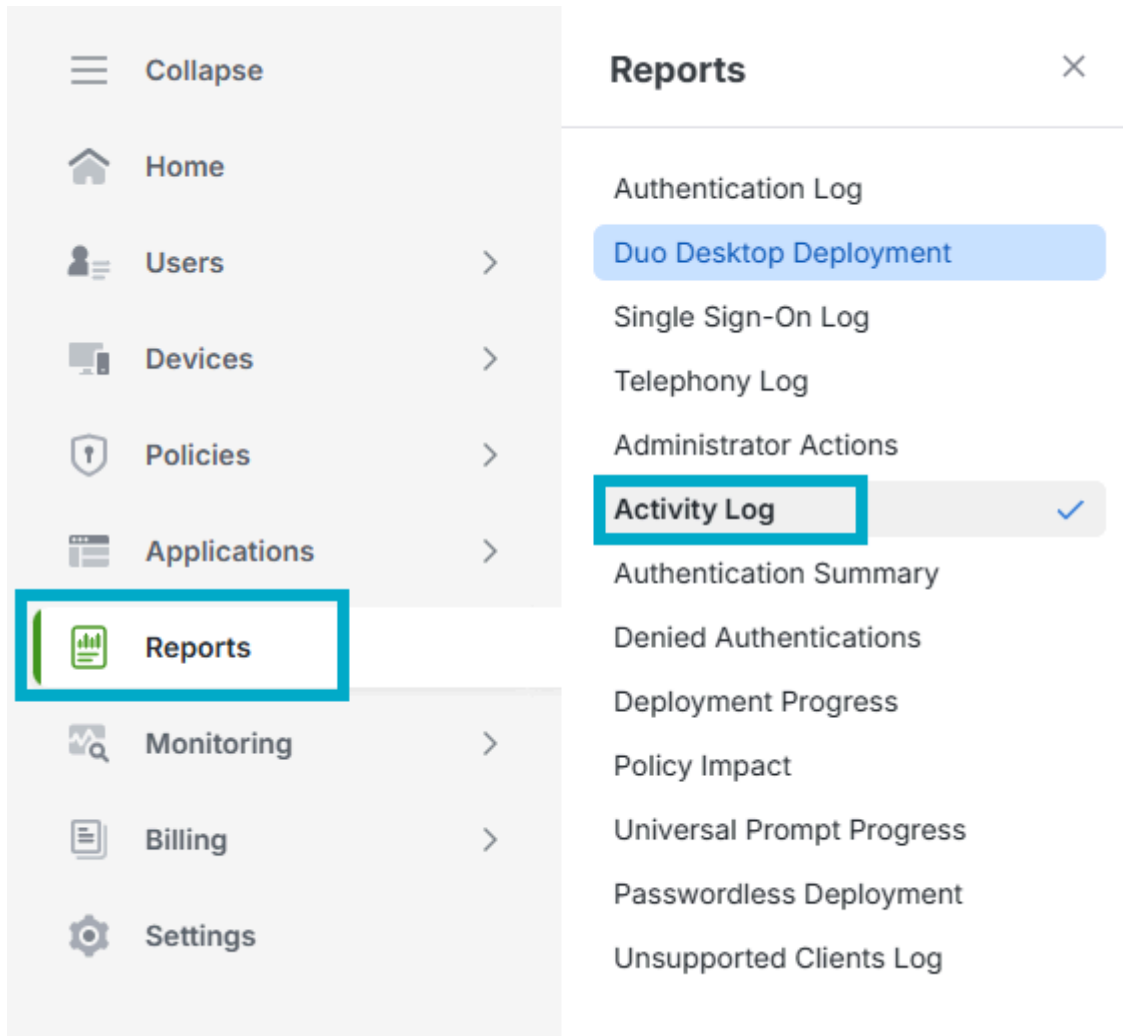
Search Type Source DUO Integration 1 results

Name	Type	Source	Directory
DUO - Users	Groups	Duo	DUO Integration

Verify Group in CSA

Verifica in DUO

- Passare a Rapporti > Log attività.



Duo Activity Log

- Filtrare in base al nome dell'applicazione.

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

Log di provisioning DUO

Informazioni correlate

[Configura provider di identità](#)

[Assegna ruoli a utenti e gruppi di Duo](#)

[Mapping attributi \(obbligatorio\)](#)

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).