

Bereitstellung von Benutzern und Gruppen für sicheren Zugriff über DUO

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurieren von Cisco Secure Access](#)

[Konfiguration der Bereitstellung in Cisco DUO](#)

[Überprüfung](#)

[Verify in Cisco Secure Access](#)

[Verifizieren in DUO](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Benutzer und Gruppen von Cisco DUO für Cisco Secure Access bereitgestellt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicherer Zugriff von Cisco
- Cisco DUO

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

- Administratorzugriff auf das Cisco Secure Access Dashboard
- Administratorzugriff auf das Cisco DUO-Dashboard als Administrator

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Cisco Secure Access unterstützt die Bereitstellung von Benutzern und Gruppen über das DUO.

Diese Bereitstellung ermöglicht Secure Access die Verwaltung eines Verzeichnisses von Benutzern, die autorisiert sind,

- Registrieren Sie sich für Zero Trust Access (ZTA).
- Herstellen einer Verbindung mit VPNaaS
- Anwendung identitätsbasierter Richtlinien auf Umbrella Roaming-Benutzer



Anmerkung: Dieses Dokument konzentriert sich speziell auf die Bereitstellung von Benutzern und Gruppen von DUO. Die Konfiguration der Entra-ID oder anderer Identitätsanbieter (IdP) für die ZTA-Registrierung, die VPNaaS-Authentifizierung oder bestimmte Umbrella Roaming-Einstellungen wird in diesem Leitfaden nicht behandelt.

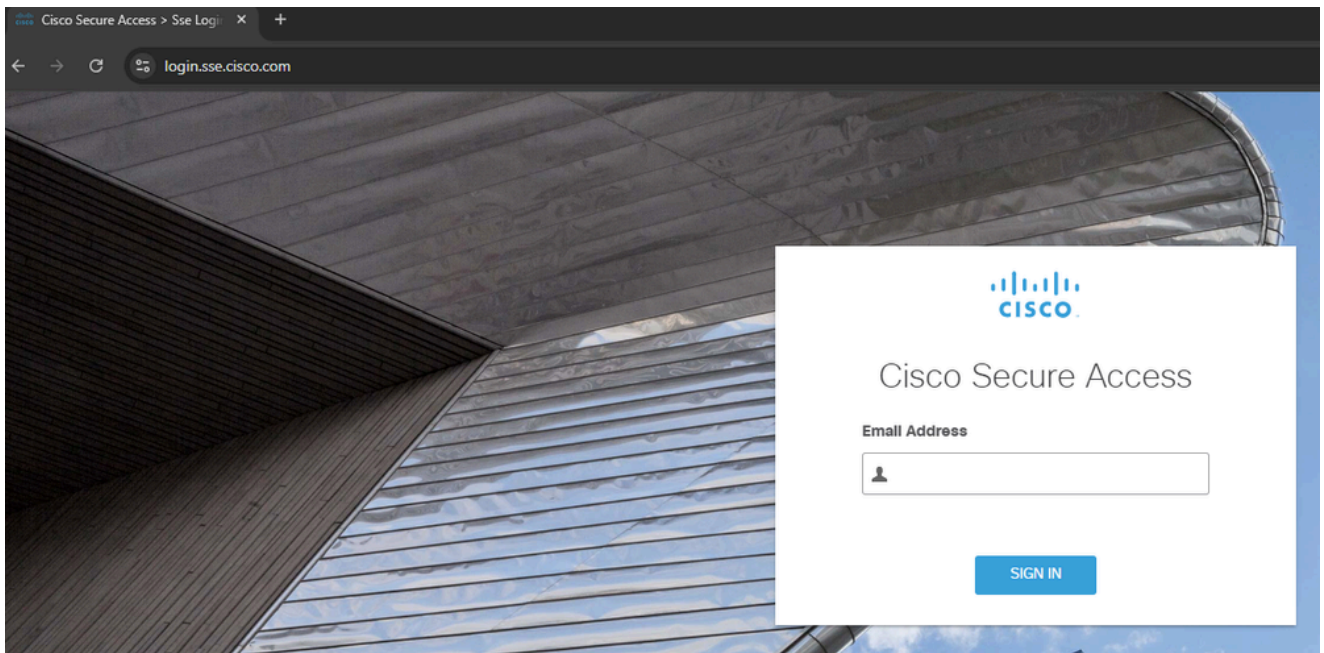
Konfigurieren

Konfigurieren von Cisco Secure Access

Um mit der Bereitstellung zu beginnen, müssen Sie zunächst die Verzeichnisintegration im Cisco Secure Access Dashboard konfigurieren. In diesem Schritt werden die erforderlichen

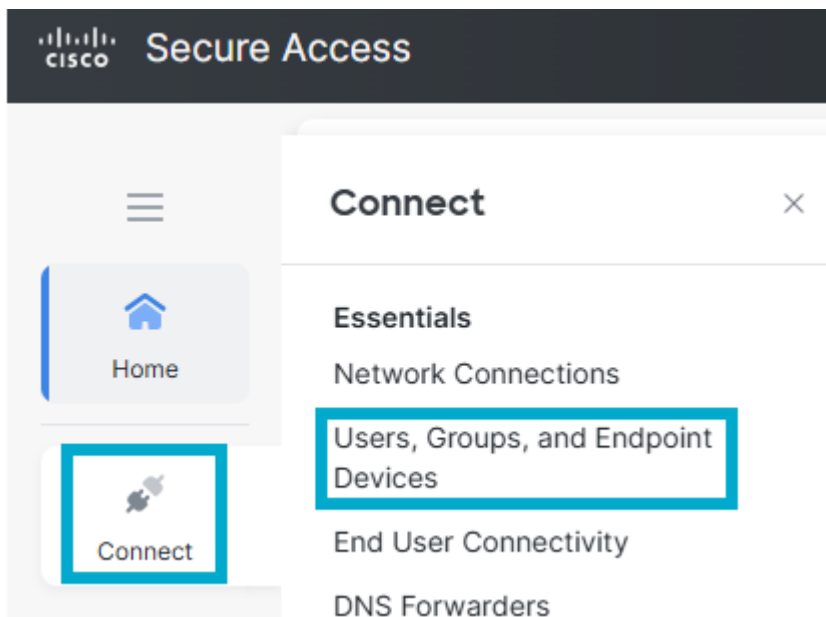
Anmeldeinformationen und Konfigurationsparameter generiert, die zum Herstellen einer sicheren Verbindung mit der Microsoft Entra-ID erforderlich sind.

1. Anmeldung beim **Cisco Secure Access Dashboard**.



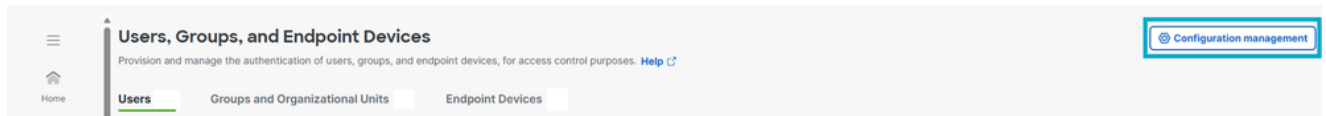
Bei CSA anmelden

2. Navigieren Sie zu **Verbinden > Benutzer, Gruppen und Endgeräte**.



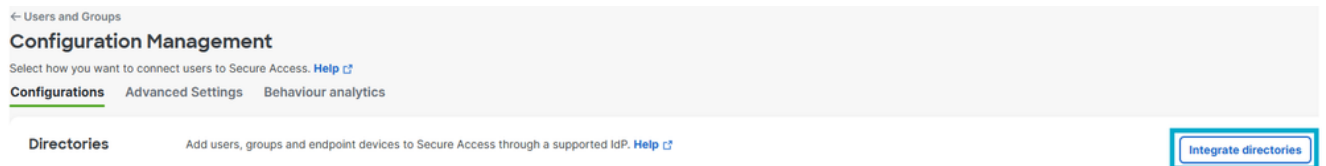
Benutzer und Gruppen

3. Klicken Sie auf **Konfigurationsmanagement**.



Konfigurationsverwaltung

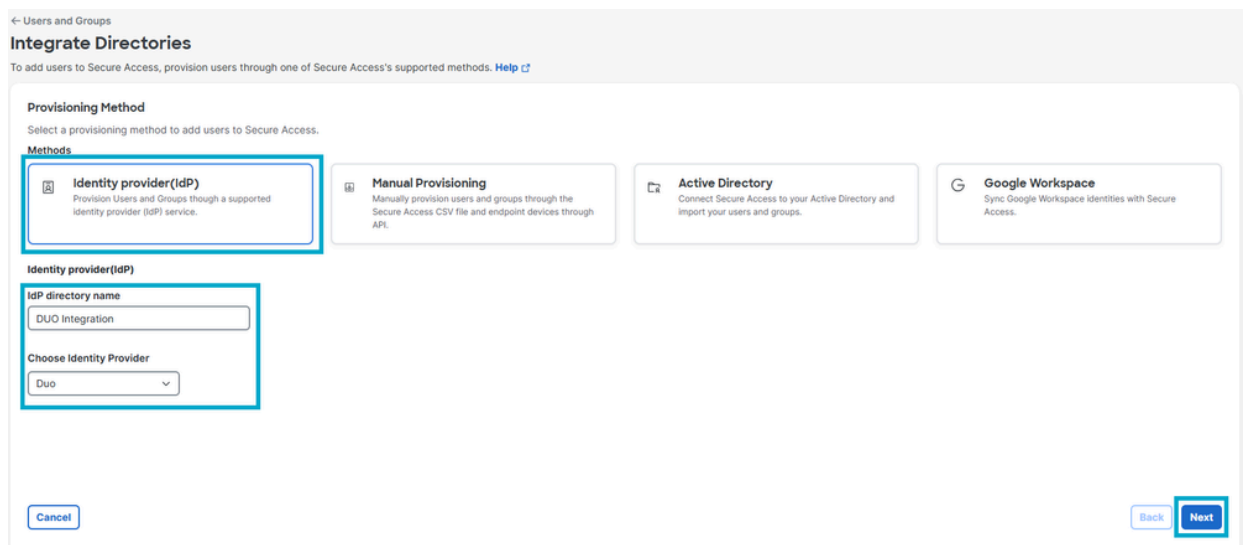
4. Klicken Sie auf **Verzeichnis integrieren**.



Integrate Directory

5. Klicken Sie unter **Bereitstellungsmethode** auf **Identitätsanbieter**.

- **IdP-Verzeichnisname: DUO-Integration:**
- **Identitätsanbieter (IdP) auswählen: DUO.**
- Klicken Sie auf **Next** (Weiter).



Verzeichniskonfiguration

6. Klicken Sie auf **Token generieren**. Speichern Sie das **generierte Token** und die **Bereitstellungs-URL**, und klicken Sie dann auf **Fertig**.

CISCO



Admin Login

Enter your admin credentials

Email address

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

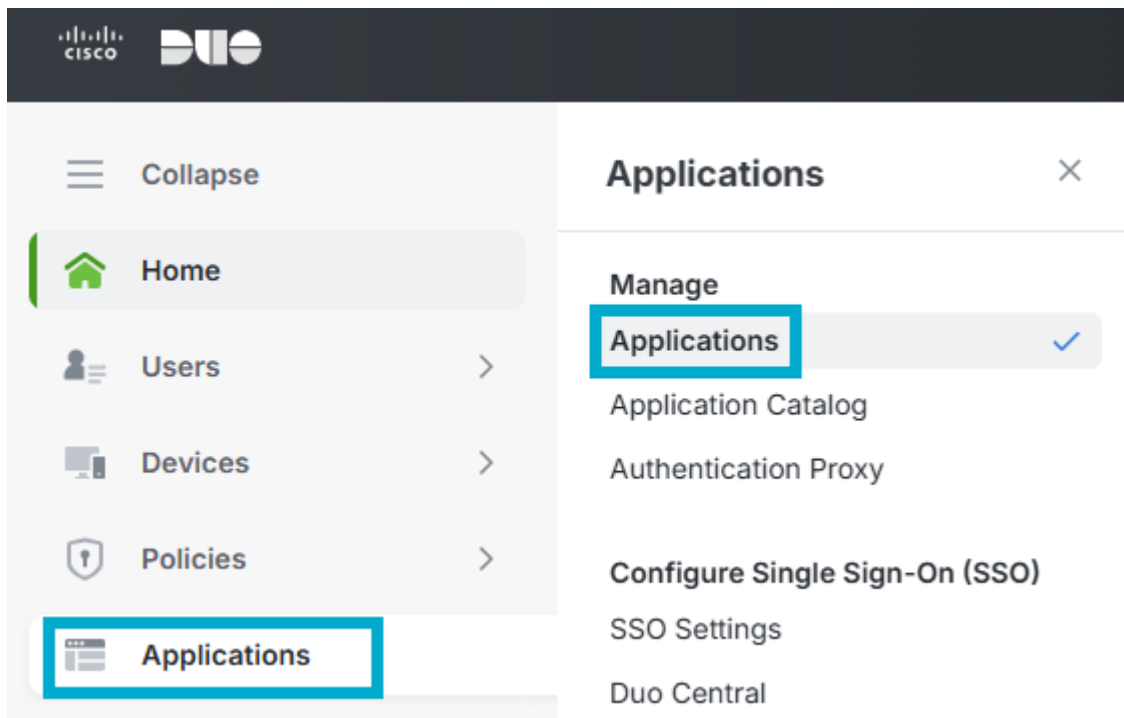
Continue

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

[Privacy Statement](#)

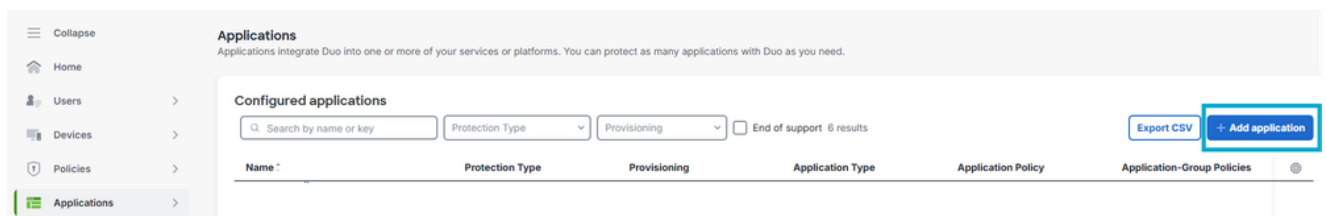
DUO-Anmeldung

2. Navigieren Sie zu Anwendungen > Anwendungen.



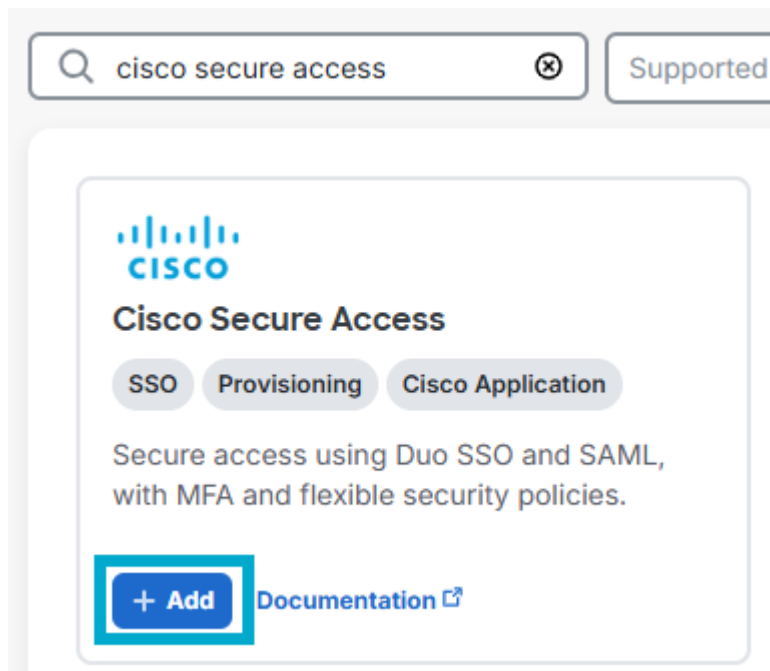
DUO-Anwendungen

3. Klicken Sie auf Anwendung hinzufügen.



DUO Add App

4. Suchen Sie nach Cisco Secure Access, und klicken Sie auf Hinzufügen.



CSA-Anwendung hinzufügen

5. Klicken Sie auf Provisioning. Geben Sie die Tenant-URL und das geheime Token ein, die aus Schritt #6 der Konfiguration für sicheren Zugriff gespeichert wurden, und klicken Sie auf Mit Anwendung verbinden.

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. Scrollen Sie auf derselben Registerkarte Provisioning nach unten zu Attribute-Zuordnung, und stellen Sie sicher, dass Ihre Attribute in der angegebenen Reihenfolge vorliegen.

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-Zuordnung

7. Scrollen Sie auf derselben Registerkarte Provisioning (Bereitstellung) nach unten zu Groups (Gruppen), und weisen Sie die zu synchronisierenden Gruppen Secure Access zu.

Groups

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

i 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

Bereitstellungsgruppe

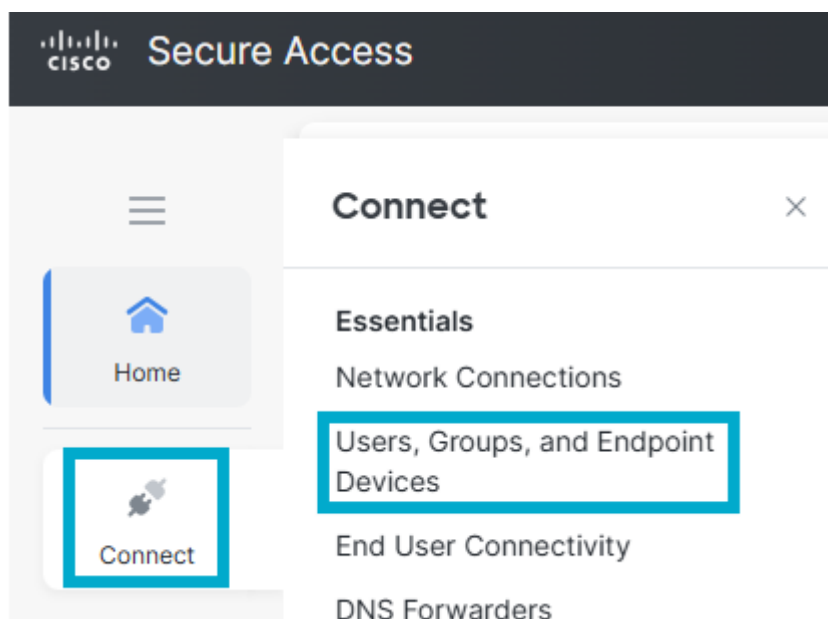


Anmerkung: Wenn Benutzer nicht im richtigen Format für den sicheren Zugriff bereitgestellt werden, stellen Sie sicher, dass Sie die Attributzuordnung wie [hier](#) angegeben konfigurieren.

Überprüfung

Verity in Cisco Secure Access

- Navigieren Sie zu Verbinden > Benutzer, Gruppen und Endgeräte.



Users and Groups in CSA

- Klicken Sie auf Benutzer.

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

- Klicken Sie auf Gruppen und Organisationseinheiten.

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**

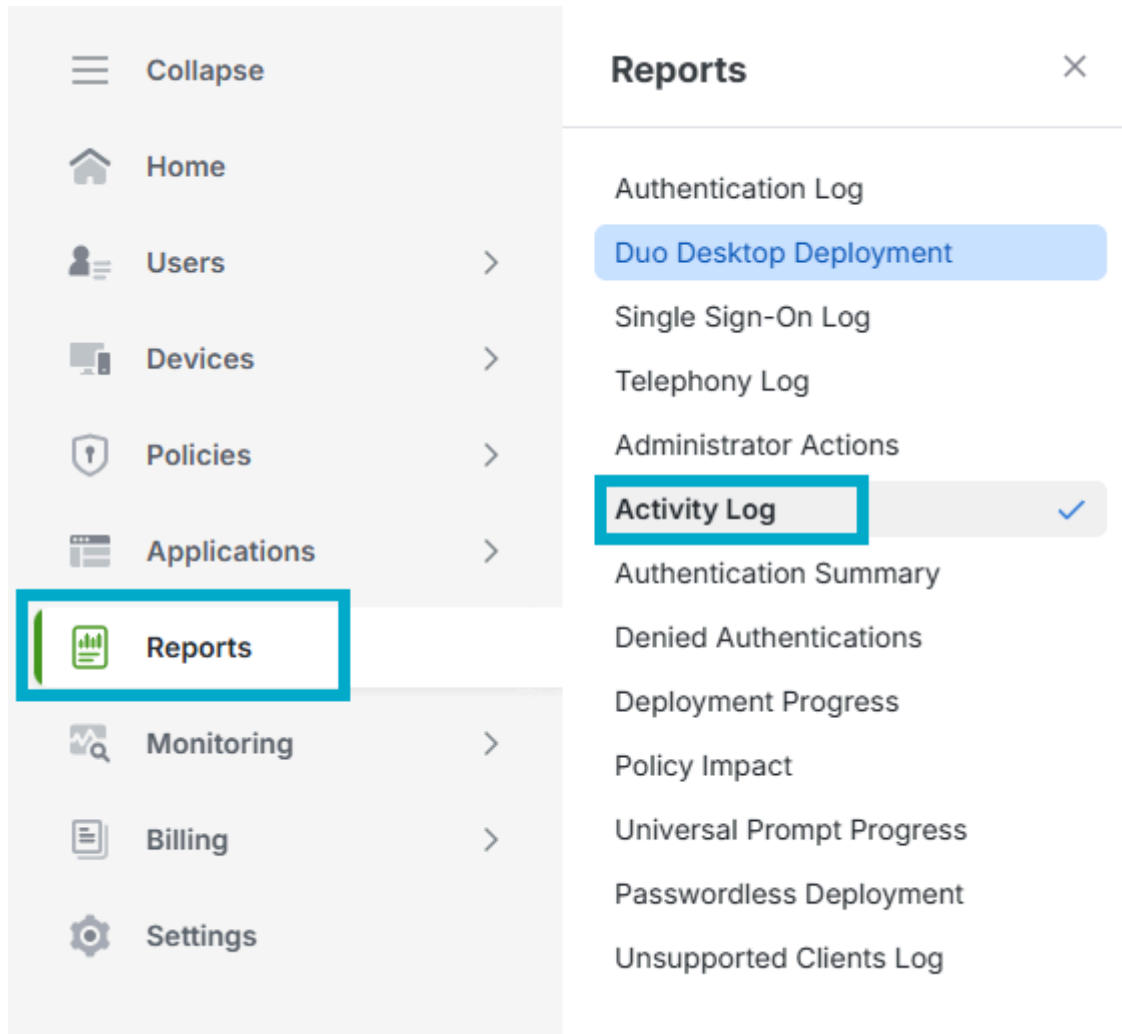
Search Type Source DUO Integration 1 results

Name	Type	Source	Directory
DUO - Users	Groups	Duo	DUO Integration

Verify Group in CSA

Verifizieren in DUO

- Navigieren Sie zu Berichte > Aktivitätsprotokoll.



Duo Activity Log

- Filtern Sie anhand des Namens der Anwendung.

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-Bereitstellungsprotokolle

Zugehörige Informationen

[Identitätsanbieter konfigurieren](#)

[Bereitstellung von Benutzern und Gruppen über Duo](#)

[Attributzuordnung \(erforderlich\)](#)

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.